Akadémia Policajného zboru v Bratislave
Katedra informatiky a manažmentu

Vedecká konferencia

AKTUÁLNE VÝZVY KYBERNETICKEJ BEZPEČNOSTI

2022

Zborník príspevkov

Bratislava
2023

AKADÉMIA POLICAJNÉHO ZBORU V BRATISLAVE
Katedra informatiky a manažmentu

ZBORNÍK PRÍSPEVKOV

z vedeckej konferencie

Aktuálne výzvy kybernetickej bezpečnosti

2022

konanej dňa 15. 12. 2022

pod záštitou rektorky Akadémie Policajného zboru v Bratislave
Dr. h. c. prof. JUDr. Lucie Kurilovskej, PhD.

Bratislava 2023

VEDECKÝ VÝBOR KONFERENCIE:

Dr. h. c. prof. JUDr. Lucia KURILOVSKÁ, PhD. (Akadémia PZ v Bratislave)

JUDr. Michal MARKO PhD. (Akadémia PZ v Bratislave)

prof. Ing. Antonín KORAUŠ, PhD., LL.M., MBA (Akadémia PZ v Bratislave)

doc. Ing. Stanislav ŠIŠULÁK, PhD. (Akadémia PZ v Bratislave)

Mgr. Rastislav JANOTA (Národný bezpečnostný úrad, Národné centrum kybernetickej bezpečnosti SK-CERT)

Mgr. Matej ŠALMÍK (Národný bezpečnostný úrad, Národné centrum kybernetickej bezpečnosti SK-CERT)

Ing. Ivan MAKATURA (Kompetenčné a certifikačné centrum kybernetickej bezpečnosti SR)

plk. gšt. v. z doc. Ing. Radoslav IVANČÍK PhD. et PhD., MBA, MSc. (Akadémia PZ v Bratislave)

ORGANIZAČNÝ VÝBOR KONFERENCIE:

JUDr. Matej KOSTREC, PhD. (Akadémia PZ v Bratislave)
Mgr. Štefan ZACHAR, PhD. (Akadémia PZ v Bratislave)

RECENZENTI:

doc. RNDr. Bohumír ŠTĚDROŇ, PhD.
RNDr. Eva KOSTRECOVÁ, PhD.

ZOSTAVIL:

Mgr. Štefan ZACHAR
JUDr. Matej KOSTREC, PhD.

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

ISBN 978-80-8054-998-5
EAN 9788080549985

OBSAH

ÚVODNÉ SLOVO

Dobrý deň, vážené dámy, vážení páni,

milé kolegyne a kolegovia, vzácni hostia!

Vojnový konflikt na Ukrajine, ekonomická kríza, balíčky reštrikčných opatrení a vysoká inflácia, to všetko sú aktuálne skutočnosti, ktoré sa premietajú aj do digitálneho priestoru. Ataky na vládne infraštruktúry, manipulácia s informáciami, ovplyvňovanie ľudského vedomia, skresľovanie reálnych situácií prostredníctvom sociálnych sietí, undergroundové aktivity a ďalšie nekalé zneužívanie kybernetických prostriedkov si vyžaduje zvýšenú pozornosť, ktorú je potrebné venovať kybernetickej bezpečnosti. Táto skutočnosť si však vyžaduje aj navýšenie počtu odborníkov zameraných na ochranu digitálneho priestoru pred jeho zneužívaním. Jedným z hlavných cieľov súčasnosti je preto aj marginálne zvýšenie možností vzdelávania v oblasti kybernetickej bezpečnosti na akademickej pôde.

Vážené dámy a páni,

som veľmi rád, že na dnešnej vedeckej konferencii, pod názvom ***„Aktuálne výzvy kybernetickej bezpečnosti 2022“***, ktorá sa už tradične koná pod záštitou rektorky Akadémie PZ v **Bratislave Dr. h. c. prof. JUDr. Lucie Kurilovskej, PhD.,** môžem osobne privítať pána prorektora pre informatizáciu a koordináciu s policajnou praxou *pplk. JUDr. Michala Marka, PhD.*. Zároveň mu ďakujem za jeho podporu a účasť.

Moje meno je Matej Kostrec a v mene vedeckého a organizačného výboru Vás vítam na dnešnej konferencii, ktorou vás budem sprevádzať.

Želám nám všetkým úspešný a bezproblémový priebeh konferencie a veľa inšpiratívnych podnetov pri riešení aktuálnych otázok spojených so zabezpečením kybernetickej bezpečnosti.

mjr. JUDr. Matej KOSTREC, PhD.

Katedra informatiky a manažmentu

Akadémie PZ v Bratislave

CIELE KONFERENCIE

Hlavným cieľom konferencie je vymedzenie a analyzovanie aktuálnych trendov spojených s kybernetickou bezpečnosťou, zovšeobecnenie teoretických prístupov a praktických skúseností kompetentných subjektov jednotlivých bezpečnostných zložiek a iných relevantných subjektov ako základného predpokladu pre vytvorenie systematického prístupu k oblasti kybernetickej bezpečnosti a systému vzdelávania v štátnej a verejnej správe. K ďalším cieľom konferencie patrí identifikácia predpokladov a teoretických väzieb na prepojenie teórie s aplikačnou praxou, ako aj zabezpečenie transferu relevantných poznatkov do praxe subjektov štátnej a verejnej správy pre empirické skúmanie špecifických problémov a aktuálnych potrieb bezpečnostnej praxe v oblasti zvyšovania úrovne kybernetickej bezpečnosti SR.

TEMATICKÉ ZAMERANIE KONFERENCIE

V zmysle vytýčených cieľov a obsahového zamerania konferencie sa budú jednotlivé vystúpenia a prezentované príspevky koncentrovať najmä na nasledovné okruhy súvisiace s predmetnou problematikou:

- vedecké základy vzťahu ľudského faktora a kybernetickej bezpečnosti,
- možnosti a perspektívy vzdelávania v oblasti kybernetickej bezpečnosti,
- certifikácia v oblasti kybernetickej bezpečnosti,
- východiská skvalitňovania spolupráce Akadémie Policajného zboru v Bratislave s ostatnými vysokými školami doma i v zahraničí, ako aj s inými inštitúciami v oblasti kybernetickej bezpečnosti s jej dopadom na systém odborného vzdelávania nielen študentov ale aj zamestnancov štátnej a verejnej správy,
- bezpečnosť občana v kybernetickom prostredí, možnosti ochrany občana v oblasti kybernetickej bezpečnosti (od analýzy hrozieb, pomoci bezpečnostných zložiek občanovi až po vzdelávanie),

Pôjde predovšetkým o riešenie nasledovných otázok:

- aktuálne problémy a výzvy ochrany kybernetického priestoru,
- postavenie a úlohy orgánov pri realizácii bezpečnosti kybernetického priestoru,
- certifikácia a vzdelávanie manažérov a audítorov kybernetickej bezpečnosti,
- organizácia a pôsobnosť jednotiek pre riešenie kybernetických incidentov,
- postavenie manažéra kybernetickej bezpečnosti,
- technické aspekty kybernetickej bezpečnosti - analýza rizík, odhaľovanie a dokumentovanie bezpečnostných incidentov,
- úlohy Akadémie Policajného zboru v Bratislave vyplývajúce z realizácie Koncepcie kybernetickej bezpečnosti SR vo vzťahu k vzdelávaniu príslušníkov PZ v tejto oblasti,
- spolupráca Akadémie Policajného zboru v Bratislave a Národného bezpečnostného úradu v systéme vzdelávania v oblasti kybernetickej bezpečnosti.

PROGRAM KONFERENCIE

08:00 – 09:00 – prezentácia účastníkov

09:00 – 09:10 – oficiálne otvorenie konferencie Rektorkou Akadémie Policajného zboru v Bratislave a úvodné slovo organizátorov

09:10 – 09:30 – Matej ŠALMÍK - SK-CERT
Možné prístupy k stavbe jednotky CSIRT v akademickom prostredí

09:30 – 09:50 – Ivan MAKATURA - KCCKB
Perspektívy vzdelávania a certifikácie osôb v oblasti kybernetickej bezpečnosti

09:50 – 10:10 – Ľuboš MOTÚZ - MIRRI
Podpora rozvoja kybernetickej bezpečnosti a kritickej infraštruktúry ITVS v rámci projektov MIRRI

10:10 – 10:30 – Ferdinand VAVRÍK - MF SR
Ekosystém riešenia kybernetických bezpečnostných incidentov

10:30 – 11:00 – Coffee break

11:00 – 11:20 – Pavol SOKOL – UPJŠ (on line)
Riešenie bezpečnostných incidentov v akademickom prostredí

11:20 – 11:40 – Roman TUCHYŇA - MICROSOFT
Moderné zabezpečenie koncových staníc

11:40 – 12:00 – Stanislav GULÁŠ - DATAsec
Sociálne inžinierstvo v praxi (ako prebiehajú útoky sociálneho inžinierstva v praxi a ako sa proti nim brániť)

12:00 – 12:20 – Milan HUDEC - Sociálna poisťovňa
Ochrana osobných údajov a neoprávnené prístupy do informačných systémov

12:20 – 12:40 – Radoslav IVANČÍK – Akadémia Policajného zboru
Kybernetická (ne)bezpečnosť a sociálne siete

12:40 – 13:30 – obed

13:30 – 14:30 – diskusia, prijaté závery, ukončenie konferencie

Perspektívy vzdelávania a certifikácie osôb v oblasti kybernetickej bezpečnosti

Ivan Makatura

Abstrakt: *Väčšina organizácií na Slovensku má závažný problém nájsť kvalifikovaných odborníkov v oblasti kybernetickej bezpečnosti. Podľa nedávnych prieskumov chýba približne pätnásťtisíc IT profesionálov, z toho najmenej päťtisíc zameraných explicitne na informačnú a kybernetickú bezpečnosť a riadenie rizík. Kritická je najmä pozícia manažér kybernetickej bezpečnosti ktorej určenie je v zmysle povinnosťou prevádzkovateľov základných služieb v zmysle zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti. Reálny dopyt na trhu práce a disponibilný počet ľudských zdrojov sa v tejto profesii odlišujú v rádovej čiarke. Stav, keď dopyt prevažuje ponuku, generuje tlak na vyššiu cenu práce a možný odliv kvalifikovanej pracovnej sily do zahraničia.*

Saturovanie pracovného trhu požadovanými kvalifikáciami prostredníctvom vysokoškolského vzdelávania štúdium v akreditovaných študijných programoch na vysokých školách je možné očakávať najskôr za 5-10 rokov. Dovtedy je potrebné vykryť požiadavky zamestnávateľov aspoň čiastočne a do zodpovedajúcich pracovných pozícií ustanoviť špecialistov z príbuzných oborov, najmä z oblasti informačných a komunikačných technológií a riadenia iných kategórií rizík. Potrebné je však pripraviť ich na postupné zvládanie špecifických požiadaviek v kybernetickej bezpečnosti .

Jedným z vhodných prístupov môže byť využitie foriem ďalšieho vzdelávania dospelých. Vzdelávanie nadväzujúce na školské vzdelávanie by umožňovalo získať čiastočnú kvalifikáciu, alebo doplniť a rozšíriť si kvalifikáciu nadobudnutú v školskom vzdelávaní.

Prednáška má ambíciu predstaviť čerstvo schválenú vyhlášku Národného bezpečnostného úradu o znalostných štandardoch kybernetickej bezpečnosti a v základnom rozsahu opísať problematiku odborných certifikátov pre oblasť informačnej a kybernetickej bezpečnosti.

Kľúčové slová: *kyberbezpečnosť, vzdelávanie, kvalifikácia, ľudské zdroje*

Abstract: *The majority of organizations in Slovakia are facing a serious challenge in finding qualified professionals in the field of cybersecurity. Recent surveys indicate a shortage of approximately fifteen thousand IT professionals, with at least five thousand specifically focused on information and cybersecurity and risk management. The position of cybersecurity manager is particularly critical, as it is mandatory for operators of essential services under Act No. 69/2018 Coll. on Cybersecurity. The real demand for skilled professionals in this field far exceeds the available human resources. This situation, where demand outweighs supply, generates pressure on higher wages and possible outflow of qualified workforce to foreign countries.*

Saturating the job market with required qualifications through tertiary education in accredited study programs at universities is only expected to happen in 5-10 years. Until then, it is necessary to partially meet the employers' requirements and establish specialists from related fields, particularly in the areas of information and communication technologies and risk management, in appropriate job positions. However, it is crucial to prepare them gradually to handle the specific demands of cybersecurity.

One suitable approach may be to utilize adult education programs. Education that builds on formal schooling could enable individuals to acquire partial qualifications or supplement and expand the qualifications acquired through formal education.

The lecture aims to introduce the newly approved regulation on knowledge standards for cybersecurity by the National Security Authority and describe, to some extent, the issue of professional certifications in the field of information and cybersecurity.

Key words: *cybersecurity, education, qualifications, human resources*

Čo je to pracovná rola a znalostný štandard?

Poučka z konca 80. rokov, používaná najmä pri riadení IT služieb, je postavená na skúsenosti, že pri akejkoľvek zmene, ktorá má byť úspešná, je potrebné sa zamerať na tri oblasti: ľudí, nástroje a procesy. Tento prístup (známy aj ako Golden Triangle) sa v novších verziách používa doteraz. A mnohí odborníci právom tvrdia, že najdôležitejším bodom trojuholníka sú ľudia. Vo svete informačnej a kybernetickej bezpečnosti sú procesy popísané v rade noriem ISO/IEC 27 000, súvisiace IT procesy a praktiky najmä v prístupe ITIL® best practice a v rade noriem ISO/IEC 20 000. Softvérových nástrojov a všeobecne technológií je dostatok a sú všeobecne známe a využívané. Ako to však vyzerá s ľuďmi? Aké roly v procesoch kybernetickej bezpečnosti zastávajú? A aké sú požiadavky na ich kvalifikáciu?

V júni 2022 Národný bezpečnostný úrad predložil do medzirezortného pripomienkového konania návrh vyhlášky Národného bezpečnostného úradu, ktorou sa ustanovujú znalostné štandardy v oblasti kybernetickej bezpečnosti (ďalej len „Vyhláška“) [4]. Návrh vyhlášky bol spracovaný na základe splnomocnenia uvedeného v § 32 ods. 1 písm. d) zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „Zákon“) [1].

Účelom vyhlášky je vykonať zákon spôsobom, aby boli určené minimálne odborné znalosti pre jednotlivých používateľov sietí a informačných systémov vykonávajúcich činnosti a úlohy v oblasti kybernetickej bezpečnosti, pričom však nezasahuje do politiky a tvorby pracovných miest.

Zodpovednosť osôb, konajúcich v kontexte kybernetickej bezpečnosti, v organizácii má byť zadefinovaná jednoznačne, prostredníctvom rolí, v ktorých osoba vystupuje v interakcii s kybernetickým priestorom. S rolami je spojená množina povinností a oprávnení pri inicializácii, návrhu, vývoji, používaní a prevádzke siete alebo informačného systému.

Charakteristika rolí, patriacich do príslušnej kategórie, zvyčajne podrobnejšie špecifikuje:

- kľúčové činnosti,
- požadované vedomosti (všeobecné a odborné),
- zručnosti (kognitívne a praktické),
- špecifické kľúčové kompetencie.

A spolu s vyššie uvedenými aj ďalšie podmienky, ktoré má spĺňať osoba zaradená do danej roly tak, aby bola schopná plniť svoje povinnosti vyplývajúce z roly, v ktorej je zaradená.

Ak chceme stanoviť priority vzdelávania zameraného na určitú profesiu, potrebujeme dobrú definíciu typových pracovných úloh a na základe toho následne identifikáciu potrebných kompetencií a vedomostí pre danú profesiu. Je to základ na vybudovanie štruktúry bezpečnostných oddelení, platové tabuľky a nastavenie vzdelávania. Ujasnime si základné pojmy. Aj keď sémantický význam týchto výrazov podvedome väčšina chápe správne, často sú používané v nesprávnom kontexte:

- **vedomosti** – to sú poznatky nadobudnuté v priebehu vzdelávania, učenia sa alebo získané skúsenosťou,
- **zručnosti** – sú schopnosti jednotlivca uplatňovať vedomosti v praxi a využívať ich na plnenie úloh a riešenie problémov,
- **kompetencie** – sú preukázané schopnosti jednotlivca použiť vedomosti, zručnosti a osobné, sociálne a/alebo metodologické schopnosti v pracovných alebo študijných situáciách a v odbornom a osobnom rozvoji,

- **kvalifikácia** – je súhrn odborných vedomostí, zručností a kompetencií potrebných na vykonávanie určitej pracovnej činnosti.

Aké roly sú teda potrebné pre pokrytie prác súvisiacich s ochranou informačných aktív?

Ľudské zdroje v kybernetickej bezpečnosti

Pomenovať vyčerpávajúcim spôsobom všetky roly a ich zodpovednosti v oblasti informačnej a kybernetickej bezpečnosti v dostatočnom rozsahu a kvalite bola netriviálna úloha, ktorá trvala mnoho mesiacov, ba vlastne niekoľko rokov. Na príprave rámca zručností, teda nájdenia množiny, spolupracovala celá odborná komunita už od roku 2017, ešte v čase úplných začiatkov legislatívnych aktivít vedúcich k zákonom stanovenému rozsahu kvalifikačných požiadaviek na výkon príslušných činností.

Oblasť kybernetickej bezpečnosti, aj keď sa vo veľkej miere prekrýva s oblasťou informačnej bezpečnosti a ochranou osobných údajov, sa odlišuje najmä právnou úpravou a vymedzením na úrovni jednotlivých štátov. Navyše, kybernetická bezpečnosť je novou a dynamicky sa rozvíjajúcou doménou, kde sa jednotlivé oblasti ešte len definujú. Donedávna tomu nebolo inak ani v časti ľudských zdrojov.

V zákone [1] sú zakotvené iba dve roly v kybernetickej bezpečnosti, ktorých činnosť by mala byť pre prevádzkovateľov záväzná a ktoré by mali spĺňať stanovený znalostný štandard:

1. **audítor KB**, keďže podľa §29 ods. 3 Zákona [1] audit kybernetickej bezpečnosti vykonáva certifikovaný audítor kybernetickej bezpečnosti, ktorým je fyzická osoba, spoločník, štatutárny orgán alebo zamestnanec právnickej osoby,
2. **manažér KB**, keďže v zmysle § 20 ods. 4 Zákona [1] bezpečnostné opatrenia musia zahŕňať najmenej určenie manažéra kybernetickej bezpečnosti.

Pre obidve tieto roly existujú certifikačné schémy a aj akreditovaní poskytovatelia certifikačných testov.

Okrem povinných rolí manažéra a audítora KB sú medzi znalostnými štandardmi nasledujúce roly v kybernetickej bezpečnosti:

- **špecialista kybernetickej bezpečnosti** –zodpovedný za plnenie špecifických úloh v rámci svojej špecializácie v kybernetickej bezpečnosti,
- **tester kybernetickej bezpečnosti** –zodpovedný za testovanie zmien v prostrediach sietí a informačných systémov z pohľadu kybernetickej bezpečnosti,
- **architekt kybernetickej bezpečnosti** –zodpovedný za navrhovanie informačnej architektúry a bezpečnostných opatrení v oblasti kybernetickej bezpečnosti,
- **špecialista riadenia rizík** –zodpovedný za analýzu a riadenie rizík v oblasti kybernetickej bezpečnosti a ochrany údajov,
- **špecialista pre analýzu digitálnych stôp** –zodpovedný za vyhľadávanie a forenzné analýzy stôp v kybernetickom priestore,
- **špecialista pre riadenie súladu** –zodpovedný za to, že všetky smernice, politiky, riadiace aj prevádzkové procesy a postupy v organizácii sú v súlade s platnou právnou úpravou v oblasti kybernetickej bezpečnosti, ako aj s požiadavkami ostatných všeobecne záväzných právnych predpisov a noriem,
- **špecialista pre riešenie kybernetických incidentov** – zodpovedný za zachytávanie, analýzu a riešenie bezpečnostných udalostí,
- **výskumník** – zodpovedný za vyhľadávanie zraniteľností systémov, identifikáciu príčin zraniteľností a hrozieb, overovanie zdrojového kódu, testovanie odolnosti

systémov, identifikáciu chýb bezpečnostných mechanizmov a vyhodnocovanie efektivity bezpečnostných opatrení,

- **lektor** – zodpovedný za realizáciu vzdelávacích aktivít v oblasti kybernetickej bezpečnosti a ochrany údajov.

Medzitým, čo na Slovensku prebiehali diskusie o tom, aké roly sú relevantné v oblasti kybernetickej bezpečnosti na slovenskom pracovnom trhu, ENISA (Európska agentúra pre kybernetickú bezpečnosť) vydala **európsky rámec zručností v kybernetickej bezpečnosti** (European Cybersecurity Skills Framework – ECSF). To je de facto popis rolí a požadovaných znalostí v kybernetickej bezpečnosti na európskej úrovni.

Schéma ECSF v grafickom vyjadrení vyzerá nasledovne:

Dobrou správou je, že roly, diskutované odbornou verejnosťou a následne navrhnuté vo vyhláške NBÚ č. 492/2022 Z. z., ktorou sa ustanovujú znalostné štandardy v oblasti kybernetickej bezpečnosti, sú v úplnom súlade s európskou schémou ECSF.

Hierarchia vzdelávacích potrieb

Znalostné štandardy sú definované hierarchicky, v závislosti od kategórie používateľov informačných a komunikačných technológií. Ako stanoviť úroveň kvalifikačných požiadaviek pre jednotlivé roly?

Ako prvé je potrebné určiť tzv. taxonómiu vzdelávacích cieľov. To je hierarchicky usporiadaná miera náročnosti a rozsahu vedomostí. Taxonómiou vzdelávania je určená miera obťažnosti učiva v procese učenia sa a vzdelávacích cieľov, ktoré majú byť prostredníctvom tohto vzdelávania dosiahnuté. Môže byť použitá aj na štruktúrovanie cieľov, hodnotení a aktivít v učebných osnovách, vzdelávacích plánoch a znalostných štandardoch. Vyhláška sa odkazuje na taxonómiu podľa B. S. Blooma [5].

Bloomova taxonómia poznávacích cieľov je spôsob, ako rozdeliť úrovne chápania a aplikácie pojmov pomocou činnostných slovies. Jej autorom je profesor Chicagskej univerzity B. Bloom, ktorý taxonómiu pôvodne vytvoril ako pomôcku na kladenie skúšobných

otázok univerzitným študentom. Neskôr táto metodika našla oveľa širšie využitie vo vzdelávaní všeobecne.

Ciele učenia sú zoradené od najjednoduchších po najkomplexnejšie. Taxonómia je sekvenčná a zároveň kumulatívna, t. j. pre dosiahnutie vyššieho vzdelávacieho cieľa musí uchádzač zvládnuť všetky predchádzajúce vzdelanostné úrovne. Taxonómia, teda jednotlivé úrovne vzdelávacích cieľov sú uvedené v prílohe č. 1 vyhlášky.

Úroveň	Vzdelávací cieľ	Popis vzdelávacieho cieľa
BL1	ZAPAMÄTANIE	Schopnosť zapamätať si potrebné informácie.
BL2	POCHOPENIE	Schopnosť porozumieť alebo pochopiť význam toho, čo bolo komunikované a využiť získanú informáciu bez toho, aby bola spájaná s inými informáciami, interpretáciami alebo materiálmi.
BL3	APLIKÁCIA	Schopnosť používať myšlienky, princípy a teórie v nových, konkrétnych situáciách.
BL4	ANALÝZA	Schopnosť rozdeliť komunikáciu na základné časti, aby bol jasne uchopený význam informácie. V tejto úrovni sa skúma podstata jednotlivých entít, s cieľom lepšie porozumieť komplexným celkom.
BL5	SYNTÉZA	Schopnosť opätovne spojiť rôzne časti alebo prvky konceptu do jednotného systému alebo celku. Úroveň vzdelávania BL5 je typicky najintenzívnejšia.
BL6	POSÚDENIE	Schopnosť dospieť k prehľadu a posúdiť hodnotu a relatívny prínos myšlienok alebo postupov pomocou vhodných kritérií.

Charakteristiku vzdelávacích potrieb tvoria špecifikované kľúčové činnosti, požadované vedomosti, zručnosti, kompetencie a ďalšie podmienky, ktoré musí spĺňať osoba zaradená do danej roly tak, aby bola schopná plniť povinnosti v oblasti kybernetickej bezpečnosti vyplývajúce z príslušnej roly.

Iné než bezpečnostné roly

Vzdelávanie a zvyšovanie povedomia je potrebné vykonávať nielen pre pracovníkov, ktorí sú špecializovaní na bezpečnosť informácií a riadenie rizík kybernetickej bezpečnosti, ale aj na všetky ostatné pracovné roly, ktoré prichádzajú do styku s kybernetickým priestorom. Vyhláška sa venuje výhradne špecializačným roliam v kybernetickej bezpečnosti. Ambíciou zákonodarcu bolo bez špecifikácie znalostného štandardu navrhnúť aspoň minimálnu úroveň kvalifikácie aj pre roly, ktoré nie sú priamo zainteresované v odbore kybernetická bezpečnosť. Tieto odporúčania sú taxatívne vymenované v prílohe č. 1 k vyhláške č. 492/2022 Z. z. – Charakteristika vzdelávacích potrieb [4].

Používatelia IKT sú v nadväznosti na ciele a potreby vzdelávania v oblasti kybernetickej bezpečnosti podľa STN EN 16234-1 rozdeľovaní do kategórií, ktorým je priradená príslušná úroveň vzdelávacích cieľov, podľa Bloomovej taxonómie.

Kategórie používateľov IKT sú vo Vyhláške [4] navrhnuté nasledovne:

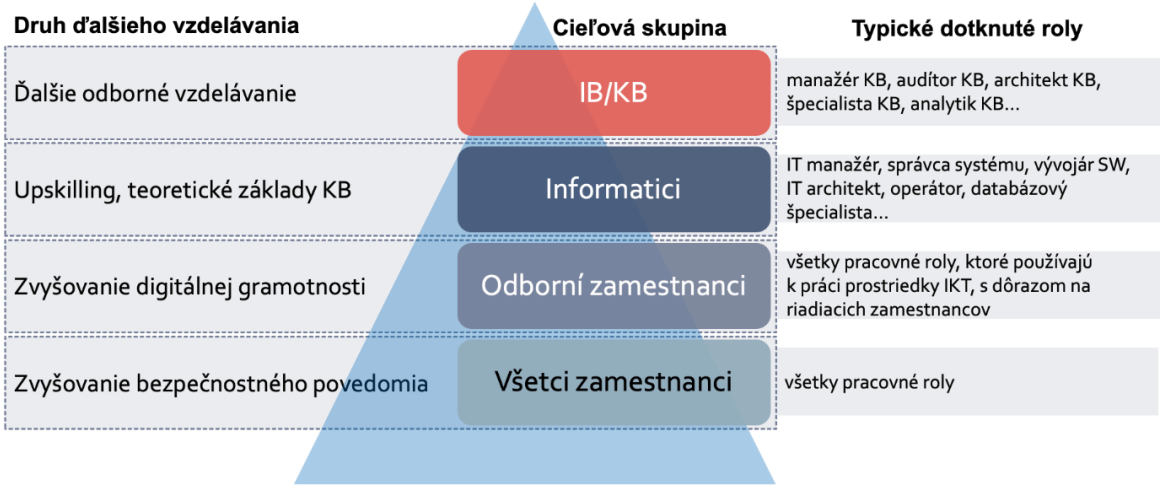
- **laici** – používatelia IKT mimo kontextu výkonu konkrétneho povolania a bez vzťahu k sieti alebo informačnému systému,
- **odborní zamestnanci** – používatelia, ktorí pri výkone konkrétneho povolania využívajú siete alebo informačné systémy,
- **manažéri** – riadiaci zamestnanci, ktorí nie sú IT manažérmi a ktorí spravidla zodpovedajú za príslušný proces alebo skupinu,
- **IT manažéri** – riadiaci zamestnanci organizačných jednotiek zodpovedných za poskytovanie IT služieb, návrh, implementáciu, obstaranie, prevádzku, údržbu a posudzovanie IKT,
- **informatici** – zamestnanci zodpovední za poskytovanie IT služieb, návrh, implementáciu, obstaranie, prevádzku, údržbu a posudzovanie IKT.

Pre pracovníkov v kybernetickej bezpečnosti v rôznych roliach vyhláška navrhuje oddelené, spresnené požiadavky na znalostný štandard, a to pre každú z rolí v samostatnej prílohe. Vyššie uvedené hierarchické rozdelenie používateľov si nemýľte s typizovanými pracovnými rolami v kybernetickej bezpečnosti. Týmto rozdelením sú **určené iba všeobecné požiadavky na kvalifikácie pre rôzne kategórie používateľov, podľa postupne sa zvyšujúcej náročnosti kvalifikačných požiadaviek** v kontexte kybernetickej bezpečnosti.

Všeobecné požiadavky na úroveň kvalifikácie

Náročnosť kvalifikačných požiadaviek je rozdielna pre skupinu pracovných rolí mimo kybernetickej bezpečnosti a skupinu pracovných rolí v rámci kybernetickej bezpečnosti. Kým pre bezpečnostných profesionálov vyhláška uvádza znalostný štandard pre každú z odborných rolí, pre ostatné kategórie používateľov stanovuje len všeobecné požiadavky, bez detailného znalostného štandardu. Konkrétne znalostné štandardy pre ostatné typické používateľské roly by mohlo v budúcnosti navrhnúť napríklad Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky. Veď len v kategórii „informatici“, t. j. u zamestnancov zodpovedných za poskytovanie IT služieb, návrh, implementáciu, obstaranie, prevádzku, údržbu a posudzovanie IKT, sa nachádza niekoľko desiatok samostatných rolí, s rôznorodými požiadavkami na ich kvalifikácie.

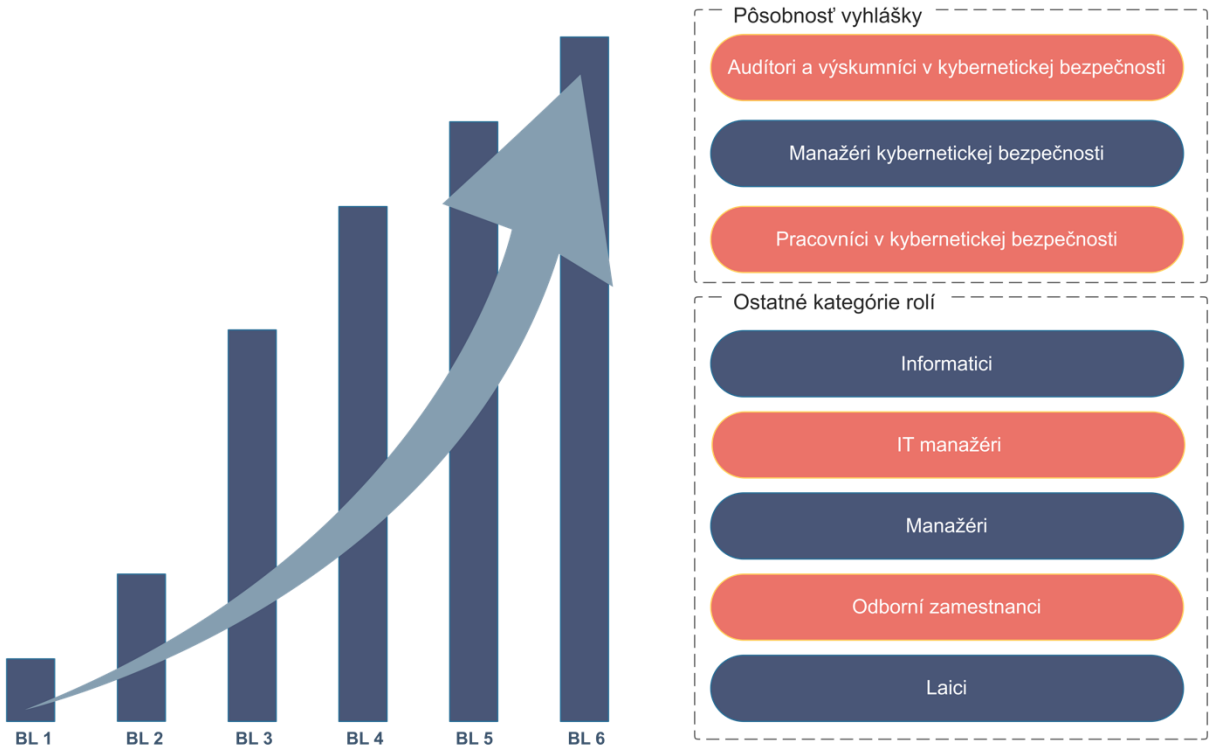
Rozdielne požiadavky na úroveň kvalifikačných požiadaviek riešila už v roku 1998 norma National Institute of Standards and Technology (NIST), konkrétne *NIST Special Publication 800-16: Information Technology Security Training Requirements*, pomocou nasledujúcej interpretácie (graf je znázornený v zjednodušenej forme):



Je taktiež vhodné zdôrazniť, že existuje niekoľko použiteľných kvalifikačných rámcov a že rámec ECSF nebol jediným, ktorý bol vzatý do úvahy v procese prípravy vyhlášky. Tými rámcami sú najmä:

- European Cybersecurity Skills Framework (ECSF) [ENISA]
- Skills Framework for the Information Age (SFIA) [IET]
- STN EN 16234 Rámec e-kompetentnosti (e-CF) — Spoločný európsky rámec pre ICT profesionálov vo všetkých priemyselných odvetviach [CEN/CENELEC]
- ISO/IEC 27021:2017 Information technology — Security techniques — Competence requirements for information security management systems professionals [ISO/IEC]
- National Initiative For Cybersecurity Education (NICE) [NIST]
- The U. S. Office of Personnel Management Competency Model for Cybersecurity [CHCO]

V kontexte rolí vymenovaných v prílohe č. 1 k vyhláške č. 492/2022 Z. z. [4] a zahrnúc aj taxonómiu vzdelávacích cieľov by sa dali tieto požiadavky zobraziť v nasledovnej transformácii:



Napríklad **laický používateľ** potrebuje porozumieť iba vybraným základným pojmom kybernetickej bezpečnosti a osvojiť si základné pravidlá bezpečnej manipulácie a používania IKT.

Cieľom vzdelávania **odborných zamestnancov** je nielen porozumieť vybraným základným pojmom kybernetickej bezpečnosti, ale aj porozumieť svojej úlohe a zodpovednosti v systéme kybernetickej bezpečnosti, chápať význam informačných aktív, s ktorými ako zamestnanec pracuje, porozumieť potrebe ochrany informácií, osvojiť si základné pravidlá bezpečnej práce s IKT, rozpoznať bezpečnostný incident a vedieť naň správne reagovať,

porozumieť bezpečnostným politikám a používaniu bezpečnostných mechanizmov v pracovných procesoch.

Manažéri procesov musia porozumieť rizikám kybernetickej bezpečnosti v nimi riadených procesoch, musia získať schopnosť analyzovať požadovanú úroveň ochrany informačných aktív, vytvárať podmienky pre riadenie bezpečnosti informácií v organizácii a integrovať požiadavky kybernetickej bezpečnosti do procesov a úloh podriadených zamestnancov. Zároveň sa musia naučiť definovať a dohliadať na plnenie požiadaviek kybernetickej bezpečnosti pri obstaraní produktov a služieb a pri procesoch podporovaných tretími stranami.

IT manažéri musia porozumieť významu kybernetickej bezpečnosti pre činnosť organizácie, poznať jednotlivé oblasti kybernetickej bezpečnosti, musia porozumieť systému riadenia bezpečnosti informácií a osvojiť si ho, získať schopnosť implementovať bezpečnostné opatrenia v konkrétnom prostredí, získať schopnosť stanoviť zodpovednosti zamestnancov organizácie vo vzťahu k informačným a komunikačným technológiám, osvojiť si metódy vyhodnocovania efektívnosti prijatých bezpečnostných opatrení, vedieť definovať a dohliadať na plnenie požiadaviek kybernetickej bezpečnosti pri objednávkach, dodávkach a prevádzke IKT systémov a IT služieb, mať schopnosť presadzovať politiky kybernetickej bezpečnosti v organizácii.

Informatici si majú doplniť vlastné odborné znalosti špecificky pre oblasť kybernetickej bezpečnosti, porozumieť podstate bezpečnostných požiadaviek na IKT systémy a IT služby, musia porozumieť zraniteľnostiam, hrozbám a rizikám spojeným s používanými IKT systémami a IT službami, potrebujú nadobudnúť schopnosť navrhnúť, implementovať, udržiavať a prevádzkovať mechanizmy na naplnenie bezpečnostných požiadaviek na IT služby. Najmä však ako tí najpodstatnejší z organizácie potrebujú nadobudnúť zručnosť kvalifikovane komunikovať a spolupracovať so špecialistami kybernetickej bezpečnosti, formulovať problémy, posudzovať a implementovať navrhované opatrenia. Pretože práve informatici sú tí, ktorí sú zodpovední za implementáciu bezpečnostných opatrení.

Oproti všetkým vyššie uvedeným, ciele vzdelávania pracovníkov zabezpečujúcich oblasť kybernetickej bezpečnosti sú už komplexnejšie. **Profesionál v kybernetickej bezpečnosti** potrebuje najmä:

- poznať a osvojiť si právne a etické požiadavky na zaručenie bezpečnosti informačných aktív,
- rozumieť zraniteľnostiam, hrozbám a rizikám v informačnej a kybernetickej bezpečnosti,
- nadobudnúť schopnosť navrhnúť, implementovať, udržiavať a prevádzkovať bezpečnostné mechanizmy a riešenia,
- získať schopnosť navrhovať a prezentovať bezpečnostné stratégie, bezpečnostné politiky a bezpečnostnú architektúru,
- získať znalosti o technikách a metódach vyhodnocovania efektívnosti bezpečnostných mechanizmov a riešení a uplatňovať ich v procesoch organizácie,
- nadobudnúť zručnosť kvalifikovane komunikovať a spolupracovať s informatikmi, formulovať problémy, posudzovať a implementovať navrhované opatrenia,
- získať schopnosť navrhovať procesy riadenia rizík v informačnej a kybernetickej bezpečnosti.

Požiadavky kladené na **manažérov kybernetickej bezpečnosti** sú ešte širšie. Manažér kybernetickej bezpečnosti potrebuje okrem všetkých predchádzajúcich vedomostí a zručností najmä nadobudnúť:

- schopnosť vytvoriť rámec riadenia kybernetickej bezpečnosti,
- schopnosť navrhovať a prezentovať bezpečnostné stratégie, bezpečnostné politiky a bezpečnostnú architektúru,
- schopnosť riadiť obstaranie, implementáciu, prevádzku a vyhodnocovanie bezpečnostných riešení,
- schopnosť navrhovať a riadiť procesy riadenia rizík v informačnej a kybernetickej bezpečnosti,
- schopnosť navrhovať a riadiť procesy riešenia kybernetických bezpečnostných incidentov, riadenia kontinuity činností a havarijnej obnovy prevádzky,
- znalosti o právnych a etických požiadavkách na zaručenie bezpečnosti informačných aktív,
- znalosti o technikách a metódach vyhodnocovania efektívnosti bezpečnostných mechanizmov a riešení a schopnosť uplatňovať ich v procesoch organizácie.

Nakoniec výskumníci a audítori potrebujú nadobudnúť všetky predchádzajúce schopnosti. A navyše aj spôsobilosť vykonať audit kybernetickej bezpečnosti a posúdiť efektívnosť prijatých bezpečnostných opatrení v zmysle platných právnych predpisov a platných auditných metodík.

Podrobnosti týkajúce sa a kvalifikačných požiadaviek kladených na jednotlivé roly sú uvedené vo Vyhláške o znalostných štandardoch.

Vyhláška o znalostných štandardoch

Znalostné štandardy sú vypracované v súlade so štandardom *STN 16234-1 Rámec e-*kompetentnosti *(e-CF) – Spoločný európsky rámec pre ICT profesionálov vo všetkých priemyselných odvetviach – Časť 1: Rámec*. Zároveň, ako už bolo spomenuté, sú znalostné štandardy v súlade s európskym rámcom zručností v kybernetickej bezpečnosti (European Cybersecurity Skills Framework – ECSF).

Špecifikácie vzdelanostných štandardov pre jednotlivé roly predstavujú nezáväzné odporúčania, ktoré však nezakladajú povinnosti pre vytváranie nových pracovných pozícií a sú v súlade s platným európskym rámcom. Znalostné štandardy sú pre jednotlivé roly kybernetickej bezpečnosti odporúčané, okrem tých rolí, o ktorých to ustanovuje zákon [1], teda manažér kybernetickej bezpečnosti [§ 20 ods. 4 písm. a) Zákona] a audítor kybernetickej bezpečnosti [§ 29 ods. 3 Zákona]. Pre osobu manažéra kybernetickej bezpečnosti a certifikovaného audítora kybernetickej bezpečnosti znalostné štandardy predstavujú záväzný rámec.

Vyhláška priamo nadväzuje na novelu vyhlášky Národného bezpečnostného úradu, ktorou sa mení a dopĺňa vyhláška Národného bezpečnostného úradu č. 436/2019 Z. z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora. Rola audítora kybernetickej bezpečnosti bola vyňatá z vyhlášky Národného bezpečnostného úradu č. 436/2019 Z. z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora a doplnená do návrhu vyhlášky, kam vecne patrí.

Vyhláška bola predmetom medzirezortného pripomienkového konania od 3. júna 2022 do 23. júna 2022. Keďže návrh vyhlášky bol pred samotným legislatívnym procesom

predmetom širokej diskusie odbornej verejnosti, na rokovanie legislatívnej rady vlády sa materiál predložil bez rozporov.

