POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

DISERTAČNÍ PRÁCE

2022 **ING. MIROSLAV ČERMÁK**

POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

Hodnocení bezpečnosti v organizacích

Disertační práce

ŠKOLITEL
Ing. Marek ČANDÍK, Ph.D.

AUTOR PRÁCE
Ing. Miroslav ČERMÁK

PRAHA
2022

POLICE ACADEMY OF THE CZECH REPUBLIC IN PRAGUE

Security evaluation of organization

Dissertation

SUPERVISOR
Ing. Marek ČANDÍK, Ph.D.

AUTHOR
Ing. Miroslav ČERMÁK

PRAGUE
2022

ABSTRAKT

Tato práce představuje návrh metodiky hodnocení úrovně kybernetické bezpečnosti organizace. V rámci dotazníkového šetření byly osloveny vybrané organizace v ČR působící v různých odvětvích národního hospodářství a byly identifikovány hrozby, které se vyskytují nejčastěji a způsobují organizacím největší škody. Výsledkem této práce je webová aplikace a unikátní sada otázek, která umožnuje během pár minut ověřit, zda má organizace zavedena vhodná bezpečnostní opatření vůči relevantním hrozbám a jak moc je zranitelná.

KLÍČOVÁ SLOVA

kyberprostor * hrozby * zranitelnosti * vektory útoku * bezpečnost * výzkum * metodika * hodnocení

ABSTRACT

This work presents a proposal for the methodology of cyber security assessment of the organization. The questionnaire survey addressed selected organizations in the Czech Republic operating in various sectors of the national economy and identified the threats that most often occur and cause the greatest damage to organizations. The result of this work is a web application and a unique set of questions that allows you to verify in a few minutes whether the organization has implemented appropriate security measures against relevant threats and how vulnerable it is.

KEYWORDS

cyberspace * threats * vulnerabilities * vector of attack * security * research * methodology * evaluation

PROHLÁŠENÍ

Prohlašuji, že předložená práce je mým původním autorským dílem, které jsem vypracoval samostatně. Veškerou literaturu a další zdroje, z nichž jsem čerpal, v práci řádně cituji a jsou uvedeny v seznamu použité literatury.

V Praze, dne 30. 05. 2022

Ing. Miroslav Čermák

PODĚKOVÁNÍ

Rád bych také poděkoval svému školiteli, Ing. Marku Čandíkovi, Ph.D., za podporu a odborné rady a cenné připomínky, které mi poskytoval v průběhu zpracování disertační práce.

OBSAH

SEZNAM ZKRATEK

A	Availability
APT	Advance Persistent Threat
Au	Authenticity
AV	Antivirus
C	Confidentiality
C&C	Command and Control server
CCTV	Closed Circuit Television
CL	cílený útok na lidi
CS	cílený útok na stroje
CSIRT	Computer Security Incident Response Team
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CWE	Common Weaknesess and Exposures
CWSS	Common Weakness Scoring System
ČAP	Česká asociace pojišťoven
ČLR	Čínská lidová republika
ČR	Česká republika
DB	Databáze
DDoS	Distributed Denial od Services
EES	Escrow Encryption Standard
HAVAC	Heating, ventilation, and air conditioning
HW	hardware
I	Integrity
ICS	Industry Control Systems/Supervisory
ID	Identifikátor
IoT	Internet of Things
ISG	Information Security Governance
ISM	Information Security Management
ISO	International Organization for Standardization
IT	Information Technology
KII	Kritická informační infrastruktura

NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVD	National Vulnerability Database
O365	Microsoft Office 365
OS	Operating Systém
OT	Operational Technology
P	Possession
PČR	Policie České republiky
PIR	Passive InfraRed sensor
PL	plošný útok na lidi
PS	Plošný útok na stroje
RCS	Remote Control Systém
SCADA	Supervisory Control and Data Acquisition
SD	Secure Digital
SDLC	System Development Life Cycle
SIEM	Security Information and Event Management
SOC	Security Operations Center
SW	software
U	Utility
UPS	Uninterruptible Power Supply
USB	Universal Serial Bus
VIS	Významná informační infrastruktura
VoKB	Vyhláška o kybernetické bezpečnosti
WoV	Windows of Vulnerability
ZoKB	Zákon o kybernetické bezpečnosti
ZS	Základní služby

SEZNAM OBRÁZKŮ, TABULEK A GRAFŮ

1 ÚVOD

Hodnocení úrovně informační a kybernetické bezpečnosti v organizacích a zavedení odpovídajících bezpečnostních opatření organizační a technické povahy probíhá zpravidla v souladu s nějakým mezinárodním standardem nebo normou. Ověřuje se, zda organizace provedla analýzu rizik, má zavedeny jednotlivé procesy na příslušné úrovni vyzrálosti, odpovídající bezpečnostní opatření organizační a technické povahy, vydala příslušné politiky, standardy a příručky. Dále zda formálně jmenovala konkrétní pracovníky do rolí v ní uvedených, kontroluje dodržování politik a standardů a průběžně vyhodnocuje úroveň bezpečnosti.

Toto hodnocení probíhá zpravidla formou auditu, kdy dochází k porovnání stávajícího stavu proti předpisové soustavě, tedy pokud organizace nějakou má, anebo proti tzv. „best practice“, pokud ji nemá, což je často případ menších a středních firem, které jsou zformulovány právě v ISO normách, vyhláškách nebo mezinárodních standardech. V zásadě se jedná o GAP analýzu, kdy auditor provádí interview s vybranými zaměstnanci a vedoucími pracovníky organizace, zaznamenává jejich odpovědi a ve vybraných případech ověřuje jejich tvrzení tím, že si nechává předložit důkaz.

Nezavedení příslušných procesů nebo opatření však ještě neznamená, že je na tom organizace z pohledu kybernetické odolnosti špatně. Záleží na tom, zda aplikuje jen způsob řízení bezpečnosti založený na opatřeních, tzv. control driven, anebo přístup založený na rizicích, tzv. risk driven, a obhájí důvod pro nezavedení např. předložením zprávy o zvládání rizik např. dle ISO 31000, ze které vyplyne, že se v jejím případě jedná o nízké riziko, organizace si ho je vědoma a rozhodla se jej akceptovat.

Další metodou hodnocení je pak provedení bezpečnostního testu, ten může mít podobu skenu zranitelností, který spočívá ve spuštění programu, který vyhodnocuje stav všech dostupných systémů, otevřené porty, aktuálnost jejich verzí apod. Dále se může jednat o hodnocení konfigurace, kdy se posuzuje, zda je stávající systém nastaven v souladu s best practice anebo standardem společnosti. V neposlední řadě pak mohou být provedeny penetrační testy nebo ethical hacking. Ideální je pak kombinace všech těchto metod.

Nevýhodou metod sloužících k posouzení úrovně zavedených bezpečnostních opatření je, že jsou příliš časově a finančně náročné, neboť dle velikosti organizace trvá toto posuzování až několik týdnů. V okamžiku, kdy chce třetí strana v roli neformálního auditora bez příslušné autority zhodnotit bezpečnost jiné organizace, tak to představuje vážný problém, protože protistrana není příliš ochotna poskytovat součinnost, především z důvodu časové náročnosti.

Z tohoto důvodu je třeba provést zhodnocení bezpečnosti takovým způsobem, který výše zmíněnými nedostatky nebude trpět. To znamená **navrhnout takové řešení, resp. sadu otázek, které zaberou minimum času, budou moci být zodpovězeny v podstatě kýmkoliv a kdykoliv a zároveň poskytnou celkem věrohodný obrázek o skutečné úrovni kybernetické bezpečnosti v dané organizaci**.

Za tímto účelem je nutné redukovat podstatným způsobem sadu otázek ověřujících zavedení jednotlivých bezpečnostních opatření uvedených v normách a standardech, resp. navrhnout vlastní. To však nejde, aniž by bylo zprvu zřejmé, **které konkrétní hrozby by měly být vzaty v úvahu, jakých zranitelností zneužívají, jaký je použit vektor útoku a jaký mají tyto útoky dopad na organizaci, a jaká bezpečností opatření by organizaci mohla před těmito útoky ochránit, a proto by je měla mít zavedena**.

Aby však tato redukce mohla být provedena, **je nutné zjistit, jaká je skutečná situace v kyberprostoru,** a to zase nelze bez analýzy sekundárních zdrojů, jako jsou bezpečnostní reporty vydávané bezpečnostními organizacemi zpravidla na roční bázi. Ovšem ty zase mohou podstatným způsobem zkreslovat realitu, takže je nutné se zaměřit především na analýzu primárních zdrojů, které lze získat jedině realizací vlastního výzkumu, např. formou dotazníkového šetření a hloubkových rozhovorů s bezpečnostními experty.

1.1 Cíl práce

Cílem této disertační práce je návrh vhodné metodiky hodnocení, která by umožnila efektivní, tj. rychlé a snadné zhodnocení úrovně kybernetické bezpečnosti, resp. odolnosti vůči kybernetickým útokům, kterým organizace v ČR aktuálně čelí a budou do budoucna i čelit, a to v libovolné organizaci

působící ve statním i soukromém sektoru bez ohledu na to, zdali je jejím cílem dosahování zisku či nikoliv.

Dílčími cíli této práce pak je identifikace:

- jednotlivých prvků kyberprostoru a objasnění vztahů mezi nimi;
- nejčetnějších kybernetických hrozeb, kterým jsou organizace vystaveny;
- kybernetických hrozeb způsobujících největší škodu;
- klíčových faktorů ovlivňujících úroveň bezpečnosti v organizaci.

Tyto dílčí cíle, které jsou přínosné i samy o sobě by měly přispět k dosažení hlavního cíle.

1.2 Vymezení zkoumaného problému

Tato práce se věnuje posouzení účinnosti bezpečnostních opatření vůči kybernetickým hrozbám, v jejich úzkém pojetí, tj. vůči kybernetickým útokům, které se odehrávají výhradně v kyberprostoru. To znamená, že jsou realizovány za použití prostředků výpočetní techniky a jsou vedeny na informační a provozní technologie[1] a jejich uživatele, kteří jsou nedílnou součástí kyberprostoru. Především pak na systémy, které představují kritickou informační infrastrukturu, významné informační systémy a systémy základních služeb. **Práce se primárně nezabývá**:

- zavedením vhodných opatření vůči hrozbám jako je působení vyšší moci, technické selhání, fyzický útok na informační systém, či únik citlivých informací, které jsou sdělovány ústně, odpozorovány anebo jsou zaznamenány na jiném než digitálním médiu;

- očerňujícími kampaněmi vedenými v kyberprostoru ze strany konkurenčních firem, působením zahraničních zpravodajských služeb, zakládáním dezinformačních webů, vytvářením a šířením fake news a deep

[1] ČERMÁK, Miroslav. Provozní technologie. *CleverAndSmart Management Consulting* [online]. 2020 [cit. 20.07.2020]. ISSN 2694-9830. Dostupné z: https://www.cleverandsmart.cz/provozni-technologie/

fakes a jejich včasným rozpoznáním a reakcí na ně, protože ty se odehrávají mimo hodnocený systém;

- kybernetickými útoky, které jsou primárně vedeny na domácnosti a jejich koncová zařízení, která nejsou součástí informačního systému organizace, byť v některých případech tomu tak být může a navržená metodika hodnocení by měla být použitelná i pro hodnocení bezpečnosti domácností, nikoliv jen organizací;

- trestnou činností páchanou za použití prostředků výpočetní techniky, jako je třeba padělání úředních listin, dokladů, smluv, poukázek, kolků, peněz, sdílení nelegálního obsahu chráněného autorským zákonem, šíření nevyžádaného obchodního sdělení, zobrazovaní závadné reklamy, provozování internetových kasin, podvodných e-shopů, prodej zakázaných prostředků, obchod s lidmi apod.;

- kyberšikanou v jakékoliv formě, která se může odehrávat i na pracovišti jakékoliv organizace a za použití výpočetní techniky a být cílena na zaměstnance, který je součástí informačního systému a tedy i kyberprostoru.

1.3 Výzkumné otázky

V současné době se organizace potýkají s nedostatečným povědomím o situaci v kyberprostoru, neboť nejsou k dispozici dostatečně věrohodné informace o tom, jakým kybernetickým útokům organizace v ČR čelí, jaké jsou finanční následky těchto útoků a jaká bezpečnostní opatření organizační a technické povahy organizace již přijaly, a zda jsou tak dostatečně chráněny vůči nejčastějším kybernetickým útokům. Alespoň to **vyplývá z rozhovorů s manažery pojišťoven a rovněž i z diskuse na posledních konferencích České asociace pojišťoven**, zkr. ČAP. Výše uvedená skutečnost představuje výzkumný problém, který je třeba vyřešit a formulovat za tímto účelem vhodné výzkumné otázky.

Výzkumná otázka by měla přispět k naplnění cíle výzkumu, a měla by být proto jasně a jednoznačně formulována, aby nebylo pochyb, na co se vlastně ptá, a přinášet odpověď na otázku co, proč, jak, kdy, kde anebo kdo[2].

V souladu s cílem práce, navrhnout jednoduchou a rychlou metodiku umožňující vyhodnotit odolnost organizace vůči kybernetickým útokům přicházejícím z kyberprostoru, byly proto formulovány následující výzkumné otázky, označené VO1, VO2 a VO3, které je nutné zodpovědět, aby mohlo být dosaženo cíle této práce.

VO1: Jaké hrozby, které by mohly narušit bezpečnost organizace, je třeba vzít v úvahu při návrhu vhodných opatření?

Je zřejmé, že vzhledem k omezeným zdrojům, kterými organizace disponuje, není možné vzít v úvahu všechny kybernetické hrozby, ale jen ty, které se např. vyskytují nejčastěji, způsobují největší škodu anebo je zde reálná obava, že by do budoucna mohly představovat pro hodnocenou organizaci vážný problém. A s tím pak souvisí další výzkumná otázka týkající se zavedených bezpečnostních opatření.

VO2: Jaká bezpečnostní opatření by měla mít organizace zavedena, aby byla co nejlépe ochráněna?

S omezenými zdroji pak souvisí i možnosti organizace investovat do zavedení vhodných bezpečnostních opatření. Jedině zodpovězením této otázky je totiž možné navrhnout takovou sadu bezpečnostních opatření organizační a technické povahy, které budou předmětnou organizaci skutečně chránit před aktuálními a případně i budoucími kybernetickými útoky a nebudou ji jen zbytečně zvyšovat náklady.

VO3: Má smysl brát v potaz při hodnocení velikost organizace, sektor, odvětví, kritičnost informačního systému?

[2] MOLNÁR, Zdeněk. *Pokročilé metody vědecké práce*. Zeleneč: Profess Consulting, 2012. ISBN 978-80-7259-064-3. s. 32.

Je zřejmé, že mezi jednotlivými hodnocenými organizacemi jsou značné rozdíly. Pokud by byla odpověď na tuto výzkumnou otázku ano, tak by pak bylo možné zacházet s organizacemi o určité velikosti, působících v určitém sektoru, odvětví a provozující systém o určité kritičnosti jinak než s ostatními. V případě opačné odpovědi by pak tyto faktory nemusely být brány v potaz a klíčové by pak byly výhradně identifikované hrozby a relevantní bezpečnostní opatření.

Po zodpovězení prvních dvou výzkumných otázek, které spolu velice úzce souvisí, resp. bez zodpovězení první, není možné zodpovědět druhou, je možné stanovit vztah hrozba vs. opatření. A je tak možné navrhnout takovou sadu bezpečnostních opatření, kdy na základě absence příslušného opatření lze predikovat, obětí jakého kybernetického útoku nebo útoků by se daná organizace mohla stát a jakou by mohla utrpět škodu. Zodpovězením třetí výzkumné otázky je pak možné tento rizikový model ještě dále zpřesnit.

1.4 Postup zpracování práce

V souladu s výzkumným cílem, kterým je návrh jednoduché metodiky a nástroje, pomocí kterého by bylo možné efektivně, tj. rychle, s minimálními náklady, a přitom objektivně vyhodnotit úroveň kybernetické bezpečnosti, byla nejprve stanovena metodika této disertační práce, která spočívá ve správném použití vhodných vědeckých metod, které jsou uvedeny v kapitole 1.6.

Metodika této práce v zásadě kopíruje postup doporučovaný v metodologických příručkách, kdy nejprve dochází ke stanovení oblasti výzkumu, formulování výzkumných otázek, stanovení plánu výzkumu, získání dat, vyhodnocení dat, navržení metodiky hodnocení kybernetické odolnosti, otestování metodiky a sepsání zprávy o výzkumu[3]. V rámci práce pak byly vykonány následující kroky, ne nutně v tomto pořadí, protože občas bylo nutné se v rámci této práce opakovaně vracet a doplňovat a zpřesňovat zjištěné informace, ověřovat výzkumné předpoklady apod.:

[3] DISMAN, Miroslav, Olga ŠMÍDOVÁ a Jiři ORT. *Jak se vyrábí sociologická znalost* [online]. 2011 [cit. 15.07.2020]. ISBN 978-80-246-2619-2. Dostupné z: http://site.ebrary.com/id/10887146.; PUNCH, Keith. *Základy kvantitativního šetření*. Praha: Portál, 2008. ISBN 978-80-7367-381-9.; REICHEL, Jiří. *Kapitoly metodologie sociálních výzkumů*. Praha: Grada, 2009. ISBN 978-80-247-3006-6.

- Sestavit pracovní skupinu bezpečnostních expertů, kteří budou seznámeni s výzkumným úkolem, a se kterými budou konzultovány výzkumné předpoklady, a od kterých bude získáván expertní názor v okamžiku potřeby.

- Zjistit jaké informace jsou k vyřešení úkolu potřeba, tedy co je potřeba vědět, aby bylo možné takovou efektivní metodiku navrhnout. Jaký je stav našeho poznání a znalostí, tedy co víme, a co nevíme. Už od počátku bylo zřejmé, že je nutné porozumět tomu, co se odehrává v kyberprostoru.

- Sestavit výzkumné otázky, definovat výzkumné předpoklady a navrhnout způsob ověření těchto výzkumných předpokladů. Už zde je jasné, že bude nutné odpovědět na otázku, jakým hrozbám organizace čelí, a jaká opatření mají zavedena.

- Stanovit způsob získání těchto informací. Zde se nabízí dotazníkové šetření, ovšem je nutné položit správné otázky a použít správné pojmy, aby nedošlo k omylu.

- Provést literární rešerši, která se týká kyberprostoru a vztahů v něm, analyzovat bezpečnostní reporty a na základě této analýzy navrhnout vhodné otázky a správně je formulovat.

- Předložit okruh otázek týmu bezpečnostních expertů a následně navrhnout strukturu dotazníku.

- Formulovat otázky, sestavit dotazník, otestovat jej na menší skupině, zapracovat připomínky.

- Umístit dotazník na internet, vytvořit webové stránky s popisem cíle výzkumu, na které bude možné odkazovat.

- Vybrat firmy a respondenty, kteří budou osloveni, ideálně tak, aby byly zastoupeny organizace z různých odvětví, sektorů, různých velikostí apod. a tvořily tak reprezentativní vzorek.

- Naplánovat, jak budou oslovováni, stanovit harmonogram rozesílání e-mailů, zvolit adresu, ze které bude e-mail rozeslán.
- Zvolit formu oslovení tak, aby respondenti dotazník vyplnili zodpovědně a poctivě.
- Oslovit jednotlivé respondenty, po týdnu se připomenout, po dalším týdnu znovu, v případě, že by dotazník nevyplnili.
- Analyzovat průběžně zaslané dotazníky a vyhodnocovat validitu, reliabilitu a objektivitu dat.
- Analyzovat data a navrhnout vhodnou matematicko-statickou metodu vyhodnocení dat dle jejich množství a povahy.
- Vyhodnotit data v souladu s navrženou vědeckou metodou.
- Ověřit výzkumné předpoklady, přijmout nebo je zamítnout.
- Zodpovědět výzkumné otázky na základě vyhodnocení dat a ověřených výzkumných předpokladů.
- Sepsat dílčí závěry, na základě kterých bude možné navrhnout analytický model.
- Navrhnout analytický model pro zhodnocení bezpečnosti na základě identifikovaných největších hrozeb.
- Navrhnout na základě dílčích závěrů vhodnou sadu otázek k ověření přítomnosti bezpečnostních opatření vůči těmto hrozbám.
- Vytvořit aplikaci, která bude pro hodnocení bezpečnosti v konkrétní organizaci použita.
- Otestovat aplikaci v konkrétní organizaci.
- Uvést výsledky testování.

- Aktualizovat tuto práci a sepsat závěr.

V souladu s vytyčeným cílem této práce bylo nejprve nutné identifikovat zdroj, cíl a způsob vedení kybernetických útoků na jednotlivé ekonomické subjekty, aby následně bylo možné určit, jaká bezpečnostní opatření organizační nebo technické povahy v jednotlivých případech scházela anebo byla nedostatečná.

Za tímto účelem byla provedena **analýza hrozeb v kyberprostoru**, ke kterým došlo v posledních letech, a jak se tyto hrozby a kyberprostor průběhu let formoval a vyvíjel. Jako zdroj dat byly požity **relevantní statistiky ČSÚ a stanoviska bezpečnostních expertů** k největším útokům, které byly zveřejněny organizacemi, které se na vyšetřování těchto útoků podílely. Posuzován byl především vektor útoku, zneužité zranitelnosti a zdroje potřebné k realizaci, délka trvání a následky daného útoku. Následně byla **provedena syntéza těchto informací** a popsány hrozby a dopady pro jednotlivé sektory národního hospodářství.

Poté proběhl **kvalitativní výzkum s vybranými manažery a bezpečnostními experty, kdy byly formou hloubkového rozhovoru** identifikovány největší hrozby a vhodná organizačně technická opatření, která by měla být vůči těmto hrozbám nasazena.

Následně byla navrhnuta sada otázek a možných odpovědí, jejichž cílem bylo zjistit, jaká je skutečná úroveň bezpečnosti v dané organizaci. Tento model byl předložen ke zkoumání vybraným bezpečnostním expertům tvořícím pracovní skupinu a jejich stanoviska byla **zapracována za použití metody Delphi**.

Dále byl proveden **kvantitativní výzkum, kdy byli formou dotazníku** osloveni manažeři informační a kybernetické bezpečnosti v různých organizacích ohledně proběhnuvších kybernetických útoků, které byly na jejich organizace vedeny a jejich obavy ohledně možných útoků v blízké budoucnosti. Výsledky tohoto výzkumu byly opět podrobeny detailní analýze, kdy byly hledány společné znaky.

Za tímto účelem byl vytvořen jednoduchý analytický nástroj, který zobrazuje webový formulář se sadou otázek a možných odpovědí a po jejich zodpovězení pak stručné zhodnocení. To má podobu čísla vyjadřujícího úroveň dosažené bezpečnosti, umožňující rychlé porovnání, a dále pak uvádí doporučení k mitigaci jednotlivých hrozeb. Tento nástroj byl vytvořen v jazyce PHP, HTML, JS, CSS a

zveřejněn na webu www.cleverandsmart.cz a zpřístupněn laické i odborné veřejnosti.

1.5 Struktura práce

Tato disertační práce popisuje jeden z možných způsobů jak efektivně přistoupit k hodnocení úrovně kybernetické bezpečnosti v organizacích působících jak ve státním sektoru, tak i soukromé sféře. **Vlastní práce je rozdělena do několika na sebe navzájem navazujících částí, které tvoří jeden kompaktní celek.** Přes úvod a nezbytnou teoreticko-metodologickou část přechází v praktickou část popisující vlastní aplikovaný empirický výzkum a z něj pak vycházející doporučení a závěr.

V první úvodní kapitole je vysvětleno pozadí, tedy co tomuto výzkumu a práci předcházelo, dále je formulován samotný cíl této práce, omezení této práce, formulovány výzkumné otázky a nastíněn postup zpracování a struktura této práce a jsou uvedeny logické a empirické metody, které jsou v rámci této práce použity.

Druhá kapitola se věnuje současnému stavu řešené problematiky, vysvětlení základních pojmů používaných v oblasti kybernetické bezpečnosti, které jsou nezbytné k pochopení samotné podstaty kybernetických útoků v širších souvislostech. Následuje analýza kyberprostoru, jednotlivých prvků, z kterých se kyberprostor skládá, a vysvětlení, jaký je mezi nimi vztah a proč vůbec ke kybernetickým útokům dochází, proč počet těchto útoků roste, kdo za nimi stojí, jaký je motiv těchto útočníků, na koho jsou tyto útoky vedeny, co rozhoduje o tom, zda se organizace stane cílem kybernetického útoku či nikoliv, jaký to na ni může mít dopad. A zda lze zavedením vhodných bezpečnostních opatření organizační a technické povahy těmto útokům předcházet, včas je detekovat, adekvátně na ně reagovat, a minimalizovat tak dopady z nich vyplývající.

Třetí kapitola se věnuje analýze sekundárních zdrojů, identifikaci klíčových faktorů, které podstatným způsobem ovlivňují situaci v kyberprostoru, a vývoji kybernetických hrozeb na území ČR za posledních několik let. Dále popisuje realizaci vlastního empirického výzkumu a všeho, co s ním souviselo. Tedy formulaci výzkumných předpokladů, přípravu dotazníku, stanovení základního souboru, průběh dotazníkového šetření a jeho vyhodnocení.

Ve **čtvrté kapitole** je představena metodika hodnocení kybernetické odolnosti organizace, která vznikla na základě výsledků výzkumu, a zároveň je zde představena jednoduchá webová aplikace sloužící k vyhodnocení úrovně kybernetické bezpečnosti a popsán způsob jejího otestování ve zvolené organizaci a výsledy tohoto testu.

V **páté kapitole** jsou shrnuty přínosy této práce pro praxi, vědu a vzdělávání a jednotlivé subjekty, které hrají určitou roli v kyberprostoru a jsou cílem kybernetických útoků.

V **šesté kapitole** jsou uvedeny návrhy a doporučení pro manažery bezpečnosti ve státním i soukromém sektoru, které byť přímo nesouvisí s cílem této práce, tak byly identifikovány v rámci analýzy primárních a sekundárních zdrojů, a dále jsou zde uvedeny oblasti informační a kybernetické bezpečnosti, na které by se mohl další výzkum zaměřit.

V **sedmé kapitole** je formulován závěr.

1.6 Použité vědecké metody

V průběhu práce a samotného výzkumu byla vyslovena celá řada výzkumných předpokladů. Výzkumný předpoklad je jakási naše představa o vztahu mezi zkoumanými proměnnými a slouží k nalezení odpovědi na výzkumnou otázku[4]. Výzkumný předpoklad musí být proto formulován jednoznačně a to tak, aby bylo možné o jejím přijetí/potvrzení nebo zamítnutí/vyvrácení za použití příslušných vědeckých metod jednoznačně rozhodnout. Výzkumný předpoklad tedy musí obsahovat nějaké tvrzení a veličinu, kterou lze ověřit, a ta musí být kvalitativní nebo kvantitativní.

Vzhledem k tomu, že výsledkem této práce má být **metodika** umožňující rychlé zhodnocení kybernetické bezpečnosti a zároveň i v této práci je postupováno systematicky podle metodiky, je na místě uvést, co že to metodika vlastně je, a co lze od ní očekávat. Metodika uvádí konkrétní způsob řešení určitého problému, tedy jak má být k řešení daného problému přistoupeno a správně postupováno,

[4] MOLNÁR, Zdeněk. *Pokročilé metody vědecké práce*. Zeleneč: Profess Consulting, 2012. ISBN 978-80-7259-064-3. s. 33.

aby bylo dosaženo cíle[5]. Metodika může v rámci daného postupu uvádět i celou řadu vědeckých **metod**, tj. specifických způsobů ověřování určitého výzkumného předpokladu a rovněž i technik užitých při aplikování dané metody.

V rámci této disertační práce byla použita celá řada vědeckých metod. Při jejím zpracování byl použit veskrze **holistický přístup**, kdy na kyberprostor, který byl předmětem zkoumání, bylo nahlíženo jako na komplexní systém skládající se z mnoha vzájemně interagujících částí, a jehož zkoumání má i jistý interdisciplinární rozměr.

K lepšímu porozumění kyberprostoru byl použit **deskriptivní** přístup induktivního charakteru, který byl provázán s přístupem **explorativním** popisujícím závislosti a rovněž i přístupem **explanačním**, jehož cílem bylo objasnit, proč k daným situacím v kyberprostoru vůbec dochází, a konečně i přístupem **evaluačním**, který byl použit k hodnocení těchto jevů[6].

Hojně použity byly **logické metody**, mezi které lze zařadit dedukci, indukci, analýzu, syntézu, abstrakci a konkretizaci[7], včetně komparace a analogie[8]. Dále byly použity **metody empirické**, kam lze zařadit pozorování, měření a experiment[9].

Některé vztahy jsou vysvětleny např. na základě znalostí ekonomických tržních principů za použití **analogie**, kterou lze definovat jako proces nalézání podobného[10], ta byla ostatně použita již v úvodu při formulování cíle, kdy nelze přehlédnout určitou podobnost mezi hrozbami v reálném světě a hrozbami, ke kterým dochází v kyberprostoru.

V teoretické části práce byla provedena základní **analýza** kyberprostoru, spočívající v rozdělení celku na menší části[11], jejímž cílem bylo popsat, z jakých

---

[5] ŠIROKÝ, Jan. *Tvoříme a publikujeme odborné texty*. Brno: Computer Press, 2011. ISBN 978-80-251-3510-5. s. 28.
[6] YIN, Robert K. *Applications of case study research*. 3rd ed. Thousand Oaks, Calif: SAGE, 2012. ISBN 978-1-4129-8916-9. s. 167.
[7] HENDL, Jan. *Kvalitativní výzkum: základní teorie, metody a aplikace*. 2016. ISBN 978-80-262-0982-9. s. 32–34.
[8] ŠIROKÝ, Jan. *Tvoříme a publikujeme odborné texty*. Brno: Computer Press, 2011. ISBN 978-80-251-3510-5. s. 29.
[9] ŠIROKÝ, Jan. *Tvoříme a publikujeme odborné texty*. Brno: Computer Press, 2011. ISBN 978-80-251-3510-5. s. 15.
[10] ŠIROKÝ, Jan. *Tvoříme a publikujeme odborné texty*. Brno: Computer Press, 2011. ISBN 978-80-251-3510-5. s. 33.
[11] HENDL, Jan. *Kvalitativní výzkum: základní teorie, metody a aplikace*. 2016. ISBN 978-80-262-0982-9. s. 32.

klíčových prvků se kyberprostor, jakožto komplexní systém skládá, a jak spolu tyto jednotlivé prvky interagují a jaké jsou mezi nimi relace. V rámci této analýzy byly identifkováni a stručně charakterizováni jednotliví aktéři v kyberprostoru a klíčové faktory ovlivňující bezpečnost v kyberprostoru.

Dále byla použita **komparace**, která spočívá v porovnávání jistých vlastností[12]. V této práci byla použita především k identifikaci signifikantních rozdílů v použité fundamentální terminologii v oblasti kybernetické bezpečnosti, shodných znaků pokud jde o přístup k evaluaci bezpečnosti, stanovení určitých trendů, co do frekvence výskytu jednotlivých kybernetických hrozeb a doporučovaných bezpečnostních opatření, tak jak byly uváděny v bezpečnostních reportech, a s tím, s čím se autor této práce ve své dosavadní praxi setkal.

V rámci pracovní skupiny, která byla sestavena z bezpečnostních expertů, došlo k seznámení se s kybernetickými útoky a při jejich následném zkoumání byl použit explorační, explanatorní i evaluační přístup a byla rovněž zjištěná analogie s dalšími podobnými případy řešenými danými bezpečnostními experty v organizacích, kde působí. Na základě výše uvedených rozborů a dále pak **hloubkových rozhovorů** a za použití **metody Delphi** byl vytvořen kvantitativní dotazník čítající řadu otázek.

S vybranými respondenty pak byly vedeny i hloubkové rozhovory za účelem zjištění jejích názoru a ověření toho, jak situaci v kyberprostoru vnímají a jak se na výsledky dotazníkového šetření dívají. Při spojení těchto dvou metod, tedy kvantitativného dotazníkového šetření a kvalitativního rozhovoru, by se pak dalo hovořit jako o smíšeném výzkumu a použití metody **triangulace**[13].

Ke zpracování výsledků dotazníkového šetření a ověření výzkumných předpokladů a zodpovězení výzkumných otázek byly použity **matematicko-statistické** metody. Kromě základních matematických a statistických metod byla ve značné míře použita v rámci tohoto empirického výzkumu především **metoda věcné významnosti** a to především proto, že výběrový soubor byl pořízen na základě dostupnosti, a tudíž se jedná o nenáhodný výběr. Proto nelze závěry

[12] REICHEL, Jiří. *Kapitoly metodologie sociálních výzkumů*. Praha: Grada, 2009. ISBN 978-80-247-3006-6. s. 28.
[13] MOLNÁR, Zdeněk. *Pokročilé metody vědecké práce*. Zeleneč: Profess Consulting, 2012. ISBN 978-80-7259-064-3. s. 47–48.

zobecňovat na základní soubor a budou mít platnost pouze pro daný výběrový soubor. Pro ověřování vztahů mezi proměnnými nelze použít statistické testování hypotéz, právě s ohledem na neexistenci náhodného výběru. Pro ověřování vztahů mezi proměnnými bude tudíž využito pojmu „**ověřování výzkumného předpokladu**“ (tento pojem není omezen podmínkami induktivní statistiky).

Důvodem, proč jsou v rámci empirického výzkumu jeho výstupy posuzovány užitím věcné významnosti, je kladení důrazu na kritické posouzení a praktické využití analýzy dat. Soukup[14] uvádí, že věcná významnost výsledku znamená, že naměřený rozdíl či zjištěná souvislost je důležitá pro vědecké poznání či praktické účely. Věcná významnost umožňuje rozhodnout, zda o výsledku má smysl polemizovat a zdá má praktické důsledky, a to i pro vědecké účely. Ke zjištění, zda je výsledek věcně významný a v jakém rozsahu byl použit již zmíněný ukazatel, tzv. míry věcné významnosti („effect size“), a byly stanoveny **kritéria a ukazatele pro ověřování výzkumných předpokladů.**

1. Jako **základní kritérium** pro ověřování výzkumných předpokladů u kategorizovaných proměnných lze zvolit **věcnou významnost reálného rozdílu na úrovni 10 %**[15] mezi adekvátními řádkovými relativními četnostmi v rámci porovnávaných uzlů u klasifikačních stromů (stejné řádky u koncových uzlů klasifikačního stromu, které mají největší heuristický význam).

2. Jako **pomocný ukazatel** zjištěných věcně významných rozdílů bude použit pro **nominální proměnné** asymetrické **Goodmanovo a Kruskalovo tau**, které má přímou procentuální interpretaci. Goodmanovo a Kruskalovo tau vyjadřuje podíl vysvětleného „nomvar“ závislé nominální proměnné ve třídách nominální proměnné nezávislé.

[14] SOUKUP, Petr. Substantive significance and it´s measures. *Data and Research – SDA Info* [online]. 2013, roč. 127, č. 2 [cit. 01.02.2022]. ISSN 23362391. DOI:10.13060/23362391.2013.127.2.41.

[15] Dosavadní zkušenosti z analýzy dat ukazují, že zjištěný minimální 10% rozdíl v řádkových relativních četnostech je zpravidla doprovázen min. velikostí Cohenova indexu „w“ na úrovni w ≥ 0,10.

3. Za situace asymetrického vlivu **nominální proměnné na proměnnou ordinální** bude použit Řehákův koeficient asociace β (ordinální regresní závislosti).[16] Asymetrický koeficient β vyjadřuje podíl vysvětleného rozptylu ordinální proměnné B ve třídách nominální proměnné A. Ordinální statistická závislost se projevuje ve změně tvaru podmíněných rozložení nebo posunutí na škále znaku. Pokud 95% interval spolehlivosti u koeficientu β obsahuje nulovou hodnotu, znamená to, že rozsah výběrového souboru by měl být větší. Měření věcně významného vlivu zabezpečuje symetrický index Cohenovo w.[17]

Při porovnání hodnot asymetrických koeficientů asociace respektujeme stanovisko de Vause. Dle něj obecně platí, jestliže Goodman a Kruskalovo tau je vyšší než koeficient β, pak to pravděpodobně signalizuje existenci nominálního statistického vztahu, nikoli ordinálního.[18]

Tabulka 1 – Effect size classes uvádí přehled používaných koeficientů a indexů věcné významnosti, index *w* s vymezením věcně významného vlivu (0,1 – malý věcně významný vliv, 0,3 – střední věcně významný vliv, 0,5 – velký věcně významný vliv).[19]

[16] ŘEHÁK, Jan a Blanka ŘEHÁKOVÁ. *Analýza kategorizovaných dat v sociologii*. Praha: Academia, 1986. s. 250.
[17] V případě příznivějších hodnot asymetrických koeficientů asociace (tau, β) je upřednostníme před hodnotami symetrického Cohenova indexu w.
[18] DE VAUS, D. A. *Surveys in social research*. Sixth edition. Abingdon, Oxon: Routledge, 2014. Social research today. ISBN 978-0-415-53015-6. s. 260–262.
[19] ELLIS, Paul D. *The essential guide to effect sizes: statistical power, meta-analysis, and the interpretation of research results*. Cambridge ; New York: Cambridge University Press, 2010. ISBN 978-0-521-19423-5. s. 41.

Tabulka 1 – Effect size classes

Test	Relevant effect size	Effect size classes		
		Small	Medium	Large
Comparison of independent means	d, Δ, Hedges' g	.20	.50	.80
Comparison of two correlations	q	.10	.30	.50
Difference between proportions	Cohen's g	.05	.15	.25
Correlation	r	.10	.30	.50
	r^2	.01	.09	.25
Crosstabulation	w, φ, V, C	.10	.30	.50
ANOVA	f	.10	.25	.40
	η^2	.01	.06	.14
Multiple regression	R^2	.02	.13	.26
	f^2	.02	.15	.35

Zdroj: ELLIS, Paul D. The essential guide to effect sizes: statistical power, meta-analysis, and the interpretation of research results. Cambridge ; New York: Cambridge University Press, 2010, s. 41. ISBN 978-0-521-19423-5.

Z uvedených měr se s ohledem na svůj obsah nejvíce koeficientu β blíží čtverec ukazatele eta (η^2). Vzhledem k tomu, že asymetrický koeficient tau i koeficient β mají přímou, procentuální interpretaci, lze analogicky přijmout pro jejich interpretaci konvenčně uznávané hodnoty koeficientu eta (η^2). Svými hodnotami 0,01 (malý efekt); 0,06 (střední efekt) a 0,14 (velký efekt) nabízí určité srovnávací hranice i pro koeficient β. Je však třeba mít na paměti, že jde o míru parametrického testu ANOVA.[20]

S ohledem na to, že typ respondenta (prediktor) má nominální charakter a většina analyzovaných proměnných kybernetické bezpečnosti jsou ordinálního typu, byla v analýze zjišťována ordinální asymetrická asociace založená na asymetrickém koeficientu β (beta). Jde o regresní koeficient ordinální statistické závislosti. Jeho velikost signalizuje, o kolik % zlepšíme odhad znalosti rozložení odpovědí závisle ordinální proměnné (posuzovaný aspekt kybernetické bezpečnosti) poznáním rozložení nezávisle nominální proměnné (typ respondenta). Pokud jde o to, jak velká hodnota obou koeficientů je potřebná

[20] KIRK, Roger E. *Statistics: an introduction*. 5th ed. Belmont, CA: Thomson/Wadsworth, 2008. ISBN 978-0-534-56478-0. s. 475.

k nalezení akceptovatelné asociace, tak lze uvést stanovisko dvou významných českých statistiků, působících v sociálních vědách.

„Při aplikacích vždy vzniká otázka, jaká hodnota koeficientů je vysoká. Význam číselné hodnoty závisí na věcném významu proměnných a na modelu, který používáme. Jestliže očekáváme, že A je jedinou příčinou B, pak význam budou mít hodnoty vyšší než 0.6 nebo 0.7. Je-li A jednou z několika málo paralelních příčin heterogenity vzhledem k B, pak koeficienty 0.3, 0.5 budou vysoké. Je-li však A jednou z mnoha drobných příčin, pak i koeficient 0.1 či 0.05 je interpretovatelný. (Uvedené hodnoty jsou uvedeny subjektivně, a proto je nelze přijmout jednoznačně a s konečnou platností.)“[21]

Uvedená úvaha výše uvedených autorů naznačuje, že posouzení velikosti efektu asociace mezi proměnnými je subjektivní záležitostí výzkumníka při respektování věcného významu proměnných a modelu, který je použit. V praktické analýze, při hledání skutečně akceptovatelných efektů se stále více dostává do popředí tzv. analýza věcné významnosti (effect of size). V tomto směru byly odbornou veřejností přijaty, i když ne s plným koncensem odborníků, určité konvence, které mají sloužit výzkumníkům v ne příliš jasných případech ve stanovení hranic (intervalů), kdy lze zjištěný efekt (skutečně zjištěný rozdíl) považovat z věcného hlediska za akceptovatelný.

Pro analýzu závislostí mezi vybranými kategorizovanými proměnnými byl použit program IBM SPSS Modeler V18.2.1, konkrétně jeho modul pro vytvoření klasifikačního stromu prostřednictvím algoritmu CHAID / C5.0. Pro výpočet asymetrického koeficientu Goodman a Kruskal tau byl použit program IBM SPSS Statistics V26. Pro výpočet asymetrického koeficientu β byla využita utilita nadstandardně vytvořená pro systém SPSS. Cohenův index w byl zjištěn za pomoci programu NCSS PASS.

Pro jednoduché výpočty jako je stanovení absolutní a relativní četnosti, minima a maxim analyzovaných hodnot a tvorbu grafů bude použit MS Excel.

Za stěžejní a nejvíce používanou metodu této práce je však nutné považovat i **indukci**, která byla použita k vyhodnocení výsledků dotazníkového šetření,

[21] ŘEHÁK, Jan; ŘEHÁKOVÁ Blanka. *Analýza kategorizovaných dat v sociologii*. Praha: Academia, 1986, s. 252.

a která umožnila stanovit nejzávažnější hrozby a nejčastější vektory útoku, kterým organizace v ČR čelí, a následně navrhnout vhodná opatření vůči těmto útokům.

Dále byla opakovaně použita **kreativní abdukce** za účelem zformulování několika výzkumných předpokladů, jejichž cílem bylo ověřit, zda jsou mezi organizacemi o různé velikosti a působících v různých odvětvích, sektorech a provozující rozličné systémy, nějaké věcně významné rozdíly, které by měly být zohledněny v hodnocení kybernetické bezpečnosti dané organizace. Zjištěné rozdíly pak vedly za použití **reduktivní abdukce** k formulaci výzkumných předpokladů snažící se o nejlepší možné vysvětlení[22], které by mohlo být předmětem dalšího výzkumu.

Následně proběhla **syntéza** získaných informací a byla sestavena jednoduchá matice hrozba vs. opatření, která mapuje, vůči jakým kybernetickým hrozbám se uplatňují jednotlivá bezpečnostní opatření, přičemž byla volena ta nejúčinnější.

V okamžiku, kdy byly známy hrozby a opatření vůči těmto hrozbám, tak byla za použití **dedukce** pečlivě formulována sada ne více jak tuctu otázek, které ověřují zavedení určitých bezpečnostních opatření, uvedených v bezpečnostních standardech jako vhodná opatření vůči těmto kybernetickým hrozbám, a umožňují tak zjistit, jak na tom organizace je, co do odolnosti vůči uvažovaným kybernetickým hrozbám.

Následně byl za použití **abstrakce**, kterou lze definovat jako proces, kdy dochází k oddělení nepodstatných vlastností[23], vytvořen **model**, ve kterém bylo zkoumáno, jaké hrozby na organizaci působí a jaká opatření by ji mohla před těmito hrozbami ochránit. Tento model pak byl přetvořen v jednoduchou webovou aplikaci, která po zodpovězení sady otázek provede vlastní vyhodnocení.

Tento model pak byl použit v rámci dotazníkového šetření ve vybrané organizaci, kdy byly v rámci jeho použití pozorovány a vyhodnocovány i bezprostřední reakce respondentů.

---

[22] PEIRCE, Charles S., Charles HARTSHORNE, Paul WEISS a Charles S. PEIRCE. *Scientific metaphysics*. 4. print. Cambridge, Mass: Belknap Press of Harvard Univ. Press, 1978. Collected papers of Charles Sanders Peirce, ed. by Charles Hartshorne ...; Vol. 6. ISBN 978-0-674-13802-5.

[23] OCHRANA, František, Vladimír ČECHÁK, Miroslav KRČ, Lenka SČERBANIČOVÁ a Jan SERÝCH. *Metodologie sociálních věd* [online]. 2013 [cit. 16.07.2020]. ISBN 978-80-246-2454-9. Dostupné z: http://site.ebrary.com/id/10852898, s. 37.

2 SOUČASNÝ STAV ŘEŠENÉ PROBLEMATIKY – teoretická část

Hodnocení kybernetické bezpečnosti a odolnosti organizace vychází z předpokladu, že každá organizace má, ať už formálně anebo neformálně, zaveden na určitém stupni vyzrálosti nějaký systém řízení informační bezpečnosti, jehož je kybernetická bezpečnost nedílnou součástí.

Základem řízení bezpečnosti je pak zpravidla řada norem jako je např. ISO/IEC 27001 a ISO/IEC 27002[24], která obsahuje 114 bezpečnostních opatření, případně NIST Cyber Security Framework for Improving Critical Infrastructure Cybersecurity[25], který obsahuje 98 bezpečnostních požadavků, anebo v ČR platný Zákon o kybernetické bezpečnosti a související Vyhláška o kybernetické bezpečnosti[26], která pak obsahuje 759 požadavků, v případě kritické informační infrastruktury.

Tyto normativy jsou průběžně revidovány a obsahují celou řadu doporučení a bezpečnostních opatření, která by organizace měla zavést. První dva pak mají celosvětovou působnost, posledně jmenovaný je pak závazný pro vybrané organizace v ČR. Lze rovněž prohlásit, že obsahují best practice neboli nejlepší praktiky v oboru, protože jsou vytvářeny odborníky působícími v mnoha různých organizacích v ČR i po celém světě.

Cílem této práce však není komparativní analýza jednotlivých přístupů, metodik a normativů co do počtu a kvality uváděných opatření, tomu se věnují jiné práce. Ve své podstatě totiž není ani tak důležité jestli ten či onen normativ a z něj vycházející nástroj uvádí a obsahuje několik stovek nebo dokonce tisíce bezpečnostních opatření. Tyto nejznámější normativy a počet v nich obsažených opatření je zde uveden jen proto, aby bylo zřejmé, že byly vzaty v úvahu, a že **počet bezpečnostních opatření je značný a rovněž i následné zjištění, zda**

---

[24] ČSN ISO/IEC 27002. *Informační technologie - Bezpečnostní techniky - Soubor postupů pro opatření bezpečnosti informací*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví. 2014.

[25] NIST. *Framework for Improving Critical Infrastructure Cybersecurity* [online]. 2014 [cit. 18.12.2019]. Dostupné z: https://www.nist.gov/document/cybersecurity-framework-021214pdf

[26] ČESKO. Vyhláška č. 82/2018 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) [online]. 2018. ISSN 1211-1244. Dostupné z: https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=38431

jsou příslušná opatření zavedena nebo ne, je otázkou několika dlouhých týdnů. Jak ostatně vyplynulo i z odpovědí oslovených manažerů informační a kybernetické bezpečnosti, a proto je nelze využít k rychlému vyhodnocení bezpečnosti v organizaci.

Nejrůznější frameworky a analytické nástroje sloužící k hodnocení bezpečnosti z pohledu rizik, pak z těchto normativů rovněž vycházejí. Jejich největší hodnota by pak měla spočívat v tom, že obsahují relevantní hrozby, zranitelnosti a vůči nim navrhnutá bezpečnostní opatření. Podmiňovací způsob v předchozí větě však není zvolen náhodou, protože skutečnost je taková, že **situace v kyberprostoru se velice rychle mění, objevují se nové hrozby, zranitelnosti a vektory útoku a proti nim je třeba nasazovat adekvátní bezpečnostní opatření**.

Za tímto účelem je nutné věnovat dostatečnou pozornost monitoringu a analýze situace v kyberprostoru, k čemuž je možné využít prostředků cyber threat intelligence, zkr. CTI, a hlášení o indikátorech kompromitace, zkr. IoC, a indikátorech útoku, zkr. IoA. Jedině studiem aktuálních bezpečnostních reportů, bulletinů a v prvé řadě sledováním securitu dashboardů, důsledným vyhodnocováním hlášení z nejrůznějších bezpečnostních řešení a analýzou bezpečnostních logů, je možné v kombinaci se CTI včas a adekvátně reagovat na probíhající kybernetický útok.

Dále je nutné si uvědomit, že informace o probíhajících nebo proběhnuvších kybernetických útocích, které se objeví ve veřejně dostupných sekundárních zdrojích, představují jen pověstnou špičku ledovce a pro skutečné poznání se musíme ponořit mnohem hlouběji pod hladinu. Proto je i v této práci **kladen větší důraz na hloubkové rozhovory s bezpečnostními experty a výsledky vlastního dotazníkového šetření, než na informace uvedené v bezpečnostních reportech**, které posloužily spíš jen pro stanovení vhodných okruhů otázek, na které se zaměřuje samotný výzkum.

Právě výše uvedená skutečnost, tedy že veřejně dostupné informace popisují jen některé vybrané případy, ke kterým v kyberprostoru došlo, představuje zásadní nedostatek, který nám v brání v poznání toho, co se v kyberprostoru skutečně odehrává. **Při hodnocení bezpečnosti se běžně vyhodnocuje zavedení všech bezpečnostních opatření, což neumožňuje rychle zjistit skutečnou úroveň bezpečnosti** v dané organizaci a dost často pak dochází pod

dojmem úspěšného zavedení odpovídajících procesů a opatření k vytvoření pouhé falešné iluze bezpečí.

Ostatně tento stav poměrně bryskně vystihují i slova jedné bývalé auditorky provádějící audit v jedné nejmenované zahraniční korporaci v ČR. Ta v narážce na použitou zkratku BIS pro oddělení bezpečnosti informačních systémů, komentovala výsledek několika týdenního auditu slovy:

„They are just Building Illusion of Security.“[27]

Tato práce z výše uvedeného důvodu nechce hodnotit množství a úroveň zavedených procesů, nýbrž výsledek, tedy čeho je možné dosáhnout z pohledu útočníka, jakou škodu je možné způsobit a zda jsou zavedena taková bezpečnostní opatření, která by tomu mohla zabránit anebo případnou škodu alespoň minimalizovat.

2.1 Vymezení základních pojmů

Nacházíme se v době, která se nazývá informační nebo také znalostní ekonomikou, a kdy jsou informace a znalosti považovány za ta nejcennější aktiva. Protože ten, kdo má ty správné informace a umí jich i efektivně využít, získává nezanedbatelnou konkurenční výhodu.

Nelze se tak divit, že na informační systémy, v kterých jsou tyto informace v elektronické podobě zpracovávány, přenášeny a uchovávány, jsou vedeny permanentní kybernetické útoky, o kterých většina subjektů nemá vůbec tušení a mnohdy se o nich nedozví ani poté, co tyto útoky proběhly a dosáhly svého cíle.

To je dáno především nehmotnou podobou informací, které když jsou zcizeny, tak na rozdíl od hmotných aktiv nikomu neschází a zhoršující se ekonomická situace organizace je pak zpravidla přisuzována jiným skutečnostem, než právě proběhnuvšímu kybernetickému útoku.

Zatímco v počátcích informační éry, kdy ještě počítače nebyly připojeny do internetu, musel útočník fyzicky proniknout do objektu, ve kterém se počítač nacházel, a tam informace zkopírovat či pozměnit, tak v pozdějších letech, jak se

[27] Což by se dalo přeložit jako: „Oni jen vytvářejí iluzi bezpečí.“

organizace začaly postupně připojovat do internetu, to již nebylo nutné a bylo možné začít vést útoky s minimálními náklady a rizikem odhalení prakticky z jakéhokoliv počítače připojeného do internetu. Vzdálenost mezi útočníkem a obětí se začala prodlužovat a pachatel se ani nemusí fyzicky nacházet na místě činu, a to před, během a ani po jeho spáchání.

Pro lepší pochopení této skutečnosti je vhodné nahlédnout do nedávné historie a připomenout si, jak na území České republiky, dále jen ČR, docházelo k postupnému pronikání počítačů do domácností a organizací a jejich následnému připojování do internetu a s jakými kybernetickými útoky jsme se mohli tehdy setkat, s jakými kybernetickými útoky se potýkáme nyní a konečně jakým kybernetickým útokům budeme čelit v nejbližší budoucnosti.

Porozumění minulosti nám pomůže lépe pochopit současnost a predikovat i možný budoucí vývoj kybernetických útoků a připravit se na nové kybernetické útoky přijetím vhodných bezpečnostních opatření organizační a technické povahy.

Ne všechny organizace však vnímají riziko kybernetický útoků na jejich informační systémy stejně, a proto nezavedly ani základní bezpečností opatření. Aby však bylo možné posoudit, zda přijatá bezpečnostní opatření jsou adekvátní či nikoliv a v ideálním případě jsme měli i možnost úroveň bezpečnosti v organizacích nějakým způsobem měřit, musíme nejprve porozumět tomu, co přesně se v kyberprostoru odehrává.

Tedy jak se kyberprostor formuje, kdo přesně za útoky v kyberprostoru stojí a jaký je jeho skutečný motiv a cíl, jak kybernetické útoky probíhají, s jakými typy útoků se můžeme setkat, jaká je četnost těchto útoků v čase, jakých zranitelností tyto útoky zneužívají, jaké jsou náklady na jejich realizaci, jaký je jejich dopad a zda jednotlivé útoky vykazují nějaké společné charakteristiky a indikují opatření, která by vůči těmto útokům měla být zavedena, aby se daly včas detekovat, zastavit a zabránit jejich opakování.

V této kapitole a příslušných podkapitolách jsou vysvětleny základní pojmy a vztahy mezi jednotlivými subjekty v kyberprostoru, které **by měly umožnit snáze porozumět problematice, která je v rámci této práce řešena**. Jedná se především o definici pojmu kyberprostor, aktivum, vlastník, kybernetická hrozba,

agent hrozby, zdroj hrozby, kybernetický útok, zranitelnost, životní cyklus zranitelnosti, vektor útoku, dopad a opatření[28].

Pokud je v textu dále použit pojem organizace, tak jím jsou míněny jak firmy založené za účelem dosažení zisku, tak i podniky jednotlivce a rovněž i organizace, jejichž cílem není generovat zisk, ale poskytovat jen vybrané služby domácnostem, odvětvím jako je např. školství, zdravotnictví, policie, soudy, uzemní samospráva a vůbec veškeré organizační složky státu.

2.1.1 Kyberprostor

Pokud hovoříme o kybernetických útocích z kyberprostoru, je nejprve nutné tyto pojmy definovat. Dle Marco Mayera není pojem kyberprostor (cyberspace) ustálen, vyvíjí se a je definován různě, takže neexistuje jedna jediná definice[29].

Poprvé tento pojem použil William Gibson v roce 1982 ve své povídce Burning Chrome a o dva roky později pak ve svém románu Neuromancer v kontextu globální počítačové sítě, do které se lidé připojují, žijí v ní své životy a stávají se na ní závislí[30]. Další autoři sci-fi pak začali tento pojem rovněž používat a vznikl specifický žánr cyberpunk.

Dle amerického NIST představuje kyberprostor komplexní prostředí, ve kterém se odehrává interakce mezi lidmi, softwarem a službami a to prostřednictvím vzájemně propojených počítačových sítí a technologických zařízení[31].

Z výše uvedeného můžeme odvodit, že kyberprostor nemá jasně definované hranice, resp. ty jsou dány pouhým fyzickým umístěním prvků, z kterých se kyberprostor skládá. A prvky, ze kterých se kyberprostor skládá, jsou tři, a to hardware (HW), software (SW) a lidé.

---

[28] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary.* Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6.

[29] MAYER, Marco, Iacopo CHIURAGI a Niccolo DE SCALZI. La politica Internazionale nell'Era Digitale (bozza da non citare) [online]. 2013, roč. 27 [cit. 16.02.2019]. Dostupné z: https://www.academia.edu/4509736/La_politica_Internazionale_nellEra_Digitale_bozza_da_non_citare_

[30] GIBSON, William. *Neuromancer*. 5. vyd. Praha: Euromedia Group, 2019. Mistrovská díla SF. ISBN 978-80-7617-760-4.

[31] PAULSEN, Celia a Robert BYERS. *Glossary of key information security terms* [online]. NIST IR 7298r3. Gaithersburg, MD: National Institute of Standards and Technology. 2019 [cit. 02.02.2022]. DOI: 10.6028/NIST.IR.7298r3.

Za vrstvu HW lze považovat veškeré hmotné vybavení, jako jsou servery, síťové prvky, přepínače, směrovače, firewally, bezdrátové přístupové body a stejně tak i osobní počítače, tablety, chytré telefony, průmyslové řídicí systémy, zkr. ICS/SCADA nebo také **operační/provozní technologie**, ale i veškerá zařízení vybavená mikroprocesorem a disponující vstupy/výstupy a patřící do tzv. internetu věcí (Internet of Things, zkr. IoT).

Za vrstvu SW pak lze považovat veškeré nehmotné vybavení, jako jsou operační systémy, které běží na těchto serverech, koncových zařízeních a síťových prvcích a zajišťující základní funkce pro práci s daty a komunikaci, a dále pak specifické aplikace, jednoúčelové programy a samotná data.

Za vrstvu lidé pak lze považovat všechny osoby, které se v kyberprostoru pohybují, využívají služeb systému, interagují s ostatními a spravují daný systém, tj. zajišťují jeho funkčnost a utvářejí jej, tedy připojují do něj další prvky.

Vzhledem k tomu, že na všechny tyto vrstvy je možné vést kybernetický útok (cyber attack), je od roku 2006 kyberprostor v národní strategii pro vojenské operace považován za pátou doménu, stojící na stejné úrovni jako souš, moře, vzduch a vesmír. Nicméně i o tomto rozhodnutí se stále vedou diskuse, neboť část odborníků na tuto doménu nahlíží jako na integrální součást všech ostatních domén, která všemi prostupuje a tvoří jejich neoddělitelnou součást, jak uvádí např. Bastl a Gruberová[32].

Obzvlášť problematická je pak identifikace jednotlivých aktérů v kyberprostoru, kdy na jedné straně proti sobě stojí právo na ochranu soukromí a na straně druhé pak požadavek na to, aby nebylo zasahováno do cizích práv a existovala možnost jednotlivé aktéry identifikovat, dopadnout je, vznést proti nim obvinění a odsoudit je. Většina států, která bere situaci v kyberprostoru vážně a je si vědoma rizika kybernetických útoků, chce mít v rámci národní bezpečnosti a sledování svých ekonomických a politických zájmů možnost situaci v kyberprostoru monitorovat a je jedno, zda se jedná o USA, Rusko, Čínu, Izrael anebo ČR.

[32] BASTL, Martin a Zuzana GRUBEROVÁ. Kyberprostor jako „pátá doména"? *Vojenské rozhledy* [online]. 2013, roč. 22, č. 4. ISSN 12103292, 23362995. DOI: 10.3849/2336-2995.22.2013.04.010-021 s. 10–21

Není však zcela vyřešena otázka, jak na kybernetický útok v kyberprostoru reagovat[33], a jak reagovat na útok, který můžeme, pokud je veden ze strany jiné mocnosti, nazvat kybernetickou válkou (cyberwarfare). Je tomu tak proto, že zatímco u fyzických útoků je zřejmé, kdo daný útok vede a zpravidla i takový útok za použití konvenčních zbraní probíhá na svrchovaném území, tak zde může útok probíhat i z mnoha různých států současně a ty o tom, že z kyberprostoru, který se fyzicky nachází na jejich území anebo z jejich systémů, které se nachází kdesi v cloudu, nemusí ani vědět, neboť dané systémy mohl někdo kompromitovat, začlenit je do botnetu a následně je zneužít k útoku.

Tím před námi zároveň vyvstává i další otázka, kdo by měl kyberprostor kontrolovat a zda již dnes není kyberprostor pod kontrolou určitých mocností, které pod záminkou boje proti kyberzločinu (cyber crime) a kyberterorismu (cyber terorrism) nesledují čistě jen svoje ekonomicko-politické zájmy. Jako příklad lze uvést požadavky omezení vývozu silné kryptografie, či jejího úmyslného oslabení, začlenění legitimních zadních vrátek (backdoorů) do systémů ze strany NSA v podobě EES[34] či obvinění ČLR a její vlajkové lodě společnosti Huawei v prosinci 2018 z úmyslného začlenění zranitelností, což se následně nepotvrdilo[35], zatímco třeba u Cisca ano[36]. Z výše uvedených konkrétních případů je patrné, že **povědomí o situaci v kyberprostoru si nelze utvářet jen na základě řízeně uvolňovaných informací z veřejně dostupných zdrojů, ale je v tomto směru nutný vlastní výzkum**.

Zde je třeba si uvědomit, že v okamžiku, kdy se jakákoliv společnost stane na trhu s prostředky výpočetní techniky dominantní a její zařízení jsou v kyberprostoru masivně nasazovány a používány ze strany vládních i nevládních organizací a soukromých subjektů, stávají se tyto prvky pro útočníky nesmírně

---

[33] POLČÁK, Radim, Jakub HARAŠTA a Václav STUPKA. *Právní problémy kybernetické bezpečnosti*. Brno: Masarykova univerzita, 2016. Spisy Právnické Fakulty Masarykovy Univerzity, svazek č. 576. Řada teoretická. ISBN 978-80-210-8426-1. s. 49.

[34] *The Administration's Clipper Chip Key Escrow Encryption Program*. B.m.: Forgotten Books, 2018. ISBN 978-0-484-26866-0.

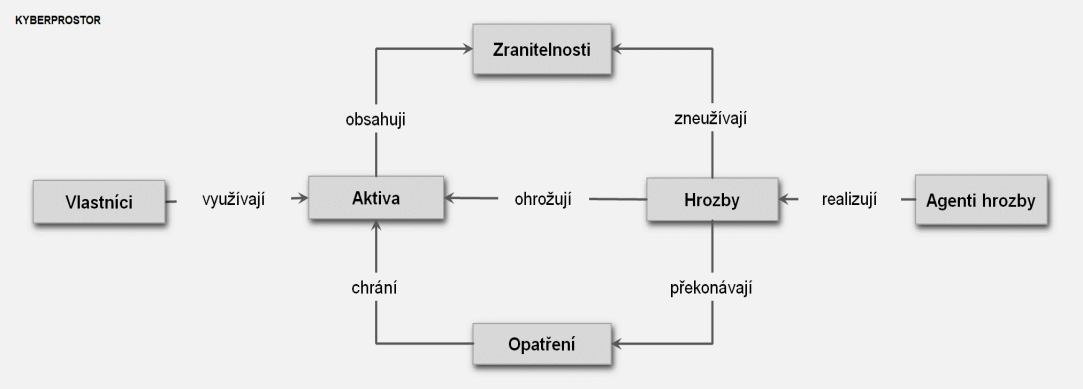
[35] Bundesamt spricht sich gegen Huawei-Boykott aus. *Spiegel.de* [online]. 2018 [cit. 09.05.2021]. Dostupné z: https://www.spiegel.de/netzwelt/netzpolitik/5g-netzausbau-bsi-spricht-sich-gegen-huawei-boykott-aus-a-1243708.html

[36] CIMPANU, Catalin. Cisco removed its seventh backdoor account this year, and that's a good thing. *ZDNet* [online]. 2018 [cit. 09.05.2021]. Dostupné z: https://www.zdnet.com/article/cisco-removed-its-seventh-backdoor-account-this-year-and-thats-a-good-thing/

atraktivní a motivuje je to k aktivnímu hledání zranitelností a k jejich následnému zneužívání.

Situaci v kyberprostoru lze vyjádřit pomocí poměrně jednoduchého modelu, zachycuje ji Obrázek 1 – Situace v kyberprostoru.

Obrázek 1 – Situace v kyberprostoru



Z obrázku je patrné, že v kyberprostoru dochází k neustále interakci mezi vlastníkem, resp. provozovatelem systému na jedné straně a útočníkem na straně druhé, který se snaží realizovat hrozbu a zneužít nějaké zranitelnosti v aktivech, které vlastníkovi přináší užitek, a způsobit mu škodu. Jednotlivé komponenty tohoto modelu jsou detailně popsány v následujících kapitolách.

2.1.2 Agent hrozby a vlastník

V kyberprostoru proti sobě stojí na jedné straně vlastník provozující nějaký informační systém a na straně druhé pak agent hrozby (threat agent nebo také threat actor), dále jen útočník, který realizuje hrozbu v podobě kybernetického útoku. Současná legislativa pojem agent hrozby nedefinuje a neuvádí ani jednotlivé typy zdrojů hrozeb[37].

Agent hrozby

Za kybernetickými útoky může stát útočník disponující různou motivací, schopnostmi a prostředky k realizaci v zásadě jakékoliv generické nebo specifické

[37] ČERMÁK, Miroslav. Cyber threat management: zdroje hrozeb. *CleverAndSmart Management Consulting* [online]. 2020 [cit. 10.07.2021]. ISSN 2694-9830. Dostupné z: https://www.cleverandsmart.cz/cyber-threat-management-zdroje-hrozeb/

hrozby. Ovšem ne každý útočník, kterým může být jedinec nebo skupina[38], disponuje odpovídajícími znalostmi, schopnostmi a prostředky k tomu, aby mohl danou hrozbu realizovat. Organizace si musí uvědomit, proti jakému útočníkovi se chce vlastně chránit, a podle toho volit i odpovídající bezpečnostní opatření, neboť útočníkem mohou být[39]:

- **haktivisté** reagující na určité společenské události, kroky vlády nebo korporací, mohou i nemusí být koordinování, ale zpravidla jsou, aby jejich akce měla požadovaný efekt, tj. aby se o ní mluvilo, výsledkem je defacement webu, koordinovaný DDoS, využívají známých zranitelností a dostupných nástrojů, spíš než způsobit škodu se na sebe a na své téma snaží upozornit;

- **kyberteroristi** usilující o narušení kritické informační infrastruktury a na rozdíl od hacktivistů je jejich cílem způsobení i co největší škody;

- **kyberkriminálníci** a organizované kriminální skupiny, jejichž motivem je získání finančních prostředků nebo ovládnutí infrastruktury k zastírání svých nelegálních aktivit, jako jsou krádeže osobních údajů, přihlašovacích údajů, převody peněz z účtů, využívjí již hotových nástrojů, zneužívají zranitelností nultého dne, nakupují již hotové exploit kity;

- **hackeři** napadající špatně zabezpečené systémy, zabývají se odhalováním zranitelností, vývojem a prodejem exploitů, záleží na nich, zda budou white hackeři anebo black hackeři a zda budou jednat v souladu se zákonem anebo se z nich stanou kriminálníci;

- **script kiddies** kteří zpravidla neumí napsat vlastní kód, a proto stahují již hotové exploity z internetu a ty spouští proti nejrůznějším zdrojům, aby se

[38] PAULSEN, Celia a Robert BYERS. *Glossary of key information security terms* [online]. NIST IR 7298r3. Gaithersburg, MD: National Institute of Standards and Technology. 2019 [cit. 02.02.2022]. DOI: 10.6028/NIST.IR.7298r3.
[39] ČERMÁK, Miroslav. Identifikace klíčových aktérů ovlivňujících subjektivní percepci událostí v kyberprostoru. *Bezpečnostní teorie a praxe*. 2020, roč. 2020, č. 3. ISSN 2571-4589. s. 81–104

mohli pochlubit mezi svými vrstevníky anebo tak činí prostě jen pro svoje potěšení a škody způsobují spíš svoji nerozvážností a neznalostí;

- **státy** a organizační složky státu, které v kyberprostoru vedou kybernetickou válku, která je mnohdy součástí hybridní války. Patří sem jak strategická komunikace, tak i informační operace defenzivní i ofenzivní povahy[40];

- **státem sponzorované skupiny** vedoucí útoky s cílem ochromit kritickou infrastrukturu protivníka, získat informace, zneužívají zranitelností nultého dne, které nakupují, případně je sami vyhledávají a vyvíjí vlastní exploity, napadají dodavatelsko-odběratelské mezičlánky, infikují HW, na rozdíl od kyberteroristů se snaží pracovat skrytě, aby nebyly odhaleny;

- **konkurence** dost často stojící za krádeží intelektuálního vlastnictví a průmyslovou špionáží, kterou může realizovat i v kyberprostoru;

- **insideři** neboli nespokojení zaměstnanci, manažeři, dodavatelé zneužívají svého legitimního přístupu a znalosti business procesů a interních kontrol ke krádeži firemního know-how, chráněných receptur, klientského portfolia, převodu finančních prostředků, případně i spolupracující s někým z vnějšího prostředí.

Hranice mezi jednotlivými aktéry není vždy zcela zřejmá, ovšem pro pochopení toho, co se odehrává v kyberprostoru je porozumění motivů jednotlivých aktérů klíčové, neboť umožňuje lépe pochopit, jak kybernetické útoky probíhají a na koho a proč jsou vedeny. Neschopnost určit zdroj hrozby pak často vede k mylnému závěru ohledně skutečného cíle probíhajícího útoku a dochází tak k vyvozování mylných závěrů ohledně skutečné situace v kyberprostoru[41].

[40] ŘEHKA, Karel. *Informační válka*. Vydání první. Praha: Academia, 2017. Edice XXI. století, sv. 46. ISBN 978-80-200-2770-2. s. 140.
[41] ČERMÁK, Miroslav. Kdo na nás útočí, nevíme, jen se to domníváme a pak z toho vyvozujeme dalekosáhlé závěry. *CleverAndSmart Management Consulting* [online]. 2020 [cit. 09.05.2021]. ISSN 2694-9830. Dostupné z: https://www.cleverandsmart.cz/kdo-na-nas-utoci-nevime-jen-se-to-domnivame-a-pak-z-toho-vyvozujeme-dalekosahle-zavery/

Vlastník

Vlastníkem je zpravidla vlastník společnosti nebo manažer jmenovaný na úrovni organizace anebo jednotlivec jako zástupce domácností.

Ten nese jednoznačně odpovědnost za ochranu informačních aktiv a může tuto svoji odpovědnost delegovat na vrcholový management organizace, zpravidla představenstvo. Lze tedy vyjádřit přesvědčení, že úroveň informační bezpečnosti se odvíjí především od neutuchající podpory ze strany vrcholového managementu, který by měl zavést proces řízení a správy informační bezpečnosti.

Někdy se v této souvislosti hovoří o modelu ISG/ISM, který spočívá v oddělení správy (Information Security Governance) a řízení (Information Security Management), nicméně v rámci této práce bude používán výhradně pojem řízení informační bezpečnosti a bude tím míněno obojí, protože ne každá organizace musí mít řízení a správu oddělenou a ukazuje se, že ve většině případů tomu tak skutečně není, obzvlášť u malých a středních firem.

Aby byl proces řízení informační bezpečnosti v organizaci skutečně efektivní, tak by měly být nejprve definovány základní role a jejich odpovědnosti. Klíčová je pak v procesu řízení informační bezpečnosti role manažera informační bezpečnosti, který by se měl seznámit s tím, jaká je mise a vize organizace a pomocí jaké strategie chce organizace této své vize dosáhnout.

Poté by měla být identifikována pro organizaci kritická aktiva, stanovena jejich hodnota a relevantní hrozby, vůči kterým jsou tato aktiva vystavena a rovněž i zranitelnosti, kterých by tyto hrozby mohly zneužít. Následně by měla být zavedena odpovídající bezpečnostní opatření organizační a technické povahy, která by měla snížit riziko zneužití dané zranitelnosti hrozbou anebo by měla minimalizovat její dopad.

Tento proces by měl být formálně podpořen vydáním odpovídajících bezpečnostních politik, standardů, procedur a směrnic, které by měly být pravidelně revidovány, aby bylo zajištěno, že jsou stále aktuální a rovněž by mělo být ověřeno, že došlo k jejich implementaci a jsou v reálné praxi skutečně dodržovány a případné odchylky jsou řádně dokumentovány a schváleny. V takovém případě pak lze hovořit o zavedení procesu informační bezpečnosti.

Na tomto místě je nutné zdůraznit, že **mezi vlastníkem a útočníkem, existuje značně asymetrických vztah, neboť**:

- Útočník může s nesrovnatelně menšími zdroji a úsilím způsobit obrovskou škodu, zatímco vlastník musí vynaložit nemalé finanční prostředky a úsilí na ochranu svých aktiv.

- Útočníkovi stačí zneužít jedné jediné zranitelnosti, prostřednictvím které pronikne do systému. Vlastník se naopak musí snažit všechny možné zranitelnosti identifikovat a odstranit dříve, než to udělá útočník.

- Útočníků je podstatně více, neboť útočníkem může být v podstatě kdokoliv, kdo je připojen do internetu a má odpovídající znalosti, prostředky a motiv. Vlastník je na ochranu svých aktiv v zásadě sám.

- Útočník má o své oběti k dispozici veškeré informace, zatímco vlastník systému v roli oběti o útočníkovi neví prakticky vůbec nic. A to dokonce ani v okamžiku, kdy útok probíhá, protože útočník útok vede nikoliv z vlastního, ale z jiného kompromitovaného systému.

- Útočník může zahájit kybernetický útok prakticky kdykoliv, a to z jakéhokoliv místa na světě. Vlastník systému naproti tomu neví, odkud a kdy útok přijde a musí být tak neustále v pohotovosti a vyhodnocovat a reagovat na všechny bezpečnostní události.

- Útočník nemusí respektovat žádné zákonné a regulatorní požadavky, zatímco vlastník systému na ochranu svých informačních aktiv může využít jen dostupných zákonných prostředků a nemůže tak např. zahájit protiútok, protože by mohl způsobit škodu jinému subjektu, jehož systém útočník kompromitoval.

Výše uvedený výčet nemusí být nutně úplný, ale zachycuje hlavní rozdíly.

2.1.3 Aktiva

Informační aktiva lze rozdělit na primární a sekundární[42]. Informace a služby pak představují primární aktiva, která jsou závislá na sekundárních aktivech, kterými jsou především HW, SW a lidé. **Kybernetický útok však není veden na primární aktiva, byť ta jsou zpravidla cílem útoku, nýbrž na aktiva sekundární** nebo také podpůrná aktiva, což jsou taková aktiva, která jsou nezbytná ke zpracování informací v rámci celého jejich životního cyklu, a to v úložišti, při přenosu a při užití a zároveň by měla zajistit jejich ochranu. Sekundární aktiva jsou:

- koncová zařízení (desktopy, notebooky, tablety, smartphony, IoT jako televize, termoregulace);
- servery (webové, aplikační, databázové, souborové, mailové, tiskové, proxy, adresářové, jmenné);
- SW (serverové operační systémy, desktopové mobilní operační systémy, ovladače třetích stran, krabicové verze aplikací a aplikace vyvíjené na zakázku, firmware);
- síťové prvky (pasivní, tj. především metalické a optické kabely, aktivní prvky, tj. rozbočovače, přepínače, směrovače, firewally);
- periférie (veškerá vstupně výstupní zařízení, jako klávesnice, myš, monitor, tiskárna, skener, fax, multimediální zařízení jako reproduktory, mikrofon);
- ICS/SCADA, průmysloví roboti;
- lidé (uživatelé systému, správci, vývojáři, softwaroví roboti);
- prostory (kanceláře, technické místnosti, datová centra, šachty).

[42] ČSN ISO/IEC 27005. *Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví. 2019.

Specifické postavení pak zaujímají aktiva, která plní rolí bezpečnostních opatření, bez nichž by systém sice mohl fungovat, ale byl by vážně ohrožen v případě jejich selhání nebo absence v okamžiku realizace útoku, patří sem např.:

- záložní zdroje napájení (UPS, dieselagregáty), klimatizace (HAVAC);
- uzavřené kamerové monitorovací systémy (CCTV);
- infračervené detektory pohybu (PIR);
- zálohy a archivy;
- dokumentace.

Všechna tato podpůrná aktiva, včetně těch, co patří mezi bezpečnostní opatření, **mohou obsahovat zranitelnosti a mohou být i cílem kybernetických útoků**.

2.1.4 Hodnocení aktiv

Každá organizace by měla identifkovat svá nejcennější aktiva a ta odpovídajícím způsobem chránit. Zpravidla se tak provádí v rámci business impact analýzy, kdy se expertní tým zabývá tím, jaký dopad by mělo narušení bezpečnosti na jeho primární aktiva.

Na tomto místě je třeba uvést, že **se může jednat o tzv. business dopad** (narušení bezpečnosti primárního aktiva) skrze **technický dopad** (narušení bezpečnosti podpůrného aktiva). Obvykle se uvádí, že narušení bezpečnosti informací spočívá v narušení důvěrnosti (confidentiality, zkr. C), integrity (integrity, zkr. I) a dostupnosti (availability, zkr. A), které tvoří základní atributy bezpečnosti[43], jak znázorňuje Obrázek 2 – CIA model. I ty jsou v různých standardech definovány různě, ale v zásadě zde panuje shoda.

[43] KOLOUCH, Jan. *CyberCrime*. 1. vydání. Praha: CZ.NIC, z.s.p.o, 2016. Edice CZ.NIC, 14. publikace. ISBN 978-80-88168-15-7. s. 56.

Obrázek 2 – CIA model

V případě důvěrnosti se hovoří jen o informacích, v případě integrity se pak hovoří jak o systému, tak i o informacích a v případě dostupnosti se hovoří jen o systému.

- **důvěrnost –** zachování důvěrnosti spočívá v tom, že informace by měly být přístupné jen tomu, kdo je oprávněn se s nimi seznamovat, a proto je třeba zabránit přístupu neautorizovaným osobám.
- **integrita** – pro zachování integrity je nutné, aby nedocházelo k neautorizované modifikaci systému a informací.
- **dostupnost** – pro zachování dostupnosti pak musíme zabránit narušení dostupnosti služeb, a tedy i systému.

Je však otázka, zdali nemůže nastat situace, kdy dojde ke kompromitaci systému a jeho ovládnutí ze strany útočníka, ale k narušení důvěrnosti, integrity anebo dostupnosti informací a systémů nikoliv. Byť se v současné době pracuje výhradně s CIA triádou, tak již v roce 1998 přišel Donn B. Parker s myšlenkou, že **tato CIA triáda je nedostatečná, a že by důvěrnost, integrita a dostupnost měly být doplněny ještě o další tři atributy, konkrétně vlastnictví**

(possession), užitečnost (utility) a autenticitu (authenticity)[44]. Jednotlivé atributy pak lze definovat následujícím způsobem:

- **vlastnictví** – v okamžiku, kdy neoprávněná osoba získá kontrolu nad něčím, co ji nepatří, tak Parker hovoří o ztrátě kontroly nebo vlastnictví a odtud pak loss of control or possesion. A jako příklad uvádí krádež citlivé informace, což nepovažuje za narušení důvěrnosti, alespoň ne do té doby, dokud nedojde k jejímu zneužití.

- **užitečnost** – v okamžiku, kdy například dojde ke ztrátě klíče k zašifrovaným datům, tak ta jsou sice dostupná, ale nejdou použít. Parker pak hovoří o ztrátě užitečnosti neboli breach of utility.

- **autenticita** – v okamžiku, kdy dojde k podvrhnutí elektronického podpisu v e-mailu útočníkem, tak byl dle Parkera narušen princip authenticity. Zcela jistě nebyla narušena důvěrnost, integrita a už vůbec ne dostupnost. (Autenticita nicméně není úplně nový atribut, ten se objevuje i v jiných InfoSec dokumentech pod pojmem non-repudiation, tedy neodmítnutelnost nebo také nepopiratelnost.)

Když stávající CIA triádu zkombinujeme s atributy definovanými Parkerem, tak získáme tzv. Parkerian Hexad model, jak uvádí Pender-Bey[45], který zachycuje Obrázek 3 – Parkerian Hexad model.

[44] PARKER, Donn B. *Fighting computer crime: a new framework for protecting information*. New York: Wiley, 1998. ISBN 978-0-471-16378-7. s. 420.
[45] PENDER-BEY, Georgie. *The parkerian hexad* [online]. 2012 [cit. 02.02.2022]. Dostupné z: http://cs.lewisu.edu/mathcs/msisprojects/papers/georgiependerbey.pdf

Obrázek 3 – Parkerian Hexad model

Z výše uvedeného by se dalo odvodit, že když dojde např. ke kompromitaci serveru s public daty a útočník si na něm spustí svou vlastní službu, umožňující mu vzdálený přístup a kontrolu, založí další účet, či provede eskalaci svých stávajících práv a začne systém používat ke svým cílům, např. jako C&C server, rozesílat z něj SPAM, či na něm těžit kryptoměnu, tak k žádnému narušení důvěrnosti, integrity a dostupnosti informací a systému sice dojít nemuselo, ale k narušení vlastnictví ano.

Otázka však je, zda při kompromitaci serveru nedochází k narušení integrity, protože útočník nejspíš nějakým způsobem neautorizovaně zasáhl do souborového systému nebo do paměťového prostoru, protože s největší pravděpodobností ani jinak server kompromitovat nemohl. A pokud bychom rozšířili pojem důvěrnost i na systém, tak získal neoprávněný přístup k systému a tím byla narušena jeho důvěrnost.

A konečně pokud nejsou k dispozici šifrovací klíče a oprávněná osoba se nedostane k datům, tak z pohledu odběratele služby, tak jak je dostupnost mnohdy definována, může být v zásadě jedno, co nedostupnost způsobilo, pro uživatele je služba prostě nedostupná.

V odborné literatuře však tomuto modelu není věnována dostatečná pozornost a bývá často jen zmíněn[46], aniž by byl vysvětlen jeho hlavní přínos, který by měl nalézt uplatnění nejen při ochraně informačních technologií, ale především při ochraně operačních technologií, na které jsou stále častěji vedeny útoky.

2.1.5 Hrozby

Kybernetický útok (cyber attack) je dle NIST[47] definován jako **útok v kyberprostoru s cílem narušit, zničit, odpojit nebo ovládnout daný systém či pozměnit nebo získat citlivá data**. Tato definice mi přijde výstižnější než definice uvedená ve výkladovém slovníku kybernetické bezpečnosti, která považuje za kybernetický útok jen útok, jehož cílem je způsobit poškození anebo získat citlivé informace[48].

S pojmem kybernetický útok pak velice úzce souvisí pojem kybernetická hrozba (cyber threat), která je dle NIST[49] definována jako událost, která má potenciál způsobit škodu na aktivech a vést k dalším následným ztrátám, vyplývajícím z narušení bezpečnosti informací a systémů.

Ve svém **úzkém pojetí** by pak za kybernetické hrozby bylo možno považovat jen **hrozby přicházející z kyberprostoru**, ovšem v **širším pojetí**, tak jak např. kybernetické hrozby v ČR vnímá aktuální Zákon o kybernetické bezpečnosti, zkr. ZoKB[50], resp. Vyhláška o kybernetické bezpečnosti VoKB[51], musí být **zohledněny i hrozby vyšší moci a fyzické povahy**, které by rovněž mohly způsobit škody na

---

[46] KOLOUCH, Jan a Pavel BASTA. *CyberSecurity*. Praha: CZ.NIC, 2019. ISBN 978-80-88168-31-7. s. 45.

[47] PAULSEN, Celia a Robert BYERS. *Glossary of key information security terms* [online]. NIST IR 7298r3. Gaithersburg, MD: National Institute of Standards and Technology. 2019 [cit. 02.02.2022]. DOI: 10.6028/NIST.IR.7298r3.

[48] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary.* Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6.

[49] PAULSEN, Celia a Robert BYERS. *Glossary of key information security terms* [online]. NIST IR 7298r3. Gaithersburg, MD: National Institute of Standards and Technology. 2019 [cit. 02.02.2022]. DOI: 10.6028/NIST.IR.7298r3.

[50] ČESKO. Zákon č. 181/2014 Sb. ze dne 23. července 2014 o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). *Sbírka zákonů České republiky* [online]. 2014. Dostupné z: https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=z&id=27231

[51] ČESKO. Vyhláška č. 82/2018 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) [online]. 2018. ISSN 1211-1244. Dostupné z: https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=38431

informačních aktivech v kritické informační infrastruktuře, významných informačních systémech a systémech základních služeb.

Kybernetický útok pak na rozdíl od hrozeb může být veden jen z kyberprostoru a jeho cílem jsou informační aktiva. Za informační aktiva pak lze dle ISO 27005:2018[52] považovat data, informace a služby poskytované informačním systémem, které jejich vlastníkovi generují zisk.

Zatímco informace a služby jsou tzv. primárními aktivy, tak informační systém, který se skládá z mnoha dalších komponent, pak představuje tzv. sekundární aktiva. Zde je nutné si uvědomit, že byť jsou cílem útočníka zpravidla primární aktiva, tak **kybernetický útok je veden na sekundární aktiva**.

Vlastník je tedy nucen za účelem ochrany svých informačních aktiv zavést vhodná bezpečnostní opatření organizační a technické povahy, a to taková, která sama o sobě nebudou z pohledu celkových nákladů dražší než možná škoda, která by mohla vzniknout v přímé souvislosti s kybernetickým útokem. Útočník pak v systému hledá jakoukoliv zranitelnost, které by mohl zneužít.

Legislativa nějakou taxonomii hrozeb neuvádí a rovněž i v bezpečnostních reportech renomovaných firem a mezinárodních organizacích jako je ENISA[53] nebo SANS[54] jsou uváděny různé typy hrozeb, což znesnadňuje jejich analýzu[55].

Hrozby můžeme rozdělit mnoha různými způsoby. Nejjednodušší je dělení podle toho, jaký atribut bezpečnosti může být hrozbou narušen. Pokud důvěrnost, lze hovořit o **hrozbách pasivních**, neboť nedochází ke změně stavu systému ani informací. Pokud dochází k narušení integrity a dostupnosti, lze hovořit o **aktivních hrozbách**, neboť jejich působením ke změně stavu dochází.

Podle původce hrozby (threat agent) můžeme hrozby rozdělit na **hrozby způsobené lidmi** a **vyšší mocí** (vis maior). V prvním případě je to osoba, která

---

[52] PAULSEN, Celia a Robert BYERS. *Glossary of key information security terms* [online]. NIST IR 7298r3. Gaithersburg, MD: National Institute of Standards and Technology. 2019 [cit. 02.02.2022]. DOI: 10.6028/NIST.IR.7298r3.
[53] ENISA. *ENISA Threat Taxonomy* [online]. 2016 [cit. 10.06.2020]. Dostupné z: https://data.europa.eu/euodp/en/data/dataset/enisa-threat-taxonomy-1
[54] LAUNIUS, Steven. *Evaluation of Comprehensive Taxonomies for Information Technology Threats* [online]. 2018 [cit. 02.02.2022]. Dostupné z: https://sansorg.egnyte.com/dl/xWK7DWrT07
[55] ČERMÁK, Miroslav. Cyber threat management: taxonomie hrozeb. *CleverAndSmart Management Consulting* [online]. 2019 [cit. 25.06.2021]. ISSN 2694-9830. Dostupné z: https://www.cleverandsmart.cz/cyber-threat-management-taxonomie-hrozeb/

realizuje danou hrozbu, ať už vědomě nebo nevědomě, a nese za své jednání plnou odpovědnost, tak ve druhém případě za ni nikdo neodpovídá[56].

Podle zdroje, tedy odkud hrozby přichází, je možné je rozdělit na vnější a vnitřní. **Vnější hrozby** pochází z vně organizace a jsou zcela mimo její kontrolu. **Vnitřní hrozby** pak přichází z prostředí organizace, které má organizace zpravidla možnost ovlivnit, neboť toto prostředí přímo utváří. Když tyto dva pohledy zkombinujeme, získáme následující matici, kterou zachycuje *Tabulka 2* – Motiv-zdroj.

Tabulka 2 – Motiv-zdroj

motiv/zdroj	interní	externí
úmyslná	zneužití přístupu, sabotáž	hacking, malware
neúmyslná náhodná	strukturální (selhání operátora, selhání stroje)	environmentální (vyšší moc, přírodní pohromy)

Tímto způsobem byly v zásadě identifikovány 4 zdroje hrozeb, které NIST 800-30 definuje takto[57]:

- **úmyslné** (adversarial) realizované ze strany jednotlivců, organizovaných skupin, konkurence, státu. Úmyslné hrozby můžeme dále rozdělit podle toho, zda útočník vede útok na konkrétní subjekt anebo je mu jedno, který subjekt se stane jeho příští obětí. Subjektem se v tomto případě myslí buď infrastruktura (koncové zařízení, server, síťový prvek), anebo lidský operátor zastávající v daném systému jakoukoliv roli (uživatel, správce, vývojář). Kdy výsledkem těchto útoků je zpravidla získání informací, kompromitace systému nebo narušení jeho dostupnosti.

- **náhodné** (accidental), kdy se jedná o chybu zaměstnance, ať už uživatele nebo správce systému při vykonávání běžných denních činností. Náhodné

[56] KINCL, Jaromír, Valentin URFUS a Michal SKŘEJPEK. *Římské právo*. Praha: C.H. Beck, 1995. ISBN 978-80-7179-031-0. s. 223.

[57] NIST. *NIST Special Publication 800-30 Guide for Conducting Risk Assessments* [online]. 2012 [cit. 17.02.2019]. Dostupné z: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf

nebo také neúmyslné hrozby jsou hrozby, kdy k narušení bezpečnosti došlo z důvodu nedbalosti nebo selhání zaměstnance, který svým konáním nebo naopak nekonáním narušení bezpečnosti způsobil. Přičemž je třeba rozlišovat mezi nedbalostí vědomou a nevědomou, protože zatímco v prvním případě zaměstnanec věděl, že by narušení bezpečnosti mohl způsobit, a v nepřiměřené míře spoléhal, že se tak nestane, tak ve druhém případě toto vůbec nepředpokládal.

