Martin Urbančok

Kybernetická bezpečnosť informácií ako zásadný prvok ochrany pred aktuálnymi hrozbami

Anotácia: Pojem kybernetická bezpečnosť predstavuje množinu procesov, technologických riešení a osvedčených postupov, ktoré pomáhajú chrániť systémy a údaje pred neoprávneným prístupom. Súčasné informačné technológie umožňujú jednoducho kopírovať, meniť a vymazávať rôzne údaje, pričom konkrétny páchateľ môže byť stovky i tisícky kilometrov od miesta činu. Tento fakt môže spoločnosti spôsobiť vážne problémy.
Keďže tento vývoj ovplyvňuje aj množstvo informácií, ktoré je možné uchovávať v informačných systémoch, do popredia sa dostáva postavenie kybernetickej bezpečnosti ako nevyhnutnej zložky správneho fungovania počítačových systémov. V počítačových systémoch rôznych druhov sa nachádza nespočetné množstvo rôznych informácií. Tieto informácie je potrebné chrániť pred neustálym nátlakom, a to aj v tom prípade, ak sa nenaplnia hrozby. Už len potenciál útoku, ktorý by v súčasnosti, keď sa informácie ukladajú do digitálnych systémov a na internet, mohol poškodiť či už jednotlivcovi alebo organizácii, vyvíja enormný tlak na organizácie, odborníkov i členov tímov kybernetického zabezpečenia, ktorí sa tieto systémy neustále pokúšajú udržať v prevádzke a informácie nachádzajúce sa v nich uchovať v bezpečí. Na zabezpečenie týchto systémov je potrebné zamerať svoju pozornosť na tie oblasti, ktoré by v kybernetickej bezpečnosti mohli do budúcnosti predstavovať hlavné prostriedky ich zabezpečenia.

Kľúčové slová: kyberzločin, opatrenia, kybernetická bezpečnosť, malvér.

Úvod

Komunikačné technológie a informačné technológie predstavujú užitočný nástroj, ktorý človek každodenne používa k uľahčeniu vykonávanej činnosti. V prvom rade je potrebné uviesť, že pojem komunikačné technológie a informačné technológie nepredstavuje iba pevnú podobu technológií, akými sú server alebo počítač, ale i programy, celé siete a aplikácie, ktoré spolu navzájom komunikujú. Existencia komunikačných a informačných technológií je pre fungovanie spoločnosti nevyhnutná. Toto tvrdenie je podporené aj tým faktom, že komunikačné a informačné technológie sú pevne a dlhodobo zakotvené v každej inštitúcií a sektore moderného sveta. Takéto technológie umožňujú elektronicky vyhľadávať, prenášať, zaznamenávať, šíriť a spracovávať informácie. Ide teda o kombináciu komunikačných a informačných technológií, ktoré vplývajú na činnosti štátov, podnikov, organizácií, domácností a podobne. V súvislosti s touto témou je veľmi podstatné neustále upozorňovať a zvyšovať povedomie spoločnosti o možných nebezpečenstvách spojených s problematikou používania moderných komunikačných technológií v kybernetickom priestore.

Kybernetický priestor možno chápať ako digitálne prostredie tvorené informačnými a komunikačnými technológiami, ktorých informácie vznikajú a spracovávajú sa a následne dochádza k ich výmene. Kybernetický priestor nie je nijakým spôsobom fyzicky ohraničený, preto o tomto priestore možno povedať, že ide o nekonečné digitálne prostredie, ktoré je nehmotné a v ktorom sa zaobchádza s informáciami prostredníctvom systémov prepojených sieťou vrátane pripojenia k verejnej sieti internetu. Tvoria ho prvky informačných a komunikačných technológií, ktoré pomocou protokolu TCP/IP vytvárajú globálnu počítačovú sieť.[1] Kybernetický priestor vytvoril človek, no práve on človek v tomto priestore predstavuje najslabší článok reťazca. Kybernetický priestor v súčasnosti pripomína bojisko. Bežní používatelia kybernetického priestoru o tomto prirovnaní k bojisku ani netušia, no informačné systémy organizácií, sektorov a štátov sú neustále pod tlakom potencionálnych pokusov o rôzne útoky. Najvýstižnejším vysvetlením pre kybernetický útok je to, že ide o akýkoľvek typ útočnej akcie, ktorá je primárne zameraná na zariadenia osobných počítačov, počítačové informačné systémy a infraštruktúru. Aký je teda najbežnejší kybernetický útok? Na túto otázku neexistuje

[1] KOLOUCH, J., P. BAŠTA a kol. *Cybersecurity,* s. 57.

trvalá odpoveď, pretože metódy útoku klesajú a strácajú na popularite. [2] Technologické inovácie vrátane inovácií v oblasti kybernetickej bezpečnosti sa stávajú súčasťou konfrontácie a rastúceho napätia v politických, hospodárskych a bezpečnostných oblastiach. [3] Presúvaním obrovského množstva informácií do kybernetického priestoru sa spolu s technickým pokrokom stupňuje obava v oblasti zraniteľnosti informačných systémov. Táto obava pramení z prepojenia medzi jednotlivými štruktúrami. Vzájomné prepojenie a závislosť medzi informačnými štruktúrami postupom času vyžadujú čoraz viac opatrení na účel zabezpečenia požadovanej úrovne ochrany kybernetického priestoru. Týmto spôsobom je potrebné reagovať na nebezpečenstvo, ktoré ohrozuje počítačové siete a chránené záujmy. Zabezpečovanie informácií a obmedzenie potenciálu ich straty predstavuje základnú úlohu kybernetickej bezpečnosti. Kybernetická bezpečnosť nemá jednu ustálenú definíciu, pre mnohých ľudí však predstavuje oblasť, ktorou sa zaoberajú len kybernetickí odborníci. Toto tvrdenie nie je pravdivé. Každý jeden používateľ, ktorý denne či sporadicky využíva akúkoľvek formu komunikačných a informačných technológií, predstavuje určitú priamu súčasť tejto štruktúry a takisto istú úroveň zabezpečenia kybernetického priestoru. Nezodpovední používatelia alebo používatelia nezasvätení do problematiky svojím konaním často uľahčujú uskutočňovanie kybernetických útokov. Kybernetickú bezpečnosť možno chápať aj ako schopnosť informačného systému alebo siete odolávať škodlivým aktivitám a náhodným udalostiam, ktoré môžu negatívne ovplyvniť princípy kybernetickej bezpečnosti. Tieto princípy sú využívané formou troch triád kybernetickej bezpečnosti, ktoré tvoria:

- CIA – dostupnosť, celistvosť a dôvernosť,
- prvky kybernetickej bezpečnosti a teda procesy, technológie a ľudia,
- životný cyklus kybernetickej bezpečnosti ako prevencia, reakcia a detekcia.

Triáda označovaná ako CIA predstavuje najpoužívanejšiu triádu kybernetickej bezpečnosti. Na to, aby sa dosiahla optimálna úroveň kybernetickej bezpečnosti, je však nevyhnutná implementácia ďalších princípov. Triáda CIA sa dá všeobecne definovať ako vlastnosť systému, ktorá zaručuje bezchybnosť, správnosť a úplnosť údajov a informácií.[4] Úlohou kybernetickej bezpečnosti je zaistiť bezpečnosť kybernetických a informačných technológií, čiže predovšetkým bezpečnosť údajov a informácií, ktoré sú pomocou týchto prvkov spracovávané, uchovávané a prenášané. S cieľom akéhokoľvek zabezpečiť štruktúru je potrebné najprv ju určiť, keďže na zabezpečovanie týchto informácií sú vynaložené enormné finančné prostriedky, ako aj celý rad určitých obmedzení pri spracúvaní informácií. Na základe dokonalej analýzy rizík je možné stanoviť požadovanú úroveň ochrany pre túto informáciu.

Dostupnosť v triáde predstavuje používateľnosť a prístupnosť služieb alebo systémov založenú na žiadosti oprávneného subjektu. Predstavuje priestor, v ktorom sa jednotlivé princípy pretínajú v prieniku jednotlivých princípov.

Celistvosť v triáde je istá bariéra, ktorá zabraňuje zásahu do informácií, údajov, kybernetických a informačných technológií, systémov a ich nastavení alebo modifikácií inou osobou ako osobou, ktorá je na to riadne oprávnená. Na účel zachovania dôveryhodnosti údajov sa tieto údaje nesmú upravovať, poškodzovať či úplne odstrániť neautorizovaným subjektom.

Dôvernosť v triáde zabezpečuje súkromie tak, aby k informáciám, údajom alebo ku komunikačným a informačným technológiám nemohli získať prístup neoprávnení používatelia.

---

[2] ANDERSEN, Ian., *Top 12 Most Common Types of Cyber attacks. [online]. [cit. 21.10.2025]. Dostupné na internete: https://netwrix.com/en/resources/blog/types-of-cyber-attacks/*

[3] NÁRODNÝ BEZPEČNOSTNÝ ÚRAD. *Národná stratégia kybernetickej bezpečnosti na roky 2021 až 2025*. s.5. [online]. [cit. 21.10.2025]. Dostupné na internete: https://www.nbu.gov.sk/data/att/2759.pdf

[4] *Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti, §3*.

Pri uvedenom musí byť zabezpečený prístup k týmto informáciám pre autorizovaných používateľov. Jedným z najdôležitejších aspektov informačnej bezpečnosti je udržiavanie dôvernosti informácií. Pre zabezpečenie dôvernosti prostredníctvom šifrovania a iných nástrojov zároveň napĺňa význam princípu integrity.

Podľa viacerých názorov je v súčasnosti triáda postačujúca. Ak však vezmeme do úvahy úvahy rýchlosť, ktorou sa dnešné technológie inovujú a vyvíjajú, v budúcnosti už táto triáda v súčasnej podobe s najväčšou pravdepodobnosťou postačovať nebude. Isté zdroje tvrdia, že daná triáda už v súčasnosti nie je postačujúca a mala by byť rozšírená minimálne o ďalšie tri prvky, ktorými sú:

- Autentickosť je narušená v momente, keď dôjde k sfalšovaniu elektronického podpisu, no zároveň nebola narušená integrita dôvernosť ani dostupnosť.
- Užitočnosť vzniká v situáciách, v ktorých dôjde ku strate kľúča od zašifrovaných údajov. V takej situácii sú údaje stále dostupné, ale nie je možné ich použiť, čím strácajú svoju užitočnosť.
- Kontrola alebo držanie má zabraňovať neoprávnenej osobe získať kontrolu nad informáciami či systémom, ku ktorým nemá mať prístup. Ak nastane takáto situácia, znamená to stratu vlastníctva alebo kontroly, čo sa bude považovať za krádež civilnej informácie.