Legislatívna rada vlády nakoniec posunula dátum účinnosti pre niektoré prílohy na 1. januára 2024. Dôvodom bola najmä pôvodná požiadavka niektorých rezortov na získanie dostatočného časového priestoru pre prípravu zamestnancov pre rolu Manažér kybernetickej bezpečnosti. Zrejme iba nedorozumením sa stalo, že spolu so znalostným štandardom pre rolu Manažér kybernetickej bezpečnosti bola posunutá účinnosť aj pre všetky ostatné znalostné štandardy (okrem roly Audítor kybernetickej bezpečnosti). Na platnosti vyhlášky to však nič nemení a riadiť sa jednotlivými znalostnými štandardmi sa dá aj pred dátumom účinnosti príslušných príloh.

Istým technickým problémom je len fakt, že portál Slov-lex pri posune účinnosti niektorých častí právneho predpisu tieto časti (v tomto prípade prílohy č. 3,4,5 a 7-14) nezverejní. Úplné znenie vyhlášky je potrebné hľadať v časti „História - Dátum účinnosti 01. 01. 2024“

Analýza požiadaviek na ľudské zdroje

Slovak Business Agency (SBA) v rámci svojich aktivít zameraných na podporu rozvoja a rastu malého a stredného podnikania (MSP) na Slovensku vykonáva pravidelný monitoring a výskum podnikateľského prostredia s dôrazom na sektor malého a stredného podnikania. Vypracované analytické materiály slúžia ako informačné a analytické vstupy v súvislosti s prípravou a realizáciou politiky podpory a rozvoja malého a stredného podnikania.

V roku 2022 SBA vykonala analýzu „*Malé a stredné podnikanie v číslach v roku 2021*“. Slovak Business Agency v tomto materiáli uplatňuje veľkostné kategórie podnikov vyplývajúce z odporúčania Európskej komisie č. 2003/361/ES zo 6. mája 2003 o definícii mikro, malých a stredných podnikov [6].

Pri definícii MSP sa posudzujú tieto tri kritériá:

Hodnotenie veľkostnej typológie podniku podľa odporúčania Európskej komisie umožňuje zachytiť skutočný rozsah, výkonnosť podniku a jeho postavenie v porovnaní s konkurenciou v rôznych oblastiach hospodárskej činnosti. V prípade, ak MSP nedodrží jedno z dvoch finančných kritérií (ročný obrat alebo celkovú ročnú bilančnú sumu), podnik si naďalej zachováva status MSP. K zmene postavenia podniku ako MSP, prípadne malého podniku alebo mikropodniku v rámci množiny MSP, dochádza až po prekročení veľkostných kritérií v dvoch po sebe nasledujúcich účtovných obdobiach. [7].

Podnikateľské prostredie na Slovensku sa dlhodobo vyznačuje vysokým zastúpením mikropodnikov. Z celkového počtu aktívnych podnikateľských subjektov v roku 2021 tvorili mikropodniky až 97,3 %. V absolútnom vyjadrení to predstavuje 618 115 subjektov. Štruktúru

podnikateľských subjektov ďalej doplnili malé podniky s podielom 2,1 % (v absolútnom vyjadrení 13 469) a stredné podniky s najmenším zastúpením 0,4 %, resp. 2 725 subjektov. Podiel veľkých podnikov na celkovom počte aktívnych podnikateľských subjektov zostal zachovaný z predchádzajúcich rokov na úrovni 0,1 %, čo v absolútnom vyjadrení znamená 655 subjektov.

Podľa registra organizácií ŠÚ SR po spracovaní SBA sú počty aktívnych podnikateľských subjektov podľa právnej formy a veľkostnej kategórie k 31. 12. 2021 nasledujúce:

Veľkostná kategória/ Právna forma	Podniky	Živnostníci	Slobodné povolania	SHR	Spolu	Podiel v %
Mirkopodniky (0-9)	242 239	349 257	22 943	3 676	618 115	97,3%
Malé podniky (10 – 49)	12 511	940	10	8	13 469	2,1%
Stredné podniky (50 - 249)	2 688	36	1	0	2 725	0,4%
Veľké podniky (250 a viac)	652	3	0	0	655	0,1%
Spolu MSP (0- 249)	257 438	350 233	22 954	3 684	634 309	99,9%
Spolu podnikateľské subjekty	258 090	350 236	22 954	3 684	634 964	100%

Táto tabuľka je podstatná pre ďalšiu analýzu, pretože na základe počtu aktívnych podnikateľských subjektov a počtu ostatných typov, najmä verejnoprávnych organizácií je možné vykonať odhad potrieb na jednotlivé pracovné miesta. Analyzované subjekty boli len tie typy organizácií, u ktorých je predpokladaná:

1. **zákonná povinnosť** vytvorenia príslušných pracovných miest v roliach podľa Vyhlášky, (typicky Prevádzkovatelia základných služieb a neskôr po transpozícii smernice NIS2 [2] do slovenského práva aj veľké podniky a niektoré MSP),
2. **akútna potreba** vytvorenia niektorej, alebo niektorých typov pracovných miest v roliach podľa Vyhlášky, (typicky niektoré MSP, vysoké školy, orgány verejnej moci a orgány činné v trestnom konaní),
3. **dobrovoľná tvorba** pracovných miest s príslušnými spôsobilosťami, vzhľadom na uvedomenie si rizík kybernetickej bezpečnosti, resp. potrieb výskumu a vývoja.

Týmito subjektami sú najmä nasledujúce typy organizácií:

- prevádzkovatelia základných služieb podľa Zákona [1] (vrátane veľkých podnikov),
- stredné podniky,
- verejná správa (ústredné orgány a samospráva),
- orgány verejnej moci pôsobiace v oblasti kybernetickej bezpečnosti (NBÚ, MIRRI),
- orgány činné v trestnom konaní,
- relevantné vysoké školy.

Z tohto pohľadu sú odhadované požiadavky pracovného trhu podľa právnej formy a veľkostnej kategórie subjektu nasledujúce:

Rola / Kategória subjektu	PZS	Stredné podniky	Verejná správa	OVM	OČTK	Vysoké školy
1.Manažér kybernetickej bezpečnosti	1	1	1	1	1	
2.Špecialista pre vyšetrovanie KBI	1		1	10	200	
3.Špecialista pre riadenie súladu	1		1	1	1	
4.Špecialista pre riešenie KBI	1			10	10	
5.Architekt kybernetickej bezpečnosti	1		1	2		
6.Audítor kybernetickej bezpečnosti				100		
7.Lektor kybernetickej bezpečnosti				50		
8.Špecialista kybernetickej bezpečnosti	2			10		
9.Výskumník kybernetickej bezpečnosti				10		20
10.Špecialista pre riadenie rizík	1		1	1	1	
11.Špecialista pre analýzu digitálnych stôp			2	10	200	
12.Tester kybernetickej bezpečnosti			1	5		
TYPOVÝ POČET RÔL V KB	8	1	8	210	413	20
POČET SUBJEKTOV	1 600	2 688	300	2	2	5
Odhadovaná potreba FTE podľa subjektov	**12 800**	**2 688**	**2 400**	**420**	**826**	**100**

Do počtu PZS nie sú zahrnuté veľké podniky, napriek predpokladu, že tieto sa v blízkom období po transpozícii novelizovanej Smernice NIS2 stanú povinnými osobami zo zákona. Analýza odráža aktuálne predpokladané požiadavky, pričom **navýšenie dopytu (napríklad aj po transpozícii smernice NIS2) zmení pomery na pracovnom trhu a vyvolá potrebu prehodnotenia tejto analýzy**.

Predpokladá sa, že prevádzkovatelia základných služieb a veľké podniky musia mať povinne vytvorenú pozíciu manažér kybernetickej bezpečnosti a ďalej sa dá predpokladať požiadavka na vytvorenie najmenej nasledovných pozícií:

- špecialista pre vyšetrovanie kybernetických bezpečnostných incidentov,
- špecialista pre riadenie súladu,
- špecialista pre riešenie kybernetických bezpečnostných incidentov,
- architekt kybernetickej bezpečnosti,
- špecialista kybernetickej bezpečnosti,
- špecialista pre riadenie rizík.

Požiadavky vo verejnej správe sú (alebo mali by byť) v porovnaní s PZS a veľkými podnikmi o niečo skromnejšie.

Počet požiadaviek u orgánov verejnej moci výrazne navyšuje počet audítorov kybernetickej bezpečnosti a počet kvalifikovaných lektorov. Počty v analýze sú však úmyselne výrazne podhodnotené, najmä vzhľadom na reálnu dostupnú kapacitu kvalifikovaných profesionálov, spĺňajúcich kritériá na tieto, povinne certifikované typy rolí.

U orgánov činných v trestnom konaní je výrazná najmä požiadavka na kvalifikovaný personál v oblasti digitálnej forenznej analýzy, t.j.:

- špecialista pre vyšetrovanie kybernetických bezpečnostných incidentov,
- špecialista pre riešenie kybernetických bezpečnostných incidentov,
- špecialista pre analýzu digitálnych stôp.

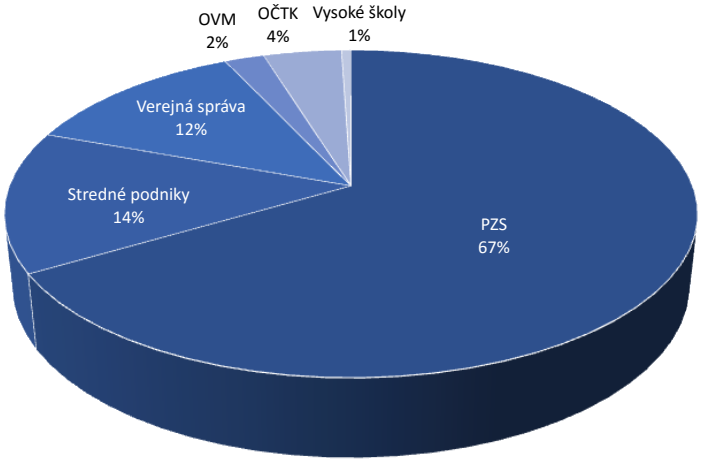
U malých a stredných podnikov, ktoré nie sú povinnými osobami, sa v analýze predpokladala len jedna univerzálna pracovná pozícia. Zvolili sme rolu manažér kybernetickej

bezpečnosti – no v skutočnosti bude zrejme táto rola vyžadovať kvalifikáciu špecialistu kybernetickej bezpečnosti.

Vysoké školy budú mať typickú požiadavku na roly výskumníkov a testerov.

Je potrebné zdôrazniť, že **zvolený bol konzervatívny prístup** a preto v celom priebehu analýzy boli hodnoty zaokrúhľované zásadne smerom nadol, možnosti naplnenia pracovných miest odhadované skepticky a požiadavky subjektov odhadované ako postupné a opatrné. **Výsledné hodnoty v tejto analýze sú oproti budúcim predpokladaným požiadavkám pracovného trhu veľmi pravdepodobne podhodnotené**.

V grafickom vyjadrení je podiel na požiadavkách na pracovné pozície v kybernetickej bezpečnosti u jednotlivých typov subjektov nasledujúci:



Niekoľko nasledujúcich údajov o požadovaných počtoch zamestnancov v kybernetickej bezpečnosti naznačuje, že pri súčasnej kapacite vysokých škôl a vzdelávacích inštitúcií môžu byť potreby zamestnávateľov naplnené iba o mnoho rokov neskôr. Hlavné analýzou odhadnuté požiadavky na pracovné pozície v kybernetickej bezpečnosti sú nasledujúce:

- Manažér kybernetickej bezpečnosti (ako zákonná povinnosť): **1 600 FTE**[1]
- Manažér kybernetickej bezpečnosti (nepovinne): **2 900** FTE
- Potrebný počet zamestnancov kybernetickej bezpečnosti u PZS: **12 800** FTE
- Celkový Potrebný počet zamestnancov kybernetickej bezpečnosti: **19 200 FTE.**

Klasifikácia vzdelávania

Medzinárodná štandardná klasifikácia vzdelania (angl.: „International standard classification of education“ - ISCED) je rámec na klasifikáciu vzdelávacích aktivít podľa

[1] Plný pracovný úväzok (z angl.: „Full-time equivalent“) označenie jednotky, ktorou sa vyjadruje miera zapojenia zamestnanca prepočítaná na 100% kapacitu v pracovnom čase. Ide o ekvivalent jedného pracovníka na plný úväzok. Jednotka je používaná v riadení ľudských zdrojov na zistenie počtu pracovníkov na plný úväzok potrebných na výkon činnosti.

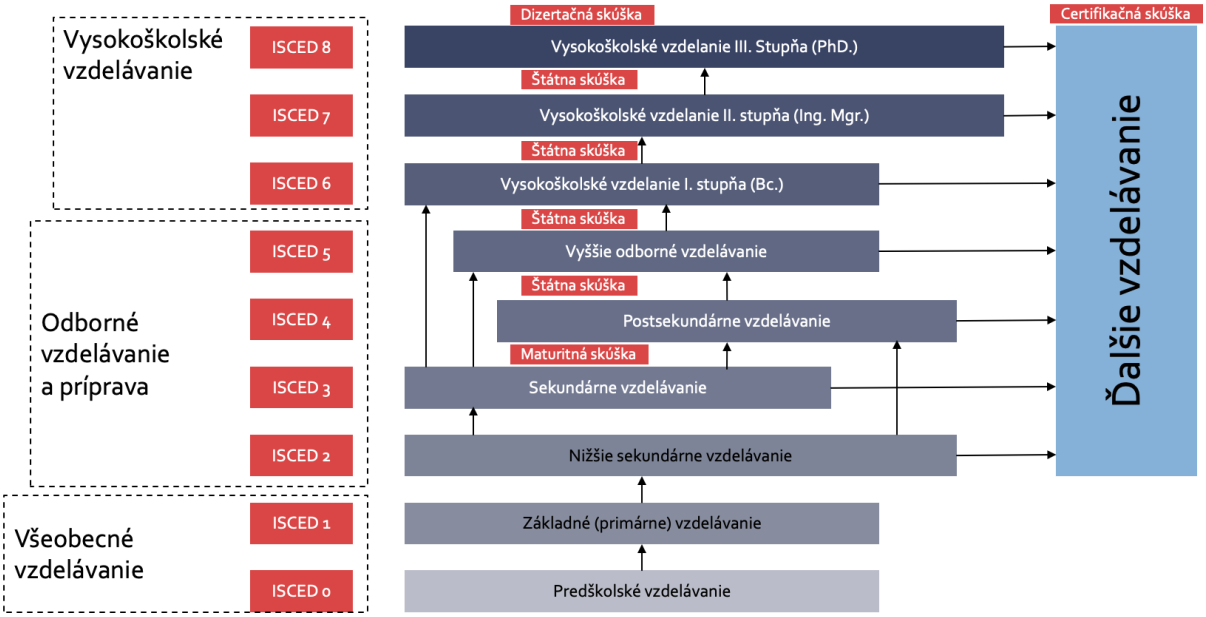
medzinárodne dohodnutých kategórií. Základné pojmy a definície ISCED sú navrhnuté tak, aby boli medzinárodne platné a komplexné pre celú škálu národných vzdelávacích systémov.

Európska únia sa usiluje o zjednodušenie uznávania kvalifikácií medzi jej členskými štátmi a nástrojom tejto snahy je Európsky kvalifikačný rámec (ďalej len „EKR“), pričom jednotlivé členské krajiny si vytvárajú vlastné národné kvalifikačné rámce. Pomocou tohto systému majú občania, firmy a úrady v celej Európskej únii možnosť porovnať svoje národné kvalifikácie s kvalifikáciami ostatných členských štátov EÚ.

V prípade Slovenskej republiky sú všetky kvalifikácie systematizované v Národnej sústave kvalifikácií a zaradené na jednu z úrovní Národného kvalifikačného rámca, t. j. Slovenského kvalifikačného rámca (ďalej len „SKKR“). V roku 2017 sa Slovenský kvalifikačný prepojil s EKR.

Odporúčanie Európskeho parlamentu a Rady z 22. mája 2017 týkajúce sa európskeho kvalifikačného rámca pre celoživotné vzdelávanie, ktorým sa zrušuje odporúčanie Európskeho parlamentu a Rady z 23. apríla 2008 o vytvorení európskeho kvalifikačného rámca pre celoživotné vzdelávanie, definuje kvalifikáciu ako *formálny výsledok procesu hodnotenia a potvrdzovania, ku ktorému sa dospeje vtedy, keď príslušný orgán stanoví, že jednotlivec dosiahol výsledky vzdelávania zodpovedajúce daným normám.*

Podľa rámca ISCED sú úrovne vzdelávania klasifikované nasledovne:



Vysokoškolské vzdelávanie je štúdium v akreditovaných študijných programoch na vysokých školách, uskutočňované podľa zákona č. 131/2002 Z.z. o vysokých školách **Úspešným absolvovaním školského vzdelávania sa získava stupeň vzdelania**.

Ďalšie vzdelávanie je vzdelávanie vo inštitúciách ďalšieho vzdelávania („vzdelávacích inštitúciách“) nadväzujúce na školské vzdelávanie alebo iné vzdelávanie, ktoré nadväzuje na školské vzdelávanie. Ďalšie vzdelávanie umožňuje získať čiastočnú kvalifikáciu alebo úplnú kvalifikáciu alebo doplniť, obnoviť, rozšíriť alebo prehĺbiť si kvalifikáciu nadobudnutú v školskom vzdelávaní, alebo uspokojiť záujmy a získať spôsobilosť zapájať sa do života

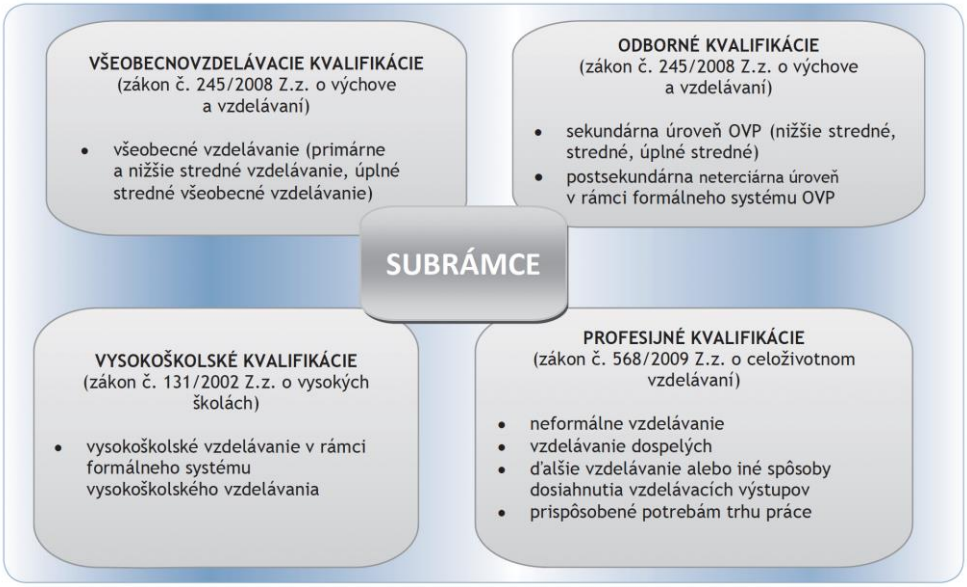
občianskej spoločnosti. **Úspešným absolvovaním ďalšieho vzdelávania nemožno získať stupeň vzdelania**.

Celoživotné vzdelávanie sú všetky aktivity, ktoré sa uskutočňujú v priebehu života s cieľom zlepšiť vedomosti, zručnosti a schopnosti. Ide o vzdelávanie podľa zákona č. 568/2009 Z. z. o celoživotnom vzdelávaní.

Zvyšovanie zručností (angl. „upskilling“) je trend, ktorý uľahčuje ďalšie vzdelávanie poskytovaním školiacich programov a príležitostí na rozvoj, ktoré rozširujú schopnosti zamestnancov a minimalizujú potenciálne nedostatky v ich zručnostiach. Zvyšovanie zručností sa zameriava na zlepšovanie zručností súčasných profesionálov. Zvyčajné metódy zvyšovania zručností sú školenia a tréningy. Motiváciou môže byť najmä napredovanie v práci, nájdenie nových príležitostí v rámci organizácie a pre zamestnávateľov zvýšenie disponibilnej kapacity ľudských zdrojov v konkrétnych profesiách a roliach.

Slovenský kvalifikačný rámec slúži ako nástroj na vytvorenie typológie kvalifikácií v národnom kontexte. Na tento účel bol prijatý prístup založený na štyroch tzv. „subrámcoch“, ktoré zodpovedajú príslušným častiam vzdelávacieho systému a sú charakterizované spoločným typom kvalifikácie.

Jednotlivé subrámce SKKR sa riadia príslušnou legislatívou SR:



Subrámec profesijných kvalifikácií sa riadi zákonom č. 568/2009 Z. z. o celoživotnom vzdelávaní. Obsahuje kvalifikácie, ktoré nemožno dosiahnuť v systéme formálneho vzdelávania.

Tak ako formálne vysokoškolské vzdelávanie je po absolvovaní štúdia formálne ukončené štátnou skúškou a potvrdené vysokoškolským diplomom, je možné formálne ukončiť aj ďalšie vzdelávanie skúškou a potvrdením získaných vedomostí a zručností certifikačnou skúškou. Certifikácia v ďalšom vzdelávaní je zásadne dobrovoľná.

Kvalifikácie sa zvyčajne priznávajú vo forme vysvedčení, osvedčení a diplomov udelených po ukončení štúdia, alebo vzdelávania. Dokladom o kvalifikácii **v subrámci**

profesijných kvalifikácií je podľa zákona „Osvedčenie o kvalifikácii“, to je však v praxi nazývané rôznym spôsobom. Používané sú najmä výrazy „osvedčenie o absolvovaní“ a „certifikát“.

Nie vždy je však výraz certifikát používaný vo vhodnom kontexte. V konečnom dôsledku existujú tri kategórie dokladov o ukončenom ďalšom vzdelávaní:

- osvedčenia o absolvovaní ďalšieho vzdelávania,
- komerčné certifikáty vydávané v neakreditovanom režime,
- certifikáty od akreditovaných vzdelávacích inštitúcií.

Posledný z uvedených typov certifikátov môžu poskytovať výhradne tie vzdelávacie inštitúcie, alebo certifikačné orgány, ktoré prešli atestáciou spôsobilosti vykonávať posudzovanie kompetencií osôb. To však neznamená, že neakreditované komerčné certifikácie sú automaticky nepravé, alebo že ich je potrebné považovať za nedôveryhodné. Mnohé, najmä tie, ktoré sú poskytované medzinárodnými organizáciami, patria medzi uznávané v oblasti kybernetickej bezpečnosti (napríklad certifikáty od ISACA, ISC2, CompTIA, GIAC, SANS a ďalšie).

Rozhodnúť o existencii primeraných záruk kvality (typicky napr. dodávateľa, konzultanta, experta, v rámci verejných obstarávaní) je možné napríklad na základe vyžiadania relevantných certifikátov. Kybernetická bezpečnosť sa však postupne delí na mnohé subdomény a tým značne narastá počet a komplexnosť certifikačných schém.

S cieľom vyhnúť sa zdržaniam, alebo obmedzeniam vo verejných obstarávaniach je potrebné pred rozhodnutím o požiadavkách na predloženie certifikátov rozhodnúť, aký predmet certifikácie je pre príslušnú časť verejného obstarávania relevantný, vyberať cielene vlastníctvo certifikátov podľa požadovanej domény a opierať sa o uznávané, optimálne akreditované certifikačné schémy.

Akreditácia vzdelávacích programov

Úspešným absolvovaním ďalšieho vzdelávania nemožno získať stupeň vzdelania, avšak overenie nadobudnutých vedomostí a zručností je typicky vykonávané certifikačnou skúškou. V oblasti informačnej a kybernetickej bezpečnosti už mnoho rokov jestvuje niekoľko desiatok rôznych uznávaných komerčných certifikácií, avšak až zákon č. 69/2018 Z.z. o kybernetickej bezpečnosti [1] umožnil implementovať štátom zaručenú certifikačnú schému a umožniť vzdelávacím inštitúciám vykonávať vzdelávanie a certifikáciu osôb v akreditovanom režime.

International Accreditation Forum (IAF) prijalo dňa 30.10.2017 na 31. Valnom zhromaždení IAF vo Vancouveri rezolúciu 2017- 19, ktorá zakazuje vydávať neakreditované certifikáty certifikačnými orgánmi v rozsahoch, kde sú akreditované.

Pod pojmom neakreditovaný certifikát sa rozumie certifikát, ktorý bol vydaný v neakreditovanom režime t. j. neobsahuje akreditačnú značku alebo odkaz na akreditáciu.

Akreditácia je štátne overenie spôsobilosti vzdelávacej inštitúcie uskutočňovať akreditovaný vzdelávací program na základe splnenia podmienok ustanovených zákonom č. 568/2009 Z. z. o celoživotnom vzdelávaní a o zmene a doplnení niektorých zákonov. O udelení akreditácie rozhoduje Ministerstvo školstva, vedy, výskumu a športu Slovenskej republiky na základe stanoviska akreditačnej komisie pre ďalšie vzdelávanie.

V súčasnosti prebiehajú prvé aktivity ohľadom akreditácie vzdelávacích programov v kybernetickej bezpečnosti prostredníctvom akreditačnej komisie Ministerstva školstva, vedy,

výskumu a športu Slovenskej republiky. Žiaľ, prvé reakcie ministerstva sa zdajú byť vyslovene odmietavé, s odvolaním sa na § 1 ods. 2 zákona č. 568/2009 Z. z. o celoživotnom vzdelávaní **Chyba! Nenašiel sa žiaden zdroj odkazov.**, podľa ktorého *tento zákon sa nevzťahuje na nadobúdanie, hodnotenie a overovanie odbornej kvalifikácie na účely výkonu povolaní podľa osobitných predpisov, na prípravu na výkon odborných činností podľa osobitných predpisov, na vzdelávanie uskutočňované podľa osobitného predpisu a na vzdelávanie uskutočňované na vysokých školách*.

Tými osobitnými predpismi na ktoré sa odvoláva § 1 ods. 2 zákona č. 568/2009 Z. z. sú:

- zákon č. 578/2004 Z. z. o poskytovateľoch zdravotnej starostlivosti, zdravotníckych pracovníkoch, stavovských organizáciách v zdravotníctve a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
- zákon č. 586/2003 Z. z. o advokácii a o zmene a doplnení zákona č. 455/1991 Zb. o živnostenskom podnikaní (živnostenský zákon) v znení neskorších predpisov,
- zákon č. 39/2007 Z. z. o veterinárnej starostlivosti v znení neskorších predpisov,
- zákon č. 346/2005 Z. z. o štátnej službe profesionálnych vojakov ozbrojených síl Slovenskej republiky a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
- § 19 zákona č. 314/2001 Z. z. o ochrane pred požiarmi v znení neskorších predpisov,
- zákon č. 73/1998 Z. z. o štátnej službe príslušníkov Policajného zboru, Slovenskej informačnej služby, Zboru väzenskej a justičnej stráže Slovenskej republiky a Železničnej polície v znení neskorších predpisov.

Súhlasiť by sa jednoznačne dalo iba s poslednou časťou ustanovenia § 1 ods. 2 zákona č. 568/2009 Z. z., pretože akreditácia vysokoškolských programov je skutočne vykonávaná iným právnym predpisom, prostredníctvom Slovenskej akreditačnej agentúry pre vysoké školstvo. Problémom je, že medzi ostatnými výnimkami, na ktoré sa odvoláva na § 1 ods. 2 zákona č. 568/2009 Z. z. sa zákon č. 69/2018 Z.z. [1] síce nenachádza, ale Ministerstva školstva tvrdí, že v tomto ustanovení sú uvedené iba príklady a že výnimka sa vzťahuje aj na zákon č. 69/2018 Z.z. o kybernetickej bezpečnosti [1].

Pri tejto argumentačnej logike Ministerstva školstva by to však znamenalo, že akékoľvek iné profesijné kvalifikácie, vyžadujúce si akreditované vzdelávacie programy, spadajú pod uvedenú výnimku a teda že **akreditáciu akýchkoľvek vzdelávacích programov vo všetkých špecifických profesiách má riešiť rezortné ministerstvo alebo iný príslušný ústredný orgán štátnej správy**. V tom prípade však nedáva zmysel ani samotná existencia akreditačnej komisia Ministerstva školstva, vedy, výskumu a športu Slovenskej republiky, samozrejme, vrátane pracovného miesta, ktoré by sa dalo využiť napríklad na vytvorenie miesta špecialistu na metodiku vzdelávania v informačnej a kybernetickej bezpečnosti na stredných a základných školách, ktoré ministerstvo doteraz vytvorené nemá.

Záver

Všeobecným problémom spoločnosti je nedostatok disponibilných profesionálov v kybernetickej bezpečnosti. Celková aktuálna potreba Slovenskej republiky na naplnenie počtu pracovných miest v príslušných roliach je **približne 19 tisíc**.

Cieľom je v najkratšom možnom čase získať potrebný počet kvalifikovaného personálu pre obsadenie aspoň povinných zákonných rolí. Najefektívnejšie riešenie je dostupné formou tzv. upskillingu, t.j. **formou ďalšieho vzdelávania vo vzdelávacích inštitúciách, postgraduálneho vzdelávania alebo ďalšieho vzdelávania na vysokých školách.** Zároveň je

potrebné, aby sa zvýšili kapacity v akreditovaných študijných odboroch blízkych kybernetickej bezpečnosti vo formálnom vysokoškolskom vzdelávaní. Ďalšie vzdelávanie umožňuje získať čiastočnú kvalifikáciu alebo úplnú kvalifikáciu alebo doplniť, obnoviť, rozšíriť alebo prehĺbiť si kvalifikáciu nadobudnutú v školskom vzdelávaní.

Vzdelávacie potreby a taxonómia vzdelávacích potrieb sú uvedené v prílohách Vyhlášky a sú určené najmä pre tvorbu vzdelávacích programov na vysokých školách a identifikáciu konkrétnych pracovných miest. Prílohy č. 1 a 2 Vyhlášky sú uplatniteľné pre vzdelávacie inštitúcie a pre tvorbu katalógov zamestnaneckých pozícií. V prílohách č. 3 až 14 sú zadefinované jednotlivé štandardy pre konkrétne roly, s uvedením konkrétnych požiadaviek na vedomosti, zručnosti, špecifické kľúčové kompetencie a pre niektoré roly aj požiadaviek na dĺžku odbornej praxe a stupeň vzdelania.

Znalostné štandardy tvoria rámec pre vytvorenie vzdelávacích programov, čím sa vypĺňa priestor nielen pre budovanie kvalitného bezpečnostného povedomia v oblasti kybernetickej bezpečnosti, ale aj pre zvyšovanie kvality vzdelávacích procesov. To má tendenciu ovplyvniť následne aj kvalitu pracovníkov vykonávajúcich činnosti v oblasti kybernetickej bezpečnosti jednak v štátnych a aj v súkromných organizáciách. Zavedenie a definovanie znalostných štandardov a ich aplikovanie v oblasti kybernetickej bezpečnosti je základným prvkom budovania stabilného a predvídateľného bezpečnostného prostredia.

Zoznam použitej literatúry:

[1] Zákon č.69/2018 Z.z. *o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.*

[2] Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo dňa 14. decembra 2022 *o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (skrátene len „smernica NIS2“).*

[3] Zákon č. 95/2019 Z.z. *o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov.*

[4] Vyhláška Národného bezpečnostného úradu č. 492/2022 Z.z. *ktorou sa ustanovujú znalostné štandardy v oblasti kybernetickej bezpečnosti*

[5] Benjamin S. Bloom :Taxonomy of Educational Objectives, Handbook 1: Cognitive Domain; ISBN-13: 978-0582280106

[6] Odporúčanie Európskej komisie č. 2003/361/ES zo 6. mája 2003 o definícii mikro, malých a stredných podnikov a nariadenia Komisie (EÚ) č. 651/2014

[7] Malé a stredné podnikanie v číslach v roku 2021, SBA 2022

[8] International standard classification of education (ISCED), Shannon 2013

[9] Vyhláška Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení

[10] Zákon č. 568/2009 Z. z. o celoživotnom vzdelávaní a o zmene a doplnení niektorých zákonov.

Kontaktné údaje:
Ing. Bc. Ivan Makatura, CRISC, CDPSE
Kompetenčné a certifikačné centrum kybernetickej bezpečnosti
Fakulta managementu Univerzity Komenského v Bratislave
e-mail: ivan.makatura@cybercompetence.sk

Manažment kybernetickej bezpečnosti a jeho ponímanie vo Francúzsku

Matej Kostrec

Abstrakt: *Kybernetická bezpečnosť je vzhľadom na vysoký stupeň elektronizácie všetkých oblastí ľudského života veľmi aktuálnou problematikou. Operácie vykonávané prostredníctvom počítačovej a komunikačnej techniky, pomocou ktorých prebiehajú medzinárodnými i národnými infraštruktúrami toky informácií tak citlivého, ako aj finančného a manažérskeho charakteru, sú preto cieľom nekalých, patologických, pirátskych i manipulačných útokov. Pre predchádzanie takýmto útokom je potrebné chrániť nielen jednotlivé prostriedky spracúvania dát a ich prenosu, ale aj monitorovanie aktérov vstupujúcich do tohto procesu, korektnosť realizácie prijatých postupov a adekvátnosť prístupov k príslušným dátam a informáciám. Pre tento účel je potrebné zabezpečiť dostatočný počet kvalifikovaných pracovníkov, ktorých široké kompetencie si vyžadujú vysokú úroveň vzdelávania. Predkladaný príspevok sa venuje prezentácii cieľov i aktivít, ktoré sú požadované od postu manažéra kybernetickej bezpečnosti od kompetentných orgánov vo Francúzsku, ale aj problematike vzdelávania budúcich manažérov kybernetickej bezpečnosti v tejto krajine. Prehľad prezentovaných aktivít môže byť inšpiráciou pri prijímaní obdobných aktivít v Slovenskej republike.*

Kľúčové slová: *Kybernetická bezpečnosť, manažment, vzdelávanie, ciele manažéra, aktivity manažéra, študijný program, študijné kurzy*

Abstract: *Cybersecurity is a very topical issue due to the high degree of computerization of all areas of human life. Therefore, operations carried out by means of computer and communication technology, by means of which flows of both sensitive, financial and managerial information flow through international and national infrastructures, are the target of unfair, pathological, piracy and manipulation attacks. In order to prevent such attacks, it is necessary to protect not only the individual means of data processing and transmission, but also the monitoring of the actors involved in the process, the correctness of the implementation of the procedures adopted and the adequacy of the accesses to the data and information concerned. To this end, it is necessary to ensure a sufficient number of qualified staff, whose broad competences require a high level of training. The present paper is devoted to the presentation of the objectives and activities required of the post of cybersecurity manager by the competent authorities in France, but also to the issue of training future cybersecurity managers in this country. The overview of the presented activities can be an inspiration for the adoption of similar activities in the Slovak Republic.*

Key words: *Cyber security, management, education, manager's goals, manager's activities, study program, study coursesÚvod*

Štatistiky viacerých európskych štátov deklarujú, že až tri štvrtiny ich podnikov sa stalo obeťami kybernetických útokov. Napríklad vo Francúzsku bolo v roku 2020 atakovaných až 90% podnikov.[1] Na základe tejto skutočnosti je možné konštatovať, že kybernetická bezpečnosť sa stáva pre podnik neodmysliteľným strategickým prvkom. Samotné podniky čoraz viac investujú do bezpečnosti ich informačných systémov, aby mali záruku, že sa ich aktivity budú vyvíjať v zabezpečenom prostredí, priaznivom pre ich rast a ich prosperitu. Pre tieto účely sa snažia zamestnať špecialistov z oblasti kybernetickej bezpečnosti. Je len samozrejmé, že títo špecialisti musia byť riadení centrálne jednou osobou, ktorá preberá zodpovednosť za kybernetickú bezpečnosť v celom podniku. Touto osobou je manažér kybernetickej bezpečnosti.

Ciele manažéra kybernetickej bezpečnosti

Informačný systém (IS) je jadrom rozvojovej stratégie podniku, rovnako ako kontrola jeho každodenného fungovania. Zo strategického hľadiska IS skutočne umožňuje vykonávať

[1] https://www.ece.fr/program/msc-manager-cybersecurite/ [Dostupné online 20.10.2022]

zložité simulácie rastu, poskytuje manažérom spoľahlivé údaje pre rozhodovanie. Pokiaľ ide o každodennú prevádzku, IS zabezpečuje všetky úlohy týkajúce sa riadenia vzťahov so zákazníkmi, riadenia marketingu, výroby, logistiky, služieb po predaji, manažmentu, komunikácie a riadenia ľudských zdrojov. Spája všetky ľudské, hardvérové a softvérové zdroje, ktoré umožňujú zber, správu, spracovanie, ukladanie a šírenie informácií v podniku.

V zmysle Národného registra profesijných certifikácií[2], by mal manažér kybernetickej bezpečnosti plniť nasledujúce ciele a úlohy:

- definovať, analyzovať, prekladať do reči počítača, aktualizovať a prevádzkovať každý obchodný proces.
- riadiť, spravovať a optimalizovať tieto procesy v súlade s politikou a stratégiou podniku. Na vykonávanie tejto misie musí tiež komunikovať, motivovať, animovať, dohliadať interne a externe na realizáciu týchto procesov.
- zaručovať konzistentnosť, výkonnosť informačného systému, kvalitu systému, integritu údajov a bezpečnosť prístupu.
- v kontexte zrýchlených technologických zmien, hospodárskej krízy a obnovy kybernetických rizík rozvíjať trvalé IS, ktoré sa prispôsobujú strategickým a prevádzkovým imperatívom podniku a zároveň optimalizovať a racionalizovať prevádzkové náklady.
- zodpovedať za urbanizáciu IS a ich bezpečnosť.
- radiť vedeniu podniku pri rozhodovaní a výbere rozvoja IS a ich bezpečnosti, s cieľom chrániť spracúvané údaje a udržiavať prevádzku aktualizovaných IS.
- riadiť náklady, riziká, kvalitu, dodávku v súlade s optimalizáciou potrebných zdrojov.

Zvýšený vplyv IS v podnikoch je prirodzene sprevádzaný požadovaným nárastom zručností manažéra kybernetickej bezpečnosti, tak v oblasti technických odborných znalosti, ako aj riadenia.

Požadované aktivity manažéra kybernetickej bezpečnosti

Aktivita 1: Manažovanie tímov a transformácia IS

Manažér kybernetickej bezpečnosti koordinuje, inšpiruje a vedie spolupracovníkov pod jeho zodpovednosťou k výkonu príslušných aktivít. Zúčastňuje sa na riadení prevádzkových nákladov IS, presadzuje rešpektovanie prevádzkových pravidiel podniku a zabezpečuje monitorovanie kvality. Je zodpovedný za dokumentáciu aplikácií a infraštruktúr, za ktoré je zodpovedný. Podieľa sa na vypracovaní plánov požadovaných zmien, za účelom uľahčiť prijatie svojich spolupracovníkov na riešení projektov vedených oddelením IT.

Aktivita 2: Dohľad nad portfóliom projektov oddelenia IT a ich implementáciou

[2] Répertoire national des certifications professionnelles. Zdroj : https://www.service-public.fr/particuliers/vosdroits/R40438 [Dostupné online 20.10.2022]

Manažér kybernetickej bezpečnosti dohliada na portfólio riešených projektov IT svojho podniku a organizuje ich vedenie tým, že riešiteľským tímom poskytuje potrebné bezpečnostné normy a rámce. Vyberá a prioritizuje projekty, ktoré sa budú realizovať, pričom garantuje ich implementáciu.

Aktivita 3: Navrhovanie infraštruktúry IS

Pri aplikácii svojich expertných znalostí v oblasti technických architektúr, manažér kybernetickej bezpečnosti navrhuje a nasadzuje sieťové, systémové, cloudové a úložiskové riešenia, ktoré spĺňajú očakávania a strategické potreby spoločnosti (spoľahlivosť, mobilita, dostupnosť, bezpečnosť). Na splnenie tejto misie zasahuje do komplexných informatických prostredí, vykonáva audit a poradenstvo, organizuje a udržiava pohotovostnú monitorovaciu činnosť. Vytvára návrhy, ktoré umožňujú prijímať informované a jasné rozhodnutia vedením podniku.

Aktivita 4: Zaisťovanie bezpečnosti infraštruktúr IS (prístupy, siete a dáta)

V oblasti aplikácie svojich odborných znalostí v kybernetickej bezpečnosti, po vykonaní auditu a analýze, navrhuje a nasadzuje technické a organizačné riešenia, ktoré reagujú na nové počítačové hrozby, ktoré vzniknú v informačnom systéme. Na vykonávanie tejto misie prísne monitoruje prevádzku IS na základe znalosti potenciálnych rizík a nedostatkov IS, ako aj na základe znalosti platných predpisov a štandardov. V rámci veľkých štruktúr IS je zodpovedný za vytvorenie a riadenie organizačnej zložky, ktorej poslaním je krízové riadenie kybernetickej bezpečnosti (SOC: Security Operation Centre - Operačné bezpečnostné centrum). Je zodpovedný za zvyšovanie povedomia, zaškoľovanie a poradenstvo pre používateľov a vedenie podniku aj tým, že sleduje a registruje kľúčové indikátory generované implementovanými technickými riešeniami (SIEM: Security Information Event Management - Správa informácií o bezpečnostných udalostiach).

Vzdelávanie v oblasti Manažmentu kybernetickej bezpečnosti vo Francúzsku

- **Prezentácia programu magisterského štúdia – Manažér kybernetickej bezpečnosti – akreditovaného na francúzskej univerzite ECE Paris - École centrale d'électronique[3]**

Magisterské štúdium

Špecializácia : Manažér kybernetickej bezpečnosti

Tento študijný program umožňuje získať dvojitú kvalifikáciu, a to manažérsku a profesionálnu technickú, pričom obe zodpovedajú požiadavkám a potrebám trhu.