- **strukturální** (structural), kdy došlo k selhání HW nebo SW ať už v důsledku stáří nebo překročení provozních parametrů. Některé tyto hrozby lze předvídat a předcházet jim v okamžiku, kdy se vytváří vanová křivka a sleduje životnost každé použité komponenty, provádí monitoring výkonnostních parametrů, realizuje kapacitní plánování a jsou připraveny příslušné scénáře.

- **environmentální** (environmental), kdy došlo k nějaké přírodní pohromě/katastrofě a k selhání infrastruktury, která je zcela mimo kontrolu organizace. Patří sem hrozby jako povodeň, požár, zemětřesení, tornádo a výpadek infrastruktury jako je voda, elektřina, telekomunikace, na kterých může být organizace rovněž závislá.

Přičemž všechny výše uvedené typy hrozeb mohou mít v případě jejich realizace negativní dopad na informační systémy. Úmyslné kybernetické hrozby mající povahu kybernetických útoků pak lze rozdělit z pohledu velikosti zásahu na útoky:

- **plošné**, kdy útočníkovi je v zásadě jedno, kdo se stane jeho obětí, a napadne **jakýkoliv subjekt**, který trpí **určitou zranitelností** (Při těchto útocích do určité míry záleží na úrovni zabezpečení ostatních subjektů na trhu, protože útočník realizuje úspory z rozsahu a cílí na tzv. low hanging fruit, doslovně přeloženo jako nízko visící ovoce, tedy ovoce, které lze snadno utrhnout, v tomto kontextu hůře zabezpečené subjekty, do kterých lze snadno proniknout.);

- **cílené**, kdy útočník vede útok na **konkrétní subjekt** a hledá **jakoukoliv zranitelnost**, které by mohl zneužít. (U těchto typů útoků nehraje úroveň zabezpečení ostatních subjektů na trhu v podstatě žádnou roli, neboť útočník je připraven vyvinout nezměrné úsilí, prostředky a čas k dosažení svého cíle.)

Z pohledu předmětu cílení, byť to ne vždy musí být na první pohled zřejmé, je možné kybernetické útoky rozdělit na útoky vedené primárně na:

- **lidi**, kdy útočník **zneužívá technik sociálního inženýrství a nedostatečného bezpečnostního povědomí** a snaží se oběť přimět k tomu, aby mu poskytla informaci nebo provedla činnost, kterou on potřebuje[58], srv. Mitnick[59].

- **infrastrukturu**, kdy útočník **zneužívá zranitelností, které se nacházejí v návrhu, v kódu anebo implementaci** aplikace, systému nebo sítě, kdy žádná interakce ze strany uživatele není vyžadována.

Když tyto dva přístupy zkombinujeme, získáme matici, kterou je Tabulka 3 – Typy útoků, která zachycuje základní 4 typy kybernetických útoků a co je pro ně charakteristické.

[58] MANN, Ian. *Hacking the human: social engineering techniques and security countermeasures*. Aldershot, England ; Burlington, VT: Gower, 2008. ISBN 978-0-566-08773-8.
[59] MITNICK, Kevin D a William L SIMON. *Umění klamu*. Gliwice: Helion, 2003. ISBN 978-83-7361-210-5. s. 6.

Tabulka 3 – Typy útoků

	Plošný (PS)	Cílený (CS)
stroje	▪ skenování určitého IP adresního rozsahu, v krajním případě celého internetu ▪ hledání **konkrétních** zranitelností ▪ zneužití konkrétní zranitelnosti ▪ začlenění do botnetu ▪ zneužití k dalšímu útoku např.: C&C, proxy, DDoS, phishing, SPAM, drop box, malvertising ▪ server side ransomware ▪ těžba kryptoměn (cryptojacking)	▪ sběr informací ▪ skenování pouze vybraného serveru nebo omezeného množství serverů ▪ hledání **jakékoliv** zranitelnosti ▪ zneužití jakékoliv zranitelnosti ▪ DoS, DDoS (aplikační, volumetrický) ▪ Změna obsahu webových stránek (defacement) ▪ Kompromitace (kompletní ovládnutí cílového systému) ▪ zneužití k dalšímu útoku, zpravidla APT
lidé	▪ Sociální inženýrství + nízké bezpečnostní povědomí ▪ Zranitelnosti (nultého dne výjimečně) ▪ drive-by download (malvertising) ▪ generické trojanizované aplikace ▪ phishing, ▪ SMShing, ▪ ransomware, premium SMS, cryptominery, bankware	▪ Sociální inženýrství + zranitelnosti nultého dne ▪ SEO poisoning, ▪ DNS poisoning, ▪ watering holes ▪ drive-by download ▪ zero-day exploit (ne nutně) ▪ specifické trojanizované aplikace ▪ spear phishing, ▪ vishing, ▪ SMShing ▪ CEO fraud, exfiltrace dat, přerušení provozu/výroby/služeb
	Plošný (PL)	Cílený (CL)

Detailní popis jednotlivých typů útoku zachycuje Příloha I – Popis hrozeb.

2.1.6 Hodnocení hrozeb

Pravděpodobnost realizace dané hrozby může ovlivňovat spousta faktorů, obzvlášť pokud se jedná o úmyslné hrozby. Už samotné aktivum a vidina potenciálního zisku může útočníka přitahovat a činit pro něj dané aktivum nesmírně atraktivní. To je i důvod, proč na některé organizace jsou útoky vedeny častěji než na jiné, a na některé vůbec. Nejčastěji se však uvádí tři faktory, které tuto pravděpodobnost ovlivňují, jsou jimi motiv, příležitost a schopnost, přičemž:

- **motiv** – může být různý, může se jednat o přímý finanční zisk, což je nejčastější případ, či nepřímý, spočívající v získání nějaké výhody, třeba i tím, že druhé straně vznikne škoda, ale může se jednat i o pomstu, touhu po respektu a uznání. Motiv sám o sobě není dostačující, neboť pokud daná osoba nemá příležitost hrozbu realizovat anebo nedisponuje odpovídajícími znalostmi, nemůže danou hrozbu s úspěchem realizovat.

- **příležitost** – zde je rozhodující, zda je možné vést útok přes internet anebo je nutné se nacházet na stejné síti anebo se dostat do fyzického kontaktu s předmětným aktivem. V okamžiku, kdy je možné vést útok přes internet, tak se pravděpodobnost hrozby podstatně zvyšuje. Ovšem i když má osoba příležitost hrozbu realizovat, tak to neznamená, že ji realizuje, neboť ještě musí mít dostatečně silný motiv a disponovat i odpovídajícími znalostmi.

- **schopnost** – čím nižší jsou nároky na její realizaci, tedy znalosti a dovednosti, a jestli jsou tyto nároky nízké a v krajním případě ji může realizovat v podstatě každý uživatel internetu, tak se tím podstatně zvyšuje pravděpodobnost, že dojde k její realizaci. Ale i zde platí, že i když bude daná osoba disponovat danou schopností a dokázala by útok realizovat, tak musí mít i motiv a příležitost.

Tyto faktory nelze vyhodnocovat odděleně, ale je třeba je vnímat komplexně, neboť, vždy musí být přítomny všechny tři, aby došlo k realizaci samotné hrozby. Na druhou stranu je třeba připustit, že v okamžiku, kdy bude existovat dostatečně silný motiv a útočník bude disponovat i odpovídajícími finančními prostředky, tak

si může najmout někoho, kdo má dané schopnosti a dokáže si vytvořit i odpovídající příležitosti k tomu, aby hrozbu realizoval.

Jednoduše tak nelze od počtu potenciálních útočníků odvozovat pravděpodobnost realizace hrozby a tvrdit, že v okamžiku, kdy danou schopností a příležitostí disponuje jen pár osob na světě, tak je pravděpodobnost takové hrozby nízká. Tento výzkumný předpoklad potvrzují i nejrůznější státem sponzorované útoky nebo útoky realizované vysoce organizovanými skupinami, kdy došlo ke kompromitaci i velice dobře zabezpečených informačních systémů a k obrovským finančním ztrátám.

Pravděpodobnost úmyslných útoků lze velice špatně odhadnout, nicméně lze monitorovat situaci v kyberprostoru a analyzovat již proběhnuvší útoky a hledat v nich určité společné charakteristiky, jako kdo útok realizoval, jaký vektor útoku byl použit, kdo byl obětí útoku, v jakém odvětví působil, jaké bylo jeho postavení na trhu, v jaké fázi životního cyklu se daná organizace nacházela apod.

A jelikož se může pravděpodobnost hrozeb v čase měnit, především v důsledku změn v kyberprostoru, měla by se analýza opakovat a být uplatňován princip předběžné opatrnosti, tzv. due care a due diligence.

Dle FireEye se doba, po kterou zůstává APT útok nedetekován, postupně zkracuje. V roce 2011 to bylo 416 dní, tedy více než rok, zatímco v roce 2018 už jen 78 dní, tedy něco přes dva měsíce[60]. To však v mnoha případech může být stále doba dostatečně dlouhá k dosažení cíle, protože např. dle společnosti Verizon je cíle dosaženo zpravidla za mnohem kratší dobu[61].

V rámci cyber threat managementu nelze nezmínit službu tak trochu eufemisticky nazvanou cyber threat intelligence, zkr. CTI. V rámci cyber threat intelligence dochází k zajišťování informací o připravovaných, probíhajících nebo již proběhnuvších útocích z nejrůznějších zdrojů.

Patří sem jak informace získávané z veřejně dostupných zdrojů včetně sociálních sítí (Open Source Intelligence, zkr. OSINT), informace získané přímo od lidí, kteří mají k určitým informacím přístup (Human Intelligence, zkr. HUMINT)

---

[60] FIREEYE. *M-Trends 2019* [online]. 2019 [cit. 08.03.2019]. Dostupné z: https://content.fireeye.com/m-trends

[61] VERIZON. *2018 Data Breach Investigations Report* [online]. 2018 [cit. 10.07.2021]. Dostupné z: https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf

a konečně i informace získávané odposlechem komunikace v jakékoliv podobě (Signal Intelligence, zkr. SIGINT).

Netřeba snad dodávat, že pokud je komunikace, která je předmětem zájmu šifrována, tak dochází i k pokusu o její dešifrování. Zdrojem informací jsou rovněž i uzavřená diskusní fóra, kam je možné vstoupit jen na základě pozvánky od jiného člena, dále pak honeypot/honeynet sondy a bezpečnostní řešení nasazená u jednotlivých zákazníků prakticky po celém světě.

Dost často také uživatelé samotných bezpečnostních produktů dají při instalaci toho či onoho produktu vědomý anebo možná i nevědomý souhlas s tím, že budou poskytovat informace zpátky do sítě, a to za účelem zlepšování kvality detekce škodlivého kódu a probíhajících kybernetických útoků.

Ostatně tohle je jediný způsob jak škodlivý kód, který se začal šířit v jedné části světa včas detekovat a reagovat na něj vydáním aktualizace pro konkrétní bezpečnostní produkt dříve, než dojde k útoku používajícímu daný škodlivý kód tam, kde byl zatím relativně klid.

Takto získané informace jsou pak vyhodnocovány bezpečnostními analytiky a týmy, a to jak ručně, tak i automatizovaně, a v rámci těchto aktivit se pak provádí tzv. modelování hrozeb, které je založené jak na předchozích zkušenostech, tak i nově získaných informacích.

Je nasnadě, že čím více má společnost nabízející službu cyber threat intelligence instalací daného bezpečnostního řešení u svých zákazníků pocházejících z rozličných sektorů ekonomiky, působících v různých státech, geografických lokalitách a časových pásmech, tím rychleji a lépe může detekovat probíhající útok, posbírat vzorky malware, aktualizovat svoje řešení a predikovat další možný vývoj hrozeb v kyberprostoru.

V rámci CTI se zveřejňují tzv. indikátory kompromitace, zkr. IoC (Indicators of compromise). Jak již název napovídá, by měly sloužit k identifikaci kompromitovaného zařízení. Tedy zařízení, kterým může být stejně tak server, jako pracovní stanice, notebook, tablet, mobilní telefon anebo síťový prvek. Jako indikátory kompromitace, jsou zpravidla uváděny konkrétní:

- IP adresy a domény, ze kterých byl veden útok, nachází se na nich malware, řídící centra, phishingové stránky, či sloužící jako tzv. drop zóna;

- e-mailové servery šířící SPAM, obsah e-mailů, e-mailové adresy, odkazy, názvy příloh;

- jména souborů v souborovém systému, dynamických knihoven a jejich hashe, klíče v registrech apod.

IoC jsou sestavovány organizacemi, které se zabývají bezpečností, monitorují situaci v kyberprostoru a mají přístup k zařízením, která již byla napadena, a mohou je analyzovat, identifikovat charakteristické příznaky a ty pak popsat ve formě IoC a distribuovat svým klientům v rámci služby Cyber Threat Intelligence, zkr. CTI.

IoC pak lze nakrmit nejrůznější bezpečnostní nástroje a sledovat, zda nějaký stroj na vnitřní síti nebyl kompromitován a nekomunikuje třeba na nějakou profláknutou adresu nebo není do organizace aktuálně doručován phishing e-mail či zda se v systému nenachází soubor s daným hashem anebo záznam v registrech.

Otázka však je, zda lze tímto způsobem skutečně včas detekovat probíhající útok anebo odhalit již kompromitované zařízení. Jistěže lze, ale jen ve velice specifických případech a obzvláště pak plošně vedených útocích. Na otázku, proč, tomu tak je se nabízí následující vysvětlení:

- IP adresy, ze kterých jsou vedeny útoky, nachází se na nich malware, řídící centra, či slouží jako drop zóna, se velice rychle mění, a jsou detekovány, takže druhý den se na nich již nachází jen naprosto legitimní business;

- e-maily jsou rozesílány z různých e-mailových adres, různých mailových serverů a mají i různý obsah, jiné názvy a velikosti příloh;

- jména souborů, dynamických knihoven a jejich hashe a klíče v registrech se mění a jsou kompilovány až na napadeném počítači a jsou generovány jako unikátní.

Významnou roli zde také hraje faktor času, protože je třeba si uvědomit, že útok nejprve musí proběhnout, poté musí být detekován, pak musí být analyzován, aby

mohly být následně sestaveny IoC, a ty nakonec musí být zpřístupněny odběratelům služby.

I když se podaří poslední krok plně zautomatizovat, tj. zajistit, aby v okamžiku, kdy je IoC sestaven byla aktualizována databáze IoC např. v SIEM řešení či síťovém skeneru, tak uběhne příliš mnoho času mezi zahájením útoku a sestavením IoC.

Ve výsledku tak může být teoreticky detekován kompromitovaný stroj, který se snaží např. komunikovat na IP adresu, na které se nachází C&C server. Spíš je však třeba počítat s tím, že na dané adrese již žádný C&C server nepoběží a bude se jednat o false positive událost[62].

Toto tvrzení lze opřít i o vlastní výzkum, který byl proveden v letech 2014-2019, kdy veškeré bezpečnostní alerty generované nástrojem SIEM na základě importovaných IoC, byly false positive.

Na základě výše uvedeného lze konstatovat, že přidaná hodnota služby CTI se zaměřením na IoC je značně nadhodnocena a její přínos není zpravidla takový, jak se obecně míní. Pozitivní je, že se zpracováním IoC se v některých případech může podstatně zkrátit Dwell time[63].

Vzhledem k tomu, že trendem posledních let je bezsouborový malware a objevují se i nové hrozby, tak je třeba se více zaměřit na vyhodnocování podezřelého chování a přejít od pasivního k aktivnímu řízení hrozeb[64] a nespoléhat se příliš na IoC. Přínos IoC a jejich importu do SIEM nástrojů lze spatřit spíše u běžného phishingu než u APT kampaní, a nelze tak zcela souhlasit s některými závěry Přenosila a Ghafira, protože než se doména a rovněž i hash souboru dostane na blacklist, tak útočník může dosáhnout svého cíle[65].

---

[62] ČERMÁK, Miroslav. Co vyplývá z většího množství false positive a false negative událostí? *CleverAndSmart Management Consulting* [online]. 2019 [cit. 18.09.2019]. ISSN 2694-9830. Dostupné z: https://www.cleverandsmart.cz/co-vyplyva-z-vetsiho-mnozstvi-false-positive-a-false-negative-udalosti/

[63] ČERMÁK, Miroslav. Cyber resilience: Dwell time. *CleverAndSmart Management Consulting* [online]. 2019 [cit. 25.06.2019]. ISSN 2694-9830. Dostupné z: https://www.cleverandsmart.cz/cyber-resilience-dwell-time/

[64] VANHORN, Thom. The Evolution of Endpoint Security: Moving from Passive to Active Threat Management. *Channel Futures* [online]. 24. leden 2018 [cit. 10.03.2019]. Dostupné z: https://www.channelfutures.com/from-the-industry/the-evolution-of-endpoint-security-moving-from-passive-to-active-threat-management

[65] PŘENOSIL, Václav a Ibrahim GHAFIR. Advanced Persistent Threat and Spear Phishing Emails. *ResearchGate* [online]. 2015 [cit. 12.03.2019]. Dostupné z:

2.1.7 Zranitelnosti

Zranitelnost je vlastnost aktiva a může se nacházet i v samotném bezpečnostním opatření, které může být nedostatečné, anebo zcela chybět, a pak může být s větším či menším úsilím překonáno. Zranitelnosti jsou nedílnou součástí informačních systémů a ten jich může obsahovat i více. Zranitelnost může být do systému zanesena úmyslně anebo neúmyslně už v okamžiku jeho návrhu (design flaw), při kódování (coding error) nebo implementaci (implementation error) v konkrétním prostředí a nacházet se v jakékoliv komponentě tvořící informační systém, avšak o její přítomnosti nemusí mít nikdo po poměrně dlouhou dobu vůbec tušení.

Na této skutečnosti nic nemění ani fakt, zda se jedná o otevřený nebo uzavřený systém a zda jsou k dispozici zdrojové kódy (open source) či nikoliv (closed source), protože zranitelnosti se běžně nacházejí v obou případech.

Je třeba si uvědomit, že v okamžiku, kdy je zranitelnost odhalena bezpečnostním výzkumníkem (security researcher) a není k dispozici žádné řešení odstraňující danou zranitelnost, tak hovoříme o **zranitelnosti nultého dne** (zero day vulnerability) a to až do té doby, dokud nejsou zveřejněny informace ohledně této zranitelnosti.

Pojem zero day je odkazem na fenomén 90 let, kdy docházelo ke krádežím oblíbených komerčních aplikací díky průnikům do firemních počítačů jednotlivých vývojářských studií a následnému zpřístupnění těchto aplikací na tzv. warez fórech, přičemž počet dnů vyjadřoval, kolik dní od oficiálního prodeje se na warez fóru aplikace objevila. A v okamžiku, kdy dříve než v obchodě, tak se hovořilo o Zero Day.

Zároveň se otevírá tzv. **okno zranitelnosti** (Window of Vulnerability, zkr. WoV) někdy též nazývané jako okno příležitosti (Window of Opportunity nebo také Window of Exposure). WoV zůstává otevřené do té doby, než uživatel nasadí **záplatu** (patch) odstraňující danou zranitelnost anebo novou verzi, která ji už neobsahuje a teprve pak se WoV uzavírá.

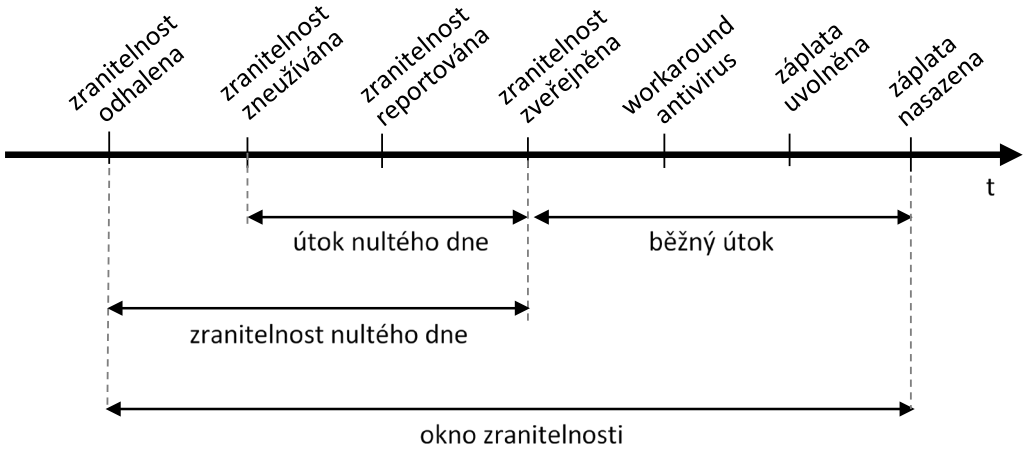
---

https://www.researchgate.net/publication/305991054_Advanced_Persistent_Threat_and_Spear_Phishing_Emails

Ovšem ne každá organizace může záplatu odstraňující nějakou zranitelnost ihned nasadit, obzvlášť pokud provozuje kritický systém. Nemůže totiž akceptovat ne zcela zanedbatelné riziko, že by záplata mohla způsobit významnou degradaci výkonu[66], pád daného systému anebo by také nemusel nastartovat vůbec[67], takže ji musí za tímto účelem nejprve otestovat. Otestování takového systému pak může trvat i několik týdnů, a proto může být taková organizace i několik týdnu po uvolnění záplaty stále zranitelná. Pro úplnost je nutné dodat, že v okamžiku, kdy se záplata na danou zranitelnost neobjeví vůbec, což není zase až tak výjimečný případ, jak by se mohlo zdát, tak se pak dá dokonce s jistou nadsázkou hovořit o věčné zranitelnosti.

Přítomnost zranitelnosti ještě neznamená, že jí bude automaticky zneužito, k tomu může dojít až v okamžiku, kdy někdo napíše funkční **exploit**, což je kód, který dokáže dané zranitelnosti zneužít, a který pak zpravidla v sobě nese i nějaký payload, který provádí vlastní škodlivou činnost. A pokud k tomu dojde, tak hovoříme o **útoku nultého dne** (zero day attack). Tato skutečnost je mainstreamovými médii nejčastěji znázorňována na jedné časové ose, tak jak uvádí *Obrázek 4 – Životní cyklus zranitelnosti*.

Obrázek 4 – Životní cyklus zranitelnosti



[66] MAURO, Andrea. Performance impact of CPU bug fixes - vInfrastructure Blog [online]. 25. srpen 2018 [cit. 17.02.2019]. Dostupné z: https://vinfrastructure.it/2018/08/performance-impact-of-cpu-bug-fixes/

[67] VENKAT0745. A patch is preventing the system from starting. In: *answers.microsoft.com* [online]. 20. únor 2014 [cit. 17.02.2019]. Dostupné z: https://answers.microsoft.com/en-us/windows/forum/all/a-patch-is-preventing-the-system-from-starting/590fab3b-6efc-46f1-beb0-9bb1d1dc7b29

Obrázek 4 – Životní cyklus zranitelnosti zachycuje, že antivirus, zkr. AV, je nasazen až poté, co je zveřejněna daná zranitelnost, ovšem může být nasazen i dříve, např. v okamžiku, kdy je detekován exploit, a ten může být detekován i dříve, než je zranitelnost reportována vývojáři a zveřejněna.

U zranitelnosti (vulnerability), exploitu a záplaty (patch) lze v zásadě identifikovat 4 různé stavy. Ty zachycuje *Tabulka 4 – Zranitelnost-exploit-záplata*. Z důvodu neexistence odpovídajícího českého výrazu je použit původní termín exploit. Jednotlivé stavy u zranitelnosti, exploitu a záplaty jsou uvedeny v pořadí, v jakém po sobě zpravidla následují, ale ne vždy tomu tak musí být.

Tabulka 4 – Zranitelnost-exploit-záplata

zranitelnost (vulnerability)	přítomna (present)	odhalena (disclosed)	nahlášena (reported)	zveřejněna (published)
exploit	neexistuje (not exists)	vyvinut (developed)	prodán (sold)	zneužit (misused)
Záplata (patch)	neexistuje (not exists)	vytvořen (created)	uvolněn (released)	nasazen (deployed)

Zranitelnost

- **přítomna** – zranitelnost může být v přítomna v produktu od začátku, jen ještě nebyla odhalena a také odhalena být nikdy nemusí, na některé zranitelnosti se přišlo až po několika desítkách let;
- **odhalena** – zranitelnost může být odhalena bezpečnostním výzkumníkem, který zranitelnosti cíleně vyhledává, vývojářem daného produktu, ale stejně tak může být odhalena i zcela náhodou uživatelem;
- **nahlášena** – zranitelnost by měla být nahlášena vývojáři, a ten by měl zranitelnost v produktu odstranit;
- **zveřejněna** – informace o zranitelnosti je zveřejněna ve veřejně dostupné databázi zranitelností.

Exploit

- **neexistuje** – exploit neexistuje minimálně do té doby, dokud někdo neodhalí konkrétní zranitelnost;
- **vyvinut** – exploit je vyvinut přímo výzkumníkem, který danou zranitelnost našel nebo někým jiným;
- **prodán** – exploit je následně poskytnut vývojáři zranitelného produktu, bezpečnostní komunitě anebo prodán tomu, kdo nejvíce zaplatí;
- **zneužit** – exploit může být zneužit přímo výzkumníkem, ale ten jej zpravidla prodá a exploit se pak stane součástí nějakého exploit kitu a je zneužíván k (APT) útokům.

Záplata

- **neexistuje** – záplata neexistuje do té doby, dokud zranitelnost není nahlášena nebo zveřejněna;
- **vytvořena** – v okamžiku, kdy se autor daného produktu o zranitelnosti dozví, může na záplatě začít pracovat a připravit ji;
- **uvolněna** – v okamžiku, kdy je záplata uvolněna, tak kdokoliv, kdo používá produkt trpící danou zranitelností, ji může nasadit;
- **nasazena** – rychlost nasazení záplaty závisí na tom, zda se uživatel daného produktu vůbec o tom, že jeho produkt nějakou zranitelnost obsahuje, dozví anebo zda se produkt sám aktualizuje.

Vzhledem k tomu, že životní cykly zranitelnosti, exploitu a záplaty jsou na sobě relativně nezávislé, jediným předpokladem je, že exploit může vzniknout až po odhalení zranitelnosti a záplata zase až poté, co je daná zranitelnost nahlášena, tak přechod mezi ostatními stavy je relativně volný. *Obrázek 5 – Exploit-zranitelnost-záplata* však zachycuje jen jeden z několika možných případů.

Obrázek 5 – Exploit-zranitelnost-záplata

V reálném světě můžeme zaznamenat hned několik situací, ke kterým může s větší či menší pravděpodobností dojít. Ty zachycuje *Tabulka 5 – Exploit-zranitelnost-záplata a možné stavy*. Další příklad uvádí *Příloha E – Životní cyklus zranitelnosti*.

Tabulka 5 – Exploit-zranitelnost-záplata a možné stavy

1.	zranitelnost zveřejněna	exploit zneužíván	záplata nasazena
2.	zranitelnost zveřejněna	záplata nasazena	exploit zneužíván
3.	exploit zneužíván	zranitelnost zveřejněna	záplata nasazena
4.	exploit zneužíván	záplata nasazena	zranitelnost zveřejněna
5.	záplata nasazena	zranitelnost zveřejněna	exploit zneužíván
6.	záplata nasazena	exploit zneužíván	zranitelnost zveřejněna

Jednotlivé situace, které zachycuje Tabulka 5 – Exploit-zranitelnost-záplata a možné stavy, lze popsat takto:

1. Bezpečnostní výzkumník objevil zranitelnost a ta byla zveřejněna včetně podstatných detailů a umožnila vytvoření exploitu ji zneužívající. Obvykle k této situaci dochází v okamžiku, kdy vývojář nespolupracuje na jejím odstranění. Záplata pak zpravidla přichází až v okamžiku, kdy je zranitelnost aktivně zneužívána.

2. Je zveřejněna základní informace o zranitelnosti, zpravidla obsahující jen nezbytně nutné informace, a v rychlém časovém sledu pak je uvolněna i záplata. Teprve poté se objevuje exploit, takže v ohrožení jsou jen ti, co záplatu nenasadili. Tento stav by se dal označit jako ideální.

3. Po objevení zranitelnosti bezpečnostním výzkumníkem dochází i k vytvoření exploitu a k aktivnímu zneužívání dané zranitelnosti, což nakonec vede ke zveřejnění zranitelnosti a následnému uvolnění záplaty. Tento stav provází většinu zero day útoků.

4. Po objevení zranitelnosti dochází k její exploitaci, je uvolněna záplata a zveřejněna zranitelnost. Spíš teoretický stav, ale nelze vyloučit.

5. Je nasazena záplata na blíže neurčenou zranitelnost, která je později zveřejněna a objeví se i exploit. Spíš teoretický stav, ale nelze vyloučit.

6. Je nasazena záplata na blíže neurčenou zranitelnost a později se objeví exploit a je zveřejněna zranitelnost.

Obvyklý, resp. bezpečnostní komunitou očekávaný a žádoucí stav je, že v okamžiku, kdy bezpečnostní výzkumník najde zranitelnost, tak ji nahlásí vývojáři daného produktu a ten uvolní odpovídající záplatu. Současně s tím zveřejní i základní informace o dané zranitelnosti.

Ne každý bezpečnostní výzkumník je však čestný, a tak se může stát, že příslušnou zranitelnost včetně exploitu prodá firmě jako je např. Revuln[68] nebo Zerodium[69], specializující se na jejich nákup a platící za ně až několik miliónů USD, vizte *Příloha A – Odměna za zranitelnosti*.

Je nasnadě, že tyto zranitelnosti jsou dále zneužívány k cíleným APT útokům a odprodávány ve formě nástrojů pro sledování[70] dalším společnostem jako je

[68] REVULN. *Revuln.com* [online]. [cit. 18.02.2019]. Dostupné z: https://revuln.com
[69] ZERODIUM - The Leading Exploit Acquisition Platform [online]. [cit. 17.02.2019]. Dostupné z: http://zerodium.com/
[70] MALÝ, Robert. Kauza Hacking Team, aneb jak funguje Remote Control System. *CleverAndSmart Management Consulting* [online]. 2015 [cit. 18.02.2019]. ISSN 2694-9830. Dostupné z: https://www.cleverandsmart.cz/kauza-hacking-team-aneb-jak-funguje-remote-control-system/

např. HackingTeam[71], který pak svůj nástroj RCS prodával dál, např. i PČR, jak rovněž uvádí Malý, který tento nástroj i analyzoval.

Kromě toho může nastat situace, kdy autor produktu, který danou zranitelností trpí, nemá zájem ji odstranit, vůbec nereaguje anebo z pohledu výzkumníka reaguje příliš pomalu a ten se rozhodne informace o dané zranitelnosti zveřejnit.

Zde existuje v rámci bezpečnostní komunity spor ohledně toho, zda by se měly informace o zranitelnostech zveřejňovat či nikoliv, přičemž oba tábory jsou přibližně stejně početné. To ostatně vyplývá i z ankety realizované mezi bezpečnostními profesionály v ČR[72].

Existuje zde ne nepodstatné riziko, že informace týkající se dané zranitelnosti povedou spíš ke vzniku exploitu a jejího aktivního zneužívání, či dokonce jeho enormního nárůstu[73], než aby přispěly k rychlejšímu uvolnění záplaty nebo virové signatury a ochraně uživatelů daného produktu, který zranitelností trpí.

Je tomu tak především proto, že drtivá většina uživatelů jakéhokoliv produktu informace o zranitelnostech nesleduje, a i kdyby ano, tak jej kvůli zranitelnosti nepřestane používat a nedokáže ani přijmout vhodná bezpečnostní opatření, která by zabránila případnému útočníkovi ve zneužití dané zranitelnosti. Jednoduše proto, že nedisponuje takovými znalostmi a dovednostmi, aby toho byla schopna.

Řešením je tzv. odpovědné zveřejňování (responsible disclosure) informací o zranitelnostech, což zachycuje Obrázek 6 – Odpovědné zveřejnění. V takovém případě je zranitelnosti přiděleno CVE-ID, uvedeno CWE ID je zaevidována v NVD, kde je následně doplněn stručný popis a hodnocení dle CVSSv3. Tak mohou provozovatelé systému na zranitelnost reagovat a útočník nezískává informace potřebné ke snadnému vytvoření exploitu.

---

[71] HackingTeam [online]. [cit. 18.02.2019]. Dostupné z: http://www.hackingteam.it/

[72] ČERMÁK, Miroslav. Měly by se informace o zranitelnostech zveřejňovat? *CleverAndSmart* [online]. 21. květen 2013 [cit. 18.02.2019]. Dostupné z: https://www.cleverandsmart.cz/mely-by-se-informace-o-zranitelnostech-zverejnovat/

[73] BILGE, Leyla a Tudor DUMITRAS. Before we knew it: an empirical study of zero-day attacks in the real world. In: *the 2012 ACM conference*: *Proceedings of the 2012 ACM conference on Computer and communications security - CCS '12* [online]. Raleigh, North Carolina, USA: ACM Press, 2012, s. 833 [cit. 18.02.2019]. ISBN 978-1-4503-1651-4. DOI: 10.1145/2382196.2382284.

Obrázek 6 – Odpovědné zveřejnění

Pokud je zranitelnost zveřejněna, tak je jí zpravidla přiděleno nějaké ID dle Common Vulnerabilities and Exposures, zkr. CVE[74] ve tvaru CVE-YYYY-NNNN, kde YYYY je rok a NNNN je pořadové číslo zranitelnosti v daném roce.

Detailní popis této zranitelnosti pak lze dohledat v National Vulnerability Database, zkr. NVD, kde se pak zpravidla nachází i odkaz na hodnocení této zranitelnosti dle všeobecně nejuznávanější metodiky pro hodnocení zranitelností CVSS organizace First, která se v době psaní této práce nachází ve verzi 3 a míru zranitelnosti hodnotí na základě několika faktorů, a dále pak související slabina dle metodiky CWE.

Řízení technických zranitelností v anglosaské literatuře označované jako vulnerability management je jedna z mnoha činností manažera kybernetické bezpečnosti, které by se měl intenzivně věnovat, neboť do značné míry rozhoduje o tom, zda útok na organizaci, pro kterou pracuje, bude úspěšný či nikoliv[75].

Je tomu tak proto, že drtivá většina útoků z kyberprostoru na informační systémy zneužívá technických zranitelností v systémech a nejsou to primárně jen tzv. zranitelnosti nultého dne, jejichž podstata je blíže vysvětlena dále v této kapitole, nýbrž zranitelnosti, které jsou veřejně známé po poměrně dlouhou dobu a existují pro ně i odpovídající záplaty.

Manažer kybernetické bezpečnosti by měl proto tyto zranitelnosti v provozovaných systémech identifikovat a řídit, tzn., že by měl vždy

[74] CVE - CVE ID Syntax Change (Archived) [online]. [cit. 18.02.2019]. Dostupné z: https://cve.mitre.org/cve/identifiers/syntaxchange.html
[75] ČERMÁK, Miroslav. Úskalí řízení technických zranitelností. *Bezpečnostní teorie a praxe*. 2020, roč. 2020, č. 4. ISSN 2571-4589. s. 101–120

posoudit závažnost dané zranitelnosti ve vztahu k provozovanému systému. Za tímto účelem by měl provádět pravidelné skeny zranitelností a odebírat bezpečnostní zpravodaje týkající se systémů, které organizace, jež ho najala, provozuje.

Je třeba si však uvědomit, že organizace se může stát jak předmětem cíleného, tak i plošného útoku a včasné odhalení bezpečnostních zranitelností a jejich odstranění anebo nasazení záplaty nebo workaroundu (náhradní řešení) podstatně snižuje dopad vyplývající z daného kybernetického útoku.

Zpravidla se za tímto účelem používají automatické skenery, které prohledávají určitý IP adresní rozsah a vyhodnocují, zda na komponentě, které je daná IP adresa přidělena, neběží nějaký produkt, který by trpěl určitou zranitelností.

Tyto automatické skenery však neprovádějí nějakou sofistikovanou heuristickou analýzu, ani nepracují na principu umělé inteligence, nýbrž jen jednoduše využívají databáze zranitelností, jakými je asi nejznámější a veřejně dostupná Common Vulnerabilities and Exposures databáze, zkr. CVE[76] a s ní pak synchronizovaná National Vulnerability Database, zkr. NVD[77] a rovněž pak i komerční databáze VulnDB[78], ve kterých se nacházejí všechny doposud objevené, resp. zveřejněné zranitelnosti.

A v okamžiku, kdy tyto skenery provádějící sken sítě, a nějaký SW, který danou zranitelností trpí, ve své databázi najdou, tak i uvedou, jaká je závažnost dané zranitelnosti dle Commom Vulnerability Scoring System, zkr. CVSS[79] a případně jakého typu daná zranitelnost je, resp. o jakou se jedná slabinu dle Common Weaknesses Enumeration, zkr. CWE[80]. Některá řešení pak navíc nabídnou i odkaz na záplatu nebo workaround, který danou zranitelnost řeší.

Celé řízení technických zranitelností je pak v zásadě postaveno jen na včasné detekci veřejně známé zranitelnosti v konkrétním produktu a nasazení patche anebo workaroundu. A to může být mnohdy zásadní problém, nehledě na to, že

---

[76] CVE - Common Vulnerabilities and Exposures (CVE) [online]. [cit. 18.02.2019]. Dostupné z: https://cve.mitre.org/index.html
[77] NVD - Home [online]. [cit. 18.02.2019]. Dostupné z: https://nvd.nist.gov/
[78] VulnDB [online]. [cit. 18.02.2019]. Dostupné z: https://vulndb.cyberriskanalytics.com/
[79] Common Vulnerability Scoring System SIG. *FIRST — Forum of Incident Response and Security Teams* [online]. [cit. 18.02.2019]. Dostupné z: https://www.first.org/cvss
[80] CWE - Common Weakness Enumeration [online]. [cit. 18.02.2019]. Dostupné z: https://cwe.mitre.org/

zde jsou i další úskalí, o kterých se běžně v mainstreamových médiích nemluví a ani odborné literatura se tomuto problému dostatečně nevěnuje.

V některých organizacích jsou pak navíc na počtu zranitelností v jednotlivých provozovaných systémech a době potřebné k jejich odstranění postavené i nejrůznější metriky sledující celkový počet zranitelností o určité výši a daného typu a sledování trendů, tedy jestli se jejich počet zvyšuje, klesá, je stabilní, a jak dlouho trvá, než jsou odstraněny, ale tím už se zabývá patch management, který s vulnerability managementem velice úzce souvisí, ale ve větších organizacích ho vykonává zcela jiný tým, než který se věnuje identifikaci zranitelností a jejich analýze.

Problém je, že v okamžiku, kdy se objeví větší počet zranitelností, tak někdo musí stanovit, kterým zranitelnostem je třeba se věnovat jako prvním, protože zdroje organizace jsou zpravidla omezené a nelze tak nasadit všechny záplaty najednou, nehledě na to, že záplaty je třeba nejprve důkladně otestovat, neboť zde vždy volíme mezi dvěma riziky.

Rizikem, že do té doby, než se záplata nasadí a otestuje v neprodukčním prostředí, tak že dané zranitelnosti někdo zneužije, anebo že když se záplata bez nějakého důkladného testování nasadí ihned, tak že to povede k úplnému nebo částečnému omezení dostupnosti daného systému.

Na tomto místě je třeba uvést, že aby se daná zranitelnost dostala do databáze zranitelností, tak ji musí nejprve někdo najít a v případě CVE/NVD i nahlásit prostřednictvím CVE Numbering Authority, zkr. CNA, a teprve ta ji může, ale také nemusí do DB přidat[81]. Možná i proto se objevují názory, že CVE/NVD neobsahuje všechny zranitelnosti, a že komerční VulnDB je lepší.

Zde je však nutné uvést, že VulnDB je postavena na Open Source Vulnerability Database, zkr. OSVDB. Ta vznikla v roce 2002, veřejnosti byla poprvé představena Jakem Kouhnsem v roce 2004, aby skončila po více jak deseti letech provozu v roce 2016, kdy bylo jako důvod ukončení činnosti uvedeno, že je to především proto, že byť měla sloužit jen pro nekomerční využití a určitá skupina

[81] CVE - Request CVE IDs [online]. [cit. 18.02.2019]. Dostupné z: https://cve.mitre.org/cve/request_id.html

firem informace z ní něj vytěžovala a poskytovala dál za úplatu, tak se zároveň nenašel nikdo, kdo by měl zájem tuto aktivitu finančně dál podporovat[82].

Je zajímavé, že navzdory těmto skutečnostem byla již v roce 2011 založena společnost Risk Based Security týmž Jakem Kouhnsem, která později začala nabízet přístup k databázi nazvané VulnDB za úplatu. Je nasnadě, že následně došlo ke ztrátě podpory ze strany bezpečnostní komunity, která do OSVDB do té doby přispívala nezištně a v dobré víře, že budou moci recipročně a bezúplatně využívat informace o zranitelnostech do této DB vložené i ostatními členy komunity. Je otázka, zdali již od počátku nebylo plánováno zpoplatnění této DB a její zpřístupnění veřejnosti nemělo sloužit jen k jejímu vybudování a získání odběratelů těchto informací.

V odborných kruzích se vedou diskuse, zda je pravda, že VulnDB obsahuje více zranitelností než CVE. A Risk Based Security se v tomto směru nebojí jít ani do u nás v ČR zakázané srovnávací reklamy, kdy porovnává počet zranitelností v jejich VulnDB databázi s počtem zranitelností uvedených ve veřejně dostupné CVE/NVD databázi[83]. Risk Based Security mapuje zranitelnosti v jejich VulnDB na zranitelnosti uvedené v CVE a tvrdí, že z tohoto mapování vyplývá, že v jejich VulnDB databázi je až o několik desítek tisíc zranitelností více.

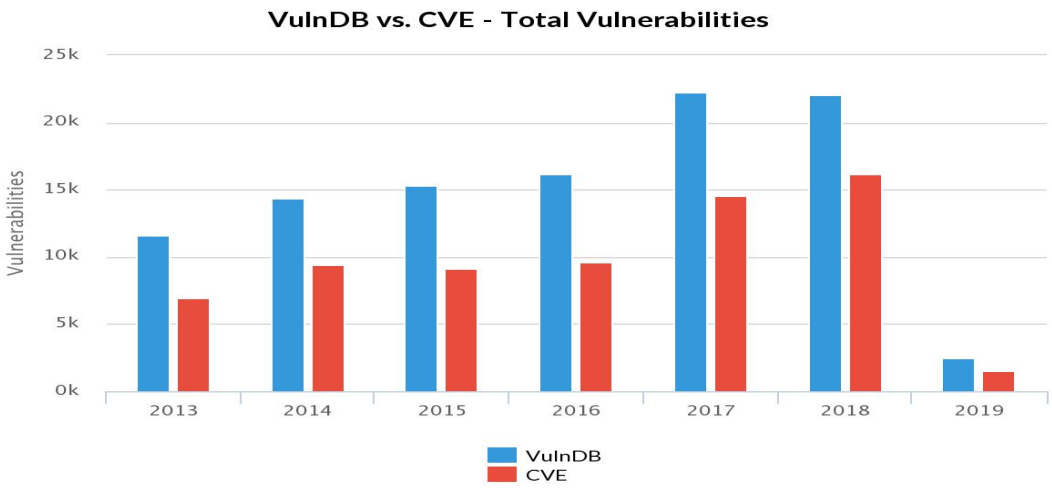
Je však nutné si uvědomit, že tento počet je kumulativní, tj. že se jedná o zranitelnosti odhalené od roku 2013 do současnosti a tudíž, že mnohé z nich již byly dávno odstraněny a prakticky jich není možné zneužít. To však nic nemění na skutečnosti, že VulnDB eviduje až o několik tisíc zranitelností více než CVE/NVD databáze. Není však zřejmé, o jaké zranitelnosti se jedná, tedy v jakých produktech se nachází a jaká je jejich závažnost.

Dalo by se předpokládat, že pokud v CVE/NVD jsou uvedeny zranitelnosti v nejpoužívanějších produktech, tak není moc pravděpodobné, že bychom ve VulnDB našli zranitelnosti, které se těchto produktů týkají, daleko pravděpodobnější je, že se v ní nachází zranitelnosti ve spíše méně používaných produktech anebo ty, kterým z nějakého důvodu nebylo přiděleno CVE-ID. Tomu by odpovídal i podobný průběh křivky, kterou zachycuje Graf 1 – VulnDB vs. CVE,

[82] OSVDB: FIN. *OSVDB* [online]. [cit. 18.02.2019]. Dostupné z: https://blog.osvdb.org/2016/04/05/osvdb-fin/
[83] VulnDB [online]. [cit. 18.02.2019]. Dostupné z: https://vulndb.cyberriskanalytics.com/

naznačující, že zde zcela jistě bude určitá korelace mezi počtem zranitelností v CVE/NVD a VulnDB.

Graf 1 – VulnDB vs. CVE



Zdroj: VulnDB vs. CVE. In: *Cyberriskanalytics.com* [online]. Risk Based Security. [cit 2022-02-02]. Dostupné z https://vulndb.cyberriskanalytics.com/

Risk Based Security však ve svém reportu[84] uvádí, že např. v roce 2017 publikovali 6295 zranitelností, které nebyly uvedeny v CVE/NVD databázi. A že cca 44 % z nich dosáhlo skóre mezi 7,0 až 10 a téměř 20 % pak 9 až 10, což představuje kritickou zranitelnost. Pokud jde o samotné produkty, tak uvádí, že se jednalo např. i o zranitelnosti v prohlížeči Chrome, ke kterým byl k dispozici i exploit a téměř 70 % zranitelností spočívalo v nedostatečné validaci vstupu.

Risk Based Security rozporuje přístup CVE/NVD k počítání zranitelností a upozorňuje na 10.000 CVE, které jsou rezervovány[85] již několik let, a dále pak na nafukování počtu zranitelností ze strany některých organizací (neuvádějí kterých, ale nejspíš narážejí na CVE/NVD) spravujících databáze zranitelností, a které započítávají některé zranitelností vícekrát s tím, že oni sami počítají zranitelnost např. v OpenSSL knihovně využívané v mnoha produktech jen

[84] SECURITY, Risk Based. Request the latest Vulnerability Quick View Report from Risk Based Security [online]. [cit. 18.02.2019]. Dostupné z: https://pages.riskbasedsecurity.com/2017-q3-vulnerability-quickview-report

[85] V CVE se skutečně nacházejí zranitelnosti označené jako **RESERVED**, v NVD však již uváděny nejsou.

jednou. A konečně na dlouhou prodlevu mezi oznámením zranitelnosti a jejím začleněním do CVE/NVD v některých případech až po více jak 30 dnech.

Ověření všech tvrzení a kvality VulnDB databáze by vyžadovalo další hlubší analýzu a k té by bylo nutné získat přístup k samotné DB, který je zpoplatněn. Dále proto bude v rámci této práce využíváno informací o zranitelnostech, které jsou uvedeny v bezplatné CVE/NVD databázi.

2.1.8 Hodnocení zranitelností

V současné době se pro hodnocení zranitelností paralelně s CVSSv3 ve stále mnoha bezpečnostních řešeních a reportech používá i hodnocení zranitelností dle CVSSv2 a vzhledem k tomu, že tyto verze generují při hodnocení stejné zranitelnosti rozdílné výsledky, je vždy žádoucí uvést, jaká verze byla pro hodnocení použita.

Cílem organizace First bylo představit veřejnosti takovou metodiku hodnocení, která by zabránila nafukování jednotlivých zranitelností do obrovských rozměrů a dělání z komára velblouda, v originále “make mountains out of mole hills”.

Base Score

CVSSv2 používá ke stanovení úrovně zranitelnosti tzv. základního skóre (Base Score, zkr. BS) následujících 6 faktorů (první 3 faktory představuji tzv. Exploitability Metrics a další 3 pak Impact Metrics):

- **Access Vector (AV) –** zde se ptáme, odkud může být veden útok. A možnosti jsou: z internetu (network, zkr. N), ze sítě, kde se nachází systém trpící danou zranitelností (adjacent network, zkr. A), nebo útočník musí mít fyzický přístup k danému systému (local, zkr. L).

- **Access Complexity (AC)** – ke zneužití dané zranitelnosti již nemusí být splněny žádné podmínky, není potřeba žádná součinnost (low, zkr. L), je nutné mít určité informace o systému, je potřeba minimální součinnost ze strany oběti, jako je třeba kliknutí na odkaz (medium, zkr. M), útok je možné realizovat jen za určitých podmínek, na určité konfiguraci a je nutné, aby oběť provedla několik kroků (high, zkr. H).

- **Authentication** (Au) – Ke zneužití zranitelnosti není nutný účet v systému (none, zkr. N), je nutné se přihlásit (single, zkr. S), je nutné se přihlásit do systému i do aplikace (multiple, zkr. M).

- **Confidentiality impact (C)** – zde se ptáme, zda zneužitím zranitelnosti dojde k získání citlivých informací, a to všech dat, která se nacházejí v paměti nebo na disku (complete, zkr. C), nebo jen části z nich (partial, zkr. P) anebo vůbec žádných (none, zkr. N).

- **Integrity impact** (I) – zde se ptáme, zda zneužitím zranitelnosti dojde ke znehodnocení všech dat, která se nacházejí v paměti nebo na disku (complete, zkr. C), nebo jen části z nich (partial, zkr. P) anebo vůbec žádných (none, zkr. N).

- **Availability impact (A)** – zde se ptáme, zda zneužitím zranitelnosti dojde k znepřístupnění dat nebo služby (complete, zkr. C) anebo jen k částečnému omezení funkčnosti a dostupnosti dat (partial, zkr. P) anebo to nemá vůbec žádných dopad (none, zkr. N).

CVSSv3 používá ke stanovení úrovně zranitelnosti tzv. základního skóre (Base Score, zkr. BS) následujících 8 otázek (prvních 5 faktorů představuje tzv. Exploitability Metrics a další 3 pak Impact Metrics):

- **Attack Vector**(AV) rozlišuje, zda je možné útok realizovat z internetu (Network, zkr. N), z místní sítě ze stejného subnetu (Adjacent, zkr. A), lokálně (Local, zkr. L) anebo zda je nutné mít i fyzický přístup k danému zařízení (Physical, zkr. P). V okamžiku, kdy je možné vést útok přes internet, tak je zde větší množství útočníků, větší anonymita a nižší šance na odhalení útočníka, a tudíž se zneužití dané zranitelnosti stává mnohem pravděpodobnější, než když je nutné k danému zařízení získat fyzický přístup.

- **Attack Complexity** (AC) může nabývat jen dvou hodnot, a to (Low, zkr. L), kdy k realizaci útoku nemusí být splněny žádné podmínky, nebo (High, zkr. H), kdy naopak musí být splněny určité podmínky. Je zřejmé, že

v okamžiku, kdy je možno útok realizovat prakticky kdykoliv a není k tomu nutné splnit žádné podmínky, tak je pravděpodobnost zneužití takové zranitelností mnohem vyšší, než když je jí možno zneužít jen při splnění určitých podmínek.

- **User Interaction** (UI) může nabývat dvou hodnot, a to (None, zkr. N), kdy žádná interakce ze strany oběti není k realizaci útoku nutná, anebo (Required, zkr. R), kdy, jak již sama hodnota napovídá, je nějak interakce ze strany oběti vyžadována. Závažnost zranitelnosti je vyšší v okamžiku, kdy žádná interakce ze strany uživatele není nutná a zneužití dané zranitelnosti je tak zcela nezávislé na vůli uživatele a jeho bezpečnostním povědomí.

- **Privileges Required** (PR) může nabývat třech hodnot. (None, zkr. N), kdy útočník nemusí disponovat žádným účtem v systému, (Low, zkr. L), kdy má útočník v systému nějaký účet s omezenými právy, a (High, zkr. H), kdy má v systému účet se silnými právy. Závažnost zranitelnosti je vyšší v okamžiku, kdy útočník žádnými privilegii v systému disponovat nemusí, v takovém případě je značně ztížena identifikace uživatele a pravděpodobnost zneužití dané zranitelnosti roste.

- **Scope** (S) bere v úvahu tu skutečnost, že byť se zranitelnost může nacházet v jedné komponentě, tak úspěšný útok může mít dopad na zcela jinou komponentu. Scope tak může nabývat dvou hodnot, nezměněn (Unchanged, zkr. U), zranitelnost i dopad se týká stejné komponenty, a změněn (Changed, zkr. C), kdy zneužití zranitelnosti má dopad na jinou komponentu.

- **Impact Metrics** se zabývá hodnocením toho, k jakému narušení bezpečnosti došlo, zda se týká důvěrnosti (Confidentiality, zkr. C), integrity (Integrity, zkr. I) a dostupnosti (Availability, zkr. A), a jakého rozsahu dané narušení je, zda žádné (none, zkr. N) nízké, (low, zkr. L) nebo vysoké (high, zkr. H). Je zřejmé, že závažnost dané zranitelnosti bude tím vyšší, čím vyšší bude onen dopad z jejího zneužití.

- **Confidentiality impact (C)** – zde se ptáme, zda zneužití zranitelnosti může vést k získání citlivých informací, a zda útočník má kontrolu nad tím, jaké informace může získat (High, zkr. H) anebo ne (Low, zkr. L), anebo nemá možnost přistoupit k žádným datům (none, zkr. N)

- **Integrity impact** (I) – zde se ptáme, zda zneužití zranitelnosti může vést ke změně dat, a zda má nad onou modifikací útočník plnou kontrolu (High, zkr. H) či nikoliv (Low, zkr. L) anebo nemůže provést žádnou neautorizovanou modifikaci (none, zkr. N).

- **Availability impact (A)** – zde se ptáme, zda zneužití zranitelnosti může vést k částečné (Low, zkr. L) anebo úplné nedostupnosti (High, zkr. H) systému anebo nemůže vůbec ohrozit dostupnost daného systému (none, zkr. N).

Ze srovnání CVSSv2 a CVSSv3 vyplývají následující podstatné skutečnosti:

- **Access vector** byl přejmenován na Attack vector, avšak nadále platí, že z čím větší vzdálenosti je možné vést útok, tím závažnější je daná zranitelnost. Nově se rozlišuje, zda je možné útok realizovat jen díky možnosti se přihlásit lokálně do daného systému (Local) anebo zda je nutné mít i fyzický přístup k danému zařízení (Physical).

- **Access complexity** faktor byl de facto rozdělen na faktory dva, a to Attack Complexity a User Interaction.

- **User Interaction** je zcela nový faktor, ale de facto se jedná o jeho vyčlenění z Access Complexity.

- **Privileges Required** je též zcela nový faktor, ale v zásadě vznikl přejmenováním Authentication, nicméně částečně došlo i k posunu významu.

- **Scope** je zcela novým faktorem, který bere v úvahu tu skutečnost, že byť se zranitelnost může nacházet v jedné komponentě, tak úspěšný útok může mít dopad na zcela jinou komponentu.

- **Impact Metrics** prošly rovněž změnou, neboť došlo v podstatě k rozšíření možností, a to ze dvou na tři, kdy u důvěrnosti, integrity a dostupnosti byly možnosti Partial a Full nahrazeny Low, Medium a High.

Tyto změny vedly ve výsledku k tomu, že stejná zranitelnost hodnocená stejným způsobem dosahuje v CVSSv2 a CVSSv3 rozdílného skóre. Ověřit to lze poměrně snadno pomocí on-line kalkulátoru CVSSv2[86] a CVSSv3[87]. V *Příloha C – Rozdílné hodnocení zranitelností dle CVSSv2 a CVSSv3* je uveden výsledek hodnocení stejné zranitelnosti.

Nejvíce se pak liší Exploitability Subscore (zneužitelnost) a Impact Subscore (dopad) vstupující do výpočtu Base Score (základní skóre), tedy toho, které je u každé zranitelnosti běžně uváděno.

Exploitable Subscore může ve CVSSv2 nabývat hodnot 1,2 až 10 a v CVSSv3 pak 0,1 až 3,9. Impact Subscore může ve verzi CVSSv2 nabývat hodnot 0 až 10 a v CVSSv3 pak 0 až 6. Exploitable Subscore a Impact Subscore v CVSSv2 a CVSSv3 jsou tak vzájemně neporovnatelné. Na první pohled dává hodnocení v CVSSv2 větší smysl. Nicméně vzhledem k tomu, že s Exploitable Subscore a Impact Subscore téměř nikdo nepracuje, tak to není až tak zásadní nedostatek.

Dále je třeba se věnovat rozdílnému hodnocení AV (vektor útoku), který v CVSSv3 používá oproti CVSSv2 čtyři stupně hodnocení namísto třech, kdy vektor útoku Local (místní), tak jak ho vnímá CVSSv3, není totéž, co v CVSSv2, neboť Local ve CVSSv2 odpovídá Physical (fyzický) v CVSSv3, kdy je skutečně nutné disponovat fyzickým přístupem k zařízení.

Temporal Score

Vzhledem k tomu, že závažnost zranitelnosti ještě ovlivňuje faktor času, tak je možné její hodnotu ještě upravit na základě další sady otázek určující tzv. Temporal Score, zkr TS, tedy dočasné, a to proto, že se skutečně v čase mění. Vzhledem k jeho nestálosti se nikde neeviduje a má smysl se jím zabývat snad

[86] NVD - CVSS v2 Calculator [online]. [cit. 18.02.2019]. Dostupné z: https://nvd.nist.gov/vuln-metrics/cvss/v2-calculator
[87] NVD - CVSS v3 Calculator [online]. [cit. 18.02.2019]. Dostupné z: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

jen v okamžiku hodnocení dané zranitelnosti. CVSSv2 i CVSSv3 hodnotí při stanovení temporal skóre následující faktory:

- **Exploitability** (E) – pokud je k dispozici malware, který se již šíří (high, zkr. H), existuje jen exploit (functional, zkr. F), bylo zmíněno, že se někomu podařilo zranitelnosti zneužít (proof-of-concept, zkr. POC) nebo byla zranitelnost popsána jen v teoretické rovině (unproven, zkr. U). Nedefinováno (Not Defined, zkr. ND) znamená, že tento faktor nebude vstupovat do výpočtu.

- **Remediation Level** (RL) – Momentálně neexistuje žádné řešení pro snížení zranitelnosti (unavailable), je k dispozici neoficiální řešení (workaround), je k dispozici oficiální dočasný fix, workaround od vendora (Temporary fix), je k dispozici kompletní řešení, patch od vendora (official fix). Pokud zvolíte Not Defined, tak nebude tento faktor vstupovat do výpočtu.

- **Report Confidence** (RC) – Zranitelnost byla oficiálně potvrzena vendorem (confirmed), zranitelnost byla potvrzena ostatnímu firmami (uncorroborated), o zranitelnosti informuje jen jeden zdroj či podsvětí a objevují se různé spekulace a protichůdné názory (uncomfirmed). Pokud zvolíte Not Defined, tak nebude tento faktor vstupovat do výpočtu.

Environmental Score

Kromě faktoru času vstupuje do hodnocení závažnosti zranitelnosti i prostředí, ve kterém je daný systém provozován, komu a k čemu slouží a jaký by mohl vzniknout následek z narušení bezpečnosti. K zohlednění této skutečnosti slouží sada otázek tzv. Environmental Score, zkr. ES, které se rovněž nikde neobjevuje, a neeviduje, protože slouží čistě jen manažerovi kybernetické bezpečnosti k přehodnocení dané zranitelnosti a stanovení priority řešení v případě, že by více zranitelností dosáhlo stejného base score a temporal score, kdy je možné AV, AC, PR, UI, S, C, I, A, CR, IR a AR předefinovat a tím zjistit, jak závažná je daná zranitelnost za aktuálních podmínek pro danou organizaci.

Vzorec pro výpočet BS je uveden v *Příloha D – Vzorec pro výpočet hodnoty zranitelnosti CVSSv3, kde* se též nachází spreadsheet, který byl vytvořen v rámci této práce a je použitelný i pro hodnocení zranitelností, které mohou být identifikovány např. během penetračních testů webové aplikace nebo infrastruktury, používané v testované organizaci, a které se nikdy v CVE/NVD neobjeví.

Závažnost zranitelnosti

Závažnost zranitelnosti může nabývat hodnot z intervalu <0,10>, přičemž pro jejich zvládání v CVSSv2 pracuje se těmito 3 stupni, zatímco CVSSv3 pak s 5 resp. 4 stupni. Tuto skutečnost přehledně zachycuje *Tabulka 6 – Srovnání hodnocení CVSSv2 a CVSSv3*.

Tabulka 6 – Srovnání hodnocení CVSSv2 a CVSSv3

CVSSv2		CVSSv3	
interval	popis	interval	popis
0,0–3,9	nízká (low)	0,0–3,9	nízká (low)
4,0–6,9	střední (medium)	4,0–6,9	střední (medium)
7,0–10,0	vysoká (high)	7,0–8,9	vysoká (high)
–	–	9,0–10,0	kritická (critical)

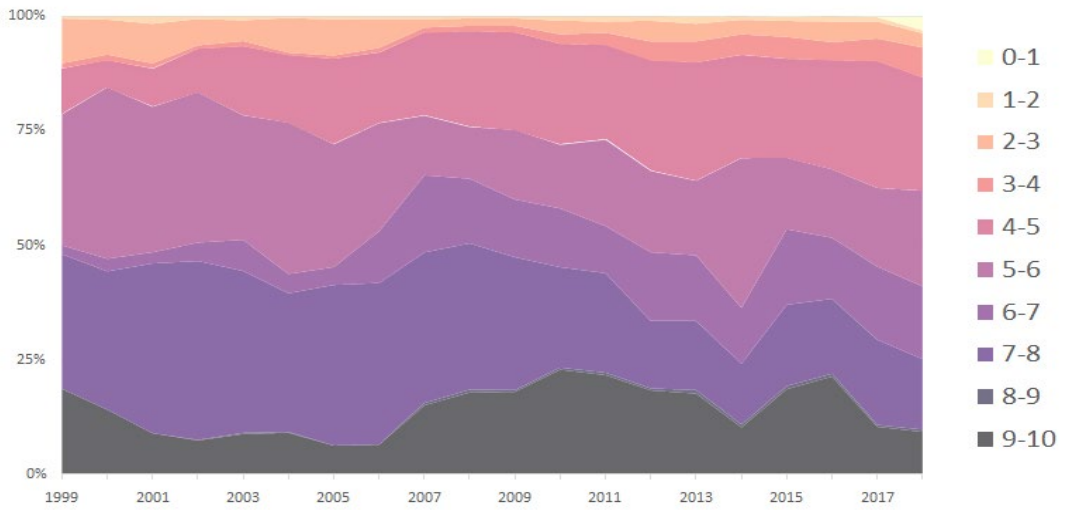
Tabulka 6 – Srovnání hodnocení CVSSv2 a CVSSv3 ukazuje, že došlo k rozdělení intervalu <7,10>, tedy zranitelností v CVSSv2 označených jako vysoké na vysoké <7,9) a kritické <9,10> v CVSSv3, což umožňuje lepší prioritizaci zranitelností.

Problém je, že **tímto způsobem lze hodnotit jen technické zranitelnosti v konkrétním produktu, nikoliv však zranitelnosti spočívají v absenci nebo nedostatečnosti generických organizačních a technických opatření**. Vzhledem k tomu, že přítomnost zranitelnosti v systému je pro hodnocení možnosti jeho kompromitace klíčová, je nutné provést analýzu jednotlivých zranitelností. Jako zdrojová data byla použita databáze zranitelností CVE/NVD,

kde jsou všechny hlášené zranitelnosti evidovány. Databáze zranitelností čítá více jako 100 000 záznamů a počet těchto záznamů roste.

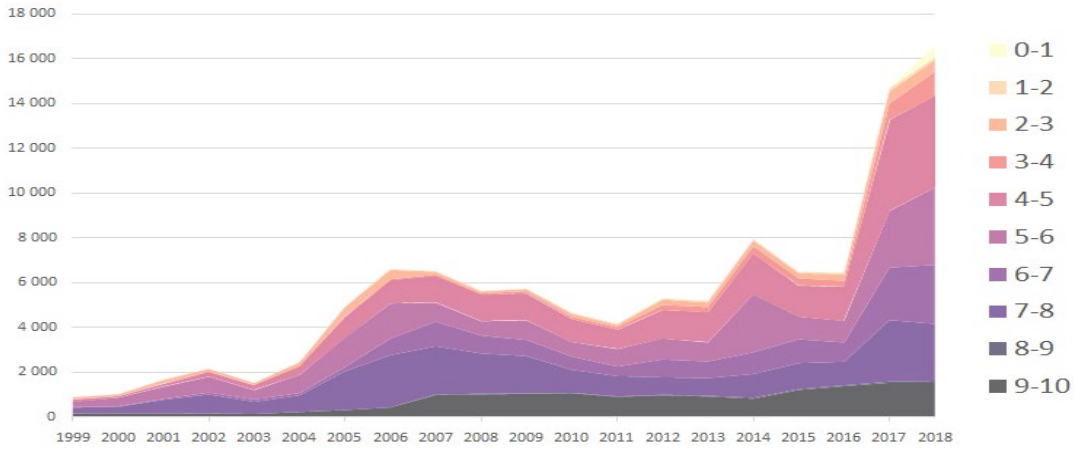
Příloha B – CVE zdrojová data obsahuje matici zachycující počet CVE se stejným CVSS skóre v jednotlivých letech. Tato data pak lze vizualizovat např. tak, jak je zachycuje Graf 2 – Relativní četnost CVE v letech, z kterého vyplývá, že přestože **v posledních dvou dekádách nedošlo k nějakým dramatickým změnám, a že zastoupení jednotlivých zranitelností hodnocených stejným stupněm závažnosti je více či méně rovnoměrné**, tak je z grafu nicméně patrné, že četnost výskytu zranitelností o stejné závažnosti z počátku až tak rovnoměrná nebyla, ale v čase lze tento trend pozorovat.

Graf 2 – Relativní četnost CVE v letech



Mnohem zajímavější přehled o vývoji zranitelností v posledních dvou dekádách však přináší *Graf 3 – Absolutní četnost CVE v letech*. Z grafu je patrné, že zatímco v prvních letech rostl počet zranitelností pozvolna, svého lokálního maxima dosáhl v roce 2006 a dalších deset letech se počet nově objevených zranitelností pohyboval mezi 4 až 7 tisící zranitelností ročně, tak v roce 2017 došlo k náhlému prudkému nárůstu zranitelností, a to o více jak 100 %.

Graf 3 – Absolutní četnost CVE v letech



Na základě výše uvedené analýzy lze předpokládat, že **počet zranitelností nepochybně nadále poroste**. Rovněž platí, že kromě zranitelností, kterým bylo přiděleno CVE-ID, existuje ještě velké množství zranitelností, které nebyly nahlášeny anebo byly nahlášeny, a přesto jim nebylo přiděleno CVE-ID.

Dle VulnDB se jedná až o několik desítek tisíc takových zranitelností[88]. Je samozřejmě otázka, zda uvedené číslo není nadhodnocené, ovšem z rozhovoru s namátkou oslovenými penetračními testery vyplynulo, že mnohé jimi identifikované zranitelnosti v CVE/NVD databázi nejsou uvedeny.

Výše uvedené grafy však nepřináší odpověď na otázku, které systémy nebo produkty obsahují nejvíce zranitelností a zda zde existuje nějaký trend, na základě kterého by se dalo usuzovat, jak se bude trh se zranitelnostmi dále vyvíjet a jakých zranitelností a v jakých produktech bude dále zneužíváno.

Když se podíváme např. na seznam 50 produktů s největším počtem zranitelností[89], tak jsou zde v zásadě uvedeny všechny nejpoužívanější OS, prohlížeče a další aplikace. Lze předpokládat, že nejvíce zranitelností bude nadále hledáno a nacházeno v nejpoužívanějších OS, aplikacích, webových službách a zařízeních, **neb tam bude vždy dostatečný počet potenciálních obětí, a nic nenaznačuje, že by se na tomto trendu mělo v nejbližších letech něco podstatného změnit. Tento dílčí závěr je pro další směřování práce a návrhu**

[88] VulnDB [online]. [cit. 18.02.2019]. Dostupné z: https://vulndb.cyberriskanalytics.com/
[89] CVSS Score Distribution For Top 50 Products By Total Number Of Distinct Vulnerabilities [online]. [cit. 18.02.2019]. Dostupné z: https://www.cvedetails.com/top-50-product-cvssscore-distribution.php

vhodné metodiky hodnocení bezpečnosti zásadní, neboť je zřejmé, že nemá v podstatě smysl se při hodnocení bezpečnosti zaměřovat na to, jaké SW a HW produkty organizace používá, protože ve většině produktů jsou v průběhu roku identifikovány nejrůznější zranitelnosti a všechny organizace jsou tak na tom z tohoto pohledu více méně stejně.

A pokud zde budou navíc ještě firmy obchodující s exploity, tak potom musíme počítat s tím, že určité zero-day zranitelnosti budou zneužívány i po dobu několika týdnů, měsíců až let k cíleným útokům na konkrétní subjekty. A dále že pokud dojde ke zveřejnění určité zranitelnosti, tak se kód zneužívající této zranitelnosti poměrně rychle stane součástí běžných exploit kitů, což dosavadní zkušenosti rovněž potvrzují.

Pro úplnost je třeba dodat, že kromě pojmu zranitelnost se můžeme ještě setkat s pojmem slabina, což ale není totéž, neboť slabinu je třeba vnímat spíše jako typ zranitelnosti[90]. **Z výše uvedeného důvodu je nutné se soustředit ani ne tak na technické zranitelnosti, jako na vhodná bezpečnostní opatření.**

2.1.9 Opatření

V anglosaské literatuře se pro pojem opatření používá pojem control. Opatření mohou být proaktivní, pak se hovoří o safeguards, anebo reaktivní, a pak se hovoří o countermeasures[91]. V češtině se však používá výhradně pojem opatření, a byť je mezi opatřením a protiopatřením rozdíl, bude v této práci používán jen pojem opatření.

Organizace by měla zavést odpovídající bezpečnostní opatření, která by ji ochránila před kybernetickými hrozbami, které by mohly zneužít technických a organizačních zranitelností a mít negativní dopad na dosažení vize a mise organizace. A **vzhledem k tomu, že každá organizace disponuje různými informačními aktivy (kapitola 2.1.3), může rovněž čelit i mnoha různým útokům (kapitola 2.1.5) ze strany různých agentů hrozeb (kapitola 2.1.2) a je**

---

[90] ČERMÁK, Miroslav. Slabina vs. zranitelnost a jaký je mezi nimi vztah. *CleverAndSmart Management Consulting* [online]. 2018 [cit. 12.04.2020]. ISSN 2694-9830. Dostupné z: https://www.cleverandsmart.cz/slabina-vs-zranitelnost-a-jaky-je-mezi-nimi-vztah/

[91] *CISA review manual*. 27th edition. Schaumburg, IL, USA: ISACA, 2019. ISBN 978-1-60420-767-5.

tak zřejmé, že každá organizace bude přistupovat k zavedení vhodných bezpečnostních opatření a dosažení požadované úrovně bezpečnosti odlišně.

Přesto by každá organizace měla zavést základní sadu bezpečnostních opatření a usilovat o tzv. obranu v hloubce (defense in depth), někdy se též hovoří o vícevrstvé bezpečnosti (multilayered security), kdy se předpokládá, že když je zavedeno více opatření v řadě, tak v okamžiku, kdy jedno opatření selže, tak jsou stále ještě funkční další opatření, která by měla zafungovat. **Pokud jde o zavedení vhodných bezpečnostních opatření, tak se v praxi můžeme setkat se dvěma základními přístupy, tzv. risk driven a control driven**[92], které se vzájemně doplňují a ve výsledku by měly vést k vytvoření strategie informační bezpečnosti, která by měla obsahovat plán implementace jednotlivých bezpečnostních opatření.

Vhodná bezpečnostní opatření jsou pak uvedena např. v mezinárodních standardech a normách jako je např. ČSN ISO/IEC 27001 a 27002, ve vyhláškách jako je VoKB, NIST Cybersecurity frameworku anebo jsou generovány nástroji na analýzu rizik. Samotná bezpečnostní opatření můžeme rozdělit podle několika různých kritérií např. na:

- organizační, někdy nazývané též administrativní nebo také direktivní;
- technická, někdy nazývané také logická;
- fyzická.

Podle toho, na jaké vrstvě informačního systému jsou nasazena, lze bezpečnostní opatření rozdělit na:

- systémová na úrovni operačního systému;
- aplikační na úrovni aplikace;
- databázová na úrovni databáze;
- komunikační na úrovni síťových prvků.

Dle účelu, který mají bezpečnostní opatření plnit, je lze rozdělit na:

- preventivní;

---

[92] ČERMÁK, Miroslav. Mělo by být řízení informační bezpečnosti postavené na rizicích nebo opatřeních? *CleverAndSmart Management Consulting* [online]. 2019 [cit. 12.04.2020]. ISSN 2694-9830. Dostupné z: https://www.cleverandsmart.cz/melo-by-byt-rizeni-informacni-bezpecnosti-postavene-na-rizicich-nebo-opatrenich/

- odstrašující;
- zdržující;
- detekční;
- reaktivní.

2.1.10 Hodnocení opatření

Na první pohled se jeví, že by se bezpečnost dala hodnotit od úrovně zavedení bezpečnostních opatření. Jednalo by se o tzv. control driven přístup, který nebere v potaz, zda dané opatření má smysl, či nikoliv. Řekněme, že existují 4 organizace, označme si je A, B, C, D, u nich budeme rozlišovat, zda je pro ně kritická důvěrnost, integrita a dostupnost či nikoliv a zda zavedly příslušnou sadu bezpečnostních opatření. V zásadě mohou nastat situace, které zachycuje Tabulka 7 – Zavedení opatření.

Tabulka 7 – Zavedení opatření

Opatření/Atribut	ANO	NE
Zavedeno	A	C
Nezavedeno	B	D

Jak interpretovat stavy zachycené v Tabulka 7 – Zavedení opatření? Pro organizaci A je daný atribut klíčový a příslušnou sadu bezpečnostních opatření zavedla, což by mělo být hodnoceno pozitivně. Pro organizaci B je daný atribut rovněž klíčový a danou sadu opatření nezavedla, což by mělo být hodnoceno negativně. Jak však přistoupit k hodnocení organizace C a D? Obě jistě měly k takovému rozhodnutí nějaký důvod.

V případě organizace C lze hovořit o předběžné opatrnosti, kdy se rozhodla dané opatření zavést přesto, že to nebylo nezbytně nutné, protože se mohly obávat změny situace v kyberprostoru v blízké budoucnosti nebo uvažují o rozšíření portfolia služeb o ty, pro které již bude bezpečnost klíčová. V případě organizace D pak lze hovořit o tom, že se rozhodla danou sadu bezpečnostních

opatření neimplementovat prostě proto, že daná hrozba pro ně není relevantní a snaží se maximálně využít svých zdrojů.

Organizace B by zcela jistě měla být hodnocena hůře než A, C, D, ale měly by organizace A, C a D dosáhnout v hodnocení úrovně bezpečnosti stejného výsledku? Pokud by ho dosáhly, mohlo by to pro nezaujatou osobu znamenat, že je jejich úroveň bezpečnosti stejná, ale ona není, tedy pokud platí původní premisa, že úroveň bezpečnosti se odvíjí od zavedených opatření a D oproti A a C žádná opatření nezavedlo. Tím se dostáváme k tomu, že A a C by mohlo být hodnoceno stejně. Rozdíl je jen v tom, že byť je úroveň bezpečnosti v A a C stejná, tak C by stačila dosáhnout nižší úrovně bezpečnosti, aby se dalo hovořit o tom, že dostatečně chrání svá aktiva.

Měla by být stejně hodnocena i úroveň bezpečnosti v organizaci B a D? Obě organizace opatření nezavedly, ale organizace B měla příslušná opatření správně zavést, ale nezavedla, zatímco organizace D žádná opatření zavést nemusela, a proto tak celkem logicky neučinila.

Jisté je, že A a B budou stát na opačné straně hodnocení. Dále platí, že A=C, a byť je A a C objektivně stejné, tak subjektivně z pohledu zevnitř organizace dosáhla organizace C vyšší úrovně než A. Obdobně je tomu i u B a D, protože obě organizace dané opatření nezavedly. Byť objektivně lze vzhledem k absenci opatření vnímat jejich úroveň bezpečnosti jako stejnou a můžeme zapsat, že B=D, tak subjektivně z pohledu organizace je na tom D lépe. **Vzhledem k tomu, že cílem je navrhnout hodnocení, který by mělo být objektivní a použitelné pro hodnocení organizace ze strany externích subjektů, je nasnadě, že bude nutné zvolit taková opatření, která by měla zavést prakticky každá organizace.**

Návrh vhodných opatření, která by byla účinná proti nejčastějším útokům, jsou představena v praktické části této práce.

3 ZHODNOCENÍ SITUACE V KYBERPROSTORU – praktická část

V teoretické části práce bylo uvedeno, co je to kyberprostor a jakým způsobem útoky v kyberprostoru probíhají, a že v kyberprostoru proti sobě vždy stojí provozovatel určitého systému na jedné straně a útočník na straně druhé.

Nabízí se tak položit si otázku, zda by se nedalo hodnocení úrovně bezpečnosti v organizaci postavit na množství a závažnosti zranitelností přítomných v jednotlivých systémech, které organizace provozuje. Je nasnadě, že v okamžiku, kdy organizace provozuje systém, který obsahuje nějakou závažnou zranitelnost, tak významně roste riziko, že této zranitelnosti někdo zneužije. Ovšem takovéto hodnocení by bylo značně volatilní, protože počet zranitelností se velice rychle mění a snadno by se tak mohlo stát, že organizace, která má zavedena všechna odpovídající bezpečnostní opatření a provozující rozsáhlý a komplexní systém složený z mnoha různých produktů, by na tom byla výrazně hůře než organizace, která žádné bezpečnostní opatření nezavedla a v jím provozovaném systému zatím žádná zranitelnost reportována nebyla.

Rovněž zavádějící je hodnocení postavené na pouhé implementaci jednotlivých bezpečnostních opatření organizační a technické povahy, protože ty, byť jsou zavedeny, nemusí poskytovat spolehlivou úroveň ochrany před aktuálními hrozbami. **Aby však bylo možné posoudit, na jaké úrovni je bezpečnost v organizaci zavedena a zda jsou přijatá bezpečnostní opatření dostatečná, musíme se ptát, jakým hrozbám je daná organizace vystavena, protože ne všechny organizace musí čelit stejným útokům.**

A zde narážíme na skutečnost, že nemáme objektivní a úplné informace o tom, co se děje v kyberprostoru. Je třeba si uvědomit, že jsou to publicisté a samotné firmy působící na trhu s bezpečnostními technologiemi, které sledují svůj vlastní zájem, tím je zpravidla generování zisku, a vytvářejí za tímto účelem určitý mediální obraz o tom, jaká je situace v kyberprostoru[93].

[93] ČERMÁK, Miroslav. O skutečné situaci v kyberprostoru máme jen mlhavou představu. *CleverAndSmart Management Consulting* [online]. 2020 [cit. 12.04.2020]. ISSN 2694-9830. Dostupné z: https://www.cleverandsmart.cz/o-skutecne-situaci-v-kyberprostoru-mame-jen-mlhavou-predstavu/

Současnou situaci v kyberprostoru by mohl vystihovat výrok „Válka zuří zuřivou zuřivostí“, který zazněl v příběhu Arnal a dva dračí zuby od Ondřeje Neffa[94]. Ale je tomu opravdu tak? Není třeba pochybovat o tom, že ke kybernetickým útokům skutečně dochází a jejich počet roste, ovšem otázka je, k jakým útokům dochází, jaký je vektor útoku, jak jsou tyto útoky cílené a k jakým dochází ztrátám.

Vzhledem k tomu, že organizace nemají povinnost hlásit, že na ně byl veden kybernetický útok, tak nevíme nic o tom, kolik těch útoků je, na koho jsou vedeny a jakým způsobem probíhají. A nedělejme si iluze, že i kdyby tady ta povinnost byla, tak by se všechny firmy snažily tuto svou povinnost splnit a útoky by poctivě hlásily a nezamlčovaly by podstatné skutečnosti. A nelze se tomu divit, protože i pouhá informace o tom, že se firma stala obětí kybernetického útoku, ji může vážně poškodit[95].

V prvé řadě je třeba si uvědomit, že úroveň bezpečnosti může být vnímána různě. Jinak bude vnímána ze strany organizací, na které je veden útok, jinak ze strany firem nabízejících bezpečnostní řešení a konečně jinak ze strany odborné i laické veřejnosti, která produktů těchto organizací využívá, přičemž všichni tito aktéři jsou podstatným způsobem ovlivněny médii, která formují jejich názor. Nesmíme však zapomínat, že informace ze strany jednotlivých aktérů jsou ve většině případů uvolňovány v rámci cílené PR kampaně a měly by zpravidla napomoci dosažení zisku.

Pro novináře a marketingové experty pracující pro společnosti, jež nabízejí bezpečnostní řešení, je pak každá informace o proběhnuvším útoku zajímavá, protože jedni mají o čem psát a druzí mohou hned nabídnout i nějaké bezpečnostní řešení. Objektivní zpravodajství poskytované nezávislými novináři může být značně zkreslené a může docházet k šíření dezinformací prvního typu[96]. Nelze si nevšimnout, že v téměř každém článku je zmíněna firma, která nabízí

---

[94] SAUDEK, Karel a Ondřej NEFF. *Arnal a dva dračí zuby & jiné příběhy*. Praha: Egmont ČR, 2002. ISBN 978-80-7186-802-6.

[95] ČERMÁK, Miroslav. Krátké zamyšlení nad reputačním rizikem. *CleverAndSmart Management Consulting* [online]. 2015 [cit. 07.08.2019]. ISSN 2694-9830. Dostupné z: https://www.cleverandsmart.cz/jak-ridit-reputacni-rizika/

[96] ČERMÁK, Miroslav. Nová média, názorové bubliny a profesionální žurnalistika: formy dezinformace. *CleverAndSmart Management Consulting* [online]. 2019 [cit. 07.08.2019]. ISSN 2694-9830. Dostupné z: https://www.cleverandsmart.cz/nova-media-nazorove-bubliny-a-profesionalni-zurnalistika-formy-dezinformace/

nějaký produkt anebo řešení, které by mělo útok detekovat, umožnit rychlé zotavení se z incidentu anebo útoku zcela zabránit.

Tento obraz, který média o útocích v kyberprostoru vytváří, může naprosto zásadně ovlivnit vnímání bezpečnosti ze strany všech aktérů. Jinými slovy, situace v kyberprostoru může být zcela odlišná od toho, jak je popisována a vnímána, což znamená, že **význam jednotlivých hrozeb může být podceňován nebo naopak přeceňován a stejně tak i dopady z nich vyplývající**.

Největší dopad mají kybernetické útoky na malé společnosti, kde není bezpečnost zpravidla vůbec řešena, neboť ty se domnívají, že jsou příliš malé na to, aby byly pro útočníky zajímavé[97], a dále pak na ty velké, kde je příliš velký počet zaměstnanců, oddělení a zařízení, které mohou selhat, a na které je možno vést útok.

Výsledkem těchto útoků může být krádež citlivých informací, odčerpání peněz z firemních účtů anebo ovládnutí informačních systémů vedoucích až k přerušení podnikání. S tím pak jsou zpravidla spojeny i přímé a nepřímé ztráty, související především s náklady na řešení incidentů, odstranění příčiny a přijetí opatření, aby se podobná situace neopakovala v budoucnu, a dále pak možné sankce z nedodržení smlouvy, pokuty za selhání v oblasti ochrany informací, pokles v příjmech v důsledku nedostupnosti systému a ztráta tržní příležitosti v důsledku negativní publicity a poškození dobrého jména. Přičemž největší obavou je přerušení podnikání, ke kterému může dojít přímo, když je veden útok na samotnou firmu, anebo nepřímo, když se cílem útok stane někdo v dodavatelsko-odběratelském řetězci. I organizace působící v odvětví relativně nezávislém na informačních systémech a síťové infrastruktuře mohou utrpět značnou škodu, protože využívají např. dopravní a síťovou infrastrukturu, která je řízena prostředky výpočetní techniky a na ty může být veden útok.

Skutečnou úroveň kybernetické bezpečnosti je velice obtížné zjistit, protože jediným skutečně objektivním řešením by byl důkladný bezpečnostní audit,

---

[97] ČERMÁK, Miroslav. Mýty informační bezpečnosti aneb proč většina firem žije v bludu. *CleverAndSmart Management Consulting* [online]. 2012 [cit. 12.08.2019]. ISSN 2694-9830. Dostupné z: https://www.cleverandsmart.cz/myty-informacni-bezpecnosti-aneb-proc-vetsina-firem-zije-v-bludu/

ideálně pak penetrační test a ethical hacking, ten však vzhledem k množství subjektů není možné realizovat. Kromě toho by byl nutný i souhlas těchto subjektů.

Jako určité kompromisní řešení se pak nabízí realizovat výzkum formou dotazníku, kdy budou jednotlivým respondentům položeny otázky týkající se hrozeb, se kterými se setkali, a následků těchto hrozeb. Nicméně ani zde se nelze zcela spolehnout na to, že ze strany respondentů budou poskytnuty zcela pravdivé odpovědi a nebudou mít snahu některé podstatné skutečnosti zamlčet z obavy, aby něco neprozradili. Proto je třeba respondentům položit v rámci výzkumu takové otázky, na které bude schopen dát odpověď prakticky každý z nich, a v rámci organizace pak oslovit i více zaměstnanců a následně pak posoudit, zda se jejich odpovědi shodují.

Zhodnotit situaci v kyberprostoru lze analýzou primárních a sekundárních zdrojů. V souladu s navrhnutou metodikou bude nejprve provedena analýza sekundárních zdrojů a provedena syntéza těchto informací do podoby otázek, které budou následně použity v rámci analýzy primárních zdrojů.

3.1 Analýza sekundárních zdrojů

Za účelem lepšího porozumění situaci v kyberprostoru je dále analyzován vývoj za posledních několik let, tak jak byl zachycen v médiích a jak ji vnímají bezpečnostní experti tvořící pracovní skupinu. A dále jsou identifikovány klíčové faktory ovlivňující nárůst kybernetické kriminality. Ty byly identifikovány na základě analýzy bezpečnostních reportů vydávaných firmami, nabízejících bezpečnostní řešení, ve kterých byly hledány společné charakteristiky co do typu a četnosti výskytu hrozeb a použitých vektorů útoku, hloubkových rozhovorů s manažery informační a kybernetické bezpečnosti působících v soukromé i veřejné sféře, a v neposlední řadě pak i na základě osobních zkušeností s šetřením závažných kybernetických útoků vedených na klienty největších českých bank v posledních několika letech.

V posledních dvou dekádách došlo v oblasti informačních technologií hned k několika na první pohled veskrze pozitivním transformacím, jako je konsolidace a virtualizace infrastruktury, digitalizace dokumentů, přesun dat do cloudů, robotizace procesů, nástup umělé inteligence a možnost vzdáleného přístupu

k systémům a datům organizace z čehokoliv, kdykoliv a odkudkoliv. Tyto změny by nás samy osobě nemusely vůbec znepokojovat, ale společně však mohou a vytváří v případě jejich nezvládnutí příznivé podmínky pro páchání závažné kybernetické kriminality a ohrožují tak většinu domácností a organizací v ČR, neboť ty jsou stále více na informačních technologiích závislé, neboť jejich prostřednictvím konzumují anebo poskytují své služby.

Vývoj informačních technologií a architektury od druhé poloviny 90. let minulého století v zásadě předurčil současnou podobu kybernetických útoků. Domácnosti i firmy, jejich zařízení a rovněž i samotná infrastruktura jsou předmětem plošných i cílených kybernetických útoků[98].

O skutečné situaci v kyberprostoru máme však jen mlhavou představu, protože neexistuje jednotná databáze, která by obsahovala informace o veškerých útocích, které byly na organizace v ČR vedeny. K dispozici jsou sice neveřejné záznamy z vyšetřování jednotlivých trestných činů, ale ty neobsahují strukturovaná data a ve formě, která by byla využitelná pro provedení potřebných analýz. Navíc spousta útoků především na soukromé subjekty není hlášena a není tudíž ani vyšetřována jako trestný čin.

3.1.1 Globální trendy a klíčové faktory

Kybernetické útoky jsou stále sofistikovanější a nabírají na intenzitě. A nic bohužel nenasvědčuje tomu, že by se tento trend měl v dohledné době změnit. Naopak lze s ohledem na dosavadní vývoj v kyberprostoru očekávat, že tento trend bude nadále pokračovat, neboť silně koreluje s růstem počtu uživatelů, jejich nízkým bezpečnostním povědomím, rostoucím počtem zařízení připojených do internetu, objemem zpracovávaných dat a informací, snadnou dostupností návodů a nástrojů potřebných k páchané této závažné trestné činnosti a v neposlední řadě pak i s množstvím a velikostí aplikací a celkové komplexity systémů.

Od roku 1995, kdy sleduji úroveň bezpečnosti ve vybraných 11 organizacích, především o stovkách a tisících zaměstnanců, a zabývám se šetřením

[98] GENES, Raimund. Targeted Attacks versus APTs: What's The Difference? *TrendLabs Security Intelligence Blog* [online]. 2015 [cit. 12.03.2019]. Dostupné z: https://blog.trendmicro.com/trendlabs-security-intelligence/targeted-attacks-versus-apts-whats-the-difference/

kybernetických bezpečnostních incidentů[99], jsem identifikoval a analyzoval klíčové faktory ovlivňující nárůst kybernetické trestné činnosti.

Oproti klasické trestné činnosti zde dochází k tomu, že se pachatel téměř nikdy fyzicky nevyskytuje na místě činu, a to před jeho spácháním, během něj a ani po jeho dokonání, což značně ztěžuje jeho odhalení a dopadení. Setkat se tak můžeme s kybernetickými útoky na domácnosti a firmy, kdy dochází především k šíření škodlivého kódu prostřednictvím e-mailu a napadení a zneužití špatně zabezpečených koncových zařízení k dalšímu útoku anebo zašifrování dat a požadování výkupného anebo zneužití přístupu do internetového bankovnictví a převodu finančních prostředků. Povětšinou hodnoceno jako trestný čin dle TZ č. 40/2009 Sb. a § 230 Neoprávněný přístup k počítačovému systému a nosiči informací[100].