Spojením triády a vyššie uvedených prvkov by vzniklo zoskupenie, ktoré sa nazýva Parkerianova šestica, pričom autorom tejto myšlienky je osoba Donn B. Parker. Pre vyššie uvedené je potrebné spomenúť tvrdenie, že kybernetická bezpečnosť znamená zachovanie dôvernosti, integrity a dostupnosti informácií v kybernetickom priestore.[5] Pod pojmom prvky kybernetickej bezpečnosti je potrebné rozumieť prvky, ktorých vzájomné prepojenie umožňuje zavrieť alebo vytvoriť kybernetickú bezpečnosť. Prvkami kybernetickej bezpečnosti sú procesy, technológie a ľudia. Kybernetika sa neustále zlepšuje a extrémne rýchlo sa vyvíja.
Je teda zrejmé, že nie je reálne pravdivo tvrdiť, že organizačné opatrenia a systémy slúžiace na jej ochranu budú postačujúce aj v budúcnosti. Na základe uvedeného je nevyhnutné zdokonaľovať nielen systémy na zabezpečenie, ale i verejné povedomie o rizikách v kybernetickom priestore. Aj v prípade, že by bol bezpečnostný systém takmer dokonalý, stále nemožno vylúčiť ľudský faktor a možnosť mechanického zlyhania. Prvky kybernetickej bezpečnosti predstavujú činnosť, ktorú je potrebné vynaložiť, aby informačné a komunikačné technológie a s nimi spojené služby mohli byť bezpečné a jednoducho prístupné pre ľudí. Týmito procesmi môžu byť testovanie zabezpečenia jednotlivých počítačových systémov, aktualizácia a údržba služieb a systémov, audit kybernetickej bezpečnosti a rôzne iné. Hlavnou funkciou daných procesov je pokúsiť sa zabrániť incidentu skôr, než sa stane to, čo predstavuje ich preventívnu funkciu.

V dnešnej modernej ére technológia predstavuje určitý prostriedok slúžiaci na uľahčenie života, pričom z hľadiska kybernetickej bezpečnosti technológia môže slúžiť nielen ako ochranný, ale aj ako útočný nástroj. Pre bežného používateľa technológia predstavuje možnosť prístupu k rôznym informáciám a sociálnym sieťam prostredníctvom internetu. Moderné technológie nám umožňujú komunikovať s inými osobami v reálnom čase na dlhé vzdialenosti. Ďalej nám umožňujú snímať za pár sekúnd fotografie a videá vo vysokom rozlíšení, ktoré je následne možné ukladať, upravovať, prijímať i odosielať. Zabezpečenie týchto technológií by malo dosahovať úroveň rozumne vynaložených finančných prostriedkov, ktorých výška by nemala presahovať určitú úroveň chráneného záujmu. Metódy ochrany informácií na technickej úrovni sú založené na ochrane hardvérových komponentov informačno-komunikačných

[5] MAKATURA, I., *Základy bezpečnostných opatrení – príručka manažéra kybernetickej bezpečnosti*, s. 4.

systémov.[6] Rýchly vývoj technológií si neustále vyžaduje inovácie technológií v kybernetickej bezpečnosti, čo má za následok, že niektoré systémy nemusia byť po krátkom čase od jej vyvinutia alebo aktualizácie dostačujúce pre zachovanie svojho riadneho účelu, a teda pre udržanie potrebnej úrovne kybernetickej bezpečnosti. Posledným, no najdôležitejším prvkom kybernetickej bezpečnosti, sú ľudia. Vo svete existuje určité tvrdenie, že systém je taký silný, aký je jeho najslabší článok. Z tohto dôvodu ľudia predstavujú cieľ kybernetických útokov. Nezastaviteľný pokrok a vývoj technológií ich používateľom neumožňuje, aby sa náležite adaptovali na všetky novovzniknuté možnosti útoku v kybernetickom priestore. V cykle kybernetickej bezpečnosti je z hľadiska dlhodobej realizácie nevyhnutné upravovať vyššie uvedenú triádu, ako aj čiastkové prvky kybernetickej bezpečnosti. V tomto prípade ide o detekciu, prevenciu a odpoveď na útok.

Pojem hrozba v oblasti kybernetickej bezpečnosti je možné chápať ako predpoklad zničenia alebo poškodenia chráneného záujmu v kybernetickom priestore ohrozením jednotlivou hrozbou. Takáto hrozba pôsobí na najzraniteľnejšie miesta každého systému. Priame ohrozenie chráneného záujmu vyplýva z predpokladaného rizika. Priame ohrozenie chráneného záujmu vzniká zo zraniteľnosti i z kybernetických hrozieb. Kybernetický priestor sa v súčasnosti čoraz viac využíva na uľahčenie plnenia rôznych úloh, komunikácie medzi jednotlivcami, organizáciami i štátmi. Pod pojmom chránený záujem alebo aktívum možno rozumieť čokoľvek hmotné či nehmotné, čo má určitú hodnotu pre jednotlivca, organizáciu, štát a podobne. Aktívum nemusí nevyhnutne znamenať, že ide o predmet, môže ísť aj o službu, reputáciu alebo ľudí. Proces analýzy predpokladaných udalostí vychádza z hodnotenia rizík, ktoré môžu mať za následok znehodnotenie hodnoty chráneného záujmu, zničenie alebo poškodenie služieb alebo systémov. Predmetné hodnotenie vychádza z výsledkov hodnotenia zraniteľnosti a hrozieb s cieľom identifikovať a hodnotiť riziko z hľadiska predpokladu výskytu možných negatívnych následkov. Môže sa vykonávať na akejkoľvek úrovni riadenia rizika s rôznymi cieľmi a s rôznou užitočnosťou informácií, ktoré sa týmto hodnotením získajú. V metodike Národného bezpečnostného úradu sa uvádzajú tri rôzne postupy, ktorými je možné analyzovať riziká. Každý z týchto postupov má svoje úrovne zložitosti a svoje výhody i nevýhody.

Prístup orientovaný na aktíva a dopady:

- Identifikuje zraniteľnosti týkajúce sa udalosti ohrozujúcich kritické aktíva, ktoré by mali vážny priaznivý vplyv na tieto aktíva.
- Umožňuje analyzovať dôsledky hrozieb a udalostí.
- Určuje kritické aktíva pre činnosť organizácie.

Prístup orientovaný na hrozby:

- Identifikuje zraniteľnosti v kontexte týchto hrozieb.
- Pomáha vytvárať scenáre a modely hrozieb.
- Zaisťuje zdroje potencionálnych hrozieb a udalostí.

