UNIVERZITA KARLOVA

Právnická fakulta

Peter Gemeri

Kriminologické aspekty kybernetické kriminality

Diplomová práce

Vedoucí diplomové práce: doc. JUDr. Bc. Tomáš Gřivna, Ph.D.

Katedra: Katedra trestního práva

Datum vypracování práce (uzavření rukopisu): [dd. mm. rrrr]

Prohlášení

Prohlašuji, že jsem předkládanou diplomovou práci vypracoval samostatně, že všechny použité zdroje byly řádně uvedeny a že práce nebyla využita k získání jiného nebo stejného titulu.

Dále prohlašuji, že vlastní text této práce včetně poznámek pod čarou má 178 504 znaků včetně mezer.

.....

Peter Gemeri

V Praze dne: 25. srpna 2021

Poděkování

Za vedení, podnětné připomínky a rady k sepsání této práce děkuji doc. JUDr. Bc. Tomáši Gřivnovi, Ph.D. Zároveň chci poděkovat hlavním respondentům Janu Beránkovi a Radkovi Živnému za jejich vřelé poskytnutí součinnosti k praktické části práce.

.....
Peter Gemeri

V Praze dne: 25. srpna 2021

Obsah

Úvod

Kybernetická kriminalita je jevem, který díky stále vyšší míře digitalizace v soukromém i veřejném sektoru nabývá na rozsahu. Tato diplomová práce se věnuje kriminologickým aspektům kyberkriminality se zaměřením na sekundární prevenci kybernetické kriminality páchané na poskytovatelích finančních služeb v České republice. Důvodem k relativně specifickému zaměření práce jsou rozporuplné názory zainteresovaných osob na ideální a reálný stav kybernetické prevence v organizacích, které jsem nabyl za dobu svého profesního působení v oblasti kybernetické bezpečnosti

V současné době existuje velké množství metodik pro zabezpečení informačních systémů vůči kybernetickým útokům. I přesto, že tyto dokumenty na první pohled přestavují kompletní a konečná kritéria pro kybernetickou bezpečnost organizace, v praxi mnohdy dochází k situacím, kdy důsledná implementace standardizovaných preventivních opatření nebyla v souladu s očekáváním a potřebami organizace (ať už z časového, finančního či funkčního hlediska). Cílem organizací ve finančním sektoru je primárně generování zisku, a je proto pochopitelné, že i adekvátní míra kybernetické bezpečnosti je pro ně pouze nástrojem pro mitigaci rizika finanční ztráty. Zatímco přehnaně restriktivní politika kybernetické bezpečnosti má v organizaci negativní dopad na efektivitu práce s informačními systémy, pak vysoká benevolence či absence preventivních opatření zvyšuje riziko úspěšnosti kybernetického útoku a s tím spojených peněžních dopadů. Je tak v zájmu organizace najít při řešení výše zmíněné disonance kompromis mezi zajištěním důvěrnosti, integrity a dostupnosti svých informačních systémů, s důrazem na faktory specifické pro povahu organizace (typ podnikatelské činnosti, její zaměstnanci, firemní kultura, technologické zázemí a další).

Cílem práce je najít odpovědi na následující otázky:

- Jaké jsou specifické kriminologické aspekty kybernetické kriminality České republice?
- Které druhy kybernetické kriminality jsou nejrizikovější pro poskytovatele finančních služeb?
- Jaká preventivní opatření tyto organizace zavádějí a jak efektivní či náročná je implementace?

Úvodní (teoretická) část práce se věnuje definici a rozebrání klíčových pojmů týkajících se oblasti kybernetické kriminality a kybernetické bezpečnosti tak, aby bylo poskytnuto dostatečné

informační východisko k praktické části práce. Podrobněji jsou zde rozebrána témata pojmů, druhů, historie, pachatelů, obětí a způsobu provedení kybernetické kriminality. Výzkumnou metodou pro teoretickou část je komparace a analýza vybraných tuzemských a cizojazyčných zdrojů.

Druhá část práce obsahuje popis zvolené metodologie pro praktickou část a myšlenková východiska pro výběr zkoumané problematiky. Výzkumnými metodami jsou analýza dokumentů a statistických zdrojů a polostrukturovaný rozhovor se dvěma odborníky v oblasti kybernetické bezpečnosti.

Závěrečná část práce pojednává o prevenčních mechanismech využívaných v boji s kybernetickou kriminalitou a z převážné části vyplývá z osobních zkušeností a praktických poznatků autora a respondentů v oboru zabezpečení informačních systémů proti kybernetickým útokům v prostředí bankovních a nebankovních poskytovatelů finančních služeb. Cílem kapitoly je představení procesních, technických a edukačních prevenčních mechanismů s důrazem na jejich silné a slabé stránky při reálném nasazení v praxi. Zabývá se konkrétními preventivními opatřeními, jejich mírou úspěšnosti v boji s kybernetickými hrozbami v praxi a vzájemnou hierarchii v politice kybernetické bezpečnosti. Výstupem této části práce je soubor doporučení pro potenciální oběti kybernetické kriminality.

1. Kybernetická kriminalita (teoretická část)

Pro další analýzu nejnebezpečnějších oblastí kybernetické kriminality z pohledu právnických osob je nutné nejprve popsat faktický rozsah tohoto pojmu. Tato kapitola se zabývá výkladem pojmu kybernetická kriminalita a dále definicí jeho znaků. Obsahuje klasifikační systémy kybernetické kriminality, přehled jejího historického vývoje a typologii pachatelů. Cílem této sekce je poskytnout čtenáři ucelený přehled o rozmanitosti takto páchaných trestných činů a poskytnutí teoretické báze pro další analýzu.

1.1 Pojem

Kybernetická kriminalita je oblastí dynamicky se rozvíjející, proto ani její definice není jednoznačná. Tuzemské zdroje uvádějí, že meziroční nárůst v počtu oznámených skutků se pohybuje okolo 20 %[1,2]. V literatuře existuje nespočet úhlů pohledu, ze kterých na danou problematiku autoři nahlíží. Pokud kriminalitou rozumíme jednání posuzované jako trestný čin (trestnou činnost)[3], pak za základní vymezení pojmu lze považovat například níže uvedenou definici z Výkladového slovníku kybernetické bezpečnosti:

> *„Trestná činnost, v níž figuruje určitým způsobem počítač jako souhrn technického a programového vybavení (včetně dat), nebo pouze některá z jeho komponent, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď jako předmět zájmu této trestné činnosti (s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako věci movité) nebo jako prostředí (objekt) nebo jako nástroj trestné činnosti (více také Počítačová kriminalita).“*[4]

Existují ovšem autoři, kteří tuto definici považují za nekompletní. Například Kolouch[5] jí označuje za problematickou z důvodu záměny pojmů počítačová kriminalita a kybernetická

1 *MINISTERSTVO VNITRA ČR. 2019 Zpráva o situaci v oblasti vnitřní bezpečnosti a veřejného pořádku na území České republiky v roce 2018. [Online] květen 2019. [Citace: 14. březen 2021.] https://www.mvcr.cz/soubor/zprava-o-situaci-v-oblasti-vnitrni-bezpecnosti-a-verejneho-poradku-na-uzemi-cr-v-roce-2018.aspx.*
(meziroční nárust 17%)

2 *MINISTERSTVO VNITRA ČR. 2020. Zpráva o situaci v oblasti vnitřní bezpečnosti a veřejného pořádku na území České republiky v roce 2018. [Online] 2020. [Citace: 14. březen 2021.] https://www.mvcr.cz/soubor/zprava-o-vbavp-2019-verze-2-5-prijate-rev-vvb-1.aspx.* (meziroční nárust 23%)

3 *SVATOŠ, R. Kriminologie. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2012. Vysokoškolské učebnice (Vydavatelství a nakladatelství Aleš Čeněk). ISBN 9788073803896.*

4 *JIRÁSEK, P.; NOVÁK L.; POŽÁR J. Výkladový slovník kybernetické bezpečnosti: Cyber security glossary. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6.*

5 *KOLOUCH, J. Cybercrime. Praha : CZ.NIC, z.s.p.o., 2019. ISBN 9788088168188. str.32*

kriminalita a dále pak pro její nekompletnost. Počítačová kriminalita v sobě implikuje pouze vazbu na počítače, nicméně dnešní okruh zařízení, kterými lze páchat trestnou činnost je mnohem širší, ať už se jedná o tablety, mobilní telefony, zařízení IoT[6] atd., a navrhuje proto následující pozitivní vymezení:

> *1) „Trestné činy, jejichž individuálním objektem charakterizujícím skutkovou podstatu je přímo ochrana počítačového systému, jeho vybavení a součástí před specifickými druhy útoků, resp. oprávněné zájmy osob na nerušené užívání těchto technických prostředků.*
>
> *2) Trestné činy, kde je způsob spáchání prostřednictvím informační a komunikační techniky jedním ze znaků skutkové podstaty.*
>
> *3) Ostatní v úvahu připadající trestné činy, které nespadají do první ani druhé kategorie, avšak které mohou být v konkrétním případě též spáchány prostřednictvím informačních technologií a které odpovídají výše uvedené definici, neboť v rámci jejich odhalování a objasňování se mohou uplatnit obdobné postupy jako při vyšetřování trestných činů z 1. a 2. kategorie (např. obdobně zaměřené znalecké posudky).“*[7]

Dalším z kriminologického hlediska relevantním zdrojem je nepochybně definice kyberkriminality orgány činnými v trestním řízení. Policie ČR definuje pro své potřeby kybernetickou kriminalitu a kyberprostor takto:

> *„Pojem kybernetická kriminalita je odvozován od pojmu kybernetický prostor, případně zkráceně kyberprostor. Kyberprostor je virtuální prostředí, které nemá začátek a ani konec, nezná hranice národních států a nelze určit, jak rozsáhlý je. Kybernetická kriminalita, dříve také označována jako informační kriminalita, je definována Policii ČR jako trestná činnost, která je páchána v prostředí informačních a komunikačních technologií včetně počítačových sítí. Samotná oblast informačních a komunikačních technologií je buď předmětem útoku, nebo je páchána trestná činnost za výrazného využití informačních a komunikačních technologií jakožto významného prostředku k jejímu páchání.“*[8]

[6] IoT = Internet of Things

[7] *KOLOUCH, cit. 5., str. 37*

[8] *POLICIE ČR. 2019. Zveřejněné informace. Kyberkriminalita. [Online] 2019. [Citace: 12. únor 2020.] https://www.policie.cz/clanek/kyberkriminalita.aspx.*

Ve výše uvedených definicích lze najít několik společných definujících znaků a to sice, že se jedná se o trestnou činnost - kybernetický útok[9] jejíž objektem, předmětem útoku, nebo klíčovým nástrojem jsou informační a komunikační technologie, s výjimkou trestné činnosti, jíž se týkají informační a komunikační technologie pouze okrajově např. jako movitá věc.

Vzhledem k zaměření této práce na prostředí právnických osob, považuji za důležité zmínit navíc pojmy kybernetická bezpečnostní událost a kybernetický bezpečnostní incident, které s kybernetickou kriminalitou úzce souvisí. Definici pojmů nalezneme v § 7 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů (dále jen ZKB nebo zákon o kybernetické bezpečnosti).

> §7(1) – *„Kybernetickou bezpečnostní událostí je událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací.“*

> §7(2) – *„Kybernetickým bezpečnostním incidentem je narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události.“*

1.2 Rozdělení

Pro bližší porozumění lze kyberkriminalitu definovat kategoriemi trestné činnosti, které do ní spadají. Literatura pro tyto účely zmiňuje celou řadu klasifikačních kritérií, jimž se blíže věnují následující podkapitoly.

1.2.1 Klasifikace podle předmětu útoku

Jedním z klasifikačních modelů je dělení dle předmětu útoku. Rozlišujeme mezi trestnou činností, jež má jako předmět útoku osobu nebo skupinu osob, věci nebo celé organizace.[10]

Osoba nebo skupina osob

Pokud je předmětem útoku osoba, nebo skupina osob, tak informační a komunikační technologie vystupují zpravidla v roli nástroje. Tento druh kybernetické kriminality hojně využívá negativních charakterových vlastností oběti jako jsou naivita, ziskuchtivost nebo strach. Jedná se jak o finanční a autorskoprávní trestnou činnost, tak i o trestné činy proti lidské důstojnosti

---

[9] *Kybernetický útok - Jakékoli protiprávní jednání útočníka v kyberprostoru, které směřuje proti zájmům jiné osoby, zdroj, KOLOUCH, cit. 4, str. 55*

[10] *MILLHORN, Thomas H. 2007. Cybercrime: How to Avoid Becoming a Victim. Boca Raton, FL : Universal-Publishers, 2007. ISBN 9781581129540.*

v sexuální oblasti, nebo i o trestné činy proti právům na ochranu osobnosti, soukromí a listovního tajemství.

Majetek

Útoky na majetek mají za předmět informační a komunikační techniku. Často mají subsidiární charakter. Může se jednat o činnost, kterou lze posoudit jako přípravu trestného činu. Cílem může být např. vytvoření zadních vrátek pro vzdálené ovládání, instalaci viru nebo exfiltraci informací. Spadají sem např. trestné činy podle § 207 Neoprávněné užívání cizí věci, § 230 Neoprávněný přístup k počítačovému systému a nosiči informací, § 231 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat zákona č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů (dále jen TZ nebo trestní zákoník).

Organizace

Útok na organizace je typický svým rozsahem a profesionalitou pachatelů, útočníci napadají celé sítě a informační systémy. Organizacemi v tomto případě rozumíme jak soukromoprávní, tak veřejnoprávní korporace. Cílem pachatelů je zejména majetkový zisk, útisk obyvatelstva státu, napadení vojenské technické infrastruktury, špionáž a šíření dezinformací. Speciálním druhem těchto aktivit je kyberterorismus. [11, 12]

1.2.2 Klasifikace podle typu jednání

Toto hledisko pro kategorizaci kyberkriminality zvolil ve své knize Crime and the Internet David Wall a často se používá i v dalších cizojazyčných zdrojích. Pro klasifikaci používá pojmy cyber-trespass, cyber-deception and theft, cyber-porn and obscenity a cyber-violence.[13]

Cyber-trespass

Cyber-trespass (kybervniknutí) je neoprávněné překonání opatření a hranic, které jsou určeny pro ochranu vlastnického práva k počítačovým systémům a sítím. Tato kategorie zahrnuje především hacking a v českém právním řádu do ní spadá hlavně čin neoprávněného přístupu k počítačovému systému a nosiči informací.

---

[11] *MILHORN, cit. 9, str.2*

[12] *DENNING, Dorothy E. 2001. Activism, Hacktivism, and Cyberterrorism. The Internet as a Tool for Influencing Foreign Policy. [Online] 8. červen 2001. [Citace: 20. leden 2020.] http://faculty.nps.edu/dedennin/publications/ Activism-Hacktivism-Cyberterrorism.pdf. str. 24-25*

[13] *WALL, D. Crime and the Internet. Londýn : Routledge, 2001. ISBN: 9780415244282. str. 4-8*

Cyber-deception and theft

Cyber-deception and theft (kyberpodvod a krádež) jsou různé druhy trestné činnosti v digitálním prostředí vedoucí k osobnímu prospěchu pachatele.[14] Zahrnuje činnost spočívající v porušování majetkových a autorských práv a získávání důvěrných informací, typicky jde o trestný čin podvodu, pojistného podvodu, úvěrového podvodu a krádeže.

Cyber-porn and obscenity

Cyber-porn and obscenity (kyberpornografie a obscénnosti) je zveřejňování nebo obchod se zbožím se sexuální tématikou.[15] Pornografie je v České republice legální, pokud nenaplňuje znaky uvedené ve skutkových podstatách trestných činů proti lidské důstojnosti v sexuální oblasti. Z tohoto důvodu je okruh trestné činnosti ve světle české právní úpravy užší než v mezinárodním pojetí. Spadají sem trestné činy uvedené v hlavě III trestního zákoníku, jmenovitě například § 186 (sexuální nátlak), § 189 (kuplířství), § 191 (šíření pornografie), § 192 (výroba a jiné nakládání s dětskou pornografií), § 193 (zneužití dítěte k výrobě pornografie), § 193a (účast na pornografickém představení), § 193b (navazování nedovolených kontaktů s dítětem).

Cyber-violence

Cyber-violence (kybernásilí) je škodlivým následkem způsobeným násilnými aktivitami v kyberprostoru.[16] Jedná se o krátkodobé i dlouhodobé násilí s psychologickými dopady na oběť, a to i přes absenci fyzických projevů. Spadají sem zejména trestné činy proti svobodě a trestné činy narušující soužití lidí, např. § 171 (omezování osobní svobody), § 175 (vydírání), § 176 (omezování svobody vyznání), § 177 (útisk), § 353 (nebezpečné vyhrožování), § 354 (nebezpečné pronásledování), § 355 (hanobení národa, rasy, etnické nebo jiné skupiny osob), § 356 (podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod) a § 357 (šíření poplašné zprávy) trestního zákoníku.

1.2.3 Klasifikace podle použití násilí

Dalším kritériem je použití násilí v průběhu trestné činnosti. Kybernetickou kriminalitu dělíme na činy násilné, potenciálně násilné a nenásilné.

---

[14] *GRAHAM Roderick S., SMITH Shawn K. Cybercrime and Digital Deviance. Londýn : Routledge, 2019. ISBN: 9781351238076. kap. 5*
[15] *GRAHAM, cit. 14, kap. 3*
[16] *GRAHAM, cit. 14, kap. 4*

Násilná kyberkriminalita

Do násilné kyberkriminality řadíme typicky kyberterorismus a trestnou činnost spojenou s dětskou pornografií. Jedná se o kriminalitu, která má násilí jako nezbytný znak, bez kterého by jí nešlo konat.

Potenciálně násilná kyberkriminalita

Potenciálně násilná kyberkriminalita označuje trestnou činnost, která může být provedena násilně, nicméně není to k jejímu provedení nutné. Jedná se o kybernetické formy stalkingu nebo vyhrožování.

Nenásilná kyberkriminalita

Nenásilná kyberkriminalita představuje převážnou část veškeré kybernetické kriminality. Toto vyplývá především ze skutečnosti, že kyberprostor je stále velice anonymní oblast, s omezenou možností fyzického kontaktu. Tyto charakteristiky jsou pro pachatele trestných činů zajímavé jak z hlediska jednoduchosti přípravy a samotného páchání trestné činnosti, tak i pro možnost vyhýbání se trestnímu řízení.[17]

1.2.4 Klasifikace Policie ČR

Potenciálním průnikem již zmíněných klasifikací je rozdělení kyberkriminality pro účely statistiky Policie ČR. Klasifikačními hledisky jsou způsob provedení, objekt trestného činu a předmět útoku. Výsledkem je rozdělení do kategorií, které buď zahrnují celou skupinu trestných činů, nebo jde o konkrétní druh jednání, jehož následkem je trestná činnost. Níže jsou uvedeny druhy trestné činnosti podle této klasifikace:

Podvodná jednání

Jedná se o nejčastěji páchaný druh kybernetické kriminality (cca 60 %). Pro celou kategorii je definičním znakem snaha pachatelů o vylákání finančních prostředků. Policie ČR uvádí jako nejčastější jednání přečin podvod dle ust. § 209 trestního zákoníku, potažmo jeho souběh s neoprávněným přístupem k počítačovému systému a nosiči informací dle ust. § 230 trestního zákoníku. Běžným jevem je také jednání směřující k anonymizaci takto nabytých peněz jejich vyvedením mimo území státu či konverzí na virtuální měny. Jako konkrétní způsoby provedení jsou uvedeny podvodné e-shopy (falešný prodej zboží, zpravidla za cenu nižší než u konkurence;

[17] *SHINDER, Littlejohn D. 2002. Scene of the Cybercrime: Computer Forensics Handbook. Rockland, MA : Syngress Publishing Inc., 2002. ISBN 9781931836654. str. 13-27*

typicky je požadována platba předem a po vyvedení finančních prostředků e-shop beze stopy zaniká), podvodné inzeráty (falešný prodej či pronájem bytů, automobilů, elektroniky, živých zvířat, sbírek), podvržené emaily (např. blagging viz. níže), krádeže peněz prostřednictvím phishingu (viz. níže) a tzv. „nigerijské podvody“, což je specifická forma podvodného e-mailu zasílaná na velké množství neznámých příjemců, ve snaze vylákat z obětí úhradu rezervačního či jiného poplatku výměnou za budoucí transakci velkého finančního obnosu. Historicky byly e-maily formulovány z pozice fiktivního člena Nigerijské aristokracie.[18] Za zmínku stojí distinkce mezi e-maily podvodnými a nevyžádanými. Podvodný e-mail ve značné části případů nemusí mít žádné následky (oběť ho záměrně ignoruje, nebo si ho ani nevšimne), ale jedná se o úkon apriori deliktní. Oproti tomu nevyžádaný e-mail neznamená nutně protiprávní jednání (například obsahuje-li sdělení reklamní povahy, která zpravidla nemají podvodný úmysl a je běžné, že k jejich zasílání uživatel nevědomky udělil souhlas). Koncový uživatel běžně nerozlišuje mezi e-maily podvodnými a nevyžádanými, na což ostatně útočníci spoléhají.

Mravnostní trestné činy

Souhrn v této kategorii nejzastoupenějších trestných činů odpovídá již popsané kategorii cyber-porn and obscenity, který je dále rozšířen o trestný čin obchodování s lidmi dle ust. § 168 trestního zákoníku. Pro kriminalitu páchanou na osobách mladších 18 let je typická snaha pachatele vylákat z oběti intimní fotografie a videa, popřípadě si dohodnout osobní setkání. Kontakt s obětí probíhá formou různých chatů, sociálních sítí nebo online her. Získaný materiál je dále sdílen v komunitách na diskuzních fórech (ty bývají zpravidla nepřístupná veřejnosti), e-mailem, popř. P2P sítěmi.[19]

Trestné činy proti duševnímu vlastnictví

Kategorii vystihuje trestný čin porušení autorského práva, práv souvisejících s právem autorským a práv k databázi dle ustanovení § 270 trestního zákoníku. Majoritní podíl na této skutkové podstatě má sdílení audiovizuálního obsahu a počítačových programů v rámci veřejných internetových uložišť a P2P[20] sítí v rozporu s autorským právem. Podle Zprávy o situaci v oblasti vnitřní bezpečnosti a veřejného pořádku na území ČR v roce 2019[21] je internet hlavním nástrojem pro prodej padělaného či ilegálního zboží. Pro tyto činy je běžný mezinárodní prvek na straně oběti

[18] *POLICIE ČR. Jednotlivé druhy kyberkriminality. Kyberkriminalita. [Online] [Citace: 4. srpen 2020.] https://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx.*
[19] *POLICIE ČR, cit. 18*
[20] *P2P (Peer to peer) - Forma počítačové komunikace, pro kterou je typický simultánní přenos dat mezi všemi účastníky*
[21] *MINISTERSTVO VNITRA ČR, cit. 1*

(zahraniční subjekty bez tuzemského zastoupení), či pachatele (zájmové servery jsou provozované v zahraničí) a pro jejich objasnění je často nutná mezinárodní policejní spolupráce.

Násilné projevy a hate crime

Do této kategorie řadí Policie ČR trestné činy „Vydírání"" dle ust. § 175 trestního zákoníku, „Nebezpečné vyhrožování" dle ust. § 353 trestního zákoníku, „Nebezpečné pronásledování" (stalking) dle ust. § 354 trestního zákoníku, nebo také „Šíření poplašné zprávy" dle ust. § 357 trestního zákoníku. Souhrnným znakem v této kategorii je anonymita pachatele, kterou lze získat využitím webových anonymizérů, proxy serverů, sítě TOR či služeb VPN. Řadíme sem dále extremistické projevy ve formě trestného činu „Hanobení národa, rasy, etnické nebo jiné skupiny osob" dle ust. § 355 trestního zákoníku, „Podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod" dle ust. § 356 trestního zákoníku a další. Stejně jako u mravnostní kyberkriminality operují pachatelé v rámci internetových komunit, které umožňují sdílení radikální levicové a pravicové tématiky, diskriminačních projevů a nabádání k násilí na náboženských, etnických či jiných minoritách. V prostředí sociálních sítí dále pozorujeme fenomén zakládání falešných osobních profilů a publikaci dezinformačních příspěvků. [22]

Hacking, blagging a phishing

Policie ČR definuje hacking, blagging a phishing jako samostatné kategorie kybernetické kriminality. V kontextu s výše uvedeným je lze považovat spíše za způsob provedení trestných činů.

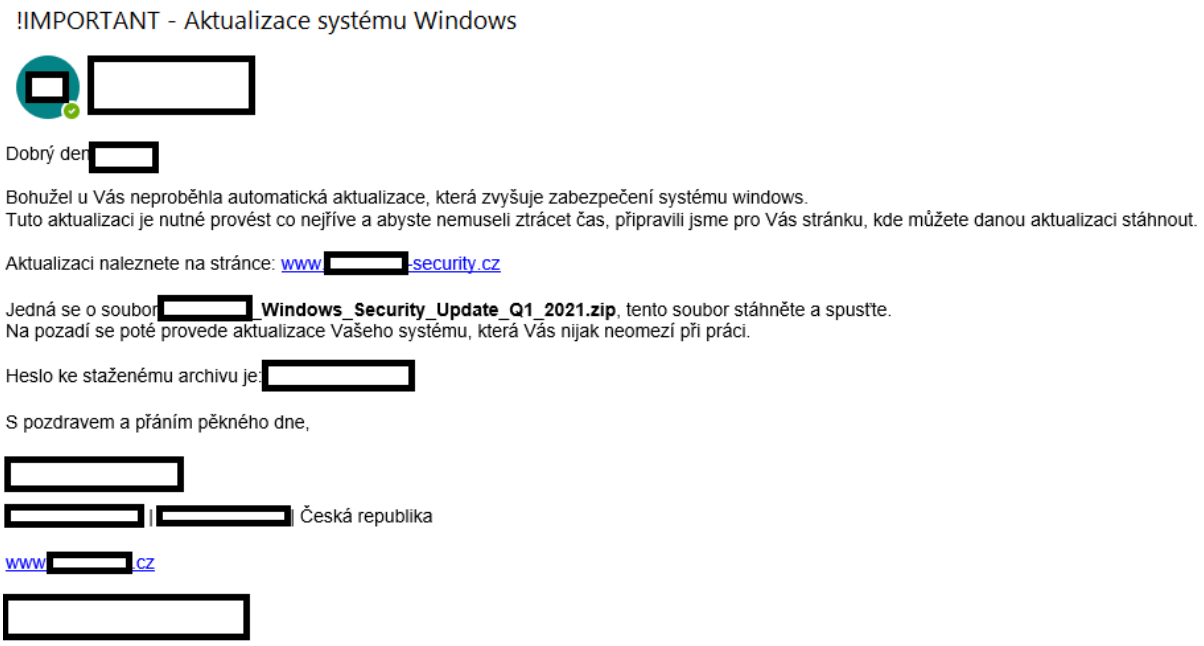
Hacking lze nejsnadněji vystihnout jako vloupání v kyberprostoru ve smyslu § 121 trestního zákoníku. Jedná se o nedovolené překročení hranic nebo překážek vytyčených v kyberprostoru například formou exploitace (využití zranitelnosti informačních systémů) nebo zavedením počítačového viru.

Phishing a blagging se částečně překrývají s kategorií podvodných jednání. Veskrze jde o techniky, které spadají do tzv. sociálního inženýrství (tj. techniky a nástroje pro psychickou manipulaci obětí, jejichž cílem je přimět oběť něco konat)[23]. Phishing je podvodné elektronické sdělení (typicky e-mail) strukturované tak, aby vzbuzovalo v příjemci důvěru. Urguje ho např. ke kliknutí na hypertextový odkaz, vyzrazení citlivých a tajných informací, nebo zaslání peněžní sumy. Blagging má za cíl víceméně totéž, nicméně pachatel při něm kontaktuje konkrétní oběť

[22] *POLICIE ČR, cit. 18*

[23] *HADNAGY, Ch. 2011. Social engineering: the art of human hacking. Indianapolis : Wiley, 2011. ISBN 9781118029718. str. 5*

napřímo, zpravidla na základě předpřipraveného scénáře (např. se vydává za bankovní instituci nebo policistu).[24]


!IMPORTANT - Aktualizace systému Windows

Dobrý den

Bohužel u Vás neproběhla automatická aktualizace, která zvyšuje zabezpečení systému windows.
Tuto aktualizaci je nutné provést co nejříve a abyste nemuseli ztrácet čas, připravili jsme pro Vás stránku, kde můžete danou aktualizaci stáhnout.

Aktualizaci naleznete na stránce: www -security.cz

Jedná se o soubor _Windows_Security_Update_Q1_2021.zip, tento soubor stáhněte a spusťte.
Na pozadí se poté provede aktualizace Vašeho systému, která Vás nijak neomezí při práci.

