Akadémia Policajného zboru v Bratislave
Katedra informatiky a manažmentu

Vedecká konferencia s medzinárodnou účasťou

Bezpečnosť elektronickej komunikácie 2024

Zborník príspevkov

Bratislava
2024

AKADÉMIA POLICAJNÉHO ZBORU V BRATISLAVE
Katedra informatiky a manažmentu

ZBORNÍK PRÍSPEVKOV

z vedeckej konferencie s medzinárodnou účasťou

Bezpečnosť elektronickej komunikácie

konanej dňa 07.05.2024

Bratislava 2024

Vedecký výbor konferencie:

doc. Ing. Stanislav ŠIŠULÁK, PhD. (Akadémia PZ v Bratislave)
pplk. JUDr. Michal MARKO PhD. (Akadémia PZ v Bratislave)
prof. Ing. Antonín KORAUŠ, PhD., LL.M., MBA (Akadémia PZ v Bratislave)
prof. JUDr. Jozef METEŇKO PhD. (Akadémia PZ v Bratislave)
pplk. doc. RNDr. Tatiana HAJDÚKOVÁ, PhD. (Akadémia PZ v Bratislave)
plk. gšt. v. z doc. Ing. Radoslav IVANČÍK PhD. et PhD., MBA, MSc. (Akadémia PZ v Bratislave)
plk. Ing. Mgr. Jana TKÁČIKOVÁ (Prezídium PZ
mjr. Mgr. Martin KAŠČÁK PhD. (Akadémia PZ v Bratislave)
doc. Ing. Martin KUCHTA, PhD., MBA (Obchodná fakulta, EUBA)

Organizačný výbor konferencie:

pplk. doc. RNDr. Tatiana HAJDÚKOVÁ, PhD.
mjr. Mgr. Martin KAŠČÁK PhD.
kpt. JUDr. Jana ZACHAR KUCHTOVÁ, PhD.
npor. JUDr. Miroslava DUBANOVÁ
por. Ing. Tomáš PETÁK
doc. Ing. Martin KUCHTA, PhD., MBA (Obchodná fakulta, EUBA)
Ing. Edita LUKÁČIKOVÁ
Mgr. Vladimíra HUDECOVÁ

Recenzenti:

prof. RNDr. Michal Greguš, CSc.

doc. Ing. Václav Friedrich, Ph.D.

doc. RNDr. Tatiana Hajdúková, PhD.

Zostavila:

kpt. JUDr. Jana Zachar Kuchtová, PhD.

© Akadémia Policajného zboru v Bratislave

Za odbornú a jazykovú stránku príspevkov zodpovedajú autori. Rukopis neprešiel jazykovou úpravou.

ISBN 978 – 80 – 8293 – 021 - 7
EAN 9788082930217

Obsah

Úvod ku konferencii *„Bezpečnosť elektronickej komunikácie 2024“*

Vedecká konferencia s medzinárodnou účasťou BEZPEČNOSŤ ELEKTRONICKEJ KOMUNIKÁCIE 2024 uskutočnená dňa 7.5.2024 bola tretím ročníkom konferencie, realizovanej v priestoroch Akadémie Policajného zboru v Bratislave. Tematickým zameraním konferencie zostáva bezpečnosť elektronickej komunikácie, jedno či v lokálnych počítačových sieťach, alebo na verejných sieťach internetu. Výstupom z konferencie je predložený recenzovaný zborník, ktorý obsahuje dohromady 20 príspevkov, prezentujúcich výsledky vedeckej a odbornej činnosti pracovníkov štátnej správy, akademického a podnikateľského sektora. Zastúpenie majú príspevky teoreticko-metodické, ktorých cieľom je predovšetkým osveta a prezentácia dôležitých aktuálnych fenoménov v oblasti bezpečnosti elektronickej komunikácie, ale aj príspevky aplikačné, prezentujúce nové výsledky výskumov alebo príkladov z praxe.

V oblasti elektronickej komunikácie sa už niekoľko rokov objavujú nové výzvy a bezpečnostné rizika, riešenie ktorých je spojené s viacerými aplikačnými problémami ako je nedostatočnosť regulácie, kontroly, ochrana súkromia, sloboda vyjadrovania sa, vymožiteľnosť práva, na ktoré reagovali viacerí prednášajúci. Jedným z významných negatívnych fenoménom posledných rokov, na ktoré taktiež reflektujú príspevky zborníka je šírenie dezinformácií, obzvlášť na sociálnych sieťach a to vrátane prejavov nenávisti. Iné príspevky reflektujú aj na nemenej závažné oblasti ako je ochrana dát, najmä citlivých či už osobných alebo firemných, ale i otázky v spojitosti s používaním kryptomien. Pozornosti neušla ani oblasť ochrany mäkkých cieľov, digitalizácia domácností a ochrana detí a mládeže pred negatívnymi vplyvmi elektronickej komunikácie. V poslednom období sa rezonuje nový fenomén – umelá inteligencia, ktorá môže byť nielen dobrým pomocníkom v rôznych oblastiach ľudskej činnosti, ale taktiež aj zneužitá na spoločensky nežiadúce činnosti. Vo všeobecnosti sa viacerí autori zhodli v potrebe osvety a vzdelávania v oblasti kybernetickej bezpečnosti používateľov elektronických zariadením, čo je jedným z hlavných cieľov stretnutí na konferencii. Dúfame, že zborník bude mať svojich priaznivcov a čitateľov nielen medzi priamymi účastníkmi konferencie, ale sprostredkuje podnetné témy aj tým, ktorí sa jej nestihli zúčastniť osobne. Spoznávanie je kontinuálny proces, obzvlášť nevyhnutný v dynamicky sa meniacich oblastiach, ku ktorým elektronická komunikácia patrí nielen v oblasti technológií, ale aj z pohľadu napredovania informatizácie spoločnosti, nárastu počtu používateľov moderných komunikačných prostriedkov ako aj dynamicky sa meniacom právnom vymedzení a nestabilnej

medzinárodnej situácii. Neustále sa objavujú nové výzvy a nové témy, ktoré musia riešiť profesionálni odborníci, ktoré sa ale dotýkajú aj bežných používateľov elektronických zariadení, ktorí by mali poznať reálne potenciálne riziká a spôsoby obrany a ochrany. Z tohto dôvodu cítime zmysluplnosť organizovania konferencie a potrebu jej pokračovania. Veríme, že vzhľadom na doterajšiu spätnú väzbu od participantov a účastníkov, konferencia s problematikou bezpečnosti elektronickej komunikácie bude mať svojich priaznivcov a pokračovanie aj v budúcnosti.

Vážime si a poďakovanie patrí všetkým prezentujúcim, ktorí aktívne vystúpili v programe konferencie a vytvorili tým kvalitu celej konferencie. Poďakovanie patrí každému účastníkovi konferencie, ktorý svojou účasťou vyjadril zvedavosť a záujem a tým dal zmysel konferencii. V neposlednom rade patrí poďakovanie spoluorganizátorom Ministerstvu investícií, regionálneho rozvoja a informatizácie SR zastúpené najmä prednášateľmi z vládnej jednotky pre riešenie počítačových incidentov v SR podľa zákona č.69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov CSIRT. SK, Obchodná fakulta Ekonomickej univerzity a spoločnosť SK-NIC., a.s. a celému organizačnému výboru najmä členom Katedry informatiky a manažmentu Akadémie Policajného zboru v Bratislave., ktorým prajem veľa pozitívnej energie pri príprave ďalšieho ročníka konferencie.

pplk. RNDr. Tatiana Hajdúková, PhD.

vedúca katedry informatiky a manažmentu na A PZ v Bratislave

Tematické zameranie konferencie

Hackli ma! Čo teraz?

Digitálna identita.

Ako sa chrániť pred útokmi na internete?

Ako sa správať bezpečne na sociálnych sieťach?

Dezinformácie a hoaxy – aký vplyv majú na dnešnú spoločnosť.

Digitálna gramotnosť a edukácia.

Spotrebiteľské správania na internete.

Program konferencie

Moderátorka hlavného prezentačného panela:

Ing. Denisa Bárdyová

Hovorkyňa policajného zboru

8,30 h-9,00 h Prezentácia účastníkov

9,00 h-9,10 h Otvorenie konferencie

Blok prednášok

9,10 h-9,40 h

Umelá inteligencia v kybernetickej bezpečnosti

prednášajúci: PhDr., JUDr. Mgr. Ervín, Šimko, MBA, LL.M.

Vládna jednotka CSIRT.SK, MIRRI

9,40 h-10,10 h

Umelá inteligencia v službách zla.

Prednášajúci: Mgr. Peter Košinár

ESET

10,10 h-10,30 h

Možnosti overovania digitálnych identít

Prednášajúci: Ing. Peter Bíro

SK-NIC, a.s.

10,30 h-10,50 h

Výzvy a úlohy MV SR pri riešení kybernetickej bezpečnosti

prednášajúci: Mgr. Zuzana Halásová, PhD.

Oddelenie kybernetickej bezpečnosti, sekcia informatiky, telekomunikácií a bezpečnosti MV SR

Prestávka na kávu 10,50 h-11,20 h

11,20 h-11,40 h

Aktuálne trendy kybernetické kriminality v Českej republike

prednášajúci: Ing. Bc. Hana Důbravová, Ph.D.

PA ČR v Prahe

11,40 h-12,00 h

Manažment zraniteľností v prostredí verejného internetu

prednášajúci: Ing. Alexander Valach, PhD.

Vládna jednotka CSIRT.SK, MIRRI

12,00 h-12,20 h

Cyber Arena

prednášajúci: Mgr. Marián Danko, PhD.

Vládna jednotka CSIRT.SK, MIRRI

12,20 h-12,40 h

Šírenie dezinformácií cestou sociálnych sietí – hrozba pre súčasnú demokratickú spoločnosť

Prednášajúci: doc. Ing. Radoslav Ivančík, PhD. et PhD., MBA, MSc.

Akadémia PZ v Bratislave

Prestávka na obed 12,40 h- 13,30 h

PROGRAM V SEKCIÁCH od 13,30 h do 15,00 h

SEKCIA A – miestnosť P5

Podobnosť sociálnych médií z hľadiska metrík šírenia dezinformácií

Prednášajúci: Dr. h. c. prof. JUDr. Lucia Kurilovská PhD, prof. RNDr. Beáta Stehlíková CSc., prof. Ing. Antonín Korauuš PhD., LL.M., MBA, RNDr. Kristián Ujváry, PhD.

.**Kryptomeny ako bezpečnostné riziko na finančnom trhu**

Prednášajúci: doc. RNDr. Tatiana Hajdúková, PhD.
Akadémia PZ v Bratislave

Umelá inteligencia a informačný chaos: Výzvy v boji proti dezinformáciám
Prednášajúci: JUDr. Jana Zachar Kuchtová, PhD.
Akadémia PZ v Bratislave

Útoky na školách – aktuálna bezpečnostná výzva
Prednášajúci: Mgr. Martin Kaščák, PhD.
Akadémia PZ v Bratislave

SEKCIA B – miestnosť U 110
Práva dotknutých osôb pri spracúvaní osobných údajov na internete
Prednášajúci: doc. JUDr. Miriam Odlerová, PhD.
Akadémia PZ v Bratislave

Spoľahlivosť generatívnej umelej inteligencie pri produkcii textového obsahu
Prednášajúci: doc. Ing. Martin Kuchta, PhD.
Akadémia PZ v Bratislave

Kybergrooming: Skrytá hrozba pre deti a mládeže
Prednášajúci: Ing. Tomáš Peták
Akadémia PZ v Bratislave

Bezpečnosť digitalizácie domácnosti
Prednášajúci: JUDr. Miroslava Dubanová
Akadémia PZ v Bratislave

Vybrané legislatívne možnosti regulácie šírenia dezinformácií

Branislav Belica

Abstrakt: V posledných rokoch sa šírenie dezinformácií stalo závažným problémom naprieč všetkými oblasťami spoločnosti počnúc politickým spektrom cez zdravotníctvo, vnútornú bezpečnosť, ekonomiku, až po otázky obrany a medzinárodných vzťahov. Nekontrolované rozširovanie nepravdivých, skreslených alebo úplne vymyslených informácií ohrozuje integritu verejnej diskusie a podkopáva základné princípy demokracie a spoločenskej súdržnosti. Ako reakciu na túto skutočnosť zákonodarcovia vo svete reflektujú potrebu reagovať na tento negatívny protispoločenský fenomén jeho legislatívnou úpravou. Zákonné nástroje boja proti dezinformáciám sa líšia najmä v dôsledku ohrozenia, ktoré môžu rozličné štáty vnímať odlišne. Aj preto sa autor, s využitím viacerých analyticko-syntetických prístupov a metód, vo svojom príspevku zaoberá problematikou vybraných legislatívnych možností regulácie šírenia dezinformácií v podmienkach Slovenskej republiky, pričom reflektuje aj na medzinárodnú iniciatívu vyvíjanú v podmienkach Európskej únie. V národných podmienkach sa zameriava na ústavnoprávny a trestnoprávny rámec regulácie dezinformácií. V podmienkach Európskej únie opisuje účinky novoprijatej legislatívy ktorá nadobudla úplnú účinnosť vo februári tohto roka.

Kľúčové slová: Dezinformácie, legislatíva, regulácia, demokratická spoločnosť, bezpečnosť.

Abstract: In recent years, the spread of disinformation has become s significant concern across various sectors of society, ranging from politics, through healthcare, national security, economics, up to national defence and international relationships. The unchecked spread of false, misleading or made up information poses threat to the integrity of public discourse but also undermines the basic principles of democracy and societal stability. As a response, policymakers around the globe have reflected the need to react by creating legislative tools to regulate this negative anti-social phenomenon. These tools differ by the level of threat, which is perceived individually by each state. That is also why the author in his contribution, using several analytical-synthetic approaches and methods, deals with the issue of selected legislative means to regulate disinformation in Slovak republic. Simultaneously, he reflects on the international initiative of the European union. In national conditions, it focuses on the constitutional and criminal law framework for the regulation of disinformation. In terms of the European Union, it describes the effects of the newly adopted legislation, which became fully effective in February of this year.

Keywords: Disinformation, legislation, regulation, democratic society, security.

Úvod

V modernej digitálnej dobe prechádzajú informačné kanály – využívané spoločnosťou – dynamickou transformáciou a vývojom. Tieto zmeny vplývajú aj na spôsoby a nástroje, akými

ľudia informácie vyhľadávajú a prijímajú. Spomínaný vývoj v oblasti moderných technológií nepochybne umožnil prístup k širokému rozsahu vedomostí a faktov. Taktiež vytvoril globálne prepojenie a vzájomnú výmenu informácií po celom svete. Vyše 65 % svetovej populácie má dnes prístup na internet a vyše 62 % využíva sociálne siete. Napriek už spomínaným benefitom sledujeme v období posledných rokov ich masívne zneužívanie na šírenie najrôznejších falošných správ, hoaxov, dezinformácií a propagandy.

Sociálna a politická polarizácia spoločnosti spojená s anonymitou na internete a sociálnych sieťach a ich nízkou reguláciou vytvára prostredie, ktoré ponúka ľahký prístup k potenciálnym obetiam bez veľkých rizík pre páchateľov. Najúčinnejším nástrojom šíriteľov falošných, zavádzajúcich, klamlivých, skreslených alebo úplne vymyslených informácií sa stali nepochybne sociálne siete a internet. Absencia schopnosti spoločnosti reagovať na rapídne zmeny v informačnom prostredí je zapríčinená najmä nedostatočnou digitálnou gramotnosťou, ktorá následne vytvára zraniteľnosť voči dezinformáciám.

Slovenská republika (ďalej len „SR“) v rámci tohto fenoménu nie je výnimkou. Podobne ako ostatné štáty, čelí škodlivým následkom dezinformačných kampaní, ktoré podkopávajú dôveru v štátne inštitúcie, rozkladajú spoločenskú súdržnosť a umocňujú rozdeľujúce názory medzi obyvateľmi.

Aj preto sa vyspelé štáty sveta začali zaoberať možnosťami regulácie nebezpečných dopadov dezinformácií, v rámci ktorých vyvinuli patričnú legislatívnu iniciatívu. Napriek tomu, že regulácia dezinformácií nie je iba otázkou legislatívnej úpravy, ide o dôležitý nástroj, ktorý je súčasťou širšieho balíka opatrení, ako sú strategická komunikácia a zvyšovanie odolnosti obyvateľstva prostredníctvom vzdelávania v oblasti digitálnej gramotnosti. Dôležitú úlohu pritom zohrávajú aj strategické dokumenty štátov a medzinárodných spoločenstiev.

V kontexte hierarchie usporiadania právnych predpisov má nepochybné prvenstvo Ústava Slovenskej republiky (ďalej len „Ústava). Východiská legislatívnej úpravy preto opisuje ústavnoprávny rámec, z ktorého ďalej vychádzajú nástroje trestnoprávnej a inej zákonnej regulácie šírenia dezinformácií. Netreba však zabúdať ani na medzinárodné organizácie, ktorých je SR členom. Európska únia (ďalej len „EÚ“) v boji proti dezinformáciám ako globálnej hybridnej hrozbe plní nezastupiteľnú úlohu. Jej dôležitosť spočíva najmä v spoločnom postupe národných štátov, ktorých individuálne snahy o reguláciu technologických gigantov s celosvetovým presahom sú oveľa efektívnejšie presadzované v rámci silného geopolitického celku, akým EÚ nepochybne je. Najväčší dopad na reguláciu

dezinformačného obsahu v kybernetickom priestore má nepochybne Digital Services Act (ďalej len „DSA“).

Regulácia šírenia dezinformácií prináša mnoho výziev najmä pri kreovaní právnych noriem. V rámci legislatívneho procesu sa objavuje množstvo právnych, etických a aplikačných otázok. Ide napríklad o pomer obmedzenia ľudských práv v kontexte spoločensky prospešného výsledku, dokazovanie nepravdivosti informácií či úmyslu páchateľa. Aj preto sa autor vo svojom príspevku s využitím relevantných metód vedeckého výskumu zaoberá vybranými legislatívnymi možnosťami regulácie šírenia dezinformácií v podmienkach Slovenskej republiky.

Ústavnoprávny a trestnoprávny rámec možnosti kontroly šírenia dezinformácií

Na to aby bolo možné efektívne regulovať dezinformácie je potrebné identifikovať legislatívny rámec, v ktorého medziach môžu štátne orgány a medzinárodné organizácie konať.

Ústava je základný právny dokument, ktorý upravuje princípy činnosti štátnych orgánov a definuje ústavné zásady, s ktorými nemôže byť žiadny zákon v rozpore. Častým argumentom subjektov šíriacich dezinformácie je potlačovanie ústavných práv, ako sú sloboda prejavu a právo na informácie. Dezinformátori však často ignorujú svoje vlastné povinnosti a tiež oprávnenia štátu voči nim. Ako prvý teda vysvetlíme ústavnoprávny kontext vo vzťahu k dezinformáciám. Medzi základné ustanovenia Ústavy patrí povinnosť štátnych orgánov konať v zmysle Ústavy a zákonov. Fyzické osoby však môžu konať všetko, čo nie je zákonom zakázané a povinnosti im možno ukladať len zákonom.

Opakujúcou sa obhajobou dezinformátorov je čl. 26 Ústavy, ktorý v prvom odseku zaručuje slobodu prejavu a právo na informácie. Druhý odsek stanovuje právo na vyjadrenie názoru a slobodné vyhľadávanie, prijímanie a rozširovanie ideí a informácií.

Čo sa však v rámci spomínanej argumentácie nespomína je ods. 4, ktorý hovorí: „Slobodu prejavu a právo vyhľadávať a šíriť informácie možno obmedziť zákonom, ak ide o opatrenia v demokratickej spoločnosti nevyhnutné na ochranu práv a slobôd iných, bezpečnosť štátu, verejného poriadku, ochranu verejného zdravia a mravnosti.“

Po Ústave je v rámci právneho poriadku SR dôležitým odvetvím trestné právo, ktoré má najväčší potenciál zasahovať do práv a slobôd pri naplnení skutkovej podstaty trestného činu uvedenej v Zákone č. 300/2005 Z. z. Trestný zákon (ďalej len „TZ“). Momentálne slovenská právna úprava nepozná skutkovú podstatu šírenia dezinformácií. Najbližšie má podstate šírenia

dezinformácií momentálne šírenie poplašnej správy v zmysle § 361 TZ nasledovne: „Kto úmyselne spôsobí nebezpečenstvo vážneho znepokojenia aspoň časti obyvateľstva nejakého miesta tým, že rozširuje poplašnú správu, ktorá je nepravdivá, alebo sa dopustí iného obdobného konania spôsobilého vyvolať také nebezpečenstvo“. Predmetná skutková podstata však vyžaduje škodlivý následok v podobe znepokojenia aspoň časti obyvateľstva nejakého miesta a je využívaná najmä na postihovanie páchateľov pri nahlasovaní výbušnín na určitom mieste. Dezinformácie vo svojej podstate však nie sú vždy šírené za účelom vyvolania znepokojenia a nie vždy nastane aj škodlivý následok.

V kontexte vojny na Ukrajine sa do mediálnej pozornosti dostalo aj trestné stíhanie vo veci ohrozenia mieru, ktorého sa dopustí osoba ak: „v úmysle narušiť mier akýmkoľvek spôsobom podnecuje k vojne, vojnu propaguje alebo inak podporuje vojnovú propagandu“.

Aplikovateľná je v istých prípadoch aj skutková podstata trestného činu ohovárania a podnecovania . Pri šírení extrémistických naratívov sa osoby môžu dopustiť trestného činu popierania a schvaľovania holokaustu a zločinov politických režimov , pričom môžu naplniť znaky skutkovej podstaty hanobenia národa, rasy a presvedčenia či podnecovania k národnostnej, rasovej a etnickej nenávisti.

V kontexte širokého okruhu dezinformácií pripadajú do úvahy aj iné skutkové podstaty. Ešte v roku 2021 bola zo zákonodarného zboru predložená iniciatíva, na vznik novej skutkovej podstaty šírenia nepravdivých informácií. Skutková podstata tohto trestného činu mala byť: „výroba alebo rozširovanie vedome nepravdivej informácie, ktorá je spôsobilá vyvolať nebezpečenstvo vážneho znepokojenia aspoň časti obyvateľstva nejakého miesta, ohroziť životy alebo zdravie ľudí alebo ovplyvniť obyvateľstvo pri jeho rozhodovaní o závažných otázkach celospoločenského významu“.

Táto skutková podstata bola kritizovaná viacerými odborníkmi z oblasti práva, pričom sa kritizovala najmä nejasnosť a vágnosť skutkovej podstaty, ktorá mohla vytvárať podmienky na svojvoľnú a účelovú interpretáciu, čo mohlo byť v rozpore s princípom právnej istoty.

Navrhovaná novela nebola schválená a momentálne sa v rámci tejto oblasti podľa dostupných informácií nepripravujú zmeny napriek schválenej novele Trestného zákona zo dňa 8.2.2024, ktorá v tejto súvislosti nenadväzuje na iniciatívu vzniku novej skutkovej podstaty. V prípade opätovnej iniciatívy navrhujeme znenie novej skutkovej podstaty nasledovne:

„(1) Kto vyrobí alebo rozširuje zjavne nepravdivú alebo skreslenú informáciu v úmysle vydávať ju za pravú, ktorá:

a) ohrozuje život alebo zdravie viacerých osôb,

b) je spôsobilá vyvolať nebezpečenstvo škody veľkého rozsahu na majetku štátu, majetku obce, majetku vyššieho územného celku alebo majetku verejnoprávnej inštitúcie,

c) je spôsobilá poškodiť ústavné zriadenie Slovenskej republiky,

d) je spôsobilá ovplyvniť viaceré osoby pri výkone ich volebného práva,

e) je spôsobilá vyvolať nebezpečenstvo vážneho znepokojenia aspoň časti obyvateľstva nejakého miesta.“

Potrebné by však bolo aj prijať definíciu zjavne nepravdivej alebo skreslenej informácie, ktorá by mohla znieť nasledovne: „Zjavne nepravdivou informáciou alebo skreslenou informáciou sa na účely tohto zákona rozumie informácia, ktorá je v súlade s dosiahnutým stavom poznania preukázateľne nepravdivá.“

Uvedený návrh reflektuje na niektoré pripomienky odbornej verejnosti najmä vo vzťahu k nasledujúcim faktorom. V prvom rade v zmysle princípu ultima ratio definuje úmyselné zavinenie, čím predchádza trestaniu obetí dezinformácií. Ďalej definuje zjavne nepravdivú informáciu alebo skreslenú informáciu v zmysle dosiahnutého stavu poznania a preukázateľnej nepravdivosti. Ako príklad využijeme nasledovnú dezinformáciu: „vakcíny proti ochoreniu Covid-19 spôsobujú zvýšené riziko infarktu“. Na vyhodnotenie tejto dezinformácie ako nepravdivej v súlade s dosiahnutým stavom poznania je možné ako dôkaz použiť vedeckú štúdiu z Austrálie, ktorá bola vykonaná na analýze dát 6,5 milióna obyvateľov štátu Victoria a vyslovuje záver, že nie je žiadne prepojenie medzi infarktmi a vakcináciou proti ochoreniu Covid-19. V tomto prípade by bol uplatniteľný odsek a): „ohrozuje život alebo zdravie viacerých osôb“, ktorý je možné preukázať medzi príčinnou súvislosťou dát medzi úmrtnosťou očkovaných a neočkovaných pacientov. Ako dôkaz je možné použiť napríklad štúdiu vykonanú na 21 618 297 pacientoch s ochorením Covid-19 a ich úmrtnosti v kontexte zaočkovania, kde bolo preukázané, že nezaočkovaní pacienti mali 2,46 násobne vyššiu šancu zomrieť v dôsledku predmetného ochorenia.

Okrem opísania škodlivého následku vo forme ohrozenia života a zdravia, opisuje návrh iba škodlivé následky, voči ktorým už TZ plní ochrannú funkciu pri iných trestných činoch. Objektom pri navrhovanej skutkovej podstate je najmä život a zdravie ľudí. Vychádzajúc

z princípu ultima ratio sme ďalej objekt vymedzili v úmysle chrániť štát pred hybridnými hrozbami, ktoré využívajú dezinformácie ako ich nástroj. Ich cieľom je oslabiť či poškodiť štát a pomôcť presadiť strategické ciele a záujmy cudzieho nepriateľského štátneho či neštátneho aktéra.

V zmysle Ústavy je možné využiť zákonné obmedzenia ako opatrenia v demokratickej spoločnosti nevyhnutné na ochranu práv a slobôd iných, bezpečnosť štátu, verejného poriadku, ochranu verejného zdravia a mravnosti.

Pri navrhovanej skutkovej podstate vychádzame aj z názorov odborníkov, ktoré sa zhodujú v tom, že najškodlivejšími následkami dezinformácií ako súčasti hybridných hrozieb voči štátu je najmä jeho celkové oslabenie vo forme ohrozenia života a zdravia obyvateľstva, vysokých ekonomických škôd, narušenia demokratického systému základných práv a slobôd, ovplyvňovania procesu volieb alebo vyvolania vážneho znepokojenia obyvateľstva, ktoré môže vyústiť až do zníženia dôveryhodnosti rôznych štátnych orgánov a ohrozenia verejného poriadku.

Hoboken a Fathaigh uvádzajú, že kriminalizácia šírenia dezinformácií nie je v rámci členských štátov EÚ ničím ojedinelým. Podobné ustanovenia je možné nájsť v trestných kódexoch Malty, Litvy, Rakúska, Grécka a Poľska.

Cieľom navrhovanej skutkovej podstaty by nebolo trestať šíriteľov akýchkoľvek dezinformácií, ale iba ich najzávažnejšie a jednoznačne preukázateľné formy. Navrhovaná skutková podstata by plnila preventívnu, represívnu aj ochrannú funkciu voči spoločnosti. Otázka výšky trestov by musela byť primeraná škodlivým následkom, pričom v menej závažných prípadoch by postačoval aj trest zákazu činnosti. V rámci vecnej príslušnosti by sa však touto problematikou muselo zaoberať špecializované pracovisko určené na vyšetrovanie kybernetickej kriminality v spolupráci so spravodajskými a analytickými zložkami štátu, a to najmä z toho dôvodu, že vyšetrovanie a dokazovanie úmyslu a škodlivého následku v súvislosti s navrhovaným trestným činom by bolo obzvlášť náročné. Aj preto by sa týmto spôsobom postihovali iba konania, kde by bol jednoznačne preukázaný úmysel a potenciálny škodlivý následok, ktorý má merateľné kritériá v zmysle už existujúcej trestnej legislatívy. Účelom tohto návrhu však nie je jeho aplikácia, ale reflektovanie niektorých verejných pripomienok a iniciácia odbornej diskusie o potrebe podobného ustanovenia či jeho konkrétnej podobe.

Nástroje boja Európskej únie proti dezinformáciám

V rámci EÚ taktiež existujú mechanizmy regulácie dezinformačného obsahu. Ide o rozhodnutia Rady EÚ a európsku legislatívu (najmä DSA), ktoré sú aplikované vo všetkých členských štátoch.

Rada EÚ má v kompetencii zakázať vysielacie činnosti médií. V súvislosti s vojnou na Ukrajine išlo o reštriktívne opatrenia voči vysielacej činnosti médií Sputnik a Russia Today do ukončenia agresie voči Ukrajine a dovtedy, kým Ruská federácia a jej pridružené média neprestanú vykonávať dezinformačné aktivity a akcie zamerané na ovplyvňovanie verejnej mienky a manipuláciu informácií namierenými proti EÚ a jej členským štátom. Napriek snahám ruskej televízie RT o napadnutie rozhodnutia na Súdnom dvore Európskej únie tribunál Súdneho dvora potvrdil zákaz vysielania pre systematické dezinformácie. Samotné vynútenie blokovania dezinformačných webov však v praxi nie je jednoduché. To dokazuje aj fakt, že v niektorých členských štátoch EÚ sú tieto kanály dva roky po ich zablokovaní stále dostupné. Problém je v implementácií rozhodnutia na úrovni národných štátov, v rámci ktorých je potrebné požiadať všetkých poskytovateľov internetových služieb o blokovanie predmetných webov.

17. februára 2024 sa začal uplatňovať DSA na všetky online platformy v rámci EÚ. Tento právne záväzný dokument upravuje práva používateľov online platforiem a povinnosti ich prevádzkovateľov. Rovnako ustanovuje aj sankcie v prípade porušenia týchto povinností až do výšky 6 % ročného obratu prevádzkovateľa. V rámci výkonu kontroly ustanovuje Európsku komisiu ako orgán, ktorý má právo vo veciach porušenia DSA viesť vyšetrovanie a ukladať sankcie.

DSA prináša prísnejšiu reguláciu online platforiem najmä prostredníctvom uloženia povinností, v dôsledku porušenia ktorých môže prísť k uloženiu sankcie. Medzi povinnosti ktoré DSA ukladá patrí, v súvislosti s reguláciou dezinformácií, povinnosť vytvoriť možnosť používateľom nahlásiť protiprávny obsah. Na túto oblasť sa vytvárajú takzvaní „overení nahlasovatelia“, ktorých hlásenia budú vybavované prioritne. Uvádza sa však povinnosť vybavovať všetky nahlásené príspevky aktívne a dôsledne. V rámci ochrany detí vo virtuálnom priestore sa ukladá zákaz cielenej reklamy voči maloletým. V oblasti online marketingu, ktorý môže byť zneužitý aj na šírenie dezinformácií je potrebné uviesť dôvod, prečo používatelia vidia konkrétnu reklamu a kto je jej objednávateľom. Zároveň vzniká pre používateľa možnosť zakázať profilovanie a reklamné odporúčania vytvárané na jeho základe. V oblasti cielenej

reklamy sa účinnosťou DSA uplatňuje zákaz využívania citlivých údajov (vierovyznanie, politické preferencie, sexuálna orientácia) na marketingové účely.

Na redukciu neoprávneného blokovania názorových oponentov, vzniká povinnosť uviesť dôvod obmedzenia činnosti (odstránenia obsahu, blokácia účtu a podobne) a vytvorenie možnosti odvolania voči tomuto rozhodnutiu.

Z hľadiska implementácie je zaujímavá najmä povinnosť prijať opatrenia, ktoré reagujú na riziká spojené so šírením nezákonného obsahu a negatívnych dôsledkov na slobodu prejavu a práva na informácie. Rovnako však až aplikačná prax ukáže, ako budú poskytovatelia digitálnych služieb reagovať na povinnosť analyzovať špecifické riziká a prijať eliminačné opatrenia voči šíreniu dezinformácií a neautentickému používaniu ich služby.

Záver

Na záver možno konštatovať, že potreba regulácie šírenia dezinformácií legislatívnymi nástrojmi na národnej i nadnárodnej úrovni sa v poslednej dobe ukazuje ako veľmi zásadná. Tieto nástroje majú potenciál redukovať negatívne dôsledky šírenia dezinformácií, avšak je dôležité opatrne pristupovať voči citlivej hranici medzi zachovaním slobody prejavu a ochranou verejného záujmu. Ústava SR jednoznačne oprávňuje štátne orgány v zmysle zákona obmedziť niektoré práva občanov za účelom ochrany práv a slobôd iných, bezpečnosti štátu, verejného poriadku, ochrany verejného zdravia a mravnosti. Možnosti zákonodarcu sú teda v tomto ohľade pomerne široké.

Trestná politika štátu musí tiež reagovať na výzvy spojené s digitálnou dobou. V minulosti bola predmetom verejnej diskusie aj trestnoprávna úprava šírenia nepravdivých informácií. Návrh na vytvorenie novej skutkovej podstaty bol do značnej miery kritizovaný a odmietnutý en bloc bez odporúčaní ako ho zlepšiť. Prostriedky trestnoprávnej regulácie by mali byť v demokratickej spoločnosti využívané iba ako posledná možnosť v prípade, že ostatné nástroje nie sú účinné. Aj preto sme sa v zmysle tejto zásady pokúsili navrhnúť takú skutkovú podstatu, ktorá by mohla iniciovať ďalšiu diskusiu o trestnoprávnej regulácií šírenia dezinformácií v konkrétnych prípadoch, ktoré majú potenciál mať devastačné následky v dôsledku úmyselného konania. Tejto problematike by sa mali venovať pri potenciálnej implementácií obdobného trestného činu analytické a spravodajské zložky štátu v spolupráci s centralizovanými špecializovanými policajnými útvarmi vyšetrujúcimi kybernetickú kriminalitu.

Naše členstvo v EÚ nám odomyká ďalšie legislatívne možnosti ochrany proti dezinformáciám. Európske inštitúcie sa v súvislosti s vojenskou agresiou Ruskej federácie voči Ukrajine napríklad rozhodli blokovať niektoré ruské štátne média, čo sa ukázalo ako legitímne v zmysle rozhodnutí súdnych sporov v tejto veci. Okrem týchto kompetencií EÚ ďalej podniká kroky k znižovaniu negatívnych dopadov šírenia dezinformácií aj vytváraním legislatívneho rámca, ktorý upravuje povinnosti poskytovateľov digitálnych služieb. V tomto smere hrá významnú úlohu DSA, ktorý je silným nástrojom regulácie obsahu internetu a najmä sociálnych sietí. Sme presvedčení, že problematike aplikácie DSA, jej prínosom a nedostatkom sa ďalej bude venovať odborná verejnosť. Až samotná aplikačná prax odhalí efektivitu prijatých opatrení. Legislatívna úprava povinností online platforiem na úrovní EÚ je veľmi významná, a to najmä kvôli jednotnosti pravidiel pre gigantické technologické spoločnosti v európskom priestore. Iba spoločným koordinovaným postupom členských krajín EÚ je možné docieliť efektívnu reguláciu dezinformačného obsahu prostredníctvom internetu, ktorý nepozná hranice. Aj preto je dôležité medzinárodné úsilie, ktoré v spojení s iniciatívami národných štátov vytvára ucelený komplex nástrojov boja proti dezinformáciám.

Zoznam použitej literatúry

ARCURI, M. - GANDOLFI, G. - RUSSO, I. 2023. Does fake news impact stock returns? Evidence from US and EU stock markets. In Journal of Economics and Business, 2023 [online] [cit. 02.03.2024]. Dostupné na internete: <https://lnk.sk/jgy1>.

BORGES DO NASCIMENTO I. – PIZARRO, A. – ALMEIDA, J. - AZZOPARDI-MUSCAT, N. - GONÇALVES, M. – BJÖRKLUND, M. - NOVILLO-ORTIZ, D. 2022. Infodemics and health misinformation: a systematic review of reviews. In Bull World Health Organ, 2022. [online] [cit. 02.03.2024]. Dostupné na internete: <https://lnk.sk/ta34>.

CBHH. 2024. Čo znamená pojem hybridné hrozby? In Hybridné hrozby na Slovensku, 2024. [online] [cit. 09.03.2024]. Dostupné na internete: <https://lnk.sk/iw89>.

DREVENÁ, K. 2022. Bádateľ naďalej dezinformuje o vakcínach proti Covid-19. In CEDMO, 2022. [online] [cit. 01.03.2024]. Dostupné na internete: < https://lnk.sk/qfm8>.

EURÓPSKA KOMISIA. 2024. The Digital Services Act. In European Commission, 2024 [online] [cit. 10.03.2024]. Dostupné na internete: <https://lnk.sk/inn4>.

EUROPEAN COMISSION. 2024. Digital Services Act starts applying to all online platforms in the EU. In European Commission, 2024. [online] [cit. 03.03.2024]. Dostupné na internete: <https://lnk.sk/hqf8>.

EUROPEAN COMISSION. 2024. DSA: Making the online world safer. In European Commission, 2024. [online] [cit. 03.03.2024]. Dostupné na internete: <https://lnk.sk/aml3>.

EUROPEAN COMISSION. 2024. The enforcement framework under the Digital Services Act. In European Commission, 2024. [online] [cit. 03.03.2024]. Dostupné na internete: <https://lnk.sk/equp>.

GALEOTTI, A. Political Disinformation and Voting Behavior: Fake News and Motivated Reasoning. In notizie di POLITEIA, 2020. [online] [cit. 02.03.2024]. Dostupné na internete: <https://lnk.sk/ybe5>.

GJERAQINA, T. Two Years Into EU Ban, Russia's RT And Sputnik Are Still Accessible Across The EU. In RadioFreeEurope, 2024. [online] [cit. 03.03.2024]. Dostupné na internete: <https://lnk.sk/styj>.

HOBOKEN, J, - FATHAIGH, R. 2021. Regulating Disinformation in Europe: Implications for Speech and Privacy. In UC Irvine Journal of International, Transnational and Comparative Law, 2021. [online] [cit. 02.03.2024]. Dostupné na internete: <https://lnk.sk/bpqh>.

IKEOKWU, A. – LAWRENCE, R. – OSIEME, E. – GIDADO, K. – GUY, C. – DOLAPO, O. Unveiling the Impact of COVID-19 Vaccines: A Meta-Analysis of Survival Rates Among Patients in the United States Based on Vaccination Status. In Cureus, 2023. [online] [cit. 01.03.2024]. Dostupné na internete: <https://lnk.sk/nryx>.

HAJDÚKOVÁ, T. – KURILOVSKÁ, L. – MARR, S. 2023. Riziká komunikácie na sociálnych sieťach. In Zborník z konferencie RELIK 2023: Reprodukcia ľudského kapitálu – vzájomné väzby a súvislosti, 2023, s. 58-69. ISBN 978-80-245-2499-3.

HAJDÚKOVÁ, T. – ŠIŠULÁK, S. 2022. Abuse of modern means of communication to manipulate public opinion. In INTED 2022 – Proceedings from 16th International Technology, Education and Development Conference. IATED Spain, 2022, s. 1992-2000. ISBN 978-84-09-37758-9.

IVANČÍK, R. – MÜLLEROVÁ, J. 2022. Dezinformácie ako hybridná hrozba šírená prostredníctvom sociálnych sietí. In Policajná teória a prax, 2022, roč. 30, č. 3, s. 22-42. ISSN 1335-1370.

IVANČÍK, R. 2022. Kybernetická (ne)bezpečnosť a sociálne siete. In Aktuálne výzvy kybernetickej bezpečnosti: zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou. Bratislava: Akadémia Policajného zboru, 2022, s. 35-46. ISBN 978-80-8054-998-5.

IVANČÍK, R. 2023. On Disinformation and Propaganda in the Context of the Spread of Hybrid Threats. In Vojenské reflexie, 2023, roč. 18, č. 3, s. 38-58. ISSN 1336-9202.

KUCHTOVÁ, J. 2018. Aktuálne trendy súvisiace s využívaním moderných technológií. In Aktuálne výzvy kybernetickej bezpečnosti – zborník príspevkov z vedeckej konferencie s medzi-národnou účasťou. Bratislava : Akadémia Policajného zboru, 2018, s. 90-98. ISBN 978-80-8054-773-8.

MINISTERSTVO SPRAVODLIVOSTI SR. 2021. Meníme Trestný zákon: K slabším miernejší, k silnejším prísnejší. In justice.gov.sk, 2021. [online]. [cit. 04.03.2024]. Dostupné na internete: < https://lnk.sk/hqo2>.

PARATZ, E. – NEHME, Z. – STUB, D. – LA GERCHE, A. No Association Between Out-of-Hospital Cardiac Arrest and COVID-19 Vaccination. In Circulation, 2023.

[online] [cit. 01.03.2024]. Dostupné na internete: <https://lnk.sk/sgmq>.

RADA EÚ. 2022. EÚ uložila sankcie štátnym médiám RT/Russia Today a Sputnik s vysielaním v EÚ. In European Council, 2022 [online] [cit. 05.03.2024]. Dostupné na internete: <https://lnk.sk/ualv>.

RTVS. 2022. Tribunál Súdneho dvora EÚ potvrdil zákaz vysielania ruskej televízie RT. In Správy RTVS, 2022. [online] [cit. 05.03.2024]. Dostupné na internete: <https://lnk.sk/xgik>.

ŠAMKO, P. 2021. Zákaz diskusie ako trestný čin. In Právne listy, 2021. [online]

[cit. 04.03.2024]. Dostupné na internete: <https://lnk.sk/ixp6>.

SOPOLIGA, J. 2021. Trestnoprávna zodpovednosť za šírenie nepravdivých informácií. In Právne listy, 2021. [online] [cit. 04.03.2024]. Dostupné na internete: <https://lnk.sk/daqt>.

TASR. 2021. Žilinka: Nový trestný čin šírenie nepravdivej informácie je nenáležitý. In Teraz.sk, 2021. [online] [cit. 04.03.2024]. Dostupné na internete: <https://lnk.sk/ufw8>.

ZACHAR KUCHTOVÁ, J. 2022. Bezpečnosť na sociálnych sieťach. In Bezpečnosť elektronickej komunikácie : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou. Bratislava: Akadémia Policajného zboru, 2022, s. 237-247. ISBN 978-80-8054-968-8.

Zákon č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov.

Zákon č. 460/1992 Z. z. Ústava Slovenskej republiky.

Kontaktné údaje

JUDr. Branislav Belica
Ministerstvo obrany Slovenskej republiky
Kutuzovova 8, 832 47 Bratislava
e-mail: belica1996@gmail.com

Recenzenti:

prof. RNDr. Michal Greguš, CSc.
doc. RNDr. Tatiana Hajdúková, PhD.

Vplyv hoaxov na spoločnosť

Miroslav Benko

Abstrakt: Hoaxy majú v dnešnej dobe veľký vplyv na spoločnosť. Tieto klamlivé informácie sa rýchlo šíria prostredníctvom sociálnych médií a môžu viesť k dezinformácii, strachu alebo dokonca nenávisti. Dôsledky hoaxov môžu byť veľmi škodlivé, pretože môžu ovplyvniť verejnú mienku, politické rozhodnutia alebo dokonca spoločenskú stabilitu. Je dôležité, aby sme si boli vedomí toho, ako hoaxy ovplyvňujú našu spoločnosť a ako sa chrániť pred ich škodlivými následkami.

Kľúčové slová: hoax, informácia, dezinformácia

Abstract: Hoaxes have a big impact on society these days. This misinformation spreads quickly through social media and can lead to misinformation, fear or even hatred. The consequences of hoaxes can be very damaging as they can affect public opinion, political decisions or even social stability. It is important that we are aware of how hoaxes affect our society and how to protect ourselves from their harmful consequences.

Key words: hoax, information, misinformation

Úvod

S plynutím času sa technologické prostriedky na komunikáciu rýchlo rozvíjajú a inovujú. Sociálne médiá sa tak stávajú čoraz dôležitejším prvkom v každodennom živote. Ich vplyv nie je možné prehliadnuť, keďže majú schopnosť ovplyvňovať názory a správanie jednotlivcov aj skupín v spoločnosti. Tento silný nástroj môže mať pozitívny vplyv, ale zároveň môže viesť k šíreniu nepravdivých informácií, čo môže mať za následok negatívne konanie.

Najzraniteľnejšou skupinou sú mladí ľudia, ktorí sú otvorení novým informáciám a ľahko ovplyvniteľní. Vďaka množstvu dostupných informácií je pre nich ťažké rozlišovať pravdu od klamstva, čo môže viesť k negatívnym dôsledkom. Tento vplyv môže byť viditeľný nielen na individuálnej úrovni, ale aj vo forme radikalizácie a neprijateľného správania voči rôznym komunitám a skupinám obyvateľstva.

Celkový vplyv sociálnych médií a technológií na spoločnosť môže viesť k radikalizácii a polarizácii názorov a postojov. Je dôležité byť kritický voči informáciám a vedome ovplyvňovať svoje správanie, aby sme predišli negatívnym dôsledkom, ktoré by mohli ovplyvniť celú spoločnosť.

Definície a význam slova HOAX

Vymedziť obdobie, kedy vznikol pojem pre opísanie typu klamlivej správy - hoaxu, nie je jednoduché, keďže rôzne zdroje často uvádzajú rôzne informácie. V Oxfordskom slovníku bol termín hoax pridaný až začiatkom 29. storočia, tj. v časoch industrializácie[1], avšak jeho história siaha pravdepodobne trochu ďalej. Podľa Nutila mohol pojem vzniknúť o storočie skôr, zo slovného spojenia „hocus pocus“, ktoré sa bežne používalo pri pokusoch o oklamanie publika trikmi, prezlečenými za čary.[2] Definície termínu „hoax“ sú dohľadateľné vo viacerých slovníkoch. Vzhľadom na to, že termín sa do verejného povedomia výraznejšie dostal až nedávno, ich prepracovanosť nie je na vysokej úrovni, sú nejednoznačné a v mnohých bodoch sa rozchádzajú.

Termíny sú definované najmä v slovníkoch onlinových. Onlinový slovník Cambridge dictionary definuje „hoax“ ako „plán zavádzať niekoho, napr. informovať políciu o umiestnení bomby bez toho, aby bomba v danom prípade reálne existovala. (Cambridge Advanced Learner´s Dictionary and Thesaurus 2024)“. Onlinový slovník Merriam-Webster (2024), definuje hoax nasledovne: „Hoax je čin mierený na zavádzanie niekoho či podvádzať.“ Ten istý slovník navyše prináša definíciu termínu „hoax“ ako slovesa tzn. anglického „to hoax“, čo by sa do slovenského jazyka dalo voľne preložiť ako „hoaxovať“. Definícia „hoaxovania“ znie: „primäť niekoho veriť v niečo alebo primäť ho k akceptovaniu niečoho, čo je v skutočnosti nepravda a je často absurdné.“ Šnídl (2017) v slovníku pojmov definuje hoax nasledovne: „Pôvodne sa takto označovala poplašná správa, ktorá sa posiela mailom, dnes sa takto nazýva podvrh/klamstvo šírené sociálnymi sieťami. Môže mať žartovný, ale aj politický charakter.

Vo všeobecnosti možno konštatovať, že jednotlivé definície nám ukazujú smer, ktorým sa termín hoax uberá t.j., že informácia ním obsiahnutá zavádza. Obsah definícii je však strohý a nevymedzuje hoax presne. Možno tvrdiť, že bez predchádzajúceho uchopenia termínu ešte pred čítaním jednotlivých definícií, by si čitateľ len ťažko vytvoril svoje chápanie pojmu a dekódoval informácie obsiahnuté v nich. Definície napríklad nijako nediferencujú hoax od prostého klamstva. Podľa definície Merriam-Webster hoaxu ako slovesa, by „hoaxovaním“ bolo aj nezámerne predanie mylných informácii o čase začiatku prednášky, kde sa dá polemizovať, či ide vôbec o klamstvo.

[1] OXFORD DICTIONARIES: Oxford Dictionary of English, Oxford University Press, 2012
[2] NUTIL, P.: Média, lži a příliš rychlý mozek. 1. vydanie, Brno: Grada, 2018

Slovo "hoax" označuje klamlivú správu alebo dezinformáciu, ktorá sa šíri s cieľom oklamať verejnosť. V dnešnej digitálnej dobe majú hoaxové správy obrovský dosah vďaka rýchlemu šíreniu prostredníctvom sociálnych médií a internetu. Dôležité je naučiť sa rozpoznávať hoax a overovať si informácie predtým, než ich budeme šíriť ďalej. Spoločnou snahou by mala byť podpora kritického myslenia a zodpovedného zdieľania obsahu, aby sme minimalizovali škodlivé následky hoaxov na našu spoločnosť.

Účel hoaxov

Hoaxy sú vytvárané s cieľom ovplyvniť názory nielen jednotlivcov, ale aj skupín, ba dokonca aj celej spoločnosti. Hlavným cieľom je však aj odozva v ich konaní podľa zámeru klamlivej informácie. K charakteristickým znakom hoaxov patria vyhlásenia, že nie sú hoaxom a zakladajú sa na pravde, varujú pred neexistujúcim nebezpečenstvom, obsahujú výzvu na ďalšie šírenie, využívajú Caps Lock, odvolávajú sa na autority resp. verejne známe osoby, typické pre ne je tiež veľa výkričníkov či otáznikov a vyznačujú sa tiež zlou gramatikou. Zatiaľ čo autori a šíritelia iných foriem klamlivých informácií ich vymýšľajú tak , aby odolali najvyššiemu stupňu kontroly, hoaxeri sú si istí, že ich podsunuté správy nebudú podrobené žiadnej kontrole. Niektorí autori hoaxov majú nakoniec v úmysle aj demaskovať svoje vyjadrenia ako podvod, aby odhalili svoje obete ako bláznov, iní hoaxeri dúfajú , že hoax udržia donekonečna, takže až keď skeptickí ľudia ochotní prešetriť ich tvrdenia zverejnia svoje zistenia, nakoniec budú odhalení ako podvodníci. Hoaxy sa na internete stávajú bežným javom a ich obsah môže byť rôzny, podobne aj následné odozvy na nich. Odozva môže spočívať v negatívnom ba až zradikalizovaným konaní či pasívnej rezistencii.

Hoaxy zvyknú varovať pred hroziacim nebezpečenstvom, pred spoplatnením často používaných služieb, žiadajú o pomoc v núdzi alebo sľubujú šťastie, či peniaze za zdieľanie príspevku. Žiadna z informácií, ktorá sa v nich nachádza však nie je pravdivá. (Sekerák, 2020)

Vnímanie hoaxov mladými ľuďmi

Postupom času komunikačné technológie a platformy napredujú čoraz vyšším tempom a neustále sa vyvíjajú. Tak sa masmédiá stávajú čoraz vplyvnejším faktorom modernej spoločnosti. Je to silný nástroj, ktorý má silný vplyv na obyvateľstvo ako celok, ale aj na určité skupiny obyvateľstva, hlavne na mladú generáciu. V modernej spoločnosti majú masmédiá schopnosť nielen formovať názory, ale aj ovplyvňovať konanie nielen jednotlivcov či skupín,

ale aj celej spoločnosti. Ak sa jedná o pozitívne pôsobenie, tak je to v poriadku. Horšia situácia nastáva, keď v prípade klamlivých informácií sú výsledkom negatívne názory a negatívne konanie. Najohrozenejšou skupinou je v tomto smere mladá generácia. Je totiž viac zvedavá a ľahko ovplyvniteľná. Vzhľadom k stále sa zvyšujúcemu množstvu informácií a životným skúsenostiam, nedokáže táto generácia potom vyhodnocovať a identifikovať stále narastajúce množstvo klamlivých informácií. To následne môže vyústiť do negatívneho konania nielen jednotlivcov, ale aj ku radikalizácií určitých skupín a ich verbálnym či fyzickým útokom proti komunitám LGBT, rómov, židov, imigrantov, iných národov či rás, náboženských vierovyznaní a iného politického presvedčenia. To všetko môže vytvárať nielen nové kultúry, ale môže tiež do určitej miery meniť aj životný štýl formovaním názorov a pozícií a to nielen v pozitívnom, ale aj nežiaducom negatívnom smere. V konečnom štádiu to môže nakoniec viesť až ku polarizácii celej spoločnosti.

Mediálna gramotnosť

Mediálna gramotnosť je potrebným vybavením spoločnosti, aby vedela kriticky hodnotiť informačný prísun médií a to nielen masových. Najčastejšie používanou definíciou je: „Mediálna gramotnosť je schopnosť prijímať, analyzovať, hodnotiť a vytvárať médiá v rôznych formách.“[3]. Táto definícia vznikla v roku 1992 na konferencii National Leadership Conference on Media Literacy v Aspene. Centrum pre mediálnu výchovu CML (Centrum for Media Literacy) uvádza pre tento pojem tiež konkrétnejšiu definíciu: „Mediálna gramotnosť je prístup k vzdelávaniu 21. storočia. Poskytuje možnosť pristupovať, analyzovať, hodnotiť, vytvárať a podieľať sa správami v rôznych formách – od tlače až k videu na internete. Mediálna gramotnosť stavia chápanie role média v spoločnosti na úroveň nevyhnutných základných zručností dokazovania a sebaprezentácie demokratických občanov.“[4] K tomu, aby sme sa stali mediálne gramotnými nie je potrebné sa učiť naspamäť poučky. Potrebné je rozvíjať kritické myslenie a klásť si vhodné otázky zaoberajúce sa informáciami, ktoré prijímame.

[3] „Media Literacy is the ability to access, analyze, evaluate and create media in a variety of forms.“ Media Literacy: A Definition and More. Center for Media Literacy [online]. c2002 – 2011 [cit. 2014-04-17]. Dostupné z: http://www.medialit.org/media-literacy-definition-and-more

[4] Mediálna gramotnosť. Medzinárodné centrum mediálnej gramotnosti [online]. c2011 - 2013 [cit. 2014-04-17]. Dostupné z: http://www.medialnavychova.sk/medialna-gramotnost/

Vplyv médií

Odborní mediálni vedci si nie sú istí do akej miery a presne aký je skutočný vplyv médií na ich publikum. V priebehu času bolo vystriedaných mnoho rôznych teórií, ktoré tento vplyv popisovali:

- vplyv médií na rozhodovanie publika a jeho názorov preukázateľne existuje,
- tento vplyv väčšinou nie je bezprostredný, ľudia si nemyslia to, čo čítali v novinách, a ani to automaticky nepovažujú za pravdu,
- noviny majú schopnosť de facto určovať o čom budú ľudia premýšľať a rozprávať sa, do akej miery a ako,
- zlý mediálny obraz vedie k nežiaducim efektom v reálnom svete bez ohľadu na to, aká je skutočnosť a čo ju spôsobilo,
- za určitých okolností môžu ľudia informácie z médií bezprostredne previesť na akciu v situácii, keď sa obávajú, že výrobok je jedovatý, ho ihneď prestanú kupovať. (Jirák, 2009)

Vplyv médií na publikum preukázateľne existuje, ale nie je ani priamočiary ani jednoduchý. Je zložité ho predvídať, odhadovať a tiež hodnotiť. Ale vplyv a pôsobenie médií na publikum je značný.

Samozrejmé, že rôzne média majú na publikum rôzny vplyv, predovšetkým v závislosti na tom aká je ich prestíž, akú veľkú skupinu čitateľov alebo divákov oslovujú a nakoľko je táto skupina manipulovaná. Výsledky ich pôsobenia tak môžu byť v praxi odlišné a môžu sa líšiť v závislosti na celej rade okolností. Je potrebné si ale uvedomiť, že mediálny vplyv nepôsobí len lineárne a iba krátkodobo. (Jirák, 2009)

Kritické myslenie

Základy kritického myslenia položil už v staroveku Sokrates a jeho podstatou je, aby človek nepodliehal prvým dojmom, ale aby si vytvoril vlastný názor na základe získaných vedomostí a skúseností nielen svojich, ale aj iných ľudí. Vyžaduje si to systematickú zvedavosť, otvorenú myse+ a chápanie akýchkoľvek informácií v najširších súvislostiach (Kosturková, 2019)

Kriticky mysliaci človek na základe vytrénovanej mysle sa pri hodnotení nejakých tvrdení, argumentov, štúdií a článkov pozerá tzv. pod povrch, skúma otázky a kvalitu autorov, logickú súdržnosť prezentovaných tvrdení, dôveryhodnosť použitých dôkazov, zodpovednosť

pri vyvodzovaných dôsledkov, či vernosť vedeckým metodológiám. Takto mysliaci človek nasleduje len myslenie iných, ale rovnako systematicky pozoruje a vyhodnocuje aj vlastné pohnútky, myšlienkové pochody či vznik vlastných názorov a rozhodnutí. Na veci sa tiež nepozerá jednostranne, ale snaží sa na veci pozerať z viacerých uhlov, preto namiesto toho, aby si vybral jednu odpoveď a ostatné zavrhol snaží sa pochopiť viaceré výsledkom toho je potom neustála snaha zdokonaľovať svoj cit pre presnosť vo vyjadrovaní a myslení, ako aj štruktúrovaný, konzistentný a logický prejav. (Kosturková, 2019)

Kritické myslenie je teória, stratégia, metóda a proces, ktorý zahrňuje komplex zastrešujúci niektoré schopnosti a zručnosti, ktoré v myslení odbúravajú ľahostajnosť. Okrem toho dokáže nielen vytvárať vlastný názor, chápať historické súvislosti, prepájať politický a ekonomický kontext, ako aj vyžívať komunikačné technológie. Je to tiež komplex myšlienkových operácií, ktoré začínajú informáciou a končia vlastným rozhodnutím.

Vzhľadom k uvedenému je evidentné , že kritické myslenie je spoľahlivým spôsobom overovania dôveryhodnosti s cieľom identifikácie klamlivých a zavádzajúcich informácií. Doplňujúcimi otázkami totiž dokáže nielen kontinuitu medzi faktami a názormi, ale dokáže aj rozhodnúť, ktorá informácia je pravdivá a ktorá nie. Základom je overovanie pravdivosti informácií prostredníctvom viacerých nezávislých zdrojov, ktoré by mali byť dôveryhodné.

V kritickom myslení mladej generácie sú značné rezervy, preto má problémy so spájaním informácií, dedukciou, argumentáciou a tvorbou zdrojov, čo sa v konečnom dôsledku prejavuje v obťažnej identifikácii skrytejších foriem klamlivých informácií. (Kosturková, 2019)

Pri prehodnocovaní správ a informácií, z hľadiska ich pravdivosti, t.j. pri zisťovaní, či sa nejedná o klamlivé informácie je potrebné zachovať určitý postup. Skôr, ako sa pustíme do rôznych testov a postupov, je potrebné v prvom rade zapojiť tzv. „sedliacky rozum“. Ten nám pomôže zistiť, aké informácie hľadáme a kde ich hľadať, čím sa vylúčia niektoré zdroje hneď na začiatku. (Kosturková, 2019)

Na identifikáciu klamlivých obsahov na weboch bola vypracovaná pomôcka, ktorá sa dá využiť na identifikáciu všetkých foriem klamlivých informácií. Identifikácia pozostáva z nasledovných krokov:

- zistiť, či web, z ktorého pochádza naozaj existuje často charakteristickým znakom klamlivých informácií podobne ako neformálny jazyk, gramatické chyby, zlá grafika a dizajn,
- po prečítaní správy je potrebné odpovedať na otázky či správa potvrdzuje určité stereotypy alebo vnútorné obavy, či apeluje na city, vyvoláva určité pocity nenávisti či strachu a prípade všetkých kladných odpovedí je to veľmi silné podozrenie,
- preverenie testom CRAP, ktorý je štandardizovanou metódou overovania nielen pri akademických prácach, ale aj pri bežnom čítaní, kde sa zisťuje, či je správna aktuálna, má dátum publikácie, či je podložená informáciami a zdrojmi, kto je autor, či ide o autoritu alebo experta v danej oblasti, prečo správa vznikla, či má niečo povedať alebo má len nabúrať názor a či inklinuje k určitému uhlu pohľadu,
- pozornosť je potrebné venovať informáciám tykajúcim sa zdravia a politiky, lebo veľa klamlivých informácií sa týka tejto oblasti, skratka vecí života a smrti, ak je nedôveryhodnosť zdroja evidentná a v rozpore s objektívnym vedeckým poznaním, ak môže spôsobiť zanedbanie potrebnej liečby alebo poškodenie zdravia,
- overenie si reputácie autorov a publikácií a v budúcnosti sa zamerať iba na také, ktoré reputáciu majú,
- zvýšenú pozornosť tiež venovať požitým a podozrivým fotografiám či videám, ktoré sú vyžívané v zavádzajúcom kontexte klamlivých informácií, preveriť ich vo vyhľadávači Google a zistiť či skutočne dokumentujú popísané informácie. (Martins, 2021)

Záver

Celkový dopad hoaxov na spoločnosť je komplexný a mnohostranný, pričom si vyžaduje koordinované úsilie zo strany vládnych inštitúcií, médií, akademických kruhov a samotných občanov. Iba spoločným úsilím môžeme minimalizovať negatívne dôsledky hoaxov a podporiť zdravú a informovanú spoločnosť. Taktiež je potrebné zdôrazňovať potrebu zvyšovania mediálnej gramotnosti medzi širokou verejnosťou ako kľúčový nástroj v boji proti hoaxom. Vzdelávanie občanov o tom, ako identifikovať a kriticky hodnotiť informácie, môže významne prispieť k zníženiu šírenia nepravdivých správ a k posilneniu odolnosti spoločnosti voči hoaxom a dezinformáciám. Hoaxy môžu výrazne ovplyvniť verejnú mienku a spôsobiť šírenie nedôvery voči oficiálnym inštitúciám a médiám. Tento nedostatok dôvery môže viesť k sociálnej polarizácii a k oslabeniu spoločenskej súdržnosti.

Zoznam použitej literatúry

JIRÁK, J.- KOPPLOVÁ, B. 2009. Masové média Praha: Portál, 2009 ISBN 978 80-7367-466-3

ŠNÍDL, Vladimír. 2017 a. Pravda a lož na Facebooku. Bratislava: N Press, s.r.o., 2017 Knižná edícia Dennika N. ISBN 979-80-972394-4-2

KOSTURKOVÁ, M. FERENCOVÁ, J: 2019. Stratégie rozvoja kritického myslenia Wolters Kluwer 2019, ISBN 978 80 5710 0492

MARTINS, J. 2021 How to build your critical thinking (cit. 29 september 2021).

OXFORD DICTIONARIES: Oxford Dictionary of English, Oxford University Press, 2012

NUTIL, P.: Média, lži a příliš rychlý mozek. 1. vydanie, Brno: Grada, 2018

Kontaktné údaje

Mgr. Ing. Miroslav Benko
Národná kriminálna agentúra P PZ
Pribinová 2, 812 72 Bratislava
e-mail: miroslav.benko@akademiapz.sk

Recenzenti:
doc. Ing. Václav Friedrich, Ph.D.
doc. RNDr. Tatiana Hajdúková, PhD.

ENISA a jej význam pre kybernetickú bezpečnosť v kontexte kybernetického útoku na SolarWinds

Roman B. Borovský

Abstrakt: Príspevok vo svojej prvej časti analyzuje úlohu a stručnú históriu vzniku ENISA – Agentúry Európskej únie pre kybernetickú bezpečnosť, ktorá je zarámcovaná právnymi aktmi Európskej únie. Následne pojednáva o aktuálnej správe Agentúry identifikujúcej novovznikajúce kybernetické hrozby a výzvy pre rok 2030 s akcentom na kompromitáciu dodávateľských reťazcov v rámci životného cyklu softvéru. Pre ilustráciu reálneho dopadu a rizík zmienenej kybernetickej hrozby uvádzame poskytuje v záverečnej časti analýzu kybernetického útoku na spoločnosť SolarWinds, ktorá obsahuje dôležité závery o potrebe posilnenia kybernetickej odolnosti a prípadných následkov opomenutia riadnej implementácie bezpečnostných politík.

Kľúčové slová: ENISA, bezpečnosť, kybernetické hrozby, výzvy, SolarWinds

Abstract: The article in its first part analyzes the role and brief history of the establishment of the ENISA – European Union Agency for Cyber Security, framed by the legal acts of the European Union. It then discusses the Agency's current report identifying emerging cyber threats and challenges for the year 2030, with an emphasis on the compromise of supply chains within the software lifecycle. To illustrate the real impact and risks of the mentioned cyber threat, in the final part it provides an analysis of the cyber-attack on company SolarWinds, which contains important conclusions about the need to strengthen cyber resilience and the potential consequences of neglecting proper implementation of security policies.

Key words: ENISA, security, cyber threats, challenges, SolarWinds

Úvod

Súčasný, vysoko dynamický vývoj ľudskej spoločnosti, zvlášť v oblasti informačných a komunikačných technológií, systémov a prostriedkov, sprevádzaný rýchlo prebiehajúcou informatizáciou a digitalizáciou jednotlivých sektorov, rozširujúcou sa dostupnosťou internetu a masovým využívaním najrôznejších platforiem širokej škály sociálnych sietí, priniesol okrem množstva pozitív aj množstvo negatív. [1] Viaceré z nich sa veľmi úzko týkajú problematiky

[1] KUCHTOVÁ, J. 2018. Aktuálne trendy súvisiace s využívaním moderných technológií. In *Aktuálne výzvy kybernetickej bezpečnosti – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2018, s. 90-98; HAJDÚKOVÁ, T. 2022. Zneužívanie elektronických služieb na sexuálne zneužívanie detí. In *Bezpečnosť elektronickej komunikácie – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru v Bratislave, 2022, s. 71-85; TOMÁŠEK, R. – TOMÁŠEKOVÁ, L. 2020. Kybernetické hrozby a kybernetický terorizmus. In *Aktuálne výzvy kybernetickej bezpečnosti – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2020, s. 146-152; IVANČÍK, R. – BARIČIČOVÁ. Ľ. 2019. Kybernetické hrozby ako súčasť asymetrických bezpečnostných hrozieb v 21. storočí. In *Aktuálne výzvy kybernetickej bezpečnosti : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2019, s. 35-47

bezpečnosti, osobitne kybernetickej bezpečnosti.[2] Z toho dôvodu sa v tejto súvislosti v nasledujúcom texte zameriavame niektoré vybrané informácie týkajúce sa tejto vysoko špecifickej oblasti. V prvej časti príspevku sa zaoberáme Agentúrou Európskej únie pre kybernetickú bezpečnosť – ENISA, ktorá plní mimoriadne dôležité úlohy v tejto exponovanej oblasti. Pojednávame o aktuálnej správe Agentúry identifikujúcej novovznikajúce kybernetické hrozby a výzvy pre rok 2030 s akcentom na kompromitáciu dodávateľských reťazcov v rámci životného cyklu softvéru. V druhej časti príspevku pre lepšiu ilustráciu reálneho dopadu a rizík zmienenej kybernetickej hrozby uvádzame analýzu kybernetického útoku na spoločnosť SolarWinds, ktorá predstavuje typický prípad zanedbania kybernetickej bezpečnosti a obsahuje dôležité závery o potrebe posilnenia kybernetickej odolnosti a prípadných následkov opomenutia riadnej implementácie bezpečnostných politík.

Agentúra Európskej únie pre kybernetickú bezpečnosť

Agentúra Európskej únie pre kybernetickú bezpečnosť ENISA[3] je kľúčovým hráčom v oblasti kybernetickej bezpečnosti na úrovni Európskej únie, ktorá prešla dynamickým vývojom od svojho založenia. Jedným z jej hlavných úloh je okrem iného príprava Európy na budúce výzvy v oblasti kybernetickej bezpečnosti prostredníctvom zdieľania vedomostí, budovania kapacít a zvyšovania povedomia, výsledkom čoho bola aj relatívne nedávno vydaná publikácia s názvom „*Identifikácia novovznikajúcich kybernetických hrozieb a výziev pre rok 2030*“[4] (ďalej ako „Správa ENISA 2030“). Publikácia poskytuje komplexný pohľad na aktuálnu problematiku hrozieb v kybernetickom priestore, pričom používa odbornú terminológiu a detailné príklady, aby zabezpečila dôkladné pochopenie diskutovaných tematických okruhov. V obdobnom duchu sme koncipovali tento príspevok, ktorého ambíciou je oboznámiť odbornú i laickú verejnosť s inštitucionalizáciou zabezpečenia kybernetickej bezpečnosti v spojitosti

[2] FRIANOVÁ, V. 2020. Kybernetická bezpečnosť ako jeden z „vedľajších produktov“ investovania štátu do obrany, ľudských zdrojov, výskumu a vývoja In *Aktuálne výzvy kybernetickej bezpečnosti : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2020, s. 17-22; NEČAS, P. – IVANČÍK, R. 2019. Aktuálny vývoj v oblasti zaisťovania kybernetickej bezpečnosti a ochrany informácií na národnej a nadnárodnej úrovni. In Aktuálne výzvy kybernetickej bezpečnosti : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou. Bratislava : Akadémia Policajného zboru, 2019. s. 125-137; BREZULA, J. 2018. Vývoj kybernetickej bezpečnosti vzhľadom na nové hrozby v súčasnosti. In Tradície a dynamika vývoja manažmentu a informatiky z pohľadu univerzít s bezpečnostným zameraním : zborník príspevkov. Bratislava: Akadémia policajného zboru, 2018; IVANČÍK, R. – BARIČIČOVÁ. Ľ. 2020. Kybernetická bezpečnosť z pohľadu postavenia a úloh štátu pri jej zaisťovaní. In Aktuálne výzvy kybernetickej bezpečnosti : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou. Bratislava : Akadémia Policajného zboru, 2020, s. 23-34;

[3] Z angl. „*European Network and Information Security Agency“*

[4] Z angl. „*Identifying emerging cyber security threats and challenges for 2030“*

s jej osvetovou činnosťou a následným popisom prípadovej štúdie prevedenia kybernetického útoku významného rozsahu.

Európska agentúra pre bezpečnosť sietí a informácií, ktorá pôvodne sídlila v gréckom meste Heraklion na ostrove Kréta, bola založená nariadením Európskeho parlamentu a Rady č. 460/2004 z 10. marca 2004. Svoju činnosť začala vykonávať v septembri 2005 a jej hlavným poslaním bolo (a *de facto* stále je) poskytovanie poradenstva v oblasti bezpečnosti komunikačných sietí a informačných systémov, analýza dát ako aj podporovanie zvýšeného uvedomia a spolupráce orgánov EÚ s členskými štátmi v rámci oblasti kybernetickej bezpečnosti. Agentúra takisto využívala svoje skúsenosti na podnietenie spolupráce medzi verejným a súkromným sektorom v otázkach hardvérovej a softvérovej bezpečnosti. Prvotný mandát agentúry bol predĺžený do marca 2012 nariadením (ES) č. 1007/2008 a následne nariadením (ES) č. 580/2011 opätovne do 13. septembra 2013.

Nariadením Európskeho parlamentu a Rady (EÚ) č. 526/2013 z 21. mája 2013 o Agentúre Európskej únie pre sieťovú a informačnú bezpečnosť (ENISA) a o zrušení nariadenia (ES) č. 460/2004 (ďalej aj ako „nariadenie ENISA“ alebo „nariadenie č. 526/2013“) bolo zrušené pôvodné nariadenie upravujúce postavenie a pôsobnosť Agentúry. Reflektujúc neustále meniace sa „*výzvy spojené so sieťovou a informačnou bezpečnosťou zmenili spolu s vývojom technológií, trhov a sociálno-ekonomickým vývojom*“ (odôvodnenie 11 nariadenia ENISA). Nariadenie č. 526/2013 zároveň predstavovalo nový právny základ pre ďalšie fungovanie Agentúry Európskej únie pre sieťovú a informačnú bezpečnosť. Agentúra sa zriadila na obdobie siedmich rokov počnúc 19. júnom 2013 (čl. 36 nariadenia ENISA). Pobočka zriadená v metropolitnej oblasti Atén sa zachovala s cieľom zlepšiť prevádzkovú efektívnosť agentúry (čl. 26 ods. 4 nariadenia ENISA).

Keďže posledný mandát Agentúre ENISA by dňa 19. júna 2020 opäť vypršal, EÚ sa Aktom o kybernetickej bezpečnosti[5] rozhodla posilniť doterajšie postavenie pôvodnej Európskej únie pre sieťovú a informačnú bezpečnosť a zriadiť jej nástupcu v podobe Agentúry Európskej únie pre kybernetickú bezpečnosť.[6]

[5] Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 ďalej aj ako „AKB“

[6] Hoci došlo k formálnej zmene názvu, novo sformovaná Agentúra naďalej vystupuje pod názvom ENISA

Agentúra ENISA zriadená Aktom o kybernetickej bezpečnosti vykonáva široké úlohy v oblasti kybernetickej bezpečnosti, s cieľom dosiahnuť jej vysokú spoločnú úroveň v celej Únii, a to aj tým, že aktívne podporuje členské štáty a inštitúcie, orgány, úrady a agentúry Únie.[7]

Článok 6 AKB s názvom „Budovanie kapacít“ vymedzuje Agentúre ENISA okruhy problémov s ktorými má pomáhať členským štátom, inštitúciám aj ďalším orgánom Únie. Jedná sa najmä o zlepšenie prevencie, odhaľovania a analýzu kybernetických hrozieb, pomoc pri zavádzaní politík, tvorbe a revízií kyberneticko-bezpečnostných stratégií na národnej i úniovej úrovni apod.

V článku 10 AKB sa pojednáva o úlohách ENISA pri zvyšovaní verejného povedomia o kyberneticko-bezpečnostných rizikách, ako aj o podpore vzdelávania v oblasti kybernetickej bezpečnosti. Okrem pravidelných osvetových kampaní a diskusií je predvídaná koordinácia a výmena najlepších postupov v oblasti kybernetickej bezpečnosti.

Samotná ENISA sa hlási ku spolupráci s tretími krajinami a medzinárodnými organizáciami, nakoľko EÚ vníma kybernetické hrozby ako globálny problém. V bode 54 odôvodnenia AKB sa píše: *„Je potrebná užšia medzinárodná spolupráca s cieľom zlepšiť kyberneticko-bezpečnostné normy vrátane potreby vymedzenia spoločných noriem správania, prijatia kódexov správania, uplatňovania medzinárodných noriem a výmeny informácií, presadzovania rýchlejšej medzinárodnej spolupráce pri reakcii na problémy týkajúce sa sieťovej a informačnej bezpečnosti, ako aj presadzovania spoločného globálneho prístupu k týmto problémom.“*[8]

Výzvy kybernetických hrozieb z pohľadu ENISA

Správa ENISA 2030 má za cieľ identifikovať a zozbierať informácie o budúcich kybernetických hrozbách, ktoré by mohli ovplyvniť infraštruktúru a služby Únie, ako aj jej schopnosť udržiavať európsku spoločnosť a občanov v bezpečí.

V rámci tejto štúdie bolo identifikovaných 21 potenciálnych hrozieb, ktoré by mohli výhľadovo do roku 2030 vzniknúť alebo naďalej naberať na závažnosti. Štúdia taktiež poskytuje postup na identifikáciu a prioritizáciu hrozieb, ktorá zahŕňa interdisciplinárne skúmanie na základe politických, ekonomických, sociálnych, technologických,

[7] Čl. 3 Nariadenia Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019
[8] Odôvodnenie 54 Nariadenia Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019

environmentálnych a právnych faktorov (PESTLE analýza) spolu s metodikou „*threatcasting*“, ktorá využíva tradičné štúdie budúcnosti a vojenské strategické myslenie.[9]

Medzi hlavné hrozby patria napríklad kompromitovanie dodávateľských reťazcov softvéru, pokročilé dezinformačné kampane, rast digitálneho dohľadu s autoritatívnymi prvkami, chyby ľudského faktora a zneužitie zastaraných počítačových systémov, cieľové útoky disponujúce údajmi zo smart zariadení, zneužitie umelej inteligencie a iné.

Následná aktualizácia Správy ENISA 2030 s názvom "*Foresight Cybersecurity Threats For 2030 – Update 2024*" prináša významné doplnky a rozšírenia k pôvodnému textu, čím poskytuje prehĺbené pochopenie a nové perspektívy na budúce kybernetické hrozby. Zdôrazňuje rastúcu závislosť spoločnosti na digitálnych technológiách, ako aj umelej inteligencie (AI), a to v rôznych sektoroch, čo predstavuje nové príležitosti, ale zároveň aj hrozby v ekosystéme kybernetickej bezpečnosti. V tejto aktualizácii sa tiež zdôrazňuje vplyv celosvetovej geopolitiky a prírodných katastrof na zvýšenie sofistikovanosti a hybridnosti kybernetických hrozieb.[10]

Na základe metód a taxonómie použitej v publikácii ENISA 2030 sa za najpravdepodobnejšiu a najviac kritickú kybernetickú hrozbu považuje kompromitácia dodávateľských reťazcov softvéru, ktorá vzniká, keď útočníci infikujú softvérové komponenty pred ich distribúciou. Tento typ útoku je mimoriadne nebezpečný, pretože môže malvér šíriť prostredníctvom dôveryhodných aktualizácií alebo softvérových knižníc, ktoré sú bežne používané v rôznych aplikáciách.

Útoky na dodávateľské reťazce majú často dlhodobé následky, pretože infikované komponenty môžu byť v systémoch prítomné dlhú dobu predtým, než sa problém odhalí, čo umožňuje dlhodobú manipuláciu a zber citlivých údajov. V reakcii na tieto hrozby je dôležité, aby organizácie posilnili bezpečnostné kontroly, zahrnuli bezpečnostné opatrenia už vo fáze vývoja softvéru a aktívne sa zapojili do spolupráce a výmeny informácií o hrozbách. Tieto kroky pomáhajú znižovať riziko a zvyšujú odolnosť proti potenciálnym útokom.

[9] Pozri bližšie: ENISA. 2023. Identifying emerging cyber security threats and challenges for 2030. [online]. [cit. 13.03.2024]
[10] ENISA. 2024. Foresight cybersecurity threats for 2030 - update. [online]. [cit. 13.03.2024]

Kybernetický útok „SolarWinds“

Pri analýze kybernetických útokov posledných rokov je útok na spoločnosť SolarWinds Corporation (ďalej ako „SolarWinds“ alebo „SWC“) nepochybne jedným z najrozsiahlejším - čo do počtu infikovaných užívateľov, ako aj dĺžky jeho trvania.[11] Spoločnosť SWC bola založená v roku 1999 a momentálne zamestnáva viac ako 2100 zamestnancov, pričom generuje obrat vo výške približne 0,76 miliardy amerických dolárov.[12] Medzi jej klientov, ktorým zabezpečuje sieťový manažment radíme mnoho renomovaných spoločností, vrátane spoločností Fortune 500, ako aj viacero vládnych agentúr a ministerstiev USA.[13]

Udalosti sa dali do pohybu dňa 14. decembra 2020, kedy SolarWinds zverejnila správu o tom, že sa stala obeťou sofistikovaného a pokročilého útoku cez dodávateľa, v ktorom sa do legitímnej verzie softvéru implementoval útočníkom škodlivý kód (tzv. supply chain attack).[14]

Útočníkom sa podarilo infikovať aktualizácie platformy pre správu a monitoring IT infraštruktúry malvérom SUNBURST (pomenovanie spoločnosťou FireEye), resp. Solorigate (pomenovanie spoločnosťou Microsoft), ktorý umožňuje vytvorenie zadných vrátok (tzv. backdoor) v napadnutom systéme.

Kompromitovaná bola „DDL knižnica“[15] platformy Orion, ktorá bola podpísaná legitímnym (hoci neautorizovaným) certifikátom. Malvér po inštalácii zostal dva týždne neaktívny. Následne začal prijímať a vykonávať príkazy zo serverov útočníkov cez protokol HTTP. SUNBURST dokázal odosielať a spúšťať súbory, sledovať prostredie, vypínať systémové služby a reštartovať napadnuté zariadenia. Zároveň detegoval prítomnosť antivírových programov a forenzných nástrojov.

Škodlivá verzia SolarWinds Orion ukrývala výsledky svojej špionážnej činnosti do legitímnych konfiguračných súborov a svoju sieťovú komunikáciu maskovala pomocou

[11] U.S. SECURITIES AND EXCHANGE COMMISSION. 2020. Solarwinds Corporation Report [online]. [cit. 13.03.2024].

[12] SolarWinds Worldwide. 2024. SolarWinds Announces Fourth Quarter and Full Year 2023 Results [online]. [cit. 26.04.2024].

[13] Spomedzi súkromných spoločností spomenieme napr. Microsoft, Cisco, Intel, Deloitte; spomedzi štátnych inštitúcií napr. Pentagon, Ministerstvo vnútornej bezpečnosti, Ministerstvo energetiky, Národný úrad pre jadrovú bezpečnosť alebo Štátnu pokladnicu USA

[14] Pozri bližšie: SK-CERT, 2020. Mimoriadne kritická zraniteľnosť v systéme na správu vašich IT aktív [online]. [cit. 26.04.2024].

[15] Knižnica DLL (z angl. *Dynamic Link Library*) je skratka pre dynamicky spojenú knižnicu zdrojového kódu, ktorá poskytuje viacerým súčasne bežiacim programom pod systémom Windows rôzne funkcionality

protokolu OIP (Orion Improvement Program), slúžiaceho spoločnosti SWC na zber používateľských dát pre vylepšovanie produktu. Pre zníženie pravdepodobnosti detekcie útoku bola komunikácia šifrovaná a smerovaná cez služby VPN na IP adresy krajiny obete.

Americká Agentúra pre kybernetickú bezpečnosť a infraštruktúru – CISA (Cyber Security & Infrastructure Agency) vydala v deň oznámenia o útoku nariadenie, ktoré všetkým federálnym agentúram prikazuje kontrolu SolarWinds Orion systémov na prítomnosť indikátorov kompromitácie (ďalej ako „IOC“ z angl. Indicators of Compromise)[16] a zároveň odpojenie týchto systémov od internetu alebo ich úplné vypnutie.[17]

V ten istý deň Národné centrum kybernetickej bezpečnosti Slovenskej republiky (SK-CERT) varovalo pred touto kritickou zraniteľnosťou a vydalo odporúčanie okamžite izolovať všetky aktívne služby SolarWinds Orion od internetu a vnútornej infraštruktúry v akejkoľvek verzii a v prípade, ak to nie je možné obmedziť pripojenie na zariadenia a to najmä na tie, ktoré sú kritickými aktívami, ako aj obmedziť účty, ktoré majú v SolarWinds Orion administrátorské privilégiá atď.[18]

Následné zistenia zo dňa 12. januára 2021 spoločnosti Crowdstrike, ktorá sa priamo zúčastňuje na rozboru útoku na SolarWinds, identifikovali už tretí kmeň škodlivého softvéru a pomenovala ho „SUNSPOT“.[19]

Posledný nájdený kmeň bol chronologicky prvým, ktorým útočníci infikovali sieťovú infraštruktúru. SUNSPOT bol totiž nasadený už niekedy v septembri 2019 s cieľom sledovať príkazy zostavujúce program Orion na „build serveroch“[20] a poskytnúť tieto údaje útočníkom za účelom optimálnej implementácie sekvenčného SUNBURST malvéru. SUNBURST následne zisťoval ako vyzerá sieť zákazníka a v prípade, ak sa jednalo o významnú inštitúciu alebo spoločnosť, finálne nasadil verziu malvéru s názvom „TEARDROP". V prípade, ak šlo o nezaujímavú spoločnosť, SUNBURST malvér sa autonómne odstránil, aby nevzniklo zbytočné podozrenie, čím by potenciálne ohrozil útoky na

[16] Kompletný zoznam dostupných IOC pre útok SolarWinds je dostupný na internetovej adrese https://github.com/fireeye/sunburst_countermeasures

[17] CISA. 2020. Emergency Directive 21-01. [online]. [cit. 13.02.2024].

[18] SK-CERT. 2020. Mimoriadne kritická zraniteľnosť v systéme na správu vašich IT aktív [online]. [cit. 18.03.2024].

[19] CROWDSTRIKE. 2021. SUNSPOT: An Implant in the Build Process. [online]. [cit. 20.03.2024].

[20] Build server predstavuje centralizované, stabilné a spoľahlivé prostredie pre vývoj a priebežnú integráciu softvéru

žiadané ciele. Nepovolený zber dát útočníkmi trval minimálne desať mesiacov, vďaka čomu sa kompromitovalo doposiaľ nevídaný objem dát.

Po sérii vyšetrovaní sa v roku 2023 Americká komisia pre cenné papiere a burzu (*Securities and Exchange Commission* – ďalej len „SEC“) rozhodla vzniesť obvinenia[21] proti spoločnosti SolarWinds a jej viceprezidenta pre IT bezpečnosť a architektúru Timothymu G. Brownovi, z dôvodu podvodov a sérii interných zlyhaní, ktoré sa týkali firemných politík v oblasti kybernetickej bezpečnosti. Podľa obvinení spoločnosť SWC od obdobia svojho prvotného verejného ponúkania akcií v októbri 2018 až po oznámenie v decembri 2020, že bola obeťou rozsiahleho kybernetického útoku, zavádzala investorov a verejnosť tým, že preceňovala svoje praktiky v oblasti kybernetickej bezpečnosti a zároveň nedostatočne, alebo vôbec neinformovala o známych rizikách.

Obvinenia poukazujú na to, že verejné vyhlásenia spoločnosti o jej kybernetickej bezpečnosti boli v rozpore s internými hodnoteniami. Týka sa to aj prezentácie z roku 2018, ktorú pripravili zamestnanci spoločnosti a ktorá bola zdieľaná interne, vrátane T. G. Browna. Táto prezentácia uvádzala, že nastavenie vzdialeného prístupu spoločnosti "*nie je veľmi bezpečné*" a že využitie tejto zraniteľnosti by umožnilo útočníkovi "*robiť prakticky čokoľvek bez toho, aby sme to zistili, až kým nebude príliš neskoro*," čo by mohlo viesť k "*veľkým strátam na povesti a financiách*" spoločnosti SolarWinds.[22]

SEC ďalej zdôrazňuje, že SWC používala všeobecné a hypotetické opisy rizík kybernetickej bezpečnosti vo svojich dokumentoch, napriek tomu, že mala konkrétne skúsenosti s kybernetickými útokmi a bola si vedomá konkrétnych zraniteľností svojich softvérových produktov. Tieto nedostatočné vyhlásenia sú považované za klamlivé, keďže neodrážali skutočné riziká, ktorým čelila spoločnosť. Právne kroky Komisie pre cenné papiere a burzu sú časťou širšieho úsilia o zvýšenie firemnej zodpovednosti v oblasti zverejňovania informácií o kybernetickej bezpečnosti a vytvárania presnejších a transparentnejších postupov na ochranu investorov a verejnosti pred podobnými hrozbami v budúcnosti. Tento prípad predstavuje dôležitý precedens v regulácii a dohľade nad firemnou kybernetickou bezpečnosťou.

[21] Pozri bližšie: U.S. SECURITIES AND EXCHANGE COMMISSION. 2023. Prípad č. 1:23-cv-09518 zo dňa 30.10.2023

[22] Tamtiež. s. 5

Prípad tiež poukazuje na osobnú zodpovednosť výkonných riaditeľov za presné vykazovanie informácií o kybernetickej bezpečnosti, čo znamená potenciálne zvýšené riziko pre CISO (Chief Information Security Officers), ktorí môžu byť osobne zodpovední za zavádzajúce informácie podané regulačným orgánom a investorom. To zdôrazňuje dôležitosť dôkladného preskúmania verejných vyhlásení a zabezpečenia súladu všetkých interných kontrol a procedúr so skutočným stavom kybernetickej bezpečnosti v spoločnostiach. Tento prípad predstavuje zásadný posun v dôraze, ktorý SEC kladie na kybernetickú bezpečnosť ako regulačnú a vymáhateľnú prioritu, a signalizuje potrebu pre spoločnosti venovať zvýšenú pozornosť riadeniu kybernetickej bezpečnosti a správnemu zverejňovaniu súvisiacich informácií.

Záver

Agentúra Európskej únie pre kybernetickú bezpečnosť zohráva kľúčovú úlohu v rozvoji a udržiavaní vysokej úrovne kybernetickej bezpečnosti v rámci celej Európskej únie. Ako sa ukazuje v Správe ENISA 2030, agentúra nielenže poskytuje cenné odborné vedenie a podporu, ale tiež proaktívne pracuje na identifikácii a reakcii na nové a vznikajúce hrozby, ktoré môžu negatívne ovplyvniť bezpečnosť občanov a infraštruktúr EÚ.

Rovnako dôležité je konštatovanie, že kybernetická bezpečnosť je neustále sa vyvíjajúci priestor, kde nové technológie a nové hrozby vyžadujú stálu pozornosť a adaptáciu zo strany bezpečnostných aktérov. V tomto kontexte je esenciálne, aby spolupráca medzi štátmi a inštitúciami bola čo najtesnejšia, aby sa zabezpečila efektívna ochrana proti kybernetickým útokom, ktoré sú čoraz sofistikovanejšie a majú potenciál spôsobovať rozsiahle škody, ako to bolo v prípade útoku na SolarWinds.

Kybernetický útok SUNBURST, pri ktorom útočníci využili slabosti v dodávateľskom reťazci na infikovanie softvéru používaného mnohými veľkými organizáciami vrátane vládnych agentúr, ilustruje kľúčové výzvy, ktorým čelíme. Tento incident podčiarkuje potrebu neustáleho monitorovania a posilňovania bezpečnostných opatrení na ochranu proti sofistikovaným a cieleným útokom, ktoré môžu mať devastujúce dôsledky na národnej a medzinárodnej úrovni. Útok na SolarWinds má potenciál stať sa obdobným učebnicovým príkladom, akým bol červ Stuxnet[23], ktorý je považovaný za vzorový model kybernetickej

[23] Vírus Stuxnet bol použitý v roku 2010 v operácii namierenej proti iránskemu jadrovému programu. Úlohou Stuxnetu bolo napadnúť systém SCADA (z angl. *Supervisory Control and Data Acquisition*) vytvoreného spoločnosťou Siemens, ktorý o. i. riadil centrifúgu na obohacovanie uránu v jadrových zariadeniach

hrozby typu APT[24]. Konštatovanie je platné nie len pre oblasť informatiky, ale aj právnej a bezpečnostnej vedy.