Prístup orientovaný na zraniteľnosti:

- Identifikuje hrozby v súvislosti s identifikovanými zraniteľnosťami.
- Identifikuje zneužiteľné zraniteľnosti.
- Rozpoznáva predpokladané podmienky.

[6] KOSTREC, M. a E. KOSTRECOVÁ. *Metódy ochrany policajne relevantných informácií. Záverečná správa čiastkovej vedecko-výskumnej úlohy*, s. 70.

Všeobecné trendy a hrozby:

Za nárast sofistikovanosti sú zodpovední útočníci, ktorí využívajú čoraz pokročilejšie techniky a nástroje často s využitím umelej inteligencie. To v sebe zahŕňa sofistikovanejšie phishingové kampane, prispôsobivý malvér a deepfake videá na manipuláciu. Phishingové kampane sú podvodné aktivity, ktorých cieľom je získať viaceré citlivé informácie od obetí tým, že sa útočníci vydávajú za dôveryhodné subjekty alebo osoby v elektronickej komunikácii. Tieto informácie môžu zahŕňať:

- **Prihlasovacie údaje:** používateľské mená a heslá.
- **Osobné údaje:** rodné čísla, dátumy narodenia, adresy.
- **Finančné údaje:** čísla bankových účtov, čísla platobných kariet a ich CVC kódy, PIN kódy.
- **Iné citlivé informácie:** rodné priezvisko matky, odpovede na bezpečnostné otázky.

Prispôsobivý malvér predstavuje určitý typ softvéru, ktorý sa v kybernetickom priestore správa škodlivým spôsobom. V čase svojho vzniku infiltroval asi 10 % počítačov pripojených k sieti Arpanet, čím spôsobil škodu v miliónoch dolárov.[7] Uvedený softvér pri svojich činnostiach mení svoju vnútornú štruktúru, správanie i kód. Cieľom tohto správania je vyhnúť sa detekcii jednotlivými bezpečnostnými nástrojmi. Jednotlivé bezpečnostné nástroje, ktorým sa vyhýba, sú systémy detekcie narušenia a antivírusové programy. Vyššie uvedené teda predstavuje snahu prispôsobivého malvéru o adaptáciu v napadnutom systéme s cieľom zostať v ňom funkčný a skrytý v čo najdlhšom čase. Predmetná adaptácia do systému môže prebiehať viacerými spôsobmi, medzi ktoré zaradujeme polymorfizmus a metamorfizmus. Správanie malvéru sa prispôsobuje prostrediu prostredníctvom modulárnej štruktúry a dynamického sťahovania modulov. Pojem polymorfizmus znamená to, že malvér pri každej svojej replikácií alebo infekcií mení svoj vlastný vnútorný kód. Pri svojej činnosti v systéme využíva rozdielne techniky, napríklad pre usporiadanie blokov kódu, vkladanie nepodstatného kódu alebo zmenu poradia inštrukcií. Zmenou kódu sa malvér snaží zmeniť i svoj podpis s cieľom skomplikovať detekciu založenú na porovnávaní podpisov s databázami známych signatúr, pričom jeho funkcionalita pri zmene kódu zostáva zachovaná a nezmenená. Metamorfický malvér predstavuje ďalšiu pomyselnú úroveň prepisovania svojho kódu v porovnaní s polymorfným malvérom, keďže metamorfický malvér pri každej replikácií kompletne prepisuje celý svoj kód. Pre bližšie vysvetlenie – metamorfický malvér vo svojej podstate nemá svoj stály kód, ale pri svojej replikácií generuje svoj celý nový kód, pričom si ponecháva svoju škodlivú funkčnosť. Predmetný malvér používa viaceré techniky, napríklad odstraňovanie blokov kódu, náhradu inštrukcií ekvivalentnými inštrukciami alebo tiež zmenu toku riadenia. Metamorfický mavér je jednoznačne zložitejší a náročnejší na vývoj ako polymorfický malvér, je však oveľa účinnejší pri obchádzaní signatúrovej detekcie. Správanie malvéru sa prispôsobuje prostrediu, pričom realizácia predmetného konania spočíva v tom, že konkrétny malvér dokáže detekovať svoje prostredie a na základe výsledkov z detekcie prostredia dokáže zmeniť svoje správanie. Aby sa malvér vyhol detekcii v kontrolovanom prostredí, zmení svoje správanie tak, že zostane neaktívny alebo zmení svoje správanie do takej miery, ktorá sa prejavuje neškodne, v napadnutom systéme však následne aktivuje svoju negatívnu, a teda škodlivú funkciu. Dynamické sťahovanie modulov a modulárna štruktúra predstavujú konanie malvéru tak, že môže v sebe obsahovať určitú časť, ktorá po vniknutí do systému sťahuje ďalšie moduly, ktoré aktivujú svoju nežiadúcu, škodlivú funkciu, napríklad sťahovanie hesiel, zakódovanie súborov. Ich detekcia na základe statickej analýzy je náročná, pretože tieto moduly sa môžu meniť v čase. Jednou z najväčších hrozieb pre organizácie akejkoľvek veľkosti sú ransomvérové útoky.

[7] EUROPEAN COMMISION. *Cybersecurity*, s. 13.