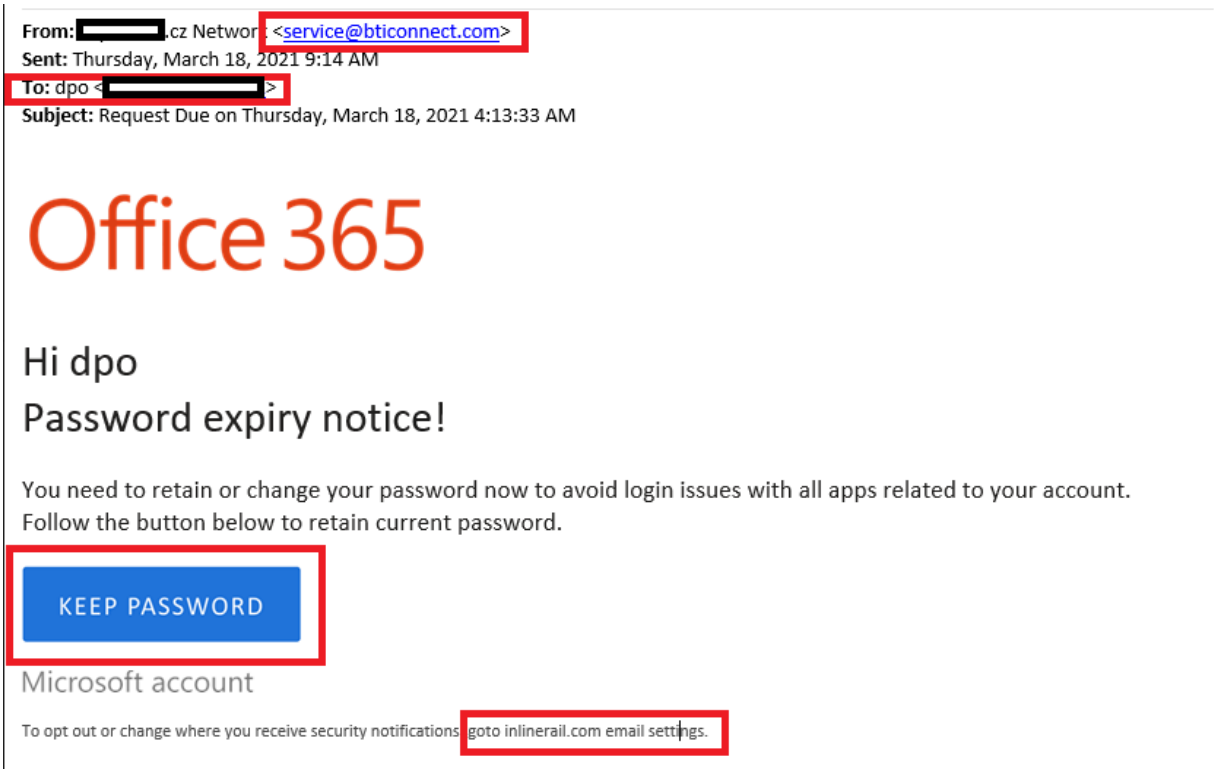
Heslo ke staženému archivu je:

S pozdravem a přáním pěkného dne,

Česká republika

www .cz

Obrázek 1 - Příklad blaggingu (zdroj: Organizace 2)


From: .cz Networ <service@bticonnect.com>
Sent: Thursday, March 18, 2021 9:14 AM
To: dpo <>
Subject: Request Due on Thursday, March 18, 2021 4:13:33 AM

Office 365

Hi dpo

Password expiry notice!

You need to retain or change your password now to avoid login issues with all apps related to your account.
Follow the button below to retain current password.

KEEP PASSWORD

Microsoft account

To opt out or change where you receive security notifications goto inlinerail.com email settings.

Obrázek 2 – Varovné znaky podvodného emailu (zdroj: Organizace 2)

[24] *WALLER, D. 2016. GCSE Computer Science for OCR. Cambridge : Cambridge University Press, 2016. ISBN 9781316504031. str. 206*

Všechny tři způsoby mohou být použity k páchání různorodé kybernetické kriminality a nelze říci, že by byl každý z nich využíván výhradně v jedné kategorii. Hacking je využíván ke spáchání majetkové trestné činnosti (např. trestného činu krádeže dle ustanovení § 40 trestního zákoníku), ovšem neméně časté je jeho použití ke spáchání trestného činu neoprávněného přístupu k počítačovému systému a nosiči informací dle ustanovení § 230 téhož zákona.

1.2.5 Ransomware

Vzhledem ke stále rozšířenějším[25] útokům typu „ransomware“ považuji za přínosné se věnovat tomuto druhu kybernetické kriminality podrobněji v rámci samostatné podkapitoly.

Pojem ransomware vznikl spojením anglických slov „ransom“ (tj. výkupné) a „malware“ (tj. škodlivý software). Podstatou ransomware je nakažení a zablokování informačních systémů oběti (počítače, mobilní telefony, servery, síťově prvky, zálohovací zařízení, IoT zařízení, PLC[26] systémy apod.). Po úspěšném napadení těchto systémů útočník oběti nabídne jejich odblokování výměnou za zaplacení výkupného. V současnosti nejběžnější způsob zablokování spočívá v zašifrování souborového systému zařízení a následného smazání dešifrovacího klíče. Pro úspěšné šíření ransomware na co největší počet systémů musí být zajištěno, že nedojde k předčasné detekci.

Typický útok začíná proniknutím útočníka do interní sítě na jednom zařízení (např. uživatelem otevřená zavirovaná příloha e-mailu, nebo zneužití hardware/software zranitelnosti, či připojení zavirovaného USB flash disku). Počítač nebo jiné zařízení v interní síti které útočník zneužívá k útoku se označuje jako tzv. pivot. Na toto zařízení je nakopírován škodlivý program (ransomware), který má za úkol provést další fáze útoku. V interní síti nakažené zařízení již zpravidla nepodstupuje takové množství přístupových kontrol jako externí systémy (vyjma informačních systémů založených na tzv. zero-trust[27] modelu). Ransomware se poměrně jednoduše šíří jak laterálně[28], tak i vertikálně[29]. Ve chvíli, kdy je útočník spokojen s dostatečným rozsahem nakažených systémů, dochází k jejich postupnému zašifrování. Šifrování má relativně

---

[25] *KASPERSKY. 2019. Kaspersky Security Bulletin '19. Statistics. [Online] 2019. [Citace: 15. únor 2020.] https://go.kaspersky.com/rs/802-IJN-240/images/KSB_2019_Statistics_EN.pdf., str. 6*

[26] PLC (*Programmable Logic Controller) – Průmyslový počítač pro ovládání výrobního procesu*

[27] *Zero-Trust model - Koncepce architektury počítačové sítě a na ní navázaných prvků, která znemožňuje uživatelům a počítačům přistupovat k informačním zdrojům nad rámec jejich definovaných oprávnění, a to bez ohledu na to, zda přistupují k těmto zdrojům z interní nebo externí sítě. Opakem je koncepce perimetru, kde uživatelé získávají důvěru na základě autentizace do interní sítě, kde již nepodléhají přístupovým kontrolám.*

[28] *Laterální šíření - Šíření na stejné úrovni oprávnění (např. na všechny ostatní uživatelské pracovní stanice)*

[29] *Vertikální šíření - Šíření z nižší na vyšší úroveň oprávnění (např. z běžného uživatelského účtu na účet lokálního administrátora a dále na doménový řadič)*

vysoké dopady na výkon nakažených zařízení. Fáze šifrování tak probíhá postupně, aby se zabránilo předčasné detekci (uživatelům může přijít pomalý počítač podezřelý). V této fázi ještě běžný uživatel nemá o útoku žádné podezření, neboť dešifrovací klíče k zašifrovaným souborům jsou stále uloženy na jeho zařízení a jsou pro operační systém bez problémů přístupné (průměrná doba detekce ransomware je 95 dní[30]). Ve chvíli, kdy jsou zašifrovány všechny systémy, ransomware smaže dešifrovací klíč a uživatel ztrácí přístup ke svému zařízení. Útočníci mají všechny dešifrovací klíče k dispozici pouze u sebe. Nakažené zařízení po skončení obsahuje jenom návod, jak zaplatit výkupné. Dešifrování bez dešifrovacího klíče je dnes vzhledem ke komplexnosti moderních šifrovacích algoritmů při kompetentním ransomware útoku prakticky nemožné. Existující dešifrovací nástroje fungují výlučně na principu již známých či sdílených šifrovacích klíčů a jejich využití je tedy možné pouze pro ransomware, jehož zdrojový kód byl zanalyzován a zveřejněn (a proto se pro další útoky zpravidla již nepoužívá). Oběť má po zašifrování dat tři možnosti, jak dále postupovat. První je obnova veškerých ztracených dat ze záloh. Druhou možností je nová výstavba infomačního prostředí (tzv. start na zelené louce). K tomuto scénáři dochází, pokud proběhlo i zašifrování záloh, nebo zálohováno vůbec nebylo. Třetí volbou je platba výkupného. Úhrada probíház důvodu zachování anonymity útočníka zpravidla v bitcoinu či jiných kryptoměnách .

Útočníci praktikují tyto útoky jako výdělečnou činnost a často mají pro tyto účely také dedikovanou uživatelskou podporu, která po zaplacení provede oběti procesem obnovy nakažených systémů. Útočníci (potažmo jejich skupiny) jsou v tomto ohledu vysoce profesionalizovaní a jejich business plán závisí na tom, zda oběti zaplatí. V závěru k falešnému odšifrování (situace, kdy uživatel zaplatí, ale data zůstanou nepřístupná) prakticky nedochází.

K výše uvedenému je nutno dodat, že s vývojem moderního ransomware jsou spojeny poměrně vysoké náklady na vývoj a distribuci. Pro útočníky je proto lukrativnější cílit spíše na firemní prostředí (popř. jiné např. státní instituce) než na běžné domácí uživatele. Vyplývá to jednak z toho, že běžný uživatel nemá k dispozici tolik peněžních prostředků na úhradu výkupného a také z toho, že často nemá k platbě přiměřenou iniciativu. Na domácích zařízeních běžný uživatel neuchovává dostatečně senzitivní informace a obnovu funkčnosti počítače vyřeší přeinstalací operačního systému. Případná ztráta dat pro něho není až tak důležitá.

Oproti tomu pro obchodní společnosti potažmo další instituce je funkčnost jejich informačních systému jedním ze základních předpokladů úspěšného fungování. Bez jejich

[30] *CROWDSTRIKE SERVICES. 2019. Cyber Front Lines Report. [Online] 2019. [Citace: 7. únor 2021.] https://apollo-is.com/white_papers/crowdstrike-services-cyber-front-lines-report/. str. 8*

existence si nelze představit fungování většiny firemních procesů, poskytování svých služeb či generování zisku. Z tohoto důvodu organizace v dnešní době investují do zabezpečení svých technologií znatelnou část svého rozpočtu.[31]

Policie ČR neprovádí sběr statistických dat pro tuto kategorii trestné činnosti.[32] Vzhledem ke stále narůstající medializaci útoků, lze předpokládat, že oblast ransomware bude v budoucnu podrobněji sledována i na vnitrostátní úrovni. Statistika v oblasti kybernetické kriminality dlouhodobě naráží na problémy[33] (rozmanitost, chybějící indikátory, nejednotná metodologie, absence kooperace mezi státními a soukromými subjekty, vysoká míra latence).

1.3 Historie

Rozmach kybernetické kriminality je přímo úměrný popularitě a dostupnosti komunikační techniky. S každým průlomovým objevem na poli informačních technologií dochází dříve nebo později k jeho zneužití pro jiný než původně zamýšlený účel. Ne vždy se jedná o zavrženíhodné chování a motivem nemusí být výhradně vlastní prospěch. Přístup k trestání konkrétních činů je navíc historicky velice různorodý. Přestože je způsob provedení vždy specifický pro dané období a technologii, lze pozorovat v těchto činech společné znaky[34]. Cílem následujících podkapitol je představení vybraných případů z minulosti a poukázání na archetypální rysy kybernetické kriminality.

1.3.1 Optický telegraf – První hack

S objevem prvního masově využívaného telekomunikačního kanálu vzniká také příležitost pro vznik nového druhu zločinu. Prototyp optického telegrafu je připisován francouzskému vynálezci Claude Chappovi, který v roce 1792 představil prototyp takzvaného „semaforu“[35]. Jednalo se o systém věží ve vzájemném dohledu, na jejichž vrcholu byl umístěna mechanická ramena. Pomocí manipulace s rameny bylo možné na první věži v sérii formulovat zprávy za pomoci nové piktogramové konvence. Ta umožňovala převod alfanumerických znaků do podoby srozumitelné pro operátory jednotlivých věží v systému. Takto naformulovanou

[31] *SOPHOS. 2020. The State of Ransomware. [Online] květen 2020. [Citace: 30. prosinec 2020.] https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf. str. 11*

[32] *POLICIE ČR, cit. 8*

[33] *MEHTA, I. 2019. The Need for Better Metrics on Cybercrime. [Online] 1. říjen 2019. [Citace: 12. říjen 2020.] https://www.thirdway.org/memo/the-need-for-better-metrics-on-cybercrime. str. 3-5*

[34] *MIDDLETON, B. 2017. A History of Cyber Security Attacks: 1980 to Present. Boca Raton, FL : CRC Press, 2017. ISBN 9781351651905.*

[35] *PEHRSON, B. 1994. The Early History of Data Networks. místo neznámé : Wiley-IEEE Computer Society Pr, 1994. ISBN 9780818667824. str. 47-97*

informaci kopírovaly další věže v pořadí, až se dostala ke svému adresátovi.[36] Řešení mělo z dnešního pohledu několik zjevných omezení. Tyto neduhy byly nicméně marginální v porovnání s dosavadními možnostmi komunikace. Jednoznakovou zprávu mezi Paříží a Lyonem (cca 1000 km) dokázala soustava dvaceti věží přenést za 2 minuty. Na první pohled významným problémem tohoto druhu komunikace byla možnost odposlechu. Riziko však nebylo reálně tak významné, protože k úspěšnému dekódování informace z polohy ramen bylo nutné znát telegrafní kód, který byl k dispozici výhradně operátorům jednotlivých telegrafních věží. Z výše uvedených důvodu byl optický telegraf seznán jako ideální komunikační prostředek pro předávání zpráv z bojiště i samotným Napoleonem Bonaparte[37], který významně přispěl k rozvoji a standardizaci telegrafních linek po celé Francii.[38] Optický telegraf byl bez významnějších změn používán až do období Krymské války (1853-1856).[39] Přestože byl celý systém určen výhradně ke státním účelům, v roce 1834 došlo k jeho zneužití k osobnímu prospěchu.

Za historicky prvním Man-in-the-Middle[40] útokem stáli François a Joseph Blancovi. Bratři Blancovi byli obchodníky se státními dluhopisy na burze v Bordeaux. Směr vývoje burzovních trhů v celé Francii udávala burza v Paříži. Tento trend se sice vždy promítl i na sekundární burzovní trhy, dělo se tomu tak ale až s několikadenním zpožděním. Před vynálezem telegrafu bylo totiž nutné spoléhat na doručení dopisů poštovními dostavníky, kurýry či holuby. Informace o budoucnosti trhu znamenají pro jejich vlastníka šanci na rychlé zbohatnutí. Bratři proto využili k úspoře času novou technologii - optický telegraf. V té době byl přístup k telegrafním věžím určen výhradně registrovaným operátorům a samotný provoz byl přísně střežen. Nebylo tak možné začlenit do přenosu informací vlastní zprávu. Bratři k přenosu využili zranitelnost mechanismu opravných zpráv. Při legitimním přenosu se chyba v signalizaci řešila opětovným zasláním opravy. Jednotlivé věže zprávu neformulovaly, ale pouze kopírovaly. K faktickému generování informace tak docházelo až na posledním bodu řetězce. François a Joseph podplatili operátora telegrafní věže

---

[36] *BURNS, Russel W. 2004. Communications: An International History of the Formative Years. Stevenage : IET, 2004. ISBN 9780863413278. str. 29-57*

[37] *ROGERS, H.C.B. 2005. Napoleon's Army. South Yorkshire : Pen & Sword Military, 2005. ISBN 9781844153107. str. 90*

[38] *CHAPPE, Ignace Urbain J. 1840. Histoire de la Télégraphie. Bruxelles : Ch. Richelet, 1840. ISBN 9780270290233. str. 239*

[39] *SELIN, S. Napoleonic Telecommunications: The Chappe Semaphore Telegraph. [Article] Internet: shannonselin.com, 2020.*

[40] *MitM (Man-in-the-middle) – Útok na přenos informací. Spočívá v nabourání důvěrnosti, integrity nebo dostupnosti datového toku. Útočník vystupuje v komunikaci mezi odesílatelem a příjemcem v roli prostředníka. Díky tomu může provádět odposlech přenášených zpráv, jejich změnu nebo přesměrování. Man-in-the-Middle útoky jsou hlavním důvodem pro rozmach kryptografie v moderních informačních systémech.*

v Tours, aby v případě dramatických změn na burze v Paříži zařadil do svého vysílání specifickou sekvenci chybových a opravných vysílání. Na druhém konci telegrafního spojení pak stál komplic s dalekohledem, který odezíral pozice ramen telegrafní věže a pokud zpozoroval dohodnutou kombinaci chyb, informoval bratry o tom, jak investovat. Výměna informací fungovala přes dva roky, než operátor v Tours onemocněl a požádal o stejnou službu svého náhradníka. Ten celý podvod odhalil a ohlásil policii. Všichni pachatelé byli zatčeni. Trestní řízení nemělo dlouhého trvání, protože neexistoval žádný zákon, který by tuto činnost zakazoval. Bratři Blancovi byli propuštěni na svobodu[41]. Incident i z dnešního pohledu nese typické znak kybernetické kriminality: Zneužití slabých článků, lidská vynalézavost a náskok před legislativou.

1.3.2 Bezdrátový telegraf - Spoofing a trolling

Známé jsou také případy, kdy nešlo pachateli ani tak o osobní zisk, ale spíše o snahu zesměšnit či poškodit někoho jiného. Dnes se pro tyto pachatele zažil název (internetový) „troll". Důkazem o tom, že trolling[42] není výlučně vázán na prostředí internetu, ale víceméně ho lze využít na jakémkoli zařízení pro výměnu informací je případ z roku 1903, známý též jako „aféra Maskelyne." Případ byl vyvrcholením dlouhodobé rivality vynálezce bezdrátového telegrafu Guglielma Marconiho a britského vynálezce Johna Nevila Maskelyna.

Maskelyne byl odpůrcem Marconiho monopolizace bezdrátové komunikace (Marconi byl vylučným držitelem patentů ke klíčovým technologiím bezdrátového telegrafu, např. uzemněné antény). Ve snaze poukázat na nedokonalosti v Marconiho konceptu telegrafie se se mu povedlo 4. června 1903 zneužít zranitelnosti v přenosu informací mezi jednotlivými vysílači. Marconi chtěl co nejvíce prodloužit vzdálenost mezi vysílačem a přijímačem, použil tedy na obou koncích spojení širokopásmové vertikální antény. Systém měl proto kromě vysokého výkonu i zásadní nevýhodu – přenos nebylo možno omezit na úzký kanál o konkrétní frekvenci. To mělo za následek, že vysílání bylo náchylné nejen k odposlechu, ale i rušení cizími vysíláními. Marconi tento nedostatek částečně vyřešil implementací sofistikovaného elektrického okruhu, který si velice rychle nechal patentovat, ale ani toto zlepšení nebylo bez chyb. Ve snaze dokázat vědecké obci, že Marconiho řešení bezdrátového telegrafu má reálné použití, že přenos informací je bezpečný a nelze jej zrušit, uspořádal ten den Marconiho asistent John Ambrose Fleming prezentaci před Královskou Institucí v Londýně. Maskelyne v čas Flemingovy přednášky začal na

[41] *GAZETTE DES TRIBUNAUX. 1836. Justice Civile. Journal de jurisprudence et des débats juiciaires. Edition de Paris., 1836, Sv. Samedi 10 Décembre 1836, 3506. str. 130-138*

[42] *Trolling - Způsob vystupování v kyberprostoru, jehož cílem je provokace, zesměšnění nebo ponížení druhé strany debaty, případně širšího okruhu adresátů.*

střeše přilehlého divadla opakovaně vysílat z vlastního telegrafního vysílače vlastní krátkovlnné vysílání. Z dnešního pohledu lze označit techniku za formu spoofingu[43]. Vzhledem k předchozím tvrzením Marconiho a Fleminga o bezpečnosti a robustnosti způsobilo toto narušení poprask nejen mezi přísedícími, ale i v denním tisku. Incident měl za důsledek nejen rozsáhlou výměnu názorů obou zúčastněných stran (převážně formou vzájemných osočujících novinových článků), ale také roční nedobrovolnou přestávku ve Flemingově vědecké kariéře. Marconi se ve snaze co nejvíce odvést pozornost od vlastního selhání od Fleminga distancoval, což v kombinaci se ztrátou důvěryhodnosti před celou vědeckou obcí způsobilo, že Fleming nikdy nedosáhl takové popularity a uznání, jakých mu bylo v kruzích radiotelegrafie předpovídáno[44]

1.3.3 Děrné štítky – Etický hacking

Technologie děrných štítků spatřila světlo světa poprvé už v roce 1890. Americký podnikatel a vynálezce Herman Hollerith začal na konceptu pracovat během svého působení v Americkém statistickém úřadu. Přestože jeho primárním cílem bylo tehdy zjednodušení a automatizace zpracování dat při pravidelném sčítání lidu, děrné štítky zůstaly spjaty s informačními technologiemi jako hlavní datové médium pro ukládání a zadávání datového obsahu až do poloviny 70. let 20. století. Za zmínku stojí také fakt, že Hollerith byl zakladatelem Tabulating Machine Company. Tento podnik se později spolu s dalšími třemi subjekty spojil do holdingu Computing-Tabulating-Recording Company, a dnes je známý jako nadnárodní korporace International Business Machines (IBM).

Děrný štítek byl vyráběn z tvrdého papíru. Nejrozšířenějším způsobem pro zadávání dat na štítek byl tzv. 80-sloupcový standard IBM (na papír bylo vytištěno 80 sloupců, v každém sloupci je 10 řádků s čísly 0-9). Do této šablony bylo nutno mechanicky (rukou, tabulátorem) vytvořit otvory v souladu s logikou čtečky (někdy bývá označována jako tabulátor) pro kterou byl štítek určen. Tabulátor následně otvory pro dané pole převedl na bitovou sekvenci a provedl s nimi požadovanou operaci. Tabulátor neměl vlastní mezipaměť, proto musel pro komplexnější operace provádět ukládání dosavadních výsledků na nové děrné štítky. Ty se následně znovu používali na další kroky výpočtu.

---

[43] Spoofing - Útok na dostupnost a důvěrnost zdroje informací. Spočívá v nahrazení legitimního původce vlastním informačním tokem, například zarušením původního vysílání, podvržením identifikačních parametrů síťového protokolu (MAC adresy, ARP tabulky, IP adresy, DNS záznamy). Konkrétní využití lze spatřit při podvržení telefonního čísla při vishingu, podvrhu adresy odesílatele emailové zprávy nebo vytvoření modifikovaného duplikátu webové stránky, který je pak vydáván za originál.

[44] BUCHWALD, Jed Z. 1996. Archimedes: New Studies in the History and Philosophy of Science and Technology. 1996, Sv. Scientific Credibility and Technical Standards in 19th and early 20th century Germany and Britain, 1996. str. 157-174

Děrné štítky se využívaly v mnoha oblastech lidské činnosti po celém světě. Nejinak tomu bylo i ve Francii, kde proces integrace nastartovali dodnes fungující společnosti jako Michelin nebo Renault. Zvýšení efektivity v soukromém sektoru posloužilo jako inspirace i pro francouzskou armádu. Hlavním lídrem byl v tomto ohledu graduát pařížské École Polytechnique René Carmille. Carmille inspirován experimenty během studia a poznatky kolegů ze zahraničí viděl v děrných štítcích možnost, jak optimalizovat náklady na provoz v továrnách na dělostřeleckou techniku. Jeho první reálná implementace proběhla v roce 1932 ve zbrojovce v Puteaux. Ve světle tamní časové i ekonomické úspory dostal Carmille mandát na zavedení evidence účetních knih na děrné štítky do dalších pěti zbrojních podniků. Carmille postupně nejen rozšiřoval funkcionalitu existujících systémů (například o kompletní řešení mzdové agendy), ale tlačil i na jejich zavádění v dalších procesech veřejné správy (např. povolávání k vojenské službě). De facto se tak dostal do pozice odborníka na děrné štítky pro celou francouzskou administrativu.

Po kapitulaci Francie v červnu 1940 Carmille inicioval zavedení centrálního registru osob. Zdroje se neshodují v tom, zda byla jeho reálným motivem získání statistických dat o vojenských silách pro mobilizaci proti okupaci nacistickými vojsky, nebo snaha o zvýšení kontroly nad francouzskou populací. Faktem ale je, že ve stejném roce byl zahájen rozsáhlý projekt populačního censu, který vedl právě Carmille. Základní premisou bylo vytvoření osobního spisu a dvou děrných štítků pro každého obyvatele Francie. V osobním spise byl zachycen relativně podrobný záznam dosavadního života osoby, popis fyzického vzhledu, datum narození (a úmrtí), údaje o rodinných vztazích. Údaje o náboženském vyznání osob se zde neevidovaly. První děrný štítek obsahoval statistické informace pro účely sčítání lidu, druhý pak jméno a aktuální doručovací adresu. Soubor osobního spisu a dvou děrných štítků byl identifikován třináctimístným číselným kódem (obdoba dnešního rodného čísla). Pro usnadnění identifikace osob došlo na popud projektu také k distribuci občanských průkazů. Ty obsahovaly kromě základní osobních údajů také výše zmíněný číselný kód.

Carmille byl členem francouzského odboje proti okupaci. Jako zarytý odpůrce antisemitských opatření, která tou dobou svírala Francii využíval dlouhodobě svoji pozici k tomu, aby sabotoval nacistické aktivity proti tamní židovské populaci. Cílem nacistického režimu byla evidence židovského obyvatelstva a její následný přesun do pracovních táborů. O zpracování statistických dat v Carmilleově systému projevili Němci zájem v roce 1941. Dosavadní sčítání židovské obce probíhalo klasickou papírovou formou, záhy se však ukázalo, že tento způsob sběru dat je nepřesný a extrémně zdlouhavý. Carmille byl coby ředitel Service National des Statistiques

(pozice, do níž byl jmenován díky své práci na centrálním registru osob) osloven s žádostí o pomoc se zpracováním výsledků sčítání. Spolupráci na evidenci židovské populace nejprve zdržoval argumentací a výmluvami na nedostatek kapacit. Když již další prodlevy nebyly možné, svou pomoc přislíbil, nicméně výsledky sabotoval, takže měly minimální vypovídající hodnotu.

Za dobu Carmilleova působení v čele statistické kanceláře docházelo k nadprůměrným ztrátám sčítací dokumentace a úspěšnost následného dohledávání židů nebyla o nic vyšší, než při původní papírové evidenci. Carmille kromě byrokratických obezliček využil toho, že znal mechanismus Bullova tabulátoru. Stroje použité ke zpracování výsledků židovského censu pozměnil tak, aby ignorovaly 11. sloupec děrného štítku. Právě tento sloupec obsahoval informace o náboženském vyznání. Za čin bývá označován jako první White-hat[45] hacker.

Carmille během projektu sčítání obyvatel vytvořil tajný sekundární registr osob. Ten měl sloužit pro povolání osob schopných vojenské služby do aktivní rezistence proti okupaci. Registr údajně obsahoval okolo 300 000 mužů a měl umožnit jejich mobilizaci do 36 hodin. V kontextu moderní terminologie se jednalo o názorný příklad fenoménu shadow IT[46]. K realizaci záměru však nikdy nedošlo. Nacisté v reakci na invazi spojenců v Alžírsku z 8. listopadu 1942 obsadili celou Francii, což rozbilo veškeré plány na tajnou mobilizaci. Carmille nakonec celý registr i veškerou související dokumentaci osobně zničil, protože se obával odhalení nacistickým režimem.

Potenciál v technologii děrných štítků viděli také Spojenci pro jejichž agenty vytvářel Carmille podvržené identity a osobní složky. Hlavním důvodem, proč se záškodnická činnost stala Carmilleovi osudnou byla nakonec jeho zřejmá neochota spolupracovat při sčítání židů v roce 1943. Pro zdánlivou neschopnost byl vyhozen z postu ředitele statistického úřadu, a na povrch díky tomu postupně vypluly důkazy o všech Carmilleových aktivitách. V únoru roku 1944 byl proto zatčen, označen za nepřítele Třetí říše a deportován do koncentračního tábora v Dachau, kde posléze v lednu 1945 zemřel na tyfus.[47,48]

---

45 White Hat/Black Hat hackeři– Termíny pro označení primárního motivu hackera (morálně korektní vs. zavrženíhodný). Pojmy odkazují na westernové filmy druhé poloviny 20. století, v nichž běžně v pozici kladného hrdiny vystupoval bíle oděný protagonista. Antagonista byl pro dosažení kontrastu znázorňován převážně v tmavém oděvu. White hat je běžně používán jako synonymum pro etický hacking. Jedná se např. o specialisty na počítačovou bezpečnost, kteří se zaměřují na zvýšení odolnosti informačních systému proti kybernetickým útokům.

46 Shadow IT – Neschválené informační technologie zavedené do existujících informačních systémů jejich správci, uživateli nebo jinou osobou (např. útočníkem). Představují bezpečnostní riziko pro celý systém (např. z důvodu jejich zranitelností, chybějící podpory, časových a ekonomických nákladů na reverse engineering apod.)

47 HEIDE, L. 2004. Monitoring People: Dynamics and Hazards of Record Management in France 1935-1944. Technology and Culture. JSTOR, 2004, Vol. 45, 1. str. 80-101

48 BLACK, E. 2001. IBM and the holocaust : the strategic alliance between Nazi Germany and America's most powerful corporation. místo neznámé : Crown, 2001. ISBN 9780609607992. str. 321-332

1.3.4 Telefon – Phreaking a legislativní inkonzistence

Patent na telefonní přístroj byl registrován pod jménem Alexandra Grahama Bella již v roce 1876, ale převahu v popularitě nad telegrafem získal vynález až po třech dekádách.[49] Ihned po uvedení technologie bylo zjevné, že pro reálné použití bude nutné vytvořit infrastrukturu telefonních ústředen. Pro jejich zřízení existovaly dva hlavní důvody. Prvním byla potřeba svedení telefonních linek od koncových telefonních zařízení do centrálních komunikačních uzlů. Tím bylo umožněno, aby si všichni majitelé telefonních aparátů mohli vzájemně volat bez potřeby propojit telefony mezi sebou napřímo. Propojení mělo vícero rovin, jednak spojení mezi zařízeními v regionu podléhající pod místní telefonní ústřednu a dále spojení se zařízeními, která spadala pod další ústředny v regionu (meziměstské hovory), či mimo něj (zahraniční hovory). Druhým argumentem pro zavádění telefonních ústředen byla potřeba vyúčtování telekomunikačních služeb. Obecně bylo zřizování a údržba telefonních linek ekonomicky nákladnou aktivitou. Poskytovatel proto financoval infrastrukturní aktivity tarifní sazbou za uskutečněný hovor. Hovory v rámci místní telefonní ústředny podléhali nižším tarifům než hovory přepojované několika ústřednami.