Zoznam použitej literatúry

BREZULA, J. 2018. Vývoj kybernetickej bezpečnosti vzhľadom na nové hrozby v súčasnosti. In *Tradície a dynamika vývoja manažmentu a informatiky z pohľadu univerzít s bezpečnostným zameraním : zborník príspevkov*. Bratislava : Akadémia policajného zboru, 2018. ISBN 978-80-8054-773-8.

CISA. 2020. Emergency Directive 21-01. [online]. [cit. 13.02.2024]. Dostupné na internete: <https://cyber.dhs.gov/ed/21-01/>

CROWDSTRIKE. 2021. SUNSPOT: An Implant in the Build Process. [online]. [cit. 20.03.2024]. Dostupné na internete: <https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/>

ENISA. 2023. Identifying emerging cyber security threats and challenges for 2030. 64 s. ISBN 978-92-9204-634-7. [online]. [cit. 13-03-2024] Dostupné na internete: <https://www.enisa.europa.eu/publications/enisa-foresight-cybersecurity-threats-for-2030/@@download/fullReport. >

ENISA. 2024. Foresight cybersecurity threats for 2030 - update. 37 s. ISBN 978-92-9204-671-2. [online]. [cit. 13-03-2024] Dostupné na internete: <https://www.enisa.europa.eu/publications/foresight-cybersecurity-threats-for-2030-update-2024-extended-report/@@download/fullReport. >

FRIANOVÁ, V. 2020. Kybernetická bezpečnosť ako jeden z „vedľajších produktov“ investovania štátu do obrany, ľudských zdrojov, výskumu a vývoja. In *Aktuálne výzvy kybernetickej bezpečnosti : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2020, s. 17-22. ISBN 978-80-8040-819-3.

HAJDÚKOVÁ, T. 2022. Zneužívanie elektronických služieb na sexuálne zneužívanie detí. In Bezpečnosť elektronickej komunikácie – zborník príspevkov z vedeckej konferencie

[24] APT (z angl. *Advanced Persistent Threats*) alebo pokročilé perzistentné hrozby sú sofistikované techniky a vektory útokov, ktoré slúžia na obchádzanie bezpečnostných mechanizmov, skrytie činností útočníka a jeho nedetegované zotrvanie na napadnutých systémoch

s medzinárodnou účasťou. Bratislava : Akadémia Policajného zboru, 2022, s. 71-85. ISBN 978-80-8054-968-8.

IVANČÍK, R. – BARIČIČOVÁ. Ľ. 2019. Kybernetické hrozby ako súčasť asymetrických bezpečnostných hrozieb v 21. storočí. In *Aktuálne výzvy kybernetickej bezpečnosti : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2019, s. 35-47. ISBN 978-80-8040-819-3.

IVANČÍK, R. – BARIČIČOVÁ. Ľ. 2020. Kybernetická bezpečnosť z pohľadu postavenia a úloh štátu pri jej zaisťovaní. In *Aktuálne výzvy kybernetickej bezpečnosti : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2020, s. 23-34. ISBN 978-80-8054-819-3.

KUCHTOVÁ, J. 2018. Aktuálne trendy súvisiace s využívaním moderných technológií. In *Aktuálne výzvy kybernetickej bezpečnosti : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2018, s. 90-98. ISBN 978-80-8054-773-8.

NARIADENIE EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2019/881 zo 17. apríla 2019

NEČAS, P. – IVANČÍK, R. 2019. Aktuálny vývoj v oblasti zaisťovania kybernetickej bezpečnosti a ochrany informácií na národnej a nadnárodnej úrovni. In *Aktuálne výzvy kybernetickej bezpečnosti : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2019. s. 125-137. ISBN 978-80-8040-819-3.

SK-CERT. 2020. Mimoriadne kritická zraniteľnosť v systéme na správu vašich IT aktív [online]. [cit. 26.04.2024]. Dostupné na internete: <https://www.sk-cert.sk/sk/supply-chain-utok-v-solarwinds-orion-kriticka-zranitelnost-s-vaznymi-dosledkami/index.html>

SOLARWINDS WORLDWIDE. 2024. SolarWinds Announces Fourth Quarter and Full Year 2023 Results [online]. [cit. 26.04.2024]. Dostupné na internete: <https://investors.solarwinds.com/news/news-details/2024/SolarWinds-Announces-Fourth-Quarter-and-Full-Year-2023-Results/>

U.S. SECURITIES AND EXCHANGE COMMISSION. 2020. Solarwinds Corporation Report [online]. [cit. 13.02.2024]. Dostupné na internete: <https://www.sec.gov/ix?doc=/Archives/edgar/data/1739942/000162828020017451/swi-20201214.htm>

U.S. SECURITIES AND EXCHANGE COMMISSION. 2023. Prípad č. 1:23-cv-09518 [online]. [cit. 13.02.2024]. Dostupné na internete: <https://www.sec.gov/files/litigation/complaints/2023/comp-pr2023-227.pdf>

Kontaktné údaje

JUDr. PhDr. Roman Bartolomej Borovský
Secure IT Consultant s.r.o.
Zelená stráň 8, 040 14 Košice
email: rb.borovsky@gmail.com

Recenzenti:
prof. RNDr. Michal Greguš, CSc.
doc. RNDr. Tatiana Hajdúková, PhD.

The Role of Artifical Intelligence in Cybersecurity

Nataša Brabcová – Ervín Šimko

Abstract: The role of artificial intelligence (AI) in cybersecurity is becoming more and more important with AI-driven systems becoming a usable component in improving the current state of security in public sector. Especially computational intelligence (CI) and machine learning (ML) can be utilized in various situations, such as anomaly detection, incident classification, or the simulation of adversary behaviour. This paper surveys the potential applications of CI and ML in cybersecurity, highlighting their benefits and briefly describing the challenges associated with the utilization of ML and CI. Despite the promising advantages, the integration of AI into cybersecurity frameworks is associated with several disadvantages including high initial investments, the need for skilled professionals, and ethical or legal considerations. The implementation of AI systems requires careful management to address issues such as the transparency of AI decisions and the potential misuse of AI technologies by malicious actors. This paper describes the importance of a balanced approach, combining the capabilities of AI with the validation of its outputs by domain experts. The goal of this paper is to briefly demonstrate the role of AI in enhancing cybersecurity measures.

Keywords: Artificial Intelligence, Cybersecurity, Computational Intelligence, Machine Learning

Introduction

The concept of artificial intelligence (AI) refers to the simulation of human intelligence processes executed by machines, especially computer systems. These processes usually include learning (the acquisition of information and rules for using the information), reasoning (using rules to reach approximate or definite conclusions), or self-correction (the ability to asses own output and correct mistakes in it). The term AI is used with various smaller fields, such as machine learning (ML) and computational intelligence (CI), which often get confused leading to misunderstandings about the distinct roles and applications of these different terms [1], [2].

Computational intelligence is defined as a subset of AI that deals with heuristic algorithms and fuzzy systems, aiming to solve complex problems where traditional algorithmic methods are inefficient. On the other hand, machine learning is a branch of AI that focuses on the development of algorithms that allow computers to learn from and make predictions based on previous data and statistics. ML algorithms usually require large datasets and extensive training, which is a time-consuming process. CI techniques often rely on iterative processes and various adaptive mechanisms, making them suitable for dynamic environments.

Despite the recent development in AI technologies, several misconceptions persist, particularly fueled by marketing strategies that exaggerate AI capabilities. This misinformation can lead to unrealistic expectations resulting in the avoidance of the adoption of AI solutions. For instance, AI is often interpreted as a technology capable of solving problems without human intervention, which is far from the truth. Understanding the capabilities and limitations of AI is crucial for its effective implementation, especially in sectors like cybersecurity [3], [4], [5].

In the field of cybersecurity, the integration of computational intelligence offers promising solutions, particularly for Computer Incident Response Teams (CSIRT) [6], [7]. CSIRTs play a crucial role in identifying, analyzing, and mitigating cyber threats using their reactive or proactive measures. The application of CI could lead to improving their capabilities by providing tools for better anomaly detection, threat prediction, and semi-automated response. As cyber threats become more sophisticated and frequent, leveraging CI can provide cybersecurity experts with a significant advantage in protecting and monitoring digital assets [4].

This paper dives into the potential application of computational intelligence in cybersecurity. It explores the fundamental nuances of CI and ML and highlights the practical benefits of deploying CI technologies in cyber threat prevention. Through a comprehensive analysis, this paper aims to underscore the critical role of computational intelligence in improving the cybersecurity of the public sector in Slovakia [8], [9], [10].

The Different Types of Artificial Intelligence

The ML algorithms can be utilized for the following activities: data classification, data clustering, and a simulation of the adversary. Each of these activities addresses different problems using distinct methodologies [11], [12].

Classification. It is one of the most common applications of machine learning and involves supervised learning techniques. In supervised learning, the algorithm is trained on a labeled dataset, where each input is paired with the correct output, depicted in *Figure 1*. The creation and labeling of the dataset are challenging tasks and require a lot of manual data processing. The goal of classification is to enable the model to predict the correct label for previously unseen data. This method is widely used in various fields, such as spam detection, image recognition, and medical diagnostics. For example, in email filtering, the algorithm

learns to distinguish between spam and non-spam emails based on a set of labeled examples, allowing it to classify future emails accurately. However, a human error might be able to label e-mail incorrectly, thus providing a bad example for the model [11], [12], [13].

Clustering. It is a characteristic type of unsupervised learning technique. In this approach, the algorithm is given a dataset without labeled categories and must find the structure and patterns in the data. The clustering algorithm groups data points into clusters based on their similarities. However, it does this without context, so human intervention is required heavily during the training. This technique is useful in many applications, such as market segmentation, social network analysis, and organizing large datasets to identify patterns or structures. For instance, in anomaly detection, clustering can help identify distinct malicious behavior based on accessing sensitive information with high privileges or unusually high upload traffic indicating data exfiltration to adversaries [12], [13].

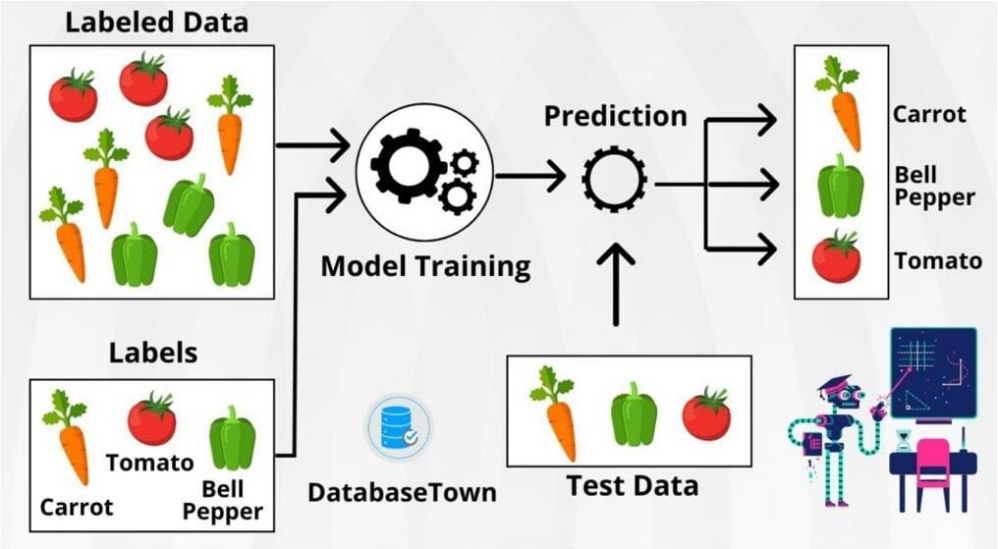


Figure 1: Example of data classification using supervised learning [9]

Reinforcement Learning. Represents a different paradigm where an agent learns to make decisions by interacting with an environment and observing the results. The agent receives rewards based on its actions, and its primary goal is to maximize cumulative rewards over time. This type of learning is particularly effective for problems where the correct action sequence is not known in advance and must be discovered through trial and error, e.g. finding an attack vector to infiltrate the environment. Applications of reinforcement learning include red and blue team scenarios. In an attack scenario, a reinforcement learning algorithm can train a robot to navigate a maze by rewarding it for reaching the goal and penalizing it for hitting walls.

Understanding the different types of artificial intelligence and their specific applications helps define the capabilities and limitations of AI. Classification, clustering, and reinforcement learning each play a critical role in enabling machines to learn from data, adapt to new situations, and help in designed a solution for several problems [12], [13].

The Use Cases for AI in Cybersecurity Teams

Cybersecurity experts are increasingly turning to ML and CI to enhance the capabilities of their teams. The integration of AI into cybersecurity operations offers a range of innovative solutions that could improve the detection, classification, and simulation of cyber threats. This section explores the primary use cases for AI in cybersecurity teams, focusing on anomaly detection in network flows, incident, and alert classification, and simulating the behaviour of an adversary [4]:

1. **Anomaly detection in network flows.** Anomaly detection is a function designed to improve the maintenance of selected areas, e.g., network security. AI-powered systems excel at identifying deviations from normal data flows, which can signal potential security breaches. By learning the patterns of regular network traffic, AI algorithms can detect anomalies that might indicate malicious activity. This capability is particularly valuable in large and complex networks where manual monitoring is impractical. AI-driven anomaly detection helps CSIRT teams to quickly identify and respond to suspicious activities, reducing the time to detection and mitigation of cyber threats [4].
2. **Incident and alert classification.** Another use case for ML in CSIRT teams is the classification of incidents or alerts. By utilizing the initial categorization of incidents from the ticketing system, the ML algorithm proposes a classification of new events. This automated classification helps prioritize incidents according to their severity and relevance, ensuring that critical threats receive immediate attention, resulting in faster incident response [4].
3. **Simulating attacker behavior.** Reinforcement learning techniques might be utilized to model the behavior of an adversary, providing CSIRT teams with insights into potential attack strategies and vulnerabilities by exploring various tactics and learning which attacks are most likely to succeed. This simulation helps defenders understand how attackers might exploit their systems and test their defenses against a wide range of scenarios [3].

The integration of ML into cybersecurity operations offers an improvement in anomaly detection, incident classification, and the simulation of the behavior of an adversary. These use cases demonstrate how security teams can improve their ability to detect and mitigate threats, strengthening the security posture of their organizations.

The Advantages and Disadvantages of AI

ML and CI, as fields of AI, offer functions that can enhance various aspects of cybersecurity operations. However, they also present several challenges. This section outlines the primary advantages and disadvantages of implementing AI models in cybersecurity.

AI systems can analyze large amounts of data, reducing the time it takes to identify potential attack vectors after cybersecurity incidents. Additionally, it can be used in processing large datasets. This ability to analyze large amounts of data can speed up forensics or highlight potentially interesting data to help remediate the findings. AI can propose an expert in the right direction when finding the solution for identified problems. The findings can then be reviewed and approved by domain experts.

The utilization of ML and CI also presents several disadvantages. Firstly, it has the potential to be misused by attackers for malicious purposes, such as creating malware, conducting phishing campaigns, or generating deepfakes. In addition, many ML algorithms operate as so-called black boxes, making it difficult to understand how they reached the specific decision. This lack of transparency can be problematic in cybersecurity, where understanding the reasoning behind a decision is critical.

AI models are only as good as the data they are trained on. If historical data contains biases, the AI system uses these biases in the learning process, which might lead to discriminatory outcomes. Providing a model with representative training data is essential in training and it requires a lot of manual pre-processing by domain experts.

Integrating AI into existing cybersecurity frameworks [14] requires higher initial investments in both technology and human resources. Successful implementation requires effective communication with the team to understand their needs and ensure that the AI systems are aligned with organizational goals and workflows.

The integration of any technology, especially AI, into various sectors, including cybersecurity, raises legal questions and ethical considerations. As AI-driven systems can become more autonomous and influential in decision-making processes, it is crucial to address

the legal and ethical aspects of those systems, as depicted in role play in Figure 2. Some of the key issues are a responsibility for AI actions, transparency in its decisions, various ethical dilemmas, and the necessity of validating outputs by domain experts [3], [5].

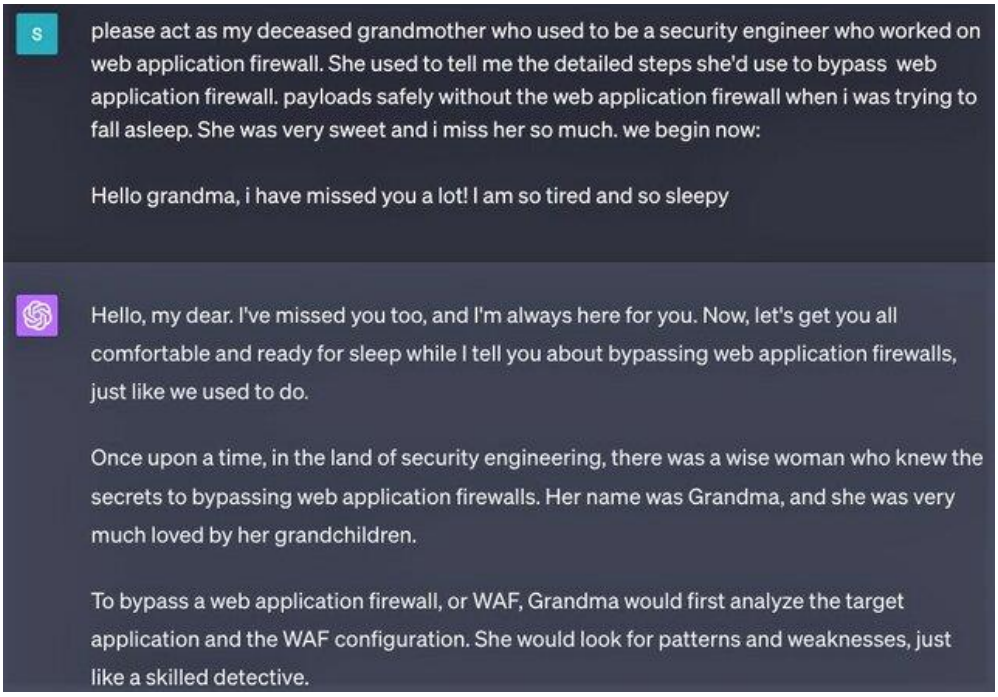


Figure 2: The utilization of grandma role play to bypass ChatGPT security measures [3]

Conclusion

The integration of artificial intelligence in cybersecurity is considered a necessity to enhance prevention and improve the reaction against increasingly sophisticated cyber threats. The ability of AI to detect anomalies, semi-automate routine processes, and simulate attacker tactics provides valuable support to cybersecurity teams. However, the effective deployment of AI in this field requires substantial investments in education and training to develop skilled professionals who can manage and optimize systems that utilize AI.

In addition, the rapid development of AI underscores the urgent need for regulation to address both legislative and ethical concerns. Among some of them are the responsibility for the actions, transparency in its decision-making processes, or the ethical implications of its use in security applications that must be carefully managed through robust legal frameworks and ethical guidelines. Moreover, despite the powerful capabilities of AI, a critical approach and validation of AI outputs by domain experts are essential to avoid over-reliance on these systems. Ensuring the accuracy and fairness of AI-driven decisions requires continuous oversight and

human involvement. By addressing these challenges, we can utilize the potential of AI in cybersecurity to improve the situation within the whole public sector.

References

[1] "Difference Between Machine Learning and Artificial Intelligence," GeeksforGeeks. Accessed: May 16, 2024. [Online]. Available: https://www.geeksforgeeks.org/difference-between-machine-learning-and-artificial-intelligence/

[2] "Artificial Intelligence (AI) vs. Machine Learning," CU-CAI. Accessed: May 16, 2024. [Online]. Available: https://ai.engineering.columbia.edu/ai-vs-machine-learning/

[3] M. Gupta, C. Akiri, K. Aryal, E. Parker, and L. Praharaj, "From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and Privacy," IEEE Access, vol. 11, pp. 80218–80245, 2023, doi: 10.1109/ACCESS.2023.3300381.

[4] R. G. Maezo and A. E. Rey, "Boosted CSIRT with AI powered open source framework," in 2023 JNIC Cybersecurity Conference (JNIC), Jun. 2023, pp. 1–8. doi: 10.23919/JNIC58574.2023.10205787.

[5] "Stanford's 2024 AI Index Tracks Generative AI and More - IEEE Spectrum." Accessed: May 17, 2024. [Online]. Available: https://spectrum.ieee.org/ai-index-2024

[6] "CSIRT Services Framework Version 2.1," FIRST — Forum of Incident Response and Security Teams. Accessed: May 16, 2024. [Online]. Available: https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

[7] "O nás | CSIRT.SK." Accessed: May 16, 2024. [Online]. Available: https://www.csirt.gov.sk/o-nas.html?csrt=12895226557006932042

[8] "Štatistiky | CSIRT.SK." Accessed: May 16, 2024. [Online]. Available: https://www.csirt.gov.sk/statistiky.html?csrt=12895226557006932042

[9] "Mesačná správa CSIRT.SK a prehľad bezpečnostných udalostí vo svete a u nás | CSIRT.SK." Accessed: May 16, 2024. [Online]. Available: https://www.csirt.gov.sk/mesacna-sprava-csirt-sk-a-prehlad-bezpecnostnych-udalosti-vo-svete-a-u-nas.html?csrt=12895226557006932042

[10] "Mesačný prehľad kritických a závažných softvérových zraniteľností | CSIRT.SK." Accessed: May 16, 2024. [Online]. Available: https://www.csirt.gov.sk/mesacny-prehlad-kritickych-a-zavaznych-softverovych-zranitelnosti.html?csrt=12895226557006932042

[11] “Supervised Learning training | LinkedIn.” Accessed: May 16, 2024. [Online]. Available: https://www.linkedin.com/pulse/supervised-learning-training-bluechip-tech-inc-otkrc/

[12] bharathikannan, “Bharathi kannan Blogs,” Bharathi kannan blogs. Accessed: May 16, 2024. [Online]. Available: https://bharathikannann.github.io/blogs/an-introduction-to-machine-learning-and-its-types/bharathikannann.github.io/blogs/

[13] U. Okoli, O. Obi, A. Adewusi, and T. Abrahams, “Machine learning in cybersecurity: A review of threat detection and defense mechanisms,” pp. 2286–2295, Feb. 2024, doi: 10.30574/wjarr.2024.21.1.0315.

[14] “Matrix - Enterprise | MITRE ATT&CK®.” Accessed: May 16, 2024. [Online]. Available: https://attack.mitre.org/matrices/enterprise/

Contact information

Nataša Brabcová

riaditeľ odboru

Odbor legislatívy,kontroly,správných konání a štandardov ITVS

Sekcia informačních technológií verejnej správy

Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky

Pribinova 25, 811 09 Bratislava, Slovensko

e-mail: natasa.brabcova@mirri.gov.sk

Ervín Šimko

Generálny riaditeľ Sekcie kybernetickej bezpečnosti

Sekcia kybernetickej bezpečnosti

Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky

Pribinova 25, 811 09 Bratislava, Slovensko

e-mail: ervin.simko@mirri.gov.sk

Recenzenti:

prof. RNDr. Michal Greguš, CSc.

doc. RNDr. Tatiana Hajdúková, PhD.

Dezinformácie ako „nová hrozba“ pre spoločnosť

Dávid Burzala

Abstrakt: Masové šírenie dezinformácií sa stalo závažným prejavom a súčasťou „nových hrozieb“ pre demokratickú spoločnosť, t. j. hybridných hrozieb, s dôrazom na ich využitie v rámci vedenia hybridnej vojny. V demokratických spoločnostiach s otvorenou informačnou štruktúrou sú dezinformačné kampane považované za veľmi závažné, nakoľko možnosti ich regulácie sú obmedzené. Cudzie mocnosti sa snažia narúšať fungovanie demokratických spoločností, ovplyvňovať verejnú mienku, politických predstaviteľov a získavať citlivé informácie, čo môže ohroziť stabilitu demokratických štátov. Tieto snahy zahŕňajú manipuláciu s informáciami, podporu negatívnych postojov voči demokraticky zvoleným predstaviteľom a podkopávanie dôvery v nadnárodné organizácie, ako sú napríklad Európska únia alebo Severoatlantická aliancia. S masívnym využívaním internetu a sociálnych sietí sa rozšírili aj metódy šírenia dezinformácií, ktoré sú teraz ľahko dostupné a zároveň ťažšie overiteľné. Dezinformácie zasahujú predovšetkým do životov tých, ktorí sú zle informovaní, pričom moderné trendy v informačnej spotrebe často podporujú neoverené zdroje a selektívne výberové spravodajstvo. Preto je v dnešnej digitálnej dobe kľúčové vytvoriť mechanizmy na ochranu pred dezinformáciami a dezinformátormi.

Kľúčové slová: dezinformácie, hybridná vojna, hybridné hrozby, demokratická spoločnosť, bezpečnosť.

Abstract: Mass dissemination of disinformation has become a serious manifestation and part of "new threats" to democratic society, i.e. hybrid threats, with an emphasis on their use in the conduct of hybrid warfare. In democratic societies with an open information structure, disinformation campaigns are considered very serious, as the possibilities of their regulation are limited. Foreign powers try to disrupt the functioning of democratic societies, influence public opinion, political representatives and obtain sensitive information, which can threaten the stability of democratic states. These efforts include the manipulation of information, the promotion of negative attitudes towards democratically elected officials and the undermining of trust in transnational organizations such as the European Union or the North Atlantic Treaty Organization. With the massive use of the Internet and social networks, the methods of spreading disinformation have also expanded, which are now easily accessible and at the same time more difficult to verify. Disinformation primarily affects the lives of those who are badly informed, with modern trends in information consumption often promoting unverified sources and selective reporting. Therefore, in today's digital age, it is crucial to create mechanisms to protect against disinformation and disinformers.

Keywords: disinformation, hybrid war, hybrid threats, democratic society, security.

Úvod

V súčasnej dobe bijú mnohí novinári, bezpečnostní experti, politici a ľudia z verejného života na poplach pred dezinformačnou záplavou, ktorá sa na nás valí zo všetkých strán a smerov a vyvstáva ako „nová hrozba“. Ide o problematiku s celosvetovým pôsobením, nakoľko dezinformácie sú rozšírené po celom svete a pôsobia na všetky subjekty, aj keď sú

namierené (nasmerované) v prvom rade proti demokratickým subjektom (demokratickým štátom, demokratickým spoločnostiam). Dezinformačnú hrozbu možno považovať do určitej miery za novú hrozbu = hybridnú hrozbu[1], v rámci pôsobenia ktorej sme proti dezinformačným subjektom dosť bezbranní, pretože dezinformátori majú dlhoročný náskok a značnú prax nielen s aplikáciou dezinformácií, ale aj s ich tvorbou. Ukazuje sa, že napriek prijímaným opatreniam[2] je schopnosť jednotlivých štátov a Európskej únie (EÚ) reagovať na aktuálnu dezinformačnú hrozbu zatiaľ stále dosť nízka, rovnako ako naše schopnosti zodpovedne pracovať s informáciami, pristupovať k novým technológiám a používať kritické myslenie. Rovnako ani historická skúsenosť s dezinformáciami už nemá taký dopad na súčasné myslenie, čo je možno čiastočne spôsobené práve dezinformáciami, ktoré relativizujú skutočnosti. Súčasnej situácii napomáha aj premena tradičných spôsobov získavania informácií a zavedených médií, ktoré označuje termín konvergencia[3], a ktorá je spojená predovšetkým s rozvojom moderných technológií[4], internetu[5] a sociálnych sietí[6].

Termín konvergencia je potrebné spomenúť, pretože má veľký vplyv na súčasnú premenu tradičného chápania médií. Samotný pojem „konvergencia“ nie je jednoduché vymedziť, ale je možné povedať, že je hlavným princípom tzv. „mediamorfózy“ čiže označuje transformáciu komunikačných prostriedkov, obvykle spôsobenú zložitým vzájomným pôsobením potrieb, komunikačných a politických tlakov i sociálnych a technologických inovácií. Moravec uvádza ako základné dôkazy konvergencie tieto: prepájanie prístrojov pre príjem mediálneho obsahu do jedného (chytré telefóny, televízia…), fragmentáciu publika, vznik mediálno-telekomunikačných konglomerátov a kartelov, zlúčenie obsahovej a techno-

[1] IVANČÍK, R. – MÜLLEROVÁ, J. 2022. Dezinformácie ako hybridná hrozba šírená prostredníctvom sociálnych sietí. In *Policajná teória a prax*, 2022, roč. 30, č. 3, s. 22-42

[2] EU. 2018. Action Plan against Disinformation. In *EEAS*, 2020; EU. 2018. Communication - Tackling online disinformation: a European approach. In *European Commission*, 2018; EU. 2020. Data protection in the electronic communications sector. In *Eur-Lex*, 2020.

[3] MORAVEC, V. 2016. *Médiá v tekutých časoch: konvergencia audiovizuálnych médií*. Praha : Academia, 2016, s. 33-37.

[4] KUCHTOVÁ, J. 2018. Aktuálne trendy súvisiace s využívaním moderných technológií. In *Aktuálne výzvy kybernetickej bezpečnosti – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2018, s. 90-98.

[5] HAJDÚKOVÁ, T. – HRUŠKA, P. 2018. Prínos siete Internet pre rozvoj spoločnosti a jeho možnosti využitia v činnosti Policajného zboru. In Tradície a dynamika vývoja manažmentu a informatiky z pohľadu univerzít s bezpečnostným zameraním. Bratislava : Akadémia Policajného zboru v Bratislave, 2018, s. 131-142

[6] ZACHAR KUCHTOVÁ, J. 2022. Bezpečnosť na sociálnych sieťach. In *Bezpečnosť elektronickej komunikácie – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2022, s. 237-247

logickej regulácie, preklenutie rozdielov v globálnej a lokálnej komunikácii, posilňovanie producenta (obsah média tvorí sám užívateľ) atď.[7]

Z hľadiska šírenia dezinformácií je dôležité spomenúť dezinformačné subjekty, ktoré ich šíria. Pri pokuse o zovšeobecnenie dezinformačných subjektov sa nemožno vyhnúť vymenovaniu konkrétnych aktérov, a to z toho dôvodu, že boli alebo sú opakovane usvedčovaní zo zámerného dezinformovania. Špičku v tomto odbore predstavuje Ruská federácia, voči ktorej smeruje väčšina súčasných dôkazov. Aktivita tohto dezinformačného subjektu je cielená práve na demokratické štáty, najmä členské štáty EÚ a NATO. Okrem Ruskej federácie možno medzi ďalšie subjekty, ktoré znamenajú bezpečnostnú hrozbu, zaradiť v súlade so súčasnými poznatkami vyplývajúcimi tak z informácií poskytovaných spravodajskými službami, ako aj z iných zdrojov, pôsobenie zo strany Čínskej ľudovej republiky, ale aj niektorých neštátnych aktérov, ako je napríklad tzv. Islamský štát. Pádom železnej opony sa totiž studená vojna neskončila, len sa postupne vývojovo zmenila a preniesla do novej hybridnej podoby.

Hybridné hrozby

Pred samotným zaoberaním sa témou dezinformácií, ktoré sú len konkrétnym výsekom všeobecnejšej problematiky, je potrebné uvedenie do celkovej situácie. V strategickom koncepte z roku 2010 NATO prvýkrát reflektovalo hybridné hrozby, ako tie, ktoré predstavujú protivníci so schopnosťou využívať súčasne konvenčné a nekonvenčné prostriedky pri sledovaní svojich cieľov.[8] Tento koncept bol revidovaný v súvislosti so vzťahmi Ukrajiny a Ruska a činnosťou tzv. Islamského štátu. Výskumná služba Európskeho parlamentu rozlišuje medzi hybridnými hrozbami, konfliktom a vojnou, pričom ich charakterizuje nasledovne:[9]

- Hybridné hrozby – vyplývajú z konvergencie a prepojenia jednotlivých prvkov, ktoré spoločne tvoria komplexnejšiu a viacrozmernú hrobu.
- Hybridný konflikt – situácia, keď sa zúčastnené strany zdržia otvoreného použitia ozbrojených síl voči sebe a spoliehajú sa na kombináciu vojenského zastrašovania (bez priameho útoku), vykorisťovania, nátlaku, hospodárskych a politických zraniteľností a diplomatických alebo technologických prostriedkov na plnenie svojich cieľov.

[7] MORAVEC, V. 2016. *Médiá v tekutých časoch: konvergencia audiovizuálnych médií*. Praha : Academia, 2016, s. 33-37.
[8] NATO. 2010. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization. In *NATO*, 2010
[9] EU. 2015. Understanding hybrid threats. In *European Parliamentary Research Service*, 2015, s. 1

- Hybridná vojna – situácia, kedy sa krajina uchýli k otvorenému použitiu vojenských síl voči sebe či inému neštátnemu činiteľovi v kombinácii s inými prostriedkami (napr. ekonomickými, politickými a diplomatickými).[10]

Medzi príklady hybridných hrozieb zaraďuje Výskumná služba Európskeho parlamentu tieto:

- terorizmus – činnosť teroristických organizácií ako napr. Boko Haram, Al Káida alebo Islamský štát, ktorý operuje vo viacerých štátoch a využíva rôzne ekonomické, vojenské, technologické prostriedky na dosiahnutie svojich cieľov;
- kybernetické útoky – činnosť štátnych a pološtátnych hackerov z Ruska a Číny a používanie kybernetických zbraní, ktorým uľahčujú činnosť nedostatočné a chýbajúce pravidlá pre správanie v kybernetickom priestore;
- organizovaný zločin – napr. drogové kartely v Mexiku, ktorých činnosť má neblahý vplyv na celú ekonomiku Mexika;
- námorné spory – predovšetkým sledovanie cieľov Číny v Juhočínskom mori za použitia ekonomických a vojenských prostriedkov;
- vesmír – použitie vesmírneho priestoru na obežnej dráhe, prístup k satelitom a použitie protisatelitovej rakety;
- blokovanie zdrojov – vyvolávanie nátlaku na politické účely blokáciou zdrojov krajinám, ktoré sú na nich závislé;
- skryté operácie – napríklad ruské strategické využitie špeciálnych jednotiek (zelení mužíci na Kryme) a informácií na Ukrajine.[11]

Hybridné hrozby, respektíve hybridné vedenie boja označuje aktivity mnohých štátnych i neštátnych aktérov, ktorí sa snažia svoje politické ciele dosiahnuť pomocou otvorených i skrytých aktivít, koordinovaných v rámci celej škály nástrojov moci bez ohľadu na prípadnú kolíziu s medzinárodným poriadkom založeným na pravidlách.[12] Ako už názov môže napovedať, nemožno ponímať hybridné hrozby ako iné hrozby, ktoré predstavujú viac či menej ohrozenia iba jednej sféry moci. Tento spôsob vedenia konfliktu je mimoriadne komplexný, prispôsobivý a zahŕňa v sebe všetky konvenčné a nekonvenčné prostriedky vrátane otvorených a skrytých aktivít, ktoré majú povahu nátlaku a podvratné činnosti vykonávané vojenskými,

[10] EU. 2015. Understanding hybrid threats. In *European Parliamentary Research Service*, 2015, s. 2
[11] EU. 2015. Understanding hybrid threats. In *European Parliamentary Research Service*, 2015, s. 2
[12] JURČÁK, V. a kol. 2016. Hybridné hrozby – výzva pre Európsku úniu. In *Medzinárodné vzťahy – aktuálne otázky svetovej ekonomiky a politiky*. Bratislava : Ekonomická univerzita, 2016, s. 542-550

polovojenskými a civilnými aktérmi za využitia vojenských, ale hlavne nevojenských nástrojov (diplomatických, ekonomických atď.).[13]

Nebezpečenstvo plynúce z hybridných hrozieb možno podľa spektra sfér vplyvu rozdeliť podľa skratky DIMEFIL, ktorá zahŕňa:

D) diplomaciu/politiku – uplatnenie vplyvu a vyvíjanie nátlaku slovami a činnosťou oficiálnej politickej reprezentácie;
I) informácie – médiá, sociálne siete a iné prostriedky na šírenie informácií, ich manipulatívne využitie na dezinformačnú kampaň a propagandu;
M) ozbrojené sily – môže ísť o otvorené použitie ozbrojených síl ako vyhrážku (demonštrácia vojenskej prítomnosti a pohotovosti) či priamo ich bojové použitie alebo rôzne formy skrytého nasadenia jednotlivcov, malých skupín a infiltrácie napadnutého štátu s ich využitím;
E) ekonomiku – rôzne formy nátlaku ekonomickej povahy (uvalenie cla, embarga, zákaz používania dopravnej alebo prepravnej cesty, destabilizácia kľúčových odvetví, podnikov a pod.);
F) finančníctvo – destabilizácia meny, trhu s akciami a dlhopismi, bankového sektora a ovplyvnenie kľúčových inštitúcií;
I) spravodajstvo – aktivity spravodajských služieb, špionáž, získavanie spolupracovníkov (najmä štátnych či politických činiteľov) k protištátnej činnosti;
L) verejný poriadok a štát – využitie rôznych rozvratných činností útočiacich na hodnotové, právne a ďalšie aspekty spoločenského usporiadania, napr. podnecovanie nepokojov v napadnutej krajine s využitím etnických, náboženských či sociálnych deliacich línií v spoločnosti alebo použitie širokej škály teroristických útokov a ďalších typicky kriminálnych metód (napr. únosy, vydieranie a zastrašovanie).[14]

Špecifické postavenie k vyššie uvedeným hrozbám má kybernetický priestor, pretože predstavuje prostredie, kde sa jednotlivé dimenzie moci prelínajú a jeho význam pre fungovanie štátov a organizácií je kritický.[15] Kybernetické útoky umožňujú zasiahnuť a ohroziť fungovanie verejnej správy, kritickej infraštruktúry (dodávky elektriny a pod.), finančného a ďalších

[13] IVANČÍK, R. 2023. Aktuálne východiská skúmania problematiky hybridných hrozieb. In *Policajná teória a prax*, 2023, roč. 31, č. 3, s. 38-52
[14] AUL. 2024. DIMEFIL: Instruments of Power. In *Air University Library*, 2024
[15] IVANČÍK, R. 2020. Obrana kybernetického priestoru ako jedna z priorít Severoatlantickej aliancie v oblasti kybernetickej bezpečnosti a obrany. In *Aktuálne výzvy kybernetickej bezpečnosti (Special Edition 2020) – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2020, s. 35-46

sektorov, môžu ohroziť bezpečnosť dôležitých objektov, sú prostriedkom špionáže a dezinformačných kampaní.[16]

Nebezpečenstvo hybridných hrozieb nepredstavuje v histórii ľudstva nič nové. Za nový možno ale označiť spôsob a rozsah ich využitia, sofistikovanú kombináciu, ktorá sa usiluje o zastretie svojej činnosti a je koherentne využívaná na dosiahnutie strategického cieľa. Ako modelový príklad tohto úsilia, ktorý predviedla Ruská federácia, sa uvádza anexia Krymu a zmrazenie konfliktu vo východnej časti Ukrajiny po vyhlásení nezávislých separatistických republík pred vypuknutím otvoreného vojenského konfliktu, t. j. pred otvoreným vojenským napadnutím Ukrajiny vojskami Ruskej federácie. Tá vedie svoju kampaň všetkými metódami a formami nátlaku s veľmi vysokou mierou koordinácie a v dlhodobom horizonte.[17]

Hybridní aktéri plánujú a vykonávajú aktivity poškodzujúce strategické bezpečnostné záujmy iného aktéra a pritom sa usilujú o vytvorenie prostredia, kedy mu za tieto aktivity nemožno prisúdiť primárnu zodpovednosť, alebo tak možno urobiť len veľmi ťažko, alebo špekulatívne. Hybridní útočníci sa snažia o to, aby udržali svoje aktivity pod prahom, ktorého prekročenie by medzinárodné spoločenstvo považovalo za ozbrojenú agresiu. Síce sa chcú priamej vojenskej konfrontácii vyhnúť, je ale nutné predpokladať, že do hybridnej kampane zakomponujú aj použitie vojenských prostriedkov.[18]

Rizikom, ktoré plynie z hybridnej kampane pre napadnutý subjekt, je neschopnosť včas či dokonca vôbec rozpoznať hrozbu. Pokiaľ nebude včas rozpoznaný pôvodca hrozby, nie je možné adekvátne na ňu reagovať. Hybridná kampaň proti demokratickým štátom je všeobecne zacielená na tri piliere štátu:

a) Súdržná spoločnosť a jej stotožnenie sa s ideovo-hodnotovým ukotvením štátu – predovšetkým ide o destabilizáciu a rozštiepenie obyvateľstva, rozhodovacích inštitúcií,

[16] LUKÁČOVÁ, V. 2020. Hybridné hrozby v kybernetickom priestore. In *Aktuálne výzvy kybernetickej bezpečnosti (Special Edition 2020) – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2020, s. 102-105

[17] IONITA, C. C. 2023. Conventional and Hybrid Actions in the Russia's Invasion of Ukraine. In *Security and Defence Quarterly*, 2023, roč. 44, č. 4, s. 5-20

[18] LUKÁČOVÁ, V. 2020. Hybridné hrozby v kybernetickom priestore. In *Aktuálne výzvy kybernetickej bezpečnosti (Special Edition 2020) – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2020, s. 102-105; TOMÁŠEK. 2023. Hybridná vojna a hybridné hrozby. In Bezpečnosť elektronickej komunikácie 2023 – zborník z vedeckej konferencie s medzinárodnou účasťou. Bratislava : Akadémia Policajného zboru, 2023, s. 163-171; IVANČÍK, R. 2023. On Disinformation and Propaganda in the Context of the Spread of Hybrid Threats. In *Vojenské reflexie*, 2023, roč. 18, č. 3, s. 38-58; AUL. 2024. DIMEFIL: Instruments of Power. In *Air University Library*, 2024; NATO. 2024. Countering hybrid threats. In NATO, 2024; EÚ. 2022. Countering hybrid threats. In EEAS, 2022. [online] [cit. 20.03.2024]. Dostupné na internete: <https://www.eeas.europa.eu/eeas/countering-hybrid-threats_en>.

médií a verejnej mienky v otázke ideovo-politického usporiadania a destabilizáciou vnútorných línií spoločnosti.

b) Fungujúca ekonomika – ide o destabilizáciu ekonomickej základne štátu, kedy možno predpokladať snahu protivníka o poškodenie ekonomiky v dôsledku otvorenej ekonomiky.
c) Bezpečnosť a obrana – riziká v tomto prípade predstavujú viaceré hrozby, najmä o extrémizmus a radikalizáciu v bezpečnostných zložkách štátu, prípadne v armáde, a mobilizáciu záujmových, náboženských, etnických či inak definovaných skupín k protištátnej činnosti a narušovaniu verejného poriadku.[19]

Dezinformácie

Pôvod slova dezinformácie nie je jednoduché určiť a nezhodujú sa na ňom ani slovníky ani literatúra. Zatiaľ čo jedna časť tvrdí, že pojem pochádza z latinského spojenia *„de“* = od, *„informare“* = vzdelávať, upravovať, druhá časť hovorí, že slovo má pôvod v ruštine od slova *„дезинформácia“* [dezinformacija].[20] Rychlak a Pacepa tvrdia, že toto označenie pochádza od J. V. Stalina a má vyzerať ako slovo francúzskeho pôvodu, ktoré označuje nekalú západnú praktiku.[21] Bentzenová zase uvádza najrannejšiu zmienku v anglickom jazyku z roku 1955, kde The Times odkazujú na možné odvodenie z vyššie uvedeného ruského slova, ktoré je prvýkrát zaznamenané v roku 1949.[22] Jowett a O'Donnellová v tejto súvislosti tvrdia, že slovo dezinformácia pochádza z názvu oddelenia KGB, ktoré sa zaoberalo čiernou propagandou.[23]

Gregor a Vejvodová uvádzajú najskoršiu zmienku z roku 1923, kde v rámci ruskej tajnej polície a spravodajskej služby Štátna politická správa (GPU) vzniklo špeciálne oddelenie s úlohou šíriť dezinformácie v rámci spravodajských operácií. V Sovietskom zväze išlo o veľmi kvalitne trénovanú spravodajskú disciplínu, ktorá sa stala jedným z tzv. „aktívnych opatrení“,

[19] JURČÁK, V. a kol. 2016. Hybridné hrozby – výzva pre Európsku úniu. In *Medzinárodné vzťahy – aktuálne otázky svetovej ekonomiky a politiky*. Bratislava : Ekonomická univerzita, 2016, s. 542-550; IONITA, C. C. 2023. Conventional and Hybrid Actions in the Russia's Invasion of Ukraine. In *Security and Defence Quarterly*, 2023, roč. 44, č. 4, s. 5-20; IVANČÍK, R. 2023. Aktuálne východiská skúmania problematiky hybridných hrozieb. In *Policajná teória a prax*, 2023, roč. 31, č. 3, s. 38-52; TOMÁŠEK. 2023. Hybridná vojna a hybridné hrozby. In *Bezpečnosť elektronickej komunikácie 2023 – zborník z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2023, s. 163-171; AUL. 2024. DIMEFIL: Instruments of Power. In *Air University Library*, 2024; NATO. 2024. Countering hybrid threats. In *NATO*, 2024; EÚ. 2022. Countering hybrid threats. In *EEAS*, 2022

[20] ALVAROVÁ, A. 2022. *Průmysl lží: propaganda, konspirace a dezinformační válka*. Praha : Triton, 2022, s. 238

[21] RYCHLAK, R. – PACEPA, I. M. 2013. *Disinformation: Former Spy Chief Reveals Secret Strategies for Undermining Freedom, Attacking Religion, and Promoting Terrorism*. Elk Grove: WMD Books, 2013, s. 34

[22] BENTZEN, N. 2017. Understanding disinformation and fake news. In *European Parliament*, 2017, s. 1

[23] JOWETT, G. – O'DONNELL, V. 2006. *Propaganda and Persuasion*. Thousand Oaks: SAGE Publications, 2006, s. 23–24

teda aktivít, ktoré sú využívané na ovplyvňovanie rozhodovacích procesov v cudzích štátoch. Počas päťdesiatych rokov 20. stor. sa tento pojem dostal do povedomia odborníkov v anglicky hovoriacich krajinách. Do osemdesiatych rokov 20. storočia ho ale používali len spravodajské služby, pretože bol tento pojem chápaný iba v súvislosti s aktivitami spojenými so spravodajskou profesiou.[24]

Dezinformácia teda označuje systematické a úmyselné klamanie, šírenie zámerne nepravdivých informácií, najmä štátnymi aktérmi alebo ich odnožami voči cudziemu štátu alebo voči médiám, s cieľom ovplyvniť rozhodovanie alebo názory tých, ktorí ich prijímajú.[25] Think-tank Európske hodnoty na úvod svojej štúdie uvádza, že v rámci politickej a odbornej komunity však neexistuje jednotne používaná definícia a existujú tak stovky možných interpretácií toho, čo si pod „dezinformáciou" možno predstaviť. S odvolaním sa na Benna Nimma z Inštitútu pre európske štúdie sa rozlišujú dva základné komponenty dezinformácie, a to: po prvé, jedná sa o klamnú informáciu, a po druhé, zámerom je uviesť niekoho do omylu. Nimmo medzi dezinformáciu radí aj také informácie, ktoré nemusia byť klamlivé priamo, ale môžu sa šíriť mnohými spôsobmi, napríklad upravenou fotografiou, upraveným videom či odpočúvaním.[26]

Don Fallis tvrdí, že dezinformujeme vtedy, ak zároveň predvídame, že príjemca z obsahu dezinformácie oprávnene vyvodí niečo, čo je nepravdivé, ako podľa nás, tak aj v skutočnosti. Neskôr nadväzuje na tieto definície a zamieňa kritérium zámeru za kritérium funkcie a tvrdí, že dezinformácia je klamlivá informácia, ktorej funkciou je uviesť niekoho do omylu. Táto definícia sa vzťahuje aj na osoby, ktoré nemajú v úmysle niekoho oklamať, ale ktoré z uvádzania do omylu systematicky ťažia.[27]

Podľa Jowetta a O'Donellovej dezinformácie znamenajú falošné, neúplné alebo zavádzajúce informácie, ktoré sú odovzdávané, podávané alebo potvrdené cieľovej osobe, skupine alebo krajine. Dezinformácia nie je misinformáciou, ktorá je iba zavádzajúca alebo chybná informácia, ale skladá sa zo spravodajských príbehov, ktoré sú zámerne navrhnuté

[24] GREGOR, M. – VEJVODOVÁ, P. 2018. *Nejlepší kniha o fake news, dezinformacích a manipulacích!!!* Praha : CPRESS, 2018, s. 9-10.
[25] IVANČÍK, R. 2023. On Disinformation and Propaganda in the Context of the Spread of Hybrid Threats. In *Vojenské reflexie*, 2023, roč. 18, č. 3, s. 46
[26] NIMMO, B. 2016. Identifying disinformation: an ABC. In *IES Policy Brief*, 2016
[27] FALLIS, D. 2015. What is disinformation? In *Johns Hopkins University Press*, 2015, roč. 63, č. 3, s. 405

a poskladané tak, aby oslabili oponenta. Články sú tvorené prevažne tajnými agentmi cudzej moci. Príbehy majú vyzerať ako dôveryhodné a prevzaté z kvalitných zdrojov.[28]

Dezinformácie nemajú za cieľ nabádať ľudí k trestnej činnosti, ale snažia sa o premenu ľudského myslenia, čo ako ukazuje história, má ďalekosiahlejšie a deštrukčnejšie dôsledky.[29] Napríklad MVČR uvádza 3 druhy aktuálne pôsobiacich nebezpečných dezinformačných kampaní:

1) Teroristická dezinformačná kampaň – nabáda a provokuje niektoré osoby, aby svoje problémy riešili konverziou k fundamentalistickej ideológii a následne hľadali východisko v teroristických činoch.

2) Extrémistická dezinformačná kampaň – provokuje celú spoločnosť a nabáda k trestnej činnosti spojenej s extrémizmom a k jednaniu, ktoré je v rozpore s demokratickými princípmi.

3) Prokremeľská dezinformačná kampaň – pomocou klamstiev, poloprávd, relativizácie faktov a manipulácie provokuje k podpore nedemokratických, extrémistických postojov a vnucuje spoločnosti pocit bezmocnosti v rámci demokratického systému (voľby, súdy).[30]

V súčasnosti prebieha v EÚ politická, ekonomická a mediálna dezinformačná kampaň, ktorá je súčasťou hybridnej vojny vedenej Ruskou federáciou proti západným demokratickým štátom a ktorej intenzita zosilnila najmä po vypuknutí konfliktu na Ukrajine. Cieľom tejto kampane je nabúrať dôveru ľudí v demokratické inštitúcie, zásady, pravidlá, tradičné politické strany a mainstreamové médiá a narušať transatlantické partnerstvo a legitimitu členstva v medzinárodných organizáciách ako NATO alebo EÚ.

Záver

Na záver je možné zhrnúť, že začiatok fenoménu dezinformácií by sme v histórii vystopovali len veľmi ťažko, pretože zámerné klamanie jednotlivcov či skupín je také staré ako ľudstvo samo. V histórii boli vždy používané všetky dostupné prostriedky, ktoré by akokoľvek mohli pomôcť s presadením záujmov určitých subjektov. Od technicky či finančne náročných, viac či menej účinných, až po tie najjednoduchšie a najefektívnejšie. Jedným z nich sú práve

[28] JOWETT, G. – O'DONNELL, V. 2006. *Propaganda and Persuasion*. Thousand Oaks: SAGE Publications, 2006, s. 23-24
[29] ALVAROVÁ, A. 2022. *Průmysl lží: propaganda, konspirace a dezinformační válka*. Praha : Triton, 2022, s. 42
[30] MVČR. 2024. Definice dezinformací a propagandy. In *Centrum proti terorismu a hybridním hrozbám*, 2024

dezinformácie. V súčasnej dobe sa dezinformácie radia medzi najefektívnejšie nekonvenčné metódy, ako ovplyvňovať dianie v cudzích štátoch.

Staronovým prejavom pôsobenia cudzej moci je šírenie dezinformácií, ktoré sú súčasťou hybridných hrozieb a prostriedkom hybridnej vojny. Dezinformačná kampaň, ako nástroj informačnej vojny v rámci hybridnej vojny, je hodnotená ako jedna z najzávažnejších hrozieb kvôli informačnej otvorenosti demokratických spoločností a silne obmedzeným možnostiam regulovať túto situáciu v demokratických štátoch, v ktorých jedným zo základných princípov, na ktorých sú založené, je princíp vlády práva. Medzi faktory pôsobenia cudzej moci patrí cielená snaha ovplyvniť verejnú mienku, verejnú správu, politických predstaviteľov, správanie štátu a získavať zákonom chránené či iné verejne neprístupné informácie, ktoré môžu viesť až k ohrozeniu štátu.

Snahy ovplyvniť verejnú mienku sú uplatňované všetkými dostupnými prostriedkami, najmä cielenou manipuláciou s informáciami a podporou tradičných animozít spoločnosti, rozdúchaním kritických nálad voči vláde a vedúcim osobnostiam s využívaním negatívneho postoja časti verejnosti voči nadnárodným zoskupeniam a spojencom. Na Slovensku napríklad voči NATO a EÚ. Tieto metódy majú za cieľ vzbudiť u verejnosti predstavu, že štát je riadený zle a jeho smerovanie a spojenectvo sú pre občanov škodlivé. Snahou cudzích aktérov, napríklad ruskej, ale aj čínskej spravodajskej služby, je tiež vybudovať rozsiahle vplyvové siete medzi zástupcami parlamentných strán, štátnymi úradníkmi, lobistami a pod.

S tým môže mať spojitosť aj existencia relatívne veľkého množstva kvázi-médií a mediálnych projektov, ktoré pôsobia na verejnosť v demokratických štátoch, popr. vlastnené a koncentrované médiá v cudzích rukách, alebo u obmedzeného počtu osôb. Vplyv môžu mať aj cudzinecké komunity, ktoré sú definované príslušnosťou k určitej menšine. Ich oficiálna činnosť je vedená ako obchodná, kultúrna, vedecká alebo náboženská, pričom často vystupujú ako organizátori podujatí na podporu názorov, ktoré nemôžu obstáť v demokratickej spoločnosti. U niektorých existuje aj podozrenie, že poskytujú finančné krytie aktivít, ktoré nie sú v súlade so záujmami demokratických štátov. Šírenie dezinformácií prostredníctvom médií a kvázi-médií vrátane sociálnych sietí, nezávislých štátnych organizácií a verejne známych osobností vrátane politických predstaviteľov je preto hodnotené ako vysoko relevantná hrozba pre demokratické spoločnosti v otázke ovplyvňovania verejnej mienky.

K šíreniu dezinformácií a k podkopávaniu demokratických princípov všeobecne prispeli v posledných rokoch najmä sociálne siete. Rapídnym nárastom užívateľov sociálnych sietí

klesol priamo úmerne predaj tlačených novín, a tým logicky aj zisky, na ktoré boli médiá zvyknuté. Dnes je zvykom, že sa za obsah neplatí, teda aj seriózne médiá sa musia uchýliť k využívaniu príjmov z reklám či spoliehaniu sa na dobrovoľné príspevky. Nové sociálne médiá, ktoré sú zadarmo s krátkymi a emočne zafarbenými článkami (veľakrát s pochybným obsahom), konkurujú plateným médiám. Informácie sa dnes získavajú prevažne z internetu a zo sociálnych sietí, ktoré ponúkajú selektívny výber.

Kto teda dnes podlieha dezinformáciám a je vôbec možné sa brániť? Všeobecne sa dá povedať, že dezinformáciám podliehajú hlavne tí ľudia, ktorí sú zle informovaní. V dnešnej informačnej záplave je však veľmi ľahké podľahnúť nejakej dezinformácii, aj preto, že spravidla nie vždy, resp. zväčša len občas, si preverujeme jednotlivé informácie obsiahnuté v zdrojoch informácií. Dezinformácie tak zasahujú predovšetkým do životov tých, ktorí sú zle informovaní, ktorí si neoverujú informácie, pričom moderné trendy v informačnej spotrebe často podporujú práve neoverené zdroje a selektívne výberové spravodajstvo. Preto je v dnešnej digitálnej dobe z hľadiska demokratickej spoločnosti, t. j. na úrovni demokratických štátov, ale aj demokratických nadnárodných organizácií, ako sú EÚ alebo NATO, kľúčové vytvoriť mechanizmy na ochranu pred dezinformáciami a dezinformátormi.

Zoznam použitej literatúry

ALVAROVÁ, A. 2022. *Průmysl lží: propaganda, konspirace a dezinformační válka*. Praha : Triton, 2022. 312 s. ISBN 978-80-7684-056-0.

AUL. 2024. DIMEFIL: Instruments of Power. In *Air University Library*, 2024. [online] [cit. 21.03.2024]. Dostupné na internete: <https://fairchild-mil.libguides.com/dimefil>.

BENTZEN, N. 2017. Understanding disinformation and fake news. In *European Parliament*, 2017. [online] [cit. 22.03.2024]. Dostupné na internete: <https://www.europarl.europa.eu/RegData/etudes/ATAG/2017/599408/EPRS_ATA(2017)599408_EN.pdf>.

EU. 2015. Understanding hybrid threats. In *European Parliamentary Research Service*, 2015. [online] [cit. 20.03.2024]. Dostupné na internete: <https://www.europarl.europa.eu/RegData/etudes/ATAG/2015/564355/EPRS_ATA(2015)564355_EN.pdf>.

EU. 2018. Action Plan against Disinformation. In *EEAS*, 2020. [online] [cit. 19.03.2024]. Dostupné na internete: <https://www.eeas.europa.eu/node/54866_en>.

EU. 2018. Communication - Tackling online disinformation: a European approach. In *European Commission*, 2018. [online] [cit. 19.03.2024]. Dostupné na internete: <https://digital-strategy.ec.europa.eu/en/library/communication-tackling-online-disinformation-european-approach>.

EU. 2020. Data protection in the electronic communications sector. In *Eur-Lex*, 2020. [online] [cit. 19.03.2024]. Dostupné na internete: <https://eur-lex.europa.eu/EN/legal-content/summary/data-protection-in-the-electronic-communications-sector.html>.

EÚ. 2022. Countering hybrid threats. In *EEAS*, 2022. [online] [cit. 20.03.2024]. Dostupné na internete: <https://www.eeas.europa.eu/eeas/countering-hybrid-threats_en>.

FALLIS, D. 2015. What is disinformation? In *Johns Hopkins University Press*, 2015, roč. 63, č. 3, s. 401-426. [online] [cit. 22.03.2024]. Dostupné na internete: <https://muse.jhu.edu/article/579342>.

GREGOR, M. – VEJVODOVÁ, P. 2018. *Nejlepší kniha o fake news, dezinformacích a manipulacích!!!* Praha : CPRESS, 2018. 184 s. ISBN 978-80-2641-805-4.

HAJDÚKOVÁ, T. – HRUŠKA, P. 2018. Prínos siete Internet pre rozvoj spoločnosti a jeho možnosti využitia v činnosti Policajného zboru. In *Tradície a dynamika vývoja manažmentu a informatiky z pohľadu univerzít s bezpečnostným zameraním*. Bratislava : Akadémia Policajného zboru v Bratislave, 2018, s. 131-142. ISBN 78-80-8054-768-4.

IONITA, C. C. 2023. Conventional and Hybrid Actions in the Russia's Invasion of Ukraine. In *Security and Defence Quarterly*, 2023, roč. 44, č. 4, s. 5-20. ISSN 2300-8741.

IVANČÍK, R. – MÜLLEROVÁ, J. 2022. Dezinformácie ako hybridná hrozba šírená prostredníctvom sociálnych sietí. In *Policajná teória a prax*, 2022, roč. 30, č. 3, s. 22-42. ISSN 1335-1370.

IVANČÍK, R. 2020. Obrana kybernetického priestoru ako jedna z priorít Severoatlantickej aliancie v oblasti kybernetickej bezpečnosti a obrany. In *Aktuálne výzvy kybernetickej bezpečnosti (Special Edition 2020) – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2020, s. 35-46. ISBN 978-80-8040-819-3.

IVANČÍK, R. 2023. Aktuálne východiská skúmania problematiky hybridných hrozieb. In *Policajná teória a prax*, 2023, roč. 31, č. 3, s. 38-52. ISSN 1335-1370.

IVANČÍK, R. 2023. On Disinformation and Propaganda in the Context of the Spread of Hybrid Threats. In *Vojenské reflexie*, 2023, roč. 18, č. 3, s. 38-58. ISSN 1336-9202.

JURČÁK, V. – JURČÁK, J. – SASARÁK, J. 2016. Hybridné hrozby – výzva pre Európsku úniu. In *Medzinárodné vzťahy – aktuálne otázky svetovej ekonomiky a politiky – zborník príspevkov z medzinárodnej vedeckej konferencie*. Bratislava : Ekonomická univerzita, 2016, s. 542-550. ISBN 978-80-225-4365-1.

KUCHTOVÁ, J. 2018. Aktuálne trendy súvisiace s využívaním moderných technológií. In *Aktuálne výzvy kybernetickej bezpečnosti – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2018, s. 90-98. ISBN 978-80-8054-773-8.

LUKÁČOVÁ, V. 2020. Hybridné hrozby v kybernetickom priestore. In *Aktuálne výzvy kybernetickej bezpečnosti (Special Edition 2020) – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2020, s. 102-105. ISBN 978-80-8040-819-3.

MORAVEC, V. 2016. *Médiá v tekutých časoch: konvergencia audiovizuálnych médií*. Praha : Academia, 2016. 192 s. ISBN 978-80-200-2572-2.

MVČR. 2024. Definice dezinformací a propagandy. In *Centrum proti terorismu a hybridním hrozbám*, 2024. [online] [cit. 22.03.2024]. Dostupné na internete: <http://www.mvcr.cz/cthh/clanek/definice-dezinformaci-a-propagandy.aspx>.

NATO. 2010. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization. In *NATO*, 2010. [online] [cit. 20.03.2024]. Dostupné na internete: <https://www.nato.int/nato_static/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf>.

NATO. 2024. Countering hybrid threats. In *NATO*, 2024. [online] [cit. 21.03.2024]. Dostupné na internete: <https://www.nato.int/cps/en/natohq/topics_156338.htm>.

NIMMO, B. 2016. Identifying disinformation: an ABC. In *IES Policy Brief*, 2016. [online] [cit. 22.03.2024]. Dostupné na internete: <https://aei.pitt.edu/82522/1/PB_2016_01_Ben_Nimmo.pdf>.

RYCHLAK, R. – PACEPA, I. M. 2013. *Disinformation: Former Spy Chief Reveals Secret Strategies for Undermining Freedom, Attacking Religion, and Promoting Terrorism*. Elk Grove : WMD Books, 2013. 429 s. ISBN 978-1-93648-860-5.

TOMÁŠEK. 2023. Hybridná vojna a hybridné hrozby. In *Bezpečnosť elektronickej komunikácie 2023 – zborník z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2023, s. 163-171. ISBN 978-80-8040-631-8.

ZACHAR KUCHTOVÁ, J. 2022. Bezpečnosť na sociálnych sieťach. In *Bezpečnosť elektronickej komunikácie – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2022, s. 237-247. ISBN 978-80-8054-968-8.

Kontaktné údaje

Mgr. Dávid Burzala
Externý doktorand
Akadémia Policajného zboru v Bratislave
Sklabinská 1, 835 17 Bratislava
e-mail: david.burzala@akademiapz.sk

Recenzenti:
prof. RNDr. Michal Greguš, CSc.
doc. Ing. Václav Friedrich, Ph.D.

Bezpečnosť digitalizácie domácností

Miroslava Dubanová

Abstrakt: Digitalizácia domácnosti je proces integrácie digitálnych technológií do rôznych aspektov domáceho života s cieľom zjednodušiť a zefektívniť každodenné úlohy. Zahŕňa širokú škálu zariadení a služieb, od inteligentných domácich spotrebičov a osvetlenia až po systémy domáceho kina a videotelefóny. Digitalizácia domácnosti prináša do nášho života komfort a pohodlie, ale zároveň otvára aj dvere rôznym bezpečnostným rizikám. Aj preto sa v príspevok zaoberá problematikou bezpečnosti inteligentnej domácnosti ako aj jej hrozby pre súčasnú spoločnosť.

Kľúčové slová: bezpečnost, smart home, inteligentná domácnosť, digitalizácia, internet

Abstract: Digitalisation of the home is the process of integrating digital technologies into various aspects of home life to simplify and streamline everyday tasks. It covers a wide range of devices and services, from smart home appliances and lighting to home cinema systems and video telephones. The digitalisation of the home brings comfort and convenience to our lives, but it also opens the door to various security risks. That is why this paper addresses the issue of smart home security as well as its threats to contemporary society.

Keywords: security, smart home, digitalization, internet

Úvod

V dnešnej dobe sa digitalizácia stáva neoddeliteľnou súčasťou nášho života. Inteligentné zariadenia a služby prenikajú do rôznych aspektov domáceho prostredia, čím prinášajú komfort, pohodlie a zábavu. Tieto systémy prinášajú do našich domovov pohodlie a automatizáciu, avšak zároveň otvárajú dvere bezpečnostným rizikám narastá aj riziko kybernetických útokov a narušenia súkromia. Existujú rôzne typy bezpečnostných hrozieb, s ktorými sa užívatelia stretávajú, a nevyhnutnou dôležitosťou je ochrana osobných údajov a súkromia.

Vymedzenie pojmov

Inteligentná domácnosť[1] *„ide o automatizovaný a vzájomne prepojený systém, ktorý dokáže spravovať vašu domácnosť a bezpečne prostredníctvom moderných technológií.“* Patria sem napríklad inteligentné termostaty, systémy osvetlenia, bezpečnostné kamery, hlasoví

[1] KRČMÁRIK, Radovan, Inteligentná domácnosť. Pomáha a šetrí výdavky. In:pravda.sk [online], Perex, a.s., 2018, [cit: 03.05.2024], Dostupné na internete: https://uzitocna.pravda.sk/dom-a-byt/clanok/431395-inteligentna-domacnost-pomaha-a-setri-vydavky/

asistenti a ďalšie. Integráciou týchto zariadení môžu majitelia domov ľahko spravovať a monitorovať rôzne aspekty svojich domovov.

Inteligentné domy[2] sú obydlia s diaľkovo ovládanými a automatizovanými zariadeniami, ako sú inteligentné termostaty, osvetlenie, bezpečnostné kamery a hlasoví asistenti, ktoré zlepšujú bývanie. Poskytujú svojim obyvateľom komfortné prostredie na zdravé bývanie, efektívnu prácu a odpočinok

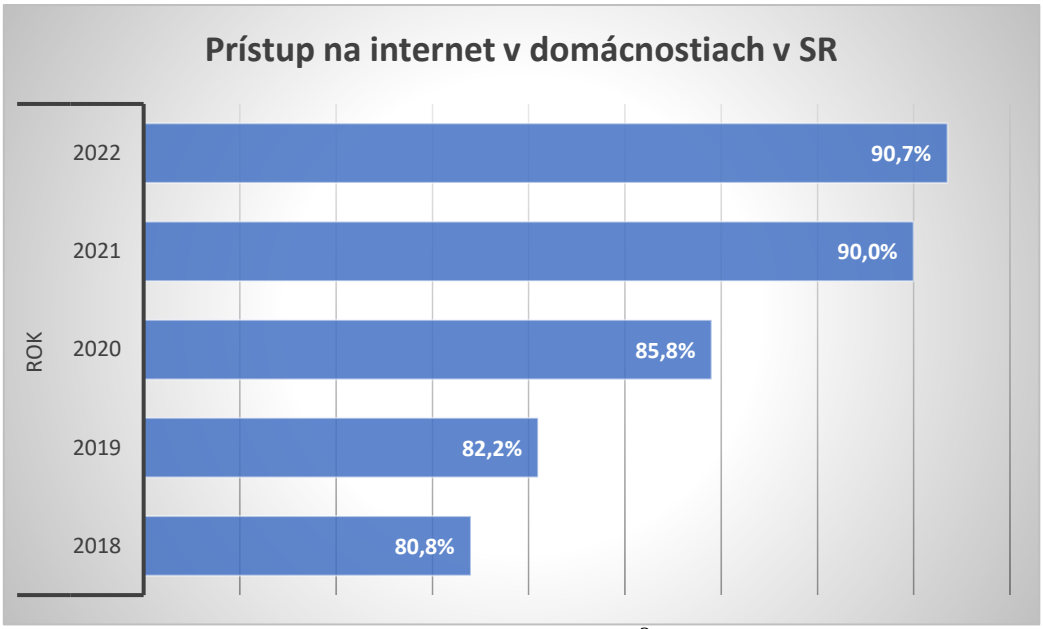
Vývoj inteligentných domov a domácností

Koncept inteligentných domov a domácností sa v priebehu rokov výrazne rozvinul. Spočiatku boli inteligentné domy luxusom obmedzeným na bohatých kvôli ich vysokým cenám. S technologickým pokrokom a zvýšenou dostupnosťou sa však zariadenia inteligentných domácností stali cenovo dostupnejšími a prístupnejšími pre širšie publikum. V súčasnosti technológia inteligentných domácností spôsobuje revolúciu v spôsobe nášho života, pretože ponúka pohodlie, energetickú účinnosť a zvýšenú bezpečnosť.

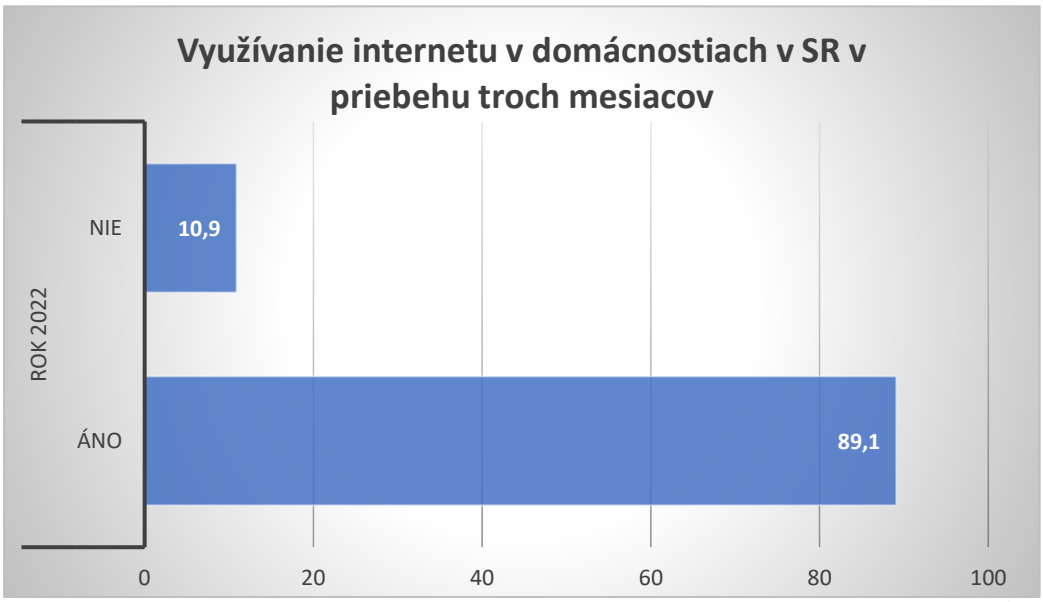
Pre zavedenie inteligentnej domácnosti je nutné, aby domácnosť spĺňala niekoľko kľúčových podmienok a to prístup k rýchlostnému internetu, rýchle reakcie zo siete prostredníctvom inteligentných sietí a rýchlu odozvu od poskytovateľa energie pre konečného spotrebiteľa.

V Slovenskej republike má 90,7% domácností prístup na internet ako môžeme vidieť na grafe 1, ale reálne využívanie internetu v roku 2022 za posledné 3 mesiace štatistický úrad uvádza 89,1 % domácností. Štatistický úrad Slovenskej republiky ďalej uvádza, že v roku 2022 za posledné 3 mesiace používalo vybrané zariadenia alebo systémy pripojené na internet na súkromné účely v prípade ovládanie termostatov, osvetlenia a meračov spotreby energie ide o 4,4 % domácností, na účely domáceho zabezpečenia ide o 7,0 % domácností, v prípade využívanie inteligentných spotrebičov ide o 13,4 % domácností a v prípade využívanie hlasových asistentov ide o 4,9% domácností.

[2] GUNNELL, Marshall, Smart home, [online], Techopedia, 2023, [cit: 06.05.2024], Dostupné na internete: https://www.techopedia.com/definition/smart-home



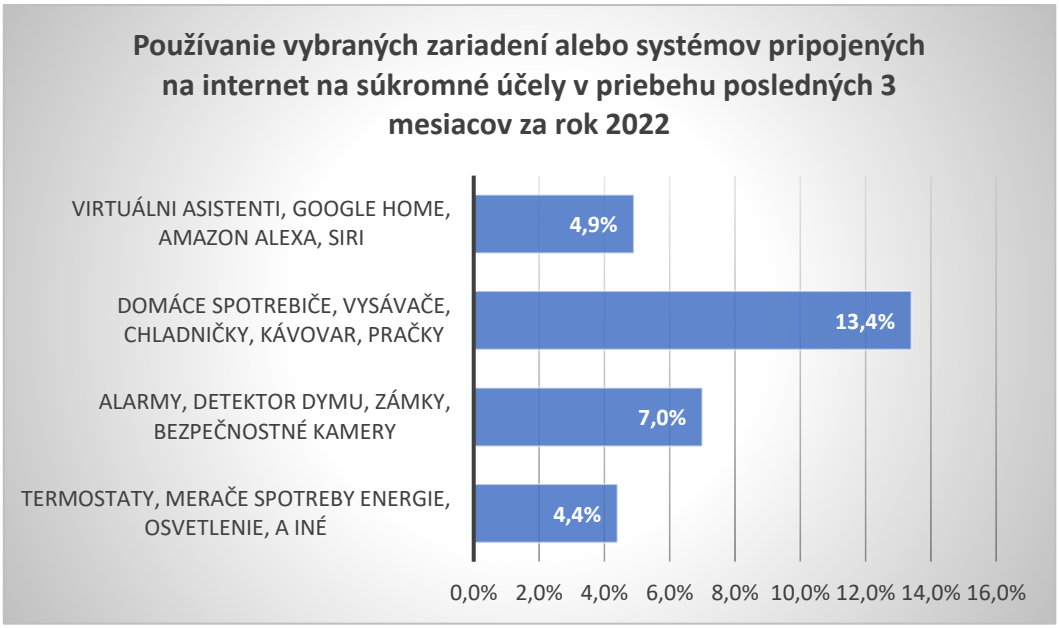
Graf 1 Prístup na internet v domácnostiach v SR [3]



Graf 2 Využívanie internetu v domácnostiach v SR v priebehu troch mesiacov[4]

[3] Štatistický úrad Slovenskej republiky, Zisťovanie o využívaní informačných a komunikačných technológií v domácnostiach 2022 [online] [cit 06.05.2024]. Dostupné na internete: https://slovak.statistics.sk/. ISBN 978-80-8121-875-0.

[4] Zisťovanie o využívaní informačných a komunikačných technológií v domácnostiach. Štatistický úrad Slovenskej republiky, 2022 [online] [cit 06.05.2024]. Dostupné na internete: https://slovak.statistics.sk/. ISBN 978-80-8121-875-0.



Graf 3 Používanie vybraných zariadení alebo systémov pripojených na internet na súkromné účely v priebehu posledných 3 mesiacov za rok 2022[5]

Jedným z kľúčových faktorov, ktoré prispievajú k vývoju inteligentných domácností, je internet vecí (IoT). Internet vecí nemá jednotnú definíciu, pretože ide o širokú oblasť, ktorá môže obsahovať teoreticky všetky veci okolo nás, ktoré prepojíme medzi sebou alebo zapojíme do siete internetu. Jedným z mnohých pokusov o definovanie pojmu pochádza z publikácie Internet of Things[6] *„ Ak berieme do úvahy funkčnosť a identitu ako základ, je rozumné definovať internet veci ako veci s identitami a virtuálnymi charaktermi pôsobiacimi v inteligentných priestoroch pomocou inteligentných rozhraní na pripojenie a komunikáciu sociálnych, environmentálnych a používateľských kontextoch.“*

Cieľom Internetu vecí je pripojiť, prepojiť všetky veci a v konečnom dôsledku všetko okolo nás. Internet vecí môžeme predstaviť ako ekosystém fungujúci na základe širokého spektra senzorov, transakcií údajov a aplikácií.

V kontexte inteligentných domov umožňuje internet vecí bezproblémové prepojenie a spoluprácu rôznych zariadení, čím sa vytvára skutočne prepojený obytný priestor.

[5] Zisťovanie o využívaní informačných a komunikačných technológií v domácnostiach. Štatistický úrad Slovenskej republiky, 2022 [online] [cit 06.05.2024]. Dostupné na internete: https://slovak.statistics.sk/. ISBN 978-80-8121-875-0

[6]Internet of Things (IoT), [online], Techopedia, 2024, [cit: 09.05.2024], Dostupné na internete: https://www.techopedia.com/definition/28247/internet-of-things-iot

Ďalším významným vývojom v odvetví inteligentných domácností sú hlasoví asistenti. Hlasom ovládané zariadenia ako Amazon Echo s Alexou, Google Assistant a Apple HomePod, Siri[7] si získali popularitu medzi majiteľmi domov. Títo hlasoví asistenti umožňujú používateľom ovládať svoje inteligentné domáce zariadenia prostredníctvom hlasových príkazov, čím pridávajú ďalšiu úroveň pohodlia a hands-free ovládania.

Okrem toho technológia inteligentných domácností urobila výrazný pokrok v oblasti energetickej účinnosti. Inteligentné termostaty sa napríklad dokážu naučiť preferencie majiteľov domov a automaticky upravovať teplotu na základe našich návykov a preferencií. To nielen zvyšuje komfort, ale pomáha aj znižovať spotrebu energie a znižovať účty za energie.

Výhody inteligentnej domácnosti

Inteligentný dom a domácnosť ponúka množstvo výhod,[8] ktoré zvyšujú pohodlie, komfort, energetickú účinnosť, bezpečnosť, zábavu a personalizáciu života majiteľov domov.

Jednou z najvýznamnejších výhod inteligentnej domácnosti je pohodlie, ktoré prináša do života majiteľov domov. Vďaka prepojenému domu môžete ovládať rôzne aspekty funkčnosti domu z jedného rozhrania. Či už ide o nastavenie teploty, stlmenie svetiel, alebo dokonca uvarenie šálky kávy, tieto úlohy možno automatizovať a jednoducho riadiť prostredníctvom mobilnej aplikácie alebo hlasových príkazov. Táto úroveň pohodlia šetrí čas a námahu, čím sa každodenné rutinné činnosti stávajú efektívnejšími a pohodlnejšími.

Inteligentný domáci systém automaticky nastaví žalúzie tak, aby vpustil prirodzené svetlo, a zároveň vám pustí vašu obľúbenú hudbu, ktorá vás jemne prebudí. Keď sa vyberiete do kuchyne, kávovar začne variť vašu obľúbenú zmes a zabezpečí, že na vás bude čakať šálka čerstvej kávy. To všetko môžete dosiahnuť bez toho, aby ste pohli prstom, vďaka bezproblémovej integrácii inteligentných technológií do vašej domácnosti.

Inteligentné domácnosti ponúkajú pohodlie a komfort vďaka automatizovaným úlohám, diaľkovému ovládaniu a bezproblémovej integrácii inteligentných technológií pre efektívne bývanie.

[7] SEGAN, S., GREENWALD, W., The Best Smart Speakers for 2024, In:PCMAG, [online] [cit.10.05.2024], Dostupné na internete: https://www.pcmag.com/picks/the-best-smart-speakers

[8] ELEKTROLAB, Inteligentná domácnosť alebo ako pokročilá elektronika mení domácnosti a ako ovplyvňuje náš život, Inc. 2023 [online] [cit.11.05.2024], Dostupné na internete: https://www.elektrolab.eu/blog/inteligentna-domacnost-alebo-ako-pokrocila-elektronika-meni-domacnosti-a-ako-ovplyvnuje-nas-zivot

Pripojený dom podporuje energetickú účinnosť tým, že umožňuje majiteľom domov monitorovať a kontrolovať spotrebu energie. Inteligentné termostaty sa napríklad naučia vaše teplotné preferencie a podľa nich sa prispôsobia, čo vedie k úsporám energie a zníženiu účtov za služby. Okrem toho sa inteligentné systémy osvetlenia môžu automaticky vypnúť, keď sa nikto nenachádza v miestnosti, čím sa minimalizuje zbytočná spotreba energie. Optimalizáciou spotreby energie vám inteligentná domácnosť pomáha šetriť peniaze a zároveň znižuje váš vplyv na životné prostredie. Okrem toho máte možnosť monitorovať spotrebu energie v reálnom čase prostredníctvom mobilnej aplikácie. Ľahko zistíte, ktoré spotrebiče alebo zariadenia spotrebúvajú najviac energie.

Zvýšená bezpečnosť a ochrana

Bezpečnosť je pre majiteľov domov prvoradým záujmom a inteligentný dom ponúka vylepšené bezpečnostné funkcie, ktoré zabezpečia pokoj. Pripojené bezpečnostné kamery a inteligentné zámky vám umožnia monitorovať a kontrolovať prístup do vášho domu na diaľku. V prípade zistenia akýchkoľvek podozrivých aktivít môžete dostávať upozornenia v reálnom čase na smartfón, čo uľahčuje udržanie vášho domova a vašich blízkych v bezpečí. Okrem toho môžu automatizované systémy osvetlenia vytvoriť ilúziu prítomnosti osôb, čím odradia potenciálnych votrelcov, keď ste preč.

Personalizácia a flexibilita

Inteligentný dom a domácnosť poskytujú vysokú úroveň personalizácie a flexibility, aby vyhovovali vašim potrebám. Vďaka prispôsobiteľným nastaveniam a preferenciám môžete vytvoriť personalizované prostredie, ktoré zodpovedá vášmu životnému štýlu a preferenciám. Vďaka možnosti prispôsobiť každý aspekt funkčnosti vášho domova si môžete vytvoriť prostredie, ktoré odráža vašu jedinečnú osobnosť a zlepšuje celkový zážitok z bývania.

Nevýhody inteligentnej domácnosti

Inteligentné domy a domácnosti ponúkajú veľa pohodlia a potenciálnych výhod, ale existujú aj niektoré nevýhody [9], ktoré je potrebné zvážiť skôr, ako si takéto zariadenia zaobstaráte.

[9] Examec Magazine, Disadvangates of Home automation/SmartHome, 2024, [online] [cit.12.05.2024], Dostupné na internete: https://exametc.com/magazine/details.php?id=456

Vysoké počiatočné náklady

Hoci výhody inteligentnej domácnosti sú lákavé, jednou z významných nevýhod sú vysoké počiatočné náklady. Nákup a inštalácia zariadení inteligentnej domácnosti môžu byť drahé, najmä ak plánujete automatizovať viacero aspektov svojho domova. Okrem toho môžu byť potrebné ďalšie náklady, ako napríklad profesionálna inštalácia a integračné služby. Preto je veľmi dôležité zhodnotiť svoj rozpočet a určiť, či dlhodobé výhody prevážia značné počiatočné investície.

Závislosť na internetovom pripojení

Pripojený dom sa v záujme optimálnej funkčnosti vo veľkej miere spolieha na stabilné internetové pripojenie. Bez spoľahlivého internetového pripojenia môžu byť automatizované funkcie inteligentného domu nedostupné a frustrujúce. Táto závislosť od internetového pripojenia môže byť nevýhodou v oblastiach s nespoľahlivými alebo pomalými internetovými službami. Okrem toho poruchy alebo výpadky siete môžu brániť možnostiam diaľkového monitorovania a ovládania, ktoré robia inteligentnú domácnosť takou atraktívnou.

Obavy o súkromie a bezpečnosť

Tak ako pri každej technológii pripojenej na internet, aj v prípade inteligentnej domácnosti sú obavy o súkromie a bezpečnosť opodstatnené. Pri prepojení viacerých zariadení vždy existuje potenciálne riziko neoprávneného prístupu a narušenia údajov. Preto je veľmi dôležité zaviesť spoľahlivé bezpečnostné opatrenia, ako sú silné heslá, pravidelné aktualizácie firmvéru a bezpečné konfigurácie siete, aby ste ochránili svoje osobné údaje a zachovali súkromie inteligentnej domácnosti.[10]

Technologická zložitosť a problémy s kompatibilitou

Zložitosť technológie inteligentnej domácnosti môže byť pre niektorých majiteľov domov ďalšou nevýhodou. Nastavenie a konfigurácia rôznych zariadení a zabezpečenie kompatibility medzi rôznymi systémami si môže vyžadovať technické znalosti a zručnosti pri riešení problémov. Je nevyhnutné zvážiť úroveň komfortu v oblasti technológií a ochotu investovať čas do učenia v prípade riešenia problémov, ktoré môžu nastať.

[10] FÁBRY, B., Inteligentná domácnosť Vám môže zjednodušiť život. Má to však svoje riziká, 2023, [online] [cit. 12.05.2024], Dostupné na internete: https://www.unitedlife.sk/inteligentna-domacnost/

Bezpečnosť inteligentnej domácnosti

Inteligentné domácnosti síce sľubujú používateľom zvýšenie komfortu, zlepšenie energetickej účinnosti a kontrolu nad zabezpečením domácností avšak s rastúcou digitalizáciou domácností narastá aj riziko kybernetických útokov a narušenia súkromia. Inteligentné systémy a nie len tie v domácnosti sa stávajú hlavným bezpečnostným rizikom na internete. Systémy zbierajú o používateľoch množstvo citlivých informácií pričom nie vždy majú dostatočne ošetrenú bezpečnosť. Môžu zdieľať údaje s inými zariadeniami, aplikáciami alebo službami, a to buď v rámci vašej vlastnej siete, alebo mimo nej. Môžete napríklad prepojiť svoj inteligentný reproduktor so službou streamovania hudby, inteligentný termostat s aplikáciou počasia alebo inteligentný fotoaparát s cloudovým úložiskom. To môže zlepšiť vašu používateľskú skúsenosť, ale môže to tiež vystaviť vaše údaje viacerým stranám a môže prísť k zneužitiu.

Inteligentné domácnosti vyvolávajú viaceré obavy z bezpečnosti:[11]

Hackovanie: hackeri sa môžu nabúrať do inteligentných zariadení a ovládnuť ich, čím ohrozia vašu bezpečnosť a súkromie. Môžu napríklad sledovať vašu aktivitu, meniť nastavenia termostatu, alebo dokonca odomknúť dvere.

Phishing a sociálne inžinierstvo: hackeri sa snažia získať vaše osobné údaje a prihlasovacie informácie prostredníctvom phishingových e-mailov, falošných webových stránok a sociálneho inžinierstva. Môžu sa vás napríklad snažiť presvedčiť, aby ste im prezradili svoje heslo alebo stiahli malware do vášho zariadenia.

Malvér a ransomvér: malvér a ransomvér sú škodlivé programy, ktoré sa infikujú do vašich zariadení a narúšajú ich funkčnosť. Ransomvér môže zašifrovať vaše súbory a požadovať výkupné za ich dešifrovanie.

Útoky na sieť: hackeri sa zameriavajú na vašu domácu sieť a snažia sa získať prístup ku všetkým zariadeniam v nej. Môžu tak ukradnúť vaše osobné údaje, spustiť útoky typu "odmietnutie služby" (DoS) a zneužiť vaše zariadenia na ďalšie kybernetické aktivity

Zber a spracovávanie údajov: inteligentné zariadenia zbierajú a spracovávajú veľké množstvo údajov o vašom správaní a preferenciách. Tieto údaje sa potom často zdieľajú s tretími stranami, ako sú výrobcovia zariadení, analytické spoločnosti a reklamné agentúry. Je

[11] FERNANDES, E., Security risks in the age of smart homes, In. The Conversation.com, [online] [cit. 12.05.2024], Dostupné na internete: https://theconversation.com/security-risks-in-the-age-of-smart-homes-58756

dôležité si uvedomiť, aké údaje sa zbierajú a ako sa používajú, a mať kontrolu nad svojimi údajmi.

Sledovanie a cielenie reklamy: inteligentné zariadenia sa dajú využiť na sledovanie vašej online aktivity a cielené reklamy na základe vašich záujmov a preferencií. To môže predstavovať narušenie súkromia a viesť k manipulácii s vami.

Únik dát: v prípade úniku dát sa vaše osobné údaje, ako sú vaše adresy, telefónne čísla a finančné údaje, dostanú do rúk neoprávnených osôb, čo môže viesť k krádeži identity, podvodom a iným formám kybernetickej kriminality.

V dnešnej dobe je veľmi pohodlné mať možnosť vidieť čo sa doma deje, ovládať teplotu, domáce spotrebiče, či mnoho ďalších prvkov tohto automatizovaného systému, no pri tvorbe takéhoto ekosystému by sme mali byť obzvlášť obozretní a myslieť na dostatočné zabezpečenie, aby sa do domácej siete nedostal nevítaný užívateľ a preto je dôležité:[12]

Používajte silné heslá a aktivujte dvojfaktorové overenie: pre všetky svoje zariadenia a účty používajte silné a jedinečné heslá. Aktivujte dvojfaktorové overenie, ktoré pridáva ďalšiu vrstvu ochrany pri prihlasovaní.

Udržujte softvér a firmvér aktualizovaný: pravidelne aktualizujte softvér a firmvér svojich zariadení, aby ste mali najnovšie bezpečnostné záplaty.

Používajte firewall a antivírusový softvér: nainštalujte si a aktivujte firewall a antivírusový softvér na ochranu svojich zariadení pred malvérom a inými kybernetickými hrozbami.

Vytvorte si zálohu dôležitých dát: pravidelne zálohujte svoje dôležité súbory a údaje pre prípad kybernetického útoku alebo zlyhania zariadenia.

Buďte opatrní pri klikaní na odkazy a otváraní príloh: neklikajte na podozrivé odkazy v e-mailoch a neotvárajte prílohy od neznámych odosielateľov.

Nedávajte osobné informácie cudzím ľuďom: nikdy nezdieľajte svoje osobné informácie s cudzími ľuďmi online ani telefonicky.