Umožňuje odborníkovi na kybernetickú bezpečnosť oboznámiť sa s novými problémami a výzvami spojnými s kybernetickou bezpečnosťou a vykonávať v praxi nasledujúce činnosti:

- Vykonáva poradenskú činnosť a audit bezpečnosti informačných systémov
- Riadi bezpečnostné projekty alebo bezpečnostné aspekty informatických projektov
- Navrhuje, vyvíja a udržiava v prevádzke bezpečnostné informačné systémy

[3] https://www.ece.fr/program/msc-manager-cybersecurite/ [Dostupné online 20.10.2022]

- Predvída hrozby
- Analyzuje bezpečnostné incidenty a reaguje na ne

Blok študijných predmetov

Moduly	Predmety	kredity	počet hodín
MSc1 (Master of Science)			
Spoločný blok - Technika	Web technológie	3,5	30
	Zložitejšie databázy	3,5	30
	Operačné systémy	3,5	30
	Počítačové siete 1	3,5	30
	DevOps s SRE	3	30
	Machine learning 1	4	30
	Bezpečnosť IS	3	24
	Bezpečnosť počítačových sietí	3	27
	Manažment IS	1	18
Voliteľný blok - technika 1	Microsoft C#	3	27
	Java pre pokročilých		
Voliteľný blok - technika 2	Programovanie mobilov	3	27
	Matematika pre vedecké databázy		
***Blok** – LFH (low-fragmentation heap)*[4]	Manažment tímu	18	108
	Manažment rozpočtu		
	Online LFH kurz		
	Manažment individuálnych vzťahov		
	Sociálny dialóg		
	Manažment podnikov		
	Online LFH kurz		
Projekt	Multidisciplinárny kolektívny projekt	8	125
Odborná prax	4-mesačná stáž (dobrovoľná)	0	
MSc2 (Master of Science)			
Produkcia, distribúcia & skladovanie	Riadenie identít a prístupov v oblasti Microsoftu	4,5	54
	Bezpečnosť IS -2	2	21
	Politiky, normy a metodológie v Kybernetickej bezpečnosti	2	18
	Správa incidentov, forensics, retro-inžiniering	3	27
	Kryptografia	1	9
	Bezpečnosť Windows	3	39
	Riadenie identít a prístupov	1,5	16
Blok - LFH	Zdravie a bezpečnosť práce	7	64
	Vedenie zmien		
	Online LFH kurz		
Projekt	Projekt ukončenia štúdia	6	125
Odborná prax	6-mesačná stáž	20	
	Diplomová práca	10	

[4] LFH (Halda nízkej fragmentácie) je používaná operačným systémom podľa potreby na obsluhu požiadaviek na pridelenie pamäte. Fragmentácia haldy je stav, v ktorom je dostupná pamäť rozdelená na malé, nesúvislé bloky. Zdroj: https://learn-microsoft-com.translate.goog/en-us/windows/win32/memory/low-fragmentation-heap?_x_tr_sl=en&_x_tr_tl=sk&_x_tr_hl=sk&_x_tr_pto=sc [Dostupné online 25.10.2022]

Spôsob záverečného hodnotenia:

Bloky osvojených zručností sa hodnotia prostredníctvom vybraných profesionálnych aplikácií (skutočné alebo simulované), ktorých cieľom je písomné vypracovanie relevantnej technickej dokumentácie.

Na záverečnej štátnej ústnej skúške študent obhajuje pred porotou profesionálov diplomovú prácu.

- **Prezentácia programu výučby špecializácie Manažér kybernetickej bezpečnosti na PPA Business School PARIS - école de commerce et de management[5]**

Pre ilustráciu uvádzame aj príklad ďalšej vysokej školy vo Francúzsku, ktorá sa venuje vzdelávaniu v problematike manažmentu kybernetickej bezpečnosti, a ktorá má obdobný študijný program ako na ECE aj s obdobnými študijnými predmetmi.

- **Kurz o štandardoch a metódach ISO 27032 - Vedúci manažér kybernetickej bezpečnosti - s certifikáciou[6]**

Dĺžka kurzu – 5 dní (35 hodín)

Pedagogické ciele / Získanie zručností

Tento kurz umožní jeho účastníkom rozvíjať nasledujúce zručnosti:

- Definovať detailne komponenty a operácie programu kybernetickej bezpečnosti v súlade s ISO/IEC 27032 a s Rámcom kybernetickej bezpečnosti NIST (National Institute of Standards and Technology - Národný inštitút štandardov a technológie)
- Popísať cieľ, obsah a koreláciu medzi ISO/IEC 27032 a Rámcom kybernetickej bezpečnosti, ako aj s inými normami a prevádzkovými rámcami
- Identifikovať koncepty, prístupy, normy, metódy a techniky na vytvorenie, implementáciu a efektívne riadenie programu kybernetickej bezpečnosti v rámci organizácie
- Interpretovať usmernenia ISO/IEC 27032 v špecifickom kontexte organizácie
- Plánovať, implementovať, riadiť, kontrolovať a udržiavať program kybernetickej bezpečnosti v súlade s normou ISO/IEC 27032 a Rámcom kybernetickej bezpečnosti NIST
- Poradiť konkrétnej organizácii osvedčené praktiky a postupy riadenia kybernetickej bezpečnosti.

[5] PPA Business School PARIS – Vysoká škola obchodu a manažmentu
Zdroj: https://www.ppa.fr/ecole-commerce-alternance.html [Dostupné online 25.10.2022]
[6] https://www.m2iformation.fr/formation-iso-27032-lead-cybersecurity-manager-avec-certification/ISO-27032LCM/ [Dostupné online 25.10.2022]

Cieľová úroveň vedomostí získaných z kurzu

Mať základné znalosti o štandarde ISO/IEC 27032 a hĺbkovú znalosť o kybernetickej bezpečnosti.

Kurz je určený

Pre odborníkov v oblasti kybernetickej bezpečnosti, odborníkov v oblasti informačnej bezpečnosti, odborníkov, ktorí chcú riadiť program kybernetickej bezpečnosti, manažérov rozvoja programu kybernetickej bezpečnosti, IT špecialistov, poradcov špecializujúcich sa na IT a odborníkov v oblasti IT, ktorí si chcú zvýšiť svoje vedomosti a technické zručnosti.

Program

1. *Deň*

   Úvod do kybernetickej bezpečnosti a vysvetlenie súvisiacich pojmov podľa odporúčania normy ISO/IEC 27032

- Ciele a štruktúra kurzu
- Normy a regulačné rámce
- Základné pojmy kybernetickej bezpečnosti
- Program kybernetickej bezpečnosti
- Definovanie programu kybernetickej bezpečnosti
- Analýza organizácie
- Leadership

2. *Deň*

   Politiky kybernetickej bezpečnosti, riadenie rizík a mechanizmy útokov

- Politiky kybernetickej bezpečnosti
- Riadenie rizík kybernetickej bezpečnosti
- Mechanizmy útokov

3. *Deň*

   Opatrenia na kontrolu kybernetickej bezpečnosti, zdieľanie informácií a koordinácia informácií

- Opatrenia na kontrolu kybernetickej bezpečnosti
- Zdieľanie a koordinácia informácií
- Program odbornej prípravy a získavania povedomia z oblasti citlivosti dát

4. *Deň*
   Riadenie incidentov, monitorovanie a neustále zlepšovanie ochrany pred incidentmi

- Kontinuita činností
- Riadenie incidentov v oblasti kybernetickej bezpečnosti
- Zásah a zotavenie v prípade incidentu v oblasti kybernetickej bezpečnosti
- Závery prijaté z riešenia incidentov
- Testy kybernetickej bezpečnosti

- Meranie výkonnosti prijatých ochranných mechanizmov
- Neustále zlepšovanie

5. *Deň*
   Priebeh certifikácie

- Cena a vykonanie skúšky sú zahrnuté v cene kurzu
- Skúška (v angličtine) sa koná posledný deň po ukončení vzdelávania a vykonáva sa online alebo na papieri, jej trvanie je v priemere 3 hodiny
- V prípade neúspechu, kandidát môže skúšku opakovať v priebehu 12 nasledujúcich mesiacov bez dodatočných nákladov

Obsah tohto programu môže byť predmetom adaptácie v závislosti od úrovní, predpokladov a potrieb účastníkov kurzu.

Spôsoby hodnotenia získaných vedomostí

- Počas kurzu, pomocou prípadových štúdií alebo praktických zadaní
- Na konci kurzu, pomocou samo-hodnotiaceho dotazníka alebo výsledkami certifikačnej skúšky (hodnotiteľ alebo editor certifikačného testu

Záver

Problematike manažmentu kybernetickej bezpečnosti sa kladie aktuálne vo Francúzsku značná priorita, o čom svedčí aj angažovanosť viacerých vládnych a certifikačných autorít. Manažment kybernetickej bezpečnosti sa dostáva ako samostatný akreditovaný študijný program na viaceré univerzity. Aj viaceré národné agentúry a komisie zodpovedné za regulačné normy a štandardy v krajine sa venujú prijímaniu noriem v oblasti manažmentu kybernetickej bezpečnosti. Ako príklad uvádzame:

- Národný orgán pre financovanie a reguláciu odbornej prípravy a učňovského školstva - Autorité nationale de financement et de régulation de la formation professionnelle et de l'apprentissage
- Komisia pre certifikáciu francúzskych zručností. - Commission de la certification professionnelle de France compétences

Naposledy menovaná vypracovala aj všeobecne záväzný štandard pre Ciele Manažéra kybernetickej bezpečnosti:

Zvládať riadenie návrhu informačných systémov upraveného z hľadiska architektúry, prijímania rozhodnutí, zachovania procesov a bezpečnosti podniku

Poznať a ovládať techniky kybernetických útokov, s cieľom lepšie ich identifikovať a navrhnúť obranné stratégie a mechanizmy.

Nasadiť a implementovať nástroje potrebné na zabezpečenie informačných systémov, webových a mobilných aplikácií.

Poznať normy, metodológie a predpisy prijaté v oblasti bezpečnosti informačných systémov.

Príklady z Francúzska môžu byť vhodnou inšpiráciou aj pre slovenskú akademickú pôdu pri zavádzaní študijných programov tak pre bakalárske, ako aj magisterské štúdium na našich Vysokých školách, Univerzitách i Akadémii Policajného zboru v Bratislave.

Zoznam použitej literatúry:

https://www.francecompetences.fr/recherche/rncp/35588/ [Dostupné online 22.10.2022]

https://www.ppa.fr/ecole-commerce-alternance.html [Dostupné online 25.10.2022]

https://www.onisep.fr/Ressources/Univers-Formation/Formations/Post-bac/master-of-science-manager-de-la-cybersecurite [Dostupné online 20.10.2022]

https://www.2itechacademy.com/programmes/manager-cybersecurite/ [Dostupné online 25.10.2022]

https://www.m2iformation.fr/formation-iso-27032-lead-cybersecurity-manager-avec-certification/ISO-27032LCM/ [Dostupné online 25.10.2022]

https://www.ece.fr/program/msc-manager-cybersecurite/ [Dostupné online 20.10.2022]

Kontakt

mjr. JUDr. Matej Kostrec PhD.
Katedra informatiky a manažmentu
Akadémia Policajného zboru v Bratislave
e-mail: matej.kostrec@akademiapz.sk

Kybernetická (ne)bezpečnosť a sociálne siete

Radoslav Ivančík

Abstrakt: *Dynamický vývoj ľudskej spoločnosti, zvlášť v oblasti informačných a komunikačných technológií, systémov a prostriedkov, sprevádzaný rozvojom internetu a masovým využívaním najrôznejších sociálnych sietí, priniesol zásadné zmeny v ľudskej komunikácii a vytvoril nové spôsoby interakcie. Sociálne siete sa postupne stali bežnou súčasťou nášho osobného, spoločenského a v mnohých prípadoch aj pracovného života. Využívame ich na komunikáciu s rodinou, priateľmi, známymi, kolegami, spolupracovníkmi alebo inými ľuďmi. Žiaľ, tak ako v prípade iných vecí, aj sociálne siete a ich hromadné využívanie prinášajú okrem množstva pozitív aj množstvo negatív. Viaceré z nich sa veľmi úzko týkajú problematiky bezpečnosti, osobitne kybernetickej bezpečnosti, a preto autor v tejto súvislosti prináša vo svojom príspevku svoj pohľad na túto vysoko špecifickú oblasť.*

Kľúčové slová: *Kybernetická bezpečnosť, sociálne siete, internet, hrozby, riziká.*

Abstract: *The dynamic development of human society, especially in the field of information and communication technologies, systems, and tools, accompanied by the development of the Internet and mass use of various social networks, brought fundamental changes in human communication, and created new ways of interaction. Social networks have gradually become a common part of our personal, social and, in many cases, work lives. We use them to communicate with family, friends, acquaintances, colleagues, co-workers, or other people. Unfortunately, as in the case of other things, social networks and their mass use bring, in addition to a lot of positives, also a lot of negatives. Many of them are very closely related to the issue of security, especially cyber security, and therefore the author, in his contribution, brings his perspective on this highly specific area.*

Keywords: *Cyber security, social networks, internet, threats, risks.*

Úvod

Dynamický vývoj ľudskej spoločnosti v prvých dvoch dekádach tretieho tisícročia, zvlášť v oblasti informačných a komunikačných technológií, systémov a prostriedkov, sprevádzaný rapídnym rozvojom internetu a doslova až búrlivým vývojom a masovým využívaním najrôznejších sociálnych sietí, priniesol zásadné zmeny v ľudskej komunikácii a vytvoril nové spôsoby interakcie. Sociálne siete sa postupne stali bežnou súčasťou nášho osobného, spoločenského a v mnohých prípadoch aj pracovného života. Mnohí z nás, hlavne mladší ľudia, si už bez nich nedokážu svoj život ani predstaviť. Využívame ich na komunikáciu s rodinou, priateľmi, známymi, kolegami a inými ľuďmi. Razantný nástup sociálnych sietí a ich masívne využívanie priniesli revolučné zmeny v tom, ako dnes využívame internet, smartfóny, tablety, notebooky a počítače na osobné a profesionálne účely. Žiaľ, tak ako v prípade iných vecí, aj sociálne siete a ich hromadné využívanie prinášajú okrem množstva pozitív aj množstvo negatív[1]. Viaceré z nich sa veľmi úzko týkajú problematiky bezpečnosti, osobitne kybernetickej

[1] Bližšie pozri: GREGA, M. – ŽENTEK, M. – NEČAS, P. 2020. Security Threats Versus New Areas and Approaches of the Cyber Synthetic Environment. In Fabián, K. – Beňuška, T. (eds.): *Analysis of Social Network Security. Threats in cyberspace*. Krakow : Apeiron University of Public and Individual Security, 2020, s. 172-229; 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; KOSTREC, M. 2020. Nebezpečné hrozby v digitálnom priestore. In *Aktuálne výzvy kybernetickej bezpečnosti – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2020, s. 78-87; KORAUŠ, A. a kol. 2017. The safety risks related to bank cards and cyber attacks. In *Journal of Security and Sustainability Issues*, Vol. 6, No. 4, s. 563-574; 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.

bezpečnosti[2], a preto autor v tejto súvislosti prináša vo svojom príspevku svoj pohľad na túto vysoko špecifickú oblasť. Kybernetická bezpečnosť sociálnych sietí totiž priamo ovplyvňuje naše používanie týchto sietí, a tým aj našu bezpečnosť.

Nadmerné zdieľanie informácií na sociálnych sieťach a problémy s tým spojené

Podľa výsledkov viacerých realizovaných prieskumov z oblasti využívania sociálnych sietí uverejnených v prácach niektorých autorov[3] cca až 85 % používateľov sociálnych sietí uverejňuje na nimi využívaných sociálnych sieťach príspevky aspoň raz týždenne, pričom polovica z tejto skupiny uverejňuje príspevky denne. Zatiaľ čo prakticky všetky sociálne platformy umožňujú svojim používateľom nejakým spôsobom alebo formou zverejňovať informácie, niektoré z nich môžu mať predvolené nastavenia ochrany osobných údajov, vďaka ktorým sú používatelia náchylnejší na verejné zdieľanie informácií o nich, ich rodinných príslušníkoch, známych, pravidelných či nepravidelných aktivitách a pod. A hoci používatelia majú možnosť rozhodovať o tom, čo sa zdieľa, väčšina používateľov ponecháva nastavenia povolení tak, ako sú predvolené.[4]

Masové používanie sociálnych sietí spolu s nedostatočným nastavením súkromia tak poskytujú kyberzločincom a iným aktérom vykonávajúcim aktivity v kybernetickom priestore príležitosť hĺbkovo študovať a sledovať dôkladne vyhliadnuté, ale aj náhodné ciele – ich online profily, správanie, prepojenia, kontakty a pod. Príspevky zverejnené na sociálnych sieťach (či už ide napríklad o miesta registrácie, osobné alebo rodinné fotografie, videá, aktualizácie stavu atď.) im umožňujú získavať a následne zneužívať informácie o súkromnom a/alebo pracovnom živote používateľov sociálnych sietí. Útoky na základe týchto informácií môžu byť starostlivo vyladené a prispôsobené tak, aby sa zvýšila ich úspešnosť. Vysoký počet používateľov

[2] Bližšie pozri: 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.

[3] SHI, L. – LUO, J. – ZHU, C. – KOU, F. – CHENG, G. – LIU, X. 2022. A survey on cross-media search based on user intention understanding in social networks. In Computers in Human Behavior, 2022. [online] [cit. 15.11.2022] Dostupné na: <https://www.sciencedirect.com/ science/article/abs/pii/S1566253522002275>
ZHANG, X. J. - WANG, J. - MA, X. J. - KAN, J. Q. - ZHANG, H. F. 2022. Influence maximization in social networks with privacy protection. In Physica A: Statistical Mechanics and its Applications. [online] [cit. 15.11.2022] Dostupné na: <https://www.sciencedirect.com/science/article/abs/pii/S0378437122007373>

[4] Bližšie pozri: 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; 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; ZACHAR, Š. 2018. Anonymizácia komunikácie zmenou IP adresy ako metóda bezpečného prehliadania internetu. In *Aktuálne výzvy prevencie počítačovej kriminality – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2018, s. 217-224; alebo 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. 8-19.

sociálnych sietí vedie k tomu, že kyberzločinci a ďalší aktéri majú k dispozícii obrovské množstvo zneužiteľných údajov.

Je preukázané, že sociálne siete napredovali v ostatných rokoch míľovými krokmi, aj preto v súčasnosti predstavujú jeden z najžiadanejších spôsobov komunikácie a zdieľania informácií. Avšak, ako už bolo naznačené vyššie, spolu s mnohými výhodami, ktoré prinášajú svojim používateľom, prinášajú aj viaceré negatíva. V tejto súvislosti, najmä v súvislosti s nadmerným zdieľaním rôznych informácií, sa preto do popredia dostáva významný faktor – bezpečnosť, existujú totiž vážne obavy o kybernetickú bezpečnosť sociálnych sietí. Sú zraniteľné a keďže počet používateľov pristupujúcich na rôzne sociálne platformy sa každým dňom zvyšuje, zvyšujú sa aj hrozby a riziká. Medzi najčastejšie problémy spojené s používaním sociálnych sietí patria nižšie uvedené, ale aj mnohé ďalšie:

a) Ochrana osobných údajov: Používatelia zdieľajú svoje osobné informácie na sociálnych médiách, čo môže spôsobiť porušenie súkromia. Napríklad informácie o používateľovi môže zobraziť každý, ak je predvolené nastavenie používateľa verejné.

b) Data mining: Všetci za sebou zanechávame dátovú stopu na internete. Keď si niekto vytvorí nový účet na sociálnej sieti a poskytne podrobnosti, ako je dátum narodenia, meno, miesto, osobné zvyky, a bez nášho vedomia, všetky tieto údaje sa využívajú a zdieľajú s treťou stranou na cielenie reklamy. Môže to spôsobiť obavy o bezpečnosť, pretože tretia strana môže zhromažďovať aktualizácie o polohe používateľa v reálnom čase.

c) Vírusové a malvérové útoky: Malvér a vírusy si pomerne často nájdu cestu do počítačového systému cez otravné reklamy. Po získaní prístupu k sieti útočník ukradne dôverné údaje alebo spôsobí úplné narušenie počítačového systému.

d) Problémy spojené s používaním aplikácií tretích strán: Väčšina aplikácií v súčasnosti vyžaduje od používateľov povolenie na prístup k osobným informáciám, ako sú kontakty, obrázok a aktuálna geografická poloha pred inštaláciou, a niektoré z týchto aplikácií, ktoré sú spustené na pozadí, môžu stiahnuť malvér na telefón alebo inteligentné zariadenia používateľa bez jeho vedomia.

e) Právne problémy: S používaním sociálnych médií, ako je napríklad uverejňovanie urážlivého obsahu voči akejkoľvek osobe, komunite alebo krajine, sú spojené právne riziká.

f) Krádež identity: Keďže milióny ľudí zdieľajú svoje osobné údaje, aby sa zaregistrovali na jednej alebo viacerých platformách sociálnych médií, tieto údaje sa stávajú zraniteľnými, pretože hackeri a zlodeji identity tieto informácie používajú na resetovanie hesiel, žiadosti o pôžičky alebo iné škodlivé ciele.

g) Romantické podvody: Romantický podvod je podvodná schéma, v ktorej podvodník predstiera romantický záujem o cieľ, nadviaže vzťah a potom sa pokúša pod zámienkou získať od cieľa peniaze alebo citlivé informácie.

h) Whistleblower: Ľudia sú na sociálnych sieťach často impulzívni; bez rozmýšľania dávajú najavo svoje rozhorčenie so svojimi kolegami alebo šéfmi. Vo svojich príspevkoch môžu zámerne odhaliť citlivé údaje, čo môže spôsobiť značné poškodenie dobrého mena organizácie.

i) Cyber Stalking: Vzťahuje sa na obťažovanie cez internet. Kyberstalkeri obťažujú obete na sociálnych sieťach posielaním nepríjemných a oplzlých správ. Premieňajú fotografie obetí

a šíria ich na sociálnych médiách, pričom tvrdia, že klebety robia život obete neznesiteľným.

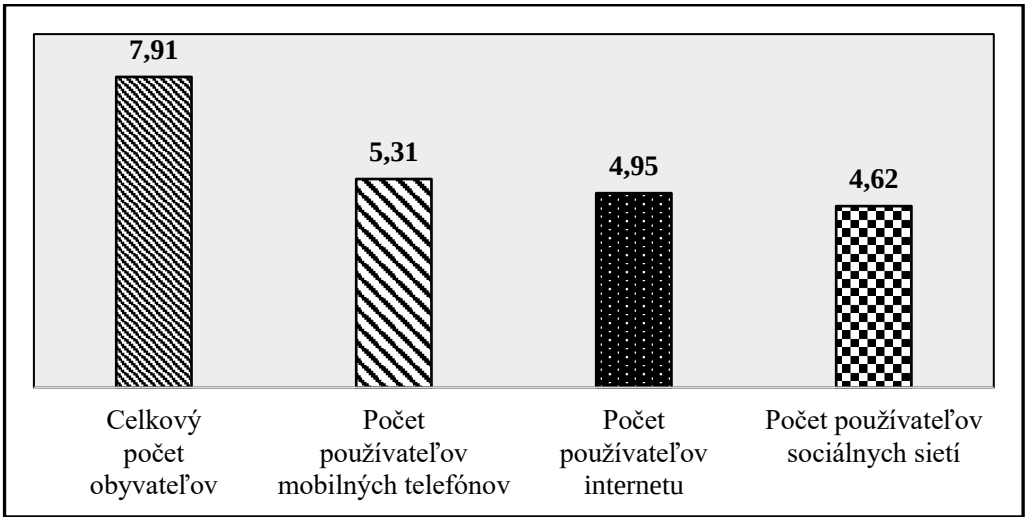
j) Kybernetické šikanovanie: Vzťahuje sa na šikanovanie prostredníctvom digitálneho média. Môže sa to odohrávať na sociálnych médiách, herných platformách, platformách na odosielanie správ atď. Je zameraný na vystrašenie, zahanbenie alebo obťažovanie cieľovej obete.

k) Kybernetický terorizmus: V súčasnosti teroristické organizácie (skupiny), ale aj iní aktéri využívajú sociálne médiá aj na uľahčenie aktivít súvisiacich s terorizmom. Môže ísť o podporu, propagáciu, zapájanie a šírenie propagandy, podnecovanie k terorizmu, nábor, výcvik a plánovanie teroristických útokov a pod.

Masové využívanie sociálnych sietí

S masovým využívaním sociálnych sietí úzko súvisí aj ďalší problém. Sociálne siete by mali poskytovať neutrálne prostredie na vyjadrenie názorov. Ale je to skutočne tak? Veď už len základná koncepcia odmeňovania lajkami a zdieľaniami môže podporovať vznik prejavov vyjadrujúcich pobúrenie, pričom pozitívna spätná väzba na poburujúce príspevky podporuje tvorbu ďalších. Takéto „stimuly“ na sociálnych sieťach potom menia spôsob, akým sa ľudia vyjadrujú a akým pridávajú príspevky. Ak príspevok vyjadrujúci pobúrenie nad nejakou udalosťou, javom, situáciou a pod. dostane viac lajkov a zdieľaní ako „bežný“ príspevok, používateľov sociálnych sietí to zväčša podnecuje k pridaniu ďalšieho príspevku podobného charakteru. Odmeny prostredníctvom sociálnych sietí vytvárajú slučky pozitívnej spätnej väzby, ktoré podporujú reakciu. Platformy sociálnych sietí, ako uvádza Jurčík, pritom neodrážajú iba to, čo sa deje v spoločnosti, vytvárajú tiež stimuly, ktoré menia spôsob, akým používatelia reagujú na politické, spoločenské a iné udalosti v spoločnosti,[5] ako často reagujú, koľko času trávia na sociálnych sieťach, aké údaje, informácie, príspevky zverejňujú atď.

Graf 1
Prehľad o používateľoch mobilných telefónov, internetu a sociálnych sietí v roku 2022 na celom svete (v mld.)



Zdroj: DataReportal, 2022

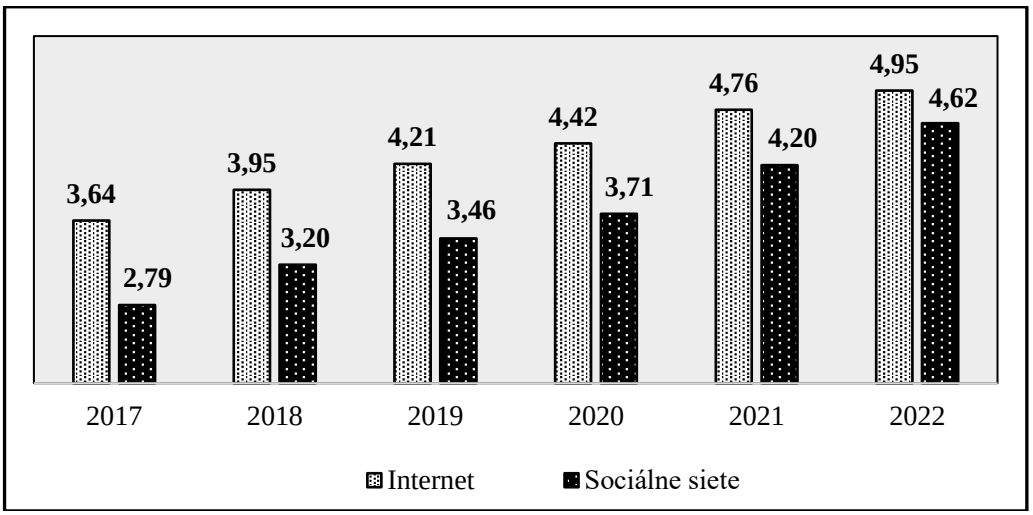
[5] JURČÍK, M. 2021. Vedci pozorovali, ako môžu sociálne siete radikalizovať používateľov. In *Živé.sk*, 2021. Dostupné na: <https://zive.aktuality.sk/clanok/8t8dxst/vedci-pozorovali-ako-mozu-socialne-siete-radikalizovat-pouzivatelov/>.

Práve túto skutočnosť využívajú rôzni kyberzločinci a ďalší aktéri. Darí sa im aj vďaka tomu, že vzhľadom na postupujúcu informatizáciu, internetizáciu a digitalizáciu ľudskej spoločnosti počet používateľov sociálnych sietí neustále rastie a ľudia trávia na nich stále viac času (grafy 1 až 3). A, žiaľ, darí sa im aj preto, že platformami používané algoritmy preferujú šokujúci, poburujúci, pozornosť vyvolávajúci obsah. K tomu, že sa im darí navyše prispela v ostatných rokoch aj pandémia koronavírusu spôsobujúceho ochorenie Covid-19 a rôzne opatrenia, resp. obmedzenia, ktoré boli prijatými vládami či samosprávami v rámci boja proti pandémii.[6]

Veľkú zásluhu na tom, že kyberzločincom využívajúcim sociálne siete sa darí má rozvoj internetu. Sociálne siete spájajú obrovské počty ľudí z rôznych častí celého sveta a umožňujú im komunikovať a navzájom si vymieňať rôzne informácie. Mobilný telefón používa dnes cca 5,31 miliardy obyvateľov, čo predstavuje viac ako dve tretiny (67,1 %) svetovej populácie, internet používa približne 4,95 miliardy ľudí, teda viac ako tri pätiny (62,5 %) svetovej populácie, a počet aktívnych používateľov sociálnych sietí dosahuje zhruba 4,62 miliardy, čo predstavuje podiel na celkovom obyvateľstve planéty na úrovni 58,4 % (graf 1). Sociálne siete používa pritom prostredníctvom mobilného telefónu až 95 % ich užívateľov.

O tom, aký dynamický je rast používateľov internetu a sociálnych sietí svedčí fakt, že za ostatných päť rokov celosvetovo stúpol počet používateľov internetu o viac ako jednu tretinu (o 36 %). Kým v roku 2017 používalo internet zhruba 3,64 miliardy ľudí, tak v roku 2022 to už bolo približne 4,95 miliardy. Rast používateľov sociálnych sietí je ešte dynamickejší, nakoľko stúpol v hodnotených rokoch o takmer dve tretiny (o 65,6 %). Kým v roku 2017 používalo sociálne siete približne 2,79 miliardy ľudí, v roku 2022 sú to už zhruba 4,62 miliardy (graf 2). Z nich jeden užívateľ strávi na sociálnych sieťach priemerne denne 2 hodiny a 27 minút a priemerne mesačne využíva 7,5 rôznych sociálnych sietí (graf 3).

Graf 2
Prehľad rastu používateľov internetu a sociálnych sietí
v rokoch 2017 až 2022 (v mld.)

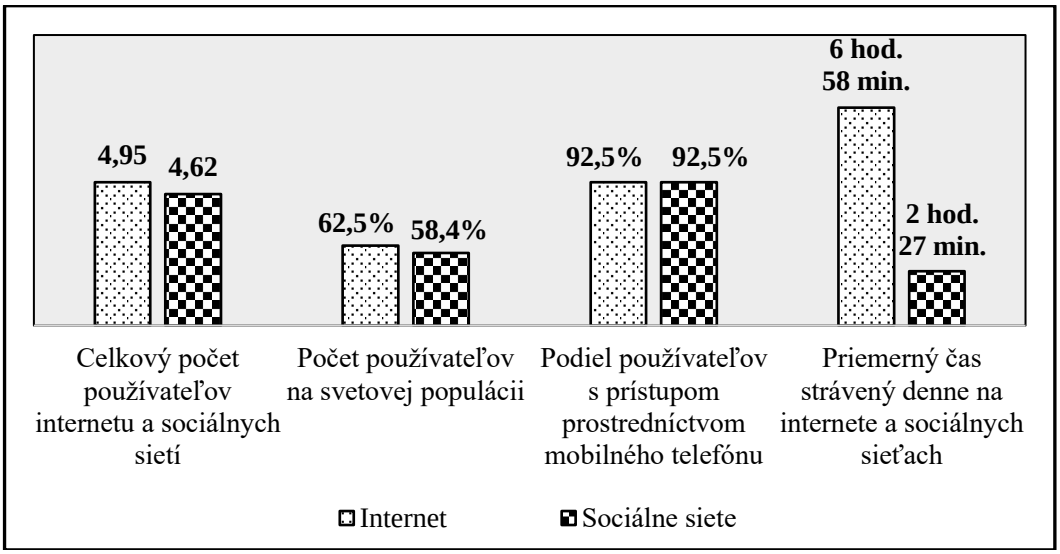


Zdroj: DataReportal, 2022

[6] Bližšie pozri: IVANČÍK, R. 2021. Boj proti dezinformáciám týkajúcich sa pandémie koronavírusu na úrovni Európskej únie. In *Almanach – aktuálne otázky svetovej ekonomiky a politiky*, 2021, roč. 16, č. 3, s. 5-15; alebo HAJDÚKOVÁ, T. – KUCHTOVÁ, J. 2020. Využitie informačných technológií v boji proti pandémii Covid-19. In *Policajná teória a prax*, 2020, roč. 28, č. 3, s. 5-26.

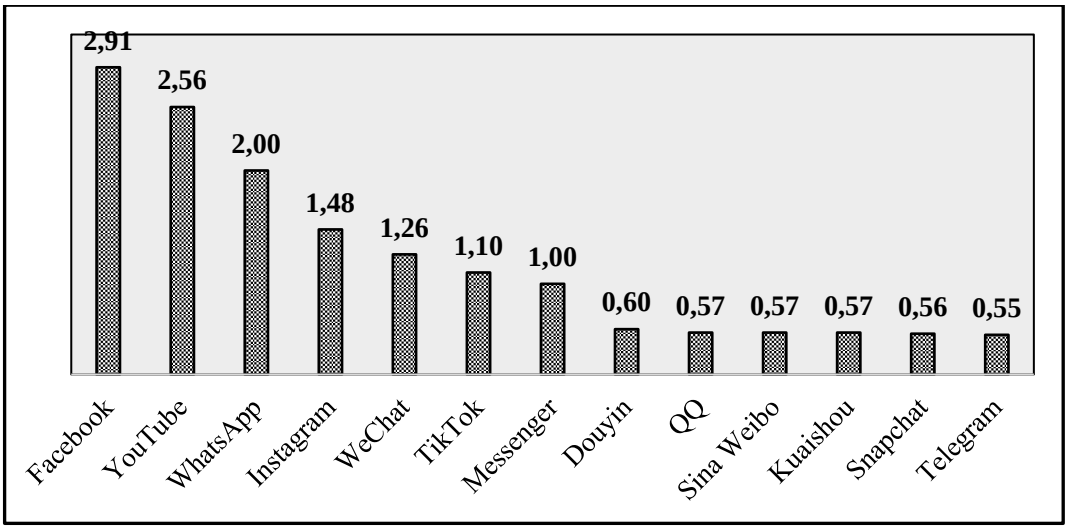
Celosvetovo najpopulárnejšiu sociálnou sieťou je Facebook, ktorý v januári 2022 využívalo približne 2,91 miliardy aktívnych používateľov, druhou v poradí je YouTube s 2,56 miliardou aktívnych používateľov a treťou WhatsApp, ktorú v súčasnosti aktívne používajú cca dve miliardy ľudí. Medzi ďalšie populárne sociálne siete, ktoré majú viac ako jednu miliardu aktívnych používateľov patria Instagram, WeChat, TikTok a Messenger. S viac ako pol miliardou aktívnych používateľov sa môžu pochváliť sociálne siete Douyin, QQ, Sina Weibo, Kuaishou, Snapchat a Telegram (graf 4).

Graf 3
Prehľad vybraných údajov o používateľov internetu a sociálnych sietí v roku 2022



Zdroj: DataReportal, 2022

Graf 4
Prehľad sociálnych sietí s najväčším počtom aktívnych používateľov v roku 2022 na celom svete (v mld.)



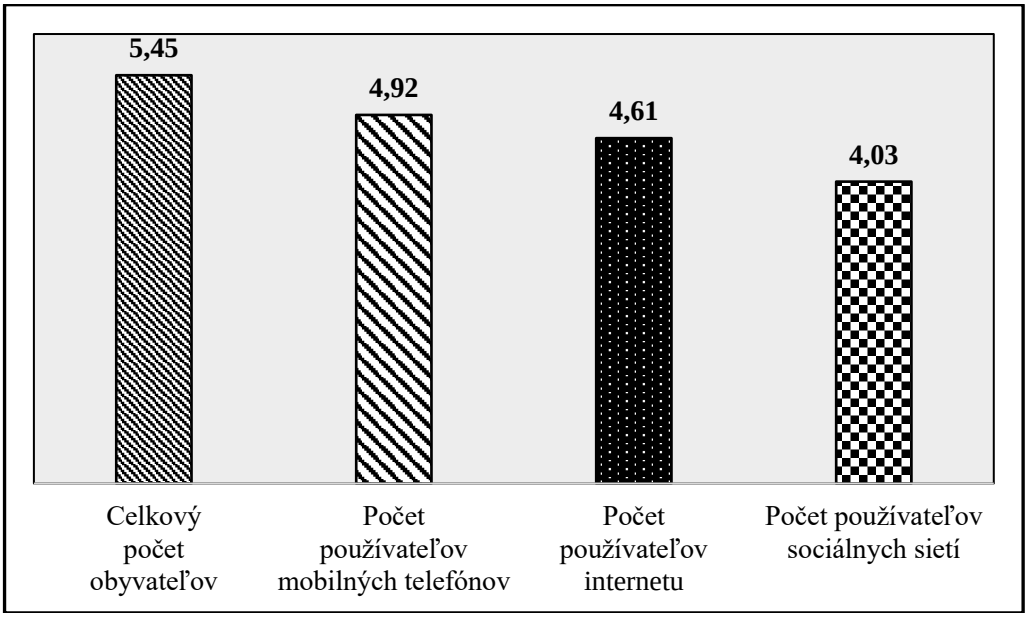
Zdroj: DataReportal, 2022

Koronakríza nás ovplyvnila všetkých, ako jednotlivcov, tak aj sociálne skupiny. S postupným nárastom izolácie, narastalo aj používanie sociálnych sietí a čas strávený pred obrazovkami počítačov, tabletov či mobilných telefónov. Nebolo to len preto, že sociálne siete a digitálne nástroje sme mohli na prvý pohľad považovať za záchranu v čase karantény a sociálneho dištancovania sa, ale tiež z dôvodu, že na sociálnych sieťach možno jednoducho a rýchlo nájsť všetky nové informácie o aktuálnej situácií.

Na Slovensku je využívanie sociálnych sietí jednou z najčastejších aktivít, ktoré Slováci na internete vykonávajú. Až 85 % Slovákov používa pravidelne nejakú sociálnu sieť, pričom 63 % ju navštívi aspoň raz denne. Podiel ľudí „pripojených“ na sociálne siete je na Slovensku v posledných rokoch stabilný. Podiel na celej populácii sa už veľmi nezvyšuje, ale rastie intenzita využívania. Vidieť to na raste podielu tých obyvateľov Slovenska, ktorí sa na sociálne siete pripájajú aspoň raz denne. Sociálne siete majú v obľube viac ženy ako muži, pričom tento trend je badateľný prakticky od vzniku sociálnych sietí.[7]

V poslednej dobe bol zaznamenaný nárast frekvencie využívania sociálnych sietí aj u ľudí starších ako 60 rokov, kde viac ako polovica z nich deklaruje, že využíva sociálne siete aspoň raz mesačne. Hoci sa celkový počet užívateľov medzi ľuďmi nad 60 rokov využívajúcich sociálne siete zvýšil iba mierne, narástol počet pravidelných denných užívateľov. Každodenná interakcia na sociálnej sieti sa tak výrazne zvýšila práve v tejto vekovej kategórii. Podiel užívateľov na dennej báze sa už blíži k úrovni 40 %.

Graf 5
Prehľad o používateľoch mobilných telefónov, internetu a sociálnych sietí v roku 2022 na Slovensku (v mil.)