Jistě by se daly nalézt i další faktory, u kterých by mohla být zjištěna obdobně silná korelace s nárůstem trestné činnosti v kyberprostoru, nicméně uvedené faktory oslovení bezpečnostní experti považují za klíčové a vnímají je i jako agregované bezpečnostní riziko[101].

Rychlost internetového připojení a výpočetní výkon

Rychlost pevného i mobilního připojení rok od roku roste, což je dáno rostoucí poptávkou a konkurencí na vyspělém telekomunikačním trhu. Rychlost připojení vzrostla z pouhých několika jednotek kilobit za sekundu až na několik megabitů za sekundu. Během dvou dekád tak vzrostla rychlost přenosu dat tisícinásobně[102], a zatímco množství citlivých dat roste, tak velikost jednotlivých citlivých dat je pořád stejná. Jinými slovy, **číslo platební karty, číslo bankovního účtu, rodné číslo anebo trvalá adresa jsou stále stejně dlouhé a tudíž mají pořád stejnou velikost**, což lze vyjádřit pomocí stejného počtu bitů.

---

[99] ČERMÁK, Miroslav. Úskalí zajišťování digitálních stop v případě podezření na trestný čin neoprávněného přístupu k počítačovému systému. *Bezpečnostní teorie a praxe*. 2019, roč. 2019, č. 3. ISSN 2571-4589. s. 125–134

[100] ČESKO. Zákon č. 40/2009 Sb. ze dne 8. ledna 2009 trestní zákoník. *Sbírka zákonů České republiky* [online]. 2009. ISSN 1211-1244. Dostupné z: https://www.mvcr.cz/soubor/sb011-09-pdf

[101] ČERMÁK, Miroslav. Jak vzniká agregované bezpečnostní riziko. *Právo a bezpečnost*. 2019, roč. 2019, č. 3. ISSN 2336−5323. s. 20–33

[102] ČSÚ [ČESKÝ STATISTICKÝ ÚŘAD]. *Informační společnost v číslech 2017* [online]. 2017 [cit. 02.02.2022]. Dostupné z: https://www.czso.cz/documents/10180/46014808/061004-17_S.pdf

Co se mění, je množství informací, a to exponenciálně roste. Nicméně velikost informace a množství informací jsou dvě na sobě zcela nezávislé veličiny. To ve výsledku znamená, že zatímco v minulém období nebylo možné v případě napadení bez povšimnutí stáhnout např. celou databázi klientů o velikosti několika stovek MB anebo ji dokonce zašifrovat, protože by se jednalo o výpočetně i datově velice náročnou operaci, tak dnes, kdy je to otázka maximálně několika málo minut, roste riziko, že si toho organizace nemusí vůbec všimnout a většina organizací si toho také nevšimne. **Z analýzy bezpečnostních reportů vyplývá, že útočník se v napadené organizaci pohybuje bez povšimnutí i několik měsíců a několik měsíců[103] trvá i vyřešení tohoto incidentu[104]**. Vyšší rychlost připojení umožňuje vést i podstatně rychlejší útok, na který mnohé organizace ani nestačí zareagovat. Rychlost připojení pak dále akcelerovala počet zařízení a uživatelů připojených do internetu a rovněž i možnost práce z domova ze soukromých zařízení.

Spolu s rychlostí přenosu rostl i výpočetní výkon, což je další nezanedbatelný faktor, který podstatně ovlivňuje rychlost provedeného útoku. Onen nárůst výpočetního výkonu je dán především použitou technologií při výrobě procesorů a zvyšování jejich hustoty v souladu s tzv. Moorovým zákonem[105], velikostí a rychlostí dostupné cache a stejně tak i volatilní jako pevné paměti.

Množství uživatelů a nezabezpečených zařízení připojených do internetu

Byť počet uživatelů internetu nadále roste, tak bez ohledu na to, že se toto tempo růstu zpomaluje a nejspíš tomu tak bude i nadále, neboť bude v zásadě kopírovat populační křivku, tak naproti tomu počet zařízení připojených do internetu roste výrazně vyšším tempem a zdaleka přesahuje aktuální počet obyvatel. Dle InternetLiveStats[106] přesáhl počet uživatelů internetu 4 miliardy a v Česku pak dle NetMonitoru[107] 7,8 miliónů uživatelů.

---

[103] FIREEYE. *M-Trends 2019* [online]. 2019 [cit. 08.03.2019]. Dostupné z: https://content.fireeye.com/m-trends

[104] 2019 Cost of a Data Breach Report. *IBM Security* [online]. [cit. 25.05.2020]. Dostupné z: databreachcalculator.mybluemix.net

[105] PADUA, David, ed. *Encyclopedia of Parallel Computing* [online]. Boston, MA: Springer US, 2011 [cit. 04.02.2022]. ISBN 978-0-387-09765-7. DOI: 10.1007/978-0-387-09766-4,

[106] Number of Internet Users (2016) - Internet Live Stats. *Internet Users* [online]. [cit. 16.02.2019]. Dostupné z: http://www.internetlivestats.com/internet-users/

[107] NetMonitor [online]. [cit. 16.02.2019]. Dostupné z: http://www.netmonitor.cz/

Z vlastního šetření provedeného v několika organizacích s více jak několika tisíci zaměstnanci, ale i v malých rodinných firmách vyplynulo, že zpočátku byl přístup do internetu možný pouze z vyhrazených počítačů, připojených do internetu přes vytáčenou telefonní linku, které byly umístěny mimo sít a byly i pod dohledem. (Ani ne tak kvůli bezpečnosti, jako kvůli nákladům.) A jen minimum domácností mělo připojení do internetu. To bylo mimo jiné dáno i poměrně vysokými poplatky za připojení, které byly účtovány dle doby připojení. Později byly počítače v organizacích připojené do internetu umístěny v samostatné síti a odděleny od zbytku sítě. V poslední fázi byl internet zpřístupněn ze všech počítačů, ale přístup byl možný pouze na vybrané stránky (white list). S růstem počtu těchto webových stránek se však stala situace neudržitelná a byl zvolený opačný přístup, kdy začal být vytvářen seznam stránek, resp. kategorií, které jsou zakázány (black list) a probíhá tzv. filtrování obsahu, ovšem vzhledem k tomu, že na malware lze narazit i na naprosto důvěryhodných stránkách, neposkytuje ani toto řešení spolehlivou ochranu. (V malých organizacích, kde nebyl dostatek zdrojů, se toto nikdy příliš neřešilo a přístup do internetu byl řízen na základě role/postavení zaměstnance v hierarchii organizace anebo vůbec.) Do internetu dnes nejsou připojeny jednotlivé počítače, ale celé sítě, a dokonce i operační technologie, což ještě před několika lety nebylo možné[108].

Dle iot-analytics[109] je do internetu připojeno více jak 17 miliard zařízení. To představuje cca 4 zařízení na uživatele, kterými zpravidla jsou stolní počítač, notebook, tablet a smartphone. S rostoucím počtem uživatelů a připojených zařízení pak dochází ke zvětšování povrchu útoku, což nejlépe vystihuje Metcalfův zákon[110]. Spolu s faktorem identifikovaným v předchozí kapitole došlo i ke zvýšení velikosti programového kódu.

Oslovení experti se shodují, že je přímo příčinou tohoto stavu, a že v důsledku toho došlo k obrovskému nárůstu počtu řádků a zvětšení velikosti operačního

---

[108] SIEMENS. Bezpečnost průmyslových dat je otázka správné strategie. *Národní centrum průmyslu 4.0* [online]. 2020 [cit. 16.06.2020]. Dostupné z: https://www.ncp40.cz/aktuality/bezpecnost-prumyslovych-dat-je-otazka-spravne-strategie

[109] LASSE LUETH, Knud. State of the IoT 2018: Number of IoT devices now at 7B – Market accelerating. *iot-analytics.com* [online]. 2018 [cit. 16.02.2019]. Dostupné z: https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/

[110] IEEE STAFF. *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT).* B.m.: Piscataway, 2016. ISBN 978-1-5090-4130-5.

systému, a to z pouhých několika stovek KB (MS DOS) na GB (Windows 10), což už samo osobě znamená, že takový kód může obsahovat v závislosti na své cyklomatické komplexitě větší množství chyb, které nemusí být včas odhaleny, byť zde zřejmá snaha je. Se zavedením agilního přístupu, který si osvojily i tradiční organizace jako jsou banky, se zkracuje vývojový cyklus a zrychluje se uvolňování nových verzí SW, které běží na těchto operačních systémech, což povrch útoku jen zvětšuje.

Kromě toho se objevují počítače v podobě nejrůznějších jednoúčelových zařízení připojitelných do internetu, ledničky, myčky, mikrovlnky, televize, žárovky, termostaty, zkrátka tzv. IoT (internet of things), ale i smartphonů a tabletů, které se stávající de facto spotřebním zbožím s krátkou dobou morální i fyzické životnosti. U takových zařízení se vzhledem k jejich ceně a překotnému vývoji dokonce ani nepočítá s nějakou dlouhou dobou životnosti a už vůbec ne s doživotním vydáváním bezpečnostních aktualizací za účelem odstranění zranitelností, kterými tato zařízení trpí už v okamžiku, kdy sjíždějí z výrobní linky, a které jsou následně zneužívány útočníky krátce po jejich připojení se do internetu. Je tomu tak proto, že většina těchto zařízení obsahuje zranitelnosti a nějaké aktualizace svého operačního systému se za doby svého života nikdy nedočká. Značný tlak na co nejnižší cenu za účelem snižování nákladů vede v konečném důsledku k tomu, že je do internetu připojeno enormní množství zařízení, která je možno napadnout, ovládnout a vést z nich útok na další cíle.

Rostoucí počet útoků na organizace pak způsobila i podpora programu BYOD (z anglického bring your own device), který zvítězil nad programem COPE (Corporate Owned Personally Enabled), která vedla ke zvětšení povrchu útoku, a tak bylo nutné zavedení dalších bezpečnostních opatření a pravidel[111]. Zaměstnanci k práci používají svá vlastní soukromá zařízení, která organizace nemá vůbec pod kontrolou namísto toho, aby používali firemní zařízení i k soukromým účelům. A i když z těchto zařízení zaměstnanci přistupují k systémům organizací přes technologii VPN (virtual private network), která

[111] KLESEL, Michael, Sebastian WEBER, Finja WALSDORFF a Bjoern NIEHAVES. Are Employees Following the Rules? On the Effectiveness of IT Consumerization Policies. In: *Wirtschaftsinformatik*: *Wirtschaftsinformatik 2019 Proceedings* [online]. 2019, s. 847–860 [cit. 02.02.2022]. Dostupné z: https://aisel.aisnet.org/wi2019/track07/papers/6

zajišťuje tzv. end-to-end šifrování, používají pro přihlášení dvoufaktorovou autentizaci a na zařízeních jim běží VDE (virtual desktop environment), což je v podstatě virtuální desktop, který má organizace zpravidla pod kontrolou a kde proběhl nějaký hardening a jsou zde bezpečnostními politikami vynuceny určité zásady, tak přesto mohou být tato zařízení zaměstnanců resp. jejich hostitelské systémy napadeny a spuštěn v nich škodlivý kód, který může dané zařízení kompletně ovládnout, začlenit jej do botnetu a umožnit útočníkovi vzdálený přístup k datům a do systému organizace[112]. Je třeba si uvědomit, že na těchto zařízeních není často aktuální operační systém, nejsou aktualizovány veškeré aplikace, které jejich uživatel používá, neběží zde antivirus a je z nich zcela bez omezení přistupováno do internetu. Práce ze soukromého zařízení už dávno není v mnoha organizacích benefitem, ale způsobem, jak snížit náklady na výpočetní techniku, a to i včetně příspěvku na nákup daného zařízení.

Zaměstnanci navíc stále častěji využívají možnosti home office neboli práce z domova[113] a do systému svého zaměstnavatele se připojují ze svého soukromého zařízení přes internetové připojení svého poskytovatele internetu. Problém však je, že zaměstnanec přistupující do systému a k datům společnosti z domova není schopen zajistit a nemá zajištěnou stejnou úroveň fyzické bezpečnosti jako zaměstnanec, který se nachází v prostředí organizace, do které je zpravidla vstup možný pouze přes recepci, probíhá zde kontrola osob a rovněž je zde výrazně nižší riziko, že by zaměstnance bez povšimnutí někdo donutil fyzickým násilím provést neautorizovanou operaci v systému. To v domácím prostředí, které není pod trvalým kamerovým dohledem a není napojeno na PCO (pult centrální ochrany) možné je. Práce z domova je trend, který už dávno není v mnoha organizacích benefitem, ale způsobem, jak ještě více snížit náklady na jedno pracovní místo a zachovat kontinuitu podnikání v okamžiku, kdy se objeví nějaká krize, jako např. problémy v dopravě v důsledku živelních pohrom anebo i šíření infekce, jako v případě Covid 19, která vyvolala i vyhlášení nouzového

[112] KREBS, Brian. Voice Phishers Targeting Corporate VPNs. *KrebsOnSecurity* [online]. 2020 [cit. 31.08.2020]. Dostupné z: https://krebsonsecurity.com/2020/08/voice-phishers-targeting-corporate-vpns/

[113] Zaměstnanci chtějí home office. Splňte tyto 2 podmínky, aby práce z domu fungovala. *LMC* [online]. 2019 [cit. 17.12.2019]. Dostupné z: https://www.lmc.eu/cs/magazin/data-a-pruzkumy/zamestnanci-chteji-home-office-splnte-tyto-2-podminky-aby-prace-z-domu-fungovala/

stavu a bylo nutné omezit fyzickou přítomnost na pracovištích a začít pracovat z domova. Okamžitě se objevil a byl šířen škodlivý kód, který této situace využíval, a docházelo pak k napadání špatně zabezpečených počítačů.

Rychlost zakládání nových domén

S klesající cenou za objem přenesených dat, rostoucí rychlostí připojení a klesající cenou za zřízení a provoz domény firmy postupně přesouvají své aktivity do kyberprostoru. **Denně vzniká až několik stovek tisíc domén, a dle některých zdrojů jsou až v 70 % případů krátce po vytvoření zneužity ke kriminálním aktivitám[114]**, např. k šíření SPAMu, phishingu, malware anebo jako C&C server. Obrovsky tomu napomohl i WEB 2.0, kdy se v podstatě kdokoliv může stát autorem obsahu, tedy i útočník, který pak může své příkazy ukrýt i do zcela na první pohled nevinného textu na renomovaném webu[115].

Z analýzy logů systémů, které provozuje společnost, ve které tato analýza proběhla, a dále pak z šetření jednotlivých případů napadení vyplynulo, že tyto domény jsou zakládány na různých doménách prvního řádu. Nejvíce jich je na doméně .com, přičemž zpravidla se jedná o domény druhého řádu (stovky tisíc) a třetího řádu (desítky tisíc), ale občas se objeví doména třeba i patnáctého řádu. Nejčastěji je doménou druhého řádu číslo, za kterým se pak nachází nějaký znak. Často se generuje celá řada domén, které v názvu obsahují řadu po sobě jdoucích čísel a znaků. Tyto domény mají krátký život, často jen několik málo hodin nebo dnů, neboť jsou bezpečnostními řešeními označeny poměrně záhy jako podvodné a přístup k nim je blokován anebo je daná doména rovnou zrušena. Nicméně zpočátku nejsou tyto domény bezpečnostními řešeními označovány jako škodlivé vůbec, a proto se nabízí všechny nově vytvořené domény preventivně blokovat na úrovni DNS a zpřístupnit je až po uplynutí určité doby.

Stejně tak lze přistoupit i k hodnocení domén, když dojde ke změně jejich vlastnictví, protože ty mohou být rovněž v okamžiku, kdy přejde doména na

---

[114] ZELJKA, Zorz. Should you block newly registered domains? Researchers say yes. *Help Net Security* [online]. 23. srpen 2019 [cit. 20.03.2020]. Dostupné z: https://www.helpnetsecurity.com/2019/08/23/block-new-domains/

[115] ČERMÁK, Miroslav. Na obzoru se objevují nové hrozby, třeste se! – 7. díl. *CleverAndSmart Management Consulting* [online]. 2020 [cit. 20.03.2020]. ISSN 2694-9830. Dostupné z: https://www.cleverandsmart.cz/na-obzoru-se-objevuji-nove-hrozby-treste-se-7-dil/

nového vlastníka zneužity ke kriminálním účelům a těžit z jejich dosavadní dobré reputace. Je však otázka, zdali je tato technika skutečně účinná? Momentálně asi ano, ale v okamžiku, kdy se stane všeobecně používanou, tak to může vést jedině k tomu, že útočník prostě pár dnů po registraci domény počká a teprve pak rozjede svoji aktivitu. Účinnost této ochrany pak bude v čase rapidně klesat.

Nehledě na to, že onen škodlivý obsah může být zpřístupněn pouze pro uživatele přistupující na daný web jen z určitého IP adresního rozsahu, což se děje už teď, takže bezpečnostní řešení o něm neví. Další problém je, že dost často jsou zneužívány již delší dobu běžící weby s dobrou reputací, nad kterými útočník de facto převzal kontrolu, ale v doménovém záznamu se to samozřejmě neobjeví. Skutečnost, že uživatelé se nechají nalákat na podvodnou doménu, je pak umocněna i tím, že se stále více používají pro přístup na internet smartphony, což lze doložit i logy z webových serverů, a na těchto zařízeních se používají nativní klienti, kteří se ne vždy nacházejí v aktuální verzi, a ve kterých lze hůře zkontrolovat skutečnou adresu odesílatele e-mailu, kam odkaz směřuje a rovněž velikost písmen znesnadňuje správně rozlišit jméno domény. Toho využívají útočníci, kteří zakládají podobně znějící anebo podobně se píšící domény a na nich rozjíždějí svůj vlastní business. Běžný uživatel pak nemá moc možností, jak zjistit, která služba je ta pravá. Že se mohou splést i odborníci, natož běžní uživatelé, dokládá případ Zoom, kdy došlo k nárůstu hodnoty akcií jiné společnosti jen díky podobnému jménu[116]. Situaci dále zhoršuje rostoucí počet domén prvního řádu, kterých je více než 1 500[117], což útočníkovi umožňuje snadno si založit doménu stejného jména, jen na jiné doméně prvního řádu, a pro skutečného vlastníka se možnost obrany značně zhoršuje. Bránit se spekulantům a typosquattingu a cybersquattingu je vzhledem k počtu TLD domén stále obtížnější a útočníci vynalézají stále nové techniky útoku, jako tomu bylo např. v případě Privnotes[118].

---

[116] NIU, Evan. The SEC Really Wants Investors to Stop Buying the Wrong Zoom Stock [online]. 2020 [cit. 22.06.2020]. Dostupné z: https://www.nasdaq.com/articles/the-sec-really-wants-investors-to-stop-buying-the-wrong-zoom-stock-2020-03-27

[117] List of Top-Level Domains - ICANN [online]. [cit. 22.06.2020]. Dostupné z: https://www.icann.org/resources/pages/tlds-2012-02-25-en

[118] KREBS, Brian. Privnotes.com Is Phishing Bitcoin from Users of Private Messaging Service Privnote.com. *KrebsonSecurity* [online]. 14. červen 2020 [cit. 22.06.2020]. Dostupné z:

Snadnost a rychlost s jakou lze zakládat nové dynamicky generované domény, pomocí Domain Generation Algorithm zkr. DGA a měnit IP adresy serverů, na které tyto domény odkazují pomocí techniky fast flux DNS v zemích, které nespolupracují, jen zhoršuje situaci a nahrává útočníkům.

Bezpečnostní povědomí

Nízké bezpečnostní povědomí zaměstnanců i manažerů vede k chybám i chybným rozhodnutím. Na základě provedení vlastního experimentu[119] v organizacích čítajících několik tisíc zaměstnanců a dále pak z informací poskytnutých nezávislými třetími stranami, které provádějí obdobné školení a testy odolnosti zaměstnanců na komerční bázi, vyplynuly následující podstatné skutečnosti. Investice do bezpečnosti a školení jsou v zásadě stále stejné, a i když se v poslední době v některých organizacích v souvislosti s GDPR zvýšily, tak nedochází k podstatné a žádoucí změně chování ze strany zaměstnanců. Stále používají slabá a stejná hesla do více systémů, nejsou odolní vůči technikám sociálního inženýrství, jinými slovy nedokáží rozpoznat probíhající phishing, vishing, baiting, a vpustí neoprávněnou osobu na pracoviště. Pouze v organizacích, ve kterých dochází spolu s osvětou i k testování odolnosti zaměstnanců vůči těmto útokům, je možné zaznamenat výrazné zlepšení oproti předchozímu období. Meziročně pak dochází i k trvalému zlepšování, kdy zaměstnanci těchto organizací jsou schopni správně identifikovat phishing, který stále představuje nejčastější vektor útoku, a tedy i způsob, jak dochází ke kompromitaci koncových zařízení zaměstnanců a proniknutí útočníka do prostředí organizace. Ve velkých organizacích je pak velice dobrým výsledkem, když se podaří snížit počet zaměstnanců náchylných na phishing na jednotky procent.

Citelně nám schází větší informovanost o skutečných zranitelnostech, hrozbách a probíhajících útocích v kyberprostoru. O jednotlivých útocích se z médií dozvídáme jen výjimečně, neexistuje jednotná taxonomie kybernetických hrozeb,

---

https://krebsonsecurity.com/2020/06/privnotes-com-is-phishing-bitcoin-from-users-of-private-messaging-service-privnote-com/

[119] ČERMÁK, Miroslav. Why Human Firewall Fails in the Battle with Sophisticated Spear Phishing Campaigns. In: Irena TUŠER a Šárka HOŠKOVÁ-MAYEROVÁ, ed. *Trends and Future Directions in Security and Emergency Management* [online]. Cham: Springer International Publishing, 2022 [cit. 28.01.2022], Lecture Notes in Networks and Systems. ISBN 978-3-030-88906-7. DOI: 10.1007/978-3-030-88907-4_16, s. 283–291

byť zde existují pokusy o její vytvoření a objevují se v různých publikacích, např. Jirovského[120]. Neexistuje přehledná statistika útoků, která by uváděla vektor útoku, zasažený sektor, výši škody apod. K dispozici jsou sice nejrůznější statistiky třeba CSIRT[121] nebo policie[122], ale ty jsou samy o sobě neúplné a nevypovídající. K dispozici jsou dále bezpečnostní reporty zahraničních firem mapující situaci ve světě, ale ani ty nepřinášejí podstatné informace a jsou mnohdy značně zavádějící.

Jistě lze namítnout, že zde jsou odborné publikace a archivy bezpečnostních složek apod., ale k těm většina odborné a laické veřejnosti přístup nemá, informace zde nehledá, alespoň to vyplynulo z rozhovorů s manažery bezpečnosti, kteří se řídí výhradně publikacemi od ISACA a konzultačních společností jako je Gartner, Deloitte, KPMG, Accenture a firem nabízejících bezpečnostní řešení, které považují za aktuální. To samo o sobě zhoršuje vnímání bezpečnosti ze strany vrcholového managementu, kterému není možné předložit konkrétní případy, ke kterým na území ČR došlo a jaké byly jejich následky a závažnost bezpečnostních hrozeb je tak bagatelizována.

V dlouhodobém horizontu však úroveň bezpečnostního povědomí spíše klesá, pokud vezmeme v úvahu skutečnost, že roste počet uživatelů, kteří se o bezpečnost svého zařízení vůbec nezajímají a počítače, tablety, mobily a IoT berou čistě jako spotřební zboží. Pro útočníky je pak mnohem snazší tyto uživatele napadnout.

Globalizace kybernality

Pro útoky v kyberprostoru je typické, že vzdálenost mezi útočníkem a obětí nehraje žádnou roli, a že domnělý útočník bývá dost často jen obětí, protože systém, ze kterého je útok veden, je plně pod kontrolou útočníka a ten může po sobě zametat stopy anebo i vytvářet stopy falešné, aby svedl vyšetřování jiným směrem. Škodlivý kód, který je dost často v rámci těchto útoků přepoužíván různými organizovanými skupinami se nachází ve více či méně modifikované

[120] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007. ISBN 978-80-247-1561-2. s. 21.
[121] Statistiky řešených incidentů - CSIRT [online]. [cit. 17.12.2019]. Dostupné z: https://csirt.cz/page/2635/statistiky-resenych-incidentu/
[122] Kyberkriminalita - Policie České republiky [online]. [cit. 17.12.2019]. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx

podobě v různých exploitech a je umísťován na napadené servery, sloužící jako watering hole, nebo je umísťován do trojanizovaných aplikací anebo distribuovaný jako příloha v rámci nejrůznějších phishing kampaní, kdy může být chybně na základě pojmenování jednotlivých proměnných, funkcí, knihoven a případně i komentářů částí kódu přisouzen někomu zcela jinému. Např. v situaci, kdy ruský programátor umístí anebo prodá na darknetu svůj exploit, který se stane součástí exploitu kitu, který je následně použit v rámci phishingu jinou organizovanou skupinou k útoku na klienty bank v ČR, může vzniknout dojem, že za útokem stojí ruská APT skupina. A stejně tak skutečnost, že server, který slouží jako C&C server se nachází kdesi v Číně, může vyvolat dojem, že za útokem stojí čínská APT skupina. Zde je třeba si uvědomit, že v kyberprostoru probíhá kybernetická válka a součástí těchto útoků může být i snaha svést útok na někoho jiného.

Z šetření vybraných případů, kdy došlo k útoku na klienty internetového bankovnictví, vyplynulo, že útočníci s oblibou využívají zranitelností v redakčních systémech (v drtivé většině případů se jednalo o systém Wordpress, což není překvapením, protože tento redakční systém má největší podíl na trhu s CMS systémy[123]) již několik let běžících na webových serverech společností s dobrou reputací.

Útočníkům je v zásadě jedno, který server napadnou, nezdá se, že by preferovali server nacházející se v konkrétní zemi nebo běžící na určité doméně prvního řádu. Kromě použitého CMS se nepodařilo vysledovat žádnou jinou společnou charakteristiku a lze se tak domnívat, že používají nějaký automatizovaný skener, kterým prohledávají web a identifikují servery, které trpí určitou zranitelností a ty pak napadnou a umístí na ně škodlivý kód nebo phishingovou stránku.

Z výše uvedeného důvodu by bylo nezodpovědné provést za těchto podmínek protiútok na systém, ze kterého útok probíhá, protože následkem tohoto útoku by mohla být ještě větší škoda, která by vznikla společnosti, která daný server provozuje. Je nutné kontaktovat provozovatele daného systému v jiné zemi a toho požádat o spolupráci, což je mnohdy velice problematické. Netřeba snad dodávat,

[123] Usage Statistics and Market Share of WordPress. *w3techs* [online]. 2020 [cit. 25.06.2020]. Dostupné z: https://w3techs.com/technologies/details/cm-wordpress

že útočník, kompromitovaný server a oběť se zpravidla nachází v různých zemích s jinou jurisdikcí. Narážíme zde nejen na neochotu spolupracovat, ale objevují se zde i kulturní a jazykové bariéry a problém přestavuje i umístění serveru v jiném časovém pásmu.

Přesunem trestné činnosti do kyberprostoru tak vzniká otázka, jak tuto trestnou činnost odhalovat už ve fázi přípravy a zda by nemělo dojít k posílení pravomoci policie, prohloubení mezinárodní spolupráce a umožnění plošného monitorování. Je proto třeba pečlivě zvažovat, jak v případě takového útoku postupovat a věnovat dostatečnou pozornost i novele zákona o vojenském zpravodajství a vést na toto téma seriózní diskusi[124].

S rychlostí internetu, cenou připojení a počtem zařízení dostupných přes internet obrovským způsobem vzrostl povrch útoku. S rozvojem webu 2.0 a možností sdílet informace a nástroje, pomocí kterých lze páchat kybernetickou kriminalitu, vzrostl i počet útočníků.

Pokud bychom na toto odvětví nahlíželi jako na jakékoliv jiné odvětví, tak bychom mohli vyjít ze slavného díla Michala F. Portera a jeho modelu pěti sil[125] a toto odvětví charakterizovat jako odvětví, kde neexistují žádné bariéry pro vstup do odvětví, je z něj možné kdykoliv odejít, není nutné disponovat v podstatě žádným kapitálem (v zásadě stačí počítač a internetová konektivita), není nutné držet vzácný zdroj (hackera, který má znalosti a schopnosti si lze koupit, a to, co ještě před pár lety bylo považováno za vtip, tzv. Hacker as a Service, je dnes naprosto běžnou realitou), a i přes probíhající konkurenční boj je zde minimální riziko ztráty investice a rovněž i dopadení a odsouzení, což spolu s nízkými náklady a vysokou návratností investice činí toto odvětví nesmírně atraktivní pro vstup dalších hráčů na tento trh.

Změnil se i motiv útočníků, zatímco před dvěma dekádami se hackovalo především pro věhlas v bezpečnostní komunitě a výsledkem útoku byl maximálně zápis do logů, defacement webové stránky a vzkaz administrátorovi systému, tak

---

[124] ŠPIDLA, Aleš. Novela zákona o vojenském zpravodajství – potřebujeme ji? *IT SECURITY NETWORK NEWS* [online]. 26. únor 2019 [cit. 12.03.2019]. Dostupné z: https://www.itsec-nn.com/novela-zakona-o-vojenskem-zpravodajstvi-potrebujeme-ji/

[125] PORTER, Michael E. *On competition*. Updated and expanded ed. Boston, MA: Harvard Business School Pub, 2008. The Harvard business review book series. ISBN 978-1-4221-2696-7.

v současné době probíhá drtivá většina útoků dle oslovených bezpečnostních expertů pro peníze a následkem je kompromitace systému a jeho zneužití k dalším útokům, např. na klienty bank, kdy dochází k hackování legitimních webů a za účelem umístění kopie bankovního webu a vylákání přihlašovacích údajů od klientů, krádež citlivých informací, zašifrování dat, jejich smazání a případně i zveřejnění.

Tomu i odpovídá zastoupení aktéru těchto hrozeb v kyberprostoru. Stále častěji se setkáváme místo osamocených hackerů s vysoce organizovanými skupinami, to lze pozorovat i na tom, jak jsou připravovány jednotlivé kybernetické útoky, které gradují přibližně od roku 2013, kdy se ČR stala na mapě světa zemí, na kterou jsou vedeny soustavné kybernetické útoky, a do kterých se ve větší míře zapojují i občané ČR, především jako bílí koně, přes které jsou vyváděny peníze z bankovního oběhu. S popularizací kryptoměny pak dochází v posledních letech k vyvedení peněz tímto způsobem, což eliminuje mezičlánky, snižuje riziko prozrazení a dál činí páchání trestných činů v kyberprostoru atraktivní.

Transformace IT

Poslední faktor, který se zatím příliš neprojevil, ale který dle oslovených bezpečnostních expertů nelze přehlížet, protože bude nabývat dále na významu a určovat, kdo se stane další obětí cílených kybernetických útoků, je **nezvládnutý proces transformace IT a OT**, resp. s tím spojené problematiky řízení bezpečnosti a rizik, především pak integrace řešení běžících v cloudu a on-premise a přístupů k nim.

V poslední dekádě bylo možné ve sledovaných organizacích (např. banky, přepravní společnosti) zaznamenat poměrně bouřlivý vývoj, kdy byla provedena **konsolidace** infrastruktury v datových centrech a následná **virtualizace** a spolu s ní došlo k **digitalizaci** dokumentů a mnohde i k zavedení biometrického podpisu za účelem snížení nákladů na generování a archivaci papírové dokumentace. Poté došlo i k **robotizaci** procesů a začaly se prosazovat tzv. RPA řešení[126]

[126] IVANČIĆ, Lucija, Dalia SUŠA VUGEC a Vesna BOSILJ VUKŠIĆ. Robotic Process Automation: Systematic Literature Review. In: Claudio DI CICCIO, Renata GABRYELCZYK, Luciano GARCÍA-BAÑUELOS, Tomislav HERNAUS, Rick HULL, Mojca INDIHAR ŠTEMBERGER, Andrea KŐ a Mark STAPLES, ed.*Business Process Management: Blockchain and Central and Eastern Europe Forum* [online]. Cham: Springer International Publishing, 2019

namísto přímé integrace a lze očekávat, že jejich počet nadále poroste[127]. Z rozhovorů s bezpečnostními experty vyplývá, že bylo preferováno okamžité snížení nákladů zavedením robotizovaného procesu namísto přímé integrace spočívající v úpravě stávající aplikace, vytvoření API apod. Nebezpečí těchto RPA řešení podle oslovených bezpečnostních expertů spočívá především v rychlosti, s jakou jsou tyto roboti schopni ovládat aplikaci využívanou v rámci robotizovaného procesu a v případě, že dostanou chybná data anebo jim někdo úmyslně podstrčí modifikovaná data, tato data zpracovat[128]. Organizace často nemají stanoveny thresholdy ve smyslu, od jakého počtu nebo objemu dat se jedná o podezřelou aktivitu, ani nemají nastaven proces, jak případné změny provedené robotem rychle vrátit zpět. Další riziko pak spočívá v tom, že tyto roboti neoplývají žádnou umělou inteligencí, takže pokud jim je předložen např. soubor v Excelu, který byť je pro tento účel naprosto nevhodný, se stále používá, tak jej zpracují, na rozdíl od člověka, který si hned všimne, že spreadsheet není v pořádku, to ostatně bylo ověřeno v rámci opakovaného experimentu (jména konkrétních řešení úmyslně neuvádím). Zatím ale útoky tohoto typu sledované organizace neevidují, nicméně RPA přesto představuje určité riziko, a to by mělo být dále monitorováno.

Roboty a umělou inteligenci však neprovozují jen firmy, ale i kyberkriminálníci. Že např. luští CAPTCHA je obecně známý fakt, ale málo se už třeba ví, protože to doposud nebylo nikde publikováno, že např. v květnu tohoto roku byl zaznamenán opakovaný phishingový útok na klienty českých bank, kdy oproti předchozím vlnám reagovala phishingová site velice rychle, v podstatě okamžitě (v minulosti byla pozorovatelná i několikaminutová prodleva na zadávané údaje), takže se lze domnívat, že **na straně útočníka byla použita nějaká forma robotizace**.

Za účelem snižování nákladů dochází i k propojování informačních a operačních technologií. Šetření incidentů a kybernetických útoků spojených

---

[vid. 26. červen 2020], Lecture Notes in Business Information Processing, s. 280–295. ISBN 978-3-030-30428-7. DOI: 10.1007/978-3-030-30429-4_19.

[127] DILMEGANI, Cem. Ultimate Guide to Robotic Process Automation (RPA) in 2020. *appliedAI* [online]. 22. listopad 2017 [cit. 25.06.2020]. Dostupné z: https://research.aimultiple.com/rpa/

[128] ČERMÁK, Miroslav. Stinná stránka robotizace. *CleverAndSmart Management Consulting* [online]. 2018 [cit. 15.06.2020]. ISSN 2694-9830. Dostupné z: https://www.cleverandsmart.cz/stinna-stranka-robotizace/

s OT je poměrně náročné[129] a stávající týmy v této oblasti nemají dostatek zkušeností[130].

Ve sledovaných organizacích bylo také možné pozorovat, jak roste podíl outsourcovaných činností, a to i těch, které se týkají správy dat a systémů. V praxi tak dochází k tomu, že data a systémy spravují zaměstnanci třetích stran a že tito pracovníci spravují i data jiných společností a mohou to být i systémy a data konkurence. Tito pracovníci tak mohou mít mnohem větší příležitost tato data vytěžovat a svého přístupu zneužít spíš než vlastní zaměstnanec organizace, který přístup k datům jiných organizací nemá. Vzhledem k tomu, že dost často byl outsourcing zvolen kvůli nižším nákladům, je zcela na místě se ptát, jak těchto nižších nákladů může být v praxi dosaženo, obzvlášť pokud má správu provádět kvalifikovaný zaměstnanec, disponující příslušnými certifikacemi a dodržovat přitom veškeré bezpečnostní požadavky. Z rozhovoru s příslušnými manažery vyplynulo, že náklady jsou jen zdánlivě nižší a jejich dosahováno především proto, že je rozsah dodávky oproti původním předpokladům značně omezen, resp. je dodáváno přesně to, co je ve smlouvě uvedeno, a na to je třeba si dát pozor[131], jak uvádí např. Rowan Legal, který se na problematiku IT smluv specializuje, a za vše ostatní se musí zaplatit a rovněž je daná činnost vykonávána v zemi, kde jsou výrazně nižší mzdové náklady a vyšší fluktuace zaměstnanců. V neposlední řadě pak manažeři uvádí, že se setkali i s jednáním, že i firma, která prošla certifikací, si pak na zpracování určitých činností za účelem dalšího snížení nákladů najala další firmu, která pro ni danou činnost vykonává a ta již certifikována nebyla.

S outsourcingem pak souvisí i **snadný přesun dat a systémů do cloudů**, což umožnila již výše zmíněna konsolidace a virtualizace IT, která tomuto kroku předcházela. Cloudy prosazují nadnárodní společnosti jako je Microsoft, Google, Amazon, avšak ty sledují výhradně své ekonomické zájmy a těmi je vysoká

---

[129] MARCELLA, Albert J. *Cyber Forensics: Examining Emerging and Hybrid Technologies* [online]. 1. vyd. Boca Raton: CRC Press, 2021 [cit. 09.02.2022]. ISBN 978-1-00-305788-8. DOI: 10.1201/9781003057888, s. 211.
[130] ČERMÁK, Miroslav. Provozní technologie: kybernetické útoky. *CleverAndSmart Management Consulting* [online]. 2020 [cit. 09.06.2020]. ISSN 2694-9830. Dostupné z: https://www.cleverandsmart.cz/provozni-technologie-kyberneticke-utoky/
[131] ČERMÁK, Miroslav. Nejčastější úskalí IT smluv. *CleverAndSmart Management Consulting* [online]. 2020 [cit. 15.06.2020]. ISSN 2694-9830. Dostupné z: https://www.cleverandsmart.cz/nejcastejsi-uskali-it-smluv/

návratnost investice a dosažení zisku, takže v jejich zájmu je přesvědčit management organizací, aby k nim své systémy a data přesunuly. Jako argumenty k tomu využívají možnost dosažení nižších nákladů, realizovaných především jako úspory z rozsahu a dále pak vyšší úroveň bezpečnosti. I to vyplývá z rozhovorů s bezpečnostními experty na pozici ISO v organizacích o několika tisících zaměstnanců. A protože už dávno došlo k oddělení vlastnictví od řízení a na okamžité hospodářské výsledky jsou vázány i manažerské bonusy, tak k tomuto masivnímu exodu do cloudu skutečně dochází[132]. Nelze se tak divit, že v okamžiku, kdy je průměrný životní cyklus manažera několik let, tak volí aktuálně nejlacinější řešení v podobě nějakého cloudu. Může se však jednat o morální hazard, neboť vrcholový management může nabýt falešného dojmu, že když jeho systémy a data spravuje renomovaná společnost, takže už nemusí řešit otázky spojené s bezpečností. Je třeba si uvědomit, že každý stát sleduje především své národní zájmy a podporuje své firmy, a že ten, kdo byl naším spojencem, již zítra spojencem být nemusí, takže v případě kritické informační infrastruktury státu je nutné provést výběr cloudu a analýzu rizik obzvlášť důkladně. Jistou obezřetnost doporučuje i Evropská komise, která cloud jinak doporučuje[133]. Ostatně skutečnost, že je cloud obousečná zbraň, je uvedeno i v Národní strategii kybernetické bezpečnosti České republiky na období let 2015-2020[134]. V akčním plánu k této strategii je však ambice řešit jen systémy, které spravuje stát[135] anebo ty, které lze označit za součást kritické informační infrastruktury, významné informační systémy anebo systémy základních služeb, což je nedostačující, protože většinu systémů stát nespravuje a ani nespadají pod působnost Zákona o kybernetické bezpečnosti a výkon národního hospodářství se odvíjí především

---

[132] ČSÚ [ČESKÝ STATISTICKÝ ÚŘAD]. *Využívání informačních a komunikačních technologií v podnikatelském sektoru* [online]. Praha: Český statistický úřad, 2019 [cit. 10.07.2021]. ISBN 978-80-250-2902-2. Dostupné z: https://www.czso.cz/documents/10180/61601888/06200518.pdf/ce31b358-2dca-4204-b507-c7e4656064e7?version=1.1,

[133] MICHLMAYR, Thomas. *European Commission Cloud Strategy* [online]. 2019 [cit. 18.12.2019]. Dostupné z: https://ec.europa.eu/info/sites/default/files/ec_cloud_strategy.pdf

[134] *Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020* [online]. 12. březen 2015 [cit. 10.07.2021]. Dostupné z: https://www.nukib.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2015-2020.pdf

[135] *Akční plán k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020* [online]. 11. srpen 2015 [cit. 02.02.2022]. Dostupné z: https://www.nukib.cz/download/publikace/strategie_akcni_plany/akcni_plan_2015-2020.pdf

od úrovně bezpečnosti soukromých firem, a ty jsou vedeny profesionálními manažery, kteří vidí v cloudech spíše řešení umožňující jim okamžitě snížit náklady, než cokoliv jiného.

Z rozhovorů s některými manažery navíc vyplynulo, že vůbec nemají vypracován postup pro případ, kdyby cloud byl nedostupný anebo potřebovali přejít k jinému poskytovateli. A pokud organizace nebudou navrhovat a vyvíjet své systémy jako cloud-native, tak přechod od jednoho poskytovatele cloudu (Cloud Service Provider, zkr. CSP) k druhému nebude možný a těmto organizacím bude hrozit vendor lock-in a to se všemi následky, které z tohoto problematického stavu vyplývají, a CSP ji v tom samozřejmě nijak pomáhat nebude, naopak. Snadno pak taková organizace může zaznamenat rostoucí náklady nebo bezpečnostní problémy.

Dále je třeba si uvědomit, že cloudy byly navrhnuty tak, aby byly odolné vůči hrozbám přírodního původu jako je zemětřesení, bouře, záplavy a rovněž i vůči klasickým zbraním a dokázaly nějak fungovat v případě dočasné nedostupnosti datového centra nebo i jeho kompletního zničení. Slabinou cloudů však vždy bude lidská chyba nebo kybernetický útok zneužívající SW zranitelnosti. Pokud jde o lidskou chybu, tak nezapomínejme, že když chybu udělá admin v DC, nemusí si toho nikdo ani všimnout, ale chyby v cloudu si okamžitě všimnou všichni, co ho využívají[136]. Napadnout takový cloud a požadovat výkupné, je velice lákavé a pokud k tomu dojde, tak ti slabí nepřežijí, protože pojišťovna jim škodu neuhradí, neboť kybernetická válka je zahrnuta ve výlukách. Jasně se to ukázalo na případu Mondelez[137].

I přes určitý pokrok v posledních letech je zde stále patrná značná závislost na CSP co do možnosti logování událostí a jejich forenzní analýze a šetření bezpečnostních incidentů, a rovněž i co do možnosti obnovy systému po havárii. Problém je, že CSP z principu ani moc nějaké logy poskytovat nemůže.

---

[136] STEVEN J. VAUGHAN-NICHOLS. Don't be the fool in the cloud. *Computerworld* [online]. 2017 [cit. 18.12.2019]. Dostupné z: https://www.computerworld.com/article/3233289/don-t-be-the-fool-in-the-cloud.html

[137] CORCORAN, Brian. What Mondelez v. Zurich May Reveal About Cyber Insurance in the Age of Digital Conflict. *Lawfare* [online]. 8. březen 2019 [cit. 18.12.2019]. Dostupné z: https://www.lawfareblog.com/what-mondelez-v-zurich-may-reveal-about-cyber-insurance-age-digital-conflict

Nezapomínejme, že v logách jsou zaznamenány informace i o jiných klientech. Je tomu tak proto, že kvůli snížení nákladů je použita sdílená infrastruktura. Náhledy na tyto logy jsou nedokonalé a neúplné, to však zjistíte až v okamžiku, kdy začnete šetřit nějaký bezpečnostní incident. Podle některých bezpečnostních expertů je ona chybovost dokonce až 50 %. Z probíhající ankety mezi bezpečnostními experty dále vyplývá, že téměř 80 % z nich je přesvědčeno, že kritická informační infrastruktura státu by neměla být umístěna v zahraničním cloudu[138].

Dle oslovených bezpečnostních expertů lze do budoucna očekávat, že stále více útoků bude používat nějakou formu robotizace ve spolupráci s **umělou inteligencí a strojovým učením** a stejným způsobem bude nutné se i bránit[139].

Dílčí závěr

Byly identifikovány klíčové faktory, které ovlivňují a do budoucna i budou ovlivňovat nárůst a podobu trestné činnosti páchané v kyberprostoru.

Sledované organizace vykazují určité společné charakteristiky. Alfou a omegou je pak snižování nákladů, to lze pozorovat ve všech sledovaných organizacích. **Zaměstnanci se připojují z domova přes svého poskytovatele internetu a ze svých soukromých zařízení, které trpí četnými zranitelnostmi do systémů a k datům svých zaměstnavatelů, která jsou umístěna v cloudu.**

- Fyzické prostory odkud se zaměstnanci připojují, nejsou pod kontrolou.
- Zařízení, ze kterých se zaměstnanci připojují, nejsou pod kontrolou.
- Datová připojení, která zaměstnanci používají, nejsou pod kontrolou.

Cloudy, kde jsou data a systémy organizací umístěna, nejsou pod kontrolou, hovoří se o sdílené odpovědnosti a vše je ošetřeno jen smluvně. **S počtem zranitelných zařízení roste i počet zařízení, na která může být veden útok a zároveň, ze kterých může být veden útok** v okamžiku, kdy dojde k jejich

[138] ČERMÁK, Miroslav. Ohrožuje přesun systémů do cloudu naše národní hospodářství a bezpečnost? *CleverAndSmart Management Consulting* [online]. 2019 [cit. 18.12.2019]. ISSN 2694-9830. Dostupné z: https://www.cleverandsmart.cz/ohrozuje-presun-systemu-do-cloudu-nase-narodni-hospodarstvi-a-bezpecnost/

[139] PARATI, Namita, DEPARTMENT OF CSE, BRECW, HYDERABAD, INDIA, Pratyush ANAND, a FUNCTIONAL CONSULTANT, FUJITSU PVT. LTD., HYDERABAD, INDIA. Machine Learning in Cyber Defence. *International Journal of Computer Sciences and Engineering* [online]. 2017, roč. 5, č. 12. ISSN 23472693. DOI: 10.26438/ijcse/v5i12.317322 s. 317–322

kompromitaci. Tato zařízení mohou být začleněna do botnetu a dále pronajímána tomu, kdo zaplatí, jedná se o tzv. Crime as a Service, zkr. CaaS.

Možnosti jejich zneužití jsou značné, mohou být zneužita pro lámání hesel, mohou být zneužita k realizaci podvodných bankovních transakcí, může z nich být veden DDoS útok na jinou organizaci, mohou z nich být hackovány další systémy, může z nich být rozesílán SPAM, mohou sloužit jako proxy servery, přes které je veden útok, takže identita útočníka zůstane skryta a co víc, může pak být na základě zdroje útoku přisouzena zcela jinému subjektu.

Otázka dne už není, zda k útoku na danou organizaci dojde, ale kdy a za jak dlouho od průniku bude organizace schopna si tuto skutečnost vůbec uvědomit a reagovat na ni. Přičemž dle statistik M-Trends, které byly vyhodnoceny za posledních 5 let, je to stále až po několika týdnech a tento čas neklesá[140].

Přesto se mezi manažery objevují názory, že se jich kybernetický útok netýká, neboť jejich organizace nedisponuje žádnou převratnou technologií ani know-how, které by bylo pro útočníka zajímavé. Nechtějí si připustit, že **kromě cílených útoků jsou tady ještě tzv. plošné útoky, které jsou mnohem častější**, a že se jejich organizace může stát obětí ransomware a její činnost může být zcela ochromena.

Obrovské množství zranitelných zařízení a uživatelů připojených do internetu pak pro útočníka představuje velice atraktivní cíl, obzvlášť když k útoku může a zpravidla také použije jiné zařízení umístěné navíc i v jiné zemi, a znemožní tak vyšetřování anebo jej svede úplně jiným směrem a podstatně tak sníží riziko odhalení a dopadení.

Výše uvedené skutečnosti, velice nízká pravděpodobnost dopadení a vysoká návratnost investice představuje pro pachatele páchání trestných činů v kyberprostoru velice zajímavou alternativu ke klasické trestné činnosti, kde je riziko odhalení a dopadení výrazně vyšší. Je zřejmé, že tyto faktory budou i nadále ovlivňovat podobu kybernetické kriminality na území České republiky a lze očekávat její další nárůst.

---

[140] ČERMÁK, Miroslav. Breach lifecycle se nám opět o něco prodloužil. *CleverAndSmart Management Consulting* [online]. 2022 [cit. 09.02.2022]. ISSN 2694-9830. Dostupné z: https://www.cleverandsmart.cz/breach-lifecycle-se-nam-opet-o-neco-prodlouzil/

3.1.2 Vývoj kybernetických hrozeb v ČR

Níže je stručně zachycen vývoj v kyberprostoru na území České republiky od pořízení prvních počítačů v Československu, přes připojení České republiky do internetu až po aktuální kybernetické hrozby, kterým jednotlivci i organizace čelí v současnosti. Výčet kybernetických útoků není samozřejmě úplný, ale zachycuje hlavní události, ke kterým došlo, a které jsou pro pochopení vývoje kybernetických hrozeb v kyberprostoru klíčové.

V zásadě se dá celé období od roku 1970 až do současnosti v ČR rozdělit do 5 dekád. Z počátku docházelo k šíření virů a napadání institucí a jejich serverů, aniž by z toho útočník něco měl, tedy kromě osobního uspokojení, demonstrace síly, poukázání na nedostatky, mediálního ohlasu, získaní prestiže v rámci komunity a uznání ze strany ostatních hackerů. Později se pak útočník již snažil o monetizaci, tedy dosažení nějakého zisku, a pro toto období je pak typické šíření jakéhokoliv malware, především pak bankware, ransomware a v posledních letech pak i cryptoware. Kromě toho pak dochází i k útokům na servery a koncová zařízení s cílem je kompromitovat, zcizit informace, ovlivnit provoz dané organizace anebo její zařízení začlenit do botnetu a vést z nich útoky na další cíle.

V současné době je drtivá většina útoků vedena za účelem dosažení zisku. Útočníci uvažuji naprosto ekonomicky a zvažují tak náklady, výnosy a celkové riziko. Je tomu tak především proto, že čím více zařízení je do internetu připojeno, tím vyšší návratnosti investice, zkr. ROI útočník dosahuje. Je tomu tak proto, že zatímco celkové náklady na vlastnictví infrastruktury potřebné k útoku, zkr. TCO, jsou v zásadě pořád stejné, tak výnosy s počtem obětí lineárně rostou. K dosažení pozitivního ROI však musí být:

- na síti dostatečné množství cílů;
- ty musí být trvale připojeny;
- disponovat odpovídající síťovou konektivitou.

Poté mohou být tato zařízení kompromitována, zajištěna persistence škodlivého kódu, vzdálený přístup a kontrola, a případně z nich mohou být úspěšně stažena citlivá data anebo veden útok na další zařízení v síti. V rámci celého období samozřejmě probíhají jak útoky na stroje, tak i lidi, a dochází i ke zneužívání nejrůznějších zranitelností a technik sociálního inženýrství, což se odvíjelo od

stavu informačních technologií, daného použitou architekturou a důrazem kladeným na zajištění bezpečnosti, jak uvádí Tabulka 8 – Vývoj informační společnosti, kde je jsou zachyceny jednotlivé dekády.

Tabulka 8 – Vývoj informační společnosti

Éra	Informační technologie	Na co byl kladen důraz
1970–1980	samostatné servery	spolehlivost
1980–1990	izolované sítě, mainframy, terminály, bez připojení do internetu, extranety	důvěrnost
1990–2000	interní el. pošta omezená konektivita do internetu, klient-server architektura	důvěrnost, integrita a dostupnost
2000–2010	data ve vlastních datových centrech, vícevrstvá architektura plná konektivita do internetu	Parkerian hexad, accountability
2010–2020	konsolidace, virtualizace, digitalizace, microservisy, data v cloudech	ochrana soukromí a osobních údajů

Stručnou charakteristiku jednotlivých dekád, která byla sestavena na základě analýzy informací v tisku a vyjádření bezpečnostních expertů v rámci pracovní skupiny, přičemž největší důraz byl kladen na poslední dekádu, zachycuje Příloha J – Vývoj kybernetických hrozeb v ČR.

3.2 Analýza primárních zdrojů

Obsahem této kapitoly je seznámení čtenáře s cíli a výsledky vlastního výzkumu. Je zde popsán výzkumný problém, předmět, účel, cíl, objekt, předmět, obsah empirického výzkumu a výzkumné předpoklady. V dalších kapitolách pak

je nastíněn plán výzkumu, způsob výběru respondentů, sestavení dotazníku a formulace jednotlivých otázek, a dále pak zpracování a vlastní analýza dat.

Výzkumný problém

Existuje nedostatečné povědomí o situaci v kyberprostoru, neboť nejsou k dispozici dostatečně věrohodné informace o tom, jakým kybernetickým útokům organizace v ČR čelí, jaké jsou finanční následky těchto útoků a jaká bezpečnostní opatření organizační a technické povahy organizace již přijaly a zda jsou tak dostatečně chráněny vůči nejčastějším kybernetickým útokům.

Cíl výzkumu

Identifikace nejčastějších kybernetických útoků a jejich dopadů na organizace, zjištění závislosti mezi útoky na jedné straně a velikostí, sektorem, odvětvím organizace a kritičností systému na straně druhé.

Účel výzkumu

Cílem této práce je navrhnout takovou metodiku, která by umožnila rychlé zhodnocení úrovně bezpečnosti v libovolné organizaci působící ve státním i soukromém sektoru bez ohledu na to, zdali je jejím cílem dosahování zisku či nikoliv, a která by zároveň nevyžadovala po respondentovi detailní znalosti z oblasti informační a kybernetické bezpečnosti, kterými většina zaměstnanců organizací nedisponuje.

Objekt empirického výzkumu

Objektem empirického výzkumu je problematika kybernetické bezpečnosti soukromých a veřejných institucí (organizací)

Předmět empirického výzkumu

Předmětem empirického výzkumu jsou názory výběrového souboru expertů působících v soukromých a veřejných institucích na vybrané otázky spojené s kybernetickou bezpečností jejich organizací.

Obsah výzkumu

Výzkum se snaží pomocí vhodných otázek zjistit, jaká je četnost jednotlivých kybernetických útoků, výše škod v případě jednotlivých kybernetických útoků a úroveň bezpečnosti v jednotlivých organizacích.

Výzkumné předpoklady

V rámci výzkumu byly stanoveny a naformulovány tyto deskriptivní a explanační výzkumné předpoklady, které by měly přispět k vyřešení samotného problému:

1. Základní bezpečnostní opatření jsou zavedena všude.
2. Čím větší je organizace, tím vyšší úrovně bezpečnosti dosahuje.
3. To, zda organizace působí v soukromém nebo veřejném sektoru rozhoduje o tom, jaká je skutečná úroveň bezpečnosti.
4. Kritické systémy jsou vždy lépe zabezpečeny než systémy, které jako kritické označeny nejsou.
5. Působení organizace v daném odvětví určuje i úroveň její bezpečnosti.
6. Čím větší je organizace, tím je na ní vedeno více útoků.
7. To, zda organizace působí v soukromém nebo veřejném sektoru, rozhoduje o tom, zda na ní bude veden větší počet útoků.
8. Čím významnější systém organizace provozuje, tím více je na něj vedeno útoků.
9. Působení organizace v daném odvětví zvyšuje počet útoků.
10. Čím významnější systém organizace provozuje, tím větší vzniká škoda v případě útoku.
11. Čím vyšší úrovně bezpečnosti organizace dosáhne, tím nižší škodu utrpí.

3.2.1 Plán výzkumného projektu

Výzkum proběhl v souladu s plánem uvedeným v této kapitole. Vlastnímu výzkumu předcházela pilotáž (listopad 2019) a předvýzkum (prosinec 2019). Harmonogram jednotlivých činností, personální zajištění a odpovědnosti jednotlivých členů výzkumného týmu uvádí **Příloha F – RAM**.

V jakém období bude výzkum probíhat

Výzkum bude probíhat od ledna do dubna 2020

Typ prováděného výzkumu

Dle cílů se bude jednat o deskriptivní/kauzální typ a dle povahy dat pak o výzkum kvantitativní.

Metoda sběru dat

Data budou získána prostřednictvím dotazníkového šetření.

Typ sběru dat

Computer Assisted Web Interviewing, zkr. CAWI, on-line elektronické přes internet, kdy budou e-mailem oslovovány zástupci z jednotlivých odvětví (šablona použitého e-mailu je uvedena v příloze č. 2)

Kde bude el. verze dotazníku umístěna

Dotazník bude umístěn na internetu na webové adrese https://www.cleverandsmart.cz/vyzkum-skutecne-urovne-kyberneticke-bezpecnosti-v-cr-dotaznik/

Typ dotazníku

Dotazník bude strukturovaný.

Typ otázek

V dotazníku budou použity otázky uzavřené, výsledkové (meritorní), analytické, kontrolní, nominální, alternativní.

Stanovení velikosti výběrového souboru

Velikost souboru bude zvolena na základě statistického přístupu.

Velikost výběrového vzorku

Bude osloveno několik desítek respondentů.

Technika výběru vzorku

Bude proveden kvazireprezentativní kvótní výběr technikou vhodného úsudku.

Kdo bude data sbírat

Samotný autor této práce, který bude vystupovat jako nezávislý a certifikovaný manažer informační bezpečnosti a bude na něj uveden e-mailový i telefonický kontakt.

Od koho budou odpovědi získávány

Od manažerů informační a kybernetické bezpečnosti, případně pověřenců pro ochranu osobních údajů a v menších organizacích pak od osoby, která danými informacemi disponuje

Způsob vyplnění dotazníku

Vyplnění dotazníku bude probíhat výběr jedné odpovědi z nabízených variant.

Způsob provedení sběru a analýzy dat

Dotazník bude vyvinut jako webová aplikace běžící na platformě UNIX, MySQL, Apache, Wordpress a bude naprogramován v jazyce PHP, HTML, CSS autorem této práce, základní statická analýza dat pak bude provedena za použití aplikace Excel z kancelářského balíku Microsoft Office 2013 pro domácnosti a vestavěných funkcí a faktorová analýza pak bude provedena za použití aplikace SPSS Modeler a Statistics od společnosti IBM.

Zpracování výstupů

Bude zobrazeno relativní vyjádření.

Třídící znaky

Data budou tříděna dle organizace, sektoru, odvětví, velikosti

Datum zveřejnění výsledků výzkumu

Výsledky budou zveřejněny ve 4Q 2020.

Forma zveřejnění výsledků

Výsledky budou zveřejněny na internetu na adrese https://www.cleverandsmart.cz/vyhodnoceni-skutecne-urovne-kyberneticke-bezpecnosti-v-organizacich-v-cr-za-rok-2019/ a PDF dokument ke stažení.

3.2.2 Podoba dotazníku

Vlastní dotazník je vytvořen v jazyce HTML a formátován za použití CSS, který je využit i pro generování výsledku, který respondent obdrží ihned poté, co dotazník vyplní.

Data zadávaná do formuláře jsou ještě před odesláním kontrolována pomocí JS a po odeslání jsou znovu kontrolována ještě před uložením do databáze pomocí PHP skriptu. To je ochrana proti tomu, kdyby někdo chtěl do MySQL databáze, do které jsou výsledky ukládány, zaslat zcela nesmyslné hodnoty.

Skript zároveň obsahuje i určitou logiku a provede základní vyhodnocení zaslaných odpovědí a zobrazí respondentovi výsledek, tj. celkové skóre, které vyjádří graficky i numericky a dále vypíše seznam hrozeb, vůči kterým respondent není zcela imunní a rovněž jaká bezpečnostní opatření by měl ve vlastním zájmu zavést.

Důvod, proč nebylo použito nějaké jiné již hotové řešení, které se běžně k realizaci obdobných výzkumů používá, byl ten, že žádné běžně používané řešení nepodporovalo okamžité vyhodnocení a zobrazení výsledků požadovaným způsobem.

Dotazník čítá celkem 61 otázek a je rozdělen do 5 částí označených římskými číslicemi I–V, přičemž:

- první část slouží ke zjištění základních charakteristik organizace, jako je sektor, odvětví, velikost;
- druhá část zkoumá odolnost organizace vůči vybraným hrozbám prostřednictvím přijatých opatření;
- třetí část se věnuje vyhodnocení četnosti hrozeb;
- čtvrtá část se věnuje hodnocení dopadů jednotlivých hrozeb;
- pátá část se věnuje obavám respondentů.

První otázka je otevřená a požaduje po respondentovi uvedení e-mailové adresy, ostatní otázky jsou uzavřené a respondent buď vybírá vhodnou odpověď z rozbalovacího menu anebo ji zaškrtává. V dotazníku bylo použito několik typů možných odpovědí: **nominální** (první část), **dichotomní** (druhá část), **ordinální** (třetí a pátá část) a **kardinální** (čtvrtá část).

Otázky a odpovědi použité v dotazníku byly sestaveny autorem této práce na základě **kvalitativní analýzy zahraničních bezpečnostních reportů a rovněž i šetření bezpečnostních incidentů** v organizaci, kde autor působí nebo v minulosti působil jako bezpečnostní konzultant.

Takto **připravený dotazník byl poté předložen bezpečnostním expertům** s několika desítek let dlouhou praxí a disponujícím teoretickými i praktickými znalostmi, které získali během svého působení v největších organizacích v ČR.

Tito experti pak vytvořili tzv. **pracovní skupinu**, která otázky a odpovědi za použití metody **Wideband Delphi** revidovala (proběhla 3 kola) a poté byl tento dotazník vystaven i na webu a uveden na něj odkaz **ve skupině Informační bezpečnost čítající více jako 300 odborníků**, kteří dostali možnost se k němu rovněž vyjádřit a někteří této možnosti i využili. Po zapracování připomínek dotazník získal svoji finální podobu. Seznam všech otázek obsahuje Příloha G – Seznam otázek.

3.2.3 Složení výběrového souboru

Nejprve byla identifikována jednotlivá odvětví národního hospodářství a následně pak byly zvoleny jednotlivé organizace a v nich dohledány osoby na pozici manažerů informační a kybernetické bezpečnosti, případně DPO, přičemž platí, že v každé organizaci se zpravidla nachází jen jedna osoba na této pozici.

Vzhledem k tomu, že v rámci jednotlivých odvětví působí různý počet organizací, bylo rozhodnuto, že bude proveden výběr organizací, které představují typické zástupce daných odvětví, a že velikost výběrového souboru v řádu desítek organizací bude pro účely tohoto výzkumu dostačující.

Ostatně obdobné zahraniční výzkumy, které jsou v této práci dále citovány, a které byly realizované ze strany bezpečnostních firem ve spolupráci s významnými univerzitami, zahrnovaly kolem několika set firem ve více než deseti státech, což více než odpovídá zvolenému počtu organizací v případě ČR, obzvlášť vzhledem k její velikosti. Rovněž statistická významnost (p-value[141]) pozbývá v tomto případě svůj hlavní význam, lze podle ní jen odhadovat dostatečnost rozsahu výběrového souboru.

[141] Hladina významnosti (p-value) odráží nejen sílu vztahu (míru asociace), ale je v přísné návaznosti na velikost výběrového souboru. Někdy odráží i vliv jiných parametrů. Proto je v rámci náhodného výběru možné mít vztah mezi proměnnými, který vyjadřuje silnou asociaci, ale není statisticky významný. To proto, že rozsah je velmi malý. Na druhou stranu mohou existovat vztahy, které zobrazují extrémně slabou asociaci, ale jsou statisticky velmi významné.

V některých odvětvích jako je např. bankovnictví, energetika nebo doprava, kde působí poměrně malé množství organizací pak i výběr jednotek organizací umožňuje zobecnit zjištěné závěry na celek.

Jednalo se tak v zásadě o kvazireprezentativní výběr[142]. Vybrané osoby pak byly následně osloveny e-mailem anebo přes sociální síť LinkedIn s požadavkem na vyplnění dotazníku. Tímto způsobem bylo osloveno 250 manažerů bezpečnosti z bank, nemocnic, univerzit, energetiky, dopravní infrastruktury atd. V hojně zastoupených odvětvích pak byl proveden náhodný výběr.

Tito respondenti byli osloveni e-mailem, jehož šablonu obsahuje Příloha H – Šablona e-mailu. Respondentům bylo vysvětleno, proč má prováděný výzkum smysl, a co jim osobně participace na výzkumu přinese. Příslib okamžitého vyhodnocení jejich situace na základě zodpovězení jednotlivých otázek pak mělo respondenty motivovat k tomu, aby odpovídali podle skutečnosti.

Respondenti byli vybráni z řad expertů, kteří se zaobírají problematikou kybernetické bezpečnosti v rámci své organizace. Základní složení výběrového souboru obsahují následující tabulky.

[142] KOZEL, Roman, Lenka MYNÁŘOVÁ a Hana SVOBODOVÁ. *Moderní metody a techniky marketingového výzkumu*. Praha: Grada, 2011. ISBN 978-80-247-3527-6.

Tabulka 9 – Velikost organizace

Skupina	Charakteristika skupiny	Četnost	Procenta
mikro	Zaměstnává do 10 osob	15	16
malý	Zaměstnává od 10 do 50 osob	12	13
střední	Zaměstnává od 50 do 250 osob	20	21
velký	Zaměstnává nad 250 osob	47	50
	celkem	94	100

Tabulka 9 – Velikost organizace zachycuje podíl organizací o různé velikosti na celkovém počtu respondentů.

Tabulka 10 – Sektor

Skupina	Charakteristika skupiny	Četnost	Procenta
SS	Působí v soukromém sektoru	67	71
VS	Působí ve veřejném sektoru	27	29
	Celkem	94	100

Tabulka 10 – Sektor zachycuje podíl soukromého a veřejného sektoru na celkovém počtu respondentů.

Tabulka 11 – Kritičnost systému

skupina	charakteristika skupiny	Četnost	Procenta
ZoKB	Provozuje systém dle Zákona o kybernetické bezpečnosti	53	56
non ZoKB	Neprovozuje systém dle Zákona o kybernetické bezpečnosti	41	44
	Celkem	94	100

Tabulka 11 – Kritičnost systému zachycuje podíl systémů spadající pod působnost ZoKB na celkovém počtu.

Tabulka 12 – Odvětví

Skupina	Charakteristika skupiny	Četnost	Procenta
A	zemědělství, lesnictví a rybářství	2	2
B	těžba a dobývání	1	1
C	zpracovatelský průmysl	6	6
D	výroba a rozvod elektřiny, plynu, tepla a klimatizovaného vzduchu	2	2
G	velkoobchod a maloobchod; opravy a údržba motorových vozidel	2	2
H	doprava a skladování	2	2
I	ubytování, stravování a pohostinství	2	2
J	informační a komunikační činnosti	29	31
K	peněžnictví a pojišťovnictví	8	9
L	činnosti v oblasti nemovitostí	1	1
M	profesní, vědecké a technické činnosti	4	4
N	administrativní a podpůrné činnosti	4	4
P	vzdělávání	11	12
Q	zdravotní a sociální péče	8	9
R	kulturní, zábavní a rekreační činnosti	2	2
S	ostatní činnosti	10	11
	Celkem	94	100

Tabulka 12 – Odvětví zachycuje zastoupení jednotlivých organizací působících v různých odvětví národního hospodářství.

3.2.4 Zpracování dat

Nemalá pozornost byla věnována i ochraně formuláře. Jako **ochrana před zašpiněním dotazníku roboty** a narušením validity dat byla implementována ochrana Google recaptha v3 a pro případ, že by se někdo pokusil znehodnotit výsledky výzkum tím, že by dotazník opakovaně odesílal, ať už se stejnými nebo různými hodnotami. Jako ochrana před manuálním odesíláním dotazníku se kromě e-mailu, který může samozřejmě respondent zadat jakýkoliv, zaznamenává i IP adresa stroje, ze kterého k odeslání dotazníku došlo a rovněž i přesný čas, kdy došlo k jeho odeslání. Tímto způsobem se podařilo identifikovat několik jednotek dotazníků, kdy respondent nebyl evidentně spokojen se svým výsledkem, a tak opakovaně zadával a zkoušel různé hodnoty, než obdržel pro

něj uspokojivého skóre. Tyto dotazníky proto byly z výše uvedeného důvodu ze zpracování vyřazeny.

Pravdivost odpovědí není samozřejmě možné stoprocentně garantovat, neboť respondent se může obávat, že v okamžiku, kdy uvede, že některé opatření nemá zavedeno, nebo že se stal obětí nějakého útoku či utrpěl nějakou ztrátu a došlo by k úniku informací z databáze, kam se výsledky dotazníků ukládají, tak by to mohlo vrhnout špatně světlo na jeho organizaci. I tohle byl důvod, proč dotazníky nebyly adresovány v papírové podobě konkrétním subjektům a byla jim dána možnost vyplnit dotazník z jakéhokoliv počítače a uvést jakoukoliv e-mailovou adresu, čehož mnozí i využili. Jedna otázka v II. sekci byla navíc postavena i tak, aby byl odhalen respondent, který na všechny otázky odpovídá ANO.

Vzhledem k tomu, že respondenti byli s cílem výzkumu seznámeni a v dopise, který obdrželi, a ve kterém bylo uvedeno, že se jim po odeslání dotazníku zobrazí vyhodnocení, tedy jakým hrozbám jsou vystaveni, jak jsou vůči nim chráněni a jaká opatření by měli ve vlastním zájmu zavést, tak byli dostatečně motivováni k tomu, aby dotazník vyplnili poctivě. Dále bylo v dopise uvedeno, jaký bude mít vyplnění dotazníku přínos pro probíhající výzkum a že pak budou moci na základě výsledků výzkum lépe obhájit jejich investice do bezpečnostních řešení. Kromě toho byly na webu, kde se dotazník nachází, a dále pak i na sociálních sítích ve větší míře publikovány články objasňující situaci v kyberprostoru a nutnost jej zkoumat.

Následnou analýzou bylo ověřeno, že nedošlo, až na ojedinělé případy k pokusům učinit výsledky výzkumu nepoužitelnými. **Díky implementovaným kontrolním mechanismům bylo možno ze zpracování vyloučit dotazníky, které byly opakovaně odeslány ze stejné IP adresy, v příliš rychlém časovém sledu apod**. Do dalšího zpracování tak vstoupily jen dotazníky, které byly odeslány z unikátní adresy z IP adresního prostoru ČR. Rovněž nebylo zaznamenáno ani větší množství nejvyššího skóre, které by mohlo znamenat, že se respondent snaží své skóre vylepšit.

Vzhledem k tomu, že respondenti byli oslovováni v několika etapách po jednotlivých odvětvích a v mnoha případech i individuálně, tak pak mohl být čas, IP adresa a použitý e-mail použit k tomu, aby mohlo být ověřeno, že se jedná skutečně o respondenta osloveného v rámci výběrového souboru a nikoliv

někoho, kdo se k dotazníku náhodou dostal. Ve sporných případech pak bylo některým respondentům i voláno, aby vyplnění dotazníku potvrdili.

Kontrola úplnosti byla zajištěna samotnou technologií, kdy docházelo ke kontrole na straně klienta i na straně serveru, takže nebylo možné odeslat a už vůbec ne uložit neúplný dotazník do DB. Respondent musel vždy uvést odpovědi na všechny otázky.

Po importu byly vyřazeny dotazníky, které se jevily jako nevalidní. **Celkem bylo vyřazeno 14 dotazníků, odeslaných z jedné IP adresy, s různými e-maily a hodnotami a v krátkém časovém sledu a dále pak dotazníky, kde bylo evidentní, že se jej respondent nesnažil vyplnit podle skutečnosti.** Např. když na všechny otázky z druhé sekce odpověděl ve všech případech ANO nebo NE. Dotazník záměrně neobsahoval neutrální odpovědi a střední hodnoty, aby byl respondent donucen se nad svou odpovědí zamyslet a odpovědět dle pravdy. Dotazník rovněž obsahoval dvojici kontrolních otázek, jejichž odpovědi byly porovnávány, a pokud nekorespondovaly, byly tyto dotazníky rovněž vyloučeny ze zpracování.

3.2.5 Analýza dat

Zdrojová data, které jsou umístěna na CD, které je přílohou této práce, byla nejprve vyexportována z databáze MS SQL ve formátu csv, kde byl jako oddělovač použit středník a kódována ve znakové sadě 1250. Následně byla naimportována do MS Excel. Každé otázce byl přidělen kód. Rozdílný počet polí je dán jen tím, že se v databázi navíc nachází i IP adresa, která byla odesílána spolu s dotazníkem jako skryté formulářové pole a dále pak přesný čas odeslání a uložení vyplněného dotazníku do databáze, spočítané skóre na základě automatického vyhodnocení otázek z II. sekce a sloupce sloužící k označení nevalidních dotazníků.

Následně byla provedena analýza dat a došlo k ověření výzkumných předpokladů týkajících se závislosti úrovně bezpečnosti na základě subsumace

organizace do příslušné skupiny dle její velikosti, sektoru[143], kritičnosti a odvětví[144].

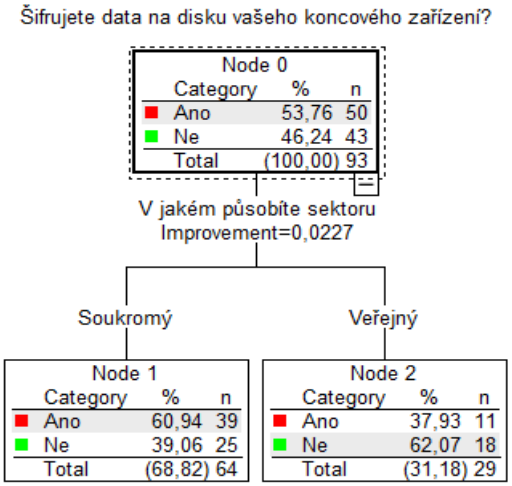
Průzkumová analýza dat ukázala, že data porovnávaných skupin nemají ve většině případů normální rozdělení ani homogenní rozptyl, což vedlo k použití metod neparametrických, jak je uvedeno v kapitole 1.6. Analýza odhalila určité rozdíly a závislosti mezi některými proměnnými. Ty jsou okomentovány níže.

Jednotlivé proměnné jsou kódovány jako PX, kde X je pořadové číslo otázky v dotazníku. IDX pak odpovídá pořadovému číslu otázky týkající se identifikace organizace (sektor, velikost, odvětví kritičnost apod.). V rámci analýzy je hledán vztah mezi IDX a PX.

V rámci analýzy dílčích závislostí pak byl zkoumán vztah mezi jednotlivými otázkami P01 až P54 a identifikátory ID01 a ID03. Pod příslušnými stromy jsou dále identifikovány možné příčiny tohoto stavu, na základě explanační analýzy ve spolupráci s bezpečnostními experty tvořícími expertní tým.

Obrázek 7 – Vliv ID01-P01 zachycuje vztah mezi sektorem a bezpečnostním opatřením spočívajícím v šifrování dat.

Obrázek 7 – Vliv ID01-P01



[143] ČERMÁK, Miroslav a Zdeněk KOVAŘÍK. Problémy determinace kybernetické bezpečnosti v prostředí České republiky – 1. část. *Bezpečnostní teorie a praxe*. 2021, roč. 2021, č. 1. ISSN 2571-4589. s. 43–62

[144] ČERMÁK, Miroslav a Zdeněk KOVAŘÍK. Problémy determinace kybernetické bezpečnosti v prostředí České republiky – 2. část. *Bezpečnostní teorie a praxe*. 2021, roč. 2021, č. 2. ISSN 2571-4589. s. 27–44

Goodman a Kruskalovo tau = 0,046 (větší než malá věcně významná asociace) Symetrický Cohenův index w = 0,213 (větší než malý věcně významný efekt)

Šifrování dat lze zahrnout mezi základní bezpečnostní opatření technické povahy, které poskytuje zajištění důvěrnosti dat v případě, že dojde ke zcizení média, na kterém se nacházejí citlivá data anebo celého koncového zařízení, na kterém jsou data rovněž uložena a zpracovávána. Přesto téměř polovina respondentů (46 %) svá data nešifruje, zatímco více jak polovina svá data šifruje (54 %).

Netřeba dodávat, že neoprávněná osoba, která k datům ať už na přenosném médiu nebo na samotném zařízení získá přístup, není schopna se bez znalosti hesla k datům dostat. Skutečnost, že organizace působící v soukromém sektoru ve výrazně větší míře šifrují data na svých koncových zařízeních (61 %), než organizace působící ve státním sektoru (38 %) si lze vysvětlit tak, že:

- jejich vlastníci a manažeři jsou si více vědomi hodnoty svých informací, které obzvláště ve vysoce konkurenčním a turbulentně se měnícím prostředí jsou předmětem nejrůznějších kybernetických útoků, konkurenčního zpravodajství a průmyslové špionáže a mohou představovat značnou konkurenční výhodu, a i jejich pouhý únik může značně poškodit dobré jméno organizace a v konečném důsledku vést i k ukončení její činnosti na trhu, což je pro ně vyšší riziko než pouhá pokuta od ÚOOÚ;

- organizace působící ve statním sektoru, a mající zpravidla i monopol na poskytování určité činnosti nemusí příliš ztrátu svého dobrého jména řešit, neboť mohou maximálně dostat pokutu od ÚOOÚ, ale ve své činnosti budou vzhledem ke svému monopolnímu postavení nadále pokračovat;

- většina zaměstnanců působících ve státním sektoru pracuje na nepřenosných zařízeních, desktopech, umístěných v kancelářích, kam za ní sice chodí veřejnost, ale kde nemůže dojít a ani nedochází k jejich krádeži a pokud už jsou zaměstnanci vybaveni notebooky, tak se s nimi zpravidla pohybují jen v prostorách svého zaměstnavatele;

- zaměstnanci působící v soukromých společnostech pracují v open space, kavárnách a na home office, kde buď dochází k většímu pohybu velkého množství osob, včetně externistů, zaměstnanci se mezi sebou neznají anebo pracují z domova, kde není zajištěna stejná úroveň fyzické bezpečnosti, a kde je riziko krádeže výrazně vyšší;

- zaměstnanci působící v soukromém sektoru za svými zákazníky více cestují, více využívají možnosti home office a zdá se, že tento trend bude dál pokračovat[145] a bude zde i vyšší riziko, že své přenosné zařízení ztratí anebo jim bude ukradeno;

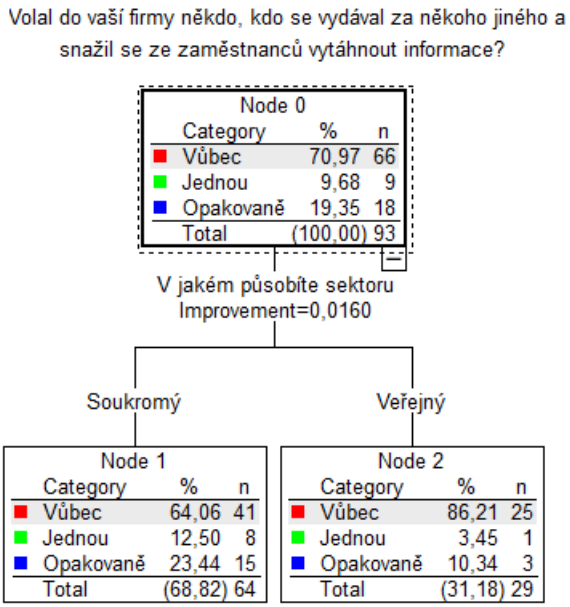
- v neposlední řadě šifrování něco stojí, a ne všechny organizace disponují zařízeními a operačními systémy, která transparentní šifrování podporují a mají vyřešenu správu klíčů.

Z rozhovoru s manažery informační bezpečnosti dále vyplynulo, že k šifrování koncových zařízení přistoupili neprodleně poté, co řešili až několik případů ročně, kdy došlo ke ztrátě a krádeži notebooků z šatních skříní, v restauracích, ze zaparkovaných aut apod. a nechtěli riskovat, že by se případný útočník mohl dostat k citlivým datům na nich uložených. A v mnoha případech nešlo ani tak o to, že by je zpřístupnění dat mohlo přímo ohrozit, jako spíše o poškození dobrého jména organizace v důsledku možné medializace takového případu.

Obrázek 8 – Vliv ID01-P19 zachycuje vztah mezi sektorem a vektorem útoku.

[145] HAMROZI, Petr. V IT byl homeoffice běžný, po koronaviru dál poroste. *Nejbusiness.cz* [online]. 2020 [cit. 08.06.2020]. Dostupné z: https://www.nejbusiness.cz/zpravy/2020-05-06-v-it-byl-homeoffice-bezny-po-koronaviru-dal-poroste

Obrázek 8 – Vliv ID01-P19



Volal do vaší firmy někdo, kdo se vydával za někoho jiného a snažil se ze zaměstnanců vytáhnout informace?	V jakém působíte sektoru				
	Soukromý	Veřejný	celkem	medián	dorvar
Vůbec	-	+	66	1,305	,471
Jednou	o	o	9	1,063	,198
Opakovaně	o	o	18	1,100	,278
celkem	64	29	93	1,227	,429

Hodnota koeficientu beta je 0,052 s 95% intervalem spolehlivosti (-0,025; 0,129), (téměř střední věcně významná asociace) Symetrický Cohenův index w = 0,228 (větší než malý věcně významný efekt) Hodnota koeficientu beta je 0,052 s 95% intervalem spolehlivosti (-0,025; 0,129) Cohenův index w = 0,228 (více než malý věcně významný efekt)

Vishing neboli phishing po telefonu patří mezi nejjednodušší techniku sociálního inženýrství, kdy se útočník vydává za někoho jiného a snaží se tak získat citlivé informace. Opakovaně se s ní setkala přibližně pětina organizací (19 %) a alespoň jednou pak necelá desetina (10 %). Skutečnost, že většina oslovených organizací (71 %) se s ní nesetkala, by nasvědčovalo tomu, že je tato technika využívána výhradně v rámci cílených útoků na konkrétní organizace a není na rozdíl od phishingu aplikována plošně, nejspíš proto, že je dražší a vyžaduje větší přípravu. Skutečnost, že se s touto technikou ve větší míře opakovaně setkávají spíše zaměstnanci soukromých společností (23 %) než zaměstnanci ve veřejném sektoru (10 %), je možné vysvětlit tak, že:

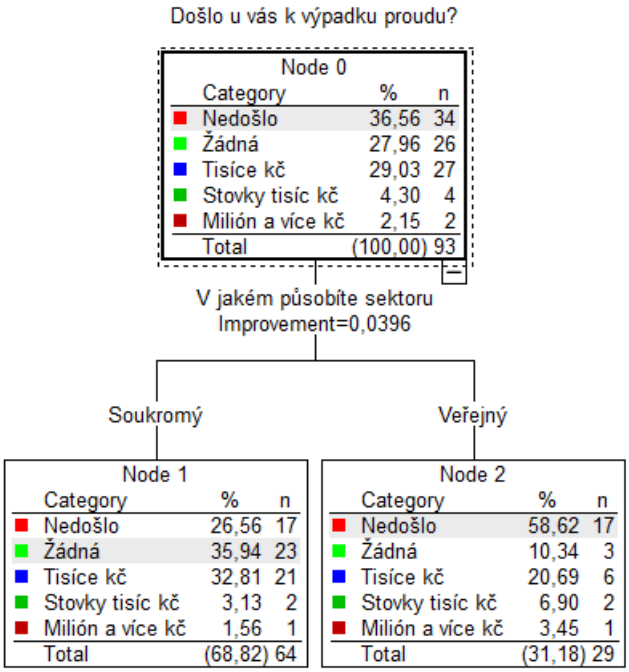
- v drtivé většině soukromých organizací lze zaznamenat zahraniční účast, a tudíž je běžné, že zaměstnanci těchto organizací jsou jazykově lépe vybaveni a jsou zvyklí, že jim běžně volají kolegové ze zahraničních poboček s nejrůznějšími dotazy.

- v soukromých organizacích je soustředěno know-how a je obtížnější zaměstnance těchto organizací přesvědčit ke spolupráci, což může být dáno např. i vyšším finančním ohodnocením.

- Drtivá většina zaměstnanců působících ve veřejném sektoru slouží občanům ČR a jako úřední jazyk používají češtinu, takže tak často do styku se zahraničními občany nepřijdou a osoba hovořící anglicky by upoutala jejich pozornost a svého cíle by nedosáhla.

Obrázek 9 – Vliv ID01-P23 zachycuje vztah mezi sektorem a výpadkem proudu.

Obrázek 9 – Vliv ID01-P23



Došlo u vás k výpadku proudu?	V jakém působíte sektoru				
	Soukromý	Veřejný	celkem	medián	dorvar
Nedošlo	--	++	34	1,500	,500
Žádná	+	-	26	1,065	,204
Tisíce kč	o	o	27	1,143	,346
Stovky tisíc kč	o	o	4	1,500	,500
Milión a více kč	o	o	2	1,500	,500
celkem	64	29	93	1,227	,429

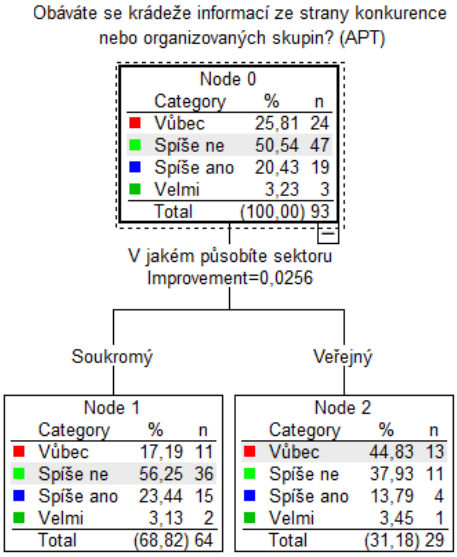
Hodnota koeficientu beta je 0,132 s 95% intervalem spolehlivosti (-0,001; 0,266), (velká věcně významná asociace) Symetrický Cohenův index w = 0,363 (střední věcně významný efekt)

- Na dodávce proudu je většina ekonomických subjektů závislá a jeho výpadek jim může způsobit s ohledem na délku jeho trvání nemalé problémy v podobě finanční ztráty v různé výši.

- Zatímco více jak čtvrtina (26 %) organizací působících v soukromém sektoru se s tímto incidentem nesetkala, tak organizací působících ve veřejném sektoru se s tímto incidentem nesetkala více jak polovina (59 %). Rozdíl mezi organizacemi působícími v soukromém a veřejném sektoru se pak projevuje i ve výši škod, zatímco v soukromém sektoru utrpěla škodu ve výši několika tisíc korun téměř třetina organizací (33 %), tak ve veřejném sektoru to byla jen pětina (21 %). Ovšem na druhou stranu zase mnohem méně organizací ze soukromého sektoru utrpělo škodu ve výši stovek tisíc korun anebo dokonce přesahující milión korun.

Obrázek 10 – Vliv ID01-P51 zachycuje vztah mezi sektorem a obavou z krádeže informací ze strany APT skupin.

Obrázek 10 – Vliv ID01-P51



Obáváte se krádeže informací ze strany konkurence nebo organizovaných skupin? (APT)	V jakém působíte sektoru				
	Soukromý	Veřejný	celkem	medián	dorvar
Vůbec	--	++	24	1,577	,497
Spíše ne	o	o	47	1,153	,359
Spíše ano	o	o	19	1,133	,332
Velmi	o	o	3	1,250	,444
celkem	64	29	93	1,227	,429

Hodnota koeficientu beta je 0,088 s 95% intervalem spolehlivosti (-0,036; 0,211), (střední věcně významná asociace) Symetrický Cohenův index w = 0,296 (střední věcně významný efekt)

V současné době, která je nazývána jako informační, se s informacemi obchoduje jako s jakoukoliv jinou komoditou[146], neboť ten, kdo má k dispozici informace a dokáže jich využít, získává na turbulentně se měnícím trhu nezanedbatelnou konkurenční výhodu. Nelze se tak divit, že předmětem cílených kybernetických útoků vedených na informační systémy a zaměstnance určitých organizací jsou právě informace.

Skutečnost, že více jak čtvrtina (26 %) respondentů se těchto útoků neobává vůbec a spíše ne pak více jak polovina (51 %) nasvědčuje tomu, že jsou tyto útoky ze strany respondentů vnímány stále jako něco, co se jich přímo netýká. Určitou

[146] PREATER, Andrew. Information as a commodity – at #radliblon. *Andrew Preater* [online]. 2014 [cit. 08.06.2020]. Dostupné z: https://www.preater.com/2014/06/03/information-as-a-commodity/

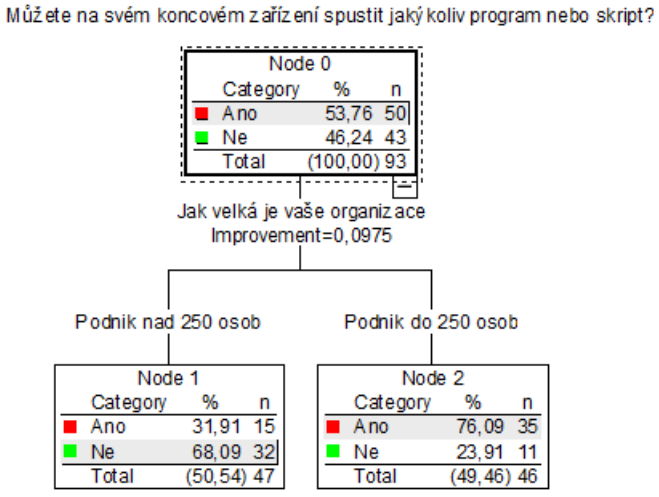
obavu vyjádřila přibližně pětina respondentů (20 %) a velmi se obává jen pouhých pár procent (3 %) respondentů.