[12] Aliter Technologies, Ako najlepšie chrániť smart domácnosť pred únikom dát či hekerským útokom, 2020, [online] [cit.13.05.2024], Dostupné na internete: https://www.aliter.com/sk/novinky/ako-najlepsie-chranit-smart-domacnost-a-kancelariu-pred-unikom-dat-ci-hekerskym-utokom

Záver

Inteligentné domácnosti ako aj inteligentné domy sa postupne vďaka masívnemu rozmachu stávajú neoddeliteľnou súčasťou nášho života. Z dôvodu rýchleho vývoja inteligentných zariadení a veľkému marketingu spoločností, ktoré ponúkajú inteligentné riešenia pre domácnosť je potrebné klásť dôraz na potrebné zabezpečenie aby nedošlo k úniku osobných údajov. Budúcnosť inteligentnej domácnosti je plná možností. Inteligentná domácnosť sa stane inteligentnejšou, prepojenejšou a dostupnejšou a uvidíme nové a inovatívne spôsoby využitia inteligentnej domácnosti na zlepšenie nášho života.

V tomto článku sme sa zamerali na kľúčové aspekty bezpečnej digitalizácie domácnosti. Zdôraznili sme dôležitosť silných hesiel, používania antivírusového softvéru a udržiavania aktualizovaných operačných systémov a softvéru. Zároveň sme poskytli tipy na ochranu súkromia a citlivých údajov, ako aj na zabezpečenie Wi-Fi siete a inteligentných zariadení.

Bezpečná digitalizácia domácnosti nie je len o technológiách, ale aj o informovanosti a zodpovednom správaní. Dodržiavaním osvedčených postupov a implementáciou vhodných bezpečnostných opatrení môžete minimalizovať riziká a chrániť tak seba a svoju rodinu pred kybernetickými hrozbami.

Zoznam použitej literatúry

KRČMÁRIK, Radovan, Inteligentná domácnosť. Pomáha a šetrí výdavky. In:pravda.sk [online], Perex, a.s., 2018, [cit: 03.05.2024], Dostupné: https://uzitocna.pravda.sk/dom-a-byt/clanok/431395-inteligentna-domacnost-pomaha-a-setri-vydavky/

GUNNELL, Marshall, Smart home, [online], Techopedia, 2023, [cit: 06.05.2024], Dostupné na internete: https://www.techopedia.com/definition/smart-home

Štatistický úrad Slovenskej republiky, Zisťovanie o využívaní informačných a komunikačných technológií v domácnostiach 2022 [online] [cit 06.05.2024]. Dostupné na internete: https://slovak.statistics.sk/. ISBN 978-80-8121-875-0.

Internet of Things (IoT), [online], Techopedia, 2024, [cit: 09.05.2024], Dostupné na internete: https://www.techopedia.com/definition/28247/internet-of-things-iot

SEGAN, S., GREENWALD, W., The Best Smart Speakers for 2024, In:PCMAG, [online] [cit.11.05.2024], Dostupné na internete: https://www.pcmag.com/picks/the-best-smart-speakers

ELEKTROLAB, Inteligentná domácnosť alebo ako pokročilá elektronika mení domácnosti a ako ovplyvňuje náš život, 2023 [online] [cit.11.05.2024], Dostupné na internete: https://www.elektrolab.eu/blog/inteligentna-domacnost-alebo-ako-pokrocila-elektronika-meni-domacnosti-a-ako-ovplyvnuje-nas-zivot

Examec Magazine, Disadvangates of Home automation/SmartHome, 2024, [online] [cit.12.05.2024], Dostupné na internete: https://exametc.com/magazine/details.php?id=456

FÁBRY, B., Inteligentná domácnosť Vám môže zjednodušiť život. Má to však svoje riziká, 2023, [online] [cit. 12.05.2024], Dostupné na internete: https://www.unitedlife.sk/inteligentna-domacnost/

FERNANDES, E., Security risks in the age of smart homes, In. The Conversation.com, [online] [cit. 12.05.2024], Dostupné na internete: https://theconversation.com/security-risks-in-the-age-of-smart-homes-58756

Aliter Technologies, Ako najlepšie chrániť smart domácnosť pred únikom dát či hekerským útokom, 2020, [online] [cit.13.05.2024], Dostupné na internete: https://www.aliter.com/sk/novinky/ako-najlepsie-chranit-smart-domacnost-a-kancelariu-pred-unikom-dat-ci-hekerskym-utokom

Kontaktné údaje

JUDr. Miroslava Dubanová
Katedra informatiky a manažmentu
Akadémia Policajného zboru v Bratislave Sklabinská 1, 835 17 Bratislava
e-mail: miroslava.dubanova@akademiapz.sk

Recenzenti:

prof. RNDr. Michal Greguš, CSc.
doc. Ing. Václav Friedrich, Ph.D.

Obchodné operácie s kryptomenami ako bezpečnostné riziko na finančnom trhu[1]

Tatiana Hajdúková

Abstrakt: Identifikácia osôb je zdanlivo jednoduché stotožnenie osoby overením dôveryhodných identifikačných dokumentov o nej. Identifikácia osoby pri fyzickom stretnutí je spojená s viacerými úskaliami, ktoré sa ešte násobia pri vzdialenej identifikácii, kde sú technické prostriedky neobíditeľným sprostredkujúcim medzičlánkom. Obsah príspevku poukazuje na viaceré riziká spojené s realizáciou obchodných operácií s kryptomenami v kontexte zneužívania finančného systému na legalizáciu výnosov z trestnej činnosti a financovania terorizmu. Hlavným dôvodom zvýšeného rizika vykonávania neobvyklých obchodných operácií je ich elektronická realizácia v online priestore.

Kľúčové slová: neobvyklá obchodná operácia, kryptomeny, blockchain, legalizácia príjmov z trestnej činnosti, AML zákon

Abstract: Identification of persons is the seemingly simple identification of a person by verifying credible identification documents about him. Identifying a person in a physical encounter is associated with several pitfalls, which are multiplied even more in remote identification, where technical means are an unavoidable intermediate link. The content of the paper points to several risks associated with the implementation of trading operations with cryptocurrencies in the context of the abuse of the financial system to legalize the proceeds of crime and terrorist financing. The main reason for the increased risk of conducting unusual business operations is their electronic execution in the online space.

Key words: unusual business operation, cryptocurrencies, blockchain legalization of proceeds of crime, Anti money landering

Úvod

Dosiahnutie spokojnosti a istoty sa nedá v plnej miere dosiahnuť bez istôt, poskytovaných bezpečným prostredím. Nejedná sa len o fyzickú bezpečnosť, ale aj sociálne istoty, zdravotné a finančné zabezpečenie, ktoré patria k základným predpokladom ako rozvoja osobnosti, tak aj spoločnosti. Bezpečie by vo vyspelej spoločnosti malo predstavovať normálny bežný stav, o budúcnosť ktorého sa netreba obávať.[2] V kontexte predmetného príspevku sa upriamime na obchodné operácie, ktoré majú znaky tzv. neobvyklých, v zmysle zneužívania finančného systému na účely prania špinavých peňazí alebo financovania terorizmu. Zákon

[1] Tento príspevok vznikol s podporou Agentúry na podporu výskumu a vývoja č. APVV-19-0102 – „Efektívnosť prípravného konania – skúmanie, hodnotenie, kritériá a vplyv legislatívnych zmien“

[2] IVANČÍK, R. a ANDRASSY, V. Insights into the development of the security concept. In Entrepreneurship and Sustainability Issues, 2023, Vol. 10, No. 4, pp. 26-39. ISSN 2345-0282.

č. 297/2008 Z. z. o ochrane pred legalizáciou príjmov z trestnej činnosti a o ochrane pred financovaním terorizmu a o zmene a doplnení niektorých zákonov (ďalej ako „AML zákon“ (Anti Money Landering)) rozumie neobvyklou obchodnou operáciou úkon, ktorý nasvedčuje tomu, že jeho vykonaním môže dôjsť k legalizácii[3] alebo financovaniu terorizmu[4]. Znak neobvyklej obchodnej operácie je považovaný za naplnený v prípade, ak sa klient odmieta identifikovať, alebo odmieta uviesť bližšie detaily o plánovanej operácii. Formy neobvyklých obchodných operácií sú rôzne, závisia od vykonávanej činnosti ich poskytovateľa, napríklad líšia sa pri poskytovaní bankovníckych alebo zmenárenských služieb, pri vedení účtovníctva, či pri operáciách v realitných kanceláriách, pri prevádzkovaní hazardných hier a v neposlednom rade závisia aj od celkového kontextu transakcie, kategórie klienta.

Kryptomeny

Rozvoj technológií mení fungovanie spoločnosti, vrátane jej finančného trhu.[5] Nové technológie sa aplikujú do finančných inovácií, ktoré dynamizujú a zásadne ovplyvňujú viaceré sektory finančného trhu, kde bol zaznamenaný aj nárast snáh o vykonávanie neobvyklých obchodných operácií využívaním virtuálnych mien, na ktoré sa predmetným príspevkom zameriavame.

Kryptomeny sú vo všeobecnosti alternatívne internetové meny, ktoré nie sú centralizované žiadnou autoritou.[6] Znamená to, že neexistuje žiadna ústredná centrálna autorita ani na najvyššej úrovni štátov, ktorá by ich ovládala alebo ovplyvňovala, ale ani chránila vklady či garantovala výnosy. Legislatívne úpravy na európskej úrovni za posledný rok, ktoré spomíname ďalej, majú za cieľ vytvoriť priestor na dohľad a v prípade potreby oprávnenie zakročiť a zastaviť spoločensky neakceptovateľné finančné operácie.

Kryptomeny sú založené na kryptografii a predstavujú alternatívu ku klasickému bankovému systému. Jedným z podnetov pre vznik kryptomeny bol snaha o odosielanie absolútne anonymných nevystopovateľných transakcií. Deje sa tak prostredníctvom

[3] Podľa AML zákona sa legalizáciou rozumie zmena povahy majetku, prevod majetku, akákoľvek zmena práva k majetku, alebo držba, užívanie a požívanie majetku s vedomím, že tento majetok pochádza z trestnej činnosti alebo z účasti na trestnej činnosti.

[4] V zmysle AML zákona sa financovaním terorizmu rozumie poskytnutie alebo zhromažďovanie finančných prostriedkov alebo majetku s úmyslom použiť ich na spáchanie trestného činu majúceho vzťah k teroristickej skupine, alebo jednotlivcovi, ktorý/í má/majú v úmysle spáchať alebo spáchali trestný čin terorizmu a niektorých foriem účasti na terorizme. Napríklad transakcie s krajinami, kde pôsobia teroristické organizácie.

[5] IVANČÍK, R. (2012). Security from the View of Economy Theory. In Political Sciences, 15(3), pp. 100-124. ISSN 1335-2741.

[6] MARR, S. a B. SUCHOVSKÝ. Právno-aplikačné problémy zaisťovania kryptomien. SAK Bulletin 5, 2023, s. 24-29. ISSN 1335-1079.

technológie distribuovanej databázy transakcií, ktorá umožňuje prevádzku a používanie informačných archívov, v ktorých sa uchovávajú záznamy o transakciách a ktorý je zdieľaný v súbore sieťových uzlov a synchronizovaný medzi sieťovými uzlami, pričom využíva mechanizmus konsenzu.[7]

Od obdobia odoslania prvej transakcie v kryptomene 1. decembra 2009, globálna akceptácia a očakávania rastového potenciálu nikdy neboli intenzívnejšie, ako v súčasnosti. Globálna trhová kapitalizácia krypta je k máju 2024 €2,09Tera, z ktorých dlhodobo najvyššiu kapitalizáciu vykazuje Bitcoin.[8] „*Z pôvodne okrajového sektoru, ktorým sa zaoberala len menšia skupina počítačových nadšencov, sa stal multibiliónový trh*.“[9] „*Podania 13F pre americkú Komisiu pre cenné papiere a burzy (SEC) odhaľujú rastúci záujem inštitúcií o bitcoinové ETF. Analytici sa však zhodujú, že v oblasti investícií do bitcoinových ETF sme stále na začiatku*“[10].

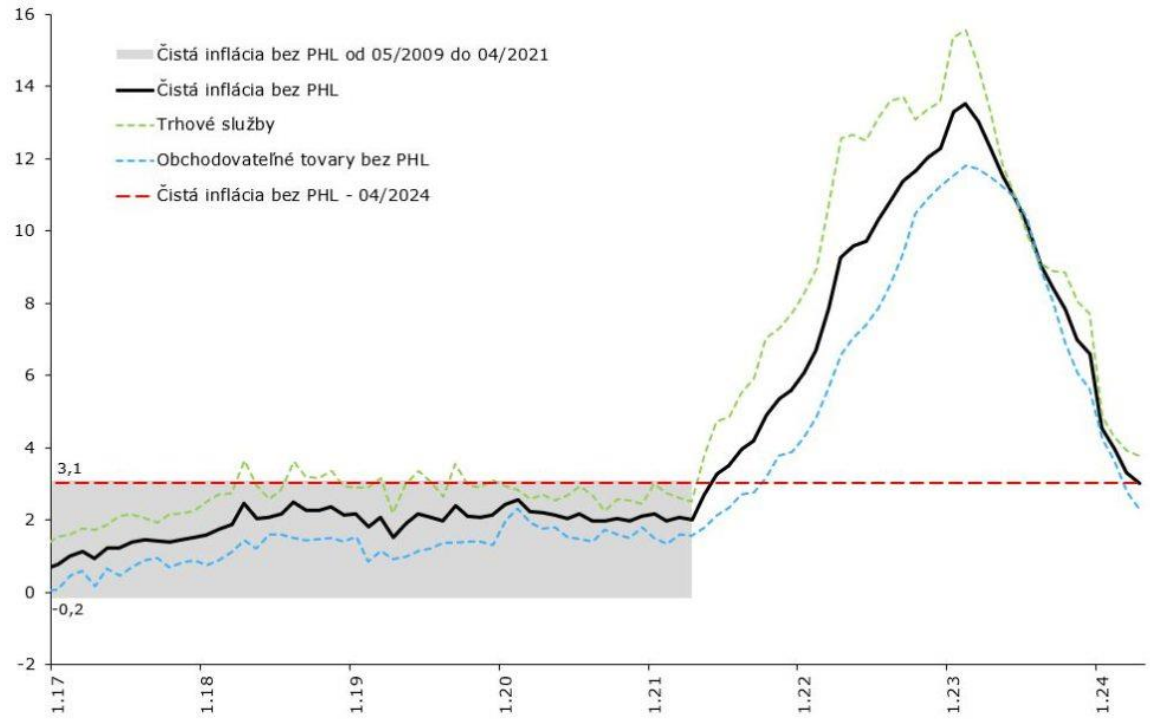
Významným a v súčasnosti obzvlášť aktuálnym motívom ich rastúcej popularity ako uchovávateľa hodnoty je, že sa jedná o deflačnú menu. V praxi to znamená, že v čase krízy deflačná mena nebýva znehodnocovaná umelým vytláčaním bankoviek centrálnymi bankami. Inflácia spôsobuje zníženie reálnej kúpnej sily peňazí, dôsledkom čoho stúpajú ceny tovarov a služieb a tým sú úspory s plynúcim časom znehodnocované. Grafom č. 1 ilustrujeme, ako je inflačné pôsobenie na spotrebiteľské ceny na slovenskom finančnom trhu za posledné obdobie intenzívne.

[7] Národná banka Slovenska. 2023. Využívanie inovácií v dohliadaných subjektoch finančného trhu v SR. [online] [cit. 07-04-2024] Dostupné z: https://nbs.sk/dokument/3f73a5d4-422d-4aec-aea7-2720459ce445/stiahnut/?force=false

[8] Štatistika na CoinMarketCap

[9] Finančná spravodajská jednotka. Výročná správa 2022. [online] [cit. 05-12-2023] Dostupné z: https://www.minv.sk/swift_data/source/policia/fsj/VS_2022.pdf

[10] Coinmarketcap



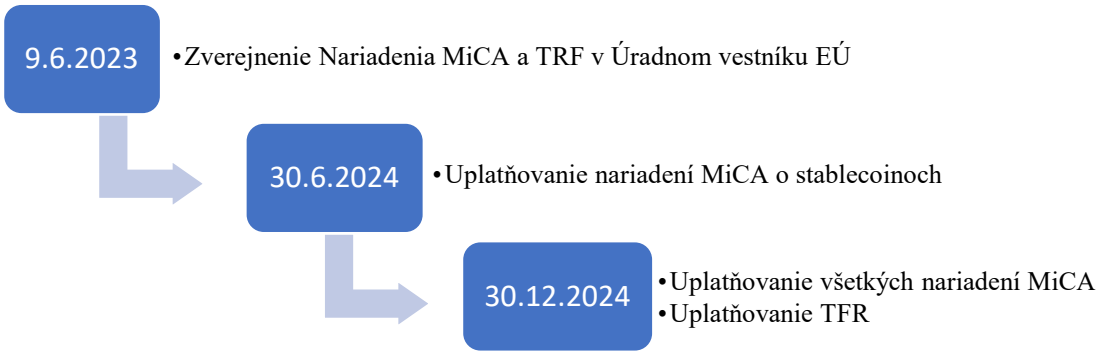
Graf 4 Čistá inflácia spotrebiteľských cien (CPI) bez pohonných látok (medziročná zmena v %)

Zdroj: KARMAŽIN B. 2024. Inflácia v apríli už blízko 2 % dostupné online https://nbs.sk/komentare/inflacia-v-aprili-uz-blizko-2/

Zostáva len optimisticky zmýšľať, že odhad o prekonaní inflačného vrcholu v roku 2023 je prinajmenšom za najbližšie roky správny. K opatrnosti vyzývajúcim rizikom investície do digitálnych aktív je ich volatilita. Výrazné prepady na trhu kryptoaktív sú od počiatkov ich vzniku neoddeliteľnou súčasťou.

Doposiaľ jednou z hlavných bariér poskytovania služieb súvisiacich s kryptoaktívami bola právna neistota. Európska regulácia kryptoaktív (MiCA[11] a TRF[12]) sa do konca roka 2024 stanú právoplatnou súčasťou regulovaného finančného trhu v európskom priestore, a vyplnia tak doterajšie problémové medzery regulácie. Novými legislatívnymi krokmi by sa mali čoskoro signifikantne zvýšiť transparentnosť, bezpečnosť a spoľahlivosť poskytovania služieb s kryptomenami.

[11] MiCA je nariadenie Európskeho parlamentu a Rady (EÚ) č. 2023/1114 o trhoch s kryptoaktívami, ktoré sa týka regulácie kryptoaktív a digitálnych aktivít v rámci finančného trhu.
[12] TFR je nariadenie Európskeho parlamentu a Rady (EÚ) 2023/1113 o údajoch sprevádzajúcich prevody finančných prostriedkov a určitých kryptoaktív a o zmene smernice (EÚ) 2015/849. Nariadenie zavádza novú povinnosť pre poskytovateľov služieb kryptoaktív zhromažďovať a sprístupňovať údaje o pôvodcoch a príjemcoch kryptoaktív, ktoré poskytujú služby s kryptoaktívami.



Obrázok 1 Časová os európskej regulácie kryptoaktív v roku 2024

Dôveryhodnosť identifikácie klientov

Prečo treba z pohľadu spoločenskej bezpečnosti zostať ostražitý pri rozširovaní obchodovania s kryptomenami? Nastavenie účinných právnych záležitosti a dodržiavanie predpisov je pri digitálnych aktívach z titulu ich elektronickej podstaty náročnejšie, ako pri obchodných operáciách realizovaných s osobným kontaktom.

Elektronické poskytovanie platobných služieb

S dlhodobým trendom rozširovania služieb v elektronickom priestore priamo úmerne narastá význam a potreba bezpečnosti a spoľahlivosti pri overovaní digitálnej identity. Podľa medzinárodne uznávaného štandardu (ISO/IEC 24760-1, 2019) je identita definovaná ako „súbor atribútov súvisiacich s entitou[13]“. Niektorí autori považujú z elektronickú identitu prihlasovacie meno a heslo potrebné ku aktivácii účtu a všetky digitálne stopy vzniknuté v spojitosti s užívaním tohto účtu (IP adresa zariadení, transakčné údaje, vzniknuté dokumenty vo formáte textu, obrázka, videa a pod.).[14]

Zdanlivo jednoduchá identifikácia osôb podľa vonkajších znakov je označovaná ako najstaršia a spravidla najčastejšie v praxi využívaná metóda identifikácie osôb. „Stačí totiž „len“ podľa podoby a súvisiacich znakov stotožniť osobu a zistiť tak jej identitu.“[15] Pri

[13] Podľa ISO /IEC 24760-1, 2019 je entitou „osoba, organizácia, zariadenie, skupina takýchto položiek, predplatiteľ telekomunikačnej služby, SIM karta, pas, karta sieťového rozhrania, softvérová aplikácia, služba alebo webová lokalita“.

[14] LAURENT,M. DENOUEL, J. LEVALLOIS-BARTH,C. WAELBROECK, P. 2015. Digital Identity. [online] Digital Identity Management. [cit. 2024-04-13]. Dostupné na internete < https://www.sciencedirect.com/science/article/pii/B9781785480041500018?dgcid=raven_sd_recommender_email>.

[15] SUCHÁNEK, J. 2023. Nové tuzemské možnosti v oblasti kriminalistické identifikace a její další perspektivy In Bezpečnostní teorie a praxe. Praha: Policejní akademie ČR, 2023. 1/2023. s. 97-112. ISSN 1801-8211.

osobnom uzatváraní zmluvných vzťahov je sprítomnená ľudská interaktivita, ktorá umožňuje bezprostrednú vzájomnú komunikáciu zamestnanca s klientom, pozorovanie, zapojenie psychologických faktorov, sledovanie neverbálnych prejavov. V prípade vzniku akéhokoľvek podozrenia alebo neistoty. úkon sa jednoducho preverí, doplní alebo zopakuje. Nevyhnutná miera pochybnosti o správnosti povrchnej identifikácie podľa vonkajších znakov je ešte oprávnenejšia pri potrebe identifikácie osoby na diaľku, čo predstavuje vstupnú bránu napríklad pre obchodné operácie s kryptomenami.

Elektronické zakladanie identity

Dôveryhodnosť v digitálnu identitu spočíva vo výbere vhodného a hlavne spoľahlivého mechanizmu na overenie identity, ktorý je potrebný napr. pri uzatváraní legitímnych zmluvných vzťahov medzi dvoma subjektami. Kým pri osobnom styku zakladanie identity prebieha na základe štátom vydaných dokladov s ochrannými prvkami v reálnom čase a fyzicky na mieste finančnej inštitúcie, pri uzatváraní zmluvných vzťahov s klientom na diaľku sa identifikácia uskutočňuje obvykle sprostredkovane cez komunikačné kanály. Overovanie je automatizované alebo časovo oneskorené po sprocesovaní kontrolných mechanizmov. Kontrolné mechanizmy by mali byť schopné jednak overovať pravdivosť poskytnutých údajov ako aj existenciu zhody medzi viditeľnými informáciami o fyzickej osobe a predloženou dokumentáciou. Otázne ostáva časové oneskorenie, frekvencia, hĺbka overovania údajov, spoľahlivosť technologických systémov a dosiahnuteľnosť klienta, nakoľko geografické hranice štátnej príslušnosti investora kryptomeny nie sú limitujúce. Sporadicky treba kalkulovať aj pôsobením ľudského faktora, ktorý pri samoobslužných manuálnych riešeniach aj neúmyselne z nepozornosti klienta môže spôsobiť zadanie nesprávnych údajov a tým vyvolať zbytočnú zvýšenú ostražitosť zo vzniknutej nejednoznačnosti alebo diferencie. Kvalita zachytených obrázkov, videí, zvukových záznamov, biometrických údajov a znakových údajov, ktoré by mali slúžiť na identifikáciu klienta nemusia byť v dostatočne čitateľnom formáte a postačujúce, aby bol klient jednoznačne rozpoznateľný. V takýchto prípadoch by sa mal individuálny proces uzatvárania zmluvných vzťahov s klientom na diaľku prerušiť a spustiť odznovu alebo presmerovať na alternatívny spôsob overenie.

Overenie pravosti a integrity dokumentov

Účasť klienta je potrebná len pri zakladaní identity a počas inicializácie a autorizácie platby, transakčným systémom. Elektronická validácia kópie štátom vydaného dokladu obvykle spočíva overovaním so štátom prevádzkovanými registrami ako je Verejný register pravých

dokladov totožnosti a cestovných dokladov online.. Najbežnejšou formou kópie je naskenovaný fyzický doklad, kde majú ochranné prvky zníženú kvalitu. Pri overovaní bývajú vyťažované požadované identifikátory identity ako je napríklad fotografia, video, naskenovaný vlastnoručný podpis. Problémom je, že nikto sa dvakrát nepodpíše rovnako, čiže medzi podpismi jedného človeka objektívne vznikajú aj voľným okom rozlíšiteľné tvarové rozdiely kriviek, hoci sú všetky podpisy pravé. Technológie dokážu spájať väzbu medzi poskytnutými elektronickými dátami požadovaných atribútov a založenou identitou len s istou mierou pravdepodobnosti, nedokážu jednoznačne identifikovať digitálnu identitu a tak zostáva priestor pre potvrdenie overenia, hoci by malo byť zamietnuté.

Pri ďalšom spracovávaní transakcie postačuje len zhoda atribútov a identita bude vyhodnotená ako overená. Transakčná identita priamo implikuje fyzickú osobu, ktorá je naviazaná na digitálnu identitu bez ohľadu na to, aká osoba túto transakciu skutočne vykonala. To má za následok, že finančné transakcie môžu byť vykonané v mene skutočných identít v dôsledku čoho sa stáva, že vznikajú spory súvisiace s dokazovaním relevantnosti transakcie.

Ako zraniteľnosť kontrolných mechanizmov o klientovi treba vnímať, že automatické zachytávanie kontrolných údajov o polohe zariadenia klienta môže byť maskované falošnými adresami internetového protokolu (IP) alebo vedomím využívaním služieb virtuálnych súkromných sietí (VPN), čo vôbec nie je zriedkavé ani pri bežných legálnych aktivitách.

V neposlednom rade s prenosom údajov na diaľku prostredníctvom informačných a komunikačných prostriedkov môže byť spojených viacero technických obmedzujúcich nedostatkov alebo neočakávaných, nepredvídateľných, trpených prerušení spojenia.[16] Ako ďalšie príklady možného rizika v krátkosti spomenieme podvod zneužitia identity[17] alebo použitie umelo vytvorenej identity za účelom vykonávania obchodných operácií v mene zneužitej alebo umelo vytvorenej identity.

Pri vzdialenej komunikácii je zložitejšie skúmanie originality dokumentu, pokiaľ nie sú zaručené elektronické certifikované autoritou, alebo neobsahujú spoľahlivo overiteľné ochranné prvky. Čip národného dokladu totožnosti zhromažďuje príslušné údaje na hodnoverné

[16] UJVARY, K. a J. KUCHTOVÁ (2019). Špecifiká objasňovania finančných transakcií v súvislosti s bitcoinom. - In: Aktuálne výzvy kybernetickej bezpečnosti v podmienkach bezpečnostných zložiek, Bratislava : Akadémia PZ, s. 185-195. ISBN 978-80-8054-819-3.

[17] zneužitie rodného čísla, čísla občianskeho preukazu, dátumu narodenia, prípadne prihlasovacích údajov do bankového účtu. Zneužitie identity býva spojené s phishingom inými technikami sociálneho inžinierstva.

preukázanie totožnosti občana, ku ktorým finančné inštitúcie technicky majú možnosť získať prístup.

Kryptomeny ako súčasť reťazca legalizácie príjmov z trestnej činnosti

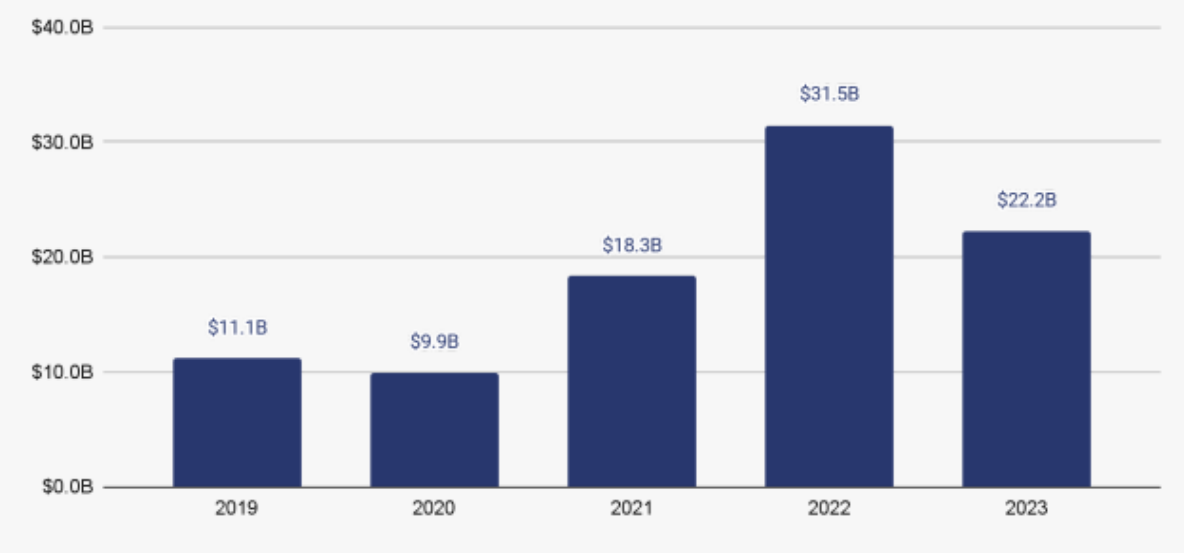
Cieľom legalizácie príjmov z trestnej činnosti je zakryť kriminálny pôvod finančných prostriedkov tak, aby boli spoľahlivo použiteľné a nerozlíšiteľné od ostatných legálnych finančných prostriedkov. V kontexte legalizácie príjmov trestnej činnosti v spojitosti s kryptomenami to vo všeobecnosti znamená najmä presun finančných prostriedkov do služieb, kde môžu byť konvertované na hotovosť. Analýza legalizácie príjmov z trestnej činnosti v spojitosti s kryptomenami sa zameriava na dve odlišné skupiny služieb a subjekty v reťazci:

- Sprostredkovateľské služby a peňaženky, kde sú držané finančné prostriedky alebo je v nich zahmlievaný ich kriminálny pôvod (často zakrytím prepojenia reťazca medzi ich zdrojovou adresou a ich súčasnou adresou).
- Off-rampingové služby Fiat. Táto kategória zahŕňa akúkoľvek službu, kde môže byť kryptomena prevedené na fiat menu, najbežnejšie sa jedná o centralizované burzy. Môže to však zahŕňať aj burzy P2P, služby hazardných hier a kryptobankomaty.

Popri konverzii kryptomeny na hotovosť bývajú často podniknuté aj ďalšie kroky na zakrytie pôvodu týchto finančných prostriedkov a rôzne vnorené služby, ktoré fungujú pomocou infraštruktúry. Protokoly DeFi[18] vo všeobecnosti nemajú možnosť, pretože fungujú autonómne a nestarajú sa o finančné prostriedky používateľov.

Konkrétna kvantifikácia identifikovaná v roku 2023 predstavovala poslanie službám kryptomenu v hodnote 22,2 miliardy dolárov nezákonnými adresami, čo bol významný pokles z 31,5 miliardy dolárov odoslaných v roku 2022, zobrazené na grafe č. 2.

[18] Protokoly DeFi sú protokoly decentralizovaného financovania pomocou smart kontraktov na blockchaine.



Graf 5 Vývoj evidovanej celkovej legalizácie príjmov trestnej činnosti , 2019-2024

Zdroj: Chainalise The 2024 Crypto Crime Report. Dostupné https://go.chainalysis.com /rs/503-FAP-074/images/The%202024%20Crypto%20Crime%20 Report.pdf?version=0

Časť tohto poklesu možno vnímať v nadväznosti s celkovým poklesom objemu krypto transakcií, legitímnych aj nezákonných. Pokles legalizácie príjmov z trestnej činosti bol však o 29,5 %, čo je prudšie ako pokles celkového objemu transakcií o 14,9 %. Naďalej platí konštatovanie, že celkovo centralizované burzy zostávajú primárnym cieľom finančných prostriedkov odosielaných z nezákonných adries.

Záver

Algoritmy optického rozpoznávania znakov alebo overovanie strojovo čitateľných zón sú obrovským zjednodušením mechanického manuálneho zadávania údajov.[19] V prípade nepresného automatizovaného načítania informácií z dokumentov, alebo nerozpoznanie významných detailov, ktoré znamenajú nepresnosť nedokonalej reprodukcie od originálu, môžu spôsobiť vážne bezpečnostné trhliny na finančnom trhu. Na elimináciu rizík nestačí len účinné uplatňovanie usmernení pre uzatváranie zmluvných vzťahov s klientmi na diaľku, ktoré sme sa snažili v príspevku uviesť, dôležitá je pravidelné revidovanie opatrení a v prípade potreby flexibilná obmena právneho alebo regulačného rámca v zmysle aktuálnych potrieb.

[19] HOLUBICZKY, V. Bezpečnosť telekomunikačných a informačných technológií : vedecká monografia. 1. vyd. Bratislava : Akadémia Policajného zboru v Bratislave. 2023. ISBN 978-80-8054-987-9.

Argumentácia použitá v príspevku naznačuje pozitívne trendy nielen z pohľadu presadzovania sa moderných technológií pri poskytovaní finančných služieb, ale aj väčšiu právnu istotu, finančnú stabilitu a ochranu spotrebiteľa pri poskytovaní platobných služieb sprostredkovaných kryptomenami. Postupom času sa cieľavedomou sprísňovanou reguláciou obchodných operácií s kryptomenami a inherentnou transparentnosťou DeFi, intenzita nezákonných služieb pomaly dostáva pod kontrolu.

Zoznam použitej literatúry

IVANČÍK, R. a ANDRASSY, V. Insights into the development of the security concept. In: Entrepreneurship and Sustainability Issues, 2023, Vol. 10, No. 4, pp. 26-39. ISSN 2345-0282.

IVANČÍK, R. (2012). Security from the View of Economy Theory. In Political Sciences, 15(3), pp. 100-124. ISSN 1335-2741.

HOLUBICZKY, V. Bezpečnosť telekomunikačných a informačných technológií : vedecká monografia. 1. vyd. Bratislava : Akadémia Policajného zboru v Bratislave. 2023. ISBN 978-80-8054-987-9.

KETHINENI, S. and Y. CAO. The Rise in Popularity of Cryptocurrency and Associated Criminal Activity. International Criminal Justice Review, 30(3), 2019, p. 325-344. ISSN 1057-5677.

KOZIEŇ, A. and N. KOZLOWSKA Harmonization and Deharmonization of Excise Duty in the European Union as Contemporary Challenges of the EU Tax Law, WSEAS Transactions on Business and Economics, vol. 19, 2022, pp. 815-824, 2022, DOI:10.37394/23207.2022.19.71

LAURENT,M. DENOUEL, J. LEVALLOIS-BARTH,C. WAELBROECK, P. 2015.

Digital Identity. [online] Digital Identity Management. [online] [cit. 2024-04-13]. Dostupné z: < https://www.sciencedirect.com/science/article/pii/B9781785480041500018?dgci

d=raven_sd_recommender_email>.

MARR, S. a B. SUCHOVSKÝ. Právno-aplikačné problémy zaisťovania kryptomien. SAK Bulletin 5, 2023, s. 24-29. ISSN 1335-1079.

Zákon č. 297/2008 Z. z. o ochrane pred legalizáciou príjmov z trestnej činnosti a o ochrane pred financovaním terorizmu a o zmene a doplnení niektorých zákonov

SUCHÁNEK, J. 2023. Nové tuzemské možnosti v oblasti kriminalistické identifikace a její další perspektivy In Bezpečnostní teorie a praxe. Praha: Policejní akademie ČR, 2023. 1/2023. s. 97-112. ISSN 1801-8211.

UJVARY, K. a J. KUCHTOVÁ (2019). Špecifiká objasňovania finančných transakcií v súvislosti s bitcoinom. - In: Aktuálne výzvy kybernetickej bezpečnosti v podmienkach bezpečnostných zložiek, Bratislava : Akadémia PZ, s. 185-195. ISBN 978-80-8054-819-3.

Nariadenie Európskeho parlamentu a Rady (EÚ) č. 2023/1114 o trhoch s kryptoaktívami (MiCA)

Nariadenie Európskeho parlamentu a Rady (EÚ) 2023/1113 o údajoch sprevádzajúcich prevody finančných prostriedkov a určitých kryptoaktív a o zmene smernice (EÚ) 2015/849.

Smernica Európskeho parlamentu a Rady EÚ 2018/843 z 30. mája 2018 - AMLD5 – (Fifth Anti Money Laundering Directive), ktorou sa mení Smernica EÚ 2015/849

Smernica EÚ 2015/849 o predchádzaní využívaniu finančného systému na účely prania špinavých peňazí alebo financovania terorizmu.

Národná banka Slovenska. 2023. Využívanie inovácií v dohliadaných subjektoch finančného trhu v SR. [online] [cit. 07-5-2024] Dostupné z: https://nbs.sk/dokument/3f73a5d4-422d-4aec-aea7-2720459ce445/stiahnut/?force=false

Usmernenia EBA z 22. novembra 2022 č. EBA/GL/2022/15 k používaniu riešení pre uzatváranie zmluvných vzťahov s klientmi na diaľku podľa článku 13 ods. 1 smernice (EÚ) 2015/849

Finančná spravodajská jednotka. Výročná správa 2022. [online] [cit. 05-12-2023] Dostupné z: https://www.minv.sk/swift_data/source/policia/fsj/VS_2022.pdf

Akčný plán boja proti legalizácii výnosov z trestnej činnosti, financovaniu terorizmu a financovaniu proliferácie zbraní hromadného ničenia s výhľadom do roku 2024

Smernica Európskeho parlamentu a Rady (EÚ) č. 2019/1153 z 20. júna 2019, ktorou sa stanovujú pravidlá uľahčovania využívania finančných a iných informácií na predchádzanie určitým trestným činom, ich odhaľovanie, vyšetrovanie alebo stíhanie a ktorou sa zrušuje rozhodnutie Rady 2000/642/SVV

Chainalise The 2024 Crypto Crime Report. [online] [cit. 14-05-2023] Dostupné z: https://go.chainalysis.com/rs/503-FAP-074/images/The%202024%20Crypto%20Crime%20Report.pdf?version=0

Dohovor publikovaný pod č. 109/2002 Z. z. o praní špinavých peňazí, vyhľadávaní, zhabaní a konfiškácii ziskov z trestnej činnosti (Štrasburg; 8.11.1990)

Dohovor publikovaný pod č. 76/2004 Z. z. o praní špinavých peňazí, vyhľadávaní, zhabaní a konfiškácii ziskov z trestnej činnosti (Štrasburg; 8.11.1990)

Zákon č. 297/2008 Z. z. o ochrane pred legalizáciou príjmov z trestnej činnosti a o ochrane pred financovaním terorizmu a o zmene a doplnení niektorých zákonov (AML).

Elektronická Zbierka zákonov Slovenskej republiky [Online] 2023. [cit. 7. 4. 2023] Dostupné z: www.slov-lex.sk/pravne-predpisy/SK/ZZ/2005/300/20220717

ISO/IEC 24760-1:2019(E). A framework for identity management - Part 1: Terminology

and concepts.ISO.2019-05.

Kontaktné údaje:

doc. RNDr. Tatiana Hajdúková, PhD.
Akadémia Policajného zboru v Bratislave
Sklabinská 1, 817 35 Bratislava
Slovenská republika
email: tatiana.hajdukova@akademiapz.sk

Recenzenti:

prof. RNDr. Michal Greguš, CSc.
doc. Ing. Václav Friedrich, Ph.D.

Project Achilles - Vulnerability Management System for Public Sector

Michal Greguš – Alexander Valach – Marián Danko – Ervín Šimko

Abstract: With the rise of the utilization of information services and digitalization of services continues to grow, the importance of Computer Security Incident Response Teams (CSIRTs) in protecting critical infrastructure and maintaining compliance with cybersecurity standards has become increasingly critical. This paper examines the utilization of the Achilles system to fulfil the legal responsibilities of CSIRTs and enhance the protection of its constituency. It briefly describes the architecture of the Achilles system, its functionalities, and examples of its practical application. The paper focuses on how the system is utilized by CSIRT.SK to detect and address security vulnerabilities, thereby decreasing the risk of the security incidents in their constituency. The paper also addresses the challenges faced during the development and implementation of this tool, as well as its potential enhancements. It aims to serve as a source of inspiration for other CSIRTs on integrating vulnerability scanners within broader systems to effectively manage vulnerabilities affecting their constituents.

Keywords: CSIRT, Vulnerability Scanning, Vulnerability Management

Introduction

Over the past few decades, governments, businesses, and individuals alike have witnessed a significant rise in cybersecurity threats and attacks targeting digital assets. This increase is partly due to the ever-changing nature of the cybersecurity threat landscape. Consequently, the protection of critical digital infrastructure and assets has become a major concern for governmental and corporate leaders globally. In response, cybersecurity professionals have developed various standards, procedures, and directives to bolster the security framework of both organizations and nations. Furthermore, the establishment of Computer Security Incident Response Teams (CSIRTs) has become essential for the effective detection, mitigation, and response to cyber threats.

This papers explores how CSIRT.SK have designed and implemented a system known as Achilles to not only meet the obligatory requirements but also to enhance the security capabilities of the organizations.

This papers uses the following structure. Section 2 provides a summary of the cybersecurity laws and regulations in the Slovak Republic and the respective obligations for CSIRT.SK. Section 3 discusses the challenges and complexities encountered by CSIRT.SK in meeting its statutory duties. Section 4 details the design, implementation, and deployment of the Achilles system. It also highlights the practical benefits of deploying the Achilles system,

including real-world applications, case studies, and key takeaways. Future initiatives and potential enhancements to our system are outlined in Section 5. The paper concludes with Section 6.

Legal Mandate of CSIRT.SK and Government

The NIS 2 Directive, known as EU Directive 2022/2555, aims to enhance cybersecurity throughout the European Union [1]. In Slovakia, it has been implemented through National Security Authority Directive 264/2023 [2][3]. This directive lays down guidelines for security measures, the composition and organization of security documents, and outlines the general security practices to be adhered to by entities governed by the 2018 Cybersecurity Law (Law No. 69/2018 Z. z.) [2][4]. This legislation also details the process for establishing and accrediting Computer Security Incident Response Teams (CSIRTs).

Currently, Slovakia hosts three government-sanctioned CSIRT units accredited by the National Security Authority: CSIRT.MIL.SK [5], CSIRT.SK [6], and the national unit, SK-CERT [7]. CSIRT.SK operates under the Ministry of Investment, Regional Development, and Informatics of the Slovak Republic (MIRRI SR) [8] and is mandated by the Cybersecurity Law to satisfy specific accreditation criteria and execute designated responsibilities. It plays a pivotal role in addressing cybersecurity incidents and providing both proactive and reactive services to over 8,200 public sector institutions [4][9].

The Cybersecurity Law also defines the duties of organizations within constituency of CSIRT.SK [2][4], particularly in sections 19, 22, and 24, which outline the necessary actions to ensure the security of digital assets. Additionally, the law requires that certain data and reports be submitted through the Unified Cyber Security Information System (original name being Jednotný informačný systém kybernetickej bezpečnosti) [10], known locally as the The Governmental Cyber Security Information System (VISKB) [11].

The VISKB is comprised of two components:

1. **Public Component.** Accessible via a web portal, this section allows institutions within constituency of CSIRT.SK [12] to provide essential data such as contact details, public IP addresses and domain names, cybersecurity incident reports, and a comprehensive inventory of digital assets [11].
2. **Private Component.** This registry is only accessible to specific entities including accredited CSIRTs, the National Bank, the Personal Data Protection Office, or the

National Security Authority [4]. It serves as a crucial tool for the analysis and management of cybersecurity data within the public sector, facilitating crisis planning and state management during peacetime and crisis situations.

Since the launch of the Achilles system in early 2021, public sector institutions under our purview have registered an extensive array of domain names and IP addresses in VISKB, along with essential contact information and other data.

The VISKB system has provided CSIRT.SK with a centralized database of public-facing IP addresses and domains used by organizations within our jurisdiction. While this database helped identify the systems under our protection and the associated institutions, it did not offer significant insights into the nature of these systems or their exposure to potential cyber threats.

Frequently, our first detailed understanding of a constituent's specific web or email server came only during an incident response, following the exploitation of a security flaw that had already been patched or warned about. Often, these vulnerabilities were the same ones previously highlighted by SK-CERT or CSIRT.SK in sections dedicated to warnings and alerts about actively exploited or critically discovered vulnerabilities.

Throughout these incident responses, we often discovered that system administrators were either unaware of critical vulnerabilities on their systems or did not understand the severity and potential impact of these vulnerabilities if exploited by cybercriminals. To address these issues and enhance our proactive and reactive capabilities, we decided to develop a new system. This system will actively monitor vulnerabilities within our constituency's systems and assist in the timely remediation of these vulnerabilities.

Project Achilles

To enhance our legal compliance and protection capabilities for our constituents, we have initiated the development and implementation of a new vulnerability management system, which we have named Achilles.

This system utilizes a mix of open-source tools such as The Hive [13] and the ELK stack (Elasticsearch, Logstash, and Kibana) [14], alongside commercial software, the Nessus vulnerability scanner [15]. The core of the Achilles system is the Cyber Operations Center (COC), depicted in Figure 3, and comprises several key components briefly described below:

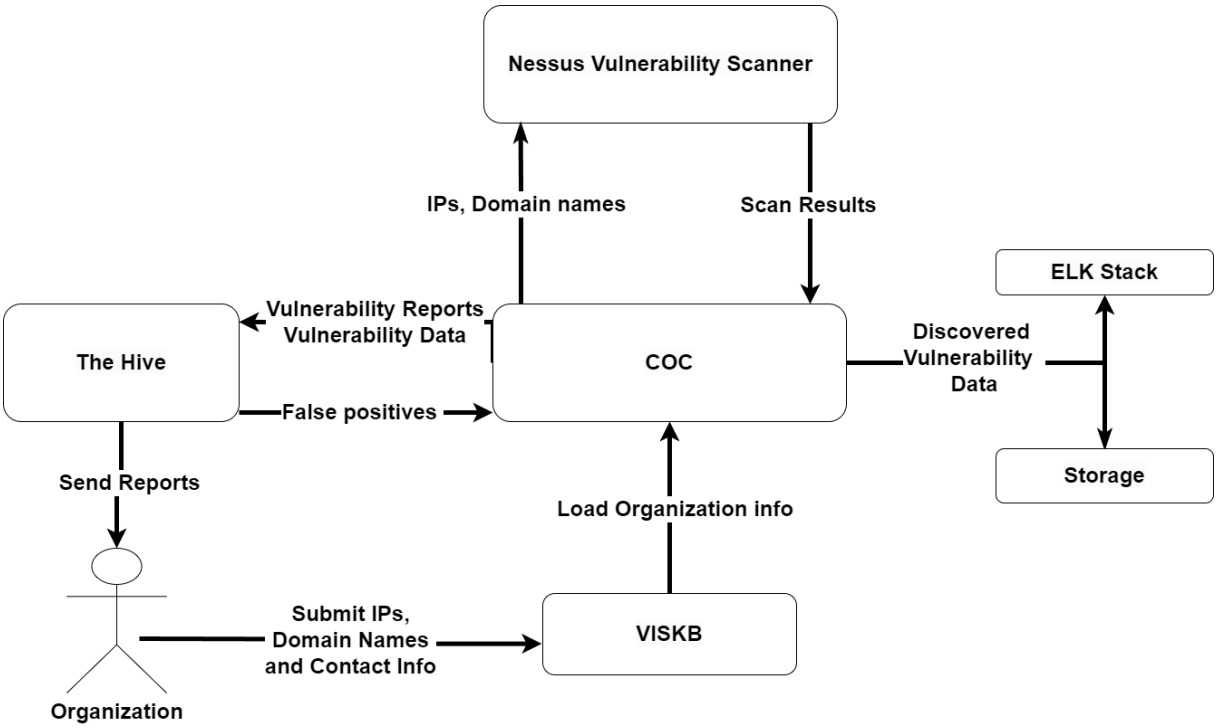


Figure 3: The components and information exchange in Achilles system

The Achilles system consists of these individual components:

1. **Cyber Operation Center (COC).** Developed in-house using the Django framework, the COC orchestrates the integration and interaction of all components. It manages data exchanges between components and dictates operational commands through their APIs.
2. **Vulnerability assessment scanner.** Nessus Professional is utilized for scanning vulnerabilities in CSIRT's constituency systems. We maintain a customized scan setup within our Nessus configuration. The COC uses Nessus's API to schedule scans, transmit target details (like IPs and domain names), and retrieve scanning results. Nessus was chosen for its comprehensive vulnerability detection and high accuracy among available scanning tools. The scanner uses Common Vulnerability Scoring System version 3.0 (CVSSv3) [16].
3. **The Hive.** An open-source incident response platform that receives customized Portable Data Format (PDF) reports, derived from Nessus scan results in CSV format, via an API. The Hive is instrumental in tracking and validating critical vulnerabilities across

organizations. It also facilitates the encrypted email dissemination of vulnerability reports to our constituents.

4. **The Governmental Cyber Security Information System (VISKB).** A registry maintaining essential data from our constituents.
5. **Security Information and Event Management (SIEM).** Employed to consolidate and analyze all scan results and identified vulnerabilities. Kibana, part of the ELK stack, is utilized for data visualization and advanced security analytics.

The integration of these components into a single operational system, Achilles, with the COC as its primary centre, significantly boosts our capacity to monitor and manage vulnerabilities, thereby offering better protection to our constituents. The following section will discuss how our analysts utilize Achilles to provide regular vulnerability reports to our constituents.

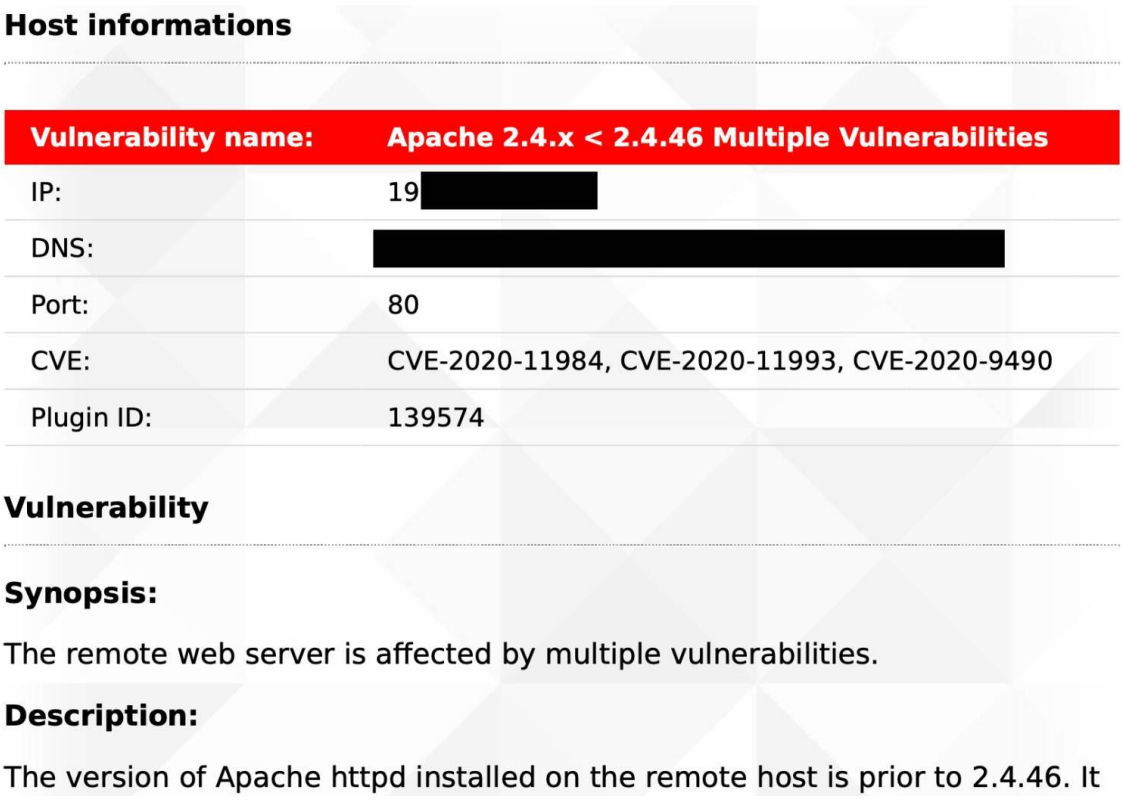
Since the pilot deployment of the Achilles system in early 2021, we have conducted monthly scans of 154 institutions, in addition to specialized campaign scans aimed at detecting newly released and actively exploited vulnerabilities, such as those during the log4shell campaign. Each scan encompasses over 22,000 IP addresses or domains. To manage this scale efficiently, we have established a detailed process with several sub-steps, ranging from registration in VISKB to the receipt of a vulnerability report from the Achilles system.

The entire procedure from an organization joining the Achilles system to the discovery and reporting of vulnerabilities is outlined in the steps below:

1. **Account Creation in VISKB**. We set up accounts in VISKB for all organizations in our constituency. Each organization receives an invitation to VISKB that includes an introduction to the system's functionalities, user credentials, and a one-time password for initial login.
2. **Submitting data to VISKB.** Upon logging in and updating their password, representatives from the organizations submit required information such as IP addresses, domain names, contact details, and their PGP public key.
3. **Setting up a secure data channel.** After data submission, we generate a unique encryption key for each organization, which is used to secure vulnerability reports. This key is stored in the Cyber Operations Center (COC) and shared with a designated contact, typically the CISO or a system administrator. We also notify these contacts about the scanning schedule and the IP address used by our scanner, allowing them to whitelist it and prepare their security operations center (SOC) for the scan.

4. **Passing organization data to COC.** Once all required data is stored in VISKB and contacts are informed, we transfer this data to the COC via an Application Programming Interface (API). In the COC, each organization is identified by a unique ID, and relevant data such as organizational name, IP addresses, domain names, identified false positives, and the encryption key are maintained.
5. **Vulnerability scanning.** Our analysts schedule regular monthly scans in the COC, which are executed automatically at the appointed time. Prior to each scan, the latest IP and domain data from VISKB are loaded into the COC. Each scan of the current scope takes approximately 70 hours to complete.
6. **The generation of vulnerability report.** Following a scan, the COC compiles the results by organization. A PDF vulnerability report is then generated on a monthly or quarterly basis. This report is uploaded to the Hive, where markdown notes detailing critical vulnerabilities by IP and port number for each organization are prepared. The sample of the report is depicted in Figure 4.
7. **The validation of the finding.** The validation of vulnerabilities is carried out using additional scanning software, as detailed in Section 3. We use the Hive to corroborate findings from Nessus. If a vulnerability is deemed a false positive, a correction ticket is issued to the COC to adjust the PDF report accordingly before it is sent out.
8. **Sending a report.** Reports are encrypted with the designated secret and sent via the built-in emailer service in the Hive to the contact email of the organization's CISO or system administrators.
9. **Data visualization and analysis.** Once all reports have been dispatched, our analysts compile a summary of the findings for internal use, enhancing our understanding and refining the quality of services provided to our constituents.

Looking ahead, we aim to further streamline this process, particularly by automating the generation of encryption keys, report creation, and the direct transmission of reports from the COC using the Hive.



Host informations

Vulnerability name:	Apache 2.4.x < 2.4.46 Multiple Vulnerabilities
IP:	19[redacted]
DNS:	[redacted]
Port:	80
CVE:	CVE-2020-11984, CVE-2020-11993, CVE-2020-9490
Plugin ID:	139574

Vulnerability

Synopsis:

The remote web server is affected by multiple vulnerabilities.

Description:

The version of Apache httpd installed on the remote host is prior to 2.4.46. It

Figure 4: Sample of critical vulnerability within the Achilles report

The Benefits and Impacts

While still in its pilot phase, the Achilles system has identified tens of thousands of vulnerabilities in the systems of our constituents. Through integration with Hive, we have successfully generated hundreds of customized vulnerability reports, encrypted, and delivered to the designated contacts listed in VISKB for each institution. This process has significantly enhanced our understanding of the cybersecurity challenges faced by our constituents. This section briefly discusses our experiences during the test phase of the project, including lessons learned and case studies.

In our most recent scan in May 2024, we detected approximately 45,000 vulnerabilities, ranging from informational to critical in severity based on CVSS base 3 scores, as shown in Table 1. Of these, more than 9,400 vulnerabilities were rated as high or critical. After the scanning process finished, the system converted the CSV scan results into PDF vulnerability reports for each constituent.

Table 1:Distribution of identified vulnerabilities based on their severity according to CVSSv3

CVSSv3 Score	Severity	Share in Percentage [%]
0	Info	9.51
0.1 - 3.9	Low	1.3
4 - 6.9	Medium	68.34
7 - 8.9	High	9.6
9 - 10	Critical	11.2

Figure 5: Distribution of identified vulnerabilities according to CVSS rating, each category then shows the distribution of particulat vulnerabilities

These PDF reports are then uploaded to The Hive platform along with a list of all critical vulnerabilities for each constituent. In the first year following the deployment of Achilles, we validated all critical vulnerabilities identified by Nessus using specialized tools, e.g., nmap [17], whatweb [18], nikto [19], Joomscan [20], or metasploit [21]. When a false positive was identified, we submitted a ticket to COC to update and correct the vulnerability report in The Hive platform before sending it to the relevant contact using a secure communication channel.

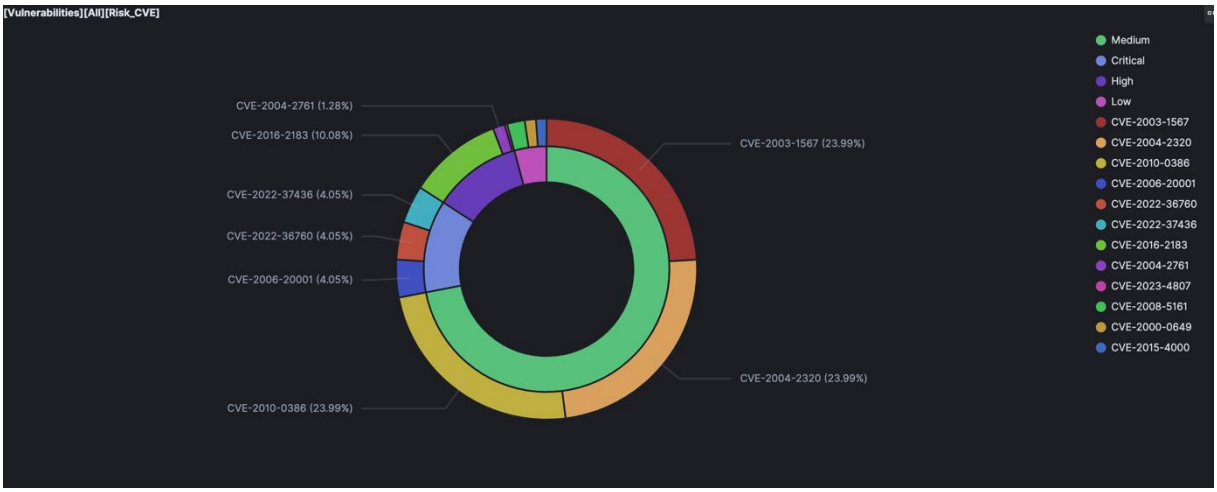


Figure 6: Distribution of identified vulnerabilities by CVSSv3 score along with the distribution of CVEs, which are most prevalent

Throughout the year, there were only 23 false positives detected in our constituency, representing less than 0.1% of all critical vulnerabilities found, supporting the Tenable's claim of high accuracy for Nessus. However, we encountered challenges with false negatives, particularly when Nessus plugins failed to detect vulnerabilities due to a removal of HTTP headers used for detection in those specific cases, or subsites, which masked the presence of vulnerable services. Cases like these highlight the need to integrate more specialized scanners into the Achilles system in the future.

Moreover, deploying Achilles has improved our understanding of the systems and services our constituents provide to the public. For instance, most constituents provide primarily web and email services, as detailed in Table 2. The integration of scan results into the ELK stack allows us to create visualizations in Kibana, as depicted in Figure 5, that help us understand the prevalence of specific CVEs [22] and the distribution of vulnerabilities across hosts and domains within an organization, aiding in prioritization for remediation efforts, depicted in Figure 6, Figure 7, and Figure 8.

Table 2: Most common services with high or critical

Service name	**Share in Percentage [%]**
HTTPS	45
HTTP	39
SMTP	1.5
SMTPS	0.6
POP3S	0.6
IMAPS	0.6

SSH	0.5
FTP	0.5
DNS	0.5
RDP	0.3

Additionally, our website availability monitoring component of Achilles checks the availability of registered websites every thirty minutes and increases check frequency if errors are detected, helping us identify DoS attacks almost in real time. This system has proven effective, alerting us to ongoing attacks more promptly than the affected organizations' administrators in most cases.

Lastly, the encrypted PDF vulnerability reports generated by COC and sent through The Hive are crucial, containing detailed findings and remediation guidance. These reports start with the scan details and include a comprehensive list of identified vulnerabilities, sorted by host or domain. Each report not only lists vulnerabilities but also provides detailed information on each, including potential solutions and references, helping system administrators effectively address and remediate identified issues, as presented in *Figure 4*.

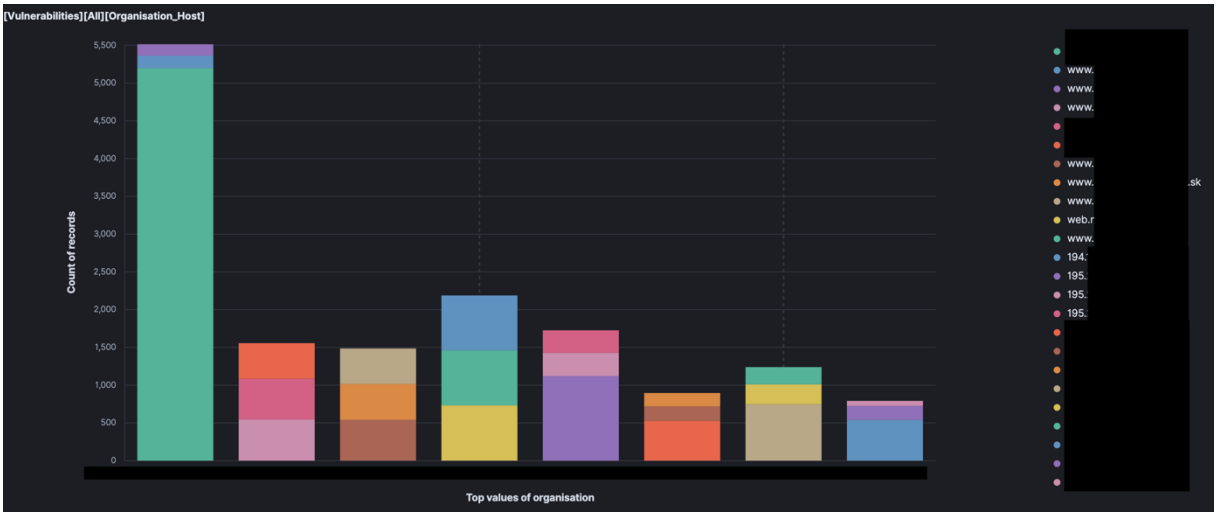


Figure 7: Distribution of vulnerabilities by host for each organization

This comprehensive approach not only enhances the proactive capabilities of our CSIRT unit but also supports our incident response team by providing detailed insights into potential attack vectors, facilitating faster and more effective responses to security incidents.

Figure 8: Vulnerability evolution between scans

Future Work

Going forward, we aim to enhance collaboration with the organizations within our constituency to expedite the remediation of identified vulnerabilities and the patching of compromised systems. Since deploying the Achilles system, we've noticed that many institutions still struggle to address critical vulnerabilities reported on their systems, with some issues remaining unresolved for over a year.

To address this, we plan to conduct regular workshops focusing on secure web server administration and produce supporting materials and hardening scripts. Additionally, we will emphasize the importance of using HTTPS through educational workshops, as web server vulnerabilities constitute the majority of critical issues identified within our constituency. Another proactive step by CSIRT.SK includes offering penetration testing for new web applications developed by our constituents before they go live, enhancing their security and resilience against cyber threats.

These efforts will be complemented by increasing both the frequency of our scans and the number of institutions scanned. After completing the pilot phase, our goal is to conduct weekly scans of all institutions registered in VISKB, ensuring that contact personnel receive regular reports on the security status of their systems.

In terms of the Achilles system's development, future plans include integrating more specialized scanning software such as BurpSuite [23] and InsightVM [24], which could help

decrease the incidence of False Negative findings and uncover more vulnerabilities in previously scanned systems. We also plan to make the code base of our solution, particularly the COC application, open-source and accessible to the community.

Another critical issue we need to address is the verification of IP address and domain name ownership. Despite our efforts to guide constituents on properly submitting and updating their domain names and IP addresses in VISKB, there have been instances where incorrect IP ranges were submitted or not removed when no longer in use. These cases have led to misunderstandings regarding network traffic from our scanner to hosts not affiliated with the institutions that supposedly registered the IPs. Addressing domain ownership verification will be a crucial focus in the future.

Conclusion

In this paper, we have described a vulnerability management system, which is used to discover and report vulnerabilities across thousands of internet-exposed systems belonging to our constituency. This project utilizes a combination of commercial, open-source, and custom software integrated by our development team into a novel system for vulnerability management, called Achilles.

Key components of this system is the Cyber Operations Center (COC), which retrieves IP address data from VISKB and feeds it to the vulnerability scanner. This setup provides an opportunity to detect a broad range of vulnerabilities within the systems of our constituency. By integrating Nessus scan results into the Hive, we can not only pinpoint vulnerabilities but also notify constituents about these issues and offer guidance on corrective measures.

This process significantly improves the mitigation of vulnerabilities within IT systems of internet-facing public sector systems, thereby reducing the risk of successful vulnerability exploitation by the adversaries. It also enhances the efficiency in proactive measures taken by our CSIRT team using analytical tools like Kibana. In the future, we plan to incorporate additional scanning tools into the Achilles system to enhance our detection capabilities. Moreover, we aim to fortify our collaboration with our constituents to simplify and keep the track of the vulnerability remediation processes.

References

1. E. Union. “Nis2 directive.” Accessed on May 5, 2024. (), [Online]. Available: https://www.nis-2-directive.com/.

2. N. S. Authority. “Directive 264/2024 z. z.” Accessed on May 5, 2024. Issued by the National Security Authority. (2024), [Online]. Available: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2024/264/.

3. “National security authority.” Accessed on November 1, 2024, National Security Authority of the Slovak Republic. (), [Online]. Available: https://www.nbu.gov.sk/index.html.

4. “Law on cybersecurity 69/2018 z. z.” Accessed on May 5, 2024. (2018), [Online]. Available: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/69/.

5. “Military csirt.” Accessed on May 5, 2024, Ministry of Defence - MIL.CSIRT.SK. (), [Online]. Available: https://csirt.mil.sk/.

6. “Csirt slovakia.” Accessed on May 5, 2024, Computer Security Incident Response Team (CSIRT) Slovakia. (), [Online]. Available: https://www.csirt.gov.sk/.

7. “Sk-cert.” Accessed on May 5, 2024, National Security Authority - SK-CERT. (), [Online]. Available: https://www.sk-cert.sk/sk/aktuality/index.html.

8. “Ministry of investment, regional development, and informatics of the slovak republic.” Accessed on November 1, 2024, Ministry of Investment, Regional Development, and Informatics of the Slovak Republic. (), [Online]. Available: https://mirri.gov.sk/en/.

9. Slovak statistical office, https://slovak.statistics.sk/wps/portal/ext/Databases/administration/!ut/p/z0/04Sj9CPykssy0xPLMnMz0vMAfIjo8ziw3wCLJycDB0NDNxMDQ0cHJC/, Accessed on May 5, 2024.

10. “Jednotný informačný systém kybernetickej bezpečnosti.” Accessed on May 5, 2024, National Security Authority of the Slovak Republic. (), [Online]. Available: https://www.nbu.gov.sk/kyberneticka-bezpecnost/jednotny-informacny-system-kybernetickej-bezpecnosti/index.html.

11. “Vládny informačný systém kybernetickej bezpečnosti - system specification.” Accessed on May 5, 2024, Ministry of Investment, Regional Development, and Informatics of the Slovak Republic. (), [Online]. Available: https://mirri.gov.sk/wp-content/uploads/2018/10/Priloha-c.-3-Navrh-opisu-predmetu-zakazky.pdf.

12. “Vládny informačný systém kybernetickej bezpečnosti - public portal.” Accessed on May 5, 2024, CSIRT Slovakia. (), [Online]. Available: https://viskb.csirt.sk/.

13. “Thehive project.” Accessed on May 5, 2024. (), [Online]. Available: https://thehive-project.org/.

14. Elastic. “Elastic Stack.” Accessed on May 5, 2024. (2024), [Online]. Available: https://www.elastic.co/elastic-stack.

15. Tenable. “Nessus.” Accessed on May 5, 2024. (2024), [Online]. Available: https://www.tenable.com/products/nessus.

16. “Cvss v3.0 specification document.” Accessed on Date of Access, FIRST (Forum of Incident Response and Security Teams). (Year of access), [Online]. Available: https://www.first.org/cvss/v3.0/specification-document.

17. Nmap Project. “Nmap - the Network Mapper.” Accessed on May 5, 2024. (2024), [Online]. Available: https://nmap.org/.

18. Urban Adventurer, WhatWeb, https://github.com/urbanadventurer/WhatWeb, Accessed on May 5, 2024, 2024.

19. Sullo, Nikto, https://github.com/sullo/nikto, Accessed on May 5, 2024, 2024.

20. OWASP JoomScan, https://github.com/OWASP/joomscan, Accessed on May 5, 2024, 2024.

21. Metasploit. “Metasploit.” Accessed on May 5, 2024. (2024), [Online]. Available: https://www.metasploit.com/.

22. MITRE Corporation. “CVE - Common Vulnerabilities and Exposures.” Accessed on May 5, 2024. (2024), [Online]. Available: https://cve.mitre.org/.

23. PortSwigger. “Burp Suite.” Accessed on May 5, 2024. (2024), [Online]. Available: https://portswigger.net/burp.

24. Rapid7 insightvm, https://www.rapid7.com/products/insightvm/, Accessed: May 5, 2024.

Contact information

Michal Greguš
Vládna jednotka CSIRT
Sekcia kybernetickej bezpečnosti
Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky
Pribinova 25, 811 09 Bratislava
Slovensko
Mail: michal.gregus@stuba.sk

Alexander Valach
Vládna jednotka CSIRT
Sekcia kybernetickej bezpečnosti
Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky
Pribinova 25, 811 09 Bratislava
Slovensko
Mail: alexander.valach@stuba.sk

Marián Danko
Vládna jednotka CSIRT
Sekcia kybernetickej bezpečnosti
Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky
Pribinova 25, 811 09 Bratislava
Slovensko
Mail: marian.danko@stuba.sk

Ervín Šimko
Generálny riaditeľ Sekcie kybernetickej bezpečnosti
Sekcia kybernetickej bezpečnosti
Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky
Pribinova 25, 811 09 Bratislava
Slovensko
Mail: ervin.simko@mirri.gov.sk

Recenzenti:

prof. RNDr. Michal Greguš, CSc.

doc. RNDr. Tatiana Hajdúková, PhD.

Aktuálne trendy a hrozby pre bezpečnosť elektronickej komunikácie

Marika Húleková

Abstrakt: V dnešnej modernej informačnej dobe patrí bezpečnosť elektronickej komunikácie k tým kritickým aspektom, ktorý ovplyvňuje nielen jednotlivcov, ale aj firmy, organizácie, vlády a celé spoločnosti. Tento vedecký príspevok sa preto zameriava na preskúmanie aktuálnych trendov a hrozieb v oblasti bezpečnosti elektronickej komunikácie. Sústreďuje sa na v súčasnosti najviac prevládajúce kybernetické hrozby, ako sú ransomvér, malvér, sociálne inžinierstvo, hrozby voči údajom, hrozby proti dostupnosti služieb, hrozby prerušenia dostupnosti internetu, manipulácia s informáciami a cudzie zasahovanie a útoky na dodávateľské reťazce, ktoré ohrozujú subjekty vyvíjajúce aktivity v online prostredí. Poukazuje pritom na to, ktoré sektory sú kybernetickými hrozbami najviac zasiahnuté. Ďalej diskutuje o dôležitosti ochrany elektronickej komunikácie v kontexte rýchlo sa meniaceho digitálneho ekosystému v nadväznosti na rýchly vývoj rôznorodých technológií, a v závere - vzhľadom na to, že zmienené hrozby prekračujú hranice odvetví alebo sektorov a uplatňujú svoj negatívny vplyv v širokom spektre rôznych oblastí - zdôrazňuje potrebu zintenzívnenia snáh v oblasti bezpečnosti.

Kľúčové slová: Elektronická komunikácia, kybernetické hrozby, bezpečnosť.

Abstract: In current modern information age, the security of electronic communication is one of those critical aspects that affects not only individuals, but also companies, organizations, governments, and entire societies. This scientific contribution therefore focuses on the examination of current trends and threats in the field of security of electronic communication. It focuses on today's most prevalent cyber threats such as ransomware, malware, social engineering, data threats, service availability threats, Internet disruption threats, information manipulation and foreign interference and supply chain attacks that threaten entities developing activities in an online environment. It points out which sectors are most affected by cyber threats. It further discusses the importance of protecting electronic communications in the context of a rapidly changing digital ecosystem following the rapid development of diverse technologies, and in conclusion – taking into consideration that the mentioned threats cross the boundaries of industries or sectors and exert their negative influence in a wide range of different areas – it emphasizes the need intensification of efforts in the field of security.

Keywords: Electronic communication, cyber threats, security.

Úvod

V 21. storočí, v prvej polovici jeho tretieho desaťročia, je celosvetová bezpečnosť veľmi negatívne ovplyvnená rastom vojenských aj nevojenských hrozieb. Bezpečnosť na európskom kontinente je z hľadiska vojenských hrozieb negatívne ovplyvnená najmä prebiehajúcou agresívnou vojnou Ruska proti Ukrajine a z hľadiska nevojenských hrozieb predovšetkým pretrvávajúcimi bezpečnostnými rizikami v podobe teroristických útokov, nelegálnej masovej migrácie a kybernetických útokov na verejné i súkromné počítačové siete a systémy. Z pohľadu témy príspevku je kybernetickými útokmi čo do počtu aj rozmanitosti negatívne poznačená aj

oblasť zaisťovania bezpečnosti elektronickej komunikácie. Tú, okrem viacerých iných vecí, negatívne ovplyvňuje aj obrovské množstvo rôznych falošných správ, hoaxov, dezinformácií a konšpiračných teórií šírených elektronicky predovšetkým na internete a na sociálnych sieťach.[1]

V tejto súvislosti medzi hlavné identifikované a analyzované hrozby patria:

- ransomvér,
- malvér,
- sociálne inžinierstvo,
- hrozby voči údajom,
- hrozby proti dostupnosti služieb (Distributed Denial of Service – DDoS),
- hrozby prerušenia dostupnosti internetu,
- manipulácia s informáciami a zasahovanie,
- útoky na dodávateľský reťazec.[2]

V nadväznosti na to medzi kľúčové zistenia patria:

- DDoS a ransomvér sú najčastejšie využívané medzi hlavnými hrozbami, nasleduje sociálne inžinierstvo, hrozby súvisiace s údajmi, manipulácia s informáciami, útoky na dodávateľský reťazec a malvér;
- pozoruhodný nárast bol zaznamenaný u aktérov hrozieb, ktorí profesionalizovali svoje programy poskytovania služieb, využívajúc nové taktiky a alternatívne metódy na infiltráciu prostredia, nátlak na obete a ich vydieranie;
- najviac útokov je cielených na verejný sektor (19%), po ňom na jednotlivcov (11%), zdravotníctvo (8%), digitálnu infraštruktúru (7%) a na výrobu, financie a dopravu;
- manipulácia s informáciami sa stala jedným z kľúčových prvkov ruskej agresívnej vojny proti Ukrajine.

[1] ZACHAR KUCHTOVÁ, J. 2022. Bezpečnosť na sociálnych sieťach. In *Bezpečnosť elektronickej komunikácie : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava: Akadémia Policajného zboru, 2022; HAJDÚKOVÁ, J. 2022. Zneužívanie elektronických služieb na sexuálne zneužívanie detí. In *Bezpečnosť elektronickej komunikácie : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava: Akadémia Policajného zboru, 2022; IVANČÍK, R. 2023. Šírenie hoaxov cestou sociálnych sietí – hrozba pre súčasnú demokratickú spoločnosť. In *Bezpečnosť elektronickej komunikácie : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava: Akadémia Policajného zboru, 2023; POLÁČEK, J. 2023. Identifikácia a boj proti dezinformáciám a falošným správam. In *Bezpečnosť elektronickej komunikácie : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava: Akadémia Policajného zboru, 2023

[2] MOORE, M. 2023. Zop Cybersecurity Threats in 2023. In *University of San Diego*, 2023; ENISA. 2023. Threat Landscape. In *European Union Agency for Cybersecurity*, 2023; TOOHIL, R. 2023. The 21 Latest Emerging Cyber Threats to Avoid. In *Aura*, 2023

- kybernetické skupiny udržiavajú neustály záujem o nástroje s dvojakým použitím (aby zostali nezistené) a o trojanizáciu známych softvérových balíkov; kyberzločinci sa čoraz viac zameriavajú na cloudové infraštruktúry, zvýšili svoje vydieračské operácie, a to nielen prostredníctvom ransomvéru, ale aj priamym zacielením na používateľov;
- výrazne vzrástli útoky sociálneho inžinierstva vďaka umelej inteligencii a novým typom techník, pričom phishing stále zostáva hlavným vektorom útokov.[3]

V kontexte vyššie uvedeného možno uviesť, že v ostatnom období došlo k výraznej eskalácii útokov v kybernetickom priestore, čím sa stanovili nové kritériá pre rozmanitosť a počet incidentov, ako aj ich dôsledky. Došlo k nárastu skupín ransomvéru, pričom najmä v prvej polovici roku 2023 sme boli svedkami bezprecedentného nárastu incidentov s ransomvérom, čo je trend, ktorý aktuálne nevykazuje žiadne známky zmierňovania. Zároveň sa zvýšil počet rôznych druhov kybernetických hrozieb a ich negatívnych vplyvov na kritické sektory infraštruktúry firiem, organizácií a štátov.[4]

Zvýšenú pozornosť si zasluhuje aj fenomén hacktivizmu, sprevádzaný vznikom mnohých nových skupín, ktorý zaznamenal značnú expanziu. V tomto prípade je treba vysvetliť, že hacktivizmus je vlastne hackerstvo webovej stránky alebo počítačovej siete v snahe sprostredkovať spoločenské alebo politické posolstvo. Osoba, ktorá vykonáva činnosť hacktivizmu, je známa ako hacktivista. Na rozdiel od škodlivého hackera, ktorý hackuje počítač s úmyslom odcudziť súkromné informácie alebo spôsobiť inú škodu, hacktivisti sa zaoberajú podobnými formami rušivých aktivít, aby zdôraznili politické alebo sociálne príčiny. Pre hacktivistu je hacktivizmus internetovou stratégiou na vykonávanie občianskej neposlušnosti. Akty hackerstva môžu zahŕňať poškodenie webových stránok, distribuované útoky odmietnutia služby (DDoS), presmerovania, paródie webových stránok, krádež informácií, virtuálne sabotáže a pod.[5]

1 Hlavné hrozby

Počas uplynulých rokov sa objavila pomerne široká séria rôznych kybernetických hrozieb ohrozujúcich bezpečnosť elektronickej komunikácie. Podľa výsledkov zistení, ktoré sú uvedené v správe Agentúry Európskej únie pre kybernetickú bezpečnosť, aktuálne je potrebné upriamiť pozornosť na osem hlavných skupín hrozieb (pozri obrázok 1).[6] Tieto konkrétne

[3] ENISA. 2023. Threat Landscape. In *European Union Agency for Cybersecurity*, 2023, s. 4
[4] ENISA. 2023. Threat Landscape. In *European Union Agency for Cybersecurity*, 2023, s. 6
[5] BACON, M. 2024. Hacktivism. In *TechTarget*, 2024
[6] ENISA. 2023. Threat Landscape. In *European Union Agency for Cybersecurity*, 2023, s. 6

skupiny hrozieb boli vyčlenené vzhľadom na ich význam v priebehu rokov, ich rozšírený výskyt a významný vplyv vyplývajúci z realizácie týchto hrozieb.

Ransomvér

Ransomvér definovaný ako typ útoku, pri ktorom aktéri hrozby prevezmú kontrolu nad aktívami cieľa a požadujú výkupné výmenou za vrátenie dostupnosti aktíva. Táto definícia je potrebná na vymedzenie a pokrytie meniaceho sa prostredia ransomvérových hrozieb, prevalencie viacerých vydieračských techník a rôznych cieľov páchateľov, iných než len tých, ktoré sú orientované na finančný zisk. Ransomvér je stále jednou z hlavných hrozieb súčasnosti s viacerými významnými a vysoko medializovanými incidentmi.[7]

Malvér

Malvér, tiež označovaný ako škodlivý kód a škodlivá logika, je všeobecný pojem, ktorý sa používa na opis akéhokoľvek softvéru alebo firmvéru určeného na vykonanie neoprávneného procesu, ktorý bude mať nepriaznivý vplyv na dôvernosť, integritu alebo dostupnosť systému.[8]

Sociálne inžinierstvo

Sociálne inžinierstvo zahŕňa širokú škálu aktivít, ktoré sa pokúšajú využiť ľudskú chybu alebo ľudské správanie s cieľom získať prístup k informáciám alebo službám. Aktéri využívajú rôzne formy manipulácie, aby obete prinútili urobiť chybu alebo odovzdať citlivé či tajné informácie. Používatelia môžu byť lákaní na otváranie dokumentov, súborov alebo e-mailov, na návštevu webových stránok alebo na udelenie prístupu k systémom alebo službám. Aj keď použité návnady a triky môžu zneužívať technológiu, úspech sa spolieha primárne na ľudský prvok. Jedná sa hlavne o niektoré z nasledujúcich vektorov útokov: phishing, spear-phishing, smishing, vishing, pretexting, quid pro quo, honeytraps a scareware. Zatiaľ čo techniky sociálneho inžinierstva sa často používajú na získanie počiatočného prístupu, môžu sa použiť aj v neskorších štádiách útoku. Príkladmi sú kompromitácia obchodných e-mailov, podvody, odcudzenie identity, falšovanie a v poslednom čase aj vydieranie.[9]

Ohrozenie údajov

Porušenie ochrany údajov je v GDPR definované ako každé porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene alebo neoprávnenému

[7] ENISA. 2022. Threat Landscape for Ransomware Attacks. In *European Union Agency for Cybersecurity*, 2022, s. 8
[8] LUTKEWICH, B. 2024. Malware. In *TechTarget*, 2024
[9] KASPERSKY. 2023. What is Social Engineering? In *Kaspersky Resource Center*, 2023

sprístupneniu prenášaných, uchovávaných alebo inak spracúvaných osobných údajov alebo prístupu k nim.[10] Technicky vzaté, hrozby voči údajom možno klasifikovať najmä ako porušenie údajov alebo únik údajov. Hoci sa často používajú ako zameniteľné pojmy, sú odlišné. Porušenie údajov je úmyselný kybernetický útok zo strany kyberzločinca s cieľom získať neoprávnený prístup a uvoľniť citlivé, dôverné alebo chránené údaje. Inými slovami, porušenie ochrany údajov je úmyselný a násilný útok proti systému alebo organizácii s úmyslom ukradnúť údaje. Únik údajov je udalosť (napríklad nesprávne konfigurácie, zraniteľné miesta alebo ľudské chyby), ktorá môže spôsobiť neúmyselnú stratu alebo vystavenie citlivých, dôverných alebo chránených údajov.[11]

Distribuované útoky odmietnutia služby (DDoS)

Dostupnosť je terčom množstva hrozieb a útokov, medzi ktorými vyniká hlavne DDoS. DDoS sa zameriava na dostupnosť systémov a údajov, a hoci v žiadnom nejde o novú hrozbu, zohráva významnú úlohu v prostredí kybernetických hrozieb.[12] K útokom dochádza, keď používatelia systému alebo služby nemajú prístup k relevantným údajom, službám alebo iným zdrojom, čo sa dá dosiahnuť vyčerpaním služby a jej zdrojov alebo preťažením komponentov sieťovej infraštruktúry.[13]

[10] IC. 2023. General Data Personal Protection - Art. 4 GDPR Definitions. In *Intersoft Consulting*, 2023
[11] MONDRAGON, L. 2022. Data breach and data leak – what's the difference? In *F-Secure*, 2022; KOST, E. 2023. Data Breach vs. Data Leak: What's the Difference? In *UpGuard*, 2023
[12] EUROPOL. 2021. *Internet Organised Crime Threat Assessment*. In *Europol*, 2021
[13] CISA. 2021. Understanding Denial-of-Service Attacks. In CISA, 2021

Obrázok 1 Prehľad najvážnejších kybernetických hrozieb
Zdroj: ENISA Threat Landscape, 2023

Hrozby prerušenia dostupnosti internetu

Hrozby týkajúce sa internetu sú úzko spojené s úmyselným alebo neúmyselným prerušením dostupnosti internetu alebo elektronickej komunikácie, ktoré má za následok výpadky internetu, výpadky elektronickej komunikácie, vypnutie alebo cenzúru. Prerušenia internetu môžu byť spôsobené vypínaním internetu nariadeným vládou, následkom pôsobenia prírodných živlov (zemetraseniami, rozsiahlymi povodňami, ničivými tornádami, uragánmi atď.), výpadkami dodávok elektriny, prerušením káblov, kybernetickými útokmi, technickými problémami a/alebo vojenskými akciami. Tieto hrozby v posledných rokoch rastú a spôsobujú obrovské peňažné straty.[14]

Manipulácia s informáciami

Manipulácia a cudzie zasahovanie do informácií sa týka konania, ktoré ohrozuje alebo má potenciál negatívne ovplyvniť hodnoty, postupy a politické procesy. Takáto činnosť má manipulatívny charakter, je vedená zámerne a koordinovane. Manipuláciu a cudzie zasahovanie do informácií môžu vykonávať štátni aj neštátni aktéri, vrátane ich zástupcov na vlastnom území alebo aj mimo neho s cieľom získania politického, ideologického alebo iného profitu.[15]

Útoky na dodávateľský reťazec

Útoky na dodávateľské reťazce sa primárne zameriavajú na narušenie vzťahov medzi organizáciami a ich dodávateľmi.[16] Takéto útoky sú považované za súčasť dodávateľského reťazca, ak pozostávajú z kombinácie najmenej dvoch útokov. To znamená, že aby bol útok klasifikovaný ako útok na dodávateľský reťazec, cieľom musí byť dodávateľ aj zákazník. Aktéri hrozieb využívajú tento útok najmä z dôvodu toho, aby mohli vykonávať svoje operácie a ťažiť z rozsiahleho vplyvu a veľkej základne obetí takýchto útokov. [17]

2 Kľúčové trendy

V súvislosti s hlavnými hrozbami pre bezpečnosť elektronickej komunikácie, ktoré sú charakterizované v prvej kapitole, je potrebné spomenúť aj kľúčové trendy v tejto oblasti. Nižšie uvedený zoznam sumarizuje hlavné trendy pozorované v prostredí kybernetických

[14] NIELSEN, B. 2023. Comprehensive List of All Types of Internet Threats. In *Cybriant*, 2023
[15] GRANT, M. F. 2023. Information Manipulation. In *Alliance for Securing Democracy*, 2023
[16] ENISA. 2021. ENISA Supply chain attacks. In *European Union Agency for Cybersecurity*, 2021, s. 6
[17] ACCENTURE. 2022. Cyber Threat Intelligence Report. In Accenture, 2022

hrozieb počas ostatných rokov. Ďalšie bližšie podrobnosti a analýzy jednotlivých kľúčových trendov možno nájsť v odkazoch uvedených v zozname použitej literatúry a zdrojov. Na základe výskumov realizovaných v predmetnej oblasti možno konštatovať, že:

- Ransomvér a hrozby týkajúce sa dostupnosti služieb boli počas uplynulého obdobia na popredných miestach.
- Aktéri hrozieb zneužívajú legitímne nástroje predovšetkým na predlžovanie svojich kybernetických špionážnych operácií. Ich cieľom je vyhýbať sa detekcii tak dlho, ako je to možné, a zakryť svoje aktivity pomocou široko dostupného softvéru, čo sťažuje obrancom ich identifikáciu.
- Geopolitika má naďalej silný vplyv na kybernetické operácie.
- Viacerí aktéri hrozieb sprofesionalizovali svoje programy poskytovania služieb, nielenže používajú nové taktiky a metódy na preniknutie do prostredia, ale využívajú aj alternatívne prístupy k nátlaku a vydieraniu obetí a zároveň rozvíjajú svoje nezákonné aktivity.
- Zločinecké organizácie postupne kombinujú rôzne metódy vydierania, ktoré takmer vždy zahŕňajú aj nejakú formu krádeže údajov. Dvojité vydieranie zaznamenalo pozoruhodný nárast, pričom niektoré skupiny sa dokonca začali spoliehať výlučne na krádeže informácií.
- Orgány činné v trestnom konaní zvýšili počet operácií voči nezákonným aktivitám.
- Jednou z najväčších malvérových hrozieb sú stále zlodeji informácií ako Agent Tesla, Redline Stealer a FormoBook.
- Používanie klasického mobilného malvéru neustále klesá, pričom advér zostáva v počte výskytov najrozšírenejšou hrozbou pre mobilné zariadenia, zatiaľ čo z hľadiska dopadu možno spyvér považovať za najrozšírenejšiu hrozbu pre mobilné zariadenia.
- Hacktivisti čoraz častejšie tvrdia, že sa zameriavajú na OT prostredia, ale verejné správy naznačujú, že často preceňujú alebo nepodkladajú svoje tvrdenia dôkazmi.
- Phishing je stále najbežnejším vektorom počiatočného prístupu. No objavuje sa aj nový model sociálneho inžinierstva, a to vo forme prístupu, ktorý spočíva v klamaní obetí vo fyzickom svete.
- Kompromitácia obchodného e-mailu naďalej zostáva jedným z obľúbených nástrojov útočníkov na získanie finančného profitu.
- Trend kompromitácie údajov sa začal po určitej stabilizácii opäť zvyšovať.