Právě vysoké poplatky za dálkové hovory vedly v USA na přelomu 60. a 70. let 20. století. Ke vzniku subkultury tzv. „phreaks“ (z angl. „Phone freaks“- volně přeloženo do češtiny jako telefonní fanatici). Konkrétní metody, jak obejít zamýšlenou funkčnost telefonních ústředen, rozvoden či veřejných budek se lišily napříč oblastmi a obdobími. V dobách rozmachu phreakingu byla výsostným telekomunikačním operátorem v USA společnost AT&T, nástupce původní Bell Telephone Company založené samotným vynálezcem telefonu A.G. Bellem. Monopolní pozice AT&T paradoxně nahrávala phreakingu do značné míry tím, že ve své infrastruktuře udržovala jednotný standard technického vybavení. Jednalo se o stroje původem ve 30. a 40. letech, přičemž hlavním cílem jejich vývoje byla především dostupnost a funkčnost spojení. [50] Telefonní ústředny pro vykonávání stavové logiky hovoru využívaly zvukové tóny ve specifickém frekvenčním rozsahu přenášené na stejném kanálu jako samotný telefonát (tzv. In-band signalizace). Ze současného pohledu nelze mluvit o efektivním bezpečnostním opatření, nicméně vzhledem k tehdejší absenci jakýchkoliv zkušeností s hackingem, lze hovořit o primitivním autentizačním mechanismu. Zranitelnost objevilo nezávisle na sobě několik osob. Někteří se o ní dozvěděli

[49] *CORDEIRO, Luis J. 2008. Telephones and Economic Growth. A Worldwife Long-Term Comparison with Emphasis on Latin America and Asia. [Online] 2008. [Citace: 27. leden 2021.] https://www.ide.go.jp/library/English/Publish/Reports/Vrf/pdf/441.pdf. str.12*

[50] *HOCHHEISER, S. 1989. The American Telephone and Telegraph Company. AT&T Archives . [Online] 1989. [Citace: 15. červen 2020.] https://www.beatriceco.com/bti/porticus/bell/pdf/tattc.pdf.*

paradoxně přímo od AT&T, konkrétně z listopadového vydání interního periodika The Bell System Technical Journal z roku 1960. Časopis obsahoval podrobný technický popis používaných signalizačních systémů v AT&T. Bylo pouze otázkou času, než někdo vymyslí, jak jej exploitovat.[51] Nicméně ne všichni, kdo o zranitelnosti věděli se o ní dozvěděli úmyslně. Příkladem je příběh nadšence telefonních technologií jménem Joe Engressia. Ten ve svých 7 letech postřehl, že při spojení hovoru zazní krátký strojem generovaný tón. Jednalo se o tón o frekvenci 2600 Hz. Engressia byl schopen ho reprodukovat zapískáním díky svému absolutnímu sluchu. K jeho překvapení došlo okamžitě k rozpojení hovoru. Povzbuzen prvotním úspěchem začal Engressia experimentovat s délkou a frekvencí tónu a dokázal postupně provést kompletní reverse engineering signalizačních sekvencí. [52]

Reprodukovat tón o specifické frekvenci vlastními ústy je pro majoritní populaci téměř nemožné. Ralph Barclay proto sestrojil v roce 1960 první "blue box". Jednalo se o kapesní zařízení s číselníkem, které dokázalo přehrávat tóny o frekvenci 2600 Hz. Informace o tom, že lze za pomoci relativně levného zařízení volat zdarma se rychle šířila. Phreaking byl od začátku založen na kolektivním brain stormingu a sdílení poznatků. Členové phreakerské komunity běžně pořádali konferenční hovory (např. na interních linkách telefonních ústředen), při kterých debatovali nad svými úspěchy a problémy. Jednalo se víceméně o obdobu současných internetových fór. K radikálnímu nárůstu popularity došlo v roce 1971, kdy časopis Esquire publikoval několikastránkový článek na téma phreakingu[53]. Tento článek inspiroval k činu např. i zakladatelé společnosti Apple Steva Wozniaka a Steva Jobse, kteří začali blue boxy vyrábět a prodávat s velkou marží[54]. Zájem o krabičky byl enormní především u odvětví, která využívala telefon jako hlavní komunikační nástroj. Jednalo se o legitimní entity, investory na Wall street, sázkové kanceláře nebo bankovní domy. Zájem o anonymní volání zdarma zanedlouho projevil i organizovaný zločin.[55]

Právní úpravy jednotlivých států na phreaking nahlížely velice různorodě (od absence právní úpravy přes legalitu až k trestům odnětí svobody). Na úrovni federálního práva sice existovalo ustanovení ve federálním trestním zákoníku (18 U.S. Code § 1343 - Fraud by wire,

---

[51] BREEN, C. a DAHLBOM, C. A. 1960. Signaling Systems for Control of Telephone Switching. The Bell System Technical Journal. November, 1960, Sv. 39, 6. str. 1399-1429

[52] LAPSLEY, P. 2013. Exploding The Phone: The Untold Story Of The Teenagers And Outlaws Who Hacked Ma Bell. místo neznámé : Grove Press, 2013. ISBN 9780802120618. str. 65-71

[53] ROSENBAUM, R. 1971. SECRETS OF THE LITTLE BLUE BOX. Esquire. 1971, October.

[54] MARKOFF, J. 2001. The Odyssey Of a Hacker: From Outlaw To Consultant. New York Times. National Edition, 2001, Sv. January 29th, Section C, Page 1.

[55] JACOBS, Sanford L. 1976. Blue Boxes Spread From Phone Freaks To the Well-Heeled. The Wall Street Journal. January 29th, 1976.

radio, or television), nicméně týkalo se spíše podvodu přes telefon, nikoliv obcházení samotného mechanismu volání. Jeho aplikace byla silně závislá na výkladu jednotlivých soudců, což nezaručovalo u soudního jednání úspěch. Tato nekonzistence donutila AT&T k tomu, aby se preakingu bránili vlastními zdroji. AT&T vytvořilo pro detekci tónů z blue boxů speciální zařízení, přes které proudil veškerý telefonní provoz. Daný způsob detekce umožňoval identifikaci pachatelů podle telefonního čísla. Zároveň vzniklo oddělení, které mělo za úkol detekovaná čísla obvolávat s výzvou k okamžitému zastavení nelegální činnosti. Takto nasbíraná data a identifikační údaje byly používány i jako důkaz u soudního řízení. Obhajoba je ovšem záhy začala označovat za formu nelegálního odposlechu, a tak mnohdy nebyly připuštěny jako důkaz.[56]

1.3.5 ARPANET - První honeypot a forenzní analýza kybernetického útoku

Když byl v srpnu roku 1986 zjištěn v Lawrence Berkley Laboratory (LBL) průnik do vnitřní sítě, rozhodli se správci systému k netradičnímu kroku. Namísto do té doby běžné reakce (snahy o co nejrychlejší blokaci útočníka odpojením počítačů od sítě a změnou přihlašovacích údajů), zvolili metodu honeypotu[57] s cílem nasbírat co největší množství dat pro počítačovou forenzní analýzu. Výsledkem bylo zjištění skutečného rozsahu útoku a získání dostatečných detailů o pachateli. Místo okamžitého potlačení bylo tímto postupem zabráněno větší škodě a zároveň došlo k faktickému dopadení pachatele. Díky forenzní analýze byl nakonec překažen nejen předmětný útok, ale také probíhající mezinárodní špionáž a přeprodej získaných dat ruské KGB. Na to, že by v síti mohl být neoprávněný útočník, přišli správci informačního systému na základě chybového hlášení v in-house vyvinutém účetním programu. Chybová hláška obsahovala informace o existenci účtu bez fakturační adresy v databázi uživatelů, což znemožňovalo programu úspěšně dokončit účetní závěrku. Zanedlouho poté dorazila do LBL zpráva z National Computer Security Center[58] s informací, že z počítačů v LBL došlo k pokusu o nabourání do sítě MILNET[59]. I po smazání problematického účtu útoky pokračovali. Vedením vyšetřování byl pověřen systémový administrátor Clifford Stoll. Ten stál před složitým problémem: Jak zjistit odkud útok probíhá? Pro zúžení okruhu podezřelých nasadil na všechny komunikační porty odposlouchávací zařízení, které směrovalo veškerý textový vstup a výstup na lokální tiskárnu.

---

[56] *LAPSLEY, P. cit. 52. str. 46-53*

[57] *Honeypot (Volně přeloženo návnada na hackery) - Jde o účelově vytvořenou část počítačové sítě, do které je útočník vpuštěn v rámci probíhajícího kybernetického útoku nebo je implementována preventivně jako detekční mechanismus. Honeypot obsahuje falešná či pozměněná data, která na první pohled v útočníkovi evokují legitimní citlivé informace. Honeypoty mají běžně nižší úroveň zabezpečení než zbytek sítě a běží v nich analytické nástroje, které sbírají informace o útočníkovi a použitých metodách.*

[58] *National Computer Security Center je odnož americké bezpečnostní agentury NSA (National Security Agency) pro boj s kybernetickou kriminalitou*

[59] *MILNET (Military Network) – Počítačová síť Ministerstva obrany Spojených států amerických*

Díky tomu bylo záhy jasné, že útok probíhal přes protokol X.25 (předchůdce nejpopulárnějšího současného protokolu pro připojení do WAN[60] – TCP/IP založený na přenosu přes telefonní linky). Při trasování přes telefonní ústředny byli operátoři schopni vystopovat útok probíhající z blíže nespecifikované adresy v Německu. Napadený počítač byl následně záměrně přeměněn na honeypot. Veškerá aktivita byla odkloněna na úrovní síťové komunikace na tiskový výstup, aby útočník nepojal podezření, že je sledován. (Monitoring uživatelských aktivit na úrovni operačního systému lze odhalit např. z běžících systémových procesů, navíc má výkonové dopady na celkovou odezvu systému, proto jej Stoll a jeho tým nemohli v dané situaci použít). Z tištěných výstupů bylo zjevné, že útočník necílil přímo na LBL, ale na další instituce, které byly s LBL propojeny v rámci sítě ARPANET a MILNET. Napadené počítače posloužili převážně jako pivot do vysoce citlivých systémů, např. informačních systémů vědeckých útvarů pro jadernou, fůzní a magnetickou fyziku spadající pod Ministerstvo energetiky. Stoll odhalil, že útočník na počítačích v MILNET zkoušel postupně běžné kombinace výchozího přihlašovacího jména a hesla. I přesto, že změna výchozích přihlašovacích údajů by měla být jedním ze základních bezpečnostních postupů při implementaci jakéhokoliv informačního systému, podařilo se útočníkovi přihlásit na cca 5 % všech počítačů, které zkusil napadnout. Útočník se po prvotním přihlášení zaměřil na to, aby získal nad systémem plnou kontrolu. Pro tyto účely používal bug[61] v textovém editoru Gnu-Emacs. Zmíněný software byl běžně nainstalován na většině počítačů té doby, standardně se spouštěl v kontextu celého systému[62] a umožňoval tak i zápis do adresářů operačního systému. Díky tomu bylo možné změnit lokální konfiguraci systémových účtů[63] a přidělit svému účtu administrátorské oprávnění. Následně útočník spouštěl vyhledávání souborů, které odpovídaly názvem nebo obsahem klíčovým heslům (např. “nuclear” “sdi[64]” “kh-11[65]” či “norad[66]”. Protože nebylo možné napadené systémy nějak zásadně modifikovat, aniž by došlo ke vzbuzení podezření, měl útočník po celou dobu útoku přístup k reálným produkčním datům. Pro minimalizaci rizika se

---

[60] WAN (Wide Area Network) – Počítačová síť složená z jednotlivých místních sítí LAN (Local Area Network) Nejznámějším příkladem takové sítě je Internet.

[61] Bug – Chyba v software, která má za následek původně nezamýšlené chování programu

[62] Software se standardně spouští buď v kontextu uživatele nebo lokálního/vzdáleného systému. Podle toho, v jakém kontextu program běží mu mohou být cíleně nebo omylem udělená práva i ke čtení a editaci běžně chráněných systémových souborů a nastavení

[63] Počítačový účet – Identita skrz kterou vystupuje uživatel vůči počítači. Účty se dělí na tzv. standardní (účet bez zvláštních oprávnění, slouží k běžné aktivitě koncového uživatele, nemá např. právo na změnu konfigurace systému) a privilegované (označovány někdy jako administrátorské účty, jsou účty s nestandardním oprávněním vůči systému, např. právo vytvářet a mazat další účty a určovat jejich typ, či právo na čtení a editaci souborů operačního systému)

[64] SDI (Strategic Defense Initiative) – Program prezidenta Spojených států amerických Ronalda Reagana na celostátní ochranu území USA před jadernými zbraněmi a balistickými raketami typu země/země a vzduch/země.

[65] KH-11 - Americký špionážní satelit

[66] NORAD (North American Aerospace Defense Command) – Organizace pro ochranu vzdušného prostoru Severní Ameriky

Stoll rozhodl ve spolupráci se správci napadených systému implementovat falešné stopy. Jednalo se o textové soubory s fiktivními citlivými informacemi nebo e-mailové zprávy, které útočníka utvrzovali o tom, že mu nikdo není na stopě. Pokud byl během monitoringu zjištěn pokus o stažení reálných citlivých dat, byli operátoři schopni mu zabránit zrušením síťového provozu a simulováním běžného výpadku X.25 spojení. [67]

Po celou dobu vyšetřování si Stoll a ostatní správci vedli podrobný deník. Ten obsahoval kromě útočníkových aktivit i poznatky jednotlivých administrátorů a úvahy o dalším postupu. Vzhledem k tomu, že útočník měl potenciálně přístup do všech informačních systému, ukládali veškerou evidenci pouze fyzickou formou. Koordinace aktivit probíhala na fyzických schůzkách úzkého okruhu účastníků či po telefonu, aby nedošlo k prozrazení. Postup Stolla a spol. vytvořil základy pro plánování odezvy na kybernetický bezpečnostní incident[68] a poskytl první příklad reálné implementace CSIRT[69].

Tým LBL sbíral data o útoku necelý rok a následně je předal FBI. Na základě těchto podkladů došlo v roce 1990 k dopadení tři občanů Spolkové republiky Německo – Markuse Hesse, Petera Carla a Dirka Brzezinskeho. Všichni tři pachatelé byli nakonec odsouzeni Vrchním zemským soudem v Celle k dvouletému nepodmíněnému trestu odnětí svobody.[70] Důvodem pro relativně nízký trest byl podle soudce Leopolda Spillera fakt, že SRN nikdy nevznikla žádná škoda.[71]

1.4 Pachatelé

Pachatelé kybernetické kriminality nezapadají do zavedených koncepcí kriminologických škol minulého století. Hlavní zásluhu na tom má sociální a technologická proměnlivost kyberprostoru. Kybernetická kriminalita se začala objevovat až s masovou dostupností moderní výpočetní techniky a k podrobnějšímu zkoumání tak dochází až v posledních 20 letech.

1.4.1 Společné znaky

I přes výše zmíněné body existují atributy, které jsou společné převážné většině pachatelů tohoto druhu trestné činnosti. Prvním z těchto znaků je anonymita. Dlouhodobě vysoká míra

---

[67] STOLL, C. 1988. Stalking the Willy Hacker. Communication of the ACM. May, 1988, Sv. 31, 5.

[68] IRP (Incident Response Planning) – Plán postupu při kybernetickém bezpečnostním incidentu. Standardně se dělí na 6 fází: 1. Příprava, 2. Identifikace, 3. Zamezení šíření, 4. Vymýcení, 5. Obnova, 6. Sumarizace poznatků

[69] CSIRT (Cyber Security Incident Response Team) – Dedikovaný tým expertů na řešení bezpečnostních incidentů

[70] HAFNER, K a MARKOFF, J. 1995. Cyberpunk: Outlaws and Hackers on the Computer Frontier, Revised. místo neznámé : Simon and Schuster, 1995. ISBN 9780684818627. str. 239-250

[71] REUTERS. 1990. 2 W. Germans Get Suspended Terms as Computer Spies. Los Angeles Times. February 16th, 1990.

latence (odhady se pohybují v rozmezí 75 až 90 % neodhalených trestných činů[72]) a nízká míra objasněnosti (cca 1 % [73]) znamenají, že se k tomuto druhu kriminality často tíhnou i pachatelé, kteří by o jiném druhu trestné činnosti vůbec neuvažovali. Zdárným příkladem tohoto fenoménu je internetové pirátství.[74] Na něm je patrné, že pokud by internetoví piráti neměli možnost pořizovat mediální obsah z internetu, neuchýlili by se k jeho získání fyzickým ekvivalentem trestné činnosti (např. trestným činem krádeže podle § 205 zák. č. 40/2009 Sb.). Toho jsou si vědomi koneckonců i producenti a distributoři autorských děl, jejichž veškerá technická opatření směřují výhradně k zamezení úniku dat z datových nosičů, nikoliv k prevenci jejich fyzického odcizení. Tuto úvahu podporují empirické výzkumy, z nichž vyplývá, že míra pirátství nemá na legální prodeje zásadní vliv (pouze 4 % ilegálně získaných kopií filmů by si pachatelé zakoupili, pokud by neměli možnost je získat zdarma[75]). Anonymita je pro pachatelé velkým lákadlem, poskytuje jim velkou šanci na úspěch a mizivou šanci na dopadení, umožňuje jim se sdružovat a kooperovat na vývoji nových metod. Druhým společným znakem je zájem pachatelů o informační technologie.

1.4.2 Typologie pachatelů

Tato podkapitola obsahuje nejčastěji skloňované archetypy pachatelů kybernetické kriminality a přiřazuje k nim definující znaky, jako jsou například motivace či forma útoku.[76]

Kyberteroristi

Kybeteroristi jsou extrémističtí jednotlivci nebo skupiny osob, kteří využívají kybernetické nástroje k zastrašování, vydírání, ovlivňování veřejného mínění nebo k propagaci své politické či náboženské agendy. Hlavním cílem těchto pachatelů je získání podpory (ekonomické i politické) a potlačení opozice pro dosažení svých ideologických cílů. Hojně k tomu využívají

---

[72] *SABADASH, V. 2004. A Latency of Computer Crimes. Computer Crime Research Center. [Online] 5. duben 2004. [Citace: 22. srpen 2020.] http://www.crime-research.org/articles/sabad03_2004/2.*

[73] *EOYANG, M, a další. 2018. To Catch a Hacker. [Online] 29. říjen 2018. [Citace: 5. květen 2020.] https://www.thirdway.org/report/to-catch-a-hacker-toward-a-comprehensive-strategy-to-identify-pursue-and-punish-malicious-cyber-actors. str. 2*

[74] *Pro podporu toho argumentu je nutné na problematiku nahlížet globálně, nikoliv v pouze v kontextu České republiky. Ačkoliv v českém právním řádu majoritní část chování spojených s internetovým pirátstvím není nijak perzekuována (jde prakticky o všechny druhy nakládání s autorskými díly pro osobní potřebu, viz. např. § 30 zák. č. 121/2000 Sb.), jedná se ve světovém kontextu spíše o výjimku z pravidla.*

[75] *INSTITUTE FOR INFORMATION LAW. 2018. Global Online Piracy Study. [Online] červenec 2018. [Citace: 14. duben 2021.] https://www.ivir.nl/publicaties/download/Global-Online-Piracy-Study.pdf. str. 23-27*

[76] *ABLON, L. 2018. Data Thieves - The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data. [Online] 15. březen 2018. [Citace: 10. září 2020.] https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT490/RAND_*CT490.pdf. str. 1-5

ničení a narušování kritické infrastruktury nebo systému s následkem újmy na majetku, zdraví či životech. Zpravidla se přitom zaměřují na specifickou zemi, sektor nebo organizaci.

První teroristický čin v kyberprostoru byl proveden v roce 1998 militatní separatistickou organizací Tygři osvobození tamilského Ílamu (Tamilští tygři), kteří použili dnes již zastaralou metodu DoS[77] útoku na Srí Lanskou ambasádu, jíž zahltili tisícovkami e-mailů a přerušili tak její provoz. Ve stejném období probíhala i válka v Kosovu, která je obecně označována jako první ozbrojený konflikt na internetu. [78] Současné teroristické skupiny jako Islámský stát (ISIS) nebo Al-Káida mají své dedikované odnože profesionálních hackerů a dezinformantů, jejichž prostřednictvím získávají tajné informace a propagují hnutí.[79]

Advanced Persistent Threat a státem sponzorované skupiny

Advanced Persistent Threat (APT) je vysoce sofistikovaná skupina pachatelů, zpravidla podporovaná národními státy, případně jinými státními organizacemi. Ti jim poskytují potřebné ekonomické a technologické zázemí, zadávají úkoly a využívají získané informace pro vlastní účely. Tyto skupiny zpravidla používají nejmodernější technologie, vyvíjejí vlastní nástroje a operují v utajení. Jejich cílem je dlouhodobý a nedetekovaný přístup do informačních systému oběti. Motivací pro jejich činnost je politický a ekonomický prospěch jejich sponzorů, a proto APT cílí na vysoce významné cíle (vlády států, státní rozvědky, nadnárodní organizace). Jejich činnost zahrnuje sběr citlivých informací, krádeže duševního vlastnictví, kompromitace, sabotáže kritické infrastruktury a kompletní převzetí informačních systémů oběti. Typický ATP útok má 5 fází:[80]

1. Výběr cíle, identifikace zranitelnosti, získání přístupu
2. Splynutí s napadeným informačním systémem
3. Eskalace přístupových práv
4. Rozšíření na všechny dostupné zdroje
5. Perzistence (setrvání, pozorování a sběr informací)

Stále častější je tzv. supply chain útok, kdy tyto skupiny místo přímého útoku na oběť cílí na jejich dodavatelský řetězec (Společnosti vyvíjející software nebo výrobci hardware). Útoky na dodavatele jsou pro APT velice perspektivní. Oběti s dodavateli mají již navázaný vztah důvěry

[77] DoS (Denial of Service) – Útok spočívající ve způsobení nedostupnosti koncové služby

[78] STERGIOU, D a GIANTAS, D. 2018. From Terrorism to Cyber-terrorism: The Case of ISIS. [Online] 7. březen 2018. [Citace: 23. srpen 2020.] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3135927. str. 5

[79] United Cyber Caliphate, Islamic State Hacking Division, Kalashnikov E-Security Team aj.

[80] IMPERVA. Advanced persistent threat (APT). Learning center. [Online] [Citace: 23.srpen 2020.] https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/.

a neočekávají z jejich strany útok. Navíc lze předpokládat, že přes jednoho dodavatele bude napadeno velké množství jeho odběratelů (například aplikace CCleaner od společnosti Avast byla za dobu své kompromitace stažena 2 270 000 krát[81], z čehož činila podstatnou část stažení v rámci korporátních počítačových sítí).

Pro rozlišení mezi APT a kyberteroristy je vhodné se zaměřit na motivaci, cíle a vztah k případné mediální publicitě. Motivací APT je politický prospěch státu nebo státní organizace. Kyberteroristi oproti tomu tíhnou k propagaci své extremistické agendy. APT zpravidla operují tajně, ke svým aktivitám se na rozdíl od kyberteroristů nehlásí. Příslušnost ATP skupin k útoku často nikdy není zjištěna a pokud ano, tak pouze na základě forenzního vyšetřování. Většina APT skupin proto nemá ani vlastní oficiální název, ale pouze číselné označení[82], které jim bylo přiřazeno vyšetřovateli pro potřeby další identifikace. Ačkoliv oba typy pachatelů používají pro dosažení svých cílů destruktivní metody, v případě APT se jedná pouze o prostředek, zatímco u kyberteroristů je cílem samotné zničení.[83]

Pro ilustraci těchto rozdílů poslouží počítačový vir Stuxnet, který v roce 2010 způsobil ochromení Íránského jaderného programu. Stuxnet nejprve napadl řídící systémy centrifug na obohacování uranu a následně způsobil jejich zničení změnou konfiguračních parametrů.[84] I přesto, že byly v tomto případě použity destruktivní metody, jednoznačnou motivací pachatele bylo odstranění jaderné hrozby na Blízkém východě. K oficiální identifikaci pachatele nikdy nedošlo, a právě proto padá primární podezření díky výše zmíněné motivaci na APT skupinu s kořeny v USA nebo Izraeli.

Organizované zločinecké skupiny

Ústřední motivací těchto pachatelů je majetkový prospěch. Oběťmi jejich útoku jsou objekty s podstatným finančním nebo informačním kapitálem (obchodní korporace, státní správa). Vývoj vlastních nástrojů pro tyto pachatele není prerekvizitou. Velká část jich je dnes dostupná na deepwebu a darkwebu, nebo vyžaduje pro své nasazení minimální zdroje (např. sociální inženýrství). Kromě obchodu s hackerskými nástroji je v současnosti běžnou praxí i poptávání

[81] *FIREEYE. 2020. M-Trends Report. [Online] 2020. [Citace: 8. září 2020.] https://content.fireeye.com/m-trends. str. 21-26*

[82] Viz. např. Veřejně dostupná databáze APT skupin MITRE ATT&CK®

[83] *FIREEYE. 2019. Double Dragon. APT41, a dual espionage and cyber crime operation. [Online] 2019. [Citace: 22. leden 2021.] https://content.fireeye.com/apt-41/rpt-apt41/.*

[84] *CENTER FOR SECURITY STUDIES. 2017. Hotspot Analysis: Stuxnet. [Online] Říjen 2017. [Citace: 10. únor 2021.] https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-04.pdf.* str. 5-12

specifických zakázek a nábor členů[85]. Populárním nástroji jsou již zmiňovaný ransomware, hacking a phishing. Cílem útoku je buď přímý finanční zisk vyvoláním nelegitimního peněžního převodu, získání jiného informačního kapitálu pro následné zpeněžení (například krádež čísel kreditních karet a následný prodej na internetu, krádež obchodního tajemství) nebo obstarání informací pro jinou následnou formu podvodu.

Specifickou organizovanou skupinou pachatelů jsou falešná call centra (85 % těchto organizací sídlí v Indii.[86,87]). Tyto skupiny pod záminkou fiktivní technické podpory donutí uživatele k instalaci viru nebo nástroje pro vzdálenou správu počítače. Hojně k tomu využívají především vishing[88]. Efektivita vishingu je podpořená skutečností, že Indie je také sídlem většiny legitimních callcenter nadnárodních technologických společností. Zajímavé je, že se tato callcentra navenek nijak neliší od těch legitimních. Mají mnohdy pronajmuty oficiální prostory, telefonní linky, zaměstnance a definovanou organizační strukturu. Jako u všech druhů kybernetické kriminality i zde k úspěchu pachatelům napomáhá internetová anonymita. Ta je navíc podpořená faktem, že i v případě úspěšné identifikace existuje minimální šance na jejich dopadení. Útoky totiž směřují na oběti v zahraničí a ambice mezinárodních policejních orgánů na dopadení útočníků v Indii nejsou vysoké. Běžnou praxí navíc je, že tyto skupiny jsou chráněny i před policejními orgány přímo v Indii, a to díky rozsáhlé korupci tamnější státní správy[89,90]. Tento druh trestné činnosti má navíc dopad nejen na přímé oběti, ale také na legitimní společnosti, za jejichž podporu se pachatelé vydávají (Microsoft, Google, Adobe). Tyto subjekty se snaží bojovat s falešnou technickou podporou vlastními prostředky[91].

Hactivists

Hactivismus je forma společenského aktivismu v prostředí kybeprostoru. Hacktivisté upozorňují na řadu sociálních, politických a ekonomických problémů, formulují i šíří svou agendu

---

[85] *PAGANINI, P. 2019. Hacking communities in the Deep Web. [Online] 15. leden 2019. [Citace: 27. srpen 2020.] https://resources.infosecinstitute.com/hacking-communities-in-the-deep-web/.*

[86] *BERG-GANZARAIN, J. Inside the Tech Support Scam Ecosystem. Pindrop Blog. [Online] Pindrop. [Citace: 27. srpen 2020.] https://www.pindrop.com/blog/inside-the-tech-support-scam-ecosystem/.*

[87] *MICROSOFT. 2018. Global Tech Support Scam Research. [Online] září 2018. [Citace: 27.srpen 2020.] https://news.microsoft.com/uploads/prod/sites/358/2018/10/Global-Results-Tech-Support-Scam-Research-2018.pdf.*

88 Vishing (Voice phishing) – Hlasový phishing, Phishing, jehož hlavním komunikačním kanálem je telefonní nebo internetový hovor

89 THOMAS, K. V. 2004. Police Corruption in India. [Online] 2004. [Citace: 4. únor 2021.] https://www.svpnpa.gov.in/images/npa/Publications/journals/2004janjun.pdf. str. 3-9

[90] *LAMANI, B. R. a VENUMADHAVA, G. S. 2013. Police Corruption in India. International Journal of Criminology and Sociological Theory. 2013, Sv. 6, 4.* str. 228-234

[91] *MICROSOFT DEFENDER ATP RESEARCH TEAM. 2018. Teaming up in the war on tech support scams. Security blog. [Online] 20. duben 2018. [Citace: 27. srpen 2020] https://www.microsoft.com/security/blog/2018/04/20/teaming-up-in-the-war-on-tech-support-scams/.*

a získávají podporu pro svou další činnost. Jejich hlavním cílem je zaměřit pozornost veřejnosti na konkrétní témata (např. boj za lidská práva, transparentnost ústavních činitelů, propagace či potlačení politických stran a hnutí). Pro zdůraznění svého ideologického postoje používají různé formy kybernetické kriminality. Jedná se převážně o krádeže a následné zveřejňování utajovaných informací, útoky na dostupnost webových služeb a doxxing[92].

Hacktivisty dělíme do třech odlišných kategorií podle jejich inklinace k páchání trestné činnosti (neetická vs. nezákonná činnost) a podle charakterových vlastností (hacker-programátor vs. umělec-aktivista). Těmito kategoriemi jsou tzv. political crackers (jednotlivci nebo skupiny páchající trestnou činnost ve formě modifikace či znehodnocení webových stránek, přesměrování URL adres, (D)DoS útoků, sabotáže a krádeže duševního vlastnictví k prosazení politického účelu), performative hacktivists (osoby často s uměleckým pozadím, které propagují svůj politický postoj v kyberprostoru morálně ambivalentními způsoby, ty však zpravidla nejsou trestnou činností) a political coders (programátorsky nadaní jedinci, jejichž cílem je obcházení represivní legislativní regulace). Veřejně poskytují programy, které tuto regulaci činí nevynutitelnou. Trestnost takového jednání je nutno posuzovat v kontextu právního řádu daného státu případ od případu.[93]

Veřejně známým exemplářem tohoto typu pachatele je hacktivistický celek Anonymous, zodpovědný například za dočasné vložení Taiwanu na seznam členských organizací na webové stránce OSN. Anonymous také stál za sérií kybernetických útoků souhrnně známých jako LulzSec a AntiSec, které cílily na soukromé i veřejné instituce. V rámci nich došlo ke zveřejnění hesel, jmen a osobních detailů zaměstnanců společností Fox, Sony Entertainments a PBS, znepřístupnění webové stránky CIA a k publikaci detailů o příslušnících ozbrojených sborů v Arizoně, Missouri a Alabamě.[94]

Insiders

O insiderech mluvíme výhradně v souvislosti s kybernetickou kriminalitou páchanou na právnických osobách. Jedná se o současné nebo bývalé zaměstnance, dodavatele a obchodní

[92] Doxxing - Publikace osobních informací oběti (jméno, adresa, kontaktní údaje, rodné číslo atp.)