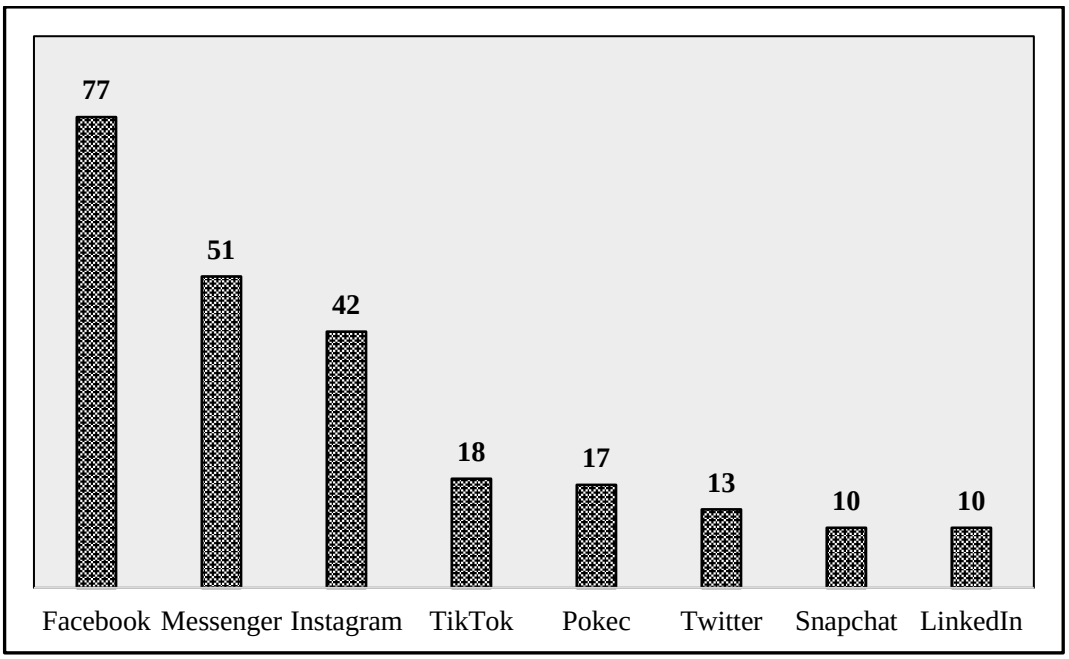
Zdroj: Go4insight, 2022

Na Slovensku, ak nepočítame špecifický You Tube, je dlhodobo najpoužívanejšou sociálnou sieťou Facebook, ktorý využíva 77 % slovenskej populácie. Druhou najpopulárnejšou sieťou je Messenger, ktorý využíva asi 51 % slovenskej populácie, a na treťom mieste je Instagram, ktorý využíva 42 % Sloveniek a Slovákov. Hoci Instagram stále môžeme považovať

[7] KOČAN, R. 2022. *Koľko Slovákov je na sociálnych sieťach?* In *Go4insight*, 2022. Dostupné na: <https://www.go4insight.com/post/koľko-slovákov-je-na-sociálnych-sieťach>.

za sociálnu sieť predovšetkým pre mladých ľudí, pomaly rastie využívanie aj medzi ľuďmi v mladšom strednom veku (do 40 rokov) a aj medzi rodičmi mladých tínedžerov. Podobný profil môže mať o niekoľko rokov aj TikTok, ktorý je v súčasnosti atraktívny predovšetkým pre mladistvých a mladých dospelých. Výraznejší počet užívateľov majú ešte sociálne siete TikTok (18 %), Pokec (17 %), Twitter (13 %) Snapchat a LinkedIn po 10 % (graf 5). Ostatné na Slovensku používané sociálne siete ako napríklad Reddit, Clubhouse, OnlyFans, Twitch alebo Discord majú menej ako 10 % používateľov. Prakticky všetky sociálne siete využívajú intenzívnejšie ženy ako muži. Jedinou sieťou, ktorú využívajú častejšie muži ako ženy je iba Twitter.[8]

Graf 6
Prehľad sociálnych sietí s najväčším počtom aktívnych používateľov v roku 2022 na Slovensku (v %)



Zdroj: Go4insight, 2022

V tejto súvislosti je dôležité si uvedomiť, že nárast počtu používateľov sociálnych sietí a času stráveného na sociálnych sieťach spôsobil, že počas pandémie koronavírusu sa negatíva, resp. problémy spojené s používaním sociálnych sietí prehĺbili. Z hľadiska boja proti kyber-zločinu a zaisťovania kybernetickej bezpečnosti možno konštatovať, že:

- kybernetická kriminalita vzrástla o 600 % v dôsledku pandémie COVID-19,
- odhaduje sa, že kybernetické zločiny budú do roku 2025 stáť celosvetovo cca 10,5 bilióna dolárov ročne,
- celosvetové ročné náklady na kybernetickú kriminalitu sa odhadujú na 6 miliárd dolárov ročne,
- náklady na kybernetickú kriminalitu predstavujú hodnotu 1 % globálneho HDP,
- v priemere stojí malvérový útok spoločnosť viac ako 2,5 milióna dolárov (vrátane času potrebného na vyriešenie útoku,
- ransomvér bol v roku 2021 57x deštruktívnejší ako v roku 2015,

[8] KOČAN, R. 2022. Koľko Slovákov je na sociálnych sieťach v roku 2022? In *Go4insight*, 2022. Dostupné na: <https://www.go4insight.com/post/koľko-slovákov-je-na-sociálnych-sieťach-v-roku-2022>.

- jednotlivci strácajú kvôli kybernetickým zločinom v priemere 4 476 USD ročnr,
- jednotlivci prichádzajú kvôli kybernetickej kriminalite o 318 miliárd dolárov ročne,
- jednotlivci z dôvodu phishingových podvodov prichádzajú v priemere o 225 dolárov ročne,
- medzi najčastejšie kybernetické zločiny v roku 2021 patrili: vydieranie, krádež identity, krádež osobných údajov a phishingové útoky,
- prístup k celej online identite jednotlivca má hodnotu približne 1 000 dolárov,
- za 50 dolárov sa dá získať malvér s návodom, ako ho používať,
- mesačná investícia 34 dolárov môže priniesť kyberzločincom 25 000 dolárov mesačne.[9]

Záver

V dnešnej modernej dobe široko dostupného rýchleho 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 sociálnych sietí. Práve ich rozmach sociálnych sietí, že predovšetkým mladí ľudia trávia na nich až príliš veľa času a je potom pre nich často oveľa pohodlnejšie získavať informácie priamo zo sociálnych sietí a nie z klasických spravodajských portálov. Nielen oni, ale aj mnohí ďalší pri používaní sociálnych sietí odovzdávajú množstvo osobných a cenných údajov, ktoré sú kyberzločincami mnohokrát ľahko zneužiteľné. Ďalším problémom je fakt (existujú o tom mnohé svedectvá a dôkazy), že množstvo priaznivcov prostredníctvom sociálnych sietí priťahujú a získavajú na svoju činnosť radikálne organizácie, ktoré šíria rôzne falošné správy, dezinformácie a propagandu.

Medzi najzraniteľnejšie z hľadiska týchto rizík patria demokratické štáty. Európska únia i jej členské štáty už prijímajú praktické opatrenia na neutralizáciu zneužívania sociálnych sietí, ale pre každý členský štát je dôležité mať aj vlastnú transparentnú a konkrétnu politiku, prípadne viac politík, stratégií alebo koncepcií zameraných na zaistenie kybernetickej bezpečnosti, teda aj na boj proti kybernetickej kriminalite. Jednou z možností je legislatívna regulácia sociálnych sietí, čo je aj jedným z aktuálnych zámerov vlády Slovenskej republiky z dôvodu toho, že sociálne siete sa jednak podieľajú na kybernetickom zločine a zároveň prispievajú k zbytočnému rozdeľovaniu spoločnosti. Ako uviedla podpredsedníčka vlády a ministerka investícií, regionálneho rozvoja a informatizácie SR Veronika Remišová: „V nadväznosti na nenávistné prejavy na sociálnych sieťach som predložila na koaličnú radu nový návrh zákona na prísnejšiu reguláciu sociálnych platforiem. Sociálne siete zarábajú miliardy eur na šírení nenávisti – čím nenávistnejší príspevok, tým viac lajkov a zdieľaní – a nenesú za to absolútne žiadnu zodpovednosť.“ [10]

Na sociálnych sieťach sa navyše často objavuje obsah, ktorý je v rozpore s našou legislatívou a preto vláda chce, aby sociálne siete niesli zodpovednosť, aby nedostali len malú pokutu, ale vysokú, významnú pokutu, ktorá ich bude odrádzať od takéhoto konania. Takúto legislatívu majú napríklad v Nemecku, ktoré ju zaviedlo pre pravicový extrémizmus a rôzne fašistické tendencie. Vláda preto podľa ministerky pripravuje zákon, ktorý v zásade kopíruje nemeckú cestu. Sloboda slova je síce jednou z najväčších hodnôt a výdobytkov demokracie, ale nenechávať voľne prístupné stránky, kde vyzývajú mládež k samovraždám a násilným činom patrí k základnej ochrane a zaisteniu bezpečnosti v spoločnosti.

---

[9] CSS. 2022. Cyber Security Statistics. In *Purplesec,* 2022. [online] [cit. 15.11.2022] Dostupné na: <https://purplesec.us/resources/cyber-security-statistics/#Cost>.

[10] CABAN, B. 2022. Ministerka Remišová chce zákonom regulovať sociálne siete, rozdeľujú podľa nej spoločnosť. IN *TouchIT,* 2022. [online] [cit. 17.11.2022] Dostupné na: <https://touchit.sk/remisova-chce-regulovat-socialne-siete/450791>.

Podrobnosti návrhu nového zákona zatiaľ nie sú známe, avšak aj po jeho prípadnom schválení bude prípadná vymožiteľnosť otázna. Slovensko je totiž pre technologických gigantov ako Meta, čo je materská spoločnosť Facebooku aj Instagramu, okrajový trh. Už len samotné vymazávanie nenávistných komentárov či blokovanie používateľov, ktorí šíria evidentne klamlivé informácie, je nedostatočné, vágne a neraz úplne absentuje. Najvhodnejšie by bolo regulovať sociálne siete priamo na úrovni Európskej únie. Príkladom úspešného zásahu voči sociálnej sieti môže byť Nemecko, ktoré začiatkom tohto roka pohrozilo komunikačnej platforme Telegram zablokovaním v krajine s možným rozšírením zákazu na celú Európsku úniu, ak sieť nezačne zasahovať proti kanálom, na ktorých sa združujú extrémisti, radikáli a šíritelia nepravdivých informácií o očkovaní alebo 5G sieťach. Hrozba v tomto prípade pomohla, keďže Telegram začal problémové kanály v Nemecku mazať. Podobnou cestou by sa malo vybrať aj Slovensko.

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.

CABAN, B. 2022. Ministerka Remišová chce zákonom regulovať sociálne siete, rozdeľujú podľa nej spoločnosť. IN *TouchIT*, 2022. [online] [cit. 17.11.2022] Dostupné na: <https://touchit.sk/remisova-chce-regulovat-socialne-siete/450791>.

CSS. 2022. Cyber Security Statistics. In *Purplesec*, 2022. [online] [cit. 15.11.2022] Dostupné na: <https://purplesec.us/resources/cyber-security-statistics/#Cost>.

DR. 2022. Global Digital Overview. In *DataReportal,* 2022. [online] [cit. 16.11.2022] Dostupné na: <https://datareportal.com/reports/digital-2022-global-overview-report>.

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.

GREGA, M. – ŽENTEK, M. – NEČAS, P. 2020. Security Threats Versus New Areas and Approaches of the Cyber Synthetic Environment. In Fabián, K. – Beňuška, T. (eds.): *Analysis of Social Network Security. Threats in cyberspace*. 2020, s. 172-229. Krakow: Apeiron University of Public and Individual Security in Kraków. ISBN 978-83-64035-70-8.

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. – KUCHTOVÁ, J. 2020. Využitie informačných technológií v boji proti pandémii Covid-19. In Policajná teória a prax, 2020, roč. 28, č. 3, s. 5-26. 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.

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.

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. 2021. Boj proti dezinformáciám týkajúcich sa pandémie koronavírusu na úrovni Európskej únie. In Almanach – aktuálne otázky svetovej ekonomiky a politiky, 2021, roč. 16, č. 3, s. 5-15. ISSN 1339-3502. [online] [cit. 29-05-2022] Dostupné na: <https://fmv.euba.sk/ www_write/files/dokumenty/veda-vyskum/almanach/almanach_ 3_2021.pdf>.

JURČÍK, M. 2021. Vedci pozorovali, ako môžu sociálne siete radikalizovať používateľov. In *Živé.sk*, 2021. Dostupné na: <https://zive.aktuality.sk/clanok/8t8dxst/vedci-pozorovali-ako-mozu-socialne-siete-radikalizovat-pouzivatelov/>.

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. 8-19. ISBN 978-80-8054-968-8.

KOČAN, R. 2022. Koľko Slovákov je na sociálnych sieťach v roku 2022? In Go4insight, 2022. [online] [cit. 30-05-2022] Dostupné na: <https://www.go4insight. com/post/koľko-slovákov-je-na-sociálnych-sieťach-v-roku-2022>.

KOČAN, R. 2022. Koľko Slovákov je na sociálnych sieťach? In Go4insight, 2022. [online] [cit. 30-05-2022] Dostupné na: <https://www.go4insight.com/post/koľko-slovákov-je-na-sociálnych-sieťach>.

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.

KORAUŠ, A. – DOBROVIČ, J. – RAJNOHA, R. – BREZINA, I. 2017. The safety risks related to bank cards and cyber attacks. In *Journal of Security and Sustainability Issues,* Vol. 6, No. 4, s. 563-574. ISSN 2029-7025.

KORAUŠ, A. – KELEMEN, P. – ZACHAR, Š. 2019. Riadenie rizika podvodu z pohľadu bezpečnosti a včasného odhalenia. In *Aktuálne výzvy kybernetickej bezpečnosti (v podmienkach bezpečnostných zložiek)*. Bratislava : Akadémia Policajného zboru, 2019, s. 66-71. ISBN 978-80-8054-819-3.

KOSTREC, M. 2019. Ochrana osobných údajov – Výsledky výskumov vykonaných vo Francúzsku, na Slovensku a v Českej republike. In *Aktuálne výzvy kybernetickej bezpečnosti (v podmienkach bezpečnostných zložiek)*. Bratislava : Akadémia Policajného zboru, 2019, s. 78-96. ISBN 978-80-8054-819-3.

KOSTREC, M. 2020. Nebezpečné hrozby v digitálnom priestore. In *Aktuálne výzvy kybernetickej bezpečnosti (Special Edition 2020) : zborník príspevkov z vedeckej konferencie*

s medzinárodnou účasťou. Bratislava : Akadémia Policajného zboru, 2020, s. 78-87. ISBN 978-80-8040-819-3.

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.

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.

MÜLLEROVÁ, J – ŠIŠULÁK, S. 2020. Criminality software control tools of environmental crime. In *20th International Multidisciplinary Scientific GeoConference Proceedings SGEM 2020,* Sofia : Stef92, s. 207-212. ISBN 978-619-7603-10-1.

OLAK, A. 2012. *Bezpieczeństwo i zagrożenia społeczne - zarys problematyki.* Rzeszów : Wydawnictwo Amelia, 2012. 146 s. ISBN 978-83-63359-32-4.

OLAK, A. – KRAUZ, A. 2014. Cyberwojna internetowa narzędziem grożnej broni cyfrowej na rubieży bezpieczeństwa globalnej infrastruktury krytycznej. In *Vojenské reflexie* 2014, roč. 9, č. 1, s. 130-143. ISSN 1336-9202.

SHI, L. – LUO, J. – ZHU, C. – KOU, F. – CHENG, G. – LIU, X. 2022. A survey on cross-media search based on user intention understanding in social networks. In *Computers in Human Behavior*, 2022. [online] [cit. 15.11.2022] Dostupné na: <https://www.sciencedirect.com/ science/article/abs/pii/S1566253522002275>

TOMÁŠEK, R. – TOMÁŠEKOVÁ, L. 2020. Kybernetické hrozby a kybernetický terorizmus. In *Aktuálne výzvy kybernetickej bezpečnosti (Special Edition 2020) : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2020, s. 146-152. 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. 8-19. ISBN 978-80-8054-968-8.

ZACHAR, Š. 2018. Anonymizácia komunikácie zmenou IP adresy ako metóda bezpečného prehliadania internetu. In *Aktuálne výzvy prevencie počítačovej kriminality – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2018, s. 217-224. ISBN 978-80-8054-773-8.

ZHANG, X. J. – WANG, J. – MA, X. J. – KAN, J. Q. – ZHANG, H. F. 2022. Influence maximization in social networks with privacy protection. In *Physica A: Statistical Mechanics and its Applications*. [online] [cit. 15.11.2022] Dostupné na: <https://www.sciencedirect.com/ science/article/abs/pii/S0378437122007373>

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

Potreba skúmania úrovne kybernetickej bezpečnosti v spoločnosti

Michaela Kiššová

Abstrakt:
Skúmanie úrovne kybernetickej bezpečnosti vnímame ako preventívny nástroj na zmiernenie rizík, ktoré v súčasnej dobe ohrozujú skoro každého člena spoločnosti v kybernetickom priestore. Autorka sa zaoberala štyrmi základnými okruhmi, ktoré rozpracovala v predmetnom príspevku a to „aktuálnu agendu Európskej únie v tejto oblasti", „analýzu kybernetickej bezpečnosti v podnikateľskom sektore" a „analýzu kybernetickej bezpečnosti na základe výskumu verejnej mienky" a „situačné povedomie a kybernetickú prevenciu vo vzťahu ku kybernetickej bezpečnosti".
Kľúčové slová:
kybernetická bezpečnosť, analýza, Slovenská republika, Európska únia, situačné povedomie, kybernetická prevencia.

Abstract:
We perceive the examination of the level of cyber security as a preventive tool for mitigating risks that currently threaten almost every member of society in cyberspace. The author dealt with four basic areas, which she described further in an article, namely "the current agenda of the European Union in this area", "cyber security analysis in the business sector" and "cyber security analysis based on public opinion research" and "situational awareness and cyber prevention in relation to cyber security".
Key words:
cyber security, analysis, Slovak republic, European Union, situational awareness, cyber prevention

Úvod

Každý jav, proces či činnosť majú svoju históriu, ktorá ich kreovala a oni sa vyvíjali až do súčasnej, poznateľnej podoby. Avšak ich vývoj neustále pokračuje, aby sa objavovali v nových podobách a mohli pôsobiť na čo najväčší počet adresátov. Touto cestou si prechádza aj kybernetická bezpečnosť[1], ktorú ovplyvnili viaceré varovné minulé prípady, ktorých dôsledky vidíme aj v súčasnosti ako napríklad sieťové infraštruktúry, ktoré vrátane noriem nepočítali so zabezpečením, internet vznikol ako nezabezpečené komunikačné prostredie, aplikácie na internete neboli zo začiatku zabezpečené, rozsiahle pokroky v umelej inteligencii a pod.

Vzniknutý stav udalostí sa do značnej miery snažili ovplyvniť a zvrátiť ich možný negatívny vplyv do budúcnosti aj orgány Európskej únie a to prostredníctvom troch základných európskych dokumentov, ktorými sú Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 zo dňa 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov), Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo dňa 6. júla 2016 o opatreniach k zaisteniu vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (ďalej len „NIS")[2], Nariadenie Európskeho parlamentu a Rady

[1] Kybernetická bezpečnosť je charakterizovaná ako „*stav, v ktorom sú siete a informačné systémy schopné odolávať na určitom stupni spoľahlivosti akémukoľvek konaniu, ktoré ohrozuje dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov*." (§ 3, písm.h) Zákon č. 69/2018 Z.z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov).

[2] V roku 2022 pristúpil Európsky parlament k Legislatívnemu uzneseniu z 10. novembra 2022 o návrhu smernice Európskeho parlamentu a Rady o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii a o zrušení smernice (EÚ) 2016/1148. Daný návrh prispôsobuje súčasným podmienkam „*existujúci právny rámec, pričom sa zohľadňuje rastúca digitalizácia vnútorného trhu počas posledných rokov a vyvíjajúce sa hrozby v oblasti kybernetickej bezpečnosti. Návrh sa zaoberá aj niekoľkými nedostatkami, ktoré bránili využiť plný potenciál smernice NIS, pričom digitálna transformácia spoločnosti (posilnená krízou spôsobenou pandémiou COVID-19) rozšírila panorámu hrozieb a prináša nové výzvy, ktoré si vyžadujú prispôsobené a inovačné reakcie. Počet kybernetických útokov naďalej narastá, pričom sú tieto útoky čoraz*

(EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (akt o kybernetickej bezpečnosti).[3]

Popri uvedených dokumentoch bol vypracovaný aj Balíček opatrení v oblasti kybernetickej bezpečnosti, ktorý mal za úlohu skvalitniť národnú a európsku pripravenosť na kybernetické útoky. Predmetný balíček obsahuje viaceré právne nástroje, ktoré do tohto obdobia neboli rozpracované do takto ucelenej podoby a to Spoločné oznámenie Európskeho parlamentu a Rady „Odolnosť, odrádzanie a obrana: budovanie silnej kybernetickej bezpečnosti pre EÚ[4], Odporúčanie Komisie (EÚ) 2017/1584 z 13. septembra 2017 o koordinovanej reakcii na kybernetické incidenty a krízy veľkého rozsahu[5], Smernica Európskeho parlamentu a Rady (EÚ) 2019/713 zo 17. apríla 2019 o boji proti podvodom s bezhotovostnými platobnými prostriedkami a proti ich falšovaniu a pozmeňovaniu, ktorou sa nahrádza rámcové rozhodnutie Rady 2001/413/SVV[6], Správa Komisie Európskeho parlamentu a Rade o posúdení rozsahu, v akom členské štáty prijali opatrenia, ktoré sú nevyhnutné na dosiahnutie súladu so smernicou 2013/40/EÚ o útokoch na informačné systémy, ktorou sa nahrádza rámcové rozhodnutie Rady 2005/222/SVV[7].[8]

Dané opatrenia vymedzili oblasti, v ktorých vznikajú kybernetické riziká a hrozby zasahujúce do bezpečnostnej politiky štátu. Európska komisia a vysoký predstaviteľ Únie pre zahraničné veci a bezpečnostnú politiku 16. 12. 2020 uverejnili spoločné oznámenie Európskeho parlamentu a Rade pod názvom - Stratégia kybernetickej bezpečnosti EÚ v digitálnej dekáde. Cieľom predkladaného dokumentu je zamerať sa na prioritné oblasti odolnosti Európy voči kybernetickým hrozbám a posilniť bezpečnosť využívania

---

dômyselnejšie a pochádzajú zo širokej škály zdrojov v rámci EÚ aj mimo nej.“ (Návrh Smernice Európskeho parlamentu a Rady o opatreniach na zabezpečenie vysokej spoločenskej úrovne kybernetickej bezpečnosti v Únii a o zrušení smernice (EÚ) 2016/1148).

[3] SEDLÁK, P.- KONEČNÝ, M. - a kol. *Kybernetická (ne)bezpečnost: Problematika bezpečnosti v kyberprostoru*. Brno: Akademické nakladatelství CERM, 2021, s. 38 - 39.

[4] K hlavným úlohám tohto dokumentu môžeme zaradiť napríklad odhalenie a vyšetrovanie akejkoľvek formy kybernetických bezpečnostných incidentov proti EÚ a jej členským štátom a primerane na ne reagovať. Taktiež aj vypracovanie účinných mechanizmov na podporovanie kybernetickej bezpečnosti na globálnej scéne a stíhanie páchateľov kybernetických incidentov. Zároveň aj zabezpečiť aby EÚ, členské štáty, organizácie či jednotlivci prijali opatrenia na zvýšenie kybernetickej bezpečnosti a uplatňovali ju na prioritnej úrovni. Práve tieto kroky vybudujú odolnosť a zabezpečenie lepšej reakcie EÚ na kybernetické útoky v súčasnosti, ale aj do budúcnosti.

[5] Hlavnými cieľmi je spolupráca na troch úrovniach a to na politickej, operačnej a technickej, pričom na každej z nich spolupráca zahŕňa výmenu informácií, spoločné kroky v spojitosti zo základnými cieľmi a to umožniť účinnú reakciu, šíriť spoločné situačné podvedomie a dohodnúť sa na kľúčových informáciách pre verejnosť. (Odporúčanie Komisie (EÚ) 2017/1584 z 13. septembra 2017 o koordinovanej reakcii na kybernetické incidenty a krízy veľkého rozsahu, s. 42).

[6] Smernica vymedzuje minimálne pravidlá, ktoré sa týkajú vymedzenia trestných činov a sankcií v oblasti podvodov s bezhotovostnými platobnými prostriedkami a ich falšovania a pozmeňovania. Uľahčuje sa ňou prevencia týchto trestných činov a poskytovanie pomoci obetiam a ich podpora. (Smernica Európskeho parlamentu a Rady (EÚ) 2019/713 zo 17. apríla 2019 o boji proti podvodom s bezhotovostnými platobnými prostriedkami a proti ich falšovaniu a pozmeňovaniu, ktorou sa nahrádza rámcové rozhodnutie Rady 2001/413/SVV, článok 1, hlava I.).

[7] Ciele tejto smernice sú aproximácia trestného práva členských štátov v oblasti útokov na informačné systémy, ako aj zlepšenie spolupráce medzi príslušnými orgánmi. Dosiahne sa to ustanovením minimálnych pravidiel týkajúcich sa vymedzenia trestných činov a príslušných sankcií v oblasti útokov na informačné systémy ako aj požiadavkou funkčných kontaktných miest, ktoré sú k dispozícii dvadsaťštyri hodín denne a sedem dní v týždni. (Správa Komisie Európskeho parlamentu a Rade o posúdení rozsahu, v akom členské štáty prijali opatrenia, ktoré sú nevyhnutné na dosiahnutie súladu so smernicou 2013/40/EÚ o útokoch na informačné systémy, ktorou sa nahrádza rámcové rozhodnutie Rady 2005/222/SVV).

[8] SK-CERT. *Kybernetický legislatívny balíček EÚ.* [online].[2022-12-08]. Dostupné na internete: https://www.sk-cert.sk/sk/kyberneticky-legislativny-balicek-eu/index.html.

hodnoverných a osvedčených služieb a digitálnych nástrojov všetkými občanmi a firmami. Následne v októbri 2022 pod vplyvom nových a čoraz sofistikovanejších kybernetických útokov na verejnú správu Rada prijala pozíciu k návrhu nariadenia, ktoré stanovuje opatrenia na zaistenie vysokej spoločnej úrovne kybernetickej bezpečnosti v inštitúciách, orgánoch, úradoch a agentúrach Únie, z dôvodu, že kybernetická bezpečnosť má podstatný význam pre činnosť verejnej správy a inštitúcií na vnútroštátnej, ako aj európskej úrovni. Kybernetická bezpečnosť v nepodstatnom rade predstavuje aj významnú hodnotu pre spoločnosť a hospodárstvo. Predmetný návrh bol súčasťou Stratégie kybernetickej bezpečnosti EÚ v digitálnej dekáde.[9]

Ďalším nástrojom bola nová Stratégia bezpečnosti únie na ochranu všetkých občanov v EÚ a na podporu európskeho spôsobu života, ktorú vypracovala Európska komisia na obdobie rokov 2020 - 2025 (ďalej len „Stratégia“). Stratégia je postavená na štyroch základných pilieroch. Prvým pilierom je bezpečnostné prostredie, ktoré obstojí v budúcnosti. Druhým pilierom je boj proti vyvíjajúcim sa hrozbám. Tretím pilierom je ochrana občanov Európy pred terorizmom a organizovanou trestnou činnosťou a štvrtým pilierom je silný európsky bezpečnostný ekosystém.

Na základe témy predkladaného článku sme vymedzili dielčie kapitoly iba prvého piliera Stratégie, ktoré sú tri. Prvá dielčia kapitola sa zameriava na ochranu kritickej infraštruktúry a jej odolnosť. Druhá dielčia kapitola upravuje kybernetickú bezpečnosť a tretia dielčia kapitola sa orientuje na ochranu verejných priestorov.

K predmetným kapitolám boli vypracované aj kľúčové opatrenia a špeciálne ku kybernetickej bezpečnosti sa viažu nasledujúce:

- revízia smernice o bezpečnosti sietí a informácií,
- ochrana a kybernetická bezpečnosť kritickej energetickej infraštruktúry a kódex,
- Európska stratégia kybernetickej bezpečnosti,
- ďalšie kroky smerujúce k vytvoreniu spoločnej kybernetickej jednotky,
- Spoločné pravidlá pre všetky orgány, inštitúcie a iné subjekty EÚ týkajúce sa bezpečností informácií a kybernetickej bezpečnosti a pod.

Na kybernetickú bezpečnosť sa kladie výrazný dôraz, čo môžeme vidieť aj v Správe o stave Únie 2022 v časti Nové kľúčové iniciatívy na rok 2023, v ktorej sa vyskytuje jeden z bodov podpory európskeho spôsobu života aj iniciatíva týkajúca sa Akadémie zručností v oblasti kybernetickej bezpečnosti.

Kybernetická bezpečnosť a jej skúmanie v Slovenskej republike vo podnikateľskom sektore

V súčasnosti kybernetický priestor je miestom, ktoré je denne využívané od začiatku dňa až po jeho koniec či už za účelom plnenia si pracovných povinností, alebo v privátnej sfére. Môžeme povedať, že zasahuje do každej ľudskej činnosti viac či menej a osoby do neho vstupujú vo veľkej miere dobrovoľne. Kladieme si otázku, či ale tieto osoby poznajú aj aktuálne hrozby a riziká kybernetického priestoru, keď mu často tak neopatrne dokážu poskytnúť a obetovať svoje súkromné informácie? Ak by ich na ulici oslovil neznámy človek a opýtal sa ich na číslo kreditnej karty a k nej PIN kód povedali by mu to? Ale keď ho s touto istou požiadavkou vyzve „niekto“ z kybernetického priestoru niekedy nad tým ani dlho neuvažuje a poskytne mu túto informáciu. Pričom v posledných obdobiach rokoch stúpa frekvencia takýchto útokov a zároveň sa zvyšuje aj sofistikovanosť páchateľov. Z tohto dôvodu je potrebné kybernetický priestor vnímať a považovať za ekvivalent reálneho sveta, spolu s uplatňovaním určitých jasne zvolených pravidiel a to nielen pre organizácie, ale aj pre každého jedinca osobitne.

[9] RADA EURÓPSKEJ ÚNIE. *Kybernetická bezpečnosť: ako EÚ bojuje proti kybernetickým hrozbám*. [online].[2022-12-08]. Dostupné na internete: https://www.consilium.europa.eu/sk/policies/cybersecurity/.

Na základe týchto skutočností je potrebné vedieť o kybernetických hrozbách, ktoré sa vyskytujú v spoločnosti a adekvátne im predchádzať, keďže iba reakcia na ne by bola neskorá a neopatrná. Kybernetický priestor sa už nikdy neuzavrie a neprestane existovať, ale práve naopak bude expandovať aj do ďalších, aktuálne, neprebádaných oblastí a uplatňovať si v nich svoj nezastupiteľný vplyv. Organizácie a jednotlivci musia byť pripravení vedieť reagovať na vzniknuté situácie a aktívne zabraňovať takýmto činnostiam, aby sa nestali obeťami kybernetických útokov.

S opakovanými kybernetickými útokmi sa denne stretávajú jednotlivci a aj organizácie[10] aj napriek určitej miere ochrany, ktorú prijali na tej ktorej úrovni. Vo svetle aktuálnych udalostí, ktoré ohrozujú spoločnosť sa ukázal aj podnikateľský sektor a verejný sektor ako vhodný cieľ pre páchateľov kybernetických útokov, najmä z dôvodu disponovania veľkým objemom údajov a dát spojených s rôznorodosťou nielen ich obsahu, ale aj ich viacúrovňovým tokom informácií medzi partnermi a dodávateľmi. Z tohto dôvodu sme sa zamerali iba na príležitosti zvyšovania znalostí a vedomostí v oblasti kybernetickej bezpečnosti, aby bolo možné včasne predchádzať kybernetickým útokom.

V Slovenskej republike tvoria malé a stredné podniky rozhodujúci pilier celkového štátneho hospodárstva a práve preto sú možným významným cieľom kybernetických útokov. Napriek tejto skutočnosti kybernetická bezpečnosť nie je prioritnou oblasťou v malých a stredných podnikoch v Slovenskej republike, ako to ukázal aj prieskum Slovak Business Agency, vykonaný v spolupráci s Národným bezpečnostným úradom a agentúrou Actly s.r.o. Prieskum bol realizovaný v mesiaci máj 2022 a to formou telefonických rozhovorov CATI na vzorke 1 099 malých a stredných podnikov pôsobiacich v Slovenskej republike. Následne sme vybrali iba tri otázky z predmetného prieskumu, ktoré sa z obsahového zamerania týkajú predkladaného príspevku.

Prvá otázka prieskumu skúmala znalosti a skúsenosti pracovníkov kybernetickej bezpečnosti, ktoré sú považované za najviac nedostatkové. Výsledky prieskumu ukázali, že „*51,8 % malých a stredných podnikov nemajú pracovníkov kybernetickej bezpečnosti. Druhú najčastejšiu odpoveď - všeobecná znalosť problematiky kybernetickej bezpečnosti, označilo 17,1 % respondentov. Ďalšia odpoveď, ktorá presahovala hodnotu 10,6 % bola technické znalosti. Ostatné odpovede nepresiahli hodnotu 10% a boli to flexibilita a konštitučné prístupy k riešeniu problémov (9,7 %), analytické schopnosti (7,4 %), komunikačné schopnosti (7,4 %), znalosť cudzieho jazyka (7,4 %), znalosti vnútorného fungovania firmy (6,5 %), manažérske schopnosti (6,5 %), iné (5,9 %) a neviem (8,8 %).*“[11]

Druhá otázka sa zameriavala na to, či malé a stredné podniky poskytujú svojim zamestnancom možnosti zvyšovania ich znalostí a schopností v oblasti kybernetickej

[10] K aktuálnym hrozbám môžeme zaradiť napríklad Bezpečnostné varovanie V20221228-03, ktoré sa označovalo ako kritická dôležitosť a CVSS (Common Vulnerability Scoring System - používa sa na hodnotenie závažnosti bezpečnostných zraniteľností počítačových systémov. Skóre sa pohybuje v rozpätí od 0 do 10, pričom hodnota 10 je najzávažnejšia.) bolo 9,8. Popis hrozby - vývojári frameworku Apache Karaf vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje kritickú bezpečnostnú zraniteľnosť. Kritická bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému. Zasiahnuté systémy - Apache Karaf vo verzii staršej ako 4.4.2, 4.3.8. Následky - vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému. Dátum prvého zverejnenia varovania bol 21.12.2022 (SK-CERT, *SK-CERT. Bezpečnostné varovanie V20221228-03*, [online].[2022-12-08]. Dostupné na internete: https://www.sk-cert.sk/threat/sk-cert-bezpecnostne-varovanie-v20221228-03/index.html).

[11] SLOVAK BUSINESS AGENCY. *Prieskum stavu kybernetickej bezpečnosti v sektore MSP: Správa z kvantitatívneho prieskumu 2022*, s. 18. [online].[2022-12-08]. Dostupné na internete: https://monitoringmsp.sk/wp-content/uploads/2022/08/Prieskum-stavu-kybernetickej-bezpe%C4%8Dnosti-v-sektore-MSP-sprava-z-prieskumu.pdfhttps://monitoringmsp.sk/wp-content/uploads/2022/08/Prieskum-stavu-kybernetickej-bezpe%C4%8Dnosti-v-sektore-MSP-sprava-z-p.

bezpečnosti. Na základe výsledkov prieskumu môžeme konštatovať, že „*32,4 % malých a stredných podnikov sa zaoberá kybernetickou bezpečnosťou, ale neposkytuje zamestnancom možnosti zvyšovania znalostí v oblasti kybernetickej bezpečnosti. Následne 30 % malých a stredných podnikov poskytuje zamestnancom možnosti zvyšovania znalostí a zručností v tejto oblasti na dobrovoľnej báze a najnižší počet malých a stredných podnikov (14,1 %) poskytuje tieto možnosti svojim zamestnancom povinne. Následne 20,9 % respondentov odpovedalo, že nemá zamestnancov a 2,6 % respondentov neodpovedalo. V porovnaní malých a stredných podnikov, tak 47,9 % malých podnikov neposkytuje možnosti zvyšovania znalostí a zručností zamestnancom v kybernetickej bezpečnosti a 33,9 % stredných podnikov poskytuje možnosti dobrovoľného zvyšovania znalostí a zručností v tejto oblasti. Povinné zvyšovanie znalostí vyžaduje 32,3 % stredných podnikov*.“ [12]

Prieskumom bola skúmaná aj tretia otázka a to aké podporné opatrenia zamerané na zlepšenie kybernetickej bezpečnosti by malé a stredné firmy uvítali. Najčastejšie bola označená odpoveď „*poskytovanie grantov, poukazov (vouchrou) na nákup technológií (hardvér a softvér) a na zabezpečenie školení a vzdelávacích kurzov (37,4 %). Následne 34,6 % malých a stredných firiem by uvítala informačné služby, 32,1 % by prijali špecifické poradenstvo, mentoring a školenia a 18,7 % malých a stredných firiem uviedlo, že podporné opatrenia v tejto oblasti nie sú potrebné. Následne 11,9 % označilo možnosť neviem a 2,4 % uviedlo, že preferujú iný typ podpory*.“ [13]

Na základe výsledkov z prieskumu malé a stredné firmy vedia, že „*najvýznamnejším faktorom na zvyšovanie kybernetickej úrovne bezpečnosti je uvedomenie si rizík, ale takmer tretina z nich neposkytuje možnosti zvyšovania znalostí v oblasti kybernetickej bezpečnosti a väčšina nemá ani vypracovanú analýzu rizík. Následne by malé a stredné firmy najviac privítali na zlepšenie kybernetickej bezpečnosti opatrenia, vo forme grantov, poukazov na nákup technológií a na zabezpečenie školení a vzdelávacích kurzov*.“ [14]

Z nášho pohľadu práve poslednú možnosť hodnotíme ako veľmi pozitívnu z hľadiska toho, že malé a stredné podniky by mali úmysel podporovať vzdelávanie svojich zamestnancov v tejto oblasti, avšak bez vynaloženia vlastných finančných prostriedkov, čo vnímané ako negatívum.

Kybernetická bezpečnosť a jej skúmanie v Slovenskej republike na základe výskumu verejnej mienky

Kybernetická bezpečnosť vo výraznej miere ovplyvňuje aj jednotlivcov a širokú verejnosť a z tohto predpokladu vychádzal aj výskum verejnej mienky, ktorý si kládol za úlohu „*čo možno najpresnejšie vyhodnotiť aktuálny stav kybernetickej bezpečnosti v Slovenskej republike a zahrnúť do premenných aj spoločenskú dimenziu, kde ústredným prvkom sú občania v domácnosti.“* Výskum verejnej mienky realizovalo Kompetenčné a certifikačné centrum kybernetickej bezpečnosti v spolupráci Národným bezpečnostným úradom a

[12] SLOVAK BUSINESS AGENCY. *Prieskum stavu kybernetickej bezpečnosti v sektore MSP: Správa z kvantitatívneho prieskumu 2022*, s. 21. [online].[2022-12-08]. Dostupné na internete: https://monitoringmsp.sk/wp-content/uploads/2022/08/Prieskum-stavu-kybernetickej-bezpe%C4%8Dnosti-v-sektore-MSP-sprava-z-prieskumu.pdfhttps://monitoringmsp.sk/wp-content/uploads/2022/08/Prieskum-stavu-kybernetickej-bezpe%C4%8Dnosti-v-sektore-MSP-sprava-z-p.

[13] SLOVAK BUSINESS AGENCY. *Prieskum stavu kybernetickej bezpečnosti v sektore MSP: Správa z kvantitatívneho prieskumu 2022*, s. 50. [online].[2022-12-08]. Dostupné na internete: https://monitoringmsp.sk/wp-content/uploads/2022/08/Prieskum-stavu-kybernetickej-bezpe%C4%8Dnosti-v-sektore-MSP-sprava-z-prieskumu.pdfhttps://monitoringmsp.sk/wp-content/uploads/2022/08/Prieskum-stavu-kybernetickej-bezpe%C4%8Dnosti-v-sektore-MSP-sprava-z-p.

[14] SLOVAK BUSINESS AGENCY. *Prieskum stavu kybernetickej bezpečnosti v sektore MSP: Správa z kvantitatívneho prieskumu 2022*, s. 52 - 53. [online].[2022-12-11]. Dostupné na internete:

s agentúrou AKO.sk.“ [15] Následne sme si vybrali výskumnú oblasť zameranú na kybernetickú bezpečnosť s poukázaním na tri otázky daného výskumu.

Prvou otázkou výskumníci zisťovali či sa respondenti zaujímajú a vyhľadávajú informácie o kybernetickej bezpečnosti z vlastnej iniciatívy, alebo nie. „*Respondenti vo výraznej miere odpovedali nie (62,7 %), ktorú zohľadnením pohlavia označilo väčšie množstvo žien (73 %) ako mužov (53 %). S prihliadnutím k ďalšiemu skúmanému sociodemografickému znaku - veku, najčastejšie zaznačili danú odpoveď respondenti vo veku od 34 rokov do 49 rokov (65 %), vo veku od 50 rokov do 65 rokov (64 %) a vo veku od 66 rokov a viac rokov (63 %).*“[16]

Druhú otázku výskumníci zamerali na to, z akých zdrojov respondenti získavajú poznatky o kybernetickej bezpečnosti. Prevažná časť respondentov zaznačila možnosť - „*Internet (elektronické média, sociálne siete, četovacie služby) a to konkrétne spolu 80,6 % výskumného súboru. Daná odpoveď dominovala pri oboch pohlaviach, ale vo väčšej miere u mužov (84 %) než u žien (74 %). Zohľadnením veku najčastejšie predmetnú odpoveď uviedla veková kategória od 66 rokov a viac rokov a to 90 % respondentov. Ďalšiu pomerne frekventovanú odpoveď - známi a priatelia, označilo 31,7 % respondentov. Pri tejto odpovedi prevládali ženy (35 %) viac ako muži (30 %) a zohľadnením pohlavia najčastejšie danú možnosť označili respondenti vo veku od 50 rokov do 65 rokov (39 %). Nasledovala odpoveď odborná literatúra, ktorú označilo 31,3 % respondentov. S prihliadnutím na sociodemografický znak - pohlavie, predmetnú odpoveď vo väčšej časti uviedli muži (37 %) ako ženy (19 %) a respondenti vo veku od 18 rokov do 33 rokov (33 %).*“[17]

Tretiu otázku výskumníci orientovali na zhodnotenie akými znalosťami a zručnosťami disponujú respondenti v oblasti kybernetickej bezpečnosti. Na základe odpovedí respondentov, môžeme povedať, že najčastejšie bola označená odpoveď - „*priemerné znalosti a zručnosti[18], ktorú spolu uviedlo 45,1 % respondentov. Zohľadnením pohlavia danú možnosť označilo väčšie množstvo mužov - respondentov (52 %) ako žien - respondentiek (38 %) a zohľadnením veku ju najčastejšie označili respondenti vo veku od 18 rokov do 33 rokov (48 %), ako aj respondenti vo vekovej kategórii od 50 rokov do 65 rokov (47 %). Následne 33,4 % respondentov uviedlo možnosť - nízke znalosti a zručnosti[19], ktorú uviedlo väčšie množstvo žien (41 %) ako mužov (25 %) a najčastejšie ju zaznačili respondenti vo veku od 66 rokov a viac (39 %). Najnižšie množstvo respondentov označilo odpoveď - vysoké znalosti a zručnosti[20], ktorú spolu uviedlo 8,8 % respondentov. Predmetnú možnosť označilo vyššie percento mužov (15 %) ako žien (3 %) a z hľadiska veku ju uviedli najčastejšie respondenti vo veku od 18 rokov do 33 rokov (15 %).*“[21]

---

[15] AKO s.r.o., NÁRODNÝ BEZPEČNOSTNÝ ÚRAD, KOMPETENČNÉ A CERTIFIKAČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI. *Kybernetická bezpečnosť*, s. 48. [online].[2022-12-11]. Dostupné na internete: https://cybersecuritymonth.eu/countries/slovakia/kyberneticka-bezpecnost-prieskum-verejnej-mienky.