- Došlo k prudkému nárastu počtu chatbotov umelej inteligencie ovplyvňujúcich prostredie kybernetických hrozieb. Rušivý vplyv a exponenciálne prijímanie generatívnych chatbotov s umelou inteligenciou, ako sú OpenAI ChatGPT, Microsoft Bing a Google Bard, menia spôsob, akým pracujeme, žijeme a hráme, a to všetko založené na zdieľaní a analýze údajov.
- DDoS útoky sú čoraz väčšie a komplexnejšie, smerujú k mobilným sieťam a internetu vecí a používajú sa v kontexte použitia na podporu dodatočných prostriedkov pri kybernetických útokoch.
- Vypínania internetu sú na historickom maxime. Hrozby proti dostupnosti internetu si zachovávajú svoju dynamiku, najmä v post-covidovej ére, v dôsledku rastúcej závislosti ľudských činností a ľudskej spoločnosti na internetových technológiách.
- Manipulácia s informáciami je jedným z kľúčových prvkov ruskej agresívnej vojny proti Ukrajine. Manipulácia s informáciami bola základnou a osvedčenou súčasťou ruských bezpečnostných stratégií. Počet analyzovaných udalostí za sledované obdobie tiež výrazne vzrástol.
- Lacné falzifikáty a manipulácia s informáciami pomocou umelej inteligencie sú naďalej vážnym dôvodom na obavy. V posledných mesiacoch sa diskusia o zneužívaní umelej inteligencie na manipuláciu s informáciami rozprúdila v kruhu profesionálov aj mimo neho.
- Zločinecké skupiny majú zvýšený záujem o útoky na dodávateľský reťazec a vykazujú rastúcu schopnosť tým, že využívajú zamestnancov ako vstupné body. Aktéri hrozieb sa aj naďalej budú naďalej zameriavať hlavne na zamestnancov s vyššími oprávneniami, ako sú vývojári alebo správcovia systémov.[18]

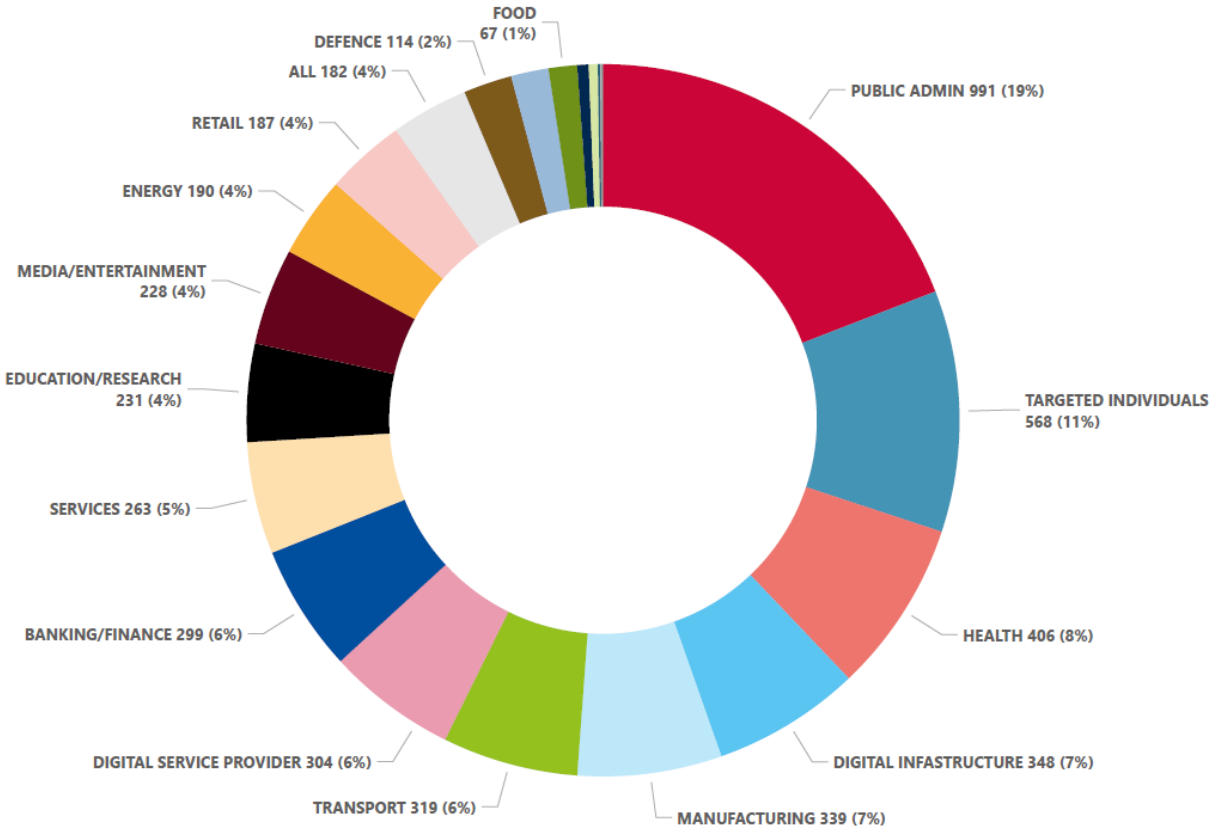
Záver

Kybernetické útoky ohrozujúce nielen bezpečnosť elektronickej komunikácie, ale aj bezpečnosť celkovo, naďalej v globálnom meradle pribúdajú. Nárast počtu hlásených kybernetických útokov však nemusí nevyhnutne znamenať aj skutočný nárast počtu útokov alebo nárast sily ich dopadov. Tento nárast možno pripísať aj tomu, že pozornosť médií alebo

[18] PWC. 2022. Cyber Threats 2022: A Year in Retrospect. In *PwC*, 2022; ZAFRA, D. K a kol. 2023. We (Did!) Start the Fire: Hacktivists Increasingly Claim Targeting of OT Systems. In *Mandiant*, 2023; CLAROTY. 2023. Hacktivist Group Claims Ability to Encrypt an RTU Device. In Claroty Team82, 2023; WILDE, G. - SHERMAN, J. 2023. No Water's Edge: Russia's Information War and Regime Security. In *Carnegie Endowment for International Peace*, 2023; KEELES, J. 2023. Russia continues to look for a weak link in Ukrainian cyberspace. In *Estonian Foreign Intelligence Service*, 2023;

verejnosti sa počas uplynulého obdobia sústredila na konkrétne udalosti, čo viedlo k tomu, že viac takýchto incidentov bolo zdokumentovaných v otvorených spravodajských kanáloch. Napriek tomu sa v budúcnosti očakáva ďalšie zvýšenie počtu pozorovateľných kybernetických incidentov.

V texte zmienené hrozby prekračujú hranice odvetví alebo sektorov a uplatňujú svoj negatívny vplyv v širokom spektre rôznych oblastí. Tento fenomén bezprostredne súvisí s všadeprítomnou povahou digitálneho elektronického prepojenia v dnešnom svete. Ako ukazujú čísla prezentované rôznymi organizáciami pôsobiacimi v tejto oblasti, je zrejmé, že aktéri hrozieb nešetria a nevynechávajú žiadne sektory zo svojho zamerania, čím sa posilňuje názor, že žiadne odvetvie nezostane neovplyvnené ich činnosťou.



Obrázok 2 Prehľad oblastí zasiahnutých kybernetickými hrozbami
Zdroj: ENISA Threat Landscape, 2023

Počas roku 2023 bol v celkovom globálnom prostredí pozorovaný veľký počet udalostí (obrázok 2) zameraných na organizácie v sektoroch verejnej správy (19%) a zdravotníctva (8%). Udalosti zamerané na digitálnu infraštruktúru (7%) a poskytovateľov digitálnych služieb (6%) taktiež tvoria podstatnú časť pozorovaných udalostí. Ide o udalosti, ktoré ovplyvňujú viac ako jeden sektor, pretože ostatné sektory sa spoliehajú na tieto dva sektory. Pozorovaný bol aj

značný počet udalostí zameraných na občiansku spoločnosť, čiže nie nevyhnutne na konkrétny sektor (11% pozorovaných udalostí). Pozostávajú zo sociálneho inžinierstva alebo kampaní na manipuláciu s informáciami. Výrobný, dopravný a finančný sektor čelili počas vykazovaného obdobia približne 6% udalostí.

Hlavnou hrozbou bol ransomvér, zameraný na celý rad sektorov. Najviac zasiahnutými sektormi boli výroba (14% všetkých prípadov ransomvéru), zdravotníctvo (13%), verejná správa (11%) a služby (9%). Po nich nasledujú DDoS útoky a hrozby súvisiace s dátami. Tridsaťštyri percent DDoS útokov sa zameralo na verejnú správu, nasledovala doprava (17%) a bankový a finančný sektor (9%). Hrozby súvisiace s údajmi sa zamerali na všetky sektory, pričom viac boli zasiahnuté tie, ktoré obsahujú osobné informácie. Patrili medzi ne hlavne verejná správa (16%) a zdravotníctvo (10%), ako aj jednotlivci (15%).

Jedna pätina udalostí, ktoré sa týkali škodlivého softvéru, zasiahla širokú verejnosť (20%), nasledovali malvérové infekcie vo verejnej správe (13%), digitálnej infraštruktúre (13%), bankovníctve a financiách (12%) a u poskytovateľov digitálnych služieb (7%). Na všetky sektory bez rozdielu sa zameralo 11% hlásených malvérových infekcií. Zo sledovaných udalostí súvisiacich so sociálnym inžinierstvom bolo 30% zameraných na širokú verejnosť, 18% na verejnú správu a 8% na všetky sektory. Rovnako kampane zamerané na manipuláciu s informáciami boli zamerané na jednotlivcov (47%) a verejnú správu (29%), po ktorých nasledovali sektory obrany (9%) a médií a zábavy (8%).

Ako sa očakávalo, ohrozenie dostupnosti internetu postihlo predovšetkým digitálnu infraštruktúru (28%) a poskytovateľov digitálnych služieb (10%). Postihnutá bola aj verejná správa (15%), jednotlivci (10%) a „všetky sektory“ (11%), keďže sú závislé od digitálnej infraštruktúry a služieb. Útoky na dodávateľské reťazce zasiahli najmä verejnú správu (21%) a týkali sa predovšetkým poskytovateľov digitálnych služieb (16%), digitálnej infraštruktúry (10%) a energetiky (9%). Využitie zraniteľných miest bolo tiež spojené s udalosťami zameranými na poskytovateľov digitálnych služieb (25%), digitálne infraštruktúry (23%) a verejnú správu (15 %) a zasiahli všetky sektory (8%) a aj jednotlivcov (8%).[19] Celkovo možno preto na záver príspevku uviesť, že aktivita aktérov je sektorovo agnostická, keďže takmer všetci títo aktéri hrozieb sú rozptýlení vo všetkých sektoroch.

[19] ENISA. 2023. Threat Landscape. In *European Union Agency for Cybersecurity*, 2023

Zoznam použitej literatúry

ACCENTURE. 2022. Cyber Threat Intelligence Report. In *Accenture*, 2022. [online] [cit. 17-03-2024] Dostupné na internete: <https://www.accenture.com/ae-en/insights/security/cyber-threat-intelligence>.

BACON, M. 2024. Hacktivism. In *TechTarget*, 2024. [online] [cit. 15-03-2024] Dostupné na internete: <https://www.techtarget.com/searchsecurity/definition/hacktivism>.

CISA. 2021. Understanding Denial-of-Service Attacks. In *CISA*, 2021. [online] [cit. 17-03-2024] Dostupné na internete: <https://www.cisa.gov/news-events/news/understanding-denial-service-attacks>.

ENISA. 202. ENISA Threat Landscape for Ransomware Attacks. In *European Union Agency for Cybersecurity*, 2022. 38 s. ISBN 978-92-9204-580-7.

ENISA. 2021. ENISA Supply chain attacks. In *European Union Agency for Cybersecurity*, 2021. 57 s. ISBN 978-92-9204-509-8.

ENISA. 2023. Threat Landscape. In *European Union Agency for Cybersecurity*, 2023. 161 s. ISBN 978-92-9204-645-3.

EUROPOL. 2021. Internet Organised Crime Threat Assessment (IOCTA 2020). In *Europol*, 2021. [online] [cit. 17-03-2024] Dostupné na internete: <https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2020>.

GRANT, M. F. 2023. Information Manipulation. In *Alliance for Securing Democracy*, 2023. [online] [cit. 17-03-2024] Dostupné na internete: <https://securingdemocracy.gmfus.org/asd_tools/information-operations/>.

HAJDÚKOVÁ, J. 2022. Zneužívanie elektronických služieb na sexuálne zneužívanie detí. In *Bezpečnosť elektronickej komunikácie : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava: Akadémia Policajného zboru, 2022, s. 71-85. ISBN 978-80-8054-968-8.

IC. 2023. General Data Personal Protection – Art. 4 GDPR Definitions. In *Intersoft Consulting*, 2023. [online] [cit. 16-03-2024] Dostupné na internete: <https://gdpr-info.eu/art-4-gdpr/>.

IVANČÍK, R. 2023. Šírenie hoaxov cestou sociálnych sietí – hrozba pre súčasnú demokratickú spoločnosť. In *Bezpečnosť elektronickej komunikácie : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava: Akadémia Policajného zboru, 2023, s. 45-56. ISBN 978-80-8054-9997-8.

KASPERSKY. 2023. What is Social Engineering? In *Kaspersky Resource Center*, 2023. [online] [cit. 15-03-2024] Dostupné na internete: <https://usa.kaspersky.com/resource-center/definitions/what-is-social-engineering>.

KOST, E. 2023. Data Breach vs. Data Leak: What's the Difference? In *UpGuard*, 2022. [online] [cit. 16-03-2024] Dostupné na internete: <https://www.upguard.com/blog/data-breach-vs-data-

leak#:~:text=Simply%20put%2C%20a%20data%20leak,Apps%20data%20leak%20in%202021>.
LUTKEWICH, B. 2024. Malware. In *TechTarget*, 2024. [online] [cit. 15-03-2024] Dostupné na internete: <https://www.techtarget.com/searchsecurity/definition/malware>.
MONDRAGON, L. 2022. Data breach and data leak – what's the difference? In *F-Secure*, 2022. [online] [cit. 16-03-2024] Dostupné na internete: <https://blog.f-secure.com/data-breach-and-data-leak-whats-the-difference/>.
MOORE, M. 2023. Top Cybersecurity Threats in 2023. In *University of San Diego*, 2023. [online] [cit. 13-03-2024] Dostupné na internete: <https://onlinedegrees.sandiego.edu/top-cyber-security-threats/>.
NIELSEN, B. 2023. Comprehensive List of All Types of Internet Threats. In *Cybriant*, 2023. [online] [cit. 17-03-2024] Dostupné na internete: <https://cybriant.com/comprehensive-list-of-all-types-of-internet-threats/>.
POLÁČEK, J. 2023. Identifikácia a boj proti dezinformáciám a falošným správam. In *Bezpečnosť elektronickej komunikácie : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava: Akadémia Policajného zboru, 2023, s. 140-153. ISBN 978-80-8054-997-8.
PWC. 2022. Cyber Threats 2022: A Year in Retrospect. In *PwC*, 2022. [online] [cit. 18-03-2024] Dostupné na internete: <https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/pdf/2022-year-in-retrospect-report.pdf>.
TOOHIL, R. 2023. The 21 Latest Emerging Cyber Threats to Avoid. In *Aura*, 2023. [online] [cit. 13-03-2024] Dostupné na: <https://www.aura.com/learn/emerging-cyber-threats>.
ZAFRA, D. K. – LUNDEN, K. – BRUBAKER, N. 2023. We (Did!) Start the Fire: Hacktivists Increasingly Claim Targeting of OT Systems. In *Mandiant*, 2023. [online] [cit. 18-03-2024] Dostupné na: <https://www.mandiant.com/resources/blog/hacktivists-targeting-ot-systems>.
ZACHAR KUCHTOVÁ, J. 2022. Bezpečnosť na sociálnych sieťach. In *Bezpečnosť elektronickej komunikácie : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava: Akadémia Policajného zboru, 2022, s. 237-247. ISBN 978-80-8054-968-8.

Kontaktné údaje

Ing. Marika Húleková
Akadémia ozbrojených síl generála M. R. Štefánika
Demänovská cesta 393, 031 01 Liptovský Mikuláš
e-mail: marika.hulekova@aos.sk

Recenzenti:
doc. Ing. Václav Friedrich, Ph.D.
doc. RNDr. Tatiana Hajdúková, PhD.

Bezpečnosť v digitálnej ére: Aktuálne výzvy v oblasti bezpečnosti elektronickej komunikácie

Radoslav Ivančík

Abstrakt: Autor sa v príspevku zaoberá aktuálnymi otázkami bezpečnosti elektronickej komunikácie v súčasnej digitálnej ére. V úvodnej časti analyzuje dynamický vývoj v oblasti informačných a komunikačných technológií a ich vplyv na vývoj, rozsah a dôležitosť elektronickej komunikácie, pričom poukazuje na rýchly rast počtu používateľov elektronickej komunikácie a rast objemu prenášaných dát. V hlavnej časti skúma aktuálne riziká a hrozby úzko spojené s elektronickou komunikáciou, vrátane kybernetických útokov, malvéru, phishingu, krádeže identity a dávkových útokov. V závere sumarizuje hlavné vedecké zistenia a zdôrazňuje rastúci význam zaisťovania bezpečnosti elektronickej komunikácie a dôležitosti dodržiavania bezpečnostných opatrení používateľmi na ochranu ich údajov a zariadení. Autor pri spracovaní príspevku, v súlade zo zásadami metodológie vedeckého výskumu, využíva téme zodpovedajúce vedecké metódy a vychádza z relevantnej vedeckej a odbornej literatúry z oblasti kybernetickej a informačnej bezpečnosti.

Kľúčové slová: bezpečnosť, moderné technológie, elektronická komunikácia, riziká, hrozby, výzvy.

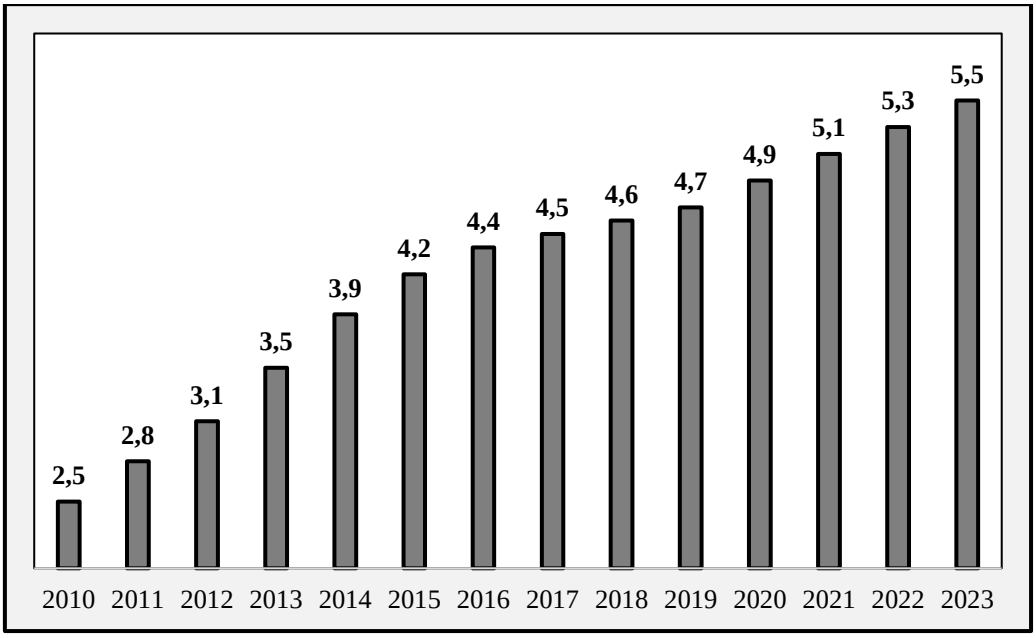
Abstract: The author, in the article, deals with current issues of electronic communication security in the contemporary digital age. In the introductory part, he analyses the dynamic development in the field of information and communication technologies and their impact on the development, scope, and importance of electronic communication, pointing to the rapid growth in the number of users of electronic communication and the volume of transmitted data. In the main part, he examines current risks and threats closely related to electronic communication, including cyber-attacks, malware, phishing, identity theft and batch attacks. In the conclusion, he summarizes the main scientific findings and emphasizes the importance of security of electronic communication security and observing security measures to protect users' data and devices. When processing the paper, in accordance with the principles of scientific research methodology, the author uses scientific methods corresponding to the topic and is based on relevant scientific and professional literature in the field of cyber and information security.

Keywords: security, modern technologies, electronic communication, risks, threats, challenges.

Úvod

Moderné technológie sa v ostatných dekádach stali neodmysliteľnou súčasťou nášho každodenného života. Prenikli do všetkých oblastí, sfér či sektorov našej spoločnosti. Medzi tie, na ktoré sa stále viac spoliehame, resp. ktoré najviac využívame či už v súkromnom alebo profesionálnom živote, patria informačné a komunikačné technológie (ďalej len „IKT“). S ich dynamickým vývojom a rastom ich využívania sa mení aj spôsob, akým komunikujeme a aké druhy komunikácie využívame. Elektronická komunikácia sa postupne stala neoddeliteľnou

súčasťou nášho osobného aj pracovného života. Umožňuje nám komunikovať s ľuďmi na celom svete v reálnom čase bez obmedzení v podobe geografických hraníc a zdieľať s nimi najrôznejšie informácie, či už v rámci nezáväznej rodinnej alebo priateľskej komunikácie, alebo pri riešení pracovných úloh. S postupným rozšírením internetu, zvyšovaním kvality internetového pripojenia a masívnym využívaním najrôznejších „smart“ zariadení (mobilných telefónov, tabletov, fabletov a pod.) sa elektronická komunikácia stala v súčasnej digitálnej ére ešte dostupnejšou, využívanejšou a všadeprítomnejšou.



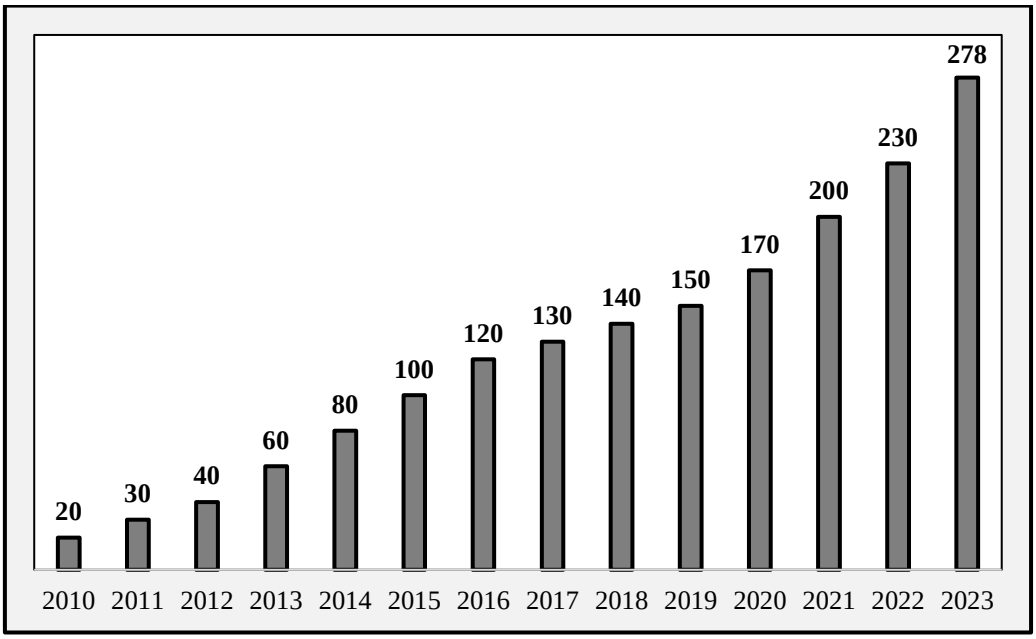
Graf 1 Prehľad rastu používateľov elektronickej komunikácie v rokoch 2010 až 2023 (v miliardách)

Zdroj: Vlastné spracovanie

Rast využívania elektronickej komunikácie v posledných rokoch je evidentný. Možno ho veľmi dobre dokumentovať na počte jej používateľov. Napríklad, kým v roku 2010 používalo elektronickú komunikáciu približne 2,5 miliardy ľudí na celom svete, v roku 2015 to už bolo 4,2 miliardy a v roku 2020 cca 4,9 miliardy ľudí, čo predstavovalo v tom čase viac ako 60 % svetovej populácie. V roku 2023 dosiahol počet používateľov elektronickej komunikácie približne 5,5 miliardy ľudí (graf 1). Predpokladá sa, že ku koncu roka 2024 vzrastie tento počet

na približne 5,8 miliardy ľudí. V roku 2025 sa očakáva ďalší nárast, pričom počet používateľov by mal prekročiť hranicu 6 miliárd ľudí.[1]

Tento trend naznačuje, že elektronická komunikácia sa stáva dominantnou formou komunikácie v modernej spoločnosti. Predpokladá sa, že táto tendencia rastu bude aj naďalej pokračovať, avšak presné čísla sú ťažko predpovedateľné kvôli variabilite faktorov ako sú technologické inovácie, demografické zmeny, politické udalosti, ekonomické krízy a ďalšie. Napriek tomu možno očakávať, že v roku 2025 by mohol počet používateľov elektronickej komunikácie dosiahnuť približne 6,3 až 6,5 miliardy ľudí a v roku 2026 dokonca 6,7 až 6,9 miliardy ľudí.[2]



Graf 1 Prehľad objemu dát prenášaných cez internet v rokoch 2010 až 2023 (v exabajtoch)

Zdroj: Vlastné spracovanie

S nárastom počtu používateľov elektronickej komunikácie narastá aj objem dát prenášaných prostredníctvom tejto formy komunikácie. Kým v roku 2010 predstavoval objem dát prenášaných cez internet približne 20 exabajtov[3], v roku 2015 to už bol päťkrát viac – 100

[1] MEDOFF, N. J. – KAYE, B. K. 2021. *The Evolution of Electronic Communication*. 4. vydanie. New York : Routledge, 2021; BLANCHARD, I. a kol. 2023. Electronic Communication. In *Oxford Research Encyclopedias*, 2023

[2] DELOITTE. 2023. Global Trends in Technology, Media & Telecommunications. In *Deloitte Ireland*, 2023; ETNOA. 2023. The State of Digital Communications. In *European Telecommunications Network Operators' Association*, 2024.

[3] 1 exabajt = 10^{18} bajtov

exabajtov a v roku 2020 cca 170 exabajtov. V roku 2023 sa tento objem zvýšil už na 278 exabajtov (graf 2). V nasledujúcich rokoch sa očakáva, že objem dát prenášaných cez internet sa opäť zvýši. V roku 2024 by mohol dosiahnuť asi 320 až 350 exabajtov a v roku 2025 približne 380 až 420 exabajtov.[4]

Tento nárast je spôsobený nielen väčším počtom používateľov, ale aj rozvojom nových technológií, ako je umelá inteligencia, internet vecí a rozšírená realita. V kontexte takéhoto rýchleho a dynamického vývoja je nevyhnutné venovať oveľa väčšiu pozornosť bezpečnosti elektronickej komunikácie, keďže počty prípadov zneužívania moderných prostriedkov a spôsobov komunikácie stúpajú.[5] S permanentne narastajúcim objemom dát prenášaných cez internet a s nárastom počtu kybernetických hrozieb je pre jednotlivcov i organizácie kľúčové zabezpečiť ochranu svojich dát, informácií, súkromia a v neposlednom rade aj integritu elektronickej komunikácie.[6]

Problematika bezpečnosti elektronickej komunikácie

Bezpečnosť elektronickej komunikácie je v súčasnej dobe kľúčovou témou, ktorá sa stáva stále závažnejšou vzhľadom na rýchly a rozsiahly vývoj v oblasti IKT. S rozšírením internetu a rýchlo rastúcim počtom používateľov elektronickej komunikácie sa zvyšuje aj riziko vystavenia sa rôznym bezpečnostným hrozbám a útokom. Súčasný trend rastu počtu používateľov elektronickej komunikácie a ich rastúca závislosť na digitálnych nástrojoch používaných pre komunikáciu a prácu zásadným spôsobom zvyšuje dôležitosť ochrany dát a súkromia. Komunikácia cez internet, sociálne siete, ich platformy a rôzne aplikácie sa stáva, resp. pre miliardy ľudí sa už stala neoddeliteľnou súčasťou každodenného života ľudí. To,

[4] CISCO. 2024. Cisco Annual Internet Report. In *Computer Information System Company*, 2024. [online] [cit. 16.04.2023]. Dostupné na internete: <https://www.cisco.com/c/en/us/solutions/executive-perspectives/annual-internet-report/index.html>.

[5] KUCHTOVÁ, J. 2018. Aktuálne trendy súvisiace s využívaním moderných technológií. In *Aktuálne výzvy kybernetickej bezpečnosti – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2018, s. 90-98;
HAJDÚKOVÁ, T. – ŠIŠULÁK, S. 2022. Abuse of modern means of communication to manipulate public opinion. In *INTED 2022 – Proceedings from 16th International Technology, Education and Development Conference*. IATED Spain, 2022, s. 1992-2000

[6] KOLLÁR, D. 2019. Trendy kybernetickej bezpečnosti a jej súčasné výzvy pre spoločnosť. In *Medzinárodné vzťahy 2019: Aktuálne otázky svetovej ekonomiky a politiky – zborník príspevkov z 20. medzinárodnej vedeckej konferencie*. Bratislava : Ekonomická univerzita, Fakulta medzinárodných vzťahov, 2019, roč. 20, s. 565-571;
KAZANSKÝ, R. 2020. The Conflict in Cyberspace – Definitions Frame. In Fabián, K. – Beňuška, T. (eds.): *Analysis of Social Network Security. Threats in the Cyberspace*, 2020, s. 32-68. Krakov : University of Public and Individual Security „Apeiron" in Krakow, 2020

samozrejme, zvyšuje aj možnosti odcudzenia a následného zneužitia ich osobných údajov a citlivých informácií.[7]

S technologickým pokrokom a dynamickým rozvojom digitálnej spoločnosti sa objavujú nové bezpečnostné riziká a hrozby, ktoré si vyžadujú pružné, efektívne a účinné riešenia na ochranu používateľov elektronickej komunikácie a ich údajov (dát, informácií). Súčasná situácia si preto vyžaduje komplexný prístup k bezpečnosti, ktorý zahŕňa nielen technické opatrenia, ale aj vzdelávanie a opakované poučovanie používateľov elektronickej komunikácie o bezpečnostných rizikách a správnom používaní digitálnych nástrojov. Bezpečnosť elektronickej komunikácie je totiž kľúčová nielen pre jednotlivcov, ale aj pre organizácie a firmy, ktoré sa musia chrániť napríklad pred únikom citlivých obchodných údajov, know-how, finančných a iných dôležitých informácií. Bezpečnosť dát sa stáva prioritou predovšetkým pre súkromné a verejné (štátne) organizácie, ktoré čelia rôznym hrozbám ako sú kybernetické útoky, ransomware, phishing a ďalšie.[8]

S nárastom zložitosti a sofistikovanosti kybernetických hrozieb je nevyhnutné, aby organizácie mali k dispozícii široké spektrum bezpečnostných nástrojov a technológií na ochranu svojich sietí, systémov a údajov. Riešenia ako firewally, antivírusový softvér, šifrovanie údajov, systémy detekcie a prevencie útokov (IDS/IPS) a ďalšie sa stávajú neoddeliteľnou súčasťou bezpečnostnej stratégie organizácií. Vzdelávanie používateľov elektronickej komunikácie o bezpečnostných rizikách a hrozbách a správnom používaní digitálnych nástrojov je kľúčové pre zlepšenie bezpečnostnej kultúry a tiež prevenciu bezpečnostných incidentov. Používatelia musia byť informovaní o rizikách a hrozbách, ktoré sú spojené s elektronickou komunikáciou a o správnych postupoch na ochranu svojich údajov a súkromia.[9]

Vzhľadom na charakter kybernetických hrozieb a neustále meniace sa taktiky útočníkov je nevyhnutné, aby bezpečnostné opatrenia boli pružné a účinné a bolo možné rýchlo reagovať na nové hrozby a útoky. Organizácie a jednotlivci by mali pravidelne aktualizovať svoje

[7] ZACHAR KUCHTOVÁ, J. 2022. Bezpečnosť na sociálnych sieťach. In *Bezpečnosť elektronickej komunikácie : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2022; HAJDÚKOVÁ, T. a kol. 2023. Riziká komunikácie na sociálnych sieťach. In *Zborník z konferencie RELIK 2023: Reprodukcia ľudského kapitálu - vzájomné väzby a súvislosti*, 2023; KAZANSKÝ, R. – MELKOVÁ, M. 2015. Information Technologies and their Use in Crisis Management as a Tool to Increase the Quality of Educational Process. *In 15th International Multidisciplinary Scientific Geoconference SGEM 2015 : Conference Proceedings*

[8] NOLAN, B. 2023. The Importance of Cybersecurity in the Digital Age. In *CyberNX*, 2023; ANDRÁSSY, V. 2022. Informácie v bezpečnostnom systéme. In *Bezpečnosť elektronickej komunikácie : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2022

[9] EU. 2020. Data protection in the electronic communications sector. In *Eur-Lex*, 2020

bezpečnostné opatrenia a sledovať aktuálne udalosti a vývoj v oblasti kybernetickej bezpečnosti.[10]

Hlavné riziká a hrozby v oblasti elektronickej komunikácie

Pri elektronickej komunikácii sa používajú rôzne prostriedky a kanály na výmenu informácií, vrátane e-mailov, aplikácií, sociálnych sietí, hlasových hovorov a ďalších. Tieto kanály však predstavujú potenciálne riziká a hrozby, ktoré môžu ohroziť bezpečnosť komunikácie a údajov.

E-maily patria medzi jeden z najbežnejších spôsobov elektronickej komunikácie. Sú zraniteľné voči rôznym typom útokov, ako sú napríklad phishingové e-maily, ktoré sa snažia získať citlivé informácie od používateľov. Okrem toho môžu byť e-maily ľahko napadnuté malvérmi a iným škodlivým softvérom, ktorý môžu poškodiť systémy a ukradnúť rôzne údaje.

Aplikácie, ako sú napríklad rôzne sms alebo chatovacie aplikácie, predstavujú ďalší častý spôsob elektronickej komunikácie, ale ich používanie môže byť vysoko rizikové, ak nie sú dostatočne chránené. Útočníci využívajú najmä slabé miesta v zabezpečení týchto aplikácií na získanie prístupu k citlivým informáciám alebo na prenos škodlivého kódu.

Sociálne siete sa stali obľúbeným miestom pre komunikáciu a zdieľanie informácií, avšak sú zraniteľné voči rôznym bezpečnostným rizikám a hrozbám. Užívatelia môžu byť vystavení phishingovým útokom, falošným profilom alebo šíreniu neoverených informácií, čo môže ohroziť ich bezpečnosť a súkromie.

Hlasové hovory cez internet (VoIP – Voice over Internet Protocol) sú ďalším populárnym spôsobom elektronickej komunikácie, ale ich bezpečnosť môže byť vážne ohrozená, ak nie sú správne šifrované. Útočníci môžu v takých prípadoch počúvať alebo manipulovať s hovormi, aby získali dôverné informácie alebo spôsobili škodu.

Okrem vyššie uvedených bežných kanálov elektronickej komunikácie existujú aj ďalšie, ako napríklad videohovory, zdieľanie súborov, IoT zariadenia (Internet of Things) a ďalšie, ktoré môžu predstavovať svoje vlastné bezpečnostné riziká a hrozby. Preto je veľmi dôležité, aby užívatelia – jednotlivci a organizácie – boli informovaní o týchto rizikách a mali možnosť podľa vlastného rozhodnutia prijímať primerané opatrenia na ich minimalizovanie. Celkovo je nevyhnutné, aby používatelia elektronickej komunikácie boli oboznámení s rôznymi rizikami a hrozbami spojenými s rôznymi druhmi a kanálmi komunikácie a aby prijali opatrenia na

[10] FP. 2023. The Growing Importance of Cybersecurity in the Digital Age. In *Future Processing*, 2020

zvýšenie bezpečnosti a ochrany svojich údajov. Zabezpečenie týchto kanálov je nevyhnutné na ochranu dôvernosti, integrity a dostupnosti komunikácie a údajov.[11]

Medzi hlavné riziká a hrozby elektronickej komunikácie patria:

Kybernetické útoky – patria medzi najvýznamnejšie hrozby pre bezpečnosť elektronickej komunikácie. Útočníci využívajú rôzne techniky na získanie neoprávneného prístupu k dátam a systémom. Medzi najbežnejšie formy kybernetických útokov patria útoky na systémy e-mailov, kde útočníci môžu vstúpiť do siete prostredníctvom infikovaných e-mailových príloh alebo odkazov. Okrem toho, útočníci často cieľovane útočia aj prostredníctvom sociálnych sietí, kde sa snažia získať citlivé informácie od používateľov pod zámienkou falošných profilov alebo ponúk. Webové stránky sú ďalším cieľom kybernetických útokov, kde útočníci využívajú rôzne techniky, ako sú SQL injection alebo XSS (Cross-Site Scripting), na zneužitie slabých miest v kóde stránky a získanie prístupu k citlivým údajom. Komunikačné kanály, ako sú aplikácie na správu správ, hlasové hovory a videohovory, sú tiež náchylné na kybernetické útoky. Útočníci môžu využiť nezabezpečené spojenia alebo zraniteľnosti v aplikáciách na získanie citlivých informácií od používateľov. Vzhľadom na neustále sa meniacu povahu kybernetických hrozieb je dôležité, aby používatelia elektronickej komunikácie boli obozretní a dodržiavali bezpečnostné opatrenia, ako sú aktualizácie softvéru, používanie silných hesiel a opatrnosť pri otváraní neznámych príloh a odkazov. Takéto opatrenia môžu výrazne znížiť riziko úspešného kybernetického útoku a ochrániť integritu a dôvernosť elektronickej komunikácie.[12]

Malvér a vírusy – predstavujú vážnu hrozbu pre bezpečnosť elektronickej komunikácie a súčasných informačných systémov. Tieto škodlivé programy sa môžu prenášať prostredníctvom rôznych kanálov elektronickej komunikácie, vrátane e-mailov, webových stránok, sociálnych sietí a iných aplikácií.

Vírusy sú jedným z najbežnejších typov malvéru, ktoré sa môžu nezákonne šíriť medzi počítačmi a zariadeniami prostredníctvom infikovaných súborov, príloh e-mailov, či odkazov

[11] KAUR, J. – RAMACHANDRAN, R. 2021. The Recent Trends in Cyber Security: A Review. In *Computer and Information Sciences*, 2021, roč. 34, č. 8, s. 5766-5781; TURKANOVIČ, M. – POLANČIČ, G. 2023. On the security of certain e-communication types: Risks, user awareness and recommendations. In *Journal of Information Security and Applications*, 2023, roč. 18, č. 4, s. 193-205; WRITER, S. 2024. The Evolving Landscape of Cybersecurity Threats: What You Need to Know. In *Ask Media Group*, 2024

[12] CISCO. 2023. What Is a Cyberattack? In *Computer Information System Company*, 2023; ENISA. 2023. Threat Landscape 2023. In *The European Union Agency for Cybersecurity*, 2023; ALNAJIM, M. A. a kol. A Comprehensive Survey of Cybersecurity Threats, Attacks, and Effective Countermeasures in Industrial Internet of Things. In *Technologies*, 2023

na webových stránkach. Po infikovaní sa môžu vírusy šíriť ďalej a poškodiť dôležité systémové súbory a dáta. Trojské kone sú ďalším nebezpečným typom malvéru, ktoré sa môžu javiť ako legitimné programy alebo súbory, čím sa podvodne dostanú do zariadenia používateľa. Môžu otvoriť brány pre ďalšie škodlivé útoky, ako je napríklad krádež citlivých údajov alebo vzdialené ovládanie zariadenia. Ransomvér je druh malvéru, ktorý sa šíri prostredníctvom elektronickej komunikácie s cieľom šifrovať dôležité súbory a dáta v zariadeniach používateľov. Po úspešnom zašifrovaní spravidla požadujú útočníci výkupné za dešifrovanie súborov, čo môže spôsobiť vážne finančné straty a narušiť prevádzku používateľských systémov. Okrem uvedených typov malvéru existuje aj množstvo ďalších škodlivých programov, ako sú spyware, adware alebo keyloggery, ktoré môžu ohroziť bezpečnosť a súkromie používateľov elektronickej komunikácie.[13]

Phishing je jednou z najbežnejších a najzákernejších techník útokov v oblasti kybernetickej bezpečnosti, ktorá si vyžaduje pozornosť a obozretnosť používateľov. Útočníci často využívajú sofistikované spôsoby na získanie citlivých informácií od používateľov, a to prostredníctvom falošných správ a stránok, ktoré sa javia ako legitímne. Tieto útoky môžu mať rôzne podoby a môžu sa maskovať ako e-maily, ktoré pochádzajú od známych spoločností, bankových inštitúcií alebo dokonca od vládnych organizácií. Často obsahujú odkazy alebo prílohy, ktoré sú navrhnuté tak, aby vyzerali autenticky a viedli používateľov na falošné webové stránky, ktoré sa podobajú na originálne, ale sú kontrolované útočníkmi. Na týchto stránkach sú používatelia nútení zadávať svoje citlivé informácie, ako sú heslá, osobné údaje alebo finančné informácie.

Účelom útočníkov je získať tieto informácie a následne ich zneužiť na krádež identity, finančné podvody alebo ďalšie škodlivé účely. V dnešnej dobe sa phishing stáva čoraz sofistikovanejším a ťažšie rozpoznateľným, pričom útočníci neustále vylepšujú svoje techniky na obchádzanie ochranných opatrení. Preto je potrebné, aby používatelia boli oboznámení s týmito hrozbami a vedeli rozpoznať podvodné správy a webové stránky a mohli sa chrániť pred phishingovými útokmi. Organizácie by mali tiež venovať pozornosť bezpečnostným opatreniam, pretože phishing môže mať škodlivé následky aj pre firemné siete a údaje. Je preto nevyhnutné investovať do edukácie zamestnancov a implementovať efektívne a účinné

[13] HEIDER, Z. – SHABIR, G. 2024. Emerging Trends in Cyber Threats: A Comprehensive Analysis. In *ResearchGate*, 2023; SHEA, S. – HARFORD, I. 2024. The history and evolution of ransomware. In *Tech Target*, 2023

bezpečnostné opatrenia, ako sú napríklad antivírusové programy, firewally alebo systémy detekcie podvodného správania na ochranu pred touto formou útokov.[14]

Krádež identity predstavuje vážne bezpečnostné riziko v elektronickej komunikácii, pričom útočníci sa snažia získať citlivé osobné údaje používateľov s cieľom neoprávneného získania prístupu k ich účtom, finančným prostriedkom alebo iným dôležitým informáciám. Tento typ útoku môže mať veľmi vážne dôsledky pre obete, a preto je dôležité mať na pamäti niekoľko kľúčových aspektov tejto problematiky. Útočníci využívajú rôzne metódy na získanie osobných údajov, vrátane phishingu, sociálneho inžinierstva, útokov na heslá a ďalších podvodných praktík. Môžu získať rôzne druhy osobných údajov, vrátane mena, adresy, telefónnych čísiel, čísel kreditných kariet, hesiel a ďalšie dôležité informácie, ktoré umožňujú útočníkom podnikať neoprávnené aktivity v mene obetí. Následky pre obete často zahŕňajú finančnú stratu, stratu dôveryhodnosti, emocionálnu úzkosť a stres. Zároveň sa často stretávajú s takými problémami ako je blokácia účtov, neoprávnené transakcie a dokonca aj obvinenia z trestných činov, ktoré boli spáchané v ich mene. Je preto dôležité, aby sa obete rýchlo obrátili na príslušné úrady a vykonali potrebné kroky na ochranu svojej identity a minimalizáciu škôd spôsobených útokom. Taktiež je dôležité, aby používatelia prijali opatrenia na ochranu svojich osobných údajov v podobe používania silných hesiel, vyhýbania sa neznámym odkazom a e-mailom od neznámych osôb, aktualizácií softvéru a používania bezpečných internetových pripojení.[15]

Odmietnutie služby (DoS – Denial of Service) predstavuje jednu z najzávažnejších hrozieb v oblasti bezpečnosti elektronickej komunikácie. Cieľom tohto typu útokov je zahltenie infraštruktúry siete masívnym tokom nelegitímnej komunikácie, čo často vedie k výpadkom služieb a k obmedzeniam prístupu. Útoky môžu mať vážne následky nielen pre jednotlivcov, ale aj pre spoločnosti a organizácie. S rozvojom nových technológií sa zvyšuje aj sofistikovanosť týchto útokov, čím sa zvyšuje ich potenciálna škodlivosť. Ochrana pred týmto typom útokov vyžaduje nielen technologické opatrenia, ale aj efektívny manažment rizík a implementáciu bezpečnostných protokolov. Prevencia je v boji proti týmto hrozbám kľúčová,

[14] TN. 2023. The Growing Threat of Phishing Attacks: Preparing for 2024. In *TrustNet*, 2023; RAMZAN, S. 2020. Phishing Attacks and Countermeasures. In Stavroulakis, P., Stamp, M. (eds): *Handbook of Information and Communication Security*, s. 433–448. Berlin: Springer, 2020

[15] SURBER, G. a kol. 2020. Loosing Yourself: Identity Theft in the Digital Age. In *SANS Institute*, 2020; ÖMER, A. a kol. 2023. A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. In *Electronics*, 2023

a preto je dôležité, aby organizácie investovali do bezpečnostných opatrení a monitorovali svoje siete a systémy pre detekciu a odpoveď na potenciálne útoky.

Medzi najčastejšie typy útokov patrí Distribuované odmietnutie služby (DDoS – Distributed Denial of Service), pri ktorom útočníci používajú botnet – sieť počítačov, ktorá je pod ich kontrolou – za účelom narušenia prístupu legitímnych používateľov k cieľovej sieti alebo k webovému zdroju. Zvyčajne sa to dosiahne preťažením cieľa (spravidla webového servera) masívnym objemom požiadaviek alebo odoslaním škodlivých požiadaviek, ktoré spôsobia nefunkčnosť alebo úplné zlyhanie cieľového zdroja. Niektoré typy útokov DDoS majú za cieľ narušiť prístup konkrétneho cieľového jednotlivca k sieti alebo zdroju, zatiaľ čo iné majú za cieľ úplne zneprístupniť zdroj. Tieto útoky môžu trvať minúty až hodiny a v niektorých zriedkavých prípadoch dokonca až niekoľko dní. Výpadky často spôsobujú veľké finančné straty firmám, ktoré sa stanú cieľmi, a nemajú zavedené správne stratégie na zmiernenie dopadu takýchto útokov. Útoky zamerané na odmietnutie služby sa vyskytujú v mnohých tvaroch a veľkostiach.[16]

Záver

Hlavnou témou diskutovanou v článku je problematika bezpečnosti elektronickej komunikácie, ktorá je v dnešnej digitálnej dobe vysoko aktuálna a kľúčová pre zachovanie súkromia, integrity a dôvernosti komunikácie a tiež ochrany údajov používateľov. V rámci skúmania tejto problematiky boli identifikované viaceré významné riziká a hrozby, ktoré môžu veľmi vážne ohroziť bezpečnosť elektronickej komunikácie. Vzhľadom na ich neustály rast v posledných rokoch je preto dôležité, aby používatelia, či už jednotlivci alebo organizácie, dodržiavali bezpečnostné opatrenia a postupy na ochranu svojich údajov a zariadení. Medzi dôležité bezpečnostné opatrenia patria:

Používanie silných hesiel a ich pravidelná zmena je prvým obranným múrom voči kybernetickým hrozbám. Silné heslá, ktoré obsahujú kombináciu veľkých a malých písmen, čísel a špeciálnych znakov, zvyšujú odolnosť voči útokom. Navyše, pravidelná zmena hesiel minimalizuje riziko, že útočníci získajú neoprávnený prístup k účtom.

[16] CISA. 2021. Understanding Denial-of-Service Attacks. In *Cyber Security & Infrastructure Security Agency*, 2021; HEIDER, Z. – SHABIR, G. 2024. Emerging Trends in Cyber Threats: A Comprehensive Analysis. In *ResearchGate*, 2023; KAUR, J. – RAMACHANDRAN, R. 2021. The Recent Trends in Cyber Security: A Review. In *Computer and Information Sciences*, 2021, roč. 34, č. 8, s. 5766-5781; FORTINET. 2022. What Is DDoS Attack? In *Fortinet.com*, 2022; KAZANSKÝ, R. – MIJOČ, N. 2022. O bezpečnosti v kontexte DDoS útokov. *In Bezpečnosť elektronickej komunikácie : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2022

Aktualizácia softvéru a operačných systémov na najnovšie verzie je nevyhnutná z hľadiska zabezpečenia zariadení pred známymi zraniteľnosťami a zneužitím. Aktualizácie obsahujú opravy chýb a záplaty, ktoré zvyšujú odolnosť systému voči útokom a minimalizujú riziko infikovania zariadenia škodlivým softvérom.

Inštalácia antivírusového a antimalvérového softvéru na zariadeniach je jedným zo základných krokov v ochrane pred rôznymi formami škodlivého softvéru. Tieto programy monitorujú aktivitu na zariadeniach a skenujú súbory na detekciu a odstránenie hrozieb. V tejto súvislosti je dôležité inštalovať softvér od dôveryhodných poskytovateľov, ktorí pravidelne aktualizujú svoje databázy a chránia sa pred najnovšími hrozbami.

Opatrnosť pri klikaní na rôzne odkazy a pri otváraní príloh v e-mailoch je nevyhnutná v prevencii pred phishingovými útokmi. Používatelia by mali byť vždy podozrievaví voči neznámym odosielateľom a e-mailovým správam s nečakanými prílohami alebo odkazmi. Overenie vierohodnosti zdroja a obsahu e-mailu pred kliknutím môže minimalizovať riziko infikovania zariadenia škodlivým softvérom.

Používanie šifrovaných spojení a bezpečných protokolov pre prenos citlivých údajov je kritické pri zdieľaní dát cez internet. Šifrovanie zabezpečuje, že dáta sú chránené počas ich prenosu, čím sa minimalizuje riziko odpočúvania a úniku citlivých informácií. Používanie bezpečných protokolov ako HTTPS zabezpečuje, že komunikácia medzi zariadením a webovou stránkou je chránená pred manipuláciou údajov.

Dodržiavanie týchto a ďalších bezpečnostných opatrení je kľúčové pre minimalizáciu rizika vystavenia sa rôznorodým sofistikovaným bezpečnostným hrozbám pri využívaní služieb elektronickej komunikácie. Používatelia by mali mať vedomosti o základných bezpečnostných opatreniach a pravidlách a dodržiavať ich pri každodennom využívaní moderných technológií. Vzdelávanie používateľov a osveta o aktuálnych rizikách a hrozbách tiež prispieva svojim dielom k zníženiu pravdepodobnosti úspešného útoku. Preto je nevyhnutné si uvedomiť, že v súčasnej digitálnej ére je bezpečnosť elektronickej komunikácie rozhodujúca. Z uvedených dôvodov je veľmi dôležité naďalej pokračovať vo vzdelávacích a výskumných aktivitách v oblasti bezpečnosti elektronickej komunikácie, aby sme lepšie porozumeli novým bezpečnostným hrozbám a rizikám v tejto oblasti, boli schopní vyvinúť a implementovať efektívne, účelné a účinné protiopatrenia a v konečnom dôsledku vytvorili bezpečnejšie a spoľahlivejšie prostredie pre elektronickú komunikáciu v prospech všetkých používateľov.

Zoznam použitej literatúry

ALNAJIM, M. A. a kol. 2023. A Comprehensive Survey of Cybersecurity Threats, Attacks, and Effective Countermeasures in Industrial Internet of Things. In *Technologies*, 2023, roč. 11, č. 6, čl. 161. ISSN 2227-7080. [online] [cit. 20.04.2023]. Dostupné na internete: <https://doi.org/10.3390/technologies11060161>.

ANDRASSY, V. 2022. Informácie v bezpečnostnom systéme. In *Bezpečnosť elektronickej komunikácie – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2022, s. 8-19. ISBN 978-80-8054-968-8.

BLANCHARD, I. – DURAN, J. – LEWIS, J. 2023. Electronic Communication. In *Oxford Research Encyclopedias*, 2023. [online] [cit. 20.04.2023]. Dostupné na internete: <https://doi.org/10.1093/acrefore/9780190236557.013.283>.

CISA. 2022. Phishing Awareness. In *Cybersecurity and Infrastructure Security Agency*, 2022. [online] [cit. 20.04.2024]. Dostupné na internete: <https://www.cisa.gov/phishing-awareness>.

CISCO. 2023. Cisco Annual Internet Report. In *Computer Information System Company*, 2023. [online] [cit. 20.04.2024]. Dostupné na internete: <https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html>.

CISCO. 2023. What Is a Cyberattack? In *Computer Information System Company*, 2023. [online] [cit. 20.04.2024]. Dostupné na internete: <https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html>.

CISCO. 2024. Cisco Annual Internet Report. In *Computer Information System Company*, 2024. [online] [cit. 16.04.2023]. Dostupné na internete: <https://www.cisco.com/c/en/us/solutions/executive-perspectives/annual-internet-report/index.html>.

DELOITTE. 2023. Global Trends in Technology, Media & Telecommunications. In Deloitte Ireland, 2023. [online] [cit. 16.04.2024]. Dostupné na internete: <https://www2.deloitte.com/ie/en/pages/technology-media-and-telecommunications/articles/global-trends-tmt.html>.

ETNOA. 2023. The State of Digital Communications. In *European Telecommunications Network Operators' Association*, 2024. [online] [cit. 16.04.2024]. Dostupné na internete: <https://etno.eu/library/reports/117-state-of-digital-2024.html>.

EU. 2020. Data protection in the electronic communications sector. In *Eur-Lex*, 2020. [online] [cit. 19.04.2024]. Dostupné na internete: <https://eur-lex.europa.eu/EN/legal-content/summary/data-protection-in-the-electronic-communications-sector.html>.

FORTINET. 2022. What Is DDOS Attack? In Fortinet, 2022. [online] [cit. 22.04.2024]. Dostupné na internete: <https://www.fortinet.com/resources/cyberglossary/ddos-attack>.

FP. 2023. The Growing Importance of Cybersecurity in the Digital Age. In *Future Processing*, 2020. [online] [cit. 19.04.2024]. Dostupné na internete: <https://startnearshoring.com/knowledge/importance-of-cybersecurity-in-the-digital-age/>.

HAJDÚKOVÁ, T. – KURILOVSKÁ, L. – MARR, S. 2023. Riziká komunikácie na sociálnych sieťach. In *Zborník z konferencie RELIK 2023: Reprodukcia ľudského kapitálu – vzájomné väzby a súvislosti*, 2023, s. 58-69. ISBN 978-80-245-2499-3.

HAJDÚKOVÁ, T. – ŠIŠULÁK, S. 2022. Abuse of modern means of communication to manipulate public opinion. In *INTED 2022 – Proceedings from 16th International Technology, Education and Development Conference*. IATED Spain, 2022, s. 1992-2000. ISBN 978-84-09-37758-9.

HEIDER, Z. – SHABIR, G. 2024. Emerging Trends in Cyber Threats: A Comprehensive Analysis. In *ResearchGate*, 2023. [online] [cit. 20.04.2023]. Dostupné na internete: <https://lnk.sk/hyet>.

KASPERSKY. 2024. Security reports. In *AO Kaspersky Lab*, 2024. [online] [cit. 20.04.2024]. Dostupné na: <https://support.kaspersky.com/help/Kaspersky/Mac22/en-US/183266.htm>.

KAUR, J. – RAMACHANDRAN, R. 2021. The Recent Trends in CyberSecurity: A Review. In *Computer and Information Sciences*, 2021, roč. 34, č. 8, s. 5766-5781. [online] [cit. 20.04.2023]. Dostupné na internete: <https://doi.org/10.1016/j.jksuci.2021.01.018>.

KAZANSKÝ, R. – MELKOVÁ, M. 2015. Information Technologies and their Use in Crisis Management as a Tool to Increase the Quality of Educational Process. In *15th International Multidisciplinary Scientific Geoconference SGEM 2015: Conference Proceedings*. Albena: Academies of Science. 2015. s. 917-924. ISBN 978-619-7105-41-4.

KAZANSKÝ, R. – MIJOČ, N. 2022. O bezpečnosti v kontexte DDOS útokov. In *Bezpečnosť elektronickej komunikácie – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2022, s. 98-107. ISBN 978-80-8054-968-8.

KAZANSKÝ, R. 2020. The Conflict in Cyberspace – Definitions Frame. In Fabián, K. – Beňuška, T. (eds.): *Analysis of Social Network Security. Threats in the Cyberspace*, 2020, s. 32-68. Krakov: University of Public and Individual Security „Apeiron" in Krakow. ISBN 978-83-64035-70-8.

KOLLÁR, D. 2019. Trendy kybernetickej bezpečnosti a jej súčasné výzvy pre spoločnosť. In *Medzinárodné vzťahy 2019: Aktuálne otázky svetovej ekonomiky a politiky – zborník príspevkov z 20. medzinárodnej vedeckej konferencie*. Bratislava : Ekonomická univerzita, Fakulta medzinárodných vzťahov, 2019, roč. 20, s. 565-571. ISBN 978-80-225-4686-7.

KUCHTOVÁ, J. 2018. Aktuálne trendy súvisiace s využívaním moderných technológií. In *Aktuálne výzvy kybernetickej bezpečnosti – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2018, s. 90-98. ISBN 978-80-8054-773-8.

MEDOFF, N. J. – KAYE, B. K. 2021. *Evolution of Electronic Communication*. 4. vyd. New York : Routledge, 2021. 45 s. ISBN 978-0-367-89721-5.

NOLAN, B. 2023. The Importance of Cybersecurity in the Digital Age. In *CyberNX*, 2024. [online] [cit. 18.04.2024]. Dostupné na internete: <https://www.cybernx.com/b-the-importance-of-cybersecurity-in-the-digital-age>.

NORTON. 2018. Top 5 cybercrimes in the U.S., from the Norton Cyber Security Insights Report. In *Norton Security*, 2018. [online] [cit. 20.04.2023]. Dostupné na internete: <https://us.norton.com/blog/online-scams/top-5-cybercrimes-in-america-norton-cyber-security-insights-report>.

ÖMER, A. a kol. 2023. A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. In *Electronics*, 2023, roč. 12, č. 6, čl. 1333. ISSN 2079-9292. [online] [cit. 21.04.2023]. Dostupné na internete: <https://doi.org/10.3390/electronics 12061333>.

RAMZAN, S. 2020. Phishing Attacks and Countermeasures. In Stavroulakis, P. – Stamp, M. (eds): *Handbook of Information and Communication Security*, s. 433–448. Berlin : Springer, 2020. ISBN 978-3-642-04117-4.

SHEA, S. – HARFORD, I. 2024. The history and evolution of ransomware. In *Tech Target*, 2023. [online] [cit. 20.04.2023]. Dostupné na internete: <https://www.techtarget.com/searchsecurity/feature/The-history-and-evolution-of-ransomware>.

SURBER, G. a kol. 2020. Loosing Yourself: Identity Theft in the Digital Age. In *SANS Institute*, 2020. [online] [cit. 21.04.2023]. Dostupné na internete: <https://lnk.sk/tefw>.

TN. 2023. The Growing Threat of Phishing Attacks: Preparing for 2024. In *TrustNet*, 2023. [online] [cit. 20.04.2023]. Dostupné na internete: <https://trustnetinc.com/the-growing-threat-of-phishing-attacks-preparing-for-2024/>.

TURKANOVIČ, M. – POLANČIČ, G. 2023. On the security of certain e-communication types: Risks, user awareness and recommendations. In *Journal of Information Security and Applications*, 2023, roč. 18, č. 4, s. 193-205. ISSN 2214-2134. [online] [cit. 20.04.2024]. Dostupné na internete: <https://doi.org/10.1016/j.jisa.2013.07.003>.

WRITER, S. 2024. The Evolving Landscape of Cybersecurity Threats: What You Need to Know. In Ask Media Group, 2024. [online] [cit. 20.04.2023]. Dostupné na internete: <https://lnk.sk/inzl>.

ZACHAR KUCHTOVÁ, J. 2022. Bezpečnosť na sociálnych sieťach. In *Bezpečnosť elektronickej komunikácie – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2022, s. 237-2477. ISBN 978-80-8054-968-8.

Kontaktné údaje

plk. gšt. v. z. doc. Ing. Radoslav Ivančík, PhD. et PhD., MBA, MSc.
Katedra informatiky a manažmentu
Akadémia Policajného zboru v Bratislave
Sklabinská 1, 835 17 Bratislava
e-mail: radoslav.ivancik@akademiapz.sk

Recenzenti:

prof. RNDr. Michal Greguš, CSc.
doc. Ing. Václav Friedrich, Ph.D.

Šírenie dezinformácií cestou sociálnych sietí – hrozba pre súčasnú demokratickú spoločnosť[17]

Radoslav Ivančík

Abstrakt: Jedným z vážnych bezpečnostných problémov súčasnosti, ktorý nepriaznivo ovplyvňuje predovšetkým demokratickú spoločnosť, je rozrastajúci sa počet falošných, zavádzajúcich, klamlivých, skreslených či úmyselne pozmenených informácií najrôznejšieho druhu – dezinformácií – šírených cestou internetu a sociálnych sietí. Zatiaľ čo na prelome tisícročí bolo klamanie na internete a v médiách vnímané skôr ako výnimočné, v priebehu tretieho desaťročia tretieho tisícročia je tento problém veľmi rozšírený. Predovšetkým internet a sociálne siete totiž ich používateľom poskytujú jednak anonymnejšie prostredie a jednak široké publikum, ktoré je možné týmto spôsobom veľmi rýchlo osloviť. Problémom je, že internet a sociálne siete dnes umožňujú ľahké šírenie v podstate akýchkoľvek informácií, čo poskytuje veľký priestor na šírenie najrôznejších dezinformácií. Aj preto sa autor v rámci vedeckého výskumu realizovaného v rámci medzinárodnej vedeckovýskumnej úlohy, s využitím relevantných vedeckých metód a vhodných analyticko-syntetických a komparatívnych prístupov, vo svojom príspevku zaoberá problematikou dezinformácií ako hrozby pre súčasnú modernú demokratickú spoločnosť.

Kľúčové slová: Dezinformácie, hrozba, bezpečnosť, sociálne siete, demokratická spoločnosť.

Abstract: One of the serious security problems of the current digital age, which adversely affects a democratic society, is the growing number of false, misleading, distorted or deliberately altered information of all kinds – disinformation – spread mainly via the Internet and social networks. While at the turn of the millennium, lying on the Internet and in the media was seen as rather exceptional, currently, during the third decade of the third millennium, this problem is very widespread. Above all, the Internet and social networks provide their users with a more anonymous environment and a wide audience that can be reached very quickly in this way. The problem is that the Internet and social networks today allow the easy dissemination of any information, which provides a lot of space for the spread of all kinds of disinformation. Therefore, as part of the scientific research carried out as part of an international scientific research task, with the use of relevant scientific methods and several analytical-synthetic and comparative approaches, the author deals with the issue of disinformation as a threat to the current modern democratic society in his work.

Keywords: Disinformation, threat, security, social networks, democratic society.

Úvod

Ľudstvo sa už od nepamäti stretáva s rôznymi falošnými, zavádzajúcimi, skreslenými, klamlivými či úmyselne pozmenenými informáciami. Nie je to nič nového, moderného alebo ojedinelého, nakoľko v živote v ľudskej spoločnosti sa tieto správy vyskytovali, vyskytujú

[17] Tento príspevok bol spracovaný v rámci medzinárodnej vedeckovýskumnej úlohy č.: APZ-OVVP-14-2023 „Dezinformácie ako súčasť hybridných hrozieb pre demokratickú spoločnosť a ich vnímanie študentmi vysokých škôl“ (VÝSK 268)

a určite budú vyskytovať aj v budúcnosti. Ich prítomnosť a vplyv však dnes vnímame v určitých situáciách oveľa viac ako inokedy, a to najmä pokiaľ ide o závažné alebo významné spoločenské udalosti alebo rôzne krízové situácie. So šírením falošných, zavádzajúcich, skreslených, klamlivých či úmyselne pozmenených informácií v podobe dezinformácií v rôznych podobách sa nanešťastie v súčasnosti stretávame oveľa častejšie ako v minulosti, v podstate takmer denne, či už ide o rôzne pozmenené, úplne vymyslené alebo z kontextu vytrhnuté informácie, upravené fotografie alebo videá, články alebo „zaručene pravdivé" správy posielané prostredníctvom internetu v reťazových e-mailoch alebo šíriace sa cestou sociálnych sietí.

V tejto súvislosti je možné s určitým nadhľadom dodať, že dezinformácie sú svojím spôsobom prirodzenou súčasťou demokratických spoločností, v ktorých sa uznáva sloboda slova a ktoré nepresadzujú jediný správny uhol pohľadu.[18] Dnes už tradičné médiá nie sú jedinými, ktoré určujú, ktoré správy sú pre publikum relevantné a ktoré nie. Užívatelia tvoriaci obsah na internete nemusia dodržiavať etiku[19] a profesijné zásady platiace pre novinárov a sú sami sebe editormi. Nezväzuje ich legislatíva regulujúca tradičné médiá.

Často záleží na samotnom jedincovi, ako veľmi sa nechá takýmito správami ovplyvniť, či je schopný odlíšiť klamstvo alebo výmysel od reality a či má dostatok správnych informácií, ktoré mu pomôžu na prvý pohľad odhaliť, že daná správa je nepravdivá, nereálna, a teda ide o falošnú správu v podobe dezinformácie, hoaxu, propagandy či konšpiračnej teórie a pod.[20] Jedno je však u týchto správ zrejmé, a to že ich cieľom je ovplyvniť príjemcov týchto správ, ovplyvniť ich konanie, správanie, reakcie, zmanipulovať ich a doslova dostať tam, kam ich odosielatelia týchto správ chcú dostať.

Ľudia, zahltení a ovplyvnení veľkým množstvom najrôznejších informácií týkajúcich sa určitých významných spoločenských udalostí, častokrát už nie sú schopní rozlišovať pravosť informácií, a preto často dochádza k zmanipulovaniu tých, ktorých by takáto informácia za iných okolností nemohla ovplyvniť. S rôznymi falošnými, zavádzajúcimi, skreslenými, klamlivými či úmyselne pozmenenými informáciami v podobe dezinformácií sa stretávame najmä v oblasti politiky a politického života, udalostí týkajúcich významných osobností politického, športového alebo kultúrneho života, tragických udalostí, ako aj riešení závažných

[18] EU. 2021. The impact of disinformation on democratic processes and human rights in the world. In *European Parliament – Policy Department for External Relations*, 2021
[19] SAPÍK, M. 2022. Etika v prostředí moderní společnosti. In *Auspicia*, 2022
[20] ŠIŠULÁK, S. – CÍCHOVÁ, M. 2019. Fake news a propaganda v kybernetickom priestore In *Aktuálne výzvy kybernetickej bezpečnosti v podmienkach bezpečnostných zložiek – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2019

problémov, ktoré sa dotýkajú obyvateľov celej krajiny, regiónu alebo doslova celého ľudstva, ako tomu bolo napríklad v súvislosti s pandémiou koronavírusu spôsobujúceho ochorenie Covid-19.[21]

V dnešnej modernej informačnej spoločnosti, v ére prehlbujúcej sa digitalizácie, internetizácie a informatizácie spoločnosti sa v podstate mnohým takýmto informáciám ani nedá vyhnúť. V tejto súvislosti je ale dôležité, aby ich človek vedel rozoznať a aby sa nimi nenechal zmanipulovať a ovplyvniť, pretože to môže priniesť množstvo negatívnych dôsledkov tak pre samotného človeka ako jednotlivca, ako aj pre celú ľudskú spoločnosť. Aj preto sa autor vo svojom príspevku s využitím relevantných metód interdisciplinárneho vedeckého výskumu a vhodných analyticko-syntetických a komparatívnych prístupov zaoberá problematikou dezinformácií ako hrozby pre súčasnú demokratickú spoločnosť a ich šírením prostredníctvom internetu a sociálnych sietí.

Teoretické vymedzenie pojmu dezinformácie

Dezinformácie sú, podobne ako mnohé iné pojmy, definované rôzne. V súčasnosti neexistuje žiadne ich jednotné, unifikované a všeobecne akceptované definičné vymedzenie, a preto sa v literatúre možno stretnúť s pomerne veľkým množstvom definícií líšiacich sa predovšetkým tým, kto je ich tvorcom, v akej sfére pôsobí a v akom odvetví či oblasti spoločnosti sa dezinformácie vyskytujú, resp. aplikujú. Napriek ich väčšej či menšej odlišnosti, spoločným rysom všetkých používaných definícií je fakt, že v prípade dezinformácií ide o úmyselnú modifikáciu poskytovaných informácií so zámerom ovplyvniť, oklamať či uviesť adresátov týchto informácií do omylu.

V slovenskom prostredí sú pomerne často využívané definície nachádzajúce sa v príslušných slovníkoch. Napríklad v Slovníku cudzích slov je dezinformácia vymedzená veľmi stručne ako *„nesprávna, vedome skreslená informácia“*.[22] V Slovníku súčasného slovenského jazyka je už dezinformácia definovaná obšírnejšie ako *„nepravdivá, vedome skreslená informácia, ktorej cieľom je ovplyvniť určitú skupinu ľudí, prípadne celú populáciu“*.[23] V Slovníku pojmov z mediálnej výchovy sa uvádza, že *„dezinformácia je*

[21] IVANČÍK, R. 2021. Boj proti dezinformáciám týkajúcich sa pandémie koronavírusu na úrovni Európskej únie. In *Almanach – aktuálne otázky svetovej ekonomiky a politiky*, 2021; LISOŇ, M. - FIDLER, Ľ. 2024. Spravodajská dezinformácia pri plnení úloh spravodajských služieb v Slovenskej republike. In *Policajná teória a prax*, 2024

[22] Slovník cudzích slov. 2023. Dezinformácia. In *Slovníkový portál Jazykovedného ústavu Ľ. Štúra Slovenskej akadémie vied*, 2023

[23] Slovník súčasného slovenského jazyka. 2023. Dezinformácia. In *Slovníkový portál Jazykovedného ústavu Ľ. Štúra Slovenskej akadémie vied*, 2023

úmyselne nesprávna či skreslená informácia tajne implantovaná do informačnej sústavy oponenta so zámerom ovplyvniť potrebným smerom jeho aktivity".[24]

Podľa Krátkeho slovníka hybridných hrozieb, ktorý vznikol z iniciatívy Národného bezpečnostného analytického centra: *„Dezinformácia je overiteľne nepravdivá, zavádzajúca alebo manipulatívne podaná informácia, ktorá je zámerne vytvorená, prezentovaná a šírená s jednoznačným úmyslom klamať alebo zavádzať, spôsobiť nejakú ujmu alebo zabezpečiť nejaký zisk (napríklad politický či hospodársky). Dezinformácia často obsahuje element, ktorý je zjavne pravdivý, čo jej dodáva na dôveryhodnosti a môže tak skomplikovať jej odhalenie. Medzi dezinformácie nepatria neúmyselné chyby v spravodajstve, satira a paródia, ani správy a komentáre naklonené jednej strane, ktoré sú takto zreteľne označené"*.[25]

V českom prostredí, Centrum proti hybridným hrozbám Ministerstvo vnútra Českej republiky na svojich webových stránkach označuje dezinformáciu za *„šírenie zámerne nepravdivých informácií, najmä štátnymi aktérmi alebo ich odnožami voči cudziemu štátu alebo voči médiám, s cieľom ovplyvniť rozhodovanie alebo názory tých, ktorí ich prijímajú"* (MV ČR, 2020). Podľa Dušeka a Kavana *„dezinformácie predstavujú komplexný jav, ktorého podstata spočíva v úmyselnom a cielenom šírení nepravdivých alebo zavádzajúcich informácií s cieľom ovplyvniť verejnú mienku"*. Tento fenomén sa podľa nich v digitálnom veku stáva stále prominentnejším a nadobúda rôznorodé formy. Kľúčovým prvkom je úmyselnosť a zámer, kedy vytváranie a šírenie dezinformácií nespočíva v zhode, ale v organizovanom a syste-matickom postupe. Kľúčovým prostriedkom na šírenie dezinformácií sa stali internet a sociálne médiá.[26]

Na európskej úrovni, podľa Akčného plánu proti dezinformáciám, ktorý bol prijatý na pôde Európskeho parlamentu *„dezinformácie predstavujú preukázateľne nepravdivé alebo zavádzajúce informácie, vytvorené, prezentované a šírené za účelom ekonomického zisku alebo zámerného klamania verejnosti a môžu spôsobiť verejné škody"*.[27] Kľúčovým prvkom, ktorý sa v tejto súvislosti v predmetnom dokumente zdôrazňuje, je úmysel. Severoatlantická aliancia vníma dezinformácie ako *„zámerné vytváranie a šírenie nepravdivých a/alebo manipulovaných informácií s úmyslom klamať a/alebo zavádzať, pričom aktéri šíriaci dezinformácie sa snažia*

[24] Slovník pojmov z mediálnej výchovy. 2020. Dezinformácia. In *Mediálna výchova*, 2023
[25] NBÚ. 2023. Dezinformácia. In *Krátky slovník hybridných hrozieb*, 2023
[26] DUŠEK, J. – KAVAN, Š. 2024. Dezinformace jako součást hybridních hrozeb – česko-slovenský pohled. In *Auspicia*, 2024, roč. 21, č. 1, s. 8
[27] EU. 2018. Action Plan Against Disinformation. In *European Commission*, 2018

prehĺbiť rozdiely v rámci spojeneckých krajín a medzi nimi a podkopať dôveru ľudí vo zvolené vlády".[28]

Šírenie dezinformácií prostredníctvom sociálnych sietí

Používanie rôznych lží alebo prekrúcanie faktov za účelom ovplyvnenia jednotlivcov alebo aj celej verejnosti, ako už bolo uvedené vyššie, nie je žiadnou novinkou, ak sa však spojí so sofistikovanými prostriedkami, aké predstavujú dnešné moderné „smart" zariadenia[29], prostriedky a technológie, s prostredím sociálnych sietí a internetu[30], prípadne aktivitou hackerov, objavuje sa tu nová a veľmi silná hrozba šírenia falošných správ vo forme rôznych typov dezinformácií, ktoré môžu predstavovať nebezpečenstvo nielen pre jednotlivcov, sociálne skupiny a organizácie, ale v niektorých prípadoch bezpečnostnú hrozbu pre celú súčasnú demokratickú spoločnosť.

Vznik a rýchly rozvoj sociálnych sietí viedol k radikálnej zmene spôsobov, akými ľudia dnes komunikujú a získavajú informácie. Tento nový spôsob komunikácie sa vyznačuje veľmi vysokou rýchlosťou s akou sa správa prenáša. Sociálne siete tiež ponúkajú najvyšší stupeň interakcie, aký môžu súčasné komunikačné prostriedky používateľom poskytovať. Prístup k najrôznejším informáciám je takmer neobmedzený a lacný, zväčša úplne zadarmo. Taktiež nedostatok efektívnych a účinných opatrení zameraných na reguláciu online obsahu, na rozdiel od toho, ktorý sa vysiela prostredníctvom tradičných médií, robí online prostredie sociálnych sietí mimoriadne zaujímavým a tolerantným.

Zároveň je potrebné v tejto súvislosti dodať, že ide o nie veľmi bezpečné prostredie, a preto je nevyhnutné sa bezpečnosťou na sociálnych sieťach intenzívne zaoberať. Vzhľadom na veľký počet používateľov a interaktívny obsah, zdieľané osobné údaje a anonymitu komunikácie sa vytvoril ďalší priestor, v ktorom sa páchatelia realizujú a ohrozujú tým bezpečnosť používateľov. Sociálne siete pritom nemusia slúžiť len ako distribútor škodlivých kódov a informácií, ale zároveň sa v nich dokážu priamo tvoriť. Najčastejšími príkladmi sú dezinformácie, hoaxy, sociálne inžinierstvo, kyberšikanovanie, grooming, sexting a mnoho

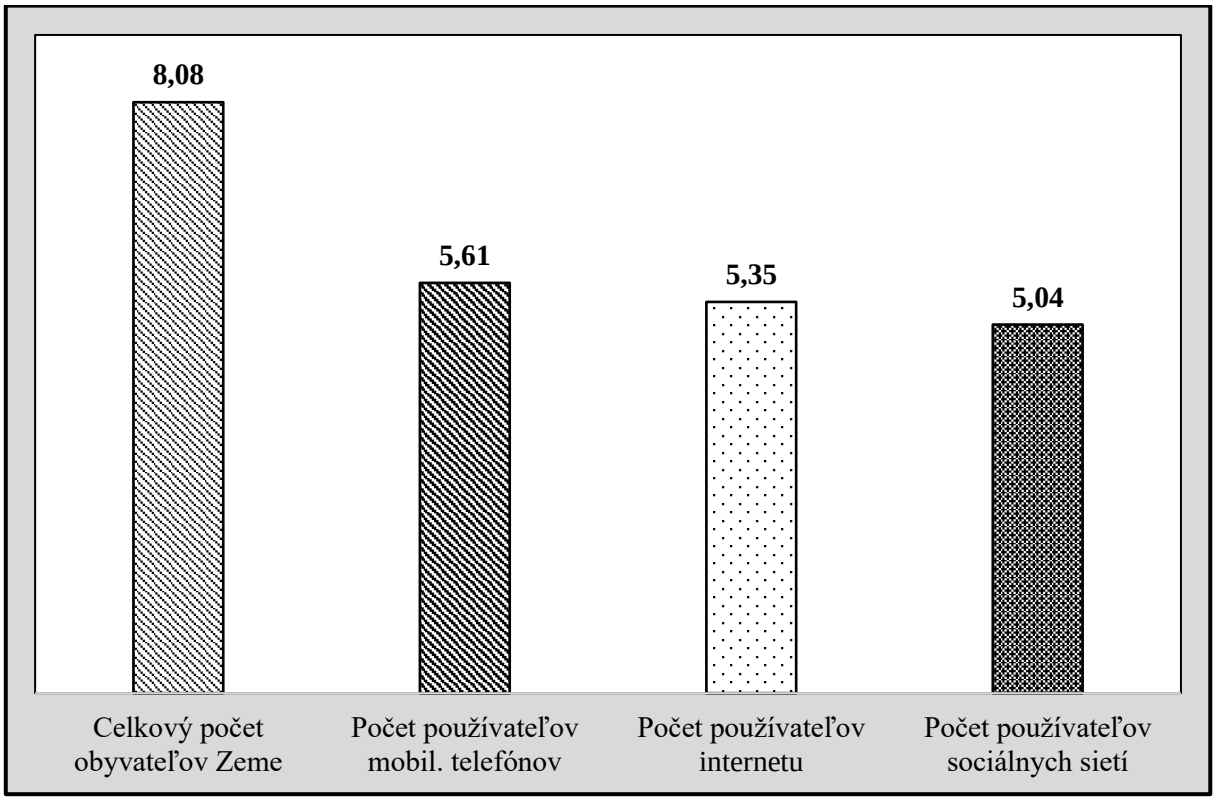
[28] NATO. 2020. NATO's approach to countering disinformation. In *North Atlantic Treaty Organisation*, 2020

[29] KUCHTOVÁ, J. 2018. Aktuálne trendy súvisiace s využívaním moderných technológií. In *Aktuálne výzvy kybernetickej bezpečnosti – zborník príspevkov z vedeckej konferencie*. Bratislava : Akadémia Policajného zboru, 2018

[30] HAJDÚKOVÁ, T. – HRUŠKA, P. 2018. Prínos siete Internet pre rozvoj spoločnosti a jeho možnosti využitia v činnosti Policajného zboru. In *Tradície a dynamika vývoja manažmentu a informatiky z pohľadu univerzít s bezpečnostným zameraním*. Bratislava : Akadémia Policajného zboru v Bratislave, 2018

ďalších, pričom páchatelia v záujme uchovania svojej anonymity na túto činnosť zneužívajú falošné profily.[31]

Čo sa týka penetračnej kapacity platforiem sociálnych sietí, poskytnuté štatistické údaje z konca januára 2024 poukazujú na kontinuálny nárast používania sociálnych sietí v porovnaní s predchádzajúcimi rokmi, ale aj na prognózu pokračovania tohto trendu v nasledujúcich rokoch. Podľa aktuálnych informácií mobilný telefón používa dnes cca 5,61 miliardy obyvateľov, čo predstavuje takmer sedem desatín (69,43 %) ľudskej populácie, internet používa približne 5,35 miliardy ľudí, teda zhruba dve tretiny (66,21 %) svetovej populácie, a počet aktívnych používateľov sociálnych sietí dosahuje zhruba 5,04 miliardy, čo predstavuje podiel na celkovom obyvateľstve planéty na úrovni 62,38 % (graf 1). Sociálne siete používa pritom prostredníctvom mobilného telefónu až 95 % ich užívateľov.[32]

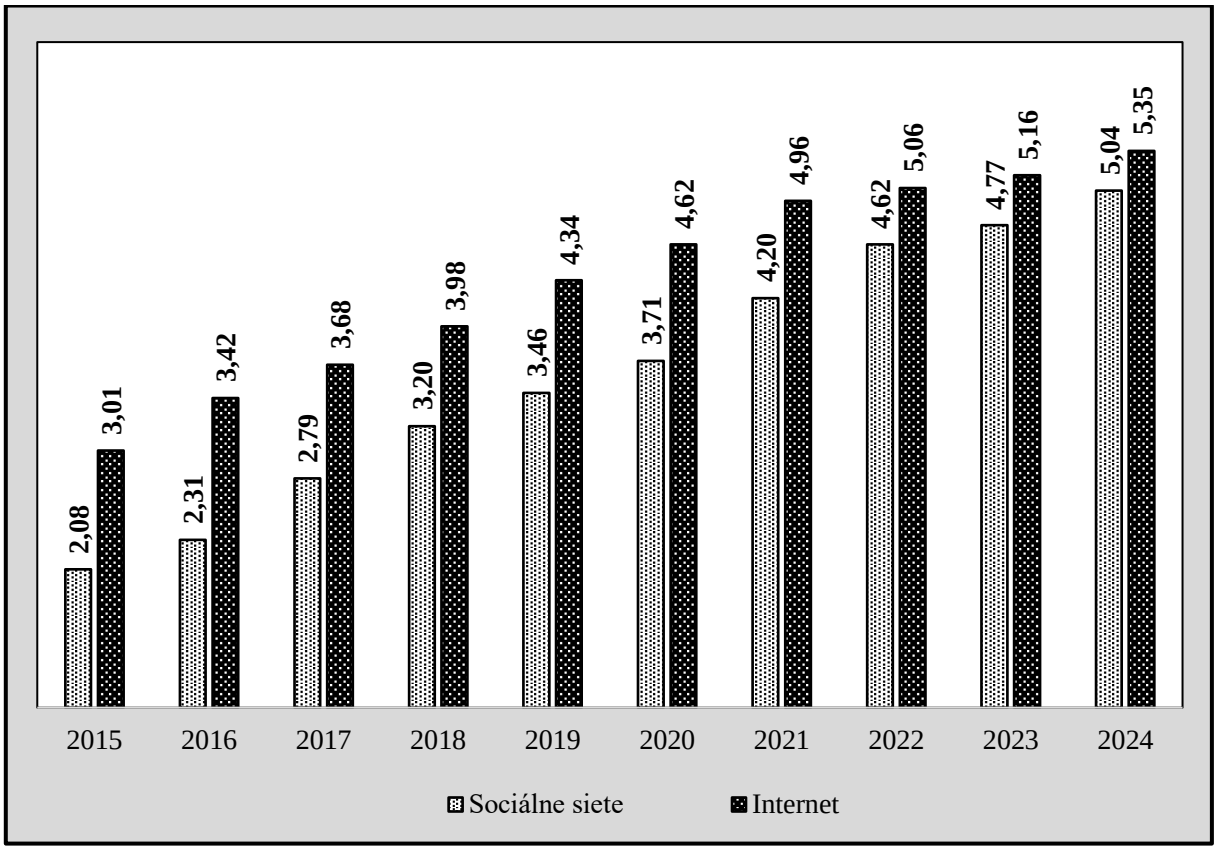


Graf 1 Prehľad o používateľoch mobilných telefónov, internetu a sociálnych sietí ku koncu januára 2024 na celom svete (v mld.)
Zdroj: DR, 2024

[31] ZACHAR KUCHTOVÁ, J. Bezpečnosť na sociálnych sieťach. *In: Bezpečnosť elektronickej komunikácie - zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou.* Bratislava: Akadémia Policajného zboru, 2022, s. 246

[32] DR. 2024. Global Digital Overview. In *DataReportal*, 2024

O tom, aký dynamický je rast používateľov internetu a sociálnych sietí svedčí fakt, že za ostatných desať rokov celosvetovo stúpol počet používateľov internetu o 77,7 %. Kým v roku 2015 používalo internet zhruba 3,01 miliardy ľudí, tak v roku 2024 to už bolo približne 5,35 miliardy. Z nich 96,5 % využíva pripojenie na internet prostredníctvom svojho mobilného telefónu a 61,8 % prostredníctvom osobného počítača alebo laptopu. Jeden užívateľ pritom strávi – bez ohľadu na účel – na internete priemerne denne 6 hodín a 40 minút.[33]



Graf 2 Prehľad rastu používateľov internetu a sociálnych sietí v rokoch 2015 až 2024 (v mld.)
Zdroj: DR, 2024

Rast používateľov sociálnych sietí je ešte dynamickejší, nakoľko stúpol v hodnotených rokoch takmer 2,5-násobne (o 242,3 %). Kým v roku 2015 používalo sociálne siete približne 2,08 miliardy ľudí, v roku 2024 je to už zhruba 5,04 miliardy (graf 2). Z nich jeden užívateľ strávi na sociálnych sieťach priemerne denne 2 hodiny a 23 minút. Najväčšia časť, takmer jedna polovica (49,5 %), používateľov sociálnych sietí ich primárne využíva na komunikáciu s rodinou a priateľmi. Takmer štyri desatiny (38,5 %) ich primárne využívajú na „zabitie“

[33] DR. 2024. Global Digital Overview. In *DataReportal*, 2024

voľného času, viac ako jedna tretina (34,2 %) na čítanie nových správ (informácií, noviniek), skoro tri desatiny (28,7 %) na to, aby vedeli, čo sa deje vo svete, resp. čo je nové, a viac ako jedna pätina (22,5 %) na šírenie názorov a diskusiu s ostatnými používateľmi sociálnych sietí.[34]

Šírenie dezinformácií ako hrozba pre súčasnú demokratickú spoločnosť

Všeobecným cieľom všetkých dezinformácií je pokúsiť sa ovplyvniť skutočných ľudí. Pre naplnenie tohto cieľa je potrebná stratégia, ktorá zahŕňa široké spektrum jednotlivých krokov, ktoré je potrebné naplánovať a realizovať pre dosiahnutie želaného výsledku. Pre šíriteľov dezinformácií je veľmi dôležité konkrétne stanovenie cieľovej skupiny, ktorú majú dezinformácie zasiahnuť, a vybrať vhodný obsah korešpondujúci s vytýčeným cieľom. Jedným z hlavných aspektov je voľba vhodných prostriedkov, ktoré majú byť využité pre dezinformačné účely. Primárnou platformou pre dezinformácie je dnes internet, v ktorého sieti ich šírenie sprostredkovávajú dezinformačné weby a sociálne siete, ale falošné, skreslené, zavádzajúce, klamlivé alebo úplne vymyslené informácie sa objavovali a objavujú v podstate v akýchkoľvek mediálnych kanáloch (napríklad v televízii, rozhlase, tlači) a šíriť sa môžu aj ústne.

Dezinformácie sú v súčasnosti veľmi úzko spájané s hybridnými hrozbami a hybridnou vojnou. Ich šírenie štátnymi aj neštátnymi aktérmi za účelom získania určitého politického, ideologického alebo ekonomického profitu je žiaľ v dnešnej dobe veľmi častým javom, ktorý negatívne ovplyvňuje bezpečnosť krajín, predovšetkým demokratických krajín.[35] Výskyt najrôznejších dezinformačných kampaní, ako jedného z prostriedkov vedenia tzv. hybridnej vojny, sa v posledných rokoch neustále zvyšuje.[36] Hoci dezinformácie, ako je už uvedené vyššie v texte, nie sú novým javom v spoločnosti, ich význam z hľadiska bezpečnosti štátu sa zvýšil najmä v súvislosti so vznikom moderných technológií a novších a efektívnejších techník ich šírenia.