Určité rozdíly pak lze zaznamenat mezi tím, jak tuto hrozbu vnímají respondenti v soukromém a veřejném sektoru. Jen necelá pětina respondentů v soukromém sektoru se této hrozby neobává vůbec (17 %) a spíše se neobává více jak polovina (56 %), ve veřejném sektoru se neobává podstatně více respondentů, téměř polovina (44 %), ale spíše se neobává jen více jak třetina (38 %).

Vyšší obava respondentů působících v soukromém sektoru se dá vysvětlit tím, že je na ně buď vedeno více útoků anebo jsou více závislé na hospodářských výsledcích organizace, ve které působí, případně se může jednat i o kombinaci obou těchto faktorů. Opomenout také nelze ani působení médií, i když v tomto případě lze vzhledem k počtu medializovaných případů o síle tohoto faktoru pochybovat. V dalším výzkumu by však bylo vhodné se zaměřit na to, co přesně ovlivňuje obavy respondentů, protože z rozhovoru s nimi vyplynulo, že od těchto jejich obav se v zásadě odvíjí obsah jejich strategie informační bezpečnosti na další rok.

Obrázek 11 – Vliv ID03-P08 zachycuje vztah mezi velikostí podniku a bezpečnostním opatřením zabraňujícím uživateli spustit libovolný program.

Obrázek 11 – Vliv ID03-P08



Goodman a Kruskalovo tau = 0,196 (velká věcně významná asociace) Symetrický Cohenův index w = 0,443 (téměř velký věcně významný efekt)

Otázka ohledně možnosti spustit jakýkoliv program nebo skript je klíčová, protože toto opatření patří mezi nejúčinnější, pokud jde o kompromitaci koncového zařízení prostřednictvím škodlivého kódu. Více jak polovina respondentů (54 %) se vyjádřila, že na svém zařízení může spustit jakýkoliv program nebo skript a necelá polovina (46 %), že nikoliv.

Dále se ukázalo, že je zde značný rozdíl mezi tím, jak k této problematice na jedné straně přistupují velké organizace, kde jen přibližně třetina (32 %) může na svém zařízení spustit libovolný kód, a na straně druhé mikropodniky, malé a střední podniky, kde jsou to více jako tři čtvrtiny (76 %), kterým to bezpečnostní politika nezakazuje. Je možné, že příčinou tohoto rozporu jsou následující skutečnosti:

- velké společnosti si uvědomují, že možnost spouštět na koncovém zařízení uživatele jakýkoliv program sice zvyšuje uživatelský komfort, ale na druhou stranu zde hrozí riziko používání SW v rozporu s licenčním ujednáním, kdy spousta SW nesmí být používána pro komerční účely;

- velké společnosti si uvědomují, že stejně jako může být spuštěn jakýkoliv skript nebo aplikace stažená z internetu, zaslaná e-mailem anebo donesená na přenositelném médiu, tak stejně tak může být spuštěn i škodlivý kód doručený obdobným způsobem a spuštěn pod profilem a s právy aktuálně přihlášeného uživatele;

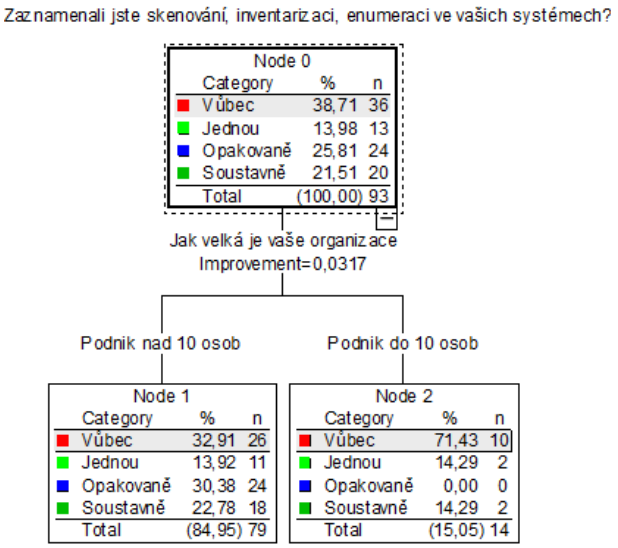
- náklady na zabezpečení koncového zařízení ve smyslu blokování neschválených aplikací, což je možné prostřednictvím funkcí operačního systému anebo bezpečnostních aplikací třetích stran, kdy lze vhodná pravidla nastavit tak, aby se daly spustit jen nainstalované aplikace a nové aplikace uživatel nainstalovat nemohl a nemohl ani spouštět neschválené skripty spouštěné pomocí schválených příkazových interpretů;

- spoléhají na zabezpečení na úrovni antimalware řešení, které by měly detekovat škodlivý kód.

Vliv ID03 na P11

Obrázek 12 – Vliv ID03-P11 zachycuje vztah mezi velikostí podniku a schopností organizace detekovat přípravnou fázi útoku.

Obrázek 12 – Vliv ID03-P11



Zaznamenali jste skenování, inventarizaci, enumeraci ve vašich systémech?	Jak velká je vaše organizace				
	Podnik do 10 osob	Podnik nad 10 osob	celkem	medián	dorvar
Vůbec	++	--	36	1,808	,401
Jednou	o	o	13	1,909	,260
Opakovaně	-	+	24	2,000	,000
Soustavně	o	o	20	1,944	,180
celkem	14	79	93	1,911	,256

Hodnota koeficientu beta je 0,099 s 95% intervalem spolehlivosti (0,006; 0,192), (více než střední věcně významná asociace) Symetrický Cohenův index w = 0,396 (více než střední věcně významný efekt)

Otázka týkající se skenování, inventarizace a enumerace v systémech organizace, resp. zda organizace tuto skutečnost zaznamenala, odhalila, že téměř dvě pětiny (39 %) organizací tuto skutečnost nezaznamenaly, více jak pětina (14 %) ji zaznamenala během roku jednou a čtvrtina (26 %) eviduje opakované skenování svých systémů a pětina (22 %) pak detekuje tuto aktivitu dokonce soustavně.

Je otázka, zda ti, co skenování, inventarizaci ani enumeraci ve svých systémech nezaznamenali, ji nezaznamenali proto, že se o to nikdo nepokoušel anebo proto, že nemají prostředky, kterými by to zjistili. Vzhledem k tomu, že

k plošným skenům celého internetu dochází spolu se zveřejněním každé kritické zranitelnosti v hojně používaných produktech, kloníme se spíš k druhé možnosti.

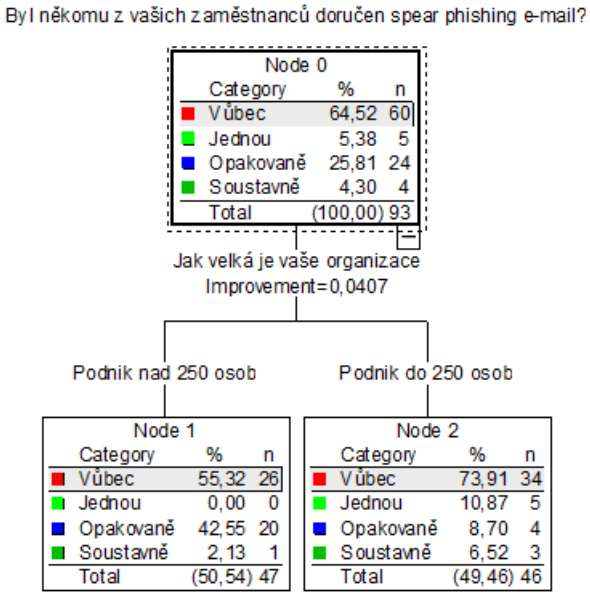
Dále jsme zaznamenali, že mezi podniky nad 10 osob a do 10 osob jsou značné rozdíly. Zatímco v první skupině je jen necelá třetina organizací (33 %), které sken nezaznamenaly, tak ve druhé skupině jsou to téměř tři čtvrtiny (71 %). Příčina tohoto stavu může spočívat především v tom, že:

- prvně jmenovaní si uvědomují, že skenování, inventarizace a enumerace jsou prvním krokem, který útočník realizuje v rámci plošně i cíleně vedených kybernetických útoků, a tudíž zavedly taková bezpečnostní opatření, pomocí kterých jsou schopni tuto první fázi útoku detekovat;

- druzí jmenovaní si tuto skutečnost nepřipouští, nemají zdroje, a to ani finanční ani lidské na to, aby mohly odpovídající bezpečnostní řešení realizovat. Rovněž z rozhovorů s vlastníky mikropodniků a ředitelů malých firem vyplynulo, že si skutečnost, že by na ně mohly být vedeny cílené útoky, nepřipouští a stejně tak si nepřipouští, že by se jejich organizace mohly stát obětí tzv. plošného útoku.

Obrázek 13 – Vliv ID03-P18 zachycuje vztah mezi velikostí podniku a spear phishing kampaní.

Obrázek 13 – Vliv ID03-P18



Byl někomu z vašich zaměstnanců doručen spear phishing e-mail?	Jak velká je vaše organizace				
	Podnik do 250 osob	Podnik nad 250 osob	celkem	medián	dorvar
Vůbec	o	o	60	1,382	,491
Jednou	+	-	5	1,000	,000
Opakovaně	---	+++	24	1,900	,278
Soustavně	o	o	4	1,167	,375
celkem	46	47	93	1,511	,500

Hodnota koeficientu beta je 0,191 s 95% intervalem spolehlivosti (0,061; 0,32), (velká věcně významná asociace) Symetrický Cohenův index w = 0,437 (téměř velký věcně významný efekt)

Spear phishing je nejčastější modus operandi používaný v rámci cílených útoků na konkrétní organizace, kdy jsou zneužívány techniky sociálního inženýrství k oslovování čelních představitelů organizace, ale i řadových zaměstnanců e-mailem, ve kterém jsou tito vyzýváni ke kliknutí na odkaz v e-mailu anebo přílohy v něm uvedené. Kvalita těchto e-mailů se může podstatně lišit, v rámci vyšetřování bezpečnostních incidentů tohoto typu v posledních letech byly zaznamenány kampaně, kde se obětí stali i bezpečnostní experti a specialisté, což vypovídá o vysoké nebezpečnosti a kvalitě těchto útoků, které byly v souladu s metodikou hodnocení míry nebezpečnosti phishingových útoků[147] hodnoceny jako kritické.

Více jak dvě třetiny respondentů (65 %) se s touto technikou nesetkalo vůbec, a čtvrtina (26 %) se s ní pak setkává opakovaně. Zde nelze argumentovat tím, že by se organizace s tímto typem útoku nesetkala proto, že by byl předmětný e-mail zastaven v perimetru dříve, než by byl doručen, protože pak by se nejednalo s největší pravděpodobností o spear phishing, ale obyčejný phishing. Daleko spíš lze předpokládat, že tyto cílené útoky jsou vedeny jen na některé organizace a pokud má útočník zájem do dané organizace proniknout, tak se o to pokouší opakovaně.

Objevují se zde rozdíly mezi organizacemi nad 250 osob a do 250 osob. Jestli se v první skupině více jak polovina (55 %) respondentů s tímto útokem nesetkala vůbec, tak ve druhé skupině to byly dokonce téměř tři čtvrtiny (74 %) respondentů.

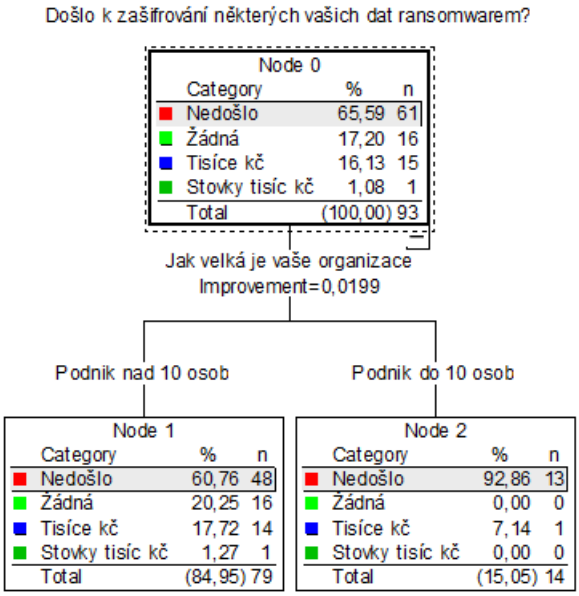
[147] ČERMÁK, Miroslav. Metodika hodnocení míry nebezpečnosti. *Hoax.cz* [online]. [cit. 08.06.2020]. Dostupné z: https://hoax.cz/cze/metodika-hodnoceni-miry-nebezpecnosti/

Bez povšimnutí také nemůžeme nechat skutečnost, že v podniku nad 250 osob se s tímto typem útoku respondenti setkávají opakovaně (43 %), zatímco v podniku do 250 osob se opakovaně s tímto útokem setkává výrazně méně respondentů (8 %).

To si lze vysvětlit tak, že v menší organizaci se informace o tom, že zde proběhl nějaký spear phishing šíří mnohem rychleji a je možné všechny zaměstnance lépe seznámit s tím, co se stalo, a útočník si proto s opakováním útoku dává na čas. Další důvod pak může být ten, že je zde omezený počet zaměstnanců, na které lze cílit.

Obrázek 14 – Vliv ID03-P33 zachycuje vztah mezi velikostí podniku a kybernetickým útokem spočívajícím v zašifrování dat.

Obrázek 14 – Vliv ID03-P33



Došlo k zašifrování některých vašich dat ransomwarem?	Jak velká je vaše organizace				
	Podnik do 10 osob	Podnik nad 10 osob	celkem	medián	dorvar
Nedošlo	+	-	61	1,865	,335
Žádná	o	o	16	2,000	,000
Tisíce kč	o	o	15	1,964	,124
Stovky tisíc kč	o	o	1	2,000	,000
celkem	14	79	93	1,911	,256

Hodnota koeficientu beta je 0,061 s 95% intervalem spolehlivosti (0,001; 0,119), (střední věcně významná asociace) Symetrický Cohenův index w = 0,248 (téměř střední věcně významný efekt)

Otázka týkající se zašifrování data ransomwarem odhalila, že navzdory tvrzení médií, že ransomware představuje největší hrozbu, tak u téměř dvou třetin (66 %) organizací k žádnému spuštění ransomware nedošlo, u necelé pětiny (17 %) nedošlo k žádné škodě a u téměř stejného počtu organizací (16 %) došlo jen ke škodě v řádu tisíců a u pouhého procenta (1 %) se škoda pohybovala ve výši stovek tisíc korun.

To může znamenat, že tyto útoky nejsou až tak časté, jsou detekovány včas a organizace mají zavedeny efektivní postupy. Ukázalo se také, že výše škody do určité míry závisí na velikosti organizace, neboť organizace nad deset zaměstnanců reportují škodu v řádech tisíců (18 %) oproti (7 %) organizacím do deseti zaměstnanců, což dává smysl, protože:

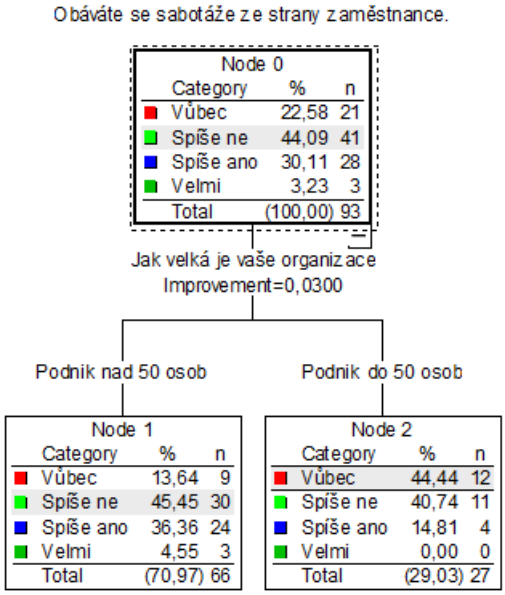
- cena za výkupné byla fixní, uvedená v bitcoinech a v možnostech organizace ji zaplatit;
- čím větší je organizace, tím více má zaměstnanců a výpočetní techniky a tím více zařízení může být v případě úspěšného napadení zašifrováno, a tedy i dat na nich;
- to v konečném výsledku vede ke zvýšení nákladů na obnovu dat, která se odvíjí od množství zašifrovaných dat a dostupnosti záloh, přičemž zašifrovány mohou být i poslední zálohy;
- v okamžiku, kdy nejsou k dispozici zálohy, ze kterých by se dala data obnovit, tak se tato data musí pořídit a zpracovat znovu.

Nemusí tomu tak však být i nadále, protože z rozhovoru s některými bezpečnostními experty vyplynulo, že i u nás se začínají objevovat útoky, kdy útočník v okamžiku, kdy zjistí, kdo se stal obětí, tak zvyšuje cenu výkupného a snaží se smlouvat[148] a je možné, že i výše výkupného se může do budoucna odvíjet od postavení daného subjektu na trhu.

[148] HALLER, Martin. Jak vypadá vyjednávání o výkupném u ransomware. *Martin Haller* [online]. 11. květen 2020 [cit. 08.06.2020]. Dostupné z: https://martinhaller.cz/ransomware/jak-vypada-vyjednavani-o-vykupnem-u-ransomware/

Obrázek 15 – Vliv ID03-P50 zachycuje vztah mezi velikostí podniku a obavy ze sabotáže ze strany zaměstnance.

Obrázek 15 – Vliv ID03-P50



Obáváte se sabotáže ze strany zaměstnance.	Jak velká je vaše organizace				
	Podnik do 50 osob	Podnik nad 50 osob	celkem	medián	dorvar
Vůbec	++	--	21	1,375	,490
Spíše ne	o	o	41	1,817	,393
Spíše ano	-	+	28	1,917	,245
Velmi	o	o	3	2,000	,000
celkem	27	66	93	1,795	,412

Hodnota koeficientu beta je 0,133 s 95% intervalem spolehlivosti (-0,008; 0,273), (téměř velká věcně významná asociace) Symetrický Cohenův index w = 0,364 (více než střední věcně významný efekt)

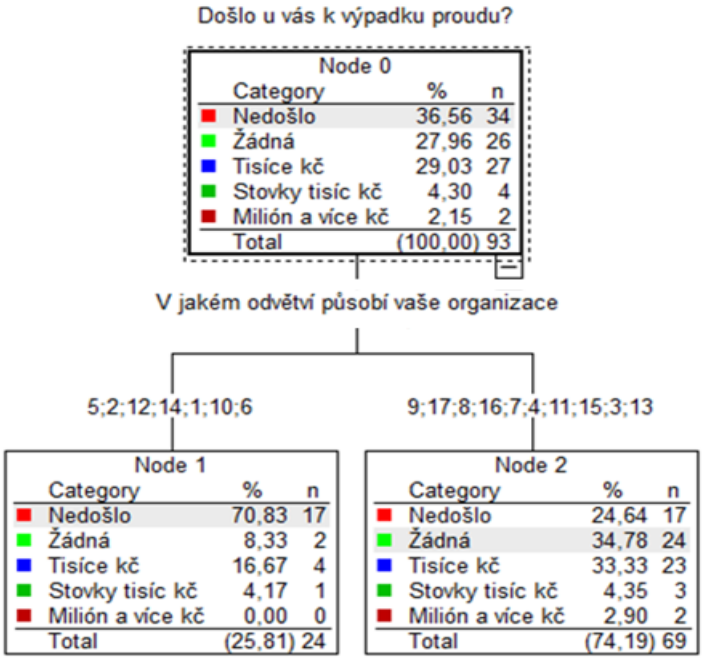
Obava týkající se sabotáže ze strany vlastního zaměstnance je větší ve velkých a střednících organizacích než v malých podnicích a mikropodnicích. To může být dáno mimo jiné tím, že:

- zaměstnanci mikropodniků a malých podniků mají větší pocit sounáležitosti s podnikem, jsou často rodinnými příslušníky, podílníky a jsou na existenci podniku životně závislí, mezi sebou se lépe znají a důvěřují si, a tudíž se sabotáže tak neobávají.

- velké a střední podniky často uvádí vyšší míru fluktuace, nižší loajalitu zaměstnanců a rovněž na tuto otázku odpovídá bezpečnostní manažer, který zpravidla jednotlivé zaměstnance nezná, a tak na ně nahlíží s jistou dávkou nedůvěry.

Obrázek 16 – P23-odvětví zachycuje, v jakém odvětví došlo k výpadku proudu a jaká vznikla organizaci škoda.

Obrázek 16 – P23-odvětví



Došlo u vás k výpadku proudu?	V jakém odvětví působí vaše organizace				
	První skupina	Druhá skupina	celkem	medián	dorvar
Nedošlo	+++	---	34	1,500	,500
Žádná	-	+	26	1,958	,142
Tisíce kč	o	o	27	1,913	,252
Stovky tisíc kč	o	o	4	1,833	,375
Milión a více kč	o	o	2	2,000	,000
celkem	24	69	93	1,826	,383

Hodnota koeficientu beta je 0,185 s 95% intervalem spolehlivosti (0,028; 0,343); (velká věcně významná asociace)[149] Symetrický Cohenův index w = 0,431 (více než střední věcně významný efekt)

[149] Pod každým klasifikačním stromem je umístěna tabulka, která prostřednictvím křížků (+) ukazuje na dominance dané buňky s ohledem na četnosti zastoupených odpovědí

Výpadky proudu mohou být způsobeny vyšší mocí anebo se může jednat o následky cílených kybernetických útoků vedených na kritickou infrastrukturu státu a provozovatele přenosových soustav energie, na kterých jsou závislé i další organizace, některé více a některé méně. Tyto cílené útoky se přibližují k ČR, naposledy byly zaznamenány např. útoky na ENTSO-E.[150]

S výpadkem proudu se setkaly téměř dvě třetiny respondentů. Více jak čtvrtina (28 %) nezaznamenala žádnou ztrátu, ale další více jak čtvrtina (29 %) zaznamenala ztrátu ve výši několika tisíc korun, jen pár jednotek procent respondentů zaznamenalo ztrátu ve výši několika stovek tisíc (4 %) a více než milión (2 %) korun. Z výše uvedeného vyplývá, že výpadek proudu není hrozba, kterou by většina organizací musela okamžitě řešit, přesto tato hrozba představuje pro několik procent organizací hrozbu, která jim může způsobit poměrně vysokou škodu.

Ještě zajímavější pohled přináší výše uvedený strom, ze kterého je patrné, že některé organizace spadající do odvětví uvedených v Node 1 výpadek proudu nezaznamenaly vůbec (71 %) anebo jejich škoda byla minimální a naproti tomu z organizací, které spadají do odvětví uvedených v Node 2, nezaznamenala výpadek jen přibližně čtvrtina z nich (25 %), což může být dáno tím, že jejich citlivost na výpadek proudu je vzhledem k povaze jejich činnosti vyšší a rovněž vyšší je i podíl organizací, které utrpěly škodu ve výši několika tisíc korun (33 %) a pár procent z nich (3 %) pak dokonce škodu vyšší než milión korun.

V dalším výzkumu by bylo vhodné se zaměřit i na příčiny těchto výpadků, a zda byla přijata vhodná opatření k minimalizaci škod.

---

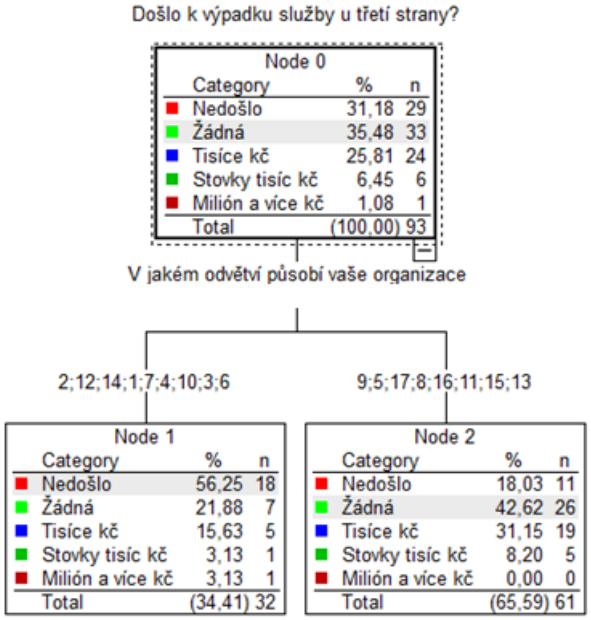
a prostřednictvím znamének (-) naopak jejich inhibici (nedostatek). Značka (+++) značí velký přebytek daného typu odpovědí a (---) velký nedostatek daného typu odpovědí.

[150] OWAIDA, Amer. European power grid organization hit by cyberattack. *WeLiveSecurity* [online]. 12. březen 2020 [cit. 04.06.2020]. Dostupné z: https://www.welivesecurity.com/2020/03/12/european-power-grid-organization-entsoe-cyberattack/

P24 – Došlo k výpadku služby u třetí strany?

Obrázek 17 – P24-odvětví zachycuje, jakou ztrátu utrpěly organizace spadající do jednotlivých odvětví v důsledku výpadku služeb třetí strany.

Obrázek 17 – P24-odvětví



Došlo k výpadku služby u třetí strany?	V jakém odvětví působí vaše organizace				
	První skupina	Druhá skupina	celkem	medián	dorvar
Nedošlo	+++	---	29	1,533	,499
Žádná	o	o	33	1,911	,257
Tisíce kč	o	o	24	1,900	,278
Stovky tisíc kč	o	o	6	1,900	,278
Milión a více kč	o	o	1	2,000	,000
celkem	24	69	93	1,826	,383

Hodnota koeficientu beta je 0,121 s 95% intervalem spolehlivosti (-0,021; 0,264); (spíše velká věcně významná asociace) Symetrický Cohenův index w = 0,429 (více než střední věcně významný efekt)

Tak, jak je stále více činností outsourcováno, tak se organizace stávají více závislé na třetích stranách, které se rovněž stávají obětí kybernetických útoků, a počet těchto útoků roste. Výpadek jejich služeb pak může mít negativní dopad na jejich podnikání, a to podle toho, jak se činnost, kterou třetí strana vykonává, podílí na samotném hodnototvorném řetězci dané organizace.

Téměř jedna třetina (31 %) organizací se s výpadkem služeb třetí strany nesetkala, další více jak třetina (36 %) se s ním setkala, ale neutrpěla žádnou škodu a přibližně čtvrtina (26 %) pak utrpěla škodu ve výši několika tisíc korun. Jen pár procent organizací pak utrpělo škodu ve výši stovek tisíc (7 %) a jedno procento (1 %) pak škodu větší než jeden milión korun.

Když se podíváme, jakých organizací se toto týkalo, tak zjistíme, že zde máme organizace působící v odvětvích uvedených v Node 1, které jsou na třetích stranách závislé minimálně, více jak polovina z nich se s výpadkem služeb nesetkala (56 %), neutrpěla žádnou škodu (22 %) anebo se škoda pohybovala v řádu tisíců (16 %), případně pak u pár procent organizací (3 %) ve stovkách tisíc (3 %) nebo v miliónech (3 %).

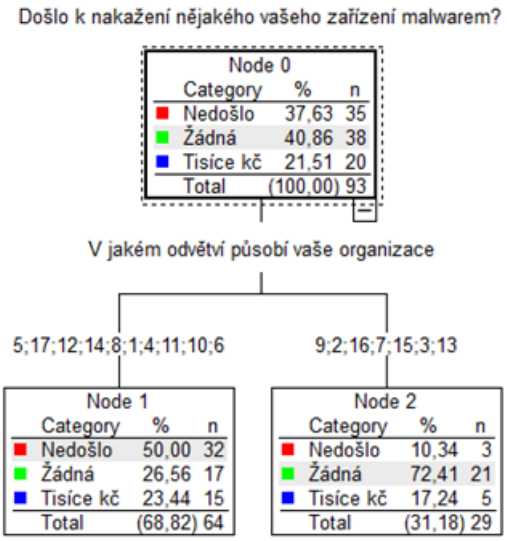
Organizace působící v odvětvích uvedených v Node 2 na tom byly, co se týče závislosti a škod, podstatně hůře. Jen necelá pětina (18 %) se s výpadkem služeb třetí strany nesetkala vůbec. A byť více jak dvě pětiny neutrpěly žádnou škodu (42 %), tak to na druhou stranu znamená, že k výpadku došlo, ale nebyl tak dlouhý anebo byla přijata odpovídající opatření k eliminaci škod, avšak téměř třetina organizací (31 %) utrpěla škodu ve výši několika tisíc korun a necelá desetina (8 %) pak dokonce ve výši několika stovek tisíc korun.

Výpadek služeb třetích stran nemusí být způsoben následkem kybernetického útoku, a přesto může způsobit značnou škodu. V dalším výzkumu by bylo vhodné se zaměřit i na příčiny těchto výpadků, a zda byla přijata vhodná opatření k minimalizaci škod.

P32 – Došlo k nakažení nějakého vašeho zařízení malwarem?

Obrázek 18 – P32-odvětví zachycuje, v jakém odvětví utrpěly organizace škodu v důsledku napadení malwarem.

Obrázek 18 – P32-odvětví



Došlo k nakažení nějakého vašeho zařízení malwarem?	V jakém odvětví působí vaše organizace				
	První skupina	Druhá skupina	celkem	medián	dorvar
Nedošlo	+++	---	35	1,047	,157
Žádná	---	+++	38	1,595	,494
Tisíce kč	o	o	20	1,167	,375
celkem	64	29	93	1,227	,429

Hodnota koeficientu beta je 0,204 s 95% intervalem spolehlivosti (0,048; 0,359); (velká věcně významná asociace) Symetrický Cohenův index w = 0,452 (více než střední věcně významný efekt)

Hrozba nákazy generickým malwarem, obzvláště v případě plošně vedených útoků, se nevyhýbá žádné organizaci, nicméně více jak třetina (38 %) organizací byla schopna se malware úspěšně ubránit a detekovat jej, takže ke kompromitaci koncového zařízení nakonec nedošlo. Dvě pětiny (41 %) organizací pak byly napadeny, ale malware jim nezpůsobil žádnou škodu a více jak pětina (22 %) pak utrpěla škodu v řádu tisíců korun, což odpovídá minimálním nákladům na odstranění malware a obnovu koncového zařízení a dat a vyžaduje mít zavedený vyzrálý proces a funkční systém zálohy a obnovy dat.

Až polovina (50 %) organizací působících v odvětví uvedených v Node 1 byla schopna útok zastavit v počátku a v pozdější fázi pak více jak čtvrtina (27 %) z nich a necelá čtvrtina (23 %) pak utrpěla škodu ve výši tisíců korun.

Jen desetina organizací působících v odvětví uvedených v Node 2 zastavila útok již v počátku a téměř tři čtvrtiny (72 %) teprve až v další fázi, ale i to je dobrý výsledek, nicméně část z nich rovněž utrpěla škodu (17 %) v řádu tisíců.

Vidíme, že byť se tyto dvě skupiny organizací liší především v tom, v jaké fázi jsou schopny zachytit útok, tak obě skupiny utrpěly škodu v řádu tisíců korun, a že i generický malware může stále způsobit nějakou škodu, byť nepatrnou, a proto má antimalware řešení stále smysl.

Z rozhovoru s bezpečnostními experty, kteří situaci v kyberprostoru sledují od roku 2012, dále vyplynulo, že nejúčinnější jsou v tomto případě řešení od českých výrobců, která jsou schopna detekovat plošně vedené útoky na české uživatele, především díky vysoké tržní penetraci a schopnosti včas detekovat a reagovat na malware, který se na našem území aktuálně šíří a to v řádu hodin, maximálně jednotek dnů, zatímco řešení zahraniční provenience jsou schopny stejný malware detekovat až po několika dnech a v mnoha případech až po týdnu.

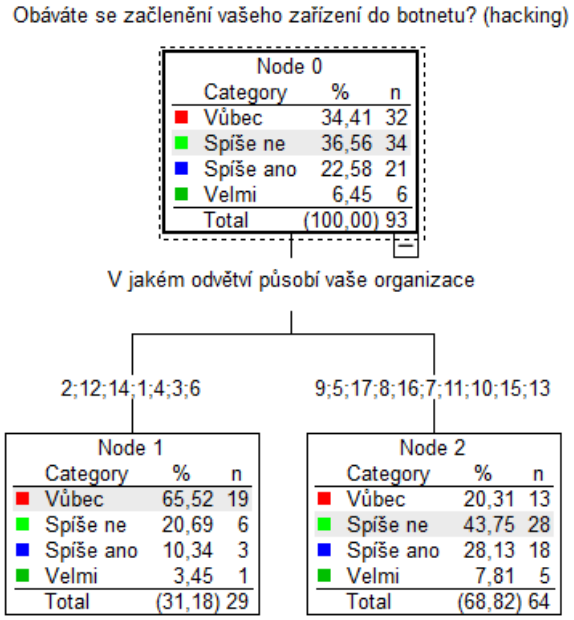
Dílčí zjištění

Pokud jde o hrozby a způsobené škody zkoumané v rámci tohoto výzkumu, tak z rozhovoru s manažery informační bezpečnosti dále vyplynulo, že neví, jak přesně mají škodu počítat, a že způsob výpočtu škody se organizace od organizace liší.

P45 – Obáváte se začlenění vašeho zařízení do botnetu? (hacking)

Obrázek 19 – P45-odvětví zachycuje organizace, v jakých odvětvích se obávají hrozby začlenění jejich zařízení do botnetu.

Obrázek 19 – P45-odvětví



Obávát se se začlenění vašeho zařízení do botnetu? (hacking)	V jakém odvětví působí vaše organizace				
	První skupina	Druhá skupina	celkem	medián	dorvar
Vůbec	+++	---	32	1,559	,498
Spíše ne	o	o	34	1,914	,251
Spíše ano	o	o	21	1,917	,245
Velmi	o	o	6	1,900	,278
celkem	24	69	93	1,826	,383

Hodnota koeficientu beta je 0,122 s 95% intervalem spolehlivosti (-0,02; 0,263); (spíše velká věcně významná asociace) Symetrický Cohenův index w = 0,442 (více než střední věcně významný efekt)

V okamžiku, kdy je zařízení začleněno do botnetu, a tato hrozba vzrostla, neboť oproti roku 2018 reportuje např. Spamhaus nárůst C&C serverů o 72 %, tak může být pronajato nejen k dalšímu útoku, ale např. i k průmyslové špionáži, jak uvádí Bederna[151], a ve výsledku může organizace utrpět značnou škodu. Více jak třetina (34 %) organizací se této hrozby neobává vůbec, spíše ne (37 %), spíše ano (23 %) a velmi se obávají jen pouhá procenta (7 %) organizací.

Zajímavé je, že z organizací působících v odvětvích uvedených v Node 1, se této hrozby vůbec neobávají téměř dvě třetiny (66 %) organizací, spíše ne pak

[151] BEDERNA, Zsolt a Tamas SZADECZKY. Cyber espionage through Botnets. *Security Journal* [online]. 2020, roč. 33, č. 1. ISSN 0955-1662, 1743-4645. DOI: 10.1057/s41284-019-00194-6 s. 43–62

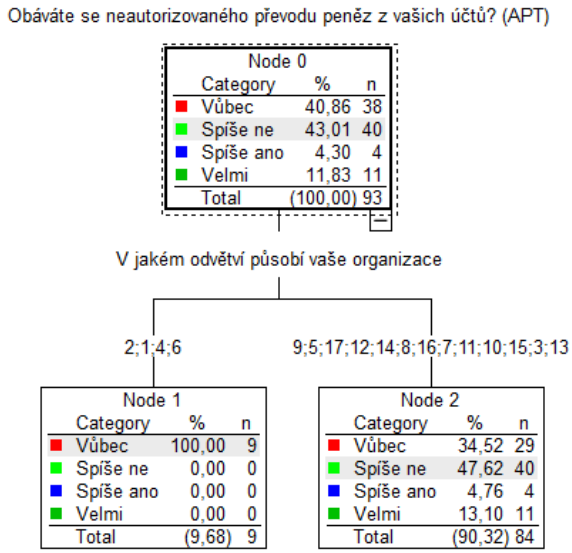
pětina organizací (21 %), spíše ano pak desetina (10 %) a velmi se obává jen pár procent (3 %) organizací. Z organizací spadajících do odvětví národního hospodářství uvedených v Node 2 se této hrozby vůbec neobává jen pětina (20 %) z nich, spíše ne pak více jak dvě pětiny (44 %), spíše ano pak téměř třetina (28 %) a velmi jen několik málo procent (8 %).

Skutečnost, že se druhá skupina obává začlenění do botnetu více, je dáno nejspíš tím, že si uvědomují, že by ji tato skutečnost mohla poškodit, což vzhledem k předmětu jejich činností dává smysl.

P47 – Obáváte se neautorizovaného převodu peněz z vašich účtů? (APT)

Obrázek 20 – P47-odvětví zachycuje obavu organizací v jednotlivých odvětví z neautorizovaného převodu peněz z jejich účtů.

Obrázek 20 – P47-odvětví



Obáváte se neautorizovaného převodu peněz z vašich účtů? (APT)	V jakém odvětví působí vaše organizace				
	První skupina	Druhá skupina	celkem	medián	dorvar
Vůbec	+	-	38	1,674	,478
Spíše ne	o	o	40	1,894	,289
Spíše ano	o	o	4	1,833	,375
Velmi	o	o	11	1,950	,165
celkem	24	69	93	1,826	,383

Hodnota koeficientu beta je 0,073 s 95% intervalem spolehlivosti (-0,031; 0,176); (více než střední věcně významná asociace) Symetrický Cohenův index w = 0,394 (více než střední věcně významný efekt)

Neautorizovaný převod finančních prostředků se řadí spolu s kompromitací systému a jeho ovládnutím a ransomware k hrozbám, které mohou způsobit největší škodu. K masivním útokům na klienty největších českých bank, kterými jsou jak domácnosti, tak i firmy, dochází od roku 2013, a že počty těchto útoků rostou, uvádí i Česká bankovní asociace.[152]

Dvě pětiny organizací se přesto této hrozby neobávají vůbec (41 %) anebo spíše ne (43 %) a spíše ano se obává jen pár jednotek procent (4 %) a velmi se obává přibližně desetina (12 %). Zajímavější však je, jak se liší obavy podle odvětví, do jakého tyto organizace patří. Všechny organizace uvedené v Node 1 nemají obavu vůbec (100 %), zatímco pokud jde o organizace uvedené v Node 2, tak se této hrozby vůbec neobává více jak třetina organizací (35 %), spíše ne pak téměř polovina (48 %) a spíše ano jednotky procent (5 %) a velmi se této hrozby obává více jak desetina organizací (13 %).

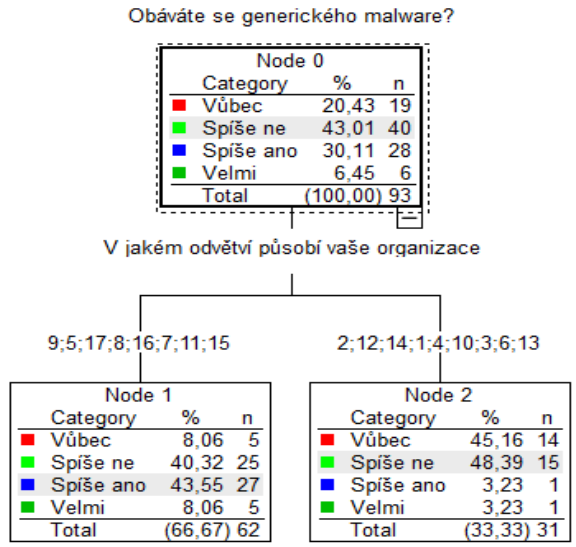
Tuto skutečnost si vysvětlujeme tím, že organizace spadající do první skupiny se s tímto útokem doposud nesetkaly a neví ani o tom, že by se obětí staly nějaké jiné organizace působící ve stejném odvětví. Mezi manažery stále převládá názor, že se jedná o cílené útoky, nikoliv o plošné.

[152] Kyberbezpečnost a index bezpečnosti 2019. *Česká bankovní asociace* [online]. [cit. 04.06.2020]. Dostupné z: https://cbaonline.cz/kyberbezpecnost-a-index-bezpecnosti-2019

P48 – Obáváte se generického malware?

Obrázek 21 – P48-odvětví zachycuje obavu organizací v jednotlivých odvětví z generického malware.

Obrázek 21 – P48-odvětví



Obáváte se generického malware?	V jakém odvětví působí vaše organizace				
	První skupina	Druhá skupina	celkem	medián	dorvar
Vůbec	---	+++	19	1,821	,388
Spíše ne	o	o	40	1,300	,469
Spíše ano	+++	---	28	1,019	,069
Velmi	o	o	6	1,100	,278
celkem	62	31	93	1,250	,444

Hodnota koeficientu beta je 0,281 s 95% intervalem spolehlivosti (0,122; 0,44); (velká věcně významná asociace) Symetrický Cohenův index w = 0,530 (velký věcně významný efekt)

Generického malware se velmi obává jen pár procent organizací (7 %), spíše ano pak téměř třetina (30 %), spíše ne více jak dvě pětiny (43 %) a vůbec pak pětina (20 %). Skutečnost, že dvě třetiny organizací se generického malware neobávají si lze vysvětlit tak, že si již na něj zvykly, neboť se s generickým malwarem setkávají po celou dobu své existence.

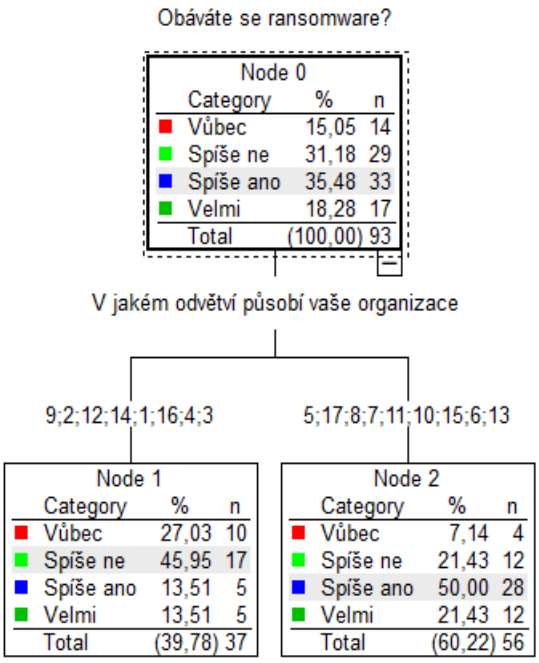
Vyprofilovaly se zde však dvě skupiny organizací, které se podstatně liší v tom, jak vnímají obavu z generického malware. Organizace uvedené v Node 1 se generického malware neobávají vůbec, jen v několika málo procentech (8 %). Organizací uvedených v Node 2, které se vůbec neobávají generického malware,

je mnohonásobně více (45 %), což si lze vysvětlit tak, že se necítí býti ohroženi generickým malwarem, neboť jsou přesvědčeni, že se jich tento problém buď netýká anebo že jsou vůči němu dostatečně chráněni pomocí stávajících bezpečnostních opatření.

P49 – Obáváte se ransomware?

Obrázek 22 – P49-odvětví zachycuje, jak se liší obava z ransomware dle odvětví.

Obrázek 22 – P49-odvětví



Obáváte se ransomware?	V jakém odvětví působí vaše organizace: První skupina	Druhá skupina	celkem	medián	dorvar
Vůbec	+++	---	14	1,200	,408
Spíše ne	o	o	29	1,841	,366
Spíše ano	-	+	33	1,931	,213
Velmi	o	o	17	1,893	,291
celkem	24	69	93	1,826	,383

Hodnota koeficientu beta je 0,205 s 95% intervalem spolehlivosti (0,017; 0,393); (velká věcně významná asociace) Symetrický Cohenův index w = 0,455 (téměř velký věcně významný efekt)

Ransomware představuje nebezpečí pro každou organizaci, protože každá organizace spravuje osobní údaje svých zaměstnanců anebo klientů, a především pak pro ty organizace, které nemají fyzicky oddělené zálohy od sítě a netestují je. Obava z ransomware je obecně větší než z generického malware, neboť zde si již

většina respondentů dovede představit nejhorší možnou škodu, která by jejich organizacím mohla vzniknout, a také škoda z ransomware je zpravidla výrazně vyšší, než z ostatního generického malware.

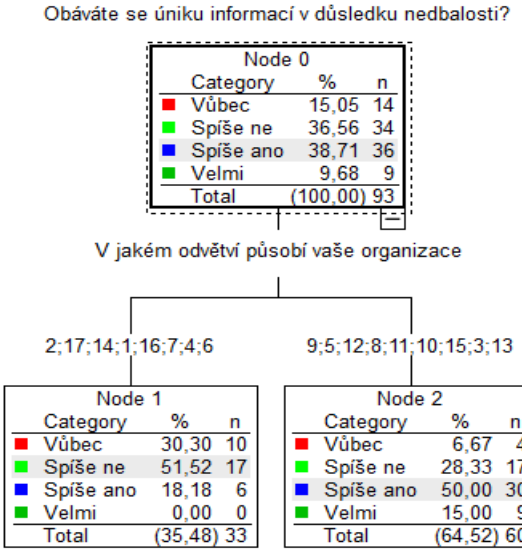
Ransomware se velmi obává téměř pětina organizací (18 %) a spíše ano pak více jak třetina (36 %). Vznikly zde dvě skupiny organizací s rozdílným vnímáním této hrozby. Organizace uvedené v Node 1 se ransomware obávají výrazně více, polovina (50 %) se vyjádřila, že spíše ano a velmi pak více jak pětina (21 %), zatímco ve druhé skupině organizací uvedených v Node 2 se jen více jak desetina organizací (14 %) vyjádřila spíše ano nebo velmi (14 %).

Vysvětlujeme si to tím, že organizace spadající do druhé skupiny jsou organizace, které se již v minulosti s ransomware setkaly anebo se s ním setkaly v době vyplňování dotazníku, a tak byly touto skutečností silně ovlivněny stejně jako zprávami v médiích, které o této hrozbě rovněž informovaly.

P53 – Obáváte se úniku informací v důsledku nedbalosti?

Obrázek 23 – P53-odvětví zachycuje, v jakém odvětví se organizace nejvíce obávají úniku informací v důsledku nedbalosti.

Obrázek 23 – P53-odvětví



Obáváte se úniku informací v důsledku nedbalosti?	V jakém odvětví působí vaše organizace				
	První skupina	Druhá skupina	celkem	medián	dorvar
Vůbec	++	--	14	1,200	,408
Spíše ne	+	-	34	1,500	,500
Spíše ano	--	++	36	1,900	,278
Velmi	-	+	9	2,000	,000
celkem	33	60	93	1,725	,458

Hodnota koeficientu beta je 0,232 s 95% intervalem spolehlivosti (0,078; 0,386); (velká věcně významná asociace) Symetrický Cohenův index w = 0,481 (téměř velký věcně významný efekt)

Pokud jde o únik informací z nedbalosti, tak zde se této hrozby obává téměř polovina respondentů, spíše ano více jak třetina (39 %) a velmi pak necelá desetina (10 %).

Z odpovědí jednotlivých respondentů vyplývá, že se zde vyprofilovaly dvě skupiny organizací. V první skupině, do které patří organizace uvedené v Node 1, se této hrozby neobává vůbec celá třetina (30 %) respondentů a spíše ne pak více jak polovina (52 %) respondentů. Naproti tomu ve druhé skupině, kam lze zařadit organizace uvedené v Node 2, se jen pouhých několik procent (7 %) z nich této hrozby neobává vůbec a necelá třetina respondentů (28 %) spíše ne.

Důvod, proč tomu tak je, si vysvětlujeme tím, že druhá skupina organizací disponuje know-how a informacemi, které mají na trhu větší hodnotu, a tudíž i jejich obava je větší. Detailní pohled na data přináší Příloha K – Opatření, útoky, vektory, škody a obavy.

3.2.6 Výsledky výzkumu

Na základě analýz uvedených v předchozí kapitole a rovněž analýz, které obsahuje Příloha K – Opatření, útoky, vektory, škody a obavy, je možné odpovědět, zda lze jednotlivé výzkumné předpoklady zamítnout anebo potvrdit a rovněž odpovědět i na výzkumné otázky.

Z výsledků výzkumu vyplývá, že **organizace v ČR se setkávají s kybernetickými útoky bez ohledu na to, do jakého patří sektoru** (veřejný, soukromý) jaká je jejich velikost (mikro, malý, střední, velký) anebo jaká je kritičnost jimi provozovaného systému (KII, VIS, SZS, žádný) a podstatnou roli dokonce nehraje ani odvětví, ve kterém organizace působí.

Všechny organizace však čelily jednotlivým kybernetickým útokům alespoň jednou a většina z nich se s nimi potýkala během roku opakovaně a některé i soustavně. **Spíš než o cílených útocích na organizace působící v konkrétním odvětví lze však hovořit o útocích plošných.** Při těchto útocích se stávají obětmi organizace, které nezavedly vhodná bezpečnostní opatření, resp. provozují systém, který trpí aktuálně zneužívanými zranitelnostmi.

Ztráty vyplývající z těchto útoků se pohybovaly ve většině případů v jednotkách tisíc, ale výjimkou nebyly ani ztráty v řádech stovek tisíc a v některých případech pak přesahující i milión korun, přičemž některé organizace čelily hned několika různým útokům a utrpěly značnou finanční ztrátu.

Dále se ukázalo, že **organizace by se měly spíše než kybernetických útoků obávat škod vyplývajících z nedostupnosti systému,** a to ať už v důsledku výpadku proudu, selhání vlastního hardware anebo problémů u poskytovatele, a stejně tak by se měly obávat krádeže dat ze strany vlastního zaměstnance anebo třetí strany, které jsou nejen mnohem častější, ale způsobují i výrazně vyšší škodu. Bez zajímavosti také není, že největší škodu může způsobit očerňující kampaň na internetu.

Pokud jde o úroveň zavedených bezpečnostních opatření, tak lze konstatovat, že ji nelze vůbec považovat za uspokojivou, neboť **většina organizací není dostatečně chráněna** nejen před pokročilými hrozbami, které se sice objevují jen zřídka, ale dokážou způsobit značnou škodu, ale není chráněna ani před hrozbami, které se ukazují jako mnohem pravděpodobnější a mají větší potenciál způsobit škodu.

Na druhou stranu je nutné konstatovat, že **organizace, kterou jsou povinny zavést bezpečnostní opatření organizační a technické povahy, tak jsou na tom, co do zavedení těchto opatření lépe** než organizace, které pod působnost Zákona o kybernetické bezpečnosti nespadají, obzvlášť pokud jde o opatření, která by organizace měla ochránit před APT útoky.

1. **Základní bezpečnostní opatření jsou zavedena všude.**

   Ukázalo se, že základní sada bezpečnostních opatření není zdaleka všude zavedena a mezi organizacemi jsou značné rozdíly, a proto by mělo být zavedení jednotlivých opatření dále hodnoceno.

   Výzkumný předpoklad je možné zamítnout.

2. **Čím větší je organizace, tím vyšší úrovně bezpečnosti dosahuje.**

   Ve všech 4 skupinách (mikro, malé, střední, velké) lze nalézt organizace, které bezpečnost podceňují a nezavedly ani základní sadu bezpečnostních opatření a stejně tak lze narazit na organizace, které si uvědomují závažnost hrozeb a zavedly všechna důležitá bezpečnostní opatření. Dalo by se očekávat, že větší organizace budou mít dostatek finančních prostředků, aby mohly zavést odpovídající bezpečnostní opatření. Z analýzy dat nicméně vyplývá, že tento předpoklad neplatí ani u jednoho posuzovaného opatření. Z interview s respondenty dále vyplynulo, že některým CISO se nedaří management přesvědčit o tom, že by měl hrozbu přicházející z kyberprostoru považovat za reálnou a uvolnit rozpočet na zavedení příslušných bezpečnostních opatření. Naproti tomu malá organizace, která má omezené množství prostředků, může být v některých případech, co do zavedení vybraných bezpečnostních opatření na vyšší úrovni, protože její informační systém není tak komplexní a rovněž její

organizační struktura je spíše jednoduchá, což managementu umožňuje některá bezpečnostní opatření snáze prosadit a implementovat.

Výzkumný předpoklad je možné zamítnout.

3. To, zda organizace působí v soukromém nebo veřejném sektoru rozhoduje o tom, jaká je skutečná úroveň bezpečnosti.

Jak ve státním, tak i soukromém sektoru lze nalézt organizace, které bezpečnost podceňují a nezavedly ani základní sadu bezpečnostních opatření, a stejně tak lze narazit na organizace, které si uvědomují závažnost hrozeb a zavedly všechna důležitá bezpečnostní opatření. Z analýzy dat vyplývá, že organizace působící v soukromém sektrou by na tom mohly být z pohledu zavedených bezpečnostních opatření o něco lépe, ovšem i zde lze narazit na opatření, kde tomu tak zdaleka není. Rovněž z pohledu věcné významnosti zde není patrná závislost mezi sektorem a zavedenými bezpečnostními opatřeními.

Výzkumný předpoklad je možné zamítnout.

4. Kritické systémy jsou vždy lépe zabezpečeny než systémy, které jako kritické označeny nejsou.

Celkově jsou na tom kritické systémy o něco lépe, ovšem není tomu tak ve všech případech. Z pohledu věcné významnosti zde lze nalézt též jen několik bezpečnostních opatření, kde jsou na tom kritické systémy výrazně lépe a je zde patrná určitá závislost.

Výzkumný předpoklad je možné zamítnout.

5. Působení organizace v daném odvětví určuje i úroveň její bezpečnosti.

Ve všech odvětvích lze nalézt organizace, které bezpečnost podceňují a nezavedly ani základní sadu bezpečnostních opatření a stejně tak lze narazit na organizace, které si uvědomují závažnost hrozeb a zavedly všechna důležitá bezpečnostní opatření. Byť relativní četnost organizací v jednotlivých odvětvích zcela neodpovídá jejich rozdělení v základním souboru, lze si všimnout, že v zásadě nejsou až na jeden případ mezi odvětvími výrazné rozdíly.

Výzkumný předpoklad je možné zamítnout.

6. Čím větší je organizace, tím je na ni vedeno více útoků.

Téměř všechny organizace se setkaly s určitými typy útoků během uplynulého roku alespoň jednou. To, zda se organizace dle počtu zaměstnanců řadí mezi mikro, malé, střední nebo velké, však nemá bezprostřední vliv na to, zda na ni bude veden větší počet útoků. Odpověď na otázku, co způsobuje vyšší počet některých typů útoků reportovaných velkými organizacemi, by mohla být předmětem další analýzy.

Výzkumný předpoklad je možné zamítnout.

7. To, zda organizace působí v soukromém nebo veřejném sektoru, rozhoduje o tom, zda na ní bude veden větší počet útoků.

Na oba typy organizací bylo vedeno přibližně stejné množství útoků. V čem se oba sektory v některých případech liší, jsou typy detekovaných útoků, ovšem věcně významný vztah byl nalezen jen u několika z nich.

Výzkumný předpoklad je možné zamítnout.

8. Čím významnější systém organizace provozuje, tím více je na něj vedeno útoků.

Z výzkumu vyplývá, že zde není patrná silná závislost mezi významností/kritičností systému z pohledu ZoKB a počtem útoků. Jinými slovy, to, že se jedná o systém kritický, významný nebo systém základních služeb automaticky neznamená, že je na něj vedeno více útoků. V mnoha případech je tomu i naopak.

Výzkumný předpoklad je možné zamítnout.

9. Působení organizace v daném odvětví zvyšuje počet útoků.

V zásadě všechna odvětví se setkala se stejným typem a vektorem útoku. To, že se v médiích a mnohdy i odborných kruzích setkáváme s názorem, že jsou vedeny cílené útoky na organizace působící v určitém odvětví, je dáno v zásadě dvěma důvody. Prvním je zvýšený zájem o dané odvětví, jeho regulace a nemožnost před veřejností zatajit, že jejich systémy byly napadeny, a druhý

důvod pak spočívá v obdobné architektuře, infrastruktuře a přístupu k řízení bezpečnosti v minulých letech, a tedy i možnosti použít stejný vektor útoku proti více subjektům. Jinými slovy, je objevena nebo dokonce i zveřejněna nová zranitelnost a útočník se jí snaží zneužít, a tak skenuje IP adresní prostor a následně napadá všechny organizace, jejichž systémy danou zranitelností trpí bez ohledu na to, do jakého odvětví daná organizace spadá.

Výzkumný předpoklad je možné zamítnout.

10. Čím významnější systém organizace provozuje, tím větší vzniká škoda v případě útoku.

Z výzkumu vyplývá, že zde není patrná silná závislost mezi významností/kritičností systému z pohledu ZoKB a výší škody v případě úspěšného útoku. Jinými slovy, to, že se jedná o systém kritický, významný nebo systém základních služeb automaticky neznamená, že v případě útoku vzniká větší škoda. Je tomu tak proto, že většina útoků je plošných, nikoliv cílených.

Výzkumný předpoklad je možné zamítnout.

11. Čím vyšší úrovně bezpečnosti organizace dosáhne, tím nižší škodu utrpí.

Závislost mezi implementovanými opatřeními a výší škody nelze prokázat, protože respondenti uvádí, jaká opatření mají zavedena v daný časový okamžik a k jejich zavedení mohlo dojít kdykoliv během roku právě jako reakce na proběhnuvší kybernetický incident nebo útok. Z tohoto důvodu by bylo vhodné tento výzkum zopakovat i v dalším roce, když už bude zřejmé, že dané opatření bylo zavedeno v roce předcházejícím. Pokud by útok proběhl a škoda by přesto vznikla, tak by to potom znamenalo, že dané opatření nebylo účinné, a naopak pokud by útok proběhl a škoda by byla nižší nebo žádná, tak by to znamenalo, že dané opatření bylo účinné a zabránilo vzniku škody.

Výzkumný předpoklad nelze ověřit bez analýzy delší časové řady. To by mělo být předmětem dalšího výzkumu.

Výzkumné otázky

Na základě analýzy dat, která byla provedena v předchozí kapitole, lze zodpovědět následující výzkumné otázky.

VO1: Jaké hrozby, které by mohly narušit bezpečnost organizace, je třeba vzít v úvahu při návrhu vhodných opatření?

V úvahu je třeba vzít hrozby, se kterými se organizace nejčastěji setkávají, kterých se nejvíce obávají a které jim potenciálně mohou způsobit největší škodu. Jedná se o hrozby přicházející zevnitř i zvnějšku organizace, a to jak útoky plošné tak i cílené.

V rámci tohoto výzkumu bylo zjištěno, že největší pozornost je třeba věnovat výpadku proudu a služeb třetích stran, což ale není přímo kybernetická hrozba. Vhodným seskupením hrozeb pak lze redukovat jejich značný počet v souladu s obsahem předchozí kapitoly na malware, únik informací, hacking, DDoS a krádež informací ze strany zaměstnance. Nicméně vzhledem k tomu, že situace v kyberprostoru se velice rychle mění, tak je nutné soustavně vyhodnocovat aktuální hrozby a navrhovat vůči nim vhodná bezpečnostní opatření.

VO2: Jaká bezpečnostní opatření by měla mít organizace zavedena, aby byla co nejlépe ochráněna?

Přestože zavedení základní sady bezpečnostních opatření by mělo představovat minimální náklad, tak ne všechny organizace ji zavedly. Za negativní zjištění lze považovat, že téměř čtvrtina organizací (27 %) stále používá pro přihlášení do počítače slabá hesla. Ačkoli by se mohlo zdát, že když tři čtvrtiny organizací (73 %) používají silná hesla nebo dvoufaktorovou autentizaci, tak je to dobrý výsledek, tak s přihlédnutím ke skutečnosti, že se skutečně jedná o nejstarší bezpečnostní požadavek, tento výsledek nelze považovat za dobrý.

Alarmující je také skutečnost, že třetina organizací (34 %) neřídí striktně přístup k datům, což je druhý nejstarší požadavek, a zaměstnanci se tak dostanou i k datům, ke kterým by se neměli dostat. A nejde jen o to, že by tohoto přístupu mohli zneužít, ale že v okamžiku, kdy dojde k napadení jejich stanice malwarem, tak malware může přistupovat ke stejným datům jako aktuálně přihlášený uživatel.

Rovněž zarážející je, že téměř polovina organizací (49 %) neprovádí účinnou bezpečnostní osvětu svých zaměstnanců, neověřuje účinnost těchto školenía neprovádí ani pravidelné bezpečnostní testy svých systémů (48 %).

Určitou výzvu pak představuje oddělení informačního systému organizace od internetu a pošty, kterou se šíří nejvíce škodlivého kódu, obzvláště když téměř čtyři pětiny (78 %) organizací umožňují svým zaměstnancům přistupovat z koncového zařízení jak do internetu a pošty, tak i do systémů organizace.

Jako pozitivní pak lze hodnotit, že drtivá většina organizací (90 %) pravidelně zálohuje svá data, má nastaveno automatické uzamčení obrazovky po určité době nečinnosti (82 %), polovina (54 %) z nich šifruje data na discích svých koncových zařízení a téměř polovina (46 %) zakazuje svým zaměstnancům spustit na koncových zařízení cokoliv a více jak dvě třetiny (68 %) jsou schopny udržovat své systémy aktuální a nasadit aktualizaci do několika málo týdnů od jejího zveřejnění.

Vůči uvedeným hrozbám by organizace měly zavést sadu opatření, která by jim umožnila zajistit obranu v hloubce. Tato opatření jsou uvedena v kapitole 4.4.

VO3: Má smysl brát při hodnocení velikost organizace, sektor, odvětví, kritičností informačního systému?

Z analýzy dat nevyplynulo, že by zde byl nějaký věcně významný vztah mezi velikostí organizace, sektorem, odvětvím a kritičností informačního systému na jedné straně a úrovní bezpečnosti, typem a počtem útoků a škod na straně druhé, a proto při návrhu metodiky hodnocení bezpečnosti nebudou tyto faktory dále brány v potaz.

4 METODIKA HODNOCENÍ ÚROVNĚ BEZPEČNOSTI ORGANIZACE

Výsledky výzkumu popsaného výše byly použity v rámci návrhu metodiky hodnocení bezpečnosti. Nicméně aby bylo hodnocení bezpečnosti co nejvíce objektivní, měl by **výše popsaný výzkum probíhat každý rok, protože jedině tak lze získat aktuální informace ohledně probíhajících kybernetických útoků** a jejich dopadů a tyto skutečnosti pak promítnout do podoby bezpečnostních opatření, které by měly organizace před těmito kybernetickými útoky chránit.

Po získání odpovědí na to, jakým hrozbám jsou organizace vystaveny, jaké jsou vektory útoku a jaké jsou následky těchto útoků, je nutné **revidovat sadu vhodných bezpečnostních opatření**, které lze nalézt v citovaných normách a které je vhodné připomínkovat v rámci expertní skupiny za použití metody Wideband Delphi, jako tomu bylo i v tomto případě.

Srozumitelnost otázek je následně vhodné otestovat v rámci průzkumu na větším počtu zaměstnanců jedné organizace s požadavkem, aby vyplnili dotazník, který se nachází na určité adrese. Tím, že budou dotazník vyplňovat zaměstnanci stejné organizace, tak by se jejich odpovědi neměly podstatně lišit. Respondentům je vhodné poskytnout i telefonický kontakt na konzultanta, který bude připraven pomoci mu případné dotazy zodpovědět.

Cílem tohoto rychlého průzkumu je **ověřit, zda jsou otázky v dotazníku srozumitelné i pro ty, kteří se bezpečností a informačními technologiemi nezabývají** a lze od nich získat spolehlivé informace o tom, jak je jejich systém zabezpečen. Pokud se tento předpoklad potvrdí, je možné aktualizovanou sadu otázek použít k vlastnímu ohodnocení bezpečnostní úrovně v dané organizaci.

Pokud by u vyhodnocení odpovědí jednotlivých respondentů došlo k výrazným odchylkám, bylo by nutné ověřit, co bylo jejich příčinou a dotazník by musel být opět revidován a otestován na podobném vzorku v jiné organizaci.

Poté co je k dispozici seznam vhodně formulovaných otázek, je možné **oslovit v zásadě libovolného zaměstnance vybrané organizace a nechat jej vyplnit dotazník anebo mu položit sadu otázek**, které jsou uvedeny v kapitole 4.6, a které slouží ke zjištění, zda vybraná sada opatření je v dané organizaci skutečně implementována.

Přestože v rámci výzkumu nebyl identifikován významný vztah mezi velikostí organizace, sektorem, odvětvím a kritičností informačního systému na jedné straně a úrovní bezpečnosti, typem a počtem útoků a škod na straně druhé, bude v metodice hodnocení bezpečnosti organizace odvětví přesto zohledněno, protože bezpečnostní experti tvořící expertní skupinu dospěli k závěru, že by mohlo mít na podobu cílených útoků vliv.

Výsledné hodnocení bezpečnosti jednotlivých organizací spadajících do příslušného odvětví, které je charakterizováno v kapitole 4.1, je založeno na přijatých bezpečnostních opatřeních vůči uvedeným hrozbám.

4.1 Organizace

Sektory ekonomiky lze rozdělit na primární (suroviny), sekundární (výrobky), terciární (služby) a někdy ještě samostatně uváděný sektor kvaternární (věda a výzkum).

Význam primárního sektoru se na celkovém výkonu hospodářství postupně zmenšuje, přesto má však nezastupitelný význam v ekonomice, neboť zajišťuje zdroje, které se spotřebovávají v sekundárním sektoru a pokud by došlo k napadení organizací působících v daném sektoru, tak by to mělo i zásadní dopad na ostatní sektory, neboť by se vybrané zdroje musely dovážet[153]. Obdobně lze odvodit, že je tomu tak i v sektoru sekundárním, kdy dochází ke zpracování surovin a jejích přeměně na výrobky, které jsou pak předmětem prodeje a jsou využívány ve všech sektorech.

Sektory lze dále členit dle standardní klasifikace ekonomických činností NACE do sekcí, oddílů, skupin a tříd[154]. Pro účely této práce je použito nejhrubší členění do sekcí, kterých je v současné době 21 a jsou označeny velkými tiskacími písmeny od A do U.

---

[153] ČSÚ [ČESKÝ STATISTICKÝ ÚŘAD]. *Postavení primárního sektoru v ekonomice ČR* [online]. 2014. Dostupné z: https://www.czso.cz/documents/10180/20534368/320258a.pdf/e3976fc8-3a2f-4974-abeb-fa490b187bd7?version=1.0

[154] ČSÚ [ČESKÝ STATISTICKÝ ÚŘAD]. *NACE REV. 2 METODICKÁ PŘÍRUČKA* [online]. 2011 [cit. 02.02.2022]. Dostupné z: https://www.czso.cz/documents/10180/23174387/metodicka_prirucka_cz_nace_rev_2.pdf/e26beee3-a5b2-48a1-a036-75e14cdb8944?version=1.0

Dále v textu jsou jednotlivé sekce charakterizovány z pohledu možných kybernetických útoků a jejich následků, tak jak byly popsány bezpečnostními experty v rámci pracovní skupiny, přičemž byly vzaty v úvahu jak útoky, které byly medializovány[155], tak i ty, kde žádné informace zveřejněny nebyly.

Přičemž vždy byl zvažován kybernetický útok na uživatele, koncové zařízení a infrastrukturu a jeho potenciál způsobit podstatnou škodu v důsledku narušení důvěrnosti, integrity, dostupnosti a vlastnictví daného systému a dat používaných v organizacích působících v dané sekci, případně pak ohrozit zájmy chráněných trestním zákoníkem.

Byť každá organizace zpracovává osobní údaje o svých zaměstnancích a jejich únik může způsobit podstatnou škodu a stejně tak má nebo by měla mít nějakou strategii, jejíž vyzrazení by ji mohlo rovněž poškodit, není tato skutečnost v rámci hodnocení jednotlivých sekcí explicitně uváděna.

V rámci této metodiky se předpokládá, že charakteristika jednotlivých odvětví bude soustavně nebo alespoň pravidelně na roční bázi aktualizována. K posouzení závislosti mezi jednotlivými odvětvími pak lze použít metodu hodnocení kaskádních a synergických efektů v systému kritické infrastruktury[156].

[155] ČERMÁK, Miroslav. Seznam organizací v ČR, na které byl veden kybernetický útok. *CleverAndSmart Management Consulting* [online]. 15. leden 2020 [cit. 26.04.2020]. Dostupné z: https://www.cleverandsmart.cz/seznam-organizaci-v-cr-na-ktere-byl-veden-kyberneticky-utok/
[156] ŘEHÁK, David, Martin HROMADA a Pavel ŠENOVSKÝ. *Resilience kritické infrastruktury: teorie, principy, metody*. 2019. ISBN 978-80-7385-224-5. s. 70.

A – zemědělství, lesnictví a rybářství

Pro organizace působící v této sekci je charakteristické, že u nich stále převažuje manuální práce, byť mnohde mechanizovaná a automatizovaná, tak ale v zásadě nezávislá na informačních a provozních technologiích. Vzhledem k tomu, že se zde plánuje ve výrazně delším časovém horizontu, než v jiných odvětvích a zakázky jsou uzavírány na dlouhou dobu dopředu, nemá výpadek informačních systémů bezprostřední a citelný dopad na hospodářský výkon těchto organizací. To samozřejmě nevylučuje útok v rámci dodavatelsko-odběratelského řetězce, ale takovýto útok se bude týkat spíše konkrétní organizace a bude obtížné prokázat, zda se jednalo o náhodu, kybernetický útok nebo sabotáž. Např. je otázka, co je příčinnou toho, že sazenice chmele, považované za zelené zlato, od Chmelařského institutu z roku 2012 jsou tak zdegenerované, že jejich šišky mají pouhou třetinovou velikost, což následně povede i k výrazně nižší produkci piva a bude významně ohrožen český export[157]. Stejně tak nelze vyloučit útok na organizace využívající pokročilé operační technologie pro řízení klimatizace, teploty vzduchu a závlahu, ovšem těch rozhodně není většina, a takovýto útok by rovněž neměl plošný dopad a týkal by se výhradně konkrétní organizace působící v této sekci. Přímým útok nebyl v průběhu let zaznamenán.

B – těžba a dobývání

Dobývání a zpracování surovin se rovněž plánuje v delším časovém horizontu, zakázky jsou uzavírány na dlouhou dobu dopředu, výpadek informačních systémů nemá bezprostřední a citelný dopad na hospodářský výkon podniku, ovšem dopad může mít útok na operační technologie, což by v konečném důsledku mohlo mít dopad i na zastavení těžby vzhledem k možnému ohrožení zdraví a života osob, které jsou vždy na prvním místě, a které těžbu, byť za použití mechanizace provádějí. Za celé hodnocené období byl zaznamenán jen jeden útok, a to na

[157] ELČIĆ, Sandro. Část piva je z vadného chmele, mnohé sazenice jsou zdegenerované, zjistila kontrola. Může to ohrozit export. *Hospodářské noviny* [online]. 12. srpen 2019 [cit. 12.08.2019]. Dostupné z: https://ihned.cz/c1-66622070-cast-piva-je-z-vadneho-chmele-mnohe-sazenice-nejrozsirenejsi-odrudy-jsou-zdegenerovane-zjistila-kontrola-muze-to-ohrozit-export

OKD, který vedl k pozastavení těžby na několik dnů[158]. Po několika měsících byly spočítány ztráty, které by měly činit více jak 5 miliónů korun[159].

C – zpracovatelský průmysl

Kybernetický útok může mít zásadní dopad jak na informační, tak i operační technologie. Koncová zařízení, ze kterých dochází k řízení výroby, jsou nedostupná. Výroba se zpomaluje, a tam kde byla již plně automatizovaná se i zcela zastavuje. Dochází k problémům v dodavatelsko-odběratelském řetězci. Není možné objednávat další suroviny a polotovary potřebné k výrobě, přijímat a vyřizovat objednávky, distribuovat hotové výrobky odběratelům. Krade se know-how v podobě technologických postupů, chráněných receptur apod.

D – výroba a rozvod elektřiny, plynu, tepla a klimatizovaného vzduchu

Koncová zařízení, ze kterých se provádí konfigurace a dohled jsou nedostupná a není tak možné okamžitě reagovat na problém. Může dojít ke změně provozních parametrů a v konečném důsledku i omezení dodávky a následným škodám vyplývajícím ze zastavení výroby u odběratelů. V ČR zatím byl kybernetický útok na tuto infrastrukturu zaznamenán jen jednou a to bez dopadu[160], nicméně v zahraničí již k ničivým útokům došlo, např. v roce 2015 na Ukrajině[161] a rovněž např. sousední Německo zaznamenává rostoucí trend[162]. K poslednímu velkému útoku pak došlo v USA na ropovodní systém Colonial Pipeline[163]. A takový výpadek pak má dopad i na ostatní subjekty, kteří jsou na dodávce energie závislí.

---

[158] OKD pokračuje v obnově dat. *ITBiz.cz* [online]. 6. leden 2020 [cit. 26.04.2020]. Dostupné z: https://www.itbiz.cz/zpravicky/okd-pokracuje-v-obnove-dat
[159] ČTK. OKD má po útoku hackerů opět plně funkční hlavní PC systémy. Škoda činí miliony. *Deník.cz* [online]. 23. únor 2020 [cit. 28.05.2021]. Dostupné z: https://www.denik.cz/regiony/okd-ma-po-utoku-hackeru-opet-plne-funkcni-hlavni-pc-systemy-skoda-cini-miliony-20200223.html
[160] LN: Hackeři napadli na začátku dubna ČEZ Distribuci, útok byl odražen. *oEnergetice.cz* [online]. 21. duben 2020 [cit. 28.05.2021]. Dostupné z: https://oenergetice.cz/prenos-elektriny/ln-hackeri-napadli-na-zacatku-dubna-cez-distribuci-utok-byl-odrazen/
[161] ZETTER, Kim. Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. *Wired* [online]. 2016 [cit. 25.07.2021]. ISSN 1059-1028. Dostupné z: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/
[162] MARCUS, Imanuel. Germany: Increasing Cyber Attacks Against Power Grid. *The Berlin Spectator* [online]. 18. únor 2019 [cit. 25.07.2021]. Dostupné z: https://berlinspectator.com/2019/02/18/germany-increasing-cyber-attacks-against-power-grid/
[163] TURTON, William a Kartikay MEHROTRA. Colonial Pipeline Cyber Attack: Hackers Used Compromised Password. *Bloomberg* [online]. 2021 [cit. 25.07.2021]. Dostupné z:

E – zásobování vodou; činnosti související s odpadními vodami, odpady a sanacemi

Koncová zařízení, ze kterých se provádí konfigurace a dohled jsou nedostupná a není tak možné okamžitě reagovat na problém. Může dojít ke změně provozních parametrů a v konečném důsledku i omezení dodávky a následným škodám vyplývajícím ze zastavení výroby u odběratelů. Voda je nezbytně nutná k životu, ovšem ČR má mnoho na sobě nezávislých zdrojů vody, takže útok na ně by sice způsobil vážnou škodu, ale musel by být koordinován. V jiných státech to tak docela neplatí, např. v Izraeli, který je hodně závislý na vodě, a tak musí její dodávku k rostlinám řídit pomocí počítače doslova po kapkách[164]. Problém však nemusí být jen s množstvím vody, ale i její kvalitou, která též může být ovlivněna ovládnutím systému, jak ukazuje útok na systém na úpravu vody v USA[165]. V ČR byl zaznamenán jediný útok a to na Povodí Vltavy[166].

F – stavebnictví

Firma se zpravidla stěhuje za prací do místa, kde k výstavbě dochází. Toto odvětví se vyznačuje vysokým podílem ruční práce i mechanizace, ovšem jednotlivé stroje jsou ovládány manuálně a nejsou propojeny do sítě, takže není možné jejich kompletní ovládnutí. Nedostupnost koncových zařízení může způsobit prodloužení termínu dodání díla, ale vzhledem k tomu, že veškeré plány jsou k dispozici i v papírové podobě dochází k prodlení spíš z jiných důvodů. Setkat se můžeme s tím, že dochází ke zcizení projektové dokumentace, výkresů a kalkulacím, za účelem předložení nižší nabídky než má konkurence a tím získání

https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

[164] KREČ, Luboš. Kapky v poušti aneb Velká reportáž z míst, kde vědí, jak vyzrát na sucho. *Forbes* [online]. 4. srpen 2019 [cit. 12.08.2019]. Dostupné z: https://www.forbes.cz/kapky-v-pousti-aneb-velka-reportaz-z-mist-kde-vedi-jak-vyzrat-na-sucho/

[165] COLLIER, Kevin. A hacker tried to poison a Calif. water supply. It was as easy as entering a password. *NBC News* [online]. 2021 [cit. 25.07.2021]. Dostupné z: https://www.nbcnews.com/tech/security/hacker-tried-poison-calif-water-supply-was-easy-entering-password-rcna1206

[166] Systém Povodí Vltavy napadli hackeři. Přehrady ani dodávky vody v ohrožení nejsou. *Aktuálně.cz* [online]. 2020 [cit. 26.04.2020]. Dostupné z: https://zpravy.aktualne.cz/domaci/informacni-system-povodi-vltavy-napadli-hackeri/r~fe9196b478d811eab115ac1f6b220ee8/

zakázky. Jedná se však o cílené útoky na konkrétní firmu v rámci konkurenčního boje, kdy je výpočetní technika jen prostředkem k dosažení cíle.

G – velkoobchod a maloobchod; opravy a údržba motorových vozidel

V důsledku nedostupnosti e-shopů není možné realizovat nákup zboží. Dochází k poklesu objemu prodeje. Zákazníci nakupují u konkurence anebo svůj nákup odkládají na později, záleží na tom, kdo všechno je zasažen a jaká je konkurence v daném segmentu. Dochází ke zcizení databáze zákazníků a smluvních ujednání za účelem nabídnutí lepších podmínek a přetáhnutí zákazníků. K těmto cíleným DDoS útokům dochází opakovaně, ovšem vzhledem k nasazení DDoS protektorů (ochrana před zahlcením v podobě síťového prvku, který filtruje provoz) na straně ISP dochází k jejich eliminaci. V minulosti došlo k několika velkým DDoS útokům, např. v roce 2011, kdy několik tisíc e-shopů bylo nedostupných[167]).

H – doprava a skladování

Koncová zařízení, ze kterých dochází k řízení dopravy, jsou nedostupná, tvoří se fronty na pokladnách, dochází k pozdnímu odbavení cestujících, zpoždění odjezdu a příjezdu jednotlivých spojů, dochází k preferenci osobní dopravy, tvoří se kolony na silnicích, zaměstnanci se dostávají pozdě do práce, v důsledku toho klesá produktivita všech firem, což má negativní dopad na výsledky hospodaření jak jednotlivých firem, tak i celého státu. Nefunguje zásobování, v obchodech nejsou některé druhy zboží, především základních potravin, klesá HDP. V roce 2021 proběhl např. útok na počítačové systémy Správy železnic i Českých drah[168], v roce 2020 pak proběhl neúspěšný útok na Letiště Praha[169]. Do budoucna je

[167] VYLEŤAL, Martin. Tisíce tuzemských e-shopů mělo výpadky, může za to masivní DDoS útok. *Lupa.cz* [online]. 2011 [cit. 11.05.2021]. ISSN 1213-0702. Dostupné z: https://www.lupa.cz/clanky/tisice-tuzemskych-e-shopu-melo-vypadky-muze-za-to-masivni-ddos-utok/

[168] Hackeři napadli sítě Správy železnic, provoz vlaků neohrozili. *ČeskéNoviny.cz* [online]. 2021 [cit. 11.05.2021]. Dostupné z: https://www.ceskenoviny.cz/zpravy/hackeri-napadli-site-spravy-zeleznic-provoz-vlaku-neohrozili/2011847

[169] Letiště Praha se stalo terčem několika kybernetických útoků. Všechny se podařilo odvrátit. *iROZHLAS* [online]. 2020 [cit. 11.05.2021]. Dostupné z: https://www.irozhlas.cz/zpravy-domov/kyberneticky-utok-prazske-letiste-vaclava-havla-it_2004171827_aur

potřeba počítat i s útoky na vozidla, v důsledku jejich autonomizace, automatizace, vzdálené správy a připojení do internetu, tzv. connected cars[170]. Stejně tak bude nutné se zabývat i bezpečností dronů, o kterých uvažují některé společnosti zabývající se přepravou a doručováním zásilek. Na drony může být veden útok a stejně tak může být veden útok za použití dronů[171].

I – ubytování, stravování a pohostinství

Není možné rezervovat ubytování přes internet, je nutno rezervace provádět přes telefon, není možné platit kartou, dochází k vytváření front u pokladen, zhoršuje se komfort klienta, dochází k určitým poklesům v příjmech. Dochází ke zcizení osobních údajů a napadání koncových zařízení hostů. V minulosti došlo v zahraničí k několika takovým útokům, od zašifrování dat[172] přes útoky na jednotlivé hosty[173], až po únik osobních údajů[174].

J – informační a komunikační činnosti

Není dostupný internet. Je omezeno fungování většiny online služeb, zastavuje se výroba, obchod, nefunguje platební styk, dochází k celkovému ochromení státu a značným ztrátám na HDP. K těmto útokům dochází v podstatě každý rok s různou intenzitou. V minulosti došlo k několika velkým DDoS útokům, např. v roce 2013 (několik dní trvající útoky na zpravodajské portály a operátory), ale od zavedení opatření po roce 2013 je dopad z pohledu kritické infrastruktury minimální[175].

---

[170] RECHTIK, Marek. Kybernetická bezpečnost v automobilovém sektoru. *Bezpečnostní teorie a praxe*. 2021, roč. 2021, č. 2. ISSN 2571-4589. s. 121–132

[171] RECHTIK, Marek, Ondrůšek JAKUB a Siřinek TOMÁŠ. Hrozby vyplývající z použití doručovacích dronů v České republice. *Bezpečnostní teorie a praxe*. 2021, roč. 2021, č. 4. ISSN 2571-4589. s. 23–46

[172] VINCENT, James. Don't believe the story about hackers locking guests in their rooms at a luxury hotel. *The Verge* [online]. 30. leden 2017 [cit. 11.05.2021]. Dostupné z: https://www.theverge.com/2017/1/30/14438226/hackers-austrian-hotel-bitcoin-ransom-ransomware

[173] DarkHotel APT: What It Is and How It Works. *www.kaspersky.com* [online]. 13. leden 2021 [cit. 11.05.2021]. Dostupné z: https://www.kaspersky.com/resource-center/threats/darkhotel-malware-virus-threat-definition

[174] TIDY, Joe. Marriott Hotels fined £18.4m for data breach that hit millions. *BBC News* [online]. 2020 [cit. 11.05.2021]. Dostupné z: https://www.bbc.com/news/technology-54748843

[175] SLÍŽEK, David. DDoS útok zasáhl weby mobilních operátorů, na možný atak se chystají i e-shopy. *Lupa.cz* [online]. 2013 [cit. 11.05.2021]. ISSN 1213-0702. Dostupné z: https://www.lupa.cz/clanky/ddos-pokracuje-cilem-jsou-dnes-weby-mobilnich-operatoru/

K – peněžnictví a pojišťovnictví

Obsluha počítače, ze kterých probíhá obsluha klienta na pobočkách, a ze kterých se přistupuje do transakčních systémů, není možná. Není možné založit nový účet, uložit hotovost, poskytnout úvěr. Dochází ke ztrátě obchodní příležitosti. Není možné obchodovat na finančních trzích a realizovat nákup a prodej finančních instrumentů. Pokud není dostupný transakční systém přes internet, nemohou ani stávající klienti realizovat jednorázové transakce, nakupovat v e-shopech, platit kartou, dochází k reklamacím a dopadům do výsledku hospodaření jednotlivých firem potažmo HDP. Dochází ke zkopírování databáze klientů, k online převodu peněz na účet útočníka. K DDoS útokům na banky došlo v roce 2013, kdy byla po dobu několika hodin omezena dostupnost služeb internetového bankovnictví největších českých bank[176]. V dalších letech pak byl veden útok na systém SWIFT, ale ten se údajně bank v ČR nedotkl[177].

L – činnosti v oblasti nemovitostí

Mohlo by dojít ke zpomalení na trhu s nemovitostmi, výběru nižší daně z převodu nemovitosti, což by mělo negativní dopad na HDP. Pravděpodobnější je však únik osobních údajů[178].

M – profesní, vědecké a technické činnosti

Dochází ke zcizení know-how, potenciálně patentově chráněných technologií, výrobních postupů, nových receptur a poškození zájmů ČR. V roce 2021 byl proveden útok na Národní knihovnu[179].

---

[176] Internetové bankovnictví zkolabovalo, další kybernetický útok mířil na banky - Novinky.cz [online]. 2013 [cit. 11.05.2021]. Dostupné z: https://www.novinky.cz/internet-a-pc/clanek/internetove-bankovnictvi-zkolabovalo-dalsi-kyberneticky-utok-miril-na-banky-183723

[177] ČERMÁK, Miroslav. Roste počet útoků na SWIFT. *CleverAndSmart Management Consulting* [online]. 31. květen 2016 [cit. 10.06.2020]. Dostupné z: https://www.cleverandsmart.cz/roste-pocet-utoku-na-swift/

[178] NOVÁK, Daniel. Únik dat z realitky ukazuje na obrovský bezpečnostní problém, říká expert. *Seznam Zprávy* [online]. 2021 [cit. 06.02.2022]. Dostupné z: https://www.seznamzpravy.cz/clanek/unik-dat-z-realitky-ukazuje-obrovsky-bezpecnostni-problem-rika-expert-173901

[179] Národní knihovnu v noci napadli hackeři, pro veřejnost je uzavřena. *ČeskéNoviny.cz* [online]. 2021 [cit. 28.05.2021]. Dostupné z: https://www.ceskenoviny.cz/zpravy/narodni-knihovnu-v-noci-napadli-hackeri-pro-verejnost-je-uzavrena/2038834

N – administrativní a podpůrné činnosti

Dochází ke zpomalení ekonomiky v důsledku nemožnosti poskytovat leasing, řídit lidské zdroje, klesá objem prostředků z cestovního ruchu, snižuje se HDP.

O – veřejná správa a obrana; povinné sociální zabezpečení

Dochází ke snížení kvality a omezení rozsahu služeb zajišťovaných státem s negativním dopadem na HDP. Dochází k úniku osobních údajů a informací, které jsou předmětem státního tajemství. V roce 2021 byl veden útok na olomoucký magistrát[180], pražský magistrát a systémy MPSV[181].

P – vzdělávání

Útočníci usilují o kompromitaci infrastruktury, získání osobních údajů, ale jdou i po výzkumech[182]. Běžné útoky se však nevyhýbají ani základním [183] a středním[184] školám.

Q – zdravotní a sociální péče

Koncová zařízení, ze kterých doktoři, sestry a další zdravotnický personál přistupuje do systému, kde jsou uloženy veškeré informace o pacientech, tedy jejich zdravotním stavu, anamnéze, probíhající léčbě, užívaných lécích, podstoupených vyšetřeních, proběhnuvších zákrocích a plánu dalších prohlídek

---

[180] Olomoucký magistrát paralyzoval útok hackerů, město podá trestní oznámení. *iDNES.cz* [online]. 7. duben 2021 [cit. 28.05.2021]. Dostupné z: https://www.idnes.cz/olomouc/zpravy/olomouc-magistrat-utok-hackeru-datova-sit-kolaps.A210407_175516_olomouc-zpravy_stk

[181] ČTK. Hackeři napadli systémy MPSV a pražského magistrátu. Data podle Maláčové neukradli. *Hospodářské noviny (iHNed.cz)* [online]. 5. březen 2021 [cit. 28.05.2021]. Dostupné z: https://domaci.ihned.cz/c1-66892210-system-verejne-spravy-napadli-hackeri-data-se-jim-podle-malacove-ukrast-nepodarilo

[182] Olomoucká univerzita čelí útokům hackerů, jdou po e-mailech i výzkumech. *iDNES.cz* [online]. 5. březen 2019 [cit. 11.05.2021]. Dostupné z: https://www.idnes.cz/olomouc/zpravy/olomouc-univerzita-palackeho-kyberneticka-bezpecnost-utoky-hackeri-kradeze-dat-e-maily-phishing.A190301_460895_olomouc-zpravy_stk

[183] Hacker napadl přerovskou školu, za zašifrovaná data žádá výkupné. *iDNES.cz* [online]. 2. prosinec 2021 [cit. 06.02.2022]. Dostupné z: https://www.idnes.cz/olomouc/zpravy/hacker-utok-prerov-travnik.A211202_204219_olomouc-zpravy_cun

[184] Plzeňské školy napadli hackeři. Za vrácení dat chtěli milionové výkupné. *iDNES.cz* [online]. 10. květen 2018 [cit. 14.08.2019]. Dostupné z: https://www.idnes.cz/plzen/zpravy/hacker-internetovy-utok-krizikovo-gymnazium-stredni-skola-plzen-kybernetika-vypalne.A180510_084940_plzen-zpravy_vb

jsou nedostupné, což v krajním případě může vést i k jejich ohrožení na životě. Na vině je ve většině případů ransomware, který zašifruje data a zobrazí výzvu k zaplacení. V průběhu několika let bylo detekováno hned několik kybernetických útoků na nemocnice, naposledy např. tří pražských poliklinik[185]. V mnoha případech útočník ani neví, koho napadl.

R – kulturní, zábavní a rekreační činnosti

Dochází k omezení poskytovaných služeb s negativním dopadem na výsledky hospodaření daného subjektu zpravidla z důvodu napadení webového portálu nebo rezervačního systému.

S – ostatní činnosti

Dochází k úniku osobních údajů.

T – činnosti domácností jako zaměstnavatelů; činnosti domácností produkujících blíže neurčené výrobky a služby pro vlastní potřebu

Zpravidla se stávají obětí plošného útoku, kdy dojde k napadení koncového zařízení ransomware nebo bankware a je zobrazena výzva k zaplacení výkupného anebo dochází k odčerpání peněz přes internetové bankovnictví.