[93] *SAMUEL, Whitney A. 2004. Hacktivism and the Future of Political Participation. [Online] September 2004. [Citace: 17. leden 2021.] https://www.alexandrasamuel.com/dissertation/pdfs/Samuel-Hacktivism-entire.pdf. str. 48-97*

[94] *CLULEY, G. 2013. Naked Security. The LulzSec hackers who boasted they were "Gods" await their sentence. [Online] Sophos, 16. květen 2013. [Citace: 7. září 2020.] https://nakedsecurity.sophos.com/2013/05/16/lulzsec-hackers-wait-sentence/.*

partnery, kteří zneužijí svůj legitimně nabytý přístup nebo znalosti k páchání trestné činnosti.[95] Tyto osoby můžeme podle jejich motivace rozdělit na insidery z pomsty, příležitostné a profesionální.[96] Motivace pomstou bývá zpravidla iniciována předchozím negativním vztahem zaměstnanec - zaměstnavatel (např. disciplinárním řízením, změnou pracovní náplně, či ukončením pracovního poměru). Cílem tohoto druhu insiderů není osobní prospěch, ale prosté poškození oběti. Klasickou formou pomsty je zveřejnění obchodního tajemství anebo útoky na dostupnost informačního systému. Příležitostným insiderem rozumíme zaměstnance, který pojal myšlenku na spáchání trestného činu až v souvislosti s tím, že se o příležitosti dozvěděl během existujícího pracovního poměru či jiného smluvního vztahu s obětí. Příležitostní insideři jsou svedeni potenciální možností osobního prospěchu, která vyplývá z jejich znalosti firemních procesů. Rizikové jsou především pozice, které mají v pracovní náplni elektronické peněžní operace a manipulaci s informacemi v různém stupni utajení. Profesionální insideři mají shodné cíle (majetkový či jiný osobní prospěch). Dělícím znakem je ovšem jejich úmysl spáchat trestný čin ještě před uzavřením pracovního poměru nebo jiného smluvního vztahu s obětí. V souvislosti s profesionálními insidery evidujeme na dark webu platformy poskytující insider trading jako službu.[97] Tyto stránky poskytují předplatitelům informace, které by za jiných případů byly předmětem obchodního nebo bankovního tajemství.[98] Takové informace lze následně přímo zpeněžit (v rámci burzovních operací nebo jiných investičních rozhodnutí) nebo využít k vedení konkrétního druhu útoku na zranitelnosti informačních systémů a procesů.

Script Kiddies

Pojem Script kiddies má prameny v raných dobách internetu[99]. Označení původně vzniklo jako pejorativní pojmenování pro programátory a hackery začátečníky. Tyto osoby typicky nemají hlubší znalost potřebnou k vývoji vlastních hackerských nástrojů a metod. Uchylují se proto ke kopírování či nákupu již zveřejněných nástrojů. Označení kiddie („děcko“) má dvojí kontext. Prvním je zmiňovaný amaterismus pachatelů. Sekundární význam víceméně vyplývá

[95] *SLOAN, R. 2020. Companies Name One of the Biggest Cybersecurity Threats: Their Employees. [Online] The Wall Street Journal, 21. červen 2020. [Citace: 8. září 2020.] https://www.wsj.com/articles/companies-name-one-of-the-biggest-cybersecurity-threats-their-employees-11592606115.*

[96] *AUSTRALIAN CYBER SECURITY CENTER. 2020. Malicious insiders. ACSC. [Online] 23. červen 2020. [Citace: 8. září 2020.] https://www.cyber.gov.au/acsc/view-all-content/threats/malicious-insiders.*

[97] *MINDER, K. 2020. DarkReading. How the Dark Web Fuels Insider Threats. [Online] 23. duben 2020. [Citace: 8. září 2020.] https://www.darkreading.com/endpoint/how-the-dark-web-fuels-insider-threats/a/d-id/1337599.*

[98] *PONEMON INSTITUTE. 2019. The Cost of Cybercrime. [Online] 2019. [Citace: 20. listopad 2020.] https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf.*

[99] *LIVEOVERFLOW. 2019. The Origin of Script Kiddie - Hacker Etymology. LiveOverflow Blog. [Online] 12. květen 2019. [Citace: 8. říjen 2020.] https://liveoverflow.com/the-origin-of-script-kiddie-hacker-etymology/.*

z doslovného překladu „Script kiddies“ jsou zpravidla mladistvé osoby mužského pohlaví. Ti buď postupem času takových aktivit zanechají, nebo zdokonalí svoje schopnosti natolik, že se z nich stanou profesionální hackeři. Script kiddies ve snaze sklidit uznání často veřejně publikují svoje snahy a úspěchy na sociálních sítích. Vzhledem k demografickému složení této skupiny pachatelů je velice častá záliba ve videohrách, kde se realizují pácháním trestné činnosti. Ta je motivována osobní pomstou, případně snahou o osobní prospěch. Typickým útokem je například DDoS útok nebo doxxing, méně častěji pak pokusy o infekci počítače oběti pomocí veřejně známých virů či RAT[100].

Lidské chyby interních uživatelů

I přesto, že uživatelské chyby nelze považovat za typ pachatele v pravém slova smyslu, jejich původci významně usnadňují páchání kybernetické kriminality. Lidská chyba je hlavní příčinou 23 % všech narušení bezpečnosti dat ve firmách[101]. Jedná se o případy, kdy konání uživatele vede ke kompromitaci informačního systému v důsledku jeho nesprávného postupu při práci s informačním systémem. Jde například o situace, kdy uživatel ve snaze ulehčit si práci stáhne z internetu a otevře na svém počítači program, který ve skutečnosti obsahuje škodlivý kód, jehož pomocí dojde k zavlečení viru do firemní sítě. Obdobně jde o nedbalostní úniky citlivých dat vztahujících se k přístupu nebo zranitelnostem informačních systémů (např. ztráta deníku zapsaných uživatelských hesel), či nesprávné administrativní praktiky správců informačních systémů, nebo bezohlednost k bezpečnostním praktikám při vývoji software. Běžnou praxí manažerů kybernetické bezpečnosti je přistupovat k výše zmíněným situacím stejně jako k pokusům o externí průnik a bránit se adekvátními opatřeními, které riziko kybernetického bezpečnostního incidentu sníží (např. školení uživatelů na téma kybernetické bezpečnosti), nebo úplně odstraní (implementace technických opatření či jiných kontrolních mechanismů, které uživatelské akci zamezí).

1.5 Oběti

Pro správné porozumění spojení „oběť kybernetické kriminality“ je nutné jej definovat nejen ve vztahu k českému právnímu řádu, ale také vůči existující literatuře a empirickým zdrojům. V zákoně č. 45/2013 Sb., Zákon o obětech trestných činů, ve znění pozdějších předpisů je definována oběť výhradně jako:

[100] *RAT (Remote Access Tools) – Softwarové nástroje pro vzdálenou správu počítače*
[101] *IBM SECURITY. 2020. Cost of a Data Breach Report. IBM.com. [Online] červenec 2020. [Citace: 19. listopad 2020.] https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/pdf.*

„Fyzická osoba, které bylo nebo mělo být trestným činem ublíženo na zdraví, způsobena majetková nebo nemajetková újma nebo na jejíž úkor se pachatel trestným činem obohatil.“ Zákon dodává, že „*každou osobu, která se cítí být obětí spáchaného trestného činu, je třeba považovat za oběť, nevyjde-li najevo opak nebo nejde-li zcela zjevně o zneužití postavení oběti podle tohoto zákona*“.

V případě kybernetické kriminality je běžné, že je trestná činnost vedena vůči organizacím jako celkům, a to na základě jejich perspektivity z hlediska potenciálního majetkového zisku, zároveň však bez zřetele ke konkrétním fyzickým osobám, například zaměstnancům či faktickým vlastníkům finančních aktiv. Dá se předpokládat, že ve snaze zabránit v takové situaci existenci trestného činu „bez oběti“ dojde na redundantně komplexní právní konstrukce s cílem najít oběť - fyzickou osobu (například akcionáře atp.). Je nutno zmínit, že pro potřeby definice entity, které byla způsobena újma trestnou činností existuje v § 43 trestního řádu pojem poškozený, ten je však vyhrazen pouze trestnímu řízení. Vzhledem k výše uvedenému je proto dána v následujících kapitolách přednost viktimologickému pojetí pojmu oběť (osoba, organizace, morální nebo právní řád, které jsou ohroženy, poškozeny nebo zničeny trestným činem[102]). Protože statistiky Policie ČR ani Institutu pro kriminologii a sociální prevenci nesledují komplexně distribuci a typologii obětí kybernetické kriminality, je nutné hledat podklady pro analýzu v zahraničním výzkumu. Tyto zdroje běžně zahrnují do obětí korporace, veřejnou správu a jiná společenství.

1.5.1 Fyzické osoby

Údaje o počtu obětí se do značné míry liší podle jejich zdroje a podle druhu kybernetické kriminality. Například podle celoevropské studie Reep-van den Berg et Junger z roku 2018 mají největší zastoupení oběti malware (2 - 15 % celkové populace za rok) a hackingu (1,2 % - 5,8 % celkové populace za rok). Vyrovnané zastoupení mají oběti podvodu při online nakupování (0,6 - 3,5 % celkové populace za rok), podvodných internetových bankovnictví a plateb (0,4 - 2,2 % celkové populace za rok) a jednoho z druhů kyberšikany (v součtu 3 %, z toho nejvýznamnější zastoupení má stalking 0,7 - 1,1 % a nebezpečné vyhrožování 0,6 - 1 %). Relativně nízké zastoupení mají oběti všech ostatních druhů podvodných jednání na internetu jako například krádeže identity či podvodů na online seznamkách (v součtu 0,4 %).

Viktimizační studie na území ČR se kybernetickou kriminalitou zabývají pouze na úrovni vybraných druhů jednání. Podle údajů ze zprávy Institutu pro kriminologii a sociální prevenci

[102] *GÖPPINGER, H. 1980. Kriminologie. Mnichov : Beck, 1980. ISBN 9783406073434. str. 589.*

z roku 2019[103] má zkušenost s podvodem při online nakupování 15,6 % populace ročně, což mírně překračuje celoevropský průměr. Se stalkingem v prostředí kyberprostoru se setkalo v ČR cca 2,8 % populace ročně. Posledním sledovaným jednáním byly tzv. podvodné emaily, jejichž obětí se stalo za stejný časový úsek 6,4 % respondentů. Studie potvrzuje, že tyto druhy kybernetické kriminality na fyzických osobách působí relativně nízkou škodu (v průměru 2300,- Kč pro online nákup a 7000,- Kč pro podvodné emaily). Pro srovnání s jinými druhy kriminality stejný zdroj uvádí, že 34 % respondentů se za poslední 3 roky stalo obětí trestného činů mimo kategorie internetových deliktů.

Roli v rozdílné míře viktimizace mezi jednotlivými státy hraje i celková digitalizace společnosti, především pak dostupnost internetu v domácnostech. V České republice mělo za rok 2019 internet doma podle dat ČSÚ[104] 87 % všech obyvatel, což je z hlediska ostatních členských států EU lehce pod průměrem (88,3 %). Při rozřazení dotazovaných na skupiny podle jejich věku je patrná korelace dat s údaji o dostupnosti internetu v domácnosti. Největší podíl na obětech podvodného nakupování mají podle Roubalové a kol. mladí lidé do 30 let a studenti, a naopak nejnižší zastoupení mají osoby v důchodovém věku. Rozdíl lze vysvětlit odlišným přístupem starší generace k používání internetu. Zatímco v domácnostech do 40 let věku je internetové připojení samozřejmostí (97,8 %), v domácnostech nad 65 let je to pouze 41,3 %. Podobnou věkovou distribuci Roubalová a kol. pozorovala i u podvodných emailů. Zajímavé je, že nejvíce podvodných zpráv obdrželi vysokoškolsky vzdělaní muži a podnikatelé. Fenomén lze vysvětlit několika způsoby. Při pohledu na distribuci přístupu k internetu podle příjmů je zřejmé, že nejméně zastoupené jsou oběti s nižším příjmem (50,4 % pro první kvintil vs. 98,8 % pro pátý kvintil). Dalším faktorem může být, že tyto osoby jsou díky svoji perspektivní kariéře v prostředí internetu více exponovány (posílají e-maily více adresátům, jejich kontaktní údaje jsou publikovány v ročenkách či reklamních materiálech atd.), čímž může dojít k zneužití jejich e-mailové adresy v rámci crawlery[105] nebo v rámci sběru informací nástroji OSINT[106]. Posledním vysvětlením může být vědomá iniciativa pachatele, který svá jednání cílí na nejperspektivnější cíle (typicky pro spear-phishing).

---

[103] *ROUBALOVÁ, M. a kol. 2019. Oběti kriminality - Poznatky z viktimizační studie. Praha : Institut pro kriminologii a sociální prevenci, 2019. ISBN 9788073381745.*

[104] *ČESKÝ STATISTICKÝ ÚŘAD. 2020. Informační společnost v číslech. [Online] 2020. [Citace: 2. březen 2021.] https://www.czso.cz/csu/czso/informacni-spolecnost-v-cislech-2020.*

[105] *Crawler – počítačový program na automatizovaný sběr dat z internetu*

[106] *OSINT (Open Source Intelligence) – Volně dostupné informační zdroje (např. sociální media, Google dorking, televize, rádio, specializované služby typu Shodan.io apod.)*

Relativně nízkou nebezpečnost kybernetické kriminality pro fyzické osoby shrnuje na závěr studie Roubalová a kol. takto: *„ Výsledky průzkumu ukázaly, že využívání internetu je běžnou součástí života napříč populací, i když z hlediska intenzity se jeví jako významný zejména věk a sociální status uživatele. Výsledky naznačují, že i když se podvodná jednání v kyberprostoru vyskytují, aktivity na internetu nepředstavují pro respondenty zásadní nebezpečí a tyto nepoctivé činnosti se svou frekvencí zásadně nevymykají porovnání s jinými druhy sledované trestné činnosti (zejména co se týče incidentů s výší škody zakládající trestnou odpovědnost). Tyto výsledky zároveň odpovídají zjištěním z výzkumů, realizovaným na toto téma v zahraničí (srovnatelné např. Domenie, 2013). Pokud se respondenti už obětí podvodu stanou, snaží se tuto situaci většinou aktivně řešit. Demografické faktory se přitom z hlediska rizika viktimizace neukázaly jako významné.“*[107]

1.5.2 Právnické osoby

O tom, že kybernetická kriminalita je převážně zaměřena na právnické osoby svědčí celková výše nákladů spojených s kybernetickou kriminalitou. Podle zprávy Institutu pro kriminologii asociální prevenci[108] činí náklady vládních a podnikatelských subjektů 85 % veškerých nákladů spojených s kybernetickou kriminalitou. Počet ohlášených kybernetických incidentů na právnických osobách je ve srovnání s fyzickými osobami nižší, ale jejich závažnost je vyšší. Pro srovnání za rok 2019 eviduje Policie ČR spáchání 8417 trestných činů v kyberprostoru. Za stejné období bylo podle zprávy o stavu kybernetické bezpečnosti Národnímu úřadu pro kybernetickou bezpečnost ohlášeno 217 incidentů. Stejný zdroj uvádí jako častý cíl kybernetických útoků státní a územní samosprávu, poskytovatele kritické infrastruktury, finanční sektor, zdravotnictví a akademické instituce.

O rostoucím riziku kyberkriminality v organizacích svědčí také pozitivní trend v alokaci rozpočtu pro boj s kybernetickou kriminalitou. Dle zprávy NÚKIB až 45 % organizací vynakládá v meziročním srovnání více finančních prostředků na boj s kybernetickou kriminalitou, zatímco pouze 5 % jich vynaložené prostředky aktivně snižuje. I přes vzrůstající tendenci až 67 % dotazovaných organizací uvedlo, že navýšení rozpočtu nebylo dostatečné. O nutnosti dále zvyšovat míru prevence v organizacích svědčí fakt, že každý třetí pokus o kybernetický útok na organizaci je úspěšný.

[107] *ROUBALOVÁ, M. a kol, cit. 103, str. 97*
[108] *NOVOTNÝ, Č., VLACH, J. a KUDRLOVÁ, K. 2019. Škody působené kybernetickou kriminalitou. Praha : Institut pro kriminologii a sociální prevenci, 2019. ISBN 9788073381752. str.63*

2. Analýza stavu (metodologická část)

2.1 Výběr zkoumané oblasti

Z předchozích kapitol vyplývá, že míra výskytu a závažnosti kybernetické kriminality na fyzických osobách nevykazuje signifikantní deviaci oproti ostatním druhům kriminality. Oproti tomu ze Zprávy o stavu kybernetické bezpečnosti v České republice za rok 2020[109] je evidentní, že pro právnické osoby se riziko kybernetického zločinu zvyšuje každý rok. Kupříkladu mezi roky 2018 a 2019 narostl počet hlášených bezpečnostních incidentů českými organizacemi o 32 %. Stejný zdroj uvádí jako jeden z nejoblíbenějších cílů bankovní sektor, a to i navzdory nejvyšší průměrné míře zabezpečení ve srovnání s ostatními obory podnikání. Tomuto trendu nasvědčují i celosvětové statistiky. Podle průzkumu společnosti Accenture[110] je několik let po sobě bankovní sektor na prvním místě v průměrné roční škodě způsobené kybernetickou kriminalitou. Skutečnost, že se subjekty finančního trhu stále potýkají s kybernetickým hrozbami, a to i navzdory své nadprůměrné snaze o jejich prevenci, indikuje, že jimi zaměstnané osoby odpovědné za implementaci kybernetické bezpečnosti by měli poskytnout nejrelevantnější vhled do stavu kybernetické kriminality v České republice. Pokud jsou finanční organizace vystaveny největšímu a nejsofistikovanějšímu náporu ze strany kyberzločinců, lze očekávat, že jimi doporučené prevenční mechanismy budou přínosné také pro organizace v jiných odvětvích podnikatelské činnosti či veřejnou správu.

2.2 Příprava rozhovoru

Pro validaci myšlenkových východisek práce byla zvolena výzkumná metoda rozhovoru s odborníky na téma kybernetické bezpečnosti. Základním motivem pro výběr metody byla obava z nedostatečně vypovídajícího výsledku v případě kvantitativního šetření. Vzhledem k tomu, že se autor práce pohybuje v prostředí kybernetické bezpečnosti v rámci svého zaměstnání, nejpřirozenějším vývojem se jevilo kontaktování těch osob, které autor v rámci svého kariérního působení považoval za vysoce kompetentní. Kompetencí je přitom myšlena nejen jejich faktická profesní znalost, ale také reálné zkušenosti dotazovaných se zaměstnáním v organizacích, které jsou nejvíce ohroženy pácháním kybernetické kriminality.

[109] *NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. 2019. Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2019. [Online] 18. září 2019. [Citace: 20. listopad 2020.] https://www.nukib.cz/download/publikace/zpravy_o_stavu/NUKIB_ZSKB_2019.pdf.*

[110] *PONEMON INSTITUTE. 2019. The Cost of Cybercrime. [Online] 2019. [Citace: 20. listopad 2020.] https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf.* str. 12

Při formulaci otázek byl kladen důraz na získání reálných poznatků a zkušeností s prevencí kybernetické kriminality. Z tohoto důvodu byla zvolena forma polostrukturovaného rozhovoru. V rámci přípravy rozhovoru byl vytvořen dokument „Informovaný souhlas účastníka výzkumu“ (*viz. Příloha 1 této práce),* jehož součástí bylo 12 otázek. Znění i pořadí dotazů je zamýšleno především jako tematická kostra verbálního dialogu a není proto rigidní. Informovaný souhlas byl oběma dotazovaným zaslán s výše uvedeným vysvětlením s týdenním předstihem před konáním rozhovoru. Dotazovaní byli v úvodu rozhovoru vyzváni k tomu, aby odpovídali v širších souvislostech a uváděli konkrétní příklady, ze kterých jejich tvrzení vyplývají. Cílem rozhovoru bylo získání co nejširšího penza relevantních praktických poznatků a oba dotazovaní byli instruováni k tomu, aby se neostýchali sdělovat v průběhu rozhovoru vlastní poznatky i za cenu prodloužení původního časového harmonogramu nebo odklonu od osnovy připravených otázek. Z tohoto důvodu reálné znění rozhovoru v některých případech nekopírovalo přesně původní pořadí ani zadání otázek.

Vzhledem k epidemiologickým opatřením z důvodu pandemie COVID 19 byly oba rozhovory vedeny přes internetovou službu Zoom. Výsledná audionahrávka byla podkladem pro zpracování textového přepisu rozhovoru. Textový přepis byl následně zaslán k validaci dotazovaným osobám e-mailem. Kompletní přepis rozhovorů je součástí příloh 2 a 3. Vzhledem k citlivé povaze tématiky kybernetické bezpečnosti jsou názvy současných zaměstnavatelů obou dotazovaných respondentů anonymizovány.

2.2.1 Radek Živný, Organizace 1, nebankovní poskytovatel finančních služeb

Radek Živný působí v oboru přes 20 let. Za svou kariéru pracoval na různorodých pozicích s IT zaměřením. Působil postupně jako správce systému, analytik, programátor a následně specialista na kybernetickou a informační bezpečnost. Od roku 2002 pracoval v jednom z prvních dedikovaných útvarů na kybernetickou bezpečnost v České republice ve společnosti Český Telekom, a.s. Po akvizici Českého Telekomu španělskou společností Telefónica byl přijat na pozici vedoucího informační bezpečnosti (CISO) v O2 Czech Republic, potažmo CETIN (CETIN vznikl jako samostatný poskytovatel fixní a mobilní síťové infrastruktury v roce 2015 oddělením od O2 Czech Republic). Později působil jako bezpečnostní architekt ve společnosti Škoda Transportation a.s. Pan Živný momentálně působí jako specialista informační bezpečnosti u nejmenované organizace (Organizace 1 - nebankovní poskytovatel finančních služeb). Tato organizace patří mezi nejvýznamnější české poskytovatele úvěrů na automobily, spotřební zboží a jiných neúčelových hotovostních půjček na českém trhu a je členem mezinárodní finanční skupiny, což má faktický dopad na její politiku kybernetické bezpečnosti. Důvodem pro výběr

respondenta byla jeho dlouholetá zkušenost s vedením kybernetické bezpečnosti napříč vícero odlišnými sektory (telekomunikace, doprava, finance) a dále jeho školící činnost v oblasti hackingu. Autor práce byl zaměstnán do roku 2020 v Organizaci 1 na pozici specialisty informační bezpečnosti. Zaměstnavatel byl během trvajícího pracovního poměru informován o záměru autora psát diplomovou práci na téma kybernetické kriminality a souhlasil s ním.

2.2.2 Jan Beránek, Organizace 2, bankovní poskytovatel finančních služeb

Jan Beránek působí jako Chief Information Security Officer (CISO) od roku 2010. Od roku 2020 je zaměstnán na stejné pozici v nejmenované organizaci (Organizace 2 - bankovní poskytovatel finančních služeb). Jedná se o českou banku s celostátní působností zaměřenou na individuální i korporátní bankovnictví. Také v předchozím zaměstnání pana Beránka se jednalo o finanční instituci. Důvodem pro výběr respondenta byla jeho dlouholetá zkušenost s kybernetickou bezpečností v sektoru finančních služeb, a to jak v subjektech ryze českých, tak i v těch s kořeny v zahraničí.

Autor práce byl zaměstnán od roku 2020 v Organizaci 2 na pozici specialisty informační bezpečnosti a byl tak přímým podřízeným pana Beránka. Zaměstnavatel byl informován o záměru autora psát diplomovou práci na téma kybernetické bezpečnosti a souhlasil s ním.

3. Preventivní opatření (praktická část)

Podle Ministerstva vnitra[111] se systém prevence kriminality v České republice dělí podle šíře okruhu adresátů na tři úrovně.

Na nejobecnější úrovni stojí primární prevence kriminality. Ta je realizována především výchovnými a vzdělávacími aktivitami zaměřenými na širokou veřejnost. Odpovědnost za výkon primární prevence nese rodina, školy a další lokální společenství.

Sekundární prevence je zaměřena na jedince a skupiny osob se zvýšeným rizikem pachatelství nebo viktimnosti. Náplní sekundární prevence je minimalizace sociálně patologických jevů a kriminogenních situací.

Terciární prevence se soustředí na resocializaci osob, které trestnou činnost fakticky páchaly, nebo jí byly postiženy. Motivací je zabránění recidivy v souvislosti s návratem kriminálně narušených osob zpět do svého běžného sociálního prostředí a udržení jejich pozitivního společenského profilu.

Cílem této kapitoly je doporučení preventivních opatření v boji s kybernetickou kriminalitou, popsání jejich výhod a nevýhod, vymezení jejich vzájemné pozice ve strategii kybernetické bezpečnosti organizací a zařazení těchto mechanismů do existující struktury prevence kriminality. Následující podkapitoly lze chápat jako součást sekundární prevence.

3.1 Sociální prevence

Sociální prevence je aktivita zaměřená na minimalizaci primárních příčin pro páchání trestné činnosti. Specifika výkonu sociální prevence upravuje § 53 a násl. zákona č. 108/2006 Sb., Zákon o sociálních službách, ve znění pozdějších předpisů. Z dřívějších kapitol této práce vyplývá, že motivace pachatelů k páchání kybernetické kriminality se od ostatních druhů trestné činnosti nijak zásadně neliší a lze proto aplikovat totožné sociálně preventční mechanismy. Tento fakt je ve spojení s tím, že efektivita sociální prevence je do značné míry neměřitelná hlavním důvodem, proč se předmětná diplomová práce sociální prevenci kybernetické kriminality dále nevěnuje.

3.2 Situační prevence - režimová ochrana

Specifickým rysem režimové ochrany při prevenci kybernetické kriminality je zásadní role tuzemských a zahraničních institucí specializovaných na kybernetickou bezpečnost. Z tuzemských lze zmínit Národní úřad pro kybernetickou bezpečnost či Národní CSIRT České republiky.

[111] *MINISTERSTVO VNITRA ČR. 2021. Prevence kriminality. [Online] 2021. [Citace: 1. červen 2021.] https://www.mvcr.cz/clanek/web-o-nas-prevence-prevence-kriminality.aspx?q=Y2hudW09Mw%3d%3d.*

Celosvětové uznávanými jsou například Mezinárodní organizace pro normalizaci (ISO) či americký National Institute of Standards and Technology (NIST). Jejich hlavním posláním je kromě obecné osvěty tvorba standardizovaných referenčních rámců pro zabezpečení informačních systémů. Výsledkem činnosti zmíněných institucí je souhrn kolektivního povědomí o nejsprávnějších a nejefektivnějších bezpečnostních opatřeních a postupech. Tento soubor doporučení bývá označován jako best practice. Organizace by měla v rámci svých schopností implementovat doporučení do interních předpisů a procesů.

3.2.1 Analýza rizik

Analýza rizik je základním předpokladem pro vytvoření funkční strategie informační a kybernetické bezpečnosti organizace. Výstupem analýzy je identifikace aktiv a jejich zranitelností (souhrnně označováno jako hrozby). Hrozbám je následně přiřazena váha podle míry jejich pravděpodobnosti a potenciální škody. Pro provedení analýzy existují standardizované metodiky jako například norma ISO/IEC 27005:2018 Information technology - Security techniques - Information security risk management.

V závislosti na výsledku analýzy rizik organizace volí mitigační mechanismy (viz. podkapitoly níže). Kromě faktického opatření je vhodné přiřadit preventivnímu mechanismu také vlastníka a specifické parametry jako čas potřebný pro provedení postupu, či další zainteresované osoby a navazující procesy. Rozsah analýzy rizik je přímo úměrný různorodosti činností dané organizace, proto je nutné katalog rizik periodicky aktualizovat. Jednou z možností, jak toho docílit je navázání rizikové analýzy na procesy řízení projektů. Tím je zaručeno, že veškeré nové aktivity budou do budoucna zohledněny a patřičně zabezpečeny ještě před nasazením do provozu.

3.2.2 Interní předpisová základna

Interní předpisy organizace musí reflektovat žádoucí stav kybernetické bezpečnosti. Pro formalizaci bezpečnostních požadavků existuje vícero důvodů. Tím hlavním je, že standardizace bezpečnostních požadavků napříč celou organizací snižuje administrativní zátěž, a to jak při sdělování informací uživatelům, tak při řešení uživatelských požadavků. Sekundárním přínosem je možnost represe v případě neplnění povinností plynoucích z takového předpisu, či přenos know-how během organizačních změn.

Při tvorbě předpisů je vhodné cílit potřebné informace pouze na předem určený okruh adresátů, v opačném případě hrozí, že se koncový uživatel kvůli rozsahu materiálu s nimi dostatečně neseznámí. Z tohoto důvodu některé organizace kategorizují předpisy podle okruhu adresátů do vícero úrovní. Předpisy týkající se obecných povinností koncových uživatelů jsou

dostupné pro všechny, konkrétní postupy pro řešení vyjmenovaných událostí jsou dostupné pro specifické osoby. V určitých případech existuje potřeba formalizace tajných informací (například detaily konfigurace či přístupové údaje). Zde je nutné zajistit, že k předpisu nebude mít přístup nikdo vyjma osob odpovědných za kybernetickou bezpečnost. V interním předpise by měly být pokryty minimálně oblasti týkající se přístupu k informačnímu systému, práce s výpočetní technikou pro uživatele a privilegované účty, řešení bezpečnostních incidentů, přístupu a nakládání s informacemi, školení uživatelů a bezpečnostních kontrol.

Nutno podotknout, že interní předpisy jsou cíleny především na chování interních uživatelů a jejím cílem je minimalizace prostoru pro lidskou chybu. Existence dostatečně robustní předpisové základny sice svědčí o tom, že organizace dbá na udržení kybernetické bezpečnosti a je také často poptávána během auditních šetření, nicméně externí útočník předpisem není nijak dotčen.