[16] AKO s.r.o., NÁRODNÝ BEZPEČNOSTNÝ ÚRAD, KOMPETENČNÉ A CERTIFIKAČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI. *Kybernetická bezpečnosť*, s. 38. [online].[2022-12-11]. Dostupné na internete: https://cybersecuritymonth.eu/countries/slovakia/kyberneticka-bezpecnost-prieskum-verejnej-mienky.

[17] AKO s.r.o., NÁRODNÝ BEZPEČNOSTNÝ ÚRAD, KOMPETENČNÉ A CERTIFIKAČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI. *Kybernetická bezpečnosť*, s. 42 - 43. [online].[2022-12-11]. Dostupné na internete: https://cybersecuritymonth.eu/countries/slovakia/kyberneticka-bezpecnost-prieskum-verejnej-mienky.

[18] t.j. ovládam základy kybernetickej bezpečnosti a viem o rizikách, ktoré prináša.

[19] t.j. viem, že existuje nejaká kybernetická bezpečnosť, ale bližšie sa o ňu nezaujímam.

[20] t.j. som skúsený používateľ a aplikujem princípy kybernetickej bezpečnosti vo svojom osobnom aj pracovnom živote.

[21] AKO s.r.o., NÁRODNÝ BEZPEČNOSTNÝ ÚRAD, KOMPETENČNÉ A CERTIFIKAČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI. *Kybernetická bezpečnosť*, s. 48. [online].[2022-12-11]. Dostupné na internete: https://cybersecuritymonth.eu/countries/slovakia/kyberneticka-bezpecnost-prieskum-verejnej-mienky.

Na základe vyhodnotenia daných otázok môžeme konštatovať, že „*len takmer 1/3 respondentov sa zaujíma a vyhľadáva informácie o kybernetickej bezpečnosti a častejšie kladne odpovedali muži než ženy. Zohľadnením veku súhlasnú odpoveď uviedli častejšie najmladší respondenti než starší respondenti. Následne za najvhodnejší zdroj poznatkov o kybernetickej bezpečnosti považovali respondenti Internet a to najmä muži. Respondenti mali zhodnotiť aj vlastné znalosti a skúsenosti z oblasti kybernetickej bezpečnosti a najčastejšie uviedli priemerné znalosti a zručnosti v tejto oblasti, pričom ale väčšie množstvo mužov zaznačilo predmetnú odpoveď*.“[22]

Predmetný výskum hodnotíme veľmi pozitívne a to nielen z hľadiska aktuálnosti daných informácií v tejto oblasti, ale aj z dôvodu komplexnejšieho pohľadu na jednotlivca a jeho správanie sa v kybernetickom priestore v Slovenskej republike.

Situačné povedomie a kybernetická prevencia vo vzťahu ku kybernetickej bezpečnosti

Na základe uvedeného je neustále potrebné dbať a klásť dôraz na kontrolu kybernetických incidentov, ktoré sa objavujú bez ohľadu na ich závažnosť, pretože aj na prvý pohľad malý incident môže prerásť do výraznejšieho problému, keď sa do neho „zapojí“ väčšie množstvo napadnutých subjektov.

Prioritným cieľom je vedieť reagovať na vzniknutý incident v každom prostredí, čo práve zabezpečuje aj dostatočná miera kybernetickej bezpečnosti. Aj v tejto oblasti platí , že „*úspech je priamo závislý od toho, do akej miery sú vybrané orgány schopné rýchlo a včas páchané a spáchané incidenty identifikovať a vytvoriť predpoklady na zabezpečenie neodvratnosti možného trestného postihu a v neposlednom rade poskytnutie ochrany a pomoc ich obetiam*.“[23]

Podľa nášho názoru je efektívnejšie vedieť predchádzať kybernetickým útokom a to aj prostredníctvom určitej miery predvídania. Dané možnosti poskytuje jednak situačné povedomie ako aj kybernetická prevencia.

Situačné povedomie „*v sebe zahŕňa vnímanie a pochopenie aktuálneho stavu kybernetickej bezpečnosti organizácie a predpoveď možných zmien*“.[24] Efektívne povedomie o kybernetickej situácií v organizácii si vyžaduje dva základné komponenty a to ľudí a technológie. Niektorí autori uvádzajú v tomto prípade na prvom mieste technológie z dôvodu, že predstavujú nástroje kybernetickej bezpečnosti a automatizačný softvér umožňuje organizáciám zhromažďovať, analyzovať a reagovať na údaje o možných hrozbách. Avšak ľudia sú kľúčový najmä z toho hľadiska, že práve oni používajú nástroje a interpretujú údaje a robia konečné rozhodnutia na posilnenie kybernetickej obrany.

Situačné povedomie umožňuje organizáciám pochopiť súčasné riziká a predvídať budúce. Na základe týchto faktorov potom môže organizácia navrhnúť alebo identifikovať požadované riešenia na posilnenie ich postavenia v oblasti kybernetickej bezpečnosti a celkovo aj zlepšenie programu riadenia rizík.[25]

---

[22] AKO s.r.o., NÁRODNÝ BEZPEČNOSTNÝ ÚRAD, KOMPETENČNÉ A CERTIFIKAČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI. *Kybernetická bezpečnosť*, s. 72-73. [online].[2022-12-11]. Dostupné na internete: https://cybersecuritymonth.eu/countries/slovakia/kyberneticka-bezpecnost-prieskum-verejnej-mienky.

[23] FEDÁKOVÁ, P.- LISOŇ, M. *Východiskové štádium odhaľovania a objasňovania domáceho násilia páchaného na ženách*, Bratislava: Akadémia Policajného zboru v Bratislave, 2022, s. 51.

[24] ANDRAŠKO, J.- MESARČÍK, M. - SOKOL, P. *Právo kybernetickej bezpečnosti*, Bratislava: Univerzita Komenského v Bratislave, 2022, s. 162.

[25] FRANKE, U.-BRYNIELSSON, J. *Cyber situational awareness e A systematic review of the literature.* online].[2022-12-11]. Dostupné na internete: https://www.foi.se/download/18.7fd35d7f166c56ebe0bfffc/1542623724812/Cyber-situational-awareness_FOI-S-4736-SE.pdf.

Kybernetická prevencia sa zameriava na odhaľovanie a predchádzanie kybernetických útokov, reagovanie na ne a zaistenie vhodnej nápravy. Prevencia v tejto oblasti sa dotýka nielen nápravy, ale najmä predchádzaniu vzniku škody či poškodenia chráneného záujmu. Z tohto pohľadu je potrebné reagovať včas a to napríklad aj prostredníctvom vzdelávania od detstva až do dospelosti, pričom je potrebné pokračovať v ňom aj naďalej.

Medzi tieto nástroje pôsobiace na širokú verejnosť môžeme zaradiť napríklad zvyšovanie povedomia o kybernetickej bezpečnosti.

Celkovo povedomie o kybernetickej bezpečnosti môžeme charakterizovať, ako poznanie potreby ochrany informácie a informačných a komunikačných technológií, ako aj povinností osobne sa ich na ochrane podieľať. Taktiež to zahŕňa aj uvedomenie si najnovších bezpečnostných hrozieb, osvedčených prístupov kybernetickej bezpečnosti, nebezpečenstva kliknutia na škodlivý odkaz alebo sťahovanie infikovanej prílohy, interakcie v online priestore, či zverejňovanie citlivých informácií. Na predchádzanie takýmto druhom správania sa realizujú viaceré školiace programy, ktoré sú zamerané na zvyšovanie povedomia o kybernetickej bezpečnosti. Dané programy pomáhajú priamo ako aj nepriamo zlepšiť stav zabezpečenia jednotlivca, ako aj organizácie pre ktorú pracuje. Dôležitosť je kladená na kontinuitu vzdelávania a efektívnosť. Práve podporenie rozvíjania povedomia o kybernetickej bezpečnosti nezabezpečí v plnej miere odstránenie rizika vzniku kybernetických incidentov, ale do istej miery ho môže eliminovať.[26]

V Slovenskej republike na základných a stredných školách je vzdelávanie v informačnej a kybernetickej bezpečnosti značne obmedzené a „*nie je strategicky uchopené, čo je vidieť aj v neexistujúcej jednotnej koncepcii vzdelávania v tejto oblasti, ako aj pri jednotlivých predmetoch, či neexistujúcej dostatočnej, resp. adekvátnej dotácii času a vedomostí na žiakov a využívania dostatočných pomôcok pri výučbe.*“[27] Z daného vyplýva, že iba veľmi malá časť základných a stredných škôl pripravuje žiakov a študentov na prácu s informáciami a poskytuje im znalosti v oblasti kybernetickej bezpečnosti.

Ďalším nástrojom pôsobiacim efektívne na širokú verejnosť je aj realizovanie preventívnych kampaní v tejto oblasti. V rámci Európskej únie pôsobí Agentúra Európskej únie pre kybernetickú bezpečnosť ENISA (ďalej len „ENISA“). ENISA podporuje a vedie kampane na zvyšovanie povedomia o kybernetickej bezpečnosti s cieľom propagovať osvedčené postupy a propagovať príklady dobrej praxe v oblasti kybernetickej bezpečnosti. ENISA spolupracuje pri preventívnych projektoch s viacerými stranami z verejného a súkromného sektora, za účelom dosiahnutia čo najväčšieho dosahu na členov spoločnosti.

ENISA prispieva do praxe aj prostredníctvom viacerých realizovaných výskumov a to v prvom kroku analyzuje získané údaje z výskumu a v druhom kroku navrhuje prístupy k zlepšeniu daného stavu do budúcnosti. Napríklad v roku 2021 ENISA realizovala výskum zameraný na riešenie nedostatku zručností a medzery vo vysokoškolskom vzdelávaní. [28]

ENISA každoročne realizuje preventívny projekt zameraný na zvyšovanie informovanosti o rizikách kybernetickej bezpečnosti v celej EÚ. Pilotný projekt bol spustený v roku 2012 pre občanov, organizácie a firmy v rámci Európskeho mesiaca kybernetickej bezpečnosti. Od tohto obdobia sú rámci Európskeho mesiaca kybernetickej bezpečnosti v októbri každoročne realizované viaceré preventívne aktivity členských štátov EÚ, ktoré sú

[26] CyberGuard Technologies. *The Importance of Cyber Security Awareness*. [online].[2022-12-11]. Dostupné na internete: https://www.ogl.co.uk/the-importance-of-cyber-security-awareness.

[27] NÁRODNÝ BEZPEČNOSTNÝ ÚRAD. *Správa o kybernetickej bezpečnosti v Slovenskej republike v roku 2021*, s. 70 - 71. [online].[2022-12-11]. Dostupné na internete: https://www.nbu.gov.sk/wp-content/uploads/urad/Vyrocne_spravy/Sprava-o-KB-SR-2021.pdf.

[28] ENISA. *About Enisa - The European Union Agency for Cybersecurity*. [online].[2022-12-11]. Dostupné na internete: https://www.enisa.europa.eu/about-enisa/about-enisa-the-european-union-agency-for-cybersecurity.

zacielené na zníženie kybernetických incidentov. V roku 2021 Slovenská republika počas tejto kampane ponúkala bezplatný kurz, ktorý bol zameraný na vzdelávanie o kybernetickej bezpečnosti. Počas tohto kurzu užívatelia získali vedomosti a zručnosti na udržanie bezpečnosti v kyberpriestore na svojom pracovisku.[29]

Nasledujúcim projektom je poukázanie na príklady dobrej praxe, ktoré spočíva vo výmene najlepších postupov medzi členskými štátmi v oblasti informovanosti a vzdelávania v kybernetickej bezpečnosti za každý rok. V rámci daných preventívnych aktivít sa v roku 2022 Slovenská republika zapojila prostredníctvom Národnej stratégie kybernetickej bezpečnosti 2021-2025 pri realizovaní školení s cieľom poskytnúť základné bezpečnostné vzdelanie pre všetky stupne vzdelávania na základných školách. [30]

Ďalšou možnosťou kybernetickej prevencie zacielenej na špecifické skupiny adresátov by mohlo byť aj e-lerningové vzdelávanie pre zamestnancov každej organizácie. Dané vzdelávanie by sa mohlo prebiehať vo forme školení, aby zamestnanci boli upozorňovaní a informovaní o možných hrozbách s prispôsobením sa na danú oblasť, v ktorej pracujú. Následne by školenie nebolo iba teoreticky zamerané, ale aj s reálnymi simuláciami v kybernetickom priestore, v ktorom si zamestnanci vedia vyskúšať akým spôsobom by reagovali a aké zručnosti si musia ešte osvojiť do praxe.

Na základe vymedzenia vzťahu situačného povedomia a kybernetickej prevencie ku kybernetickej bezpečnosti môžeme povedať, že v súčasnosti nenastáva kontinuita vzdelávania, čím osoby sa môžu vzdelávať v tejto oblasti dobrovoľne a iba málokedy je dané vzdelávanie povinné. Podľa nášho názoru je potrebné zlepšiť vzdelávanie v oblasti kybernetickej bezpečnosti nielen na základných a stredných školách, ale aj v súkromnom a verejnom sektore za účelom predchádzania vzniku kybernetických incidentov.

Záver

Potreba skúmania kybernetickej bezpečnosti v spoločnosti má podľa nášho názoru nezastupiteľné miesto nielen pre odbornú verejnosť, aby videla ďalšie možnosti rozvoja a prepojenia teoretických poznatkov s praktickými skúsenosťami, ale taktiež aj pre laickú verejnosť, aby im poskytla informácie o hrozbách a rizikách pôsobiace na nich či už priamo alebo nepriamo.

Na základe aktuálneho prieskumu a výskumu máme prehľad o tom, akým spôsobom sa o kybernetickú bezpečnosť zaujímajú organizácie a jednotlivci v Slovenskej republike a následne je podľa nášho názoru na mieste zamerať sa na oblasť zvyšovania vzdelávania v predmetnej oblasti, v ktorej existujú viaceré nástroje určené pre odlišné skupiny adresátov.

K daným nástrojom môžeme zaradiť či už zvyšovanie bezpečnostného povedomia, ktoré sa realizuje vo forme vzdelávacích činností rôzneho druhu za účelom či už vytvorenia alebo zdokonalenia určitých znalostí a vedomostí súvisiacich s kybernetickou bezpečnosťou pre všetky kategórie osôb a to aj vrátene každého zamestnanca. Alebo aj vzdelávanie vedeckých pracovníkov a špecialistov v oblasti informačnej bezpečnosti, ktorí poznajú svoje kvalifikačné nedostatky a vedia veľmi podrobne určiť svoje vzdelávacie potreby v danej problematike.

Zoznam použitej literatúry:

AKO s.r.o., NÁRODNÝ BEZPEČNOSTNÝ ÚRAD, KOMPETENČNÉ A CERTIFIKAČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI. *Kybernetická bezpečnosť*. [online].[2022-

[29] ENISA. *European cybersecurity moth (ECSM) 2021*, s. 22. [online].[2022-12-11]. Dostupné na internete: https://www.enisa.europa.eu/publications/european-cybersecurity-month-2021-deployment-report?v2=1.

[30] ENISA. *Cybersecurity Education Initiatives in the EU Member States*, s. 17. [online].[2022-12-11]. Dostupné na internete: https://www.enisa.europa.eu/publications/cybersecurity-education-initiatives-in-the-eu-member-states?v2=1.

12-11]. Dostupné na internete: https://cybersecuritymonth.eu/countries/slovakia/kyberneticka-bezpecnost-prieskum-verejnej-mienky
ANDRAŠKO, J.- MESARČÍK, M. - SOKOL, P. *Právo kybernetickej bezpečnosti*, Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2022, 186 s. ISBN 978-80-7160-632-1
CyberGuard Technologies. *The Importance of Cyber Security Awareness*. [online].[2022-12-11]. Dostupné na internete: https://www.ogl.co.uk/the-importance-of-cyber-security-awareness
ENISA. *About Enisa - The European Union Agency for Cybersecurity*. [online].[2022-12-11]. Dostupné na internete: https://www.enisa.europa.eu/about-enisa/about-enisa-the-european-union-agency-for-cybersecurity
ENISA. *Cybersecurity Education Initiatives in the EU Member States*. [online].[2022-12-11]. Dostupné na internete: https://www.enisa.europa.eu/publications/cybersecurity-education-initiatives-in-the-eu-member-states?v2=1
ENISA. *European cybersecurity moth (ECSM) 2021*, s. 22. [online].[2022-12-11]. Dostupné na internete: https://www.enisa.europa.eu/publications/european-cybersecurity-month-2021-deployment-report?v2=1
FEDÁKOVÁ, P.- LISOŇ, M. *Východiskové štádium odhaľovania a objasňovania domáceho násilia páchaného na ženách*, Bratislava: Akadémia Policajného zboru v Bratislave, 2022, 243 s. ISBN 978-80-8054-944-2
Zákon č. 69/2018 Z.z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov
FRANKE, U.-BRYNIELSSON, J. *Cyber situational awareness e A systematic review of the literature.* online].[2022-12-11]. Dostupné na internete: https://www.foi.se/download/18.7fd35d7f166c56ebe0bfffc/1542623724812/Cyber-situational-awareness_FOI-S-4736-SE.pdf
NÁRODNÝ BEZPEČNOSTNÝ ÚRAD. *Národná stratégia kybernetickej bezpečnosti na roky 2021 až 2025*. [online].[2022-12-08]. Dostupné na internete: https://www.nbu.gov.sk/wp-content/uploads/kyberneticka-bezpecnost/Narodna-strategia-kybernetickej-bezpecnosti.pdf
NÁRODNÝ BEZPEČNOSTNÝ ÚRAD. *Správa o kybernetickej bezpečnosti v Slovenskej republike v roku 2021*. [online].[2022-12-11]. Dostupné na internete: https://www.nbu.gov.sk/wp-content/uploads/urad/Vyrocne_spravy/Sprava-o-KB-SR-2021.pdf
Návrh Smernice Európskeho parlamentu a Rady o opatreniach na zabezpečenie vysokej spoločenskej úrovne kybernetickej bezpečnosti v Únii a o zrušení smernice (EÚ) 2016/1148
Odporúčanie Komisie (EÚ) 2017/1584 z 13. septembra 2017 o koordinovanej reakcii na kybernetické incidenty a krízy veľkého rozsahu
Spoločné oznámenie Európskeho parlamentu a Rady „Odolnosť, odrádzanie a obrana: budovanie silnej kybernetickej bezpečnosti pre EÚ
RADA EURÓPSKEJ ÚNIE. *Kybernetická bezpečnosť: ako EÚ bojuje proti kybernetickým hrozbám*. [online].[2022-12-08]. Dostupné na internete: https://www.consilium.europa.eu/sk/policies/cybersecurity/
SEDLÁK, P.- KONEČNÝ, M. - a kol. *Kybernetická (ne)bezpečnost: Problematika bezpečnosti v kyberprostoru*. Brno: Akademické nakladatelství CERM, 2021, 429 s, ISBN 978-80-7623-068-2
SK-CERT. *Kybernetický legislatívny balíček EÚ* [online].[2022-12-08]. Dostupné na internete: https://www.sk-cert.sk/sk/kyberneticky-legislativny-balicek-eu/index.html
SK-CERT, *SK-CERT. Bezpečnostné varovanie V20221228-03,* online].[2022-12-08]. Dostupné na internete: https://www.sk-cert.sk/threat/sk-cert-bezpecnostne-varovanie-v20221228-03/index.html
SLOVAK BUSINESS AGENCY. *Prieskum stavu kybernetickej bezpečnosti v sektore MSP: Správa z kvantitatívneho prieskumu 2022*. [online].[2022-12-08]. Dostupné na internete:

https://www.nbu.gov.sk/wp-content/uploads/2022/08/SBA-Sprava_z_prieskumu_Kyberbezpecnost_SBA_09082022_Actly_RR.pdf
Smernica Európskeho parlamentu a Rady (EÚ) 2019/713 zo 17. apríla 2019 o boji proti podvodom s bezhotovostnými platobnými prostriedkami a proti ich falšovaniu a pozmeňovaniu, ktorou sa nahrádza rámcové rozhodnutie Rady 2001/413/SVV
Správa Komisie Európskeho parlamentu a Rade o posúdení rozsahu, v akom členské štáty prijali opatrenia, ktoré sú nevyhnutné na dosiahnutie súladu so smernicou 2013/40/EÚ o útokoch na informačné systémy, ktorou sa nahrádza rámcové rozhodnutie Rady 2005/222/SVV
Zákon č. 69/2018 Z.z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov

Kontaktné údaje:
Mgr. Michaela Kiššová, PhD.
Katedra kriminológie
Akadémia Policajného zboru v Bratislave
Sklabinská 1, 835 17 Bratislava
michaela.kissova@akademiapz.sk

Bezpečnosť blockchainu

Andrej Lipták

Abstrakt: *Autor sa v článku venuje problematike blockchain technológie z pohľadu jej bezpečnosti. Prostredníctvom analýzy jednotlivých prvkov blockchain technológie autor charakterizuje podstatu bezpečnostného mechanizmu blockchainu vo vzťahu k ochrane dát a na základe vyvodených záverov zhodnotí aktuálny stav stability blockchain technológie s poukázaním na prednosti a riziká spojené s používaním blockchain technológie.*

Kľúčové slová: *Bezpečnosť, blockchain, mechanizmus konsenzu, hash, digitálny podpis*

Abstract: *In the article, the author deals with the question of blockchain technology from the point of view of its security. Through the analysis of individual elements of blockchain technology, the author characterizes the basis of the security mechanism of blockchain in relation to data protection, and based on the conclusions drawn and appropriately used case studies, evaluates the current state of stability of blockchain technology, pointing out the advantages and risks associated with the use of blockchain technology.*

Key words: *Security, blockchain, consensus mechanism, hash, digital signature*

Úvod

Od momentu, kedy sa výmena informácií a údajov pretransformovala do dátového prostredia, vznikla aj potreba špeciálnej ochrany tohto dátového toku. Možnosti ochrany dát je množstvo a odvíjajú sa od druhu ochrany, od stupňa ochrany a od iných vplyvov, ktoré môžu pôsobiť na celistvosť a pravdivosť podstaty dátového prenosu. Pre účely tohto článku sa budeme venovať tomu druhu ochrany dát, ktorý má zaistiť istotu pri uchovávaní informácií. Veď každý, kto má záujem chrániť informácie a údaje v elektronickom prostredí, vytvára si vlastný bezpečnostný systém. Či už sa jedná o elementárne vytvorenie zálohy na externom nosiči alebo o zavedenie prístupového hesla, prípadne využívania rôznych lokálnych technologických rozhraní, ktoré majú zaistiť bezpečnosť dát. Relatívne jednoduché je dosiahnuť vysoký stupeň ochrany dát mimo sieťového prostredia, kedy si účastník siete jemu vlastnými prostriedkami zaistí takúto ochranu. Zložitejšie to je však v sieťovom prostredí, pričom rozsiahlosť siete pôsobí v tomto ohľade ako determinant zníženia istoty chránených dát a dátového toku. Je vôbec možné v tomto prostredí s určitosťou potvrdiť, či sa odoslané dáta zhodujú s prijatými, či na niektorom stupni nedošlo k zámene alebo k úprave, resp. k vymazaniu dát ? V tomto ohľade blockchain technológia predstavuje jednu z relevantných možností, ktorá svojimi kryptografickými prvkami umožňuje ukladanie dát v rámci distribuovanej alebo decentralizovanej siete a zaisťuje ich nemennosť, čím poskytuje účastníkovi siete značnú mieru stability. Je však táto technológia odolná voči nečestným praktikám útočníkov? Sú jednotlivé prvky blockchain technológie dostatočne rezistentné voči kybernetickým útokom ? Je miera rizika ukladania dát do blockchainu primeraná vzhľadom k úžitku, ktorý deklaruje ? Pojem informácie a údaje budú v článku využívané s pre ne typickým logickým významom, a to na základe relevantnosti ich informačného obsahu. Pojem dáta bude pre tieto účely zahŕňať aj informácie aj údaje, pričom významná bude v tomto ohľade typická vlastnosť dát a to, že sú schopné elektronického prenosu.

Blockchain

Elektronická účtovná kniha zachytávajúca digitálne záznamy (dáta) tak, že po ich zapísaní nie je umožnená ich dodatočná zmena. Zapisovanie je realizované prostredníctvom

mechanizmu konsenzu, ktorým účastníci siete deklarujú akceptovanie digitálnych záznamov. Tieto akceptované dáta sú v podstate binárnymi číslicami, bitmi, pre ktorých uloženie je potrebné vyhradiť určitú pamäť. Táto pamäť determinuje veľkosť súboru, bloku, do ktorého je možné ukladať žiadané dáta. Jednotlivé bloky digitálnych záznamov na seba kryptograficky nadväzujú, akákoľvek zmena v bloku predchádzajúcom ovplyvní všetky kryptografické výstupy blokov nasledujúcich. Každý účastník siete drží kópiu tejto elektronickej účtovnej knihy a v každom momente môže porovnať jednotlivé bloky s ostatnými účastníkmi, a tým zaistiť dôveru a transparentnosť siete.[1] Z uvedeného vyplýva, že v celom blockchainovom ekosystéme neexistuje správca, resp. tretia osoba, ktorá by určovala chod blockchainu, a ktorá by mohla upravovať už zapísané digitálne záznamy. Strata jednej kópie blockchainu neaktivitou účastníka siete alebo snaha o individuálne manipulovanie dát v blockchaine tým pádom nie sú pre chod blockchainu a celistvosť, nemennosť digitálnych záznamov v ňom uchovaných, významne relevantné. Môžeme povedať, že blockchain má decentralizovaný charakter.[2] Takýto blockchain sa označuje aj ako verejný blockchain, a to najmä preto, že vstup do ekosystému nie je účastníkovi podmienený (okrem minimálnych znalostí a vybavenia) žiadnymi špeciálnymi podmienkami. Ak je však tento vstup do ekosystému, do siete podmienený rozhodnutím administrátora alebo je počínanie účastníka siete obmedzené treťou osobou, nemožno hovoriť o verejnom blockchaine, ale o privátnych alebo konzorčných blockchainoch. Privátne a konzorčné blockchainy sú podobné tradičným databázovým systémom, sú typické pre obchodné spoločnosti alebo inštitúcie, ktoré chcú mať pod kontrolou vstup účastníkov do siete, zapisovanie a udržiavanie digitálnych záznamov. Dané je pochopiteľné najmä smerom k transparentnosti, ktorá síce podporuje bezpečnosť blockchainu ako takého, ale nie vždy je potrebná, a to najmä ak sa jedná o uchovávanie utajovaných skutočností alebo iných dát, ktorých prezradenie by mohlo vystaviť inštitúciu do nepriaznivého stavu. Konzorčné a privátne blockchainy sa od seba líšia hlavne stupňom zásahu a kontroly zo strany správcu siete. Konzorčné blockchainy v sebe síce nesú prvky decentralizácie, no zároveň aj zvýšenú mieru kontroly, najčastejšie sú využívané v aplikáciách internetu vecí.[3]

Bezpečnosť blockchainu

Bezpečnosť blockchainu je považovaná za súčasť manažmentu rizík - riadenia rizík, ktorá je špecifikovaná pre blockchainové siete. Zaoberá sa analýzou vplyvov, ktoré pôsobia na blockchain, ako sú napríklad prejavy kybernetickej kriminality, vytváraním rámcov a postupov na predchádzanie negatívnych javov, prípadne určovaním opatrení po vzniku neželanej udalosti. [4] Napríklad ak sa blockchain technológia aktívne používa v internete vecí, ktorého cieľom je plná autonómnosť spracovania, výmeny dát tak, aby do tohto systému nemusel zasahovať človek, môže byť problémom udržanie stability siete. Zahltenie blockchainu Denial-

1 PERWEJ, Y., AKHTAR, N., PARWEJ, F. 2018. A TECHNOLOGICAL PERSPECTIVE OF BLOCKCHAIN SECURITY. [online] [cit. 03.01.2023]. DOI: 10.24327/ijrsr.2018.0911.2869 Dostupné na internete: <
https://www.researchgate.net/publication/329337003_A_Technological_Perspective_of_Blockchain_Security>

2 AL-SHABI, M., AL-QARAFI, A. 2022. Improving blockchain seurity for the internet of things: challenges and solutions. [online] [cit. 03.01.2023]. DOI: 10.11591/ijece.v12i5.pp5619-5629. Dostupné na internete: < https://www.ijece.iaescore.com/index.php/IJECE/article/view/26459>

[3] NABBEN, K., 2021. Blockchain Security as "People Security": Applying Sociotechnical Security to Blockchain Technology. [online] [cit. 03.01.2023]. DOI: https://doi.org/10.3389/fcomp.2020.599406. Dostupné na internete: < https://www.frontiersin.org/articles/10.3389/fcomp.2020.599406/full>

[4] What Is Blockchain Security: Challenges and Examples. [online] [cit. 04.01.2023]. Dostupné na internete: < https://www.simplilearn.com/what-is-blockchain-security-and-its-examples-article>

Of-Service[5] útokom, prípadne iné zlyhanie siete môže znamenať nefunkčnosť systému. Alebo napríklad v prostredí zdieľanej ekonomiky, ktorej podstatou je spájať dodávateľov a odberateľov, zákazníkov a predajcov bez nutnosti spoliehať sa na tretiu stranu, ktorá obchodný vzťah sprostredkuje, môže byť problémom únik citlivých údajov zúčastnených strán.[6] Blockchain bezpečnosť možno rozdeliť do jednotlivých sfér v logike teórie množín. Prvá a najdôležitejšia je bezpečnosť uložených dát. Od nezmeniteľnosti, celistvosti, neporušiteľnosti a integrity týchto dát sa odvíjajú všetky ostatné nadväzujúce druhy bezpečnosti a ak táto ochrana dát zlyhá, respektíve je prelomená, nemožno hovoriť o stabilite blockchain technológie. Blockchain bezpečnosť na tejto úrovni je však dostatočne kryptograficky ošetrená. Druhá množina je bezpečnosť na úrovni sieťového protokolu, ktorá je potrebnou nadstavbou k ochrane dát. P2P[7] sieť blockchainu pozostáva z účastníkov siete, ktorí majú jednotlivé úlohy. Získaním nadvlády nad sieťou môže dôjsť k neželaným úkonom v protokole, v sieti. Treťou množinou je mechanizmus konsenzu. Pri konsenze dochádza k uloženiu dát do blockchainu, po uložení sú tieto dáta prakticky nezmeniteľné. O uložení dát rozhodujú účastníci siete. Na základe čoho a akým spôsobom sa vedia dohodnúť rieši práve táto množina. Štvrtá množina blockchain bezpečnosti zahŕňa ochranu smart kontraktov[8]. Uložené dáta v blockchaine môžu mať za určitých podmienok formu napísaného programu. Dôležitosť nezmeniteľnosti tohto programu je determinantom jeho funkčnosti a jeho nezmeniteľnosť zabezpečuje práve blockchain technológia. Piata množina blockchain bezpečnosti zahŕňa bezpečnosť decentralizovaných aplikácii. Táto množina je v aktuálnom období príznačná vysokou mierou rizikovosti v rámci blockchain bezpečnosti. Rizikovosť porušenia blockchain bezpečnosti narastá smerom k najširšej množine a opäť postupne klesá smerom dovnútra. Príčinou je dynamickosť blockchain ekosystému, v ktorom prvá množina predstavuje tú najstaršiu najfundamentálnejšiu, najmenej dynamickú no zároveň najviac zaručenú časť blockchain bezpečnosti. Naopak piata množina predstavuje veľmi dynamickú oblasť, je zároveň najmladšia, dochádza v nej k častým zmenám, a je z pohľadu narušenie bezpečnosti blockchainu najrizikovejšia. [9]

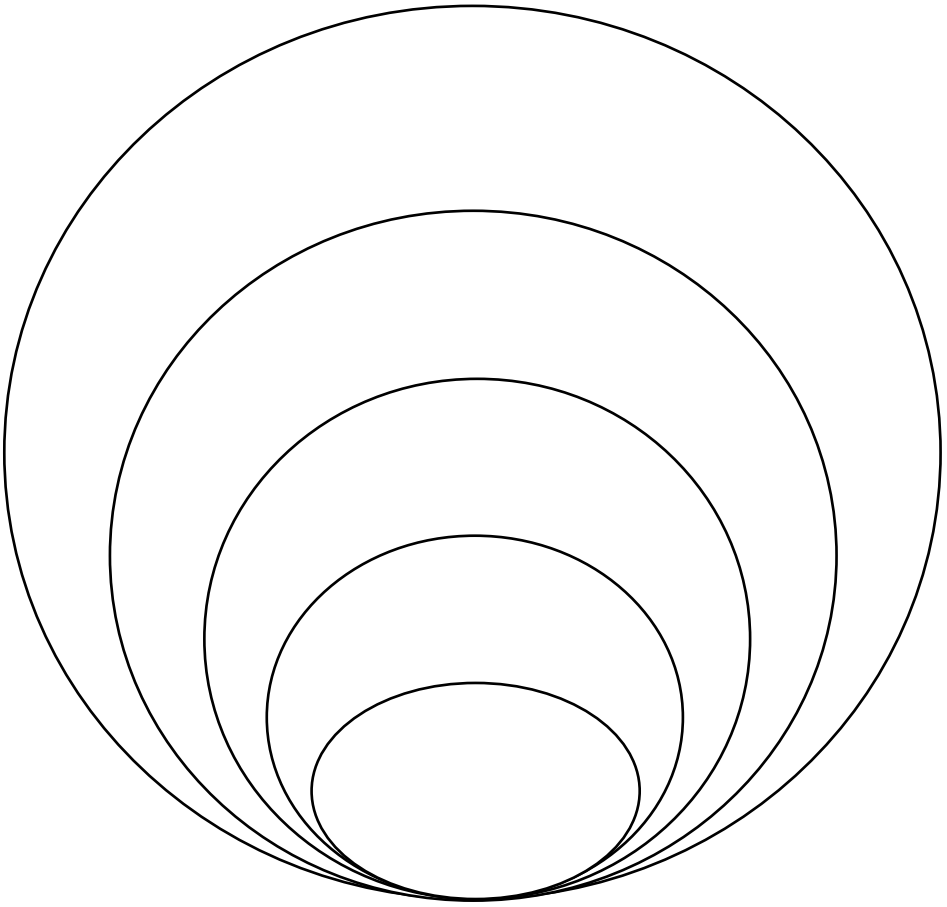
[5] Security Tip (ST04-15). [online] [cit. 04.01.2023]. Dostupné na internete: <https://www.cisa.gov/uscert/ncas/tips/ST04-015>

[6] MATTILA, V., 2022. Techniques and Research Direction of Blockchain Security and Privacy. [online] [cit. 04.01.2023]. DOI: 10.37602/IJSSMR.2022.54151 Dostupné na internete: <https://www.researchgate.net/publication/365959899_Techniques_and_Research_Direction_of_Blockchain_Security_and_Privacy>

[7] What Is Peer To Peer Network, And How Does It Work ?. [online] [cit. 04.01.2023]. Dostupné na internete: < https://www.blockchain-council.org/blockchain/peer-to-peer-network/>

[8] INTRODUCTION TO SMART CONTRACTS. [online] [cit. 04.01.2023]. Dostupné na internete: < https://ethereum.org/en/developers/docs/smart-contracts/

[9] LENG, J., ZHOU, M., THAO, J., HUANG, Y., BIAN, Y. 2022. [online] [cit. 08.01.2023]. DOI: 10.1109/TSC.2020.3038641. Dostupné na internete: < https://ieeexplore.ieee.org/document/9271868>



Obrázok 1: Úrovne blockchain bezpečnosti
Zdroj: Dostupné na internete: < https://www.computer.org/csdl/journal/sc/2022/04/09271868/1p2RaCvQ7dK>

Blockchain bezpečnosť na úrovni ochrany dát bloku

- Privátny a verejný kryptografický kľúč ako prvok bezpečnosti

Privátny kľúč pri využívaní blockchain technológie pôsobí ako bezpečnostný mechanizmus v tom zmysle, že reprezentuje účastníka siete a je nevyhnutný na ďalšie kryptografické operácie. Privátnym kľúčom sa preukazuje vlastníctvo virtuálnych mien, slúži na priradenie dát k účastníkovi siete, ktorý uviedol údaje do bloku v blockchaine. Typ a kvalita privátneho kľúča sa môže líšiť v závislosti od blockchainu, vo všeobecnosti však ide o reťazec bitov, ktorý si užívateľ siete môže vytvoriť v rámci možností samostatne, prípadne a čo je častejšie, na jeho vytvorenie využíva tzv. peňaženku virtuálnej meny, ktorá realizuje všetky potrebné kryptografické úkony za užívateľa. Napríklad v blockchaine virtuálnej meny Bitcoin je vytvorenie privátneho kľúča podmienené uvedením 256 – miestneho binárneho kódu, potom sa aplikuje kryptografická funkcia Elliptic Curve[10], pričom je vo funkcii uvedený náhodne určený binárny kód ako násobiteľ. Privátny kľúč, ktorý si účastník siete vytvoril samostatne je

[10] Elliptic Curve Cryptography: A Basic Introduction. [online] [cit. 08.01.2023]. Dostupné na internete: < https://www.pcrisk.com/removal-guides/12266-blackruby-ransomware/>

pri splnení všetkých podmienok rovnako validný ako kľúč vytvorený peňaženkou virtuálnej meny. Je potrebné spomenúť, že blockchain technológia neskúma, kto je držiteľom alebo vlastníkom privátneho kľúča, privátny kľúč a jeho ochrana je v kompetencii účastníka siete. Ak si účastník siete vytvoril privátny kľúč sám, sám si udržiava aj jeho bezpečnosť. Účastníci siete, ktorí na jeho vytvorenie použili peňaženku virtuálnej meny majú možnosť využiť podpornú ochranu privátneho kľúča, ktorú ponúka peňaženka virtuálnej meny. Či už sa jedná o udržiavanie kľúča mimo internetovú sieť, alebo o poskytnutie prístupového hesla, prípadne bezpečnostnej otázky. V konečnom dôsledku je stále zodpovedný za uchovanie privátneho kľúča účastník siete.

Z privátneho kľúča, ktorý je fundamentálnym aspektom pre interakciu s blockchain dátami kryptograficky vychádza verejný kľúč. Napríklad v blockchaine virtuálnej meny Bitcoin sa pre vytvorenie verejného kľúča na aplikuje na privátny kľúč kryptografická funkcia SHA 256[11], a potom RIPEMD 160[12]. Verejný kľúč je explicitne vyjadrený v bloku a je súčasťou dát v blockchaine. Aj keď je tento kľúč transparentne uvedený v blockchaine, vyjadruje jeden z prvkov bezpečnosti, pretože síce vychádza z privátneho kľúča účastníka siete, nie je za obvyklých podmienok spätne vyjadriteľný. Uvedením verejného kľúča v blockchaine alebo jeho iným uverejnením sa teda účastník siete nevystavuje zvýšenému riziku zneužitia dát v jeho mene ale naopak, chráni znenie privátneho kľúča. [13]

- Riziká spojené s bezpečnostnými prvkami blockchain technológie – útok na privátny kľúč

Útoky spojené s prelomením bezpečnostného prvku privátneho kľúča nie sú v sfére blockchain technológie na úrovni dát častou udalosťou. Ak k útokom dochádza, tak zväčša na úrovni krádeže privátneho kľúča, resp. jeho zneužitia, ktorého príčinou je nezodpovedná manipulácia s vlastným privátnym kľúčom jednotlivého účastníka siete; to však neznamená, že neexistuje riziko kybernetického napadnutia fundamentálnej stránky privátneho kľúča. Najzraniteľnejšou oblasťou je z tohto hľadiska moment vytvárania privátneho kľúča prostredníctvom peňaženky virtuálnej meny, a to v kroku aplikácie Elliptic Curve digitálneho algoritmu. Útočník po napadnutí tohto algoritmu dokáže zaznamenať vytvorený privátny kľúč bez toho, aby došlo k povšimnutiu zo strany účastníka siete. Prostriedky, ktoré na uvedené typicky využívajú útočníci sú malwéry ako je Dridex, CoreBOT, IceID[14], BlackRubyRansomware[15], SmokeLoader[16] alebo Terdot. Dridex je formou „trojského koňa“.[17] Využíva Microsoft Word, Excel makrá, ktoré po otvorení začnú simultánne vykonávať

[11] SHA-256 [online] [cit. 09.01.2023]. Dostupné na internete:
< https://freemanlaw.com/sha-256/>
[12] RIPEMD160 Class. [online] [cit. 09.01.2023]. Dostupné na internete:
<https://learn.microsoft.com/en-us/dotnet/api/system.security.cryptography.ripemd160?view=netframework-4.8.1>
[13] HOSP, J. Kryptomeny. 2018. Bratislava: Vydavateľstvo TATRAN. s 169.
[14] Security Primer – IcedID. [online] [cit. 09.01.2023]. Dostupné na internete:
< https://www.cisecurity.org/insights/white-papers/security-primer-icedid/>
[15] BlackRuby Ransomware. [online] [cit. 09.01.2023]. Dostupné na internete:
< https://www.pcrisk.com/removal-guides/12266-blackruby-ransomware/>
[16]Trojan.SmokeLoader. [online] [cit. 09.01.2023]. Dostupné na internete:
< https://www.malwarebytes.com/blog/detections/trojan-smokeloader/>
[17] SINGH, S., HOSEN, A., YOON, B. 2021. Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network. [online] [cit. 09.01.2023]. DOI: 10.1109/ACCESS.2021.3051602 Dostupné na internete: <https://www.ieeexplore.ieee.org/document/9323061 >

neželanú aktivitu za účelom sledovania a odcudzenia privátneho kľúča. [18] CoreBOT je typický skutočnosťou, že po infikovaní internetových prehliadačov dokáže snímať históriu prehľadávania, automatický dopĺňane formuláre, uložené heslá a pod. Ak si účastník siete vytváral privátny kľúč prostredníctvom internetového prehliadača a zároveň bol jeho prehliadač infikovaný CoreBOT malwarom je veľká šanca, že tento privátny kľúč bezpečný nie je. [19] Terdot je typ malware-u, ktorý dokáže sledovať a modifikovať dátový tok na sociálnych sieťach alebo e-mailových platformách. Dokáže automaticky stiahnuť a odosielať dostupné údaje podľa vyžiadania útočníka.