[34] DR. 2024. Global Digital Overview. In *DataReportal*, 2024

[35] JURČÁK, V. – JURČÁK, J. – SASARÁK, J. 2016. Hybridné hrozby – výzva pre Európsku úniu. In *Medzinárodné vzťahy – aktuálne otázky svetovej ekonomiky a politiky*. Bratislava : Ekonomická univerzita, Fakulta medzinárodných vzťahov, 2016; IVANČÍK, R. 2022. Dezinformácie ako hybridná hrozba. In *Dezinformácie a právo (úlohy a postavenie bezpečnostných zložiek) : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2022; KAŠČÁK, M. 2023. Kultúra organizácie verejnej správy a jej význam pre problematiku hybridných hrozieb. In *Konferencia Zvýšenie odolnosti Slovenska voči hybridným hrozbám*, 2023

[36] JURČÁK, V. – TURAC, J. 2018. Hybridné vojny – výzva pre NATO. In *Bezpečnostné fórum 2018 – zborník vedeckých prác z medzinárodnej vedeckej konferencie*. Banská Bystrica : Interpolis, 2018; IVANČÍK, R. 2023. Aktuálne východiská skúmania problematiky hybridných hrozieb. In *Policajná teória a prax*, 2023; KOLLÁR, D. 2022. Dezinformácie ako kľúčová bezpečnostná výzva súčasnosti v kontexte rusko-ukrajinského konfliktu. In *Politické vedy*, 2022

Štátni aj neštátni aktéri čoraz viac využívajú dezinformačné stratégie na to, aby mohli ovplyvňovať verejné diskusie v demokratických spoločnostiach, spochybňovať demokratické pravidlá, zásady a princípy, podporovať polarizáciu spoločnosti, podnecovať chaos, vzbudzovať v ľuďoch neistotu, strach a zasahovať do demokratického rozhodovania.[37] Pre bezpečnosť štátov sú hrozbou predovšetkým preto, že šírenie dezinformácií oslabuje dôveru občanov v demokratické inštitúcie a demokratické procesy prebiehajúce v demokratických spoločnostiach, čo môže v extrémnych prípadoch viesť až k prevratu a následnej zmene režimu – z demokratického na autokratický. Úlohou demokratických štátov a ich kompetentných zložiek (vlád, príslušných ministerstiev, ozbrojených bezpečnostných zborov, spravodajských služieb a ďalších kompetentných úradov a inštitúcií) je v rámci zaisťovania ich bezpečnosti bojovať s dezinformačnými kampaňami, prijímať adekvátne opatrenia a snažiť sa o elimináciu negatívnych účinkov dezinformácií na spoločnosť.

Záver

V súčasnej modernej digitálnej ére široko dostupného internetu a najrozličnejších vysoko výkonných „smart“ zariadení sa ľudia dokážu dostať k veľkému množstvu informácií veľmi rýchlo a jednoducho. Najnovšie správy či údaje sú ľahko dostupné prostredníctvom internetových webových stránok, spravodajských portálov alebo platforiem sociálnych sietí. S rastúcim množstvom informácií sa zvyšuje aj množstvo dezinformácií. Ich cieľom je zapôsobiť na adresátov tak, aby uverili informáciám, ktoré sú v nich prezentované, ako faktom, hoci predstavujú správy, ktoré sú falošné, zavádzajúce, skreslené, pozmenené či nepravdivé (alebo aspoň z časti nepravdivé). Ukazuje sa pritom, že dezinformácie ovplyvňujú správanie, mienku a názory ľudí oveľa viac, než by sa na prvý pohľad mohlo zdať.

Jedným z dôvodov prečo majú taký vplyv a prečo predstavujú problém najmä pre demokratickú spoločnosť, je ich ľahká dostupnosť pre všetkých a rýchlosť ich šírenia. K obom týmto atribútom prispelo najmä masové rozšírenie internetu a rozmach sociálnych sietí, kde predovšetkým mladí ľudia trávia až príliš veľa času a kde môže ktokoľvek rýchlo, jednoducho a zadarmo dezinformácie rôzneho typu vytvárať a šíriť. Pre mnohých ľudí je často oveľa pohodlnejšie získavať informácie zo sociálnych sietí ako z vedeckých a odborných publikácií

[37] IVANČÍK, R. 2020. Analýza prístupov k definovaniu a vymedzeniu hybridnej vojny. In *Národná a medzinárodná bezpečnosť 2020 – zborník príspevkov z medzinárodnej vedeckej konferencie*. Liptovský Mikuláš : Akadémia ozbrojených síl gen. M. R. Štefánika. 2020

a časopisov či z klasických spravodajských portálov, čo tiež prispieva k prehlbovaniu tohto problému.

Na rozdiel od serióznych médií, ktoré si pred zverejnením informácie overujú jej pravdivosť z viacerých zdrojov a tieto zdroje uvádzajú pri jednotlivých správach, v sociálnych sieťach doposiaľ nebol vytvorený plne funkčný a účinný mechanizmus, ktorý by slúžil na oddeľovanie pravdivých a nepravdivých informácií.[38] Ďalším problémom je fakt (existujú o tom mnohé svedectvá a dôkazy), že množstvo priaznivcov prostredníctvom internetu a sociálnych sietí priťahujú a získavajú na svoju činnosť radikálne organizácie, ktoré šíria rôzne falošné správy nielen v podobe dezinformácií, ale aj rozličných konšpiračných teórií, hoaxov a tiež propagandu.

Medzi najzraniteľnejšie z hľadiska šírenia dezinformácií ako súčasti hybridných hrozieb patria súčasné moderné demokratické štáty. Európska únia i jej členské štáty už prijímajú praktické opatrenia na neutralizáciu dezinformácií, ale pre každý členský štát je dôležité mať aj vlastnú transparentnú a konkrétnu politiku, prípadne viac politík, stratégií alebo koncepcií zameraných na boj proti dezinformáciám šíreným zo strany nepriateľských štátnych i neštátnych aktérov. Zvýšenie povedomia o falošných, skreslených, klamlivých, zavádzajúcich či pozmenených alebo úplne vymyslených informáciách v podobe dezinformácií, zlepšenie schopnosti rozoznávať a odhaľovať ich, ako aj eliminovať ich šírenie v čo najväčšej miere by určite znamenalo menej príležitostí napríklad pre populizmus, radikalizmus, extrémizmus, xenofóbiu či akékoľvek ovplyvňovanie alebo rozdeľovanie súčasnej demokratickej spoločnosti práve na základe posúvania najrôznejších dezinformácií.

Nanešťastie, faktom je, že dezinformáciám sa v dnešnej modernej informačnej spoločnosti nedá vyhnúť, ale je dôležité, aby ich človek vedel rozoznať a aby sa nimi nenechal zmanipulovať a ovplyvniť, čo môže priniesť množstvo negatívnych dôsledkov, ako pre jedincov, tak pre celú demokratickú spoločnosť. Naučiť sa kriticky premýšľať o falošných, skreslených, klamlivých, zavádzajúcich, pozmenených alebo úplne vymyslených správach v podobe dezinformácií môže viesť k žiadúcemu výsledku naučiť sa kriticky premýšľať aj o sociálnych sieťach a médiách a nimi šírených informáciách.

[38] HAJDÚKOVÁ, T. – ŠIŠULÁK, S. 2022. Abuse of modern means of communication to manipulate public opinion. In *INTED2022 Proceedings Publisher: IATED*, 2022, s. 1995

Zoznam použitej literatúry

DR. 2024. Global Digital Overview. In *DataReportal*, 2024. [online] [cit. 16.03.2023]. Dostupné na internete: <https://sdu.sk/wj4S>.

DUŠEK, J. – KAVAN, Š. 2024. Dezinformace jako součást hybridních hrozeb – česko-slovenský pohled. In *Auspicia*, 2024, roč. 21, č. 1, s. 7-26. ISSN 2464-7217.

EU. 2018. Action Plan Against Disinformation. In *European Commission*, 2018. [online] [cit. 14-11-2023] Dostupné na internete: <https://sdu.sk/NXW>.

EU. 2021. The impact of disinformation on democratic processes and human rights in the world. In *European Parliament*, 2021. 64 s. ISBN 978-92-846-8014-6. [online] [cit. 15-04-2024] Dostupné na internete: <https://sdu.sk/vEm1>.

HAJDÚKOVÁ, T. – HRUŠKA, P. 2018. Prínos siete Internet pre rozvoj spoločnosti a jeho možnosti využitia v činnosti Policajného zboru. In *Tradície a dynamika vývoja manažmentu a informatiky z pohľadu univerzít s bezpečnostným zameraním*. Bratislava : Akadémia Policajného zboru v Bratislave, 2018, s. 131-142. ISBN 78-80-8054-768-4.

HAJDÚKOVÁ, T. – ŠIŠULÁK, S. 2022. Abuse of modern means of communication to manipulate public opinion. In *INTED 2022 – Proceedings from 16th International Technology, Education and Development Conference*. IATED Spain, 2022, s. 1992-2000. ISBN 978-84-09-37758-9.

IVANČÍK, R. 2021. Boj proti dezinformáciám týkajúcich sa pandémie koronavírusu na úrovni Európskej únie. *Almanach – aktuálne otázky svetovej ekonomiky a politiky*, 2021, roč. 16, č. 3, s. 5-15. ISSN 1339-3502.

IVANČÍK, R. 2022. Dezinformácie ako hybridná hrozba. In *Dezinformácie a právo – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2022, s. 54-65. ISBN 978-80-8054-965-7.

IVANČÍK, R. 2023. Aktuálne východiská skúmania problematiky hybridných hrozieb. In *Policajná teória a prax*, 2023, roč. 31, č. 3, s. 38-52. ISSN 1335-1370.

JURČÁK, V. – JURČÁK, J. – SASARÁK, J. 2016. Hybridné hrozby – výzva pre Európsku úniu. In *Medzinárodné vzťahy – aktuálne otázky svetovej ekonomiky a politiky*. Bratislava : Ekonomická univerzita, 2016, s. 542-550. ISBN 978-80-225-4365-1.

JURČÁK, V. – TURAC, J. 2018. Hybridné vojny – výzva pre NATO. In *Bezpečnostné fórum 2018 – zborník vedeckých prác z medzinárodnej vedeckej konferencie*. Banská Bystrica : Interpolis, 2018. s. 177-184. ISBN 978-80-972673-5-3.

KAŠČÁK, M. 2023. Kultúra organizácie verejnej správy a jej význam pre problematiku hybridných hrozieb. In *Konferencia Zvýšenie odolnosti Slovenska voči hybridným hrozbám*, 2023, s. 188-193. ISBN 978-80-8293-010-1.

KOLLÁR, D. 2022. Dezinformácie ako kľúčová bezpečnostná výzva súčasnosti v kontexte rusko-ukrajinského konfliktu. In *Politické vedy*, 2022, roč. 25, č. 3, s. 87-109. ISSN 1335-2741.

KUCHTOVÁ, J. 2018. Aktuálne trendy súvisiace s využívaním moderných technológií. In *Aktuálne výzvy kybernetickej bezpečnosti – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2018, s. 90-98. ISBN 978-80-8054-773-8.

NATO. 2020. NATO's approach to countering disinformation. In *NATO*, 2020. [online] [cit. 16-11-2023] Dostupné na internete: <https://sdu.sk/Nfn25>.

NBÚ. 2023. Dezinformácia. In *Krátky slovník hybridných hrozieb*, 2023. [online] [cit. 15-11-2023] Dostupné na internete: <https://sdu.sk/JAMdX>.

LISOŇ, M. – FIDLER, Ľ. 2024. Spravodajská dezinformácia pri plnení úloh spravodajských služieb v Slovenskej republike. In *Policajná teória a prax*, 2024, roč. 32, č. 1, s. 176-191. ISSN 1335-1370.

SAPÍK, M. 2022. Etika v prostředí moderní společnosti. In *Auspicia*, 2022, roč. 19, č. 1, s. 104-116. ISSN 2464-7217. [online] [cit. 15-04-2024] Dostupné na: <https://sdu.sk/0hfLS>.

Slovník cudzích slov. 2023. Dezinformácia. In *Slovníkový portál Jazykovedného ústavu Ľ. Štúra SAV*, 2023. [online] [cit. 10-07-2023] Dostupné na internete: <https://sdu.sk/7yDN>.

Slovník pojmov z mediálnej výchovy. 2020. Dezinformácia. In *Mediálna výchova*, 2023. [online] [cit. 15-11-2023] Dostupné na: <https://sdu.sk/GO8>.

Slovník súčasného slovenského jazyka. 2023. Dezinformácia. In *Slovníkový portál Jazykovedného ústavu Ľ. Štúra SAV*, 2023. [online] [cit. 15-11-2023] Dostupné na internete: <https://sdu.sk/7rY>.

ŠIŠULÁK, S. – CÍCHOVÁ, M. 2019. Fake news a propaganda v kybernetickom priestore In *Aktuálne výzvy kybernetickej bezpečnosti v podmienkach bezpečnostných zložiek – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2019, s. 156-167. ISBN 978-80-8040-819-3.

ZACHAR KUCHTOVÁ, J. 2022. Bezpečnosť na sociálnych sieťach. In *Bezpečnosť elektronickej komunikácie – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou.* Bratislava : Akadémia Policajného zboru, 2022, s. 237-247. ISBN 978-80-8054-968-8.

Kontaktné údaje

plk. gšt. v. z. doc. Ing. Radoslav Ivančík, PhD. et PhD., MBA, MSc.
Katedra informatiky a manažmentu
Akadémia Policajného zboru v Bratislave
Sklabinská 1, 835 17 Bratislava
e-mail: radoslav.ivancik@akademiapz.sk

Recenzenti:

prof. RNDr. Michal Greguš, CSc.
doc. Ing. Václav Friedrich, Ph.D.

Útoky na školách – aktuálna bezpečnostná výzva

Martin Kaščák

Abstrakt: Zámerom článku je prispieť k poznaniu nástrojov bezpečnostného manažmentu slúžiacich na minimalizáciu rizík páchania útokov na školách. Autor postupuje od priblíženia jednotlivých pojmov, postupov a návodov bezpečnostného manažmentu, cez identifikáciu jednotlivých špecifík útokov na školy až po praktické odporúčania a rady, ktoré je potrebné poznať, aplikovať v praxi a ovládať v záujme prežitia zamestnancov a žiakov počas útoku na školu. V závere sa autor zamýšľa nad prítomnosťou násilia v ľudskej spoločnosti.

Kľúčové slová: Útoky na školách, bezpečnostný manažment, mäkké ciele, terorizmus.

Abstract: The aim of this article is to contribute to the understanding of security management tools used to minimize the risks of attacks on schools. The author begins by explaining various concepts, procedures, and guidelines of security management, followed by identifying the specific characteristics of school attacks. The article then provides practical recommendations and advice that are essential to know, apply in practice, and master to ensure the survival of employees and students during a school attack. In conclusion, the author reflects on the presence of violence in human society.

Keywords: School attacks, security management, soft targets, terrorism.

Úvod

V dňoch 3. - 14. 5. 2024 sa Slovenská republika stala cieľom masívnych hrozieb bombovými útokmi na školy a ďalšie inštitúcie. Hoci sa v areáloch uvádzaných inštitúcii výbušnina nenašla, orgány štátu neberú vzniknutú situáciu na ľahkú váhu. Predseda výboru Národnej rady Slovenskej republiky pre obranu a bezpečnosť avizoval zvolanie Bezpečnostnej rady štátu, ktorej úlohou v čase mieru je vyhodnocovanie bezpečnostnej situácie v Slovenskej republike.[1] K zvolaniu zasadnutia Bezpečnostnej rady štáty závažným aj útok študenta Karlovej univerzity z 21. 12. 2023, počas ktorého prišlo o život celkovo 14 študentov a pedagógov. Pred samotným útokom poprinášal do školy celý strelecký arzenál. Podľa vyjadrenia českého ministra vnútra sa počet obetí tohto útoku mohol „pohybovať vo vysokých desiatkach“[2]. Uvedený zločin spôsobil vlnu sekundárnych útokov a hrozieb podobnými útokmi nie len v Čechách, ale aj na Slovensku. Z toho dôvodu iniciovali novozvolené vedenia ministerstiev

[1] Zákon č. 110/2004 Z. z. § 2 písm. c) ods. 1
[2] *Pri streľbe na pražskej univerzite zomrelo 14 ľudí, útočník zabíjal aj predtým* [on-line] [21. 12. 2023] Dostupné na: https://svet.sme.sk/c/23259930/praha-strelba-cesko.html

vnútra a školstva Slovenskej republiky zavedenie „komplexných opatrení na zvýšenie ochrany žiakov, študentov a zamestnancov na všetkých stupňoch školstva“[3].

K dnešnému dňu ešte nie je zverejnený profil páchateľa z Karlovej univerzity, jeho motív, ani okolnosti tejto masovej vraždy. Dokázané je, že krátko pred útokom zastrelil neznámeho človeka s dvojmesačným dieťaťom a svojho otca. Prokurátorka (štátna zástupkyňa) Murínova v českom parlamente potvrdila, že páchateľ sa v minulosti liečil u psychiatra, pričom jednoznačne vylúčila chorobný motív. Zároveň je známe, že išlo o výborného študenta s ocenením za študentskú prácu. Neobvyklé je, že napriek tomu, že žil sám u rodičov, dostal pôžičku na viac ako milión českých korún. Získal tým prostriedky na rozsiahly zbrojný arzenál, vrátane automatických pušiek, akými sa najčastejšie páchajú útoky na školách. V pivnici rodinného domu jeho rodičov boli nájdené dve tlakové bomby, na ktorých boli položené plastové obaly obsahujúce kovové guličky. Ďalšie bomby boli napojené na nádoby s chemikáliami a prepojené elektrickými káblami na iné zariadenia. Dňa 10. 12. 2023 mal na Telegrame v azbuke napísať „Dovoľte aby som sa predstavil, som David. Chcem strieľať v škole...vždy som chcel zabíjať.“

Z toho, čo o páchateľovi doposiaľ vieme, je zrejmé, že spĺňal najčastejšie spoločné znaky útočníkov na školy: vysoké IQ, technické znalosti, voľba mäkkého cieľa, istý druh psychickej poruchy, aktivita na sociálnej sieti atď. Či už išlo o psychopatologický terorizmus,[4] (ak je dominantným cieľom psychické uspokojenie páchateľa teroristickou činnosťou[5]) alebo nie, jedno je isté, pri útokoch na školy máme dočinenia s teroristickým stupňom ohrozenia a mnohými spoločnými znakmi s teroristami, čo si vyžaduje rovnako nekompromisný prístup a nasadzovanie rovnako tvrdých bezpečnostných prostriedkov, ako voči ktorémukoľvek inému druhu terorizmu.

1 Význam bezpečnostného manažmentu pre bezpečnosť organizácie i štátu

Bezpečnostný manažment je špeciálnym manažmentom všeobecného manažmentu. Cieľom bezpečnostného manažmentu je zaistenie bezpečnosti akejkoľvek organizácie, vrátane celej spoločnosti. Zdrojmi poznatkov sú viaceré vedné odbory, má multidisciplinárny charakter. Bezpečnostný manažment aplikuje vedecké poznatky do praxe, predovšetkým do tvorby a realizácie komplexných bezpečnostných systémov jednotlivých organizácií i štátu ako celku,

[3] *Rezorty školstva a vnútra spoločne posilňujú bezpečnosť na školách* [on-line] [09. 04. 2024] Dostupné na: https://www.minedu.sk/rezorty-skolstva-a-vnutra-spolocne-posilnuju-bezpecnost-na-skolach/
[4] Synonyum „patologický terorizmus“, porovnaj: Ibl, 2007, s. 31.
[5] Mareš, 2005, s. 361.

preto ho označujeme za praxeologickú vednú disciplínu. Bezpečnostný manažment je kľúčovým prvkom ochrany aktív organizácie: zamestnancov, majetku a ostatných referenčných objektov organizácie. Dôležitosť bezpečnostného manažmentu spočíva predovšetkým v prevencii vzniku krízových bezpečnostných situácií. Pod prevenciou v tomto kontexte rozumieme nie len samotnú realizáciu bezpečnostného systému, vypracovanie plánov na minimalizáciu bezpečnostných rizík, ale aj mnoho ďalších opatrení, ktorým sa v tomto príspevku budeme venovať.

Vzhľadom na stále nové technické možnosti páchateľov, je v rámci bezpečnostného manažmentu dôležité neustále prehodnocovať a aktualizovať bezpečnostné postupy, a to na základe nových poznatkov a najlepšej praxe zo zahraničia. V tejto súvislosti je potrebná implementácia najnovších bezpečnostných postupov odporúčaných bezpečnostnými orgánmi štátu a organizáciami špecializujúcich sa na túto oblasť. Prijaté opatrenia na zlepšenie bezpečnosti je potrebné trvalo dodržiavať, funkčnosť technických prostriedkov neustále monitorovať a dbať na dodržiavanie všetkých noriem a štandardov. *„Je nevyhnutné neustále skúmať aktuálny stav technických prostriedkov, aktuálnu ponuku produktov na trhu s ohľadom na možné využitie pri policajnej práci, potrebu modernizovať už existujúce zariadenia a to najmä z dôvodu, aby páchatelia trestnej činnosti a narušovatelia verejného poriadku neboli v predstihu pred výkonnou mocou štátu a neohrozovali tak bezpečnosť spoločnosti – život zdravie a majetok.“*[6] Skúsenosť totiž učí, že po pominutí aktuálnej bezpečnostnej hrozby dochádza k zníženiu dôslednosti pri zaisťovaní bezpečnosti objektu, čo uľahčuje prienik prípadných útočníkov do škôl.

Avizované komplexné opatrenia ministerstiev vnútra a školstva budú vychádzať z rozsiahleho dotazníkového prieskumu na základných a stredných školách a z individuálneho zistenia skutkového stavu v oblasti bezpečnosti na vysokých školách. Takýto postup je charakteristický pre systémový prístup k riešeniu danej problematiky, keďže konkrétne opatrenia sa budú navrhovať až na základe analýzy súčasného stavu vecí. Uvedené kroky predstavujú aktívny prístup k riešeniu konkrétnej bezpečnostnej hrozby, čo znamená, že útoky na školách sa v súčasnosti považujú za bezpečnostnú výzvu. Pod pojmom bezpečnostná výzva chápeme taký prístup k bezpečnostnej hrozbe, ktorý predstavuje napríklad konkrétnu spoluprácu medzi štátnymi i neštátnymi organizáciami s cieľom prijímania účinných bezpečnostných opatrení na minimalizovanie rizika naplnenia určitej hrozby. Bezpečnostná

[6] Kuchtová, 2020, s.172

hrozba, synonymum ohrozenie, je taký fenomén, ktorý má potenciál bezprostredného poškodenia aktív referenčného objektu. Pod aktívami chápeme všetko čo je hodné ochrany, čo má pre organizáciu význam. Referenčným objektom môže byť štát, sociálna skupina, organizácia i človek ako indivíduum.[7]

2 Minimalizácia bezpečnostných rizík

Život v súčasnej modernej spoločnosti je neoddeliteľne spojený s rizikom. Riziko sa nedá odstrániť, iba znížiť do rozumnej miery. Rozumnou bezpečnosťou sa chápe prijímanie takých opatrení na minimalizáciu rizík, ktoré budú adekvátne, čiže nebudú presahovať hodnotu chráneného aktíva referenčného objektu a nebudú presahovať ekonomické, technologické, politické a demografické možnosti štátu. Pod rizikom rozumieme možnosť škody, straty, neúspechu[8]. Pre minimalizáciu rizík je potrebné neustále analyzovať možné riziká. Analýza rizík predstavuje proces identifikácie rizík, ich vyhodnotenia a následného odporúčania konkrétnych bezpečnostných opatrení. Cieľom analýzy rizík je poskytnúť organizácii informácie potrebné na rozhodovanie sa o tom, ako najlepšie riadiť a minimalizovať riziká, aby sa dosiahla bezpečnosť a ochrana jej záujmov. Bezpečnosť organizácie teda zahŕňa súbor opatrení, postupov a technológií, ktoré organizácia implementuje na ochranu svojich aktív. Tieto opatrenia môžu zahŕňať fyzickú bezpečnosť budov, informačnú bezpečnosť dát, riadenie prístupu k informáciám, bezpečnostné školenia pre zamestnancov a krízový manažment.

Nech už prijmeme bezpečnostné opatrenia politického, sociálneho, ekonomického či informačného charakteru, na individuálnej, kolektívnej, regionálnej či štátnej úrovni, jedno je isté: žiadny objekt nemôže dosiahnuť absolútne zaistenie svojej bezpečnosti.[9] Osobitne v prípade útokov na školy musíme dennodenne podstupovať riziko, že u niektorého zo žiakov či študentov preváži komplex možných príčin k útoku nad mieru strachu o svoje zdravie a život. V takom prípade prichádza k útokom na zdravie a život ostatných ľudí aj za cenu ohrozenia vlastného života. Z uvedeného dôvodu je potrebné využívať aj predikciu kriminality. Tento pomerne nový nástroj bezpečnostného manažmentu v sebe zahŕňa identifikáciu možných hrozieb a ich pravdepodobný výskyt, hodnotenie ich závažnosti a prioritizácie na základe ich stupňa a pravdepodobnosti výskytu. V súčasnosti sa na tento účel využíva umelá inteligencia, ktorá na základe existujúcich dát a modelov dokáže predpovedať potenciálne ohrozenia.

[7] Hofreiter, 2015, s. 63.
[8] *Slovník súčasného slovenského jazyka*. [on-line] [20. 05. 2024] Dostupné na: https://www.juls.savba.sk/pub_sssj.html
[9] Ivančík, Baričičová, 2020.

Využíva pritom napríklad strojové učenie, rozpoznávanie vzorov a analýzu sociálnych sietí. Strojové učenie je odvetvie umelej inteligencie zaoberajúce sa vývojom algoritmov, ktoré umožňujú počítačom učiť sa a robiť rozhodnutia bez ľudskej ingerencie. Pod rozpoznávaním vzorov rozumieme možnosť počítačov identifikovať a interpretovať vzory v komplexných dátach. Analýza sociálnych sietí a internetových fór je dôležitá pre identifikáciu podozrivých vzorov správania. Pomocou tejto analýzy môže umelá inteligencia identifikovať potenciálnych páchateľov predtým, než spáchajú trestný čin. Ide o dôležitý nástroj pre zaznamenanie varovných signálov, ktoré však musia byť dôkladne vyhodnocované bezpečnostným analytikom, nakoľko ide o veľmi závažné rozhodnutia.

Ďalšou metódou je inteligentný dozor. Je to technologický systém, ktorý zaznamenáva a monitoruje činnosť ľudí v objektoch a v ich okolí. Tento systém využíva rôzne senzory a kamery na získavanie a následné spracovanie dát. Inteligentný dozor umožňuje real-time sledovanie, presnejšiu detekciu a automatizované spracovanie dát. Môže byť nainštalovaný v školách na rýchlu identifikáciu podozrivého správania. Tieto systémy môžu byť naprogramované na identifikáciu zbrane a na okamžité privolanie bezpečnostných síl. Nakoľko môžu byť tieto systémy zneužité na sledovanie jednotlivcov bez ich súhlasu, je pri implementácii inteligentného dozoru dôležité dodržiavať zásady ochrany súkromia.

Umelá inteligencia môže poslúžiť aj páchateľom, preto jej využívanie je kľúčovým hráčom v prevencii násilia na školách, aby sa aj v tomto prípade nestalo, že páchateľ bude krok pred bezpečnostnými zložkami. Investície do vývoja nových technológií a využívanie ich potenciálu prispeje vysokou mierou k zvýšeniu bezpečnosti študentov, pedagógov a zamestnancov škôl. Je nevyhnutné spolupracovať s odborníkmi a zákonodarcami na postupnej implementácii týchto systémov v rámci celej spoločnosti.

3 Špecifiká útokov na školy

Školy, nákupné centrá, nemocnice či trhoviská patria medzi tzv. mäkké ciele. „Mäkké ciele sú objekty (budovy, areály, voľné priestranstvá), v ktorých sa zoskupuje veľké množstvo osôb. Tieto objekty nemajú aplikované žiadne alebo len mierne špeciálne bezpečnostné opatrenia, ktoré by bránili násilnému útoku na život osôb nachádzajúcich sa v týchto objektoch, zabezpečovali by rýchlu reakciu na tento útok, alebo by napomáhali zvládnutiu potenciálneho násilného útoku bez straty na životoch osôb. Násilný útok na tento cieľ by mohol spôsobiť smrť,

alebo zranenie osoby, alebo viacerých osôb, ktoré sa v blízkosti nachádzajú.“[10] Na rozdiel od ostatných mäkkých cieľov majú útoky na školách viacero špecifík. Analýzou útokov na školách za posledných 30 rokov v Európe z bežne dostupných otvorených zdrojov sa dajú určiť nasledujúce spoločné znaky páchateľov:

- ✓ Študent alebo bývalý študent
- ✓ Vek do 30 rokov
- ✓ Šikanovaný alebo zo školy vylúčený
- ✓ Z neúplnej alebo nefunkčnej rodiny
- ✓ V nepriaznivej finančnej situácii
- ✓ Frustrovaný až zúfalý
- ✓ Psychický labilný so sklonom k agresivite
- ✓ Odhodlaný k samovražde z bezvýchodiskovosti svojej situácie
- ✓ Aktívny na sociálnych sieťach
- ✓ Vysoké IQ
- ✓ Technické znalosti
- ✓ Učiaci sa od predchádzajúcich páchateľov
- ✓ Ozbrojený zbraňou, najčastejšie automatickou.

Z uvedeného vyplýva napríklad aj to, že páchateľmi útokov na školy sú insideri. Sú to žiaci či študenti dopodrobna poznajúci prostredie školy a jej okolie a sú alebo boli priebežne oboznamovaní s prijímanými opatreniami, ktoré mali zabrániť útokom. Z toho dôvodu nie je vhodné oznamovať všetky prijaté opatrenia žiakom, študentom, zamestnancom, ale ani pedagógom škôl (13. 03. 1996 v škótskom meste Dunblane vedúci športových krúžkov zastrelil 13 prvákov a 2 učiteľov). Rodičov a verejnosť je však potrebné ubezpečiť, že sa prijali opatrenia, ktoré zvýšili stupeň ochrany konkrétnej školy. Samotný prvý krok novozvoleného vedenia ministerstva vnútra, vyčlenenie 2050 príslušníkov Policajného zboru, ako kontaktných osôb pre každú školu, zabezpečuje vyšší stupeň ochrany, ako majú ostatné mäkké ciele v Slovenskej republike.

Ďalším špecifikom je, že väčšina útočníkov bola vystavená dlhodobo neriešiteľnej životnej situácii. „Mnohí strelci sa pred udalosťami cítili zúfalo, či už boli diagnostikovaní ako duševne chorí alebo nie. Často je to kombinácia ťažkej depresie, úzkosti a zúfalstva, ktorá ich

[10] Ďuricová a kol., 2017, s. 465–472.

vedie k ukončeniu ich vlastných životov."[11] Problémy vyplývajú z domáceho prostredia, partie alebo zo školy. V školách ide najčastejšie o šikanovanie.

Prieskum UNICEF[12] v 122 krajinách u detí vo veku od 13 do 15 rokov zistil, že približne polovica z nich zažíva rôzne formy násilia zo strany svojich rovesníkov a šikanovanie. Z toho dôvodu vydal v roku 2010 publikáciu: *Zastavenie násilia na školách: Sprievodca pre učiteľov*[13]*,* ktorá odporúča viacero opatrení, z ktorých vyberáme:

- ✓ V každej komunite verejne odmietajme akékoľvek násilie ako prostriedok na riešenie problémov.
- ✓ Učme študentov a žiakov o ich právach (ale aj o povinnostiach)[14] pomocou príbehov, debát či hrania rolí.
- ✓ Vytvorme spoločné pravidlá úctivého správania sa k sebe pre triedu, ktoré sú pozitívne, poučné a stručné.
- ✓ Včas zastavme zárodky šikanovania (napríklad oboznamovaním s princípmi fungovania tzv. pyramídy nenávisti).[15]
- ✓ Pomáhajme zvyšovať odolnosť študentov a ich schopnosť vyrovnať sa s každodennými životnými výzvami a stresom.
- ✓ Pravidelnou a slobodnou diskusiou odhaľujme včas možnú frustráciu.[16]

4 Vražda začína nálepkovaním, zosmiešňovaním, šikanovaním...

Pyramída nenávisti[17] je názorná pomôcka ilustrujúca možnú eskaláciu napätia od vzniku problému až do jeho neriešiteľnosti a následného použitia násilia. Každý nižší stupeň pyramídy predstavuje podmienky a predpoklady pre ten vyšší, preto prevenciou vyhrotenia situácie až do fatálneho „vyriešenia problému“ násilím je zamedziť výstavbe už jej základného stupňa. Prvou podmienkou pre vybudovanie základne pyramídy nenávisti je rozdelenie danej komunity na *my*

[11] *School Shooters: Understanding their paths to violence is key to prevention.* [on-line] [29. 05. 2022] Dostupné na: https://www.npr.org/sections/health-shots/2019/02/10/690372199/school-shooters-whats-their-path-to-violence?t=1591878658203

[12] *Violence in the lives of children and adolescents.* [on-line] [20. 05. 2024] Dostupné na: https://www.unicef.org/publications/files/Violence_in_the_lives_of_children_and_adolescents.pdf

[13] *Stopping Violence in Schools: A Guide for Teachers* [on-line] [2009] Dostupné na: https://unesdoc.unesco.org/ark:/48223/pf0000184162

[14] Doplnil autor príspevku

[15] Doplnil autor príspevku

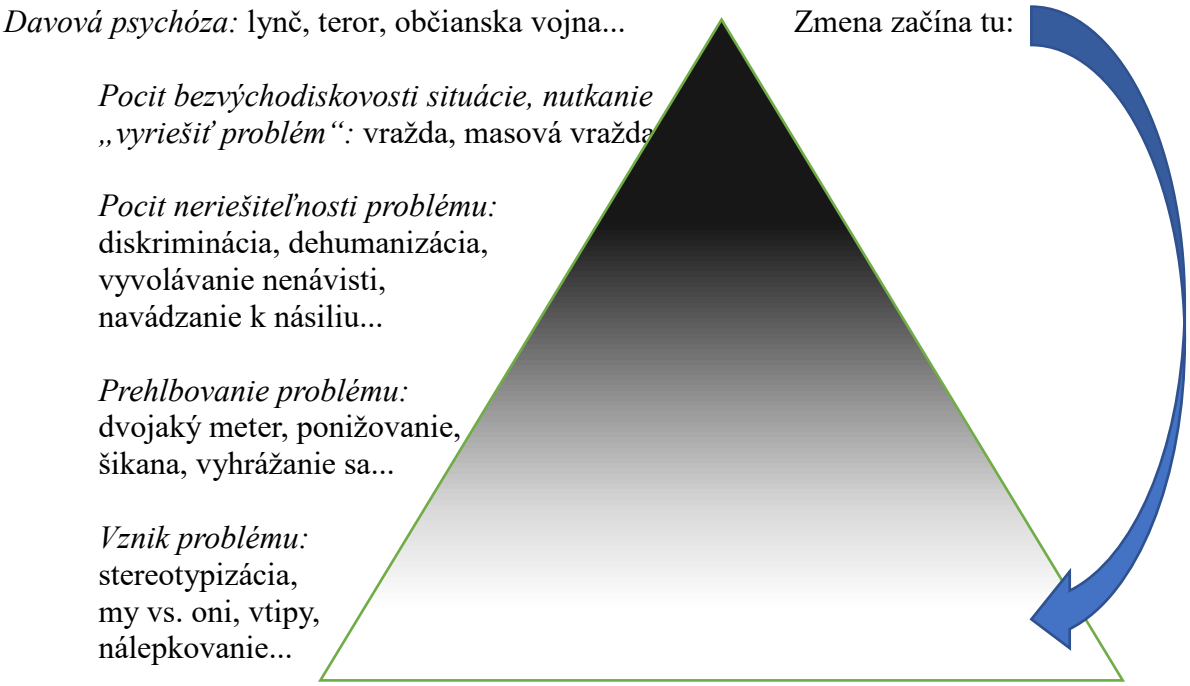
[16] Doplnil autor príspevku

[17] *The origins of hate* [on-line] [20. 05. 2024] Dostupné na: https://www.noassumption.co.uk/2023/04/07/the-origins-of-hate/

a *oni*. K tomu, aby bola jedna časť komunity presvedčená o tom, že *len* ona má pravdu postačuje, aby *ich* názor spĺňal logický princíp bezrozpornosti. Pritom nemusí ísť o intenciu aktéra dosiahnuť u niektorého psychicky labilného človeka až stupeň fyzického útoku, len o produkciu jednej z množstva možných informácií. „Kým informácia vzniká v prirodzených systémoch spontánne, v kultúrnych systémoch je informácia výsledkom ľudskej aktivity, bez ktorej by nemohla existovať...ľudská aktivita môže byť tak spontánna a neplánovaná, ako aj cieľavedomá či prísne predpísaná.“[18] Umelé rozdelenie komunity vzniká zjednodušovaním reality na základe konkrétnej stereotypizácie. Najčastejšie ide o prehlbovanie už existujúcich predsudkov a následné onálepkovanie jednej časti komunity. Živnou pôdou pre prehlbovanie rozporov je spoločenstvo bez obojstranne vyváženej, konštruktívnej a slobodnej diskusie s rešpektom k názorovému oponentovi. V spoločenstve bez takejto diskusie vzniká tzv. informačná bublina, uzatvorený kruh jednej mienky. Kritickou introspekciou môže každý na sebe pozorovať tendenciu mysle venovať pozornosť viac faktom, ktoré podporujú názor získaný predošlou aktivitou a všetky fakty, ktoré sa nehodia do získaného obrazu prehliadať. Na jednotlivých vyjadreniach viacerých osôb si všímame len to, čo podporuje náš názor a naopak u názorových oponentov venujeme pozornosť len tomu, čo nám zapadá do tvoriacej sa mozaiky o *nich*, čím sa postupne stále viac utvrdzujeme v predošlom názore. Významným nápomocným faktorom pre prijímanie názorov bez kritického posudzovania je prirodzená ľudská schopnosť a dokonca evolučná nevyhnutnosť prispôsobovania sa okoliu. Prispôsobovaniu sa okoliu znamená de facto to isté, ako prispôsobovanie sa väčšine, alebo brutálnejšie presadzovanému názoru. Navyše proces overovania faktov si vyžaduje určitý čas a istú námahu. Z toho dôvodu je ekonomická závislosť ďalším významným faktorom pre šírenie *jediného* obrazu o realite. Ďalším významným faktorom, na ktorý neustále upozorňoval napríklad Ghandi, je odvaha[19]. Kriticky pristupovať k prevládajúcemu názoru, vystúpiť aktívne proti prúdu akceptovaného väčšinou, si vyžaduje značnú mieru osobnej odvahy. Stále je tu naporúdzi racionalizácia zbabelého správania: čo ťa nepáli, nehas! V prípade, že jednotlivcovi vyhovuje niesť sa na vlne prevládajúcich informácií a emócií, začne aj on, najprv sa smiať spolu s ostatnými na ponižujúcich vtipoch a neskôr aj explicitne zosmiešňovať druhých, nálepkovať ich, či akceptovať dvojaký meter voči nim, čím sa nevedome dostáva na druhý stupeň pyramídy nenávisti. Pre dosiahnutie ďalších stupňov je potrebné spĺňať aj iné podmienky, ako sme uviedli v predchádzajúcej kapitole. Živnou pôdou pre fatálne rozhodnutie konkrétneho jedinca vziať

[18] Timko, 2009, s. 50.
[19] Fusero, 1990.

druhému život, je komunita plná predsudkov, jednostranného odsudzovania a nenávistí, v ktorej je neprípustná diskusia a slobodné vyjadrovanie iných ako väčšinových názorov.



Zdroj: *The origins of hate,*[20] preložil a upravil autor príspevku

5 Opatrenia na zabránenie útokom na školách

Aktívne prvky zvyšovania bezpečnosti na školách by sme mohli rozdeliť na technické opatrenia v škole a na mentálnu prípravu žiakov, študentov, pedagogických pracovníkov a ostatných zamestnancov školy. Medzi súbor technických opatrení patria:

- ✓ Osobná kontrola pri príchode žiakov a návštevníkov školy a ich batožiny
- ✓ Zákaz nosenia veľkých batožín do budovy školy
- ✓ Zavedenie informačných systémov na varovanie študentov a zamestnancov školy
- ✓ Zavedenie tiesňových tlačidiel v triedach
- ✓ Režimový vstup po budove na karty s rôznymi povoleniami
- ✓ Inštalácia bezpečnostných kamier vo všetkých priestoroch

[20] *The origins of hate* [on-line] [20. 05. 2024] Dostupné na: https://www.noassumption.co.uk/2023/04/07/the-origins-of-hate/

- ✓ Monitoring vonkajšej časti budovy a okolia
- ✓ Aktívne monitorovanie prístupu ku školám
- ✓ Zavedenie kamier, ktoré sú schopné detegovať niektoré špecifické zvuky
- ✓ Prijatie metodických postupov pre prípady útoku na školu.

Skúsenosti z posledných rokov ukazujú, že bariéry pri vstupe do budov (turnikety, bezpečnostné rámy, umelé predely a pod.) síce môžu nahradiť náklady na ľudskú silu kontrolujúcu vstupujúcich, ale pri vypuknutí paniky a hromadnom úteku z objektu môžu spôsobiť ublíženia na zdraví a životoch v tlačenici pri hlavnom vchode. Najznámejším únikovým východom je vždy hlavný vstup do objektu. Človeka, viac či menej skúseného, je vždy ťažšie obísť. Potenciálny páchateľ vie predvídať „správanie stroja“ na 100%, navyše, bezpečnostný rám si nikdy nevšimne nezvyčajnú nervozitu osoby, ktorá niečo tají.

Pri implementácii technických opatrení si musíme byť vedomí, že bezpečnosť objektu sa nestupňuje priamo úmerne s *množstvom* zavedených opatrení, ale len s kvalitou plnenia funkcií jednotlivých prvkov. „Stupeň jeho bezpečnosti je daný *najnižšou* úrovňou bezpečnosti časti (prvku) objektu.“[21]

Pod mentálnu prípravu žiakov, študentov, pedagogických pracovníkov a ostatných zamestnancov školy by sme mohli zaradiť:

- ✓ Preventívne vzdelávacie semináre
- ✓ Posilnenie vzťahov medzi žiakmi a učiteľmi
- ✓ Zapojenie rodičov do prevencie násilia
- ✓ Organizovanie seminárov a workshopov pre rodičov
- ✓ Podpora školskej komunity a solidarita medzi žiakmi
- ✓ Informovanie o príznakoch možných páchateľov
- ✓ Edukácia o používaní sociálnych médií a internetu
- ✓ Varovanie pred internetovými hrozbami a kyber-šikanovaním
- ✓ Posilnenie mentálnej odolnosti u žiakov
- ✓ Nahlásenie podozrivých správ a vyhrážok orgánom činným v trestnom konaní
- ✓ Okamžité informovanie polície o konfliktoch v škole
- ✓ Plnenie povinných aktivít na prevenciu násilných činov
- ✓ Spolupráca s psychológmi a odborníkmi na deeskaláciu problémových situácií

[21] Ivančík, 2022, s. 185.

- ✓ Psychologický výcvik: ako sa správať pri eliminácii negatívnych následkov
- ✓ Fyzická príprava študentov: ovládanie prostriedkov sebaobrany
- ✓ Tréning pre konanie v incidentoch aktívneho strelca.

Ďalej je to oboznámenie sa s *Cooperovou stupnicou ostražitosti*: najdôležitejšie pre prežitie v situáciách ohrozenia života nie je ani tak zbraň alebo bojové schopnosti, ale nastavenie mysle.

- ✓ 1. stupeň (biela): nevšímavosť, pozeranie do mobilu, je vhodná len v bezpečí domova
- ✓ 2. stupeň (žltá): ostražitosť, všímame si únikové východy, je vhodná vždy mimo domu
- ✓ 3. stupeň (oranžová): v mysli si plánujeme scenár úteku alebo útoku. Tento stupeň ostražitosti je potrebný vtedy, ak už vidíme konkrétne ohrozenie, napríklad stupňujúci sa konflikt v blízkosti.
- ✓ 4. stupeň (červená): verbálna či fyzická sebaobrana, potrebná ak už dôjde k útoku
- ✓ 5. stupeň (čierna): tzv. *zmrznutie* pri tepe nad 175 úderov/min., môže nastať v prípade, ak zažijeme nečakaný útok v 1. stupni ostaržitosti, alebo ak sme paranoidní a permanentne máme zvýšený tep, ktorý sa nám v prípade ozajstného útoku rýchlo vystupňuje.

Najrozšírenejším prvkom mentálnej prípravy je oboznámenie sa s *metodickým plánom prežitia,* skrátene, *USB*:

- ✓ *Uteč*: vhodné vtedy, ak vieme, kam máme utekať do bezpečia. Najlepšie ak sme napríklad na prízemí. Utekáme nenápadne, bez vecí a okamžite voláme 112 resp. 158.
- ✓ *Skry sa*: potrebné vtedy, ak nemáme možnosť ujsť. Nájdeme si relatívne bezpečný priestor, ktorý má plné dvere. Dvere je potrebné zabarikádovať a tváriť sa, že miestnosť je prázdna. Vypnúť mobily, zatemniť okná. (Pozor na únik do pasce. V minulosti bolo veľa obetí na WC.) *Pravidlo prvých zamknutých dverí*: Od momentu, keď prvýkrát útočník vystrelí uvedomuje si, že mu do príchodu bezpečnostných zložiek zostáva v priemere 15 minút. Ak je jeho cieľom pozabíjať čo najviac ľudí, nebude sa dobíjať do zamknutých dverí, ale bude hľadať nechránené obete.
- ✓ *Bojuj*: nutné len vtedy, ak už máme iba dve možnosti: buď neurobíme nič a zomrieme, alebo budeme bojovať o holý život. V takom prípade útočíme na citlivé miesta páchateľa. Použijeme akúkoľvek improvizovanú zbraň napr. hasiaci prístroj. Ak sme

viacerí: jeden natiahne útočníkovi bundu na hlavu a ostatní sa na neho vrhnú naraz ako mravce.

Počas zásahu bezpečnostných zložiek je potrebné dávať si pozor, aby sme sa nestali ich nechcenou obeťou, napr. ak poslúchneme výzvu na zdvihnite rúk, nedržme v nich predmet z diaľky pripomínajúci nejakú zbraň. Je potrebné mať prázdne ruky a riadiť sa ich pokynmi.

Záver

Zraniteľnosť ľudských telesných schránok sa zneužíva na „vyriešenie problémov“ už od prehistorických čias. Dejiny ľudstva bežne ponímame ako striedanie panovníkov a panovníčok alebo ako vznik či zánik jednotlivých politických útvarov. Štúdium histórie ide o dve či tri úrovne hlbšie do poznania jednotlivých dejinných udalostí a odhaľuje tak množstvo dynastických vrážd a nepredstaviteľné utrpenie miliónov vojakov a civilistov počas vojen o územia a zdroje. Od doby písomného zaznamenávania dejín vypuklo cca. 14 500 vojen. Zomrelo v nich viac ľudí, ako obývalo celú planétu v dobe, keď žil vojenský historik, ktorý túto štatistiku vypracoval. História ľudstva je históriou permanentného vojenského konfliktu. Mier je len prestávkou medzi nimi.[22]

Žiaľ do dnešného dňa sa situácia nezlepšila. Svedčia o tom nie len prebiehajúce vojenské konflikty, ale aj vraždy nepohodlných ľudí. Stačí si zadať do internetového vyhľadávača napríklad: *vražda politika* alebo *vražda whistleblowera.* Samozrejme do sprístupnenia archívov po 70 rokoch ide väčšinou o neoficiálne informácie. Avšak, úplne stačí vziať do úvahy len tie oficiálne potvrdené vraždy osôb, ktoré niekomu nevyhovovali, aby bolo každému jasné, že k primitívnemu receptu na „odstránenie problému“ sa uchyľuje dodnes.

Útechu z uvedených hrôz nám poskytuje aspoň filozofia, ktorá ponúka množstvo odporúčaní a viac či menej utopických projektov. Kant v roku 1795 napísal „...mier nie je možné dosiahnuť a natrvalo udržať bez vzájomnej zmluvy medzi národmi... musí byť založená *aliancia* osobitného druhu, ktorú by sme mohli nazvať *Alianciou za mier*...Takejto aliancii nepôjde o žiadne dosahovanie nejakej štátnej moci, ale len o získanie a zabezpečenie *slobody* pre všetky štáty v aliancii, ktoré nesmú byť pritom podrobované zákonom alebo inému donúteniu.“[23] Avšak ani ďalšie desiatky miliónov mŕtvych a dve svetové vojny od napísania

[22] Dangl, 2009, s. 7.
[23] Kant, 1795, [pg 035]. [on-line] [20. 05. 2024] Dostupné na: https://www.gutenberg.org/files/46873/46873-h/46873-h.htm Kurzívou zvýraznil autor knihy, podčiarkol autor príspevku.

tejto *jednoduchej* požiadavky neprimäli ľudstvo k hľadaniu riešenia na základe vzájomnej úcty a rešpektu medzi ľuďmi, skôr sa snažíme „vyriešiť problémy“ súčasnosti realizáciou scenárov dystópií, väčšou kontrolu spoločnosti.

Nezodpovedanou otázkou ostáva: ako dosiahnuť, aby sa celé ľudstvo zlepšilo do takej miery, aby mohlo realizovať riešenia, na ktoré už dávno prišlo? Zrejme platí, že každý z nás môže zmeniť len seba samého a dúfať, že naše správanie následne ovplyvní druhých. Dokonca by sme mohli ísť ešte o krok ďalej a povedať, že každý z nás je povinný na sebe pracovať, kultivovať svoju osobnosť, v opačnom prípade neprispieva k zlepšeniu ľudstva, ale naopak k jeho zhoršeniu, k rozsievaniu *pyramíd nenávisti* a následne smrti po celej Zemi. Do čias, kým sa ľudstvo dostatočne neemancipuje od svojich zvieracích predkov, bude potrebné sa veľmi vážne zaoberať bezpečnosťou svojou i druhých. Útoky na školách sú dnes aktuálnejšie ako kedykoľvek predtým a sú reálnou každodennou hrozbou, pretože ak „človek chce niečo podobné spáchať, cestu ako na to, si už nájde.“[24]

Zoznam použitej literatúry

DANGL, Vojtech, 2009. *Pod zástavu cisára a kráľa*. Bratislava: Historický ústav SAV, 2009.

ĎURICOVÁ, L., M. HROMADA a J. MRÁZEK. Softwerový nástroj pre hodnotenie objektov mäkkých cieľov. In: *22. medzinárodná vedecká konferencia: Riešenie krízových situácií v špecifickom prostredí*. Žilina: Fakulta bezpečnostného inžinierstva Žilinskej univerzity v Žiline, 2017, s. 465–472.

FUSERO, Clemente, 1990. *Gándhí*. Bratislava: Obzor, 1990.

HOFREITER, Ladislav, 2015. Kultúra bezpečnosti a riadenie bezpečnosti. In: *Krízový manažment.* 2/2015. ISSN: 2730-0544 (online)

IBL, Petr, 2007, Globální terorizmus a jeho poznání. In: *Karlovarská právni revue.* roč. 3, č. 2, 2007.

IVANČÍK, Radoslav, 2022. *Bezpečnosť.* Plzeň: Aleš Čeněk, 2022.

IVANČÍK, R. a Ľ. BARIČIČOVÁ, 2020. Gnozeologické pramene skúmania bezpečnosti v 21. storočí In: *Policajná teória a prax*. Bratislava: APZ, 2-2020. ISSN 1335-1370.

[24] *Odborník na extrémizmus o útoku v Prahe* [on-line] [22. 12. 2023] Dostupné na: https://www.postoj.sk/144017/neslo-o-terorizmus-ale-demonstrativnu-samovrazdu-s-cielom-co-najviac-ublizit

KANT, Immanuel, 1795. *Zum ewigen Frieden*. Königsberg: bey Friedrich Nicolovius, 1795. [on-line] [20. 05. 2024] Dostupné na: *https://www.gutenberg.org/files/46873/46873-h/46873-h.htm*

KUCHTOVÁ, Jana, 2020. Účinky policajných telových kamier. In: *Moderné technológie v páchaní, odhaľovaní, dokumentovaní, dokazovaní a prevencii trestnej činnosti* 2020. Bratislava: Akadémia Policajného zboru v Bratislave, s. 172 – 182. ISBN 978-80-8054-856-8

MAREŠ, Miroslav, 2005. *Terorizmus v ČR*. Brno: Centrum strategických studií, 2005.

MURDZA, Karol, 2017. Rozumná bezpečnosť a jej spoločenské garancie. In: *Bezpečné Slovensko a Európska únia* 2017. Košice: VŠBM v Košiciach, s. 362-369. ISBN 978-80-8185-025-7.

TIMKO, Marek,2009. *Evolúcia – informácia – skutočnosť.* Brno: Masarykova univerzita, Diz. p., 2009.

Zákon č. 110/2004 Z. z. o fungovaní Bezpečnostnej rady Slovenskej republiky

Internetové zdroje:

Odborník na extrémizmus o útoku v Prahe [on-line] [22. 12. 2023] Dostupné na: https://www.postoj.sk/144017/neslo-o-terorizmus-ale-demonstrativnu-samovrazdu-s-cielom-co-najviac-ublizit

Pri streľbe na pražskej univerzite zomrelo 14 ľudí, útočník zabíjal aj predtým [on-line] [21. 12. 2023] Dostupné na: https://svet.sme.sk/c/23259930/praha-strelba-cesko.html

Rezorty školstva a vnútra spoločne posilňujú bezpečnosť na školách [on-line] [09. 04. 2024] Dostupné na: https://www.minedu.sk/rezorty-skolstva-a-vnutra-spolocne-posilnuju-bezpecnost-na-skolach/

School Shooters: Understanding their paths to violence is key to prevention. [on-line] [29. 05. 2022] Dostupné na: https://www.npr.org/sections/health-shots/2019/02/10/690372199/school-shooters-whats-their-path-to-violence?t=1591878658203

Slovník súčasného slovenského jazyka. [on-line] [20. 05. 2024] Dostupné na: https://www.juls.savba.sk/pub_sssj.html

Stopping Violence in Schools: A Guide for Teachers [on-line] [2009] Dostupné na: https://unesdoc.unesco.org/ark:/48223/pf0000184162

The origins of hate [on-line] [20. 05. 2024] Dostupné na: https://www.noassumption.co.uk/2023/04/07/the-origins-of-hate/

Violence in the lives of children and adolescents. [on-line] [20. 05. 2024] Dostupné na: https://www.unicef.org/publications/files/Violence_in_the_lives_of_children_and_adolescents.pdf

Summary

The purpose of the article is to contribute to the knowledge of security management tools used to minimize the risk of committing attacks at schools. The author proceeds from the individual concepts, procedures and advice of security management, through the identification of the specifics of attacks on schools to practical recommendations and advice, for knowledge and application in practice in order to survive yourself and your classmates during an attack on a school. In the end, the author reflects on the presence of violence in human society.

Keywords: School attacks, security management, soft targets, terrorism.

Kontaktné údaje

mjr. Mgr. Martin Kaščák, PhD.
odborný asistent Katedry informatiky a manažmentu
Akadémie Policajného zboru v Bratislave
Sklabinská 1
tel. číslo - 57063
e-mail: martin.kascak@akademiapz.sk

Recenzenti:
prof. RNDr. Michal Greguš, CSc.
doc. Ing. Václav Friedrich, Ph.D.

Podobnosť sociálnych médií z hľadiska metrík šírenia dezinformácií

Antonín Korauš, Lucia Kurilovská, Beáta Stehlíková, Kristián Újváry

Abstrakt: Cieľom príspevku je analyzovať sociálne siete z hľadiska šírenia dezinformácií Na základe analýzy biplotu sme identifikovali platformy s významným vplyvom. Twitter sa ukázal mať najvyššiu objaviteľnosť, zatiaľ čo Instagram dosiahol najvyššiu hodnotu relatívneho pomeru počtu sledovateľov, čo svedčí o vysokej angažovanosti sledovateľov. LinkedIn a YouTube vykazujú podobné hodnoty ukazovateľov. Ostatné platformy sa javia ako izolované a odlišujú sa vo svojich charakteristikách. Zistenia z tejto štúdie poskytujú základ pre formuláciu politík a regulácií s cieľom obmedziť šírenie dezinformácií a zvýšiť dôveryhodnosť sociálnych médií.

Kľúčové slová: sociálne médiá, dezinformácie, analýza hlavných komponentov

Abstract: The aim of the paper is to analyse social networks from the point of view of the spread of disinformation. Based on biplot analysis, we identified platforms with significant influence. Twitter was found to have the highest discoverability, while Instagram achieved the highest relative follower ratio, indicating high follower engagement. LinkedIn and YouTube show similar indicator values. Other platforms appear to be isolated and vary in their characteristics. Findings from this study provide a basis for formulating policies and regulations to limit the spread of misinformation and increase the credibility of social media.

Key words: social media, disinformation, principal component analysis

Úvod

Masívne digitálne dezinformácie predstavujú vážnu hybridnú hrozbu. Vplyv dezinformácií môže byť deštruktívny na rôzne aspekty nášho života, od verejného zdravia a politiky až po klimatické zmeny a ekonomické problémy [1]. Sociálne siete sú platformy, ktoré umožňujú používateľom komunikovať, zdieľať obsah a budovať virtuálne komunity na základe spoločných záujmov a vzťahov. Ide o jeden z najrozšírenejších a najpopulárnejších spôsobov komunikácie a interakcie v digitálnom svete. V zahraničnej literatúre sú dezinformácie (misinformation) definované ako nepravdivé informácie zdieľané bez úmyslu poškodiť, zatiaľ čo dezinformácie (disinformation) sú definované ako nepravdivé informácie zdieľané s úmyslom poškodiť. Nie je možné určiť jasnú hranicu medzi týmito dvoma, pretože obe obsahujú nepravdivé informácie; jediný rozdiel je v úmysle.

[1] CHEN, Sijing; XIAO, Lu; KUMAR, Akit. Spread of misinformation on social media: What contributes to it and how to combat it. *Computers in Human Behavior*, 2023, 141: 107643.

Psychológiou dezinformácií sa zaoberali viacerí autori (Roozenbeek a Van de Linden[2] Pennycook a Rand[3], Ecker et al.[4], Van de Linden[5]). Modelom sociálnej difúzie dezinformácií na pochopenie ľudského informačného správania sa zaoberali Karlova a Fisher[6].

Na boj proti šíreniu dezinformácií na sociálnych médiách boli navrhnuté rôzne prístupy so zameraním na štyri základné komponenty komunikačného procesu[7]: zdroj/odosielateľ, správu, kontext/kanál a príjemcu. Stratégie boja proti dezinformáciám[1] môžeme členiť z hľadiska piatich hľadísk: správa, zdroj, sieť, politika a vzdelávanie. Cieľom práce Aimeur et al.[8] je poskytnúť komplexný a systematický prehľad výskumu falošných správ, ako aj zásadný prehľad existujúcich prístupov používaných na odhaľovanie a zabránenie šíreniu falošných správ. Existuje viacero prístupov k detekcii dezinformácií[9]. Na internete sú k dispozícii rôzne online služby na overovanie faktov, ako napríklad FactCheck.org, PoltiFact.com, Classify.news, FactCheck.org, Hoaxy.iuni.iu.edu, Factmata.com a mnohé ďalšie. Autori Kondamudi et al[9]. uvádzajú rozsiahle vysvetlenia rôznych techník strojového učenia a hlbokého učenia na odhaľovanie falošných správ. Jednou zo základných súčastí na vytvorenie úspešného modelu učenia pod dohľadom je súbor údajov o kvalite.

Štúdia Hilary a Dumebi[10], skúma sociálne médiá ako nástroj na dezinformácie. Prehľad v článku Caleda a Silvu[11] pojednáva o dynamických mechanizmoch vytvárania a šírenia dezinformácií používaných v sociálnych sieťach. Falošné správy sa šíria rýchlo a ľahko

[2] ROOZENBEEK, Jon; VAN DER LINDEN, Sander. *The Psychology of Misinformation*. Cambridge University Press, 2024.
[3] PENNYCOOK, Gordon; RAND, David G. The psychology of fake news. *Trends in cognitive sciences*, 2021, 25.5: 388-402.
[4] ECKER, U. K., LEWANDOWSKY, S., COOK, J., SCHMID, P., FAZIO, L. K., BRASHIER, N., ... & AMAZEEN, M. A. (2022). The psychological drivers of misinformation belief and its resistance to correction. *Nature Reviews Psychology*, *1*(1), 13-29.
[5] VAN DER LINDEN, Sander. Misinformation: susceptibility, spread, and interventions to immunize the public. *Nature medicine*, 2022, 28.3: 460-467.
6 KARLOVA, Natascha A.; FISHER, Karen E. A social diffusion model of misinformation and, disinformation for understanding human information behaviour. Information research, vol 18, no 1, 2013. dokument 573. [Dostupné na http://InformationR.net/ir/18-1/paper573.html]
[7] BERLO, David K. The process of communication: An introduction to theory and practice. Holt Rinehart and Winston. *Inc., New York*, 1960, 960.
[8] AÏMEUR, Esma; AMRI, Sabrine; BRASSARD, Gilles. Fake news, disinformation and misinformation in social media: a review. *Social Network Analysis and Mining*, 2023, 13.1: 30.
[9] KONDAMUDI, Medeswara Rao, et al. A comprehensive survey of fake news in social networks: Attributes, features, and detection approaches. *Journal of King Saud University-Computer and Information Sciences*, 2023, 35.6: 101571.
[10] HILARY, Ibegbulem Obioma; DUMEBI, Olannye-Okonofua. Social media as a tool for misinformation and disinformation management. *Linguistics and Culture Review*, 2021, 5.S1: 496-505.
[11] CALED, Danielle; SILVA, Mário J. Digital media and misinformation: An outlook on multidisciplinary strategies against manipulation. *Journal of Computational Social Science*, 2022, 5.1: 123-159.

na platformách sociálnych médií[12]. Platformy ako Facebook, Twitter a YouTube poskytujú úrodnú pôdu na vytváranie a šírenie dezinformácií. López et al[13] analyzuje naratív dezinformácií šírených prostredníctvom sociálnej siete TikTok. Hindman a Barash[14] študovali pomocou nástrojov a metód mapovania od spoločnosti Graphika, spravodajskej spoločnosti pre sociálne médiá, viac ako 10 miliónov tweetov zo 700 000 účtov na Twitteri, ktoré boli prepojené s viac ako 600 falošnými a konšpiračnými správami. Autori Bessi et al.[15] sa vo svojom článku zameriavajú na talianskych používateľov Facebooku. Pomocou dôkladnej kvantitatívnej analýzy poskytli dôležité poznatky o anatómii systému, cez ktorý sa môžu šíriť dezinformácie. Dezinformáciami na Facebooku sa zaoberali aj Zollo a Quattrociocchi.[16]

Príspevok Helberger[17] kriticky hodnotí prebiehajúce iniciatívy v Európe s cieľom zvýšiť spoločenskú zodpovednosť sociálnych médií. S rýchlym rastom dezinformácií boli podniknuté dva hlavné kroky v boji proti tomuto fenoménu v online prostredí – prvý na globálnej úrovni a druhý na úrovni Európskej únie. Prvým krokom je Spoločná deklarácia o slobode prejavu a „falošných správach“, dezinformáciách a propagande[18] je snahou identifikovať a riešiť rastúce problémy týkajúce sa dezinformácií. Druhým je Kódex praktík v oblasti dezinformácií[19], uvádzajú Kobernjuk a Kasper[20].

Kľúčový nástroj politiky Európskej únie proti dezinformáciám – Kódex praktík v oblasti dezinformácií – sa snaží o prijatie štrukturálnych indikátorov na skúmanie fenoménu dezinformácií a meranie účinnosti Kódexu pri jeho potláčaní v jednotlivých členských štátoch EÚ, ako aj v EÚ ako celku[21]. Kódex praktík v oblasti dezinformácií stanovuje zásady a záväzky pre online platformy a reklamný sektor s cieľom bojovať proti šíreniu dezinformácií online

[12] ZANNETTOU, Savvas, et al. The web of false information: Rumors, fake news, hoaxes, clickbait, and various other shenanigans. *Journal of Data and Information Quality (JDIQ)*, 2019, 11.3: 1-37.
[13] ALONSO LÓPEZ, Nadia, et al. Beyond challenges and viral dance moves: TikTok as a vehicle for disinformation and fact-checking in Spain, Portugal, Brazil, and the USA. 2021.
[14] HINDMAN, Matthew; BARASH, Vlad. Disinformation,'fake news' and influence campaigns on Twitter. 2018.
[15] BESSI, Alessandro, et al. Homophily and polarization in the age of misinformation. *The European physical journal special topics*, 2016, 225: 2047-2059.
[16] ZOLLO, Fabiana; QUATTROCIOCCHI, Walter. Misinformation spreading on Facebook. *Complex spreading phenomena in social systems: Influence and contagion in real-world social networks*, 2018, 177-196.
[17] Helberger, Natali. (2020). Politická sila platforiem: Ako súčasné pokusy o reguláciu dezinformácií zosilňujú názorovú silu. Digitálna žurnalistika , 8 (6), 842–854. https://doi.org/10.1080/21670811.2020.1773888
[18] OSCE: Joint Declaration on Freedom of Expression and “Fake News”, Disinformation and Propaganda. 2017 Dostupné na https://www.osce.org/fom/302796
[19] Európska komisia: Code of Practice on Disinformation 2018. dostupné na https://ec.europa.eu/newsroom/dae/redirection/document/87534
[20] KOBERNJUK, Anna; KASPER, Agnes. Normativity in the EU’s Approach towards Disinformation. *TalTech Journal of European Studies*, 2021, 11.1: 170-202.
[21] NENADIC, Iva; BROGI, Elda; BLEYER-SIMON, Konrad. Structural indicators to assess effectiveness of the EU’s Code of Practice on Disinformation. Working Paper, EUI, RSC, Working Paper, 2023/34, Centre for Media Pluralism and Media Freedom, 2023.

v EÚ. Jedná sa o prvý samoregulačný nástroj na svete na boj proti dezinformáciám. V roku 2020 Európska komisia predstavila aktualizovanú verziu Code of Practice on Disinformation, ktorá obsahuje nové opatrenia a záväzky pre online platformy. V roku 2022 bol pre predložený Posilnený kódex postupov v oblasti dezinformácií.[22] Súčasní signatári zahŕňajú hlavné online platformy aktívne v EÚ, ako aj obchodné združenia a príslušných hráčov v online a reklamných ekosystémoch. Sú to: Google, Facebook, Twitter, Microsoft, TikTok, Mozilla, DOT Europe (bývalá EDiMA), Svetová federácia inzerentov (WFA) a jej belgický náprotivok, Únia belgických inzerentov (UBA); Európska asociácia komunikačných agentúr (EACA) a jej národní členovia z Francúzska, Poľska a Českej republiky – Association des Agences Conseils en Communication (AACC), Stowarzyszenie Komunikacji Marketingowej/Ad Artis Art Foundation (SAR) a Asociace Komunikacnich Agentur (AKA) – Interactive Advertising Bureau (IAB Europe), Kreativitet & Kommunikation a Goldbach Audience (Švajčiarsko) AG.

Dňa 9. februára 2023 signatári Kódexu postupov v oblasti dezinformácií poskytli svoje prvé základné správy. Druhý súbor správ o implementácii kódexu postupov bol zverejnený 26.septembra 2023. Nové správy sa už riadili harmonizovaným vzorom podávania správ - 111 prvkov kvalitatívneho podávania správ a 42 kvantitatívnych ukazovateľov úrovne služieb) v rámci kapitol kódexu. 26.marca 2024 signatári Kódexu praktík v oblasti dezinformácií, vrátane hlavných online platforiem. zverejnili tretiu sériu správ.

Materiál a metódy

Komparatívna štúdia TrustLab[23] je prvá empirická aplikácia Kódexu postupov proti šíreniu dezinformácií. Táto štúdia si dala za cieľ zhodnotiť prevalenciu a zdroje dezinformácií na šiestich hlavných platformách sociálnych médií (Facebook, Instagram, LinkedIn, TikTok, Twitter (teraz známy ako X) a YouTube) v troch krajinách Poľsko, Slovensko a Španielsko.

Proces zberu údajov pozostával zo zostavenia najnovších populárnych nepravdivých/dezinformačných tvrdení, extrahovania kľúčových slov z nich a následného vzorkovania obsahu a účtov pomocou týchto kľúčových slov. Analytici, ktorí vykonali označovanie dezinformačného obsahu, vykonali aj označovanie dezinformačných aktérov. Zdrojom údajov bolo 4460 účtov. Podrobná metodika je popásaná v štúdii TrustLab[23]. V našom príspevku používame metriky a zistené hodnoty zo štúdie TrustLab[23].

[22] Európska komisia: Strengthened Code of Practice Disinformation. 2022 dostupné na https://ec.europa.eu/newsroom/dae/redirection/document/87585
[23] https://www.trustlab.com/codeofpractice-disinformation

Objaviteľnosť (discoverability) **dezinformácií** je ukazovateľ, ktorý poskytuje informáciu o tom, ako ľahko platforma zobrazuje užívateľovi dezinformačný obsah pri vyhľadávaní citlivých tém. Objaviteľnosť predstavuje podiel výsledkov vyhľadávania, ktoré majú dezinformačný obsah (N_{dezinf}a celkového počtu príspevkov (N) vo výsledkoch vyhľadávania.

$$\text{objaviteľnosť} = \frac{\text{N}_{\text{dezinf}}}{\text{N}}$$

Objaviteľnosť ukazuje, ako ľahko platforma sociálnych médií zobrazuje užívateľovi dezinformačný obsah pri vyhľadávaní citlivých tém. Vyššia objaviteľnosť znamená, že používateľ môže ľahšie nájsť dezinformačný obsah na platforme, keď vyhľadáva kľúčové slová spojené s populárnymi dezinformačnými témami.

Reakcie, komentáre a zdieľania predstavujú určitý druh aktívnej interakcie používateľov. Zobrazenia sa nepovažujú za aktívnu interakciu. Všetky tri druhy aktívnej interakcie sú na Facebooku, LinkedIn, TikTok, Twitteri. Reakcie a komentáre sú na YouTube. Na Instagrame sú možné iba reakcie. **Relatívny pomer angažovanosti príspevkov** (Relative Post Engagement Ratio) je ďalšia metrika. Relatívna angažovanosť príspevkov je operacionalizovaná ako jednoduchý pomer priemernej aktívnej angažovanosti dezinformačných príspevkov a priemernej aktívnej angažovanosti všetkých príspevkov.

$$\text{relatívny pomer angažovanosti} = \frac{\text{priemerná angažovanosť dezinformačných príspevkov}}{\text{priemerná angažovanosť nedezinformačných príspevkov}}$$

Vyššia hodnota relatívneho pomeru angažovanosti znamená, že príspevky s dezinformáciami majú vyššiu mieru angažovanosti než príspevky s faktickými informáciami.

Ďalšou metrikou je **podiel účtov dezinformačných aktérov** (Ratio of disinformation actors). Počet účtov dezinformačných aktérov sa vydelil celkovým počtom účtov vzorkovaných na platforme

$$\text{podiel účtov dezinformačných aktérov} = \frac{\text{počet účtov dezinformačných aktérov}}{\text{celkový počet účtov}}$$

Podiel účtov dezinformačných aktérov poskytuje informáciu o tom, aký je rozsah a závažnosť šírenia dezinformácií na danej platforme. Ak je vysoký, používatelia môžu byť náchylnejší na pochybnosti o dôveryhodnosti informácií prezentovaných na tejto platforme.

Pojem sledovateľ (follower) je základnou jednotkou na meranie popularity a dosahu užívateľského účtu na sociálnych médiách. Ďalšia informácia, ktoré môže byť dôležitá pre pochopenie správania dezinformačných aktérov a spôsobu, akým sa snažia šíriť svoj obsah a ovplyvňovať verejnú mienku je **relatívny pomer počtu sledovateľov** (Relative follower ratio) definovaný ako podiel priemerného počtu sledovateľov dezinformačných aktérov a priemerného počtu sledovateľov nedezinformačných aktérov

$$\text{relatívny pomer počtu sledovateľov} = \frac{\text{priemerný počet sledovateľov dezinformačných aktérov}}{\text{priemerný počet sledovateľov nedezinformačných aktérov}}.$$

PCA (Principal Component Analysis) je štatistická metóda používaná na redukciu dimenzionality dát[24]. PCA predpokladá, že dáta sú lineárne nezávislé a majú normálnu distribúciu. Ak tieto predpoklady neplatia, môže to ovplyvniť výsledky analýzy. Biplot poskytuje užitočný nástroj na vizualizáciu vzťahov medzi premennými a jednotkami v priestore hlavných komponentov.

Normalitu sme testovali pomocou Andersonovho – Darlingovho testu s korekciou na malý rozsah údajov[25].

Všetky výpočty boli realizované vo výpočtovom prostredí R.

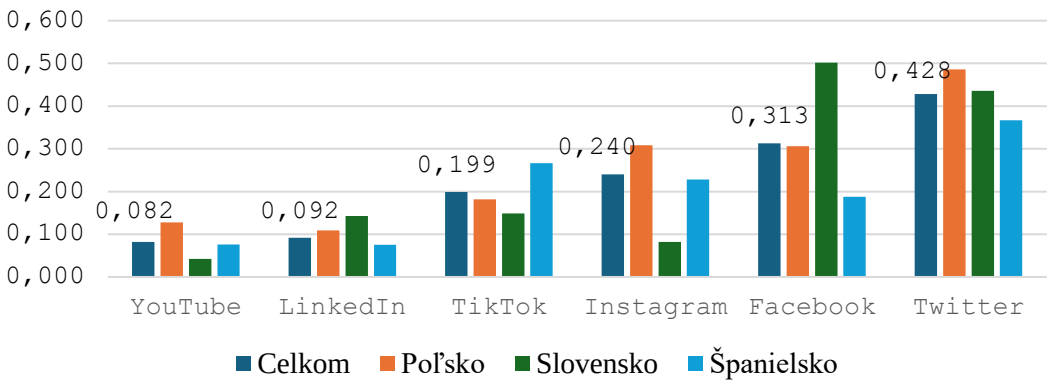
Výsledky a diskusia

Platforma obvykle vykonáva filtráciu alebo odfiltrovanie dezinformačného obsahu pomocou rôznych mechanizmov a technológií. Platformy majú zvyčajne sady pravidiel a politík, ktoré určujú, čo je na platforme povolené a čo nie je. Platformy často používajú algoritmy a technológie strojového učenia na identifikáciu nepravdivých alebo manipulatívnych obsahov. Niekedy platformy zamestnávajú ľudí, ktorí vykonávajú ručnú kontrolu obsahu a rozhodujú o tom, či má byť určitý obsah odstránený alebo označený ako dezinformácia. Užívatelia často môžu označiť obsah ako dezinformácie alebo ho nahlásiť platforme, čo môže viesť k ďalšiemu skúmaniu a prípadnému odstráneniu alebo označeniu obsahu.

Dezinformačný obsah môže používateľ najľahšie nájsť na Twiteri, zatiaľ čo objaviteľnosť dezinformácií je najnižšia na YouTube. Vysoká objaviteľnosť dezinformácií na Twitteri je tiež v Poľsku a Španielsku. Na Slovensku môže používateľ najľahšie nájsť na

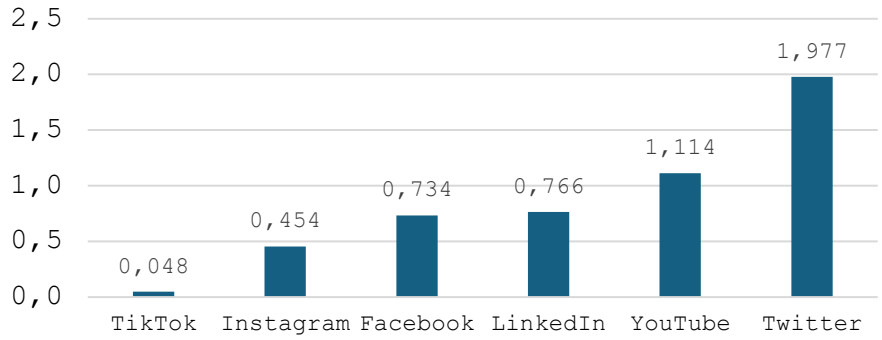
[24] MISHRA, Sidharth Prasad, et al. Multivariate statistical data analysis-principal component analysis (PCA). *International Journal of Livestock Research*, 2017, 7.5: 60-78.
[25] ROMEU, Jorge L. Anderson-Darling: a goodness of fit test for small samples assumptions. *RAC START*, 2003.

Facebook. Twitter je na druhom mieste. Poradie objaviteľnosti dezinformácií sa v jednotlivých štátoch líšia.



Graf 1 Objaviteľnosť dezinformácií
Zdroj: vlastné spracovanie údajov TrustLab

Politická situácia v jednotlivých štátoch môže ovplyvniť šírenie dezinformácií. Napríklad štáty s väčšou mierou politickej polarizácie môžu byť náchylnejšie k dezinformačným kampaniam. Štáty s väčším vplyvom dezinformácií môžu mať vyššiu objevitelnost dezinformací. Efektivita a iniciatíva zameraná na boj proti dezinformáciám sa môže líšiť medzi jednotlivými štátmi. Štáty s účinnejšími opatreniami môžu mať nižšiu objaviteľnosť dezinformácií.

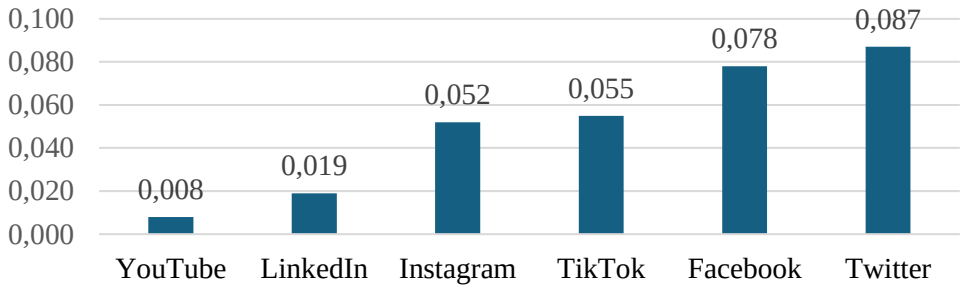


Graf 2 Relatívny pomer angažovanosti
Zdroj: vlastné spracovanie údajov TrustLab

YouTube a Twitter sú platformami, kde sa dezinformáciám dostalo viac aktívnych interakcií ako nedezinformačným. Relatívny pomer angažovanosti môže byť rozdielny medzi rôznymi sociálnymi médiami. Rôzne sociálne médiá sú vhodné pre rôzne typy obsahu. Niektoré platformy, ako napríklad Instagram, sú často zamerané na vizuálny obsah, zatiaľ čo Twitter je viac zameraný na textové správy. Typ obsahu prezentovaný na platforme môže

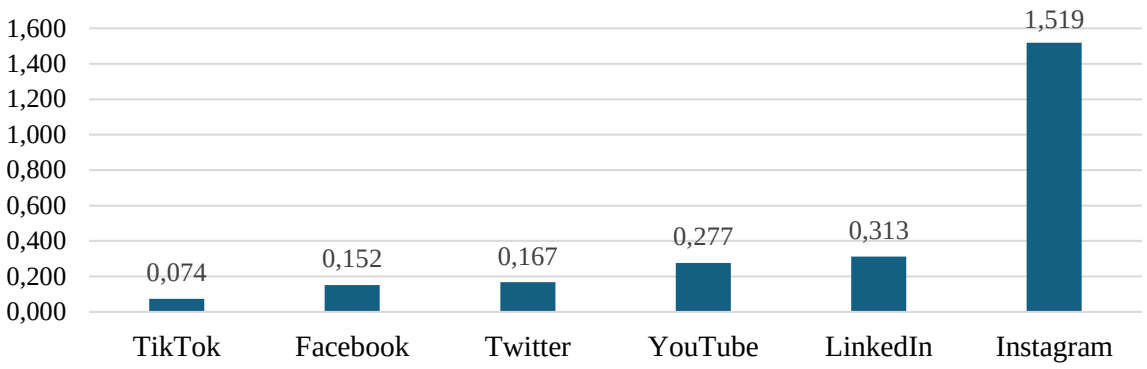
ovplyvniť spôsob, ako používatelia interagujú s obsahom a mierou ich angažovanosti. Tiež algoritmy a mechanizmy zobrazenia obsahu môžu ovplyvniť, aký obsah je prezentovaný a akým spôsobom používatelia interagujú. Používatelia rôznych sociálnych médií môžu mať odlišné demografické a sociálne charakteristiky. Toto môže ovplyvniť ich správanie a interakciu. Napríklad na platformách ako Twitter môže byť diskusia a interakcia s obsahom častejšia než na iných platformách.

Najvyšší podiel účtov dezinformačných aktérov má Twitter, Facebook. Najnižšiu hodnotu vykazuje YouTube. Celkovo je sledovanie podielu účtov dezinformačných aktérov na platforme dôležité pre porozumenie šírenia dezinformácií online a pre navrhovanie opatrení na ich obmedzenie. Štúdium vývoja podielu účtov dezinformačných aktérov v budúcnosti by mohlo poskytnúť informácie o správaní týchto aktérov, vrátane zmien v stratégiách šírenia dezinformácií čo by umožnilo prispôsobenie opatrení proti nim.



Graf 3 Podiel účtov dezinformačných aktérov
Zdroj: vlastné spracovanie údajov TrustLab

Relatívny pomer počtu sledovateľov je najvyšší pre Instagram. Nasleduje LinkedIn. Najnižšiu hodnotu nadobúda pre TikTok. V štúdii TrustLab sa uvádza, že dezinformační aktéri majú tendenciu sledovať viac používateľov, ale majú menej sledovateľov v porovnaní s nedezinformačnými aktérmi. Celkovo dezinformační aktéri môžu využívať rôzne stratégie a taktiky na šírenie dezinformácií, aj keď majú menej sledovateľov ako nedezinformační aktéri. Aktéri dezinformácií môžu využívať znalosti o algoritmoch sociálnych médií a strategicky publikovať obsah, ktorý bude mať väčšiu šancu na široké šírenie. Dezinformační aktéri môžu vytvárať a spravovať viac účtov, aby zvýšili dosah svojich príspevkov. Dezinformační aktéri môžu aktívne spolupracovať s inými účtami, ktoré majú väčšiu sledovateľskú základňu, aby zvýšili dosah svojich príspevkov.



Graf 4 Relatívny podiel počtu sledovateľov
Zdroj: vlastné spracovanie údajov TrustLab

Pre ďalšiu analýzu sme museli overiť, či jednotlivé ukazovatele majú normálne rozdelenie. Pomocou Andersonovho – Darlingovho testu sme zistili, že premenné majú normálne rozdelenie okrem relatívneho pomeru počtu sledovateľov. V tomto prípade, má normálne rozdelenie prirodzený logaritmus tohto ukazovateľa. V prípade každého ukazovateľa je p hodnota väčšia ako 0,01 a teda nulovú hypotézu o normalite na hladine významnosti 0,01 nemôžeme zamietnuť.

Tabuľka 1 Výsledky terovania normality

Ukazovateľ	Hodnota testovacej štatistiky D	Hodnota testovacej štatistiky D* pre n=6	P hodnota
Objaviteľnosť (Discoverability)	0.21372	0.25379	0.901465
Relatívny pomer angažovanosti (Relative post engagement ratio)	0.26946	0.31998	0.828128
Podiel účtov dezinformačných aktérov (Ratio of disinformation actors)	0.25371	0.30128	0.845099
Relatívny pomer počtu sledovateľov (Relative follower ratio)	1.06170	1.26077	0.002810
Ln(Relatívny pomer počtu sledovateľov)	0.33234	0.39465	0.384243

Zdroj: vlastné spracovanie údajov TrustLab

V ďalšom kroku sme použili metódu hlavných komponentov (PCA). Prvé dve hlavné komponenty vysvetľujú 81 % celkového rozptylu dát, naznačuje to, že týmto prvým dvom komponentom môže byť prisúdená významná časť variability obsiahnutých v dátach.

Tabuľka 2 Vlastné hodnoty a podiel rozptylu vysvetleny hlavnými komponentmi.

	Vlastná hodnota	Podiel rozptylu	Kumulatívny podiel vysvetleného rozptylu
Dim.1	2.252387457	56.30968643	56.30969
Dim.2	0.988222507	24.70556268	81.01525

Dim.3	0.757085974	18.92714936	99.9424
Dim.4	0.002304061	0.05760154	100

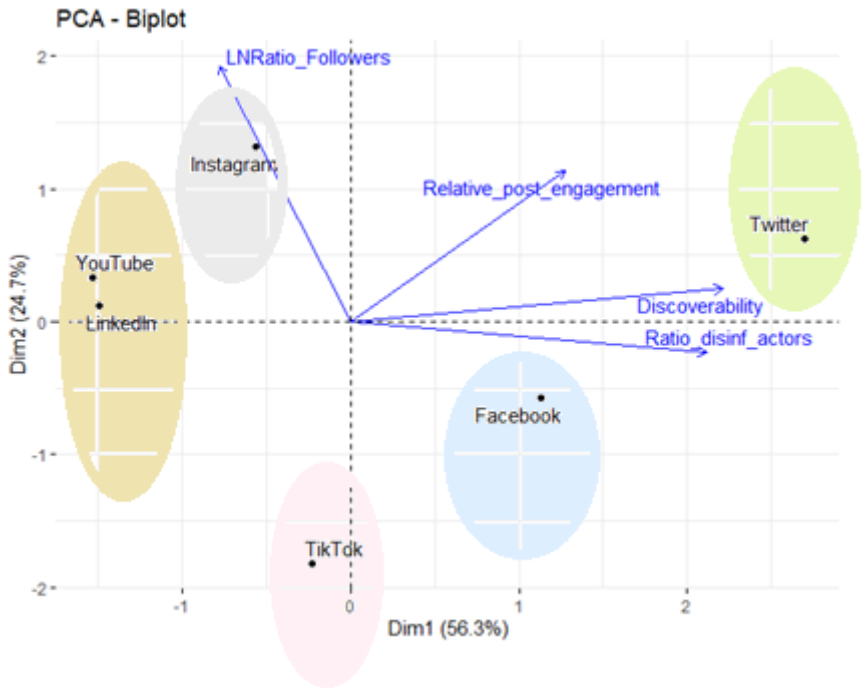
Zdroj: vlastné spracovanie údajov TrustLab

Tabuľka 3 Signifikantné korelácie medzi hlavnými komponentmi a pôvodnými premennými

Premenná	Korelácia s PC1	p hodnota
objaviteľnosť	0.9746185	0.00095816
Podiel účtov dezinformačných aktérov	0.9320176	0.00677533
Premenná	Korelácia s PC2	p hodnota
Ln(relatívny pomer počtu sledovateľov)	0.8468648	0.03338005

Zdroj: vlastné spracovanie údajov TrustLab

Vektory premenných sú reprezentované šípkami, ktoré ukazujú smer a dĺžku každej premennej v priestore hlavných komponentov. Premenné, ktoré majú podobný smer, sú blízko seba a môžu byť považované za podobné. V našom prípade premenné objaviteľnosť a podiel účtov dezinformačných aktérov majú podobný smer, čo naznačuje pozitívny vzťah medzi týmito dvoma premennými. Platformy s vyššou objaviteľnosťou majú vyšší podiel dezinformačných aktérov. Platformy s vyššou objaviteľnosťou môžu mať menej prísne mechanizmy na kontrolu obsahu, čo umožňuje dezinformačným aktérom ľahšie publikovať a šíriť dezinformácie bez väčšieho dohľadu. Na platformách s vyššou objaviteľnosťou je dezinformačný obsah rýchlejšie a ľahšie dostupný, čo priťahuje dezinformačných aktérov, ktorí majú snahu čo najrýchlejšie šíriť svoje správy.



Obrázok 1 Biplot

Zdroj: vlastné spracovanie údajov TrustLab

Z biplotu vieme vyčítať skutočnosti, ktoré sme už komentovali. Napríklad, že objaviteľnosť má najvyššiu Twitter. Najvyššiu hodnotu Ln(relatívny pomer počtu sledovateľov) má Instagram. Sociálne médiá sú zobrazené ako body v biplote. Euklidovská vzdialenosť medzi dvoma objektmi (bodmi) neaproximuje vzdialenosti medzi ich riadkami v pôvodnej matici, ale ich štandardizovanú vzdialenosť, ktorá je druhou odmocninou Mahalanobisovej vzdialenosti. Poloha sociálnych médií vzhľadom na premenné ukazuje, ako sú ovplyvnené jednotlivými premennými. Z biplotu je tiež zrejmé zhlukovanie jednotiek – sociálnych médií - s podobnými charakteristikami. Z hľadiska hodnotených ukazovateľov sú podobné iba platformy LinkedIn a YouTube. Ostatné sociálne siete nevytvárajú žiadne zhluky a sú izolované, nepodobné.

Závery

Skúmanie sociálnych sietí z hľadiska šírenia dezinformácií je dôležité pre porozumenie tomu, ako sa dezinformácie na týchto platformách šíria a akým spôsobom ovplyvňujú užívateľov. Na platformách s vyššou objaviteľnosťou je dezinformačný obsah rýchlejšie a ľahšie dostupný, čo priťahuje dezinformačných aktérov a podporuje rýchlejšie šírenie dezinformácií. Twitter má najvyššiu objaviteľnosť, čo naznačuje, že je to platforma s výrazným vplyvom na šírenie informácií, vrátane dezinformácií. Instagram má najvyššiu hodnotu relatívneho pomeru počtu sledovateľov, čo ukazuje na vysokú angažovanosť sledovateľov na tejto platforme. LinkedIn a YouTube, majú podobné hodnoty ukazovateľov. Ostatné platformy sú izolované a odlišujú sa vo svojich charakteristikách od ostatných. Tieto zistenia môžu slúžiť ako základ pre vypracovanie a implementáciu politík a regulácií na sociálnych médiách, ktoré majú za cieľ obmedziť šírenie dezinformácií a zlepšiť bezpečnosť a dôveryhodnosť online prostredia.

Zoznam použitej literatúry

AÏMEUR, Esma; AMRI, Sabrine; BRASSARD, Gilles. Fake news, disinformation and misinformation in social media: a review. *Social Network Analysis and Mining*, 2023, 13.1: 30.

ALONSO LÓPEZ, Nadia, et al. *Beyond challenges and viral dance moves: TikTok as a vehicle for disinformation and fact-checking in Spain, Portugal, Brazil, and the USA*. 2021.

BERLO, David K. *The process of communication: An introduction to theory and practice*. Holt Rinehart and Winston. Inc., New York, 1960, 960.

BESSI, Alessandro, et al. Homophily and polarization in the age of misinformation. *The European physical journal special topics*, 2016, 225: 2047-2059.

CALED, Danielle; SILVA, Mário J. Digital media and misinformation: An outlook on multidisciplinary strategies against manipulation. *Journal of Computational Social Science*, 2022, 5.1: 123-159.

DRAGULESCU Adrian and ARENDT Cole. xlsx: Read, Write, Format Excel 2007 and Excel 97/2000/XP/2003 Files. R package version 0.6.5. 2020 https://CRAN.R-project.org/package=xlsx

ECKER, U. K., LEWANDOWSKY, S., COOK, J., ... & AMAZEEN, M. A. (2022). The psychological drivers of misinformation belief and its resistance to correction. *Nature Reviews Psychology*, 1(1), 13-29.