Predmetné útoky spočívajú v tom, že útočníci zašifrujú určité údaje obetí a potom od nich za ich odšifrovanie alebo obnovenie požadujú nejaké plnenie. Nejde pritom iba o jednostranné útoky, ale i o mnohostranné útoky s cieľom vydierať poškodených. Využívanie umelej inteligencie na nekalé účely predstavuje určitú dvojsečnú zbraň, pričom na jednej strane umelá inteligencia pomáha pri ochrane prostredníctvom detekcie anomálií, na druhej strane však umelú inteligenciu útočníci využívajú na vytváranie sofistikovaných útokov či automatizáciu škodlivých aktivít. Útoky útočníkov smerujú prevažne na organizácie a spoločnosti, ktoré sú menej zabezpečené a ktoré pôsobia v dodávateľskom reťazci. Takéto útoky majú v sebe určitý skrytý účel. Ich účelom je dostať sa cez predmetné dodávateľské spoločnosti k ich partnerom, ktorí sú pre útoky omnoho zaujímavejší. Ďalšími druhmi kybernetických útokov sú útoky, ktorých podnetom je geopolitické napätie, ktoré vedie k zvýšeniu počtu kybernetických útokov financovaných štátmi alebo štátnymi inštitúciami so zameraním sa na špionážnu činnosť a ohrozenie kritickej infraštruktúry. Medzi zraniteľné oblasti kybernetických útokov môžeme zaradiť i zdravotnícke zariadenia, napríklad zdravotnú poisťovňu Dôvera, ktorá v minulosti musela čeliť viacerým kybernetickým útokom. Tento príklad predstavuje momentálnu rastúcu tendenciu kybernetických útokov smerujúcich voči organizáciám tohto druhu.

Pod pojmom decentralizácia kyberzločinu sa rozumie významný a narastajúci trend v kybernetickej bezpečnosti. Tento trend sa naplno prejavuje v roku 2025, kedy zo zaužívaných hierarchických a organizovaných zločineckých skupín pôsobiacich v kybernetickom priestore sa ich rozpadom stávajú menší, flexibilnejší a anonymní aktéri. Pri svojich činnostiach vykonávajú súčinnosti na viacerých úrovniach, pričom používajú decentralizované technológie. Pojem decentralizácia kyberzločinu sa vyznačuje určitými črtami, medzi ktoré patrí zníženie významu a postavenia centralizovaných gangov. Na rozdiel od minulého trendu, keď vznikali rozsiahle a stabilne štruktúrované skupiny či organizácie, dnes ich rozklad alebo vznik nových subjektov umožňuje, aby sa štruktúrou jednoduchšie a menšie skupiny, organizácie alebo aj jednotlivci zameriavali na plnenie konkrétnych špecifických úloh. Na plnenie čo najväčšieho utajenia nelegálnych finančných tokov je možné vyššie uvedenými skupinami, organizáciami a jednotlivcami využívať kryptomeny, napríklad Monero a Bitcoin. Medzi ďalšie typické znaky decentralizácie kyberzločinu môžeme zaradiť darknetové trhoviská. Darknetové trhoviská sú určité skryté platformy v online formáte, ktoré majú za účel obchodovanie s nelegálnymi službami a nelegálnymi obchodmi s rozličným tovarom. Medzi ďalšie platformy môžeme zaradiť aj malvér ukradnutých dát i kybernetických útokov, ktorý predstavuje obchodovanie so službou pre objednávateľa. Darknet neslúži iba na vyššie uvedené účely, keďže prostredníctvom fóra, nástrojov a iných skrytých spôsobov komunikácie kyberzločinci zdieľajú vedomosti, nástroje a môžu kooperovať na kybernetických útokoch bez akejkoľvek potreby existencie organizačnej štruktúry. Súčasné trendy vývoja kyberzločinov smerujú k vytváraniu malých skupín a jednotlivcov, ktorí sa sústreďujú na určité konkrétne časti kybernetického útoku. Medzi tieto časti môžeme zaradiť vývoj malvéru, získavanie prístupov, legalizáciu príjmov z trestnej činnosti. Medzi výhody, ktoré pre kyberzločincov predstavuje decentralizácia, môžeme zaradiť jednoznačne zvýšenú mieru anonymity, pretože decentralizácia a kryptomeny sťažujú individuálnu identifikáciu jednotlivých páchateľov protiprávnej činnosti. Decentralizácia a kryptomeny majú za následok i zvýšenie odolnosti voči snahe o likvidáciu organizácie tvorenej kyberzločincami. Rozptýlená infraštruktúra sa dá totiž dá omnoho zložitejšie zlikvidovať ako centralizované servery. Jednotlivci, ktorí majú určité zručnosti v oblasti kyberzločinu, majú jednoduchú možnosť svojimi schopnosťami prispievať k páchaniu kyberzločinu, a to bez potreby svojej účasti v určitej organizačnej štruktúre. Ak nie je stanovená organizačná štruktúra páchateľov kyberzločino, je veľmi náročné odhaliť lídrov a dôležitých členov zoskupenia. Decentralizácia siete vytvára možnosť efektívne a rýchlo sa prispôsobovať zmenám v oblasti kybernetickej bezpečnosti a takisto možnosti pre útoky.

Súčasné hrozby a incidenty na Slovensku

Kybernetický útok cielený na kataster nehnuteľností v januári roku 2025 poukázal na možnú a reálnu zraniteľnosť dôležitých systémov obsahujúcich veľké množstvo informácií, ktoré môžu byť použité nežiadúcim spôsobom. Tento kybernetický útok na infraštruktúru štátu upozornil na vysokú mieru ohrozenia predmetných systémov, pričom ich najzraniteľnejšou časťou je ich samotný správca – teda človek. Systém bezpečnostných opatrení v danom prípade zlyhal. Kataster nehnuteľností Slovenskej republiky bol upozorňovaný na nedostatky zabezpečenia vo svojom systéme, teda na zvýšenú možnosť úspešného vykonania kybernetického útoku. Na tieto upozornenia však príslušné orgány nereagovali správne. Ochrana pred kybezločinmi spočíva v prevencii a ochrane. Kým prevencia sa sústreďuje na to, aby žiadny kybernetický útok nenastal, ochrana systému kybernetický útok odvracia. Ochrana pred kybernetickými útokmi je ucelený, stále sa vyvíjajúci celok, ktorý vyžaduje neustálu súčinnosť subjektov – jednotlivcov, skupiny, organizácie či štátu. V súčasnosti sú najdôležitejšími určité skupiny opatrení, medzi ktoré patria opatrenia pre jednotlivcov, organizácie a opatrenia pre úroveň štátnych organizácií.