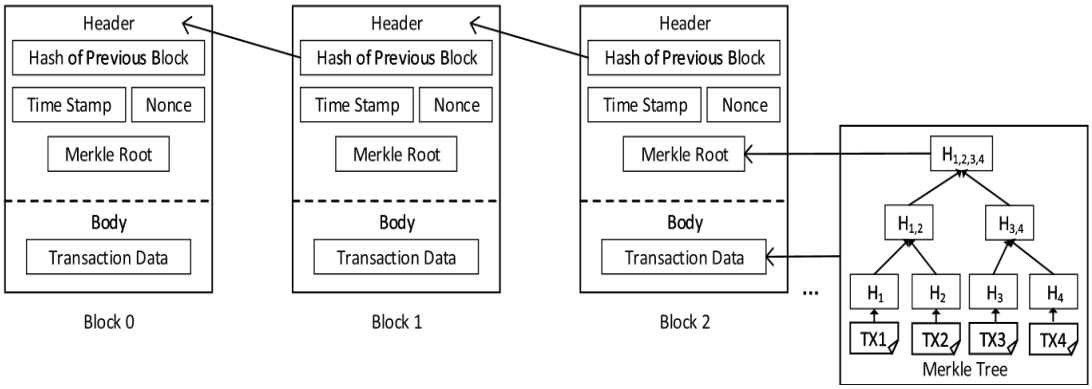
Ďalším rizikom v tejto oblasti vychádza z podstaty asymetrickej kryptografie. Ako bolo spomínané, blockchain technológia využíva prvky asymetrickej kryptografie pri dualite kľúčov, pričom jeden slúži na zakódovanie dát – verejný kľúč a druhý slúži na dekódovanie dát – privátny kľúč. Každý, kto drží verejný kľúč môže dáta kódovať, alebo iba ten, kto drží súkromný kľúč môže dáta dekódovať. Verejný kľúč sa derivuje z privátneho kľúča za využitia zložitej matematickej úlohy, ktorá nie je spätne vyvoditeľná. To znamená, že z privátneho kľúča je možno veľmi jednoducho vyvodiť verejný kľúč no z verejného kľúča nie je možné vyvodiť privátny kľúč. Útočník je teda obmedzený na „hádanie“ bitového kódu, ktorý predchádza vytvoreniu privátneho kľúča tak, aby po jeho následnom kryptovaní získal želaný privátny kľúč. Či bitový kód a následný privátny kľúč uhádol si môže overiť následným derivovaním a porovnaním verejných kľúčov. To, že sa to útočníkovi podarí je pri použití aktuálnych technických možností vysoko nepravdepodobné, blížiace sa nemožnosti. V budúcnosti sa však počíta s využívaním kvantovej mechaniky, ktorá by tieto šance zvýšila. Bežný počítač vie určiť, či sa jedná o bit s hodnotou 0 alebo o bit s hodnotou 1, na rozdiel od toho kvantový počítač dokáže určiť bit s hodnotou 0, bit s hodnotou 1 alebo, že bit ma zároveň hodnotu 0 a 1. Tento fenomén rapídne zväčšuje možnosti paralelného spracovávania údajov. V takomto prípade by uhádnutie jednotlivého privátneho kľúča bolo pravdepodobnejšie a predstavovalo by to veľké riziko pre bezpečnosť blockchain technológie.[20] Podľa Národného inštitúty pre štandardy a technológie „ďalej NIST“ - vládnej agentúry USA sa 80-bitový kryptografický level už aktuálne nepovažuje za dostatočne bezpečný a predstavuje zvýšené riziko pre bezpečnosť blockchainu. Inštitút predpokladá, že do roku 2031 bude predstavovať zvýšené riziko aj 112–bitový kryptografický level. NIST vykonáva aktívnu činnosť v oblasti ochrany pred prelomením používanej kryptografie prostredníctvom kvantových počítačov. 6 rokov trvajúci program, ktorého podstatou bolo vytvorenie novej kryptografie rezistentnej voči kvantovej mechanike sa skončil zverejnením štyroch kryptografických algoritmov.

[18] Dridex malware. [online] [cit. 09.01.2023]. Dostupné na internete:
< https://www.techtarget.com/searchsecurity/definition/Dridex-malware/>
[19] What CoreBOT malware ?. [online] [cit. 09.01.2023]. Dostupné na internete:
< https://www.tutorialspoint.com/what-is-corebot-malware/>
[20] Cryptography & Challenges posed by Quantum Computers. [online] [cit. 09.01.2023]. Dostupné na internete:
< https://www.hsc.com/resources/blog/cryptography-challenges-posed-by-quantum-computers/>

Crystals-Dilithium[21], FALCON[22], SPHINCS+[23] pre digitálne podpisy a CRYSTALS-Kyber[24] pre všeobecné kódovanie. [25]

- Blockchain štruktúra ako prvok blockchain bezpečnosti

V blockchain štruktúre sú dáta zapísané v blokoch. Blok pozostáva z hlavičky a obsahu. Hlavička bloku obsahuje hash[26] predchádzajúceho bloku, časové označenie, hodnoty nonce[27] a hash vrcholu Merkle tree[28] (ďalej „Merkle root"). Hash predchádzajúceho bloku je zakomponovaný v aktuálnom bloku, čím sa zabezpečuje kontinuita jednotlivých blokov. Akákoľvek zmena v dátach v ľubovoľnom bloku ovplyvní hash výstupy každého nasledujúceho bloku. Takýmto spôsobom je možné jednoducho zistiť, či a v akom bloku došlo



Obrázok 2: **Blockchain štruktúra**
Preklad: Header – hlavička bloku
Hash of Previous Block – hash predchádzajúceho bloku
Time Stamp – časové označenie
Body – obsah bloku
H – Hash
TX – skupina dát
Transaction Data – transakčné dáta (dáta, ktoré chce účastník siete umiestniť do blockchainu)

Zdroj: Dostupné na internete: <https://link.springer.com/chapter/10.1007/978-981-15-0776-2_5/figures/1>

[21] CRYSTALS Cryptographic Suite for Algebraic Lattices. [online] [cit. 09.01.2023]. Dostupné na internete: < https://www.pq-crystals.org/dilithium/index.shtml/>
[22] Fast-Fourier Lattice-based Compact Signatures over NTRU. [online] [cit. 09.01.2023]. Dostupné na internete: < https://www.falcon-sign.info>
[23] SPHINCS+. [online] [cit. 09.01.2023]. Dostupné na internete: < https://www.sphincs.org>
[24] CRYSTALS Cryptographic Suite for Algebraic Lattices. [online] [cit. 09.01.2023]. Dostupné na internete: < https://www.pq-crystals.org/dilithium/index.shtml/>
[25] CHEN,L., JORDAN,S. LIU, Y., MOODY, D., PERALTA, R., PERLNER, R., SMITH-TONE, D. 2016. Report on Post-Quantum Cryptography. [online] [cit. 09.01.2023]. DOI: http://dx.doi.org/10.6028/NIST.IR.8105 Dostupné na internete: <https://www.nvlpubs.nist.gov./nistpubs/ir/2016/NIST.IR.8105.pdf >
[26] Blockchain Hash Function. [online] [cit. 10.01.2023]. Dostupné na internete: <https://www.javatpoint.com/blockchain-hash-function>
[27] The Significance Of Nonce In Blockchain [online] [cit. 10.01.2023]. Dostupné na internete: <https://101blockchains.com/nonce-in-blockchain/>
[28] Merkle Tree in Blockchain: What is it, How does it work and Benefits. [online] [cit. 10.01.2023]. Dostupné na internete: <https://www.simplilearn.com/tutorials/blockchain-tutorial/merkle-tree-in-blockchain/>

k zmene dát. V hlavičke sa ďalej nachádza časové označenie, ktoré označuje čas, kedy bol blok vytvorený; nonce, ktorý je dôležitý pre vytvorenie a overenie bloku; a Merkle root, ktorý je vrcholom Merkle tree. Merkle tree pozostáva z jednotlivo zahashovaných skupín dát, ktorých výstupy sa ďalej opäť hashujú až nevznikne jeden hash výstup – Merkle root. Takáto redukcia dát nemá negatívny vplyv na bezpečnosť uložených dát, keďže akákoľvek zmena v týchto dátach zmení hodnotu Merkle root. Výhodou Merkle tree je schopnosť rýchlejšieho overenia pravdivosti dát v rámci siete a pri realizovaní mechanizmu konsenzu. Merkle tree je obsahom bloku.[29]

- Riziká spojené s bezpečnostnými prvkami blockchain technológie – útok na blockchain štruktúru

Štruktúra blockchainu je vo svojej podstate prostá technológia, ktorú v decentralizovanom systéme môže, abstrahovaním od špecifík sieťového protokolu a mechanizmu konsenzu, ovplyvňovať akýkoľvek účastník siete. Ovplyvnením dát v štruktúre blockchainu však nevyhnutne dochádza k zmene hash výstupov blockchainu. Zmenou v dátach vzniká nový blockchain, ktorého štruktúra je stále rozdielna od pôvodnej (a to od bloku, v ktorom boli ovplyvnené dáta), a predstavuje odklon od doteraz platného, pravdivého blockchainu. Pravdivý blockchain je v decentralizovanom systéme ten, ktorý obsahuje najväčší počet blokov a zároveň ho prijala nadpolovičná väčšina účastníkov siete. To znamená, že ak útočník dokáže za určitú časovú jednotku zmeniť dáta v bloku a odklonený blockchain rozposlať viac než nadpolovičnej väčšine účastníkov siete, bude jeho upravený a odklonený blockchain považovaný za pravdivý. Rizikom bezpečnosti blockchain štruktúry je v tomto ohľade Sybil attack, ktorý spočíva v tom, že jednotlivý účastník siete vygeneruje veľké množstvo uzlov, ktoré reprezentujú účastníkov siete decentralizovaného systému. Ak by počet takýchto uzlov dosiahol nadpolovičnú väčšinu zo všetkých účastníkov siete, mohol by útočník ovplyvňovať štruktúru dát v blockchaine podľa svojho uváženia. Do úvahy je potrebné brať aj skutočnosť, že tieto dáta, ako každé iné, majú svoju veľkosť, a teda platí, že čím viac blokov v blockchaine, tým väčšie miesto je potrebné pre blockchain na úložisku vyhradiť. Úložisko v decentralizovanej sieti v kompetencii jednotlivých účastníkov siete, preto je potrebné dbať na celkovú veľkosť blockchainu. Dá sa predpokladať, že pri narastajúcej veľkosti blockchainu bude počet účastníkov siete zodpovedných za overovanie blockchainu klesať, a tým sa stane Sybil attack jednoduchším na vykonanie. [30]

Blockchain bezpečnosť na úrovni štruktúry blockchainu je preto potrebné spájať s bezpečnostnými prvkami na iných úrovniach blockchain bezpečnosti, čím sa znižuje riziko úspešného útoku a zmeny v celistvosti dát uložených v blockchaine.

[29] LIANG Y. 2019. Blockchain for Dynamic Spectrum Management. [online] [cit. 10.01.2023]. DOI: 10.1007/978-981-15-0776-2_5 . Dostupné na internete: < https://link.springer.com/chapter/10.1007/978-981-15-0776-2_5>

[30] AL-SHABI, M., AL-QARAFI, A. 2022. Improving blockchain seurity for the internet of things: challenges and solutions. [online] [cit. 11.01.2023]. DOI: 10.11591/ijece.v12i5.pp5619-5629. Dostupné na internete: < https://www.ijece.iaescore.com/index.php/IJECE/article/view/26459>

Blockchain bezpečnosť na úrovni sieťového protokolu

- P2P sieť ako prvok blockchain bezpečnosti

P2P sieť je technologickým aspektom, ktorý zabezpečuje decentralizáciu blockchain technológie. Túto sieť tvoria rovnocenné uzly, ktoré si môžu medzi sebou rozposielať potrebné informácie bez toho, aby dátový tok prebiehal prostredníctvom centrálneho servera a klientov. Výhodou P2P siete je, že aj keď je kybernetickým útokom napadnutý a znefunkčnený určitý uzol, nepredstavuje to veľký zásah do funkčnosti celej siete, ako by to bolo v prípade napadnutia a znefunkčnenia servera pri sieťovej architektúre klient-server.[31] Pre P2P sieť blockchainu je typické, že uzly v sieti majú možnosť realizovať odlišné druhy úloh. Do tohto momentu sme pre všetky tieto uzly používali pomenovanie účastníci siete, čo subsumovalo všetky uzly bez ohľadu na vykonávané úlohy. Táto diferenciácia je dôležitým aspektom, ktorý vplýva na bezpečnosť blockchain technológie. Light-node uzly zväčša neukladajú celý blockchain, neoverujú pravdivosť dát, dáta nezapisujú do blockchainu. Tieto uzly najčastejšie vytvárajú požiadavku o uloženie dát do blockchainu, pričom tú následne zasielajú iným účastníkom siete - Full-node uzlom. Úlohou Full-node uzlov je overovanie prípustnosti zaslaných požiadaviek a overovanie správnosti, pravdivosti prijatých dát s dátami už uloženými v blockchaine. Tieto uzly ukladajú a aktualizujú celý blockchain v reálnom čase podľa podmienok určených v sieti. Treťou formou sú ťažiarenské uzly. Ich úlohou je zapisovanie informácií do blockchainu a vykonávanie činností spojených s mechanizmom konsenzu. [32]

- Riziká spojené s bezpečnostnými prvkami blockchain technológie – útok na P2P sieť

Eclipse útok je jedným z kybernetických útokov, ktorý dokáže ovplyvniť funkčnosť jednotlivých uzlov v P2P sieti a narušiť jej funkčnosť a bezpečnosť. Uzol v takomto prípade nedokáže prijímať informácie od iných než napadnutých uzlov, útočník takisto ovplyvňuje všetky vychádzajúce informácie. Dátový tok, uzol a uložený blockchain môže útočník ovplyvňovať bez toho, aby bol pri svojej činnosti identifikovaný. Tento útok môže mať formu botnet útoku, ktorý vo väčšej miere zahltí dátový tok uzla, alebo môže mať formu infraštruktúrneho útoku, ktorý ohrozuje najmä tie uzly, ktoré sú pripojené do siete internet prostredníctvom totožných IP adries.

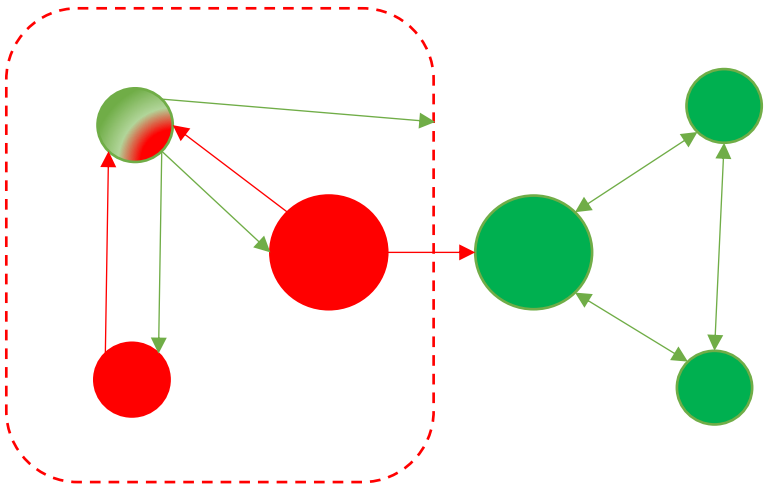
Ďalším útokom na sieť blockchainu môžeme považovať Routing útok, ktorý sa zvykne nazývať aj únos blockchainu, resp. časti P2P siete blockchainu. V tomto prípade sa však nejedná o únos v zmysle aktuálnej legislatívnej ani technickej terminológie, preto sa budeme venovať pojmu a podstate Routing útoku. Na rozdiel od Eclipse útoku je útočníkovým cieľom rozdelenie siete tak, aby ním kontrolované uzly stratili možnosť kontroly dátového toku s uzlami mimo ovládnutej časti siete. V takomto prípade útočník môže dosiahnuť stav, kedy budú všetky požiadavky o overenie a zápis dát ukladané do lokálneho paralelného blockchainu, ktorý nekorešponduje s dátami v originálnom blockchaine. Čím výraznejšie je rozdelenie siete, tým menšia je pravdepodobnosť, že sa uzly v sieti vôbec dozvedia o tom, že sú súčasťou

[31] WARARKAR, P., KAPIL, N., REHANI, V., MEHRA, Y., BHATNAGAR, Y. 2015. Resolving Problems Based on Peer to Peer Network Security Issue‘s. [online] [cit. 13.01.2023]. DOI: 10.1016/j.procs.2016.02.113. Dostupné na internete: < https://www.sciencedirect.com/science/article/pii/S1877050916001150?via%3Dihub>

[32] HOSP, J. Kryptomeny. 2018. Bratislava: Vydavateľstvo TATRAN. s 52-53.

Routing útoku. Každá snaha o overenie blockchainu stroskotá na ovládnutom Full-node uzle, ktorý účastníka siete ubezpečí o pravosti falošného paralelného blockchainu.

Eclipse a Routing útok svojím spojením predstavujú značné riziko v spoľahlivosti P2P siete v rámci bezpečnosti blockchainu. Spojením s ďalšími prvkami bezpečnosti je však toto riziko považované za tolerovateľné vzhľadom k výhodám, ktoré P2P sieť ponúka. [33]



Obrázok 3: Eclipse v spojení s Routing útokom na P2P sieť v rámci blockchain technológie
Zdroj: Dostupné na internete: <www.academy.binance.com/en/articles/what-is-an-Eclipse-Attack>

Blockchain bezpečnosť na úrovni mechanizmu konsenzu

- Proof of work ako prvok blockchain bezpečnosti

Na to, aby mohli byť údaje zapísané do blockchainu, musí existovať zhoda medzi jednotlivými uzlami siete o tom, kto je oprávnený tieto údaje zapísať. Zapísaním a uložením údajov do blockchainu sa údaje stávajú nemenné, a preto je dôležité, aby túto úlohu nemohol vykonávať akýkoľvek účastník siete. Ak by tento mechanizmus konsenzu nebol súčasťou blockchain technológie, neexistoval by jeden distribuovaný záznam s celistvými a nemennými informáciami, ale množstvo lokálnych jednoducho ovplyvniteľných záznamov. Pri vytváraní konsenzu majú nezastupiteľné miesto ťažiarenské uzly, ktoré prijímajú požiadavky na zápis dát do blockchainu a za splnenia podmienok zapisujú dáta do blockchainu. Mechanizmov konsenzu je viacero, pre naše účely spomenieme niektoré, no skrz analýzu sa budeme venovať len najčastejšie využívanému proof of work mechanizmus konsenzu.

Pri Proof of work mechanizmu konsenzu musia ťažiarenské uzly vyriešiť zložitú matematickú úlohu, ktorá je typická tipovaním a následným aplikovaním hashovacej funkcie. Princíp hádania a tipovania je podobný, ako bolo uvedené v časti o kvantových počítačoch. Ťažiarenské uzly zvyšujú svoju pravdepodobnosť uhádnutia úlohy tým, že zvyšujú počet hádaní za určitú časovú jednotku, ktorá sa v konečnom dôsledku prejavuje v spotrebovanej elektrickej energii. Táto elektrická energia predstavuje dôkaz o vykonanej práci a vychádzaním z teórie

[33] PERWEJ, Y., AKHTAR, N., PARWEJ, F. 2018. A TECHNOLOGICAL PERSPECTIVE OF BLOCKCHAIN SECURITY. [online] [cit. 14.01.2023]. DOI: 10.24327/ijrsr.2018.0911.2869 Dostupné na internete: <
https://www.researchgate.net/publication/329337003_A_Technological_Perspective_of_Blockchain_Security>

pravdepodobnosti sa predpokladá, že ten uzol, ktorý uhádol úlohu minul dostatočné množstvo energie, aby preukázal sieti svoju dôveryhodnosť. Po uhádnutí matematickej úlohy si potom ťažiarenský uzol vyberie údaje z prijatých požiadaviek, ktoré do nového bloku blockchainu zapíše. Zložitosť tejto úlohy je dynamická, upravuje sa podľa celkového objemu použitej energie všetkých ťažiarenských uzlov. [34]

Pri Proof of stake jednotlivé ťažiarenské uzly preukazujú svoju dôveryhodnosť uzamknutím kolaterálu v sieti na určité, predom definované obdobie. Ak by ťažiarenský uzol nevykonával úlohy spojené s uzatváraním blokov, zapisovaním informácií do blokov čestne, o tento kolaterál by prišiel. Ktorý ťažiarenský uzol získa právo na vykonanie týchto úloh je determinované náhodou. Vyššiu pravdepodobnosť získa ten ťažiarenský uzol, ktorý v sieti uzamkne vyššiu hodnotu kolaterálu. Tento mechanizmus konsenzu oproti Proof of work síce znižuje riziko centralizácie (pretože na riadne vykonávanie úloh ťažiarenské uzla nie je potrebné množstvo energie), na druhú stranu však vzniká nové riziko bezpečnosti v rámci blockchain technológie, a ním je útok na uzamknutý kolaterál.[35]

Medzi ďalšie mechanizmy konsenzu môžeme zaradiť napríklad Proof of Activity, ktorý je hybridom hore spomínaných mechanizmov konsenzu,[36] Proof of Importance, ktorý ako dôkaz dôveryhodnosti používa dobu čestnej aktivity jednotlivého uzlu v sieti,[37] Proof of Luck, pri ktorom ťažiarenské uzly náhodne vygenerujú čísla a podľa určených pravidiel (napr. pravidlo najväčšieho čísla) disponujú možnosťou uzatvoriť nový blok, Proof of Elapsed Time, v ktorom má každý ťažiarenský uzol časovač s náhodne vygenerovaným časom. Ten uzol, ktorému čas uplynie najskôr uzatvára dáta do nového bloku. Čas je generovaný náhodne. [38]

- Riziká spojené s bezpečnostnými prvkami blockchain technológie – útok na proof of work

Proof of work mechanizmus konsenzu predstavuje aktuálne jeden z najbezpečnejších, ak nie najbezpečnejší mechanizmus konsenzu vôbec. Bezpečnosť uložených dát v blockchaine, rastie s celkovým objemom spotrebovanej energie všetkých ťažiarenských uzlov a s dobou uloženia dát v blockchaine. Na zapísanie informácií do nového bloku je potrebné „n“ elektrickej energie (ktorá je reprezentovaná výpočtovým výkonom ťažiarenských uzlov, resp. presnejšie výkonom potrebným na aplikovanie určitého počtu hashovacích funkcií za jednu sekundu). Na zmenu dát v bloku, po ktorom nasleduje „x“ blokov je potrebné použiť „n“- násobné množstvo energie v závislosti od „x“. Spojením s dynamickou zložitosťou matematickej hádanky, ktorej uhádnutie trvá určitý čas (závisí od jednotlivého blockchainu), sa pravdepodobnosť úspešne vykonaného útoku znižuje, zvýšením „n“ objemu energie potrebnej na uzatvorenie bloku.

Rizikom je však 51% útok. Ak ťažiarenský uzol – môže reprezentovať aj množinu uzlov, za ktorým stojí jeden útočník, ako bolo spomínané pri Sybil útoku – dosiahne väčšinu

[34] RAJCANIOVA, M., CIAIAN, P. 2021. Interdependencies between Mining Costs, Mining Rewards and Blockchain Security. [online] [cit. 14.01.2023]. Dostupné na internete: <https://www.researchgate.net/publication/354270393_Interdependencies_between_Mining_Costs_Mining_Rewards_and_Blockchain_Security>

[35] PROOF-OF-STAKE (POS). [online] [cit. 14.01.2023]. Dostupné na internete: <https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/>

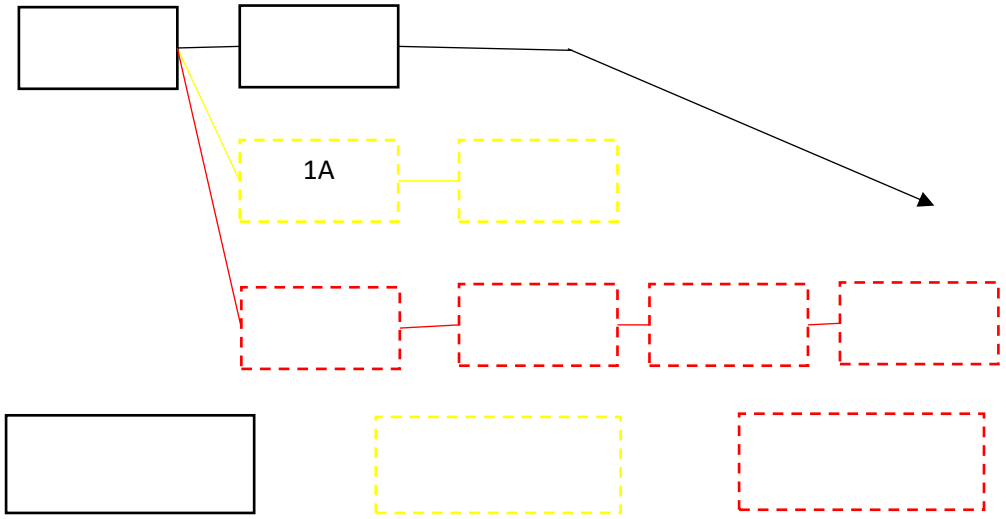
[36] Proof of Acrivity (PoA) in Blockchain. [online] [cit. 14.01.2023]. Dostupné na internete: < https://www.naukri.com/learning/articles/proof-of-activity-in-blockchain/

[37] Proof of Importance (Pol) in Blockchain. [online] [cit. 14.01.2023]. Dostupné na internete: <https://www.naukri.com/learning/articles/proof-of-importance-poi-in-blockchain/>

[38] What is Proof of Elapsed Time (PoET)? [online] [cit. 14.01.2023]. Dostupné na internete: < https://www.analyticssteps.com/blogs/what-proof-elapsed-time-poet/>

vo výpočtovom výkone všetkých ťažiarenských uzlov, môže tento uzol namiesto uzatvorenia nového bloku ovplyvniť dáta v celom blockchaine a rozoslať ho ostatným uzlom ako pravý blockchain.

Ďalším útokom pri Proof of work mechanizme je Selfish mining, ktorého podstatou je odklon blockchainu od určitej úrovne a vytvorenie paralelného blockchainu, ktorý je potom prezentovaný sieti. Útočník sieti najprv zatají, že úspešne uhádol matematickú úlohu a uzavrel blok s dátami, pričom sa snaží uzavrieť ďalší blok, aby tým udržal najdlhšiu vetvu. Útočník teda od určitého momentu, aj keď v rámci pravidiel, upravuje blockchain od určitého bloku podľa svojich predstáv. Všetok výpočtový výkon a dáta uzatvorené iným ťažiarenským uzlom v konečnom dôsledku nebudú validné a uložené v blockchaine. [39]



Obrázok 4 Schéma Selfish mining - uzatváranie blokov v rámci viacerých paralelných privátnych blockchainov
Zdroj: Dostupné na internete: <www.eprint.iacr.org/2019/486.pdf>

Záver

Autor sa v článku venoval bezpečnosti blockchain technológie na úrovni dát, sieťového protokolu a mechanizmu konsenzu. Analýzou dát bolo zistené, že blockchain technológia predstavuje jednu z alternatív, ktorou je možné zaistiť celistvosť, pravdivosť a nemennosť dát v decentralizovanej sieti. Bezpečnosť dát je závislá od nastavenia jednotlivých technologických aspektov blockchain technológie, ktoré vo vzájomnom prepojení vytvárajú systém odolný voči externým vplyvom vyplývajúcich z kybernetickej kriminality.

[39] SINGH, S., HOSEN, A., YOON, B. 2021. Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network. [online] [cit. 14.01.2023]. DOI: 10.1109/ACCESS.2021.3051602 Dostupné na internete: <https://www.ieeexplore.ieee.org/document/9323061 >

Zoznam použitej literatúry:

HOSP, J. *Kryptomeny*. Bratislava: Vydavateľstvo TATRAN,2018. 172s. ISBN 978-80-222-0945-8

PERWEJ, Y., AKHTAR, N., PARWEJ, F. 2018. A TECHNOLOGICAL PERSPECTIVE OF BLOCKCHAIN SECURITY. [online] [cit. 03.01.2023]. DOI: 10.24327/ijrsr.2018.0911.2869

Dostupné na internete:
https://www.researchgate.net/publication/329337003_A_Technological_Perspective_of_Blockchain_Security

AL-SHABI, M., AL-QARAFI, A. 2022. Improving blockchain seurity for the internet of things: challenges and solutions. [online] [cit. 03.01.2023].DOI:10.11591/ijece.v12i5.pp5619-5629. Dostupné na internete:
https://www.ijece.iaescore.com/index.php/IJECE/article/view/26459

NABBEN, K., 2021. Blockchain Security as "People Security": Applying Sociotechnical Security to Blockchain Technology. [online] [cit. 03.01.2023]. DOI:
https://doi.org/10.3389/fcomp.2020.599406.
Dostupné na internete: https://www.frontiersin.org/articles/10.3389/fcomp.2020.599406/full

MATTILA, V., 2022. Techniques and Research Direction of Blockchain Security and Privacy. [online] [cit. 04.01.2023]. DOI: 10.37602/IJSSMR.2022.54151 Dostupné na internete:https://www.researchgate.net/publication/365959899_Techniques_and_Research_Direction_of_Blockchain_Security_and_Privacy

LENG, J., ZHOU, M., THAO, J., HUANG, Y., BIAN, Y. 2022. [online] [cit. 08.01.2023]. DOI: 10.1109/TSC.2020.3038641. Dostupné na internete:
https://ieeexplore.ieee.org/document/9271868

SINGH, S., HOSEN, A., YOON, B. 2021. Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network. [online] [cit. 09.01.2023]. DOI: 10.1109/ACCESS.2021.3051602 Dostupné na internete:
https://www.ieeexplore.ieee.org/document/9323061

CHEN,L., JORDAN,S. LIU, Y., MOODY, D., PERALTA, R., PERLNER, R., SMITH-TONE, D. 2016. Report on Post-Quantum Cryptography. [online] [cit. 09.01.2023]. DOI: http://dx.doi.org/10.6028/NIST.IR.8105 Dostupné na internete:
https://www.nvlpubs.nist.gov./nistpubs/ir/2016/NIST.IR.8105.pdf

LIANG,Y. 2019. Blockchain for Dynamic Spectrum Management. [online] [cit. 10.01.2023]. DOI: 10.1007/978-981-15-0776-2_5 . Dostupné na internete:
https://link.springer.com/chapter/10.1007/978-981-15-0776-2_5

WARARKAR, P., KAPIL, N., REHANI, V., MEHRA, Y., BHATNAGAR, Y. 2015. Resolving Problems Based on Peer to Peer Network Security Issue's. [online] [cit.13.01.2023]. DOI: 10.1016/j.procs.2016.02.113. Dostupné na internete:
https://www.sciencedirect.com/science/article/pii/S1877050916001150?via%3Dihub

RAJCANIOVA, M., CIAIAN, P. 2021. Interdependencies between Mining Costs, Mining Rewards and Blockchain Security. [online] [cit. 14.01.2023]. Dostupné na internete:
https://www.researchgate.net/publication/354270393_Interdependencies_between_Mining_Costs_Mining_Rewards_and_Blockchain_Security>

What Is Blockchain Security: Challenges and Examples. [online] [cit. 04.01.2023]. Dostupné na internete: https://www.simplilearn.com/what-is-blockchain-security-and-its-examples-article

Security Tip (ST04-15). [online] [cit. 04.01.2023]. Dostupné na internete: https://www.cisa.gov/uscert/ncas/tips/ST04-015

What Is Peer To Peer Network, And How Does It Work ?. [online] [cit. 04.01.2023]. Dostupné na internete: https://www.blockchain-council.org/blockchain/peer-to-peer-network/

INTRODUCTION TO SMART CONTRACTS. [online] [cit. 04.01.2023]. Dostupné na internete: https://ethereum.org/en/developers/docs/smart-contracts/

Elliptic Curve Cryptography: A Basic Introduction. [online] [cit. 08.01.2023]. Dostupné na internete: https://www.pcrisk.com/removal-guides/12266-blackruby-ransomware/

SHA-256 [online] [cit. 09.01.2023]. Dostupné na internete: https://freemanlaw.com/sha-256/

RIPEMD160 Class. [online] [cit. 09.01.2023]. Dostupné na internete: https://learn.microsoft.com/en-us/dotnet/api/system.security.cryptography.ripemd160?view=netframework-4.8.1

Security Primer – IcedID. [online] [cit. 09.01.2023]. Dostupné na internete: https://www.cisecurity.org/insights/white-papers/security-primer-icedid/

BlackRuby Ransomware. [online] [cit. 09.01.2023]. Dostupné na internete: https://www.pcrisk.com/removal-guides/12266-blackruby-ransomware/

Trojan.SmokeLoader. [online] [cit. 09.01.2023]. Dostupné na internete: https://www.malwarebytes.com/blog/detections/trojan-smokeloader/

Dridex malware. [online] [cit. 09.01.2023]. Dostupné na internete: https://www.techtarget.com/searchsecurity/definition/Dridex-malware/

What CoreBOT malware ?. [online] [cit. 09.01.2023]. Dostupné na internete: https://www.tutorialspoint.com/what-is-corebot-malware/

Cryptography & Challenges posed by Quantum Computers. [online] [cit. 09.01.2023]. Dostupné na internete: https://www.hsc.com/resources/blog/cryptography-challenges-posed-by-quantum-computers/

CRYSTALS Cryptographic Suite for Algebraic Lattices. [online] [cit. 09.01.2023]. Dostupné na internete: https://www.pq-crystals.org/dilithium/index.shtml/

Fast-Fourier Lattice-based Compact Signatures over NTRU. [online] [cit. 09.01.2023]. Dostupné na internete: https://www.falcon-sign.info

SPHINCS+. [online] [cit. 09.01.2023]. Dostupné na internete: https://www.sphincs.org

CRYSTALS Cryptographic Suite for Algebraic Lattices. [online] [cit. 09.01.2023]. Dostupné na internete: https://www.pq-crystals.org/dilithium/index.shtml/

Blockchain Hash Function. [online] [cit. 10.01.2023]. Dostupné na internete: https://www.javatpoint.com/blockchain-hash-function

The Significance Of Nonce In Blockchain [online] [cit. 10.01.2023]. Dostupné na internete: https://101blockchains.com/nonce-in-blockchain/

Merkle Tree in Blockchain: What is it, How does it work and Benefits. [online] [cit. 10.01.2023]. Dostupné na internete: https://www.simplilearn.com/tutorials/blockchain-tutorial/merkle-tree-in-blockchain/

PROOF-OF-STAKE (POS). [online] [cit. 14.01.2023]. Dostupné na internete: https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/>

Proof of Acrivity (PoA) in Blockchain. [online] [cit. 14.01.2023]. Dostupné na internete: https://www.naukri.com/learning/articles/proof-of-activity-in-blockchain/

Proof of Importance (Pol) in Blockchain. [online] [cit. 14.01.2023]. Dostupné na internete: https://www.naukri.com/learning/articles/proof-of-importance-poi-in-blockchain/>

Kontaktné údaje:
Mgr. Andrej Lipták
Akadémia Policajného zboru v Bratislave Sklabinská 1, 835 17 Bratislava
Tel.: +421903440783,
andrej.liptak@akademiapz.sk

Úvod do anonymných sietí - história ich vzniku a základné prvky

Štefan Zachar

Abstrakt: *Autor príspevku sa zameriava na problematiku anonymných sietí. Anonymita je kontroverzný fenomén na webe, pretože je často spájaná s kriminálnou aktivitou alebo s prezeraním nelegálneho obsahu. Avšak, anonymitu využívajú aj jednotlivci, ktorí hľadajú súkromie, ochranu pred sledovaním a možnosť prístupu k informáciám bez obmedzení. Tento článok skúma primárnych používateľov Tor siete, ako aj terminológiu súvisiacu s online anonymitou, vrátane súkromia, anonymity a pseudonymity. Koncept súkromia je definovaný ako schopnosť jednotlivca kontrolovať distribúciu osobných informácií.*

Kľúčové slová: *TOR, cibuľové smerovanie, anonymita, pseudonymita, súkromie*

Abstract*: The author of the article focuses on the issue of anonymous networks. Anonymity is a controversial phenomenon on the web, as it is often associated with criminal activity or viewing illegal content. However, anonymity is also utilized by individuals seeking privacy, protection from surveillance, and the ability to access information without restriction. This paper explores the primary users of the Tor network, as well as terminology related to online anonymity, including privacy, anonymity and pseudonymity. The concept of privacy is defined as an individual's ability to control the distribution of personal information.*

Key words*: TOR, onion routing, anonymity, pseudonymity, privacy*

Úvod

Súčasný dynamický a turbulentný vývoj ľudskej spoločnosti so sebou prináša mnohé pozitívne, ale zároveň aj negatívne skutočnosti, ktoré sa prejavujú v rôznych oblastiach života človeka i celej ľudskej civilizácie. Dôkazom toho sú početné pôvodné i novo sa objavujúce bezpečnostné hrozby a riziká, ktoré oprávnene stavajú otázky bezpečnosti na popredné miesto.[1] Bezpečnosť totiž tvorí základnú a nevyhnutnú podmienku rozvoja každej spoločnosti a dnes, v ére prehlbujúcej sa globalizácie, už neexistuje oblasť spoločenského života, ktorá by s ňou nebola spojená.[2] Aj preto sa snažia všetky štáty, organizácie či akékoľvek iné entity zaistiť svoju bezpečnosť na čo najvyššej úrovni prostredníctvom efektívneho, účelného a najmä funkčného bezpečnostného systému,[3] ktorého neoddeliteľnou súčasťou sú informačné systémy a siete.

V súčasnosti sme svedkami častých útokov na informačné systémy, sociálne siete či informačné služby. Tieto skutočnosti sa do povedomia spoločnosti dostávajú najmä prostredníctvom médií vo verejnoprávnej ale aj súkromnej sfére. Typickým príkladom je konflikt na Ukrajine, ktorý neprebieha len vo fyzickej rovine reálneho sveta ale aj virtuálne v prostredí internetu. V súvislosti s uvedeným sa stretávame s volaním užívateľov po vyššej bezpečnosti či anonymite a práve anonymita je rozporuplný fenomén dnešného WEBu.

Často prevláda v spoločnosti názor, že kto chce byť na WEBe anonymný, robí tak preto aby mohol páchať trestnú činnosť, prípadne prehliadať si stránky s nelegálnym obsahom bez pocitu strachu, že je sledovaný treťou stranou. V tomto prípade sa stretávame najčastejšie s pojmom DARKNET. Toto je však len jedna strana mince. Na tej druhej sú osoby, ktoré

[1] IVANČÍK, R. *Bezpečnosť. Teoreticko-metodologické východiská*. Plzeň : Vydavatelství a nakladatelství Aleš Čeněk, 2022, s. 7

[2] IVANČÍK, R. 2021. Security Theory: Security as a Multidimensional Phenomenon. In *Vojenské reflexie*, 2021, roč. 16, č. 3, s. 32

[3] 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 (v podmienkach bezpečnostných zložiek) : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2019. s. 126

využívajú anonymitu na komunikáciu s okolitým svetom, získavanie citlivých informácií, či len prenášanie citlivých údajov.

Libor Polčák[4] vo svojej technickej správe uvádza, že primárnymi používateľmi siete TOR sú:

- osoby snažiace sa prekonať reštriktívne obmedzenia k prístupu k zahraničným informáciám, ktoré platia v niektorých štátoch v rôznych kútoch sveta,
- osoby snažiace sa o obmedzenie sledovania webovými servermi napr. za účelom cielenia reklamy,
- obeti trestných činov a choré osoby, ktoré sa nechcú o svojom stave zverovať verejne,
- novinári pri vyhľadávaní informácií do článku kvôli zaisteniu anonymity,
- zamestnanci neziskových organizácií pri pripájaní k infraštruktúre svojej organizácie bez toho aby dávali monitorovacím nástrojom vedieť, že sú zamestnanci danej neziskovej organizácie,
- firmy monitorujúce svoju konkurenciu, bez toho aby dávali svojmu konkurentovi informáciu o svojich aktivitách na ich webových stránkach,
- agenti a iné zložky úradov činných v trestnom konaní pri vyšetrovaní a práci v teréne,
- zločinci pro výmenu informácií, alebo páchaní trestnej činnosti.