U – činnosti exteritoriálních organizací a orgánů

Dochází ke změně informací a chybným rozhodnutím, což může mít negativní dopad na HDP.

Metodická poznámka

Pokud by se ukázalo, že uvedené členění je nevyhovující, je samozřejmě možné jej změnit a provést hrubší nebo jemnější členění. Případně je možné

[185] Hackeři se nabourali do systému tří pražských poliklinik, nefungují e-maily ani objednávkový systém. *iROZHLAS* [online]. 2021 [cit. 11.05.2021]. Dostupné z: https://www.irozhlas.cz/zpravy-domov/hackersky-utok-poliklinika-ipp-hackeri_2103161619_ada

použít i úplně jiné členění např. takové, jaké uvádí Nařízení vlády č. 315/2014 Sb.[186]

4.2 Hrozby

Na základě stručné charakteristiky možných kybernetických útoků a jejich dopadů, lze nalézt určité společné charakteristiky a je možné prohlásit, že:

- Téměř každá organizace má konektivitu do internetu a využívá prostředky informačních technologií, minimálně webovou prezentaci a e-mail, na kterých je do větší nebo menší míry závislá. Tam, kde je větší závislost, tak může také vzniknout podstatně větší škoda v případě narušení bezpečnosti.
- Na každou organizaci může být veden kybernetický útok, a to jak plošný, tak i cílený, přičemž jeho pravděpodobnost roste s významem organizace, a dopad pak je dán závislostí organizace na IT a absencí nebo nedostatečností přijatých bezpečnostních opatření organizační a technické povahy.
- Každá organizace působící na trhu zpracovává ve větší či menší míře osobní údaje, ať už svých klientů nebo vlastních zaměstnanců, má nějakou strategii, která by ji měla zajistit pozici na trhu a může být pro konkurenci zajímavá stejně jako know-how, kterým může být chráněná receptura, technologický postup apod.
- Každá organizace musí nějakým způsobem hradit své závazky a používá za tímto účelem elektronické bankovnictví a jeho prostřednictvím převádí peníze mezi účty, platí faktury apod.

Útoky lze rozlišit na plošné a cílené. Pokud jde o pravděpodobnost cílených útoků, tak ta se odvíjí od postavení organizace na trhu, její hodnoty a významu pro stát, neboť jak již byl uvedeno, cílem útočníka je se buď obohatit, anebo způsobit škodu někomu jinému. Zatímco DoS a zpravidla i SP je vždy cílený tak ostatní uvedené útoky jako KH, PD, MT být cílené v prvopočátku nemusí, obzvlášť

[186] *Nařízení vlády č. 315/2014 Sb., Nařízení vlády, kterým se mění nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury v posledním znění*

v případě RW, kdy útočník mohl provést plošný sken a narazit při něm na zranitelnost, kterou se prostě jen rozhodl zneužít. Platí, že na některé organizace jsou vedeny útoky jen proto, že jsou přítomny na internetu a na jiné, proto, proč tam jsou.

Je zřejmé, že organizace, která je např. součástí kritické informační infrastruktury, provozuje významný informační systém nebo systém základních služeb, tak bude spíše cílem DoS, SP či jiného útoku než organizace, která se na hospodářských výsledcích státu takovou měrou nepodílí a ani neposkytuje své služby velkému počtu občanů. Jednoduše proto, že útočník by zde svého cíle nedosáhl, nezpůsobil by v podstatě žádnou škodu.

Podobně i útok, jehož cílem je získání citlivých informací jako je know-how bude veden spíše na organizace, které daným citlivým know-how skutečně disponují anebo lze u nich očekávat, že by jím disponovat mohly, a je nasnadě, že to budou především organizace, kde probíhá nějaký výzkum a vývoj, může se tak jednat jak o zavedenou organizaci, tak i technologický startup. Jinými slovy, kde nic není, ani hacker nebere.

V případě PD a MT, kdy se jedná o cílené útoky, které jsou vedeny na organizace, které zpracovávají velké množství osobních údajů anebo provádějí velké množství finančních transakcí, lze předpokládat, že v tom množství a objemu prostředků, které se denně převádí mezi nejrůznějšími účty, si podvodné transakce nikdo nevšimne anebo alespoň ne hned a útočníkovi se mezitím podaří peníze vyvést z bankovního oběhu.

Z výše uvedeného vyplývá, že pravděpodobnost hrozby ovlivňuje několika faktorů. Nemá zde však příliš smysl hodnotit motiv, příležitost a schopnost útočníka, tak jak je to běžně doporučováno, protože ten se vždy najde, obzvlášť pokud je útočníkem např. státem sponzorovaná skupina, která disponuje značnými finančními zdroji a prostředky k realizaci útoku. Mnohem důležitější je však atraktivita aktiva, a zda již k útoku někdy nebo někde došlo.

Obětí plošného útoku, kdy je jako vektor útoku použit nějaký generický malware, se může stát jakákoliv organizace. **Pravděpodobnost že se jí i stane, je dána především úrovní jejího zabezpečení vůči ostatním tržním subjektům** a to nejen vůči těm spadajícím do dané sekce/odvětví, ale vůči celému globálnímu trhu. Těmito hrozbami jsou jak plošné, tak i cílené útoky, jejichž cílem je:

- **odepření služby** (Denial of Service, zkr. DoS) a tím způsobení nedostupnosti daného systému pro jeho konzumenty, přičemž předmětem hodnocení jsou skutečné DoS útoky, nikoliv jen výhružné e-maily adresované čelním představitelům organizace, tzv. extortion letters, ve kterých útočník vyhrožuje, že když organizace do určité doby nezaplatí, tak že útok provede, a přitom ani nedisponuje takovou silou, aby byl schopen útok realizovat po dostatečně dlouhou dobu. Za sledované období došlo k několika masivním DDoS útokům na vybrané cíle v ČR, a to v roce 2011 a 2013, což neznamená, že v dalších letech již k DDoS útokům nedocházelo, docházelo, a dochází k nim každý rok, ale již nebyly schopny způsobit viditelný výpadek, neboť na ně bylo včas reagováno;

- **ovládnutí systému** (System Possession, zkr. SP) a způsobení škody a to změnou konfigurace ICS/SCADA zařízení sloužících k řízení výroby[187], smazáním anebo zašifrováním dat s úmyslem zastavit produkci, snížit výkon, generovat zmetky, způsobit v dané zemi chaos, ohrozit životy, poškodit zdraví, životní prostředí, ochromit její infrastrukturu nebo napomoci chybným rozhodnutím apod., což může v některých případech vést i k ukončení činnosti dané organizace na trhu, např. z důvodu ztráty důvěry ze strany zákazníků. Vzhledem k tomu, že v tomto případě je motiv útočníka způsobit především škodu, přičemž nelze odmítnout možnost, že díky tomu může získat i nemalý finanční prospěch, tak zpravidla je tento útok realizován tzv. APT skupinami a je veden na subjekty, které zaujímají dominantní postavení na trhu a jsou součástí kritické infrastruktury státu, a je pravděpodobnější v zemích, kde je nižší index bezpečí;

- **získání citlivých informací** jako je know-how, zkr. KH, unikátní výrobní postup, chráněné receptury anebo i obchodního tajemství a jeho následný prodej konkurenci nebo využití ve vlastním podnikání, což v konečném důsledku může vést k podstatnému propadu v příjmech a v delším horizontu

[187] MINAŘÍK, Pavel. Bezpečnost průmyslových sítí a systémů SCADA/ICS. *Bezpečnost průmyslových sítí a systémů SCADA/ICS* [online]. 2. říjen 2018 [cit. 12.03.2019]. Dostupné z: https://m.systemonline.cz/rizeni-vyroby/bezpecnost-prumyslovych-siti-a-systemu-scada-ics.htm

pak i k ukončení činnosti organizace na trhu, neboť již nebude konkurenceschopná. Tyto útoky jsou realizovány jak jednotlivci, např. nespokojenými zaměstnanci, ze strany konkurence anebo vysoce organizovanými APT skupinami, kterým jde o získání citlivých informací. Na území ČR pak lze zaznamenat především krádež informací ze strany stávajících zaměstnanců, kteří jsou nespokojeni a jsou připraveni si informace o klientech odnést sebou a mnohdy je i cíleně a soustavně po delší dobu shromažďují;

- **získání osobních údajů** klientů nebo zaměstnanců (Personal Data, zkr. PD) za účelem jejich přetažení, prodání anebo zveřejnění a poškození v důsledku uplatnění sankcí dle GDPR, která může činit až 4 % celkového ročního celosvětového obratu. Ne všechny organizace však zpracovávají všechny typy osobních údajů. Ty nemají stejnou hodnotu, vždy je proto nutné uvažovat o tom, kolik osobních údajů unikne a jak moc jsou citlivé a zneužitelné. Zpravidla pak dochází ke zcizení osobních údajů klientů ze strany zaměstnance dané společnosti anebo je únik informací výsledkem činnosti hackera, kterému se podařilo získat přístup do DB přes webovou aplikaci dostupnou z internetu. Výsledná škoda pak odpovídá výši pokuty, ztráty obchodní příležitosti a odlivu části klientů. Odliv klientů v důsledku úniku informací však bývá často značně přeceňován a reálné případy spíše ukazují, že k nějakému masivnímu odlivu klientů z důvodu úniku osobních údajů nedochází, což je dáno především tím, že se útoky týkaly organizací s dominantním postavením na trhu aneb naopak menších organizací, kterým klienti i přesto zachovali věrnost;

- **odčerpání peněz** (Money Transfer, zkr. MT) z firemního účtu organizace, což může být výsledkem generického i specifického malware, které útočníkovi umožnilo získat kontrolu nad počítačem, ze kterého je možné tyto transakce realizovat. V případě domácností je pravděpodobnost nákazy výrazně vyšší než v organizacích, protože v organizacích zpravidla provádí finanční transakce jen pověřená osoba a dost často jen na dedikovaném zařízení, které je vybaveno čtečkou čipových karet apod. Škoda je v takovém případě

odvislá od objemu prostředků na bankovním účtu, a především pak výši limitů finančních transakcí a průměrně převáděné částce. V případě domácností se pohybuje v řádu desítek tisíc, v případě organizací pak ve stovkách tisíc a u bank, kde se již ale jedná výhradně o cílené útoky, pak v miliónech korun, přičemž útočník se snaží převést jen takovou částku, aby si toho nikdo nevšiml anebo aby si toho všiml pozdě a on mezitím stihl tuto částku vyvést z bankovního oběhu[188];

- **zašifrování dat** (Ransomware, zkr. RW) a požadování výkupného za jejich opětovné dešifrování, přičemž ransomwarem je zde míněn výhradně plošně šířený ransomware, který cílí na koncová zařízení, připojené síťové disky a servery, nikoliv wiper, jehož cílem je smazat data v konkrétní organizaci, a který je uvažován již v rámci hrozby SP. Většinu ransomware útoků pak tvoří útoky na koncová zařízení, to v konečném důsledku vede k nemožnosti přistupovat k datům uloženým lokálně a na síťových discích a dále pak do jednotlivých systémů, zpracovávat poštu, komunikovat přes internet, či provádět správu zařízení a obsluhovat klienty. Menší procento útoků se pak týká přes internet dostupných serverů s SQL databází, kdy útočník šifruje nikoliv soubory, ale obsah databáze, a i v tomto případě požaduje platbu za zpřístupnění klíče a dešifrování. Výnosnost z těchto útoků je však podstatně nižší, neboť DB bývají zpravidla pravidelně zálohovány a jsou promptně obnoveny na rozdíl od koncových zařízení a síťových disků, které dost často zálohovány nejsou. Výsledná škoda se pak odvíjí od toho, zda má oběť aktuální a čitelnou zálohu dat, ze které je schopna data obnovit. Odstranění ransomware nebývá zpravidla problém, pohybuje se v řádu jednotek tisíc na jeden počítač, škoda však spočívá především ve ztrátě pro organizaci důležitých dat, která pokud nejsou zálohována, se v mnoha případech již nepodaří obnovit nikdy anebo až za několik měsíců, kdy se bezpečnostním expertům podaří získat šifrovací klíč nebo odhalit chybu v kódu samotného ransomware. Tak dlouho nemůže většina organizací čekat, a tak pokud nejsou

[188] ČERMÁK, Miroslav a Vladimír ŠULC. Kybernetická bezpečnost - praktický příklad kybernetického útoku. *Právo a bezpečnost*. 2018, roč. 2018, č. 3. ISSN 2336−5323. s. 123–136

schopny data obnovit, tak zaplatí požadovanou částku, jež se pohybuje od několika desítek do stovek tisíc.

- **APT útok je možný a dochází k němu i v ČR**, nicméně je třeba uvést, že České republice patří v žebříčku NCSI[189], který hodnotí připravenost států na kybernetické útoky a incidenty, 1. místo mezi 131 státy. Stejně dobře se Česká republika umístila i v žebříčku GPI[190], který hodnotí mírumilovnost dané země, kde ji náleží 10. pozice mezi 163 státy a teritorii a toto dobré umístění si ČR drží dlouhodobě. Na základě této skutečnosti lze usuzovat, že pravděpodobnost úspěšného APT útoku na organizaci působící na území ČR je relativně nízká, neboť nízký jest motiv útočníka a vysoká jest úroveň bezpečnosti, alespoň v této teoretické rovině. Otázka však je, zda tomu tak opravdu je. V zásadě existují jen dvě možnosti, k APT útokům na území ČR **nedochází**, protože zde neprobíhá takový výzkum, o nějž by měly cizí mocnosti zájem, anebo našly jednodušší způsob, jak se k jeho výsledkům dostat, např. prostřednictvím agentů provádějících průmyslovou špionáž. Anebo k nim **dochází**, jsou vedeny vůči konkrétním subjektům, ale ti vzhledem k jejich sofistikovanosti nejsou schopni je odhalit, a proto o nich nevíme, anebo k jejich odhalení již došlo, ale z obav ze ztráty dobrého jména nebyly přesto hlášeny. Vzhledem k tomu, že k nějaké podstatné změně chování managementu dle Mary T. Franz z Enterprise Knowledge Partners nedochází, nýbrž je zde patrný určitý vzorec chování rozpoznatelný i napříč odvětvími, podle kterého se do bezpečnosti investuje krátce po incidentu, kdy se zavedou bezpečnostní opatření a po jejich zavedení se rozpočet opět drasticky sníží[191], lze předpokládat obdobný průběh i v budoucnu. Pravděpodobnost takového útoku, odolnost systému vůči němu a následky takového útoku tak mohou být stanoveny na základě některého již z mnoha proběhnuvších útoků, jako byl

[189] NCSI :: Ranking. *e-Governance Academy* [online]. [cit. 02.08.2019]. Dostupné z: https://ncsi.ega.ee/ncsi-index/
[190] HUMANITY, Vision of. Global Peace Index. *Vision of Humanity* [online]. [cit. 02.08.2019]. Dostupné z: http://visionofhumanity.org/indexes/global-peace-index/
[191] BRUMFIELD, Cynthia. Equifax's data breach disaster: Will it change executive attitudes toward security? *Equifax's* [online]. 2019 [cit. 02.02.2022]. Dostupné z: https://www.csoonline.com/article/3411139/equifax-s-billion-dollar-data-breach-disaster-will-it-change-executive-attitudes-toward-security.html

např. WannaCry, kdy bylo zneužito nikoliv zranitelnosti nultého dne, nýbrž zranitelnosti operačního systému, pro který již byla dávno k dispozici záplata.

Tabulka 13 – Hodnocení pravděpodobnosti výskytu hrozby představuje vodítka hodnocení. Pokud jde o stanovení míry pravděpodobnosti, tak se volí ta vyšší hodnota, např. v okamžiku, kdy je možno hodnotit podle různých kritérií rozdílně.

Tabulka 13 – Hodnocení pravděpodobnosti výskytu hrozby

#	Pravděpodobnost (četnost) hrozby	Vodítka hodnocení s ohledem na četnost výskytu a atraktivitu aktiva
1	Nepravděpodobná (vůbec)	Žádná organizace v ČR se zatím s tímto typem útoku nesetkala, nelze ho přesto zcela vyloučit. Organizace nedisponuje žádným specifickým know-how, nezaujímá významné postavení na trhu, rovněž není zpracovatelem velkého množství osobních údajů, nevykazuje velký obrat. (drobní podnikatelé, mikropodniky)
2	Pravděpodobná (jednou)	Některé organizace působící na území ČR se s tímto typem útoku již setkaly a je možné, že k němu dojde i v jiné sekci hospodářství. Organizace nedisponuje až takovým know-how, které by mohlo být předmětem zájmu ze strany konkurence, nezaujímá významné postavení na trhu, nedosahuje vysokého obratu (malé podniky, oligopolní lem).
3	Vysoce pravděpodobná (opakovaně)	Některé organizace působící ve stejné sekci hospodářství se s tímto typem útoku již setkaly, takže je vysoce pravděpodobné, že k obdobnému útoku dojde. Organizace disponuje know-how, které by mohlo být předmětem zájmu ze strany konkurence, obzvlášť v případě, kdy se společnost nachází v recesi a dochází k zostření konkurenčního boje. (střední podniky, nachází se v roli následovníka nebo vyzyvatele).
4	Téměř jistá (soustavně)	Organizace ze stejné sekce danému typu útoku čelily v posledním roce hned několikrát a je téměř jisté, že se útok bude znovu opakovat. Organizace disponuje specifickým know-how nebo zaujímá významné místo na trhu, případně zpracovává velké množství osobních údajů či vykazuje takový obrat, který by mohl být pro útočníka dostatečně atraktivní, aby vynaložil i značné prostředky na realizaci útoku. (velké podniky a mezinárodní korporace)

Tabulka 14 – Sekce a hrozby ukazuje, že ne všechny sekce jsou vystaveny stejným hrozbám. Pravděpodobnost je možné stanovit na základě minulých zkušeností, tedy zda organizace působící v dané sekci takovému útoku někdy v minulosti již čelily.

Tabulka 14 – Sekce a hrozby

kód	Sekce	Nedostupnost systému (DDoS)	Krádež know -how	Ovládnutí systému	Krádež osobních dat	Neautorizovaný převod peněz	Zašifrování dat
A	zemědělství, lesnictví a rybářství	1	1	2	1	1	1
B	těžba a dobývání	1	1	4	1	1	4
C	zpracovatelský průmysl	1	2	2	1	1	2
D	výroba a rozvod elektřiny, plynu, tepla a klimatizovaného vzduchu	2	1	2	1	1	1
E	zásobování vodou; činnosti související s odpadními vodami, odpady a sanacemi	2	1	4	1	1	1
F	stavebnictví	1	1	1	1	1	1
G	velkoobchod a maloobchod; opravy a údržba motorových vozidel	4	1	1	4	4	4
H	doprava a skladování	2	1	2	2	1	1
I	ubytování, stravování a pohostinství	1	1	2	2	1	1
J	informační a komunikační činnosti	4	1	3	4	1	1
K	peněžnictví a pojišťovnictví	3	1	2	4	2	3
L	činnosti v oblasti nemovitostí	1	1	1	1	1	1
M	profesní, vědecké a technické činnosti	1	4	1	1	1	1
N	administrativní a podpůrné činnosti	1	1	1	1	1	1
O	veřejná správa a obrana; sociální zabezpečení	2	1	4	2	1	4
P	vzdělávání	1	4	2	3	1	4
Q	zdravotní a sociální péče	2	1	4	2	1	4
R	kulturní, zábavní a rekreační činnosti	1	1	1	1	1	1
S	ostatní činnosti	1	1	1	1	1	1
T	činnosti domácností jako zaměstnavatelů;	1	1	1	1	1	1
U	činnosti exteritoriálních organizací a orgánů	1	1	1	1	1	1

Metodická poznámka

Je nutné evidovat veškeré kybernetické útoky a bezpečnostní incidenty a zaznamenávat u nich jakého sektoru a odvětví se týkaly a zda se jednalo o kybernetické útoky plošné nebo cílené, protože jedině na základě této analýzy lze vyhodnocovat, na jaká odvětví jsou útoky cíleny a zda vůbec jsou cíleny anebo se jedná o útoky spíše plošné.

Situaci zhoršuje skutečnost, že k**romě jednotné taxonomie hrozeb v ČR neexistuje veřejná databáze, ze které by se dalo čerpat**, a je tak možné vycházet jen z případů, které byly zveřejněny v médiích.

V okamžiku, kdy bude k dispozici databáze kybernetických bezpečnostních incidentů a kybernetických útoků, je možné použít i kvantitativní hodnocení pravděpodobnosti hrozeb, kdy vyjádříme absolutní počet výskytů dané hrozby za rok jako ARO (Annual Rate of Occurence) a četnost výskytu dané hrozby pak jako podíl počtu výskytu této hrozby vůči celkovému počtu hrozeb v dané organizaci, sektoru nebo odvětví, a to podle toho na jaké úrovni abstrakce chceme úroveň bezpečnosti hodnotit.

4.3 Dopady

Velikost dopadu v případě realizace určité hrozby se může v rámci jednotlivých sekcí a organizace od organizace podstatně lišit. Někde bude přímá i nepřímá škoda minimální a rovněž i obnovení provozu proběhne velice rychle, zatímco jinde to podstatně ohrozí její fungování a podstatu samotné organizace. Je tak možné identifikovat sekce, kde DoS, malware, a hacking bude mít větší šanci způsobit nějakou podstatnou škodu a sekce, kde bude dopad naopak minimální.

Je zřejmé, že i když dojde k realizaci dané hrozby, tak jiný dopad bude mít DoS na portál státní správy, který denně využívá velké množství občanů a jiný na webovou prezentaci organizace podnikající v těžbě dřeva, kterou využije jen případný nový odběratel v rámci B2B.

Obdobně tomu pak bude i v případě RW, který zašifruje data na koncovém zřízení, ze kterého probíhá dohled nad letovým provozem, anebo naopak zařízení, ze kterého se přistupuje na web a zadávají inzeráty s nabídkou prodeje a koupě nemovitostí. Zde může podstatnou roli hrát rychlost zpřístupnění a např.

organizace působící v sekci C, G, Q raději zaplatí, aby měly systémy a data přístupná hned, jinde počkají anebo prostě jen přeinstalují své stroje a data obnoví ze zálohy, případně je znovu zpracují.

Stejně tak tomu bude v případě SP, kdy dojde ke změně konfigurace na zařízení, které slouží ke správě chladícího zařízení bloku jaderné elektrárny, anebo na zařízení, které reguluje teplotu v openspace nejmenované korporace.

A nejinak tomu bude v případě PD, kdy uniknou osobní údaje o zaměstnancích univerzity a kdy budou pro změnu zkopírovány anamnézy pacientů středně velké nemocnice nebo praktického lékaře.

Jiný dopad bude mít únik KH spočívající ve zveřejnění strategie organizace působící v oblasti zábavy a jiný u organizace působící ve zpracovatelském průmyslu.

K hodnocení dopadů vyplývajících z jednotlivých hrozeb je třeba vzít v úvahu škody, které vznikají přímo dané organizaci, a které ve výsledku vedou ke ztrátě, konkrétně se jedná o náklady na obnovu, ztrátu tržní příležitosti, ztrátu produktivity, sankce, pokuty, pokles ceny akcií apod. A dále pak škody na životním prostředí, škody na majetku, poškození zdraví a v krajním případě i ztráty na životech.

Dále je nutné si uvědomit, že v některých případech vznikají i nepřímé škody mající podstatný dopad i na ostatní tržní subjekty, neboť se zde uplatňuje **multiplikativní efekt a dochází k negativní publicitě, což by si oboje zasloužilo samostatný výzkum**. Níže jsou uvedena možná vodítka hodnocení jednotlivých dopadů, která vychází z metodiky FAIR[192] a zohledňují primární i sekundární škodu.

Zanedbatelná škoda (žádná)

- Organizace je v zásadě nezávislá na IT, využívá jen e-mail, webovou prezentaci a má nízké požadavky na bezpečnost.

[192] FREUND, Jack. *Measuring and managing information risk: a FAIR approach*. Amsterdam: Butterworth-Heinemann, 2015. ISBN 978-0-12-420231-3. s. 66.

- Nehrozí riziko z prodlení, ztráta produktivity, ani ztráta tržních příležitostí a vzhledem k tomu, že se incident podařilo vyřešit v rámci SLA, tak nebudou uplatňovány ani žádné sankce a pokuty.
- K nápravě stavu postačí využít části pracovního kapitálu, tj. hotovosti na pokladně nebo běžných účtech v bance.
- Vzhledem k tomu, že selhání nikdo nezaznamenal, tak se o něm veřejnost nedozví a nedojde k jeho medializaci, a tedy ani k poškození dobrého jména.

Střední škoda

- Organizace je částečně závislá na IT, je však schopna se přepnout i do manuálního módu.
- Hrozí menší ztráta produktivity, tržní příležitosti, incident se nepodařilo vyřešit v rámci SLA.
- Náklady na obnovu provozu úhradu pokut a sankcí je nutné uhradit z rezervního fondu
- O události se dozví veřejnost, ovšem vzhledem k tomu, že se jedná o omluvitelné selhání, nepředpokládá se nějaká negativní publicita.

Vysoká

- Organizace je velmi závislá na IT, možnosti přepnutí se do manuálního módu jsou omezené.
- Hrozí podstatná ztráta produktivity, tržní příležitosti, vysoké náklady na obnovu provozu, udělení nejvyšších možných pokut.
- Očekává se škoda ve výši ročního zisku.
- Jedná se o neomluvitelné selhání a s tím bude spojena negativní publicita a poškození dobrého jména.

Ohrožující

- Organizaci je zcela závislá na IT, veškerý provoz je plně automatizován a řízen počítači.
- Hrozí riziko z prodlení, zastavení nebo omezení výroby na delší dobu, dochází k produkci zmetků a stahování výrobků z trhu.

- Očekává se škoda ve výši celkového jmění, společnost bude muset požádat o ochranu před věřiteli, představit plán a zahájit restrukturalizaci.
- Jedná se o zásadní selhání, a proto bude následovat intenzivní negativní publicita, nevratné poškození dobrého jména, ohrožena existence organizace, poškození životního prostředí, zdraví, ztráty na životech.

V rámci pracovní skupiny byly dopady hodnoceny způsobem, jak zachycuje Tabulka 15 – Dopady.

Tabulka 15 – Dopady

kód	Sekce	Nedostupnost systému (DDoS)	Krádež know -how	Ovládnutí systému	Krádež osobních dat	Neautorizovaný převod peněz	Zašifrování dat
A	zemědělství, lesnictví a rybářství	1	1	1	1	2	1
B	těžba a dobývání	2	1	2	1	3	1
C	zpracovatelský průmysl	2	4	3	1	2	3
D	výroba a rozvod elektřiny, plynu, tepla a klimatizovaného vzduchu	3	1	4	2	3	4
E	zásobování vodou; činnosti související s odpadními vodami, odpady a sanacemi	3	1	4	2	2	4
F	stavebnictví	1	2	2	1	2	2
G	velkoobchod a maloobchod; opravy a údržba motorových vozidel	2	1	2	2	2	2
H	doprava a skladování	4	1	4	2	2	4
I	ubytování, stravování a pohostinství	2	1	2	2	2	2
J	informační a komunikační činnosti	4	3	4	2	2	4
K	peněžnictví a pojišťovnictví	4	2	4	3	4	4
L	činnosti v oblasti nemovitostí	1	1	1	1	2	2
M	profesní, vědecké a technické činnosti	1	4	1	1	2	3
N	administrativní a podpůrné činnosti	1	1	1	2	2	2
O	veřejná správa a obrana; sociální zabezpečení	4	1	4	3	2	4
P	vzdělávání	1	3	1	2	2	2
Q	zdravotní a sociální péče	4	2	4	4	2	3
R	kulturní, zábavní a rekreační činnosti	1	1	1	1	1	1
S	ostatní činnosti	1	1	1	1	1	1
T	činnosti domácností jako zaměstnavatelů;	1	1	1	1	1	1
U	činnosti exteritoriálních organizací a orgánů	1	1	1	1	1	1

Metodická poznámka

U každého bezpečnostního incidentu nebo kybernetického útoku je nutné evidovat i výši škody, která může být spočtena jako součet primární a sekundární škody. Tuto informaci je vhodné aktualizovat, protože konečná škoda nebývá zpravidla hned zřejmá a může být vyčíslena až po několika měsících.

Vzhledem k tomu, že neexistuje oficiální metodika, jak výši škody počítat, je možné se řídit doporučením uvedeným v metodice FAIR[193]. Kvantifikace skutečných škod v korunách by pak měla umožnit lepší řízení rizik a investic do bezpečnosti.

V okamžiku, kdy je k dispozici databáze kybernetických bezpečnostních incidentů a kybernetických útoků včetně výše primárních a sekundárních škod, je možné použít i kvantitativní hodnocení dopadů, kdy vyjádříme celkovou škodu vyplývající z realizace dané hrozby.

V případě, že bychom k dispozici tyto údaje neměli a chtěli hodnotit celkový dopad na organizaci působící v daném sektoru, tak můžeme vyjít z § 1 Nařízení vlády č. 432/2010 Sb., který uvádí průřezová kritéria dle počtu obětí na životech, počtu hospitalizovaných, ekonomického dopadu anebo dle dopadu na určitý počet osob, a od těchto kritérií pak odvíjet hodnoty dopadu i pro ostatní organizace, které kritickou infrastrukturu neprovozují[194]. Možné hodnocení zachycuje Tabulka 16 – Dopady dle kritičnosti. Přesné stanovení jednotlivých hodnot v řádcích 2 až 4 by mělo být předmětem dalšího výzkumu.

Tabulka 16 – Dopady dle kritičnosti

Dopad	Zásah do každodenního života (v jednotkách osob)	Ztráta na životech (v jednotkách osob)	Poškození zdraví (v jednotkách osob)	Finanční ztráta (v % HDP)
nízký	<0,1000)	0	<0,10)	<0,1
střední	<1000,75000)	<1,125)	<10,1250)	0,1 až 0,2
vysoký	<75000,12500>	<125,250>	<1250,2500>	0,2 až 0,5
kritický	>125000	>250	>2500	>0,5

[193] FREUND, Jack. *Measuring and managing information risk: a FAIR approach*. Amsterdam: Butterworth-Heinemann, 2015. ISBN 978-0-12-420231-3. s. 36–40.
[194] *Nařízení vlády č. 432/2010 Sb., Nařízení vlády o kritériích pro určení prvku kritické infrastruktury v posledním znění*

4.4 Riziková odvětví

Na základě kvantifikace hrozeb a dopadů lze vyjádřit rizikové oblastí národního hospodářství, kterým by měla být věnována větší pozornost. Tuto skutečnost zachycuje Tabulka 17 – Rizika v odvětví.

Tabulka 17 – Rizika v odvětví

kód	Sekce	Nedostupnost systému (DDoS)	Krádež know -how	Ovládnutí systému	Krádež osobních dat	Neautorizovaný převod peněz	Zašifrování dat
A	zemědělství, lesnictví a rybářství	1	1	2	1	2	1
B	těžba a dobývání	2	1	8	1	3	4
C	zpracovatelský průmysl	2	8	6	1	2	6
D	výroba a rozvod elektřiny, plynu, tepla a klimatizovaného vzduchu	6	1	8	2	3	4
E	zásobování vodou; činnosti související s odpadními vodami, odpady a sanacemi	6	1	16	2	2	4
F	stavebnictví	1	2	2	1	2	2
G	velkoobchod a maloobchod; opravy a údržba motorových vozidel	8	1	2	8	8	8
H	doprava a skladování	8	1	8	4	2	4
I	ubytování, stravování a pohostinství	2	1	4	4	2	2
J	informační a komunikační činnosti	16	3	12	8	2	4
K	peněžnictví a pojišťovnictví	12	2	8	12	8	12
L	činnosti v oblasti nemovitostí	1	1	1	1	2	2
M	profesní, vědecké a technické činnosti	1	16	1	1	2	3
N	administrativní a podpůrné činnosti	1	1	1	2	2	2
O	veřejná správa a obrana; sociální zabezpečení	8	1	16	6	2	16
P	vzdělávání	1	12	2	6	2	8
Q	zdravotní a sociální péče	8	2	16	8	2	12
R	kulturní, zábavní a rekreační činnosti	1	1	1	1	1	1
S	ostatní činnosti	1	1	1	1	1	1
T	činnosti domácností jako zaměstnavatelů;	1	1	1	1	1	1
U	činnosti exteritoriálních organizací a orgánů	1	1	1	1	1	1

4.5 Bezpečnostní opatření

Vůči hrozbám popsaným v kapitole 4.2 byla navrhnuta sada bezpečnostních opatření. U každého následujícího opatření je uveden účel podobně jako v revidovaném mezinárodním standardu ISO/IEC 27002:

1. **Používání vlastních dedikovaných účtů a silného hesla** nebo vícefaktorové autentizace by mělo zajistit, že takové heslo nebude útočníkem zneužito, uhádnuto ani prolomeno.
2. **Automatické uzamykání** obrazovky po určité době nečinnosti by mělo být dostatečnou ochranou před neoprávněným přístupem do zařízení, které může obsahovat citlivá data, nebo ze kterého lze přistupovat ke kritickým systémům.
3. **Striktní řízení přístupu,** a to jak k interním systémům a datům, tak i na internet, by mělo zajistit, že k datům a službám má přístup jen oprávněný uživatel, a to na základě nezbytné potřeby a může rovněž provádět jen nezbytně nutné operace, tím se podstatně zmenšuje povrch útoku, protože nestačí kompromitovat účet jakéhokoliv zaměstnance.
4. **Šifrování dat** v úložišti by mělo zajistit, že v okamžiku, kdy dojde ke ztrátě nebo krádeži zařízení, tak se útočník k uloženým datům nedostane, protože nebude znát šifrovací klíč.
5. **Bezpečnostní osvěta a trénink** zaměstnanců zvyšuje jejich odolnost vůči technikám sociálního inženýrství a zaměstnanci by se tak snadno neměli stát obětí útoku jako je phishing, vishing, SMShing, bating, tailgating apod.
6. **Nemožnost stahovat a spouštět jakýkoliv SW** je dostatečná ochrana před doručením škodlivého kódu prostřednictvím webové stránky ať už vědomě stažením anebo i nevědomě pouhou návštěvou dané stránky, e-mailem anebo paměťového média patřícímu uživateli anebo útočníkovi. Přičemž za SW je nutné považovat vše, tedy i nejrůznější doplňky, pluginy, skripty a makra.
7. **Včasné odstranění, nahrazení nebo aktualizace používaného SW,** a to jak krabicových, tak i těch vyvíjených na zakázku by mělo zajistit, že i kdyby útočník přišel na to, jak škodlivý kód spustit zneužitím nějaké známé zranitelnosti, tak v tomto případě nebude úspěšný, protože daný systém již nebude předmětnou zranitelnost obsahovat.

8. **Penetrační testy** by měly vést k odhalení nedostatků v systémech, které mohou být cílem hackingu nebo DDoS či DoS útoku.
9. **Oddělení interních systémů od internetu**, prostřednictvím samostatného zařízení, ať už fyzického nebo virtuálního pro přístup k poště a do internetu by mělo zajistit, že i v okamžiku, kdy by útočník zneužil zranitelnosti nultého dne a dané zařízení se mu podařilo kompromitovat, tak se z něj nedostane do interních systémů.
10. **IRP pro nejčastější kybernetické útoky**, např. odpojit uživatele, jehož účet byl kompromitován, anebo který je podezřelý ze zneužití svého přístup k interním systémům organizace, od sítě. To předpokládá odpojení jeho stanice i zablokování všech logických přístupů tohoto uživatele.
11. **DRP/BCP plány** předpokládají, že probíhá záloha, a testuje se i pravidelně čitelnost záloh a organizace si již obnovu dat a zprovoznění svých služeb v jiné lokalitě vyzkoušela.
12. **Detekce anomálií**, by měla zajistit, že nestandardní komunikace, větší datový tok v důsledku kopírování citlivých informací, pokus o zápis do registrů a chráněných částí operačního systému apod. bude včas detekován a tím bude odhalen škodlivý kód nebo nežádoucí aktivita zaměstnance.

Výše uvedená opatření nepůsobí izolovaně, ale vytvářejí tzv. obranu v hloubce před kybernetickými hrozbami, a to jak plošnými, tak i cílenými, která spočívá v tom, že když jedno opatření selže, tak je zde ještě určitá šance, že další opatření v řadě zafunguje.

Tabulka 18 – Typy opatření uvádí jednotlivá opatření včetně tagů tak, jak jsou uvedeny v revidované ISO/IEC 27002, aby bylo zřejmé, o jaký typ opatření se jedná (vzhledem k tomu, že některé pojmy jsou nové a není jisté, jak budou přeloženy, jsou uvedeny v původním znění):

- control types (#preventive, #detective, #corrective) – tedy zda opatření slouží k prevenci, detekci nebo nápravě;
- Information security properties (#confidentiality, #integrity, #availability) – tedy zda opatření slouží k zajištění důvěrnosti, integrity a dostupnosti;

- cybersecurity concepts (#identify, #protect, #detect, #respond, #recover) – tedy zda opatření slouží k identifikaci aktiv, ochraně, detekci, reakci a obnově po incidentu nebo útoku;

Tabulka 18 – Typy opatření

Opatření	control types	Information security properties	Cyber security concepts
1	#preventive	#confidentiality #integrity #availability	#protect
2	#preventive	#confidentiality #integrity #availability	#protect
3	#preventive	#confidentiality #integrity #availability	#protect
4	#preventive	#confidentiality #integrity	#protect
5	#preventive		#protect
6	#preventive	#confidentiality #integrity #availability	#protect
7	#preventive	#confidentiality #integrity #availability	#protect
8	#preventive	#confidentiality #integrity #availability	#detect
9	#preventive	#confidentiality #integrity #availability	#protect
10	#preventive		#respond
11	#corrective		#recover
12	#detective		#detect

4.6 Formulace vhodných otázek

Vhodná sada bezpečnostních opatření vyplynula z provedeného dotazníkového šetření a následného společného stanoviska expertní skupiny.

Nemenší pozornost je však třeba věnovat i správné formulaci jednotlivých otázek, a to tak, aby byla získána pokud možno pravdivá a ideálně i nezávislá odpověď na tom, kdo bude na otázku odpovídat.

Když se bude např. konzultant ptát ohledně zavedení určitého bezpečnostního opatření, tak se ze strany respondenta přímo nabízí odpověď, že je dané opatření zavedeno. Odpověď může být ANO, protože se to daná osoba domnívá, co víc, může o tom být i bytostně přesvědčena. Tento požadavek je přeci uveden v politice a slyšela to i na školení. Jenže zkusme se zeptat jinak, uvést konkrétní příklad, navodit určitou situaci, a dočkáme se najednou úplně jiné odpovědi.

Zde je lepší se neptat, zda je zavedeno konkrétní bezpečnostní opatření, ale vycházet z toho, že pokud by dané opatření bylo skutečně zavedeno, tak by nemohla nastat určitá situace. Zde dochází k efektivnímu využití dedukce, kdy v okamžiku, kdy máme zavedeno opatření A, které chrání aktivum před určitou hrozbou B, tak nemůže nastat situace C a v okamžiku, kdy nastane, tak víme, že A není pravda. Tedy jinými slovy, dané opatření není zavedeno vůbec anebo není efektivní.

Vzhledem k tomu, že cílem navrhnutých opatření je žádoucí změna chování ze strany zaměstnanců, tak je třeba se ptát, nikoli zda je dané opatření zavedené a na jakém stupni vyzrálosti, ale jak by reagoval konkrétní zaměstnanec dané organizace v určité situaci.

Otázky jsou proto záměrně formulovány tak, aby nevytvářely od počátku v zaměstnanci dojem, že se dopouští něčeho špatného a nenabízely správnou odpověď. Otázky je možné upravit podle toho, s kým bude interview vedeno, a to, co je např. kvůli běžnému uživateli vyjádřeno opisem, nahradit příslušným odborným termínem.

Byť je dotazník k dispozici v el. podobě, nepředpokládá se, že jej bude vždy vyplňovat respondent. Ideální je, když otázky pokládá analytik, a to tváří v tvář, aby mohl vyhodnotit, zda respondent správně porozuměl položené otázce a nemá tendenci lhát. Je třeba si dát pozor na sugestivní otázky a způsob, jakým jsou otázky pokládány[195]. Respondentovi je možné naznačit obě možné odpovědi, ale

[195] ČÍRTKOVÁ, Ludmila. *Policejní psychologie*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2015. ISBN 978-80-7380-581-4. s. 256.

nemělo by z toho vyplynout, která je ta správná. Dále je nutné si uvědomit, že respondent může tyto otázky vnímat jako citlivé a mít tendenci odpovídat tak, jak si myslí, že je očekáváno, jedná se o tzv. sociální desirabilitu[196]. Případně může z nejrůznějších důvodů odpovídat nepravdivě, což lze poznat z příznaků vyskytujících se ve shlucích[197], a pak je nutné jej přesvědčit, aby odpovídal dle skutečnosti[198].

1. Uživatelé si často stěžují, že je systém nutí si nastavit dostatečně dlouhé a silné heslo. Je tomu tak i ve vašem případě, jste nuceni si volit alespoň 12 znaků dlouhá hesla obsahující velká a malá písmena a čísla?
2. Uzamčení obrazovky po pár minutách nečinnosti většina uživatelů považuje za obtěžující. Dochází k tomu i ve vašem případě, uzamkne se obrazovka vašeho počítače po určité době nečinnosti, když na něm nepracujete, např. když telefonujete anebo se vzdálíte na toaletu nebo si uděláte ze zákona povinnou přestávku v práci?
3. Jedním z problémů současnosti je zahlcení informacemi. Máte vy i vaši kolegové přístup jen k informacím, které nezbytně nutně potřebujete pro svoji práci?
4. Jsou data na všem pracovním počítači šifrována? Pokud ne nebo neví, tak ověřit. V MS Windows je zpravidla hned viditelné v průzkumníku, kdy je disk označen ikonou zámku, v opačném případě ověřit např. kliknutím pravým tlačítkem myši na ikonu disku a vybrat Bitlocker Encryption Options nebo vlastnosti.
5. Jste školení a testování v oblasti kybernetické bezpečnosti, zkouší vás zaměstnavatel, jak jste obezřetní, např. zda otevřete přílohu každého e-mailu, který dostanete, jak zareagujete, když se vás někdo začne vyptávat na určité informace po telefonu, jak se zachováte, když najdete v zasedačce flashdisk, zda společně s vámi nemůže projít do budovy i neoprávněná osoba?

---

[196] CHYLÍKOVÁ, Johana. Úvod do problematiky výzkumu citlivých témat ve výběrových šetřeních. *Data a výzkum - SDA Info*. 2011, roč. 5, č. 2. ISSN 1802-8152. s. 185–206
[197] CRAIG, David. *Staňte se lidským detektorem lži: jak spolehlivě odhalit lháře*. Praha: Grada, 2014. ISBN 978-80-247-5365-2. s. 53.
[198] KONRÁD, Zdenek, Miroslav NEMEC a Frantisek NOVOTNÝ. *Vybrané otázky teorie a praxe výslechu*. Praha: Policejní akademie České republiky v Praze, 2008. ISBN 978-80-7251-294-2. s. 11.

6. Když byste zjistili, že k dokončení nějakého úkolu potřebujete nějaký speciální program, včetně skriptů, maker, pluginů do prohlížeče nebo Outlooku, který na svém pracovním počítači nemáte, můžete si jej donést na flashdisku, stáhnout z internetu, či poslat e-mailem? Pokud uživatel odpoví, že to je zakázáno, tak by měl následovat dotaz, zda je to zakázáno v interním předpise anebo to opravdu nejde a zda je možné to případně ověřit jednoduchým testem. (Uživateli se pošle odkaz, příloha se s neškodným skriptem, makrem a spustitelným souborem.)
7. Je veškerý váš SW aktuální? Běžný uživatel nebude nejspíš schopen na uvedenou otázku odpovědět, ale je možné provést namátkovou kontrolu. Tj. zeptat se, jaký SW používá a zjistit, jaká je jeho aktuální verze. (Např. kliknout v hlavním menu na položku Nápověda a O aplikaci…)
8. Provádíte pravidelně penetrační testy vašich systémů? Myšleno skutečné penetrační testy, nikoliv jen skeny zranitelností nebo kontrolu shody daného systému s politikou. Pravdivost odpovědi je možno ověřit dalšími dotazy, jako kdy naposledy a jakého systému se test týkal a zda je k dispozici závrečná zpráva apod.
9. Můžete z jednoho zařízení, aniž byste se museli hlásit na jiný účet nebo spouštět další systém, přistupovat do pošty, na internet a zároveň do ostatních systémů organizace, které potřebujete pro svoji práci?
10. Představte si, že by váš počítač nebo účet byl napaden hackerem. Dokáže vaše IT v případě potřeby zablokovat všechny vaše účty, aby z nich útočník do systému, k službám a k datům organizace nemohl přistupovat? Dokážete vybranému pracovníkovi zabránit v přístupu do všech systémů, kde má účet, a rovněž i do pošty a do internetu a odpojit jeho zařízení od podnikové sítě?
11. Když byste si omylem smazal nějaký důležitý soubor na síťovém disku anebo disk odešel, či byla data zašifrována ransomwarem, bude IT schopno tato data obnovit? Už se to někomu ve firmě stalo? Prováděli jste někdy test obnovy celého systému v jiné lokalitě?
12. Představte si, že se necítíte dobře, ale potřebujte ještě něco dodělat, můžete si v takovém případě poslat e-mailem soubor, na kterém pracujete, na svůj soukromý e-mail nebo nahrát na USB flash disk, aniž byste o to musel někoho žádat? Dokážete detekovat nestandardní provoz na sítí, kopírování citlivých

dat na paměťová média, stahování většího objemu dat z interních systémů apod.?

Tabulka 19 – Vyhodnocení kybernetické odolnosti zachycuje matici hrozba vs. opatření, včetně nastavení vah, které mohou být upraveny dle potřeby. Otázky jsou respondentovi pokládány po telefonu anebo má možnost vyplnit on-line dotazník, případně může vyplnění dotazníku probíhat asistovaným způsobem, kdy má respondent při vyplňování konzultanta na telefonu.

Tabulka 19 – Vyhodnocení kybernetické odolnosti

#	Bezpečnostní opatření vs. kybernetická hrozba **nastavení váh**	Správná odpov	DDoS (nevolumetrický)	Hacking webu, e-shopu,	Únik informací v důsledku	Generic malware	Ransomware	APT (krádež dat, ovládnutí IB, SCADA,	Insider theft	Účinnost opatř
1	Jsou šifrovaná data na disku vašeho koncového	ANO			70					70
2	Používáte dlouhá a komplexní hesla nebo	ANO			20					20
3	Dochází k automatickému	ANO			5				5	10
4	Když si omylem smažete nějaký soubor, dokáže	ANO				5	5			10
5	Jste pravidelně školeni a testování ohledně	ANO				15	10			25
6	Provádíte pravidelně bezpečnostní testy svého	ANO	80	80		15	10			185
7	Jsou všechny vaše systémy a aplikace	ANO		20		10	5			35
8	Je omezeno spouštění programů a skriptů?	ANO				20	20			40
9	Je oddělen přístup do internetu a e-mailu od	ANO				20	20		45	85
10	Dostanete se jen k datům nezbytně nutným	ANO			5	5	5		5	20
11	Můžete si do firemní sítě připojit své vlastní	NE				5	20		40	65
12	Dokážete okamžitě zablokovat všechny	ANO	20			5	5		5	35
	Maximální skóre, kterého lze dosáhnout	x	100	100	100	100	100		100	100

5 PŘÍNOSY PRÁCE

Přínos této práce lze spatřovat hned v několika oblastech, a to jak pro teorii, tak i pro praxi a vzdělávání.

5.1 Přínosy pro praxi

Hlavním přínosem této práce je především **veřejně dostupná metodika hodnocení bezpečnosti organizací, resp. jejich odolnosti vůči kybernetickým útokům.** Ta byla otestována a bylo ověřeno, že je použitelná jak pro soukromý, tak i pro veřejný sektor, a to bez ohledu na velikost organizace. V metodice hodnocení je rovněž uvedeno, jak by se dalo přistoupit k hodnocení celého sektoru nebo odvětví.

Vzhledem k tomu, že k dispozici je jak samotná metodika hodnocení, tak i **veřejně dostupná online webová aplikace, pomocí které zhodnocení může provést prakticky kdokoli, kdykoliv a odkudkoliv,** tak ji lze využít např. k rychlému zhodnocení situace organizace, organizační složky státu, ale i domácnosti, např. studenta nebo zaměstnance pracujícího z domova.

A nemusí se jednat jen o organizaci vlastní, protože stejným způsobem může být celkem rychle vyhodnocena bezpečnost v zahraniční pobočce, u potenciálního dodavatele, odběratele, v organizaci, která se má stát předmětem akvizice či fúze apod.

Byly identifikovány kybernetické hrozby, kterým organizace v ČR skutečně čelí, a škody, které organizacím v souvislosti s kybernetickými útoky reálně vznikají. **Navržená sada bezpečnostních opatření, pokud se ji organizace rozhodne implementovat, by ji měla před těmito hrozbami ochránit anebo alespoň minimalizovat následné škody**.

Tato veřejně dostupná metodika a nástroj pak může být dále rozvíjen, přizpůsobován a optimalizován s ohledem na aktuální situaci v kyberprostoru a potřeby konkrétních organizací nebo organizačních složek státu.

Práce ukazuje, jaký přístup k hodnocení kybernetické odolnosti organizace je možné zvolit. Tedy přístup je ryze pragmatický, protože určité vyhodnocení je vhodné mít vzhledem k turbulentním změnám v kyberprostoru ideálně hned.

Přínosy této práce lze spatřovat i v tom, že v okamžiku, kdy uvedenou metodiku nebo její obdobu budou pro hodnocení bezpečnosti používat i pojišťovny, bude **ve výsledku vyvinut větší tlak na pojistníky**, aby zavedly základní bezpečnostní opatření. To by mělo vést ke snížení objemu vzniklých škod, vytvoření bezpečnějšího prostředí a v konečném důsledku tak minimálně ke **zpomalení tempa růstu trestných činů páchaných v kyberprostoru**, které bude nutné vyšetřovat.

5.2 Přínosy pro vědu

Práce hned v úvodu poukázala na nejednoznačnost terminologie používané v oblasti informační a kybernetické bezpečnosti, především pokud jde o definici a chápání kybernetických hrozeb jako takových.

Práce popsala a objasnila vztahy mezi jednotlivými aktéry v kyberprostoru a vysvětlila, kdo za útoky stojí, a jakým typům kybernetických útoků organizace čelí, jak je zneužíváno zranitelností, jak dochází k průnikům do systémů a jaké to může mít dopady na samotnou organizaci i celé odvětví (kapitola 2.1).

Dalším přínosem je pak **objasnění hlavních příčin vzniku zranitelností, jejich zneužívání ze strany útočníků**, tak jak se vyvíjela informační architektura a měnily se i požadavky na zajištění bezpečnosti (kapitola 3.1.1 a 3.1.2). Tato část práce může být použita v rámci výuky předmětu informační a kybernetická bezpečnost.

Práce rovněž přinesla odpověď na otázku, **proč dochází k určitému zkreslování situace v kyberprostoru, kdo za ním stojí** a proč není možné vycházet jen ze sekundárních zdrojů, byť je lze považovat za důvěryhodné a proč je nutné se věnovat i vlastnímu výzkumu.

5.3 Přínosy pro pedagogiku/andragogiku

Dílčí dosažené výsledky byly zahrnuté do výuky na Policejní akademii v předmětech Bezpečnost informací – pro bakalářské studijní programy, Manažerská informatika – pro magisterské studijní programy, i v rámci kurzů celoživotního vzdělávání organizovaných Policejní akademií ČR „Kybernetická

trestná činnost“, které byly určené pro příslušníky Policie ČR s vyšší úrovní znalostí páchání kybernetické trestné činnosti zařazené na Služby kriminální policie a vyšetřování, zejména v pozicích analytiků a vyšetřovatelů.

6 NÁVRHY A DOPORUČENÍ

V průběhu psaní této práce byly identifikovány určité problematické oblasti, které by si zasloužily další pozornost.

1. Definovat pojem kybernetická hrozba a agent hrozby, aby bylo zřejmé, proti jakým hrozbám mají být bezpečnostní opatření nasazována.

2. Definovat exaktně taxonomii hrozeb, tj. jmenný výčet jednotlivých typů hrozeb, protože mezinárodní standardy a metodiky vydávané organizacemi jako je NIST, ENISA, SANS definují hrozby různě, a začlenit ji do VoKB.

3. Definovat exaktně zdroje hrozeb, tj. uvést jmenný výčet jednotlivých agentů hrozeb a začlenit jej do VoKB.

4. Doplnit metodiku výpočtu rizika, která není jednoznačná, neboť není zřejmé, zda se mají hrozby, zranitelnosti a dopad násobit či sčítat a jak výsledná rizika rozdělit do 4 stupňů.

5. Definovat způsob výpočtu škod, tj. exaktně stanovit, jak počítat následky kybernetických útoků, aby byly vzájemně porovnatelné, tak jak jej definuje např. metodika OpenFAIR.

6. Do hodnocení dopadů začlenit i dopady vyplývající z odmítnutelnosti, ztráty užitečnosti nebo převzetí kontroly nad systémem, neboť kritickou infrastrukturu státu tvoří nikoliv jen informační, ale i operační technologie.

7. Začlenit Parkerian hexad model do nové verze VoKB, tak aby byly správně klasifikovány kybernetické incidenty a útoky mající dopad na ztrátu kontroly nad systémem, ztrátu užitečnosti a narušení principu neodmítnutelnosti.

8. Zaměřit se na definici domén[199] a vinět[200] pro jednotlivé sektory národního hospodářství, minimálně pro KII, VIS a SZS, a jejich využití pro účely řízení rizik dle ZoKB a VoKB v ČR.

9. Realizovat výzkum zaměřený na stav kybernetické bezpečnosti v organizacích v ČR ze strany národní autority, aby zde byla větší důvěra ze strany respondentů a tím zajištěna i větší návratnost dotazníků.

10. Zvolit větší výběrový soubor, aby mohla být detailně analyzována i jednotlivá odvětví, která v tomto výzkumu měla nízkou relativní četnost.

11. Oslovovat každý rok stejné organizace se stejnou sadou otázek a sledovat vývoj v daném odvětví, protože jedině tak lze identifikovat trendy v dané oblasti.

12. Zaměřit se na firmy, které jsou součástí dodavatelského řetězce, a to nejen organizací provozující kritickou informační infrastrukturu, protože i na ty jsou vedeny útoky.

13. Detailně analyzovat věcnou významnost mezi odvětvím a velikostí organizace, sektorem a kritičností systému, protože nelze vyloučit, že zde nedojde ke změně a závislost zde nebude identifikována.

14. Vytvořit veřejně dostupnou centralizovanou databázi kybernetických incidentů a útoků na subjekty v ČR, které již byly porůznu zveřejněny. Umožnit důvěryhodným subjektům do této databáze přispívat za účelem získání představy o tom, co se skutečně děje v kyberprostoru.

15. Zveřejňovat s ohledem na situaci v kyberprostoru riziko ohrožení pro jednotlivá odvětví národního hospodářství.

16. Věnovat se více otázce ochrany operačních technologií a vydávat závazná doporučení i v této oblasti.

---

[199] CWE - CWRAF Domains [online]. [cit. 08.07.2021]. Dostupné z: https://cwe.mitre.org/cwraf/data/domains.html
[200] CWE - CWRAF Vignetes [online]. [cit. 08.07.2021]. Dostupné z: https://cwe.mitre.org/cwraf/creatingyourownvignettes.html

17. Podpořit výzkum AI/ML v oblasti rozpoznávání hrozeb za účelem včasné detekce těchto hrozeb SOC týmy využívajících SIEM řešení.

18. Provádět přísnější kontrolu, zda dochází k dodržování požadavků ZoKB a související VoKB v příslušných organizacích.

Ideálním kandidátem na realizaci výše uvedených doporučení by mohl být např. NÚKIB, který by na něm mohl spolupracovat s jednotlivými CSIRT týmy u nás i v zahraničí. **Výstupy z toho výzkumu by pak mohly být použitelné i pro policii, která by tak mohla lépe subsumovat jednotlivé trestné činy v kyberprostoru** a vyhodnocovat, v jaké oblasti dochází např. k nárůstu trestné činnosti, tedy v jakém odvětví, jaké systémy jsou napadány, jaké jsou použity vektory útoku, jaká opatření byla překonána a na jaký atribut bezpečnosti měl útok dopad, a jaká byla výše škod.

7 ZÁVĚR

Práce poukázala na skutečnost, že existují značné diskrepance mezi tím, jak kybernetické útoky interpretují média, která o nich informují, a jak probíhá jejich percepce ze strany samotné organizace a bezpečnostních expertů, kteří příslušné systémy a bezpečnostní opatření provozují.

V rámci výzkumu se podařilo identifikovat, jakým kybernetickým útokům organizace v ČR skutečně čelí, a že se v rozporu s mediálním diskursem zdaleka nejedná o útoky cílené, nýbrž především o útoky plošné zneužívající dlouho známých zranitelností, a dále pak kterých hrozeb se organizace nejvíce obávají a jaké finanční ztráty v případě materializace těchto hrozeb vznikají a jaká je úroveň bezpečnosti, resp. resilience jednotlivých organizací vůči těmto kybernetickým útokům.

V rámci výzkumu bylo dále zjištěno, že velikost organizace, sektoru a odvětví, ve kterém organizace působí, a rovněž i kritičnost provozovaného systému nemá věcně významný vliv na úroveň kybernetické resilience dané organizace, a tudíž subsumace organizace na základě těchto bazálních klasifikátorů neovlivňuje negativně exaktnost hodnocení ani rizikové skóre dané organizace.

V souladu s cílem práce byla navrhnuta a vytvořena metodika popisující způsob, jak je možné ke zhodnocení kybernetické odolnosti organizace vůči nejfrekventovanějším kybernetickým útokům přistoupit, a jak rychle a snadno identifikovat a kvantifikovat úroveň implementace relevantních bezpečnostních opatření.

Kromě metodiky hodnocení byl i vytvořen jednoduchý model a webová aplikace dostupná na adrese https://www.cleverandsmart.cz/kyberneticke-hrozby-dotaznik/. Funkčnost metodiky a aplikace pak byla opakovaně validována dotazníkovým šetřením ve vybrané organizaci, čímž bylo potvrzeno, že poskytuje opakovatelné a měřitelné výsledky a umožňuje toto zhodnocení provést kdykoliv a kýmkoliv a identifikovat tak rychle zásadní nedostatky spočívající v naprosté absenci některých fundamentálních bezpečnostních opatření.

Právě skutečnost, že evaluaci může realizovat v zásadě kdokoliv, tedy ne nutně jen expert v roli manažera informační nebo kybernetické bezpečnosti, je možné považovat za další nesporný benefit této metodiky, neboť tímto způsobem je

garantována i vyšší úroveň objektivity, neboť odpovědi na jednotlivé otázky nejsou poznamenány osobními zájmy manažera nesoucího odpovědnost za úroveň bezpečnosti v dané organizaci.

Výsledné hodnocení je však přesto nutné považovat spíše jen jako orientační, neboť jeho cílem není provést komplexní zhodnocení informační nebo kybernetické bezpečnosti v dané organizaci, nýbrž jen poukázat na nejfrekventovanější hrozby, vůči kterým organizace není dostatečně odolná a jaká bezpečnostní opatření by měla přijmout.

Lze předpokládat, že s ohledem na probíhající konvergenci operačních a informačních technologií, pokračující transformaci informačních technologií, a především zkracování životního cyklu vývoje, budou v dalších letech růst požadavky na pravidelné a rychlé vyhodnocování úrovně bezpečnosti a k vývoji těchto progresivních metodik a nástrojů by tato práce mohla rovněž pomoci. Nicméně aby to bylo možné, bude muset být i tato metodika pravidelně revidována a aktualizována rovněž s ohledem na aktuální kybernetické hrozby a značně turbulentní situaci v kyberprostoru.

Již teď se ukazuje, že by do hodnocení měla být zapracována např. otázka týkající se využití AI/ML v SIEM řešeních, které využívají SOC týmy, neboť pokud dojde ke zlepšení stávající úrovně bezpečnosti v organizacích, bude nutné počítat s větším počtem APT útoků. A ty organizace nebudou schopny se stávajícími řešeními odhalit, obzvláště pokud tyto útoky budou vedeny na operační technologie.

V rámci této práce bylo na základě analýzy proběhnuvších útoků, které byly dokumentovány v nejrůznějších reportech vydávaných organizacemi specializujícími se na kybernetickou bezpečnost, a dále pak vlastního výzkumu realizovaného mezi organizacemi v ČR, zjištěno, jaké jsou reálné hrozby, kterým organizace v ČR čelí, jakých hrozeb se tyto organizace obávají, jaké jsou dopady a materializace těchto hrozeb a jaká je úroveň kybernetické bezpečnosti, resp. odolnosti jednotlivých organizací vůči těmto kybernetickým útokům.

Bylo zjištěno, že největší hrozbu pro organizace z pohledu četnosti výskytu a možných následků představuje selhání vlastního HW a SW, výpadek služby třetí strany, výpadek proudu, krádež dat zaměstnancem a až pak typické kybernetické hrozby, jako je malware šířený plošně anebo v rámci APT útoku. Což je v rozporu

s tím, že jako největší hrozbu tyto organizace vnímají malware, kterým jim největší škodu zatím nezpůsobil.

Na základě zjištěných vektorů útoků byla navrhnuta metodika, která obsahuje sadu několika otázek, pomocí kterých lze velice rychle a snadno identifikovat úroveň zavedení bezpečnostních opatření v organizaci.

Tato metodika hodnocení byla opakovaně použita v praxi, čímž byla ověřena její použitelnost. Výhodou této metodiky je, že otázky mohou zodpovědět i běžní zaměstnanci, kteří se o bezpečnost nezajímají. Odpovědi tak nejsou zatíženy osobními zájmy manažera informační nebo kybernetické bezpečnosti, který zpravidla na podobné dotazy běžně odpovídá.

Zatímco vůči klasickým hrozbám jsou organizace poměrně dobře chráněny, neboť zavedly odpovídající bezpečnostní opatření, tak vůči pokročilým hrozbám již chráněny nejsou. Záloha dat, používání komplexních hesel, dvoufaktorová autentizace, aktualizace systémů a řízení přístupu k datům totiž nepředstavují dostatečnou ochranu před APT útoky. A v okamžiku, kdy k takovému útoku dojde, tak se pak škoda pohybuje v řádech statisíců až miliónů korun, takže investice do bezpečnostních opatření je v tomto případě nezbytná.

8 SEZNAM POUŽITÉ LITERATURY

Monografie

[1] BILGE, Leyla a Tudor DUMITRAS. Before we knew it: an empirical study of zero-day attacks in the real world. In: *the 2012 ACM conference*: *Proceedings of the 2012 ACM conference on Computer and communications security - CCS '12* [online]. Raleigh, North Carolina, USA: ACM Press, 2012, s. 833 [cit. 18.02.2019]. ISBN 978-1-4503-1651-4. DOI: 10.1145/2382196.2382284.

[2] *CISA review manual*. 27th edition. Schaumburg, IL, USA: ISACA, 2019. ISBN 978-1-60420-767-5.

[3] CRAIG, David. *Staňte se lidským detektorem lži: jak spolehlivě odhalit lháře*. Praha: Grada, 2014. ISBN 978-80-247-5365-2.

[4] ČÍRTKOVÁ, Ludmila. *Policejní psychologie*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2015. ISBN 978-80-7380-581-4.

[5] ČSÚ [ČESKÝ STATISTICKÝ ÚŘAD]. *Využívání informačních a komunikačních technologií v podnikatelském sektoru* [online]. Praha: Český statistický úřad, 2019 [cit. 10.07.2021]. ISBN 978-80-250-2902-2. Dostupné z: https://www.czso.cz/documents/10180/61601888/06200518.pdf/ce31b358-2dca-4204-b507-c7e4656064e7?version=1.1

[6] DE VAUS, D. A. *Surveys in social research*. Sixth edition. Abingdon, Oxon: Routledge, 2014. Social research today. ISBN 978-0-415-53015-6.

[7] DISMAN, Miroslav, Olga ŠMÍDOVÁ a Jiři ORT. *Jak se vyrábí sociologická znalost* [online]. 2011 [cit. 15.07.2020]. ISBN 978-80-246-2619-2. Dostupné z: http://site.ebrary.com/id/10887146

[8] ELLIS, Paul D. *The essential guide to effect sizes: statistical power, meta-analysis, and the interpretation of research results*. Cambridge ; New York: Cambridge University Press, 2010. ISBN 978-0-521-19423-5.

[9] FREUND, Jack. *Measuring and managing information risk: a FAIR approach*. Amsterdam: Butterworth-Heinemann, 2015. ISBN 978-0-12-420231-3.

[10] GARCIA, Sebastian a Michal PĚCHOUČEK. Detecting the Behavioral Relationships of Malware Connections. In: *PrAISe '16: International Workshop on AI for Privacy and Security*: *Proceedings of the 1st International Workshop on AI for Privacy and Security* [online]. The Hague Netherlands: ACM, 2016, s. 1–5 [cit. 06.02.2022]. ISBN 978-1-4503-4304-6. DOI: 10.1145/2970030.2970038.

[11] GIBSON, William. *Neuromancer*. 5. vyd. Praha: Euromedia Group, 2019. Mistrovská díla SF. ISBN 978-80-7617-760-4.

[12] HENDL, Jan. *Kvalitativní výzkum: základní teorie, metody a aplikace*. 2016. ISBN 978-80-262-0982-9.

[13] IEEE STAFF. *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT).* B.m.: Piscataway, 2016. ISBN 978-1-5090-4130-5.

[14] IVANČIĆ, Lucija, Dalia SUŠA VUGEC a Vesna BOSILJ VUKŠIĆ. Robotic Process Automation: Systematic Literature Review. In: Claudio DI CICCIO, Renata GABRYELCZYK, Luciano GARCÍA-BAÑUELOS, Tomislav HERNAUS, Rick HULL, Mojca INDIHAR ŠTEMBERGER, Andrea KŐ a Mark STAPLES, ed. *Business Process Management: Blockchain and Central and Eastern Europe Forum* [online]. Cham: Springer International Publishing, 2019 [cit. 26.06.2020], Lecture Notes in Business Information Processing. ISBN 978-3-030-30428-7. DOI: 10.1007/978-3-030-30429-4_19, s. 280–295

[15] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary.* Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6.

[16] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007. ISBN 978-80-247-1561-2.

[17] KINCL, Jaromír, Valentin URFUS a Michal SKŘEJPEK. *Římské právo*. Praha: C.H. Beck, 1995. ISBN 978-80-7179-031-0.

[18] KIRK, Roger E. *Statistics: an introduction*. 5th ed. Belmont, CA: Thomson/Wadsworth, 2008. ISBN 978-0-534-56478-0.

[19] KOLOUCH, Jan. *CyberCrime*. 1. vydání. Praha: CZ.NIC, z.s.p.o, 2016. Edice CZ.NIC, 14. publikace. ISBN 978-80-88168-15-7.

[20] KOLOUCH, Jan a Pavel BASTA. *CyberSecurity*. Praha: CZ.NIC, 2019. ISBN 978-80-88168-31-7.

[21] KONRÁD, Zdenek, Miroslav NEMEC a Frantisek NOVOTNÝ. *Vybrané otázky teorie a praxe výslechu*. Praha: Policejní akademie České republiky v Praze, 2008. ISBN 978-80-7251-294-2.

[22] KOZEL, Roman, Lenka MYNÁŘOVÁ a Hana SVOBODOVÁ. *Moderní metody a techniky marketingového výzkumu*. Praha: Grada, 2011. ISBN 978-80-247-3527-6.

[23] LACEY, David a INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION. *Advanced persistent threats: how to manage the risk to*

your business [online]. Rolling Meadows, IL: ISACA, 2013 [cit. 08.03.2019]. ISBN 978-1-60420-347-9. Dostupné z: http://www.books24x7.com/marc.asp?bookid=62388

[24] MANN, Ian. *Hacking the human: social engineering techniques and security countermeasures*. Aldershot, England ; Burlington, VT: Gower, 2008. ISBN 978-0-566-08773-8.

[25] MARCELLA, Albert J. *Cyber Forensics: Examining Emerging and Hybrid Technologies* [online]. 1. vyd. Boca Raton: CRC Press, 2021 [cit. 09.02.2022]. ISBN 978-1-00-305788-8. DOI: 10.1201/9781003057888.

[26] MITNICK, Kevin D a William L SIMON. *Umění klamu*. Gliwice: Helion, 2003. ISBN 978-83-7361-210-5.

[27] MOLNÁR, Zdeněk. *Pokročilé metody vědecké práce*. Zeleneč: Profess Consulting, 2012. ISBN 978-80-7259-064-3.

[28] OCHRANA, František, Vladimír ČECHÁK, Miroslav KRČ, Lenka SČERBANIČOVÁ a Jan SERÝCH. *Metodologie sociálních věd* [online]. 2013 [cit. 16.07.2020]. ISBN 978-80-246-2454-9. Dostupné z: http://site.ebrary.com/id/10852898

[29] PADUA, David, ed. *Encyclopedia of Parallel Computing* [online]. Boston, MA: Springer US, 2011 [cit. 04.02.2022]. ISBN 978-0-387-09765-7. DOI: 10.1007/978-0-387-09766-4.

[30] PARKER, Donn B. *Fighting computer crime: a new framework for protecting information*. New York: Wiley, 1998. ISBN 978-0-471-16378-7.

[31] PEIRCE, Charles S., Charles HARTSHORNE, Paul WEISS a Charles S. PEIRCE. *Scientific metaphysics*. 4. print. Cambridge, Mass: Belknap Press of Harvard Univ. Press, 1978. Collected papers of Charles Sanders Peirce, ed. by Charles Hartshorne ...; Vol. 6. ISBN 978-0-674-13802-5.

[32] POLČÁK, Radim, Jakub HARAŠTA a Václav STUPKA. *Právní problémy kybernetické bezpečnosti*. Brno: Masarykova univerzita, 2016. Spisy Právnické Fakulty Masarykovy Univerzity, svazek č. 576. Řada teoretická. ISBN 978-80-210-8426-1.

[33] PORTER, Michael E. *On competition*. Updated and expanded ed. Boston, MA: Harvard Business School Pub, 2008. The Harvard business review book series. ISBN 978-1-4221-2696-7.

[34] PUNCH, Keith. *Základy kvantitativního šetření*. Praha: Portál, 2008. ISBN 978-80-7367-381-9.

[35] REICHEL, Jiří. *Kapitoly metodologie sociálních výzkumů*. Praha: Grada, 2009. ISBN 978-80-247-3006-6.

[36] ŘEHÁK, David, Martin HROMADA a Pavel ŠENOVSKÝ. *Resilience kritické infrastruktury: teorie, principy, metody*. 2019. ISBN 978-80-7385-224-5.

[37] ŘEHÁK, Jan a Blanka ŘEHÁKOVÁ. *Analýza kategorizovaných dat v sociologii*. Praha: Academia, 1986.

[38] ŘEHKA, Karel. *Informační válka*. Vydání první. Praha: Academia, 2017. Edice XXI. století, sv. 46. ISBN 978-80-200-2770-2.

[39] SAUDEK, Karel a Ondřej NEFF. *Arnal a dva dračí zuby & jiné příběhy*. Praha: Egmont ČR, 2002. ISBN 978-80-7186-802-6.

[40] ŠIROKÝ, Jan. *Tvoříme a publikujeme odborné texty*. Brno: Computer Press, 2011. ISBN 978-80-251-3510-5.

[41] *The Administration's Clipper Chip Key Escrow Encryption Program*. B.m.: Forgotten Books, 2018. ISBN 978-0-484-26866-0.

[42] YIN, Robert K. *Applications of case study research*. 3rd ed. Thousand Oaks, Calif: SAGE, 2012. ISBN 978-1-4129-8916-9.

Časopisecké články

[1] BASTL, Martin a Zuzana GRUBEROVÁ. Kyberprostor jako „pátá doména"? *Vojenské rozhledy* [online]. 2013, roč. 22, č. 4. ISSN 12103292, 23362995. DOI: 10.3849/2336-2995.22.2013.04.010-021.

[2] BEDERNA, Zsolt a Tamas SZADECZKY. Cyber espionage through Botnets. *Security Journal* [online]. 2020, roč. 33, č. 1. ISSN 0955-1662, 1743-4645. DOI: 10.1057/s41284-019-00194-6.

[3] BINDE, Beth E, Russ MCREE a Terrence J O'CONNOR. Assessing Outbound Traffic to Uncover Advanced Persistent Threat [online]. 2011 [cit. 2022-02-02]. DOI: 10.13140/RG.2.2.16401.07520.

[4] ČERMÁK, Miroslav. DigiNotar: Operation Black Tulip. *CleverAndSmart Management Consulting* [online]. 2011 [cit. 17.02.2019]. ISSN 2694-9830. Dostupné z: https://www.cleverandsmart.cz/diginotar-operation-black-tulip/

[5] ČERMÁK, Miroslav. APT je jen další buzzword. *CleverAndSmart Management Consulting* [online]. 2012 [cit. 04.03.2019]. ISSN 2694-9830. Dostupné z: https://www.cleverandsmart.cz/apt-je-jen-dalsi-buzzword

[6] ČERMÁK, Miroslav. Mýty informační bezpečnosti aneb proč většina firem žije v bludu. *CleverAndSmart Management Consulting* [online]. 2012 [cit. -12.08.2019]. ISSN 2694-9830. Dostupné z: https://www.cleverandsmart.cz/myty-informacni-bezpecnosti-aneb-proc-vetsina-firem-zije-v-bludu

[7] ČERMÁK, Miroslav. Měly by se informace o zranitelnostech zveřejňovat? *CleverAndSmart Management Consulting* [online]. 2013 [cit. 18.02.2019]. ISSN 2694-9830. Dostupné z: https://www.cleverandsmart.cz/mely-by-se-informace-o-zranitelnostech-zverejnovat

[8] ČERMÁK, Miroslav. Přečtěte si, jak se najímají muly a vyvádějí peníze z bank – 4. díl. *CleverAndSmart Management Consulting* [online]. 2014 [cit. 28.05.2021]. ISSN 2694-9830. Dostupné z: https://www.cleverandsmart.cz/prectete-si-jak-se-najimaji-muly-a-vyvadeji-penize-z-bank-4-dil

[9] ČERMÁK, Miroslav. Jaký má bankovní malware reálný dopad do hospodářských výsledků bank. *CleverAndSmart Management Consulting* [online]. 2015 [cit. 28.05.2021]. ISSN 2694-9830. Dostupné z: https://www.cleverandsmart.cz/jaky-ma-bankovni-malware-realny-dopad-do-hospodarskych-vysledku-bank

[10] ČERMÁK, Miroslav. Krátké zamyšlení nad reputačním rizikem. *CleverAndSmart Management Consulting* [online]. 2015 [cit. 07.08.2019]. ISSN 2694-9830. Dostupné z: https://www.cleverandsmart.cz/jak-ridit-reputacni-rizika

[11] ČERMÁK, Miroslav. Roste počet útoků na SWIFT. *CleverAndSmart Management Consulting* [online]. 2016 [cit. 10.06.2020]. ISSN 2694-9830. Dostupné z: https://www.cleverandsmart.cz/roste-pocet-utoku-na-swift

[12] ČERMÁK, Miroslav. Slabina vs. zranitelnost a jaký je mezi nimi vztah. *CleverAndSmart Management Consulting* [online]. 2018 [cit. 12.04.2020]. ISSN 2694-9830. Dostupné z: https://www.cleverandsmart.cz/slabina-vs-zranitelnost-a-jaky-je-mezi-nimi-vztah

[13] ČERMÁK, Miroslav. Stinná stránka robotizace. *CleverAndSmart Management Consulting* [online]. 2018 [cit. 15.06.2020]. ISSN 2694-9830. Dostupné z: https://www.cleverandsmart.cz/stinna-stranka-robotizace

[14] ČERMÁK, Miroslav. Co vyplývá z většího množství false positive a false negative událostí? *CleverAndSmart Management Consulting* [online]. 2019 [cit. 18.09.2019]. ISSN 2694-9830. Dostupné z: https://www.cleverandsmart.cz/co-vyplyva-z-vetsiho-mnozstvi-false-positive-a-false-negative-udalosti

[15] ČERMÁK, Miroslav. Cyber resilience: Dwell time. *CleverAndSmart Management Consulting* [online]. 2019 [cit. 25.06.2019]. ISSN 2694-9830. Dostupné z: https://www.cleverandsmart.cz/cyber-resilience-dwell-time

[16] ČERMÁK, Miroslav. Cyber threat management: taxonomie hrozeb. *CleverAndSmart Management Consulting* [online]. 2019 [cit. 25.06.2021]. ISSN 2694-9830. Dostupné z: https://www.cleverandsmart.cz/cyber-threat-management-taxonomie-hrozeb

[17] ČERMÁK, Miroslav. Jak vzniká agregované bezpečnostní riziko. *Právo a bezpečnost*. 2019, roč. 2019, č. 3. ISSN 2336−5323.

[18] ČERMÁK, Miroslav. Mělo by být řízení informační bezpečnosti postavené na rizicích nebo opatřeních? *CleverAndSmart Management Consulting* [online]. 2019 [cit. 12.04.2020]. ISSN 2694-9830. Dostupné z: https://www.cleverandsmart.cz/melo-by-byt-rizeni-informacni-bezpecnosti-postavene-na-rizicich-nebo-opatrenich

[19] ČERMÁK, Miroslav. Nová média, názorové bubliny a profesionální žurnalistika: formy dezinformace. *CleverAndSmart Management Consulting* [online]. 2019 [cit. 07.08.2019]. ISSN 2694-9830. Dostupné z: https://www.cleverandsmart.cz/nova-media-nazorove-bubliny-a-profesionalni-zurnalistika-formy-dezinformace

[20] ČERMÁK, Miroslav. Ohrožuje přesun systémů do cloudu naše národní hospodářství a bezpečnost? *CleverAndSmart Management Consulting* [online]. 2019 [cit. 18.12.2019]. ISSN 2694-9830. Dostupné z: https://www.cleverandsmart.cz/ohrozuje-presun-systemu-do-cloudu-nase-narodni-hospodarstvi-a-bezpecnost

[21] ČERMÁK, Miroslav. Úskalí zajišťování digitálních stop v případě podezření na trestný čin neoprávněného přístupu k počítačovému systému. *Bezpečnostní teorie a praxe*. 2019, roč. 2019, č. 3. ISSN 2571-4589.

[22] ČERMÁK, Miroslav. Cyber threat management: zdroje hrozeb. *CleverAndSmart Management Consulting* [online]. 2020 [cit. 10.07.2021]. ISSN 2694-9830. Dostupné z: https://www.cleverandsmart.cz/cyber-threat-management-zdroje-hrozeb

[23] ČERMÁK, Miroslav. Identifikace klíčových aktérů ovlivňujících subjektivní percepci událostí v kyberprostoru. *Bezpečnostní teorie a praxe*. 2020, roč. 2020, č. 3. ISSN 2571-4589.

[24] ČERMÁK, Miroslav. Kdo na nás útočí, nevíme, jen se to domníváme a pak z toho vyvozujeme dalekosáhlé závěry. *CleverAndSmart Management Consulting* [online]. 2020 [cit. 09.05.2021]. ISSN 2694-9830. Dostupné z: https://www.cleverandsmart.cz/kdo-na-nas-utoci-nevime-jen-se-to-domnivame-a-pak-z-toho-vyvozujeme-dalekosahle-zavery

[25] ČERMÁK, Miroslav. Na obzoru se objevují nové hrozby, třeste se! – 7. díl. *CleverAndSmart Management Consulting* [online]. 2020 [cit. 20.03.2020]. ISSN 2694-9830. Dostupné z: https://www.cleverandsmart.cz/na-obzoru-se-objevuji-nove-hrozby-treste-se-7-dil

[26] ČERMÁK, Miroslav. Nejčastější úskalí IT smluv. *CleverAndSmart Management Consulting* [online]. 2020 [cit. 15.06.2020]. ISSN 2694-9830. Dostupné z: https://www.cleverandsmart.cz/nejcastejsi-uskali-it-smluv

[27] ČERMÁK, Miroslav. O skutečné situaci v kyberprostoru máme jen mlhavou představu. *CleverAndSmart Management Consulting* [online]. 2020 [cit. 12.04.2020]. ISSN 2694-9830. Dostupné z: https://www.cleverandsmart.cz/o-skutecne-situaci-v-kyberprostoru-mame-jen-mlhavou-predstavu

[28] ČERMÁK, Miroslav. Provozní technologie. *CleverAndSmart Management Consulting* [online]. 2020 [cit. 20.07.2020]. ISSN 2694-9830. Dostupné z: https://www.cleverandsmart.cz/provozni-technologie

[29] ČERMÁK, Miroslav. Provozní technologie: kybernetické útoky. *CleverAndSmart Management Consulting* [online]. 2020 [cit. 09.06.2020]. ISSN 2694-9830. Dostupné z: https://www.cleverandsmart.cz/provozni-technologie-kyberneticke-utoky

[30] ČERMÁK, Miroslav. Seznam organizací v ČR, na které byl veden kybernetický útok. *CleverAndSmart Management Consulting* [online]. 15. leden 2020 [cit. 26.04.2020]. Dostupné z: https://www.cleverandsmart.cz/seznam-organizaci-v-cr-na-ktere-byl-veden-kyberneticky-utok

[31] ČERMÁK, Miroslav. Úskalí řízení technických zranitelností. *Bezpečnostní teorie a praxe*. 2020, roč. 2020, č. 4. ISSN 2571-4589.

[32] ČERMÁK, Miroslav. Breach lifecycle se nám opět o něco prodloužil. *CleverAndSmart Management Consulting* [online]. 2022 [cit. 09.02.2022]. ISSN 2694-9830. Dostupné z: https://www.cleverandsmart.cz/breach-lifecycle-se-nam-opet-o-neco-prodlouzil

[33] ČERMÁK, Miroslav. Why Human Firewall Fails in the Battle with Sophisticated Spear Phishing Campaigns. In: Irena TUŠER a Šárka HOŠKOVÁ-MAYEROVÁ, ed. *Trends and Future Directions in Security and Emergency Management* [online]. Cham: Springer International Publishing, 2022 [cit. 28.01.2022], Lecture Notes in Networks and Systems. ISBN 978-3-030-88906-7. DOI: 10.1007/978-3-030-88907-4_16, s. 283–291

[34] ČERMÁK, Miroslav a Zdeněk KOVAŘÍK. Problémy determinace kybernetické bezpečnosti v prostředí České republiky – 1. část. *Bezpečnostní teorie a praxe*. 2021, roč. 2021, č. 1. ISSN 2571-4589.

[35] ČERMÁK, Miroslav a Zdeněk KOVAŘÍK. Problémy determinace kybernetické bezpečnosti v prostředí České republiky – 2. část. *Bezpečnostní teorie a praxe*. 2021, roč. 2021, č. 2. ISSN 2571-4589.

[36] ČERMÁK, Miroslav a Vladimír ŠULC. Kybernetická bezpečnost - praktický příklad kybernetického útoku. *Právo a bezpečnost*. 2018, roč. 2018, č. 3. ISSN 2336−5323.

[37] CHYLÍKOVÁ, Johana. Úvod do problematiky výzkumu citlivých témat ve výběrových šetřeních. *Data a výzkum - SDA Info*. 2011, roč. 5, č. 2. ISSN 1802-8152.

[38] MALÝ, Robert. Kauza Hacking Team, aneb jak funguje Remote Control System. *CleverAndSmart Management Consulting* [online]. 2015 [cit. 18.02.2019]. ISSN 2694-9830. Dostupné z: https://www.cleverandsmart.cz/kauza-hacking-team-aneb-jak-funguje-remote-control-system

[39] PARATI, Namita, DEPARTMENT OF CSE, BRECW, HYDERABAD, INDIA, Pratyush ANAND, a FUNCTIONAL CONSULTANT, FUJITSU PVT. LTD., HYDERABAD, INDIA. Machine Learning in Cyber Defence. *International Journal of Computer Sciences and Engineering* [online]. 2017, roč. 5, č. 12. ISSN 23472693. DOI: 10.26438/ijcse/v5i12.317322.

[40] RECHTIK, Marek. Kybernetická bezpečnost v automobilovém sektoru. *Bezpečnostní teorie a praxe*. 2021, roč. 2021, č. 2. ISSN 2571-4589.

[41] RECHTIK, Marek, Ondrůšek JAKUB a Siřinek TOMÁŠ. Hrozby vyplývající z použití doručovacích dronů v České republice. *Bezpečnostní teorie a praxe*. 2021, roč. 2021, č. 4. ISSN 2571-4589.

[42] SLÍŽEK, David. DDoS útok zasáhl weby mobilních operátorů, na možný atak se chystají i e-shopy. *Lupa.cz* [online]. 2013 [cit. 11.05.2021]. ISSN 1213-0702. Dostupné z: https://www.lupa.cz/clanky/ddos-pokracuje-cilem-jsou-dnes-weby-mobilnich-operatoru

[43] SOUKUP, Petr. Substantive significance and it´s measures. *Data and Research – SDA Info* [online]. 2013, roč. 127, č. 2 [cit. 01.02.2022]. ISSN 23362391. DOI: 10.13060/23362391.2013.127.2.41.

[44] VYLEŤAL, Martin. Tisíce tuzemských e-shopů mělo výpadky, může za to masivní DDoS útok. *Lupa.cz* [online]. 2011 [cit. 11.05.2021]. ISSN 1213-0702. Dostupné z: https://www.lupa.cz/clanky/tisice-tuzemskych-e-shopu-melo-vypadky-muze-za-to-masivni-ddos-utok

[45] WOLF, Karel. Matt Watchinski (Cisco Talos): Spamových e-mailů bylo jen v prosinci rozesláno přes 311 miliard. *Lupa.cz* [online]. 2019 [cit. 12.03.2019]. ISSN 1213-0702. Dostupné z: https://www.lupa.cz/clanky/matt-watchinski-cisco-talos-spamovych-emailu-bylo-jen-v-prosinci-rozeslano-pres-311-miliard

[46] ZETTER, Kim. Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. *Wired* [online]. 2016 [cit. 25.07.2021]. ISSN 1059-1028. Dostupné z: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid

Konferenční příspěvky

[1] KLESEL, Michael, Sebastian WEBER, Finja WALSDORFF a Bjoern NIEHAVES. Are Employees Following the Rules? On the Effectiveness of IT Consumerization Policies. In: *Wirtschaftsinformatik*: *Wirtschaftsinformatik 2019 Proceedings* [online]. 2019, s. 847–860 [cit. 02.02.2022]. Dostupné z: https://aisel.aisnet.org/wi2019/track07/papers/6

Zákonná úprava

[1] ČESKO. Zákon č. 40/2009 Sb. ze dne 8. ledna 2009 trestní zákoník. *Sbírka zákonů České republiky* [online]. 2009. ISSN 1211-1244. Dostupné z: https://www.mvcr.cz/soubor/sb011-09-pdf

[2] ČESKO. Zákon č. 181/2014 Sb. ze dne 23. července 2014 o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). *Sbírka zákonů České republiky* [online]. 2014. Dostupné z: https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=z&id=27231

[3] ČESKO. Vyhláška č. 82/2018 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) [online]. 2018. ISSN 1211-1244. Dostupné z: https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=38431

[4] ČSN ISO/IEC 27002. *Informační technologie - Bezpečnostní techniky - Soubor postupů pro opatření bezpečnosti informací*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví. 2014.

[5] ČSN ISO/IEC 27005. *Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví. 2019.