3.2.3 Bezpečnost vývoje

Pro organizace ve finančním sektoru je typické, že velká část jejich činnosti je závislá na funkcionalitě několika klíčových aplikací. Jedná se především o core banking systémy, CRM[112], DMS[113], CMS[114] a reportovací workflow. Ať už jsou tyto aplikace dodávány v rámci vývoje na míru nebo jako stávající produkt, platí, že v průběhu času je nutné je aktualizovat či úplně nahradit. Vzhledem k rozsahu aktivit spojených s danými aplikacemi je tento proces relativně rizikový. Organizaci hrozí nebezpečí výpadku dostupnosti, ztráty či úniku citlivých dat, či poškození reputace u klientů v důsledku suboptimální náhrady. Pro hladký průběh výměny takového systému je nutné podrobně zpracovat zadání business funkcí a technických i bezpečnostních požadavků. Jako základní východisko pro bezpečný vývoj aplikace lze použít veřejně dostupné metodiky. Významným autorem best practice pro bezpečný vývoj je OWASP[115] Foundation, která stojí za publikací metodik OWASP Top 10 nebo OWASP Mobile Application Verification Standard. Dalším z nástrojů pro zvýšení bezpečnosti vývoje je revize zdrojového kódu. Ta může probíhat jak interně ze strany zákazníka či dodavatele, tak externě, zpravidla v rámci zpoplatněné služby poskytované třetí osobou. Cílem revize je odhalení chyb v dodávané

[112] CRM (Customer Relationship Management) – Aplikace pro efektivní řízení vztahu se zákazníky. Obsahuje osobní informace o klientech, jejich závazky k organizaci, historii transakcí atd. Např. Microsoft Dynamics, Helios CRM.
[113] DMS (Document Management System) – Aplikace pro centrální správu dokumentů. Slouží pro správu elektronické podoby různých druhů dokumentů. Např Software602 Digitální Archiv, Autodesk Vault, Microsoft Sharepoint
[114] CMS (Content Management Systém) – Aplikace pro tvorbu a správu digitálního obsahu. Aplikace, která umožňuje koncovým uživatelům publikovat obsah bez zásahu administrátora. Např. WordPress, Drupal,, Joomla.
[115] OWASP (Open Web Application Security Project) – Nezisková organizace jejímž cílem je globální zvýšeni bezpečnosti software.

aplikaci před nasazením do produkce a také tlak na dodržení dohodnuté úrovně vývoje ze strany dodavatele. Pro zajištění bezpečnosti aplikace po nasazení do infrastruktury organizace se provádí penetrační testy. Testy lze opět provádět jak interně, tak skrze specializované externí subjekty. Pointou penetračního testu je to, že k implementovanému systému je záměrně připuštěn white-hat hacker. Ten má za cíl odhalit zranitelnosti konkrétní implementace, ať už se jedná o chyby v samotné aplikaci, či v konfiguraci prvků, na kterých tato aplikace běží. Podle rozsahu informací, které jsou white-hat hackerům poskytnuty je dělíme na black-box (najmutý hacker neví o systému nic a musí všechno zjistit sám), grey-box (hackerovi je poskytnuta pouze část klíčových informací, např. názvy serverů nebo jejich operační systém) a white-box (poskytnuta je celá technická dokumentace) testy. Výsledkem penetračních testů je koncová zpráva se souhrnem nalezených zranitelností. Tato slabá místa je vhodné opravit před nasazením dodávaného řešení do produkce. Obě organizace provádějí penetrační testy všech nově dodávaných aplikací, a to i pokud se jedná o pouhou aktualizaci. Zároveň provádí každý rok pravidelný test veškerých aplikací s přístupem do internetu.

3.2.4 BCP a DRP

BCP[116] je soubor kroků a opatření, díky kterým může organizace fungovat i v krizovém režimu. Důvodem pro krizový režim může být například živelná katastrofa, nebo válečný stav. Z hlediska kyberkriminality se může jednat o nedostupnost informačního systému v důsledku kybernetického incidentu. V rámci kybernetické bezpečnosti je proto vhodné mít pro případ rozsáhlého výpadku připraven plán, který umožní organizaci vykonávat svoji činnost s co nejmenším dopadem na klientské aktivity. Běžnou součástí plánu je ustanovení krizového výboru, souhrn konkrétních aktivit nutných pro zajištění fungování a seznam osob, které jsou zodpovědné za jejich provedení. Zatímco BCP je aktivitou preemptivní a má za úkol přípravu organizace pro případ krize, DRP[117] je souhrn aktivit v důsledku krize, které mají za cíl co nejrychleji obnovit původní funkčnost organizace. Pokud je kybernetický útok tak rozsáhlý, že má za následek aktivaci DRP, lze předpokládat, že jím bude dotčena podstatná část produkční infrastruktury organizace. Z tohoto důvodu je vhodné mít pro DRP provoz vyhrazenou dedikovanou lokalitu s vlastním IT vybavením. Toto vybavení by mělo být pokud možno co nejvíce odděleno od produkčního prostředí organizace (zabrání se tak např. šíření ransomware). Podle konkrétní

[116] *BCP (Business Continuity Plan) - Plán kontinuity podnikání*
[117] *DRP (Disaster Recovery Plan) – Plán obnovy*

parametrizace RTO[118] a RPO[119] může organizace svojí záložní lokalitu udržovat jako hot site (shodné prostředí s produkcí, které je v kontinuálním provozu, může dojít k okamžitému přesunu provozu), warm site (prostředí obsahuje prvky nezbytné pro plnění DRP, ale k přesunu je nezbytná jejich další konfigurace) nebo cold site (lokalita neobsahuje technické vybavení a je nutný jeho přesun). Obě organizace mají kromě kompletní BCP dokumentace k dispozici DRP warm-site mimo hlavní zaměstnanecké prostory.

3.3 Situační prevence – Fyzická a technická ochrana

Fyzická a technická ochrana je soubor preventivních opatření založených na implementaci bezpečnostních prvků do informačních systémů. Bezpečnostním prvkem rozumíme jakékoliv řešení, které má za cíl mitigaci konkrétního typu útoku. Společným znakem technických a fyzických prevenčních mechanismů je, nezávislost jejich aplikace na vůli koncového uživatele.

Pro účely udržení jasné distinkce mezi fyzickou a technickou ochranou v této práci platí, že fyzickými preventivními opatřeními jsou myšleny veškeré hmatatelné překážky pro páchání trestné činnosti, bez ohledu na to, zda se jedná o faktický fyzický dohled příslušnými osobami nebo zabezpečení objektů mechanickými překážkami. Fyzická ochrana slouží k zamezení neoprávněného fyzického přístupu k informačnímu systému. Funkční fyzická ochrana je základním předpokladem pro návrh a aplikaci technických opatření. Pachatel má v případě překonání fyzické ochrany k dispozici prakticky neomezené množství technik pro průnik do informačního systému, vůči kterým se nelze efektivně bránit technickými opatřeními.

Technická ochrana je soubor preventivních opatření sloužících k prevenci neoprávněného logického přístupu k informačnímu systému. Technická opatření dělíme do tří oblastí:

- Bezpečná konfigurace
- Bezpečnostní software
- Bezpečnostní hardware

Cílem technických opatření je minimalizace prostoru pro lidskou chybu a fungují zpravidla jako nástroj poslední instance.

---

[118] RTO (Recovery Time Objective) – Maximální akceptovatelný časový interval mezi výpadkem systému a jeho opětovnou dostupností. Udává se v hodinách (např. H+12) případně ve dnech (např. D+2)

[119] RPO (Recovery Point Objective) – Maximální akceptovatelný časový interval pro ztrátu dat. K zálohování dat zpravidla nedochází kontinuálně ale pouze v předem stanovených časech. RPO udává kolik času může uplynout mezi poslední zálohou a následnou ztrátou dat. Například při RPO=H-1 je akceptovatelná ztráta dat za poslední hodinu provozu systému.

3.3.1 Bezpečná konfigurace

Bezpečná konfigurace je souhrn nastavení na existujícím IT vybavení (pracovní stanice, servery, síťové prvků), která znemožňuje útočníkovi použít jeho funkce nezamýšleným způsobem. Pro tento druh opatření se někdy používá pojem „hardening“. Zahrnujeme sem vynucení specifické konfigurace operačních systémů, aplikační whitelisting a blacklisting, vynucení bezpečných komunikačních protokolů, minimalizaci uživatelských oprávnění, minimalizaci počtu a segmentaci privilegovaných účtů, šifrování data-in-motion a data-at-rest, vytvoření pravidel pro whitelisting a blacklisting síťového provozu, segmentace sítě a další.

Konfigurace operačních systémů a změna výchozích hodnot

Operační systém počítače obsahuje velké množství konfigurovatelných nastavení, která mají od výrobce předem vyplněné hodnoty tak, aby vyhovovali co nejširšímu spektru uživatelů. Výchozí (default) nastavení jsou veřejně dostupná na internetu v rámci dokumentace k SW/HW. Útočník může tyto výchozí parametry využít pro průnik do informačních systémů (např. zkouší výchozí heslo k administrátorskému účtu, nebo díky znalosti výchozího nastavení antispam filtru ví, jak připravit phishing e-mail, který zaručeně dorazí až k uživateli atd.). Proto je důležité výchozí nastavení ve vhodných případech změnit.

V organizacích je běžné, že uživatel počítač využívá převážně k pracovním účelům a nepotřebuje (nebo přímo nesmí) využívat některé jeho funkce tak, jak výrobce ve výchozím nastavení zamýšlel (například přidávat libovolně uživatele a měnit jejich oprávnění). Organizace může přistoupit také k tomu, že uživateli některé funkce systému úmyslně předpřipraví (např. zmapuje pracovní adresář na síťovém uložišti, přidá oblíbené záložky do internetového prohlížeče atp.), aby zvýšila úroveň uživatelského komfortu a s tím spojenou efektivitu práce. Součástí nastavení operačního systému jsou položky, které určují, jak se bude v určitých potenciálně rizikových situacích počítač chovat (například zda vyžaduje pro přihlášení heslo, jakou má mít heslo komplexitu, jakou úroveň oprávnění má uživatel, jak systém nakládá s certifikáty atd.).

Pro zachování co nejvyšší bezpečnosti platí, že konfigurace operačního systému by měla být v co největší možné míře nastavena automaticky již v rámci instalace počítače (tzv. instalační image), bez možnosti změny uživatelem. Ne všechny konfigurační položky to však umožňují. Například pro nejzastoupenější operační systém pro počítače i servery (Microsoft Windows) proto poskytuje Microsoft grafické rozhrání a seznam šablon pro správu (GPO[120]), které slouží

[120] *GPO – Group Policy Object. Předdefinované konfigurační šablony pro správu operačních systémů Windows*

ke konfiguraci již nainstalovaných systémů. V organizacích obou respondentů se konfigurace systémů řeší přes GPO.

Aplikační whitelisting a blacklisting

Z nekontrolovaného spouštění aplikací na koncových systémech vyplývají pro organizaci bezpečnostních rizika (zavlečení malware, shadow IT, únik citlivých dat, zranitelnosti, porušení licenčních ujednání apod.). Pro minimalizaci těchto rizik zavádí organizace tzv. aplikační whitelist. Whitelisting (obecně) je metoda pro tvoření výjimek v kybernetické bezpečnosti. Výchozím stavem při whitelistingu je systém, ve kterém je vše zakázáno. Výjimku tvoří schválené položky na whitelistu (česky doslova „bílá listina“). Aplikační whitelisting znamená vytvoření seznamu schválených bezpečných aplikací a zakázání spouštění všech aplikací na pracovních stanicích koncových uživatelů a serverech mimo tento seznam. Pro efektivní aplikační whitelisting je nutné provést důkladnou analýzu potřeb koncových uživatelů. Výstupem takové analýzy je tzv. aplikační registr. Aplikační registr by měl obsahovat seznam všech aplikací nutných pro chod organizace, popis účelu aplikace, seznam jejich cílových uživatelů, kontakt na osobu či organizační jednotku odpovědnou za správu a podporu aplikace a business vlastníka aplikace (osoba či organizační jednotka z jejíž iniciativy byla aplikace nasazena).

Příliš restriktivní whitelisting může vést k tomu, že uživatelé nebudou schopni efektivně vykonávat svou pracovní náplň, protože k tomu nebudou mít dostatečné programové vybavení. S opačným případem (příliš rozsáhlý whitelist) se v praxi běžně nesetkáváme. Jednak je tento koncept z podstaty neefektivní (příliš rozsáhlý whitelist je v rozporu s účelem whitelistingu), ale hlavně je nutné vynaložit velké úsilí na jeho vytvoření (whitelist by musel obsahovat obrovské množství nadefinovaných položek). V situacích, kdy organizace není schopná z jakéhokoliv důvodu provést důkladnou analýzu aplikací potřebných pro svůj provoz, je možné zvolit strategii aplikačního blacklistingu. Při blacklistingu je ve výchozím stavu vše povoleno a selektivně se zakazují vybrané položky (zpravidla na základě doporučení nebo zkušenosti). Na blacklistu (černé listině) se nejčastěji objevují aplikace z rizikových kategorií (hry, klienti pro P2P[121] přenos, RAT[122], malware, prokazatelně zranitelné aplikace apod.). Efektivita blacklistingu závisí na tom, s jakou pílí byl blacklist vytvořen a jak často je aktualizován. Při srovnání s whitelistingem se jedná o méně bezpečné řešení (vždy existuje riziko, že blacklist nepojme všechny nebezpečné aplikace na světě).

---

[121] P2P (Peer-to-Peer) – Aplikační architektura pro přenos dat vzájemně mezi jednotlivými účastníky (peery) datových sítí.

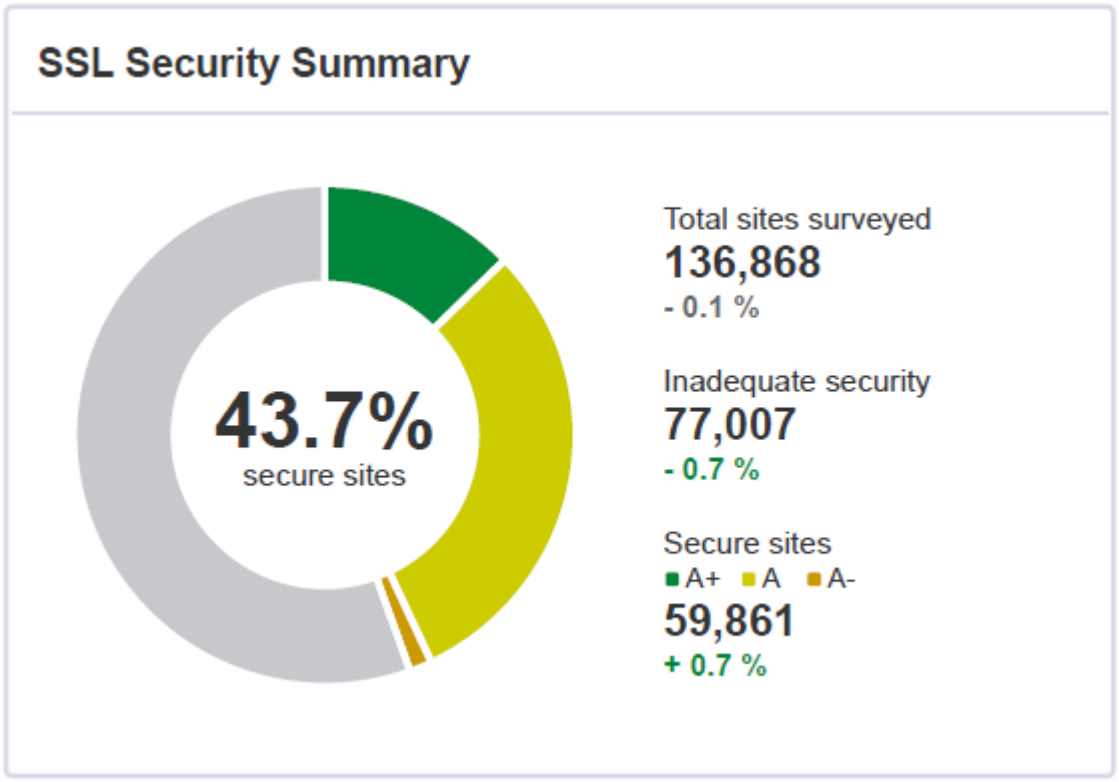
[122] RAT (Remote Access Tools) – Nástroje pro vzdálenou správu počítače

Vynucení aplikačního blacklistu a whitelistu se provádí buď pomocí bezpečnostních endpoint agentů nebo přímo konfigurací operačního systému. Endpoint agent je program nainstalovaný na všech počítačích v organizaci a slouží k vynucení bezpečnostní politiky. Agent v sobě zpravidla zahrnuje vícero funkcí (VPN klient, Anti Virus, Host-Based IPS apod.). Příkladem jsou produkty jako Symantec Endpoint Protection, Check Point Endpoint Security či Sophos Intercept-X. Moderní operační systémy nativně poskytují šablony pro správu a kontrolu běžících aplikací a umožňují tak v omezené míře spravovat tato nastavení *(viz. GPO v kapitole 2.3.1.1).* Organizace 1 aplikuje whitelisting instalovaných aplikací na produkčních serverech, naopak Organizace 2 využívá aplikačního blacklistingu riskware napříč celou infrastrukturou.

Bezpečné komunikační protokoly

Zařízení s přístupem k síti (počítače, síťové prvky, servery) často podporují z důvodu zachování kompatibility vícero druhů komunikačních protokolů. Některé z těchto protokolů mohou obsahovat bezpečnostní zranitelnosti, a proto je nelze považovat za bezpečné (např. TLS[123] verze 1.0). Na tyto zranitelnosti cílí tzv. downgrade[124] útoky. Best practice je všechny nebezpečné a nevyužívané komunikační protokoly zakázat jak přímo na zařízení, tak na síťovém či aplikačním firewallu. Vynucení bezpečnostních protokolů je obzvlášť důležité na prvcích s přímým přístupem do internetu. Podle měsíčních statistik Qualys SSL Labs má v květnu 2021 bezpečně nakonfigurované protokoly pouze 43,7 % webových stránek.[125]

[123] *TLS (Transport Layer Security) – Soubor kryptografických protokolů pro šifrování komunikace na síti. Aktuální verze je 1.3.*
[124] *Downgrade útok je typ útoku, kdy se útočník úmyslně vydává za uživatele se zastaralým zařízením a nutí tak server pro zachování kompatibility zvolit méně bezpečný komunikační protokol.*
[125] *QUALYS SSLLABS. SSL Pulse. [Online] [Citace: 3. června 2021.] https://www.ssllabs.com/ssl-pulse/.*



Graf 1 - Rozložení bezpečnosti webových stránek (Zdroj: Qualys SSL Labs[126])

Minimalizace uživatelských oprávnění

Informační systémy zpravidla umožňují uživateli velký rozsah operací (přístupy k souborům, změna konfigurace systému apod.). Zatímco pro domácí použití je běžné, že koncový uživatel má k dispozici pod jedním účtem veškerá oprávnění pro práci s počítačem, v organizacích se o správu informačního systému stará dedikovaný útvar. Pro běžné uživatele nejsou tato oprávnění nijak využitelná, protože nemají dostatečné znalosti o tom, jak mechanismy fungují. Podle průzkumu v organizaci respondenta připadá na adresářové služby pro autentifikaci uživatelů měsíčně cca 17 % útoků. V případě kompromitace uživatelského účtu dostává útočník k dispozici veškerá oprávnění spojená s účtem, je proto nutné udržovat rozsah oprávnění pouze na operace nutné v rámci běžné každodenní aktivity. Tento přístup je označován jako princip nejnižších oprávnění.

Správa a segmentace privilegovaných účtů

Privilegované účty jsou účty spojené s oprávněními na operace nad rámec běžných uživatelských aktivit (např. právo zápisu do instalační složky operačního systému, právo instalovat

[126] *QUALYS SSL LABS. Cit. 125*

programy, právo vytvářet uživatelské účty atd.). 74 % všech průniků do informačního systému má původ ve zneužití privilegovaného účtu[127], a je proto v zájmu organizace minimalizovat počet takových účtů na minimum.

V průběhu života informačních systémů se vytváří velké množství administrátorských účtů pro aktivity spojené s jejich implementací a správou. Některé účty se prakticky již nepoužívají, nebo jim bylo historicky uděleno zbytečně mnoho oprávnění či nastavené slabé heslo. Best practice pro správu privilegovaných účtů je, že za každý účet by měl mít zdokumentovaný svůj účel a vlastníka. Nezdokumentovaná aktivita privilegovaných účty může v lepším případě znamenat lhostejný vztah IT administrátorů ke správě kmene uživatelů, v horším případě se může jednat aktivitu útočníka, který si vytvořil vlastní účet, nebo převzal identitu účtu již existujícího.

Segmentace účtů znamená rozdělení účtů do skupin na základě jejich společných atributů, účelu, odpovědných majitelů apod. V oblasti privilegovaných účtů je běžnou praxí segmentace podle typu administrátorských aktivit (správa pracovních stanic, správa serverů, správa síťových prvků, správa domény, správa privátních klíčů apod.). Účty v daném segmentu mají možnost přihlašovat se a vykonávat operace výhradně na systémech určených k těmto aktivitám (např. administrátorský účet pro správu koncových stanic musí mít zakázáno přihlášení na všechny systémy vyjma těchto stanic). Zákaz přihlášení lze vynutit na Microsoft-based systémech na úrovni Active Directory[128] objektů (nastavením oprávnění) a GPO (zákazem přihlášení na koncová zařízení), popřípadě lze využít platformy třetích stran pro správu privilegovaných přístupů (produkty typu Wallix Bastion, CyberArk Privileged Access Management apod.).

Šifrování a dat

Nutností pro ochranu dat je jejich zašifrování. Cílem šifrování dat je zaručení jejich důvěrnosti (přístup mají pouze zamýšlení uživatelé), autenticity (data jsou hodnověrná a nebylo s nimi manipulováno) a nepopiratelnosti (data mají původ, který nelze zpochybnit).

Šifrování dat je proces, na jehož vstupu jsou informace v původní podobě (plaintext). Jedná se např. o položky databáze, soubory na pevném disku či soubor s hesly. Na výstupu je stejná informace v podobě, která není čitelná bez znalosti dešifrovacího klíče (ciphertext). K překladu slouží šifrovací algoritmy, což je souhrnný název pro operace nad plaintextem (např. substistuce

[127] *CENTRIFY. 2019. Privilleged Access Management in the Modern Threatscape. Centrify. [Online] 2019. [Citace: 3. červen 2021] https://www.centrify.com/media/4909003/centrify_pam_survey.pdf.*

[128] *Active Directory – Adresářová služba vyvinutá pro počítačové domény Micrososft Windows-based systémů. Obsahuje objekty reprezentující jednotlivé uživatele a počítače, které lze následně shlukovat do skupin a nastavovat nad nimi různé úrovně oprávnění.*

či posun znaků, matematické operace) provedené v předem definovaném sledu jejichž výsledkem je ciphertext. Ačkoliv šifrovacím klíčem může být prakticky cokoliv (např. substituční tabulka, nebo počet pozic o které je posunut plaintext atd.), z praktických důvodů se v moderních informačních technologiích využívají 2 druhy šifrování. Jsou jimi symetrické a asymetrické šifrovací algoritmy.

Symetrické šifrovací algoritmy používají pro šifrování i dešifrování informací stejný klíč. Z tohoto důvodu je pro zachování důvěrnosti symetricky zašifrovaných dat nutné udržet klíč v tajnosti (každý, kdo klíč zná, může data dešifrovat a přečíst, z tohoto důvodu je označován klíč jako privátní). V závislosti na počtu adresátů dat rychle narůstají požadavky na zabezpečenou distribuci privátního klíče. Zároveň nelze zajistit, že recipienti klíč nesdělí dalším neoprávněným osobám. Symetrické šifrování je rychlejší, protože k jeho provedení není potřeba tak vysokého výpočetního výkonu. Z tohoto důvodu se symetrické šifrování používá především pro data at-rest[129]. Konkrétním případem využití je šifrování dat na pevném disku počítače nástrojem Windows Bitlocker. Populárními symetrickými šifrovacími algoritmy jsou Advanced Encryption Standard (AES128, AES256), Data Encryption Standard (2DES, 3DES), Rivest-Cipher (RC2, RC4) nebo Blowfish. Obě dotazované organizace v současné době symetricky šifrují disky pevných stanic.

Výše zmíněný problém s bezpečnou distribucí klíče řeší asymetrické šifrování, někdy nazývané také jako kryptografie veřejných klíčů. Při asymetrickém šifrování se pro šifrování používá klíč veřejný (sdílený se všemi adresáty) a pro dešifrování klíč soukromý (ten má k dispozici zpravidla pouze autor zašifrovaných dat). Tím je zaručeno, že data jsou během přenosu šifrována oběma směry, ale k jejich dešifrování může dojít pouze u adresáta s privátním klíčem. Asymetrické šifrování se používá především pro data-in-motion[130]. Konkrétním příkladem použití je šifrování e-mailové komunikace, kdy odesílatel šifruje e-mail veřejným klíčem adresáta, který už zná (protože je veřejně dostupný, nebo je přenášen v rámci předchozí e-mailové komunikace, např. el. podpisem) a adresát dešifruje vlastním privátním klíčem. V uvedeném scénáři je zamezeno Man-in-the-Middle útokům (útočník nemá k dispozici privátní klíč pro dešifrování, proto odposlechnutá data nemůže přečíst). Populárními asymetrickými šifrovacími algoritmy jsou Rivest-Shamir-Adleman (RSA), Eliptic Curve Cryptography (ECC), Digital Signature Algorithm (DSA) nebo Diffie-Hellman-Merkle Key Exchange (DH). E-mailové

[129] Data-at-rest (česky data v klidu) – Šifrování dat na uložišti, např. šifrování pevných disků (Bitlocker, PGP, Check Point FDE a další), šifrování databází (Transparent Data Encryption), šifrování záloh na páskách apod.
[130] Data-in-motion (česky data v pohybu) - Šifrování dat během jejich přenosu, např. protokol TLS (Transport Layer Security)

brány obou dotazovaných organizací podporují šifrování e-mailové komunikace, pokud to podporuje i strana recipienta.

Základním požadavkem na bezpečnost šifrovacího algoritmu je jeho neprolomitelnost. V historii došlo k několika případům prolomení šifrovacího mechanismu a následnému dešifrování ciphertext bez znalosti šifrovacího klíče. Prolomené šifrovací algoritmy nezajišťují dostatečnou ochranu dat, a proto jejich použití v informačních systémech nelze doporučit (jedná se např. o algoritmy RC4 a 3DES).

K detekci použitých slabých šifrovacích algoritmů v informačních systémech slouží specializované služby (Např. Qualys SSL Labs). Podobně jako většina OSINT nástrojů, i tyto služby slouží jak obráncům, tak útočníkům.

Whitelisting a blacklisting síťového provozu

Moderní firewally umožňují rozpoznávat typ síťového provozu a jeho případnou rizikovost. Klíčovou součástí bezpečnostní politiky pro správu síťového provozu je vytvoření pravidel pro konkrétní systémy, síťové prvky a uživatele. V informačním systému by měla být vždy umožněna pouze zamýšlená a řádně zdokumentovaná síťová komunikace. V opačném případě může útočník využít nespravovaného provozu pro vlastní komunikaci (např. pro nedetekovanou exfiltraci dat, či komunikaci na C&C[131] server). Současnou běžnou praxí je blacklisting rizikových kategorií internetových stránek pro koncové uživatele tak, aby nedošlo ke kompromitaci jejich stanic. Jedná se především o portály pro stahování nelegálního digitálního obsahu, weby pro stahování programů, sociální media apod. Obě dotazované organizace v současné době provádí kontrolu síťového provozu na firewallu.

Segmentace sítě

Segmentace sítě zabraňuje vertikálnímu i horizontálnímu šíření kybernetické nákazy. Podstatou síťové segmentace je umístění odlišných počítačových systému do vzájemně neprostupných síťových lokalit (segmentů). Při kompromitaci jednoho druhu prvků tak lze efektivně zabránit šíření do zbytku infrastruktury, protože síťový provoz mezi jednotlivými VLAN je zakázán. Běžná bývá segmentace sítí pro uživatelské pracovní stanice, produkční, testovací, vývojová či edukační prostředí, IoT zařízení, VoIP telefonii či prvků pro IT administraci. Segmentace sítě je také nástroj, jak zabránit kompromitaci vysoce zranitelných prvků, jež nelze zabezpečit běžnou aktualizací (např. servery s end-of-life operačními systémy, na kterých jsou

[131] *C&C server (Command and Control server) – Útočníkem ovládaný server, ke kterému se připojit nakažený koncový bod a skrze který útočník tento bod ovládá.*

závislé firemní procesy). Nejvyšší úrovní segmentace je tzv. mikrosegmentace. Zatímco běžná segmentace probíhá na úrovni fyzické (segment označován jako VLAN[132], odpovídá vrstvě 2 OSI[133] modelu) nebo logické (segment označován jako subnet, odpovídá vrstvě 3 OSI modelu) adresace, mikrosegmentace spočívá v nezávislosti aplikovaných pravidel na logickém či fyzickém umístění daného prvku v síti. Toho je dosaženo obohacením logiky pro vyhodnocování síťového provozu o dodatečné informace z transportní a aplikační vrstvy (například nasazením koncových agentů, inspekcí https komunikace nebo spárováním identity uživatelů se síťovým provozem). Mikrosegmentace je klíčovou součástí Zero-Trust modelu[134]. Obě organizace mají vytvořen systém segmentace sítě.

Segmentace implementačních prostředí

Segmentací implementačních prostředí je kombinací síťové, datové a autentifikační segmentace, jejímž cílem je kompletní (fyzická, logická, datová, síťová) izolace prostředí pro běh produkčních systémů od prostředí pro jejich testování a vývoj. Běžnou praxí a prvním krokem při nasazování nových informačních technologií je jejich vývoj ve vývojovém prostředí. Pro provoz vývojového prostředí platí v praxi několik specifik. Do tohoto prostředí přistupují jak interní, tak externí vývojáři. Z tohoto důvodu je nutné umožnit přístup do prostředí i pro osoby mimo organigram (např. přístupem přes VPN). Při přístupu cizích osob je zároveň nutno dbát na to, aby tyto osoby neměli díky přístupu do vývojové větve k dispozici informace, jež jím nepřísluší znát v souladu s principem need-to-know a least privillege (např. klientská data). Před importem do vývojového prostředí by měla veškerá citlivá data podstoupit anonymizaci či zašifrování. Primárně je při vývoji kladen veškerý důraz na zprostředkování funkčnosti. Ve specifických případech může ve vývojovém prostředí vzniknout požadavek na výjimku z existující bezpečnostní politiky (např. připojení USB disku k počítači či přenos souborů mezi pracovní stanicí vývojáře a jump hostem[135]).