Napriek rôznorodosti ďalších anonymných sietí je možné konštatovať, že uvedený zoznam typov používateľov je platný aj pre nich.

Terminológia aspektov anonymity

Z pohľadu anonymných sietí je samotná anonymita vyjadrovaná mierou a spôsobom ukrytia identity používateľa. Goldberg[5] vo svojich definíciách rozoberá nasledujúce pojmy:

- súkromie (privacy),
- anonymita (anonymity),
- pseudonymita (pseudonymity),
- dopredné utajenie (forward secrecy) a
- prepojiteľnosť (linkability).

Podobne aj Pfitzman a Hansen[6] vo svojej terminológii o súkromí minimalizáciou údajov uvádzajú termíny:

- anonymita (anonymity),
- neprepojiteľnosť (unlinkability),
- nezistiteľnosť - neodhaliteľnosť (undetectability),
- nesledovateľnosť - nepozorovateľnosť (unobservability),
- pseudonymita (pseudonymity) a
- riadenie identity (riadenie identity).

[4] POLČÁK L. *Základní informace o síti Tor* (online, cit. 7.12.2022). Dostupné na internete: https://www.fit.vut.cz/research/publication-file/11513/tr.pdf

[5] Goldberg, I. A.: A pseudonymous communications infrastructure for the internet. University of California, 2000. (online, cit. 7.12.2022). Dostupné na internete: https://books.google.sk/books/about/A_Pseudonymous_Communications_Infrastruc.html?id=shyfIwAACAAJ&redir_esc=y

[6] Pfitzmann, A.; Hansen, M.: A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management, 2010, (online, cit. 7.12.2022). Dostupné na internete: https://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf

Súkromie je definované ako schopnosť jednotlivca kontrolovať distribúciu informácií o sebe. Goldberg ďalej uvádza, že sa tým nemyslí skutočnosť, že nikdy nedôjde j odhaleniu osobných informácií, ale skôr je tým myslené že systém ako taký rešpektuje právo jednotlivca rozhodnúť sa aké informácie o ňom budú poskytnuté a rovnako aj to komu budú poskytnuté. Za informácie o jednotlivcovi pritom môžeme považovať prakticky akúkoľvek informáciu, ktorá sa týka jeho osoby – napríklad bydlisko, vek, zvyky, emailovú adresu, IP-adresu a podobne. V Slovenskej republike je definícia osobných údajov zakotvená v zákone 18/2018 Z. z. článok 1. § 2 *„Osobnými údajmi sú údaje týkajúce sa identifikovanej fyzickej osoby alebo identifikovateľnej fyzickej osoby, ktorú možno identifikovať priamo alebo nepriamo, najmä na základe všeobecne použiteľného identifikátora, iného identifikátora, ako je napríklad meno, priezvisko, identifikačné číslo, lokalizačné údaje,1) alebo online identifikátor, alebo na základe jednej alebo viacerých charakteristík alebo znakov, ktoré tvoria jej fyzickú identitu, fyziologickú identitu, genetickú identitu, psychickú identitu, mentálnu identitu, ekonomickú identitu, kultúrnu identitu alebo sociálnu identitu.“*[7]

Anonymita a pseudonymita sú podľa Goldberga[8] dve formy súkromia identity aj keď často sú obe označované ako anonymita. Rozdiel je v tom či systém umožňuje používanie pseudonymov, a zároveň či osoba pseudonym používa. Za pseudonym považujeme perzistentnú virtuálnu identitu používateľa, ktorá s však nie je jeho fyzickou identitou. Dá sa teda povedať, že pseudonym je identifikátor subjektu, ktorý nie je jeho skutočným menom.[9] Pri komunikácii však vieme, že komunikujeme vždy s tou istou osobou. Systém, ktorý je výlučne anonymný neumožňuje zachovávanie takéhoto perzistentného identifikátora neexistuje teda spôsob ako zistiť, či napríklad pri komunikácii komunikujeme s tou istou osobou alebo nie.

Z uvedeného vyplýva aj používanie pojmov **prepojiteľnosť a neprepojiteľnosť**. Môžeme ich považovať za skutkový stav, ktorý vyjadruje či môžeme alebo nemôžeme nájsť alebo vytvoriť vzťah medzi takými identifikátormi subjektu, ktoré by umožnili jeho jednoznačnú identifikáciu. Prepojiteľnosť teda znamená možnosť takéto vzťahy v rámci systému nájsť alebo vytvárať, a neprepojiteľnosť je jej negáciou.

Neodhaliteľnosť a nepozorovateľnosť zase určujú, či je možné v rámci komunikácie rozlíšiť existenciu identifikárorov subjektu a ich možné sledovanie.

Dopredné utajenie znamená nemožnosť odhaliť identifikátory subjektu potom ako odoslal správu napríklad tým, že systém neudržiava záznamy o transakciách počas komunikácie.[10]

Riadenie identity znamená správu čiastočných identít – pseudonymov subjektu v zmysle ich používania v konkrétnom kontexte alebo úlohe[11].

---

[7] zákon 18/2018 Z. z. článok 1. § 2 . (online, cit. 7.12.2022). Dostupné na internete: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/18/

[8] Goldberg, I. A.: A pseudonymous communications infrastructure for the internet. Dizertacní práce, University of California, 2000 – 16 strana (online, cit. 7.12.2022). Dostupné na internete: https://books.google.sk/books/about/A_Pseudonymous_Communications_Infrastruc.html?id=shyfIwAACAAJ&redir_esc=y

[9] Pfitzmann, A.; Hansen, M.: A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management, 2010, (online, cit. 7.12.2022). Dostupné na internete: https://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf strana 21

[10] Zdeňek Coufal,Libor Polčák Anonymizační síť Tor Technická zpráva č. FIT-TR-2014-02 (online, cit. 7.12.2022). Dostupné na internete: https://www.fit.vut.cz/research/publication-file/10626/tr.pdf

[11] Pfitzmann, A.; Hansen, M.: A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management, 2010, (online, cit.

Hlavný problém anonymity a pseudonymity v prostredí počítačových sietí sú IP adresy. Tieto fungujú ako identifikátory a za určitých okolností[12] umožňujú odhaliť umiestnenie koncového zariadenia. V kombinácii s ďalšími identifikátormi naviazanými na koncové zariadenie je možné určiť identitu používateľa a tým pádom dochádza k de-anonymizácii.

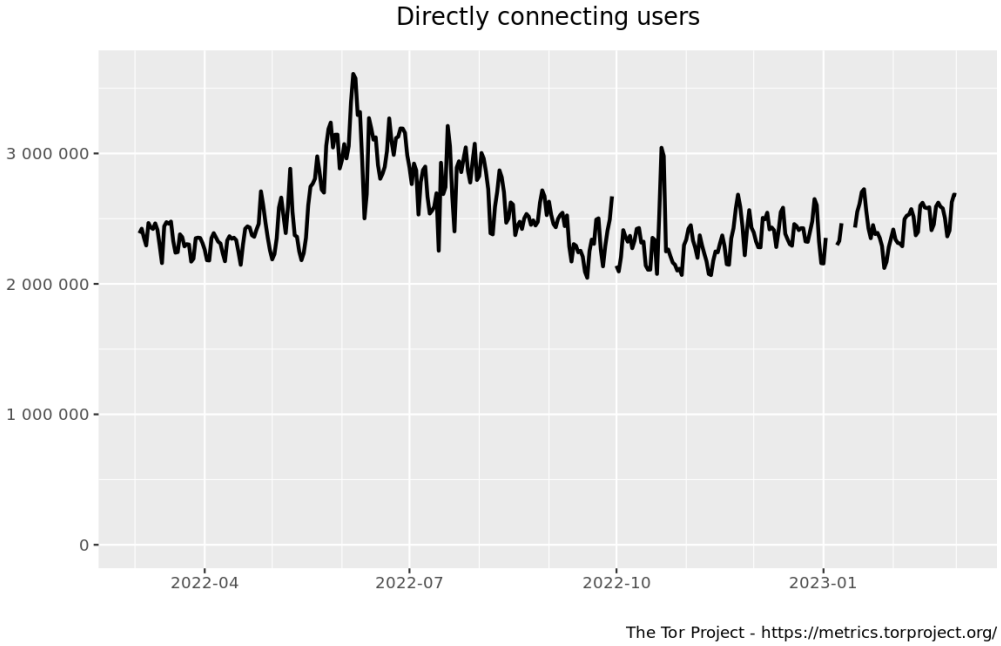
Prostredie DARKNET

Prostredie DARKNET je tvorené rôznymi anonymnými sieťami, ktorých spoločným cieľom je anonymizácia účastníkov konkrétnych sietí. Anonymizácia je dosahovaná sofistikovanými metódami komunikácie v anonymizačných sieťach, ktoré rozširujú možnosti tradičného komunikačného protokolu TCP/IP.

Najčastejšie používanými anonymizačnými sieťami sú

- TOR (The Onion Router)
- I2P (Invisible Internet Project)
- FREENET
- Zero net a mnohé ďalšie

Napriek existencii väčšieho množstva anonymných sietí, najpoužívanejšou je sieť TOR. Podľa oficiálnej metriky siete TORpripojených používateľov bolo za posledný rok pripojených od 2 do 3,6 milióna používateľov. Naproti tomu v sieti I2P je pripojených pomerne stabilných



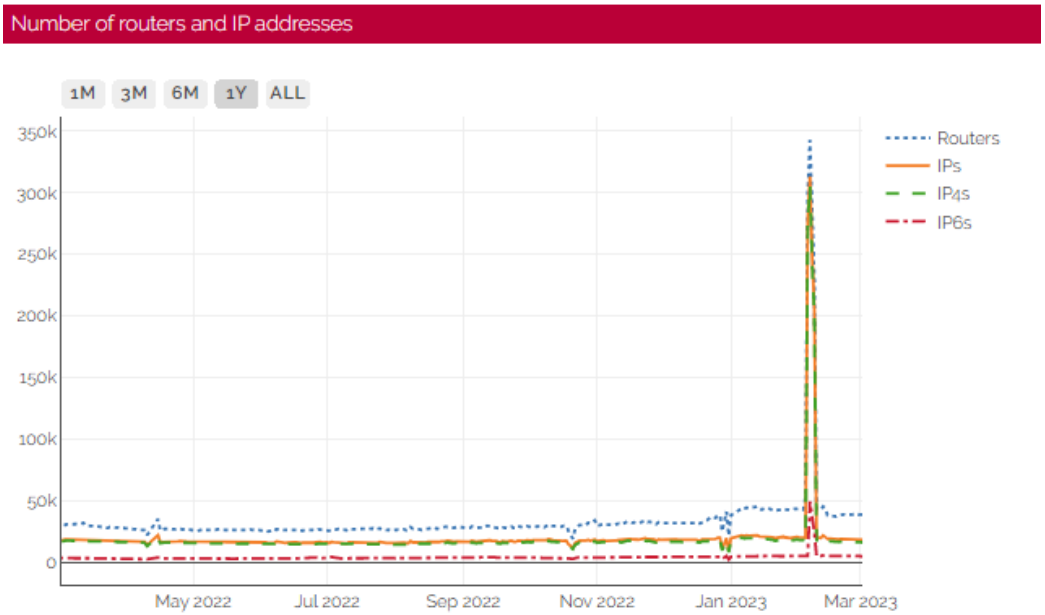
Obr. 1: Veľkosť siete tor z pohľadu pripojených používateľov, Zdroj: TOR Metrics

7.12.2022). Dostupné na internete: https://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf strana 33

[12] Zistenie konkrétneho umiestnenia IP adresy v sieti je závislé na používanom štandarde a zvolenom postupe. Štandard IPV4 je orientovaný na počítačovú sieť, takže presné učenie konkrétneho koncového zariadenia je možné len v rozsahu IP adries konkrétnej siete v ktorej sa koncové zariadenie nachádza. Mimo tejto siete je viditeľná len verejná IP adresa routra pripojeného do tejto siete. Pri štandarde IPV6 ktorá je orientovaná na koncové zariadenia by toto malo byť lokalizovateľné z akéhokoľvek miesta v sieti.

15 – 20 tisíc IP adries. Na pripojenom grafe však môžeme vidieť aj anomáliu zobrazujúcu krátkodobý skokový nárast na hodnotu viac ako 300 000 IP adries počas intervalu 4.2. – 9.2. 2023.

Ďalšie spomínané anonymné siete stránky s oficiálnymi metrikami parametrov jednotlivých prvkov siete neposkytujú, avšak existuje niekoľko prípadových vedeckých štúdií ohľadom štatistík v sieti freenet[13] aj ZeroNet[14].



Obr. 2: Veľkosť siete I2P z pohľadu pripojených používateľov, Zdroj: I2P Metrics

Značné rozdiely v počte používateľov v prospech siete TOR môže ovplyvňovať niekoľko faktorov:

- **Široká podpora a popularita:** Sieť Tor je najviac známou anonymizačnou sieťou a má širokú podporu od mnohých organizácií, ako napríklad Electronic Frontier Foundation a The Tor Project, ktoré sa snažia zlepšovať a propagovať sieť Tor. Táto popularita môže priviesť viac používateľov do siete.
- **Jednoduchosť použitia:** Sieť Tor má relatívne jednoduché používateľské rozhranie a je ľahká na inštaláciu a použitie, čo môže prilákať používateľov, ktorí nemajú technické znalosti.
- **Veľké množstvo výstupných uzlov:** Sieť Tor má veľké množstvo výstupných uzlov, ktoré môžu byť použité na prehliadanie webu a prístup k iným službám. Toto množstvo

[13] Roos, S., Shiller, B., Hacker, S., Strufe, T., Measuring Freenet in the Wild: Censorship-resilience under Observation (online, cit. 7.12.2022). Dostupné na internete: https://petsymposium.org/2014/papers/paper_71.pdf

[14] Wang, S., Gao, Y., Shi, J., Wang, X., Zhao, C., Yin, Z. (2020). Look Deep into the New Deep Network: A Measurement Study on the ZeroNet. In: , et al. Computational Science – ICCS 2020. ICCS 2020. Lecture Notes in Computer Science(), vol 12137. Springer, Cham. (online, cit. 7.12.2022). Dostupné na internete: https://doi.org/10.1007/978-3-030-50371-0_44

výstupných uzlov umožňuje rýchlejší prístup k obsahu a môže prilákať viac používateľov.

- **Všeobecné využitie:** Sieť Tor je často využívaná na prístup k cenzurovanému obsahu, k ochrane súkromia a bezpečnosti a na iné účely, ktoré súvisia s anonymitou. Táto široká paleta využitia môže prilákať rôznych používateľov, ktorí hľadajú rôzne riešenia pre svoje potreby.

Naproti tomu napríklad siete Freenet a I2P sú skôr komunitné, neobsahujú výstupné body ktoré by umožňovali prehliadanie webu so skrytou IP adresou ako je to v prípade siete TOR. So sieťou Tor ich však spájajú nasledujúce vlastnosti:

- **Bezpečnosť:** anonymné siete ponúkajú vysokú mieru bezpečnosti a súkromia, čo je obzvlášť dôležité pre používateľov, ktorí sa snažia ochrániť svoje dáta pred sledovaním a monitorovaním.
- **Anonymita:** základná vlastnosť vlastná všetkým anonymným sieťam umožňuje používateľom anonymný prístup k obsahu a službám, čo je užitočné pre používateľov, ktorí sa snažia vyhnúť sa cenzúre a obmedzeniam v slobode prejavu.
- **Decentralizovaná architektúra:** anonymné siete sú založené na decentralizovanej architektúre, čo znamená, že obsah a služby sú distribuované medzi mnoho uzlov a serverov. Táto architektúra umožňuje väčšiu odolnosť voči útokom a cenzúre.
- **Vysoká odolnosť voči útokom:** Anonymné siete a zvlášť Freenet a I2P sú navrhnuté tak, aby boli odolné voči rôznym druhom útokov, ako sú DDoS útoky a útoky typu "man-in-the-middle".
- **Možnosť hosťovať obsah:** tak ako v bežných počítačových sieťach anonymné siete rovnako umožňujú prevádzkovanie webových služieb s vlastnými koreňovými DNS úrovňami .onion (Tor), i2p, freenet. Používatelia anonymných sietí môžu hosťovať svoj vlastný obsah a zdieľať ho s ostatnými používateľmi siete. Toto je užitočné pre používateľov, ktorí sa snažia zdieľať obsah, ktorý by inak bol zakázaný alebo cenzurovaný.

Na základe uvedeného môžeme konštatovať, že sieť TOR je najrozšírenejšou anonymnou počítačovou sieťou.

História vzniku siete TOR

Za predchodcu siete Tor je považovaná sieť Mixnet[15]. Je to počítačový systém založený na sieti počítačov, ktoré umožňujú súkromnú a bezpečnú komunikáciu medzi viacerými stranami. Mixnet je navrhnutý tak, aby umožnil odosielateľovi poslať správu s náhodným výberom náhodných serverov (mixov) v sieti, ktoré následne správu opakovane a náhodne premiešajú pred odoslaním prijímateľovi.

Mixnet tak zabezpečuje súkromie a anonymitu komunikácie tým, že sťažuje alebo úplne znemožní sledovanie správ a prepojenie odosielateľov a prijímateľov.

[15] Danezis, G., Mix-Networks with restricted routes, (online, cit. 7.12.2022). Dostupné na internete: https://books.google.sk/books?id=x2OnhrVLMX0C&pg=PA1&redir_esc=y#v=onepage&q&f=false

Mixy prijímajú správy od viacerých klientov, zamiešajú ich a v určitých intervaloch takto vytvorenú dávku spolu s výplňovými správami preposielajú ďalej. Dĺžka každého kola je určená algoritmom, ktorý berie do úvahy prahovú hodnotu založenú na počte prijatých správ v vyrovnávacej pamäti alebo na časovači, alebo ich kombináciu.

Tento spôsob doručovania správ v systéme Mix-Net zaručuje, že okrem odosielateľa a adresáta pozná každý uzol na ceste len predchádzajúci a nasledujúci uzol v anonymizačnej sieti. Preposielajúce uzly tak nemajú možnosť zistiť identitu komunikujúcich strán. Posledný uzol v anonymizačnej sieti však môže odhadnúť, že je posledný a pozorovať obsah pôvodnej správy. Tento systém však znevýhodňovala veľmi vysoká latencia odosielaných správ.

Tento problém mal vyriešiť systém Onion Routing ako obecné riešenie na anonymizáciu spojení pre rôzne aplikácie, vrátane HTTP, FTP, SMTP a telnetu. Tento systém je založený na predpoklade že existuje známa sieť anonymizujúcich staníc s dostupnými verejnými kryptografickými kľúčmi. Zdroj komunikácie vytvorí virtuálny okruh pomocou štruktúry cibule, ktorá určuje cestu k cieľu vo vrstvách.

Smerovače Onion Routing udržujú medzi sebou TCP/IP spojenia a vytvárajú topológiu Onion Routing siete. Informácie o aktuálnom stave siete (topológii) sa šíria cez všetky aktívne smerovače a používateľské proxy.

V porovnaní s Mix-Netom, ktorý vyžadoval, aby používateľ vytvoril pre každú odosielanú správu samostatnú cibuľu a používal často operácie asymetrickej kryptografie, je Onion Routing vhodnejší pre interaktívne aplikácie. Mix-Net bol vhodnejší pre prípad komunikácie cez e-mail.

Do praxe sa však dostala až ďalšia generácia systému onion routing s niekoľkými vylepšeniami známa pod názvom Tor.

Podľa popisu histórie vzniku siete Tor na oficiálnych stránkach www.torproject.org[16] sa Projekt Tor, Inc. stal neziskovou organizáciou v roku 2006. Avšak koncepcia "cibulového smerovania" má počiatky už v 90. rokoch. Vývojári, výskumníci a zakladatelia, ktorí umožnili Tor, zdieľajú spoločné presvedčenie o súkromnom prístupe k necenzurovanému internetu pre všetkých jeho používateľov.

Nakoľko sa v 90. rokoch objavili obavy o bezpečnosť a sledovanie na internete, výskumníci z U.S. NRL[17] vytvorili v roku 1995 prvý návrh cibuľového smerovania, aby používateľom umožnili súkromnejšie a bezpečnejšie používanie internetu. Idea spočívala v smerovaní dátového toku cez viacero šifrovaných serverov. Tento princíp stále predstavuje jednoduchý spôsob ako vysvetliť fungovanie siete Tor.

Princípy siete TOR

Sieť Tor je takzvaná overlay network teda sieť, ktorá je vytvorená nad existujúcou sieťou, nazývanou aj underlay network. Overlay sieť sa tvorí pomocou softvérových alebo hardvérových prostriedkov, ktoré umožňujú virtuálnu komunikáciu medzi zariadeniami a

[16] História siete TOR (online, cit. 17.11.2020). Dostupné na internete: https://www.torproject.org/about/history/
[17] U.S. Naval Research Lab

uzlami, ktoré tvoria túto sieť. Jedno takéto riešenie je práve sieť Tor. Ako ďalšie môžeme spomenúť VPN (Virtual Private Petwork[18]) alebo SDN (Software Defined Networking[19]).

Základnými komponentami siete Tor sú[20]:

- **Onion routers** – smerovače vytvárajú topológiu siete a sú hlavným prvkom technológie "onion routing", ktorá posiela dáta cez viacero náhodne vybraných smerovačou (nazývaných aj relays alebo uzky) poznáme tri typy:
    - guards – vstupné smerovače,
    - middle – prostredné smerovače,
    - exits – výstupné smerovače
- **Onion proxy** - získava informácie o aktuálnom stave a topológii siete Tor z adresárových serverov. Následne vytvára virtuálne okruhy a riadi prenos dátových tokov medzi užívateľskými aplikáciami a sieťou Tor. Tento program sa obvykle spúšťa na zariadeniach koncových používateľov.,
- **Directory servers** - servery, ktoré uchovávajú informácie o topológii a stave siete Tor, vrátane informácií o uzloch v sieti. Tieto servery poskytujú klientským programom dôležité informácie, ktoré potrebujú pre spojenie do siete Tor.,
- **Hidden services** - mechanizmus skrytých služieb, ktorý umožňuje serverom poskytovať služby anonymne bez odhalenia ich identity. Tieto služby sú prístupné pomocou upravených doménových mien v rámci siete Tor a sú hostované na sieťových uzloch, ktoré sú tiež súčasťou siete Tor.
- **Bridges** – mosty sú uzly v sieti Tor, ktoré sú používané na obchádzanie cenzúry a blokovania siete Tor. Tieto uzly nie sú tajné a ich adresy nie sú verejne dostupné, čo umožňuje používateľom v obmedzených alebo cenzurovaných oblastiach pripojiť sa k sieti Tor a získať anonymitu.
- **Pluggable transports** - mechanizmy v sieti Tor, ktoré umožňujú skryť prevádzku siete Tor pred cenzúrovacími systémami, ktoré sa snažia detegovať a blokovať takéto prevádzky. Tieto mechanizmy pracujú na úrovni prenosových protokolov a umožňujú používateľom pripojenie sa k sieti Tor prostredníctvom rôznych šifrovacích techník a protokolov, ako napríklad SSL alebo SSH. Pluggable transports sú dôležitým prvkom siete Tor pre zabezpečenie anonymného a slobodného prístupu k informáciám pre používateľov v obmedzených a cenzurovaných oblastiach.

[18] Virtuálna súkromná sieť - VPN je sieťová technológia, ktorá umožňuje vytvoriť súkromné a zabezpečené spojenie medzi dvoma bodmi cez verejnú sieť, ako je napríklad internet. VPN technológia umožňuje, aby sa dáta prenášali medzi týmito bodmi bezpečne, šifrovane a anonymne.

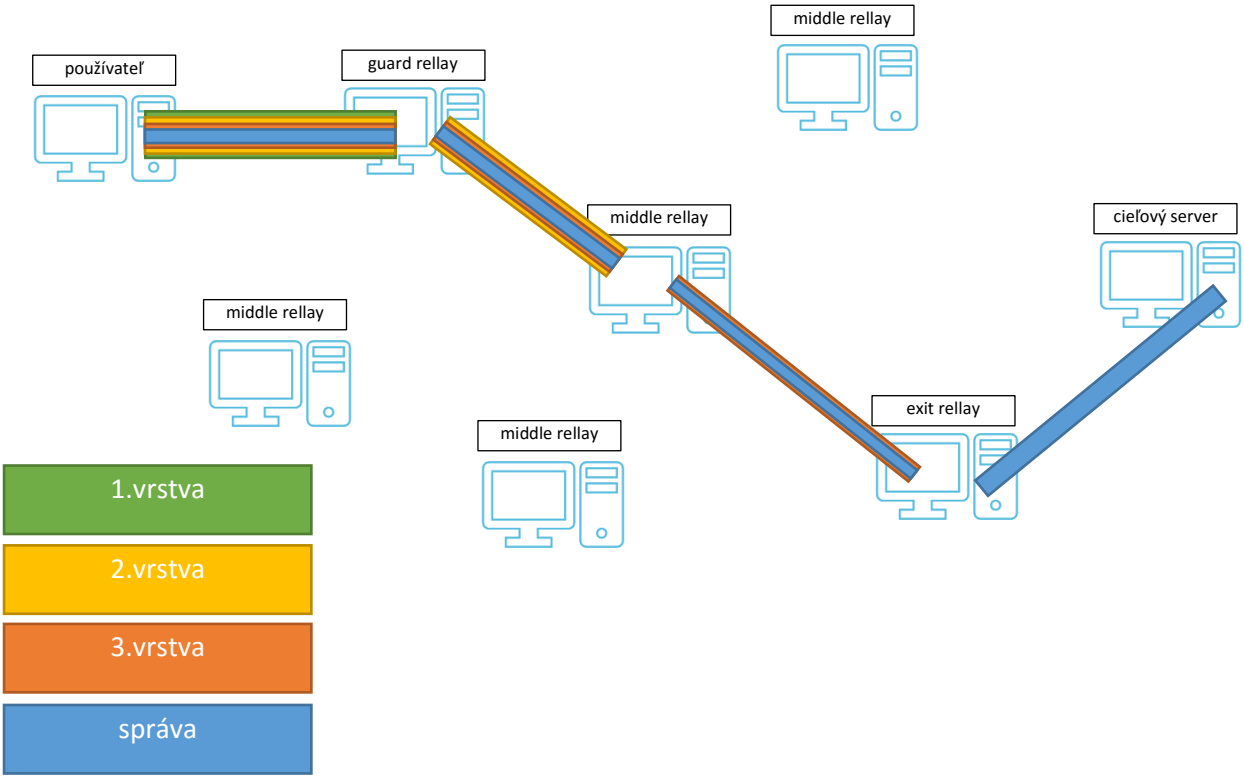
[19] Software-Defined Networking je architektúra siete, ktorá oddeluje riadenie siete od fyzickej infraštruktúry. V tradičných sieťach sú riadiace a prenosové funkcie väčšinou zapojené do jednotlivých sieťových zariadení, ako sú napríklad prepínače a smerovače. V SDN sa riadiace funkcie sieťových zariadení oddelia od prenosových funkcií a prenesú sa na centrálne umiestnený riadiaci server, ktorý môže využívať programovateľné rozhrania na konfiguráciu a riadenie celej siete.

[20] Coufal. Z., Polčák. L., Anonymizační síť, Fakulta informačních technologií VUT v Brně, (online, cit. 7.12.2022). Dostupné na internete: https://www.fit.vut.cz/research/publication/10626/.cs?years=20&author=pol%C4%8D%C3%A1k

- **Users** - používatelia využívajúci služby siete Tor. Môžeme ich deliť na používateľov s priamym prístupom cez vstupné uzly a na používateľov s nepriamym prístupom cez mosty

Princíp onion routing (cibuľového smerovania)

V Onion Routing sú pakety rozdelené na malé kúsky a prenášajú sa cez sieť Tor v kryptovaných vrstvách nazývaných "onion". Keď sa paket dostane do siete Tor, prechádza cez viaceré náhodne vybrané uzly, ktoré sú nazývané "relays" a ktoré odhaľujú vrstvu za vrstvou. Každý relay odhaľuje iba jednu vrstvu kryptovania, čím umožňuje paketu pokračovať v ceste cez sieť Tor. Po prejdení série uzlov a odstránení kryptovania, paket dorazí k určenej destinácii. Týmto spôsobom je zabezpečená anonymita prenosu, pretože každý uzol vidí iba predchádzajúci a nasledujúci uzol v prenose, ale nemá informáciu o pochádzajúcom a cieľovom uzle.



Obr. 3: Systém cibuľového smerovania, Zdroj: vlastné spracovanie

Záver

Je nesporné, že potreba odhaľovania nelegálnej či trestnej činnosti v prostredí DARKNETu je aktuálna téma, ktorej riešenie je vzhľadom na vysokú úroveň anonymizácie veľmi problematické až nereálne. Z uvedeného dôvodu je dôležité definovanie postupov, ktoré by umožnili identifikovať prvky nelegálnej činnosti nepriamo za pomoci digitálnych stôp zanechávaných v prostredí DARKNETu.

Za digitálne stopy v kontexte obsahu DARKNETu môžeme považovať napríklad adresy peňaženiek kryptomien, osobné identifikačné údaje, audiovizuálne dátové objekty, dátové štruktúry určujúce alebo opisujúce čas, miesto, objekt, dej alebo iné.

Nepriamou identifikáciou v kontexte DARKNETu je myslené vyhľadávanie digitálnych stôp v prostredí DARKNETU a ich komparácia s už známymi digitálnymi stopami, alebo tiež odhaľovanie nových digitálnych stôp prostredníctvom dataminingu. Zhromažďovanie takých dátových štruktúr, ktorých výskyt je v prostredí DARKNETu pravdepodobné.

Zoznam použitej literatúry:

IVANČÍK, R. *Bezpečnosť. Teoreticko-metodologické východiská*. Plzeň : Vydavatelství a nakladatelství Aleš Čeněk, 2022, s. 7

IVANČÍK, R. 2021. Security Theory: Security as a Multidimensional Phenomenon. In *Vojenské reflexie*, 2021, roč. 16, č. 3, s. 32

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 (v podmienkach bezpečnostných zložiek) : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2019. s. 126

POLČÁK L. *Základní informace o síti Tor* (online, cit. 7.12.2022). Dostupné na internete: https://www.fit.vut.cz/research/publication-file/11513/tr.pdf

GOLDBERG, I. A.: A pseudonymous communications infrastructure for the internet. University of California, 2000. (online, cit. 7.12.2022). Dostupné na internete: https://books.google.sk/books/about/A_Pseudonymous_Communications_Infrastruc.html?id=shyfIwAACAAJ&redir_esc=y

PFITZMANN, A.; HANSEN, M.: A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management, 2010, (online, cit. 7.12.2022). Dostupné na internete: https://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf

COUFAL, Z., POLČÁK, L.,Anonymizační síť Tor Technická zpráva č. FIT-TR-2014-02 (online, cit. 7.12.2022). Dostupné na internete: https://www.fit.vut.cz/research/publication-file/10626/tr.pdf

ROOS, S., SHILLER, B., HACKER, S., STRUFE, T., Measuring Freenet in the Wild: Censorship-resilience under Observation (online, cit. 7.12.2022). Dostupné na internete: https://petsymposium.org/2014/papers/paper_71.pdf

WANG, S., GAO, Y., SHI, J., WANG, X., ZHAO, C., YIN, Z. (2020). Look Deep into the New Deep Network: A Measurement Study on the ZeroNet. In: , et al. Computational Science – ICCS 2020. ICCS 2020. Lecture Notes in Computer Science(), vol 12137. Springer, Cham. (online, cit. 7.12.2022). Dostupné na internete: https://doi.org/10.1007/978-3-030-50371-0_44

DANEZIS, G., Mix-Networks with restricted routes, (online, cit. 7.12.2022). Dostupné na internete: https://books.google.sk/books?id=x2OnhrVLMX0C&pg=PA1&redir_esc=y#v=onepage&q&f=false

História siete TOR (online, cit. 17.11.2020). Dostupné na internete: https://www.torproject.org/about/history/

zákon 18/2018 Z. z. článok 1. § 2 . (online, cit. 7.12.2022). Dostupné na internete: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/18/

Kontakt
Mgr. Štefan Zachar, PhD.
Katedra informatiky a manažmentu
Akadémia Policajného zboru v Bratislave
e-mail: stefan.zachar@akademiapz.sk

Analýza stratégie študentov pri overovaní vedomostí elektronickou formou testovania

Štefan Zachar

Anotácia: *Autor príspevku, prináša informácie o stratégii, aká je študentami používaná pri overovaní nadobudnutých vedomostí prostredníctvom elektronickej formy testovania. Opisuje zmeny stratégií pri vybraných študentoch, ktorí neuspeli na riadnom a ani prvom opravnom termíne, teda absolvovali tri skúšky prostredníctvom elektronického testovania. Overovanie vedomostí bolo realizované prostredníctvom testovacieho softvéru TCExam využívanej vo vyučovacom procese predmetu Informatika.*

Kľúčové slová: *vzdelávanie, overovanie vedomostí, TCExam,*

Annotation: *The author of the article provides information about the strategy used by students for verifying acquired knowledge through electronic testing. The article describes changes in strategies used by selected students who did not pass the regular or first make-up exam, and therefore completed three exams through electronic testing. The verification of knowledge was carried out using the TCExam testing software used in the teaching process of the subject of Computer Science.*

Keywords: *education, knowledge verification, TCExam,*

Úvod

Aplikácia automatizovaného systému na overovanie vedomostí nie je nová myšlienka a prvé zmienky o štandardizovaných testoch siahajú do obdobia dynastie HAN (260BC - AD220) v Číne kde boli využívané na overovanie znalostí kandidátov na úradnícke posty impéria[1]. Vo všeobecnosti môžeme overovanie vedomostí prostredníctvom štandardizovaných testov považovať za jeden z viacerých postupov riešiacich problematiku vzťahov medzi množinou vedomostí obsiahnutých vo vzdelávacom procese a jej podmnožinou tvorenou vedomosťami, ktoré si študent osvojil.

Podľa Turka2 sa vyučovací proces skladá z dvoch na sebe závislých činností a to zisťovania výsledkov vyučovacieho procesu a posúdenie výsledkov vyučovacieho procesu.

Rafajlovičová a Štulrajterová3 uvádzajú, že overovanie výsledkov edukačného procesu sa rrealizuje skúšaním a hodnotením, pričom výsledky sa posudzujú vzhľadom na stanovené krátkodobé a dlhodobé ciele. Predmetom tejto kontroly je práca študentov a učiteľov.

Elektronický systému overovania vedomostí prináša iný pohľad na systém skúšania a preverovania študentov. Nemá byť náhradou za štandardné ústne skúšky alebo písomné testy, ale možnou alternatívou, kedy je vykonanie iných foriem overovania vedomostí menej vhodné. Typickým príkladom bola situácia ovplyvnená pandémiou Covid-19, keď online forma

---

[1] Özturgut, O., Standardized Testing In The Case Of China And The Lessons To Be Learned For The U.S., (online, cit. 17.12.2021). Dostupné na internete: https://www.researchgate.net/publication/298911898_Standardized_Testing_In_The_Case_Of_China_And_The_Lessons_To_Be_Learned_For_The_US

[2] TUREK I. 1998: Zvyšovanie efektívnosti vyučovania. - Združenie pre vzdelávanie EDUKÁCIA, Bratislava, 1998. - 2. dopln. vyd. - 326 s. ISBN 80-88796-89-X strana 255

[3] RAFAJLOVIČOVÁ, R., ŠTULRAJTEROVÁ,M., 2002. Skúšanie, testovanie a hodnotenie v edukačnom procese. Bratislava: Štátny pedagogický ústav. 2002, 53s, ISBN 80-8575-667-6, (online) (online, cit. 20.12.2021), Dostupné na internete: https://encyklopediapoznania.sk/data/eknihy/pedagogika2/skusanie_testovanie.pdf strana 4

elektronického systému overovania vedomostí je prakticky jedinou možnosťou ako overiť úroveň nadobudnutých vedomostí študentov.

Uvedený spôsob overovania vedomostí tvorí súčasť vzdelávacieho procesu pri vyučovaní predmetov na katedre informatiky a manažmentu. Využitie jeho analytických možností nám umožňuje precizovanie a kontrolu smerovania vzdelávacieho procesu a teda zvyšovanie úrovne informatického povedomia študentov.

Výber softvéru

Dôležitým aspektom pri elektronickom overovaní nadobudnutých vedomostí je výber správneho softvérového riešenia. V našom prípade sme hľadali softvér, ktorý spĺňa nasledujúce požiadavky:

- Softvér typu klient – server, nakoľko toto riešenie umožňuje jednoduchú manipuláciou s pripravovanými otázkami, testami a aj výsledkami testov z jedného počítača v sieti.
- Možnosť vytvárať databázy otázok pre rôzne predmety a rovnako aj možnosť kategorizovania otázok v rámci jednotlivých predmetov. Takáto databáza otázok značne uľahčuje vytváranie alebo generovanie jednotlivých testov.
- Vytváranie otázok rôzneho typu. Napríklad:
  - Výber jednej správnej odpovede z viacerých odpovedí,
  - Výber viacerých správnych odpovedí z viacerých odpovedí,
  - Určenie správneho poradia.
- Využitie grafických objektov v otázkach.
- Vytváranie jedinečných testov. Jedinečné testy sú pri overovaní získaných vedomostí veľmi dôležité. Takto sú eliminované príležitosti na odpisovanie prípadne iné formy podvádzania.
- Generovanie prehľadných výsledkov testovania. Takéto výsledkové tabuľky by mali obsahovať všetky potrebné informácie na určenie dosiahnutého stupňa ohodnotenia. S tým je spojené aj štatistické vyhodnocovanie výsledkov.

Pre účely tejto analýzy sme sa rozhodli použiť testovací softvér TCExam[4]. Je to Open Source systém na elektronické overovanie nadobudnutých vedomostí známe aj ako CBA – Computer-Based Asseessment, CBT – Computer-Based Testing alebo E-Exam. Jeho zameranie je teda generovať študijné testy, plánovať testovanie, manažovať používateľov a zároveň pomáhať pri analýze zistených výsledkov. Pri inštalácii na server s aktívnym mailovým serverom umožňuje pedagógovi doručovať výsledky testov, skúšok alebo kvízov.

Program je webovo orientovaný, platformne nezávislý a vytváraný v súlade s pokynmi organizácie W3C. Je to výhradne sieťová verzia klient / server, pričom na strane klienta nie je potrebná inštalácia žiadneho softvéru len prítomnosť web prehliadača štandardu XHTML 1.0 čo dnes prakticky spĺňa akýkoľvek prehliadač na ktorejkoľvek platforme či už po hardvérovej alebo softvérovej stránke. Vyvíjaný je na populárnej platforme LAMP a spĺňa nami požadované parametre.

[4] TCExam (online, cit. 20.12.2021), Dostupné na internete: https://tcexam.org/

Parametre analýz

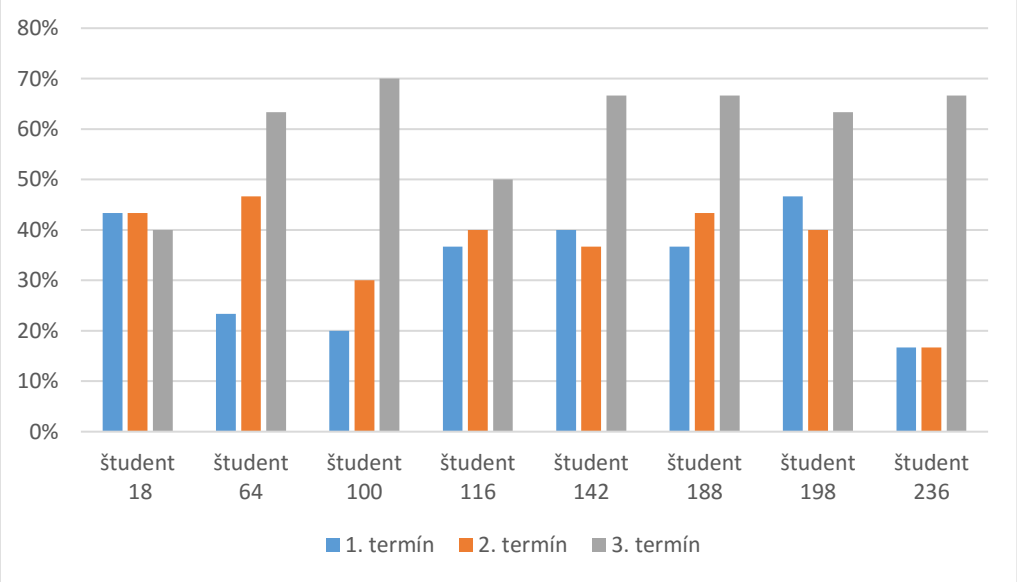
Pre potreby našich analýz sme použili výstupné údaje testovacieho softvéru TCExam. Testy boli aplikované u študentov prvého ročníka v predmete Informatika I. Boli generované z databázy otázok rozdelenej do ôsmych tematických celkov s celkovým počtom 166 otázok. Každý test obsahoval 30 otázok a bol časovo obmedzený na 25 minút. Minimálny počet otázok potrebných na splnenie testu bol 16.

Z výstupných zostáv sme vykonali niekoľko analýz. V tomto článku uvádzame analýzu týkajúcu sa otázky, či je možné analýzou získaných údajov zistiť stratégiu študenta pri overovaní vedomostí. Analyzovali sme výsledky študentov, ktorí boli najmenej úspešní, teda absolvovali viac testov (tri skúšobné termíny) po sebe. Zároveň sne analyzovali, aký vplyv má na výsledky testovania doba medzi dvomi testami.