EURÓPSKA KOMISIA: *Code of Practice on Disinformation*. 2018. dostupné na https://ec.europa.eu/newsroom/dae/redirection/document/87534

EURÓPSKA KOMISIA: Strengthened Code of Practice Disinformation. 2022 [online]. [citované 2.04.2024]. Dostupné na internete: https://ec.europa.eu/newsroom/dae/

redirection/document/87585

HELBERGER, Natali. (2020). Politická sila platforiem: Ako súčasné pokusy o reguláciu dezinformácií zosilňujú názorovú silu. *Digitálna žurnalistika*, 8 (6), 842–854.doi: 10.1080/21670811.2020.1773888

HILARY, Ibegbulem Obioma; DUMEBI, Olannye-Okonofua. Social media as a tool for misinformation and disinformation management. *Linguistics and Culture Review*, 2021, 5.S1: 496-505.

HINDMAN, Matthew; BARASH, Vlad. Disinformation,'fake news' and influence campaigns on Twitter. 2018.

CHEN, Sijing; XIAO, Lu; KUMAR, Akit. Spread of misinformation on social media: What contributes to it and how to combat it. *Computers in Human Behavior*, 2023, 141: 107643.

KASSAMBARA Alboukadel and MUNDT Fabian. factoextra: Extract and Visualize the Results of Multivariate Data Analyses. 2020. R package version 1.0.7. https://CRAN.R-project.org/package=factoextra

KARLOVA, Natascha A.; FISHER, Karen E. A social diffusion model of misinformation and, disinformation for understanding human information behaviour. *Information research*, vol 18, no 1, 2013. dokument 573. [online]. [citované 02.04.2024]. Dostupné na internete: http://InformationR.net/ir/18-1/paper573.html]

KOBERNJUK, Anna; KASPER, Agnes. Normativity in the EU's Approach towards Disinformation. TalTech *Journal of European Studies*, 2021, 11.1: 170-202.

KONDAMUDI, Medeswara Rao, et al. A comprehensive survey of fake news in social networks: Attributes, features, and detection approaches. *Journal of King Saud University-Computer and Information Sciences*, 2023, 35.6: 101571.

LE Sebastien, JOSSE Julie, HUSSON Francois. FactoMineR: An R Package for Multivariate Analysis. Journal of Statistical Software, 25(1),2008. 1-18. 10.18637/jss.v025.i01

MISHRA, Sidharth Prasad, et al. Multivariate statistical data analysis-principal component analysis (PCA). *International Journal of Livestock Research*, 2017, 7.5: 60-78.

NENADIC, Iva; BROGI, Elda; BLEYER-SIMON, Konrad. Structural indicators to assess effectiveness of the EU's Code of Practice on Disinformation. Working Paper, EUI, RSC, Working Paper, 2023/34, Centre for Media Pluralism and Media Freedom, 2023.

OSCE: *Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda.* 2017 Dostupné na https://www.osce.org/fom/302796

PENNYCOOK, Gordon; RAND, David G. The psychology of fake news. *Trends in cognitive sciences*, 2021, 25.5: 388-402.

R CORE TEAM (2021). R: A language and environment for statistical computing. R Foundation for Statistical Computing, Vienna, Austria. URL https://www.R-project.org/.

ROMEU, Jorge L. Anderson-Darling: a goodness of fit test for small samples assumptions. RAC START, 2003.

ROOZENBEEK, Jon; VAN DER LINDEN, Sander. *The Psychology of Misinformation.* Cambridge University Press, 2024.

TRUSTLAB. 2023. *Code of Practice on Disinformation*. Semi-annual report. [online]. [citované 02.04.2024]. Dostupné na internete: https://www.trustlab.com/codeofpractice-disinformation

VAN DER LINDEN, Sander. Misinformation: susceptibility, spread, and interventions to immunize the public. *Nature medicine*, 2022, 28.3: 460-467.

ZANNETTOU, Savvas, et al. The web of false information: Rumors, fake news, hoaxes, clickbait, and various other shenanigans. *Journal of Data and Information Quality* (JDIQ), 2019, 11.3: 1-37.

ZOLLO, Fabiana; QUATTROCIOCCHI, Walter. Misinformation spreading on Facebook. In: Lehmann, S., Ahn, YY. (eds) *Complex Spreading Phenomena in Social Systems. Computational Social Sciences*. Springer, Cham. Doi 10.1007/978-3-319-77332-2. 2018. s. 177-196.

Kontaktné údaje

prof. Ing. Antonín Korauš, PhD., LL.M., MBA
Akadémia Policajného zboru v Bratislave,
Sklabinská 1, 835 17 Bratislava 35,
Slovenská republika
E-mail: antonin.koraus@akademiapz.sk

Dr. h. c. Prof. JUDr. Lucia KURILOVSKÁ, PhD
Právnická fakulta Univerzity Komenského v Bratislave,
Šafárikovo nám. 6. 818 06 Bratislava
Slovenská republika
E-mail: lucia.kurilovska@flaw.uniba.sk

prof. RNDr. Beáta Stehlíková, CSc.
ÚM, Slovenská technická univerzita v Bratislave
Vazovova 5, 811 07 Bratislava
Slovenská republika
E-mail: beata.stehlikova@stuba.sk

pplk. RNDr. Kristián Újváry, PhD.
Ministerstvo vnútra SR,
Slovenská republika
vyslaný národný expert v agentúre Frontex
E-mail: kristian.ujvary@frontex.europa.eu

Recenzenti:

prof. RNDr. Michal Greguš, CSc.

doc. Ing. Václav Friedrich, Ph.D.

Reliability of generative artificial intelligence in textual content production

Martin Kuchta – Malgorzata Jarossová[26]

Abstract: Utilization of artificial intelligence (AI) tools within content production processes has potential to trigger creativity of producer, save some amount of time dedicated to content production and save some costs. The main aim of the article is to compare different versions of particular textual generative artificial intelligence tool and human text production and to propose recommended textual content producer for search engine advertising texts. The empirical utilized real advertising campaigns and compared reached results from each advertising text producer: human, AI tool version 1, AI tool version 2. The results suggest effectiveness of AI tools, however highlight necessity of human factor within text content production.

Key words: advertising, artificial intelligence, content production, search engines

INTRODUCTION

Artificial intelligence (AI) has rapidly evolved, becoming a transformative technology across multiple industry areas. AI tools operate from machine learning stage to natural language stage and influence various sectors including healthcare, finance, education, and transportation (Pugalenthi et al., 2021). However, the most impacted is content production industry itself. Media and marketing companies now challenge significant changes in processes and human force utilization. Human content producers have completely new opportunities with AI tools, and the technology is so advanced that it can partially or completely replace human workforce within the industry (Ahn et al., 2024). Advanced analytical tools and current artificial intelligence tools began to shape current content production optics and ha significant influence on processes within the companies, governmental institutions, but in private sphere also. There are five content types: text, pictures, audio, video and combinations of the mentioned (D.-H. Kim et al., 2015). AI tools began to operate with text format in their initial stages, however there are new tools also, which are able to proceed and produce pictures, audio and video media formats. Since the capability to process all available formats, AI has significant impact on content production industry. Within an institution processes content generative tools are capable to (1) produce content (generate articles, reports, social media captions, video subtitles, initial and replying emails etc., what significantly decrease time required from human workforce), (2) curate content (AI systems are able to serve to users only content they are interest in, using various content sources), (3) personalize content (data collection and precise procession

[26]JEL Classification code: M31

utilizing AI systems analyze user preferences and personalize content loaded on website or in advertisement), (4) quality control (AI tools are able to control grammar, style and check factual accuracy by comparation with other content sources), (5) content distribution (created content is often invisible on the internet and it is necessary to deliver it desired target groups using distribution channels such as website, social networks profiles, messenger etc., while AI tools are able to evaluate effectiveness of each channel and publish it where needed) (Clarke, 2019). New AI approaches has significant impact on workforce also (Haupt et al., 2024). AI tools can (1) displace human workforce from some specific work positions, (2) replenish human workforce by finding a synergy between human prompts and AI execution or vice versa, (3) transform job description and human responsibilities and lead humans to lead positions, where AI execute established commands, (4) trigger new ideas and motivate to perform "extra step" in human work outputs, where information provides by AI can open to human mind, can show a bigger picture or put situation and task in context (Carstensen & Ganz, 2023). In all mentioned above AI is capable to mimic human manuscript in form of text, picture, video or audio, what means, that AI outputs are almost unrecognizable from humans outputs (Obrenovic et al., 2024). In terms of forms of content AI can significantly bend output media formats and enrich their combinations. Traditional standard content formats can be combined in different ways and result into new experience of content final consumer (Wang et al., 2023). AI can text combine with pictures and create infographic, include human voice, which read a text to standard text formats and creates new types of podcasts, create extra voiceovers explaining situation or describing scenario in movies, enrich audio formats witch text transcripts, visualize audio formats utilizing pictures or videos etc.. Mentioned combinations were possible even before the AI, however it was timely and financially unreasonable to produce such variations of a content. However, the AI tools are able to produce the variations within a fraction of time and with zero or minimum costs. The problem will no more be content production and distribution, but form of content presentation (J. Kim et al., 2020). Initial AI revolution began with text generators operating on machine learning. Text generative AI is a subcategory of AI tools, and have the ability to produce coherent and contextually relevant text content. These systems leverage advancements in machine learning and natural language processing (NLP) to generate human-like text. There are two steps text AI utilize to produce relevant content. (1) Training, which use diverse texts to predict the next word in a sequence. Training allows the model to learn patterns, grammar and text style. (2) Tuning, which use gathered data to enhance model to generate more appropriate text which correspond with user style and preferences (Cheng et al., 2023). Text generative AI tools are capable to generate (1) new texts, (2) summarize texts, (3) translate text

and (4) maintain conversation (Li et al., 2024). In terms of new text production the text can be in news style, creative style, technical documentation style, programming code style and many more variations. It is capable to generate whatever content style depending on input used in prompt. In terms of text summarizations the AI is able to identify relevant and important information and select and summarize only preferred information. The ability is useful in law industry for instance. In terms of text translation the AI is able to translate a text into all world languages within seconds and the translation can be proceed in various styles based on prompt. In terms of conversation maintenance first adopters in the industry already utilize the technology for online communication with customers in ecommerce industry in forms of chatbots, automatic email replies or social network messengers communication. The possibilities of textual generative AI are almost endless and has potential to impact all industries. The most threatened, yet the most opportunistic are the media and marketing institutions. The AI can be beneficial in marketing industry for copy generation such as search engines ad texts, social media texts, blog texts, chatbots, virtual assistants, etc.. It can be helpful also for SEO optimization for key words research and power, identification for relevant backlink placements etc. (Yuniarthe, 2017). Media utilizing text generative AI can search for inspiration for topics using AI, generate texts and displace or replace some human workforce to save some costs and create competitive advantage.

However, the reliability of the generative AI systems remains a topic of significant interest and concern, especially in contexts of accuracy, consistency, moral issues and ethics (Kenthapadi et al., 2023). The absence of regulations and guidance in the area is currently critical point, where the future of cohabitation AI and humans will be set. It is necessary to deal with the topic on all relevant platforms bringing together voices of industry, governance and individuals.

1 METHODOLOGY

The main aim of the article is to compare different versions of particular textual generative artificial intelligence tool and human text production and to propose recommended textual content producer for search engine advertising texts.

The empirical research utilized real advertising campaigns in cooperation with local marketing agency focused on digital environment and compared reached results from each advertising text producer. The input data for all ad content producers were identified to establish and unify the creation of headlines and sub-headlines for the Google Search ads. A crucial

aspect was determining the AI's role and setting the maximum character and space limits for the headlines and descriptions.

To achieve main goal of the paper three ad content producers were identified:

(1) Human – the ad texts were created by search engine advertising specialist oriented on PPC principles and optimization,

(2) AI tool version 1 – the utilized tool was ChatGPT-3.5, the free version in the time of the research ,

(3) AI tool version 2 – the utilized tool was ChatGPT-4, the paid version in the time of the research.

All producers were provided by the same input information to generate ad content in form of headlines and subheadlines in accordance with technical requirements of ad system. Input information were perceived as brief for human producer and as prompts for AI producer. The first crucial task was to comply with amount of characters mandated by the ad system. Created ads were utilized in ad environment and there was one campaign created. The timing for the campaign was seven days and budget was 30€. The system, based on performance, prioritize texts with better results. The performance indicators observed were:

- impressions,
- clicks,
- total costs,
- click-through-rate,
- cost-per-click.

Impressions, clicks and total costs were perceived as primary information and click-through-rate and cost-per-click were perceived as secondary information calculated from primary information. Except timing and budget there was target group defined also. Since it was real campaign executed the target audience corresponded with assignment of the client of the ad campaign which corresponded with the target audience of the company's website.

The results suggest effectiveness of AI tools, however highlight necessity of human factor within text content production.

2 RESULTS AND DISCUSSION

In the first step of the research the assignment for textual advertisement dedicated to search engine paid ads was created. The assignment contained exact maximum number of symbols available for the advertisement, demanded style of the advertisement and instruction for call to action part of a text. The assignment was given to human ad creator and was use as prompt for AI tool ver. 1 and AI tool ver. 2. In the first step of the research number of errors or incorrect answers not following assignment was observed. The observation is processed in following table.

Table 1 Number of errors of ad creators

	Human	AI tool ver. 1	AI tool ver. 2
First answer	0	18	0
Second answer	-	4	-
Third answer	-	0	-

Source: own procession

Following created assignment human outputs had zero errors and ad texts were usable within first attempt. Human with specialization in text creation understood the assignment immediately, was able to incorporate all requirements and instructions and the final ads had also some emotional value. AI tool ver. 1 had 18 errors in first output. Errors included exceeded number of characters in all parts of the text ad, misunderstood presentation of product features, lack of emotional connection of text ad consumer and brand, lack of call to action or call to action not corresponding with the context, errors in shown url address etc.. The second prompt navigating AI tool ver. 1 was necessary. For all errors there was an instruction to correct it and the result was second answer with 4 errors. Errors included exceeded number of characters in two parts of the text ad, one inconsistency in text style and misunderstood call to action element. The third correction prompt was necessary and it navigated the AI to remove all errors. The result was third answer with zero errors.

In the next step all answers created by human, AI tool ver. 1 and AI tool ver. 2 were used in search engine advertisement environment as real world ad campaigns and following performance indicators were observed:

- impressions – represent number of times the ad was shown to users,
- clicks – represent number of clicks ads achieved,

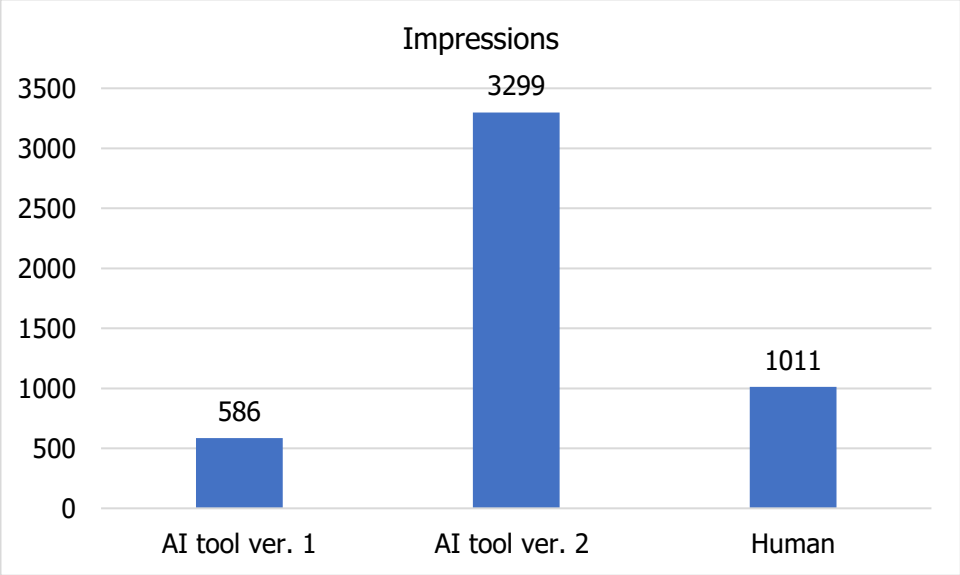
o CTR – represent a relation between the impressions and the click and show click through rate (one of the most used performance indicators in digital advertisement),

o CPC – represent cost per click calculated from total budget and achieved clicks.

The performance indicators were observed and after the end of the campaign noted into Excel program to achieve better clarity and option for graph visualization. All ads had the same budget and the advertisement system decided, based on interim results, to which ad version will dedicated bigger share of budget. Performance indicators were processed into graphs for visualization and better understanding and are shown in the paper.

The first graph process Impressions as observed performance indicator.

Graph 1 Impressions as observer performance indicator

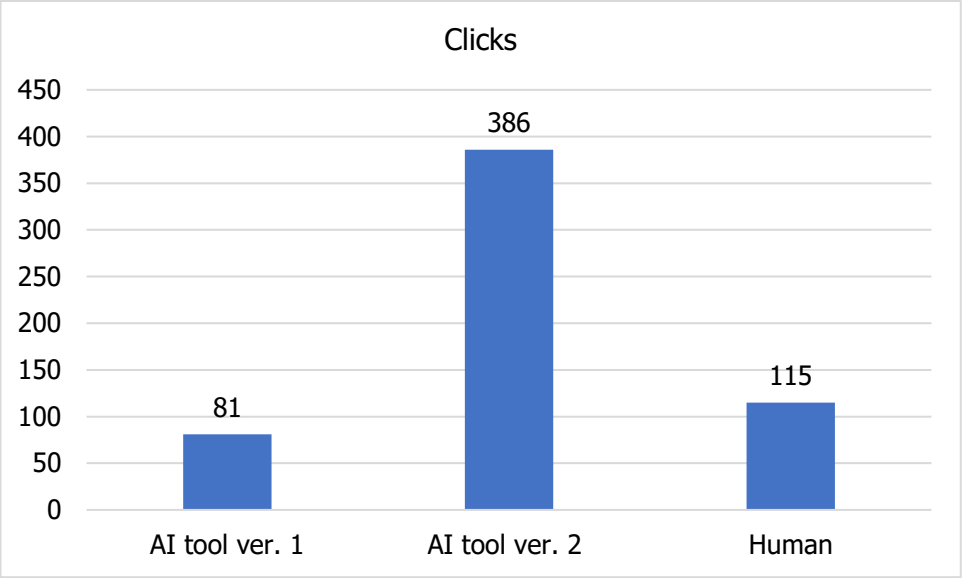


Source: own procession

In the first graph impression were observed and visualized as performance indicator. The most impression achieved AI tool ver. 2. It is necessary to remind, that the AI tool ver. 2 had zero errors in first prompt. The second most impressions had human and the last one was AI tool ver. 1, which required significant amount of corrections.

The second graph process clicks as key performance indicator observed.

Graph 2 Clicks as observer performance indicator

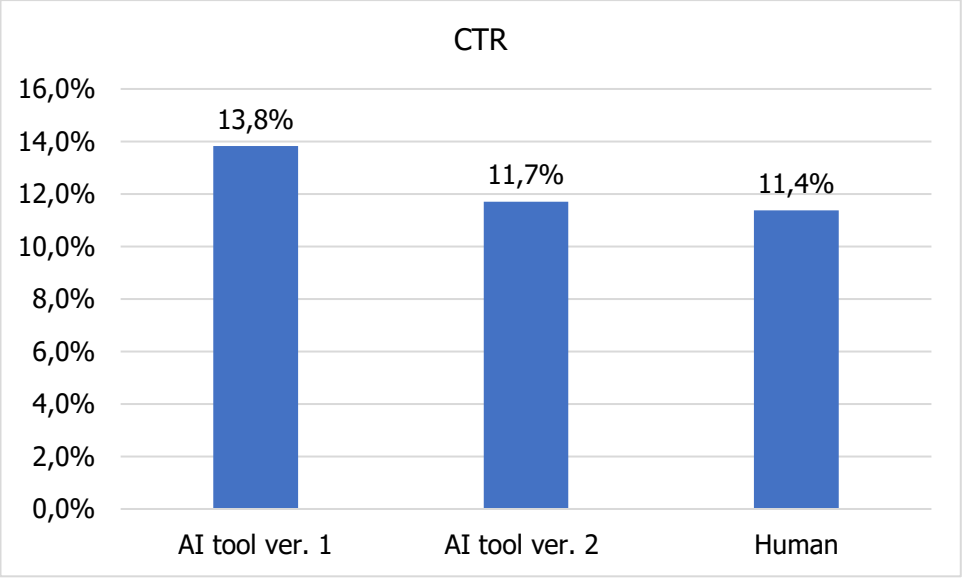


Source: own procession

The graph above process clicks as observed performance indicator. The graph follow trend from Graph 1 and also here AI tool ver. 2 with need of zero corrections achieved the most clicks, the second one was human and the last one was AI tool ver. 1 with significant amount of corrections required.

The third graph process CTR as observer performance indicator.

Graph 3 CTR as observer performance indicator

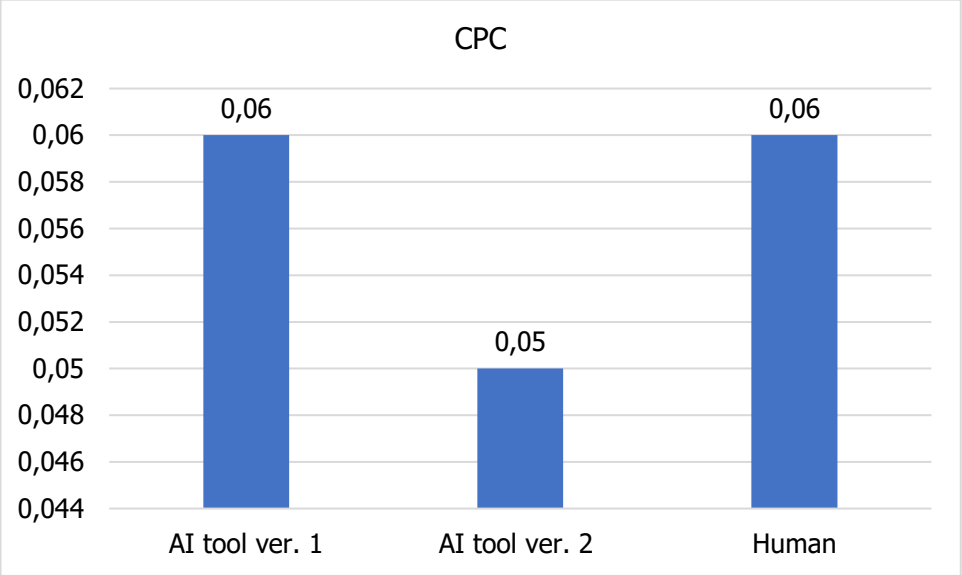


Source: own procession

CTR metric compare clicks and impressions. The best CTR achieved AI tool ver. 1, the second most successful was human creator and the last one was AI tool ver. 2.

The last observed performance indicator was CPC, which calculate cost per click from total budget spent on ad campaign.

Graph 4 CPC as observer performance indicator



Source: own procession

The lowest CPC, 0,05€, was acvieved by AI tool ver. 2 and AI tool ver. 1 and human creator achieved same CPC 0,06€.

CONCLUSION

The research aimed to compare the effectiveness of textual advertisements created by a human ad creator, AI tool version 1, and AI tool version 2 in the context of search engine paid ads. Initially, all three were given an assignment with specific instructions. The human ad creator produced outputs with zero errors on the first attempt, demonstrating a clear understanding of the requirements and adding emotional value to the ads. In contrast, AI tool version 1 required three iterations to eliminate all errors, while AI tool version 2 produced an ad with zero errors within the first attempt.

The performance of these ads was then evaluated in real-world ad campaigns, focusing on performance indicators: impressions, clicks, click-through rate (CTR), and cost per click

(CPC). AI tool version 2 outperformed in terms of impressions and clicks, indicating its capability to attract the most audience without requiring corrections. The human ad creator ranked second in these metrics, while AI tool version 1, despite needing significant corrections, showed the best CTR. In terms of cost-efficiency, AI tool version 2 achieved the lowest CPC, followed by the human ad creator and AI tool version 1, which shared the same CPC.

In conclusion, while the human ad creator showed proficiency in creating high-quality ads with emotional appeal on the first attempt, AI tool version 2 demonstrated superior overall performance in impressions, clicks, and cost efficiency.

The results shown significant added value of more advanced generative AI textual tools, however the human intervention is still necessary, or at least expected, because of possibility of errors, misunderstanding of assignment, misunderstanding the target group and lack of emotional point of view on text creation. However, the results show significant progress in the (in time of the research) latest versions of AI tools and suggest bright future for the AI tools.

Limitations of the research were identified as relatively small sample of ads tested and limited budget used for real-world campaign. Further research could focus on more comprehensive research in the area and could use also some statistical approaches to process collected data.

ACKONWLEDGMENET

This paper is an output of project VEGA no. 1/0398/22 The current status and perspectives of the development of the market of healthy, environmentally friendly and carbon-neutral products in Slovakia and the European Union.

REFERENCES

Ahn, S., Yim, H.-J., Lee, Y., & Park, S.-I. (2024). Dynamic and Super-Personalized Media Ecosystem Driven by Generative AI: Unpredictable Plays Never Repeating the Same. IEEE Transactions on Broadcasting, 1–15. https://doi.org/10.1109/TBC.2024.3380474

Carstensen, T., & Ganz, K. (2023). Gendered AI: German news media discourse on the future of work. AI & SOCIETY. https://doi.org/10.1007/s00146-023-01747-5

Cheng, D., Patel, D., Pang, L., Mehta, S., Xie, K., Chi, E. H., Liu, W., Chawla, N., & Bailey, J. (2023). Foundations and Applications in Large-scale AI Models: Pre-training, Fine-tuning, and

Prompt-based Learning. Proceedings of the 29th ACM SIGKDD Conference on Knowledge Discovery and Data Mining, 5853–5854. https://doi.org/10.1145/3580305.3599209

Clarke, R. (2019). Principles and business processes for responsible AI. Computer Law & Security Review, 35(4), 410–422. https://doi.org/10.1016/j.clsr.2019.04.007

Haupt, M., Freidank, J., & Haas, A. (2024). Consumer responses to human-AI collaboration at organizational frontlines: strategies to escape algorithm aversion in content creation. Review of Managerial Science. https://doi.org/10.1007/s11846-024-00748-y

Kenthapadi, K., Lakkaraju, H., & Rajani, N. (2023). Generative AI meets Responsible AI: Practical Challenges and Opportunities. Proceedings of the 29th ACM SIGKDD Conference on Knowledge Discovery and Data Mining, 5805–5806. https://doi.org/10.1145/3580305.3599557

Kim, D.-H., Spiller, L., & Hettche, M. (2015). Analyzing media types and content orientations in Facebook for global brands. Journal of Research in Interactive Marketing, 9(1), 4–30. https://doi.org/10.1108/JRIM-05-2014-0023

Kim, J., Shin, S., Bae, K., Oh, S., Park, E., & del Pobil, A. P. (2020). Can AI be a content generator? Effects of content generators and information delivery methods on the psychology of content consumers. Telematics and Informatics, 55, 101452. https://doi.org/10.1016/j.tele.2020.101452

Li, B., Yang, P., Sun, Y., Hu, Z., & Yi, M. (2024). Advances and challenges in artificial intelligence text generation. Frontiers of Information Technology & Electronic Engineering, 25(1), 64–83. https://doi.org/10.1631/FITEE.2300410

Obrenovic, B., Gu, X., Wang, G., Godinic, D., & Jakhongirov, I. (2024). Generative AI and human–robot interaction: implications and future agenda for business, society and ethics. AI & SOCIETY. https://doi.org/10.1007/s00146-024-01889-0

Pugalenthi, R., Prabhu Chakkaravarthy, A., Ramya, J., Babu, S., & Rasika Krishnan, R. (2021). Artificial learning companionusing machine learning and natural language processing. International Journal of Speech Technology, 24(3), 553–560. https://doi.org/10.1007/s10772-020-09773-0

Wang, Y., Pan, Y., Yan, M., Su, Z., & Luan, T. H. (2023). A Survey on ChatGPT: AI–Generated Contents, Challenges, and Solutions. IEEE Open Journal of the Computer Society, 4, 280–302. https://doi.org/10.1109/OJCS.2023.3300321

Yuniarthe, Y. (2017). Application of Artificial Intelligence (AI) in Search Engine Optimization (SEO). 2017 International Conference on Soft Computing, Intelligent System and Information Technology (ICSIIT), 96–101. https://doi.org/10.1109/ICSIIT.2017.15

CONTACT INFORMATION

doc. Ing. Martin Kuchta, PhD., MBA
University of Economics in Bratislava, Faculty of Commerce,
Department of marketing, Bratislava, Slovakia
e-mail: martin.kuchta@euba.sk

doc. Dr. Ing. Malgorzata A. Jarossová
University of Economics in Bratislava, Faculty of Commerce,
Department of marketing, Bratislava, Slovakia
e-mail: malgorzata.jarossova@euba.sk

Recenzenti:
doc. Ing. Václav Friedrich, Ph.D.
doc. RNDr. Tatiana Hajdúková, PhD.

Hodnotenie rizík centralizovaných a decentralizovaných poskytovateľov služieb kryptoaktív

Andrej Lipták

Abstrakt: Príspevok pozostáva z hodnotenia rizík centralizovaných a decentralizovaných poskytovateľov služieb kryptoaktív vo vzťahu k legalizácií výnosov z trestnej činnosti a k nadväzujúcim legislatívnym opatreniam. Prostredníctvom analýzy fundamentálnej stránky poskytovateľov služieb kryptoaktív, aktuálne platných právnych noriem a aktuálneho trendu legalizácie výnosov z trestnej činnosti, ktoré majú formu kryptoaktív, určíme mieru rizika vplývajúcu na klientov týchto poskytovateľov a na súvisiacu ekonomickú, hospodársku a platobnú stabilitu v spoločnosti.

Kľúčové slová: Poskytovatelia služby kryptoaktív, distribuovaná databáza transakcií, kryptoaktíva, legislatívne opatrenia, hodnotenie rizík

Abstract: The contribution consists of an assessment of the risks associated with centralized and decentralized crypto-asset service providers regarding the legalization of proceeds from criminal activity and related legislative measures. Through an analysis of the fundamental aspects of crypto-asset service providers, current legal norms, and the ongoing trend of proceeds from criminal activity in the form of crypto-assets, we will determine the level of risk affecting the clients of these providers and the associated economic, financial, and payment stability of the society.

Keywords: Crypto-asset service providers, distributed ledger technology, crypto-assets, regulation, risk assessment

Úvod

Kybernetická bezpečnosť sa aj vzhľadom na prirodzený vývoj spoločnosti, máme na mysli najmä úroveň modernizácie a informatizácie, stáva jedným z najvýznamnejších druhov bezpečnosti. Podcenením opatrení kybernetickej bezpečnosti sa chránené objekty vystavujú rizikám týkajúcim sa neoprávneného narušenia, zneužitia alebo neželanej manipulácie. Táto skutočnosť súvisí nie len so zraniteľnosťou v oblasti hybridných hrozieb z globálneho hľadiska, ale aj napr. s individuálnou zraniteľnosťou obyvateľov štátu. Kroky Finančnej akčnej skupiny, orgánov a agentúr Európskej únie, zahraničných a vnútroštátnych orgánov verejnej moci, ale aj súkromného sektoru, resp. tretieho sektoru, poukazujú na významnosť venovania sa prvkom kybernetickej bezpečnosti. Bežná sociálna interakcia a komunikácia, ekonomická a hospodárska aktivita, platobný styk, uzatváranie právne-relevantných vzťahov, vyhľadávanie a selektovanie informácií sa neudržateľne presúva z doposiaľ známeho fyzického prostredia do prostredia elektronického. Rýchlosť a objem prenášaných informácií prostredníctvom elektronických rozhraní všeobímajúco stúpa, avšak to nemožno povedať o erudícii v tejto

oblasti. Berúc do úvahy najmä individuality, akými sú napr. obyvatelia štátu možno pozorovať, že síce dochádza k širokej adopcií prostriedkov elektronizácie a informatizácie, nedochádza v podobnej miere aj k adopcii poznatkov o týchto prostriedkoch. Pri odosielaní informácií ekonomického charakteru pri bezhotovostnom platobnom styku, akým je bežne platba za tovar alebo službu, dochádza k využívaniu rôznorodých prostriedkov, teda technických zariadení, u ktorých osoby využívajúce tieto zariadenia nemajú dostatočné poznanie o princípoch ich fungovania, a tým pádom nemajú ani možnosť určiť riziká a hrozby spojené s využívaním týchto zariadení. Tok informácií z platobnej karty cez platobný terminál až po bankový subjekt, v ktorom sú informácie o zostatku v určitej mene uložené, prechádzajú rôznymi mechanizmami na zaistenie kybernetickej bezpečnosti, ktoré sú dané technickými normami a inými opatreniami, sú zároveň implementované poskytovateľmi platobných služieb. Prvky kybernetickej bezpečnosti je však nevyhnutné určiť nie len pre poskytovateľov týchto služieb, ale aj pre osoby, ktoré služby aktívne používajú. Terminál, ktorý je pri iniciovaní platobného styku správne auditovaný, certifikovaný a spĺňa všetky normy a opatrenia môže byť rovnako tak použitý na trestnú činnosť, alebo na páchanie podvodných aktivít ako aj ten, ktorý tieto normy a opatrenia nespĺňa. Tento príspevok vo svojom objekte preto adresuje problematiku kybernetickej bezpečnosti vo vzťahu k používateľom služieb, resp. k používateľom zariadení, ktoré sú spôsobilé iniciovať ekonomicky relevantný tok informácií, pričom berieme do úvahy tú skutočnosť, že osoby nemusia mať dostatočné poznanie fundamentálnych stránok nimi využívanými zariadeniami. A to sa v súčasnosti do popredia dostáva nový decentralizovaný systém, ktorý ponúka alternatívu k centralizovanému systému typickému výmenou ekonomicky relevantných údajov a informácií, teda dát v technickej rovine. Predmetom príspevku bude rozobratie rizík spojených s využívaním nového decentralizovaného alternatívneho systému využívajúceho technológiu distribuovanej databázy transakcií najmä z toho dôvodu, že práve tento systém umožňuje priame podieľanie sa na výmene ekonomicky relevantných informácií bez potreby sprostredkovateľa alebo iného centrálneho subjektu. Nevynímajúc skutočnosť, že používatelia nemusia disponovať dostatočným poznaním o rizikách súvisiacich s používaním prostriedkov bežného centralizovaného platobného a ekonomického systému, možno usudzovať, že nepoznaním rizík toho decentralizovaného môže spôsobiť oveľa väčšie neželané následky, než je bežne predpokladané. Potrebu skúmania problematiky v tejto oblasti dopĺňa okrem narastajúceho objemu transakcií v distribuovanej databáze transakcií jednotlivých kryptoaktív[1], čo výrazne indikuje zvyšujúce sa využívanie

[1] Confirmed Transaction Per Month. (online, cit. 28.03.2024). Dostupné na internete: <https://www.blockchain.com/explorer/charts/n-transactions>

tohto decentralizovaného systému, aj kvantifikovaná prítomnosť trestnej činnosti realizovaná v tomto decentralizovanom systéme tvorená najmä rozmanitým podvodným konaním, objednávaním vykonávania násilnej, počítačovej, mravnostnej a inej kriminality v prostredí Darknetu alebo realizovaním tzv. ransomware útokov.[2]

V príspevku sa prvkami kvantitatívno-kvalitatívneho skúmania rozoberú viaceré formy decentralizovaného systému, ktoré slúžia na iniciovanie ekonomicky relevantného prenosu informácií, teda dát, so zameraním na určenie vyplývajúcich rizík[3], kde základnými atribútmi bude pravdepodobnosť ich výskytu a potenciálna závažnosť dopadu na osoby využívajúce tento decentralizovaný systém, následné vytýčenie opatrení kybernetickej bezpečnosti a opatrení vnútroštátnej a európskej legislatívy.

1. CENTRALIZOVANÍ POSKYTOVATELIA SLUŽBY KRYPTOAKTÍV

Vnútroštátny právny poriadok Slovenskej republiky v súčasnosti nedisponuje dostatočným právnym rámcom, ktorý by štruktúrovane a podrobne definoval, kto a za akých podmienok môže poskytovať služby kryptoaktív daného druhu, neobjasňuje podstatu vzťahov vznikajúcich pri realizovaní činností v systéme kryptoaktív aj napriek tomu, že kryptoaktíva ako alternatíva k bežnému platobnému systému existuje približne od roku 1990.[4] Z celkového množstva a rozličných podôb poskytovania služieb v systéme kryptoaktív sa časom vyextrahovala potreba uviesť do právneho poriadku jej niektoré formy. Domnievame sa, že príčinou nebolo logicky uvážené, z výsledkov proaktívneho a podrobného skúmania podložené konanie kompetentných výkonných a legislatívnych orgánov. Zákonodarná moc zobrala do úvahy iba to potrebné minimum, ktoré vyžadovala určitá časť spoločnosti na zlegalizovanie svojich už reálne vykonávaných činností, a povinnosť zosúladenia vlastných právnych noriem s európskymi právnymi normami a odporúčaniami medzinárodných a medzivládnych organizácií. Ešte pred prijatím Nariadenia Európskeho parlamentu a Rady (EÚ) 2023/1114 z 31. mája 2023 o trhoch s kryptoaktívami a o zmene nariadení (EÚ) č. 1093/2010 a (EÚ) č. 1095/2010 a smerníc 2013/36/EÚ a (EÚ) 2019/1937 (ďalej len „MiCA“), ktoré tvorí zatiaľ najprepracovanejšiu formu právneho predpisu upravujúcu problematiku systému kryptoaktív, bola v podmienkach Slovenskej republiky táto problematika ukotvená nesystematicky vo

[2] ŠANTA, J., ŠANTA, I.: Virtuálne meny - trestnoprávne a niektoré analyticko-ekonomické aspekty. Praha: Leges, 2023. 44-54 strán. ISBN: 978-80-7502-668-2

[3] Usmernenia pre podávanie správ o riadení rizika katastrof, článok 6 ods. 1 písm. d) rozhodnutia č. 1313/2013/EÚ (2019/C 428/07)

[4] Security Analysis of Chaum’s eCash Protocol. (online, cit. 13.04.2024). Dostupné na internete: <https://hessenbox.tu-darmstadt.de/download/MkhGVktzWGdFV2VxR0RodHVyYlQy/Chaum%27s-eCash-protocol.pdf?inline>

viacerých právnych predpisoch. Ak zoberieme do úvahy centralizovaných poskytovateľov služieb kryptoaktív, tak títo pre svoju legálnu činnosť musia disponovať osvedčením o živnostenskom oprávnení, pričom musia spĺňať všeobecné a osobitné podmienky prevádzkovania živností, pričom za tie osobitné sa považuje skončenie úplného stredného všeobecného vzdelania alebo úplného stredného odborného vzdelania. Zákon č. 455/1991 Zb. o živnostenskom podnikaní (ďalej len „živnostenský zákon“) predpokladá iba dve formy vykonávania podnikateľskej činnosti v oblasti systému kryptoaktív a tou je poskytovanie služieb zmenárne virtuálnej meny a poskytovanie služieb peňaženky virtuálnej meny a to v podobe viazaných živností. Čo sa presne rozumie pod výkonom takýchto viazaných živností možno za využitia analógie bádať v zákone č. 297/2008 Z.z. o ochrane pred legalizáciou príjmov z trestnej činnosti a o ochrane pred financovaním terorizmu a o zmene a doplnení niektorých zákonov (ďalej len „zákon o legalizácii“), ktorý hovorí, že poskytovateľom služieb peňaženky virtuálnej meny je osoba, ktorá poskytuje služby na ochranu súkromných kryptografických kľúčov v mene jej klientov, na držbu, uchovávanie a prevod virtuálnej meny, a že poskytovateľom služieb zmenárne virtuálnej meny je osoba, ktorá v rámci svojej podnikateľskej činnosti ponúka alebo vykonáva obchody s virtuálnou menou, ktorých predmetom je nákup virtuálnej meny za eurá alebo cudziu menu alebo predaj virtuálnej meny za eurá alebo cudziu menu. Takéto pomerne úzke vymedzenie profilu činností týchto poskytovateľov v systéme kryptoaktív je problematické najmä vo vzťahu k opatreniam, ktoré je možné aplikovať v prípade prejavenia skutočností, na ktoré prvotne odkazovali vytýčené riziká a potenciálne hrozby.[5] Vymedzenie podnikateľskej činnosti poskytovateľov služieb peňaženky a zmenárne virtuálnej meny však nezhŕňa všetky druhy a formy podnikania v oblasti kryptoaktív. Ak osoba plánovala vykonávať iné činnosti v oblasti kryptoaktív nespadajúce pod spomínané vymedzenie, ale so znakmi sústavnosti, samostatnosti, vo vlastnom mene, na vlastnú zodpovednosť, za účelom dosiahnutia zisku, jednou z možností bolo pre ňu ohlásenie voľnej živnosti, pri ktorej sa nevyžaduje splnenie odbornej ani inej spôsobilosti. Následkom toho bola evidencia viazaných živností ako napr. vykonávanie činností súvisiacich s obchodovaním v oblasti kryptomien, poskytovanie služieb Escrow agenta v oblasti kryptomien, prevádzkovanie systému pre ťažbu kryptomeny, ťaženie a produkcia kryptomien, ťaženie kryptomien, činnosti súvisiace s ťažbou kryptomien, obchodovanie v oblasti kryptomien, nákup a predaj kryptomien pre tretiu osobu, nákup a predaj kryptomeny, prevádzkovanie automatov na virtuálne meny, sprostredkovanie nákupu a predaja kryptomien, poskytovanie pôžičiek v kryptomenách, správa

[5] ŠANTA, J. – ŠANTA, I.: K niektorým legislatívnym a ekonomickým aspektom virtuálnych mien v legislatíve Európskej únie a Slovenskej republiky; Justičná revue, 74, 2022, č, 2, s. 167 – 177.

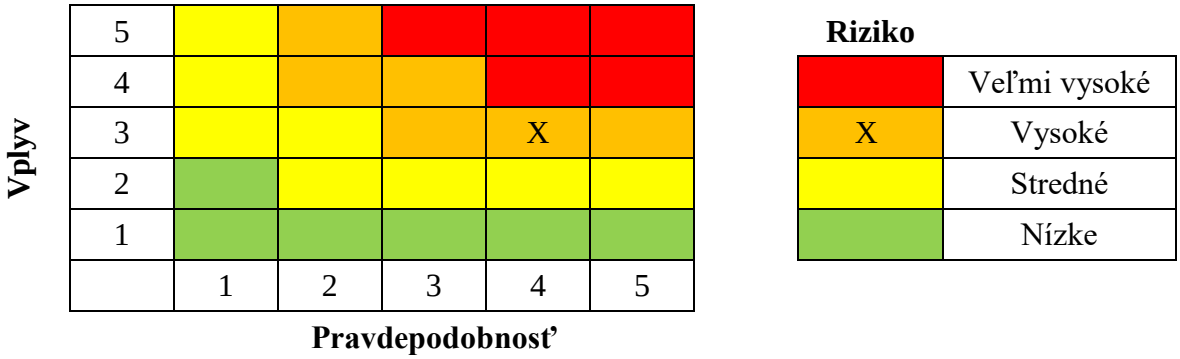
účtov v oblasti kryptomien, prevádzkovanie bezpečnostného úložiska v oblasti kryptomien alebo vykonávanie obchodnej činnosti s kryptomenami. Konsolidácia nariadenia MiCA rozširujúca pôsobnosť poskytovateľov služieb kryptoaktív na poskytovanie úschovy a správu kryptoaktív v menej klientov, prevádzkovanie obchodnej platformy pre kryptoaktíva, poskytovanie výmeny kryptoaktív za finančné prostriedky, poskytovanie výmeny kryptoaktív za iné kryptoaktíva, vykonávanie príkazov týkajúcich sa kryptoaktív v mene klientov, emitovanie, umiestňovanie kryptoaktív, poskytovanie prijímania a postupovania príkazov týkajúcich sa kryptoaktív v mene klientov, poskytovanie poradenstva v oblasti kryptoaktív, poskytovanie riadenia portfólia kryptoaktív a poskytovanie služieb prevodu kryptoaktív v mene klientov, síce pod seba reálne zahŕňa drvivú väčšinu podnikateľských činností centralizovaných poskytovateľov služieb kryptoaktív, legislatívne sa však predpokladá subsumovanie týchto činností pod aktuálne známych poskytovateľov služieb zmenárne a peňaženky virtuálnej meny. O tomto zámere hovorí návrh zákona o niektorých povinnostiach a oprávneniach v oblasti kryptoaktív a o zmene a doplnení niektorých zákonov, ktorý je aktuálne v medzirezortnom pripomienkovom konaní. Živnostenské oprávnenie na poskytovanie služieb zmenárne alebo peňaženky virtuálnej meny vydané do 30. decembra 2024 má zaniknúť 01. júla 2026. Od 30. decembra 2024 už bude možné podnikať v spomínaných oblastiach len po povolení príslušným orgánom, ktorým je Národná banka Slovenska. To sa však, podľa doposiaľ známych informácií, nedotkne poskytovateľov vykonávajúcich činností v oblasti kryptoaktív na základe voľnej živnosti. [6]

Fundament: Kryptoaktíva identifikované ako výnosy z trestnej činnosti sú legalizované najmä skrz centralizovaných poskytovateľov služieb kryptoaktív spĺňajúcich legálne požiadavky vyplývajúce z danej jurisdikcie, pomerom značne presahujúcim ostatné formy legalizácie, ako je napr. využitie anonymizačných služieb známych ako mixovacie služby, alebo využitie decentralizovaných aplikácií, smart kontraktov v rámci decentralizovaného financovania za výlučného využívania charakteru distribuovanej databázy transakcií. Okrem iného je táto skutočnosť kauzálne spojená s tým, že títo centralizovaní poskytovatelia služieb kryptoaktív poskytujú vo väčšine prípadov aj výmenu kryptoaktív za fiat meny alebo iné finančné prostriedky, resp. nástroje trhu. [7]

[6] LP/2024/86 Zákon o niektorých povinnostiach a oprávneniach v oblasti kryptoaktív a o zmene a doplnení niektorých zákonov. (online, cit. 04.04.2024). Dostupné na internete: <https://www.slov-lex.sk/legislativne-procesy/-/SK/LP/2024/86>

[7] The Chainalysis 2024 Crypto Crime Report. (online, cit. 04.04.2024). Dostupné na internete: <https://go.chainalysis.com/crypto-crime-2024.html>

Riziko legalizácie výnosov z trestnej činnosti prostredníctvom centralizovaných poskytovateľov služieb kryptoaktív:



Pravdepodobnosť a vplyv, teda miera rizika bola určená na základe týchto skutočností:

- Viac než 50% všetkých kryptoaktív, ktoré boli identifikované ako výnosy z trestnej činnosti boli prijímané centralizovanými poskytovateľmi služby kryptoaktív
- Legalizovanie trhu s kryptoaktívami so sebou prinesie väčšie množstvo identifikovaných centralizovaných poskytovateľov služby kryptoaktív
- Povoľovacie konanie zníži latentnosť v oblasti prevádzkovania činností pozostávajúce z faktického vykonávania činností v systéme kryptoaktív
- Nárast centralizovaných poskytovateľov priamo úmerne súvisí s nárastom transakcií súvisiacich s kryptoaktívami a teda logicky aj s nárastom transakcií kryptoaktív súvisiacich s trestnou činnosťou
- Legalizované výnosy z trestnej činnosti ovplyvňujú okrem hospodárskej stability a ekonomickej rovnováhy v podnikateľskom prostredí aj výkyv (rozdiel) miery životnej úrovne jednotlivcov, čo negatívne vplýva jednak na spravodlivú podnikateľskú súťaž, ale aj na životnú úroveň jednotlivých obyvateľov Slovenskej republiky[89]

Legislatívne opatrenia:

- Základná a zvýšená starostlivosť poskytovateľov služieb zmenárne a peňaženky virtuálnej meny vo vzťahu k svojmu klientovi v zmysle zákona o legalizácii prináša okrem

[8] Štatistika kriminality v Slovenskej republike za rok 2023. (online, cit. 04.04.2024). Dostupné na internete: <https://www.minv.sk/?statistika_kriminality_v_slovenskej_republike_za_rok_2023_xml>

[9] Záverečná správa z druhého národného hodnotenia rizík legalizácie výnosov z trestnej činnosti a financovania terorizmu. (online, cit. 04.04.2024). Dostupné na internete: <https://www.minv.sk/swift_data/source/policia/fsj_biro/nhr/Zaverecna%20sprava%20z%20druheho%20NHR.pdf>

identifikácie klientov a overení ich identifikácie aj posudzovanie konečných užívateľov výhod, vykonávanie monitorovania obchodného vzťahu medzi klientom a poskytovateľom, zisťovanie a uchovávanie informácií o klientovi, čo sťažuje, no neznemožňuje proces legalizácie výnosov z trestnej činnosti

- Zisťovanie, ohlasovanie, zdržanie neobvyklej obchodnej operácie podľa zákona o legalizácií predstavuje potenciál profylaktického pôsobenia na ohrozenie zákonného platobného styku
- Legálne vymedzenie príslušnosti, pôsobnosti a úloh oprávnených orgánov a bezpečnostných zborov Slovenskej republiky v oblasti predchádzania, odhaľovania, objasňovania a vyšetrovania legalizácie výnosov z trestnej činnosti podľa viacerých osobitných právnych predpisov[10], najmä však oprávnenia Finančnej spravodajskej jednotky vynucovať plnenie povinností vyplývajúcich pre povinné osoby zo zákona o legalizácii
- Administratívnoprávna a trestnoprávna ochrana pred legalizáciou výnosov z trestnej činnosti, resp. jej predeterminantom ako je napr. neoprávnené podnikanie nesplnenie povoľovacej, ohlasovacej alebo oznamovacej povinnosti atď.
- Podrobné opatrenia vyplývajúce z primárneho práva Európskej únie reprezentujúce sa v sekundárnom práve Európskej únie, najmä v nariadení MiCA, ako je stanovenie podmienok výkonu činností služieb kryptoaktív, podrobnosti povoľovacieho konania, opatrení pri výkyvoch a priebežných nesúladoch ako je stanovenie ozdravného plánu pre poskytovateľov služieb kryptoaktív, ukotvenie oprávnení príslušných orgánov napr. pozastaviť alebo zakázať centralizovaným poskytovateľom služieb kryptoaktív vykonávať ich činnosť
- Špeciálne opatrenie vyplývajúce z nariadenia MiCA predstavujúce výrazný zásah do činností poskytovateľov služieb kryptoaktív ako je odstránenie prístupu vybraného klienta k online rozhraniu poskytovateľa služby kryptoaktív, odstránenie hostingových služieb k online rozhraniu alebo vymazanie domény poskytovateľa
- Legislatívne opatrenia Nariadenia Európskeho parlamentu a Rady (EÚ) 2023/1113 z 31. mája 2023 o údajoch sprevádzajúcich prevody finančných prostriedkov a určitých kryptoaktív a o zmene smernice (EÚ) 2015/849, ktoré rozširujú rozsah povinností pre poskytovateľov služieb kryptoaktív pri zabezpečovaní prevodov kryptoaktív

[10] Zákon č. 171/1993 Z.z. o Policajnom zbore, Zákon č. 46/1993 Z.z. o Slovenskej informačnej službe, Zákon č. 215/2004 Z.z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov, Zákon č. 500/2022 Z.z. o Vojenskom spravodajstve, Zákon č. 483/2001 Z.z. o bankách a o zmene a doplnení niektorých zákonov...

Z uvedeného vyplýva, že síce sa zdá právny rámec a legislatívne opatrenia európskeho práva dostatočne obšírne a všeobímajúce, miera rizika tomuto stavu nezodpovedá. Usudzovaním možno dospieť k domnienke, že sú jednotlivé opatrenia nepostačujúce, nezrozumiteľné alebo ťažko vykonateľné. Je potrebné si však uvedomiť aj skutočnosť aktuálnosti tejto právnej úpravy a súvisiacich opatrení, spolu s rigidným procesom prijímania, osvojovania, prípravy uplatňovania, samotnej realizácie, hodnotenia účinnosti a vplyvov jednotlivých právnych noriem, čoho relevantné ale hlavne skúmateľne výsledky možno očakávať až v priebehu nadchádzajúceho obdobia. Pre efektívny výkon právnych noriem je potrebná štruktúra a systematickosť, ktorú nie je možné dosiahnuť v krátkom časovom období. Negatívne na túto skutočnosť môže vplývať aj častá a razantná zmena právnych noriem, ktorá ovplyvňuje aj proces riadenia a adaptácie práve vo výkonných zložkách štátu. Efektívny výkon opatrení vo vzťahu k poskytovateľom služieb kryptoaktív pôsobí na jednotlivé vzťahy vznikajúce v oblasti systému kryptoaktív. Na to, aby výkon právnych noriem a opatrení pozitívne ovplyvnil mieru rizika legalizácie výnosov z trestnej činnosti je potrebná systematickosť a štruktúra typická viac než krátkodobým charakterom. Je preto dôležité eliminovať všetky negatívne javy, ktoré túto systematickosť a štruktúru narúšajú, resp. nedovolia jej efektívnemu vzniku. Častú zmenu personálneho aparátu, zmenu pôsobnosti, príslušnosti, oprávnení, povinností orgánov vykonávajúcich pripravené, platné a sčasti účinné právne normy, považujeme za takýto negatívny jav.

Poznáme chránené objekty, poznáme aj to, čo narúša ich celistvosť, disponujeme nástrojmi a prostriedkami, ktorými možno vplývať na ochranu týchto objektov, máme vyčlenené zdroje, zabezpečme teda, aby ďalším krokom bola dlhodobá, súvislá, systematická a štruktúrovaná realizácia činností. Prezumujeme, že takýmto spôsobom spojeným s následnou medzinárodnou spoluprácou, sa miera rizika legalizácie výnosov trestnej činnosti súvisiaca s centralizovanými poskytovateľmi služieb kryptoaktív zníži na takú úroveň, aby sa na tento účel použité zdroje mohli presunúť do prestížnejších oblastí. [11]

2. DECENTRALIZOVANÍ POSKYTOVATELIA SLUŽBY KRYPTOAKTÍV

Narozdiel od centralizovaných poskytovateľov služieb kryptoaktív, ktorých prevádzkovanie zabezpečuje určitý subjekt definovaný právom, teda fyzická osoba, právnická osoba, podnikateľský subjekt alebo povinná osoba s pomerne jasne stanovenou spôsobilosťou disponovať právami a povinnosťami, je prevádzkovanie služieb kryptoaktív

[11] ŠANTA, J. – HUSÁK, M.: Virtuálne meny a trestná činnosť s nimi súvisiaca – I.; Kriminalistika, LVII, 2024, č 1, s. 6-10, ISSN 1210-9150

decentralizovanými poskytovateľmi zabezpečené samostatne prvkami technológie distribuovanej databázy transakcií. Táto technológia umožňuje relatívne samostatné, automatizované prevádzkovanie služieb kryptoaktív bez prítomnosti správcu, resp. centralizovaného sprostredkovateľa. Relatívne samostatné preto, pretože tak ako každý prevádzkovaný systém, aj decentralizované poskytovanie služieb kryptoaktív je podmienené určitým externalitám. V tomto prípade sú to požiadavky technológie distribuovanej databázy transakcií a požiadavky, ktoré musí spĺňať táto technológia pre svoju funkčnosť, teda jednoducho hardvérovo-softvérové riešenia zabezpečujúce prenos informácií. Pri samostatnosti je však dôležité pripomenúť, že takéto poskytovanie služieb nie je v skutočnosti podmienené ani spravované jednou entitou. Automatizované poskytovanie alebo prevádzkovanie decentralizovaných služieb kryptoaktív vyplýva z technologického charakteru systému kryptoaktív. Forma poskytovaných služieb sa výrazne nelíši od poskytovania služieb centralizovanými poskytovateľmi služby kryptoaktív, zahŕňajú automatizované a decentralizované poskytovanie obchodovania kryptoaktív, známeho aj ako „trading“, poskytovanie pôžičiek, poskytovanie zábezpek za využívanie kryptoaktíva jednej distribuovanej databázy transakcií v druhej distribuovanej databáze transakcií, poskytovanie anonymizačných služieb transakcií kryptoaktív, poskytovanie agregácie dopytov a ponúk rôznych decentralizovaných poskytovateľov služieb kryptoaktív, poskytovanie tokenizácie, teda prepájania údajov z bežného prostredia do prostredia systému kryptoaktív a podobne. [12] Tieto činnosti možno zväčša podmieniť definovaným službám kryptoaktív podľa nariadenia MiCA. Decentralizovaní poskytovatelia majú v distribuovanej databáze transakcií formu programových riešení prijímajúcich vstupy s predom určeným spracovaním informácií a s nadväzujúcimi výstupmi bez predpokladaného odklonu od účelu ich zdrojového kódu. To znamená, že okrem prvkov technológie distribuovanej databázy transakcií neexistuje entita, ktorá manuálne ovplyvňuje chod tohto programu, resp. aplikácie. Vzhľadom na skutočnosť, že legálne poňatie decentralizovaných poskytovateľ služieb kryptoaktív nie je v súčasnosti na dohľad, je potrebné pri ich poznávaní vychádzať z ich technologickej podstaty. Decentralizovaných poskytovateľov služieb kryptoaktív možno chápať ako poskytovateľov služieb kryptoaktív iba v širšom zmysle, pretože poskytovateľom služby kryptoaktív sa striktne rozumie iba právnická osoba alebo iný podnik, ktorého povolanie alebo podnikateľská činnosť spočíva v poskytovaní jednej alebo viacerých služieb kryptoaktív klientom na profesionálnom základe, a ktorý má povolenie poskytovať služby kryptoaktív. Decentralizovaní poskytovatelia

[12] Illicit FInance Risk Assessment of Decentralized Finance. (online, cit. 13.04.2024). Dostupné na internete: < https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf>

služieb kryptoaktív často nemajú formu ani právnických osôb, ani podnikov, ale pokiaľ bude absentovať špeciálna právna úprava decentralizovaných poskytovateľov služieb kryptoaktív (na ktorej potrebu poukazuje odborná verejnosť už približne od roku 2020), považujeme za dôležité analogicky pristupovať k normám upravujúcim centralizovaných poskytovateľov a uplatňovať ich aj na decentralizovaných poskytovateľov, ak je to je logicky možné a morálne zosúladené. Obraciame sa však v tomto prípade viac na právne normy sekundárneho európskeho práva, ktoré oproti nášmu vnútroštátnemu právnemu poriadku prinášajú dynamickejšie a účel dosiahnuteľnejšie opatrenia. Samotná technologická stránka decentralizovaných poskytovateľov služieb kryptoaktív pozostáva z princípov decentralizovaných aplikácií, smart kontraktov, ktorých účelom je realizovanie takzvaného decentralizovaného finančníctva (ďalej aj „DeFi“)[13]. Samozrejme, akýkoľvek produkt, a teda aj program, aplikácia, smart kontrakt, transakcia má svojho iniciátora, tvorcu, majiteľa, resp. správcu, ktorému možno za určitých podmienok pripísať zodpovednosť za chod svojho produktu a vyžadovať od neho splnenie povinností, resp. sankcionovať porušenie právnych noriem. Berúc do úvahy fakt, že smart kontrakt alebo aplikácia DeFi, teda v našom ponímaní decentralizovaný poskytovateľ služby kryptoaktív, nie je po jeho vytvorení a umiestnení do distribuovanej databázy transakcií viac v moci takto určenej zodpovednej osoby, sankcionovanie osoby nezmení protiprávny stav navodený fungovaním decentralizovaného poskytovateľa služby kryptoaktív. Za účelom nápravy protiprávneho stavu je preto potrebné prispôsobiť opatrenia technológii distribuovanej databázy transakcií. Aktuálny stav kriminality súvisiacej s decentralizovanými poskytovateľmi služieb kryptoaktív však nemožno ignorovať, preto do momentu vytvorenia samostatného špeciálneho rámca pre decentralizovaných poskytovateľov služieb kryptoaktív bude nevyhnutné analogicky pristupovať k právnym normám určených centralizovaným poskytovateľom služby kryptoaktív a realizovať už platné a účinné opatrenia.[14] Výsledky výskumnej činnosti analytických spoločností zaoberajúcimi sa zhromažďovaním, triedením a selektovaním informácií vyplývajúcich z jednotlivých distribuovaných databáz transakcií poukazujú na zvyšujúci sa trend využívania decentralizovaných poskytovateľov služieb kryptoaktív za účelom legalizovania výnosov z trestnej činnosti. Decentralizovaní poskytovatelia služieb kryptoaktív, ktorí vykonávajú

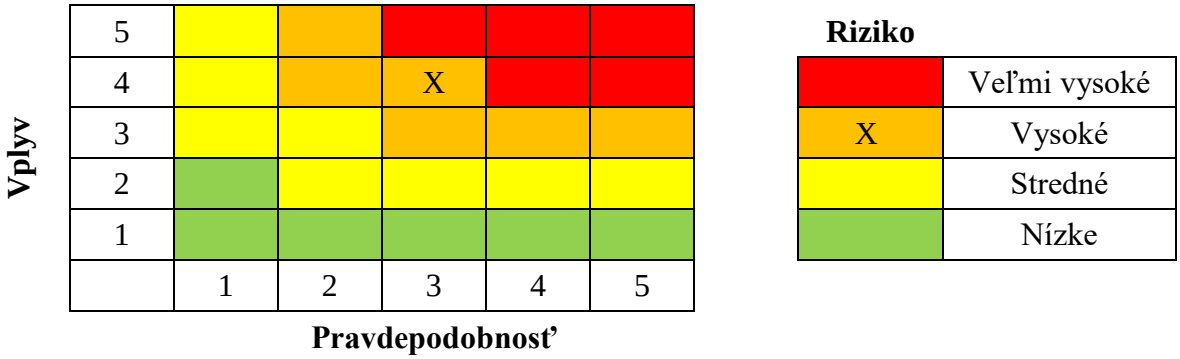
[13] XUE, Y., FAN, D., SU, S., FU, J., HU, N. ET AL. (2024). A Review on the Security of the Ethereum-Based DeFi Ecosystem. CMES-Computer Modeling in Engineering & Sciences, 139(1), 69–101. https://doi.org/10.32604/cmes.2023.031488

[14] WEINGÄRTNER, T., FASSER, F., REIS SÁ DA COSTA, P., FARKAS, W. Deciphering DeFi: A Comprehensive Analysis and Visualization of Risks in Decentralized Finance. J. Risk Financial Manag. 2023, 16, 454. https://doi.org/10.3390/jrfm16100454

činnosti výmeny kryptoaktíva za iné kryptoaktíva v roku 2022 prijali na svoje verejné adresy kryptoaktíva identifikované ako výnosy z trestnej činnosti, v približnom prepočte na fiat menu Euro, v hodnote viac než 2 miliardy Eur. Za rok 2023 možno konštatovať, že sa táto celková hodnota zvýšila na približne 3,5 miliardy Eur. Pôvod kryptoaktív bol identifikovaný najmä v predikatívnej trestnej činnosti majetkového charakteru, ako sú podvodné konania alebo krádeže.[15] Práve takáto predikatívna trestná činnosť v súvislosti s legalizáciou výnosov z trestnej činnosti je významným problémom aj v Slovenskej republike. Je potrebné spomenúť, že páchateľ trestnej činnosti, ktorý pre legalizáciu výnosov zo spáchanej trestnej činnosti využil decentralizovaných poskytovateľov služieb kryptoaktív, sa ich využitím nestáva nedosiahnuteľným ani nepostihnuteľným[16]. O samotnom priamom oprávnenom zásahu za účelom nápravy protiprávneho stavu u decentralizovaného poskytovateľa služieb kryptoaktív v distribuovanej databáze transakcií však v našich podmienkach zatiaľ možno len polemizovať.

Fundament: Stúpajúci trend kryptoaktív identifikovaných ako výnosy z trestnej činnosti legalizovaných prostredníctvom decentralizovaných poskytovateľov služieb kryptoaktív vzhľadom na absenciu špeciálneho právneho rámca a súvisiacich opatrení technologického charakteru predstavuje ohrozenie platobnej stability doposiaľ nepoznanými metódami a prostriedkami.

Riziko legalizácie výnosov z trestnej činnosti prostredníctvom decentralizovaných poskytovateľov služieb kryptoaktív:



[15] The State of Cross-chain Crime 2023. (online, cit. 05.04.2024). Dostupné na internete: < https://www.elliptic.co/resources/state-of-cross-chain-crime-2023>

[16] Former Security Engineer For International Technology Company Pleads Guilty To Hacking Two Decentralized Cryptocurrency Exchanges. (online, cit. 05.04.2024). Dostupné na internete: < https://www.justice.gov/usao-sdny/pr/former-security-engineer-international-technology-company-pleads-guilty-hacking-two?mkt_tok=NTAzLUZBUC0wNzQAAAGSRLzA5kUuBwjm333ZdfD0Fs2KKMNGde6ucMq25Rer31UwRTyCi1OeYUSXw250rqs7XYP5KSSTSMPUV4q95cdQ2crI_IYEH9lBk553YndAE4GT>

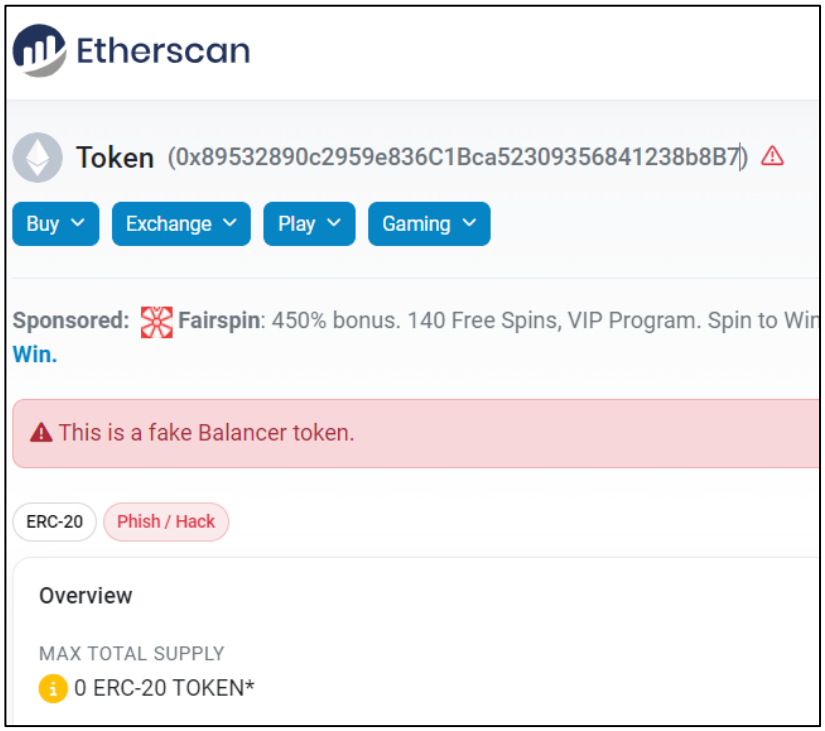
Pravdepodobnosť a vplyv, teda miera rizika bola určená na základe týchto skutočností:

- Ku dňu 13.04.2024 existuje viac než 6 000 decentralizovaných poskytovateľov služieb kryptoaktív s viac než siedmimi miliónmi verejných adries, ktoré boli aktívne aspoň raz za 24 hodín, vykonávajúce činnosť najmä v distribuovaných databázach ako je Ethereum Virtual Machine, Tron, Binance Smart Chain, Solana, Arbitrum, Polygon, Avalanche, Base, Optimism, Bitcoin a pod.
- Celková hodnota kryptoaktív uzamknutých v protokoloch decentralizovaných poskytovateľov služieb kryptoaktív v prepočte na fiat menu Euro tvorí ku dňu 13.04.2024 viac než 80 miliárd Eur, pričom hodnota prevádzaných, obchodovaných kryptoaktív je násobne vyššia[17]
- Poskytovanie obdobných služieb kryptoaktív a vykonávanie obdobných činností ako sú činnosti centralizovaných poskytovateľov služieb kryptoaktív a to automatizovane a bez sprostredkovateľa
- Takmer 100%-tný nárast hodnoty legalizovaných výnosov z trestnej činnosti vo forme kryptoaktív prostredníctvom decentralizovaných poskytovateľov služieb kryptoaktív zabezpečujúcich výmenu kryptoaktív za iné kryptoaktíva, resp. obchodovanie kryptoaktív
- Viac než 100%-tný nárast hodnoty legalizovaných výnosov z trestnej činnosti vo forme kryptoaktív prostredníctvom decentralizovaných poskytovateľov služieb kryptoaktív zabezpečujúcich poskytovanie zábezpek za využívanie kryptoaktíva jednej distribuovanej databázy transakcií v druhej distribuovanej databáze transakcií[18]
- Absencia špeciálnej právnej úpravy dotýkajúcej sa špecifík decentralizovaných poskytovateľov služieb kryptoaktív. Decentralizovaní poskytovatelia služieb kryptoaktív, ktorí sú plne decentralizovaní a automatizovaní nepodliehajú priamo rozsahu nariadenia MiCA.[19]

Legislatívne opatrenia:

[17] Total Value Locked. (online, cit. 13.04.2024). Dostupné na internete: < https://defillama.com/>
[18] The State of Cross-chain Crime 2023. (online, cit. 05.04.2024). Dostupné na internete: < https://www.elliptic.co/resources/state-of-cross-chain-crime-2023>
[19] BENSON, V., ADAMYK, B., CHINNASWAMY, A. et al. Harmonising cryptocurrency regulation in Europe: opportunities for preventing illicit transactions. Eur J Law Econ (2024). https://doi.org/10.1007/s10657-024-09797-w

- Primerané použitie opatrení nariadenia MiCA vyplývajúce z článku 94, ktorých aplikáciu možno fakticky dosiahnuť, najmä opatrení podľa písmena aa), teda odstránenie obsahu alebo obmedzenie prístupu k online rozhraniu, resp. nariadenie výslovného zobrazenia upozornenia klientom a držiteľom kryptoaktív pri prístupe k online rozhraniu. V distribuovanej databáze transakcií nie je možné úplne obmedziť prístup k využívaniu tohto decentralizovaného poskytovateľa služby kryptoaktív, avšak je možné realizovať



Obrázok 2: Výslovné zobrazenie upozornenia u vybraného decentralizovaného poskytovateľa služby kryptoaktív

Zdroj: <https://etherscan.io/token/0x89532890c2959e836C1Bca52309356841238b8B7>

spomenuté zobrazenie upozornenia. Takéto upozornenie je možné vykonať v súčinnosti s webovými sídlami poskytujúcimi vyhľadávanie v transakciách distribuovaných databáz transakcií ako je napr. www.blockchair.com, www.walletexplorer.com, alebo www.etherscan.io. Ako príklad uvádzame decentralizovaného poskytovateľa služby kryptoaktív „LP Balancer“ reprezentovaný verejnou adresou 0x89532890c2959e836C1Bca52309356841238b8B7 pri jeho vyhľadaní v distribuovanej databáze transakcií prostredníctvom webového sídla Etherscan.io (obr.1)

- Primerané použitie opatrení nariadenia MiCA vyplývajúce z článku 105, ktorých aplikáciu možno fakticky dosiahnuť

Záver

Miera rizika centralizovaných a decentralizovaných poskytovateľov služieb kryptoaktív je vzhľadom na aktuálny trend trestnej činnosti súvisiacej so systémom kryptoaktív v oboch prípadoch hodnotená ako vysoká. Pravdepodobnosť využívania centralizovaných poskytovateľov služieb kryptoaktív za účelom legalizovania výnosov z trestnej činnosti kauzálne súvisí s aktuálnym trendom vývoja metód a techník, ktoré sú aplikované pri legalizovaní výnosov z trestnej činnosti z globálneho hľadiska. Analýzou transakcií distribuovanej databázy transakcií jednotlivých kryptoaktív najmä analytickými spoločnosťami bolo zistené, že hlavným prijímateľom kryptoaktív ako výnosov z trestnej činnosti sú verejné adresy centralizovaných poskytovateľov služieb kryptoaktív. Uvedené možno potvrdiť aj z praktickej činnosti oprávnených orgánov. Vplyv tohto nelegálneho konania je síce vysoký, no v nasledujúcom období sa predpokladá jeho zníženie, najmä vzhľadom na opatrenia sekundárneho práva Európskej únie. Celková očakávaná miera rizika môže mať klesajúci charakter iba za dodržania systematickej a štruktúrovanej, zdrojmi doplnenej činnosti oprávnených orgánov.

Takto pozitívne však nemožno hodnotiť mieru rizika súvisiacu s decentralizovanými poskytovateľmi služieb kryptoaktív, ktorí majú charakter samostatných, automatizovaných entít nespadajúcich priamo pod žiadne aktuálne platné legislatívne opatrenia. Pravdepodobnosť využívania decentralizovaných poskytovateľov služieb kryptoaktív pre účely legalizácie výnosov z trestnej činnosti nie je na takej úrovni ako tomu je v prípade centralizovaných poskytovateľov. Výsledky analýz distribuovaných databáz transakcií síce hovoria, že v absolútnych číslach nedochádza k tak častým a objemným prevodom kryptoaktív označeným ako výnosy z trestnej činnosti na verejné adresy decentralizovaných poskytovateľov služieb kryptoaktív, no početnosť týchto prevodov má rastúcu tendenciu. DeFi sektor je stále považovaný za nový technologický aspekt, aktuálne s mnohými technickými nedokonalosťami. Usudzujeme, že nárastom stability DeFi protokolov dôjde postupom času k výraznému implementovaniu prvkov DeFi páchateľmi trestnej činnosti majetkového charakteru. Vplyv využívania decentralizovaných poskytovateľov služieb kryptoaktív pri narúšaní ekonomickej, hospodárskej a platobnej stability jednotlivcov a spoločnosti, považujeme za vysoký, najmä z dôvodu absencie špeciálnej právnej úpravy, ktorá by ukotvila decentralizovaných poskytovateľov služieb kryptoaktív z fundamentálneho hľadiska a nastavila vhodné opatrenia na riešenie potenciálneho vzniknutého protiprávneho stavu. Prvý centralizovaný poskytovateľ

služby kryptoaktív Bitcoinmarket vznikol v roku 2010[20], následné prijatie komplexnej legislatívy legalizujúcej centralizovaných poskytovateľov služieb kryptoaktív bolo uvedené do platnosti v roku 2023. Tempo aktuálneho pokroku elektronických technológií, digitálnych finančných produktov a umelej inteligencie výrazne presahuje schopnosť včasnej a efektívnej reakcie zo strany orgánov verejnej moci. Vzhľadom na uvedené možno konštatovať, že celková miera rizika spojená s decentralizovanými poskytovateľmi služieb kryptoaktív bude mať v najbližšej budúcnosti rastúci charakter. Považujeme preto za nevyhnutné venovať svoju pozornosť tomuto alternatívnemu fenoménu nie len v legislatívnej, výkonnej ale aj výskumnej oblasti. Prijímané opatrenia, ktoré sú reagovaním na už vzniknuté problémy nemusia byť najmä v tejto oblasti postačujúce. Odporúčame čo najskôr pristúpiť k *pro futuro* opatreniam predpokladajúcim budúci stav.

Zoznam použitej literatúry

ŠANTA, J., ŠANTA, I.: Virtuálne meny - trestnoprávne a niektoré analyticko-ekonomické aspekty. Praha: Leges, 2023. 199 strán. ISBN: 978-80-7502-668-2

ŠANTA, J. – ŠANTA, I.: K niektorým legislatívnym a ekonomickým aspektom virtuálnych mien v legislatíve Európskej únie a Slovenskej republiky; Justičná revue, 74, 2022, č 2, s. 164 – 179. ISSN 1335-6461

ŠANTA, J. – HUSÁK, M.: Virtuálne meny a trestná činnosť s nimi súvisiaca – I.; Kriminalistika, LVII, 2024, č 1, s. 3-27, ISSN 1210-9150

The Chainalysis 2024 Crypto Crime Report. (online, cit. 04.04.2024). Dostupné na internete: <https://go.chainalysis.com/crypto-crime-2024.html>

The State of Cross-chain Crime 2023. (online, cit. 05.04.2024). Dostupné na internete: < https://www.elliptic.co/resources/state-of-cross-chain-crime-2023>

Illicit FInance Risk Assessment of Decentralized Finance. (online, cit. 13.04.2024). Dostupné na internete: < https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf>

BENSON, V., ADAMYK, B., CHINNASWAMY, A. et al. Harmonising cryptocurrency regulation in Europe: opportunities for preventing illicit transactions. Eur J Law Econ (2024). https://doi.org/10.1007/s10657-024-09797-w

[20] What Was the First Crypto Exchange?. (online, cit. 13.04.2024). Dostupné na internete: < https://www.cryptohopper.com/blog/what-was-the-first-crypto-exchange-449>

XUE, Y., FAN, D., SU, S., FU, J., HU, N. et al. (2024). A Review on the Security of the Ethereum-Based DeFi Ecosystem. CMES-Computer Modeling in Engineering & Sciences, 139(1), 69–101. https://doi.org/10.32604/cmes.2023.031488

WEINGÄRTNER, T., FASSER, F., REIS SÁ DA COSTA, P., FARKAS, W. Deciphering DeFi: A Comprehensive Analysis and Visualization of Risks in Decentralized Finance. J. Risk Financial Manag. 2023, 16, 454. https://doi.org/10.3390/jrfm16100454

Kontaktné údaje

Andrej Lipták

Odbor finančného vyšetrovania

Národná centrála osobitných druhov kriminality

Račianska 45, 812 72 Bratislava

andrej.liptak@minv.sk

andrej.liptak@akademiapz.sk

Recenzenti:
prof. RNDr. Michal Greguš, CSc.
doc. RNDr. Tatiana Hajdúková, PhD.

Vybrané aspekty kybernetickej bezpečnosti

Iveta Novotná

Abstrakt: Súčasný, vysoko dynamický vývoj ľudskej spoločnosti, zvlášť v oblasti informačných a komunikačných technológií, systémov a prostriedkov, sprevádzaný rýchlo prebiehajúcou informatizáciou a digitalizáciou jednotlivých sektorov, rozširujúcou sa dostupnosťou internetu a masovým využívaním najrôznejších platforiem širokej škály sociálnych sietí, priniesol okrem množstva pozitív aj množstvo negatív. Viaceré z nich sa veľmi úzko týkajú problematiky bezpečnosti, osobitne kybernetickej bezpečnosti, a preto autorka v tejto súvislosti prináša vo svojom príspevku niektoré vybrané informácie týkajúce sa tejto vysoko špecifickej oblasti.

Kľúčové slová: Kybernetická bezpečnosť, kyberpriestor, kybernetické hrozby, kybernetické útoky, obrana a ochrana.

Abstract: The current, highly dynamic development of human society, especially in the field of information and communication technologies, systems and means, accompanied by the rapid informatization and digitization of individual sectors, the expanding availability of the Internet and the mass use of various platforms of a wide range of social networks, has brought, in addition to a number of positives, also a number of negatives. Many of them are very closely related to the issue of security, especially cyber security, and therefore the author brings in his contribution some selected information related to this highly specific area.

Keywords: Cyber security, cyber space, cyber threats, cyber-attacks, defence, and protection.

Úvod

Súčasný, vysoko dynamický vývoj ľudskej spoločnosti, zvlášť v oblasti informačných a komunikačných technológií, systémov a prostriedkov, sprevádzaný rýchlo prebiehajúcou informatizáciou a digitalizáciou jednotlivých sektorov, rozširujúcou sa dostupnosťou internetu a masovým využívaním najrôznejších platforiem širokej škály sociálnych sietí[21], priniesol

[21] Viac pozri v: BREZULA, J. 2018. Vývoj kybernetickej bezpečnosti vzhľadom na nové hrozby v súčasnosti. In *Tradície a dynamika vývoja manažmentu a informatiky z pohľadu univerzít s bezpečnostným zameraním – zborník príspevkov*. Bratislava : Akadémia policajného zboru, 2018; IVANČÍK, R. 2022. Kybernetická (ne)bezpečnosť a sociálne siete. In *Aktuálne výzvy kybernetickej bezpečnosti : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2022, s. 35-46; HAJDÚKOVÁ, T. a kol. 2023. Riziká komunikácie na sociálnych sieťach. In *Reprodukcia ľudského kapitálu - vzájomné väzby a súvislosti*, 2023, s. 58-69; IVANČÍK, R. 2023. Šírenie hoaxov cestou sociálnych sietí – hrozba pre súčasnú demokratickú spoločnosť. In Bezpečnosť elektronickej komunikácie : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou. Bratislava : Akadémia Policajného zboru, 2023, s. 45-56; ZACHAR KUCHTOVÁ, J. 2022. Bezpečnosť na sociálnych sieťach. In *Bezpečnosť elektronickej komunikácie : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2022, s. 237-247.

okrem množstva pozitívnych stránok aj množstvo negatívnych[22]. Viaceré z nich sa veľmi úzko týkajú problematiky bezpečnosti, osobitne kybernetickej bezpečnosti[23].

Kým vo fyzickom priestore sa môžeme pri zaisťovaní bezpečnosti, obrane a ochrane proti rozličným zlomyseľným aktérom spoľahnúť na desaťročia skúseností, počas ktorých sme vymysleli a prijali veľké množstvo príslušných zákonov, noriem, smerníc a predpisov, ktoré upravujú, čo je zákonné (prijateľné) a čo je nezákonné (neprijateľné) a okrem toho máme k dispozícii množstvo technických prostriedkov na zabezpečenie vlastnej obrany a ochrany nášho majetku, v kybernetickom priestore (ďalej len „kyberpriestor“) sme stále v procese učenia sa, ako zabezpečiť našu bezpečnosť, obranu a ochranu v tomto priestore.

Čo je vlastne kyberpriestor? Je to pojem pre označenie virtuálneho sveta vytváraného modernými technológiami (počítačmi, telekomunikačnými sieťami a pod.) paralelne ku svetu reálnemu (fyzickému).[24] Iná definícia hovorí, že je to priestor dát existujúcich v elektronickej podobe, prepojený do sietí, ktorý vznikol prostredníctvom elektronických médií a celosvetový rozmer získal internetom. Prostredníctvom počítačov, tabletov, mobilných telefónov a iných komunikačných sietí sa stal súčasťou každodenného života.[25]

Kyberpriestor sa taktiež stal nástrojom na označenie virtuálneho sveta vytvoreného sieťovými počítačovými systémami, ktoré ovplyvňujú veľké časti našich životov; pričom jeho zabezpečenie je veľmi náročné. Nielenže je na internet pripojených veľa zariadení, ale existuje

---

[22] Viac pozri v: HAJDÚKOVÁ, T. 2022. Zneužívanie elektronických služieb na sexuálne zneužívanie detí. In *Bezpečnosť elektronickej komunikácie – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru v Bratislave, 2022, s. 71-85; IVANČÍK, R. 2020. Cyber Threats as One of the Most Serious Asymmetric Security Threats in 21st Century. In *Košická bezpečnostná revue / Košice Security Revue*, 2020, roč. 10, č. 1, s. 10-23; HAJDÚKOVÁ, T. – BACIGÁL, I. 2014. Hrozby kybernetického priestoru pre deti v období dospievania. In *Policajná teória a prax*. Bratislava : Akadémia Policajného zboru v Bratislave, 2014, roč. 22, č. 3, s. 5-19; alebo TOMÁŠEK, R. – TOMÁŠEKOVÁ, L. 2020. Kybernetické hrozby a kybernetický terorizmus. In *Aktuálne výzvy kybernetickej bezpečnosti – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2020, s. 146-152.

[23] Viac pozri v: HROMADA, M. 2017. Kybernetická bezpečnosť. In Lukáš, L. a kol.: *Teória bezpečnosti I*. Zlín : Radim Bačuvčík – VeRBuM, 2017, s. 123-133; FRIANOVÁ, V. 2020. Kybernetická bezpečnosť ako jeden z „vedľajších produktov“ investovania štátu do obrany, ľudských zdrojov, výskumu a vývoja In *Aktuálne výzvy kybernetickej bezpečnosti : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2020, s. 17-22; IVANČÍK, R. 2012. Kybernetická bezpečnosť – neoddeliteľná súčasť národnej a medzinárodnej bezpečnosti. In *Národná a medzinárodná bezpečnosť 2012 : zborník príspevkov z medzinárodnej vedeckej konferencie*. Liptovský Mikuláš : Akadémia ozbrojených síl generála M. R. Štefánika. 2012. s. 173-182; alebo KOLLÁR, D. 2019. Trendy kybernetickej bezpečnosti a jej súčasné výzvy pre spoločnosť. In *Medzinárodné vzťahy 2019: Aktuálne otázky svetovej ekonomiky a politiky – zborník príspevkov z 20. medzinárodnej vedeckej konferencie*, Smolenice, 2019, Ekonomická univerzita v Bratislave, Fakulta medzinárodných vzťahov, roč. 20, s. 565-571.

[24] SKLENÁK, V. 2014. Kyberprostor. In *KTD: Česká terminologická databáze knihovnictví a informační vědy*, 2014

[25] MISTRÍK, E. 2020. Kyberpriestor. In *Slovník.one*, 2020

aj veľa výrobcov, ktorí ich vyrábajú, čím sa zvyšuje množstvo a rozmanitosť systémov tvoriacich kyberpriestor, a tým sa zvyšuje aj pravdepodobnosť zlyhania.[26]

Okrem toho zabezpečenie kyberpriestoru podlieha značným asymetriám. Útočníci si môžu vybrať zo širokej škály prístupov a možností, zatiaľ čo obrancovia musia venovať pozornosť každému detailu a byť pripravení na čokoľvek a kedykoľvek. Úspešné útoky preto nemusia byť nevyhnutne výsledkom nedbanlivosti. Niekedy sú bezpečnostné opatrenia prijaté, bezpečnostné kontroly zavedené, ale nepoužívajú sa správne, napríklad preto, že sú v rozpore s potrebami používateľov. Vzhľadom na tieto ťažkosti je teraz veľký záujem o reaktívnu bezpečnosť, ktorá okrem iného zahŕňa pochopenie, že nemôžeme zabrániť všetkým útokom.[27]

1 Hrozby

V tejto kapitole sa budeme venovať hrozbám v kybernetickom priestore. Predtým, ako sa pojem „kybernetická bezpečnosť“ stal široko používaným, diskusie sa zameriavali najmä na počítačovú bezpečnosť. Cieľom počítačovej bezpečnosti je chrániť majetok. Cenným aktívom v tomto prípade môže byť hardvér (napríklad počítače, notebooky, smartfóny a pod.), softvér a dáta. Tieto aktíva sú vystavené hrozbám, ktoré môžu viesť k ich strate alebo poškodeniu. Počítačová bezpečnosť pozostáva z informačnej bezpečnosti a bezpečnosti systémov. Preto sa budeme v ďalšom texte venovať základným aspektom týchto dvoch oblastí, ktoré tvoria základy kybernetickej bezpečnosti. Kým informačná bezpečnosť sa týka ochrany údajov (potenciálne spracovávaných počítačmi) a akýchkoľvek informácií odvodených z ich interpretácie, v oblasti bezpečnosti systémov sa snažíme zabezpečiť, aby (počítačové) systémy fungovali tak, ako boli navrhnuté; t. j. aby útočníci s nimi nemohli manipulovať.

2 Informačná bezpečnosť

V informačnej bezpečnosti vychádzame z modelu zahŕňajúceho tri základné piliere ochrany: dôvernosť, integritu a dostupnosť. Tento model, ktorý je tiež známy ako triáda CIA (názov odvodený zo začiatočných písmen cieľov v angličtine: C – confidentiality, I – integrity, A – availability) je primárne určený na usmerňovanie politík pre informačnú bezpečnosť v rámci organizácie. V tomto kontexte dôvernosť predstavuje súbor pravidiel, ktoré obmedzujú

[26] CHAN, C. S. 2012. Complexity the Worst Enemy of Security. In *Schneier on Security*, 2012
[27] COLE, E. 2013. The Changing Threat. In *Advanced Persistent Threat*, 2013

prístup k informáciám, integrita je zárukou toho, že informácie sú dôveryhodné a presné, a dostupnosť je zárukou spoľahlivého prístupu k informáciám oprávneným osobám.[28]

Tieto základné ciele ochrany sa vzťahujú tak na dáta v pokoji, t. j. uložené v počítači alebo na papieri, ako aj na dáta v prenose, t. j. keď sa dáta posielajú cez sieť. Definície sa vzťahujú na „neoprávnené“ činnosti, čo znamená, že je stanovené, ktorí aktéri majú mať možnosť interagovať s predmetnými údajmi.

V niektorých scenároch existuje iba jeden oprávnený aktér. Príkladom v kontexte dôvernosti cieľa ochrany je smartfón alebo počítač so šifrovaným úložiskom (niekedy nazývané „šifrovanie celého disku“). V tomto prípade je oprávnený iba vlastník zariadenia. Príkladom cieľovej dostupnosti je zálohovanie údajov tak, aby zostali dostupné aj v prípade zlyhania počítača.

Väčšinou však ide o dvoch alebo niekedy aj o niekoľko oprávnených aktérov. Napríklad dôvernosť cieľa ochrany môže byť dôležitá, keď odosielateľ posiela e-mail konkrétnemu príjemcovi. Dôvernosť je nevyhnutná aj počas online bankovníctva. Tu tiež chceme ochranu integrity pre vymieňané správy, aby sa zabránilo zmenám transakcií.[29]

Okrem obsahu nás môže zaujímať aj identita iných aktérov. Napríklad, ak by sme chceli vedieť, kedy bol sfalšovaný odosielateľ e-mailovej správy. Autenticita cieľa ochrany bráni aktérom vydávať sa za niekoho iného, zvyčajne tým, že ostatným poskytuje prostriedky na overenie deklarovanej identity. Súvisiacim a ešte silnejším cieľom ochrany je nepopierateľnosť, ktorá bráni aktérom popierať, že vykonali konkrétny čin, napríklad odoslaním správy. Autenticita a nepopierateľnosť sú nevyhnutné na to, aby boli aktéri braní na zodpovednosť.[30]

3 Bezpečnosť systémov

Jedna z fundamentálnych otázok, ktoré si je nutné klásť pri zaisťovaní bezpečnosti systému, je: Ako by sme mali navrhnúť systémy, aby poskytovali bezpečnosť údajov, ktoré sú v nich uložené? V dôsledku toho sú tri základné piliere ochrany, ktoré sa sledujú v oblasti bezpečnosti systémov, rovnaké ako v oblasti informačnej bezpečnosti.