Neméně významným krokem před nasazením nových informačních technologií je ověření jejich zamýšlené funkcionality a odkrytí případných závad a zranitelností před nasazením

---

[132] VLAN (Virtual Local Area Network) – Logický podcelek v rámci počítačové sítě

[133] OSI (Open Systems Interconnection Model) – Referenční model pro popis interkonektivity počítačových systémů

[134] Zero-Trust model – Přístup k ochraně informačních systémů založený na preemptivní kontrole všech známých i neznámých uživatelů a počítačových systémů vně i uvnitř sítě. Nahrazuje tradiční model bezpečnosti perimetru, který je založen pouze na ochraně před hrozbami zvenčí (mimo perimetr).

[135] Jump Host – Virtuální server, na který se připojují uživatelé pro přístup na další úroveň koncových bodů. Slouží ke koncentraci síťových prostupů a oprávnění na jeden kontrolovaný bod tak, aby nebylo nutné povolit přístupy z ostatních míst v síti.

do produkce. To probíhá v rámci UAT[136] v testovacím prostředí. Zatímco do vývojového prostředí přistupují výhradně povolané osoby s vysokou technickou znalostí, v testu se objevují mnohdy samotní koncoví uživatelé. Z tohoto důvodu je nutno klást větší důraz na jim udělená oprávnění tak, aby nedošlo miskonfiguraci či nedostupnosti prostředí. Protože UAT má novou technologii připravit na reálný provoz platí, že prostředí by mělo být do co nejvyšší míry zrcadlovým obrazem produkce (hardware, software, konfigurace). Zároveň ze stejného důvodu jako v případě vývoje platí, že by testovací prostředí nemělo obsahovat citlivá data.

Produkční prostředí je finálním prostorem pro běh implementované technologie. Pro udržení co nejvyšší bezpečnosti je v zájmu organizace, aby nasazení probíhalo výhradně v režii interního IT oddělení. V produkci je na rozdíl od testu a vývoje běžně implementován monitoring běhu služeb, auditing prováděných administrátorských i uživatelských operací a vynucen nejpřísnější režim bezpečnostních ochran. Produkční systémy navíc často běží z důvodu udržení vysoké dostupnosti na vícero bodech najednou tak, aby v případě výpadku jednoho bodu došlo k přesměrování na bod druhý. Specifickým krokem při nasazení do produkce je penetrační testování, při kterém je nezávislá třetí strana pověřena prověřením bezpečnostního standardu nové technologie. Ani bezvadný výsledek penetračního testu však neznamená, že technologie je stoprocentně bezpečná. Převážná část penetračního testování následuje existující metodiky (např. OWASP[137]). Zároveň je při penetračním testu testerům zpravidla zakázáno způsobit nedostupnost produkčních systémů. Z těchto důvodů tak k odhalení skrytých zranitelností někdy vůbec nedojde.

Nejextrémnější požadavky na zabezpečení je nutno klást na systémy s přímou dostupností z internetu. Prostředí na pomezí síťového perimetru, do kterého je vidět jak z vnitřní sítě, tak z veřejné sítě se označuje jako DMZ (demilitarizovaná zóna). Zatímco v interní síti je riziko zneužití jakékoliv zranitelnosti podmíněno vždy minimálně fyzickým či vzdáleným vniknutím do sítě (což obráncům dává prostor pro detekci a reakci), při útoku z internetu je zranitelný systém viditelný pro neomezený okruh potenciálních útočníků, což značně zvyšuje šanci, že někdo během pokusu o útok skutečně uspěje. Systémy v DMZ navíc běžně slouží k poskytování služeb třetím stranám, a jsou proto velice citlivé i z hlediska jejich faktického datového obsahu či případného reputačního rizika v případě jejich nedostupnosti.

---

[136] *UAT (User Acceptance Testing) – Akceptační testy dodávaného software/hardware*

[137] *OWASP (Open Web Application Security Project) – Nezisková organizace vytvořená pro standardizaci požadavků na bezpečnost webových aplikací*

Z výše uvedených situací vyplývá, že možnost aplikovat na různá prostředí odlišné úrovně ochrany nejen snižuje riziko kybernetických incidentů, ale i zvyšuje efektivitu, s jakou jsou nové technologie implementovány a využívány. Organizace 1 dělí prostředí na vývojové, testovací a produkční, Organizace 2 má prostředí produkční a spojené prostředí pro testování a vývoj.

3.3.2 Bezpečnostní software

Bezpečnostní software je souhrnný název pro programové vybavení, jehož cílem je mitigace konkrétních druhů útoku. Software může být přitom provozován jak v rámci dedikovaného zařízení on-premise (např. na fyzické či virtuálním serveru nebo jednotlivých pracovních stanicích), tak i v cloudu (zpravidla jako centrální bod pro správu).

Současným trendem je nabídka all-in-one řešení (digitálních ekosystémů), které umožňují rychlé nasazení do existující infrastruktury a zároveň usnadňují jejich správu a monitoring. Zpravidla jsou tato řešení také levnější než ekvivalentní služby poskládané z vícero produktů několika dodavatelů. Opačným přístupem (kombinací vícero specifických produktů od několika vendorů), je možné na úkor vyšších pořizovacích a provozních nákladů snížit riziko vendor-lock[138] a docílit vyšší bezpečnosti (v all-in-one řešeních se běžně vyskytuje jedna zranitelnost napříč mnoha subprodukty). Bezpečnostní software dělíme podle reakce na kybernetický útok na software pro aktivní mitigaci (dokáží útoku přímo zabránit, jde např. o nástroje typu Anti-Malware, EDR, IPS) a pasivní mitigaci (útok je jimi pouze detekován nebo je snižována pravděpodobnost jeho vzniku, sem spadá např. IDS, skenery zranitelností, DLP či SIEM).

Anti-malware a EDR

Anti-malware je souhrnný název pro počítačové programy na ochranu před malware. Jedná se o software instalovaný na koncových bodech, jehož hlavním účelem je detekce a odstranění škodlivého kódu. Moderní Anti-malware software kombinuje v jednom koncovém agentu jak tradiční anti-virus (provádí detekci virů na základě signatur prostřednictvím korelace vůči virovým databázím, ale lze snadno překonat například změnou file-hash[139]), tak pokročilé

[138] *Vendor-lock - Závislost chodu jednoho či více procesů, potažmo celé organizace na spolupráci nenahraditelného dodavatele*

[139] *File-hash – Unikátní řetězec znaků vytvořený aplikací hashovací funkce na bitovou sekvenci daného souboru. Při sebemenší změně obsahu souboru dochází vždy ke změně file-hash. Toho lze zneužít pro maskování již identifikovaného malware pro další použití. Útočník provede pouze formální změnu ve zdrojovém kódu a zkompilovaný malware má následně nový antivirem neidentifikovaný file-hash.*

automatizované nástroje jako forenzní analýza[140], sandboxing[141] a strojové učení. Zatímco v minulosti fungoval anti-malware výhradně jako ochrana před již jednou identifikovanými hrozbami, současná řešení dokáží detekovat nákazu pouze na základě jejich faktického chování na koncovém bodu (např. detekce velkého množství operací nad soubory na disku může indikovat šifrování ransomwarem, či síťové DNS dotazy na neznámou IP mohou znamenat dotaz na C&C server). V závislosti na typu produktu může anti-malware fungovat výhradně v proaktivním (provádí plánované nebo manuální skeny celého systému, např Malwarebytes Anti-malware či RogueKiller), nebo v reaktivním režimu (provádí pouze kontrolu právě spouštěných nebo běžících souborů jako např. Crowdstrike Falcon), případně může kombinovat obě funkcionality v jednom (např. Check Point Endpoint Security či Symantec Endpoint Protection).

Nejvyšší úrovní zabezpečení koncových bodů proti malware je EDR (Endpoint Detection and Response). EDR funkcionalitu může obsahovat přímo anti-malware agent, případně se může jednat o specializovaný produkt (např. Symantec EDR) či službu (např. produkt AEC Endpoint Detection and Response je kombinací EDR agentů a jejich externího 24/7 monitoringu a analýzy dedikovaným personálem v dohledovém centru). Technologie EDR umožňuje z centrálního bodu pro správu provést detekci, analýzu i asanaci, (odstraněním malware nebo izolací koncového bodu od sítě), přičemž v závislosti na konfiguraci mohou být tyto kroky plně automatizovány napříč všemi napadenými systémy. Další výhodou centrálně spravovaného EDR řešení je schopnost reagovat na neznámé hrozby, které v době útoku žádná z anti-malware kontrol nedetekuje formou tzv. Indicators of Compromise[142]. Nasazení EDR vedlo v organizaci respondenta k poklesu počtu bezpečnostních incidentů o 76 % a jeví se tak jako extrémně efektivní.

IDS a IPS

IDS (Intrustion Detection System) a IPS (Intrusion Prevention System) je technologie prevence nechtěných průniků do počítačových sítí. Obě technologie fungují na principu analýzy síťové komunikace. Základem této analýzy je porovnávání vůči databázi rizikových signatur

---

[140] Forenzní analýza je technologie konstantního monitoringu provozu koncových bodů. Forenzní analýza kontroluje všechny běžící procesy a ověřuje, že neprovádí podezřelé či nestandardní aktivity. V případě detekce anomálního chování může anti-malware notifikovat uživatele či správce, případně v závislosti na konfiguraci tuto aktivitu přímo zablokovat nebo koncový bod úplně odpojit od sítě.

[141] Sandboxing – Spuštění neznámého datového obsahu v izolovaném kontejneru pro účely detekce potenciálně škodlivých aktivit

[142] Indicators of Compromise (IoC) – Jedná se o indikátory kybernetického útoku na informační systém. V případě centrálně spravovaného EDR lze na úrovni politiky vyspecifikovat tyto indikátory ručně a vydefinovat reakci EDR agenta v případě detekce. Podoba IoC je různá, běžně se jedná například o komunikaci na rizikové IP adresy nebo file-hash škodlivých souborů. Nově nalezené IoC se běžně sdílejí v rámci security awareness kampaní uvnitř (s dotčenými útvary) i vně organizace (s partnery, klienty, či oborově dotčenými organizacemi), případně o nich informují specializované třetí strany (např. doporučení Národního úřadu pro kybernetickou bezpečnost).

a statistických anomálií. Signatura je soubor značek specifických pro škodlivý provoz (např. nestandardní HTTP request[143]) Databáze signatur pravidelně aktualizují výrobci bezpečnostních řešení na základě celosvětově detekovaných útoků. IPS i IDS může běžet buď přímo na koncových bodech (Host-based) nebo přímo na síťovém firewallu, skrze který prochází veškerý síťový provoz (Network-base, perimeter-based). Zásadní rozdíl mezi IPS a IDS je v jejich reakci na škodlivý provoz. IDS závadný síťový provoz pouze detekuje a notifikuje. Z tohoto důvodu se IDS využívá v případech, kdy není žádoucí, aby útočník věděl, že je detekován (např. v rámci honeypotu). Oproti tomu IPS provoz závadný provoz rovnou blokuje. Nutno podotknout, že klasické dělení IPS/IDS je v moderních sítích do jisté míry irelevantní, protože dnešní řešení poskytují obojí funkcionalitu a záleží pouze na správci, jakým způsobem reakci na škodlivý provoz nastaví. Realitou je také to, že organizace často spoléhají na výchozí nastavení IPS/IDS, protože nemají dostatečnou personální kapacitu pro jejich obsluhu. IPS a IDS vyžadují vzhledem k obrovskému množství existujících signatur manuální ladění, aby nedocházelo k vyhodnocování false positives a negatives. Některá řešení minimalizují nároky na obsluhu IPS pravidelnou vzdálenou aktualizací všech signatur včetně příslušných reakcí přímo od vendora (např. Check Point Next Generation Firewall), případně implementací umělé inteligence, která dokáže upravit reakci na detekovanou signaturu podle dodatečného kontextu (např. Sophos XG Firewall). V obou dotazovaných organizacích funguje sdružené řešení IPS/IDS. Podle dat z Organizace 2 je podíl detekovaných a zablokovaných spojení přibližně 60:40 ve prospěch blokací.

Skenery zranitelností a centrální správa aktualizací

Pro posouzení stavu informačního systému z hlediska bezpečnosti slouží skenery zranitelností. Skener zranitelností umožňuje obráncům zkontrolovat, zda daný prvek neobsahuje bezpečnostní zranitelnosti. Skenery dělíme podle toho, kde se ve vztahu ke skenovanému prvku nachází na interní (v interní síti) a externí (v externí síti – obvykle v internetu).

Účelem interního skeneru je detekce všech zranitelností na cílovém systému. Běžnou praxí je, že jsou pro skener vytvořeny výjimky ze všech ostatních vrstev ochrany tak, aby se odhalila primární příčina zranitelnosti. Interní skenery fungují buď v režimu credentialed (skener má k dispozici privilegované přihlašovací údaje na koncový systém a má proto více informací a tím

[143] *HTTP komunikace funguje na principu, kdy přistupující klient se dotazuje serveru (tzv. request, např. klik na OK v přihlašovacím formuláři) a server na dotaz odpovídá (tzv. response, např. autentizace uživatele a umožnění přístupu na webovou stránku). Útočník může http request záměrně modifikovat tak, aby obešel zamýšlenou logiku na serveru a přivedl server do stavu, který by za jiných okolností nenastal (nedostupnost služby, vypnutí bezpečnostních mechanismů apod.). Příkladem takového útoku je path traversal (modifikace requestu tak, aby server spustil příkaz v jiném cílovém adresáři) či SQL injection (Vložení specificky formulovaného příkazu do requestu tak, aby došlo ke spuštění operace přímo nad podběhovou databází služby)*

i více šancí na detekci zranitelnosti) a non-credentialed (skener přistupuje na slepo a musí ke skenovanému systému získat přístup přes brute-forcing[144], v opačném případě získá pouze informace ze služeb dostupných všem ostatním v síti[145]). Pro zajištění účinné mitigace zranitelností je vhodné sken zranitelností provádět na celém interním síťovém rozsahu. Majoritní část zranitelností je opravena instalací bezpečnostních aktualizací. Populárním interním skenerem jsou produkty společnosti Tenable (Nessus Vulnerability Scanner či Tenable.io).

Externí skenery slouží k posouzení toho, jak je systém zranitelný pro útočníka mimo interní síť (osoba v internetu). Zatímco existence interně detekované zranitelnosti nemusí nutně znamenat, že je nutné jí opravit, v případě externích zranitelností je tomu tak vždy. Všechny služby dostupné z internetu jsou pravidelně skenovány velkým množstvím robotizovaných nástrojů s více[146] či méně[147] legitimními úmysly, a tak je riziko, že někdo zranitelnost objeví nepoměrně vyšší než v případě, kdy je viditelná pouze z interní sítě.

V obou organizacích probíhá pravidelné automatizované interní skenování zranitelností. Organizace 1 dostává výsledky externího skenu zprostředkovaně v rámci svého vztahu k mezinárodní finanční skupině. Organizace 2 externí skeny provádí sama.

Pravidelné skenování nepřímo slouží i jako motivace pro příslušné správce systémů pro implementaci automatizovaného procesu aktualizací v organizaci. V počítačových sítích o malém rozsahu lze instalaci aktualizací na koncových bodech provádět manuálně, nebo za pomoci výchozích aktualizačních nástrojů (např. automatické aktualizace Windows Update). S narůstajícím počtem prvků dochází k tomu, že takto nastavený proces začíná v jednotkách případů selhávat. Výraznějším problémem však je, že v organizaci neexistuje standardizovaná konfigurace koncových bodů, protože každý systém má odlišnou verzi nainstalovaného software. Testování a debugging nových aplikací je v takovém prostředí prakticky nemožný, protože nelze zaručit jejich funkcionalitu napříč všemi koncovými body. Ideálním východiskem z tohoto problému je implementace řešení na centrální správu a distribuci aktualizací. Jedná se například o produky Microsoft SCCM (System Centre Configuration Manager), Symantec Endpoint Management, či Microsoft WSUS (Windows Server Update Services). Výše zmíněné nástroje umožňují správci počítačového systému nakonfigurovat zásady

[144] *Brute Forcing (česky útok hrubou silou); Pokus o uhodnutí přihlašovacích údajů do informačního systému ručním nebo strojovým vyplňováním náhodných či pseudonáhodných řetězců znaků*
[145] *Např. Ping, Netstat apod.*
[146] *Např. Roboti na indexaci webů pro internetové vyhledávače typu Google, Seznam a další*
[147] *Např. Crawleři na test otevřených komunikačních portů či jiných zranitelností typu Shodan.io a další*

pro aktualizaci software a distribuovat takto standardizovanou konfiguraci na všechny počítače. Obě organizace mají standardizovaný postup na distribuci aktualizací na koncové systémy.

DLP

DLP (Data Loss Prevention) je řešení na ochranu organizace proti úmyslnému či nedbalostnímu úniku citlivých dat. DLP rozlišujeme podle způsobu monitorování na síťové DLP a DLP na koncových bodech. U obou druhů platí, že dochází k monitoringu síťové komunikace (e-mail, internet atd.) a běžících procesů (textové editory, e-mailoví klienti, operace se soubory apod.). Tyto aktivity jsou v reálném čase porovnávány vůči centrálnímu repozitáři DLP zásad. DLP zásady definuje pověřený správce (zpravidla útvar odpovědný za informační bezpečnost) a udržuje je v tajnosti, aby uživatelé neměli představu o tom, jak zásady obcházet. Zásady jsou postaveny na kontrole komunikace a souborů na přítomnost klíčových slov či konkrétních metadat. Zároveň bývá zvykem rozdělení komunikace směrem k adresátům uvnitř a vně organizace. Na základě nastavení zásad dochází v případě korelace zásady s aktivitou uživatele buď k notifikaci správce DLP řešení, notifikaci uživatele či blokaci aktivity.

DLP na koncových bodech spoléhá na detekci uživatelských aktivit přímo na úrovni pracovní stanice daného uživatele. Endpoint řešení (např. Forcepoint One Endpoint, Symantec Endpoint DLP) mají zpravidla díky své blízkosti ke zdroji uživatelské aktivity k dispozici detailnější informace, nicméně k DLP monitoringu dochází pouze tam, kde je DLP agent nainstalován. Síťové DLP (např. Check Point NGFW DLP Blade) naslouchá síťovému provozu buď odklonem veškeré síťové komunikace z interního a externího firewallu nebo je přímo jeho součástí. Síťové řešení je nicméně funkční pouze na zařízeních, která jsou takové síti přítomny. Optimálním řešením se tak jeví implementace síťového a koncového DLP najednou, ale v takovém případě je nutné počítat s extrémními nároky na kapacitu obsluhy a správy obou řešení (především pak při ladění false-positives). Při reálném nasazení často dochází k tomu, že DLP generuje obrovské množství incidentů a duplicit jejichž odbavení není v silách určených útvarů. Takový stav zpravidla eliminuje veškerý zamýšlený přínos.

Vzhledem k povaze DLP (nerozlišuje se mezi pracovní a soukromou aktivitou uživatelů) je vhodné o jeho existenci informovat napříč organizací. Běžně je úprava základních pravidel pro nakládání uživatelů s informacemi stanovena v interním předpisu. Správně vedená informační kampaň vede ke snížení detekovaných incidentů a k efektivnímu řešení prohřešků.

Organizace 1 provozuje síťové DLP řešení, Organizace 2 DLP na koncových bodech. Oba respondenti indikovali problémy s odladěním DLP zásad a množstvím vygenerovaných false positive.

SIEM

SIEM (Security Information and Event Management) je komplexní nástroj pro centrální sběr a analýzu událostí z klíčových systémů v organizaci. Moderní SIEM umožňuje integraci všech technologií, které generují provozní, auditní nebo bezpečnostní logy. Největší přidaná hodnota SIEM spočívá v automatické korelaci anomálií napříč vícero systémy, standardizaci formátu logů a centralizaci přístupu v jednom grafickém rozhrání. Moderní SIEM používají současně pro korelaci jak člověkem naprogramovanou logiku, tak umělou inteligenci ve formě strojového učení. V závislosti na míře integrace lze SIEM provozovat jako výhradní nástroj pro bezpečnostní monitoring v organizaci. Při implementaci SIEM je nutné zohlednit kritičnost integrovaných prvků a jimi poskytovaných výstupů. V opačném případě dojde k tomu, že je systém zahlcen obrovským množstvím nepotřebných informací, což snižuje výkon a stěžuje vyhledávání. Aby SIEM poskytoval relevantní informace, je nutné v něm provádět konstantní profylaxe pravidel a vstupních zdrojů. Podobně jako u DLP je potřebné vyčlenit pro obsluhu systému dostatečnou kapacitu lidských zdrojů. V opačném případě dochází k rychlé ztrátě efektivity, protože systém generuje více událostí, než je obsluha schopna odbavit. Při konstantním backlogu docházení k řetězení neodbavených událostí, což má za následek ztrátu primárních informací. Z tohoto důvodu některé organizace používají pro dohled třetí strany. Vzhledem k vysoké míře vzájemných závislostí je nutné dbát při správě systému na důsledné vedení technické dokumentace. Nejznámějšími SIEM produkty jsou například Splunk, Elasticsearch, IBM Qradar nebo LogRhythm.

Obě organizace provozují on-premise SIEM, nicméně Organizace 1 momentálně zvažuje odklon od současného řešení směrem k modernější platformě.

3.3.3 Bezpečnostní hardware

Bezpečnostní hardware jsou fyzická zařízení pro ochranu před kybernetickými útoky. Nutno podotknout, že i bezpečnostní hardware je závislý při plnění své funkce na software (v podobě proprietárního firmware). Zásadní rozdíl je ve specifikaci tohoto programového vybavení. Zatímco standardní bezpečnostní software je možné používat na široké škále zařízení v rámci podporovaných operačních systémů, bezpečnostní hardware má firmware předinstalován už v rámci dodávaného produktu od výrobce. Vyjma instalace zařízení do infrastruktury a běžné

údržby do něj zákazník již víceméně nezasahuje. Z tohoto důvodu bývají tyto prvky označovány pojmem „standalone appliance“ (samostatné zařízení).

Firewall

Firewall je fyzický síťový prvek, který zajišťuje kontrolu nad příchozími a odchozími síťovými toky v organizaci v souladu s nastavenými pravidly. V minulosti bylo zvykem firewally dělit do mnoha kategorii podle umístění na OSI modelu či funkcionalitě. Tento koncept postupně zaniká s tím, jak se výrobci moderních firewallů soustředí na stále komplexnější integraci všech funkcionalit do jednoho zařízení. V současné době je trendem nástup firewallů nové generace (NGFW - Next generation Firewalls). NGFW integruje do jednoho produktu veškerou funkcionalitu pro zajištění bezpečnosti síťového provozu. Kromě klasického filtrování paketů a monitoringu spojení tak NGFW zajištuje i web-filtering, IPS/IDS, identifikaci uživatelů, HTTPS inspekci, DLP, webový aplikační firewall či VPN přístup.

V organizacích je běžně nutné zprostředkovat uživatelům spojení současně jak v interní (například přístup na sdílené uložiště) tak v externí síti (internet). Aby organizace zajistila co nejvyšší míru ochrany před kybernetickými útoky, je běžnou praxí kombinace firewallu interního a externího. Zatímco interní firewall zajišťuje kontrolu nad laterálními datovými toky v rámci organizace (zde se konfiguruje oprávnění na síťový přístup na interní zdroje), externí firewall poskytuje nezávislou ochranu před útoky přímo z internetu a blokuje případnou nežádoucí aktivitu uživatelů směrem ven z organizace. Pro zajištění bezpečnosti síťového perimetru je klíčová centralizace síťového provozu na příslušný firewall.

Zajímavým trendem je integrace sandbox funkcionalit do inspekce síťového provozu. Některé firewall produkty jako například Check Point NGFW či Sophos XG umožňují v současnosti provádět sandboxing spustitelných souborů přímo při jejich stahování, či před doručením e-mailové zprávy do schránky uživatele. V případě detekce malware či jiného škodlivého obsahu v sandboxovaném souboru dojde k automatickému odstranění, což výrazně snižuje prostor pro chybný úsudek uživatele při pohybu v internetu.

E-mailová brána

E-mailová brána je zařízení, které zajišťuje zabezpečené centrální odesílání a doručování e-mailů uživatelům v organizaci. Podobně jako firewall, také e-mailová brána umožňuje konfigurací zabránit nechtěnému e-mailovému provozu a významně omezit e-mailový phishing, spam a spoofing. Klasické on-premise emailové brány jsou umístěny na hranici mezi interním perimetrem a internetem. Ze své podstaty musí být e-mailová brána viditelná z internetu

pro všechny servery, které by na ní potenciálně mohli odeslat zprávu, proto je správná konfigurace tohoto prvku velice důležitá. Některé organizace implementují z tohoto důvodu e-mailové brány ve dvou či více vrstvách. Externí brána e-maily dále přeposílá na interní bránu a až následně dojde k doručení uživatelům. Díky zdvojení kontroly je zajištěna bezpečnost doručovaných zpráv i v případě kompromitace externího prvku útočníkem z internetu. V návaznosti na trend postupného mazání hranic mezi internetem a perimetrem organizace začíná stále větší procento výrobců poskytovat namísto fyzického on-premise řešení cloudovou variantu e-mailových bran.

E-mailová brána provádí tři základní druhy kontrol. Tou první je reputační blacklisting. V současné době existuje celá řada pravidelně aktualizovaných seznamů IP adres, ze kterých je zasílán spam. Při reputačním blacklistingu se brána při obdržení e-mailu z takové IP adresy ani nepokouší o doručení. Na této úrovni je odfiltrováno cca 90 % celkového spamu a phishingu. Druhou úrovní kontroly je ověření DKIM[148] a SPF[149] (souhrnně DMARC[150]). Poslední vrstvou je anti-malware sken příchozích příloh a odkazů. Kromě klasické kontroly vůči známým virovým signaturám e-mailové brány dnes provádí sandboxing a strojovou forenzní analýzu.

Některá e-mailová řešení obsahují time-of-click ochranu, která zaručí, že pokud doručený e-mail obsahuje hypertextový odkaz, ten bude automaticky nahrazen proklikem na záchytný portál e-mailové brány. Pokud tedy i přes všechny kontrolní úrovně dorazí škodlivý e-mail až k uživateli, který ho rozklikne, je místo škodlivé akce přesměrován na stránku s varováním. V závislosti na nastavení je pak jeho následný přístup podmíněn udělením souhlasu, nebo úplně zablokován.

Obě organizace mají fyzickou externí a interní e-mailovou bránu, nicméně Organizace 2 plánuje přechod na cloudové řešení ke konci roku 2021.

HSM

HSM (Hardware Security Module) je vysoce specializované fyzické zařízení pro centrální ochranu a správu digitálních klíčů. Jedná se buď o samostatné zařízení či rozšiřující kartu připojenou do serveru. V obou případech slouží HSM k tomu, aby na něm probíhal kompletní životní cyklus kryptografických klíčů. V závislosti na konkrétním výrobci může HSM přímo

---

[148] DKIM (Domain Keys Identified Mail) - Kontrola integrity emailové zprávy, funguje na principu kryptografie veřejných klíčů. Pouze legitimní odesílací server má k dispozici pro podpis zprávy privátní klíč a veřejný klíč je publikován v DNS záznamů domény organizace. Díky tomu může příjemce rychle validovat, zda byla zpráva odeslána z organizace či nikoliv.

[149] SPF (Sender Policy Framework) - Kontrola, zda za organizaci někdo neposílá e-maily z jiné IP adresy než z té uvedené v DNS záznamu domény organizace.

[150] DMARC (Domain-based Messange Authentication, Reporting and Conformance) - Kombinace kontroly SPF a DKIM do jednoho ověřovacího mechanismu

provádět kryptografické operace a neubírat tak serverům výpočetní výkon. HSM chrání proti odcizení, pozměnění či ztrátě klíčů a zároveň vytváří detailní auditní stopu. Díky vyčlenění do HSM lze tato zařízení podrobit extrémnímu stupni ochrany jako síťový whitelisting, či fyzická ostraha. Navíc je díky němu zajištěno, že se v organizaci využívají výhradně bezpečně šifrovací sady. Ekvivalentem HSM z pohledu režimové ochrany je management kryptografických klíčů na procesní úrovni.

Při implementaci HSM je nutno myslet na to, že pokud organizace šifruje data, stává se z HSM extrémně důležitý prvek, jehož nedostupnost může znamená kompletní ztrátu přístupu k těmto datům. Z tohoto důvodu je důrazně doporučováno nasazovat HSM minimálně ve dvojici a každý HSM by se měl nacházet v jiné fyzické lokalitě.

Organizace 2 plánuje implementaci HSM v průběhu roku 2022, v Organizaci 1 zatím o implementaci neuvažují, obě organizace nicméně řeší problematiku správy kryptografických klíčů procesně.

MFA Tokeny

Vícefaktorová autentizace (MFA) je v současné době nejdoporučovanější způsob, jak zabránit neoprávněnému přístupu útočníka v případě ztráty jednoho z přihlašovacích údajů. Klasické přihlášení jménem a heslem spoléhá pouze na faktor uživatelské znalosti, a proto při vyzrazení hesla útočníkovi ve zneužití údajů již nic nebrání. Oproti tomu MFA vyžaduje pro úspěšně ověření od uživatelé předložení několika ověřovacích faktorů současně. Nejběžnější kategorizací ověřovacích faktorů je dělení na něco, co znám (přihlašovací jméno a heslo) něco, co mám (MFA Token ve formě usb klíče, smart card či OTP [151]) a něco, co jsem (sken sítnice, otisku prstu či další biometrické údaje). V závislosti na použití existují i ověřovací faktory závislé například na GPS poloze uživatele či IP adrese přistupujícího zařízení. MFA je ideálním nástrojem pro zabezpečení služeb, nad kterými nelze vynutit vlastní úroveň ochrany (např. cloudové služby). Vícefaktorová autentizace je jedním z nutných požadavků na ověření elektronických plateb tzv. Strong Customer Authentication (SCA) podle nařízení Komise (EU) 2018/389 (doplňující nařízení ke směrnici PSD2) a je proto nutnou součástí všech tuzemských webových i mobilních aplikací pro internet banking. I přesto, že MFA minimalizuje prostor pro uživatelskou chybu, není toto řešení bez zranitelností. Důkazem budiž úspěšnost v současnosti silně medializovaných vishingových kampaní, které cílí na získání ověřovacích faktorů přímo od uživatele. Bypass MFA a následná

[151] *OTP (One-Time Password) – Jednorázový dynamický přihlašovací kód pro vícefaktorovou autentizaci, např. Google Authenticator nebo ověřovací kód přes SMS*

kompromitace infrastruktury pro výdej MFA tokenů Cisco Duo byly hlavní příčinou jednoho z největších kyberincidentů roku 2020, a to útoku na americkou společnost SolarWinds.