[6] *Nařízení vlády č. 315/2014 Sb., Nařízení vlády, kterým se mění nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury v posledním znění*

[7] *Nařízení vlády č. 432/2010 Sb., Nařízení vlády o kritériích pro určení prvku kritické infrastruktury v posledním znění*

Webové stránky a elektronické zdroje

[1] 2019 Cost of a Data Breach Report. *IBM Security* [online]. [cit. 2020-25-05]. Dostupné z: databreachcalculator.mybluemix.net

[2] Advanced Persistent Threats - Learn the ABCs of APT: Part A. *Secureworks.com* [online]. 2016 [cit. 2019-06-03]. Dostupné z: https://www.secureworks.com/blog/advanced-persistent-threats-apt-a

[3] *Akční plán k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020* [online]. 11. srpen 2015 [cit. 02.02.2022]. Dostupné z: https://www.nukib.cz/download/publikace/strategie_akcni_plany/akcni_plan_2015-2020.pdf

[4] BRUMAGHIN, Edmund. Covert Channels and Poor Decisions: The Tale of DNSMessenger [online]. [cit. 28.05.2021]. Dostupné z: http://blog.talosintelligence.com/2017/03/dnsmessenger.html

[5] BRUMFIELD, Cynthia. Equifax's data breach disaster: Will it change executive attitudes toward security? *Equifax's* [online]. 2019 [cit. 02.02.2022]. Dostupné z: https://www.csoonline.com/article/3411139/equifax-s-billion-dollar-data-breach-disaster-will-it-change-executive-attitudes-toward-security.html

[6] Bundesamt spricht sich gegen Huawei-Boykott aus. *Spiegel.de* [online]. 2018 [cit. 09.05.2021]. Dostupné z: https://www.spiegel.de/netzwelt/netzpolitik/5g-netzausbau-bsi-spricht-sich-gegen-huawei-boykott-aus-a-1243708.html

[7] CIMPANU, Catalin. Cisco removed its seventh backdoor account this year, and that's a good thing. *ZDNet* [online]. 2018 [cit. 09.05.2021]. Dostupné z: https://www.zdnet.com/article/cisco-removed-its-seventh-backdoor-account-this-year-and-thats-a-good-thing

[8] COLLIER, Kevin. A hacker tried to poison a Calif. water supply. It was as easy as entering a password. *NBC News* [online]. 2021 [cit. 25.07.2021]. Dostupné z: https://www.nbcnews.com/tech/security/hacker-tried-poison-calif-water-supply-was-easy-entering-password-rcna1206

[9] *Common Cyber Attacks: Reducing The Impact* [online]. 2015 [cit. 12.07.2021]. Dostupné z: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/400106/Common_Cyber_Attacks-Reducing_The_Impact.pdf

[10] Common Vulnerability Scoring System SIG. *FIRST — Forum of Incident Response and Security Teams* [online]. [cit. 18.02.2019]. Dostupné z: https://www.first.org/cvss

[11] CORCORAN, Brian. What Mondelez v. Zurich May Reveal About Cyber Insurance in the Age of Digital Conflict. *Lawfare* [online]. 8. březen 2019 [cit. 18.12.2019]. Dostupné z: https://www.lawfareblog.com/what-mondelez-v-zurich-may-reveal-about-cyber-insurance-age-digital-conflict

[12] Creating an AutoRun-Enabled Application (Windows). *Microsoft Docs* [online]. 2018 [cit. 25.06.2021]. Dostupné z: https://docs.microsoft.com/en-us/previous-

versions/windows/desktop/legacy/cc144206(v=vs.85)?redirectedfrom=MSDN

[13] CVE - Common Vulnerabilities and Exposures (CVE) [online]. [cit. 18.02.2019]. Dostupné z: https://cve.mitre.org/index.html

[14] CVE - CVE ID Syntax Change (Archived) [online]. [cit. 18.02.2019]. Dostupné z: https://cve.mitre.org/cve/identifiers/syntaxchange.html

[15] CVE - Request CVE IDs [online]. [cit. 18.02.2019]. Dostupné z: https://cve.mitre.org/cve/request_id.html

[16] CVSS Score Distribution For Top 50 Products By Total Number Of Distinct Vulnerabilities [online]. [cit. 18.02.2019]. Dostupné z: https://www.cvedetails.com/top-50-product-cvssscore-distribution.php

[17] CWE - Common Weakness Enumeration [online]. [cit. 18.02.2019]. Dostupné z: https://cwe.mitre.org

[18] CWE - CWRAF Domains [online]. [cit. 08.07.2021]. Dostupné z: https://cwe.mitre.org/cwraf/data/domains.html

[19] CWE - CWRAF Vignetes [online]. [cit. 08.07.2021]. Dostupné z: https://cwe.mitre.org/cwraf/creatingyourownvignettes.html

[20] ČERMÁK, Miroslav. Metodika hodnocení míry nebezpečnosti. *Hoax.cz* [online]. [cit. 08.06.2020]. Dostupné z: https://hoax.cz/cze/metodika-hodnoceni-miry-nebezpecnosti

[21] České zpravodajské servery čelily kybernetickému útoku - Novinky.cz [online]. 2013 [cit. 28.05.2021]. Dostupné z: https://www.novinky.cz/internet-a-pc/clanek/ceske-zpravodajske-servery-celily-kybernetickemu-utoku-183487

[22] ČSÚ [ČESKÝ STATISTICKÝ ÚŘAD]. *NACE REV. 2 METODICKÁ PŘÍRUČKA* [online]. 2011 [cit. 02.02.2022]. Dostupné z: https://www.czso.cz/documents/10180/23174387/metodicka_prirucka_cz_nace_rev_2.pdf/e26ebee3-a5b2-48a1-a036-75e14cdb8944?version=1.0

[23] ČSÚ [ČESKÝ STATISTICKÝ ÚŘAD]. *Postavení primárního sektoru v ekonomice ČR* [online]. 2014 [cit. 02.02.2022]. Dostupné z: https://www.czso.cz/documents/10180/20534368/320258a.pdf/e3976fc8-3a2f-4974-abeb-fa490b187bd7?version=1.0

[24] ČSÚ [ČESKÝ STATISTICKÝ ÚŘAD]. *Informační společnost v číslech 2017* [online]. 2017 [cit. 02.02.2022]. Dostupné z: https://www.czso.cz/documents/10180/46014808/061004-17_S.pdf

[25] ČTK. OKD má po útoku hackerů opět plně funkční hlavní PC systémy. Škoda činí miliony. *Deník.cz* [online]. 23. únor 2020 [cit. 28.05.2021].

Dostupné z: https://www.denik.cz/regiony/okd-ma-po-utoku-hackeru-opet-plne-funkcni-hlavni-pc-systemy-skoda-cini-miliony-20200223.html

[26] ČTK. Hackeři napadli systémy MPSV a pražského magistrátu. Data podle Maláčové neukradli. *Hospodářské noviny (iHNed.cz)* [online]. 5. březen 2021 [cit. 28.05.2021]. Dostupné z: https://domaci.ihned.cz/c1-66892210-system-verejne-spravy-napadli-hackeri-data-se-jim-podle-malacove-ukrast-nepodarilo

[27] DarkHotel APT: What It Is and How It Works. *www.kaspersky.com* [online]. 13. leden 2021 [cit. 11.05.2021]. Dostupné z: https://www.kaspersky.com/resource-center/threats/darkhotel-malware-virus-threat-definition

[28] DILMEGANI, Cem. Ultimate Guide to Robotic Process Automation (RPA) in 2020. *appliedAI* [online]. 22. listopad 2017 [cit. 25.06.2020]. Dostupné z: https://research.aimultiple.com/rpa

[29] ELČIĆ, Sandro. Část piva je z vadného chmele, mnohé sazenice jsou zdegenerované, zjistila kontrola. Může to ohrozit export. *Hospodářské noviny* [online]. 12. srpen 2019 [cit. 12.08.2019]. Dostupné z: https://ihned.cz/c1-66622070-cast-piva-je-z-vadneho-chmele-mnohe-sazenice-nejrozsirenejsi-odrudy-jsou-zdegenerovane-zjistila-kontrola-muze-to-ohrozit-export

[30] ENISA. *ENISA Threat Taxonomy* [online]. 2016 [cit. 10.06.2020]. Dostupné z: https://data.europa.eu/euodp/en/data/dataset/enisa-threat-taxonomy-1

[31] Fenix [online]. [cit. 28.05.2021]. Dostupné z: https://fe.nix.cz/#about

[32] Fileless attacks against enterprise networks. *Securelist* [online]. 2017 [cit. 28.05.2021]. Dostupné z: https://securelist.com/fileless-attacks-against-enterprise-networks/77403

[33] FIREEYE. *M-Trends 2019* [online]. 2019 [cit. 08.03.2019]. Dostupné z: https://content.fireeye.com/m-trends

[34] GENES, Raimund. Targeted Attacks versus APTs: What's The Difference? *TrendLabs Security Intelligence Blog* [online]. 2015 [cit. 12.03.2019]. Dostupné z: https://blog.trendmicro.com/trendlabs-security-intelligence/targeted-attacks-versus-apts-whats-the-difference

[35] *Global threat report* [online]. 2011 [cit. 12.07.2021]. Dostupné z: https://www.virusradar.com/sites/default/files/reports/2011-12-Global_Threat_Trends_December_2011.pdf

[36] *Global threat report* [online]. 2011 [cit. 25.06.2021]. Dostupné z: http://download.microsoft.com/download/0/3/3/0331766E-3FC4-44E5-B1CA-

2BDEB58211B8/Microsoft_Security_Intelligence_Report_volume_11_English.pdf

[37] GOLOVANOV, Sergey. ATMitch: remote administration of ATMs. *Securelist* [online]. 2017 [cit. 28.05.2021]. Dostupné z: https://securelist.com/atmitch-remote-administration-of-atms/77918

[38] Hacker napadl přerovskou školu, za zašifrovaná data žádá výkupné. *iDNES.cz* [online]. 2. prosinec 2021 [cit. 06.02.2022]. Dostupné z: https://www.idnes.cz/olomouc/zpravy/hacker-utok-prerov-travnik.A211202_204219_olomouc-zpravy_cun

[39] Hackers stole $6 million from Russian bank via SWIFT system, central bank says. *The Japan Times* [online]. 2018 [cit. 28.05.2021]. Dostupné z: https://www.japantimes.co.jp/news/2018/02/16/business/financial-markets/hackers-stole-6-million-russian-bank-via-swift-system-central-bank-says/#.XBpRfNVKiUk

[40] Hackeři napadli sítě Správy železnic, provoz vlaků neohrozili. *ČeskéNoviny.cz* [online]. 2021 [cit. 11.05.2021]. Dostupné z: https://www.ceskenoviny.cz/zpravy/hackeri-napadli-site-spravy-zeleznic-provoz-vlaku-neohrozili/2011847

[41] Hackeři se nabourali do systému tří pražských poliklinik, nefungují e-maily ani objednávkový systém. *iROZHLAS* [online]. 2021 [cit. 11.05.2021]. Dostupné z: https://www.irozhlas.cz/zpravy-domov/hackersky-utok-poliklinika-ipp-hackeri_2103161619_ada

[42] HackingTeam [online]. [cit. 18.02.2019]. Dostupné z: http://www.hackingteam.it

[43] HALLER, Martin. Jak vypadá vyjednávání o výkupném u ransomware. *Martin Haller* [online]. 11. květen 2020 [cit. 08.06.2020]. Dostupné z: https://martinhaller.cz/ransomware/jak-vypada-vyjednavani-o-vykupnem-u-ransomware

[44] HAMROZI, Petr. V IT byl homeoffice běžný, po koronaviru dál poroste. *Nejbusiness.cz* [online]. 2020 [cit. 08.06.2020]. Dostupné z: https://www.nejbusiness.cz/zpravy/2020-05-06-v-it-byl-homeoffice-bezny-po-koronaviru-dal-poroste

[45] HAY, Phil. Lnk files in Email Malware Distribution. *Trustwave* [online]. 2014 [cit. 28.05.2021]. Dostupné z: https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/lnk-files-in-email-malware-distribution

[46] HUMANITY, Vision of. Global Peace Index. *Vision of Humanity* [online]. [cit. 02.08.2019]. Dostupné z: http://visionofhumanity.org/indexes/global-peace-index

[47] Internetové bankovnictví zkolabovalo, další kybernetický útok mířil na banky - Novinky.cz [online]. 2013 [cit. 11.05.2021]. Dostupné z: https://www.novinky.cz/internet-a-pc/clanek/internetove-bankovnictvi-zkolabovalo-dalsi-kyberneticky-utok-miril-na-banky-183723

[48] KREBS, Brian. Privnotes.com Is Phishing Bitcoin from Users of Private Messaging Service Privnote.com. *KrebsonSecurity* [online]. 14. červen 2020 [cit. 22.06.2020]. Dostupné z: https://krebsonsecurity.com/2020/06/privnotes-com-is-phishing-bitcoin-from-users-of-private-messaging-service-privnote-com

[49] KREBS, Brian. Voice Phishers Targeting Corporate VPNs. *KrebsOnSecurity* [online]. 2020 [cit. 31.08.2020]. Dostupné z: https://krebsonsecurity.com/2020/08/voice-phishers-targeting-corporate-vpns

[50] KREČ, Luboš. Kapky v poušti aneb Velká reportáž z míst, kde vědí, jak vyzrát na sucho. *Forbes* [online]. 4. srpen 2019 [cit. 12.08.2019]. Dostupné z: https://www.forbes.cz/kapky-v-pousti-aneb-velka-reportaz-z-mist-kde-vedi-jak-vyzrat-na-sucho

[51] KUSHNER, David. The Real Story of Stuxnet - IEEE Spectrum. *IEEE Spectrum: Technology, Engineering, and Science News* [online]. [cit. 25.06.2021]. Dostupné z: https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

[52] Kyberbezpečnost a index bezpečnosti 2019. *Česká bankovní asociace* [online]. [cit. 04.06.2020]. Dostupné z: https://cbaonline.cz/kyberbezpecnost-a-index-bezpecnosti-2019

[53] Kyberkriminalita - Policie České republiky [online]. [cit. 17.12.2019]. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx

[54] LASSE LUETH, Knud. State of the IoT 2018: Number of IoT devices now at 7B – Market accelerating. *iot-analytics.com* [online]. 2018 [cit. 16.02.2019]. Dostupné z: https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b

[55] LAUNIUS, Steven. *Evaluation of Comprehensive Taxonomies for Information Technology Threats* [online]. 2018 [cit. 02.02.2022]. Dostupné z: https://sansorg.egnyte.com/dl/xWK7DWrT07

[56] LAYNE, Tom Bergin, Nathan. Special Report: Cyber thieves exploit banks' faith in SWIFT transfer network. *Reuters* [online]. 2016 [cit. 28.05.2021]. Dostupné z: https://www.reuters.com/article/us-cyber-heist-swift-specialreport-idUSKCN0YB0DD

[57] Letiště Praha se stalo terčem několika kybernetických útoků. Všechny se podařilo odvrátit. *iROZHLAS* [online]. 2020 [cit. 11.05.2021]. Dostupné z:

https://www.irozhlas.cz/zpravy-domov/kyberneticky-utok-prazske-letiste-vaclava-havla-it_2004171827_aur

[58] List of Top-Level Domains - ICANN [online]. [cit. 22.06.2020]. Dostupné z: https://www.icann.org/resources/pages/tlds-2012-02-25-en

[59] LN: Hackeři napadli na začátku dubna ČEZ Distribuci, útok byl odražen. *oEnergetice.cz* [online]. 21. duben 2020 [cit. 28.05.2021]. Dostupné z: https://oenergetice.cz/prenos-elektriny/ln-hackeri-napadli-na-zacatku-dubna-cez-distribuci-utok-byl-odrazen

[60] MARCUS, Imanuel. Germany: Increasing Cyber Attacks Against Power Grid. *The Berlin Spectator* [online]. 18. únor 2019 [cit. 25.07.2021]. Dostupné z: https://berlinspectator.com/2019/02/18/germany-increasing-cyber-attacks-against-power-grid

[61] MAURO, Andrea. Performance impact of CPU bug fixes - vInfrastructure Blog [online]. 25. srpen 2018 [cit. 17.02.2019]. Dostupné z: https://vinfrastructure.it/2018/08/performance-impact-of-cpu-bug-fixes

[62] MAYER, Marco, Iacopo CHIURAGI a Niccolo DE SCALZI. La politica Internazionale nell'Era Digitale (bozza da non citare) [online]. 2013, roč. 27 [cit. 16.02.2019]. Dostupné z: https://www.academia.edu/4509736/La_politica_Internazionale_nellEra_Digitale_bozza_da_non_citare_

[63] MICHLMAYR, Thomas. *European Commission Cloud Strategy* [online]. 2019 [cit. 18.12.2019]. Dostupné z: https://ec.europa.eu/info/sites/default/files/ec_cloud_strategy.pdf

[64] MILLS, Elinor. Attack on RSA used zero-day Flash exploit in Excel. *CNET* [online]. 2011 [cit. 08.03.2019]. Dostupné z: https://www.cnet.com/news/attack-on-rsa-used-zero-day-flash-exploit-in-excel

[65] MINAŘÍK, Pavel. Bezpečnost průmyslových sítí a systémů SCADA/ICS. *Bezpečnost průmyslových sítí a systémů SCADA/ICS* [online]. 2. říjen 2018 [cit. 12.03.2019]. Dostupné z: https://m.systemonline.cz/rizeni-vyroby/bezpecnost-prumyslovych-siti-a-systemu-scada-ics.htm

[66] MITRE ATT&CK® [online]. [cit. 25.06.2021]. Dostupné z: https://attack.mitre.org

[67] MUSA, Sam. Advanced Persistent Threat - APT [online]. 2014 [cit. 06.03.2019]. Dostupné z: https://www.academia.edu/6309905/Advanced_Persistent_Threat_-_APT

[68] Národní knihovnu v noci napadli hackeři, pro veřejnost je uzavřena. *ČeskéNoviny.cz* [online]. 2021 [cit. 28.05.2021]. Dostupné z:

https://www.ceskenoviny.cz/zpravy/narodni-knihovnu-v-noci-napadli-hackeri-pro-verejnost-je-uzavrena/2038834

[69] *Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020* [online]. 12. březen 2015 [cit. 10.07.2021]. Dostupné z: https://www.nukib.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2015-2020.pdf

[70] *Nařízení vlády č. 315/2014 Sb., Nařízení vlády, kterým se mění nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury v posledním znění*

[71] *Nařízení vlády č. 432/2010 Sb., Nařízení vlády o kritériích pro určení prvku kritické infrastruktury v posledním znění*

[72] NCSI :: Ranking. *e-Governance Academy* [online]. [cit. 02.08.2019]. Dostupné z: https://ncsi.ega.ee/ncsi-index

[73] NetMonitor [online]. [cit. 16.02.2019]. Dostupné z: http://www.netmonitor.cz

[74] New Banking Malware Uses Network Sniffing for Data Theft - TrendLabs Security Intelligence Blog [online]. 27. červen 2014 [cit. 28.05.2021]. Dostupné z: https://blog.trendmicro.com/trendlabs-security-intelligence/new-banking-malware-uses-network-sniffing-for-data-theft

[75] NIST. *NIST Special Publication 800-30 Guide for Conducting Risk Assessments* [online]. 2012 [cit. 17.02.2019]. Dostupné z: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf

[76] NIST. *Framework for Improving Critical Infrastructure Cybersecurity* [online]. 2014 [cit. 18.12.2019]. Dostupné z: https://www.nist.gov/document/cybersecurity-framework-021214pdf

[77] NIU, Evan. The SEC Really Wants Investors to Stop Buying the Wrong Zoom Stock [online]. 2020 [cit. 22.06.2020]. Dostupné z: https://www.nasdaq.com/articles/the-sec-really-wants-investors-to-stop-buying-the-wrong-zoom-stock-2020-03-27

[78] NOVÁK, Daniel. Únik dat z realitky ukazuje na obrovský bezpečnostní problém, říká expert. *Seznam Zprávy* [online]. 2021 [cit. 06.02.2022]. Dostupné z: https://www.seznamzpravy.cz/clanek/unik-dat-z-realitky-ukazuje-obrovsky-bezpecnostni-problem-rika-expert-173901

[79] Number of Internet Users (2016) - Internet Live Stats. *Internet Users* [online]. [cit. 16.02.2019]. Dostupné z: http://www.internetlivestats.com/internet-users

[80] NVD - CVSS v2 Calculator [online]. [cit. 18.02.2019]. Dostupné z: https://nvd.nist.gov/vuln-metrics/cvss/v2-calculator

[81] NVD - CVSS v3 Calculator [online]. [cit. 18.02.2019]. Dostupné z: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

[82] NVD - Home [online]. [cit. 18.02.2019]. Dostupné z: https://nvd.nist.gov

[83] OKD pokračuje v obnově dat. *ITBiz.cz* [online]. 6. leden 2020 [cit. 26.04.2020]. Dostupné z: https://www.itbiz.cz/zpravicky/okd-pokracuje-v-obnove-dat

[84] Olomoucká univerzita čelí útokům hackerů, jdou po e-mailech i výzkumech. *iDNES.cz* [online]. 5. březen 2019 [cit. 11.05.2021]. Dostupné z: https://www.idnes.cz/olomouc/zpravy/olomouc-univerzita-palackeho-kyberneticka-bezpecnost-utoky-hackeri-kradeze-dat-e-maily-phishing.A190301_460895_olomouc-zpravy_stk

[85] Olomoucký magistrát paralyzoval útok hackerů, město podá trestní oznámení. *iDNES.cz* [online]. 7. duben 2021 [cit. 28.05.2021]. Dostupné z: https://www.idnes.cz/olomouc/zpravy/olomouc-magistrat-utok-hackeru-datova-sit-kolaps.A210407_175516_olomouc-zpravy_stk

[86] OSVDB: FIN. *OSVDB* [online]. [cit. 18.02.2019]. Dostupné z: https://blog.osvdb.org/2016/04/05/osvdb-fin

[87] OWAIDA, Amer. European power grid organization hit by cyberattack. *WeLiveSecurity* [online]. 12. březen 2020 [cit. 04.06.2020]. Dostupné z: https://www.welivesecurity.com/2020/03/12/european-power-grid-organization-entsoe-cyberattack

[88] PAULSEN, Celia a Robert BYERS. *Glossary of key information security terms* [online]. NIST IR 7298r3. Gaithersburg, MD: National Institute of Standards and Technology. 2019 [cit. 02.02.2022]. DOI: 10.6028/NIST.IR.7298r3.

[89] PENDER-BEY, Georgie. *The parkerian hexad* [online]. 2012 [cit. 02.02.2022]. Dostupné z: http://cs.lewisu.edu/mathcs/msisprojects/papers/georgiependerbey.pdf

[90] Plzeňské školy napadli hackeři. Za vrácení dat chtěli milionové výkupné. *iDNES.cz* [online]. 10. květen 2018 [cit. 14.08.2019]. Dostupné z: https://www.idnes.cz/plzen/zpravy/hacker-internetovy-utok-krizikovo-gymnazium-stredni-skola-plzen-kybernetika-vypalne.A180510_084940_plzen-zpravy_vb

[91] PREATER, Andrew. Information as a commodity – at #radliblon. *Andrew Preater* [online]. 2014 [cit. 08.06.2020]. Dostupné z: https://www.preater.com/2014/06/03/information-as-a-commodity

[92] PŘENOSIL, Václav a Ibrahim GHAFIR. Advanced Persistent Threat and Spear Phishing Emails. *ResearchGate* [online]. 2015 [cit. 2019-12-03]. Dostupné z: https://www.researchgate.net/publication/305991054_Advanced_Persistent_Threat_and_Spear_Phishing_Emails

[93] RADZIKOWSKI, Przemek Shem. CyberSecurity: Expanded Look at the APT Life Cycle and Mitigation. *Dr.Shem* [online]. 11. únor 2016 [cit. 08.03.2019]. Dostupné z: http://DrShem.com/2016/02/11/cybersecurity-expanded-look-apt-life-cycle-mitigation

[94] RASCAGNÈRES, Paul. Poweliks: the persistent malware without a file [online]. 25. listopad 2016 [cit. 28.05.2021]. Dostupné z: https://www.gdatasoftware.com/blog/2014/07/23947-poweliks-the-persistent-malware-without-a-file

[95] REVULN. *Revuln.com* [online]. [cit. 18.02.2019]. Dostupné z: https://revuln.com

[96] SAMANI, Raj. „McAfee Labs Threats Report" Examines Cryptocurrency Hijacking, Ransomware, Fileless Malware. *McAfee Blogs* [online]. 12. březen 2018 [cit. 28.05.2021]. Dostupné z: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/mcafee-labs-threats-report-examines-cryptocurrency-hijacking-ransomware-fileless-malware

[97] SECURITY, Risk Based. Request the latest Vulnerability Quick View Report from Risk Based Security [online]. [cit. 18.02.2019]. Dostupné z: https://pages.riskbasedsecurity.com/2017-q3-vulnerability-quickview-report

[98] Shodan [online]. [cit. 17.02.2019]. Dostupné z: https://www.shodan.io

[99] SCHNEIER, Bruce. Advanced Persistent Threat (APT) - Schneier on Security. *Schneier on Security* [online]. 9. listopad 2011 [cit. 04.03.2019]. Dostupné z: https://www.schneier.com/blog/archives/2011/11/advanced_persis.html

[100] SIEMENS. Bezpečnost průmyslových dat je otázka správné strategie. *Národní centrum průmyslu 4.0* [online]. 2020 [cit. 16.06.2020]. Dostupné z: https://www.ncp40.cz/aktuality/bezpecnost-prumyslovych-dat-je-otazka-spravne-strategie

[101] Statistiky řešených incidentů - CSIRT [online]. [cit. 17.12.2019]. Dostupné z: https://csirt.cz/page/2635/statistiky-resenych-incidentu

[102] STEVEN J. VAUGHAN-NICHOLS. Don’t be the fool in the cloud. *Computerworld* [online]. 2017 [cit. 18.12.2019]. Dostupné z: https://www.computerworld.com/article/3233289/don-t-be-the-fool-in-the-cloud.html

[103] Systém Povodí Vltavy napadli hackeři. Přehrady ani dodávky vody v ohrožení nejsou. *Aktuálně.cz* [online]. 2020 [cit. 26.04.2020]. Dostupné z: https://zpravy.aktualne.cz/domaci/informacni-system-povodi-vltavy-napadli-hackeri/r~fe9196b478d811eab115ac1f6b220ee8

[104] ŠPIDLA, Aleš. Novela zákona o vojenském zpravodajství – potřebujeme ji? *IT SECURITY NETWORK NEWS* [online]. 26. únor 2019 [cit. 12.03.2019]. Dostupné z: https://www.itsec-nn.com/novela-zakona-o-vojenskem-zpravodajstvi-potrebujeme-ji

[105] The 2018 State of Endpoint Security Risk. *Ponemon Institute* [online]. 2018 [cit. 28.05.2021]. Dostupné z: https://www.ponemon.org/news-updates/news-press-releases/news/the-2018-state-of-endpoint-security-risk.html

[106] *The Non-Advanced Persistent Threat* [online]. 2014 [cit. 12.07.2021]. Dostupné z: https://www.imperva.com/docs/HII_The_Non-Advanced_Persistent_Threat.pdf

[107] TIDY, Joe. Marriott Hotels fined £18.4m for data breach that hit millions. *BBC News* [online]. 2020 [cit. 11.05.2021]. Dostupné z: https://www.bbc.com/news/technology-54748843

[108] TURTON, William a Kartikay MEHROTRA. Colonial Pipeline Cyber Attack: Hackers Used Compromised Password. *Bloomberg* [online]. 2021 [cit. 25.07.2021]. Dostupné z: https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

[109] Usage Statistics and Market Share of WordPress. *w3techs* [online]. 2020 [cit. 25.06.2020]. Dostupné z: https://w3techs.com/technologies/details/cm-wordpress

[110] VAMOSL, Robert. SQL Slammer: How it works--prevent it. *ZDNet* [online]. 2003 [cit. 25.06.2021]. Dostupné z: https://www.zdnet.com/article/sql-slammer-how-it-works-prevent-it

[111] VANHORN, Thom. The Evolution of Endpoint Security: Moving from Passive to Active Threat Management. *Channel Futures* [online]. 24. leden 2018 [cit. 10.03.2019]. Dostupné z: https://www.channelfutures.com/from-the-industry/the-evolution-of-endpoint-security-moving-from-passive-to-active-threat-management

[112] VENKAT0745. A patch is preventing the system from starting. In: *answers.microsoft.com* [online]. 20. únor 2014 [cit. 17.02.2019]. Dostupné z: https://answers.microsoft.com/en-us/windows/forum/all/a-patch-is-preventing-the-system-from-starting/590fab3b-6efc-46f1-beb0-9bb1d1dc7b29

[113] VERIZON. *2018 Data Breach Investigations Report* [online]. 2018 [cit. 10.07.2021]. Dostupné z: https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf

[114] VINCENT, James. Don't believe the story about hackers locking guests in their rooms at a luxury hotel. *The Verge* [online]. 30. leden 2017 [cit. 11.05.2021]. Dostupné z: https://www.theverge.com/2017/1/30/14438226/hackers-austrian-hotel-bitcoin-ransom-ransomware

[115] VulnDB [online]. [cit. 18.02.2019]. Dostupné z: https://vulndb.cyberriskanalytics.com

[116] Without a Trace: Fileless Malware Spotted in the Wild - TrendLabs Security Intelligence Blog [online]. 20. duben 2015 [cit. 28.05.2021]. Dostupné z: https://blog.trendmicro.com/trendlabs-security-intelligence/without-a-trace-fileless-malware-spotted-in-the-wild

[117] Worm:W32/CodeRed Description. *F-Secure Labs* [online]. 2001 [cit. 25.06.2021]. Dostupné z: https://www.f-secure.com/v-descs/bady.shtml

[118] Zaměstnanci chtějí home office. Splňte tyto 2 podmínky, aby práce z domu fungovala. *LMC* [online]. 2019 [cit. 17.12.2019]. Dostupné z: https://www.lmc.eu/cs/magazin/data-a-pruzkumy/zamestnanci-chteji-home-office-splnte-tyto-2-podminky-aby-prace-z-domu-fungovala

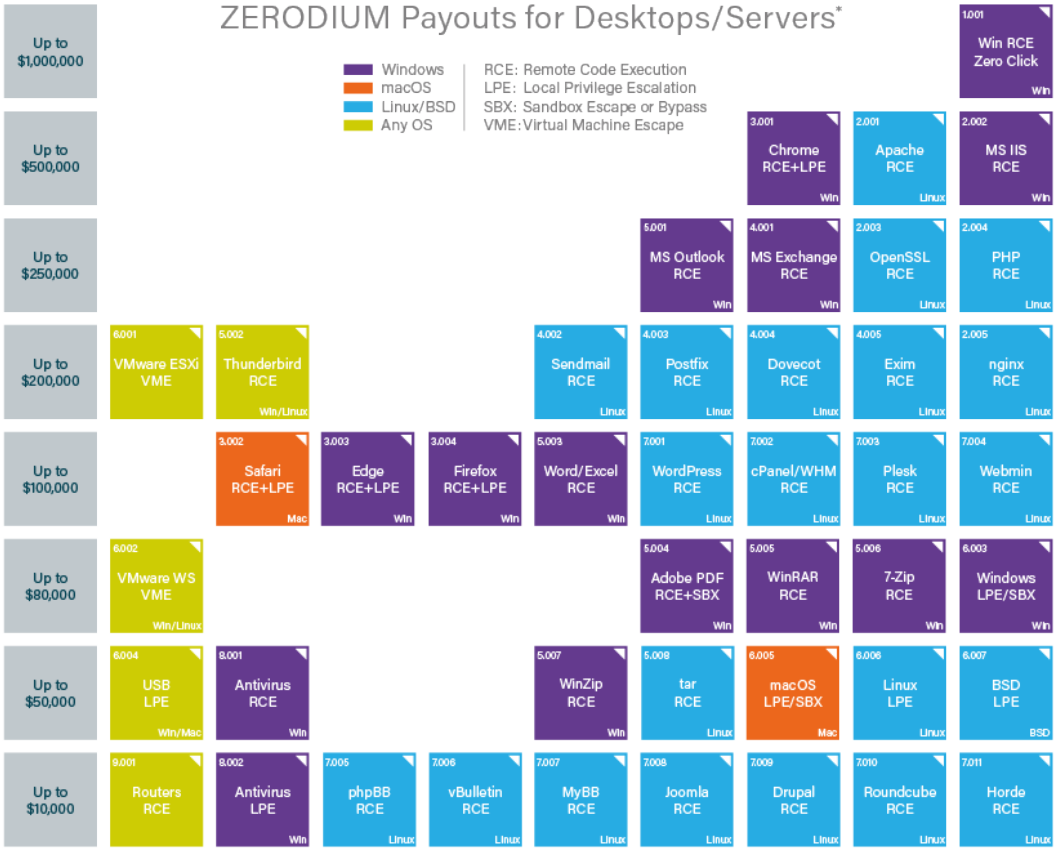
[119] ZDRNJA, Bojan. *Conficker's autorun and social engineering* [online]. 2009 [cit. 25.06.2021]. Dostupné z: https://isc.sans.edu/diary/Conficker%27s+autorun+and+social+engineering/5695

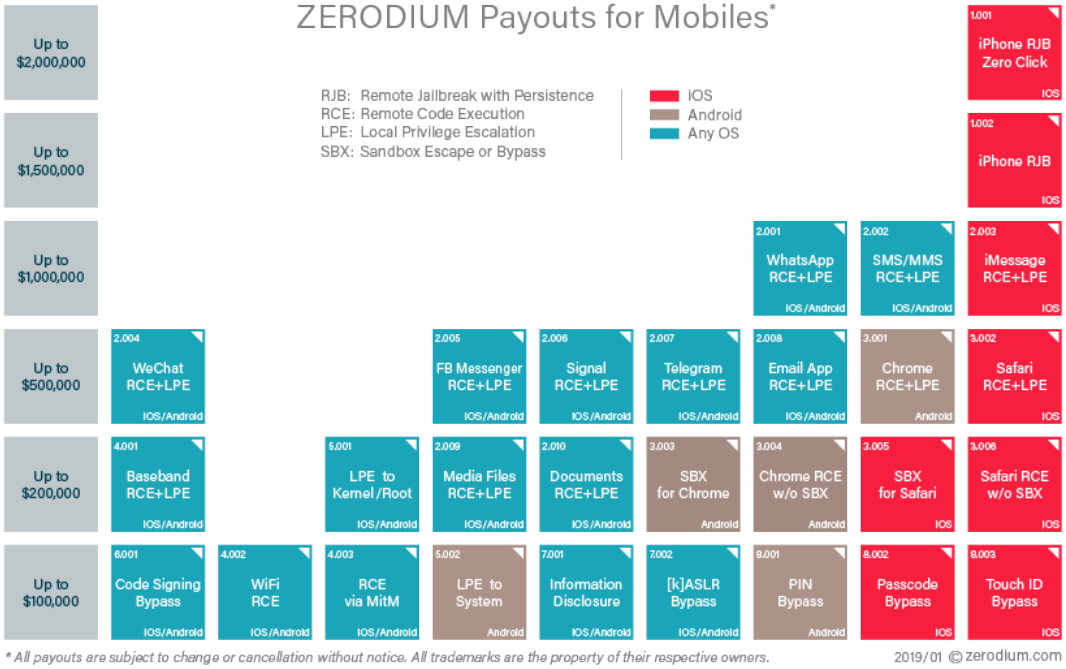
[120] ZELJKA, Zorz. Should you block newly registered domains? Researchers say yes. *Help Net Security* [online]. 23. srpen 2019 [cit. 20.03.2020]. Dostupné z: https://www.helpnetsecurity.com/2019/08/23/block-new-domains

[121] ZERODIUM - The Leading Exploit Acquisition Platform [online]. [cit. 17.02.2019]. Dostupné z: http://zerodium.com

9 SEZNAM PŘÍLOH

Příloha A – Odměna za zranitelnosti



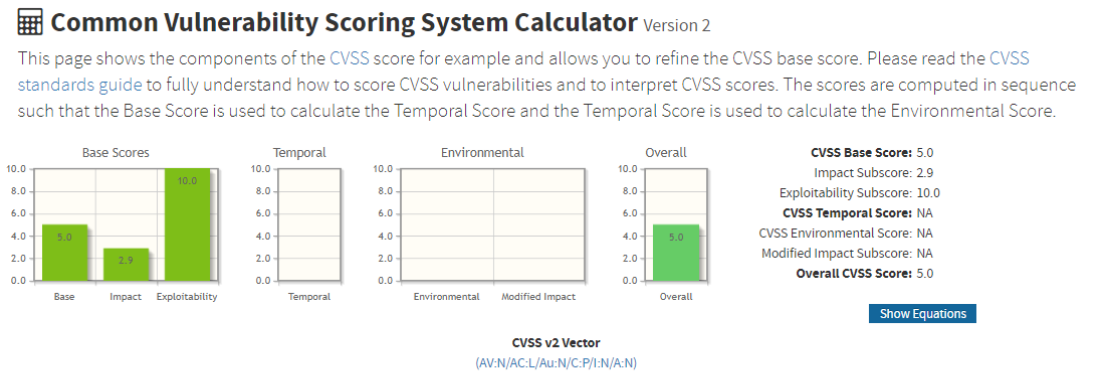


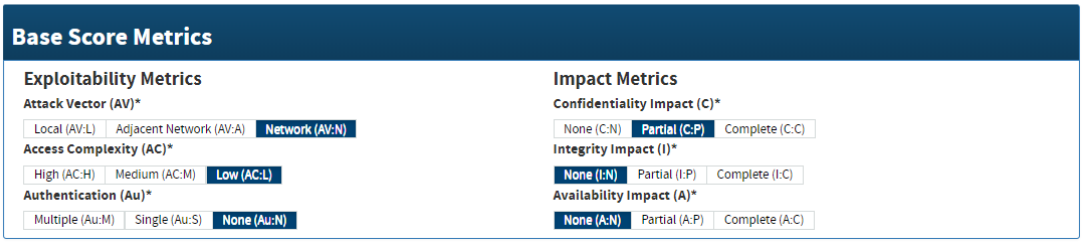
Příloha B – CVE zdrojová data

	9-10	8-9	7-8	6-7	5-6	4-5	3-4	2-3	1-2	0-1	Celkem
1999	164	-	259	17	252	88	10	86	4	14	880
2000	144	-	308	28	382	60	13	78	7	-	1 020
2001	150	-	622	41	533	141	18	145	27	-	1 677
2002	159	3	842	87	708	204	17	124	12	-	2 156
2003	134	4	540	104	415	230	18	69	13	-	1 527
2004	222	4	743	103	811	360	14	186	8	-	2 451
2005	309	1	1730	193	1 323	922	36	389	30	2	4 935
2006	427	1	2333	747	1 560	1 025	62	419	34	2	6 610
2007	980	34	2 145	1 099	848	1 179	76	120	35	4	6 520
2008	1 005	36	1 799	795	636	1 175	70	92	24	-	5 632
2009	1 033	21	1 665	723	873	1 220	83	94	21	3	5 736
2010	1 062	22	1 020	597	646	1 026	98	137	44	-	4 652
2011	899	23	902	428	783	860	112	102	46	-	4 155
2012	970	24	778	796	940	1 277	222	239	49	2	5 297
2013	914	39	784	745	845	1 340	241	200	78	5	5 191
2014	813	51	1 055	969	2 599	1 794	354	252	56	3	7 946
2015	1 204	46	1 151	1 069	1 013	1 402	309	225	54	11	6 484
2016	1 375	40	1 055	859	965	1 533	257	292	70	1	6 447
2017	1 524	61	2 739	2 349	2 525	4 070	737	548	133	28	14 714
2018	1 529	87	2 545	2 630	3 461	4 090	1 084	517	108	504	16 555
2019	80	5	60	153	105	223	47	34	4	374	1 085

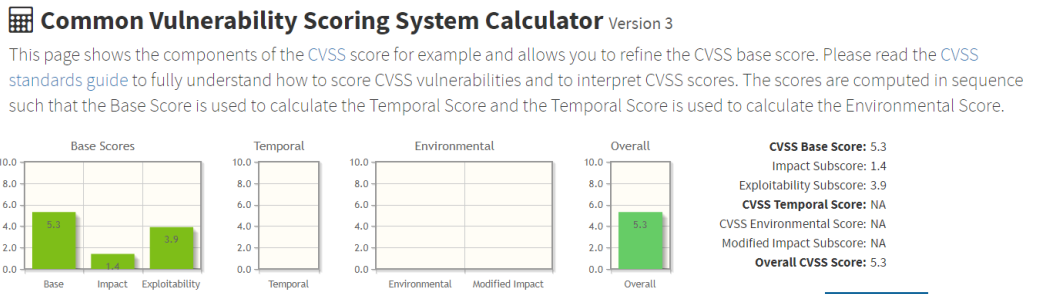
Příloha C – Rozdílné hodnocení zranitelností dle CVSSv2 a CVSSv3

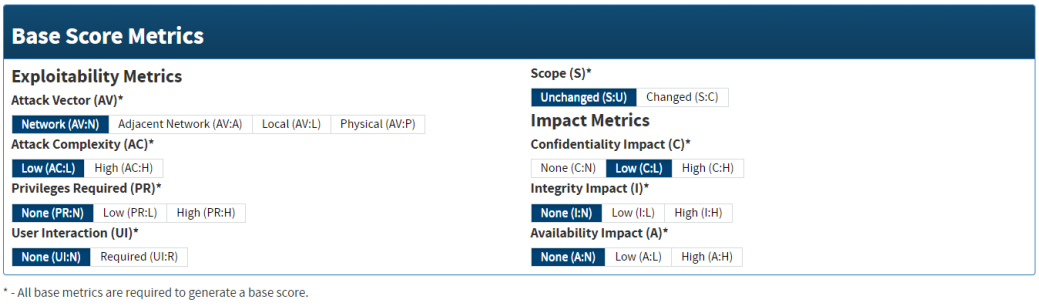
https://nvd.nist.gov/vuln-metrics/cvss/v2-calculator?vector=(AV:N/AC:L/Au:N/C:P/I:N/A:N)





https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N





Příloha D – Vzorec pro výpočet hodnoty zranitelnosti CVSSv3

If (Impact sub score <= 0) 0 else Scope Unchanged Round up (Minimum [(Impact + Exploitability), 10])
Scope Changed Round up (Minimum [1.08 × (Impact + Exploitability), 10])

Impact Subscore

Scope Unchanged $6.42 \times ISC_{Base}$
Scope Changed $7.52 \times [ISC_{Base} - 0.029] - 3.25 \times [ISC_{Base} - 0.02]^{15}$

$ISC_{Base} = 1 - [(1 - Impact_{Conf}) \times (1 - Impact_{Integ}) \times (1 - Impact_{Avail})]$

Exploitability sub score

ESC= 8.22 × AttackVector × AttackComplexity × PrivilegeRequired × UserInteraction

Metric	Metric Value	Numerical Value
Attack Vector	Network Adjacent Network Local Physical	0.85 0.62 0.55 0.2
Attack Complexity	Low High	0.77 0.44
Privilege Required	None Low High	0.85 0.62 (0.68 if Scope changed) 0.27 (0.50 if Scope / changed)
User Interaction	None Required	0.85 0.62

Metric	Metric Value	Numerical Value
C, I, A Impact	High Low None	0.56 0.22 0

Zdroj: https://www.first.org/cvss/specification-document

Příloha E – Životní cyklus zranitelnosti

Detailní scénář možného životního cyklu zranitelnosti:

- Vývojář vyvine SW, který obsahuje chybu, které je možno zneužít k napadení a ovládnutí koncového zařízení.
- Bezpečnostní výzkumník tuto chybu, resp. zranitelnost nultého dne (zero day vulnerability) v SW odhalí a informuje o ní firmu, která daný SW vyvinula. Ta však na oznámení této zranitelnosti nereaguje tak, jak očekával, tj. poděkováním a vyplacením odměny.
- Bezpečnostní odborník proto informaci o dané zranitelnosti často i spolu s exploitem, pomocí kterého je možné dané zranitelnosti zneužít, prodává na černém trhu.
- Bezpečnostní odborník informuje členy komunity na uzavřeném diskusním fóru o nalezené zranitelnosti a tím se tato zranitelnost stává známou většímu počtu lidí. Vznikají další exploity.
- Bezpečnostní odborník píše o nalezené zranitelnosti a jednání výrobce daného SW na svém blogu a informaci o nalezené zranitelnosti publikují i další média. O nalezené zranitelnosti se velice záhy dozvídají jak uživatelé daného SW, tak i útočníci. A je otázka, komu zveřejnění těchto informací vlastně pomůže.
- Exploit je dále prodáván a stává se součástí nejrůznějších nástrojů pro vývoj malware. Na webu jsou pak prodávány jak samotné nástroje umožňující začlenit tento exploit do nového malwaru, tak i samotný malware obsahující již tento exploit (Malware as a Service, zkr. MaaS anebo dokonce Crime as a Service, zkr. CaaS).
- Malware zneužívající zranitelnost nultého dne se dostává na zařízení nic netušících uživatelů daného SW, kdy jsou zneužívány různé vektory útoku.

- Malware provádí svoji škodlivou činnost, krade a šifruje data, provádí finanční transakce nebo se napadené zařízení stává součástí botnetu a je dále zneužíváno k dalším útokům.

- Vývojář SW, který obsahuje chybu, jež se dá zneužít, pracuje na jejím odstranění, anebo také ne, pokud se např. jedná o nějaké zařízení, u kterého se s žádným upgradem ani podporou nepočítalo.

- Vývojář SW uvolňuje patch, který odstraňuje nalezenou chybu, je však otázka, kdy bude na koncových zařízeních nasazen.

- Uživatel SW stahuje a instaluje patch, který danou chybu odstraňuje. Anebo také ne, pokud má třeba telefon s Androidem, nemusí se aktualizace dočkat nikdy.

- Chyba v SW je odstraněna a exploit již této chyby nemůže zneužít.

- Malware se však stále může nacházet na počítači uživatele a dál škodit, protože byť byla chyba v dané aplikaci odstraněna, malware tím odstraněn nebyl.

- Výrobce antiviru uvolňuje verzi, která je schopna daný malware detekovat a odstranit.

- Antimalware řešení na zařízení uživatele stahuje aktuální verzi virové databáze a vzorce chování[201], pomocí kterých je schopno daný malware detekovat a odstranit.

Výše uvedený seznam není vyčerpávající a také pořadí jednotlivých aktivit se může případ od případu lišit a k některým nemusí ani dojít.

[201] GARCIA, Sebastian a Michal PĚCHOUČEK. Detecting the Behavioral Relationships of Malware Connections. In: *PrAISe '16: International Workshop on AI for Privacy and Security*: *Proceedings of the 1st International Workshop on AI for Privacy and Security* [online]. The Hague Netherlands: ACM, 2016, s. 1–5 [cit. 06.02.2022]. ISBN 978-1-4503-4304-6. DOI: 10.1145/2970030.2970038.

Příloha F – RAM matice

V této matici je stručně zachycen harmonogram hlavních činností trvajících několik týdnů v rámci výzkumu realizovaného od května 2019 do června 2020, tedy něco přes rok.

Činnost	Čermák	Kovařík	Pracovní skupina	Harmonogram
Formulace výzkumného problému	A/R	I		květen 2019
Plán projektu	A/R	C		červen 2019
Naprogramování dotazníku	A/R	I	I	srpen–září 2019
Formulace otázek a odpovědí	A/R	C	C	květen–říjen 2019
Pilotáž	A/R	I	S	listopad 2019
Předvýzkum	A/R	I	S	prosinec 2019
Sběr dat	A/R	I		leden–duben 2020
Zpracování dat	A/R	I		květen 2020
Analýza dat	A/R	C		červen–září 2020
Sepsání a publikování závěrečné zprávy	A/R			říjen–prosinec 2020
Testování dotazníku na hodnocení firem	A/R		S	leden–březen 2021
Vyhodnocení dotazníku	A/R		S	duben–květen 2021

Legenda:

R – Responsible (realizuje)

A – Accountable (odpovídá)

S – Support (poskytnutí podpory)

C – Consult (daná osoba poskytuje konzultaci)

I – Inform (daná osoba je informována)

Čermák – Ing. Miroslav Čermák, CISM, CRISC
Kovařík – Dr. Zdeněk Kovařík, CSc.

Pracovní skupina – Ing. J. K., CSc., Bc. M. R., Dis., CISA, CISSP, Ing. R. M., CISM, CEH, CHFI (+ virtuální skupina Informační bezpečnost na sociální síti LinkedIn)

Harmonogram – přibližný harmonogram v měsících (naprogramování dotazníku a formulace otázek probíhala paralelně.) Na základě pilotáže a předvýzkumu došlo k drobným úpravám v logice dotazníku a úpravě otázek (tuto skutečnost harmonogram nepostihuje).

Příloha G – Seznam otázek

Sekce I. identifikace respondenta

Otázky v sekci I. slouží k získání základních informací o subjektu, jako je země, ve které se organizace nachází (Česká republika, Slovenská republika), sektor, ve kterém organizace působí (soukromý, veřejný), odvětví národního hospodářství dle klasifikace ekonomických činností NACE (A až U), velikost organizace dle počtu zaměstnanců (mikro podnik, malý podnik, střední podnik a velký podnik), významnost provozovaného informačního systému (žádný, SZS, VIS, KII) a v neposlední řadě i uváděnou konkurenční výhodou dle Portera. Respondent svou **nominální** odpověď vybírá z rozbalovacího menu. V této sekci je rovněž po respondentovi požadováno zadání e-mailu, ale jeho smysl není primárně v identifikaci klienta, jak je vysvětleno v kapitole 3.2.5.

Sekce II. Vyhodnocení opatření

Otázky v II. části slouží ke zjištění, zda má organizace zavedena vybraná bezpečnostní opatření. Kromě otázky je zde vždy uvedeno, jak otázku chápat a jak na ni odpovídat. Jedná se o **dichotomní** otázku a respondent na ní odpovídá jen „ANO“ nebo „NE“. Dále následuje seznam otázek v této sekci, včetně vysvětlení motivace otázky, které je uvedeno v závorce.

1. **Šifrujete data na disku vašeho koncového zařízení?**

Pokud šifrujete data, případně celé disky na svých koncových zařízeních a rovněž i paměťová média ve vašich mobilních zařízeních jako jsou SD karty a USB flash disky, na kterých přenášíte data, odpovězte ANO. V opačném případě odpovězte NE. (Pokud šifrování disků aktivováno není, tak kdokoliv, kdo se fyzicky zmocní daného zařízení, se může dostat k datům, která jsou na disku uložena, a data si zkopírovat anebo na něj i něco nahrát.)

2. **Používáte pro přihlášení do počítače komplexní hesla, passphrase nebo 2FA?**

Pokud jsou vaší bezpečnostní politikou pro přihlašování do systému a aplikací vynucována komplexní hesla obsahující velká a malá písmena, čísla a speciální znaky a jsou dlouhé více jak 9 znaků anebo používáte passphrase obsahující minimálně 4 slova či dvoufaktorovou autentizaci, odpovězte ANO. V opačném případě odpovězte NE. (Pokud nejsou vaši bezpečnostní politikou vynucena hesla delší než 8 znaků a obsahující minimálně velká a malá písmena a čísla anebo passphrase a následně dojde k úniku hashů hesel, tak tato hesla mohou být poměrně rychle prolomena.)

3. **Dochází k automatickému uzamčení obrazovky při nečinnosti?**

Pokud používáte zámek obrazovky a vaše zařízení se automaticky po určité době uzamkne, odpovězte ANO. Pokud se vaše koncové zařízení po určité době nečinnosti samo neuzamkne, odpovězte NE. (Pokud k uzamčení obrazovky nedochází, tak hrozí, že v okamžiku, kdy dojde ke ztrátě zařízení anebo jej někdo ukradne, tak se dostane k datům na něm uloženým.)

4. **Zálohujete pravidelně svá data?**

Pokud svá data zálohujete pravidelně, odpovězte ANO. Pokud pravidelně nezálohujete, odpovězte NE. (Pokud dojde ke ztrátě nebo zničení HW nebo napadení koncového zařízení ransomwarem a nebude k dispozici záloha, tak uživatel o veškerá svá data přijde.)

5. **Školíte a testujete své zaměstnance ohledně možných kybernetických útoků?**

Pokud školíte a testujete své zaměstnance, zda bezpečně zachází s informacemi a jsou odolní vůči technikám sociálního inženýrství, abyste si ověřili, jak zareagují např. na spear phishing, vishing, SMShing apod. alespoň jednou ročně, odpovězte ANO. Pokud školení a testy v této oblasti neprovádíte, odpovězte NE. (Školení a testy zaměstnanců by se měly provádět minimálně jednou ročně. Je zde pak podstatně větší šance, že si zaměstnanci včas všimnou, že je na ně veden kybernetický útok za použití sociálního inženýrství.)

6. **Provádíte pravidelné bezpečnostní testy vašich webových aplikací a infrastruktury?**

Pokud penetrační testy vašich webových a mobilních aplikací a rovněž i síťové infrastruktury provádíte alespoň jedenkrát ročně, odpovězte ANO. V opačném případě odpovězte NE. (Pravidelné bezpečnostní testy by měly zajistit, že chyby v aplikaci nebo infrastruktuře budou včas odhaleny a odstraněny a ochránit tak organizaci před útoky z internetu.)

7. **Jsou všechny vaše systémy a aplikace aktuální?**

Pokud provozujete jen podporované verze OS, máte nastavené automatické aktualizace OS včetně aplikací jako je prohlížeč, MS Office, JAVA, Adobe apod., případně jste schopni nasadit příslušný patch nebo novou verzi firmware ve vašich síťových zařízeních jako jsou Wi-Fi routery apod. do několika málo týdnů od zveřejnění zranitelnosti, odpovězte ANO. Pokud vám nasazení patche nebo nové verze trvá až několik měsíců, odpovězte NE. (Drtivá většina kybernetických hrozeb zneužívá již dlouho známé zranitelnosti, takže pokud bude systém a aplikace aktuální a budou včas nasazeny bezpečnostní patche, tak by organizace měla být před většinou z nich chráněna. Aktualizovány musí být včas všechny komponenty systému včetně síťových prvků.)

8. **Můžete na svém koncovém zařízení spustit jakýkoliv program nebo skript?**

Pokud můžete na firemním zařízení instalovat nový SW, doplňky do prohlížeče anebo spouštět spustitelné soubory a makra, které si stáhnete z internetu, pošlete e-mailem anebo donesete na USB flash disku, tak odpovězte ANO. V opačném případě, tj. kdy nic z výše uvedeného nemůžete, odpovězte NE. (Pokud na zařízení může uživatel spustit jakýkoliv program nebo skript, tak se může i poměrně snadno nakazit malwarem. Běžný uživatel by neměl mít právo na svém počítači instalovat a spouštět jiné než organizací schválené aplikace, a to včetně doplňků do prohlížeče a maker stažených nebo doručených e-mailem z internetu, což je vůbec nejčastější vektor útoku.)

9. **Používáte pro přístup do internetu/e-mailu jiné zařízení než do firemních systémů?**

Pokud můžete z firemního zařízení přistupovat jak na webové stránky na internetu, tak i zároveň pracovat v podnikovém systému, pak na tuto otázku odpovězte NE. V případě, že používáte dvě různá zařízení, a to ať už fyzická nebo virtuální, odpovězte ANO. (Pokud uživatel používá pro přístup do internetu i do firemního systému stejná zařízení a nakazí se, tak pak malware bude moci provádět ve firemním počítači a systému totéž co uživatel a dál se v síti šířit. V okamžiku, kdy používáte oddělené prostředí a jedno zda fyzické nebo virtuální, tak malware tuto možnost nemá.)

10. **Dostanete se jen k datům nezbytně nutným pro vaši práci?**

Pokud se dostanete jen k datům, které nezbytně nutně potřebujete pro svoji práci a k jiným datům a informacím se nedostanete, odpovězte ANO. Pokud se dostanete i k datům, které pro výkon své práce nepotřebujete, např. k datům, se kterými spíše pracují zaměstnanci z vedlejšího oddělení anebo kolega na jiné pozici, než jste vy, odpovězte NE, protože je zřejmé, že přístup k datům není striktně řízen. (Práva uživatelů v systému by měla být omezena na nezbytné minimum, protože v okamžiku, kdy dojde k napadení koncového zařízení malwarem, tak tento malware bude mít stejná práva jako aktuálně přihlášený uživatel.)

Výše uvedená opatření nepůsobí izolovaně, ale vytvářejí tzv. obranu v hloubce před kybernetickými hrozbami, a to jak plošnými, tak i cílenými, která spočívá v tom, že když jedno opatření selže, tak je zde ještě určitá šance, že další opatření v řadě zafunguje. Např. phishing může detekovat příjemce e-mailu, pokud však přílohu spustí, tak pak škodlivý kód může ještě detekovat antivirus, ale pokud i ten selže, tak pak může dojít ke kompromitaci daného zařízení, ale také nemusí.

Sekce III. Vyhodnocení četnosti útoků

Cílem sady otázek v této sekci je zjistit, s jakými útoky se respondent v minulém roce setkal a jak často. Vzhledem k tomu, že neexistuje jednotná taxonomie hrozeb, jak již bylo uvedeno v teoretické části této práce, tak byl seznam typických

hrozeb vytvořen na základě konsensu pracovní skupiny. Četnost výskytu jednotlivých útoků nebyla stanovena v intervalech udávajících počet výskytů daných útoků v průběhu roku, protože neexistuje metodika, jak jednotlivé útoky počítat, a byla místo toho použita **ordinální** škála umožňující lépe hodnotit zda je útok častý nebo nikoliv. Pokud se respondent s takovým útokem vůbec nesetkal, volí možnost "vůbec". Pokud se s takovým útokem setkal jen jednou, volí možnost "jednou". Pokud se s takovým útokem setkali během roku vícekrát, volí možnost "opakovaně" a konečně pokud se s takovým útokem setkává prakticky skoro každý týden nebo dokonce ještě častěji, volí možnost "soustavně".

11. **Zaznamenali jste skenování, inventarizaci, enumeraci ve vašich systémech?**

Někdo skenoval naše systémy, weby, aplikace, API, porty a snažil se zjistit, co na nich běží za služby, jaké jsou jejich verze, pokoušel se o enumeraci uživatelů apod.

12. **Došlo k hacknutí nějakého vašeho zařízení?**

Došlo ke zneužití zranitelnosti v provozovaném síťovém prvku, systému, webové aplikace vystavené do internetu, spoofingu, tamperingu, eskalaci privilegií, neošetřenému vstupu.

13. **Byl na vás veden volumetrický DDoS útok?**

Byl detekován volumetrický DDoS, realizovaný z více počítačů.

14. **Byl na vás veden aplikační DoS útok?**

Byl detekován aplikační DoS na zdroje, jako je paměť, diskový prostor, web, aplikace, služby.

15. **Došlo k nakažení nějakého vašeho koncového zařízení drive-by download malwarem?**

Při surfování po internetu byl na webové stránce antivirem detekován škodlivý kód.

16. **Byl někomu z vašich zaměstnanců doručen phishing e-mail se škodlivým kódem?**

V příloze e-mailu byl antivirem detekován škodlivý kód.

17. **Byl někomu z vašich zaměstnanců doručen phishing e-mail s odkazem?**

Do e-mailové schránky byl doručen e-mail, který byl příjemcem e-mailu označen jako phishing.

18. **Byl někomu z vašich zaměstnanců doručen spear phishing e-mail?**

Do e-mailové schránky byl doručen e-mail, který byl přesně zacílený na danou osobu.

19. **Volal do vaší firmy někdo, kdo se vydával za někoho jiného a snažil se ze zaměstnanců vytáhnout informace?**

Bylo voláno konkrétní osobě a proběhl pokus získat informace nebo ji donutit k provedení určité akce.

20. **Stáhl si někdo z vašich zaměstnanců do svého koncového zařízení trojanizovanou aplikaci?**

Ve stahované aplikaci byl antivirem detekován škodlivý kód.

21. **Připojil někdo z vašich zaměstnanců do sítě externí médium se škodlivým kódem?**

Bylo zajištěno externí paměťové médium, např. USB flash disk, SD karta se škodlivým kódem, HW keylogger.

22. **Došlo k fyzickému průniku neoprávněné osoby do chráněných prostor?**

Neoprávněná osoba fyzicky pronikla do prostor organizace, piggybacking, tailgating apod.

Sekce IV. Vyhodnocení dopadů

Cílem této sady otázek je zjistit, jaký byl následek útoku, tedy zda vznikla nějaká škoda a pokud ano, tak v jaké výši. Respondent, pokud uvedený útok na jeho organizaci neznamenal, tak volí možnost "nedošlo". Pokud útok proběhl, ale nevznikla žádná škoda, např. proto, že má účinná bezpečnostní opatření, tak volí **kardinální** možnost "žádná", a konečně, pokud mu nějaká škoda vznikla, měl by se pokusit určit, v jaké výši, stačí uvést hrubý odhad, tedy zda škoda byla v řádu tisíců, statisíců anebo přes milión, přičemž by respondent neměl zapomenout do výše škody započíst i ztrátu produktivity, tržní příležitosti, náklady na obnovu apod. Odhady možných škod v této sekci byly stanoveny v korunách a uvedená rozmezí byla zvolena s ohledem na možné škody, ke kterým v organizacích v podobných případech, které byly vyšetřovány, došlo.

23. Došlo u vás k výpadku proudu?

(výpadek dodávky el. proudu)

24. Došlo k výpadku služby u třetí strany?

(výpadek u provozovatele DC, cloudu, ISP)

25. Došlo k selhání vašeho vlastního HW/SW?

(selhání vlastního HW/SW bez cizího přičinění v důsledku vyšší moci)

26. Došlo k nedostupnosti v důsledku volumetrického DDoS útoku?

(systém/služba/infrastruktura nedostupná v důsledku volumetrického DDoS útoku)

27. Došlo k nedostupnosti v důsledku aplikačního DoS útoku?

(systém/služba/infrastruktura nedostupná v důsledku aplikačního DoS útoku)

28. Došlo ke kompletnímu ovládnutí vašeho systému útočníkem? (APT)

(informační systém organizace nebo ICS/SCADA zcela pod kontrolou útočníka, došlo ke změně kritických dat, výroba stála/služba nebyla poskytována, docházelo k chybám, produkci zmetků)

29. **Došlo k začlenění nějakého vašeho zařízení do botnetu? (hacking)**

(hack serverů, stanic, IoT a jejich zneužití k dalším podvodným aktivitám, začlenění do botnetu, rozesílání SPAMu, provoz PROXY, phishing web, VoIP volání apod.)

30. **Došlo v důsledku hackingu ke změně vaší webové stránky? (Defacement)**

(pozměněna úvodní webová stránka)

31. **Došlo k neautorizovanému převodu peněz z vašeho firemního účtu? (APT)**

(odčerpání značného množství finančních prostředků z účtu v důsledku napadení a ovládnutí systému umožňující bezhotovostní převod finančních prostředků)

32. **Došlo k nakažení nějakého vašeho zařízení malwarem?**

(v systému byl nalezen škodlivý kód, který musel být odstraněn)

33. **Došlo k zašifrování některých vašich dat ransomwarem?**

(zašifrována data na discích v důsledku napadení koncového zařízení nebo serveru)

34. **Došlo ze strany vašeho zaměstnance nebo třetí strany k sabotáži?**

(zneužití přístupu zaměstnancem, který měl nebo získal přístup do systému a k datům a pozměnil je nebo nainstaloval logickou bombu)

35. **Došlo k úniku citlivých informací v důsledku APT útoku?**

(zcizeny citlivé osobní údaje klientů, zaměstnanců, hesel, strategické plány, chráněné receptury, firemní know-how, popisy a technické výkresy nových produktů a služeb)

36. Došlo ke krádeži citlivých dat vaším zaměstnancem?

(zneužití přístupu zaměstnancem, který měl nebo získal přístup k datům a zkopíroval je, zneužil pro svoji potřebu anebo prodal)

37. Došlo k úniku informací v důsledku nedbalosti?

(odeslání e-mailu omylem, ztráta/vyřazení počítače či médií s citlivými daty)

38. Došlo k očerňující kampani vaší organizace na internetu?

(negativní recenze, příspěvky v diskusním fóru, dezinformační kampaň, otrávení výsledků vyhledávání apod.)

Sekce V. Obavy

Cílem této sady otázek je zjistit, jakých událostí se manažer informační a kybernetické bezpečnosti nejvíce obává. Možné obavy byly stanoveny na základě řízeného rozhovoru s manažery informační a kybernetické bezpečnosti a pracovníky útvaru CSIRT provádějícími cyber threat intelligence a predikce a kvalitativní analýzu bezpečnostních reportů a predikce hrozeb. Respondent vybírá z možných odpovědí „vůbec, spíše ne, spíše ano, velmi“.

39. Obáváte se výpadku proudu?

(výpadek dodávky el. proudu)

40. Obáváte se výpadku služeb u třetí strany?

(výpadek u provozovatele DC, cloudu, ISP)

41. Obáváte se selhání vlastního HW/SW?

(selhání vlastního HW/SW bez cizího přičinění v důsledku vyšší moci)

42. Obáváte se volumetrických DDoS útoků?

(systém/služba/infrastruktura nedostupná v důsledku volumetrického DDoS útoku)

43. Obáváte se aplikačních DoS útoků?

(systém/služba/infrastruktura nedostupná v důsledku aplikačního DoS útoku)

44. Obáváte se kompletního ovládnutí vašeho systému útočníkem? (APT)

(informační systém organizace nebo ICS/SCADA zcela pod kontrolou útočníka, došlo ke změně kritických dat, výroba stála/služba nebyla poskytována, docházelo k chybám, produkci zmetků)

45. Obáváte se začlenění vašeho zařízení do botnetu? (hacking)

(zneužití k dalším podvodným aktivitám, začlenění do botnetu, rozesílání SPAMu, provoz PROXY, phishing web, VoIP volání apod.)

46. Obáváte se neautorizované změny vašich webových stránek?

(Defacement)

47. Obáváte se neautorizovaného převodu peněz z vašich účtů? (APT)

(odčerpání značného množství finančních prostředků z účtu v důsledku napadení a ovládnutí systému umožňující bezhotovostní převod finančních prostředků)

48. Obáváte se generického malware?

(v systému byl nalezen škodlivý kód, který musel být odstraněn)

49. Obáváte se ransomware?

(zašifrována data na discích v důsledku napadení koncového zařízení nebo serveru běžným ransomwarem)

50. Obáváte se sabotáže ze strany zaměstnance.

(zneužití přístupu zaměstnancem, který měl nebo získal přístup do systému a k datům a pozměnil je nebo nainstaloval logickou bombu)

51. Obáváte se krádeže informací ze strany konkurence nebo organizovaných skupin?

(zcizeny citlivé osobní údaje klientů, zaměstnanců, hesel, strategické plány, chráněné receptury, firemní know-how, popisy a technické výkresy nových produktů a služeb)

52. Obáváte se krádeže informací ze strany vlastních zaměstnanců?

(zneužití přístupu zaměstnancem, který měl nebo získal přístup k datům a zkopíroval je, zneužil pro svoji potřebu anebo prodal)

53. Obáváte se úniku informací v důsledku nedbalosti?

(odeslání e-mailu omylem, ztráta/vyřazení počítače či médií s citlivými daty)

54. Obáváte se očerňující kampaně na internetu?

(negativní recenze, příspěvky v diskusním fóru, dezinformační kampaň, otrávení výsledků vyhledávání apod.)

Příloha H – Šablona e-mailu

Tato příloha obsahuje šablonu e-mailu, který byl rozesílán v různých drobných modifikacích na odpovědné osoby v organizaci z vlastního SMTP serveru, aby se eliminovalo riziko umístění serveru na blacklist a označení e-mailu jako SPAM.

Odesílatel: Miroslav Čermák <mc@cleverandsmart.cz>
Příjemce: buď byl uveden jen jeden v poli „To“ anebo pokud byl e-mail adresován většímu počtu osob současně, tak byli uvedeny v poli „ Bcc“.
Předmět e-mailu: Průzkum skutečné úrovně kybernetické bezpečnosti v ČR

Dobrý den,
obracím se na vás jako na osobu, která by dle informací uvedených na webových stránkách vaší organizace měla mimo jiné nést odpovědnost i za informační bezpečnost, a tedy i mít povědomí o kybernetických hrozbách a přijatých bezpečnostních opatřeních.
Rád bych vás poprosil o vyplnění dotazníku, na který uvádím odkaz níže. Vyplnění dotazníku by vám nemělo zabrat více jak 15 minut a mělo by mít okamžitý přínos i pro vás, protože:

- ihned po odeslání dotazníku se vám zobrazí rychlé zhodnocení vaší situace, tedy jak na tom skutečně jste, jaké hrozby vás ohrožují a jaká bezpečnostní opatření byste měli přijmout;
- s odkazem na výsledky průzkumu, které budou po jeho skončení zveřejněny, budete moci lépe obhájit své investice do bezpečnostních řešení ve vaší organizaci;
- svými odpověďmi přispějete k lepšímu pochopení toho, co se skutečně odehrává v kyberprostoru a jak je na tom celkově vaše odvětví, na které jsou vedeny kybernetické útoky.

Dotazník se nachází na této adrese:
https://www.cleverandsmart.cz/vyzkum-skutecne-urovne-kyberneticke-bezpecnosti-v-cr-dotaznik/

V případě dotazů mne neváhejte kontaktovat.

Děkuji moc za váš čas,

Ing. Miroslav Čermák, CISM
www.cleverandsmart.cz
mc@cleverandsmart.cz
Tel: +420 737 201 649

Plošné útoky na lidi (PL)

Plošné útoky vedené na lidi spočívají nejčastěji ve zneužití technik sociálního inženýrství a nízkého bezpečnostního povědomí, je při nich vyžadována větší či menší interakce ze strany oběti. Nejčastějším vektorem útoku je phishingový e-mail, trojanizovaná aplikace nebo web zobrazující výzvu k instalaci aplikace.

Zde je třeba podotknout, že v podstatě každý se může stát obětí takovéhoto útoku a dosažená úroveň formálního vzdělání a inteligence nehraje prakticky vůbec žádnou roli. Jde jen o to zvolit ten správný způsob.

V případě aktivního přístupu, který má zpravidla podobu phishingu, útočník rozesílá e-mail na velké množství adres, které buď koupil, stáhl z internetu anebo si je sám podle nějakého klíče vygeneroval.

Samotný e-mail je pak zpravidla napsán tak, aby v příjemci zprávy vzbudil důvěru, emoce a zároveň ho dostal do časové tísně. Pokud e-mail přichází od nějaké autority či důvěryhodné instituce jako je banka, police, exekutorský úřad, pošta, je napsán správně česky a používá i stejný design, tak příjemce nevěnuje příliš pozornost tomu, kdo je uveden jako odesílatel a má tendenci obsahu zprávy důvěřovat.

Stejně tak, pokud e-mail přichází od osoby, se kterou příjemce běžně komunikuje, a tudíž takový e-mail očekává, nenapadne ji, že by mohl být počítač odesílatele napaden malwarem a e-mail odešel ze schránky odesílatele bez jeho vědomí.

Žádoucí emoce, ať už negativní nebo pozitivní jsou pak v příjemci e-mailu vzbuzeny např. tím, že je mu vyhrožováno, že by vůči němu mohlo být vzneseno obvinění, bude muset uhradit pokutu anebo naopak něco může získat, přičemž musí reagovat do určité doby.

V okamžiku, kdy obsah e-mailu koresponduje a je zasazen do kontextu aktuálního dění a pohotově reaguje na aktuální politickou, kulturní či jinou společenskou událost, tak příjemce e-mailu vzhledem k množství podobných e-mailů přestává věnovat pozornost tomu, od koho e-mail přichází.

Kombinace těchto faktorů vede ke změně stavu mysli a snížené obezřetnosti. Když pak takový e-mail obsahuje přílohu nebo odkaz, tak je pak větší pravděpodobnost, že na ni příjemce e-mailu klikne a dojde ke spuštění škodlivého

kódu nebo přesměrování na podvodnou stránku, kde je vyžadováno zadání citlivých údajů.

V případě spíše pasivního přístupu útočník začleňuje škodlivý kód do nějaké široce používané aplikace, dostupné mimo oficiální repository, ale ne nutně, a která vyžaduje vyšší než nezbytně nutná oprávnění, která musí uživatel povolit, a dochází ke kompromitaci tímto způsobem.

Dalším možným vektorem útoku je zobrazení výzvy uživateli při jeho běžném surfování po internetu, kdy se na kompromitovaném webu zobrazí uživateli výzva napodobující systémové hlášení k instalaci falešného antiviru nebo jiného bezpečnostního produktu.

Nejčastějším výsledkem těchto útoků jsou zašifrovaná data na disku, uzamčené zařízení a nemožnost pracovat (ransomware), neautorizovaný převod finančních prostředků (bankware), požadavek na zaplacení jinak dojde ke zveřejnění citlivých dat (scareware) anebo je cílem útočníka těžba kryptoměny (cryptominery) či začlenění zařízení oběti do botnetu.

Tyto útoky se vyznačují velice nízkými náklady a krátkou dobou přípravy i trvání, neboť útočník předem počítá s tím, že jeho útok bude poměrně brzy odhalen, protože je pravděpodobné, že takovéhoto rozsáhlého útoku si někdo všimne a zareaguje na něj. Nicméně útočník realizuje úspory z rozsahu a v součtu může být výnos z jedné takové kampaně ve výši několika miliónů korun. Přičemž útočníkovi nic nebrání v tom, útok mírně modifikovat a realizovat jej opakovaně.

Plošné útoky na stroje (PS)

Útočník v tomto případě využívá skutečnosti, že každé zařízení může obsahovat nějakou zranitelnost, která mohla vzniknout v jakékoliv fázi SDLC, ať už na jeho samotném počátku, v rámci návrhu nebo kdykoliv později během kódování anebo při jeho nasazení, kdy došlo k nevhodnému nastavení. Zařízení jednoduše nemusí být secure by design, secure by default a secure by deployment.

Přičemž útočník může danou zranitelnost odhalit sám, koupit ji na černém trhu anebo i oficiálně, neboť se zranitelnostmi se běžně obchoduje jako s jakýmikoliv

jinými komoditami[202], anebo se jedná o zranitelnost veřejně známou, pro kterou zatím nebyl vydán patch anebo byl a daný subjekt ji z nějakého důvodu nenasadil.

Plošné útoky na stroje, resp. koncová zařízení a servery, pak mohou být aktivní, kdy útočník skenuje určitý IP adresní rozsah, v krajním případě celý internet a hledá zařízení, které trpí jednou konkrétní zranitelností a té zneužívá, a to buď ručně, anebo automatizovaně za použití nějakého online nástroje typu Shodan, který s jistou nadsázkou tvrdí, že je schopen internet analyzovat v řádu sekund[203], případně si útočník napíše za tímto účelem nástroj vlastní.

V případě spíše pasivního přístupu útočník škodlivý kód začlení do webových stránek, které má pod kontrolou (může se např. jednat o vložený iframe o nulové velikosti, skript, php kód) anebo jej vkládá na web jako běžný uživatel do diskusního fóra, případně škodlivý kód začleňuje do reklamního banneru, který se na webových stránkách zobrazuje v rámci výměnného reklamního systému a využívá skutečnosti, že ten, kdo na danou webovou stránku zavítá, tak se nakazí. Jedná se o tzv. drive-by download malware.

V neposlední řadě může útočník začlenit škodlivý kód do široce používané aplikace, která zneužívá nějaké zranitelnosti v systému nebo jiné běžící aplikace a bez jakékoliv interakce s uživatelem dochází k exploitaci dané zranitelnosti a zajištění persistence.

Ve všech případech se pak kompromitované zařízení stává součástí celosvětového botnetu, který slouží útočníkovi anebo je prodáván za úplatu a může být snadno zneužit k dalším útokům. Anebo je dané zranitelnosti neprodleně zneužito k pokusu o okamžitou monetizaci, kdy útočník zašifruje veškerá data a požaduje platbu za jejich dešifrování anebo stroj zneužije k těžbě nějaké kryptoměny.

Náklady na realizaci těchto útoků jsou poměrně nízké, tyto útoky mohou probíhat zcela automatizovaně a mohou zůstat i dlouhou dobu bez povšimnutí, neboť výsledkem útoku zpravidla bývá začlenění stroje do botnetu a jeho prodej nebo pronájem k dalšímu využití. A až v okamžiku, kdy dojde ke zneužití botnetu k dalším útokům, bývá odhalen.

---

[202] ZERODIUM - The Leading Exploit Acquisition Platform [online]. [cit. 17.02.2019]. Dostupné z: http://zerodium.com/
[203] Shodan [online]. [cit. 17.02.2019]. Dostupné z: https://www.shodan.io/

Cílené útoky na lidi (CL)

Při cílených útocích na konkrétní osoby v organizaci je rovněž zneužíváno technik sociálního inženýrství. Tyto útoky probíhají přes internet, e-mail a za použití dalších prostředků komunikace a v krajním případě dochází i k fyzickému průniku do prostředí organizace a kontaktování oběti ať už přímo nebo nepřímo. Tento případ ale není tak častý, protože pro útočníka představuje zvýšené riziko, že bude přistižen při činu.

Jedná se o tzv. **piggybacking** nebo také tailgating, kdy se útočník pokusí dostat do budovy spolu s ostatními zaměstnanci, kdy s někým naváže rozhovor, nese objemnější předmět a nechá si podržet dveře, případně se vydává za někoho jiného. V krajním případě se nechá zaměstnat buď přímo v dané organizaci anebo v organizaci, od které organizace, o kterou má primární zájem odebírá určité služby. V okamžiku, kdy útočník pronikne do prostředí dané organizace, tak může instalovat HW keylogger, falešné přístupové body (access point), vlastní síťové prvky a zaznamenávat přihlašovací údaje.

Útočník se snaží o své oběti získat maximum informací, a to z veřejných zdrojů jako jsou např. sociální sítě, kde o sobě uživatelé sami informace uvádějí, webové stránky firmy, kde informace o svých zaměstnancích uvádí samotná firma anebo v médiích, kde informace uvádí nezávislí novináři, a rovněž i z neveřejných interních zdrojů. Vlastnímu útoku předchází pečlivá příprava, která může trvat i po dobu několika týdnů.

V těchto případech dochází k falšování identity, kdy se útočník vydává za jinou důvěryhodnou nebo blízkou osobu, cílí na konkrétní osoby v organizaci a volá (**vishing**) do dané organizace a snaží se získat další informace nebo je zcizit. Nebo zasílá na míru připravený e-mail, tzv. **spear phishing** (whaling, CEO fraud, BEC), který na první pohled vypadá jako důvěryhodný a obsahuje přílohu, která zpravidla, ale ne nutně, zneužívá nějaké zranitelnosti nultého dne (zero day vulnerability) a v okamžiku, kdy na ni příjemce zprávy klikne, tak se spustí a provede perzistenci.

Další často používanou technikou je tzv. **watering hole attack**, kdy útočník umísťuje svůj škodlivý kód na webové stránky, které oběť navštěvuje, a ty se zobrazí jen dané oběti např. za použití geoIP funkcionality, otisku počítače či

pokročilejších technik jako je rozpoznávání obličeje, takže ke spuštění škodlivého kódu dojde jen v okamžiku, kdy z daného zařízení přistupuje konkrétní osoba.

Poslední, ale neméně používanou technikou je pak pohození paměťového média (např. USB flash disku nebo SD karty) v prostorách organizace anebo v její těsné blízkosti, kdy útočník spoléhá na přirozenou lidskou zvědavost, tzv. **baiting**.

Cílené útoky na osoby jsou zpravidla součástí tzv. **APT útoků**. Náklady na realizaci těchto útoku jsou vyšší než v předchozích případech a vyžadují i podstatně delší přípravu a neumožňují realizovat úspory z rozsahu. Nicméně, příslušné techniky je možné opakovaně použít k útokům na další subjekty, obzvláště v případě použití tzv. zero day zranitelností a exploitů, neboť zpravidla nedochází k jejich medializaci. Délka trvání takovéhoto útoku se pohybuje v řádu měsíců a náklady na realizaci pak ve výši několik stovek tisíc až jednotek miliónů. Ale těmto vysokým nákladům pak na druhou stranu odpovídají i výnosy z těchto útoku, které se pohybují v řádech desítek až stovek miliónů korun. V ojedinělých případech pak i jednotek miliard.

Cílené útoky na stroje (CS)

Útočník v tomto případě hledá jakoukoliv zranitelnost, kterou by daný stroj mohl obsahovat. Používá za tímto účelem nějaký automatizovaný skener, kdy zjišťuje, jaké služby na daném serveru běží, a jaká zde běží verze OS a aplikací. Pokud automatizovaný skener zranitelností selže, tak pak útočník hledá zranitelnosti ručně. Následně se snaží jakékoliv zranitelnosti zneužít k průniku do systému nebo k narušení důvěrnosti, integrity nebo dostupnosti, to podle toho, co je jeho cílem.

V případě, že je cílem útočníka odepření služby, tak může realizovat aplikační nebo volumetrický DoS/DDoS útok, kdy daný systém, pokud před tímto typem útoku není chráněn, se tímto stává nedostupným.

Náklady na realizaci těchto útoků jsou minimální a škody pak mohou být značné. Vzhledem k tomu, že útočník nemá z tohoto útoku zpravidla přímý zisk, jsou tyto útoky vedeny s cílem získat výkupné, kdy je tímto útokem jen vyhrožováno, a útočník rozesílá tzv. extortion letter a případně demonstruje svou schopnost v podobě kratšího útoku o menší intenzitě.

V případě, že k útoku skutečně dojde a má delší dobu trvání, a to v řádu hodin až dnů, tak je realizován státem sponzorovanou skupinou a lze jej označit za kyberterorismus a je zpravidla veden na KII, VIS nebo ZS.

V některých případech může také dojít k tomu, že útok byl cílený, ale může se navenek jevit jako plošný, např. v okamžiku, kdy útočník cílí na firmu využívající služeb třetí strany provozující např. datové centrum a v důsledku útoku jsou pak nedostupné systémy všech zákazníků daného poskytovatele.

Náklady na realizaci těchto útoků, vyjma DDoS, které lze pořídit za pouhých několik USD, se pohybují v řádech stovek tisíc, výnosy pak minimálně v řádech jednotek miliónů korun.

Zřetězené útoky

Na tomto místě je nutné uvést, že v praxi pak dochází k řetězení těchto útoků, takže jestliže došlo v rámci PL ke kompromitaci blíže neurčitých koncových zařízení a ty byly začleněny do botnetu, tak pak z těchto zařízení mohou být následně vedeny CS, např. DDoS.

A rovněž z nich mohou být vedeny CL, např. spear phishing, což sice nebývá tak časté, ale nelze tuto možnost zcela vyloučit. Servery, které byly kompromitovány v rámci PS, mohou být zneužity PL, kdy např. na nich může být umístěn phishing web anebo se na nich může nacházet malware a rovněž i k CL, kdy vybraný server může sloužit jako watering hole.

Vyloučit samozřejmě nelze ani situaci, kdy dochází k CL nebo CS a jen za tím účelem, aby pak následně bylo možné vést další CL nebo CS, k čemuž dochází v rámci APT útoků, které představují specifický typ útoků, jsou přesně cílené a jsou často vedeny jak na konkrétní osoby, tak i stroje. A mohou využívat plošných útoků jako kouřové clony k realizaci vlastního cíleného útoku na konkrétní subjekt.

V okamžiku, kdy dojde ke kompromitaci stroje, ať už v důsledku PL, PS, CL nebo CS, tak z něj může být opět veden PL, PS, CL nebo CS. Teoreticky může nastat 16 různých útoků, nicméně v reálném světe ne všechny kombinace nastávají, a proto je možné uvažovat spíše jen o osmi různých útocích, které zachycuje Tabulka 20 – Zřetězené útoky.

Je tomu tak proto, že např. k cílenému útoku na konkrétní osobu je efektivnější odeslat e-mail ze schránky osoby, které daná osoba důvěřuje nebo exploit umístit na web, který daná osoba navštěvuje.

Při plošném útoku, kdy je útočníkovi jedno, čí stroj kompromituje, tak může umístit exploit na jakýkoliv web, který má určitou návštěvnost, anebo rozeslat e-mail na všechny adresy, které najde v adresáři, neboť jeho cílem je co největší zásah.

Podobně při cíleném útoku na konkrétní server je útočníkovi v zásadě jedno z jakého zařízení DDoS útok nebo hacking provede a využije za tímto účelem jakékoliv zařízení, které bude pod jeho kontrolou, aby zahladil stopy a znesnadnil tak své odhalení.

Tabulka 20 – Zřetězené útoky

zdroj/cíl	PS	PL	CS	CL
PS		phishing web, exploit kit	DDoS, hacking	
PL		spear phishing	DDoS, hacking	
CS			hledání zranitelností	spear phishing, watering hole
CL			hledání zranitelností	spear phishing

APT

Na některé společnosti jsou vedeny útoky jen proto, že jsou přítomny na internetu, na jiné však proto, co dělají. V takovém případě se jedná se o tzv. APT útoky.

Dle SANS[204] byl pojem APT poprvé použit v roce 2006 analytiky United States Air Force, a měl vyjadřovat pokročilou a přetrvávající hrozbu (Advanced Persistent Threat, zkr. APT).

[204] BINDE, Beth E, Russ MCREE a Terrence J O'CONNOR. Assessing Outbound Traffic to Uncover Advanced Persistent Threat [online]. 2011 [cit. 02.02.2022]. DOI: 10.13140/RG.2.2.16401.07520

Ve výkladovém slovníku NIST[205] je pak APT hrozba definována jako hrozba, kdy útočník disponuje sofistikovanými znalostmi a významnými zdroji, které mu umožňují vytvářet si příležitosti k dosažení svých cílů, které obvykle vedou k průniku a uhnízdění se v infrastruktuře organizace, která je předmětem zájmu útočníka za účelem získání informací, narušení provozu nebo způsobení škody a to hned anebo kdykoliv v budoucnu, opakovaně, během delšího časového období, kdy se útočník brání odhalení, maskuje se, zahlazuje stopy a zároveň si zajišťuje potřebnou úroveň interakce za účelem splnění svých cílů.

Musa[206] pak dodává, že APT útok je kontinuální proces, kdy dochází k pečlivě připravenému, postupnému a nenápadnému hackování vyhlédnuté entity.

Naproti tomu dle Bruce Schneiera nejsou pokročilé a přetrvávající hrozby (Advanced Persistent Threat, zkr. APT) nic jiného než cílené útoky[207] a jedná se tak trochu o buzzword. A mohlo by se stejně tak hovořit i o léty prověřených technikách, Aged Proven Techniques nebo ještě poetičtěji Ancient Proven Techniques[208], protože se vždy jedná o kombinaci technik sociálního inženýrství a zranitelností nultého dne.

To potvrzují i nejrůznější analýzy, např. společnost Imperva tvrdí, že mnohdy je spíše než nějakých pokročilých technik využito technik naprosto běžných[209]. TrendMicro pak poukazuje na častou záměnu mezi cíleným útokem APT, kdy k tomu, aby cílený útok bylo možné označit za APT, tak musí použit kód, který nebyl použit nikde jinde, a pokročilé techniky sociálního inženýrství[210].

---

[205] PAULSEN, Celia a Robert BYERS. *Glossary of key information security terms* [online]. NIST IR 7298r3. Gaithersburg, MD: National Institute of Standards and Technology. 2019 [cit. 02.02.2022]. DOI: 10.6028/NIST.IR.7298r3.
[206] MUSA, Sam. Advanced Persistent Threat - APT [online]. 2014 [cit. 06.03.2019]. Dostupné z: https://www.academia.edu/6309905/Advanced_Persistent_Threat_-_APT
[207] SCHNEIER, Bruce. Advanced Persistent Threat (APT) - Schneier on Security. *Schneier on Security* [online]. 9. listopad 2011 [cit. 04.03.2019]. Dostupné z: https://www.schneier.com/blog/archives/2011/11/advanced_persis.html
[208] ČERMÁK, Miroslav. APT je jen další buzzword. *CleverAndSmart Management Consulting* [online]. 2012 [cit. 04.03.2019]. ISSN 2694-9830. Dostupné z: https://www.cleverandsmart.cz/apt-je-jen-dalsi-buzzword/
[209] *The Non-Advanced Persistent Threat* [online]. 2014 [cit. 12.07.2021]. Dostupné z: https://www.imperva.com/docs/HII_The_Non-Advanced_Persistent_Threat.pdf
[210] GENES, Raimund. Targeted Attacks versus APTs: What's The Difference? *TrendLabs Security Intelligence Blog* [online]. 2015 [cit. 12.03.2019]. Dostupné z: https://blog.trendmicro.com/trendlabs-security-intelligence/targeted-attacks-versus-apts-whats-the-difference/

Předmětem APT útoků jsou zpravidla organizace, které jsou součástí kritické infrastruktury státu, provozující kritickou informační infrastrukturu, zkr. KII, významné informační systémy, zkr. VIS, a systémy základních služeb, zkr. SZS, disponují cenným know-how, které je předmětem průmyslové špionáže anebo realizují velké obraty peněz.

Tyto útoky jsou realizovány ze strany vysoce organizovaných a dost často i státem sponzorovaných skupin a probíhají i po dobu několika měsíců až let. A byť jsou náklady na tyto útoky značné a pohybují se v řádu stovek tisíc až miliónů, tak výnosy se pohybují v řádu vyšších stovek miliónů až jednotek miliard.

Samotný APT útok lze rozdělit do několika na sebe navzájem navazujících fází, přičemž jejich počet a pojmenování se autor od autora výrazně liší. Některé zdroje uvádí 12 fází[211], jiné 10 fází[212], 7 fází[213] a některé jen 5 fází[214]. Onen rozdíl je však způsoben jen detailním rozepisováním čtyřech základních fází[215], kterými jsou: příprava, průnik, kompromitace a dokončení.

Příprava

V této fázi se útočník snaží o předmětu svého cíle zjistit co nejvíce informací. Informace čerpá z veřejných zdrojů, jako jsou sdělovací prostředky, výroční zprávy, webové stránky dané organizace a sociální sítě. Vytváří si tak představu o tom, jak veliká daná organizace je, jaká je její organizační struktura, kdo jsou její zaměstnanci, na jakých pozicích se nachází, a s jakými dalšími organizacemi v odběratelsko-dodavatelském řetězci organizace spolupracuje, protože mnohdy je snazší vést útok na organizaci, která např. dodává HW a SW vybavení a začlenit

---

[211] Advanced Persistent Threats - Learn the ABCs of APT: Part A. *Secureworks.com* [online]. 2016 [cit. 06.03.2019]. Dostupné z: https://www.secureworks.com/blog/advanced-persistent-threats-apt-a

[212] RADZIKOWSKI, Przemek Shem. CyberSecurity: Expanded Look at the APT Life Cycle and Mitigation. *Dr.Shem* [online]. 11. únor 2016 [cit. 08.03.2019]. Dostupné z: http://DrShem.com/2016/02/11/cybersecurity-expanded-look-apt-life-cycle-mitigation/

[213] LACEY, David a INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION. *Advanced persistent threats: how to manage the risk to your business* [online]. Rolling Meadows, IL: ISACA, 2013 [cit. 08.03.2019]. ISBN 978-1-60420-347-9. Dostupné z: http://www.books24x7.com/marc.asp?bookid=62388,

[214] MILLS, Elinor. Attack on RSA used zero-day Flash exploit in Excel. *CNET* [online]. 2011 [cit. 08.03.2019]. Dostupné z: https://www.cnet.com/news/attack-on-rsa-used-zero-day-flash-exploit-in-excel/

[215] *Common Cyber Attacks: Reducing The Impact* [online]. 2015 [cit. 12.07.2021]. Dostupné z: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/400106/Common_Cyber_Attacks-Reducing_The_Impact.pdf

do něj backdoor, nechat se u dané organizace zaměstnat a tím následně získat fyzický přístup do organizace, která je primárním cílem útočníka. V této fázi dále dochází k zjišťování informací o provozovaných systémech, probíhá skenování služeb vystavených do internetu a využívá se jejich odpovědí na dotazy. Následně pak probíhá hledání zranitelností v provozovaných technologiích a vývoj nebo nákup exploitů potřebných k jejich zneužití, případně k začlenění backdooru do HW nebo SW používaného danou organizací. Tato přípravná fáze, kdy dochází rovněž k vytvoření nezbytné infrastruktury, C&C serverů, phishingových, e-mailů, falešných identit apod. může probíhat i po dobu několika týdnů až měsíců a útočník při ní může využívat technik sociálního inženýrství, navazovat i intimní vztahy se zaměstnanci dané organizace za účelem získání informací nebo přístupu, neboť mnohdy je spolupráce s někým zevnitř nezbytná. Tuto přípravnou fázi tak lze rozdělit v zásadě na dvě části sběr informací (external reconnaissance) a vývoj nástrojů a přípravu infrastruktury k realizaci útoku (weaponization).