Porovnanie výsledkov jednotlivých termínov

V tejto analýze, sme hľadali podobnosť v súbore otázok a ich riešení u študentov, ktorí absolvovali tri termíny skúšok, teda boli úspešní až na tretí krát, prípadne sa o ďalšiu skúšku nepokúsili. Analyzovali sme akademický rok 2021/2022.

V tomto akademickom roku absolvovali tri termíny postupových skúšok v predmete Informatika I. ôsmi študenti. Z dôvodu ochrany osobných údajov sú ich mená nahradené slovom študent a poradovým číslom v databáze študentov.



Graf 1: Úspešnosť študentov na 1. - 3. termíne skúšok v AR 2021/2022
Zdroj: Vlastné spracovanie

Ako prvé sme vykonali porovnanie stúpajúceho alebo klesajúceho trendu úspešnosti pri jednotlivých termínoch skúšok.

Z uvedeného grafu a tabuľky môžeme vidieť, že študent 18 nijako nereflektoval na výsledky skúšok kedy na prvý a druhý termín dosiahol rovnaký výsledok a tretí termín pozorujeme dokonca zhoršenie výsledku.

Tabuľka 1: Úspešnosť študentov na 1. - 3. termíne skúšok v AR 2021/2022
Zdroj: Vlastné spracovanie

Termín\študent	študent 18	študent 64	študent 100	študent 116	študent 142	študent 188	študent 198	študent 236
1. termín	43%	23%	20%	37%	40%	37%	47%	17%
2. termín	43%	47%	30%	40%	37%	43%	40%	17%
3. termín	40%	63%	70%	50%	67%	67%	63%	67%

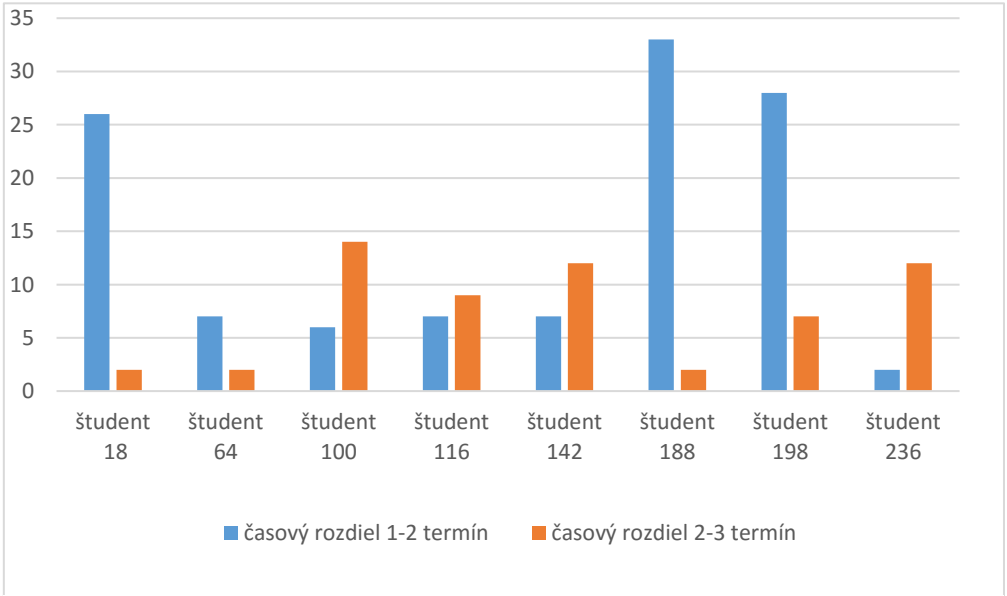
V prípade študentov 142, 198 a 236 môžeme pozorovať zvýšenú reflexiu až po druhom termíne skúšok, pričom prvé skúšky nezaznamenali žiadny progres a v prípade študentov 142 a 198 zhoršenie výsledku. Spomínaný študent 236 je zaujímavý z toho hľadiska, že na prvých dvoch termínoch dosiahol najnižšie hodnotenie, no na tretí termín skúšok dosiahol druhé najlepšie hodnotenie z uvedenej skupiny spolu so študentmi 142 a 188. V tomto prípade by sme mohli hovoriť o akomsi efekte uvedomenia si skutkového stavu po druhom kole skúšok.

Ideálnymi príkladmi môžeme označiť študentov 64 a 116 kedy k dochádzalo k rovnomernému progresu po absolvovaní každého testu. Rovnako aj študenti 100 a 188 vykazujú progres avšak výraznejšie zlepšenie vidno až pri treťom termíne skúšky.

Porovnanie časových rozdielov medzi jednotlivými termínmi

Ako ďalšie sme vykonali porovnanie časových rozdielov medzi jednotlivými skúškami. V tejto analýze sme hľadali spojitosť medzi získanými výsledkami skúšok a časovým rozdielom medzi nimi.

Zobrazením týchto údajov sme získali predstavu o časovom rozložení termínov skúšok, ktoré študenti využili. V prípade študentov 18, 188 a 198 môžeme pozorovať výrazné časové rozdiely pohybujúce sa v intervale od 2 do 33 dní ktoré patria študentovi 188. Naproti tomu



Graf 2: Porovnanie časového rozdielu v dňoch medzi jednotlivými termínmi skúšok v AR 2021/2022
Zdroj: Vlastné spracovanie

ostatní študenti mali rozpätie medzi jednotlivými skúškami v intervale od 2 do 14 dní, čo je pri hornej hranici intervalu skrátenie časového rozdielu o 19 dní.

Tabuľka 2: Časový rozdiel v dňoch medzi termínmi skúšok v AR 2021/2022
Zdroj: Vlastné spracovanie

Termín\študent	študent 18	študent 64	študent 100	študent 116	študent 142	študent 188	študent 198	študent 236
časový rozdiel 1-2 termín	26	7	6	7	7	33	28	2
časový rozdiel 2-3 termín	2	2	14	9	12	2	7	12

Očakávali sme, že viac svetla do problematiky nám môže priniesť porovnanie časového rozdielu medzi dvomi termínmi v súvislosti zo získaným rozdielom bodov.

Tabuľka 3: Časový rozdiel v dňoch medzi termínmi skúšok v súvislosti so získaným rozdielom bodov v AR 2021/2022
Zdroj: Vlastné spracovanie

Termín\študent	študent 18	študent 64	študent 100	študent 116	študent 142	študent 188	študent 198	študent 236
časový rozdiel 1-2 termín	26	7	6	7	7	33	28	2
rozdiel bodov 1.-2. termín	0%	23%	10%	3%	-3%	7%	-7%	0%
časový rozdiel 2-3 termín	2	2	14	9	12	2	7	12
rozdiel bodov 2.-3. termín	-3%	17%	40%	10%	30%	23%	23%	50%

Porovnaním doby prípravy, ktorú si študenti zvolili medzi jednotlivými skúškami a výslednou úspešnosťou spracovania otázky sme dospeli k nasledujúcim záverom:

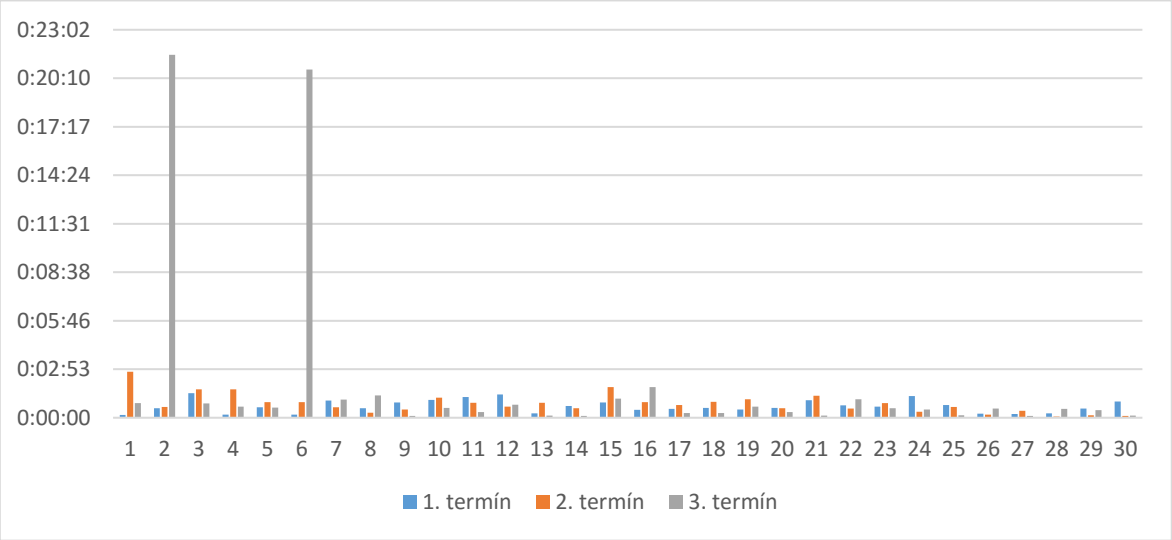
- Najefektívnejší interval doby prípravy medzi skúškami je medzi 10 a 15 dňom.
- Doba prípravy väčšia ako 15 dní neprináša vyššiu úspešnosť pri spracovaní otázky, skôr naopak študenti po takto dlhej dobe dosahujú veľmi slabé výsledky.
- Doba prípravy v intervale 2-10 dní nám v grafe neprináša konkrétne informácie o efektivite tejto doby na prípravu. Úspešnosť sa u každého študenta mení, pričom interval je od -3% po 24%. z toho je možné usúdiť, že v prípade úspešnosti 15 % a menej sa mohlo jednať o študentov, ktorí prišli „vyskúšať skúšku s tým že sa im možno podarí trafiť do správnej odpovede“. Naopak, pri úspešnosti vyššej o 15% môžeme počítať s tým, že študenti sa na test pripravili

Zaujímavý je údaj priemerného času spracovania otázky. TCExam započítava do času riešenia otázky čas od jej otvorenia až do zaznačenia odpovede. To znamená, že celkový súčet časov môže byť výrazne vyšší ako celkový čas pridelený na spracovanie testu. Ak je to v teste povolené, študenti často využívajú možnosť si otázku prečítať, preskočiť a vrátiť sa k nej neskôr.

Analyzovali sme ôsmych študentov. Bližšie opisujeme analýzu študentov 18 a 236, ktorých výsledky boli výrazne odlišné od zvyšných šiestich.

Študent 18

Študent 18 absolvoval skúšky v termínoch 20.12.2021, 15.1.2022 a 17.1.2022 pričom ani v jednom termíne nedosiahol požadovaný počet bodov.



Graf 3: Študent 18 - porovnanie časov spracovania otázok v jednotlivých termínoch
Zdroj: Vlastné spracovanie

Na základe extrahovaných údajov zobrazených v tabuľke vidíme, že u študenta 18 nedošlo k žiadnemu progresu.

Tabuľka 4: Úspešnosť študenta 18 na jednotlivých termínoch skúšok
Zdroj: Vlastné spracovanie

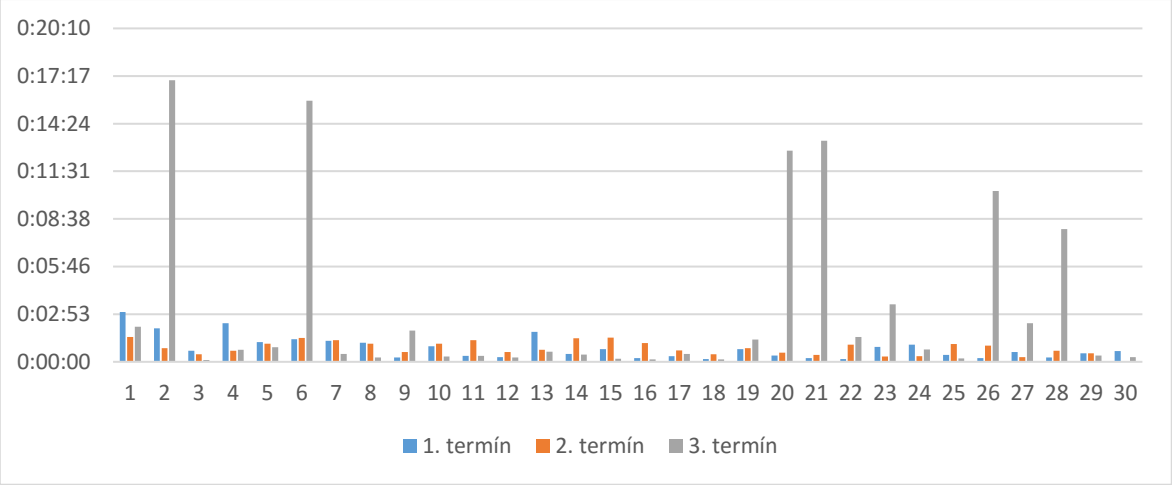
Študent 18	*otázky 1. Termín*	*otázky 2.Termín*	*otázky 3.Termín*
úspešnosť	43%	43%	40%
otázky s 1 odpoveďou	20	20	19
otázky s 2 odpoveďami	4	5	6
otázky s 3 odpoveďami	6	2	4
otázky s 4 odpoveďami	0	3	1
priemerný čas na otázku	0:00:41	0:00:50	0:01:57

Viditeľný je rozdiel v čase strávenom pri riešení otázok, kedy tento čas postupne narastal avšak priemerná hodnota 1:57 v treťom termíne je značne ovplyvnená tým, že otázky

2 a 6 boli študentom spracovávané až 20 minút. Ak sa pozrieme na zloženie otázok pomer jedno - odpoveďových k viac - odpoveďovým je takmer rovnaký, rozdiely sú len v pomeroch dvoj, troj a štvor - odpoveďových otázok čo nemá na výsledok vplyv. Dovolíme si konštatovať, že u študenta 18 sa výsledky jeho úsilia nezlepšovali.

Študent 236

Študent 236 absolvoval skúšky v termínoch 13.12.2021, 15.12.2022 a 27.1.2022 pričom aj v prvom a druhom termíne dosahoval veľmi nízke výsledky zhodne na úrovni 17%. na poslednom treťom termíne však dosiahol výsledok 67%, čo v uvedenej skupine bol druhý najlepší výsledok avšak dosiahlo ho viac študentov.



Graf 4: Študent 236 - porovnanie časov spracovania otázok v jednotlivých termínoch
Zdroj: Vlastné spracovanie

Tabuľka 5: Úspešnosť študenta 236 na jednotlivých termínoch skúšok
Zdroj: Vlastné spracovanie

Študent 236	*otázky 1. Termín*	*otázky 2.Termín*	*otázky 3.Termín*
úspešnosť	17%	17%	67%
otázky s 1 odpoveďou	17	15	21
otázky s 2 odpoveďami	6	11	2
otázky s 3 odpoveďami	5	4	5
otázky s 4 odpoveďami	1	0	1
priemerný čas na otázku	0:00:50	0:00:52	0:03:14

Na základe extrahovaných údajov zobrazených v tabuľke vidíme, že u študenta 236 nedošlo k žiadnemu progresu počas prvých dvoch termínov. Rozloženia rôznych typov otázok by mohli mať vplyv pri 2. termíne skúšok, kedy test obsahoval 15 otázok s viacerými odpoveďami. Naproti tomu úspešnosť pri 3. termíne skúšok mohla byť ovplyvnená vyšším počtom otázok s jednou odpoveďou (21 otázok).

Pri pohľade na časové rozdelenie spracovania odpovedí môžeme pozorovať, že pri 3. termíne skúšok sa študent 236 viac zamýšľal nad znením otázok a pravdepodobne pri otázkach

2, 6, 20, 21, 23, 26 a 28 si znenie najprv prečítal, pokračoval spracovaním ďalšej otázky a k uvedeným otázkam sa vrátil až nakoniec.

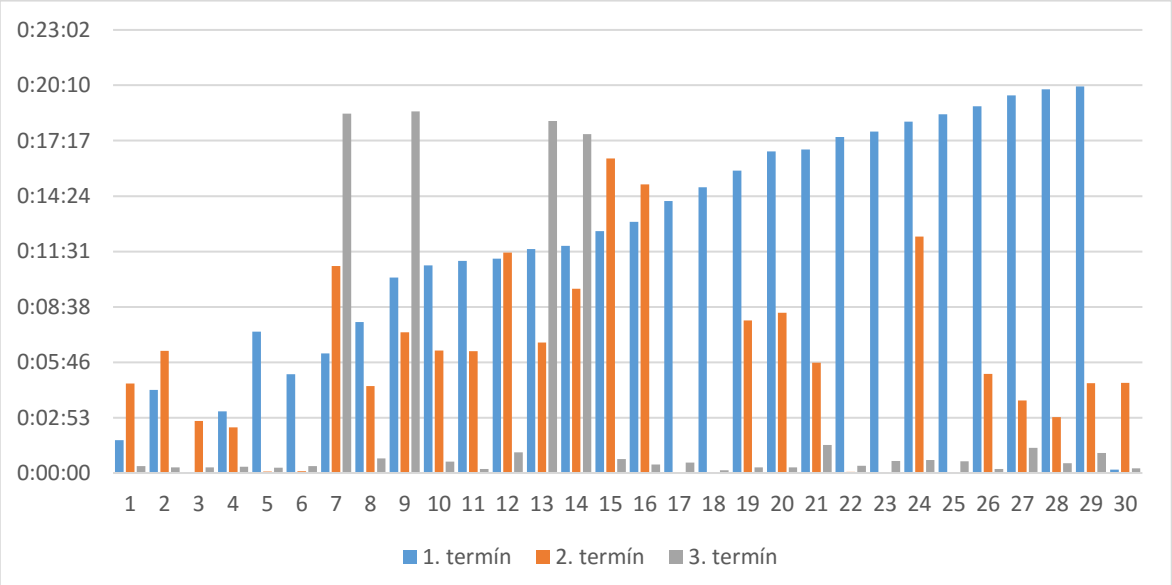
Týmto si dovolíme konštatovať, že u študenta 236 mohla mať táto zmena prístupu k spracovaniu otázok pozitívny vplyv na výsledok jeho úsilia v 3. termíne skúšok.

Ostatní študenti – postrehy z analýzy

U ostatných študentov boli pozorované podobné rozloženia otázok aj prístup k spracovaniu testov. Väčšina zo zvyšných šiestich študentov mala tendenciu sa zlepšovať okrem študentov 142 a 198. Tí mali zo začiatku vyššiu mieru úspešnosti a prepad v 2. termíne skúšok predstavoval 3% a 7%. Rozloženie rôznych typov otázok však bolo v oboch prípadoch veľmi rovnomerné, preto si dovoľujeme tvrdiť že pokles úspešnosti bol spôsobený nižšou mierou prípravy na skúšku.

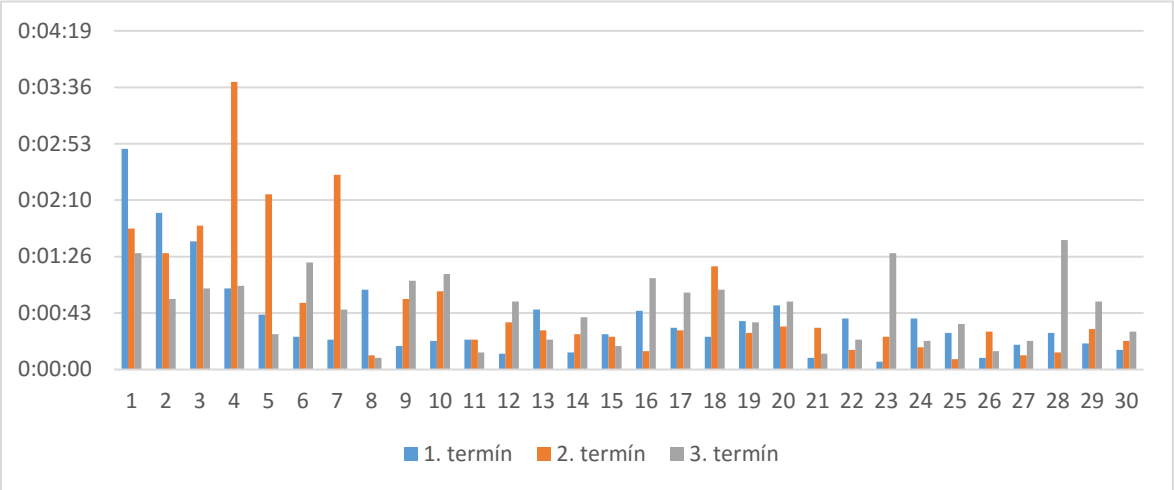
Čo sa týka porovnania časov spracovania jednotlivých otázok, stoja za zmienku študenti 100 a 188, ktorí mali pri spracovaní odpovedí opačnú taktiku avšak veľmi podobné výsledky.

Študent 100 zvolil taktiku prvotného prečítania si otázok testu. Viditeľné je to najmä v druhom termíne skúšok, kedy najprv odpovedal na prvé štyri otázky, no od otázky číslo 5 čas spracovania narastá s každou ďalšou otázkou. Zaujímavé je, že túto taktiku najprv využil na prvom termíne na približne dvoch tretinách otázok, no na treťom termíne skúšok ju využil len štyri krát. Vplyv na toto rozhodnutie mohlo mať aj zloženie testov, keďže v druhom termíne test obsahoval 10 nových a 15 viac - odpoveďových otázok oproti tretiemu termínu kde bola nová otázka len jedna a viac - odpoveďových desať.



Graf 5: Študent 100 - porovnanie časov spracovania otázok v jednotlivých termínoch
Zdroj: Vlastné spracovanie

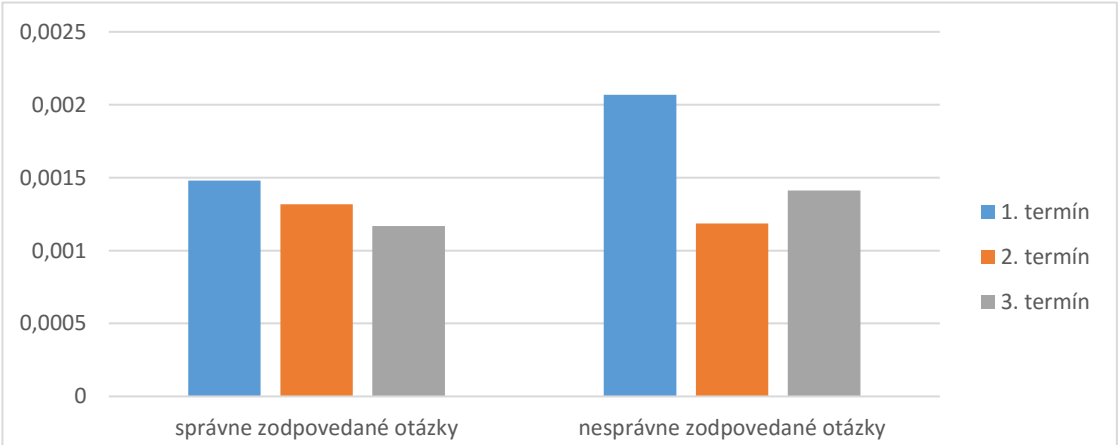
Študent 188 zvolil taktiku postupného odpovedania pri všetkých troch termínoch. Zloženie testovacích sád mal rovnomerné vo všetkých termínoch, pričom v druhom aj treťom termíne zaznamenal progres v úspešnosti spracovania testu.



Graf 6: Študent 188 - porovnanie časov spracovania otázok v jednotlivých termínoch
Zdroj: Vlastné spracovanie

Závislosť priemerného času spracovania odpovede od úspešnosti

Ďalšou analýzou je porovnanie závislosti výsledkov na čase. Ak sa pozrieme na celkové porovnanie priemerných časov odpovedí, zistíme, že pri správnych odpovediach sa priemerné časy skracovali a pri neprávnych kolísali.



Graf 7: Porovnanie priemerného času spracovania otázky v závislosti na správnych a nesprávnych odpovediach
Zdroj: Vlastné spracovanie

Záver

Počas skúšania študentov elektronickou formou, sme overili, že táto stratégia spracovania testu je identifikovateľná na základe časových rozdielov pri spracovaní jednotlivých otázok. Zároveň nám analýza indikuje skutočnosť, že často sa opakujúci dlhý časový úsek pri jednej odpovedi naznačuje jej vyššiu zložitosť oproti ostatným otázkam.

V prípade analýzy vplyvu časového obdobia medzi dvomi testami môžeme zhrnúť, že pri prvom a poslednom termíne bol priemerný čas správne zodpovedaných otázok nižší ako pri nesprávne zodpovedaných, pričom výrazný rozdiel vidno pri prvom termíne. Naopak, rozdiely priemerných časov splnenia pri druhom termíne boli opačné, teda rýchlejšie boli spracované nesprávne zodpovedané otázky a pomalšie správne zodpovedané. Túto skutočnosť si možno vysvetliť nasledovne:

- Na prvom termíne študenti relatívne rýchlo odpovedajú na otázky, ktorých odpovede sú im známe a viac sa zaoberajú otázkami, na ktoré nie sú dostatočne pripravení. Najčastejšia stratégia je „prečítam si otázku, ak viem hneď odpoviem ak nie pokračujem a k otázke sa vrátim“.
- Na druhom termíne boli študenti istejší, doučili sa časť učiva, tým pádom odpovedali rýchlejšie ako na prvom termíne. Na otázky, na ktoré neboli pripravení pravdepodobne odpovedali náhodne bez hlbšieho rozmýšľania.
- Tretí termín bol posledný, teda sa pravdepodobne oveľa viac pripravili a tým pádom si boli istejší v správnych odpovediach a spracovali ich rýchlejšie ako v predchádzajúcich termínoch.. V prípade otázok, na ktoré neboli dostatočne pripravení vidno vyšší rozdiel v čase spracovania, teda snahu rozpamätať sa na správnu odpoveď.

Interpretácia získaných údajov formou takýchto analýz, nám umožňuje prehodnotiť celý proces overovania vedomostí študentov v predmete Informatika I. s tým, že máme identifikované problematické otázky a tým aj konkrétne tematiky, ktorým treba venovať väčšiu pozornosť pri prednáškach, prípadne prehodnotiť vhodnosť niektorých otázok.

Rovnako dôležité je zistenie vplyvu konfigurácie testu na jeho výsledok, čo nám umožní precizovať toto nastavenie za účelom dosahovania podrobnejších výsledkov pri testovaní.

Rozloženie otázok podľa tematických celkov síce nemá výrazný vplyv na výsledky testovania, avšak ovplyvňuje práve jeho konfigurovanie. Z tohto dôvodu je potrebné upraviť aj databázu otázok tak, aby jednotlivé tematické celky obsahovali rovnaký počet testovacích otázok.

Výsledky analýzy týkajúce sa stratégie študentov pri opakovaných testoch a s tým spojeným časovým rozpätím nám dáva do pozornosti potrebu pracovať so študentami aj v oblasti motivácie pri neúspešných pokusoch, kedy príliš krátka a zároveň aj príliš dlhá doba medzi testami zväčša neprináša požadované zlepšenie úrovne v odpovediach otázok testu.

Príspevok vznikol v rámci riešenia vedecko-výskumnej úlohy Výsk. 161 „Metódy spracovania policajne relevantných informácií“ na Akadémii Policajného zboru v Bratislave.

Zoznam použitej literatúry:

Özturgut, O., Standardized Testing In The Case Of China And The Lessons To Be Learned For The U.S., (online, cit. 17.12.2021). Dostupné na internete: https://www.researchgate.net/publication/298911898_Standardized_Testing_In_The_Case_Of_China_And_The_Lessons_To_Be_Learned_For_The_US

TUREK I. 1998: Zvyšovanie efektívnosti vyučovania. - Združenie pre vzdelávanie EDUKÁCIA, Bratislava, 1998. - 2. dopln. vyd. - 326 s. ISBN 80-88796-89-X strana 255

RAFAJLOVIČOVÁ, R., ŠTULRAJTEROVÁ,M., 2002. Skúšanie, testovanie a hodnotenie v edukačnom procese. Bratislava: Štátny pedagogický ústav. 2002, 53s, ISBN 80-8575-667-6, (online) (online, cit. 20.12.2021), Dostupné na internete: https://encyklopediapoznania.sk/data/eknihy/pedagogika2/skusanie_testovanie.pdf strana 4

TCExam (online, cit. 20.12.2021), Dostupné na internete: https://tcexam.org/

Kontakt

Mgr. Štefan Zachar, PhD.
Katedra informatiky a manažmentu
Akadémia Policajného zboru v Bratislave
e-mail: stefan.zachar@akademiapz.sk

RECENZNÉ POSUDKY

RECENZNÝ POSUDOK

na Zborník príspevkov z vedeckej konferencie

KATEDRY INFORMATIKY A MANAŽMENTU
AKADÉMIE POLICAJNÉHO ZBORU V BRATISLAVE

AKTUÁLNE VÝZVY KYBERNETICKEJ BEZPEČNOSTI

2022

Recenzent: doc. RNDr. Bohumír Štědroň, PhD.

Masarykova univerzita Brno, Česká republika

Autori recenzovaného výstupu: autorský kolektív aktívnych účastníkov vedeckej konferencie.

Zborník z prezentovaných a predložených príspevkov je výstupom, ktorý je možné odporúčať ako odbornú publikáciu pre nadobudnutie nielen teoretických, metodických, odporúčacích, ale i praktických znalostí pre akademickú i odbornú verejnosť. Súčasne môže, v rámci prevencie, slúžiť aj na podporu osvety a informovanosti širokej verejnosti v oblasti uplatňovania bezpečnostných mechanizmov na ochranu v súvislosti so spracúvaním citlivých a osobných údajov, ako aj na ochranu súkromia a predchádzanie realizácie hrozieb v digitálnom priestore.

7 prezentovaných príspevkov predstavuje aktuálne otázky týkajúce sa nových systémových trendov v IT. Úvodný príspevok "Perspektívy vzdelávania a certifikácie osôb v oblasti kybernetickej bezpečnosti"(Ivan Makatura) sa zaoberá problematikou kvalifikácie v segmente IT.

Kľúčovým príspevkom je príspevok "Manažment kybernetickej bezpečnosti a jej vnímanie vo Francúzsku" (Matej Kostrec), ktorý umožňuje porovnanie problematiky s krajinami EÚ.

Medzi ďalšie príspevky patria analýzy týkajúce sa prierezovo oblasti kybernetickej bezpečnosti:

1. "Kybernetická (ne)bezpečnosť a sociálne siete",
2. "Potreba skúmať úroveň kybernetickej bezpečnosti v spoločnosti",
3. veľmi aktuálna téma "Bezpečnosť blockchainu",
4. "Úvod do anonymných sietí",
5. a pedagogická téma "Analýza stratégií študentov pri overovaní vedomostí prostredníctvom elektronického testovania".

Po formálnej stránke všetky príspevky uverejnené v predkladanom zborníku obsahujú povinné náležitosti kladené na vedecké a odborné príspevky, sú logicky usporiadané a obsahovo vyvážené. Autori príspevkov založili jednotlivé prezentácie na svojich vedeckých i odborných skúsenostiach a špecifickú odbornú terminológiu sa snažili čo najzrozumiteľnejšie predstaviť tak, aby bola v logickom slede prístupná nielen pre odborné publikum, ale aj pre študentov APZ, pre potreby príslušníkov PZ i pre laickú verejnosť.

Záver:

Predkladaný zborník príspevkov prezentovaných v rámci Vedeckej konferencie, je možné, vzhľadom na vysokú odbornú úroveň všetkých príspevkov k pertraktovanej a veľmi aktuálnej problematike zvyšovania úrovne kybernetickej bezpečnosti, považovať za kvalitný a prínosný publikačný výstup, ktorý bezpochyby oboznámi svojho čitateľa s nebezpečnými hrozbami v digitálnom priestore, ako aj s možnosťami prevencie pred nimi. Samotná konferencia splnila očakávané ciele a po odbornej stránke dokonca kvalitou prevýšila očakávanú úroveň, pretože zborník z nej môže slúžiť nielen pre potreby aplikačnej praxe príslušníkov PZ a prípravy študentov APZ v oblasti kybernetickej bezpečnosti, ale aj pre zvýšenie informovanosti a povedomia odbornej i laickej verejnosti o možných útokoch na počítačovú a komunikačnú infraštruktúru.

Na základe vyššie uvedených skutočností konštatujem, že zborník pod názvom **„Aktuálne výzvy kybernetickej bezpečnosti. 2022“,** má v predloženej podobe všetky potrebné atribúty s vysokým potenciálom budúcej úspešnosti využitia aj pre aplikačnú prax a vzdelávacie kurzy, a preto **o d p o r ú č a m jeho schválenie a publikovanie v predloženom obsahu.**

V Prahe, 15.6.2023 doc. RNDr. Bohumír Štědroň, Ph.D.

RECENZNÝ POSUDOK

na Zborník príspevkov z vedeckej konferencie

KATEDRY INFORMATIKY A MANAŽMENTU
AKADÉMIE POLICAJNÉHO ZBORU V BRATISLAVE

AKTUÁLNE VÝZVY KYBERNETICKEJ BEZPEČNOSTI 2022

Recenzent: RNDr. Eva KOSTRECOVÁ, PhD.
Fakulta managementu Univerzity Komenského v Bratislave
Katedra informačných systémov

Autori recenzovaného výstupu: autorský kolektív aktívnych účastníkov vedeckej konferencie.

Téma vedeckej konferencie je v rámci programu Digitálna Európa, ktorý na nadchádzajúce roky vyhlásila Európska Komisia, vysoko aktuálnou problematikou. Kybernetická infraštruktúra sa stáva čoraz častejšie predmetom útokov a zneužívania na nekalé, manipulačné, vydieračské a trestné aktivity. Z týchto dôvodov je nevyhnutné predchádzať takýmto útokom a monitorovať toky dát prechádzajúcich cez kybernetickú infraštruktúru. Avšak táto činnosť si vyžaduje špecialistov z oblasti kybernetickej bezpečnosti, ktorých nedostatok pociťujú všetky oblasti využívajúce elektronickú a dátovú komunikáciu. Jedným z hlavných cieľov vedeckej konferencie bol preto aj pohľad na perspektívu vzdelávania takýchto odborníkov.

Autori príspevkov prezentovaných na tejto vedeckej konferencii vychádzali z poznatkov nadobudnutých skúmaním pôsobiacich faktorov a doterajších trendov vývoja v oblasti kybernetickej bezpečnosti a súčasne poskytli pohľad na možný smer napredovania do budúcnosti vzdelávania a implementácie poznatkov z tejto oblasti, ktoré majú potenciál osloviť vedcov a odborníkov zo širokej škály oblastí, nielen štátnej a verejnej správy, ale aj súkromného sektora.

V prvom príspevku, pod názvom „Perspektívy vzdelávania a certifikácie osôb v oblasti kybernetickej bezpečnosti“, poukazuje jeho autor na nedostatok odborníkov v oblasti správy, riadenia a monitorovania stavu a úrovne kybernetickej bezpečnosti. Naznačuje proces možného doplnenia si kompetencií, ktorý je daný aj návrhom legislatívneho textu v podobe Vyhlášky Národného bezpečnostného úradu, a ktorý ustanovuje znalostné štandardy v podobe charakteristiky rolí, s ktorými je spojená množina povinností, kľúčových činností, zručností, ale i oprávnení pri správe a používaní informačných systémov. Autor vymenúva rôzne posty, ktoré sú určené pre špecialistov kybernetickej bezpečnosti, spolu s certifikačnými schémami a možnosťami absolvovania certifikačných testov. Uvádza aj štatistiky potrieb počtu

pracovných miest v oblasti kybernetickej bezpečnosti v Slovenskej republike. Príspevok môže byť inšpiratívnym podkladom pri stanovovaní plánovania počtu a zamerania vzdelávacích programov a kurzov kybernetickej bezpečnosti.

Autor druhého príspevku, pod názvom „Manažment kybernetickej bezpečnosti a jeho ponímanie vo Francúzsku“, sa zameral na konkrétnu oblasť vzdelávania role manažéra kybernetickej bezpečnosti vo Francúzsku, a predstavil akreditované samostatné programy magisterského štúdia na viacerých francúzskych univerzitách spolu s blokmi študijných predmetov, ich náplňou a spôsobom hodnotenia. Rovnako sa venoval detailnej špecifikácii obsahu kurzov pre post vedúceho manažéra kybernetickej bezpečnosti, ktorého záverom je získanie certifikačného osvedčenia. Tieto detailné a veľmi užitočné informácie uvedené v príspevku môžu byť konkrétnou inšpiráciou pri tvorbe sylabov i študijných programov pre vzdelávanie v oblasti kybernetickej bezpečnosti na slovenských univerzitách.

V treťom príspevku, pod názvom „Kybernetická (ne) bezpečnosť a sociálne siete“, uvádza jeho autor prehľad a využívanie rôznych sociálnych sietí, ako aj druhy jednotlivých možných útokov na dáta i užívateľov týchto sietí. Poskytuje aj dáta o finančných stratách za jednotlivé druhy kybernetických útokov. Vzhľadom na nízke bezpečnostné povedomie užívateľov sociálnych sietí, môže byť príspevok využitý pre potreby osvety a zvýšenia prijímania bezpečnostných mechanizmov pre laickú verejnosť.

Autorka štvrtého príspevku, pod názvom „Potreba skúmania úrovne kybernetickej bezpečnosti v spoločnosti“, sa venuje analýzam uplatňovania legislatívnych textov, prijatých pre oblasť kybernetickej bezpečnosti tak v rámci EÚ, ako aj v Slovenskej republike, analýzam úrovne kybernetickej bezpečnosti v podnikateľskom prostredí a analýzam o povedomí o tejto problematike, ktoré zmapovala na základe výskumu vykonaného Kompetenčným a certifikačným centrom kybernetickej bezpečnosti v spolupráci Národným bezpečnostným úradom. Výsledky tohto výskumu svedčia o nedostatočnom povedomí širokej verejnosti o nebezpečenstvách pri používaní kybernetických nástrojov a aplikácií. Autorka príspevku vidí aspoň čiastočnú nápravu tohto stavu vo forme identifikácie kybernetických incidentov a ich riešenia v podobe prijatia preventívnych opatrení proti ich opätovnému vzniku. Tento postoj autorky je veľmi prínosný a môže byť podkladom pre podrobnejšie popisy identifikácie kybernetických incidentov.

Autor piateho príspevku, pod názvom „Bezpečnosť blockchainu“, prezentuje novú technológiu ukladania obrovských množstiev dát, ktorá je vzhľadom na jej základný princíp „nekonečného ukladania dát bez možnosti ich dodatočnej zmeny“, vybavená od tvorcov technológie aj určitým stupňom bezpečnosti a ochrany uložených dát. Príspevok je vhodné využiť pre prezentáciu tejto novej technológie, ktorá je ešte stále takmer neznáma vo verejnosti, tak na akademickej pôde, ako aj pri rôznych kurzoch venovaných informačným technológiám a ich uplatňovaniu v praxi.

Autor ďalších dvoch príspevkov, pod názvami „Úvod do anonymných sietí – história ich vzniku a základné prvky“ a „Analýza stratégie študentov pri overovaní vedomostí elektronickou formou testovania“, v nich predstavuje nové technológie, ktorými sú na jednej strane anonymné siete, zdroj, vzhľadom na anonymitu, pre páchanie nelegálnej činnosti, ale aj výmeny popisov atakov medzi kybernetickými pirátmi. Súčasne tieto siete ponúkajú aj vysokú mieru bezpečnosti a súkromia, čo je dôležité pre používateľov, ktorí sa snažia ochrániť svoje dáta pred sledovaním a monitorovaním. Na druhej strane autor detailne popisuje a analyzuje

možnosti využívania aplikačného softvéru pre overovanie vedomostí. Táto nová forma overovania vedomostí má už v súčasnosti rôzne oblasti využitia, napríklad overovanie teoretických vedomostí pri získavaní vodičského preukazu. Oba príspevky môžu byť využité pre študijné účely pri poznávaní možností nových technológií, ktoré zásadne ovplyvňujú dynamiku prebiehajúcich zmien v digitálnom svete, ako aj úrovni ich bezpečnosti pri ukladaní a spracúvaní dát.

Celkové zhodnotenie:

Predkladaný Zborník príspevkov z vedeckej konferencie je spracovaný na vysokej odbornej úrovni, založenej na dlhodobom vedeckom skúmaní pertraktovanej problematiky autormi jednotlivých príspevkov. Podnecuje inovatívnym, kreatívnym a v mnohom stimulujúcim pohľadom budúci smer vzdelávania v oblasti kybernetickej bezpečnosti, ktorý má potenciál osloviť mnohých študentov, učiteľov i vedeckých pracovníkov vysokých škôl, ale i rôznych odborných pracovníkov z viacerých vedeckých oblastí zameraných na bezpečnosť digitálneho priestoru. Z vyššie uvedených dôvodov

o d p o r ú č a m schválenie zborníka a jeho publikovanie v predloženom obsahu.

V Bratislave, 18.6.2023 RNDr. Eva Kostrecová, PhD.

Názov: **Aktuálne výzvy kybernetickej bezpečnosti 2022**

Vydala: Akadémia Policajného zboru v Bratislave

Sklabinská 1, 835 17 Bratislava

Pracovisko: Katedra informatiky a manažmentu

Zostavil: Mgr. Štefan ZACHAR, PhD.

Technická redakcia: mjr. JUDr. Matej KOSTREC, PhD.
Mgr. Štefan ZACHAR, PhD.

Recenzenti: doc. RNDr. Bohumír ŠTĚDROŇ, PhD.
RNDr. Eva KOSTRECOVÁ, PhD.

Rozsah: 100 strán

Rok vydania: 2023

ISBN 978-80-8054-998-5

EAN 9788080549985