Obě organizace používají MFA pro uživatelský přístup do VPN. V Organizaci 2 je MFA povinné pro všechny cloudové služby, které jej podporují.

3.4 Prevence viktimnosti - Security Awareness program

Pro prevenci viktimnosti organizace kontinuálně realizuje vlastní Security Awareness program. Security Awareness (česky bezpečnostní osvěta) je pojem pro informační aktivitu cílenou na koncové uživatele informačních systému. V oblasti kybernetické bezpečnosti se jedná o jeden ze základních pilířů bezpečnostní politiky organizace. O vysokém významu osvěty svědčí i její obsažení v mezinárodních metodologiích pro auditování kybernetické bezpečnosti (např. standard ISO 27000). Premisa bezpečnostní osvěty je založena na tom, že uživatel je nejslabším článkem informačního systému a je s ním spojeno největší riziko úspěšného útoku. Protože útočníci v kyberprostoru používají stále sofistikovanější metody pro útok, je nutné mezi uživateli vytvořit a udržovat dostatečné povědomí o potenciálních hrozbách při práci s výpočetní technikou. Cílem úspěšné kampaně je uživatel, který dokáže identifikovat a mitigovat kybernetická rizika nezávislé na jiných bezpečnostních mechanismech.

Úroveň technického detailu bezpečnostní osvěty je nutné vždy upravit přiměřeně pracovní náplni adresátů. Diametrálně odlišný bude technický detail školení pro IT administrátory versus vstupní školení nových zaměstnanců na pozice, jež pracují s počítačem pouze výjimečně. Stejně důležité je brát v potaz rizikovost určitých pracovních skupin recipientů této osvěty a upozornit je na specifické druhy útoků, které na ně mohou být vedeny (např. mediální expozice top managementu může vést ke zvýšené snaze o jejich impersonaci při phishingu; s pozicí finančního ředitele je běžně spojená pravomoc elektronického schvalování plateb, hacker se bude snažit o získání jejich podpisového elektronického certifikátu; oddělení nákupu přichází do styku s velkým množstvím externích subjektů, může se jednat o falešného IT dodavatele, jehož cílem je zanesení malware pro průmyslovou špionáž atd.).

Pro vedení osvětové kampaně lze zvolit běžné firemní komunikační kanály (informační e-maily, tištěný infotainment, dálková školení přes videochat či osobní setkání s vybranými skupinami uživatelů). Pro sofistikovanější metody zvýšení bezpečnostního povědomí uživatelů existují dnes dedikované externí platformy. Tyto umožnují tvorbu elektronických školení a testů

či zasílání fake-phishingu[152]. Příkladem platformy jsou user security awareness produkty od firem Proofpoint, Sophos či KnowBe4. I přes to, že tyto služby jsou placené, platí, že s user awareness jsou spojeny ve srovnání s ostatními druhy preventivních opatření velice nízké finanční náklady.

Nevýhodou tohoto druhu opatření je časová náročnost jejich přípravy a faktická nevymahatelnost. Zatímco první nevýhodu lze částečně mitigovat externí dodávkou (viz. awareness platformy výše), jen velice těžko lze uživatele přesvědčit, aby získané znalosti aktivně využívali v praxi.

Iniciativu uživatelů lze částečně pozitivně motivovat (např. celofiremní soutěží o ceny pro zaměstnance s nejvíc nahlášenými spamy), tyto aktivity však jsou realizovatelné pouze v určitém typu firemní kultury. Nadále platí, že mnozí zaměstnanci budou inciativu záměrně ignorovat. Negativní motivace (např. podmínění výplaty ročního bonusu splněním bezpečnostních školení) může mít krátkodobý pozitivní dopad, nicméně dlouhodobě vede k prohlubování negativního vztahu uživatelů k oblasti kybernetické bezpečnosti. Nesprávně vedená osvěta může mít až kontraproduktivní efekt vyúsťující ve snížený zájem zaměstnanců o kybernetickou bezpečnost. To následně vede k nízkému důrazu na dodržování bezpečnostních politik a snaze opatření obcházet, zlehčovat, či rozporovat. Pro user awareness více než pro ostatní druhy preventivních opatření platí, že pouze zmenšuje attack surface[153].

Organizace 1 má při školení uživatelů velkou míru podpory ze strany mateřské společnosti ve formě předpřipravených informačních materiálů či phishing kampaní na míru. Organizace 2 využívá pro osvětovou kampaň spolupráci marketingového oddělení a pro phishingové kampaně je využita specializovaná služba třetí strany.

3.5 Shrnutí nálezů z dokumentů a rozhovorů

Primárním analytickým zdrojem pro následující podkapitolu jsou data z publikací Národního úřadu pro kybernetickou a informační bezpečnost[154] a Institutu pro kriminologii a sociální prevenci[155].

---

[152] Fake-Phishing - Phishing rozesílaný záměrně na vlastní uživatele. Cílem je monitoring obecného povědomí uživatelů o správných návycích při práci s phishingovými e-maily (Měří se kolik uživatelů prokliknulo hypertextový odkaz, otevřelo přílohu apod.). Některé platformy umožňují po kliknutí na podvodný odkaz uživatele přesměrovat na e-learning materiál, který mu vysvětlí, jak identifikovat rizikové znaky podvodných emailů

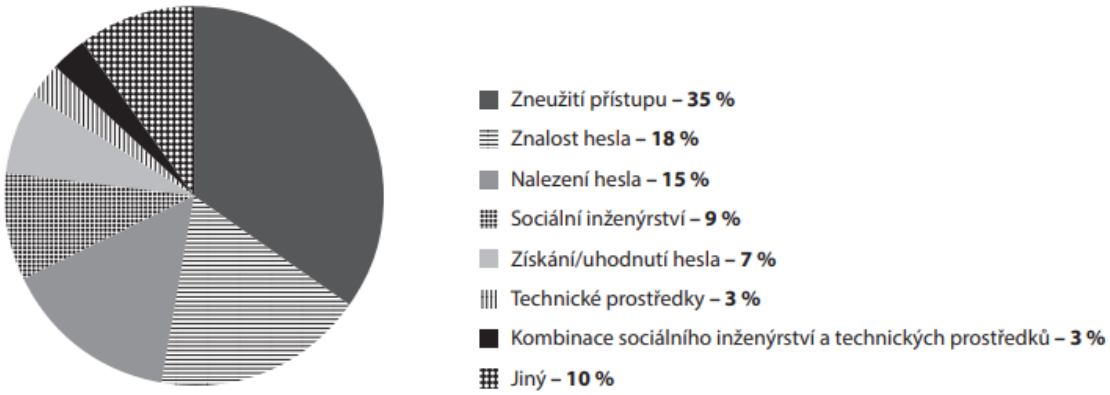
[153] Attack surface – Souhrn všech příležitostí, které může útočník zneužít k průniku do informačního systému (např. počet nedostatečně informovaných uživatelů informačního systému)

[154] *NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. 2019. Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2019. [Online] 18. září 2019. [Citace: 20. listopad 2020.] https://www.nukib.cz/download/publikace/zpravy_o_stavu/NUKIB_ZSKB_2019.pdf.*

[155] *VLACH, J., KUDRLOVÁ, K. a PALOUŠOVÁ, V. 2020. Kyberkriminalita v kriminologické perspektivě. [Online] 2020. [Citace: 30. duben 2021.] http://www.ok.cz/iksp/docs/463.pdf. ISBN 9788073381899.*

Podle zprávy NÚKIB trend růstu výskytu a závažnosti kybernetické kriminality nadále pokračuje. Nejčastějším typem útoků je spam, phishing a podvodné e-maily. Naopak na ústupu je malware pro těžbu kryptoměn. Zvýšenou profesionalitu útočníků lze pozorovat na vývoji ransomware, kdy dochází k pozvolnému opuštění plošných kampaní a dochází k cílení na konkrétní oběti. Obor kybernetické bezpečnosti se dlouhodobě potýká s nedostatkem pracovních sil, přičemž nejzásadnější potíže s chybějícím personálem má sektor zdravotnictví. Ze zprávy vyplývá, že kromě majetkově orientovaných kyberzločinců v České republice byla detekovaná aktivita APT skupin s kořeny v Rusku a v Číně. Ostatní známé archetypy aktérů jako kyberteroristé, script kiddies či hacktivisté nepředstavují v českém kyberprostoru významnější riziko. V souvislosti s útokem na společnost Avast zpráva varuje před potenciálním nárůstem supply-chain útoků. Pro finanční sektor je uveden jako nejrizikovější faktor interní uživatel, ovšem pouze v roli oběti či předmětu útoku. Ve výhledu na rok 2021 figurují na prvních příčkách nejvýznamnějších příčin kybernetické kriminality ransomware, útoky na cloudovou infrastrukturu, mobilní malware, různé formy phishingu a chybějící personální kapacity.

Z publikace IKSP Kyberkriminalita v kriminologické perspektivě vyplývá, že nejčastější motivací českého pachatele jsou finance, mezilidské vztahy a zaměstnanecký podvod. K tématu zaměstnaneckého podvodu zdroj uvádí, že vyšší riziko hrozí organizacím v soukromém sektoru. Nejčastěji je útok veden přes počítač, útoky z mobilních zařízení jsou spíše výjimkou. Jako komunikační kanál jsou nejčastěji využívány fyzická přítomnost u počítače, e-mail a sociální sítě. Významnou převahu ve způsobu spáchání má zneužití oprávněného (35 %) a neoprávněného přístupu (55 %). Z tohoto údaje vyplývá, že sofistikované útoky, které nespoléhají na získání přihlašovacích údajů, ale přímo na zranitelnosti systému jsou v České republice zastoupeny spíše marginálně.



Graf 2 - Způsob spáchání (Zdroj: IKSP[156])

Ve srovnání se zjištěním z rozhovorů lze říci, že část východisek z dostupných dokumentů se potvrdila, nicméně v některých bodech jsou tvrzení respondentů odlišná. Radek Živný v průběhu dotazování uvedl, že riziko kybernetické kriminality se meziročně nezvyšuje, ale je konstantně extrémně vysoké. Naopak souhlasí s tím, že integrace informačních technologií do většiny odvětví lidské činnosti má za následek větší četnost pokusů o útok. Stejně tak současná snaha o maximální zabezpečení kybernetického perimetru vede k tomu, že pachatelé jsou stále vynalézavější. Nicméně zatímco v minulosti bylo útoků v kyberprostoru podstatně méně, jejich šance na úspěch byla díky neexistenci jakýchkoliv bezpečnostních opatření řádově vyšší než dnes. Shodně se zprávou NÚKIB pan Živný uvádí nedostatek finančních kapacit jako jeden z významných důvodů pro sníženou schopnost reagovat na kybernetické hrozby. Jako poznatek z praxe v českých organizacích uvádí problematiku kanibalizace rozpočtu na kybernetickou bezpečnost ve prospěch ostatních oddělení, nejběžněji pak oddělení IT. Je toho názoru, že na kybernetickou bezpečnost by mělo připadnout minimálně 5-10 % z celkových investic do informačních technologií.

Druhým nešvarem českých organizací je reaktivní přístup ke kybernetickým hrozbám. Důraz na kybernetickou bezpečnost je tak dáván až v případech, kdy organizaci hrozí nebo v ní probíhá bezpečnostní audit či reálný kybernetický útok. Podle respondenta je nedostatek odborníků v oboru způsoben vysokými nároky na technické a sociální schopnosti zaměstnance, přičemž velmi významnou roli hraje vzhledem k dynamické proměnlivosti kybernetické kriminality ochota těchto osob stále se učit novým věcem.

[156] *VLACH, J., KUDRLOVÁ, K. a PALOUŠOVÁ, V, cit. 155, str.66*

Na téma největších hrozeb uvedl, že v organizacích s vyspělou kybernetickou bezpečností se riziko externího aktéra nikdy nevyrovná riziku interního uživatele, přičemž uvádí pro podporu svého tvrzení poměr výskytu kybernetických incidentů až 20:1 ve prospěch incidentů zapříčiněných interními uživateli. Při uživatelsky zaviněných incidentech se jedná převážně o úmyslnou majetkově motivovanou trestnou činnost.

K hrozbě ze strany interních uživatelů pan Živný zmínil, že riziko je z jeho zkušenosti nejvyšší u zaměstnanců na manažerských pozicích a dále pak u pozic souvisejících s marketingem, obchodem a dále u oddělení s vysokou fluktuací osob, typicky call centra pro vymáhání nebo zákaznický servis. Jako nejčastější způsob spáchání činu uvádí odhalení zranitelnosti v interních procesech a aplikacích, které uživatelé mají tendenci rychle vytipovat. Jedná se většinou o chyby či miskonfiguraci při schvalování plateb, či objednávek zboží v informačních systémech. Primární motivací je dle rozhovoru finanční záměr jako kompenzace nedostatečného mzdového ohodnocení, případně nespokojenost se vztahy na pracovišti. Podle slov prvního dotazovaného se v českých organizacích nevyskytuje ve významné míře malware nebo hacking na míru. Naopak generický spam, malware, phishing a pokusy o zneužití zranitelností jsou v praxi běžné, avšak míra úspěšnosti je mizivá. Shodně se zprávou NÚKIB se vyjádřil i k problematice malwaru na těžbu kryptoměn, přičemž pokles výskytu byl zdůvodněn snížením rentability útoku.

Co se týče doporučení pro prevenci kybernetické kriminality, hlavní prioritou pro funkční kybernetickou bezpečnost je vytvoření politiky informační bezpečnosti na míru organizace. Základním vstupem pro politiku by měl být existující rámec bezpečnostních opatření jako například ISO 27000, nicméně veškerá opatření musí být přizpůsobena na míru dané organizaci. Za klíčový krok považuje Radek Živný provedení analýzy rizik. Výstup analýzy by měl poskytnout dostatečný náhled na silné a slabé stránky dosavadního stavu kybernetické bezpečnosti organizace. Pro minimalizaci rizika interních útoků se doporučuje implementace bezpečnostního monitoringu nástrojem typu SIEM, přičemž respondent varuje před několika úskalími z praxe. Jedním je nutnost jasně vydefinovat kritické prvky a informace, které bude SIEM sledovat. Druhým doporučením je nutnost tvorby dodatečné logiky pro vyhodnocování proběhlých událostí v závislosti na analýze rizik. Pan Živný nedoporučuje při implementaci SIEM používat jako nástroj pro sběr všech logů, ale pouze selektivně vybraných systémů, u nichž bude zaručeno, že jejich sledování poskytuje oddělení kybernetické bezpečnosti přidanou hodnotu, aby při analýze nedošlo k informačnímu šumu. K ostatním technickým opatřením uvádí, že se jedná ve finančním sektoru o standard, jehož implementace je nutná, ale sama o sobě nedostatečná. Stejně tak

se vyjadřuje k problematice uživatelské osvěty. U obou druhů preventivních opatření zdůrazňuje nutnost podpořit je dostatečně represivní předpisovou základnou.

Také řada tvrzení z rozhovoru s panem Beránkem je shodných s nálezy ve zmíněných analytických zdrojích. Ke způsobu spáchání činu respondent považuje za největší riziko únik nebo zneužití uživatelské identity a s tím spojenou znalost přihlašovacích údajů.

K problematice nedostatečné pozornosti v tématu kybernetické kriminality v organizacích na českém trhu druhý respondent spatřuje výrazně rostoucí tendenci, ale zároveň podotýká, že je stále co zlepšovat. K současným trendům kybernetické kriminality a prevence uvádí dotazovaný jako příklad specializaci rolí a kompetencí pachatelů i bezpečnostních týmů.

Jako zajímavým se jeví důraz Organizace 2 na procesní stránku věci, a to ve všech oblastech kybernetické bezpečnosti (prevence, detekce, represe, kontrola). Jedním z důvodů může být vyšší regulatorní tlak na kontrolní systémy v bankovním prostředí a s tím spojená potřeba prokazatelnosti při případném auditu.

Podobně jako v Organizaci 1, také v Organizaci 2 je spatřováno největší kybernetické riziko v nekalé aktivitě neloajálních zaměstnanců. Z rozhovoru vyplývá, že Organizace 2 aktuálně realizuje pro mitigaci problému rozsáhlý projekt na implementaci centrální správy identit všech uživatelů a do budoucna plánuje nasazení technického řešení pro centrální správu privilegovaných přístupů na citlivé systémy. O důrazu druhé organizace na prevenci rizika interního útoku svědčí i zvolený prevenční mechanismus, kdy je veden výběr zaměstnanců se zahrnutím screeningu. Z technických opatření vyzdvihuje pan Beránek sandboxing veškeré příchozí komunikace, který má za cíl snížit pravděpodobnost zneužití zranitelností a zároveň minimalizovat prostor pro lidský faktor.

Oba respondenti totožně uvádí, že nasazení DLP nepřineslo organizaci předpokládaný přínos. Další shoda panuje v oblasti využití bezpečnostních standardů a frameworků třetích stran (ať už se jedná o regulatorní povinnost či nikoliv), kde dotazovaní uvádí, že jde o důležitý nástroj ke stanovení cílů a oblastí, kterým je nutné se dále věnovat.

Závěr

Komparací zjištění z rozhovorů s odborníky v oblasti kybernetické bezpečnosti s východisky z analytických zdrojů a dalších dokumentů se podařilo v dostatečné míře zodpovědět na všechny tři zkoumané otázky.

K problematice specifických kyberkriminologických aspektů v České republice lze uvést, že finanční instituce v převážné míře splňují technickou best practice podle obecně známých celosvětových standardů a vnější útočníci proto míří na nejzranitelnější článek - uživatele. V důsledku nejsou externí útoky nijak technicky sofistikované a často se jedná o generické plošné phishingové a malware kampaně. I přesto, že převažující motivací pachatelů je majetkový zisk, organizace na českém trhu nevěnují dostatečnou finanční ani organizační pozornost kybernetické bezpečnosti. Z toho vyplývající absence finančních prostředků a lidských kapacit je částečným vysvětlením pro další specifikum, a to sice, že i navzdory znalosti existujících doporučení převažuje v českých organizacích pouze reaktivní přístup k řešení kybernetických hrozeb. Ze stejného důvodu také nejspíše v českých organizacích chybí zakotvení klíčových procesních mechanismů v dokumentaci či interních procesech, což má dopad na schopnost konzistentního přístupu k řešení kybernetických incidentů a sdílení know-how v rámci dotčených útvarů.

Jako nejrizikovější druh kybernetické kriminality pro finanční instituce v České republice byla jednohlasně označena nekalá aktivita interních uživatelů, a to především ve vztahu k jejich uživatelské identitě. Zásadní část kybernetické kriminality je způsobena zneužitím přihlašovacích údajů nebo zneužitím privilegovaného oprávnění v informačním systému. To je v souladu s faktem, že techniky pro kybernetické útoky jsou v reálných případech především o hledání skulin v logické koncepci informačního systému a navazujících procesů, nikoliv ve zranitelnostech technologie či nadprůměrné technické zdatnosti útočníka. Ve spojení se zmiňovanou absencí procesních a kontrolních mechanismů, může být v některých oblastech velice obtížné detekovat, že ke kriminalitě vůbec dochází. Útoky zevnitř jsou hlavní motivací pro to, aby organizace zabezpečovala svůj informační systém nejen ve vztahu k internetu, ale také vůči vlastním zaměstnancům.

Co se týče prevenčních mechanismů, české organizace ve finančním sektoru obecně přebírají koncepci prioritizace a vrstvení preventivních opatření na základě analýzy rizik a neliší se v tomto ohledu nijak od jiných organizací mimo ČR. Praktickým poznatkem obou respondentů je, že organizace mají tendenci implementovat za pomoci dodavatelů moderní technické nástroje

pro prevenci kybernetických útoku, ale často jim chybí lidská kapacita na jejich údržbu a další vývoj.

Ve vztahu k vysokému riziku útoku zevnitř organizace lze doporučit jako vhodný mitigační nástroj kvalitní výběr a screening zaměstnanců, centrální správu identit a privilegovaných přístupů a zakotvení represivně orientované interní předpisové základny. Nedílnou součástí musí být harmonogram bezpečnostních školení pro všechny dotčené osoby s průběžným ověřováním jejich povědomí formou povinných kurzů, testů a phishingových kampaní.

Důležitým prvkem na cestě k větší vizibilitě do anomálních aktivit v informačním systémů je SIEM. Na ten však lze spoléhat pouze v případě, že je jasně definováno co, kde a jak se má detekovat. V opačném případě hrozí, že systém generuje větší množství upozornění, než na které je možno reagovat. DLP řešení se zprvu jeví jako ideální opatření pro snížení rizika úniku informací ze strany neloajálního zaměstnance. Z praxe dotazovaných nicméně vyplývá, že reálný přínos DLP neodpovídá původním očekáváním ani finanční investici. Lze ho využít pouze jako podpůrný nástroj.

Tato práce se z důvodu profesního zaměření autora z velké míry věnovala problematice kyberkriminality ve finančnímu sektoru. Subjekty poskytující finanční služby zpravidla prezentují bezpečnost svých služeb vůči klientům jako jeden z definujících aspektů své činnosti a jsou tak s pojmem kybernetické bezpečnosti pevně spjaty. Jiné podnikatelské obory na první pohled neimplikují potřebu zvýšených nároků na kybernetické zabezpečení, ačkoliv opak je pravdou. Zajímavým podnětem pro navazující výzkum se tak jeví sběr a analýza poznatků o stavu kybernetické kriminality v maloobchodních a velkoobchodních subjektech malého a středního rozsahu, zvláště pak ve vztahu k jejich prezentační a prodejní činnosti na internetových e-shopech či jiných digitálních kanálech. Tyto subjekty s největší pravděpodobností nemohou vynaložit na zabezpečení svých služeb stejnou míru finančních prostředků, jako například bankovní domy, a riziko spojené s úspěšným kybernetickým útokem lze považovat ve většině potenciálních scénářů za likvidační.

Seznam použitých zdrojů

1. Seznam použité literatury

BLACK, E. 2001. *IBM and the holocaust: the strategic alliance between Nazi Germany and America's most powerful corporation*. místo neznámé : Crown, 2001. ISBN 9780609607992.

BREEN, C. a DAHLBOM, C. A. 1960. *Signaling Systems for Control of Telephone Switching. The Bell System Technical Journal*. Listopad, 1960, Sv. 39, 6.

BUCHWALD, Jed Z. 1996. *Archimedes: New Studies in the History and Philosophy of Science and Technology*. místo neznámé : Kluwer Academic Publishers, 1996, Sv. Scientific Credibility and Technical Standards in 19th and early 20th century Germany and Britain.

BURNS, Russel W. 2004. *Communications: An International History of the Formative Years*. Stevenage : IET, 2004. ISBN 9780863413278.

CHAPPE, Ignace Urbain J. 1840. *Histoire de la Télégraphie*. Bruxelles : Ch. Richelet, 1840. ISBN 9780270290233.

GAZETTE DES TRIBUNAUX. 1836. *Justice Civile. Journal de jurisprudence et des débats juiciaires*. Edition de Paris., 1836, Sv. Samedi 10 Décembre 1836, 3506.

GÖPPINGER, H. 1980. *Kriminologie*. Mnichov : Beck, 1980. ISBN 9783406073434.

GRAHAM, Roderick S. a SMITH, Shawn K. 2019. *Cybercrime and Digital Deviance. Londýn* : Routledge, 2019. ISBN 9781351238076.

HADNAGY, Ch. 2011. *Social engineering: the art of human hacking*. Indianapolis : Wiley, 2011. ISBN 9781118029718.

HAFNER, K a MARKOFF, J. 1995. *Cyberpunk: Outlaws and Hackers on the Computer Frontier*, Revised. místo neznámé : Simon and Schuster, 1995. ISBN 9780684818627.

HEIDE, L. 2004. *Monitoring People: Dynamics and Hazards of Record Management in France 1935-1944*. Technology and Culture. JSTOR, 2004, Vol. 45, 1.

JACOBS, Sanford L. 1976. *Blue Boxes Spread From Phone Freaks To the Well-Heeled*. The Wall Street Journal. 29. leden 1976.

JIRÁSEK, P., NOVÁK, L. a POŽÁR, J. 2013. *Výkladový slovník kybernetické bezpečnosti - třetí aktualizované vydání*. Praha : Jirásek, Novák, Požár, 2013. ISBN 9788072514366.

KOLOUCH, J. 2019. *Cybersecurity*. Praha : CZ.NIC, z.s.p.o., 2019. ISBN 9788088168348.

KOLOUCH, J. 2019. *Cybercrime*. Praha : CZ.NIC, z.s.p.o., 2019. ISBN 9788088168188.

LAMANI, B. R. a VENUMADHAVA, G. S. 2013. *Police Corruption in India. International Journal of Criminology and Sociological Theory*. 2013, Sv. 6, 4.

LAPSLEY, P. 2013. *Exploding The Phone: The Untold Story Of The Teenagers And Outlaws Who Hacked Ma Bell*. místo neznámé : Grove Press, 2013. ISBN 9780802120618.

MARKOFF, J. 2001. *The Odyssey Of a Hacker: From Outlaw To Consultant. New York Times*. National Edition, 2001, Sv. January 29th, Section C, Page 1.

MIDDLETON, B. 2017. *A History of Cyber Security Attacks: 1980 to Present*. Boca Raton, FL : CRC Press, 2017. ISBN 9781351651905.

MILLHORN, Thomas H. 2007. *Cybercrime: How to Avoid Becoming a Victim*. Boca Raton, FL : Universal-Publishers, 2007. ISBN 9781581129540.

NOVOTNÝ, Č., VLACH, J. a KUDRLOVÁ, K. 2019. *Škody působené kybernetickou kriminalitou*. Praha : Institut pro kriminologii a sociální prevenci, 2019. ISBN 9788073381752.

PEHRSON, B. 1994. *The Early History of Data Networks*. místo neznámé : Wiley-IEEE Computer Society Pr, 1994. ISBN 9780818667824.

REEP-VAN DEN BERGH, M. M. C. a JUNGER, M. 2018. *Victims of cybercrime in Europe: a review of victim surveys*. Crime Sci. 7, 2018, Sv. 5.

REUTERS. 1990. *2 W. Germans Get Suspended Terms as Computer Spies. Los Angeles Times*. 16. únor 1990.

ROGERS, H.C.B. 2005. *Napoleon's Army*. South Yorkshire : Pen & Sword Military, 2005. ISBN 9781844153107.

ROSENBAUM, R. 1971. *Secrets Of The Little Blue Box*. Esquire. 1971, Říjen.

ROUBALOVÁ, M. a kol. 2019. *Oběti kriminality - Poznatky z viktimizační studie*. Praha : Institut pro kriminologii a sociální prevenci, 2019. ISBN 9788073381745.

SHINDER, Littlejohn D. 2002. *Scene of the Cybercrime: Computer Forensics Handbook*. Rockland, MA : Syngress Publishing Inc., 2002. ISBN 9781931836654.

STOLL, C. 1988. *Stalking the Willy Hacker. Communication of the ACM*. Květen, 1988, Sv. 31, 5.

SVATOŠ, R. 2012. *Kriminologie*. Plzeň : Vydavatelství a nakladatelství Aleš Čeněk, 2012. ISBN 9788073803896.

WALL, D. 2001. *Crime and the Internet*. Londýn : Routledge, 2001. ISBN: 9780415244282.

WALLER, D. 2016. *GCSE Computer Science for OCR*. Cambridge : Cambridge University Press, 2016. ISBN 9781316504031.

2. Seznam použitých elektronických zdrojů

AUSTRALIAN CYBER SECURITY CENTER. 2020. *Malicious insiders*. ACSC. [Online] 23. červen 2020. [Citace: 8. září 2020.] https://www.cyber.gov.au/acsc/view-all-content/threats/malicious-insiders.

BERG-GANZARAIN, J. *Inside the Tech Support Scam Ecosystem*. Pindrop Blog. [Online] Pindrop. [Citace: 27. Srpen 2020.] https://www.pindrop.com/blog/inside-the-tech-support-scam-ecosystem/.

CENTER FOR SECURITY STUDIES. 2017. *Hotspot Analysis: Stuxnet*. [Online] Říjen 2017. [Citace: 10. únor 2021.] https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-04.pdf.

CENTRIFY. 2019. *Privilleged Access Management in the Modern Threatscape*. Centrify. [Online] 2019. [Citace: 2021. 3. červen] https://www.centrify.com/media/4909003/centrify_pam_survey.pdf.

ČESKÝ STATISTICKÝ ÚŘAD. 2020. *Informační společnost v číslech*. [Online] 2020. [Citace: 2. březen 2021.] https://www.czso.cz/csu/czso/informacni-spolecnost-v-cislech-2020.

CLULEY, G. 2013. *Naked Security. The LulzSec hackers who boasted they were "Gods" await their sentence*. [Online] Sophos, 16. květen 2013. [Citace: 7. září 2020.] https://nakedsecurity.sophos.com/2013/05/16/lulzsec-hackers-wait-sentence/.

CORDEIRO, Luis J. 2008. *Telephones and Economic Growth. A Worldwife Long-Term Comparison with Emphasis on Latin America and Asia*. [Online] 2008. [Citace: 27. leden 2021.] https://www.ide.go.jp/library/English/Publish/Reports/Vrf/pdf/441.pdf.

CROWDSTRIKE SERVICES. 2019. *Cyber Front Lines Report*. [Online] 2019. [Citace: 7. únor 2021.] https://apollo-is.com/white_papers/crowdstrike-services-cyber-front-lines-report/.

DENNING, Dorothy E. 2001. *Activism, Hacktivism, and Cyberterrorism*. The Internet as a Tool for Influencing Foreign Policy. [Online] 8. červen 2001. [Citace: 20. leden 2020.] http://faculty.nps.edu/dedennin/publications/Activism-Hacktivism-Cyberterrorism.pdf.

EOYANG, M, a další. 2018. *To Catch a Hacker*. [Online] 29. říjen 2018. [Citace: 5. květen 2020.] https://www.thirdway.org/report/to-catch-a-hacker-toward-a-comprehensive-strategy-to-identify-pursue-and-punish-malicious-cyber-actors.

FIREEYE. 2019. *Double Dragon. APT41, a dual espionage and cyber crime operation*. [Online] 2019. [Citace: 22. leden 2021.] https://content.fireeye.com/apt-41/rpt-apt41/.