Medzi opatrenia pre jednotlivcov môžeme zaradiť jednoznačne unikátne a silné prístupové heslá. Vo viacerých opatreniach je uvedené používanie unikátnych a silných hesiel pre všetky online účty, pričom sa odporúča tieto heslá v žiadnom prípade nerecyklovať. Najefektívnejšou formou prevencie proti zneužitiu hesla alebo jeho prekonaniu je používanie správcu hesiel. Ďalej sa odporúča používanie dvojitej autentifikácie, ktorá sa aktivuje tam, kde je to potrebné alebo dôležité pre spravovanie účtov v rôznych oblastiach (napríklad bankovníctvo, e-mail a podobne). Ďalšou oblasťou, v ktorej sa odporúča prijatie bezpečnostných opatrení proti kybernetickým útokom, je obozretnosť pri podozrivých správach. V tejto oblasti treba byť ostražitý v prípade nežiadúcich elektronických správ v podobe e-mailov, podozrivých telefonátov, správ na sociálnych sieťach, ktorých obsah nekorešponduje s realitou alebo ktoré obsahujú žiadosti o interakciu adresáta správy. Predmetné správy môžu od ich adresátov požadovať i poskytnutie citlivých informácií rôzneho charakteru, ktoré v prípade, že sa žiadateľovi poskytnú, môžu sa stať predmetom ich zneužitia alebo vydierania. S cieľom zamedziť protiprávnemu konaniu je dôležité venovať svoju pozornosť verifikácii informácií priamo pri ich zdroji. V tejto oblasti je takisto potrebné preverovať bezpečnosť prehliadania internetu. Pri uvedenom je dôležité kontrolovať, či sa internetový odkaz začína skratkou https://, pričom netreba zabúdať i na overenie, či konkrétna stránka má bezpečnostný certifikát. Jedným z najdôležitejších opatrení je jednoznačne i potreba aktualizovania softvéru zariadenia – antivírusového softvéru. Na účel zachovania bezpečnosti v spoločnostiach aj v súkromnej sfére je nevyhnutní, silným a bezpečným heslom chrániť Wi-Fi sieť, pričom treba upriamiť svoju pozornosť i na použitie WPA3 šifrovania. Opatrenia, ktorými by sme sa mali riadiť pri prihlasovaní sa do internetovej siete, spočívajú aj v tom, že s cieľom udržať čo najvyššiu mieru bezpečnosti, je potrebné vyhýbať sa prihlasovaniu do verejných Wi-Fi sietí, ktoré sú spravidla nezabezpečené a voľne prístupné. Ak je ale v určitom momente potrebné pripojiť sa do takýchto sietí, spravidla sa odporúča prihlásenie do siete VPN, teda do virtuálnej privátnej siete. Aktuálne odporúčania pre jednotlivcov obsahujú i odporúčanie pravidelné zálohovať údaje, a to dvomi odporúčanými spôsobmi. Prvým spôsobom je zálohovanie údajov na externý harddisk. Druhým odporúčaným spôsobom ukladania dôležitých údajov sú cloudové úložiská. Tieto opatrenia sa vzťahujú na prípady, v ktorých sa v prípade ransomvérového útoku zamedzí možnosť útočníka požadovať výkupné za obnovenie uzamknutých alebo odcudzených údajov. Medzi určité možnosti na vykonávanie

prevencie pred nežiadúcimi kybernetickými útokmi môžeme zaradiť aj možnosť vzdelávania a informovanosti širokej verejnosti o tejto problematike. Je potrebné zameriavať sa na všetky vekové a sociálne kategórie subjektov. Ako ďalšie odporúčanie na účel prevencie a ochrany voči kyberzločinom môžeme uviesť vyhýbanie sa zdieľania osobných informácií online formou. Je potrebné zvážiť, aké informácie ako používatelia na rôznych sociálnych sieťach zdieľame, aby sme zabránili ich zneužitiu inou stranou, ktorá tieto informácie môže použiť na páchanie protiprávnej činnosti.

Ďalší druh opatrení súvisí s organizáciami, aby zaviedli komplexné bezpečnostné postupy a politiky, v ktorých sa určujú jasné pravidlá, ako pristupovať k údajom, používať zariadenia a internet. Bezpečnostné hrozby môžu mať svoj pôvod nielen vo fyzickom svete, ale aj v kybernetickom priestore. Bezpečnostné požiadavky sú kľúčové pre posúdenie dopadu kybernetických hrozieb na aktíva organizácie.[8] Medzi opatrenia vzťahujúce sa na organizácie je potrebné zaradiť aj školenia jednotlivých zamestnancov, pretože ľudský faktor predstavuje v problematike kyberzločinu najslabší článok. Zvýšenie povedomia o bezpečnosti, implementácia bezpečnostných politik a tréning zamestnancov sú len niektoré z opatrení, ktoré môžu byť účinné pre zníženie rizík a zlepšení celkovej bezpečnosti organizácie.[9] Pri opatreniach zameraných na organizácie je dôležité zahrnúť aj používanie pokročilých bezpečnostných technológií, pričom sa odporúča zavádzanie firewallov, systémov prevencie a detekcie narušenia a ďalších bezpečnostných nástrojov. V súčasnosti nastupuje trend overovať bezpečnosť a zraniteľnosť systému a infraštruktúry organizácie aj prostredníctvom nezávislých odborníkov. Jedným z opatrení, ktoré môže organizácia vykonať na elimináciu nebezpečenstva kybezločinov, je určenie prístupov a privilégií k jednotlivým údajom na rôznych úrovniach po jednotlivom uvážení pre konkrétnych používateľov. V tejto oblasti je potrebné prideľovať len tie nevyhnutné práva, ktoré jednotlivci potrebujú na výkon svojich pracovných povinností. Takéto prerozdelenie prístupov je potrebné systémovo kontrolovať a monitorovať ich dodržiavanie. Aby sa dosiahla maximalizácia úrovne bezpečnosti a ochrany pred kyberzločinom, je potrebné sledovať akékoľvek podozrivé správanie a odhaliť ho v čo najkratšom časovom horizonte. Včasnou reakciou na kybernetický útok sa vytvorí časový fond na jeho reakciu voči nemu, ktorá by mala byť vopred stanovená. Je teda potrebné, aby organizácia už vopred vedela, akým spôsobom bude reagovať na predpokladaný kybernetický útok. Organizácie si musia vopred stanoviť presný plán, ako budú postupovať v prípadoch kybernetického útoku. V tomto pláne je potrebné stanoviť identifikáciu útoku, jeho izolovanie, následnú obnovu a komunikáciu. Kontrola, monitorovanie a zaznamenávanie aktivít by nemalo byť zamerané len na vnútorné procesy organizácie, ale aj na to, čo sa deje smerom von. Pri tomto smere kontroly a monitoringu by sa jednotlivé organizácie mali zameriavať i na preverovanie dodávateľov prostredníctvom zavádzania bezpečnostných opatrení.