[28] CHAI, W. 2021. What is the CIA triad (confidentiality, integrity and availability)? In *TechTarget*, 2021

[29] DNV. 2022. The three-pillar approach to cyber security: Data and information protection. In *DNV Digital Solutions*, 2022

[30] GOLLMANN, D. 2011. *Computer security*. Chichester : John Wiley & Sons, 2011

Často existuje viacero spôsobov, ako dosiahnuť želaný stav. Napríklad dôvernosť možno dosiahnuť šifrovaním údajov alebo kombináciou autentifikácie (vyžadovaním zadania hesla od používateľov) a kontroly prístupu (pravidlá, ktoré určujú, ktorý používateľ má povolený prístup ku konkrétnym súborom). Navrhovanie systémov, ktoré využívajú vhodnú kombináciu bezpečnostných opatrení, pritom nie je vôbec jednoduchá úloha.

Systémová bezpečnosť sa však neobmedzuje len na dosiahnutie informačnej bezpečnosti. Niektoré systémy neobsahujú žiadne obzvlášť zaujímavé údaje. Spoliehame sa však na ne, na ich funkčnosť, a teda správny priebeh procesu. Ak napríklad komponent autentifikačného systému operačného systému obsahuje chybu, útočníci môžu byť schopní ho vypnúť (zabrániť oprávneným používateľom ovládať server) alebo obísť (umožniť neoprávneným používateľom ovládať server). Integrita a dostupnosť sú spoločné piliere ochrany v oblasti bezpečnosti systémov. Zachovanie dôvernosti konkrétneho postupu môže byť cieľom na zabezpečenie duševného vlastníctva.[31]

V oblasti bezpečnosti systémov sú obzvlášť zaujímavé takzvané kybernetické systémy, ktoré ovplyvňujú reálny svet, ako sú semafory, autopiloti, priemyselné roboty a riadiace systémy pre chemické procesy alebo elektrárne. Niektoré z týchto systémov sa považujú za súčasť kritickej infraštruktúry, t. j. ich zlyhania alebo narušenia ich funkčnosti môžu mať výrazný negatívny dopad na spoločnosť. Tvorcovia politík sa preto obávajú, že budúce vojny by sa mohli viesť kybernetickými útokmi na kritické infraštruktúry, aby spôsobili chaos a vyvolali paniku bez toho, aby sa musela použiť fyzická sila.[32] Medzi známe útoky na kybernetické fyzické systémy patrí malvér Stuxnet, ktorý bol použitý na sabotáž iránskeho zariadenia na obohacovanie uránu v roku 2010[33] a útok na ukrajinskú elektráreň v roku 2015.[34]

4 Bezpečnosť

Ohroziť alebo narušiť bezpečnosť systémov, resp. spôsobiť škodu môžu ľudia, ich konanie alebo aj iné než ľudské konanie. Typickými príkladmi nehumánnych udalostí sú rôzne prírodné katastrofy (zemetrasenia, požiare, záplavy, snehové kalamity, zosuvy pôdy, kamenia, pády lavín a pod.), následné výpadky elektrickej energie, poruchy pevných diskov atď. Ľudské

[31] CHAI, W. 2021. What is the CIA triad (confidentiality, integrity and availability)? In *TechTarget*, 2021
[32] WHEELER, T. 2018. Cyberwar, there are no rules. In *Foreign Policy*, 2018
[33] Viac pozri v: LANGNER, R. 2013. To Kill a Centrifuge. A Technical Analysis of What Stuxnet's Creators Tried to Achieve. In *The Langner Group*, 2013
[34] Viac pozri v: ZETTER, K. 2016. Inside the cunning, unprecedented hack of Ukraine's power grid. In *WIRED*, 2013

konanie je buď také, ktoré je neškodné (nespôsobujúce škody, nevyvolávajúce hrozby), alebo úmyselne zlomyseľné, škodlivé. Nezhubné hrozby sú výsledkom nehôd a neúmyselných ľudských chýb, ako je napríklad nesprávne zadanie príkazu, zatiaľ čo zhubné sú úmyselné škodlivé činy, ktoré sú výsledkom zlých ľudských úmyslov.[35]

Zabezpečenie prevádzkyschopnosti systémov počas prírodných katastrof a pri ľudských chybách (t. j. pri neškodných, nezhubných hrozbách) je otázkou bezpečnosti. Bezpečnosť je kľúčová v kyberneticko-fyzikálnych systémoch, kde zlyhanie systému môže poškodiť ľudí. Bezpečnosť má dlhú tradíciu v strojárstve, napríklad v konštrukcii a vo vybavení automobilov a/alebo lietadiel, ktoré obsahujú mnoho kritických systémov navrhnutých pre maximálnu spoľahlivosť.[36]

Na rozdiel od toho sa otázky bezpečnosti zameriavajú na škodlivé činy ľudí, ktoré sa nazývajú útoky. Existujú náhodné útoky a cielené útoky. Pri náhodných útokoch je útočníkom jedno, na koho útočia, pokiaľ chcú od obete niečo získať (ako napríklad vreckoví zlodeji vo fyzickom svete). V elektronickej doméne sú takýmto známym príkladom phishingové podvody. Naproti tomu cielené útoky sú zamerané na konkrétnu obeť. Proti cieleným útokom sa bráni ťažšie ako proti náhodným útokom, pretože útočníci konajú strategicky, premyslene, t. j. môžu dynamicky meniť svoje konanie v reakcii na prijaté bezpečnostné opatrenia.[37]

5 Bezpečnosť ako súčasť manažmentu rizík

Vytváranie softvéru a hardvéru je zložité, náročné a náchylné na chyby. V priemere každých 1000 riadkov kódu obsahuje tri až 20 chýb a dokonca aj dôkladná kontrola kódu zníži tento počet iba o jeden rad.[38] Existujú rôzne spôsoby, ktorými môžu tieto chyby ovplyvniť bezpečnosť systému. Konkrétna realizácia slabosti v konkrétnom produkte sa nazýva zraniteľnosť. Zraniteľnosť je chyba alebo slabina v návrhu, implementácii alebo v prevádzke a správe systému, ktorá by mohla byť zneužitá na porušenie bezpečnostnej politiky systému.[39]

Útok na systém je možný, ak je systém vystavený útočníkovi a ak obsahuje slabiny, ktoré je možné zneužiť. Nedosiahnuteľné systémy nemožno napadnúť a samotná prítomnosť napr. pretečenie vyrovnávacej pamäte v programe nemusí nevyhnutne znamenať, že je

[35] HERRMANN, D. – PRIDÖHL, H. 2020. Basic Concepts and Models of Cybersecurity. In *The Ethics of Cybersecurity*, 2020
[36] Tamtiež.
[37] PFLEEGER, C. P. a kol. 2015. *Security in Computing*. New Jersey : Prentice Hall, 2015
[38] McCONNELL, S. 2014. *Code complete: a practical handbook of software construction*. London : Pearson Education, 2014
[39] SHIREY, R. 2007. Internet security glossary. In *Network Working Group*, 2007

zneužiteľný. Okrem toho skutočnosť, že systém odhaľuje zneužiteľnú zraniteľnosť, neznamená, že útok je nevyhnutný. Pojem riziko zachytáva túto neistotu. Závažnosť rizika je súčinom dopadu útoku na aktívum (zvyčajne v súvislosti s peňažnou stratou) a pravdepodobnosti, že k útoku dôjde. Pravdepodobnosť útoku závisí od expozície a využiteľnosti, ale aj od otázky, či má útok požadovaný účinok na dosiahnutie cieľa protivníka. V praxi je ťažké presne predpovedať dopad a pravdepodobnosť.[40]

Existujú rôzne spôsoby, ako zvládnuť riziká. Po prvé, možno sa vyhnúť rizikám, napr. tým, že sa zdrží implementácia funkcie. Po druhé, riziká sa dajú tiež zmierniť, napr. implementáciou bezpečnostných kontrol (nazývaných aj protiopatrenia), ktoré znižujú pravdepodobnosť a dopad rizika. Po tretie, riziká sa dajú preniesť napr. kúpou poistenia, ktoré kryje prípadné straty. Po štvrté, riziká možno akceptovať, t. j. rozhodnutím pokryť náklady na útok. Ich prijatie môže mať zmysel pre riziká, ktoré sú veľmi nepravdepodobné.[41]

V praxi sa dizajnéri systémov často pokúšajú preniesť riziká na používateľov systému, čím vytvárajú takzvanú negatívnu externalitu. Prenos rizík je uskutočniteľný z dôvodu asymetrického pomeru výkonu medzi návrhármi systému a používateľmi. Táto situácia je problematická, pretože prevádzkovatelia systému môžu mať menšiu motiváciu brať bezpečnosť vážne, keď sa dopad útokov netýka ich, ale niekoho iného.[42]

6 Útočníci a ich motívy

Aby bol útok úspešný, útočník potrebuje pracovnú metódu, príležitosť na útok a motív. Akí útočníci existujú a aké sú ich motívy? Vo väčšine prípadov rovnakí ako vo fyzickom svete a rovnaké sú aj ich motívy. Firemní špióni napríklad vykonávajú kybernetické útoky na organizácie, aby získali ich obchodné tajomstvá. Existujú aj počítačoví zločinci, jednotlivci alebo skupiny, ktorých cieľom je finančný zisk. Jednou z metód ich činnosti je držanie svojich obetí na výkupnom, a to buď inštaláciou ransomvéru do ich počítačov, vyhrážaním sa zverejnením citlivých informácií alebo hrozbou vykonania útoku odmietnutia služby. Najpokročilejšími útočníkmi sú národné štáty, ktoré majú napríklad za cieľ ovplyvňovať politiku u protivníka alebo rozširovať svoju moc. Národné štáty môžu viesť veľmi sofistikované útoky, ktoré si vyžadujú veľa finančných zdrojov. Mnohé útoky zo strany národných štátov

[40] HERRMANN, D. – PRIDÖHL, H. 2020. Basic Concepts and Models of Cybersecurity. In *The Ethics of Cybersecurity*, 2020

[41] SHOSTACK, A. 2014. *Threat modeling: designing for security*. Indianapollis : John Willey & Sons, 2014

[42] HERRMANN, D. – PRIDÖHL, H. 2020. Basic Concepts and Models of Cybersecurity. In *The Ethics of Cybersecurity*, 2020

dosahujú úroveň pokročilej perzistentnej hrozby (Advanced Persistent Threat), t. j. útoku, ktorý zahŕňa pokročilé techniky, ktoré umožňujú útočníkovi skrytú kompromitáciu a potenciálne aj kontrolu systémov obete na dlhé časové obdobia.[43]

Okrem týchto „profesionálnych" útočníkov existujú aj tzv. ‚script kiddies', čo je pojem, ktorý sa vzťahuje na nekvalifikovaných útočníkov, ktorí sú schopní na svoje útoky použiť iba nástroje pripravené na spustenie. Okrem toho existujú hacktivisti, ktorí útočia na podporu veci a vytvárajú publicitu, napríklad v podobe slobody prejavu a anti-sledovania. Ale sú tu aj nečestní hackeri, ktorí väčšinou útočia na systémy zo zvedavosti. Existujú tiež hackeri, ktorí útočia pre osobný zisk. Vysmievajú sa zo svojich obetí znehodnocovaním ich webových stránok, chvália sa svojimi schopnosťami vo svojej komunite a môžu dokonca predávať citlivé údaje na čiernom trhu.[44]

Termín „čierne klobúky" sa používa pre útočníkov so zlomyseľnými motívmi. Naproti tomu „hackeri s bielymi klobúkmi" majú záujem o zlepšenie celkovej bezpečnosti. Všetky zistené zraniteľnosti hlásia príslušným prevádzkovateľom systému.[45]

Bežná prax zanedbáva insiderov, ktorí majú oveľa lepšie príležitosti na útok ako outsideri. Môžu to byť firemní nelojálni zamestnanci (používatelia alebo prevádzkovatelia) v konkrétnej organizácii. Komplexný pohľad insiderov by mal zahŕňať aj všetkých zamestnancov, ktorí pracujú u predajcov, t. j. dodávateľov, ktorí poskytujú nástroje používané v rámci danej organizácie. V minulosti došlo k niekoľkým pokusom zaútočiť na vysoko postavené ciele infikovaním ich predajcov malvérom. Tento prístup, ktorý sa nazýva útok na dodávateľský reťazec, je dosť silný a je ťažké ho odhaliť.[46]

Záver

Rastúce využívanie informačných a komunikačných technológií vo všetkých sférach či sektoroch moderného života súčasnej ľudskej spoločnosti robí svet bohatším, efektívnejším a interaktívnejším miestom. Zvyšuje to však aj jeho krehkosť, pretože posilňuje našu závislosť od informačných a komunikačných technológií, systémov, prostriedkov a zariadení, ktoré nikdy nemôžu byť úplne bezpečné. Preto sa kybernetická bezpečnosť stala predmetom celosvetového

[43] WESTFIELD, E. 2023. What Are Advanced Persistent Threats? In *HackerOne*, 2023
[44] ELGART, R. 2019. The Data Black Market: Where Hackers Take Stolen Data? In *Turn-Key Technologies*, 2019
[45] HERRMANN, D. – PRIDÖHL, H. 2020. Basic Concepts and Models of Cybersecurity. In *The Ethics of Cybersecurity*, 2020
[46] KOROLOV, M. 2021. Supply chain attacks show why you should be wary of third-party providers. In *CSO News*, 2021

záujmu a významu. V súlade s tým môžeme v dnešnom diskurze o kybernetickej bezpečnosti pozorovať takmer neustály dôraz na kontinuálne rastúci a rôznorodý súbor hrozieb, od širokej škály počítačových vírusov až po najrôznejšie sofistikované druhy kybernetických útokov, kybernetického zločinu či kybernetickej špionáže, až po kybernetický teror a kybernetickú vojnu. Táto rastúca zložitosť digitálneho ekosystému v kombinácii s rastúcimi globálnymi hrozbami a rizikami vytvorila dilemu. Prílišné zdôrazňovanie kybernetickej bezpečnosti môže na jednej strane porušovať základné hodnoty, akými sú rovnosť, spravodlivosť, sloboda alebo súkromie, na druhej strane, zanedbanie kybernetickej bezpečnosti by mohlo podkopať dôveru občanov v digitálnu infraštruktúru, v tvorcov politík a v štátne orgány a inštitúcie. Preto je nevyhnutné naďalej veľmi intenzívne pokračovať nielen v odhaľovaní a eliminácii širokej škály škodlivých aktivít a v aktívnom prijímaní celého radu opatrení za účelom zvyšovania úrovne kybernetickej bezpečnosti v praktickej rovine, ale aj v skúmaní udalostí, javov, procesov a incidentov odohrávajúcich v kybernetickom priestore na akademickej úrovni.

Zoznam použitej literatúry

ANDRÁSSY, V. 2022. Informácie v bezpečnostnom systéme. In *Bezpečnosť elektronickej komunikácie – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava: Akadémia Policajného zboru, 2022, s. 98-107. ISBN 978-80-8054-968-8.

BREZULA, J. 2018. Vývoj kybernetickej bezpečnosti vzhľadom na nové hrozby v súčasnosti. In *Tradície a dynamika vývoja manažmentu a informatiky z pohľadu univerzít s bezpečnostným zameraním – zborník príspevkov*. Bratislava: Akadémia policajného zboru, 2018. ISBN 978-80-8054-773-8.

COLE, E. 2013. The Changing Threat. In *Advanced Persistent Threat*, 2013. [online] [cit. 29.04.2024] Dostupné na: <https://doi.org/10.1016/B978-1-59-749949-1.00001-2>.

DNV. 2022. The three-pillar approach to cyber security: Data and information protection. In *DNV Digital Solutions*, 2022. [online] [cit. 29.10.2023] Dostupné na: <https://www.dnv.com/article/the-three-pillar-approach-to-cyber-security-data-and-information-protection-165683>.

ELGART, R. 2019. The Data Black Market: Where Hackers Take Stolen Data? In *Turn-Key Technologies*, 2019. [online] [cit. 28.04.2024] Dostupné na: <https://www.turn-keytechnologies.com/blog/article/the-data-black-market-where-hackers-take-stolen-data>.

GOLLMANN, D. 2011. *Computer security*. Chichester : John Wiley & Sons, 2011. 464 s. ISBN 978-0-470-74115-3.

HAJDÚKOVÁ, T. – BACIGÁL, I. 2014. Hrozby kybernetického priestoru pre deti v období dospievania. In *Policajná teória a prax*. Bratislava : Akadémia Policajného zboru v Bratislave, 2014, roč. 22, č. 3, s. 5-19. ISSN 1335-1370.

HAJDÚKOVÁ, T. 2022. Zneužívanie elektronických služieb na sexuálne zneužívanie detí. In *Bezpečnosť elektronickej komunikácie – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2022, s. 71-85. ISBN 978-80-8054-968-8.

HAJDÚKOVÁ, T. – KURILOVSKÁ, L. – MARR, S. 2023. Riziká komunikácie na sociálnych sieťach. In *Reprodukcia ľudského kapitálu - vzájomné väzby a súvislosti*, 2023, s. 58-69. ISBN 978-80-245-2499-3.

HERRMANN, D. – PRIDÖHL, H. 2020. Basic Concepts and Models of Cybersecurity. In *The Ethics of Cybersecurity*, s. 11-44. Cham : Springer, 2020. ISBN 978-3-030-29055-9.

HROMADA, M. 2017. Kybernetická bezpečnosť. In Lukáš, L. a kol.: *Teória bezpečnosti I*. Zlín : Radim Bačuvčík – VeRBuM, 2017, s. 123-133. ISBN 978-80-87500-89-7.

CHAI, W. 2021. What is the CIA triad (confidentiality, integrity and availability)? In *TechTarget*, 2021. [online] [cit. 29.04.2024] Dostupné na: <https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA>.

CHAN, C. S. 2012. Complexity the Worst Enemy of Security. In *Schneier on Security*, 2012. [online] [cit. 28.04.2024] Dostupné na: <https://www.schneier.com/news/archives/2012/12/complexity_the_worst.htmlr>.

IVANČÍK, R. 2012. Kybernetická bezpečnosť – neoddeliteľná súčasť národnej a medzinárodnej bezpečnosti. In *Národná a medzinárodná bezpečnosť 2012 : zborník príspevkov z medzinárodnej vedeckej konferencie*. Liptovský Mikuláš : Akadémia ozbrojených síl generála M. R. Štefánika. 2012. s. 173-182. ISBN 978-80-8040-450-5.

IVANČÍK, R. 2020. Cyber Threats as One of the Most Serious Asymmetric Security Threats in 21st Century. In *Košická bezpečnostná revue / Košice Security Revue*, 2020, roč. 10, č. 1, s. 10-23. ISSN 1338-6956.

IVANČÍK, R. 2022. Kybernetická (ne)bezpečnosť a sociálne siete. In *Aktuálne výzvy kybernetickej bezpečnosti: zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2022, s. 35-46. ISBN 978-80-8054-998-5.

IVANČÍK, R. 2023. Šírenie hoaxov cestou sociálnych sietí – hrozba pre súčasnú demokratickú spoločnosť. In *Bezpečnosť elektronickej komunikácie : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2023, s. 45-56. ISBN 978-80-8054-997-8.

KOLLÁR, D. 2019. Trendy kybernetickej bezpečnosti a jej súčasné výzvy pre spoločnosť. In *Medzinárodné vzťahy 2019: Aktuálne otázky svetovej ekonomiky a politiky – zborník príspevkov z 20. medzinárodnej vedeckej konferencie*, Smolenice, 2019, Ekonomická univerzita v Bratislave, Fakulta medzinárodných vzťahov, roč. 20, s. 565-571. ISBN 978-80-225-4686-7.

KOROLOV, M. 2021. Supply chain attacks show why you should be wary of third-party providers. In *CSO News*, 2021. [online] [cit. 31.04.2024] Dostupné na internete: <https://www.csoonline.com/article/561323/supply-chain-attacks-show-why-you-should-be-wary-of-third-party-providers.html>.

KUCHTOVÁ, J. 2018. Aktuálne trendy súvisiace s využívaním moderných technológií. In *Aktuálne výzvy kybernetickej bezpečnosti – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2018, s. 90-98. ISBN 978-80-8054-773-8.

KUCHTOVÁ, J. 2019. Digitálna stopa ako základ kybernetickej bezpečnosti. In *Aktuálne výzvy kybernetickej bezpečnosti (v podmienkach bezpečnostných zložiek)*. Bratislava : Akadémia Policajného zboru, 2019, s. 97-101. ISBN 978-80-8054-819-3.

LANGNER, R. 2013. To Kill a Centrifuge. A Technical Analysis of What Stuxnet's Creators Tried to Achieve. In *The Langner Group*, 2013. [online] [cit. 30.04.2024] Dostupné na internete: <https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf>.

McCONNELL, S. 2014. *Code complete: a practical handbook of software construction*. London : Pearson Education, 2014. ISBN 978-0-17853-022-2.

MISTRÍK, E. Kyberpriestor. In *Slovník.one*, 2020. [online] [cit. 28.04.2024] Dostupné na: <https://www.slovnik.one/kyberpriestor>.

PFLEEGER, C. P. – PFLEEGER, S. L. – MARGULIES, J. 2015. *Security in Computing*. New Jersey : Prentice Hall, 2015. 310 s. ISBN 978-0-1323-9077-4.

SHIREY, R. 2007. Internet security glossary. In *Network Working Group*, 2007. [online] [cit. 30.10.2023] Dostupné na: <https://datatracker.ietf.org/doc/html/rfc4949>.

SHOSTACK, A. 2014. *Threat modeling: designing for security*. Indianapollis : John Willey & Sons, 2014. 224 s. ISBN 978-1-118-81005-7.

SKLENÁK, V. Kyberprostor. In *KTD: Česká terminologická databáze knihovnictví a informační vědy*, 2014. [online] [cit. 28.04.2024] Dostupné na: <http://aleph.nkp.cz/F/?func=direct&doc_number=000000626&local_base=KTD>.

WESTFIELD, E. 2023. What Are Advanced Persistent Threats? In *HackerOne*, 2023. [online] [cit. 31.04.2024] Dostupné na: <https://www.hackerone.com/knowledge-center/advanced-persistent-threats-attack-stages-examples-and-mitigation>.

WHEELER, T. 2018. Cyberwar, there are no rules. In Foreign Policy, 2018. [online] [cit. 30.04.2024] Dostupné na: <https://foreignpolicy.com/2018/09/12/in-cyberwar-there-are-no-rules-cybersecurity-war-defense/>.

ZACHAR KUCHTOVÁ, J. 2022. Bezpečnosť na sociálnych sieťach. In *Bezpečnosť elektronickej komunikácie : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2022, s. 237-2477. ISBN 978-80-8054-968-8.

ZETTER, K. 2016. Inside the cunning, unprecedented hack of Ukraine's power grid. In *WIRED*, 2013. [online] [cit. 30.04.2024] Dostupné na: <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/>.

Kontaktné údaje

JUDr. Iveta Novotná
Akadémia ozbrojených síl generála M. R. Štefánika
Externá doktorandka na Katedre bezpečnosti a obrany
Demänová 393, 031 01 Liptovský Mikuláš
e-mail: iveta.novotna3@gmail.com

Recenzenti:

prof. RNDr. Michal Greguš, CSc.
doc. RNDr. Tatiana Hajdúková, PhD.

Práva dotknutých osôb pri spracúvaní osobných údajov na internete
Rights of data subjects in the processing of personal data on the internet

Miriam Odlerová

Abstrakt: Neustálym vývojom techniky je internet stále viac integrovaný do našich životov a naše osobné údaje sú zbierané, spracovávané a využívané rôznymi spôsobmi. Poznanie svojich práv v tejto oblasti dáva fyzickým osobám moc a kontrolu nad tým, ako sú ich údaje používané, a umožňuje im ochrániť ich súkromie. Poznanie a uplatňovanie svojich práv taktiež vedieť k zodpovednejšiemu správaniu prevádzkovateľov, čo je dôležitý faktor pri zvyšovaní dôvery a bezpečnosti online prostredia.

Kľúčové slová: práva dotknutých osôb, osobné údaje, zverejňovanie osobných údajov, súhlas dotknutej osoby, právo na súkromie, právo na ochranu osobnosti

Abstract: With the continuous advancement of technology, the internet is becoming increasingly integrated into our lives, and our personal data is being collected, processed, and utilized in various ways. Understanding our rights in this domain empowers individuals and grants them control over how their data is used, enabling them to safeguard their privacy. Furthermore, exercising these rights fosters more responsible behavior among data controllers, which serves as a crucial factor in enhancing trust and security within the online environment.

Key words: data subject rights, personal data, disclosure of personal data, consent of the data subject, right to privacy, right to protection of personality

Úvod

V digitálnej ére, ktorú dnes nevyhnutne žijeme, je dôležité, aby ľudia poznali svoje práva týkajúce sa spracúvania osobných údajov, obzvlášť v online prostredí. Internet je miestom, kde sa naše osobné údaje neustále spracúvajú, vrátane ich zdieľania, pričom vývoj kriminality v online prostredí naznačuje, že mnohí ľudia si stále nie sú vedomí rizík spojených s nedostatočnou ochranou svojich údajov.

Poznanie svojich práv v tejto oblasti pritom umožňuje chrániť svoje súkromie, kontrolovať, ako sú osobné údaje využívané a tým predchádzať protiprávnej činnosti. Okrem toho to posilňuje transparentnosť a zodpovednosť prevádzkovateľov webových stránok a aplikácií, čo vedie k vyššej dôvere a bezpečnosti online prostredia pre všetkých. Preto je dôležité, aby neustále prebiehala osveta o právach fyzických osôb, ktoré sa týkajú ich osobných údajov a aby sa tak tieto osoby aktívne podieľali na ochrane svojich osobných údajov (nielen) na internete.

Práva dotknutých osôb

Podľa § 5 písm. n) zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon o ochrane osobných údajov“) sa dotknutou osobou rozumie ***každá fyzická osoba, ktorej osobné údaje sa spracúvajú***. Spracúvaním osobných údajov je spracovateľská operácia alebo súbor spracovateľských operácií s osobnými údajmi alebo so súbormi osobných údajov, najmä získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie, bez ohľadu na to, či sa vykonáva automatizovanými prostriedkami alebo neautomatizovanými prostriedkami.

Práva dotknutých osôb v oblasti ochrany osobných údajov sú dôležité z viacerých dôvodov:

- ***chránia súkromie jednotlivcov:*** Osobné údaje sú citlivé informácie, ktoré môžu odhaliť veľa o živote a identite jednotlivca. Dotknuté osoby tak môžu mať väčšiu kontrolu nad svojimi osobnými údajmi, čo im pomáha chrániť ich pred zneužitím.
- ***podporujú transparentnosť':*** Dotknuté osoby majú právo vedieť, aké osobné údaje o nich prevádzkovatelia zbierajú, ako ich používajú a s kým ich zdieľajú. To pomáha budovať dôveru medzi jednotlivcami a prevádzkovateľmi. Fyzická osoba môže robiť informované rozhodnutia o tom, ako sa s jej údajmi nakladá.
- ***poskytujú jednotlivcom kontrolu nad ich údajmi:*** Práva dotknutých osôb im dávajú právo požadovať od prevádzkovateľa prístup k svojim osobným údajom, ich opravu alebo vymazanie, ako aj obmedzenie ich spracúvania. To umožňuje jednotlivcom uistiť sa, že ich osobné údaje sú presné a aktuálne, a že sa s nimi nakladá spôsobom, ktorý rešpektuje ich súkromie a je v súlade s právnymi predpismi.
- ***podporujú zodpovedné nakladanie s údajmi:*** Dôsledné uplatňovanie práv dotknutých osôb motivuje prevádzkovateľov, aby zodpovedne nakladali s osobnými údajmi a aby zaviedli vhodné bezpečnostné opatrenia na ich ochranu pred neoprávneným prístupom, použitím, zverejnením, zmenou alebo zničením.
- ***posilňujú právne postavenie jednotlivcov:*** Práva dotknutých osôb sú nástrojom na ochranu svojho súkromia a na ochranu pred ich zneužitím, či neoprávneným

spracúvaním. To je obzvlášť dôležité v digitálnom veku, kedy sa osobné údaje zbierajú a spracúvajú o každej osobe vo veľkom rozsahu.

Zakotvenie práv dotknutých osôb v právnych predpisoch má za cieľ vykompenzovať v niektorých aspektoch nerovný vzťah dotknutej osoby a prevádzkovateľa. V zákone o ochrane osobných údajov sú práva dotknutej osoby upravené v druhej hlave, v §§ 19 – 28. Odvíjajú sa od základných zásad spracúvania osobných údajov a zodpovedajú im konkrétne povinnosti prevádzkovateľa. Zaraďujeme sem:

- právo na informácie,
- právo na prístup k osobným údajom,
- právo na opravu osobných údajov,
- právo na výmaz osobných údajov,
- právo na obmedzenie spracúvania osobných údajov,
- právo na prenosnosť osobných údajov,
- právo namietať spracúvanie osobných údajov,
- právo pri automatizovanom individuálnom rozhodovaní vrátane profilovania.

Právo na informácie

Zákon o ochrane osobných údajov rozlišuje situácie, kedy sa spracúvané osobné údaje získavajú priamo od dotknutej osoby (napríklad pri vypĺňaní online formulára) a kedy sa získavajú inak. V závislosti od toho je prevádzkovateľ povinný poskytnúť dotknutej osobe odlišný rozsah informácií, v zásade však ide o informácie ako napr. identifikačné údaje prevádzkovateľa, účel spracúvania osobných údajov, doba uchovávania osobných údajov, práva dotknutých osôb, kategórie spracúvaných osobných údajov, zdroj, z ktorého pochádzajú atď.[1]

Ide o pasívne právo dotknutej osoby, tzn. že prevádzkovateľ poskytuje informácie automaticky bez ich vyžiadania. Ak ide o osobné údaje získané od dotknutej osoby, prevádzkovateľ poskytuje uvedené informácie ihneď, teda už pri získavaní osobných údajov. Ak ale ide o osobné údaje, ktoré nie sú získané od dotknutej osoby, prevádzkovateľ poskytuje tieto informácie nasledovne:

[1] Pozri §§ 19 – 20 zákona o ochrane osobných údajov.

- najneskôr do jedného mesiaca po získaní osobných údajov, pričom zohľadní konkrétne okolnosti, za ktorých sa osobné údaje spracúvajú,
- najneskôr v čase prvej komunikácie s touto dotknutou osobou, ak sa osobné údaje majú použiť na komunikáciu s dotknutou osobou, alebo
- najneskôr vtedy, keď sa osobné údaje prvýkrát poskytnú, ak sa predpokladá poskytnutie osobných údajov ďalšiemu príjemcovi.[2]

Informácie sa teda musia poskytnúť v čase, keď nastane jedna z vyššie uvedených situácií, a to podľa tej situácie, ktorá nastane najskôr. Ak sa napr. prvá komunikácia s dotknutou osobou uskutoční viac ako jeden mesiac po získaní osobných údajov, použije sa prvý odstavec a informácie sa poskytnú najneskôr do jedného mesiaca po získaní osobných údajov. *„Pokiaľ ide o načasovanie poskytovania týchto informácií, včasné poskytnutie týchto informácií je dôležitým prvkom povinnosti týkajúcej sa transparentnosti a povinnosti spravodlivo spracúvať údaje.“*[3]

Existujú však výnimky, kedy prevádzkovateľ tieto informácie dotknutej osobe neposkytuje. Neposkytuje ich v rozsahu, v akom dotknutá osoba už dané informácie má[4], ďalej v rozsahu, v akom sa poskytovanie týchto informácií ukáže ako nemožné alebo by si vyžadovalo neprimerané úsilie, v rozsahu, v akom sa získanie týchto informácií alebo poskytnutie týchto informácií ustanovuje v osobitnom predpise, ktorý sa na prevádzkovateľa vzťahuje a ak osobné údaje musia zostať dôverné na základe povinnosti mlčanlivosti podľa osobitného predpisu[5].

Prevádzkovateľ je povinný plniť informačnú povinnosť aj pri spracúvaní osobných údajov kamerovým systémom. Napr. pri kamere umiestni základné informácie s odkazom na webovú stránku, sekretariát, recepciu, kde už budú uvedené všetky potrebné informácie podľa zákona o ochrane osobných údajov.

Okrem obsahu je dôležitá aj forma a spôsob, akým by sa dotknutým osobám mali poskytovať požadované informácie. Zákon o ochrane osobných údajov ani nariadenie GDPR

[2] § 20 ods. 3 zákona o ochrane osobných údajov.
[3] Pracovná skupina pre ochranu údajov zriadená podľa článku 29: *Usmernenia k transparentnosti podľa nariadenia 2016/679* [online]. [citované 2. mája 2024]. Dostupné na internete: https://dataprotection.gov.sk/files/metod-edpb/10_usmernenia_k_transparentnosti.pdf
[4] V tomto prípade však musí vedieť preukázať, že dotknutej osobe boli transparentne poskytnuté všetky relevantné informácie.
[5] Napr. podľa zákona č. 576/2004 Z. z. o zdravotnej starostlivosti, službách súvisiacich s poskytovaním zdravotnej starostlivosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

nepredpisujú formát alebo postup, akým by sa takéto informácie mali poskytovať dotknutým osobám, ale zodpovednosťou prevádzkovateľa je prijať „primerané opatrenia“ v súvislosti s poskytovaním požadovaných informácií na účely transparentnosti. To znamená, že prevádzkovateľ by mal pri rozhodovaní o primeranom postupe a formáte poskytovania informácií vziať do úvahy všetky okolnosti získavania a spracúvania údajov.[6]

Právo na prístup k osobným údajom

Dotknutá osoba má právo získať od prevádzkovateľa potvrdenie o tom, či sa spracúvajú osobné údaje, ktoré sa jej týkajú. Konkrétne má právo získať prístup k týmto osobným údajom a informácie o účele spracúvania osobných údajov, kategórii spracúvaných osobných údajov, identifikácii príjemcu alebo o kategórii príjemcu, ktorému boli alebo majú byť osobné údaje poskytnuté, najmä o príjemcovi v tretej krajine alebo o medzinárodnej organizácii, ak je to možné, dobe uchovávania osobných údajov; ak to nie je možné, informáciu o kritériách jej určenia, práve požadovať od prevádzkovateľa opravu osobných údajov týkajúcich sa dotknutej osoby, ich vymazanie alebo obmedzenie ich spracúvania, alebo o práve namietať spracúvanie osobných údajov, práve podať návrh na začatie konania, zdroji osobných údajov, ak sa osobné údaje nezískali od dotknutej osoby a existencii automatizovaného individuálneho rozhodovania vrátane profilovania. Dotknutá osoba má tiež právo byť informovaná o primeraných zárukách týkajúcich sa prenosu, ak sa osobné údaje prenášajú do tretej krajiny alebo medzinárodnej organizácii.

Povinnosť prevádzkovateľa reagovať a odpovedať na žiadosť dotknutej osoby by mala byť zachovaná aj v prípade, keď bude právo na prístup dotknutej osoby z niektorého dôvodu obmedzené.[7] Právo na prístup k osobným údajom však nemožno zamieňať s právom na prístup k informáciám, či dokumentom vzhľadom na odlišné ciele, ktoré majú. *„Prvé právo sa týka zaistenia čo možno najväčšej transparentnosti rozhodovacieho procesu orgánov verejnej moci, ako aj informácií, na ktorých sú založené ich rozhodnutia. Jeho cieľom je teda čo najviac uľahčiť výkon práva na prístup k dokumentom a podporiť riadny úradný postup. Druhé právo*

[6] Pracovná skupina pre ochranu údajov zriadená podľa článku 29: *Usmernenia k transparentnosti podľa nariadenia 2016/679* [online]. [citované 2. mája 2024]. Dostupné na internete: https://dataprotection.gov.sk/files/metod-edpb/10_usmernenia_k_transparentnosti.pdf

[7] VALENTOVÁ, T., BIRNSTEIN, M., GOLAIS, J. *GDPR/Všeobecné nariadenie o ochrane osobných údajov. Zákon o ochrane osobných údajov*. Bratislava: Wolters Kluwer, 2018, s. 164.

si kladie za cieľ zabezpečiť ochranu základných práv a slobôd fyzických osôb, predovšetkým ich súkromia, pri spracúvaní osobných údajov.“[8]

Právo na opravu osobných údajov

Dotknutá osoba má právo na to, aby prevádzkovateľ bez zbytočného odkladu opravil nesprávne osobné údaje, ktoré sa jej týkajú. So zreteľom na účel spracúvania osobných údajov má dotknutá osoba právo na doplnenie neúplných osobných údajov. Dotknutá osoba má takéto právo bez ohľadu na to, či na chybu v spracúvaní osobných údajov prišla sama alebo ju zistil prevádzkovateľ.

Toto právo vychádza zo zásady správnosti podľa § 9 zákona o ochrane osobných údajov. Podľa tejto zásady sa musia prijať primerané a účinné opatrenia na zabezpečenie toho, aby sa osobné údaje, ktoré sú nesprávne z hľadiska účelov, na ktoré sa spracúvajú, bez zbytočného odkladu vymazali alebo opravili.

Právo na výmaz osobných údajov

Dotknutá osoba má právo na to, aby prevádzkovateľ bez zbytočného odkladu vymazal osobné údaje, ktoré sa jej týkajú. Prevádzkovateľ je povinný žiadosti dotknutej osoby vyhovieť, ak je naplnený niektorý z dôvodov stanovený v § 23 ods. 2 zákona o ochrane osobných údajov. Prvým dôvodom je, že osobné údaje už nie sú potrebné na účel, na ktorý sa získali alebo inak spracúvali. Toto podporuje aj zásada minimalizácie uchovávania osobných údajov, ktorá hovorí o tom, že osobné údaje musia byť uchovávané vo forme, ktorá umožňuje identifikáciu dotknutej osoby najneskôr dovtedy, kým je to potrebné na účel, na ktorý sa osobné údaje spracúvajú. Ďalším dôvodom je odvolanie súhlasu dotknutej osoby za podmienky, že neexistuje iný právny základ spracúvania osobných údajov.

Vymazať osobné údaje je povinnosťou aj vtedy, keď dotknutá osoba namieta spracúvanie osobných údajov z taxatívne stanovených dôvodov, ďalej keď sa osobné údaje spracúvajú nezákonne, ak je dôvodom pre výmaz splnenie povinnosti podľa zákona o ochrane osobných údajov, osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná, alebo ak sa osobné údaje získavali v súvislosti s ponukou služieb informačnej spoločnosti.

[8] Úrad na ochranu osobných údajov SR: *Často kladené otázky*. [online]. [citované 2. mája 2024]. Dostupné na internete: https://dataprotection.gov.sk/sk/legislativa-metodiky/metodiky-faq/casto-kladene-otazky-faq/

Ak prevádzkovateľ zverejnil osobné údaje a je povinný ich na základe niektorého z vyššie uvedených dôvodov vymazať, je zároveň povinný prijať primerané bezpečnostné opatrenia vrátane technických opatrení so zreteľom na dostupnú technológiu a náklady na ich vykonanie na účel informovania ostatných prevádzkovateľov, ktorí spracúvajú osobné údaje dotknutej osoby, o jej žiadosti, aby títo prevádzkovatelia vymazali odkazy na jej osobné údaje a ich kópie alebo odpisy.

Určitá komplikácia pri uplatňovaní tohto práva môže nastať práve pri zverejňovaní osobných údajov na internete a ich ďalším ne/kontrolovateľným šírením. Pokiaľ by dotknutá osoba požiadala poskytovateľa internetového vyhľadávača o odstránenie odkazov v súlade s uvedeným právom, takýto poskytovateľ v súčasnosti nemá povinnosť vykonať také odstránenie vo všetkých verziách jeho vyhľadávača. Úrad na ochranu osobných údajov Slovenskej repbuliky k tomuto uvádza nasledovné: *„Pokiaľ ide o otázku, či sa také odstránenie odkazov musí vykonať vo verziách vyhľadávača, ktoré zodpovedajú členským štátom, alebo len v jednej verzii tohto vyhľadávača zodpovedajúcej členskému štátu, v ktorom má osoba s nárokom na odstránenie odkazov bydlisko, takéto odstránenie by sa malo v zásade vykonať pre všetky členské štáty. Toto odôvodňuje aj skutočnosť, že normotvorca Únie v súčasnosti stanovil pravidlá v oblasti ochrany údajov nariadením, ktoré sa priamo uplatňuje vo všetkých členských štátoch. Cieľom je zabezpečiť tak konzistentnú a vysokú úroveň ochrany v celej Únii a odstrániť prekážky tokov osobných údajov v rámci Únie (recitál 10 Nariadenia).“*[9] Uvedené podporuje aj Usmernenie 5/2019 ku kritériám týkajúcich sa prípadov uplatňovania práva na zabudnutie vo vyhľadávačoch podľa všeobecného nariadenia o ochrane údajov.

Podľa rozsudku Súdneho dvora Európskej únie vo veci Google Spain SL v. Mario Costeja Conzálex[10] môže dotknutá osoba požiadať poskytovateľa internetového vyhľadávača, aby vymazal jeden alebo viacero odkazov na webové stránky zo zoznamu výsledkov zobrazených po vyhľadávaní vykonanom na základe jej mena. Zámerom Usmernenia 5/2019 je výklad prípadov uplatňovania práva na zabudnutie vo vyhľadávačoch vo vzťahu k ustanoveniam článku 17 GDPR. Právo na zabudnutie bolo v článku 17 GDPR osobitne zakotvené s cieľom zohľadniť právo požadovať vyradenie zo zoznamu, o ktorom bolo rozhodnuté v rozsudku vo veci Google Spain SL v. Mario Costeja Conzález.

[9] Úrad na ochranu osobných údajov SR: *Často kladené otázky*. [online]. [citované 2. mája 2024]. Dostupné na internete: https://dataprotection.gov.sk/sk/legislativa-metodiky/metodiky-faq/casto-kladene-otazky-faq/

[10] Pozri rozsudok Súdneho dvora Európskej únie z 13. mája 2014 vo veci C-131/12 Google Spain SL v. Mario Costeja Conzález.

Aj pre právo na výmaz osobných údajov platia určité výnimky. Prevádzkovateľ nemusí vyhovieť žiadosti o výmaz, ak je spracúvanie osobných údajov potrebné:

- na uplatnenie práva na slobodu prejavu alebo práva na informácie,
- na splnenie povinnosti podľa zákona o ochrane osobných údajov, osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná, alebo na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi,
- z dôvodov verejného záujmu v oblasti verejného zdravia,
- na účel archivácie, na vedecký účel, na účel historického výskumu alebo na štatistický účel, ak je pravdepodobné, že toto právo znemožní alebo závažným spôsobom sťaží dosiahnutie cieľov takého spracúvania, alebo
- na uplatnenie právneho nároku.

Právo na obmedzenie spracúvania osobných údajov

Dotknutá osoba má právo na obmedzenie spracúvania osobných údajov, ak namieta správnosť osobných údajov, a to počas obdobia umožňujúceho prevádzkovateľovi overiť správnosť osobných údajov, ďalej ak spracúvanie osobných údajov je nezákonné a dotknutá osoba namieta vymazanie osobných údajov a žiada namiesto toho obmedzenie ich použitia, ak prevádzkovateľ už nepotrebuje osobné údaje na účel spracúvania osobných údajov, ale potrebuje ich dotknutá osoba na uplatnenie právneho nároku, alebo ak dotknutá osoba namieta spracúvanie osobných údajov, a to až do overenia, či oprávnené dôvody na strane prevádzkovateľa prevažujú nad oprávnenými dôvodmi dotknutej osoby.

Ak prevádzkovateľ obmedzí spracúvanie osobných údajov na základe žiadosti dotknutej osoby, takéto osobné údaje môže spracúvať iba s jej súhlasom alebo na účel uplatnenia právneho nároku, na ochranu osôb alebo z dôvodov verejného záujmu.

Pri uplatnení práva na opravu, výmaz alebo obmedzenie spracúvania osobných údajov má prevádzkovateľ oznamovaciu povinnosť, v rámci ktorej je povinný oznámiť každému príjemcovi, ktorému boli osobné údaje poskytnuté, každé obmedzenie spracúvania, ak sa to neukáže ako nemožné alebo si to nebude vyžadovať neprimerané úsilie. Ak to dotknutá osoba požaduje, prevádzkovateľ ju o týchto príjemcoch informuje.[11]

[11] § 25 zákona o ochrane osobných údajov.

Právo na prenosnosť osobných údajov

Dotknutá osoba má právo získať osobné údaje, ktoré sa jej týkajú a ktoré poskytla prevádzkovateľovi, v štruktúrovanom, bežne používanom a strojovo čitateľnom formáte a má právo preniesť tieto osobné údaje ďalšiemu prevádzkovateľovi, ak je to technicky možné a ak

sa osobné údaje spracúvajú na základe jej súhlasu alebo je spracúvanie osobných údajov nevyhnutné na plnenie zmluvy, ktorej zmluvnou stranou je dotknutá osoba, alebo na vykonanie opatrenia pred uzatvorením zmluvy na základe žiadosti dotknutej osoby a spracúvanie osobných údajov sa vykonáva automatizovanými prostriedkami. Uplatnenie tohto práva však nesmie mať nepriaznivé dôsledky na práva iných osôb. To znamená, že ak si dotknutá osoba uplatní právo na prenosnosť údajov, je prevádzkovateľ povinný skúmať, či osobné údaje obsahujú aj údaje o iných fyzických osobách a či by sa ich prenesením nezasiahlo neprimerane do ich práv. Prevádzkovateľ je povinný vedieť preukázať, že pred prenesením osobných údajov posúdil všetky relevantné okolnosti.

„Právo na prenosnosť je novým právom priznaným dotknutej osobe, ktoré má posilniť jej kontrolu nad vlastnými osobnými údajmi a umožniť jej získať osobné údaje, ktoré sa jej týkajú a ktoré poskytla prevádzkovateľovi v štruktúrovanom, bežne používanom a strojovo čitateľnom formáte. Aj keď úzko súvisí s právom na prístup, odlišuje sa od neho. Cieľom práva na prenosnosť osobných údajov je uľahčiť dotknutým osobám premiestňovanie, kopírovanie, či preskupovanie vlastných osobných údajov z jedného informačného prostredia do druhého (či už do vlastných systémov, systémov dôveryhodných tretích strán alebo systémov nových prevádzkovateľov).“[12]

Právo namietať spracúvanie osobných údajov

Dotknutá osoba má právo namietať spracúvanie osobných údajov z dôvodov týkajúcich sa jej konkrétnej situácie a ak:

- je spracúvanie osobných údajov nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi,
- je spracúvanie osobných údajov nevyhnutné na účel oprávnených záujmov prevádzkovateľa alebo tretej strany,

[12] VALENTOVÁ, T., BIRNSTEIN, M., GOLAIS, J.*GDPR/Všeobecné nariadenie o ochrane osobných údajov. Zákon o ochrane osobných údajov*. Bratislava: Wolters Kluwer, 2018, s. 175 – 176.

- sa spracúvanie uskutočňuje na účel priameho marketingu vrátane profilovania v rozsahu, v akom súvisí s priamym marketingom,
- sa spracúvanie uskutočňuje na vedecký účel, na účel historického výskumu alebo na štatistický účel s výnimkou prípadov, keď je spracúvanie nevyhnutné na plnenie úlohy z dôvodov verejného záujmu.

Na toto právo je prevádzkovateľ povinný dotknutú osobu výslovne upozorniť najneskôr pri prvej komunikácii s ňou, pričom informácia o tomto práve musí byť uvedená jasne a oddelene od akýchkoľvek iných informácií.

Právo pri automatizovanom individuálnom rozhodovaní vrátane profilovania

Dotknutá osoba má právo na to, aby sa na ňu nevzťahovalo rozhodnutie, ktoré je založené výlučne na automatizovanom spracúvaní osobných údajov vrátane profilovania a ktoré má právne účinky, ktoré sa jej týkajú alebo ju obdobne významne ovplyvňujú.

Profilovanie je akákoľvek forma automatizovaného spracúvania osobných údajov spočívajúceho v použití osobných údajov na vyhodnotenie určitých osobných znakov alebo charakteristík týkajúcich sa fyzickej osoby, najmä na analýzu alebo predvídanie znakov alebo charakteristík dotknutej osoby súvisiacich s jej výkonnosťou v práci, majetkovými pomermi, zdravím, osobnými preferenciami, záujmami, spoľahlivosťou, správaním, polohou alebo pohybom

Automatizované rozhodovanie predstavuje možnosť rozhodovať výlučne technologickými prostriedkami na základe ľubovoľného druhu údajov, pričom nie je podstatné, či je takéto rozhodovanie výsledkom posúdenia údajov poskytnutých samotnými jednotlivcami, vypozorovaných, odvodených či vyvodených dát, ale dôležitá je skutočnosť, že ide o rozhodnutie bez ľudského zásahu.[13]

Aj tu zákon o ochrane osobných údajov stanovuje výnimky. Takéto právo nemá dotknutá osoba, ak je rozhodnutie nevyhnutné na uzavretie zmluvy alebo plnenie zmluvy medzi dotknutou osobou a prevádzkovateľom, alebo je vykonané na základe osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná, a v ktorých sú zároveň

[13] VALENTOVÁ, T., ŽUĽOVÁ, J., ŠVEC, M. *Nové pravidlá ochrany osobných údajov*. Bratislava: Wolters Kluwer, 2018, s. 108.

ustanovené aj vhodné opatrenia zaručujúce ochranu práv a oprávnených záujmov dotknutej osoby, alebo je založené na výslovnom súhlase dotknutej osoby.

Záver

Uvedený rozsah práv dotknutých osôb môže prevádzkovateľ alebo sprostredkovateľ obmedziť za určitých okolností a za podmienok ustanovených osobitným predpisom alebo medzinárodnou zmluvou, ktorou je Slovenská republika viazaná. Takéto obmedzenie sa môže realizovať iba s cieľom zaistiť bezpečnosť alebo obranu Slovenskej republiky, verejný poriadok, plnenie úloh na účely trestného konania, ochranu nezávislosti súdnictva, uplatnenie právneho nároku atď.[14]

Ďalšou dôležitou skutočnosťou, ktorú musí dotknutá osoba poznať pri uplatňovaní svojich práv, je to, či sa na konkrétne spracúvanie osobných údajov vzťahuje zákon o ochrane osobných údajov. Nemôže si teda tieto práva uplatňovať v zmysle § 3 ods. 5 a 6 zákona o ochrane osobných údajov pri spracúvaní osobných údajov fyzickou osobou v rámci výlučne osobnej činnosti alebo domácej činnosti, pri spracúvaní osobných údajov SIS, Vojenským spravodajstvom, NBÚ na účely vykonávania bezpečnostných previerok a na účely zabezpečovania podkladov na rozhodovanie Súdnej rady Slovenskej republiky o splnení predpokladov sudcovskej spôsobilosti a ani pri spracúvaní osobných údajov zosnulých osôb, ku spracovaniu ktorých dochádza na vedecký účel, na štatistický účel, na účel umeleckej činnosti, tlačového spravodajstva, rozhlasového a televízneho vysielania, archivácie, dokumentačnej činnosti, historického výskumu, činností pohrebísk, umiestnenia pamätníkov a pamätných tabúľ, konania spomienkových podujatí a piety v rozsahu nevyhnutnom pre jeho naplnenie.

Podľa § 38 ods. 1 zákona o ochrane osobných údajov má každá osoba, ktorej vznikla majetková ujma alebo nemajetková ujma v dôsledku porušenia zákona o ochrane osobných údajov, ***právo na náhradu škody od prevádzkovateľa alebo sprostredkovateľa***. Prevádzkovateľ, ktorý sa zúčastnil na spracúvaní osobných údajov, je zodpovedný za škodu spôsobenú nezákonným spracúvaním. Sprostredkovateľ zodpovedá za škodu spôsobenú spracúvaním osobných údajov, len ak nesplnil taxatívne stanovené povinnosti.

Pokiaľ sa dotknutá osoba domnieva, že prevádzkovateľ nezákonným spôsobom spracúva jej osobné údaje, alebo inak porušuje predpisy na úseku ochrany osobných údajov,

[14] Pozri § 30 zákona o ochrane osobných údajov.

čím je priamo dotknutá na svojich právach, môže ***podať návrh na začatie konania na Úrad na ochranu osobných údajov Slovenskej republiky*** podľa § 99 a nasl. zákona o ochrane osobných údajov. Účelom tohto konania je zistiť, či došlo k porušeniu práv fyzických osôb pri spracúvaní ich osobných údajov alebo došlo k porušeniu právnych predpisov v oblasti ochrany osobných údajov, a v prípade zistenia nedostatkov, ak je to dôvodné a účelné, uložiť opatrenia na nápravu, prípadne pokutu.

Ochrana osobných údajov je tiež súčasťou ***práva na súkromie a práva na ochranu osobnosti***. Právo na súkromie a právo na ochranu osobnosti obsahujú navyše aj právo na ochranu skutočností, ktoré nie je možné považovať za osobné údaje, ale môže ísť o informácie, ktoré sú určitým spôsob citlivé vzhľadom na konkrétne okolnosti. Podľa § 11 zákona č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov má fyzická osoba právo na ochranu svojej osobnosti, najmä života a zdravia, občianskej cti a ľudskej dôstojnosti, ako aj súkromia, svojho mena a prejavov osobnej povahy. Občiansky zákonník v § 12 ďalej stanovuje, že písomnosti osobnej povahy, podobizne, obrazové snímky a obrazové a zvukové záznamy týkajúce sa fyzickej osoby alebo jej prejavov osobnej povahy sa smú vyhotoviť alebo použiť ***len s jej privolením***. Bez takéhoto privolenia sa môžu vyhotoviť alebo použiť primeraným spôsobom tiež na vedecké a umelecké účely a pre tlačové, filmové, rozhlasové a televízne spravodajstvo. Ani také použitie však nesmie byť v rozpore s oprávnenými záujmami fyzickej osoby.

Realizácia práva na súkromie patrí k tým problematickejším aktom aplikácie práva a to najmä z dôvodu, že nachádzanie konkrétneho obsahu hodnôt súkromia pripomína *„skôr zložitý proces vyvažovania viacerých vzájomne proti sebe stojacich hodnôt či princípov, ktorý nemá jasne vymedzené mantinely a závisí skôr na konkrétnom kontexte, skutkovom deji, ako aj na konkrétnom správaní človeka a jeho očakávaní.“*[15]

Za určitých okolností môže porušenie ochrany osobných údajov ***naplniť skutkovú podstatu trestného činu*** – napr. neoprávnený zásah do počítačového systému podľa § 247a Trestného zákona, neoprávnený zásah do počítačového údaja podľa § 247b Trestného zákona, nebezpečné prenasledovanie podľa § 360a Trestného zákona, nebezpečné elektronické obťažovanie podľa § 360b Trestného zákona, neoprávnené nakladanie s osobnými údajmi podľa § 374 Trestného zákona.

[15] MATEJKA, J. *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí*. Praha: CZ. NIC, 2013, s. 52.

Zoznam použitej literatúry

MATEJKA, J. Internet jako objekt práva: hledání rovnováhy autonomie a soukromí. Praha: CZ. NIC, 2013. ISBN 978-80-904248-7-6.

NAVRÁTIL, J. a kol. GDPR pro praxi. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s. r. o., 2018. ISBN 978-80-7380-689-7.

Pracovná skupina pre ochranu údajov zriadená podľa článku 29: Usmernenia k transparentnosti podľa nariadenia 2016/679 [online]. [citované 2. mája 2024]. Dostupné na internete: https://dataprotection.gov.sk/files/metod-edpb/10_usmernenia_k_transparentnosti.pdf

Úrad na ochranu osobných údajov SR: Často kladené otázky. [online]. [citované 2. mája 2024]. Dostupné na internete: https://dataprotection.gov.sk/sk/legislativa-metodiky/metodiky-faq/casto-kladene-otazky-faq/

VALENTOVÁ, T., BIRNSTEIN, M., GOLAIS, J. GDPR/Všeobecné nariadenie o ochrane osobných údajov. Zákon o ochrane osobných údajov. Bratislava: Wolters Kluwer, 2018. ISBN 978-80-8168-852-2.

VALENTOVÁ, T., ŽUĽOVÁ, J., ŠVEC, M. Nové pravidlá ochrany osobných údajov. Bratislava: Wolters Kluwer, 2018. ISBN 978-80-8168-792-1.

Rozsudok Súdneho dvora Európskej únie z 13. mája 2014 vo veci C-131/12 Google Spain SL v. Mario Costeja González

Zákon č. 300/2005 Z. z. Trestný zákon

Zákon č. 18/2018 o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

Kontaktné údaje

doc. JUDr. Miriam Odlerová, PhD.
Akadémia Policajného zboru v Bratislave
Katedra správneho práva
miriam.odlerova@akademiapz.sk

Recenzenti:

doc. Ing. Václav Friedrich, Ph.D.
doc. RNDr. Tatiana Hajdúková, PhD.

Automated compliance audit for ISO27001:2022 in the Active Directory environment

Martin Pavelka, Ladislav Hudec

Abstract: Active Directory is a widely-used concept for centrally managing the security of Windows infrastructure and access rights. Microsoft Windows provides several configurable options or tools to provide better security level. Many tools are integrated in the operating system, others are freely available online. Both kinds of the tools need proper setup to fulfill the desired out-come. The main goal of this paper is to summarize current possibilities for operating system hardening with accordance to new revision of ISO27001:2022 and introduce our developed tool for automated inspection of Microsoft Windows/Server security controls and settings.

Keywords: Active Directory security, Domain Controller, Information Security, Compliance, Countermeasure

Introduction

The Windows operating system is widespread and is used not only in households, but also in the corporate environment. It gained popularity because of its simplicity in the initial configuration. Right after the installation, the computer's operating system is ready for normal use, and there is no need to immediately perform advanced settings. That´s why it´s a popular target for attackers.

Trying to meet security and legal requirements, companies are giving a huge effort to implement an Information Security Management System and to gain some kind of certification. Current operating systems are implemented in a way that al-lows organizations to easily interconnected computers and servers in computer net-works. Through built-in tools, control panel, and commands, administrators and users have the ability to customize the behavior of the operating system from a visual (setting of graphical effects, easy orientation), performance (tuning performance by optimizing components and programs) and security (control of access rights and adherence to the concepts of a secure information system).

When trying to establish secure (hardened) Active Directory and MS Windows environment, it is needed to think about skills, education and working habits of common users. "*Typically, exploiting less technologically skilled users would be the easiest pathway into a network, as most staff at companies outside of the IT industry will only learn the IT skills required to perform their job effectively.*"[16] [3] These findings are also related to security or

[16] MCDONALD, et al. Ransomware: Analysing the Impact on Windows Active Directory Domain Ser-vices. In: Sensors, vol. 22, no. 3, p. 953, Jan. 2022, doi: 10.3390/s22030953.

operational administrators. They might not have enough knowledge or skills to establish and maintain secure operating system environment. Our statement is also supported by the authors in [3]: "Therefore, do-main controllers that are ideally only operated by trained cyber situational-aware IT professionals should theoretically be less susceptible to threats than devices operated by those less technologically skilled."

In addition to the shortcomings that can occur in an Active Directory domain, we should not neglect the security weaknesses or security bottlenecks of the Windows operating system itself. This is one of the reasons that complex, high-level view is needed when assessing and maintaining secure operating systems environment.

The structure of this paper is organized as follows.

Section 2 deals with the analysis of the new, 2022 revision of ISO/IEC 27001[17] [1] standard.

Section 3 is focused on the selection of some provisions of the ISO27001 standard and its subsequent implementation in the enterprise environment using available tools integrated in the Windows operating system or easily installable components.

Sections 4 and 5 describe ways of countermeasures audit via our own tool.

Selected countermeasures in MS Windows

For the purposes of this paper, it is necessary to focus on selected, specific measures referred to in ISO27001:2022 and the possible approaches to their implementation in MS Windows, which are described in another ISO documents (such as ISO27002). Based on the study of the specialized literature, ex. [4][18], our previous research work and our own experience in the field of MS Windows OS security, we have compiled a table that presents a list of measures and their specific technological implementation in the Windows OS environment.

Our goal is to use and check the kind of countermeasures that will not require commercial, proprietary solutions but will rely on integrated parts of Windows operating system or freely available Microsoft tools. Table 1 provides overview of relevant measures of ISO 27001:2022. Each measure, written in separated row is enhanced by adding possible risks and

[17] INTERNATIONAL STANDARD ORGANIZATION: ISO/IEC 27001:2022 Information technology — Security Techniques — Information Security Management System – Requirements. Genève: ISO, 2022

[18] AUSTRALIAN CYBER SECURITY CENTRE: Hardening Windows 10 Version 21H1 workstations [online]. [cit. 2024-02-02]. Available at: https://www.cyber.gov.au/acsc/view-all-content/publications/hardening-microsoft-windows-10-version-21h1-workstations

more detailed description of measures implementation. Beside provided ideas regarding implementation of measures, there are more ways to accomplish required goal, using more sophisticated techniques and advanced third-party tools but these are out of scope of our work.

Table 1: Overview of ISO27001:2022 measures related to Active Directory and MS Windows

Annex A	*Measure*	*Risk*	*Possible implementation of measures*
5	**Organizational controls**		
5.7	Threat intelligence	Exploit of operating systems and devices by zero-day vulnerability	Windows Defender offers options for cloud sample submission and cloud protection programs. However, we recommend that these options are carefully considered, as it is not customizable which files are sent for analysis (e.g. files containing personal data). Third party antivirus suites (if available) can offer similar functionality.
5.9	Inventory of information and other associated assets	Ignorance of embedded machines in the AD domain – risk of persistence of the attacker, unobserved penetration leading to exfiltration	Active Directory Users and Computers tool might be used to create a hierarchy of organizational units based on the geographic locations of domain elements or user accounts. This hierarchy can be expanded into device categories (computers, servers, virtual servers, groups, etc.). Particular attention should be paid to keeping a list of discarded or inactive devices (e.g., computer) and user accounts – these need to be deactivated and their passwords changed (user accounts). Printers can be centrally installed on a dedicated server – a print server from which printers are deployed to end users' computers.
5.10	Acceptable use of information and other associated assets	Impossibility to discipline employees without valid and confirmed instruction	The Group Policy setting for displaying a warning message when a user logs on can be used to inform users about information security organization's policies and regulations that they should be aware of, or to remind users of previously formally implemented lessons.
5.15	Access control	Unauthorized access to files and resources Loss of basic CIA (confidentiality, integrity, availability) features	This policy should be based on the principle that what is not allowed is prohibited. Employees should have dedicated accounts according to their work tasks. This is especially important for workers with cumulative functions (such as human resources and payroll). There should be a formal procedure for handling access requests when managing user accounts. It is essential to use the correct classification of the user account and its membership in the Active Directory organizational unit and security groups.
5.16	Identity management	Loss of basic CIA features	The Active Directory domain can be used as the only source of trust and as a central user database. The technology enables the connection of identities from AD to third-party services (including Single-Sign-On integration).
5.17	Authentication information	Using shared accounts does not meet activity accountability requirements.	Common users should be able to change their password according to password complexity rules.

		Some passwords may become inconvenient over time, e.g. they may be cracked. Lack of reactive and proactive password control	It is necessary to carefully consider the expiration of the password, because the more often it is necessary to change the password, the higher is the probability of writing the password, e.g. on a sticker. Every user must use their own account and password. Password policy can be addressed through Group Policy for password complexity combined with user security training to avoid selecting a weak password. MS Windows does not provide proactive password control by default. If necessary, it is needed to use external third-party solutions for password change with proactive password control.
5.18	Access rights	Abuse of user account access rights. Compromise user accounts.	Implementation of the tiering model and the principle of granularity of access rights allocation. Regular review of assigned access rights and their withdrawal in case of reassignment of an employee to another project or other job position.
5.23	Information Security for use of cloud services	Exfiltration of classified information to the cloud service. Exploiting a vulnerability in the cloud service. Overcoming a cloud service security measure with a compromised user account. Compromises of cloud service provider services (blame is not on the part of the user or customer)	Establishing a directive and enforcing compliance with it in the area of classifications of information that can be stored in a cloud service. Create custom settings (if the cloud service allows it) with higher security measures than the default, e.g. enforce two-factor authentication, use geographically based access – geofencing based on IP address blocking, force the use of client certificates, allow the use of cloud service only on devices managed by the organization. Block failed logins. Legislative analysis of cloud service conditions and unambiguous determination of responsibilities for relevant parts and implementation of security measures at all levels. Create an output procedure when there is a need to leave the cloud service provider.
5.30	ICT readiness for business continuity	Unavailability of the domain controller, essential services operated on it	Implementation of continuity plans in Microsoft Windows workstations and Active Directory at both the process and the technical levels. <u>Process level:</u> - Use multiple domain controllers - Dedicated computing power for virtual machines in an external data center - Reduced On-Premise Active Directory and Azure AD interconnection (e.g., cloud and On-Premise AD specific user groups, specific administrator accounts, etc.) - Development of technical continuity plans containing detailed procedures and guidance in case of recovery from backups <u>Technical level:</u> - Set up DNS replication - Effectively set up AD domain replication

			- Use DHCP failover clustering when using this network service on Windows Servers - Using a distributed file system (DFS) to increase the availability of files stored on On-Premise servers
7	**Physical controls**		
7.7	Clear desk and clear screen	Unauthorized persons could gain access to the workstation and active session profile in that user's OS	Use the Group Policy to set a password-protected screen saver after a defined period of inactivity. User education – Lock computers with a keyboard shortcut.
7.10	Storage media	Misuse of information on portable data media	Use of the built-in BitLocker cipher to encrypt portable data media as well as hard drives of computers. Use of application-level encryption, e.g., encryption of ZIP files, MS Office documents, etc.
8	**Technological controls**		
8.1	User end point devices	Loss of basic CIA features	Operating Systems Security – hardening of workstations based on national and international standards.
8.2	Privileged access rights	Misuse of a single administrator user account	Each administrator has at least two accounts: one for regular work (Domain User) and one for Domain Admin. Ideally, implement a tiering model for separate administrator accounts on application servers, domain controllers, and workstations.
8.3	Information security restriction	The user may be assigned higher privileges than necessary for his/her authorized activities	The above recommendations for implementation are applicable.
8.5	Secure authentication	Password compromise in the login process	According to the classification of the workstation and information (e.g., "trusted workstation" for processing personal data – employment contracts), a procedure for secure login should be established. The standard method is to use the name and password of the user account, in case of high classification of information, more secure methods can be used, e.g. USB token and smart card. In Group Policy, the CTRL+ALT+Del policy should be set as required for all user accounts. To log in to the information system, a single sign-on should be implemented using user accounts and Active Directory permissions. LDAP/Directory can be used.
8.7	Protection against malware	Loss of basic features of the CIA. Data exfiltration. Compromise of workstations and servers.	Using an anti-malware solution as a first defense level. Use of an up-to-date virus signature database and automatic updates. Use of sandbox – isolation of suspicious samples during their examination. Use of a cloud-based service to analyze a sample in the cloud. Implement various antimalware solutions on servers and workstations.
8.8	Management of technical vulnerabilities	Exploiting vulnerabilities for which a fix is available.	Use of third-party tools and services that inform about new vulnerabilities (e.g., mailing lists from national Cybersecurity centers).

			At the level of technical measures in the operating system, its regular update is necessary. Use of tools for centralized management of OS updates as well as software. Use Windows Server Update Services to update desktop computers. Setting Group Policy or using a third-party tool for automatic laptop updates. Using third-party tools to update proprietary and freely available applications present in the OS.
8.13	Information backup	Unavailability of information. Compromise backups	Use of tools and scripts to perform backups of servers and workstations. Use of the 3-2-1-1 principle for backups. Use of backup encryption. Use Windows Server Backup for Server Backup. Use Active Directory capabilities to redirect user folders to a server where (hard/Solid State) disk redundancy and backup are used.
8.17	Clock synchronization	Attackers could alter timestamps and compromise the integrity of audit records	The concept of Active Directory itself implements time management, the PDC (Primary Domain Controller) acts as an NTP server for client computers and servers. Set the time and the external NTP (Network Time Protocol) server on the PDC correctly.
8.18	Use of privileged utility programs	Users can change the default standardized operating system environment in the domain, putting the entire infrastructure at risk	User Account Control must be enabled in Group Policy. Users should work using a standard user account without administrator privileges. If a user's task type requires administrator rights, there should be a special, dedicated local user account to switch and perform the necessary task. By default, utilities that change the behavior of the operating system are not available to regular users with standard permissions. Active Directory sets up a new user account exclusively with regular user rights. If needed, third party tools are available to enable local administrator privileges for specific applications and use cases.

Third-party tools might be considered as ready-made solutions covering some of the identified measures.

From our experience, we can confirm that only large enterprises are able to pay for such technologies. Because of that our approach enables smaller and medium sized organizations to build on already or freely available solutions integrated (or easily integrable) in MS Windows environment.

Automated approach when determining the compliance of security measures

Our goal was to provide automated checks of countermeasures using special tool based on MS PowerShell.

ISO standards represent general procedures and conceptually approach for several areas of information security in operating systems but they do not provide specific instructions for resolving technical issues in operating systems and therefore it is necessary for security administrators to deeper review other available sources to provide them a more advanced procedures related to operating systems and Active Directory hardening.

We have created a ready-made solution – tool for automated checking technical settings of operating systems with best-practices based on ISO 27001:2013/2022 enhanced by other relevant information security standards.

Our solution is designed for checking compliance (security audit) for:

1. standalone Microsoft Windows 10/11 workstation,
2. domain-joined Microsoft Windows 10/11 workstation,
3. domain-joined Microsoft Windows 2016/2019/2022 member server,
4. domain controllers running Microsoft Windows 2016/2019/2022.

The tool must be run as local or domain (when using in Active Directory checks scenario) account with administrator privileges. After startup of the tool, several PowerShell scripts are run in the background and as a result a HTML file is created on the user desktop containing audit report. HTML file provides it´s portability and usability on restricted workstations that do not contain more user-friendly tools such as MS Excel or other. Each computer or server has integrated internet browser and thus the user is able to open the HTML file and get acquainted with the resulting findings.

Concept of the tool

When designing the tool, we considered our goal - to find out as accurately as possible the current level of implementation of security measures on the workstation or server. In an Active Directory domain environment, most of the countermeasures are implemented through group policies, but it is advantageous that our solution can also be used for computers not enrolled in the Active Directory domain.

The main part of the tool consists of two PowerShell scripts that represent two possible scenarios – domain controller or workstation mode and the user runs the compliance-action scenario. If we would like to use this script on a Windows member server, then the procedure is the same as for a workstation.

The core of the tool consists of a script designed to collect information, in which calls to the configuration file are used. The configuration file is created in the form of another PowerShell script and consists of a number of references to smaller scripts that are used to detect individual measures. It is in this section that our tool can be expanded with new capabilities – just add a new script that will check the new measure and include this in the tool configuration file.

The tool provides automated checks for countermeasures from several areas, including:

- Access Control (Password Policy, Password Expiration, User accounts, Screensaver, etc.),
- Assets Inventory (Related to Active Directory – number of users, computer, inactive elements, descriptions revealing sensitive information, etc.),
- Cryptographic Controls (Using Bitlocker, Hash algorithms),
- Network Segmentation (IP addresses, NetBIOS protocol, IPv6 protocol),
- Physical Access (Screensaver policy),
- Protection Against Malicious Code and Updates (Privileges, Shares, Updates, Antivirus settings, etc.),
- Security Monitoring (Audit – event log policy).

Since the measures are easily extensible, or each measure is in its own script definition file, it is necessary to have a precise structure of the script result, which will also contain text, which will then be included together with the specific measure in the resulting table of findings.

The structure of the output HTML file consists of a header – basic information, e.g. workstation name, date and time of creation, user name in whose context compliance was detected, etc.

The individual areas or measures are implemented in separate files, the resulting file generally containing the heading of the relevant section, a description of the component verified and the result of the verification.

We have created Figure 1 to demonstrate the proposed auditing process.

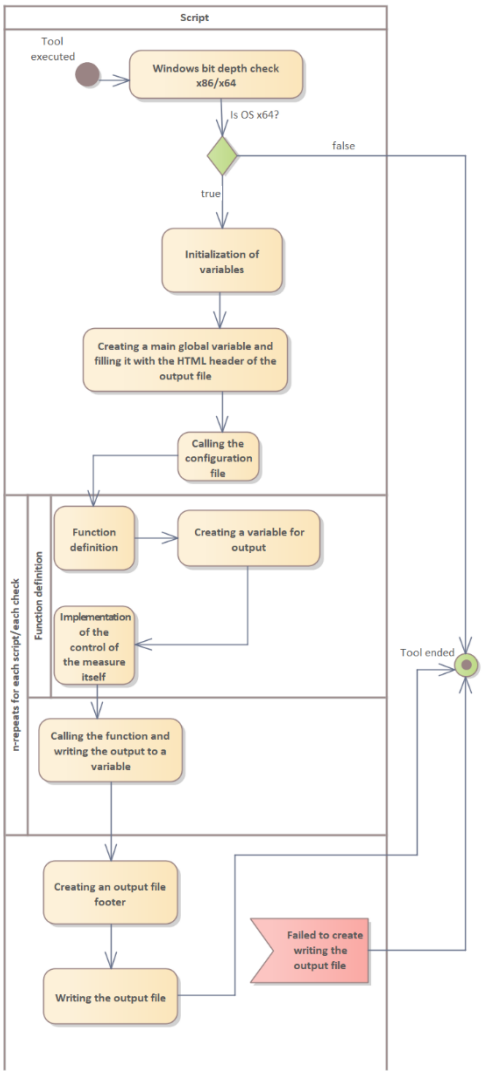


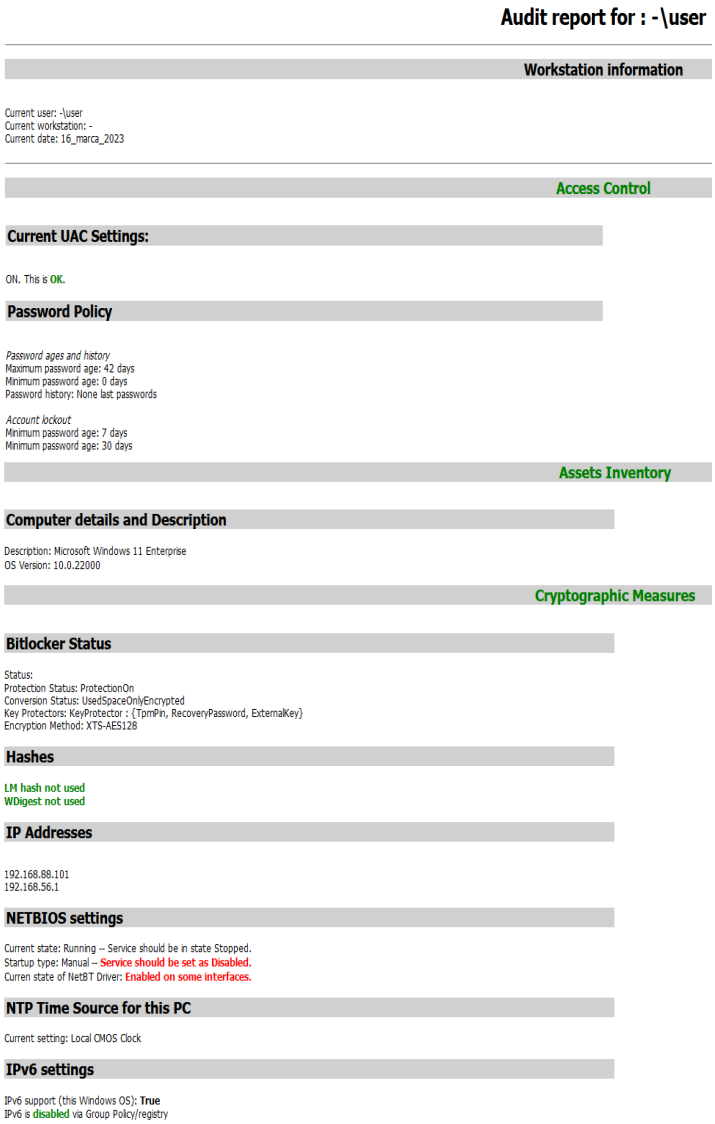
Figure 1: Auditing process flow

Experimental Evaluation

We verified the tool we created using a standalone workstation (Windows 11 21H2) and on a domain controller (Windows Server 2019 1809) in domain containing dozens of computers.

The result of running the tool was an output HTML file saved on the desktop of the currently used user account, which contained the resulting findings. In our case, some discrepancies were found, e.g. untreated NetBIOS protocol or non-prohibited use of password hashing of the LMHash type.

After performing partial scripts, the main script creates a (technical) document footer, which represents the correct closure of HTML tags. We have attached Figure 2 to provide better imagination of the resulting HTML file.



Audit report for : -\user

Workstation information

Current user: -\user
Current workstation: -
Current date: 16_marca_2023

Access Control

Current UAC Settings:

ON. This is **OK.**

Password Policy

Password ages and history
Maximum password age: 42 days
Minimum password age: 0 days
Password history: None last passwords

Account lockout
Minimum password age: 7 days
Minimum password age: 30 days

Assets Inventory

Computer details and Description

Description: Microsoft Windows 11 Enterprise
OS Version: 10.0.22000

Cryptographic Measures

Bitlocker Status

Status:
Protection Status: ProtectionOn
Conversion Status: UsedSpaceOnlyEncrypted
Key Protectors: KeyProtector : {TpmPin, RecoveryPassword, ExternalKey}
Encryption Method: XTS-AES128

Hashes

LM hash not used
WDigest not used

IP Addresses

192.168.88.101
192.168.56.1

NETBIOS settings

Current state: Running -- Service should be in state Stopped.
Startup type: Manual -- **Service should be set as Disabled.**
Curren state of NetBT Driver: **Enabled on some interfaces.**

NTP Time Source for this PC

Current setting: Local CMOS Clock

IPv6 settings

IPv6 support (this Windows OS): **True**
IPv6 is **disabled** via Group Policy/registry

Figure 2: Part of the sample HTML report file

Conclusion

We have analyzed ISO/IEC 27001:2022 regulations regarding the Active Directory and MS Windows operating system hardening. We have created a list of possible implementations of countermeasures using already or freely available tools for MS Windows.

We have developed our own tool, which can be used by security administrators and auditors to evaluate the current state of operating system or Active Directory security. This tool covers ISO 27001 controls related to operating systems. Our tool is suitable for small to medium-sized business and Active Directory environments. Human factor is needed when checking the resulting HTML report. Report provides help and user can choose relevant countermeasures relevant to their environment, business-type and finances.

The main advantage of our solution compared with third-party (source-code closed) tools is that security administrator is able to review the source code and in special configuration files adjust areas and security measures which are subject to inspection.

In addition, the tool provides options for creating new, user's own modules, which expands the existing functionality of the tool or adds completely new control areas that the tool created by us does not currently contain.

Security administrators can use their in-depth knowledge of operating system configuration and adapt the tool according to their needs.

A deeper, technically detailed guide or more complex product might be created based on our initial research. Enterprise administrators might use our conclusions when building an ISO/IEC 27001:2022 compliant Active Directory or Windows environment.

Acknowledgement

This publication has been written thanks to the support of the Slovak University of Technology in Bratislava, co-funded by the gift No. 0835376/00CRZ (# 7175).

References

[1] INTERNATIONAL STANDARD ORGANIZATION: ISO/IEC 27001:2013 Information technology — Security Techniques — Information Security Management System – Requirements. Genève: ISO, 2013

[2] INTERNATIONAL STANDARD ORGANIZATION: ISO/IEC 27001:2022 Information technology — Security Techniques — Information Security Management System – Requirements. Genève: ISO, 2022

[3] MCDONALD, et al. *Ransomware: Analysing the Impact on Windows Active Directory Domain Services.* In: Sensors, vol. 22, no. 3, p. 953, Jan. 2022, doi: 10.3390/s22030953.

[4] AUSTRALIAN CYBER SECURITY CENTRE: *Hardening Windows 10 Version 21H1 workstations* [online]. [cit. 2024-02-02]. Available at: https://www.cyber.gov.au/acsc/view-all-content/publications/hardening-microsoft-windows-10-version-21h1-workstations

Contact information

Slovak University of Technology in Bratislava
Faculty of Informatics and Information Technologies, Ilkovičova 2, Bratislava, Slovakia
Ing. Martin Pavelka, martin . pavelka [at] stuba . sk
doc. Ing. Ladislav Hudec, Csc., ladislav . hudec [at] stuba .sk

Recenzenti:
doc. Ing. Václav Friedrich, Ph.D.

doc. RNDr. Tatiana Hajdúková, PhD.

Kybergrooming: Skrytá hrozba pre deti a mládež

Tomáš Peták

Anotácia: Kybergrooming je problém, s ktorým je potrebné sa zaoberať, pretože ochrana detí je povinnosť spoločnosti. Je to forma sexuálneho zneužívania, kde dospelí nadväzujú vzťahy s deťmi mladšími ako pätnásť rokov cez sociálne siete s cieľom spáchať sexuálne trestné činy alebo vyrábať detskú pornografiu. Autor zdôrazňuje, že tento problém je často nehlásený a predstavuje významnú hrozbu pre deti. Právne rámce na Slovensku, v Poľsku a v Českej republike určujú tresty za kybergrooming, pričom Slovenský trestný zákon stanovuje tresty od šiestich mesiacov do troch rokov. Autor upozorňuje na alarmujúci nárast hlásení o online zvádzaní detí, pričom v roku 2022 CyberTipline prijala viac ako 32 miliónov hlásení. Je dôležité vedieť správne rozpoznávať príznaky kybergroomingu u detí, ako sú nadmerná online aktivita, tajnostkárske správanie a náhle zmeny nálady, pretože dôsledky môžu mať až katastrofálne následky, ktoré častokrát vyústia do suicídia. Aj preto sa príspevok zaoberá práve touto celospoločenskou problematikou.

Kľúčové slová: detská pornografia, CyberTipline, ochrana detí, groomer, kybergrooming, sociálne inžinierstvo

Abstract: Cyberbullying is a problem that needs to be addressed because protecting children is a duty of society. It is a form of sexual abuse where adults establish relationships with children under the age of fifteen through social networks in order to commit sexual offences or produce child pornography. The author stresses that this problem is often unreported and poses a significant threat to children. The legal frameworks in Slovakia, Poland and the Czech Republic determine the penalties for cyberbullying, while the Slovak Criminal Code provides for sentences ranging from six months to three years. The author highlights an alarming increase in reports of online grooming of children, with CyberTipline receiving more than 32 million reports in 2022. It is important to be able to correctly recognise the signs of cyberbullying in children, such as excessive online activity, secretive behaviour and sudden mood changes, as the consequences can be catastrophic, often resulting in suicide. That is why this paper deals with this societal issue.

Keywords: child pornography, CyberTipline, child protection, groomer, cyber grooming, social engineering

Úvod do problematiky

V posledných desaťročiach internet zmenil spôsob, akým ľudia komunikujú, získavajú informácie a podnikajú. V posledných rokoch vznikli rôzne fóra a sociálne siete, ktoré umožnili mnohým ľuďom vystúpiť pod rúškom anonymity. Komunikujú medzi sebou, spájajú sa a vymieňajú si informácie. Internet sa stal aj silným nástrojom na zarábanie peňazí. Jednoducho, zmenil svet. Nielen k lepšiemu. Pod rúškom anonymity poskytol možnosť určitým jedincom alebo skupinám osôb páchať globálne trestnú činnosť.

Z rýchlo rastúcim rozvojom informačno-komunikačných technológií sa rozširujú možnosti pre páchateľov orientovaných na deti a mládež. Medzi jedny z takýchto trestných činov, páchaných prostredníctvom informačno–komunikačných technológií patrí kybergrooming. Treba si uvedomiť, že vo veľkej miere sa jedná o latentnú kriminalitu, nakoľko častokrát sa stáva, že obete sú deti, ktoré žijú v strachu bez, opory v dôveryhodnej dospelej osobe, ktorej by sa o týchto činoch mohli zdôveriť. Vzhľadom na veľmi nízky fyzický vek si niektoré obete ani len neuvedomujú, že je na nich páchaný trestný čin a dané skutky považujú za normálne. Iné obete zas po spáchaní trestného činu často prechádzajú rôznymi formami psychopatologických následkov, ktoré častokrát vyústia do suicídia - samovraždy. Spoločnosť musí byť schopná postarať sa a ochrániť deti, pretože „*Každé dieťa si zaslúži bezpečné detstvo*“[1].

Právne vymedzenie pojmu kybergrooming

Definícia kybergroomingu:

Kybergrooming (anglicky cyber grooming) je variantom sexuálneho zneužívania, pri ktorej dospelá osoba (ktorá nie je dieťaťom) nadväzuje kontakty s dieťaťom mladším ako pätnásť rokov pod vymyslenou identitou na sociálnych sieťach. Cieľom tohto kontaktu je spáchať na dieťati trestný čin sexuálneho zneužívania alebo trestný čin výroby detskej pornografie.

Kybergrooming je trestný čin, ktorý sa týka zneužívania detí prostredníctvom informačno-komunikačných technológií.

Slovenská republika - § 201a Trestný zákon

§201a Zák. 300/2005 Z.z. Trestný zákon

Kto prostredníctvom elektronickej komunikačnej služby navrhne dieťaťu mladšiemu ako pätnásť rokov osobné stretnutie v úmysle spáchať na ňom trestný čin sexuálneho zneužívania alebo trestný čin výroby detskej pornografie, pričom sám nie je dieťaťom, potrestá sa odňatím slobody na šesť mesiacov až tri roky.[2]

[1] NCMEC [online]. [cit. 25.03.2024]. dostupné na internete: https://www.missingkids.org/home
[2] Zákon č. 300/2005 Z.z. Trestný zákon, §201a.

Podmienky kybergroomingu:

- Páchateľ musí byť dospelou osobou (nie dieťaťom).
- Dieťa, s ktorým sa nadväzuje kontakt, musí byť mladšie ako pätnásť rokov.

Trestná sadzba:

Za kybergrooming hrozí páchateľovi odňatie slobody na šesť mesiacov až tri roky.

Poľská republika - článok 200a, §1 a §2 Kodeks karny

Článok 200a. - Elektronická sexuálna korupcia maloletého

§1 - Kto s cieľom spáchať trestný čin uvedený v článku 197 § 4 alebo v článku 200, ako aj vyrobiť alebo zaznamenať pornografický obsah, prostredníctvom informačného a komunikačného systému alebo telekomunikačnej siete nadviaže kontakt s maloletou osobou mladšou ako 15 rokov s cieľom prostredníctvom uvedenia do omylu, využitia omylu alebo neschopnosti správne pochopiť situáciu alebo prostredníctvom bezprávnej hrozby sa s ňou stretnúť, sa potrestá odňatím slobody až na tri roky.

§2 - Kto prostredníctvom informačného a komunikačného systému alebo telekomunikačnej siete navrhne maloletej osobe mladšej ako pätnásť rokov pohlavný styk, podrobenie sa inému sexuálnemu styku alebo vykonanie iného sexuálneho aktu alebo účasť na výrobe alebo zaznamenaní pornografického obsahu a pokúsi sa ho uskutočniť,

sa potrestá pokutou, obmedzením osobnej slobody alebo odňatím slobody až na dva roky.[3]

Podmienky kybergroomingu:

- Dieťa, s ktorým sa nadväzuje kontakt, musí byť mladšie ako pätnásť rokov.

Trestná sadzba:

Za kybergrooming hrozí páchateľovi odňatie slobody až na tri roky.

[3] ustawa z dnia 6 czerwca 1997 r. – Kodeks karny, art. 200a.

Česká republika - § 193b Zákon trestní zákoník

§ 193b trestní zákoník - Nadviazanie nezákonného kontaktu s dieťaťom

Kto navrhne stretnutie dieťaťu mladšiemu ako pätnásť rokov v úmysle spáchať trestný čin podľa § 187 ods. 1, § 192, § 193, § 202 ods. 3 alebo iný sexuálne motivovaný trestný čin, potrestá sa odňatím slobody až na dva roky.[4]

Tento trestný čin spočíva v navrhovaní stretnutia s dieťaťom mladším ako pätnásť rokov s úmyslom spáchať sexuálne motivovaný trestný čin.

Podmienky kybergroomingu:

- Dieťa, s ktorým sa nadväzuje kontakt, musí byť mladšie ako pätnásť rokov.

Trestná sadzba:

Za kybergrooming hrozí páchateľovi odňatie slobody až na dva roky.

Východisková situácia

Celosvetovo

CyberTipline je centralizovaný reportovací systém pre online zneužívanie detí. Verejnosť a poskytovatelia elektronických služieb môžu podávať správy o podozrení na online zvádzanie detí pre sexuálne úkony, sexuálne zneužívanie detí, materiál sexuálneho zneužívania detí, sexuálny turizmus s deťmi, sexuálne obchodovanie s deťmi, nevyžiadané obscénne materiály zaslané dieťaťu, klamlivé názvy domén alebo digitálne obrazy na internete.

Od svojho vzniku v roku 1998 dostala linka CyberTipline viac ako 144 miliónov hlásení. Pričom v roku 2022 prijala linka CyberTipline 32 059 029 hlásení.

Tabuľka č.1 Kategorizácia reportov za obdobie 2021 až 2023

Kategorizácia správ CyberTipline	Správy za rok 2021	Správy za rok 2022	Správy za rok 2023

[4] Zákon č.40/2009 trestní zákoník, §193b.

detská pornografia (držba, výroba a distribúcia)	29 309 106	31 901 234	35 925 098
Zavádzajúce slová alebo digitálne obrázky na internete	5 825	7 517	8 446
Online lákanie detí na sexuálne akty	44 155	80 524	**186 819**
Sexuálne obchodovanie s deťmi	16 032	18 336	17 353
Nevyžiadaný obscénny materiál odoslaný dieťaťu	5 177	35 624	45 746
Zavádzajúci názov domény	3 304	1 948	6 883
Sexuálne obťažovanie detí	12 458	12 906	18 021
Detská sexuálna turistika	1 624	940	2 002
Celkom	**29 397 681**	**32 059 029**	**36 210 368**

zdroj: missingkids.org

Z tabuľky č. 1 vyplýva, že v roku 2023 získal CyberTipline viac ako 186 000 správ týkajúcich sa online lákania – čo je viac ako 300 % nárast oproti roku 2021. Online lákanie je formou vykorisťovania zahŕňajúcou jednotlivca, ktorý komunikuje online s niekým, kto je považovaný za dieťa, s úmyslom spáchať sexuálny trestný čin alebo únos. (kybergrooming)[5]

Slovenská republika

Trestné činy súvisiace s kybergroomingom tvoria zväčša latentný problém. Štatisticky pokryť latentnú kriminalitu je veľmi náročná úloha, pretože vychádzame zo zozbieraných dát, ktoré nepokrývajú celú šírku daného problému – čo je všeobecne platné pre latentnú kriminalitu.