Průnik

V této fázi dochází k fyzickému nebo vzdálenému průniku do prostředí dané organizace, ať už v přestrojení nebo jako skutečný zaměstnanec třetí strany a zapojením vlastního zařízení, např. falešného access pointu, HW keylogeru do vnitřní sítě organizace anebo dodáním HW nebo SW opatřeného backdoorem. Případně může dojít k podvržení falešné aktualizace podepsané klíčem, ke kterému je vydán certifikát od důvěryhodné certifikační autority, která byla za tímto účelem již dříve kompromitována[216]. Daleko častěji se však můžeme setkat s napadením jiného webu, který organizace navštěvuje a umístění exploitu tam (watering hole attack), a v okamžiku, kdy jej zaměstnanec dané organizace navštíví, tak dojde k exploitaci a stažení škodlivého kódu do jeho počítače (drive-by download). Anebo, což je vůbec nejčastější případ, může dojít k distribuci škodlivého kódu e-mailem (spear phishing) nebo na médiu (baiting), které útočník pohodí např. na parkovišti nebo na střeše budovy. I v této fázi se využívá technik sociálního inženýrství v kombinaci se zranitelnostmi nultého dne. Tato fáze má nejkratší trvání a zpravidla probíhá vzdáleně přes internet, neboť se zde útočník

[216] ČERMÁK, Miroslav. DigiNotar: Operation Black Tulip. *CleverAndSmart Management Consulting* [online]. 2011 [cit. 17.02.2019]. ISSN 2694-9830. Dostupné z: https://www.cleverandsmart.cz/diginotar-operation-black-tulip/

vystavuje největšímu riziku, že si probíhajícího útoku někdo všimne, a proto se vše odehraje během několika málo minut nebo hodin. Tato fáze se dá opět rozdělit do několika částí, doručení exploitu (delivery), spuštění exploitu (exploitation) obsahující nálož (payload), kdy se útočník pokouší o zvýšení svých oprávnění v napadeném systému (escalate privileges) zajištění perzistence (establish persistence) a instalace komponenty za účelem vzdáleného přístupu (remote access trojan, zkr. RAT) do napadeného systému.

Kompromitace

V této fázi se již útočník nachází v prostředí organizace, kde kompromitoval jedno či více koncových zařízení nebo serverů, zajistil si v nich perzistenci a nyní se seznamuje se síťovou infrastrukturou (internall reconnaissance) a vyhledává systémy, které by mohl dále napadnout (colaterall movement). Za tímto účelem zachycuje přihlašovací údaje, pořizuje snímky obrazovky, zaznamenává činnosti zaměstnanců ve formě videa a tyto informace pak zasílá na C&C server útočníka k analýze a stanovení dalšího postupu, a to tak dlouho, dokud není dosaženo cíle. Komunikace s C&C serverem pak probíhá šifrovaně, je schována do DNS komunikace anebo je využito pokročilé lingvistické steganografie, kdy informace jsou umně schovány v prostém textu nacházejícím se na webech, které uživatel běžně navštěvuje, jako jsou sociální sítě, O365 nebo Google. Vlastní malware na koncových zařízeních a serverech organizace má pak často podobu tzv. fileless malwaru, tedy bezsouborového malwaru, který se ukrývá do registrů a běžných procesů a maximálně využívá součástí systému, jako je powershell apod., a je proto velice obtížné jej odhalit. Tato fáze, podobně jako fáze přípravy může trvat poměrně dlouho, a to po dobu několika měsíců až let, než se útočníkovi podaří zcela ovládnout daný systém nebo získat přístup k citlivým informacím, které jsou předmětem jeho zájmu.

Dokončení

V okamžiku, kdy dojde ke kompromitaci cílového systému, kompletního ovládnutí infrastruktury, výroby, služby, vyřazení daného systému z provozu anebo získání citlivých informací, které jsou shromážděny (data gathering) a připraveny ke zkopírování na server útočníka (data exfiltration), tak se přesouváme do poslední fáze. Tato fáze trvá rovněž poměrně krátce, ovšem délka jejího trvání do značné míry závisí na tom, co je cílem útočníka, protože pokud je

cílem útočníka exfiltrace informace, tak nemusí být vůbec odhalen a přístup k informacím si může udržovat po poměrně dlouhou dobu. Zde jen záleží na tom, jaké je ono množství informací, které potřebuje exfiltrovat, tedy zkopírovat do tzv. drop zóny, a zda si někdo všimne zvýšeného provozu, či jiné anomálie, ke které ale také nemusí dojít, pokud bude jako drop zóna zvolen např. cloud Microsoftu, Googlu anebo Amazonu, který organizace běžně využívá. V případě nedostupnosti anebo pozměnění informací či dat pak zpravidla dojde k nějaké škodě a v tu chvíli se i rozjíždí vyšetřování a je zahájen audit a forenzní analýza. Zde pak záleží na tom, zda se útočníkovi podařilo malware a případné účty a logy odstranit, a jak zkušený je analytik provádějící forenzní analýzu, a zda najde stopy po přítomnosti malwaru v systému anebo dokonce samotný malware.

Výše popsaný cyklus v té nejjednodušší podobě zachycuje Obrázek 24 – APT. Barevné odlišení jednotlivých fází APT útoku není samoúčelné, nýbrž indikuje míru rizika, kterému je organizace vystavena, velikost šipky pak znázorňuje i velikost dopadu. Pořadí, v jakém jsou jednotlivé fáze uvedeny, zároveň představuje časovou osu. Jen délka jednotlivých fází neodpovídá realitě, neboť ty trvají zpravidla různě dlouho. Tento cyklus se navíc může opakovat tak dlouho, dokud útočník nedosáhne svého cíle.

Obrázek 24 – APT

Cíle kybernetických útoků můžeme rozlišit podle toho, na koho jsou jednotlivé kybernetické útoky vedeny a jakého cíle může útočník dosáhnout. Útoky mohou být vedeny jak na fyzické, tak i právnické osoby, kterými mohou být jak podnikatelské subjekty, tak i nevýdělečné organizace a organizační složky státu, potažmo celý stát. Cíle kybernetických útoků mohou být různé, ale zpravidla je cílem útočníka:

- **zcizit citlivé informace**, jako jsou osobní údaje, informace, které jsou předmětem státního a obchodního tajemství, specifické know-how nebo

chráněné receptury potřebné pro výrobu určitého produktu, strategické marketingové plány a vůbec informace, které představují pro jejich vlastníka nezanedbatelnou konkurenční výhodu. Následně pak útočník může tyto informace zcizit za účelem jejich použití k realizaci vlastní podnikatelské činnosti, k útoku na další subjekt, k vydírání, anebo prodeji jinému subjektu, který za ně bude ochoten zaplatit. Ale stejně tak je může i vystavit na internetu a tím organizaci rovněž způsobit značnou škodu, neboť se v očích svých klientů stává nedůvěryhodnou, neboť citlivé informace nedokázala ochránit, a profitovat tak ze ztráty jejího dobrého jména a tržního podílu.

- **pozměnit informace či data**, na základě kterých v dané organizaci dochází ke strategickému rozhodování a směrování organizace anebo je na jejich základě řízen denní provoz organizace, její produkce ať už ve formě výrobků nebo poskytovaných služeb, což v konečném důsledku může vést ke značné materiální škodě, v důsledku produkce zmetků, poškození výrobního zařízení a v krajním případě pak může být ohroženo i životní prostředí, zdraví občanů anebo dokonce i jejich životy, k čemuž může dojít např. v okamžiku, kdy útočník ovládne systém pro řízení letového provozu, drážních signalizačních zařízení, systém ovládající chlazení atomového reaktoru, nemocniční informační systém apod.

- **způsobit nedostupnost** kritické informační infrastruktury, významných informačních systémů a základních služeb, což v konečném důsledku může vést k celkovému zhoršení konkurenceschopnosti, výkonu národního hospodářství, oslabení měny, zhoršení ratingu dané země ve světě a výraznému snížení objemu investic a exportu.

- **získat přístup do systému** jen za účelem demonstrace moci a poškození důvěry občanů ve stát či organizaci, která daný systém provozuje anebo jen k vedení dalšího kybernetického útoku na jiný subjekt.

Poznámka: Jednotlivé techniky použité v rámci kybernetického útoku jsou na rozdíl od hrozeb de facto standardizovány v podobě ATT&CK Matrix[217] pro účely této práce však není nutné se jim blíže věnovat.

[217] MITRE ATT&CK® [online]. [cit. 25.06.2021]. Dostupné z: https://attack.mitre.org/

Příloha J – Vývoj kybernetických hrozeb v ČR

1970–1979

V tomto období se v ČR objevují první počítače, které však nebyly připojeny do sítě, programy byly psány na děrných štítcích a zaváděny do feritových pamětí. Ty se nacházely v přísně střežených prostorách, jejich ovládání bylo z dnešního pohledu velice komplikované a sloužily především k výpočtům, nikoliv k uchovávání dat, takže důraz byl kladen především na jejich správnou funkčnost a spolehlivost. K žádným kybernetickým útokům v té době v ČR nedocházelo.

1980–1989

Objevují se první osobní osmibitové počítače, nepřipojené do internetu, viry prakticky neexistují. Až koncem dekády, kdy se začaly objevovat ve větší míře i šestnáctibitové počítače, se škodlivý kód se začal šířit na disketách, které sloužily k výměně dat anebo na BBS systémech, které ještě před internetem sloužily k výměně dat mezi uživateli. Viry byly ukryty v zaváděcím sektoru disket (bootviry), v office dokumentu (macroviry) anebo ve spustitelném souboru (trojan). Důraz byl kladen především na zajištění důvěrnosti.

1990–1999

Domácnosti a firmy si pořizují první počítače. Objevují se první samoreplikující se viry, ty se úspěšně šíří v lokálních sítích, přes diskety a později pak i přes optická média a USB flash disky. Viry, boot viry, makroviry, trojští koně, addware. Pro viry této doby je typické, že většina z nich se jen šíří, zvětšuje se velikost souborů, zabírá místo na disku, zobrazuje neškodné hlášení, takže způsobuje spíš jen nepřímou škodu spočívající ve ztrátě produktivity a nákladů na odstranění viru. Vzhledem k tomu, že internetové připojení ještě zdaleka není vzhledem k ceně a stávající infrastruktuře v každé domácnosti a je navíc velice pomalé, tak se SW hodně často šíří především na CD, DVD a USB. Pro toto období je typický virus, který se objevil poprvé v roce 1995 v operačním systému Microsoft Windows 95 a zneužíval funkce AutoRun[218], která umožňovala definovat, který program se má automaticky spustit poté, co je disk, zpravidla optické médium vloženo do mechaniky. Společnost MS tuto funkci zavedla za účelem automatického spuštění

[218] Creating an AutoRun-Enabled Application (Windows). *Microsoft Docs* [online]. 2018 [cit. 25.06.2021]. Dostupné z: https://docs.microsoft.com/en-us/previous-versions/windows/desktop/legacy/cc144206(v=vs.85)?redirectedfrom=MSDN

instalace programového vybavení, které se na daném médiu nacházelo. K automatickému spuštění pak stačilo do kořenového adresáře daného média umístit textový soubor autorun.inf, který obsahoval cestu ke spustitelnému souboru, v tomto případě viru. Této funkce bylo později zneužito i u USB flash disků. Soubor autorun.inf mohl být umístěn do libovolného adresáře, a pak byl spustitelný soubor spuštěn i při poklepání na daný adresář. Tato vlastnost, které bylo aktivně zneužíváno se dostala i do dalších verzích Windows, jako Windows 98, ME, 2000, Xp, Vista a bylo ji nutné buď manuálně zakázat anebo naistalovat příslušný patch. Dle společnosti Eset se jednalo o nejzneužívanější zranitelnost roku 2011[219], která představovala infekční vektor i pro další malware, jako byl třeba síťový červ Conficker, který se šířil nejvíce v letech 2009 až 2011 a umísťoval svůj autorun.inf soubor na síťové disky a tím si zajistil další šíření[220] a využíval při tom i technik sociálního inženýrství, kdy funkce AutoPlay zobrazuje ikonu složky, která je definována v souboru autorun.inf[221], ale kdy ve skutečnosti nedojde k otevření složky, jak by uživatel mohl předpokládat, ale k instalaci. S připojením do internetu dochází ke krádežím hesel, k zobrazování reklamy, výzev k instalaci falešného antiviru a nástrojů na optimalizaci Windows, aktualizaci ovladačů apod. s cílem uvést uživatele internetu v omyl a podvodným způsobem ho nalákat ke koupi SW, který v lepším případě neškodí, v horším pak ve větší míře zobrazuje reklamní bannery, krade hesla, e-mailové adresy a další citlivé údaje nebo rozesílá e-maily na další kontakty, které má uživatel ve svém adresáři. V organizacích vznikají první LAN sítě, na počítačích běží zpravidla operační systém MS DOS, později pak i Windows 3.11 a Novell Netware. Pro komunikaci ve firmě se začíná používat elektronická pošta. S vnějším světem se však nadále komunikuje spíše pomocí faxu. A přístup do internetu je zpravidla možný jen z dedikovaných počítačů. Ani ne tak kvůli bezpečnosti, jako spíše poplatkům za

[219] *Global threat report* [online]. 2011 [cit. 12.07.2021]. Dostupné z: https://www.virusradar.com/sites/default/files/reports/2011-12-Global_Threat_Trends_December_2011.pdf
[220] *Global threat report* [online]. 2011 [cit. 25.06.2021]. Dostupné z: http://download.microsoft.com/download/0/3/3/0331766E-3FC4-44E5-B1CA-2BDEB58211B8/Microsoft_Security_Intelligence_Report_volume_11_English.pdf
[221] ZDRNJA, Bojan. *Conficker's autorun and social engineering* [online]. 2009 [cit. 25.06.2021]. Dostupné z: https://isc.sans.edu/diary/Conficker%27s+autorun+and+social+engineering/5695

připojení. Hlavní důraz je kladen na důvěrnost, začínají se objevovat první HW šifrátory povětšinou od firmy Decros.

2000–2009

Firmy budují velká datová centra. Vznikají firemní webové stránky. Domácnosti a firmy se začínají stále více připojovat do internetu. Firmy sice nadále omezují přístup do internetu, ale ten už začíná být dostupný ze všech počítačů v organizaci, filtruje se obsah, především pak obrázky a multimédia, ale spíše kvůli garantování rychlosti připojení pro business aplikace. Začíná se ve větší míře komunikovat s vnějším světem. Síťový operační systém Novell začíná ztrácet a je postupně vytlačován MS Windows, který se objevuje i na serverech. Viry se šíří hlavně po sítí a elektronickou poštou. Koncem dekády se objevuje web 2.0, který umožňuje i uživatelům vkládat na web vlastní obsah, což vede k většímu zájmu v hledání zranitelností ve webových aplikacích a k prvním útokům zneužívajícím zranitelnosti XSS, SQL injection, CSRF apod. Nejčastějšími následky útoků jsou však jen defacement webu nebo odepření služeb. Objevuje se první bezsouborový malware, v roce 2001 (Code Red[222]), a i v letech 2003 (SQL Slammer[223]), 2005 (Stuxnet[224]). Bezsouborový malware, jak již jeho název napovídá, je takový malware, který se nachází jen ve volatilní paměti počítače (RAM). Z principu, na jakém RAM funguje, je zřejmé, že s restartem počítače je z paměti tento kód v důsledku poklesu napětí na čipech do několika sekund odstraněn, takže není možné provést jeho forenzní analýzu. Tu je možné provést jen v okamžiku, kdy je tento malware do paměti zaveden. Možnost provedení analýzy však zhoršuje ta skutečnost, že je tento malware i obtížné detekovat, protože zneužívá systémových nástrojů a utilit, které jsou naprosto běžnou součástí systému, např. wscript, csript, sc, netsh, java, PowerShell (PS) či Windows Management Instrumentation (WMI) a umožňují útočníkovi vést jejich prostřednictvím útok. Ten zpravidla není detekován, protože tyto systémové nástroje a utility jsou

[222] Worm:W32/CodeRed Description. *F-Secure Labs* [online]. 2001 [cit. 25.06.2021]. Dostupné z: https://www.f-secure.com/v-descs/bady.shtml
[223] VAMOSL, Robert. SQL Slammer: How it works--prevent it. *ZDNet* [online]. 2003 [cit. 25.06.2021]. Dostupné z: https://www.zdnet.com/article/sql-slammer-how-it-works-prevent-it/
[224] KUSHNER, David. The Real Story of Stuxnet - IEEE Spectrum. *IEEE Spectrum: Technology, Engineering, and Science News* [online]. [cit. 25.06.2021]. Dostupné z: https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

považovány za důvěryhodné a často bývají používány i samotnými správci systému pro vzdálenou správu daného počítače nebo serveru a rovněž i aktivity provedené pomocí těchto nástrojů jsou považovány za legitimní. Netřeba zmiňovat, že pomocí těchto nástrojů získává útočník kompletní kontrolu nad systémem a může přistupovat k souborovému systému, k datům, kopírovat je, modifikovat, ale i zašifrovat nebo nahrát na internet a napadat další zařízení v síti.

2010–2020

Počítače v domácnostech a firmách jsou trvale připojeny do internetu. Firmy snižují náklady, začíná docházet ke konsolidaci a virtualizaci infrastruktury. Firmy přesouvají svá data do cloudů a využívají i jeho výpočetní výkon. Koncem dekády přesouvají svá data do cloudů i do té doby velice konzervativní organizace jako jsou např. banky.

V roce 2013 proběhla v rámci jednoho týdne vlna DDoS útoků cílená na zpravodajské servery[225], mobilní operátory[226], klienty internetového bankovnictví[227]. Reakcí na tento útok byl vznik projektů Fénix, který umožňuje organizacím, které jsou jeho součástí fungovat i v okamžiku, kdyby ostatní byly pod útokem[228]. SMS se stává nedůvěryhodnou, začíná se přecházet na Smart OTP v mobilu. Ve firmách se nahrazují čtečky čipově propojené s počítačem za čtečky s vlastní klávesnicí. Ve větší míře se objevuje phishing a snaha vylákat z uživatelů přihlašovací údaje, karetní údaje a ty pak prodat nebo zneužít k nákupu zboží na internetu. Ale ty nejsou moc účinné, protože k úspěšnému dokončení transakce je nutné zadat jednorázový kód, který ve formě SMS dostává uživatel internetového bankovnictví na dumbphone (hloupý telefon), který poskytuje jen základní funkce, jako je telefonování, příjem SMS a pár dalších funkcí, které jsou součástí firmware a nelze je tudíž kompromitovat. Během následujících několika málo let se však situace dramaticky mění, příčinou je nástup nové generace

[225] České zpravodajské servery čelily kybernetickému útoku - Novinky.cz [online]. 2013 [cit. 28.05.2021]. Dostupné z: https://www.novinky.cz/internet-a-pc/clanek/ceske-zpravodajske-servery-celily-kybernetickemu-utoku-183487

[226] SLÍŽEK, David. DDoS útok zasáhl weby mobilních operátorů, na možný atak se chystají i e-shopy. *Lupa.cz* [online]. 2013 [cit. 11.05.2021]. ISSN 1213-0702. Dostupné z: https://www.lupa.cz/clanky/ddos-pokracuje-cilem-jsou-dnes-weby-mobilnich-operatoru/

[227] Internetové bankovnictví zkolabovalo, další kybernetický útok mířil na banky - Novinky.cz [online]. 2013 [cit. 11.05.2021]. Dostupné z: https://www.novinky.cz/internet-a-pc/clanek/internetove-bankovnictvi-zkolabovalo-dalsi-kyberneticky-utok-miril-na-banky-183723

[228] Fenix [online]. [cit. 28.05.2021]. Dostupné z: https://fe.nix.cz/#about

telefonů, tzv. smartphone (chytrý telefon), které obsahují plnohodnotný operační systém a trpí obdobnými zranitelnostmi jako klasické počítače. Tyto telefony jsou úspěšně napadány trojskými koňmi a dvoufaktorová autentizace v podobě SMS je tímto prolomena. Začíná se psát rok 2014, který je z pohledu malware a výše škod v ČR přelomový. Ve velké míře se začíná šířit bankovní malware, který se šíří především e-mailem, a útočník se v něm vydává za nejrůznější instituce a vybízí příjemce e-mailu k otevření přílohy. Jedná se o tzv. phishing. ČR se prohnalo několik takových phishingových kampaní s různým stupněm závažnosti, v nichž se odesílatel vydával za exekutora, Českou poštu informující o problémech s doručením balíku apod[229]. Ve všech případech e-mail přišel z adresy, která buď neměla s danou institucí vůbec nic společného anebo přišel z adresy, která byla skutečné adrese, kterou daná instituce pro komunikaci s ostatními subjekty používá, celkem podobná.

Byť byl vlastní obsah e-mailu napsán poměrně dobře česky, tak by pozornému příjemci neměly určité gramatické a stylistické nedostatky uniknout. Příjemce mělo zarazit i to, že v e-mailu není oslovován svým jménem, nýbrž jen jako vážený zákazník, což nebývá u podobných institucí, které mají k dispozici osobní údaje svých klientů běžným zvykem. E-mail obsahoval přílohu, kterou byl spustitelný soubor maskující se jako dokument vytvořený v aplikaci Wordpad anebo v pozdějších vlnách útoku archiv obsahující rovněž spustitelný soubor.

Banky od roku 2015 začínají nasazovat systémy na detekci podvodů založené na behaviorálních charakteristikách klienta, tedy jeho chování tzv. Fraud Detection Systém nebo také Fraud Prevention System. zkr. FDS. Tyto systémy vyhodnocují, odkud klient přistupuje, tedy z jakého počítače, a dochází přitom k vytvoření unikátního otisku, který se pak porovná s otiskem uloženým v databázi. K pořízení otisku je často používán obyčejný JS, který zjišťuje rozlišení, barevnou hloubku, verzi operačního systému, prohlížeče, nainstalované fonty, pluginy a další parametry, přičemž posledně známá technologie využívá i specifických charakteristik grafických karet a jejich procesorů, kdy nechává klienta

[229] ČERMÁK, Miroslav. Přečtěte si, jak se najímají muly a vyvádějí peníze z bank – 4. díl. *CleverAndSmart Management Consulting* [online]. 2014 [cit. 28.05.2021]. ISSN 2694-9830. Dostupné z: https://www.cleverandsmart.cz/prectete-si-jak-se-najimaji-muly-a-vyvadeji-penize-z-bank-4-dil/

v neviditelném canvasu renderovat 3D objekt. Kromě spolehlivé identifikace klientova zařízení probíhá i snaha o pořízení behaviorálních charakteristik klienta, tedy kdy se do internetového bankovnictví přihlašuje, jaké částky a na jaké účty posílá, a v některých případech se analyzuje i způsob psaní na klávesnici, pohyby myší apod. ve snaze detekovat jakékoliv nestandardní chování a na to reagovat. Tyto systémy nejspíš byly účinné, protože v následujícím roce podstatně poklesl objem škod, a to z několika desítek miliónů na jednotky miliónů v celém bankovním sektoru, které byly způsobeny tímto typem útoků[230].

Útočníci se začínají více soustředit na napadení bank samotných, protože byť jsou tyto útoky mnohem náročnější a nákladnější na přípravu, tak generují i mnohem větší výnos. Ve větší míře se objevuje pokročilý bezsouborový malware (fileless malware) a jeho popularita roste. Dle Ponemon institutu byl bezsouborový malware použit v roce 2017 v sedmdesáti sedmi procentech případů a má až desetkrát větší úspěšnost než klasický souborový malware[231]. Pak je tu i malware, který je někde na půl cesty mezi souborovým a bezsouborovým, který si svou perzistenci zajišťuje zápisem do registrů Windows a ukládá sem v zašifrované nebo enkódované podobě i zcizené informace, jako to dělá např. Emotet[232], Poweliks[233], PhaseBot[234] či DNSmessenger[235], anebo se spouští přes modifikovaného zástupce, který volá systémový příkaz cmd.exe s parametrem c

[230] ČERMÁK, Miroslav. Jaký má bankovní malware reálný dopad do hospodářských výsledků bank. *CleverAndSmart Management Consulting* [online]. 2015 [cit. 28.05.2021]. ISSN 2694-9830. Dostupné z: https://www.cleverandsmart.cz/jaky-ma-bankovni-malware-realny-dopad-do-hospodarskych-vysledku-bank/

[231] The 2018 State of Endpoint Security Risk. *Ponemon Institute* [online]. 2018 [cit. 28.05.2021]. Dostupné z: https://www.ponemon.org/news-updates/news-press-releases/news/the-2018-state-of-endpoint-security-risk.html

[232] New Banking Malware Uses Network Sniffing for Data Theft - TrendLabs Security Intelligence Blog [online]. 27. červen 2014 [cit. 28.05.2021]. Dostupné z: https://blog.trendmicro.com/trendlabs-security-intelligence/new-banking-malware-uses-network-sniffing-for-data-theft/

[233] RASCAGNÈRES, Paul. Poweliks: the persistent malware without a file [online]. 25. listopad 2016 [cit. 28.05.2021]. Dostupné z: https://www.gdatasoftware.com/blog/2014/07/23947-poweliks-the-persistent-malware-without-a-file

[234] Without a Trace: Fileless Malware Spotted in the Wild - TrendLabs Security Intelligence Blog [online]. 20. duben 2015 [cit. 28.05.2021]. Dostupné z: https://blog.trendmicro.com/trendlabs-security-intelligence/without-a-trace-fileless-malware-spotted-in-the-wild/

[235] BRUMAGHIN, Edmund. Covert Channels and Poor Decisions: The Tale of DNSMessenger [online]. [cit. 28.05.2021]. Dostupné z: http://blog.talosintelligence.com/2017/03/dnsmessenger.html

a jménem souboru ke spuštění[236], který je spustitelným souborem, ale má zpravidla jinou příponu a ikonu odpovídající PDF dokumentu, otevíraném v běžně používané aplikaci Adobe Reader. Registry a zástupci jsou pak ve výše uvedených případech využívány proto, že je zpravidla žádný AV nástroj nekontroluje a malware tak zůstává dlouho nedetekován. Bezsouborový malware pak byl použit i při útocích na banky. Dle McAfee roste bezsouborový malware rychlostí až několika stovek procent ročně[237].

Primárním cílem útoku se stává kompromitace koncových bankovních zařízení, ze kterých se přistupuje do bankovních systémů, systému SWIFT a spravuje bankomatová síť. SWIFT (Society for Worldwide Interbank Financial Telecommunication) je systém, který slouží především k mezinárodnímu platebnímu styku a využívá ho přibližně 11 tisíc bank a finančních i nefinančních institucí po celém světě a denně jsou přes něj realizovány transakce v objemu několika miliard dolarů. Útoky na banky používající SWIFT probíhaly především v letech 2015 až 2016 a došlo k pokusu o vyvedení téměř 1 miliardy USD z bangladéšské centrální banky. Útok však byl odhalen a útočníkům se tak nakonec povedlo vyvést jen 101 miliónu USD, přičemž 81 miliónů směřovalo na Filipíny a 20 miliónů na Srílanku. Další útok pak byl veden ještě na ekvádorskou Banco del Austro, kde bylo převedeno 12 miliónů USD[238], a poslední dokumentovaný útok v roce 2016 pak byl veden ještě na vietnamskou Tien Phong Bank, kde ale útočníkovi pokus o vyvedení 1 miliónu USD nevyšel. Útoky však pokračovaly i v roce 2017 a dle sdělení Ruské centrální banky bylo koncem roku 2017 z jedné ruské banky tímto způsobem převedeno téměř 6 miliónu USD[239].

---

[236] HAY, Phil. Lnk files in Email Malware Distribution. *Trustwave* [online]. 2014 [cit. 28.05.2021]. Dostupné z: https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/lnk-files-in-email-malware-distribution/

[237] SAMANI, Raj. „McAfee Labs Threats Report" Examines Cryptocurrency Hijacking, Ransomware, Fileless Malware. *McAfee Blogs* [online]. 12. březen 2018 [cit. 28.05.2021]. Dostupné z: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/mcafee-labs-threats-report-examines-cryptocurrency-hijacking-ransomware-fileless-malware/

[238] LAYNE, Tom Bergin, Nathan. Special Report: Cyber thieves exploit banks' faith in SWIFT transfer network. *Reuters* [online]. 2016 [cit. 28.05.2021]. Dostupné z: https://www.reuters.com/article/us-cyber-heist-swift-specialreport-idUSKCN0YB0DD

[239] Hackers stole $6 million from Russian bank via SWIFT system, central bank says. *The Japan Times* [online]. 2018 [cit. 28.05.2021]. Dostupné z: https://www.japantimes.co.jp/news/2018/02/16/business/financial-markets/hackers-stole-6-million-russian-bank-via-swift-system-central-bank-says/#.XBpRfNVKiUk

Celkový počet případů, jména konkrétních bank, které se staly obětí útoku, stejně jako celková částka, která byla z bankovního sektoru vyvedena, není známa, protože SWIFT odmítl tyto informace zveřejnit. V ČR údajně k žádným ztrátám v bankovním sektoru v důsledku tohoto útoku nedošlo, nicméně malware použitý v rámci tohoto útoku byl přesto detekován a cílil na SWIFT na platformě Windows, přičemž největší české banky provozují SWIFT na UNIX platformě[240].

Mezitím, co probíhaly útoky na SWIFT, tak se pomalu začaly připravovat další útoky na banky, telekomunikační společnosti a vládní organizace po celém světě, kdy bylo ve výsledku napadeno přes 140 organizací ve 40 zemích světa[241] a jen v Rusku bylo v červnu 2016 vybráno z bankomatů během jedné jediné noci téměř 800 000 USD[242].

Od roku 2014 také zažívají renesanci útoky z počátku počítačové éry spočívající v zašifrování dat na lokálním i síťovém disku, které však mají vzhledem k celkovému počtu trvale připojených zařízení do internetu nesrovnatelně větší úspěch než ve svých počátcích, kdy uživatelé nebyly do internetu připojeni vůbec. Výsledkem je zašifrování několika desítek tisíc počítačů. DDoS útoky probíhají i nadále a jsou zneužívány v konkurenčním boji a k útokům na kritickou infrastrukturu státu.

Od roku 2018 pak probíhají ve větší míře útoky na mobilní telefony, tzv. overaly attack. Aplikace, které sledují, které aplikace běží, a v okamžiku, kdy dojde ke spuštění tak se protlačí do popředí a zobrazí obrazovku ne nepodobnou aplikaci smartbankingu a požadují po uživateli zadání přihlašovacích údajů.

Probíhají ve větší míře útoky na servery vystavené do internetu, jsou masivně napadány koncová zařízení uživatelů včetně chytrých telefonů, tabletů a IoT. Důraz je mimo jiné kladen především na ochranu osobních údajů, což si vyžádalo i vznik nového nařízení známého jako GDPR. Dochází k digitalizaci dat, robotizace procesů a objevují se první útoky na organizace provozující ICS/SCADA systémy. Firmy podporují práci z domova a umožňují svým zaměstnancům se připojovat z jejich soukromých zařízení, která nemají zcela pod kontrolou do vnitřních

[240] Vyplynulo z rozhovorů s CSO největších bank v ČR.
[241] Fileless attacks against enterprise networks. *Securelist* [online]. 2017 [cit. 28.05.2021]. Dostupné z: https://securelist.com/fileless-attacks-against-enterprise-networks/77403/
[242] GOLOVANOV, Sergey. ATMitch: remote administration of ATMs. *Securelist* [online]. 2017 [cit. 28.05.2021]. Dostupné z: https://securelist.com/atmitch-remote-administration-of-atms/77918/

systémů. Objevují se tzv. těžařské viry (cryptominery), které neoprávněně zneužívají výpočetní výkon počítačů k těžbě virtuální měny. Z rozhovoru s víceprezidentem Cisco Mattem Watchinski vyplynulo, že byť objem SPAMu v posledních letech klesá, stále však přestavuje drtivou většinou rozeslaných e-mailů, tak je stále agresivnější a rozesílatelé využívají pokročilých technik k tomu, aby SPAM protlačili skrz nejrůznějších antispamové filtry[243]. Objem SPAMu činí více jak 80 % všech zpráv a v některých organizacích i více jak 90 %. Watchinski jako největší hrozbu uvádí vyděračský malware (ransomwarem) i když zde je patrný určitý pokles, těžbu kryptoměny (cryptojacking) kde je rovněž patrný určitý pokles, a v neposlední řadě pak bezsouborový malware (fileless malware), jehož objem naopak roste.

Koncem dekády stále více zaměstnanců pracuje z domova, z nezabezpečených počítačů a z nezabezpečeného prostředí, tento trend pak akcelerovala pandemie COVID-19. Spolu s tím vzrostl i počet kybernetických útoků vedených na soukromý i veřejný sektor. Nejvíce postižené se jeví organizace působící ve zdravotnictví, ale útoky jsou vedeny i na státní správu a další organizace. Počet napadených subjektů je však výrazně vyšší, než kolik uvádí média. **Oslovení zástupci firem, které se věnují obnově provozu informačních systémů po kybernetickém útoku, hlásí až desetinásobně větší počet obětí, než o kterých píší média.** Tomu by odpovídal i propastný rozdíl mezi počtem medializovaných případů a počtem hlášených kybernetických útoků.

[243] WOLF, Karel. Matt Watchinski (Cisco Talos): Spamových e-mailů bylo jen v prosinci rozesláno přes 311 miliard. *Lupa.cz* [online]. 2019 [cit. 12.03.2019]. ISSN 1213-0702. Dostupné z: https://www.lupa.cz/clanky/matt-watchinski-cisco-talos-spamovych-emailu-bylo-jen-v-prosinci-rozeslano-pres-311-miliard/

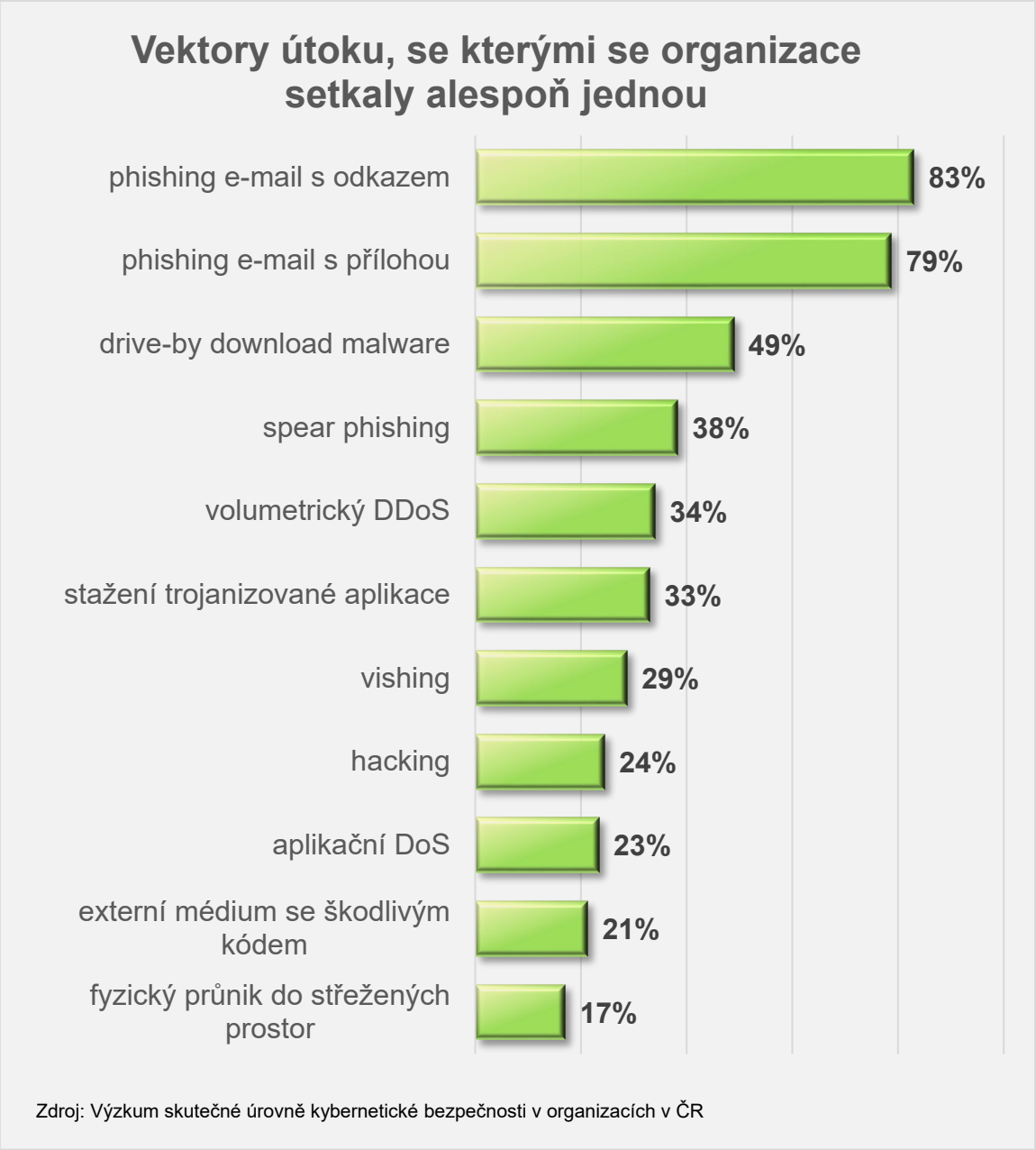
Vektory útoku

V případě kybernetických útoků se potvrdilo, že **nejčastějším vektorem útoku je phishing**, ať už s odkazem nebo s přílohou, se kterým se setkaly více jak tři čtvrtiny organizací. S velkým odstupem, jej pak následuje drive-by download malware, se kterým se setkala téměř polovina organizací. Což je poměrně hodně, obzvlášť když si uvědomíme, že výrazně poklesl podíl webů obsahujících a zobrazujících flashový obsah, který byl exploit kity umístěnými v reklamních banerech zobrazovaných v reklamních systémech dříve tak hojně využíván.

Dalším vektorem útoku je pak volumetrický DDoS útok a škodlivý kód umístěný v trojanizované aplikaci, s tím se potýkala přibližně třetina organizací. Určitým překvapením je **vishing, který donedávna nebyl příliš častým vektorem útoku**, především kvůli jazykové bariéře. Nicméně setkala se s ním více jak čtvrtina organizací. Téměř čtvrtina organizací se pak setkala s hackingem a aplikačním DOSem.

Nejčastější vektory útoku pak uzavírají útoky, při kterých se útočník musí dostat do bezprostřední blízkosti organizace. Těmto útokům čelila přibližně pětina organizací, jak zachycuje Graf 4 – Vektory útoku. Toto zjištění by mělo představovat pro organizace určité varování, že kromě kybernetické bezpečnosti je nutné se soustředit i na obranu fyzického perimetru. Dochází zde zpravidla k **pohození média se škodlivým kódem v prostorách organizace** anebo k **fyzickému průniku do objektu organizace**.

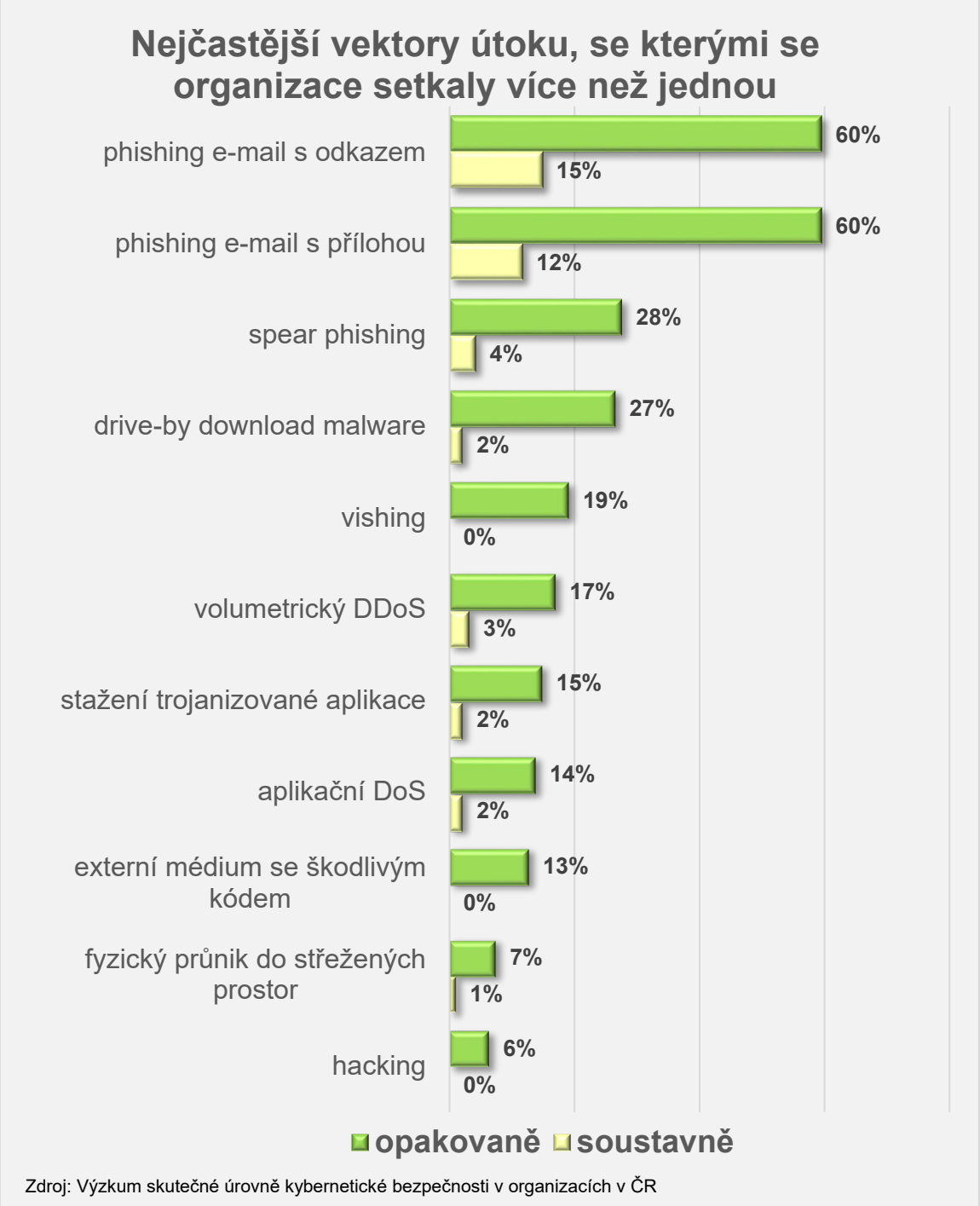
Graf 4 – Vektory útoku



Graf 5 – Nejčastější vektory útoku zachycuje, co se stane, když se zaměříme na vektory útoku, se kterými se organizace setkaly během roku více než jednou, anebo kterým jsou vystaveny soustavně. Vidíme, že se nám podstatně zásadním způsobem nezměnilo pořadí vektorů útoku. Phishing nadále zůstává nejčastějším vektorem útoku, do první poloviny se přesunul vishing a naopak hacking se dostal na poslední místo, což by mohlo znamenat, že po prvním průniku organizace

rychle přijme nějaká opatření, anebo že v případě neúspěchu jde hacker jinam a cílí na tzv. low hanging fruit.

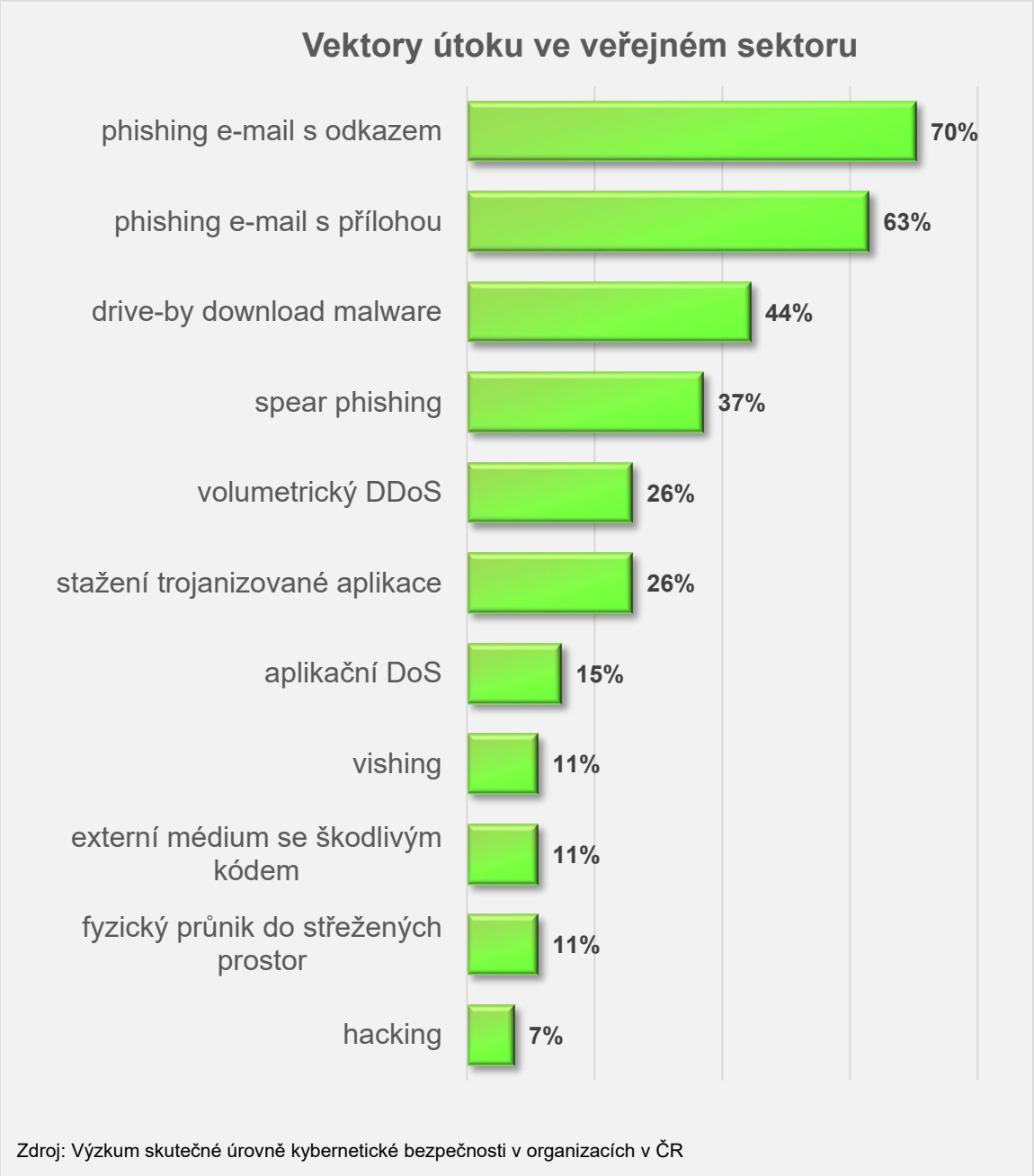
Graf 5 – Nejčastější vektory útoku



Zdroj: Výzkum skutečné úrovně kybernetické bezpečnosti v organizacích v ČR

Vliv sektoru na volbu vektoru útoku zachycují následující grafy. Graf 6 – Vektory útoku a veřejný sektor zachycuje, s jakými vektory útoku se potýkaly organizace působící ve veřejném sektoru.

Graf 6 – Vektory útoku a veřejný sektor

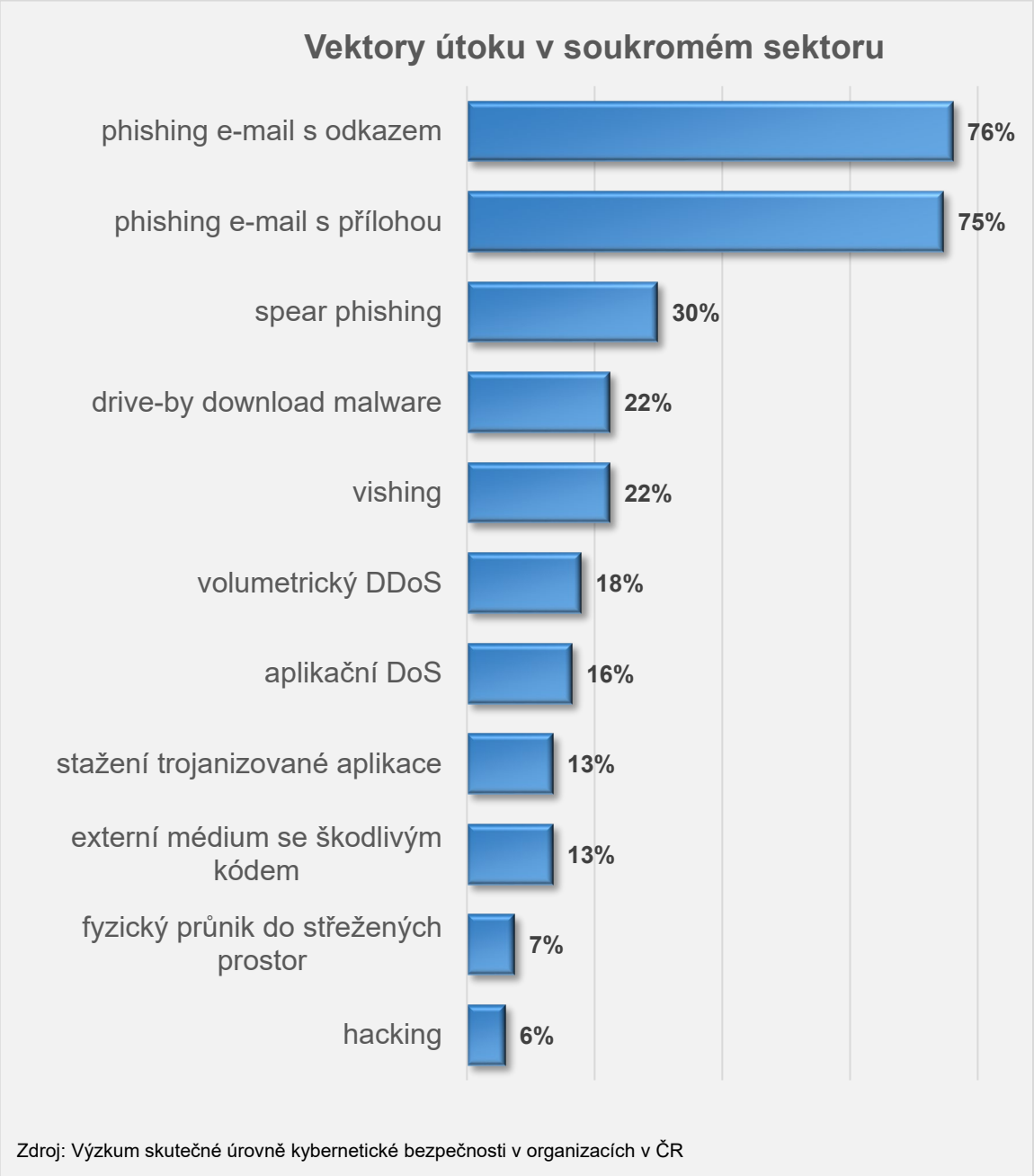


Zdroj: Výzkum skutečné úrovně kybernetické bezpečnosti v organizacích v ČR

Na první pohled je patrné, že zde k žádné podstatné změně, co do preference vektorů útoků, nedošlo. Pořadí nejčastějších, a naopak nejméně častých vektorů útoku se prakticky vůbec nezměnilo.

Obdobou situaci pak můžeme pozorovat i v soukromém sektoru, což zachycuje Graf 7 – Vektory útoku a soukromý sektor. I zde zůstalo pořadí nejčastějších a nejméně častých vektorů útoků více méně stejné.

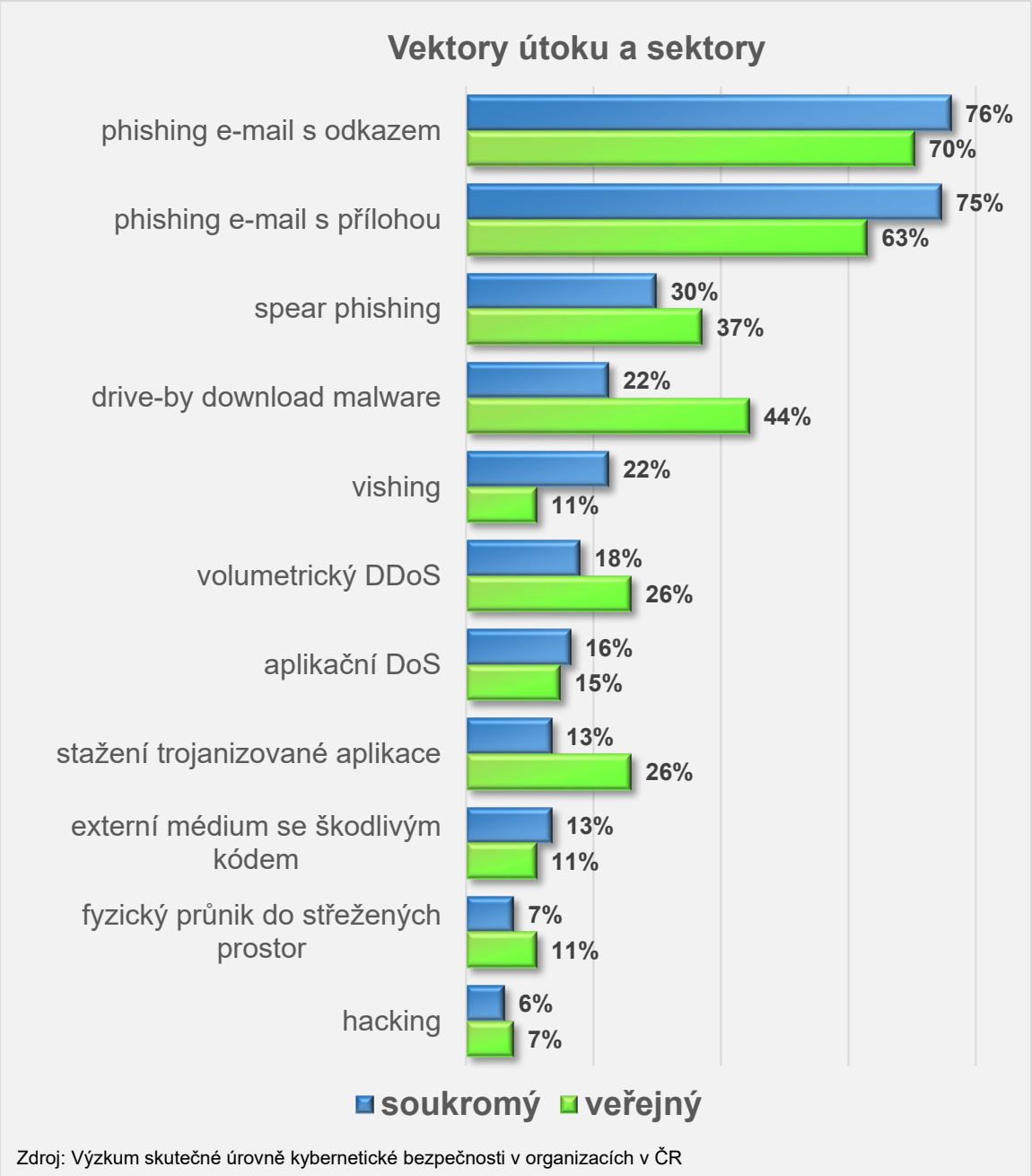
Graf 7 – Vektory útoku a soukromý sektor



Zdroj: Výzkum skutečné úrovně kybernetické bezpečnosti v organizacích v ČR

Když pak oba tyto pohledy na soukromý a veřejný sektor promítneme do jednoho, získáme Graf 8 – Vektory útoku a sektory, kde vidíme, že zde nejsou až na výjimky podstatné rozdíly. Nicméně nabízí se otázka, proč organizace působící ve veřejném sektoru reportují výrazně více drive-by download malware útoků nebo trojanizovaných aplikací.

Graf 8 – Vektory útoku a sektory

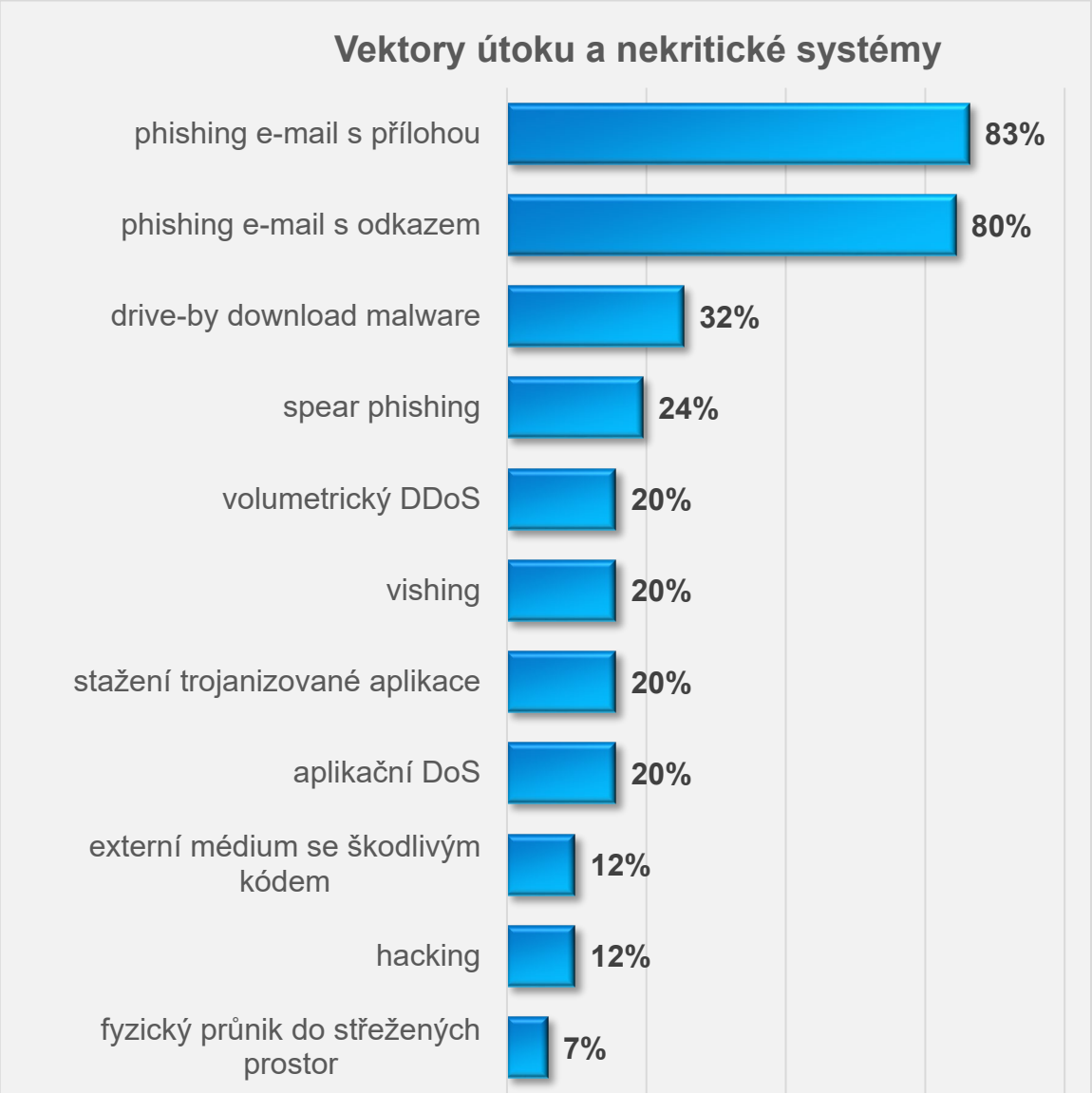


Zdroj: Výzkum skutečné úrovně kybernetické bezpečnosti v organizacích v ČR

Pokud jde o to, zda kritičnost systému nějakým způsobem ovlivňuje volbu vektoru

útoku, tak ani zde nedochází ke změně preferencí. Graf 9 – Vektory útoku a nekritické systémy zachycuje vektory útoku, se kterými se setkaly organizace provozující systém, který nespadá pod působnost ZokB.

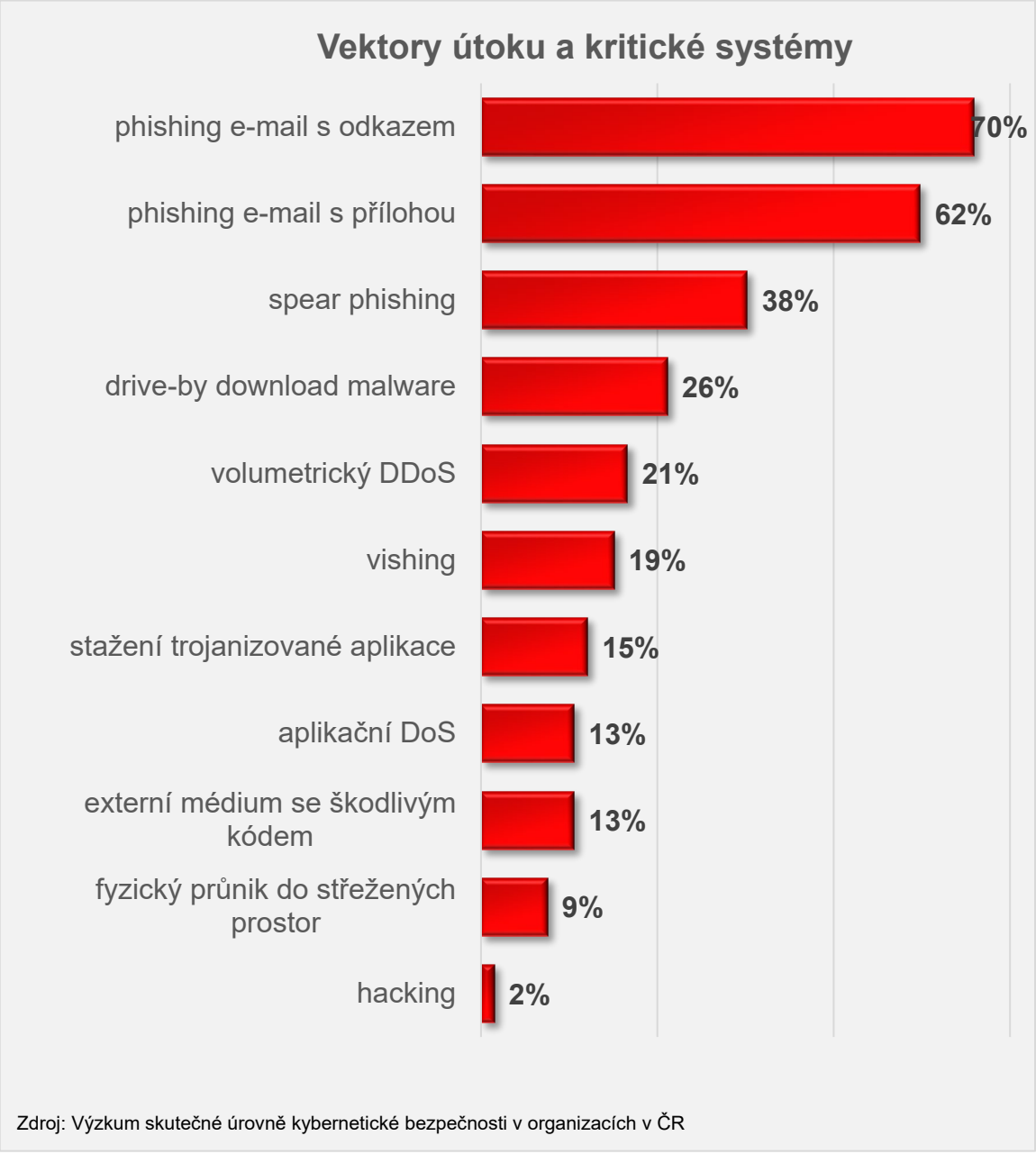
Graf 9 – Vektory útoku a nekritické systémy



Zdroj: Výzkum skutečné úrovně kybernetické bezpečnosti v organizacích v ČR

Graf 10 – Vektory útoku a kritické systémy zachycuje vektory útoku, se kterými se naopak setkaly organizace provozující systém, který spadá pod působnost ZoKB. Ani zde nenastává žádná významná změna.

Graf 10 – Vektory útoku a kritické systémy

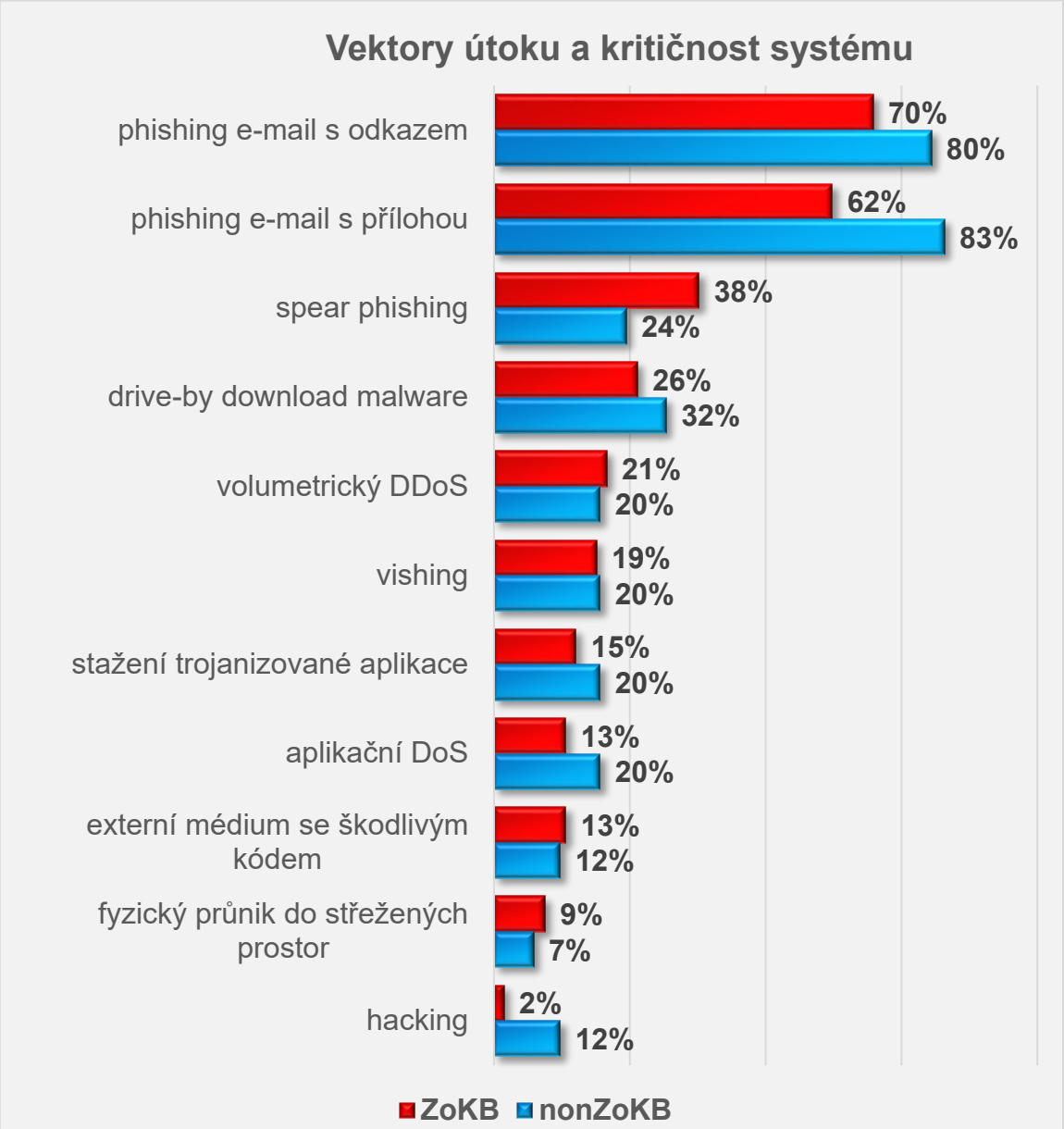


Zdroj: Výzkum skutečné úrovně kybernetické bezpečnosti v organizacích v ČR

Když oba tyto grafy spojíme do jednoho, tak získáme Graf 11 – Vektory útoku a kritičnost systému, z kterého je patrné, že útočníci preferují vesměs stejné vektory útoku. A pokud jde o kumulativní četnost detekce vektorů útoku, tak ta je nepatrně vyšší u organizací, které neprovozují systém, který by spadal pod

působnost Zákona o kybernetické bezpečnosti (non ZoKB). Ony rozdíly jsou ale natolik nevýrazné, že jim nelze přikládat zásadní význam.

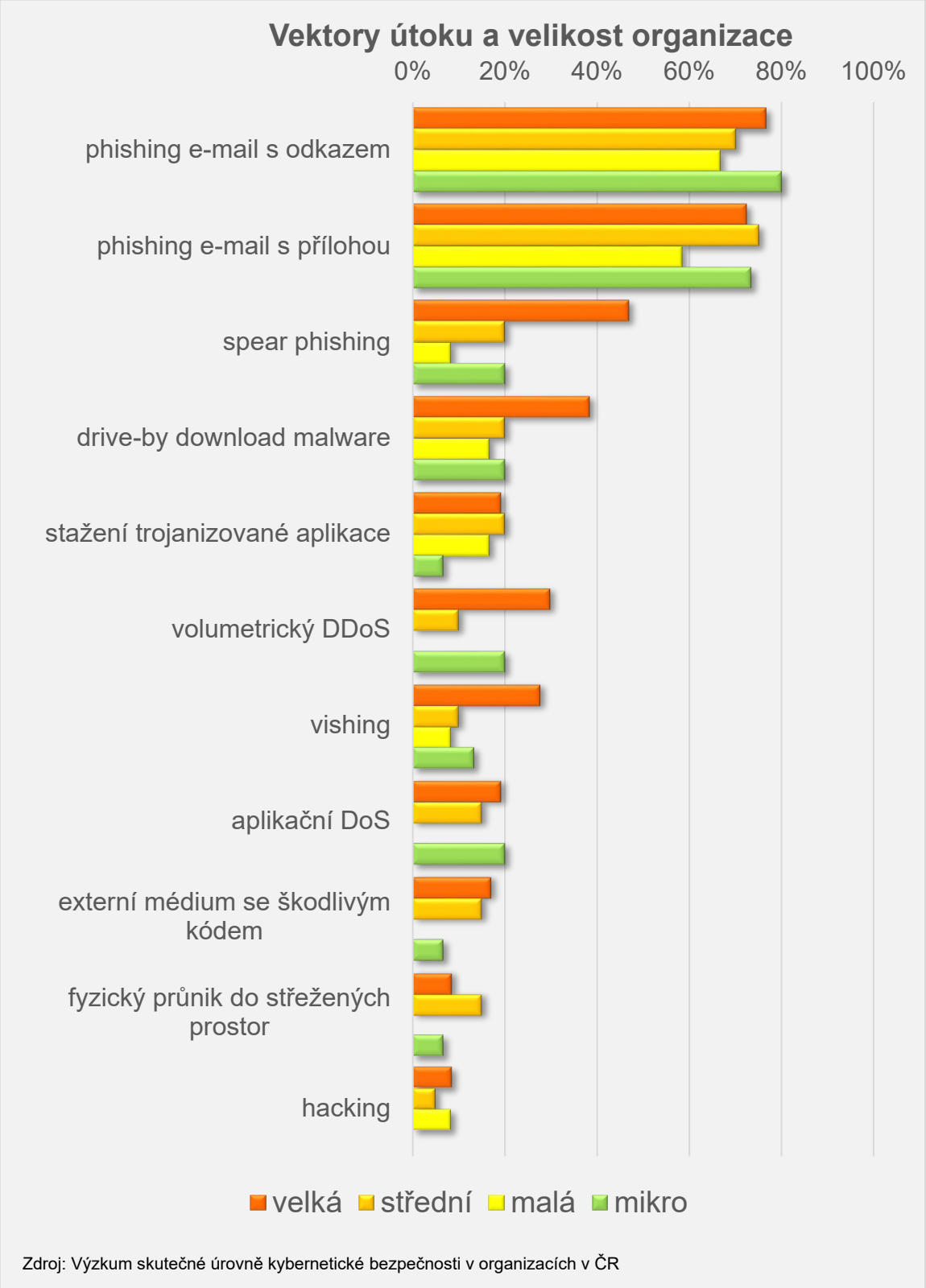
Graf 11 – Vektory útoku a kritičnost systému



Zdroj: Výzkum skutečné úrovně kybernetické bezpečnosti v organizacích v ČR

Pokud jde o závislost vlivu velikosti organizace na zvolené vektory útoku, tak ani zde se pořadí nemění, jak ostatně zachycuje Graf 12 – Vektory útoku a velikost organizace. Jen s některými méně častými vektory útoku, jako je DDoS, DoS, baiting, tailgating a hacking se mikro a malé organizace vůbec nesetkaly.

Graf 12 – Vektory útoku a velikost organizace



Zdroj: Výzkum skutečné úrovně kybernetické bezpečnosti v organizacích v ČR

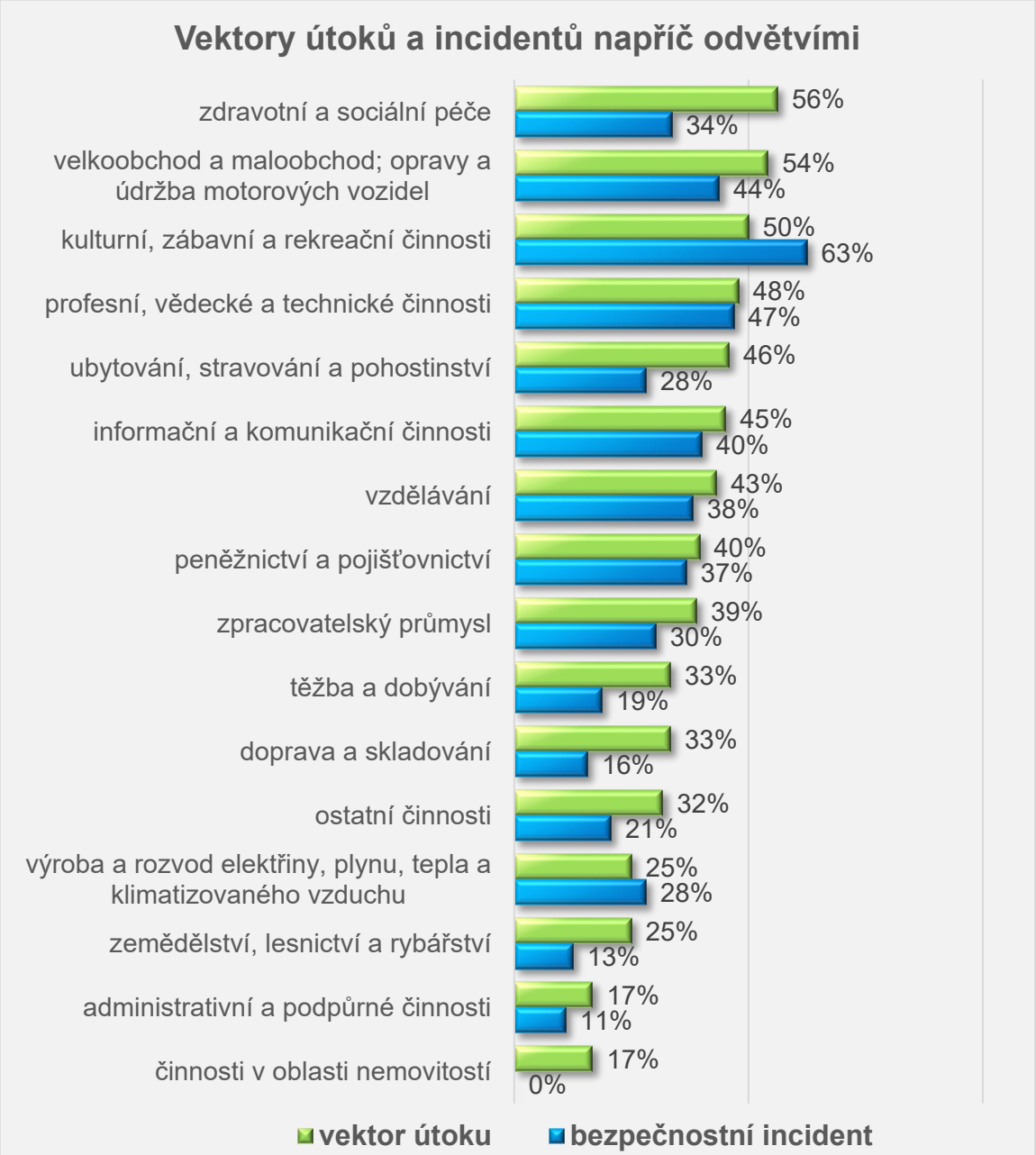
Výše uvedená zjištění, tj. nepreference vektorů útoku v závislosti na kritičnosti systému a sektoru hospodářství nasvědčují spíše tomu, že organizace mají ve

většině případů co do činění spíše s plošnými než cílenými útoky. Zároveň je však v rámci objektivity třeba upozornit, že skutečnost, zda organizace detekovala dané vektory útoku, může být do značné míry ovlivněna ani ne tak počtem těchto útoků, jako úrovní zavedení samotných bezpečnostních řešení umožňujících jejich detekci.

Graf 13 – Vektory útoku a odvětví zachycuje situaci v jednotlivých odvětvích, nicméně je třeba jej brát se značnou rezervou, protože počet organizací v jednotlivých odvětvích výběrového souboru nedopovídá zcela podílu těchto organizací v základním souboru. Nicméně je zřejmé, že např. zdravotnictví není jediné odvětví, které by detekovalo kybernetické útoky a zároveň není tím odvětvím, které by evidovalo nejvíce incidentů.

Média nemaje informace o probíhajících útocích v jiných odvětvích, pak z hlášených útoků ze strany provozovatelů nemocnic vyvozují mylný závěr, že se jedná o útoky cílené jen výhradně na toto odvětví.

Graf 13 – Vektory útoku a odvětví



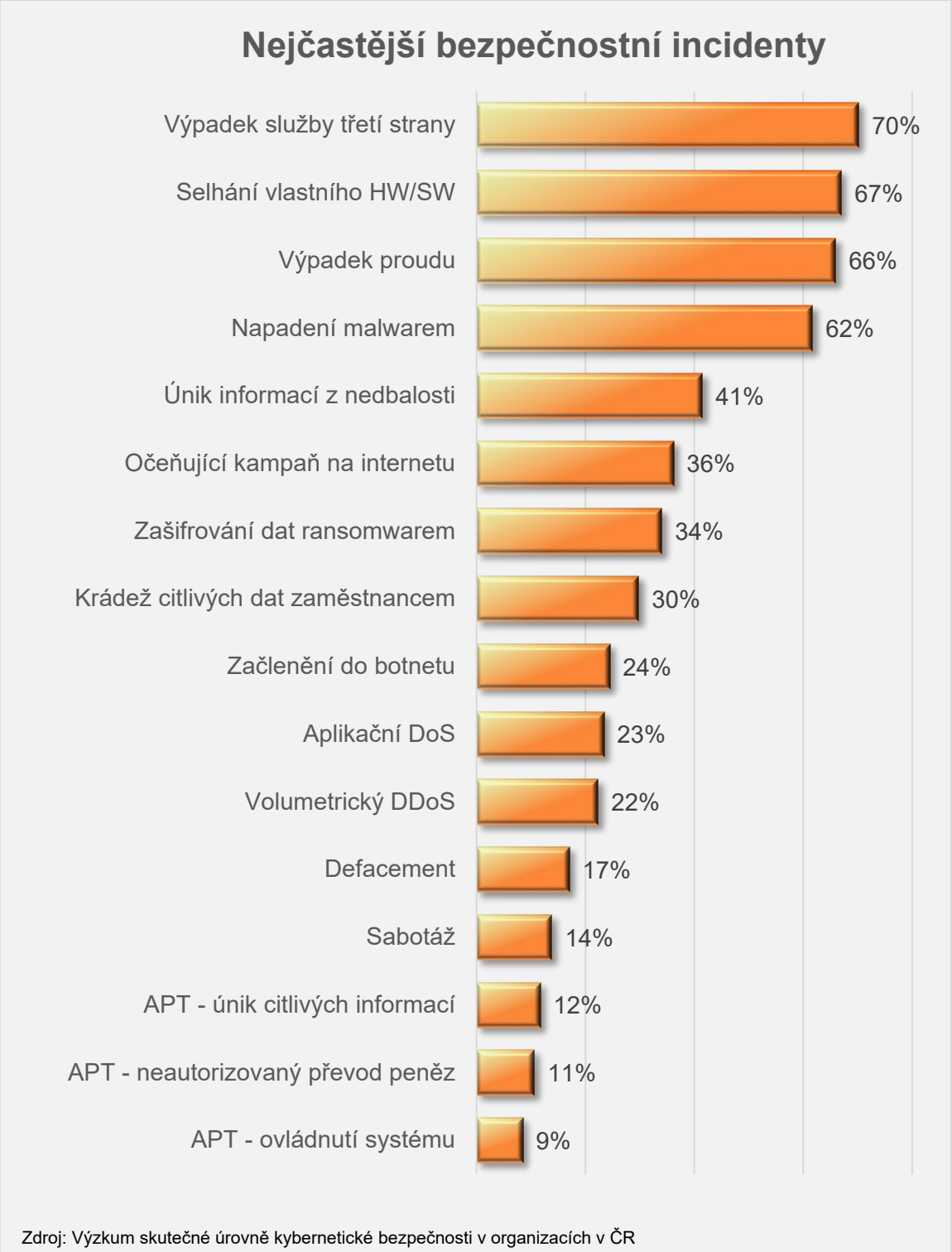
Zdroj: Výzkum skutečné úrovně kybernetické bezpečnosti v organizacích v ČR

Incidenty

Mnohem zajímavější, než jednotlivé vektory útoku jsou bezpečnostní incidenty, ke kterým v organizacích došlo. Graf 14 – Bezpečnostní incidenty zachycuje četnosti výskytu jednotlivých incidentů, na prvním místě se nachází výpadek služeb třetích stran, následovaný selháním vlastního HW/SW, výpadkem proudu a napadení malwarem, ke kterému se přiznaly téměř dvě třetiny organizací. S odstupem pak následuje únik informací z nedbalosti, zašifrování dat

ransomwarem, očerňující kampaň na internetu, krádež dat zaměstnancem. Nejméně se pak organizace setkávaly s APT útoky.

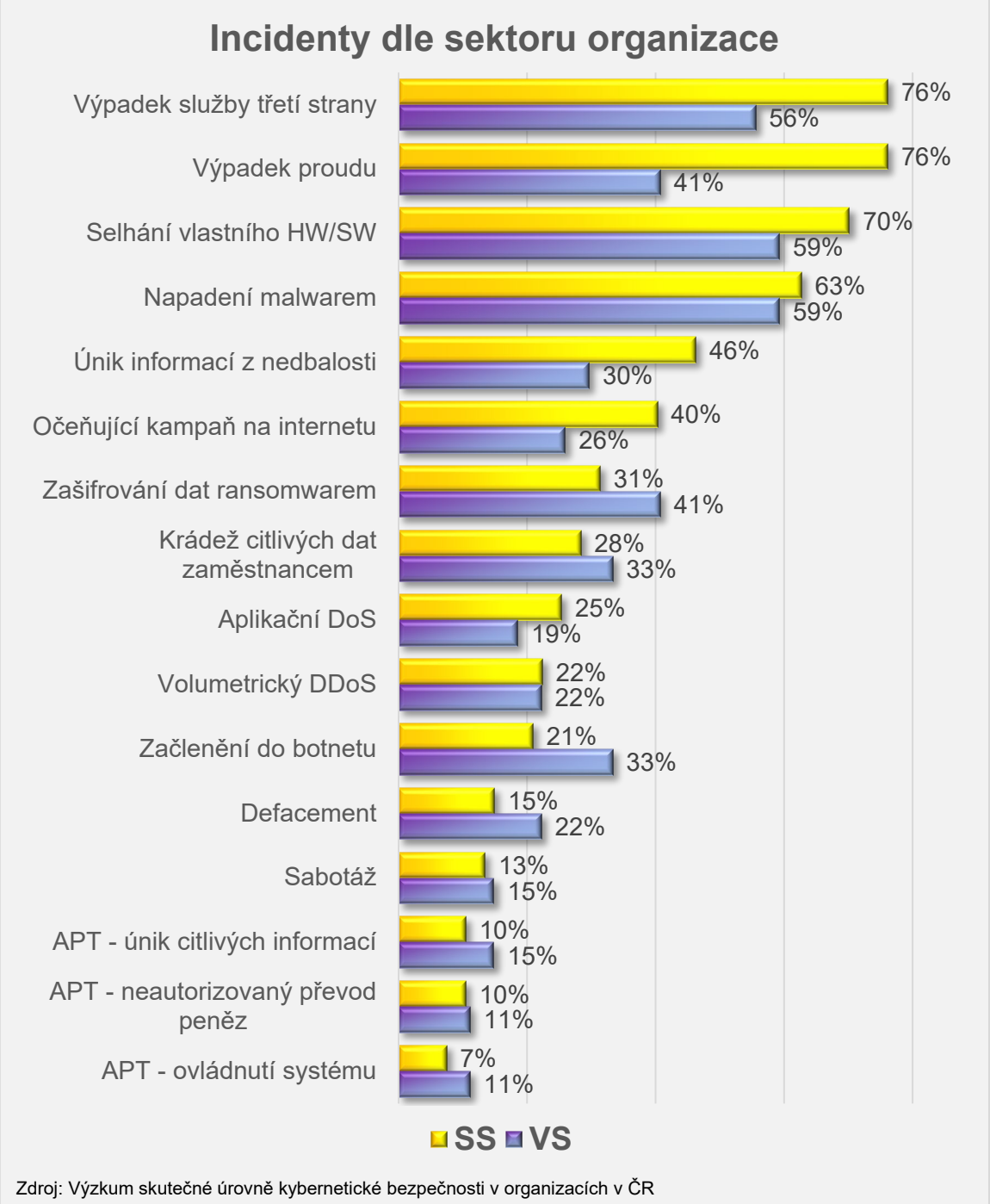
Graf 14 – Bezpečnostní incidenty



Zdroj: Výzkum skutečné úrovně kybernetické bezpečnosti v organizacích v ČR

Graf 15 – Incidenty dle sektoru zachycuje, k jakým incidentům docházelo nejčastěji v soukromém a veřejném sektoru.

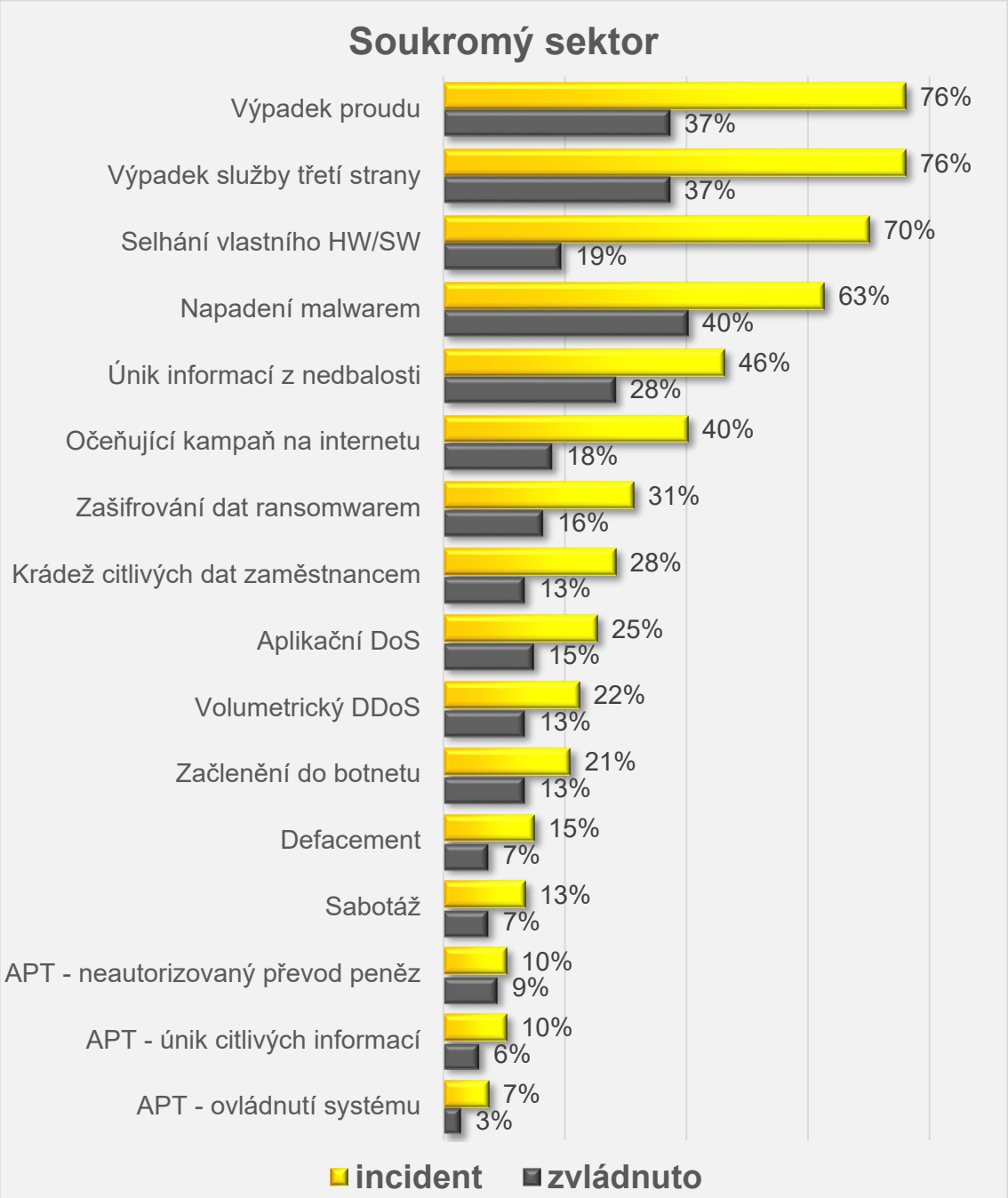
Graf 15 – Incidenty dle sektoru



Zdroj: Výzkum skutečné úrovně kybernetické bezpečnosti v organizacích v ČR

Jak se s bezpečnostními incidenty vypořádal soukromý sektor, zachycuje Graf 16 – Incidenty v soukromém sektoru. Vidíme, že v mnoha případech se soukromému sektoru podařilo až polovinu incidentů zvládnout, aniž by utrpěl nějakou ztrátu.