Netreba pritom zabúdať aj na ďalšie opatrenia pre organizácie i jednotlivcov, ktorými sú zálohovanie či obnova rôznych potrebných alebo cenných údajov. Tento druh opatrenia si vyžaduje pravidelné overovanie funkčnosti procesov obnovy. Kontrola a monitoring predstavujú zásadnú zložku bezpečnosti v súvislosti s kyberzločinom, preto je dôležité vychádzať zo zásady nulovej dôvery voči každému používateľovi a ku každému zariadeniu pred tým, ako sa mu pridelí prístup k zdrojom. Uvedené je potrebné vykonávať bez ohľadu na to, či sa nachádzajú v internej alebo externej sieti. Na zavádzanie bezpečnostných opatrení nie je súčasnosti organizácia odkázaná sama. Ak ide o väčšie aj menšie organizácie, je potrebné zvážiť i možnosť outsourcingu vybraných bezpečnostných činností prostredníctvom na to špecializovaných externých firiem.

---

[8] RUBISOVÁ, I. a V. HOLUBICZKY. *Dvadsať rokov Slovenskej republiky v Európskej únii – prínosy, výzvy očakávania*, 54 s.

[9] ANDRAŠKO, J., M. MESARČÍK a P. SOKOL. *Právo kybernetickej bezpečnosti,* 39 s.

V neposlednom rade treba uviesť aj opatrenia určené pre úroveň štátnych organizácií. Na tejto úrovni opatrení kooperujú viaceré inštitúcie, medzi ktoré môžeme zaradiť i Národné centrum kybernetickej bezpečnosti, ktoré pri svojej činnosti poskytuje informácie, varovania i koordináciu vo sfére kybernetickej bezpečnosti. S Národným centrom kybernetickej spolupracuje aj organizácia Slovak National CERT, ktorá sa vo svojej činnosti zaoberá riešením kyberneticko-bezpečnostných incidentov a v rámci uvedenej problematiky sa využíva aj medzinárodná spolupráca. Kybernetické hrozby a ohrozenia vo všeobecnosti predstavujú potencionálne riziko pre narušenie bezpečnosti. Takéto narušenia bezpečnosti môžu spôsobiť straty, ujmy a škody na úžitkových hodnotách, a teda negatívne ovplyvniť život jednotlivca a fungovanie inštitúcií, podnikov a štátu.[10] Jednou z foriem opatrení je i zavádzanie, vytváranie a aktualizovanie zákonných predpisov zaoberajúcich sa kybernetickou bezpečnosťou. Uvádzanie a aktualizovanie je veľmi potrebné, pretože zákony a predpisy musia vychádzať z aktuálneho stavu. Je preto potrebné poukázať na neustály vývoj kybernetickej kriminality ktorý má spravidla časový náskok pred legislatívou. Tá sa snaží predmetný časový náskok v čo najkratšej miere skracovať. Skracovanie náskoku sa nemusí realizovať len uvádzaním aktualizácií do legislatívy, ale i podporou vzdelávania, čiže zvyšovania povedomia v oblasti kybernetickej bezpečnosti medzi občanmi jednotlivých štátov alebo i v jednotlivých podnikateľských sférach. Preto je nevyhnutné, aby jednotlivé štáty medzi sebou spolupracovali a odovzdávali si potrebné informácie, inovácie a skúsenosti v predmetnej oblasti. Uvedené je obsiahnuté i v opatreniach zameraných na medzinárodnú spoluprácu v oblasti boja proti kybernetickej kriminalite páchanej cezhraničnou formu. Jednou z neoddeliteľných súčastí opatrení proti kybernetickej kriminalite je aj podpora a rozvoj kybernetickej bezpečnosti, a to najmä prostredníctvom výskumu a vzdelávania vo vzdelávacích inštitúciách. Kybernetické hrozby pochádzajú z mnohých zdrojov, ako sú nepriateľské vlády, teroristické skupiny, nespokojní zamestnanci a zlomyseľní votrelci.[11] Všetky uvedené opatrenia smerujú i k ochrane kritickej infraštruktúry štátu, medzi ktoré je možné zaradiť ochranu finančného sektoru, zdravotníctva, dopravy a energetiky, pričom na ich ochranu je potrebné klásť zvláštny dôraz.