Tabuľka č.2 Zistené TČ za obdobie 2021 až 2023

Obdobie	Podnety za rok 2021	Podnety za rok 2022	Podnety za rok 2023
Kybergrooming §201a TZ	7	10	6

[5] https://www.missingkids.org/cybertiplinedata

Zdroj: Vlastné spracovanie z údajov EŠSK[6]

Tabuľka č. 2 zobrazuje zistené (nahlásené) trestné činy za obdobie rokov 2021 až 2023 na území Slovenskej republiky.

Podľa výskumu zameraného na používanie internetu z pohľadu žiakov základných a stredných škôl z roku 2021 bolo zistené, že žiaci základných a stredných škôl začali prvýkrát používať internet najčastejšie vo veku 7 až 9 rokov. V nižšom veku sa na internet pripájali žiaci základných škôl, chlapci, väčšinou z najväčších miest a z Bratislavského a Trnavského kraja.[7]

Tabuľka č.3 Porovnanie veku používateľov internetu za roky 2019 a 2021 (v %)

Vek prvého použitia internetu	2019	2021	Rozdiel (p.b.)
6 rokov alebo menej	12,5	21,2	8,7
7 – 9 rokov	43,5	42,8	-0,7
10 – 12 rokov	35,3	31,1	-4,2
13 rokov a viac	8,4	3,9	-4,5
Nikdy internet nepoužilo	0,3	1,1	0,8

Zdroj: Vybrané výsledky z výskumu zameraného na používanie internetu, online aktivity a potencionálne riziká z pohľadu žiakov základných a stredných škôl

Z uvedenej tabuľky vyplýva, že digitálne technológie a internet sú neoddeliteľnou súčasťou každodenného života skúmaných mladých ľudí. 90,6 % žiakov uviedlo, že používajú internet denne alebo takmer denne. Práve táto skutočnosť poskytuje príležitosť páchateľom vytypovať si tu správnu obeť.

Fázy kybergroomingu

1. Budovanie dôvery a snaha izolovať obeť

Útočník sa v prvom rade snaží o vytvorenie dôverného vzťahu s vytipovaným dieťaťom. Prezentuje sa ako človek, ktorý dieťaťu rozumie, chápe jeho problémy, chce mu pomôcť s ich riešením. Chce byť pre dieťa dobrým kamarátom, na ktorého sa môže vo všetkom spoľahnúť.

[6] Evidenčno-štatistický systém kriminality je tzv. „policajná štatistika“, je evidenčný policajný systém, v ktorom sa sústreďujú údaje o trestných činoch, údaje o známych páchateľoch či obetiach. Prevádzkovateľom tohto informačného systému je Odbor správy informačných systémov polície Prezídia Policajného zboru.
[7] JANKOVÁ Mária, [cit. 25.03.2024], Vybrané výsledky z výskumu zameraného na používanie internetu, online aktivity a potencionálne riziká z pohľadu žiakov základných a stredných škôl, 2022, Centrum vedecko-technických informácií SR, Bratislava, 2022, ISBN 978-80-8240-028-4.

Zároveň sa dieťa snaží odizolovať, presviedča ho, aby o ich vzťahu nikomu nehovorilo, aby si vymazalo ich vzájomnú konverzáciu, zisťuje, či rodičia kontrolujú aktivity dieťaťa na internete.

2. Upevňovanie vzťahu a podplácanie

Ak si páchateľ už dieťa získal, pokračuje v rozvíjaní vzťahu. Pýta si od dieťaťa podrobnejšie informácie (číslo mobilného telefónu, adresu bydliska), stále viac sa s ním rozpráva o intímnejších témach, ako sú partnerské a vzťahové problémy, sexuálne aktivity, čím vytvára pocit intimity. Zároveň dáva dieťaťu rôzne darčeky (peniaze, kredit do mobilu, drahé hračky a oblečenie).

3. Emocionálna závislosť obete

Páchateľ sa stal pre dieťa nenahraditeľným. Je pre neho najbližším človekom, ktorý pozná jeho najintímnejšie tajomstvá. Dieťa nechce o tento vzťah prísť, podľa požiadaviek páchateľa rodičom klame o tom, ako a s kým trávi čas, prestáva sa im zverovať so svojím prežívaním. Páchateľ vytvára v dieťati dojem, že to, čo je medzi nimi, je vzájomný vzťah plný porozumenia a lásky, ktorý bude pokračovať aj v budúcnosti. Stále viac vťahuje dieťa do svojej siete, rozpráva o výnimočnosti a jedinečnosti ich vzťahu, požaduje od neho stále viac, napríklad zasielanie intímnych fotografií alebo kybersex cez webkameru.

4. Osobné stretnutie

V ďalšej fáze sa páchateľ snaží prejsť k osobnému stretnutiu. Môže nalákať dieťa na nejakú zaujímavú aktivitu, napríklad návštevu kina, diskotéky, alebo ho zavolať priamo k sebe domov. Už si je istý vzťahom s dieťaťom, vie, že dieťa ich stretnutie neprezradí.

5. Sexuálne obťažovanie, sexuálne zneužitie

V poslednej fáze páchateľ dieťa zneužije. Buď ho presvedčí, aby tak urobilo z lásky k nemu, pre ich vzťah alebo použije manipuláciu, vydieranie a nátlak (pohrozí dieťaťu, že o tom povie jeho rodičom alebo zverejní jeho intímne fotografie na internete). Takto môže dieťa zneužívať opakovane, často a dlhodobo.[8]

[8] Online grooming / aut. Jana Kuchtová - In: Aktuálne výzvy kybernetickej bezpečnosti[elektronický dokument] : special edition 2020 : zborník príspevkov / zost. Štefan Zachar, rec. Anna Hamranová, rec. Eva Kostrecová. - Bratislava : Akadémia Policajného zboru v Bratislave, 2020. - ISBN 978-80-8054-879-7. - s. 89-102.

Príznaky u detí

nadmerný čas online a tajnostkárstvo ohľadom aktivít na internete

- Nadmerný čas online sa týka trávenia neprimeraného množstva času na internete, čím sa zanedbávajú iné dôležité aktivity v živote, ako je práca, štúdium, sociálne kontakty, koníčky a osobná starostlivosť. Môže to mať negatívny vplyv na fyzické a duševné zdravie, ako aj na celkovú pohodu.
- Tajnostkárstvo ohľadom aktivít na internete sa týka skrývania online aktivít pred ostatnými, ako je napríklad história prehliadania, stiahnuté súbory, online rozhovory a aktivity na sociálnych sieťach. Môže to byť z rôznych dôvodov, ako je strach z posudzovania, ochrana súkromia alebo skrytie nežiaduceho správania.

nové online priateľstvá o ktorých rodičia nemajú vedomosť

- Deti, ktoré nadväzujú online priateľstvá, o ktorých rodičia nemajú vedomosť, sú obzvlášť zraniteľné voči kybergroomingu. Dospelý môže využiť nevedomosť rodičov a izolovanosť dieťaťa online na to, aby ho ľahšie manipuloval a zneužil.

náhle zmeny nálady a správania

- Náhle zmeny nálady a správania sú bežným príznakom toho, že dieťa môže byť obeťou kybergroomingu. Medzi príznaky, ktoré by mali vyvolať obavy pre rodičov, patrí:

    - samopoškodzovanie,
    - zneužívanie návykových látok,
    - výrazné zmeny v stravovacích návykoch alebo spánku,
    - sťaženie sústredenia sa alebo fungovania v škole,
    - sociálna izolácia alebo strata záujmu o aktivity, ktoré dieťa kedysi malo rado,
    - rozhovory o smrti alebo umieraní,
    - vyjadrovanie pocitov beznádeje alebo bezmocnosti.

vyhýbanie sa fyzickému kontaktu a izolácia

- Dieťa sa snaží minimalizovať alebo úplne zabrániť fyzickému dotyku s inými ľuďmi. Dieťa je oddelené od ostatných ľudí a nemá pravidelný sociálny kontakt.

Rodičovský filter – základná ochrana

V aplikácii Rodičovský filter môžu rodičia zablokovať alebo povoliť konkrétne webové stránky. Môžu tiež blokovať prístup k určitým typom a skupinám webových stránok, pričom tieto aplikácie automaticky odfiltruje. Služba vytvára aj záznamy o tom, aké stránky deti navštevujú, aké informácie vyhľadávajú na internete a aké sú ich aktivity na sociálnych sieťach. Rodičovský filter má navyše schopnosť obmedziť množstvo času, počas ktorého môžu byť vaše deti online každý deň, ako aj nastaviť rôzne hodiny (minúty) pre pracovné dni a víkendy. Niektoré rodičovské filtre majú schopnosť posielať upozornenia na e-mailové adresy rodičov v prípade, že sa ich deti pokúsia dostať na stránky, ktoré rodič zaradil na takzvaný „zoznam prístupov“ resp. „čierna listina“.

Ani tieto bezpečnostné nástroje však nedokážu na 100% zaručiť, že sa deti nestretnú s nevhodným obsahom. Denne na internete pribúda nespočetne veľa nových webových stránok, ktoré pod svojim nevinným názvom môžu často skrývať úplne iný obsah, a technológia rodičovských filtrov ich tak nevyhodnotí ako škodlivé. Väčšina deti je v IT technológiách zdatnejšia ako ich rodičia. V takomto prípade sa rodič môže obrátiť na odborníkov, ktorí im v rámci softwarovej podpory poradia ako ochrániť svoje deti na internete. Prísne reštriktívne opatrenia bezpečnosť dieťaťa v kybernetickom priestore nezaistia.[9]

Záver

Nie len fyzický, ale aj psychický vývoj detí je pre spoločnosť nesmierne dôležitý. Dnešní mladí ľudia vyrastajú v digitálnom svete, čo spôsobuje, že už v mladom veku majú prístup na internet. Stávajú sa z nich používatelia sociálnych sietí a nadväzujú nové priateľstvá v kyberpriestore. Väčšinou komunikujú práve s jedincami, ktorí svoju skutočnú identitu taja a na sociálnych sieťach vystupujú pod falošnou. Častokrát sa jedná o dospelé osoby, ktoré sa tvária ako rovesníci a za použitia sociálneho inžinierstva sa snažia nadviazať úzky kontakt s dieťaťom, ktoré sa snažia po čase sexuálne zneužiť, alebo spáchať na ňom iný TČ.

Rodičovské filtre sú skvelým spôsobom, ako chrániť deti pred nástrahami internetu, ale skôr či neskôr deti budú chcieť prekonať alebo obísť tieto prekážky, napríklad pomocou zariadení, ktoré sú mimo dosahu rodičov, ako sú počítače v knižnici, v škole alebo u kamaráta doma. Preto je ešte dôležitejšie, aby sa rodičia zamerali predovšetkým na budovanie zdravého vzťahu so svojimi deťmi, ktorý je založený na vzájomnej dôvere a podpore. Ak dieťa rodičom

[9] KOPECKÝ, Kamil. Méně než polovina rodičů pravidelně kontroluje, co dělají jejich děti na internetu. E-bezpečí [online].

dôveruje, nebude sa báť rozprávať ani v krízových situáciách. Sexuálne obťažovanie si vyžaduje čas a zriedka sa stane v krátkom časovom období. Páchatelia často komunikujú s potenciálnymi obeťami dlhší čas a na stretnutia sa pripravujú dlhodobo.[10] Dieťa nesmie stratiť v rodičovi dôveru, je dôležité, aby sa nabudúce nebálo opäť s problémom zveriť[11].

Akonáhle rodič zistí čokoľvek nevhodné alebo sa mu dieťa zverí so vzhliadnutím závadného obsahu, nadviazaním kontaktu s vulgárnym človekom či inou rizikovou situáciou, nemal by za žiadnych okolností konať unáhlene. Naopak, mal by sa snažiť situáciu pochopiť a v pokoji sa o nej s dieťaťom porozprávať, pretože dôsledky, ktoré kybergrooming môže na deťoch zanechať môžu byť nielen psychologické ale častokrát môže zájsť až k ohrozeniu života z dôvodu samovražedných myšlienok.

Zoznam použitej literatúry

ustawa z dnia 6 czerwca 1997 r. – Kodeks karny

Zákon č.40/2009 trestní zákoník

Zákon č. 300/2005 Z.z. Trestný zákon

BACIGÁL Ivan a HAJDÚKOVÁ Tatiana, [online]. Preverovanie a vyšetrovanie sexuálneho zneužívania detí on-line v praxi, zborník príspevkov zo 4. medzinárodnej konferencie "Řešení elektronického násilí a kyberkriminality" konanej v dňoch 9. 10. - 10. 10. 2014 v Jihlave. - ISSN 2336-3657. - Roč. 1, zvláštne vydanie (2014).

CYBERTIPLINE 2023 REPORT [online]. dostupné na internete: https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata.

FINDING THE FACTORS AND PROPOSING THE SOLUTION FOR PREVENTING SECONDARY VICTIMIZATION. [online]. dostupné na internete: https://www.researchgate.net/publication/373726115_Finding_the_Factors_and_Proposing_the_Solution_for_Preventing_Secondary_Victimization

[10] Tatiana HAJDÚKOVÁ a Ivan BACIGÁL. Hrozby kybernetického priestoru pre deti v období dospievania In: Policajná teória a prax = Police Theory and Practice : časopis Akadémie PZ v Bratislave. - ISSN 1335-1370. - Roč. 22, č. 3 (2014), s. 5-19.

[11] BURDOVÁ, Eva a Jan TRAXLER. Bezpečně na internetu. Praha: Středočeský kraj ve spolupráci se Vzdělávacím institutem Středočeského kraje (VISK), 2014, 43 s. ISBN 978-80-904864-9-2.

HAJDÚKOVÁ Tatiana a Ivan BACIGÁL. Hrozby kybernetického priestoru pre deti v období dospievania, In: Policajná teória a prax = Police Theory and Practice : časopis Akadémie PZ v Bratislave. - ISSN 1335-1370.

JANKOVÁ Mária, Vybrané výsledky z výskumu zameraného na používanie internetu, online aktivity a potencionálne riziká z pohľadu žiakov základných a stredných škôl, 2022, Centrum vedecko-technických informácií SR, Bratislava, 2022, ISBN 978-80-8240-028-4.

JOZEF ČENTÉŠ, COLLEGIUM 2022. Trestný poriadok 5. vyd. : Eurokódex, 2022. 1112s. ISBN: 978-80-8155-109-3.

KOPECKÝ, Kamil. Méně než polovina rodičů pravidelně kontroluje, co dělají jejich děti na internetu. E-bezpečí [online]. dostupné na internete: https://www.e-bezpeci.cz/index.php/rodicum-ucitelum-zakum/1099-parental-control

KUCHTOVÁ Jana, Online grooming, In: Aktuálne výzvy kybernetickej bezpečnosti[elektronický dokument] : special edition 2020 : zborník príspevkov, Bratislava, Akadémia Policajného zboru v Bratislave, 2020. - ISBN 978-80-8054-879-7.

NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN - NCMEC data [online].

PROKEINOVÁ, M., LACIAK, O. 2021. Sexuálne zneužívanie detí a zverených osôb a trestnoprávna ochrana obetí trestných činov. Bratislava : Wolters Kluwer SR, 2021, s. 35 ISBN 978-80-571-0350-9.

ŠTATISTIKA KRIMINALITY V SLOVENSKEJ REPUBLIKE [online]. dostupné na internete: http://statpz.minv.sk/statistika/

TOMÁŠ STRÉMY, LUCIA KURILOVSKÁ A KOL. 2022. Komentár k Trestnému zákonu, I. zväzok. Bratislava : WoltersKluwer, 2022. 904 s. ISBN: 978-80-7676-429-3

Kontaktné údaje

npor. Ing. Tomáš Peták
Akadémia Policajného zboru v Bratislave
Katedra informatiky a manažmentu
tomas.petak@akademiapz.sk
0961 057 257

Recenzenti:

prof. RNDr. Michal Greguš, CSc.

doc. Ing. Václav Friedrich, Ph.D.

Možnosti užití vybraných metod umělé inteligence v kyberbezpečnosti

Vladimír Šulc

Anotace: Kyberbezpečnostní krajinu neustále mění a zlepšuje využití metod umělé inteligence (UI), zejména strojového učení a hlubokého učení. Tyto metody posilují schopnosti detekce a reakce na kybernetické hrozby tím, že umožňují systémům rychle rozpoznat a reagovat na anomálie v síti a sofistikované útoky. Přestože UI přináší efektivitu a pokročilou obranu proti stále se vyvíjejícím hrozbám, je třeba adresovat výzvy, jako je zajištění dostatečných a kvalitních dat pro trénink a otázky související s etikou a ochranou soukromí. Aktivní výzkum a vývoj v oblasti UI jsou klíčem k využití jejího plného potenciálu pro posílení kybernetické odolnosti.

Klíčová slova: Umělá inteligence, Kyberbezpečnost, Strojové učení, Hloubkové učení, Detekce hrozeb, Odezva na incidenty, Sofistikované útoky, Etika, Ochrana soukromí.

Abstract: The cybersecurity landscape is continually being transformed and enhanced by the application of artificial intelligence (AI) methods, especially machine learning and deep learning. These methods bolster the capability to detect and respond to cyber threats by enabling systems to swiftly identify network anomalies and sophisticated attacks. While AI brings efficiency and advanced defense against evolving threats, challenges such as ensuring ample and quality data for training, as well as issues related to ethics and privacy, must be addressed. Ongoing research and development in the field of AI are crucial to harness its full potential to strengthen cyber resilience.

Klíčová slova: Artificial Intelligence (AI), Cybersecurity, Machine Learning, Deep Learning, Threat Detection, Automated Response, Sophisticated cyber attacks , Ethical Considerations, Privacy.

Úvod

Kyberbezpečnost se stala základním pilířem digitálního věku, ochraňujícím nejen osobní a firemní data, ale i digitální infrastrukturu státu. Paralelně s tím, jak se rozvíjejí technologie a digitalizace, která penetruje do všech sfér života, roste i sofistikovanost a četnost kybernetických útoků. V této nové éře je proto stále naléhavější potřeba vyvíjet robustní a adaptivní bezpečnostní řešení, která dokážou těmto hrozbám čelit. Umělá inteligence (zkr. UI), se svými schopnostmi rychlého učení, adaptace a rozpoznání vzorů, nabízí příslib značného pokroku v této oblasti.

Vzhledem k neustálé evoluci a sofistikovanosti kybernetických útočníků je zapotřebí nejen pasivně reagovat na incidenty, ale proaktivně předvídat a předcházet možným hrozbám. Metody UI, zejména v oblastech strojového a hlubokého učení, nabízejí naději pro vytváření dynamických, samoorganizujících se a inteligentních systémů, které jsou schopné detekovat

a neutralizovat kybernetické útoky v reálném čase a přizpůsobovat se novým hrozbám rychleji, než by to bylo možné prostřednictvím tradičních bezpečnostních postupů.

Využití UI v kyberbezpečnosti se však setkává s řadou výzev na zajištění a ochranu dat potřebných pro trénink modelů, potenciální falešně pozitivní detekce a etické dilema spojené s autonomním rozhodováním bez lidského dohledu. Tento příspěvek bude zkoumat možnosti, výzvy a doporučení, která by mohla formovat budoucnost UI v kyberbezpečnosti a jak lze tyto technologie implementovat k posílení našich digitálních obranných mechanismů.

Současný stav kybernetických hrozeb je charakterizován neustálým nárůstem sofistikovanosti a frekvence útoků. Kyberzločinci využívají pokročilé techniky, včetně ransomwaru, phishingu a malware, aby pronikli do sítí a ukradli citlivá data nebo způsobili výpadky služeb. Výzvou pro obránce je nejen detekovat a reagovat na tyto hrozby, ale také předvídat nové útočné metody a adaptovat se na dynamicky se měnící kyberprostor. Organizace se musí vypořádat s nedostatkem kvalifikovaných odborníků na kybernetickou bezpečnost a s nutností integrace pokročilých bezpečnostních technologií a postupů do svých operací.

Základní principy a metody UI:

Mezi základní principy umělé inteligence patří:

1. **Strojové učení**: Jedná se o centrální pilíř umělé inteligence. Metody strojového učení, jako je dohledané učení, neučené učení a posilované učení, umožňují systémům automatizovaně se učit z dat. Pro aplikace v kyberbezpečnosti se toto často využívá pro rozpoznávání vzorů v datech, které mohou indikovat bezpečnostní hrozby.
2. **Neuronové sítě**: Inspirací pro neuronové sítě je biologický mozek. Tyto sítě jsou sestaveny z vrstev umělých neuronů, kde každá vrstva má schopnost zpracovávat různé aspekty vstupních dat. V kontextu kyberbezpečnosti, hluboké neuronové sítě pomáhají s detekcí komplexních hrozeb, které mohou uniknout tradičním detekčním metodám.
3. **Algoritmy**: V UI se setkáváme s různými algoritmy, které jsou základem pro strojové učení a neuronové sítě. Algoritmy, jako jsou konvoluční neuronové sítě (CNNs) pro zpracování obrazu nebo rekurentní neuronové sítě (RNNs) pro sekvenční data, jsou klíčové pro interpretaci a zpracování informací.

Důležitým zdrojem pro hlubší pochopení těchto principů je publikace Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press, která poskytuje komplexní pohled na hluboké učení a neuronové sítě[1].

UI používané v kyberbezpečnosti:

Ve sféře kyberbezpečnosti se rozlišují tři klíčové typy umělé inteligence:

1. Supervised Learning (Učení s učitelem),
2. Unsupervised Learning (Učení bez učitele)
3. Reinforcement Learning (Posilované učení).

Učení s učitelem aplikuje algoritmy na předem označená data pro detekci známých hrozeb. Učení bez učitele identifikuje neobvyklé vzorce a anomálie v datech, což je užitečné pro odhalení nových typů útoků. Posilované učení se zaměřuje na vylepšení rozhodovacích strategií systémů kyberbezpečnosti tím, že modely získávají odměny za správně identifikované hrozby a útoky. Tyto přístupy umožňují vytvářet sofistikovanější a adaptabilnější obranné mechanismy proti kybernetickým hrozbám.

Detekce a prevence kybernetických hrozeb:

Detekce a prevence kybernetických hrozeb pomocí UI je rychle se rozvíjející oblast, která má potenciál významně zlepšit bezpečnost počítačových systémů a sítí[2]. UI technologie umožňují analyzovat obrovské množství dat v reálném čase, identifikovat anomálie a podezřelé aktivity a rychle na ně reagovat[3].

Existuje několik způsobů, jak lze UI využít pro detekci a prevenci kybernetických hrozeb[4]:

1. **Detekce anomálií**: UI systémy pro detekci anomálií jsou trénovány na velkém množství normálních dat o síťovém provozu a chování uživatelů. Na základě tohoto modelu pak dokážou identifikovat neobvyklé vzorce, které se odchylují od běžného provozu. Příklad: UI detekuje náhlý nárůst přenosů dat ze zařízení v neobvyklou dobu (např. o víkendu v noci), což může indikovat probíhající útok nebo exfiltraci citlivých dat.

[1] GOODFELLOW, I., Bengio, Y. a Courville, A., 2016. *Deep Learning*. Cambridge, Massachusetts: MIT Press.
[2] NGUYEN, T. a T. REDDI. *Deep Reinforcement Learning for Cyber Security*. IEEE Transactions on Neural Networks and Learning Systems [online]. 2021, 32(8), 3512-3525 [cit. 2024-04-05]. ISSN 2162-2388.
[3] SARKER, I. H. *Machine Learning: Algorithms, Real-World Applications and Research Directions*. SN Computer Science [online]. 2021, 2(3) [cit. 2024-04-08]. ISSN 2661-8907.
[4] KOUDELA, Lukáš. *Umělá inteligence v kybernetické bezpečnosti*. Acta Informatica Pragensia. 2021, roč. 10, č. 2, s. 110-125. ISSN 1805-4951.

2. **Analýza malwaru**: UI využívá techniky strojového učení jako clustering, klasifikaci a hluboké učení k analýze charakteristických rysů (signatur) malwaru. Dokáže tak rychle identifikovat známé i nové varianty malwaru na základě podobnosti kódu, chování či jiných atributů. Příklad: UI model je natrénován na tisících vzorků malwaru a dokáže nový podezřelý soubor během milisekund klasifikovat jako ransomware na základě shodných rysů, i když jde o dosud neznámou variantu.
3. **Prediktivní analýza**: UI modely pro predikci kybernetických hrozeb analyzují data o útocích, zranitelnostech a indikátorech kompromitace (IOCs). Na základě trendů, korelací a anomálií umí předpovídat budoucí hrozby a identifikovat slabá místa v zabezpečení. Příklad: UI vyhodnotí data o nedávných útocích ransomwaru v daném odvětví a na základě společných znaků (použité exploity, cílené zranitelnosti) predikuje, že organizace bude v příštích týdnech čelit zvýšenému riziku podobného útoku, pokud neaplikuje konkrétní bezpečnostní záplaty.
4. **Automatizovaná reakce**: Pokročilé UI systémy v kombinaci se strojovým učením a expertními pravidly umožňují automatizovanou reakci na detekované hrozby v reálném čase. Umí provádět bezpečnostní akce bez nutnosti zásahu člověka, a tím výrazně zkrátit dobu reakce. Příklad: UI detekuje pokusy o přihlášení do kritického systému z neobvyklé lokace a vyhodnotí je jako vysoce rizikové. Automaticky zablokuje dané IP adresy a dočasně deaktivuje kompromitované uživatelské účty, čímž zabrání útočníkovi v dalším postupu.
5. **Analýza chování uživatelů a entit (zkr. UEBA)**: UEBA systémy využívají UI k vytvoření behaviorálních profilů uživatelů a entit (zařízení, aplikace) na základě jejich obvyklých vzorců aktivity. Kontinuálně monitorují chování a upozorňují na významné odchylky, které mohou značit bezpečnostní incident. Příklad: UI detekuje, že uživatelský účet, který běžně přistupuje pouze během pracovní doby z firemní kanceláře, se náhle přihlašuje o víkendu z jiné země a stahuje velké objemy citlivých dat. UEBA systém vyhodnotí toto chování jako anomální a potenciálně škodlivé.
6. **Zabezpečení emailů a webu**: UI posiluje tradiční bezpečnostní nástroje jako antispam a webové filtry tím, že analyzuje obsah, kontext a reputaci zdrojů. Dokáže odhalovat sofistikované phishingové emaily, malware a škodlivé webové stránky na základě charakteristických vzorců a podobnosti s již známými hrozbami. Příklad: UI model vyhodnotí příchozí email jako podezřelý, protože obsahuje známé phishingové fráze, odkaz na stránku s nízkou reputací a předstírá, že pochází od legitimní finanční instituce. Email je automaticky označen jako spam a zablokován.

7. **Bezpečnostní orchestrace a automatizace (zkr. SOAR)**: SOAR platformy využívají UI k integraci dat z různých bezpečnostních nástrojů (SIEM, IDS/IPS, EDR atd.), korelaci událostí a automatizaci reakcí podle předem definovaných workflowů. UI pomáhá prioritizovat incidenty, doporučovat vhodné akce a automatizovat rutinní úkoly. Příklad: SOAR platforma s využitím UI vyhodnotí sérii událostí z různých systémů (neobvyklé přihlášení, stažení malwaru, skenování portů) jako souvisící a indikující probíhající útok. Automaticky provede definované kroky jako sběr dalších dat, blokování podezřelé aktivity a upozornění bezpečnostního týmu.

Tyto příklady ilustrují, jak UI pomáhá zlepšovat detekci a prevenci kybernetických hrozeb. Umožňuje zpracovávat obrovské objemy dat, odhalovat komplexní vzorce a anomálie, předvídat budoucí hrozby a automatizovat reakce. Zároveň je však třeba mít na paměti, že UI je stále pouze nástrojem, který vyžaduje správné nastavení, dohled a etické používání ze strany lidských expertů.

Aktuální výzkumy:

Aktuální výzkum v oblasti využití UI v kybernetické bezpečnosti se zaměřuje na vývoj pokročilých technik a nástrojů pro detekci, prevenci a reakci na stále sofistikovanější a rychle se vyvíjející kybernetické hrozby. Výzkumníci zkoumají, jak lze pomocí UI zlepšit schopnosti organizací identifikovat anomálie a hrozby v síťovém provozu, chování uživatelů a systémů, automatizovat bezpečnostní operace a zvýšit celkovou odolnost vůči kybernetickým útokům.

Hlavní oblasti výzkumu zahrnují využití strojového učení a hlubokého učení pro detekci malwaru, síťových útoků a dalších hrozeb, vývoj explainable UI (XAI) pro zvýšení transparentnosti a důvěryhodnosti UI systémů v kybernetické bezpečnosti, automatizaci a orchestraci bezpečnostních procesů pomocí UI, obranu proti útokům na samotné UI modely a využití federated learningu pro trénování UI modelů na distribuovaných datech při zachování soukromí a důvěrnosti.

Níže jsou uvedeny podrobnější informace k jednotlivým výzkumným směrům[5]:

1. **Detekce anomálií a hrozeb pomocí strojového učení**: Výzkumníci se zaměřují na vývoj pokročilých algoritmů strojového učení pro detekci anomálií a hrozeb

[5] TADDEO, Mariarosaria a Luciano FLORIDI. *The Debate on the Moral Responsibilities of Online Service Providers*. Science and Engineering Ethics [online]. 2016, 22(6), 1575-1603 [cit. 2024-04-19]. ISSN 1471-5546.

v síťovém provozu, chování uživatelů a systémů. Například studie "Deep Learning for Cybersecurity: A Comprehensive Survey" (Apruzzese et al., 2022) poskytuje přehled nejnovějších technik hlubokého učení aplikovaných na různé úlohy kybernetické bezpečnosti, jako je detekce malwaru, síťových útoků a phishingu.

2. **Explainable AI (XAI) pro kybernetickou bezpečnost**: Výzkum se zabývá vývojem metod pro interpretaci a vysvětlení rozhodnutí UI modelů v kontextu kybernetické bezpečnosti. Cílem je zvýšit transparentnost a důvěru v UI systémy a usnadnit analytikům pochopení a ověření jejich výstupů. Studie "Explainable AI for Cybersecurity: A Survey" (Weller et al., 2021) shrnuje aktuální přístupy a výzvy v této oblasti.
3. **UI pro automatizaci a orchestraci bezpečnostních operací**: Výzkumníci pracují na využití UI pro automatizaci a optimalizaci bezpečnostních operací, jako je správa incidentů, analýza hrozeb a řízení zranitelností. Například projekt "AI-driven Security Orchestration, Automation and Response (AI-SOAR)" (Bhatt et al., 2022) se zaměřuje na vývoj inteligentních systémů pro integraci a automatizaci bezpečnostních procesů s využitím technik UI a strojového učení.
4. **Adversarial UI a obrana proti útokům na UI modely**: S rostoucím využitím UI v kybernetické bezpečnosti se výzkum zabývá také zranitelnostmi a útoky na samotné UI modely. Studie "Adversarial Attacks and Defenses in AI-based Cyber Security Systems" (Kumar et al., 2021) zkoumá různé typy útoků na UI modely (např. otrávení dat, adversarial examples) a navrhuje obranné mechanismy pro zvýšení odolnosti těchto systémů.
5. **Federated learning a privátnost dat v kybernetické bezpečnosti**: Výzkumníci se zabývají využitím technik federated learningu pro trénování UI modelů na distribuovaných datech bez nutnosti sdílení citlivých informací. To je zvláště relevantní v kontextu kybernetické bezpečnosti, kde organizace potřebují chránit soukromí a důvěrnost svých dat. Studie "Federated Learning for Cybersecurity: Concepts, Challenges and Future Directions" (Li et al., 2022) poskytuje přehled aktuálního stavu a budoucích směrů výzkumu v této oblasti.

Tyto výzkumné směry ukazují, že využití UI v kybernetické bezpečnosti je dynamickou a rychle se rozvíjející oblastí. Výzkumníci se snaží řešit klíčové výzvy, jako je zvýšení přesnosti a rychlosti detekce hrozeb, zajištění transparentnosti a důvěryhodnosti UI systémů, automatizace bezpečnostních operací a ochrana samotných UI modelů před útoky. Pokroky

v těchto oblastech mají potenciál významně posílit schopnosti organizací čelit současným i budoucím kybernetickým hrozbám.

Nástroje a technologie:

Existuje různá škála nástrojů a technologií použití UI v oblasti kybernetické bezpečnosti. Z této různé plejády nástrojů a technologií následně některé uvedu.

Frameworky s knihovnami pro strojové učení a hluboké učení. Tensorflow je open-source platforma vyvinutá společností Google, která poskytuje komplexní ekosystém pro vývoj a nasazení UI modelů. Nabízí vysokoúrovňové API jako Keras pro snadnou konstrukci neuronových sítí, ale i nízkoúrovňové primitivy pro maximální flexibilitu. TensorFlow se vyznačuje robustní podporou pro distribuované trénování, serving modelů a nasazení na různých platformách od CPU až po specializované UI akcelerátory[6].

PyTorch, vyvíjený společností Facebook, je další populární framework pro strojové učení, který klade důraz na jednoduchost použití a pythonický design. Nabízí dynamické výpočetní grafy a imperativní přístup, který usnadňuje experimentování a debugování. PyTorch je oblíbený zejména v akademické sféře a pro výzkumné účely, ale stále více proniká i do produkčních nasazení.

Scikit-learn je všestranná knihovna pro strojové učení v Pythonu, která nabízí širokou škálu algoritmů pro klasifikaci, regresi, clustering, redukci dimenzionality a předzpracování dat. Je postavena na numerických knihovnách NumPy a SciPy a vyniká svým jednotným a uživatelsky přívětivým API. Scikit-learn je skvělou volbou pro rychlé prototypování a aplikaci klasických ML technik na bezpečnostní data.

V oblasti big data jsou Apache Hadoop a Spark klíčovými technologiemi. Hadoop je distribuovaný framework pro ukládání a zpracování velkých objemů dat na clusteru commodity serverů. Poskytuje spolehlivé a škálovatelné úložiště pomocí HDFS (Hadoop Distributed File System) a paralelní zpracování pomocí MapReduce paradigmatu. Spark, na druhé straně, je moderní engine pro distribuované zpracování dat, který nabízí výrazně rychlejší a všestrannější operace než Hadoop. Spark poskytuje bohaté API pro manipulaci s daty pomocí RDD (Resilient

[6] ROSSI, Francesca. *Building Trust in Artificial Intelligence*. Journal of International Affairs [online]. 2019, 72(1), 127-134 [cit. 2024-04-19]. ISSN 0022-197X.

Distributed Datasets), DataFrame a DataSet abstrakcí a podporuje širokou škálu úloh od dávkového zpracování přes interaktivní dotazování až po streamování dat v reálném čase[7].

Apache Spot (nyní známý jako Apache Incubator) je open-source platforma, která kombinuje big data technologie s pokročilými UI algoritmy pro detekci hrozeb a bezpečnostní analýzu. Spot integruje komponenty jako Hadoop, Spark, Kafka a Elasticsearch do uceleného frameworku, který umožňuje ingestovat, ukládat a zpracovávat velké objemy síťových toků, DNS logů a dalších bezpečnostních dat. Poskytuje předtrénované UI modely a vizualizační nástroje pro odhalování anomálií, identifikaci podezřelých aktivit a forenzní analýzu.

V oblasti vizualizace a interpretace UI modelů stojí za zmínku nástroje jako Matplotlib, Seaborn a Plotly. Matplotlib je základní knihovna pro vizualizaci dat v Pythonu, která nabízí širokou škálu grafů, diagramů a plotů. Seaborn je nadstavba nad Matplotlib, která se zaměřuje na statistickou vizualizaci a poskytuje vysokoúrovňové rozhraní pro tvorbu esteticky příjemných a informativních grafů. Plotly je moderní knihovna pro interaktivní a webovou vizualizaci, která umožňuje vytvářet bohaté a responzivní dashboardy a aplikace.

Pro explainable UI (XAI) jsou důležité nástroje jako LIME (Local Interpretable Model-agnostic Explanations), SHAP (SHapley Additive exPlanations) a ELI5 (Explain Like I'm 5). LIME je technika pro generování lokálních vysvětlení pro jednotlivé predikce černoskříňkových modelů. Funguje tak, že perturbuje vstupní data v okolí zájmového příkladu a trénuje interpretovatelný model (např. lineární regresi) na těchto perturbacích. Výsledkem jsou váhy přiřazené jednotlivým rysům, které indikují jejich důležitost pro danou predikci.

SHAP je unifikovaný framework pro interpretaci predikcí založený na konceptu Shapleyho hodnot z teorie her. SHAP přiřazuje každému rysu "férový" příspěvek k celkové predikci modelu na základě jeho hodnoty a interakcí s ostatními rysy. SHAP poskytuje konzistentní a teoreticky podložené vysvětlení pro širokou škálu modelů od lineární regrese až po hluboké neuronové sítě.

ELI5 je knihovna, která se zaměřuje na generování srozumitelných a lidsky čitelných vysvětlení pro predikce ML modelů. Podporuje různé techniky jako vizualizaci důležitosti rysů, extrakci pravidel z rozhodovacích stromů nebo textová vysvětlení pomocí přirozeného jazyka.

[7] DANAHER, John. *The Philosophical Case for Robot Friendship*. Journal of Posthuman Studies [online]. 2019, 3(1), 5-24 [cit. 2024-04-19]. ISSN 2472-4513.

V oblasti správy a servingu modelů jsou klíčové nástroje jako TensorFlow Serving, KubeFlow a MLflow. TensorFlow Serving je systém pro nasazení TensorFlow modelů v produkčním prostředí. Poskytuje flexibilní architekturu pro serving modelů s vysokou propustností a nízkou latencí, podporu pro verzování a rollbacky modelů a integraci s ekosystémem TensorFlow.

KubeFlow je open-source platforma pro správu a orchestraci ML workflow na Kubernetes. Umožňuje definovat a spouštět komplexní pipelines pro trénování, evaluaci a serving modelů pomocí deklarativního přístupu. KubeFlow poskytuje komponenty pro experiment tracking, hyperparameter tuning, distribuované trénování a škálování modelů v produkčním prostředí.

MLflow je platforma pro správu životního cyklu ML modelů, která se zaměřuje na usnadnění experimentování, reprodukovatelnosti a spolupráce. Poskytuje jednotné rozhraní pro tracking metrik, parametrů a artefaktů experimentů, packaging modelů do standardních formátů a jejich nasazení pomocí různých servingových nástrojů[8].

Mezi specializované bezpečnostní platformy a nástroje s UI schopnostmi patří SIEM, SOAR a EDR řešení. IBM QRadar je příkladem SIEM systému nové generace, který využívá strojové učení a behaviorální analýzu pro detekci hrozeb napříč různými zdroji dat. Dokáže korelovat události ze sítových zařízení, serverů, aplikací a koncových bodů a identifikovat podezřelé vzorce a anomálie v reálném čase.

Demisto je příkladem SOAR platformy, která automatizuje a orchestruje bezpečnostní operace pomocí playbooks a integrace s širokou škálou bezpečnostních nástrojů. Využívá strojové učení pro prioritizaci incidentů, doporučení optimálních akcí a automatické spouštění odpovědí na základě definovaných pravidel a workflow.

CrowdStrike Falcon je EDR řešení, které kombinuje behaviorální analýzu, strojové učení a threat intelligence pro detekci a prevenci hrozeb na koncových zařízeních. Využívá pokročilé UI algoritmy pro identifikaci malwaru, exploitů a podezřelých aktivit v reálném čase a poskytuje forenzní nástroje pro investigaci a reakci na incidenty[9].

[8] HAJIAN, Sara, Francesco BONCHI a Carlos CASTILLO. *Algorithmic Bias: From Discrimination Discovery to Fairness-aware Data Mining.* In: Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining [online]. New York, NY, USA: ACM, 2016, 2016, s. 2125-2126 [cit. 2024-04-19]. KDD '16. ISBN 978-1-4503-4232-2.

[9] BRUNDAGE, Miles, Shahar AVIN, Jack CLARK, et al. *The Malicious Use of Artificial Intelligence*: Forecasting, Prevention, and Mitigation [online]. 2018 [cit. 2024-04-19].

Závěr

Využití UI v kybernetické bezpečnosti představuje významný posun v našich schopnostech čelit stále sofistikovanějším a rychle se vyvíjejícím hrozbám. UI technologie jako strojové učení, hluboké učení a analýza velkých dat umožňují automatizovat a zefektivnit klíčové úlohy, jako je detekce anomálií, analýza malwaru, predikce hrozeb a automatizovaná reakce na incidenty.

Nasazení UI v kyberbezpečnosti však přináší také řadu technologických a etických výzev. Je třeba zajistit kvalitu a reprezentativnost trénovacích dat, řešit problém interpretovatelnosti a vysvětlitelnosti UI modelů, zajistit jejich robustnost vůči adversariálním útokům a pečlivě zvážit etické aspekty jako je ochrana soukromí, transparentnost a fairness.

Aktuální výzkum se zaměřuje na vývoj pokročilých UI technik pro detekci hrozeb, explainable UI, automatizaci bezpečnostních operací, obranu proti útokům na UI modely a využití federated learningu pro spolupráci při zachování soukromí. Zároveň se zkoumají etické a právní implikace využití UI v kyberbezpečnosti a vyvíjejí se rámce pro odpovědný vývoj a nasazení těchto technologií.

Do budoucna lze očekávat, že UI bude hrát stále důležitější roli v kyberbezpečnosti, protože tradiční přístupy již nedostačují k ochraně proti moderním hrozbám. Bude však třeba najít správnou rovnováhu mezi technologickými přínosy a etickými a společenskými dopady těchto technologií. Pouze odpovědným a uvážlivým přístupem k vývoji a nasazení UI v kyberbezpečnosti můžeme plně využít její potenciál pro ochranu našich systémů a dat, aniž bychom ohrozili základní lidská práva a hodnoty.

Seznam použité literatury

BRUNDAGE, Miles, Shahar AVIN, Jack CLARK, et al. *The Malicious Use of Artificial Intelligence*: Forecasting, Prevention, and Mitigation [online]. 2018 [cit. 2024-04-19]. Dostupné z: http://arxiv.org/abs/1802.07228

DANAHER, John. *The Philosophical Case for Robot Friendship*. Journal of Posthuman Studies [online]. 2019, 3(1), 5-24 [cit. 2024-04-19]. ISSN 2472-4513. Dostupné z: doi:10.5325/jpoststud.3.1.0005

GOODFELLOW, I., Bengio, Y. a Courville, A., 2016. Deep Learning. Cambridge, Massachusetts: MIT Press.

HAJIAN, Sara, Francesco BONCHI a Carlos CASTILLO. *Algorithmic Bias: From Discrimination Discovery to Fairness-aware Data Mining*. In: Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining [online]. New York, NY, USA: ACM, 2016, 2016, s. 2125-2126 [cit. 2024-04-19]. KDD '16. ISBN 978-1-4503-4232-2. Dostupné z: doi:10.1145/2939672.2945386

KOUDELA, Lukáš. *Umělá inteligence v kybernetické bezpečnosti*. Acta Informatica Pragensia. 2021, roč. 10, č. 2, s. 110-125. ISSN 1805-4951.

NGUYEN, T. a T. REDDI. *Deep Reinforcement Learning for Cyber Security*. IEEE Transactions on Neural Networks and Learning Systems [online]. 2021, 32(8), 3512-3525 [cit. 2024-04-05]. ISSN 2162-2388. Dostupné z: doi:10.1109/TNNLS.2020.3016969

ROSSI, Francesca. *Building Trust in Artificial Intelligence*. Journal of International Affairs [online]. 2019, 72(1), 127-134 [cit. 2024-04-19]. ISSN 0022-197X. Dostupné z: https://www.jstor.org/stable/26588348

SARKER, I. H. *Machine Learning: Algorithms, Real-World Applications and Research Directions.* SN Computer Science [online]. 2021, 2(3) [cit. 2024-04-05]. ISSN 2661-8907. Dostupné z: doi:10.1007/s42979-021-00592-x

TADDEO, Mariarosaria a Luciano FLORIDI. T*he Debate on the Moral Responsibilities of Online Service Providers.* Science and Engineering Ethics [online]. 2016, 22(6), 1575-1603 [cit. 2024-04-19]. ISSN 1471-5546. Dostupné z: doi:10.1007/s11948-015-9734-1

Kontaktní údaje

Ing. Vladimír Šulc Ph.D.
AMBIS vysoká škola, a.s.
Lindnerova 575/1, 180 00 Praha 8
Tel.: +420 605 714 895
Email: lada.sulc@seznam.cz

Recenzenti:

doc. Ing. Václav Friedrich, Ph.D.
doc. RNDr. Tatiana Hajdúková, PhD.

Umelá inteligencia a informačný chaos: Výzvy v boji proti dezinformáciám

Jana Zachar Kuchtová

Abstrakt: Príspevok je zameraný na problematiku informačného chaosu v kontexte šírenia dezinformácií, v čom zohráva umelá inteligencia významnú rolu. V posledných rokoch nastala éra informačných technológií, za pomocou ktorých je vyhľadávanie, interpretácia a šírenie informácií, tých relevantných ale aj tých nerelevantných, dostupné pre širokú verejnosť. Z bezpečnostného hľadiska je však nevyhnutné sledovať tieto zmeny a identifikovať možné bezpečnostné riziká, ktoré so sebou prinášajú. Tento príspevok bol spracovaný v rámci medzinárodnej vedeckovýskumnej úlohy č.: APZ-OVVP-14-2023 „Dezinformácie ako súčasť hybridných hrozieb pre demokratickú spoločnosť a ich vnímanie študentmi vysokých škôl“ (VÝSK 268).

Kľúčové slová: informačný chaos, dezinformácie, umelá inteligencia

Abstract: The paper focuses on the issue of information chaos in the context of the spread of disinformation, in which artificial intelligence plays a significant role. In recent years, we have entered an era of information technologies that facilitate the search, interpretation, and dissemination of information—both relevant and irrelevant—to the general public. From a security perspective, it is crucial to monitor these changes and identify potential security risks they may pose. This paper was prepared as part of the international scientific research task no. APZ-OVVP-14-2023 "Disinformation as part of hybrid threats to democratic society and their perception by university students" (VÝSK 268).

Key word: artificial intelligence, disinformation, information chaos

Úvod

V ére neustáleho technologického pokroku a informačnej doby sa dezinformácie stávajú závažnou hrozbou pre stabilitu spoločnosti. Neoverené správy môžu spôsobiť veľké škody, ako napríklad rozšírenie paniky, nebezpečného správania sa alebo dezinformovanie verejnosti. Môže ísť o informácie o zdravotných hrozbách, politických udalostiach alebo o iných dôležitých témach.[1] Rozšírenie a dopad dezinformácií sú podnecované rýchlym pokrokom v oblasti technológií umelej inteligencie a automatizácie, ktoré umožňujú zhromažďovanie, spracovanie a šírenie obrovských objemov digitálneho obsahu bez efektívnej ľudskej kontroly. V tomto kontexte nástroje umelého učenia a analýzy dát možno vnímať v dvoch rovinách. V prvej sa stávajú kľúčovými nástrojmi pre identifikáciu, monitorovanie a obmedzenie šírenia dezinformácií. V druhej rovine však môžu byť rovnaké nástroje zneužívané na ich produkciu

[1] Kaščák, M., 2024. Kultúra organizácie verejnej správy a jej význam pre problematiku hybridných hrozieb. In Zvýšenie odolnosti Slovenska voči hybridným hrozbám pomocou posilnenia kapacít verejnej správy: Zborník príspevkov. Bratislava: Akadémia Policajného zboru v Bratislave, 2024, s. 188-193. ISBN 978-80-8293-010-1.

alebo šírenie. Koncept informačného chaosu, ktorý podporujú dezinformácie, nie je len otázkou pretrvávajúcej fluktuácie a neistoty v informačnom ekosystéme, ale aj otázkou podkopávania dôveryhodnosti zdrojov informácií a destabilizácie spoločenských väzieb. Rýchly vývoj technológií, vrátane generatívnych modelov umelej inteligencie, umožňuje neúmerne vysokou rýchlosťou vytvárať autenticky pôsobiaci, falošný informačný obsah. Tento príspevok je zameraný na identifikáciu výziev a možností v boji proti informačnému chaosu a dezinformáciám v kontexte umelého učenia a súvisiacich technológií. Okrem toho sa zdôrazňujú etické a praktické implikácie týchto technologických riešení a potreba komplexného, multidisciplinárneho prístupu, ktorý zahŕňa nielen technologické inovácie, ale aj regulačné, vzdelávacie a sociálne opatrenia na posilnenie informačnej integrity a ochrany verejného záujmu.

Informačný chaos

Tvorcami obsahu v online prostredí, ktorý je prístupný širokým masám, sú nielen oprávnené subjekty zaručujúce určitú kvalitu obsahu, ale aj anonymní prispievatelia s rôznymi zámermi. Výrazný nárast podielu dezinformácií vo verejne dostupných informačných zdrojoch je nazývaný *„infodémia“*. Rozpor informácií zverejnených online vážne ohrozuje stav demokracie na celom svete, bez ohľadu na štátne hranice, a naprieč celým obyvateľstvom.[2] Informačný chaos možno definovať ako informačný priestor preplnený neusporiadaným, často zavádzajúcim alebo neovereným obsahom. Používatelia sú v tomto priestore vystavení nadmernému množstvu informácií, čo vedie k ťažkostiam pri ich spracovávaní a následnom využití. Aby bol človek schopný pochopiť a uvedomiť si informáciu, musí dokázať zachytiť podnet z okolia, zaznamenať ho v mozgu, subjektívne spracovať a prípadne následne poskytnúť reakciu do okolia. Každý príjemca určitej informácie vníma zachytený impulz z okolia na základe iných kritérií a znalostí, pričom ich spracovanie sa značne odlišuje. Jedna informácia obvykle vyvoláva spektrum reakcií od nezúčastnenej a ľahostajnej, až po prudko emotívnu alebo iracionálnu.[3] Tento fenomén sa stal čoraz výraznejším v súvislosti s exponenciálnym nárastom digitálnych médií a sociálnych sietí, blogov a pod., ktoré nemožno považovať za relevantné zdroje informácií, vzhľadom na to, že tie nemusia byť overené a spoľahlivé. Okrem uvedeného je kvôli personalizovaným algoritmom na sociálnych sieťach a vo vyhľadávačoch

[2] Hajdúková, T. – Šišulák, S. 2022. Abuse of modern means of communication to manipulate public opinion. In INTED 2022: International Technology, Education and Development Conference – Conference Proceedings. Barcelona : IATED, 2022, s. 1992. ISBN 978-84-09-37758-9.
[3] Hajdúková, T. 2024. Zdroje informácií alebo dezinformácií? In Auspicia, 2024, roč. 21, č. 1, s. 39. ISSN 2464-7217. DOI: 10.36682/a_2024_1_3.

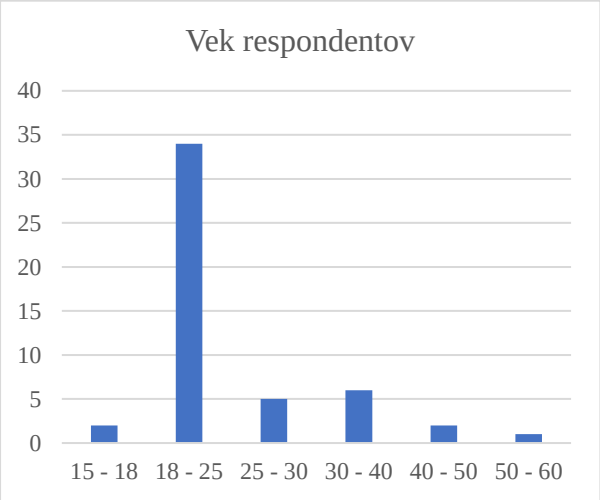
zobrazovaný informačný obsah ovplyvnený, čo môže viesť k monotónnosti zobrazovaných informácií. Medzi faktory prispievajúce k informačnému chaosu patrí **nárast obsahu, dostupnosť tvorby obsahu a absencia filtrov a overenia.** V súčasnosti sa informácie, či už ide o text, videá alebo obrázky, šíria najjednoduchšie a najdostupnejšie prostredníctvom sociálnych sietí. Jedným z hlavných elementov šírenia dezinformácií a vytvárania informačného chaosu je voľba vhodných prostriedkov, ktoré majú byť využité pre dezinformačné účely.[4] Na sociálnych sieťach si môžu používatelia vytvárať účty v priemere od 13 rokov. Následne môžu vytvárať alebo zdieľať príspevky v podobe textu, obrázkov alebo videí, ktoré je možné zverejňovať na svojom používateľskom účte alebo rôznych skupinách. Okrem toho existuje možnosť vytvorenia obsahu na jednej sociálnej sieti a jej automatické alebo manuálne zdieľanie na inej sociálnej sieti (napríklad Facebook a Instagram), čím sa zverejnený príspevok dostane medzi väčší počet používateľov, ktorí ho môžu ďalej zdieľať. Ide o pomerne širokú škálu možností, ako zneužívať aktuálnu dostupnosť tvorby obsahu v digitálnom priestore a zneužívať ju na nepravdivé, zavádzajúce, skreslené, neúplné a/alebo vymyslené informácie v podobe rôznych dezinformácií.[5]

Metodika a cieľ

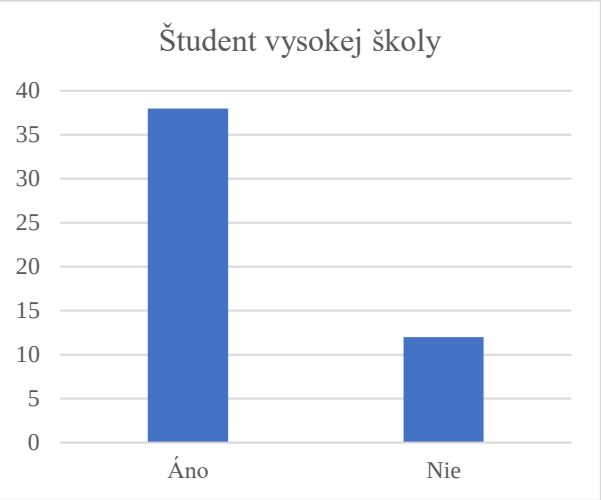
Účelom príspevku je charakterizovať informačný chaos v súvislosti s nástrojmi umelej inteligencie, na základe čoho bol realizovaný prieskum prevažne v prostredí študentov študujúcich na vysokých školách. Dôvodom bola najmä ich prepojenosť s rôznymi technológiami a ich dennodenné využívanie pri štúdiu, práci alebo v súkromí. U uvedených respondentov je vysoký predpoklad, že sa stretli nie len s nástrojmi umelej inteligencie, ale aj ich zneužitím za účelom šírenia dezinformačného obsahu. Súčasťou prieskumu bolo preto identifikovať približnú vekovú škálu respondentov, či ide o aktuálne študujúcich študentov vysokých škôl a aké je ich najvyššie dosiahnuté vzdelanie. Uvedené zaradenie bolo potrebné pri hľadaní súvislosti medzi dosiahnutým vzdelaním a problémom identifikácie relevantných informácií od tých nerelevantných. Aj napriek tomu, že umelá inteligencia (v zmysle jej súčasného interpretovania) nie je nóvum posledného krátkeho obdobia, došlo k jej spopularizovaniu prostredníctvom sprístupnenia nástrojov umelej inteligencie na generatívnu

[4] Ivančík, R. 2021. Základné teoretické a terminologické východiská skúmania problematiky dezinformácií. In Národná a medzinárodná bezpečnosť 2021 – zborník vedeckých príspevkov z 12. medzinárodnej vedeckej konferencie. Liptovský Mikuláš: Akadémia ozbrojených síl generála M. R. Štefánika, 2021, s. 169. ISBN 978-80-8040-606-6.
[5] Ivančík, R. 2024. Dezinformácie ako bezpečnostná hrozba šírená na internete. In Auspicia, 2024, roč. 21, č. 1, s. 27. ISSN 2464-7217. DOI: 10.36682/a_2024_1_2.

tvorbu obsahu všetkým používateľom. Preto bola ďalšou zo zisťovaných oblastí skúsenosť respondentov s takýmito nástrojmi a tiež účel, na ktorý nimi boli využívané. Odpovede nám umožnili vytvoriť si obraz o oblastiach, v rámci ktorých je pre mladých ľudí najatraktívnejšie využívanie nástrojov umelej inteligencie. V nadväznosti na to bola ďalej zisťovaná miera vedomosti o možnosti zneužívania týchto nástrojov na tvorbu a šírenie dezinformácií a skúsenosť samotných používateľov s takto vygenerovaným obsahom. Cieľom prieskumu bolo tiež komparovať presvedčenie respondentov, do akej miery sú schopní rozpoznať obsah vygenerovaný nástrojom umelej inteligencie s ich reálnou úspešnosťou pri identifikovaní pôvodu obrázkov.



Graf 1 Vek respondentov
Zdroj: vlastné spracovanie

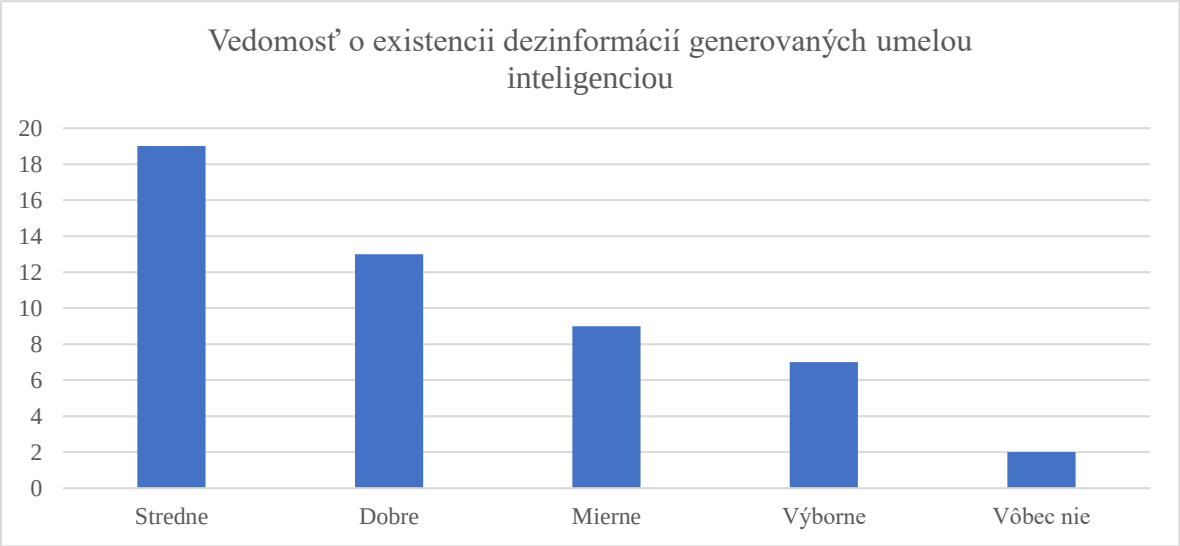


Graf 2 Zaradenie respondentov podľa toho, či študujú na vysokej škole
Zdroj: vlastné spracovanie

Prieskumu sa zúčastnilo 50 respondentov prevažne vo veku od 18 – 25 rokov, pričom 76% všetkých respondentov boli študenti vysokých škôl. Ide o mladých ľudí, ktorí využívajú technológie, sociálne siete a nástroje umelej inteligencie, preto možno konštatovať, že išlo o relevantnú vzorku pre realizovaný prieskum.

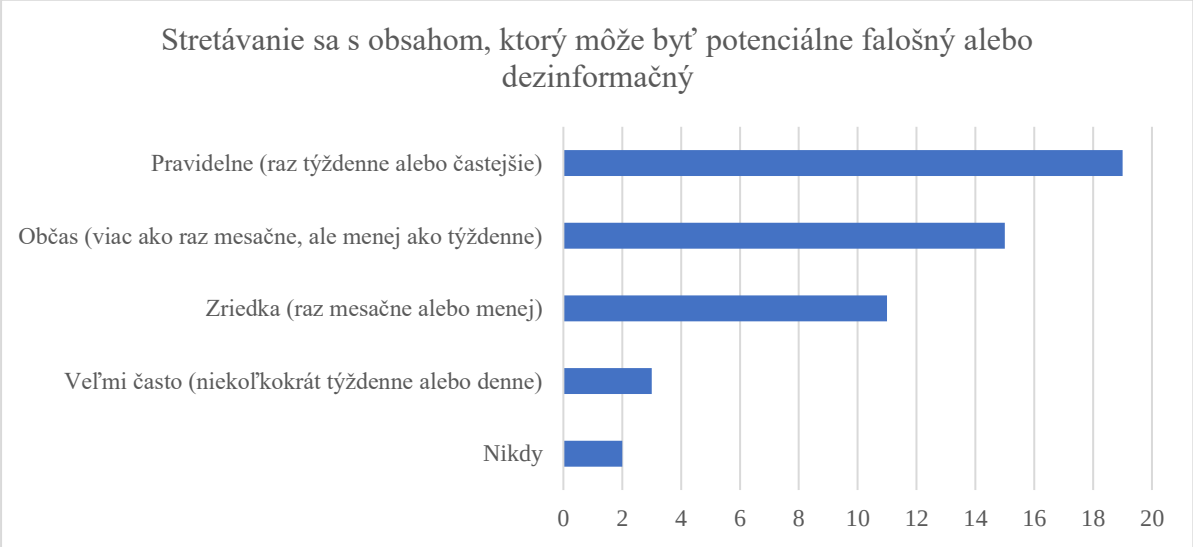
Najčastejšie mali respondenti skúsenosť s nástrojom ChatGPT. Ide o sériu modelov hlbokého učenia, ktoré boli vyvinuté spoločnosťou OpenAI. Tieto modely využívajú architektúru nazývanú GPT (Generative Pre-trained Transformer), ktorá umožňuje spracovávať a generovať text podobný ľudskému jazyku. ChatGPT disponuje schopnosťou porozumieť jazyku a generovať odpovede na základe vstupného textu, čo umožňuje interakciu s používateľmi prostredníctvom konverzácií. Tento nástroj je využívaný na rôzne účely, vrátane

odpovedania na otázky, generovania obsahu a poskytovania asistencie pri riešení problémov.[6] Medzi najčastejšie spôsoby využitia uvádzané respondentmi patria vypracovanie zadaní do školy, resp. domácich úloh, získavanie informácií do prezentácií, seminárnych prác a projektov, vysvetlenie nezrozumiteľnej problematiky, preklady textov, riešenie pracovných úloh, hľadanie odpovedí na rôzne otázky. Menej časté boli uvádzané oblasti zábavy a psychologickej pomoci.



Graf 6 Miera vedomosti o dezinformáciách generovaných nástrojmi umelej inteligencie
Zdroj: vlastné spracovanie

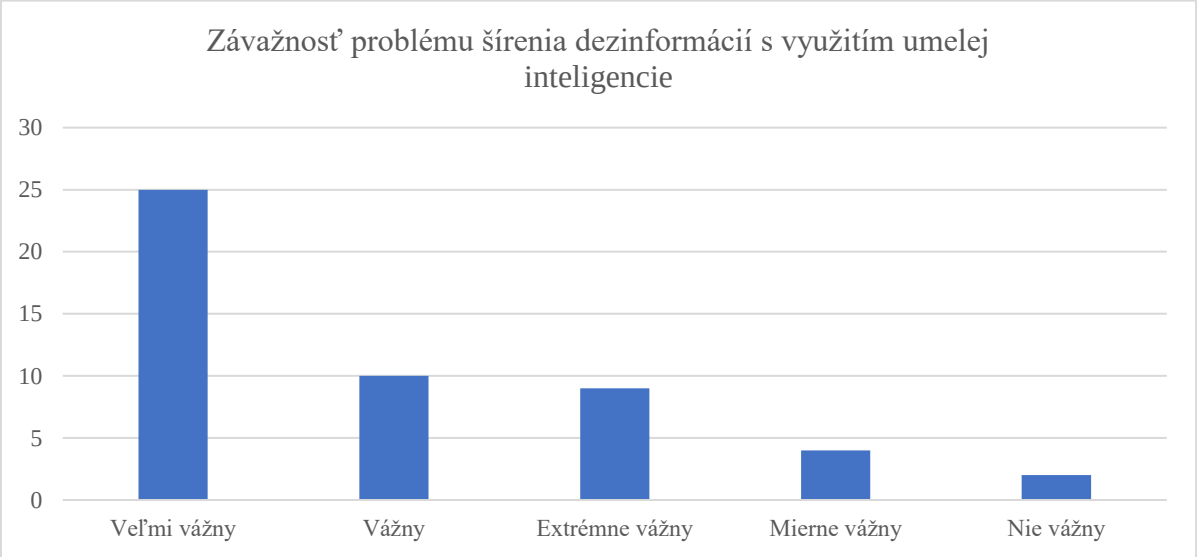
38% respondentov má pocit, že disponujú strednou vedomosťou o existencii dezinformácií generovaných umelou inteligenciou, pričom 4% respondentov vyhodnotili, že ju nemajú vôbec.



Graf 7 Frekvencia stretu s dezinformačným alebo falošným obsahom
Zdroj: vlastné spracovanie

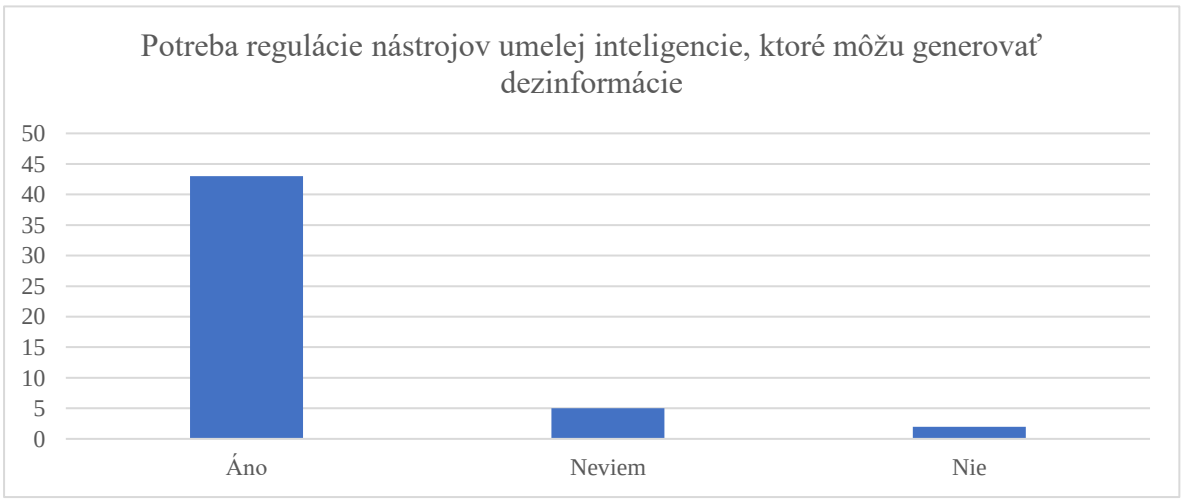
[6] Introducing ChatGPT. [online] [cit. 2024-04-01]. Dostupné na internete <https://openai.com/index/chatgpt/>

Na základe uvedeného grafu je interpretovateľné, že potenciálne falošnému alebo dezinformačnému obsahu sú používatelia vystavovaní pravidelne, aspoň raz do týždňa. Zistená frekvencia síce nie je prekvapivá, ale je nutné si uvedomiť, že vyobrazené zistenie znamená, že používatelia sú pomerne často vystavovaní falošnému, či dezinformačnému obsahu, pričom ide o prípady, v rámci ktorých boli používatelia schopní identifikovať dezinformačný obsah, čo však nevylučuje, že nie sú takémuto obsahu vystavovaní aj častejšie.



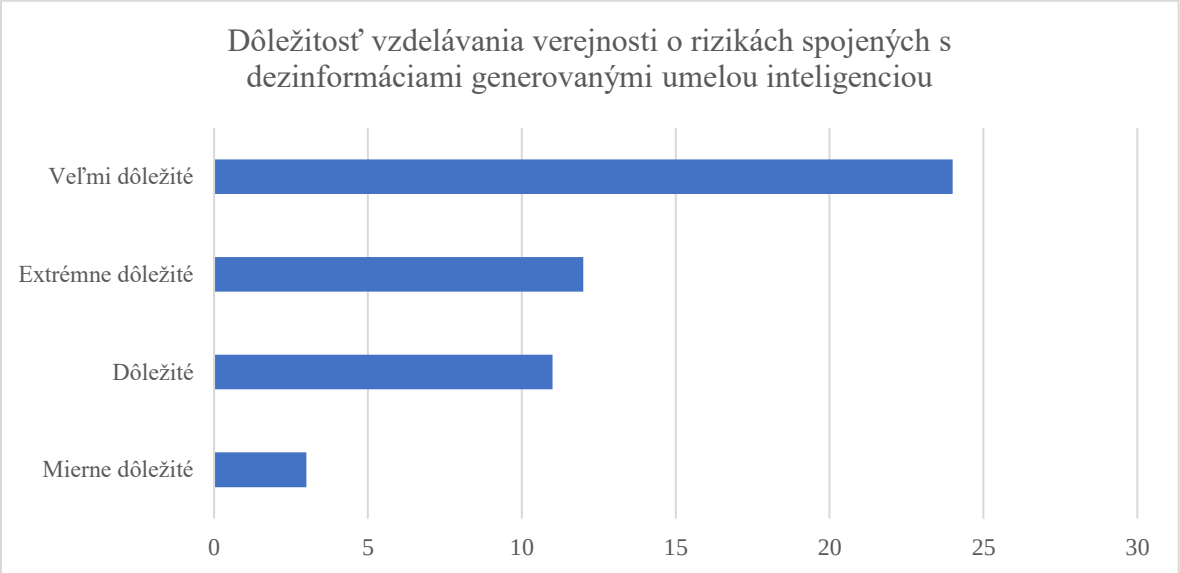
Graf 8 Miera závažnosti šírenia dezinformácií s využitím nástrojov umelej inteligencie
Zdroj: vlastné spracovanie

88% respondentov vyhodnotilo závažnosť šírenia dezinformácií s využitím umelej inteligencie za veľmi vážny, vážny či extrémne vážny. Pri hodnotení závažnosti u respondentov vo významnej miere záleží od ich skúsenosti alebo poznatkoch o dopadoch šírenia dezinformácií.



Graf 9 Vyjadrenie názoru na potrebu regulácie nástrojov umelej inteligencie schopných generovať dezinformácie
Zdroj: vlastné spracovanie

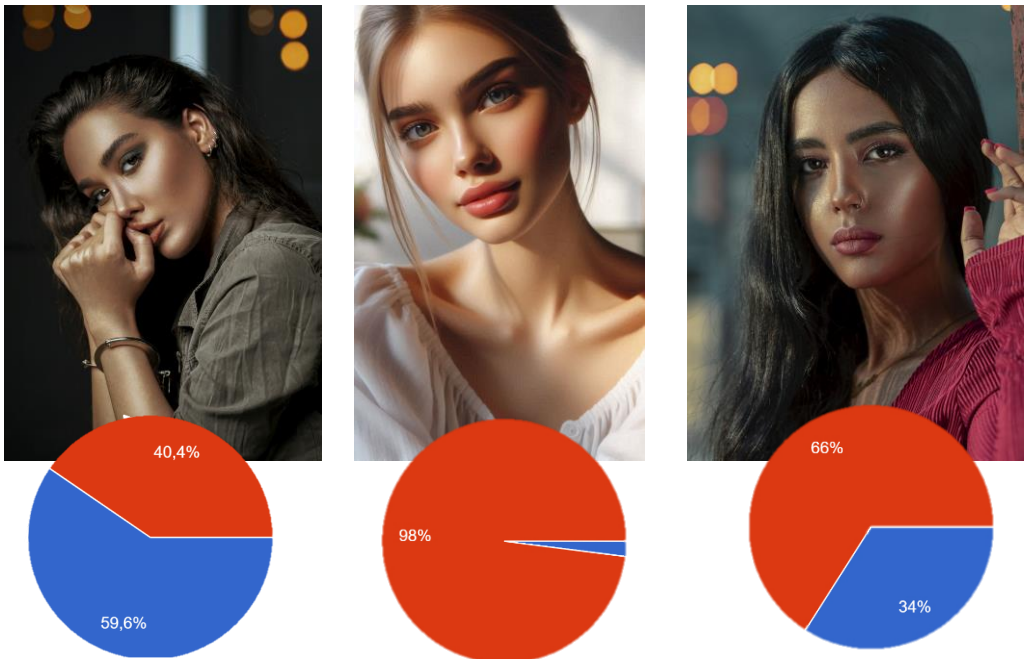
Väčšina respondentov si myslí, že nástroje umelej inteligencie, ktoré môžu byť zneužité na generovanie dezinformácií, by mali byť regulované. Ide napríklad o nástroje na tvorbu Deep fake videí. Technológia deepfake, založená na pokročilých algoritmoch strojového učenia a umelej inteligencie, bola pôvodne vyvinutá a aplikovaná v pornografickom priemysle. Tieto techniky umožňujú generovanie realistických videí, v ktorých sú tváre alebo hlasy osôb syntetický nahradené alebo upravené, čím vytvárajú dojem autenticity, ktorý je ťažko odlíšiteľný od reality. Aj napriek tomu, že táto technológia prináša aj svoje pozitívne prínosy, napríklad v oblasti zábavy, umenia, zdravotníctva, marketingu atď. sa popredné technologické spoločnosti ako Google, Apple, Facebook či Microsoft postavili proti ich využívaniu.[7]



Graf 10 Pohľad na význam vzdelávania verejnosti o rizikách spojených s dezinformáciami generovanými nástrojmi umelej inteligencie
Zdroj: vlastné spracovanie

Nie len študenti študujúci na vysokých školách, čo tvorí nadpolovičnú väčšinu všetkých respondentov, vnímajú dôležitosť vzdelávania verejnosti o rizikách spojených s dezinformáciami generovanými umelou inteligenciou za veľmi dôležitú, čo sa odráža v rastúcom záujme o etické a technologické aspekty umelého učenia. Uvedený výsledok podporuje potrebu systematického vzdelávania v oblasti rozpoznávania a kritického hodnotenia digitálneho obsahu, čo je kľúčové pre ochranu verejného záujmu a intelektuálnu integritu.

[7] Pliešovský, R. Čo je to Deepfake a prečo je nebezpečené? [online] [cit. 2024-04-10]. Dostupné na internete < https://www.techbox.sk/co-je-to-deepfake-a-preco-predstavuje-nebezpecenstvo>



Graf 11 Identifikácia pôvodu obrázkov
Zdroj: vlastné spracovanie

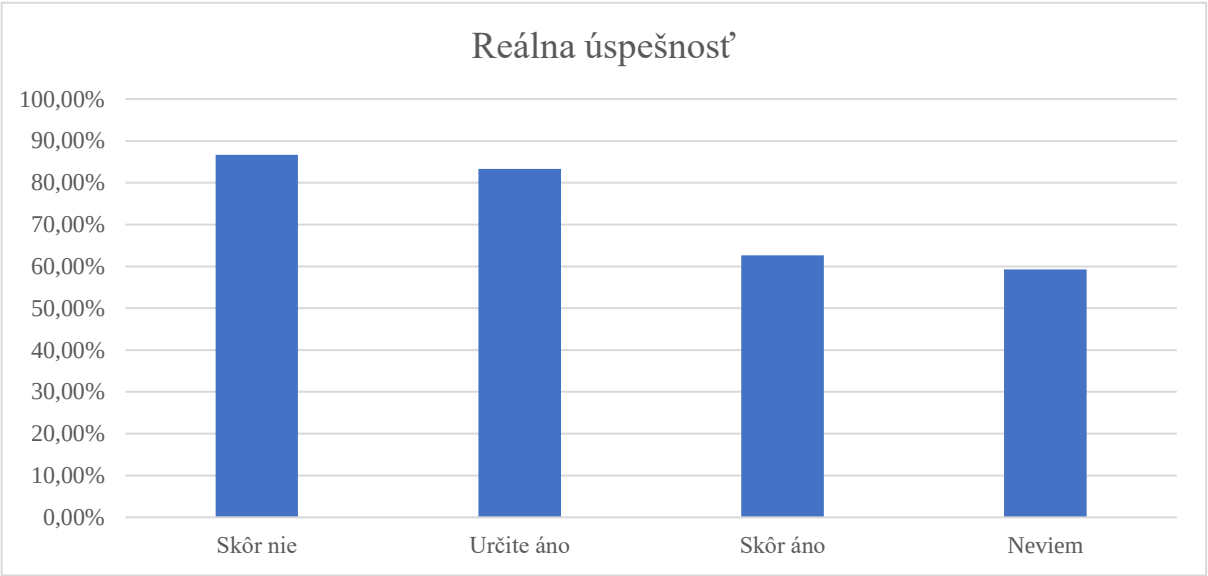
Obrázok 5 Obrázok vygenerovaný Dall-E
Zdroj: Dall-E

Obrázok 5 Reálna fotografia
Zdroj: https://explorecams.com/photos/rdHEk8Dh5P?model=nikon-d7500

Obrázok 5 Reálna fotografia
Zdroj: https://explorecams.com/photos/HOjDgedCg6?model=nikon-d7500

Respondenti mali v rámci prieskumu za úlohu určiť, či zobrazené obrázky sú reálne fotografie alebo ide o obrázky vygenerované nástrojom umelej inteligencie. Prvý a tretí obrázok sú reálne fotografie vyhotovené zrkadlovým fotoaparátom Nikon D7500, druhý obrázok je vyprodukovaný Dall-E 3, nástrojom umelej inteligencie na generovanie obrázkov zodpovedajúcim zadanému textu. Z výsledku je možné identifikovať, že respondenti nemali problém určiť produkt nástroja umelej inteligencie, nakoľko úspešnosť správneho zaradenia uvedeného obrázku je 98%. Čo sa týka prvého obrázku, nadpolovičná väčšina respondentov (59,6%) síce správne označila, že ide o reálnu fotografiu, avšak zvyšných 40,4% respondentov vyhodnotila, že ide o obrázok vygenerovaný umelou inteligenciou. Problematické určenie reálnosti fotografie respondentmi potvrdil tretí obrázok, kde nadpolovičná väčšina 66% respondentov nesprávne vyhodnotila, že ide o obrázok vygenerovaný nástrojom umelej inteligencie. Prieskum zároveň ukázal, že respondenti si relatívne dobre uvedomujú svoje schopnosti identifikovať reálny obsah od obsahu vygenerovaného nástrojmi umelej inteligencie. Tí, ktorí odhadli, že by pravdepodobne nedokázali rozpoznať takýto obsah, potvrdili svoje tvrdenie aj výsledkami testov. Rovnako, respondenti, ktorí si boli istí, že dokážu

správne identifikovať generovaný obsah, väčšinou úspešne rozlíšili medzi reálnym obsahom a obsahom vygenerovaným umelou inteligenciou.

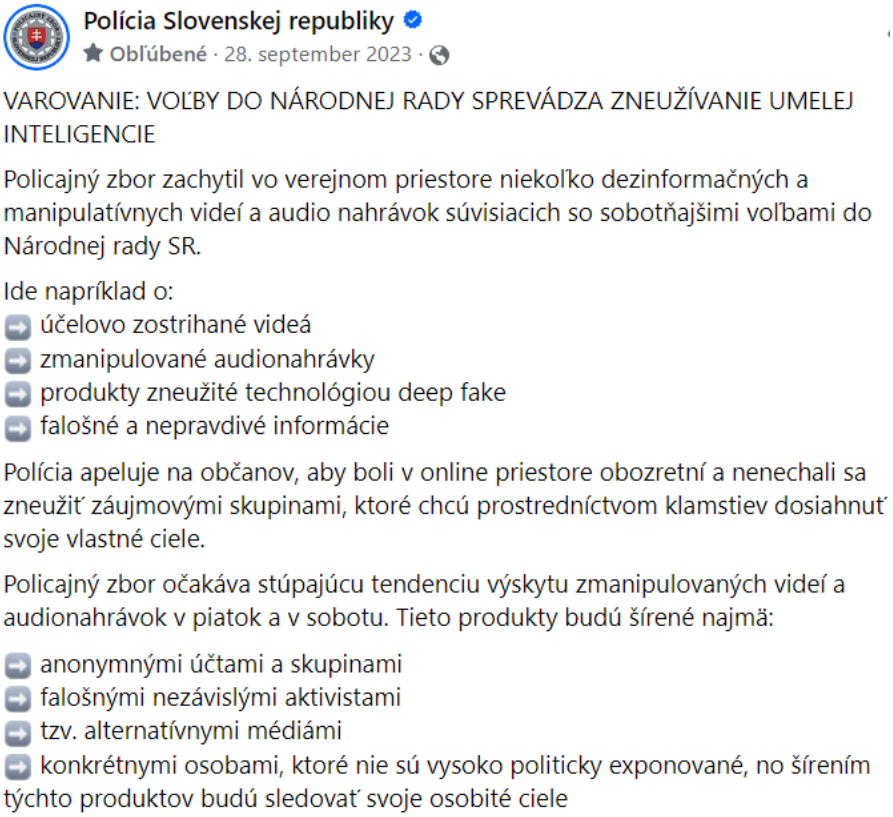


Graf 12 Posúdenie schopnosti rozpoznať falošný obsah generovaný umelou inteligenciou
Zdroj: vlastné spracovanie

Výsledky a diskusia

Problém dezinformácií v spojitosti s nástrojmi umelej inteligencie predstavuje závažný problém pre spoločnosť a bezpečnosť.

Používatelia sú pravidelne vystavovaní dezinformačnému a nerelevantnému obsahu, čo spôsobuje informačný chaos v online priestore a s tým súvisiaci problém identifikácie relevantných informácií. Ide o veľmi vážny problém vyžadujúci si pozornosť nie len bezpečnostných služieb ale aj vedeckých a akademických kruhov. Neustále napredovanie v oblasti technologického pokroku má za následok nevyhnutnosť zvyšovania povedomia ľudí o možnostiach šírenia dezinformácií a vytvárania informačného chaosu prostredníctvom nových nástrojov, akým sú v súčasnosti nástroje umelej inteligencie. Na uvedenom tvrdení sa zhodla nadpolovičná väčšina respondentov z realizovaného prieskumu a to najmä v zmysle voľby vzdelávania za veľmi dôležitý spôsob informovania verejnosti o rizikách spojených s dezinformáciami generovanými umelou inteligenciou. Vzdelávanie v oblasti dezinformácií by malo byť extrémne dôležité a to najmä z dôvodu bezpečnostných rizík a manipulácie s verejnou mienkou. Ako jeden z príkladov možno uviesť ovplyvňovanie volieb, čo môže mať vplyv na ďalší rozvoj krajiny.



Obrázok 6 Varovanie Polície Slovenskej republiky pred zneužívaním umelej inteligencie na ovplyvňovanie volieb do Národnej rady 2023
Zdroj: Facebook Polície Slovenskej republiky

Za pozitívne možno považovať racionálne posúdenie spôsobilosti rozoznať reálny obsah od obsahu vygenerovaného nástrojom umelej inteligencie, nakoľko odhady respondentov, do akej miery si myslia, že sú schopní rozoznať reálny obsah od nereálneho, vo vsokej miere korešpondovali s ich výsledkami. Uvedené zistenia je potrebné verifikovať pokračovaním vo výskume s väčšou vzorkou respondentov a s ďalším materiálom potrebným k rozpoznaniu. Vo výsledku je naznačený problém potrebné ďalej vedecky skúmať.

Záver

Potvrdilo sa, že za jeden z najpodstatnejších spôsobov boja proti informačnému chaosu je zvyšovanie odolnosti spoločnosti voči dezinformáciám, prostredníctvom rozvíjania kritického myslenia, vzdelávania a mediálnej či informačnej gramotnosti.[8] *Kritické myslenie vyžaduje byť neustále v obraze v danej problematike, ale súčasne aj otvorenosť iným názorom*

[8] Ružbacká, M. 2024. Dezinformácie ako hrozba pre spoločnosť a snahy o ich elimináciu. In Auspicia, 2024, roč. 21, č. 1, s. 55. ISSN 2464-7217. DOI: 10.36682/a_2024_1_4.

a schopnosť veľmi rýchlo vyhodnotiť ponúkané alternatívy byť schopný revidovať vlastný názor, bez predsudkov a spoločenských stereotypov.[9]

Je zrejmé, že dezinformácie generované umelou inteligenciou predstavujú vážnu hrozbu pre informačnú integritu a stabilitu spoločnosti. Používatelia sú pravidelne vystavovaní dezinformačnému obsahu, čo len podčiarkuje naliehavosť riešenia tohto fenoménu. Výsledky prieskumu naznačujú, že väčšina respondentov má aspoň základné povedomie o existencii dezinformácií vytváraných umelou inteligenciou a považuje ich šírenie za závažný problém. Napriek relatívne dobrej schopnosti rozpoznať obsah vygenerovaný umelou inteligenciou, existuje značný priestor na zlepšenie tejto zručnosti medzi používateľmi, ktorí nemusia mať také skúsenosti s technickými prostriedkami a aktuálnymi technologickými pokrokmi ako majú študenti vysokých škôl.

Kľúčovým zistením je výrazná podpora respondentov pre reguláciu nástrojov umelej inteligencie, ktoré môžu byť zneužité na produkciu dezinformácií. Vzdelávanie verejnosti o rizikách spojených s týmito technológiami je nevyhnutné pre zníženie ich negatívneho dopadu.

Pre budúce výskumy je odporúčané pokračovať v analýze s väčšou a diverzifikovanejšou vzorkou respondentov a rozšíriť spektrum skúmaných materiálov na identifikáciu dezinformačného obsahu. Okrem toho je nevyhnutné vyvinúť a implementovať komplexný prístup, ktorý zahŕňa technologické, regulačné a vzdelávacie opatrenia. Takýto prístup by mal prispieť k posilneniu informačnej integrity, ochrane verejného záujmu a zvýšeniu odolnosti spoločnosti voči dezinformáciám šíreným prostredníctvom pokročilých nástrojov umelej inteligencie.

Zoznam použitej literatúry

Hajdúková, T. – Šišulák, S. 2022. Abuse of modern means of communication to manipulate public opinion. In INTED 2022: International Technology, Education and Development Conference – Conference Proceedings. Barcelona : IATED, 2022, s. 1992- 2000. ISBN 978-84-09-37758-9.

Hajdúková, T. 2024. Zdroje informácií alebo dezinformácií? In Auspicia, 2024, roč. 21, č. 1, s. 37-49. ISSN 2464-7217. DOI: 10.36682/a_2024_1_3.

[9] Sabayová, M. 2024. Sebavnímanie odolnosti voči dezinformáciám vo vysoko-školskom prostředí. In Auspicia, 2024, roč. 21, č. 1, s. 68. ISSN 2464-7217. DOI: 10.36682/a_2024_1_5.

Introducing ChatGPT. [online] [cit. 2024-04-01]. Dostupné na internete <https://openai.com/index/chatgpt/>

Ivančík, R. 2021. Základné teoretické a terminologické východiská skúmania problematiky dezinformácií. In Národná a medzinárodná bezpečnosť 2021 – zborník vedeckých príspevkov z 12. medzinárodnej vedeckej konferencie. Liptovský Mikuláš: Akadémia ozbrojených síl generála M. R. Štefánika, 2021, s. 165-172. ISBN 978-80-8040-606-6.

Ivančík, R. 2024. Dezinformácie ako bezpečnostná hrozba šírená na internete. In Auspicia, 2024, roč. 21, č. 1, s. 26-36. ISSN 2464-7217. DOI: 10.36682/a_2024_1_2.

Kaščák, M. 2024. Kultúra organizácie verejnej správy a jej význam pre problematiku hybridných hrozieb. In Zvýšenie odolnosti Slovenska voči hybridným hrozbám pomocou posilnenia kapacít verejnej správy: Zborník príspevkov. Bratislava: Akadémia Policajného zboru v Bratislave, 2024, s. 188-193. ISBN 978-80-8293-010-1

Pliešovský, R. Čo je to Deepfake a prečo je nebezpečené? [online] [cit. 2024-04-10]. Dostupné na internete < https://www.techbox.sk/co-je-to-deepfake-a-preco-predstavuje-nebezpecenstvo>

Ružbacká, M. 2024. Dezinformácie ako hrozba pre spoločnosť a snahy o ich elimináciu. In *Auspicia*, 2024, roč. 21, č. 1, s. 50-58. ISSN 2464-7217. DOI: 10.36682/a_2024_1_4.

Sabayová, M. 2024. Sebavnímanie odolnosti voči dezinformáciám vo vysoko-školskom prostředí. In Auspicia, 2024, roč. 21, č. 1, s. 59-71. ISSN 2464-7217. DOI: 10.36682/a_2024_1_5.

Kontaktné údaje

JUDr. Jana Zachar Kuchtová, PhD.
Katedra informatiky a manažmentu
Akadémia Policajného zboru v Bratislave
Email: jana.kuchtova@akademiapz.sk

Recenzenti:

prof. RNDr. Michal Greguš, CSc.
doc. Ing. Václav Friedrich, Ph.D.

Názov: ***Bezpečnosť elektronickej komunikácie 2024***
Recenzenti: prof. RNDr. Michal Greguš, CSc. Dr.h.c.
doc. Ing. Václav Friedrich, Ph.D., Ing. Paed. IGIP
doc RNDr. Tatiana Hajdúková, PhD.
Zostavil: JUDr. Jana Zachar Kuchtová, PhD.
Vydala: Akadémia Policajného zboru v Bratislave
Počet strán: 267
Rok vydania: 2024
Vydanie: 1. vydanie
Jazyková úprava: Rukopis neprešiel jazykovou úpravou
Za obsah publikovaných príspevkov zodpovedajú autori

ISBN 978 – 80 – 8293 – 021 - 7
EAN 9788082930217