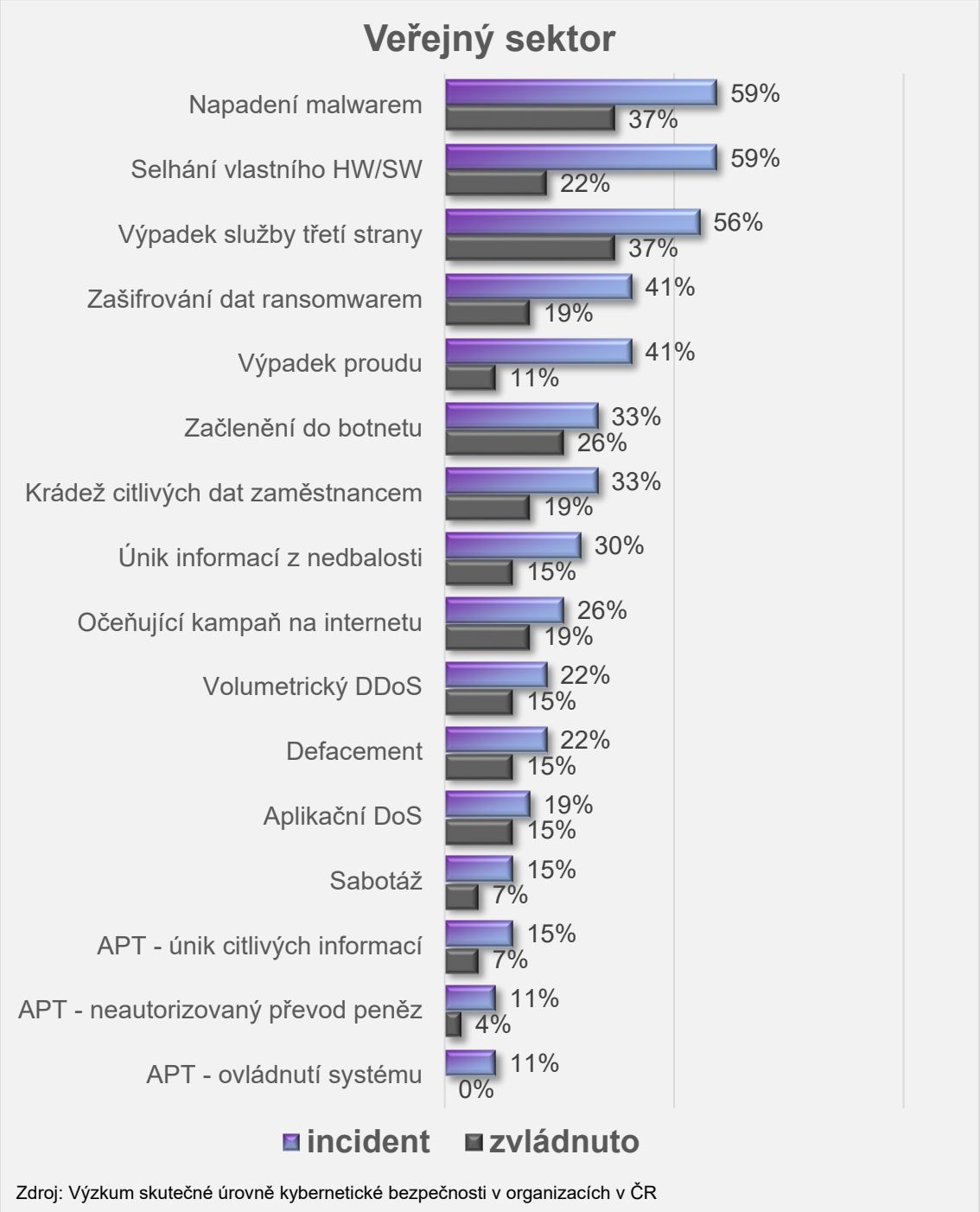
Graf 16 – Incidenty v soukromém sektoru



Zdroj: Výzkum skutečné úrovně kybernetické bezpečnosti v organizacích v ČR

Graf 17 – Incidenty a veřejný sektor ukazuje, že v případě veřejného sektoru je situace velice podobná, i on se dokázal s bezpečnostními incidenty velice dobře vypořádat.

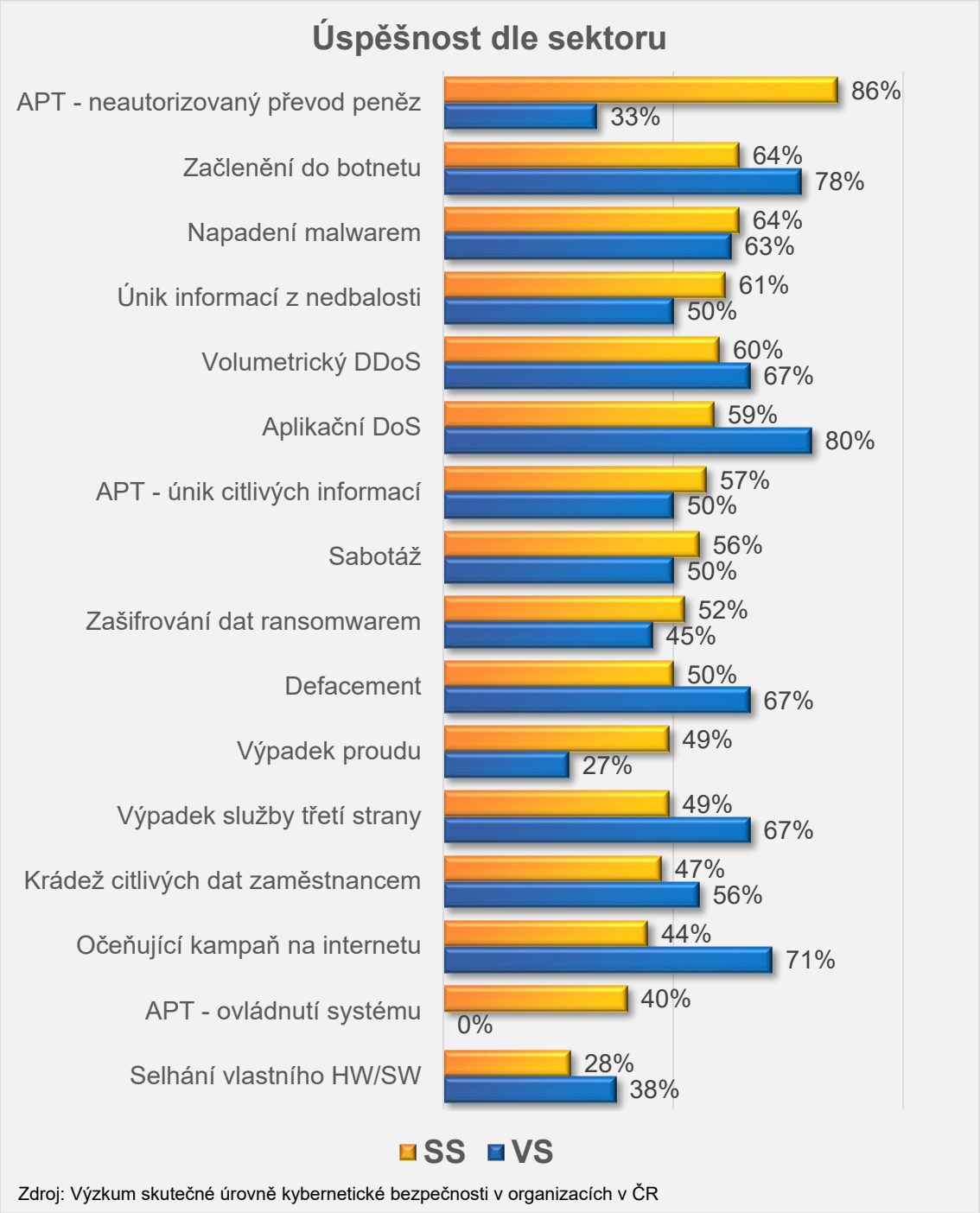
Graf 17 – Incidenty a veřejný sektor



Zdroj: Výzkum skutečné úrovně kybernetické bezpečnosti v organizacích v ČR

Když pak porovnáme úspěšnost soukromého a veřejného sektoru, tak zjistíme, že s některými incidenty se dokázal lépe vypořádat soukromý sektor a s některými zase naopak veřejný sektor, jak zachycuje v Graf 18 – Vypořádání s incidenty, takže nelze prohlásit, který sektor je na tom celkově lépe.

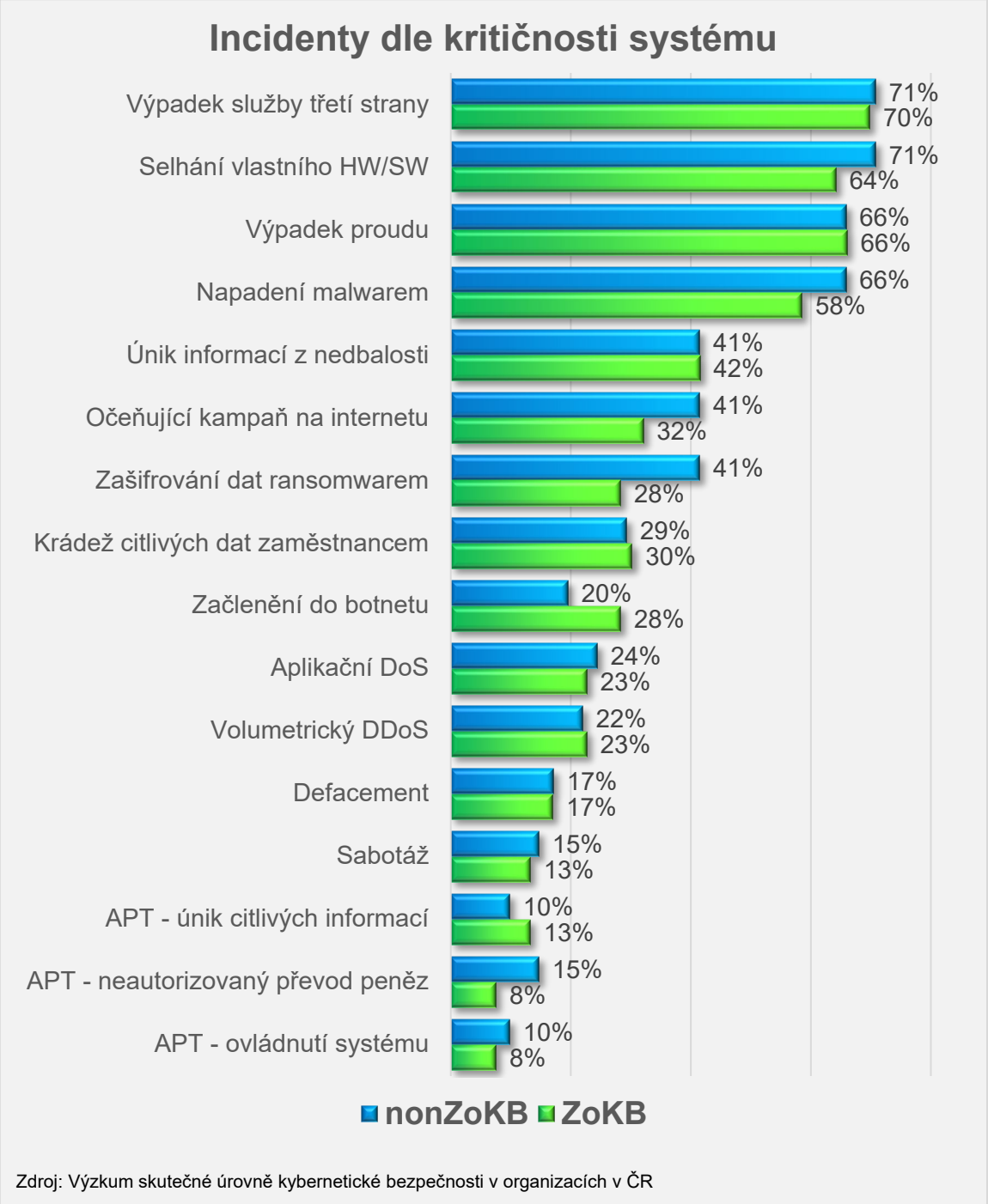
Graf 18 – Vypořádání s incidenty



Zdroj: Výzkum skutečné úrovně kybernetické bezpečnosti v organizacích v ČR

Jiný pohled pak nabízí Graf 19 – Incidenty dle kritičnosti systému, kde dochází k porovnání zastoupení incidentů z pohledu kritičnosti systému, ale i zde vidíme, že je situace poměrně vyrovnaná.

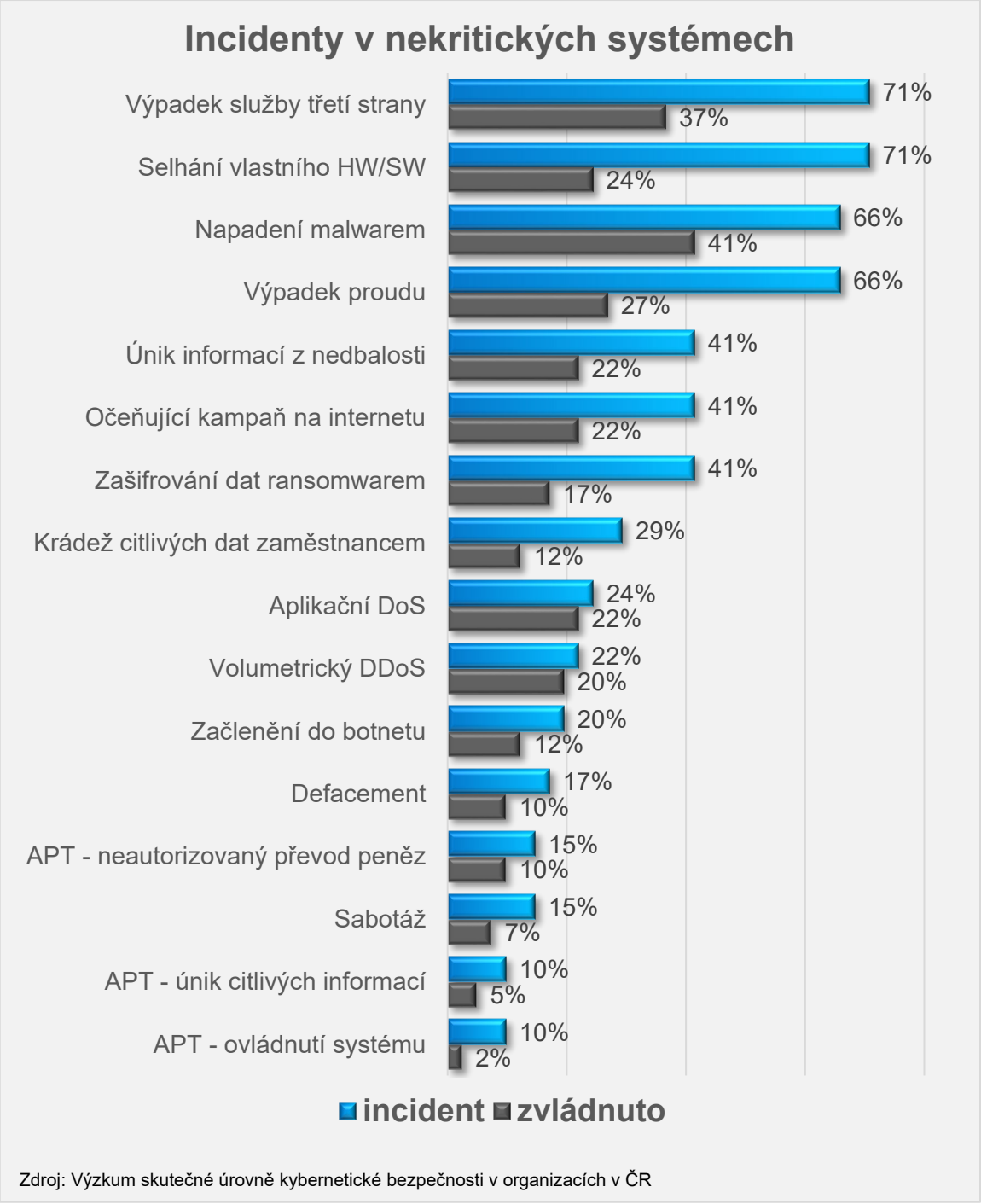
Graf 19 – Incidenty dle kritičnosti systému



Zdroj: Výzkum skutečné úrovně kybernetické bezpečnosti v organizacích v ČR

Graf 20 – Incidenty v nekritických systémech pak přináší odpověď na otázku, jak se s incidenty vypořádaly organizace provozující nekritické systémy.

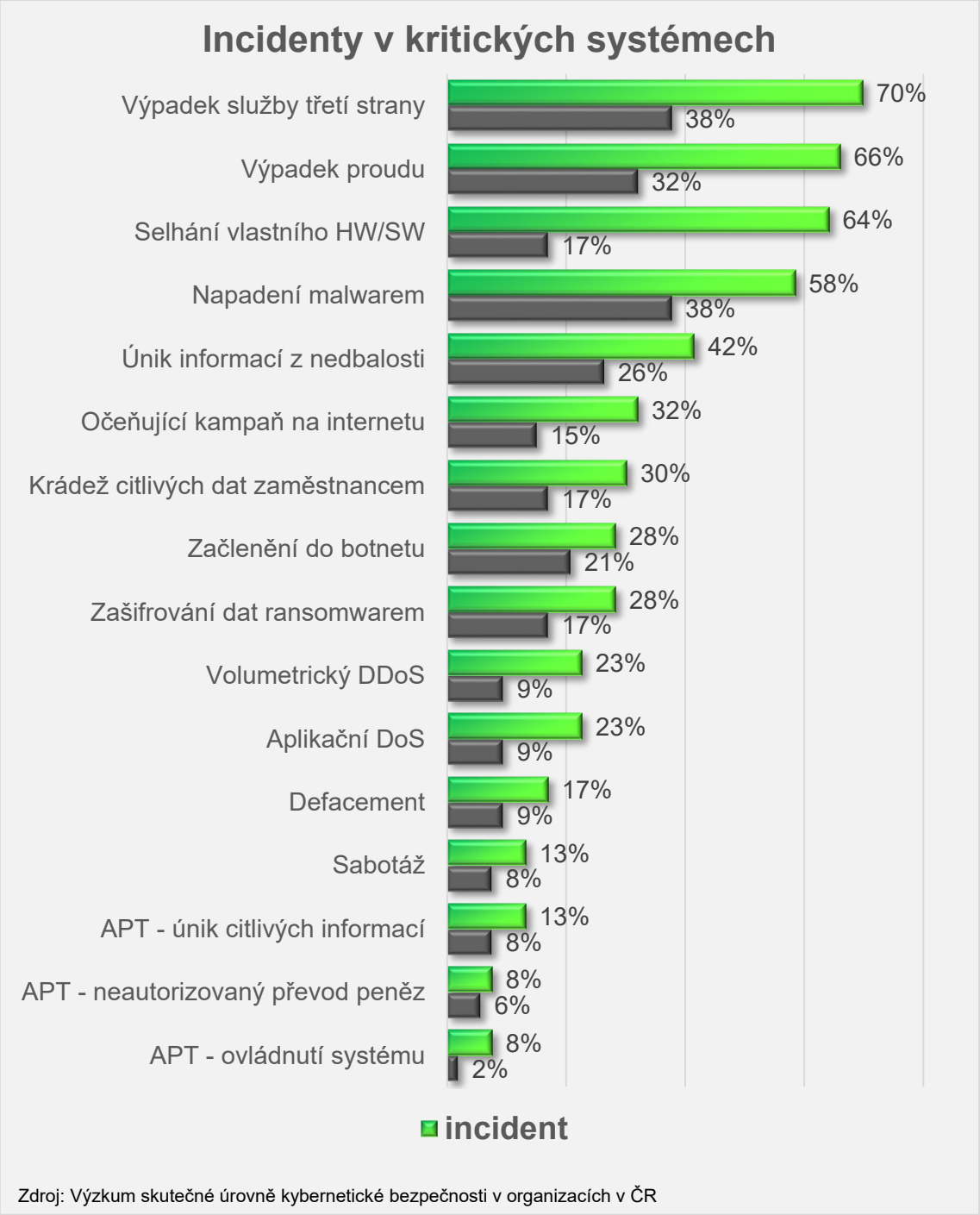
Graf 20 – Incidenty v nekritických systémech



Zdroj: Výzkum skutečné úrovně kybernetické bezpečnosti v organizacích v ČR

Pokud jde o organizace provozující kritické systémy, tak zde je situace velice podobná a tu zachycuje Graf 21 – Incidenty v kritických systémech.

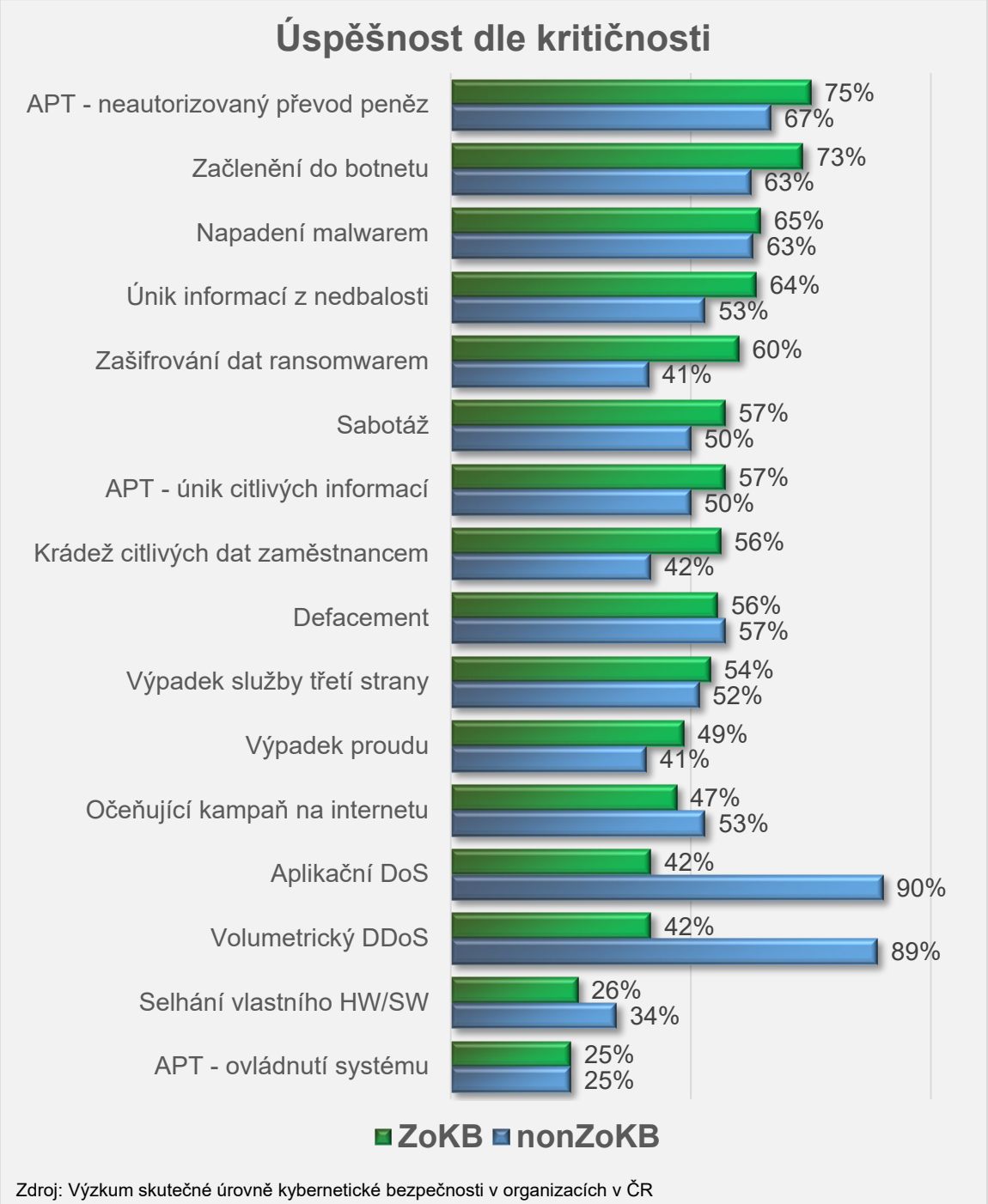
Graf 21 – Incidenty v kritických systémech



Zdroj: Výzkum skutečné úrovně kybernetické bezpečnosti v organizacích v ČR

Když pak porovnáme úspěšnost organizací provozujících kritické a organizací provozující nekritické systémy, tak ani zde nevidíme příliš velké rozdíly, s výjimkou DDoS a DoS útoků, jak zachycuje Graf 22 – Zvládání incidentů.

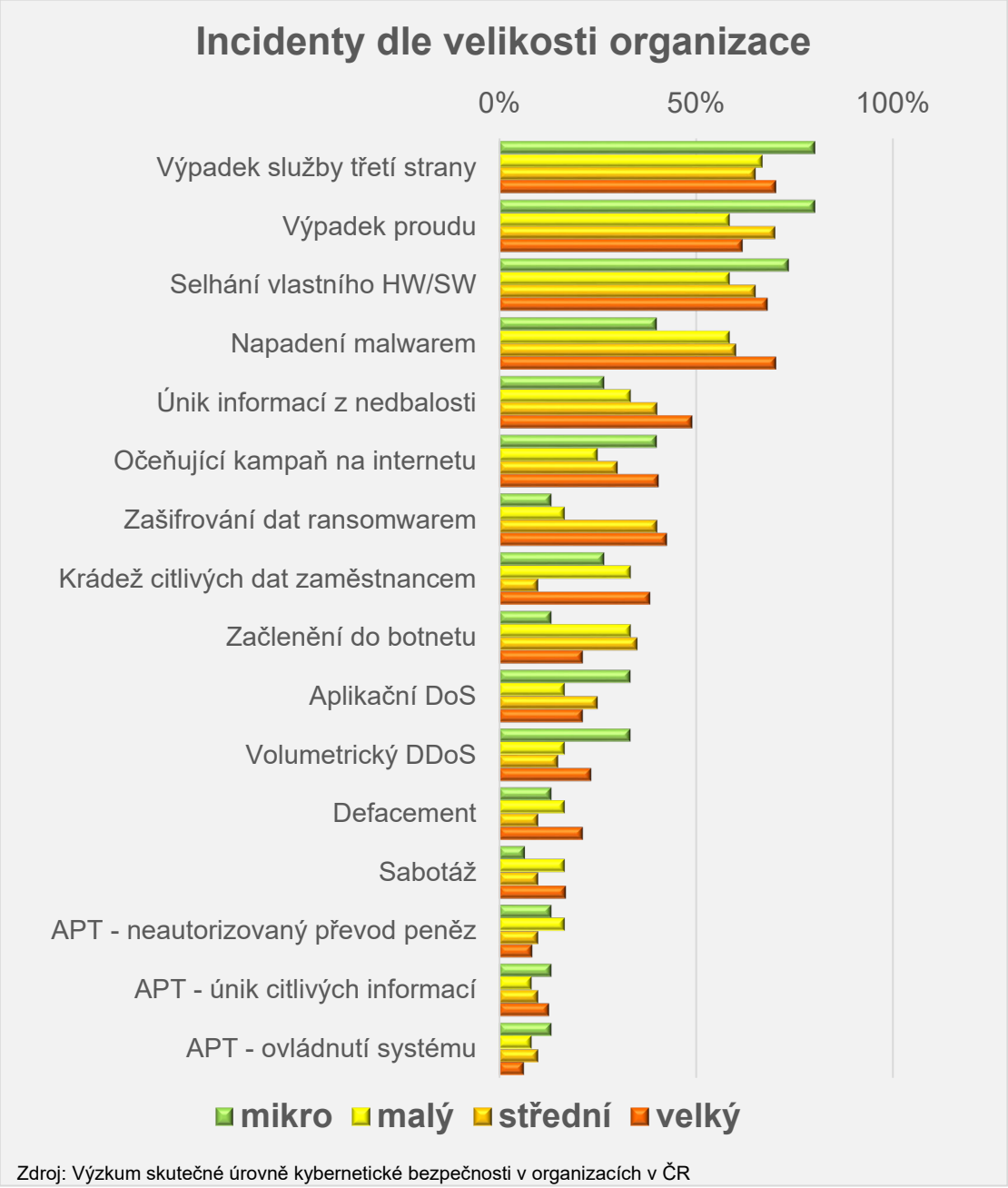
Graf 22 – Zvládání incidentů



Zdroj: Výzkum skutečné úrovně kybernetické bezpečnosti v organizacích v ČR

Pokud jde o incidenty z pohledu velikosti organizace, tak i zde lze velice obtížně hledat nějakou závislost, jak zachycuje Graf 23 – Incidenty dle velikosti organizace. Nezdá se, že by velikost organizace sama o sobě přitahovala útočníky. Mnohde jsou rozdíly jen v jednotkách procent. U úniku informací z nedbalosti, malware a ransomware roste počet incidentů s velikostí organizace, ale u ostatních incidentů tomu tak není.

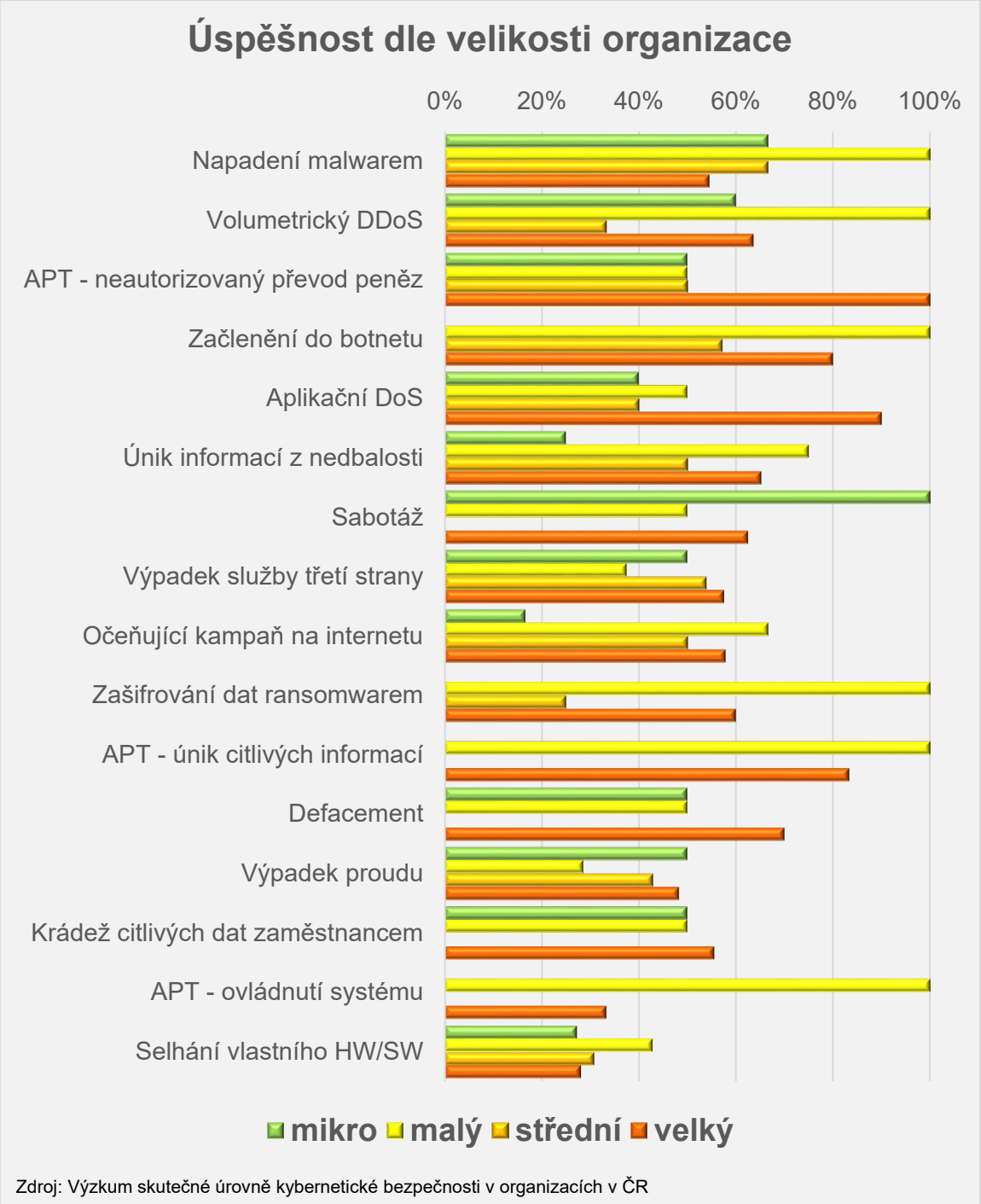
Graf 23 – Incidenty dle velikosti organizace



Zdroj: Výzkum skutečné úrovně kybernetické bezpečnosti v organizacích v ČR

Pokud jde o úspěšnost vypořádání se s incidenty, tak je zajímavé, že malé organizace jsou v tomto směru velice efektivní, jak zachycuje Graf 24 – Zvládání incidentů dle velikosti organizace.

Graf 24 – Zvládání incidentů dle velikosti organizace

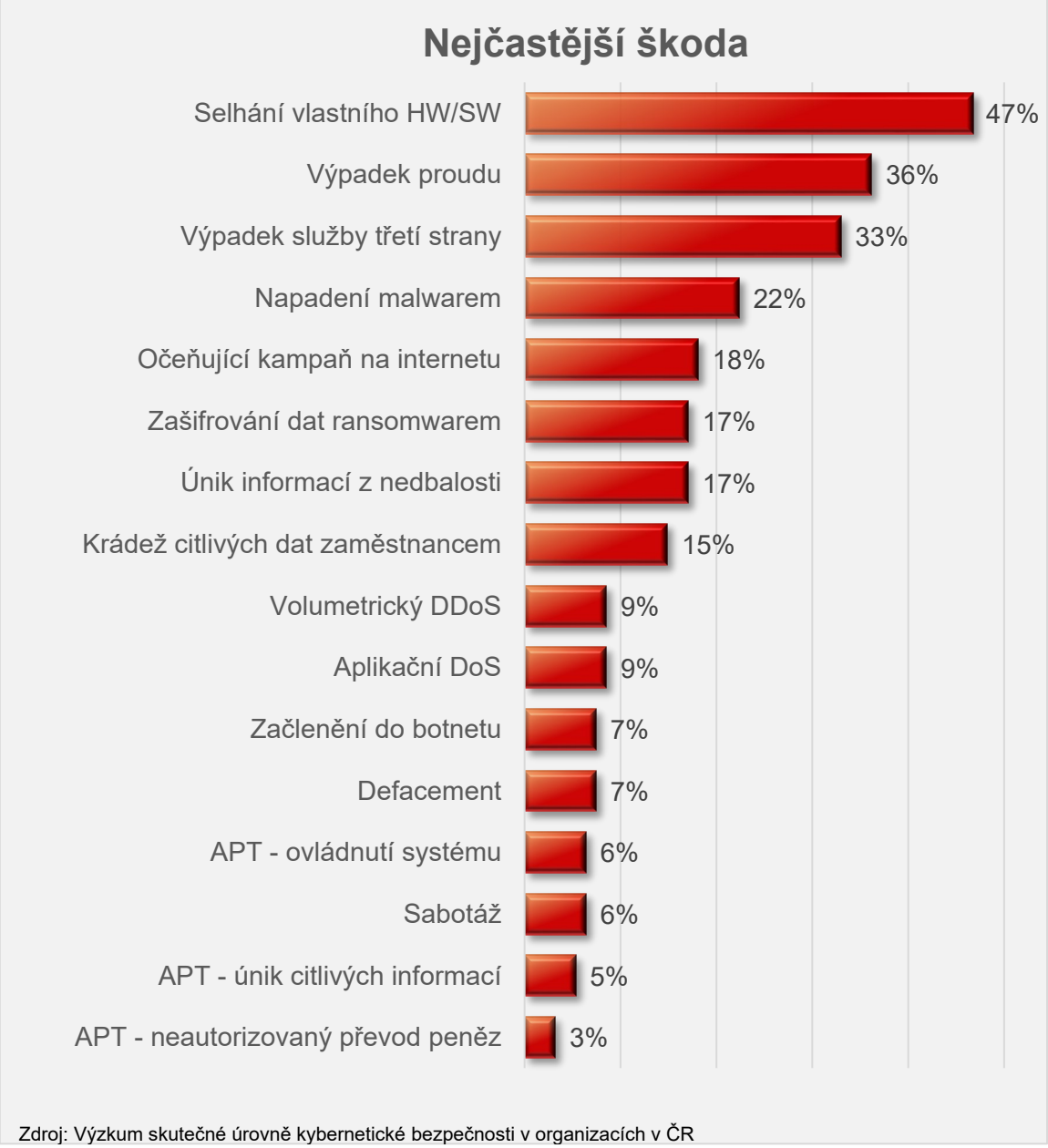


Zdroj: Výzkum skutečné úrovně kybernetické bezpečnosti v organizacích v ČR

Škody

Než pouhý počet incidentů je mnohem zajímavější, co způsobilo nejčastější škodu, jak zachycuje Graf 25 – Škody. Zde je třeba si uvědomit, že incident ještě automaticky nemusí způsobit nějakou podstatnou škodu, může dojít jen k narušení bezpečnosti, pak hovoříme o technickém dopadu, ale k business dopadu nemusí dojít. Ale ani z tohoto pohledu se na tomto pořadí v zásadě nic nezměnilo.

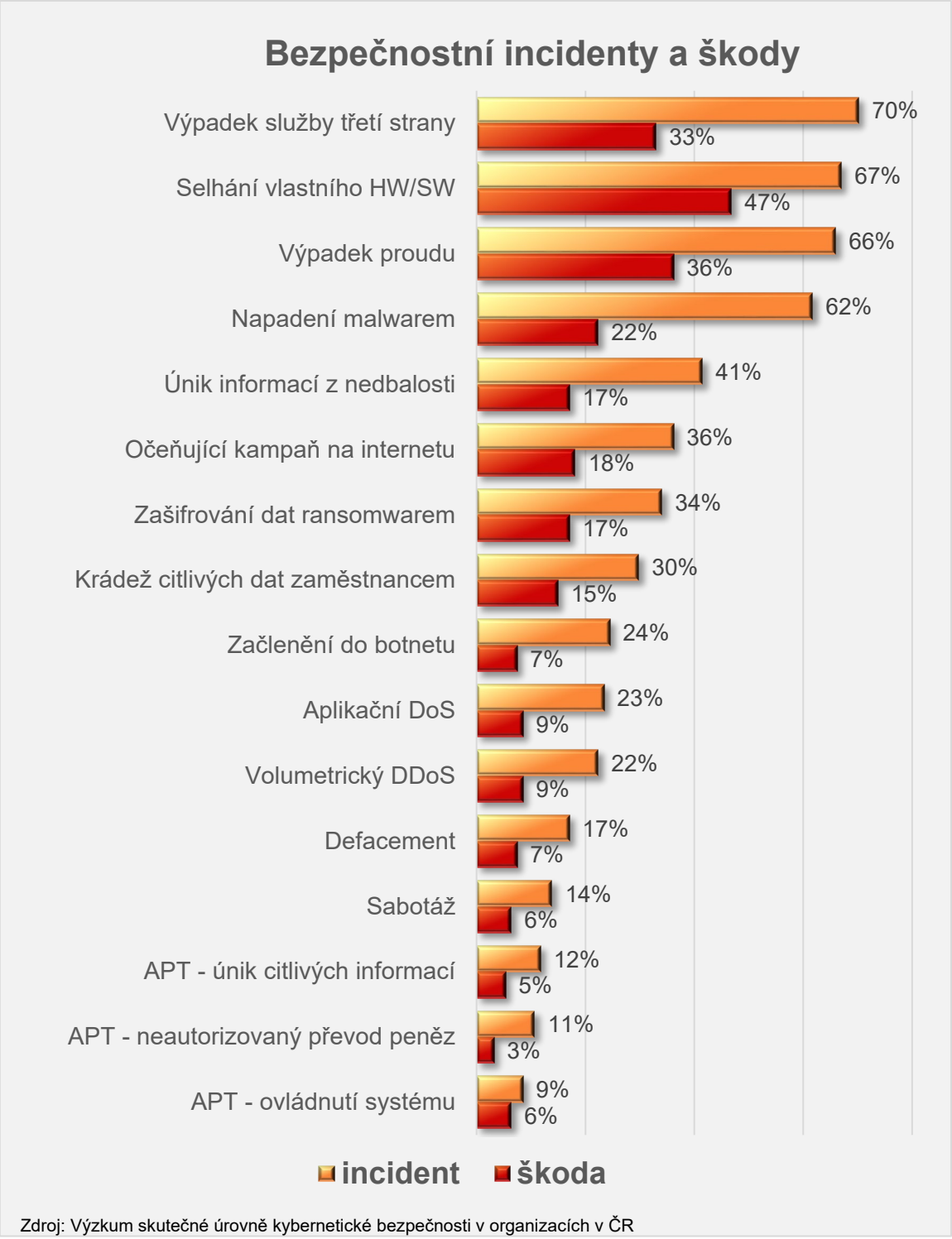
Graf 25 – Škody



Zdroj: Výzkum skutečné úrovně kybernetické bezpečnosti v organizacích v ČR

Když oba pohledy spojíme do jednoho, uvidíme, že až na výjimky se většinu incidentů daří organizacím zvládat bez větších škod, jak zachycuje Graf 26 – Incidenty a škody, což je pozitivní zjištění.

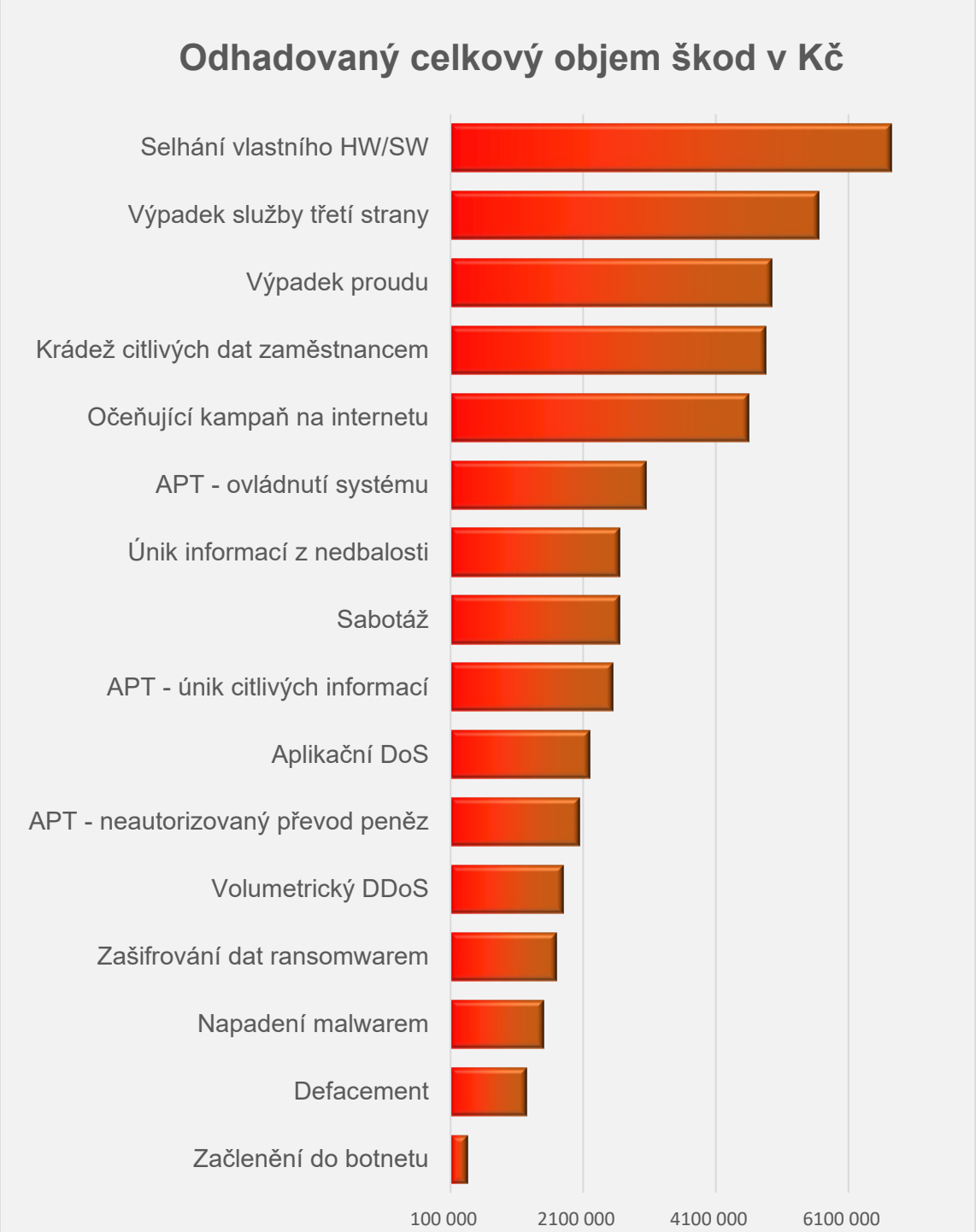
Graf 26 – Incidenty a škody



Zdroj: Výzkum skutečné úrovně kybernetické bezpečnosti v organizacích v ČR

Jiný pohled pak přináší Graf 27 – Incidenty způsobující největší škody, který zachycuje, které incidenty způsobily v součtu organizacím největší škody.

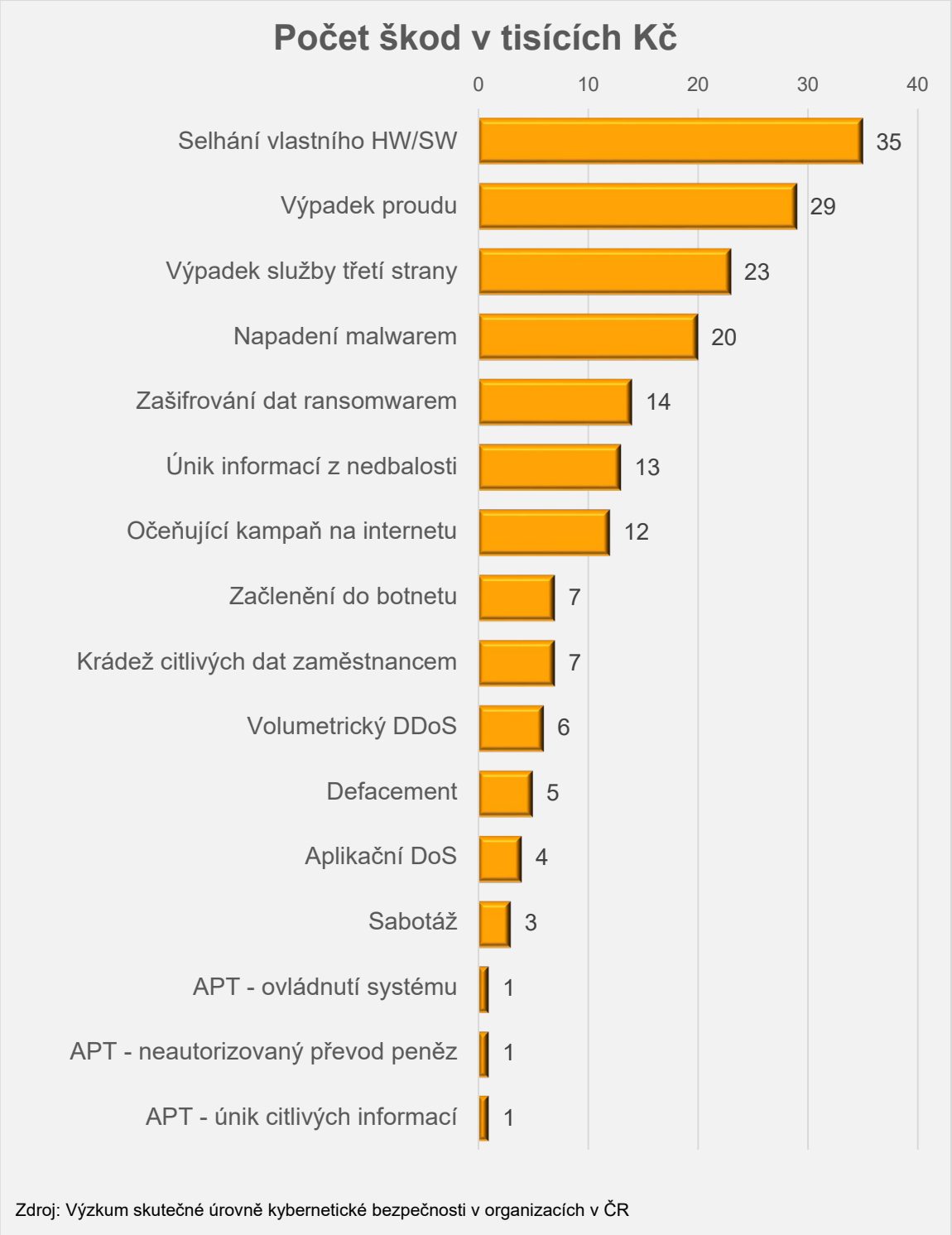
Graf 27 – Incidenty způsobující největší škody



Zdroj: Výzkum skutečné úrovně kybernetické bezpečnosti v organizacích v ČR

Když se však podíváme na to, co způsobilo největší škody, tak se v zásadě rovněž nic nemění, jak zachycuje Graf 28 – Počet škod v tisících.

Graf 28 – Počet škod v tisících



Zdroj: Výzkum skutečné úrovně kybernetické bezpečnosti v organizacích v ČR

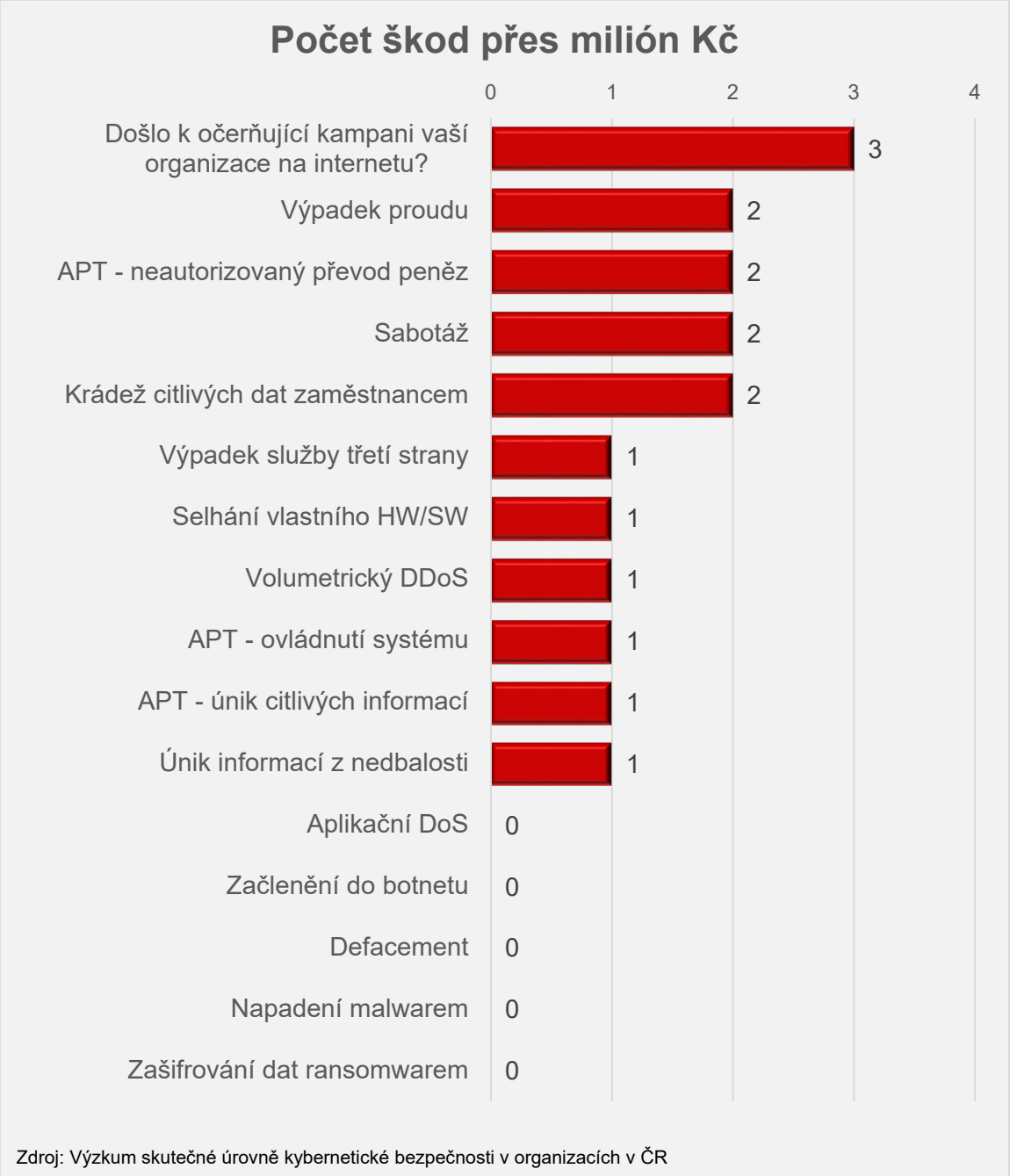
A rovněž i v řádech statisíců, což je už mnohem zajímavější, protože vidíme, že počet organizací reportujíce takovouto ztrátu je výrazně nižší, a že největší ztráty nezpůsobil malware, jak by se dalo očekávat, nýbrž prosté selhání vlastního HW/SW, výpadek služeb třetí strany (můžeme spekulovat, co ho způsobilo) a krádež dat ze strany zaměstnance, jak zachycuje Graf 29 – Počet škod ve statisících.

Graf 29 – Počet škod ve statisících

Zdroj: Výzkum skutečné úrovně kybernetické bezpečnosti v organizacích v ČR

U škod převyšujících milión korun vidíme ještě menší počet organizací, které utrpěly škodu, a především se nám opět trochu změnilo pořadí. Na první místo se dostala očerňující kampaň na internetu následovaná výpadkem proudu, krádeží dat ze strany vlastního zaměstnance, sabotáží a neautorizovaným převodem peněz, jak zachycuje Graf 30 – Počet škod přes milión.

Graf 30 – Počet škod přes milión

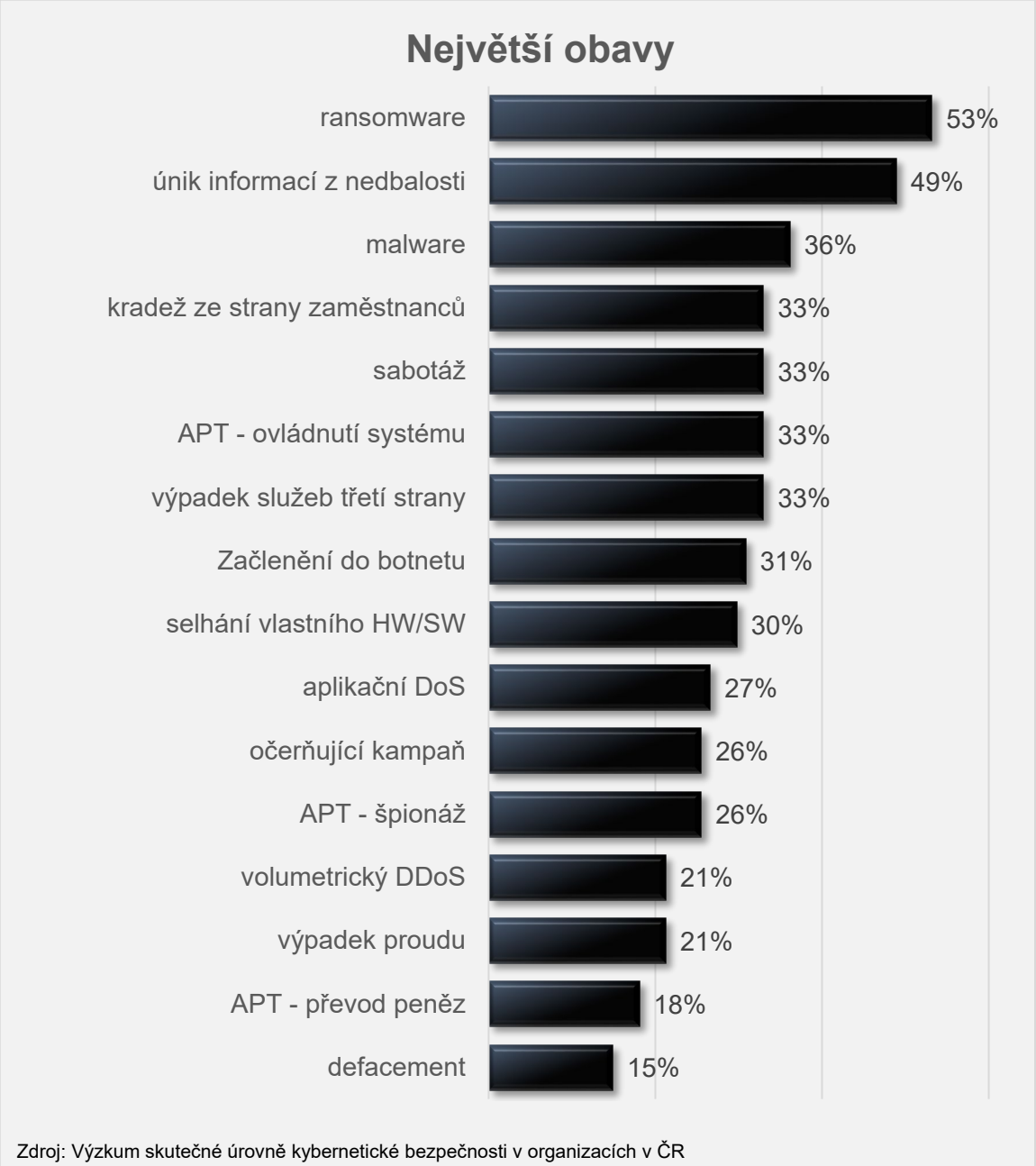


Zdroj: Výzkum skutečné úrovně kybernetické bezpečnosti v organizacích v ČR

Obavy

Navzdory počtu incidentů a škodám, které organizace evidují, se jejich obavy týkají ransomware, úniku informací z nedbalosti a malware, jak zachycuje Graf 31 – Největší obavy. Jejich obavy však v zásadě kopírují trend vyplývající ze zpráv z médií, které formují jejich pohled na situaci v kyberprostoru.

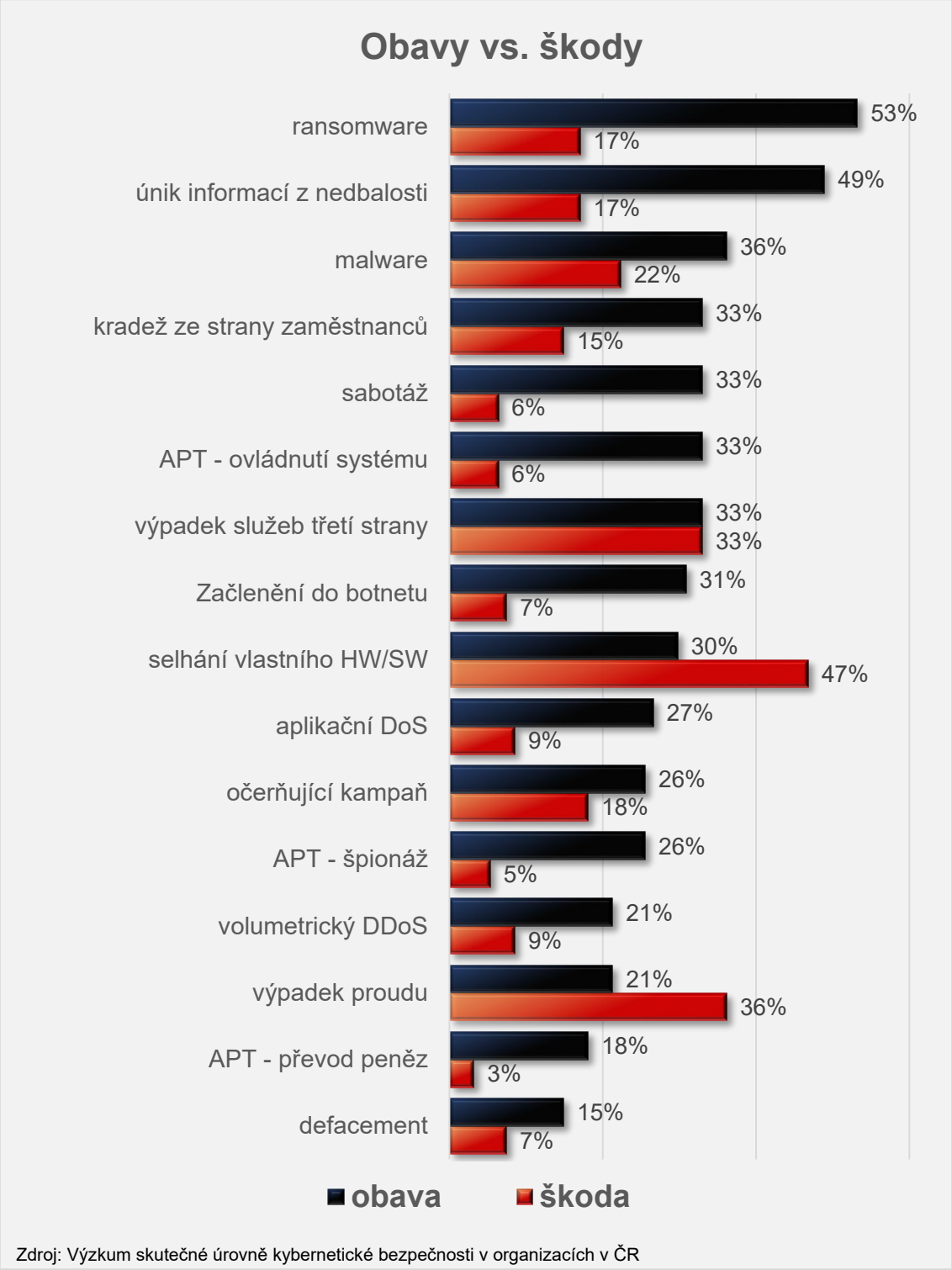
Graf 31 – Největší obavy



Zdroj: Výzkum skutečné úrovně kybernetické bezpečnosti v organizacích v ČR

Organizace by se však měly obávat trochu jiných hrozeb. Těch, které jim reálně hrozí a kde jim může vzniknout i mnohem vyšší škoda. Rozpor mezi obavou a škodou zachycuje Graf 32 – Obavy vs. škody.

Graf 32 – Obavy vs. škody



Zdroj: Výzkum skutečné úrovně kybernetické bezpečnosti v organizacích v ČR

Opatření

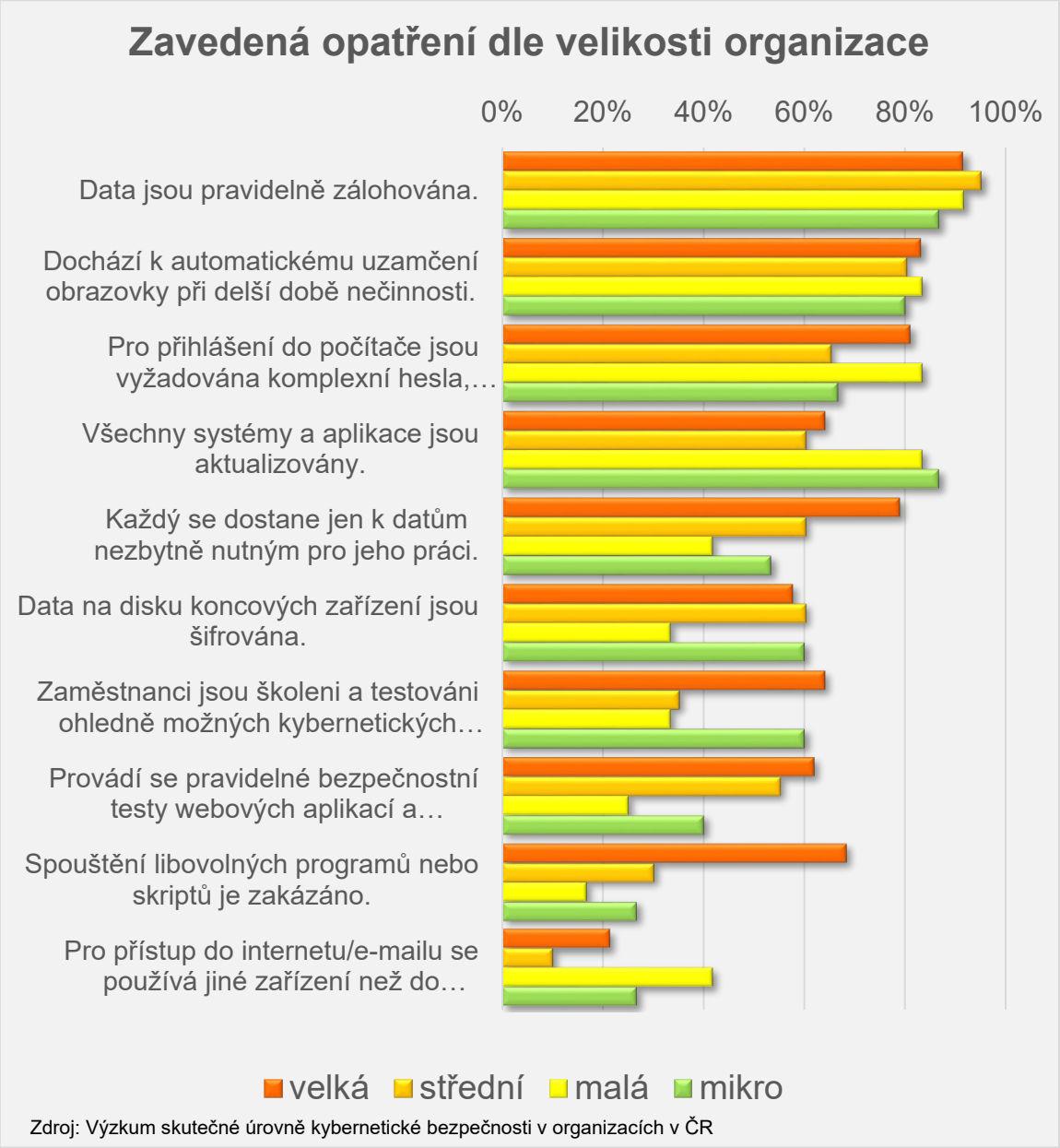
Pokud jde o jednotlivá opatření, tak lze jako pozitivní hodnotit, že se organizace naučily zálohovat svá data, nastavily automatické uzamykání obrazovky a zavedly silnou autentizaci. Horší to však je, co se týká udržování všech systémů aktuálních, řízení striktního přístupu na principu need-to-know a šifrování dat, což provádí jen pouhá polovina organizací, stejně jako školení a testování zaměstnanců, aplikací a infrastruktury, jak zachycuje Graf 33 – Bezpečnostní opatření.

Graf 33 – Bezpečnostní opatření

Zdroj: Výzkum skutečné úrovně kybernetické bezpečnosti v organizacích v ČR

Když se podíváme na zavedení opatření z pohledu velikosti organizace, tak zde již jsou patrné výraznější rozdíly např. u aktualizací, které je podstatně náročnější udržet u větších organizací, jak zachycuje Graf 34 – Bezpečnostní opatření dle velikosti organizace. Mikro mají automaticky aktualizovaný OS MS Windows, antivirus i prohlížeč, a další programy nepoužívají anebo je mají v cloudu, ale neřídí tak striktně přístup k datům. Pokud jde o školení a trénink zaměstnanců, tak ten nejvíce podceňují malé a střední organizace.

Graf 34 – Bezpečnostní opatření dle velikosti organizace



Zdroj: Výzkum skutečné úrovně kybernetické bezpečnosti v organizacích v ČR

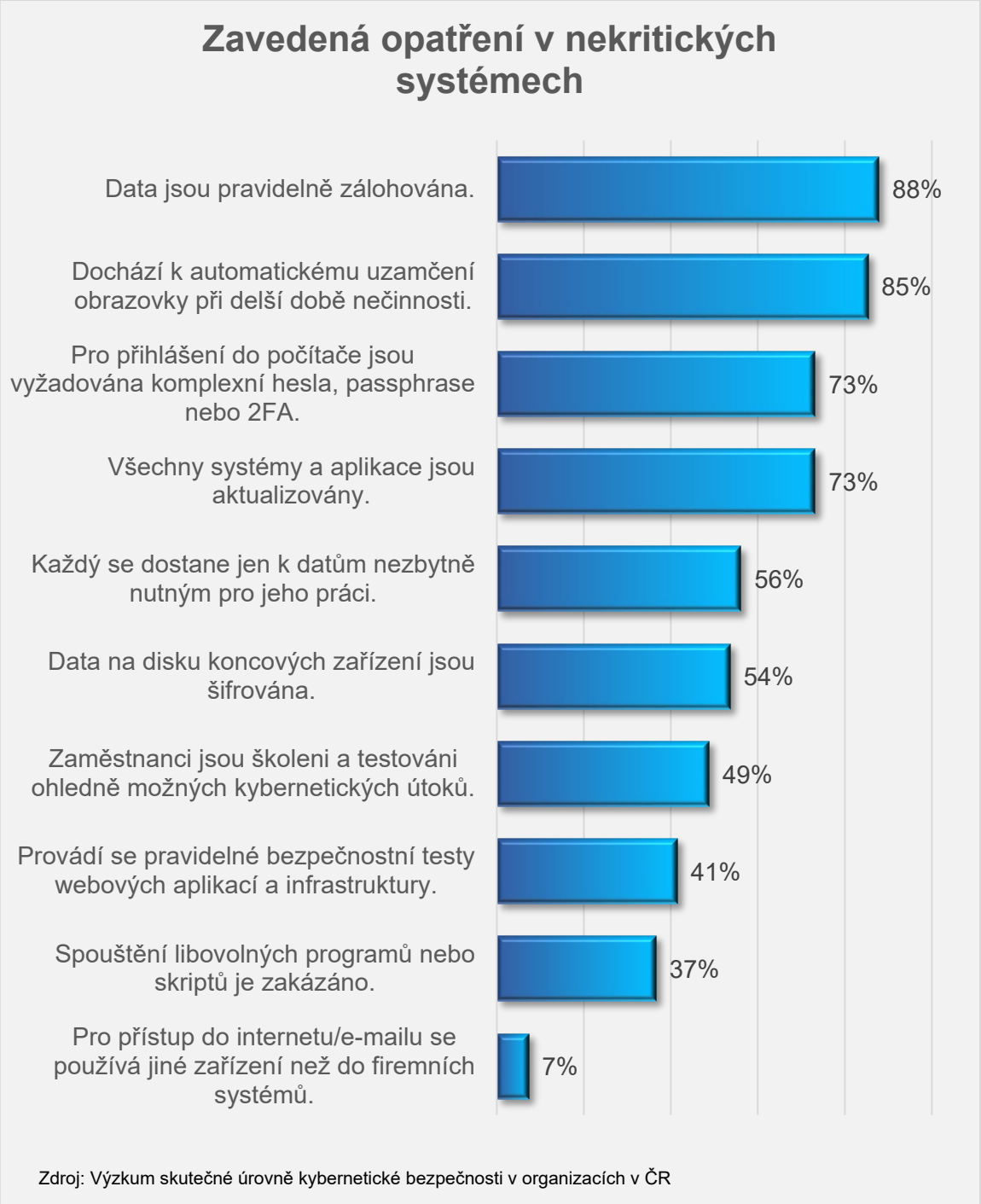
Další zajímavý pohled pak přináší Graf 35 – Zavedení opatření v kritických systémech, který zachycuje srovnání mezi organizacemi, které spadají pod působnost Zákona o kybernetické bezpečnosti, zkr. ZoKB, tedy provozují kritické informační systémy, významné informační systémy a systémy základních služeb a organizace, které tyto systémy neprovozují, zkr. non ZoKB.

Graf 35 – Zavedení opatření v kritických systémech

Zdroj: Výzkum skutečné úrovně kybernetické bezpečnosti v organizacích v ČR

Graf 36 – Bezpečnostní opatření v nekritických systémech ukazuje, že opatření jsou jak v kritických, tak i nekritických systémech zaváděna téměř stejně.

Graf 36 – Bezpečnostní opatření v nekritických systémech



Zdroj: Výzkum skutečné úrovně kybernetické bezpečnosti v organizacích v ČR

Zde by se dalo očekávat, že prvně jmenované organizace na tom budou co do zavedení jednotlivých opatření výrazně lépe. A skutečně tomu tak je. Ve většině případů však rozdíl není značný, liší se jen o pár jednotek procent, ale u spouštění skriptů a oddělení systémů je rozdíl až v desítkách procent. V čem by se však měla naopak první skupina polepšit, je aktualizace systémů, protože zde jsou na tom non ZoKB organizace o něco lépe, jak zachycuje Graf 37 – Bezpečnostní opatření dle kritičnosti systému.

Graf 37 – Bezpečnostní opatření dle kritičnosti systému

Zdroj: Výzkum skutečné úrovně kybernetické bezpečnosti v organizacích v ČR

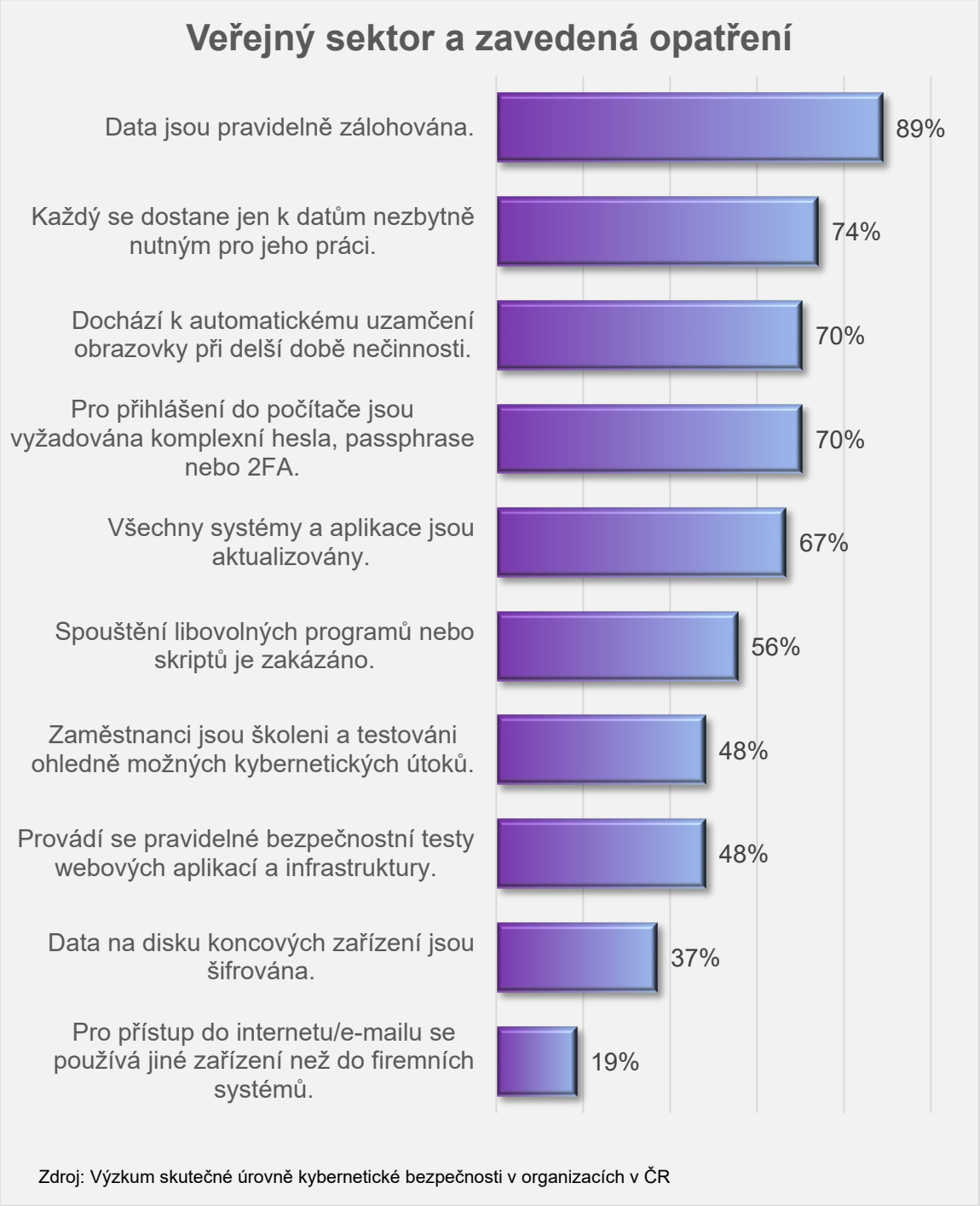
Další pohled na zavedená bezpečnostní opatření je pak možný z pohledu sektoru, ve kterém organizace působí. Ani zde se nám pořadí téměř nezměnilo, jak zachycuje Graf 38 – Bezpečnostní opatření a soukromý sektor.

Graf 38 – Bezpečnostní opatření a soukromý sektor

Zdroj: Výzkum skutečné úrovně kybernetické bezpečnosti v organizacích v ČR

A podobně je tomu i ve veřejném sektoru, kde se na druhé místo vyhouplo striktní řízení přístupu k datům, jak zachycuje Graf 39 – Bezpečnostní opatření a veřejný sektor.

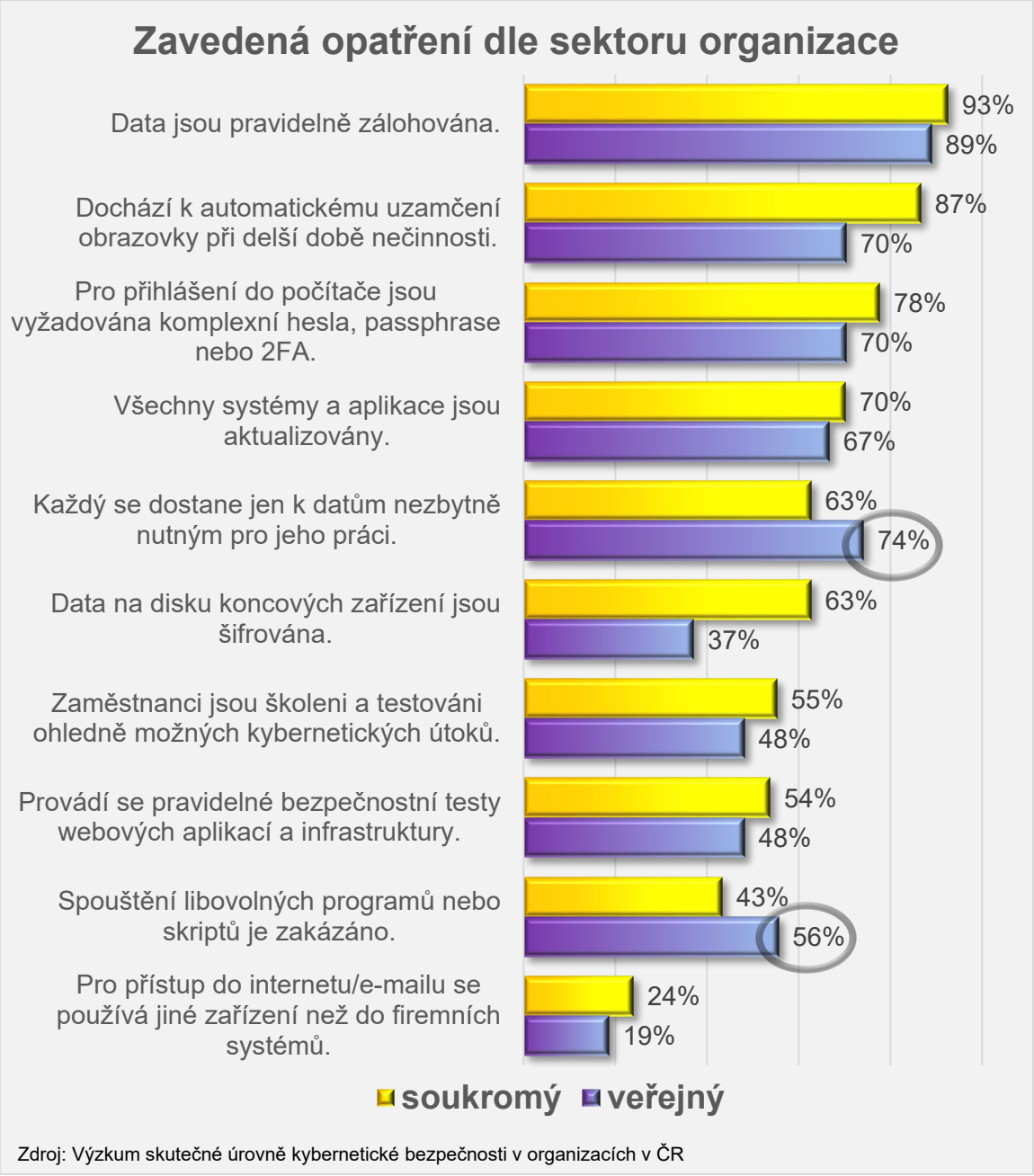
Graf 39 – Bezpečnostní opatření a veřejný sektor



Zdroj: Výzkum skutečné úrovně kybernetické bezpečnosti v organizacích v ČR

Když se podíváme, jaký vliv má sektor, ve kterém organizace působí, na zavedení bezpečnostních opatření, tak zjistíme, že téměř ve všech případech je na tom soukromý sektor co do zavedení bezpečnostních opatření o něco málo lépe, jak zachycuje Graf 40 – Bezpečnostní opatření dle sektoru. Jediné, v čem je veřejný sektor lepší, je striktní řízení přístupu a nemožnost spouštění SW staženého z internetu nebo doneseného na USB flash disku. Zůstává otázka, proč tomu tak je.

Graf 40 – Bezpečnostní opatření dle sektoru



Zdroj: Výzkum skutečné úrovně kybernetické bezpečnosti v organizacích v ČR

Dále se nabízí otázka, zda má nějaký vliv na zavedení bezpečnostních opatření nejen sektor, ve které organizace působí, ale i kritičnost daného systému, což zachycuje Graf 41 – Bezpečnostní opatření a kritické systémy. Z něj je patrné, že ve většině případů je soukromý vlastník lepší hospodář, nicméně jsou zde oblasti, kde se zodpovědněji chová stát, např. v oblasti řízení přístupu k datům, školením zaměstnanců a blokováním neschválených programů.

Graf 41 – Bezpečnostní opatření a kritické systémy

Zdroj: Výzkum skutečné úrovně kybernetické bezpečnosti v organizacích v ČR

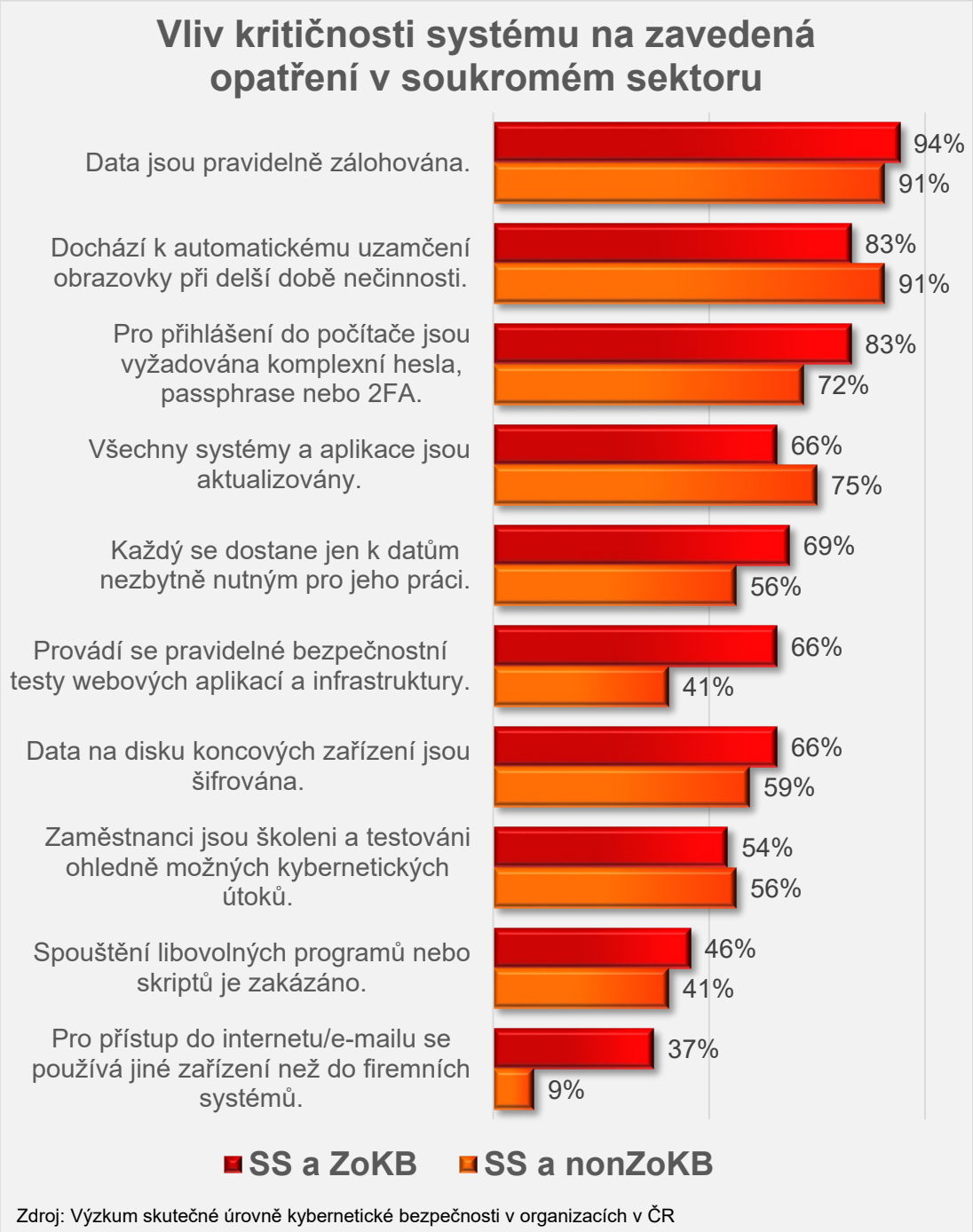
Pro úplnost pak uveďme, jak jsou na tom organizace v soukromém a veřejném sektoru provozující systém, který nespadá pod působnost ZoKB, jak zachycuje Graf 42 – Bezpečnostní opatření a nekritické systémy. Opět vidíme, že tam, kde je provozovatelem systému soukromý vlastník, tak jsou bezpečnostní opatření zavedena ve větší míře.

Graf 42 – Bezpečnostní opatření a nekritické systémy

Zdroj: Výzkum skutečné úrovně kybernetické bezpečnosti v organizacích v ČR

To vyvolává i otázku, zda se soukromý sektor chová jinak v případě kritických systémů a jinak v případě nekritických systémů. Graf 43 – Bezpečnostní opatření v soukromém sektoru ukazuje, že u ZoKB systémů více organizací zavedlo uvedená bezpečnostní opatření.

Graf 43 – Bezpečnostní opatření v soukromém sektoru



Zdroj: Výzkum skutečné úrovně kybernetické bezpečnosti v organizacích v ČR

Ve veřejném sektoru je tento rozdíl ještě patrnější, jak zachycuje Graf 44 – Bezpečnostní opatření ve veřejném sektoru a dal by se tak vyslovit závěr, kritické systémy bývají častěji lépe zabezpečeny, což koneckonců není překvapující, protože by tomu tak mělo být.

Graf 44 – Bezpečnostní opatření ve veřejném sektoru

Zdroj: Výzkum skutečné úrovně kybernetické bezpečnosti v organizacích v ČR

Riziko ohrožení

S ohledem na zavedená bezpečnostní opatření si lze představit řadu hrozeb, vůči kterým organizace nebudou dostatečně chráněny. Mezi jednotlivými organizacemi jsou samozřejmě určité rozdíly, nicméně většina organizací není zdaleka imunní vůči APT, což se dalo očekávat, ale více jak polovina z nich nepřijala ani dostatečná opatření vůči hackingu a dalším běžným vektorům útoku, jak zachycuje Graf 45 – Zranitelnost vůči hrozbám.

Graf 45 – Zranitelnost vůči hrozbám

Zdroj: Výzkum skutečné úrovně kybernetické bezpečnosti v organizacích v ČR