Záver

Cieľom príspevku bolo stručne objasniť aktuálne kybernetické hrozby súvisiace s používaním moderných technológií a zároveň opísať najčastejšie páchané druhy kybernetických zločinov. Prínosom článku bolo upriamiť pozornosť na aktuálne hrozby v kybernetickom priestore, objasniť spôsoby páchania týchto protiprávnych konaní a zároveň predstaviť príklady preventívnych a represívnych opatrení zameraných na ich elimináciu.

Kybernetická bezpečnosť predstavuje určitý neustále vyvíjajúci sa proces inovácií, pri ktorom nie je možné určiť, akým smerom sa v budúcnosti bude uberať. Nebezpečenstvo kybernetických útokov hrozí nielen jednotlivcom, ale i organizáciám neštátneho i štátneho charakteru. Z toho dôvodu bolo potrebné v článku venovať pozornosť opatreniam určeným pre túto kategóriu subjektov. Keďže používateľ pôsobiaci v kybernetickom priestore predstavuje najslabší článok bezpečnostného systému, táto kapitola sa zameriava na možné opatrenia, ktorých cieľom je eliminovať bezpečnostné hrozby vyplývajúce z ľudských chýb, nedostatkov či nevedomosti, ktoré je možné obmedziť vykonaním viacerých opatrení. Tieto opatrenia sa nevzťahujú len na ľudský faktor, ale aj na organizácie súkromného a štátneho sektoru. Opatrenia na elimináciu kybernetickej kriminality a kybernetických bezpečnostných hrozieb budú vždy o určitý pomyselný krok pozadu za súčasným stavom, a preto je potrebné zamerať

[10] LEVICKÝ, D. *Úvod do kybernetickej bezpečnosti*, s. 19 – 21.
[11] TAYLOR, H. *What Are Cyber Threats and What to Do About Them*, s.7.

pozornosť na ich dôsledné dodržiavanie, aby sa zabezpečila maximálna miera možnej ochrany ohrozených subjektov. Tento článok sa preto zameriava aj na zvýšenie povedomia spoločnosti o možných hrozbách, ktorým sú subjekty v kybernetickom priestore vystavené, keďže aj zvýšené povedomie môže v jednotlivých používateľských subjektoch vyvolať potrebu neustálej opatrnosti pri používaní technológií, ktoré sú súčasťou ich každodenného života.

Literatúra

AHMED AL ZAIDY. *What Are Cyber Threats and What to Do About Them.* [online]. [cit. 21.10.2025]. Dostupné na internete: https://www.researchgate.net/publication/349043516_What_are_Cyber-Threats_Cyber-Attacks_and_how_to_defend_our_Systems

ANDERSEN, Ian. *Top 12 Most Common Types of Cyber attacks*. [online]. [cit. 21.10.2025]. Dostupné na internete: https://netwrix.com/en/resources/blog/types-of-cyber-attacks/

ANDRAŠKO, Jozef, Matúš MESARČÍK a Pavol SOKOL. *Právo kybernetickej bezpečnosti.* Bratislava: Univerzita Komenského v Bratislave, 2022, 186 s. ISBN 978-80-7160-632.

EUROPEAN COMMISION. *Cybersecurity*, 2020, ISBN 978-92-76-19957-1.

KOLOUCH, Jan, Pavel BAŠTA a kol. *Cybersecurity. Praha: CZ.NIC, 2019, ISBN 978-80-8816-831-7.*

KOSTREC, Matej a Eva KOSTRECOVÁ. *Metódy ochrany policajne relevantných informácií,*

Záverečná správa čiastkovej vedecko-výskumnej úlohy. - 1. vyd. - Bratislava: *Akadémia Policajného zboru*. 2016, ISBN 978-80-8293-040-8.

LEVICKÝ, Dušan. *Úvod do kybernetickej bezpečnosti. Elfa, Košice*, 2019, ISBN 978-80-8086-276-3.

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD. *Národná stratégia kybernetickej bezpečnosti na roky 2021 až 2025.* [online]. [cit. 21.10.2025]. Dostupné na internete: https://www.nbu.gov.sk/data/att/2759.pdf

RUBISOVÁ, Ivana a Vincent HOLUBICZKY. *Dvadsať rokov Slovenskej republiky v Európskej únii – prínosy, výzvy očakávania*. *Bratislava: Akadémia Policajného zboru*, 2024, ISBN 978-80-8293-034-7.

Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti

Key words: cybercrime, measures, cybersecurity, malware.

Summary

The aim of the paper was to briefly explain current cyber threats when using modern technologies and also describe the most frequently committed types of cybercrimes. The asset of this study is to draw attention to current threats in connection with cyberspace, point out the methods of committing the relevant illegal acts, and also provide examples of measures aimed at preventing and repressing the given threats.

Cybersecurity represents a constantly evolving process of innovation, in which it is impossible to determine which direction it will take in the future. The danger of cyber attacks threatens not only individuals but also non-state and state organizations, therefore, in this article it was necessary to pay attention to the measures intended for this category of entities. Since

the user operating in cyberspace, that is, a person, represents the weakest link in the security system, it was necessary to present possible measures aimed at eliminating the security threats resulting from human errors, shortcomings or ignorance, which can be reduced by implementing several measures. These measures are not directed only against human factors, but also against private and state sector organizations. Measures aimed at combating cybercrime and cyber security threats will always get behind the current state, and that is why attention must be focused on their proper compliance in order to ensure the maximum possible level of protection for threatened entities.

This article is therefore also aimed at increasing society's awareness of the possible threats to which entities in cyberspace are exposed, because even seeming awareness can trigger in individual users the need for constant caution when using technologies that are a part of our everyday lives.

kpt. Mgr. Martin Urbančok
Interný doktorand
Akadémia Policajného zboru
Sklabinská 1
835 17 Bratislava 35
e-mail: martin.urbancok@akademiapz.sk

Recenzenti: mjr. PhDr. Vladimír Malíček, PhD.,
mjr. JUDr. Michaela Jurisová, PhD.