FIREEYE. 2020. *M-Trends Report*. [Online] 2020. [Citace: 8. září 2020.] https://content.fireeye.com/m-trends.

HERJAVEC, R. 2019. *The History Of Cybercrime, From 1834 To Present*. Cybersecurity CEO. [Online] 18. červenec 2019. [Citace: 13. únor 2021] https://www.herjavecgroup.com/history-of-cybercrime/.

HOCHHEISER, S. 1989. *The American Telephone and Telegraph Company. AT&T Archives* . [Online] 1989. [Citace: 15. červen 2020.] https://www.beatriceco.com/bti/porticus/bell/pdf/tattc.pdf.

IBM SECURITY. 2020. *Cost of a Data Breach Report*. IBM.com. [Online] Červenec 2020. [Citace: 19. listopad 2020.] https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/pdf.

IMPERVA. *Advanced persistent threat (APT)*. Learning center. [Online] [Citace: 2020. Srpen 23.] https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/.

INSTITUTE FOR INFORMATION LAW. 2018. *Global Online Piracy Study*. [Online] Červenec 2018. [Citace: 14. duben 2021.] https://www.ivir.nl/publicaties/download/Global-Online-Piracy-Study.pdf.

KASPERSKY. 2019. *Kaspersky Security Bulletin '19*. Statistics. [Online] 2019. [Citace: 15. únor 2020.] https://go.kaspersky.com/rs/802-IJN-240/images/KSB_2019_Statistics_EN.pdf.

KASPERSKY. 2019. *What Is an Advanced Persistent Threat (APT)*. [Online] Kaspersky. [Citace: 23. srpen 2020.] https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats.

LIVEOVERFLOW. 2019. *The Origin of Script Kiddie - Hacker Etymology*. LiveOverflow Blog. [Online] 12. květen 2019. [Citace: 8. říjen 2020.] https://liveoverflow.com/the-origin-of-script-kiddie-hacker-etymology/.

MEHTA, I. 2019. *The Need for Better Metrics on Cybercrime*. [Online] 1. říjen 2019. [Citace: 12. říjen 2020.] https://www.thirdway.org/memo/the-need-for-better-metrics-on-cybercrime.

MICROSOFT DEFENDER ATP RESEARCH TEAM. 2018. *Teaming up in the war on tech support scams*. Security blog. [Online] 20. duben 2018. [Citace: 27. srpen 2020] https://www.microsoft.com/security/blog/2018/04/20/teaming-up-in-the-war-on-tech-support-scams/.

MICROSOFT. 2018. *Global Tech Support Scam Research*. [Online] Září 2018. [Citace: 27. srpen 2020.] https://news.microsoft.com/uploads/prod/sites/358/2018/10/Global-Results-Tech-Support-Scam-Research-2018.pdf.

MINDER, K. 2020. *DarkReading. How the Dark Web Fuels Insider Threats*. [Online] 23. duben 2020. [Citace: 8. září 2020.] https://www.darkreading.com/endpoint/how-the-dark-web-fuels-insider-threats/a/d-id/1337599.

MINISTERSTVO VNITRA ČR. 2021. *Prevence kriminality*. [Online] 2021. [Citace: 1. červen 2021.] https://www.mvcr.cz/clanek/web-o-nas-prevence-prevence-kriminality.aspx?q=Y2hudW09Mw%3d%3d.

MINISTERSTVO VNITRA ČR. 2019. *Zpráva o situaci v oblasti vnitřní bezpečnosti a veřejného pořádku na území České republiky v roce 2018*. [Online] květen 2019. [Citace: 14. březen 2021.] https://www.mvcr.cz/soubor/zprava-o-situaci-v-oblasti-vnitrni-bezpecnosti-a-verejneho-poradku-na-uzemi-cr-v-roce-2018.aspx.

MINISTERSTVO VNITRA ČR. 2020. *Zpráva o situaci v oblasti vnitřní bezpečnosti a veřejného pořádku na území České republiky v roce 2019*. [Online] 2020. [Citace: 14. březen 2021.] https://www.mvcr.cz/soubor/zprava-o-vbavp-2019-verze-2-5-prijate-rev-vvb-1.aspx.

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. 2019. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2019*. [Online] 18. září 2019. [Citace: 20. listopad 2020.] https://www.nukib.cz/download/publikace/zpravy_o_stavu/NUKIB_ZSKB_2019.pdf.

PAGANINI, P. 2019. *Hacking communities in the Deep Web*. [Online] 15. leden 2019. [Citace: 27. srpen 2020.] https://resources.infosecinstitute.com/hacking-communities-in-the-deep-web/.

POLICIE ČR. *Jednotlivé druhy kyberkriminality*. Kyberkriminalita. [Online] [Citace: 4. srpen 2020.] https://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx.

POLICIE ČR. 2019. *Zveřejněné informace*. Kyberkriminalita. [Online] 2019. [Citace: 12. únor 2020.] https://www.policie.cz/clanek/kyberkriminalita.aspx.

PONEMON INSTITUTE. 2019. *The Cost of Cybercrime*. [Online] 2019. [Citace: 20. listopad 2020.] https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf.

QUALYS SSLLABS. *SSL Pulse*. [Online] [Citace: 3. červen 2021.] https://www.ssllabs.com/ssl-pulse/.

SABADASH, V. 2004. *A Latency of Computer Crimes. Computer Crime Research Center*. [Online] 5. duben 2004. [Citace: 22. srpen 2020.] http://www.crime-research.org/articles/sabad03_2004/2.

SAMUEL, Whitney A. 2004. *Hacktivism and the Future of Political Participation*. [Online] Září 2004. [Citace: 17. leden 2021.] https://www.alexandrasamuel.com/dissertation/pdfs/Samuel-Hacktivism-entire.pdf.

SELIN, S. 2020. *Napoleonic Telecommunications: The Chappe Semaphore Telegraph*. [Online] 2020. [Citace: 10. červenec 2020.] https://shannonselin.com/2020/05/chappe-semaphore-telegraph/.

SLOAN, R. 2020. *Companies Name One of the Biggest Cybersecurity Threats: Their Employees*. [Online] The Wall Street Journal, 21. Červen 2020. [Citace: 8. září 2020.]

https://www.wsj.com/articles/companies-name-one-of-the-biggest-cybersecurity-threats-their-employees-11592606115.

SOPHOS. 2020. *The State of Ransomware*. [Online] Květen 2020. [Citace: 30. prosinec 2020.] https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf.

STERGIOU, D a GIANTAS, D. 2018. *From Terrorism to Cyber-terrorism*: The Case of ISIS. [Online] 7. březen 2018. [Citace: 23. srpen 2020.] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3135927.

THOMAS, K. V. 2004. *Police Corruption in India*. [Online] 2004. [Citace: 4. únor 2021.] https://www.svpnpa.gov.in/images/npa/Publications/journals/2004janjun.pdf.

VLACH, J., KUDRLOVÁ, K. a PALOUŠOVÁ, V. 2020. *Kyberkriminalita v kriminologické perspektivě*. [Online] 2020. [Citace: 30. duben 2021.] http://www.ok.cz/iksp/docs/463.pdf. ISBN 9788073381899.

3. Seznam použitých právních předpisů

Zákon č. 181/2014 Sb., Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů

Zákon č. 40/2009 Sb., Trestní zákoník, ve znění pozdějších předpisů

Zákon č. 45/2013 b., Zákon o obětech trestných činů, ve znění pozdějších předpisů

Zákon č. 108/2006 Sb., Zákon o sociálních službách, ve znění pozdějších předpisů

4. Seznam ostatních použitých zdrojů

ISO/IEC 27001:2013 - Information security management

ISO/IEC 27005:2018 - Information security risk management

ISO/IEC 27017:2015 - Code of practice for information security controls based on ISO/IEC 27002 for cloud services

NIST Cybersecurity Framework (CSF)

Seznam obrázků a grafů

Seznam příloh

Příloha č. 1

Informovaný souhlas účastníka výzkumu:

Vážený pane, vážená paní,

v souladu se zásadami etické realizace výzkumu[1] Vás žádám o souhlas s Vaší účastí ve výzkumném projektu v rámci diplomové práce:

Název projektu: Kriminologické aspekty kybernetické kriminality
Řešitel projektu: Peter Gemeri
Název pracoviště: Katedra trestního práva Právnické fakulty Univerzity Karlovy v Praze
Vedoucí práce: doc. JUDr. Bc. Tomáš Gřivna, Ph.D.
Cíl výzkumu: Rešerše stavu a vývoje preventivních opatření proti kybernetické kriminalitě
Popis výzkumu: Vaše účast na výzkumu bude probíhat formou polostrukturovaného rozhovoru v délce 1-2 hodin. Písemný transkript tohoto rozhovoru bude použit jako vstup pro praktickou část diplomové práce a bude v jejím rámci i publikován. Rozhovor bude nahráván na digitální diktafon. Znění otázek Vám bude poskytnuto v časovém předstihu 1-2 týdnů před samotným rozhovorem. V případě nesouhlasu se zveřejněním Vašich identifikačních údajů (Jméno, pracovní pozice, zaměstnavatel) budou tyto informace anonymizovány. Vaše účast na výzkumu je dobrovolná a máte možnost jej bez udání důvodu kdykoliv opustit.

…….
datum a podpis řešitele projektu

Prohlášení a souhlas účastníků s jejich zapojením do výzkumu:

Prohlašuji a svým níže uvedeným vlastnoručním podpisem potvrzuji, že dobrovolně souhlasím s účastí ve výše uvedeném projektu a že jsem měl/a možnost si řádně a v dostatečném čase zvážit všechny relevantní informace o výzkumu, zeptat se na vše podstatné týkající se účasti ve výzkumu a že jsem dostal/a jasné a srozumitelné odpovědi na své dotazy. Byl/a jsem poučen/a o právu odmítnout účast ve výzkumném projektu nebo svůj souhlas kdykoli odvolat bez represí resp. mého dítěte.

Jméno a příjmení účastníka:……. Datum narození:……

Adresa trvalého bydliště účastníka:…….

Podpis účastníka: ……

[1] Všeobecnou deklarací lidských práv, nařízením Evropského parlamentu a Rady (EU) č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) a dalšími obecně závaznými právními předpisy *(jimiž jsou zejména Helsinská deklarace přijatá 18. Světovým zdravotnickým shromážděním v roce 1964, ve znění pozdějších změn (Fortaleza, Brazílie, 2013), zákon č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách), ve znění pozdějších předpisů, zejména ustanovení jeho § 28 odst. 1, a Úmluva na ochranu lidských práv a důstojnosti lidské bytosti v souvislosti s aplikací biologie a medicíny: Úmluva o lidských právech a biomedicíně publikované pod č. 96/2001 Sb. m. s., jsou-li aplikovatelné).*

Otázky:

1. Jaká je Vaše historie v oboru informační bezpečnosti?
2. V jaké oblasti působí Váš současný zaměstnavatel?
3. Spadá Vaše současné působiště pod ISO27000, ZKB, GDPR, PCIDSS nebo jinou regulaci kybernetické bezpečnosti?
4. V čem spatřujete největší kybernetické riziko současnosti pro soukromé/právnické osoby?
5. Který druh pachatele (především z hlediska motivace, národnost, technická zdatnost, násilnost…) a kybernetické trestné činnosti (skutková podstata, způsob provedení, rozsah škody) považujete za nejpravděpodobnější/nejnebezpečnější?
6. Jaké aktuální trendy v oblasti kybernetické kriminality a její prevence pozorujete?
7. Jaká preventivní opatření jsou momentálně zavedena ve Vašem současném působišti? Jaká opatření se plánují zavést v budoucnu?
8. Co je podle Vás nejdůležitějším preventivním opatřením v politice kybernetické bezpečnosti?
9. Co naopak z Vaší zkušenosti nepřináší slibovanou přidanou hodnotu?
10. Jaký prostor je z Vaší zkušenosti věnován kybernetické bezpečnosti v každodenním chodu právnických osob?
11. Máte zkušenost s trestním řízením jako následkem kybernetické kriminality?
12. Používáte v rámci bezpečnostní politiky frameworky nebo standardy třetích stran?

Příloha č. 2

Textový přepis rozhovoru: Peter Gemeri – Radek Živný (Organizace 1), 23.10.2020

PG: Jaká je Vaše historie v oboru kybernetické bezpečnosti?

RŽ: Moje historie sahá zpět přibližně 20 let. Postupně jsem prošel několika IT pozicemi v různých společnostech, mimo jiné například v Komerční bance. Od správce systému, analytika a programátora, až jsem se stal členem nově vytvořeného týmu informační bezpečnosti v Českém Telekomu. Vzhledem k tomu, že zde tou dobou informační potažmo kybernetická bezpečnost prakticky neexistovala, měl jsem možnost se podílet na jejím vytváření na zelené louce. V Českém Telekomu jsem se také podílel kolem roku 2002 na implementaci jednoho z prvních řešení SIEM v České republice.

V té době nebyl svět kyberprostoru svázán prakticky žádnou legislativní regulací. Existovaly sice standardy třetích stran, jako například tzv. Orange Books (Department of Defense Trusted Computer System Evaluation Criteria – pozn. autora), jejichž autorem bylo ministerstvo obrany Spojených států amerických, nicméně jejich aplikace byla čistě dobrovolná. My jsme je tehdy chápali jako best practice, byl to pro mě obecný informační rámec. Základy úspěšné bezpečnostní politiky ale byly tehdy stejné jako dnes. Jsou jimi především kvalitní specifikace požadavků, analýza rizik a následný monitoring.

Po akvizici Českého Telekomu španělskou společností Telefónica jsem se díky zkušenosti z Telco dostal do pozice Chief Security Officera v O2 Czech Republic, potažmo v CETIN (ten vznikl jako samostatný poskytovatel fixní a mobilní síťové infrastruktury v roce 2015 oddělením od O2 Czech Republic – pozn. autora), kde jsem zastřešoval agendu informační bezpečnosti pro celou společnost. Dále jsem působil jako Security Architect ve Škoda Transportation. V současnosti pracuji na pozici specialisty informační bezpečnosti ve společnosti Organizace 1. Mimo zaměstnání se věnuji školení etického hackingu, řízení bezpečnosti informací a dalších oblastí kybernetické bezpečnosti. Jsem také certifikovaný vedoucí auditor ISMS podle ISO 27001.

PG: Zmiňujete dlouhou praxi napříč několika obdobími a odvětvími, jaký je tedy podle Vás současný stav kybernetické bezpečnosti? Je riziko kybernetické kriminality nižší, nebo naopak vyšší než před dvaceti lety?

RŽ: Dle mého se riziko újmy v důsledku kyberkriminality nijak zásadně nemění, protože je stále extrémně vysoké. Je třeba brát v potaz fakt, že bezpečnostní technologie se vyvíjejí adekvátně metodám narušení bezpečnostního perimetru. Metody průniku do perimetrů a extrakce dat, které fungovaly několik let zpět, jsou už dnes díky možnostem automatické detekce zastaralé a nefunkční. Problém je v tom, že současné kybernetické útoky jsou dnes vedeny velice specificky. Dochází k cílení na konkrétní procesy a uživatele, škodlivý kód se píše na míru, často je používán sofistikovaný phishing, kterému předchází detailní analýza subjektu ať už metodami typu OSINT (Open-Source Intelligence – pozn. autora), potažmo i nasazením malicious insidera přímo do firmy. Vynalézavosti pachatelů se opravdu meze nekladou, což často vede k selhání zmiňovaných automatických prevenčních mechanismů.

Přetrvávající brzdou kybernetické bezpečností jsou stále ekonomické náklady na nové technologie. V současnosti ve většině českých společností existují dva zaběhnuté organizační modely informační bezpečnosti. Buď je informační bezpečnost součástí úseku informačních technologií a reportuje společnému nadřízenému, nebo funguje odděleně od IT a reportuje přímo členovi statutárního orgánu, například v rámci divize operačních rizik. Oba modely mají své

výhody a nevýhody, nicméně abych navázal na předchozí myšlenku - velice často jsem se v minulosti setkal s tím, že v případě integrace do IT dochází ke kanibalizaci rozpočtu na kybernetickou bezpečnost. Druhým nešvarem, se kterým se v českém prostředí setkávám po celou dobu mojí kariéry je, že se kybernetické bezpečnosti dává adekvátní ekonomická pozornost až na základě dostatečně kritického bezpečnostního incidentu nebo auditu. Obojí má za následek, že kybernetická bezpečnost ve firmách často nefunguje proaktivně, ale pouze reaguje na již existující hrozby.

PG: Vy máte jistě díky svému návratu do prostředí finančnictví zajímavé srovnání. Co byste řekl, že je tou hlavní změnou, která za dvacet let na tomto poli proběhla?

RŽ: Při porovnání mé zkušenosti z Komerční banky před dvaceti lety se současným stavem jsou zdejší pojetí, technologie i integrace kybernetické bezpečnosti diametrálně odlišné, a to v pozitivním smyslu slova. Nicméně nutno zmínit, že tamní stav byl před dvaceti lety byl tak napřed, že již tehdy odpovídal současnému stavu kyberbezpečnosti v ostatních odvětvích. Pokud bych měl vypíchnout jednu věc, tak to je přístup k uživatelům.

V současnosti mají uživatelé na svých pracovních stanicích oprávnění striktně pouze k tomu, co potřebují k výkonu práce. Tím se jednak razantně minimalizuje prostor pro případnou nákazu, zároveň se zmenšuje i možnost k elevaci práv útočníka. Dnes zde již mluvíme o prostředí na bázi whitelistů, tedy že specificky definujeme, co uživatel může, nikoliv co nesmí. Toto je stav, ke kterému mají dle mého ostatní segmenty na českém trhu cestou dlouhou minimálně dva roky. Nemalý podíl na tom má podstav bezpečnostních odborníků na trhu práce.

PG: Nedostatek lidí se v oblasti kybernetické bezpečnosti skloňuje relativně často, čím myslíte, že je to způsobeno?

RŽ: Myslím, že to je hlavně tím, že je potřebná detailní technická znalost chráněných systémů. Zmiňoval jsem společnosti, kde je informační bezpečnost (jejíž součástí je kybernetická bezpečnost) oddělena od IT, čímž dochází k oproštění od každodenního styku s aktuálními technologickými trendy. Osobně si navíc myslím, že otázka důsledné separace bezpečnosti od IT je dnes již překonaná, protože spolupráce těchto dvou entit je klíčová k zajištění úspěšného fungování celé firmy.

V extrémních případech dochází k patovým situacím, kdy bezpečnostní týmy nedokážou posoudit, jak svěřené informační systémy chránit, protože zkrátka nerozumí technologiím, na kterých jsou vystavěny. Je smutnou pravdou, že pokud někdo v oblasti kybernetické bezpečnosti aktivně nedrží krok s dobou, velice rychle zakrní a snižují se jeho předpoklady pro úspěšnou kariéru. Tady vidím jako zásadní téma iniciativu firmy, která ve vlastním zájmu musí podporovat sebevzdělávání bezpečnostního personálu. Nutno nicméně podotknout, že v případě, kdy o to samotný zaměstnanec zájem nemá, je velice obtížné ho přesvědčit. Toto vede ve finále k tomu, že se v oboru drží pouze omezené množství nadšenců, kteří střídavě rotují mezi zaměstnavateli.

PG: Názor na zahrnutí informační bezpečnosti do IT je trochu proti současnému trendu. Co se změnilo, že se vracíme k modelu, který známe z dob, kdy kybernetická bezpečnost teprve začínala?

RŽ: Vidím za tím dva důvody. Prvním je, že současní šéfové IT berou otázku bezpečnosti na rozdíl od minulosti velice vážně. Druhým důvodem je, že dnes již existuje ověřený best practice model, co se týče dělení rozpočtu mezi IT a bezpečnost a to sice, že 5 až 10 % investic do IT by mělo být vyhrazeno pro informační a kybernetickou bezpečnost.

PG: Jaký je Váš názor na k legislativní regulaci kybernetické kriminality a kybernetické bezpečnosti? Je vůbec reálné tuto oblast postihnout v rámci právního předpisu?

RŽ: Vzhledem k tomu, že jsem se byl přítomen u vzniku a připomínkování zákona o kybernetické bezpečnosti vím, že jeho hlavním myšlenkovým východiskem byl standard ISO

27000. Česká republika byla v tomto ohledu jedním z prvních států, které tento přístup adaptovali. ISO 27000 je pro mě základem pro kybernetickou bezpečnost, odvíjí se od něj nejen zákon o kybernetické bezpečnosti, ale také GDPR (Nařízení Evropského parlamentu a Rady o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů) nebo PCI DSS (Payment Card Industry Data Security Standard).

Celkově myslím, že vliv této legislativy je veskrze pozitivní. Vidět to je mimojiné na úrovni kybernetické bezpečnosti všech subjektů, které pod ZKB spadají, ať jde o některé orgány státní správy nebo provozovatele kritické infrastruktury. Většina současné legislativy pramení v dokumentech z BSI Group a NIST, a proto nelze říct, že by v ní byly nějaké zásadní rozdíly.

PG: Mají pro Vás tyto normy nějakou přidanou hodnotu?

RŽ: Chápu je především jako vodítko a mantinely, ve kterých se pohybuji při vytváření konkrétních opatření či politik. Norma obsahuje oblasti, které nelze při zabezpečování prostředí opomenout.

Toto je nutné doplnit o aktuální trendy best practice, které se týkají technologické stránky věci. Nejlépe to lze vysvětlit na příkladu: ISO tvrdí, že je nutná ochrana přístupu uživatelů přihlašovacím jménem a heslem, které je maximálně odolné. K tomu současný stav best practice zní, že heslo má být dlouhé minimálně 12 znaků a obsahovat 3 ze 4 znakových sad. V praxi mám pak jasnou představu, co a jak nastavit nebo doporučit. Norma je zkrátka polovina znalosti a vždy je potřeba ji obohatit o současné trendy.

PG: A jaké ty trendy v současnosti jsou? Jaké útoky jsou nejčastější? Co firmy nejčastěji dělají proto, aby tomu zabránily?

RŽ: Za posledních 5 let nabral obrovskou popularitu buzzword „ransomware“. To je typ škodlivého programu, který má za cíl poškodit či znepřístupnit informace na nakaženém systému a pak za jejich opětovné zpřístupnění požaduje od oběti výkupné.

I přes snahu firmy vyškolit zaměstnance formou e-learningových školení, awareness sessions atd. se vždy najde někdo, kdo pravidla poruší. To, zda se nákaza rozšíří, pak záleží už pouze na vyspělosti prevenčních a detekčních mechanismů, které firma má. Ransomware i přes svoje specifické chování je malware jako každý jiný. Do systému ho musí někdo pustit, případně mu udělat cestu, například zneužitím zranitelnosti na firewallu.

Nutno podotknout, že celkového z počtu bezpečnostních incidentů, je tento typ útoku (externí nákaza z venku) zastoupený nejméně. Majoritní právě incidenty s interním prvkem. Z mé zkušenosti je poměr cca 10-20 případů zaměstnaneckého fraudu, proti třem pokusům o překonání firewallu, hacknutí, nasazení backdooru apod.

Jedná se o klasický interní fraud a různé druhy pomsty zhrzených zaměstnanců nebo třeba úmyslný únik dat. Bohužel i v prostředí kybernetické bezpečnosti platí, že příležitost dělá zloděje. Firmy proti tomuto bojují mnoha způsoby, nasazují technologie jako SIEM, IPS a IDS. Problém s těmito systémy je, že generují obrovské množství událostí, které je nutné efektivně zpracovat. Toto je asi největší kámen úrazu, protože při nastavování váhy jednotlivých upozornění vycházíme vždy pouze z vlastního předpokladu a doporučení, ale lidská vynalézavost je bezmezná.

Zažil jsem případy, kdy zaměstnanci našli v interní účetní aplikaci zranitelnost, díky které bylo možné odlévat peníze „bokem“. Nikdo nic nehacknul, neprolomil – administrátor pouze díky svým právům v systému spustil skript a umožnil automaticky schválit všechny nákupní objednávky pod 150 000,- Kč. Z hlediska bezpečnostních ochran je to vyhodnoceno jako legitimní situace. Uživatel měl právo to udělat, tak proč mu bránit. Selhání bylo samozřejmě na straně interního schvalovacího procesu, ale apriori tuto situaci do té doby nikdo nepředpokládal, proto jí ani kontrolní mechanismy nemohly zabránit.

Běžná populace si s pojmem kyberkriminalita spojuje sofistikované hackerské útoky. Pravda je taková, že zločinec stále používá selský rozum a hledá nejslabší článek.

PG: Takže velká část bezpečnostních incidentů má původ v interních uživatelích. Jsou to aktivity spíše úmyslné, nebo nedbalostní?

RŽ: Co se týče nedbalostních věcí, jako prozrazená hesla, omyly v přístupových právech, tak to nikdy nemělo zásadní dopad. Z mého pohledu proto tyto uživatelské „omyly" není nutno řešit nad běžný rámec, např. domluvou. Zajímáme se víceméně výhradně o úmyslnou činnost.

PG: Z Vaší zkušenosti nastupují lidé už s myšlenkou, že něco provedou?

RŽ: Minimálně. Zpravidla to je někdo, kdo je ve firmě delší dobu. Jednak má více zkušeností s tím, jak to ve firmě chodí, a navíc za tu dobu stihne nasbírat mnoho důvodu proč si přilepšit - stagnace platu, negativní vztahy na pracovišti atp. Když se naskytne příležitost, jak si beztrestně přivydělat, rychle ji využijí.

PG: A jak tomu zabránit?

RŽ: Na úrovni kvalitního monitoringu. Dnes se tomu říká SIEM. Já během své kariéry implementoval SIEM několikrát. Existuje mnoho druhů technologií, ale premisa je vždy stejná. Jde o databázi událostí, do které reportují všechny IT systémy ve firmě. Nad touto hromadou záznamu je pak potřeba nastavit vnitřní logiku a limity, které v případě že dojde k jejich překročení vygenerují upozornění.

Pravidel existuje nespočet, může to být například počet nesprávných přihlášení, množství schválených objednávek, průnik externí IP adresy do interního systému. Ta pravidla se v průběhu času vyvíjí a upravují. Děláme to více méně podle vlastních zkušeností, bohužel nelze tady použít nějakou jednotnou konfiguraci, protože každé informační prostředí má úplně jiné předpoklady.

PG: Takže cesta budoucnosti je SIEM?

RŽ: Ne tak zcela. Jak jsem zmiňoval, je potřeba SIEM „ušít" na míru. Mnohokrát jsem se setkal s tím, že do SIEM padá obrovské množství informací ze všech systémů, které pak ale nedokáže nikdo logicky roztřídit a využít. Taková masa dat po pár měsících skončí tak, že se v ní nikdo nevyzná a generuje obrovské množství irelevantních upozornění. To přináší víc starostí než užitku.

Je například hezké, že dnešní operační systémy dokáží generovat podrobné záznamy o všech operacích, které provedou. Realita je ale ta, že 99 % těchto informací k ničemu neslouží. Oproti tomu pak existují softwarové relikvie, např. staré účetní systém, které logovat pořádně ani neumí, a přitom riziko je u nich násobně vyšší.

Dnes bych proto doporučil k SIEM přistupovat opačně, minimalisticky. Jasně definovat rizikové oblasti a pro ty potom postupně implementovat scénáře. Všemu musí předcházet důsledná business impact analýza.

Klasický SIEM je pro mě dneska mrtvá záležitost. Osobně myslím bych to dnes zafixoval někde na úrovni nějakého ad-hoc managementu a nad tím stavěl vlastní vrstvu, která by byla specifická pro prostředí, ve kterém nacházíš. Já jsem třeba byl ve stavu, kdy jsem implementoval s IT firmami jako HP nebo IBM jejich SIEM řešení, nicméně to bylo pouze na úrovni technologie. To znamená, ty firmy měly problém vůbec SIEM implementovat a více či méně se neustále opíraly o funkcionalitu, která tam byla defaultně nastavena od počátku na úrovni jednoduchých pravidel. Pokud k tomu někdo nepřistoupil, jako majitel problému se znalostí prostředí, tak to bylo naprosto k ničemu a skončilo to problémem.

Osobně myslím, že dneska se technologie SIEM nachází ve slepé uličce. Já, kdybych dneska byl majitel firmy, tak si SIEM nekoupím. Spíše bych šel do úrovně nestrukturovaného dohledu, toho co vím, že chci kontrolovat. Dával bych do budoucna prioritu řešení, které rozezná kontext,

co se s kontrolovanou oblastí děje. Tady je prostor dát volnost umělé inteligenci, kterou je ale opět nutno odladit v kontextu s tím, co je pro firmu důležité. Alfa a omega těchto projektů je kvalitní zadání, které musí jasně obsahovat informace o tom, kdo poskytne relevantní zdroje dat, jak je budeme vyhodnocovat a jakou jim máme dát prioritu a kritičnost.

Nechci tím říci, že by firmy neměly znalost svého prostředí, ale často se stane, že IT dodavatel přinese pouze technologii, která je tupě postavená. Jde o případy, kdy 40 až 50 % datového obsahu SIEM jsou výchozí logy, které generuje každý informační systém. Mě ale zajímají pouze oblasti, kde eventuelně firma může přijít o peníze. Takže v případě finanční skupiny mne budou zajímat finanční systémy, v případě telco operátora mě budou zajímat billingy, telco-systémy a další systémy, které zaručují integritu komunikace. Proto jsem spíše zvyklý nejprve udělat analýzu rizik a říct si: Tady jsou směrodatné systémy, kde firma může přijít o peníze a následně postavím ochranu tak, aby to odpovídalo zjištěným rizikům.

Je hezké monitorovat dneska Windows stanice a servery, ale ta pravděpodobnost je tam opravdu nízká, oproti třeba SAP se špatně nastaveným schvalovacím workflow může být likvidační, ale málokterá firma takové operace v SIEM audituje.

PG: Takže pokud to chápu správně, považujete za nejdůležitější na začátku stanovit si kritické součásti informačního systému a monitorovat pouze kritické události, abych se vyvaroval riziku, že pro stromy nevidím les?

RŽ: Je nutné, abyste věděl, co děláte a měl přehled o tom co chcete skutečně uchránit. Nejhorší past je alibisticky spoléhat na antiviry, behaviorální analýzy apod., ale jaké je skutečné riziko sofistikovaného hackerského útoku oproti zaměstnanci, který se o to může pokoušet každý měsíc, týden, den? Nejdůležitější element je podle mě lidský faktor. Stroj se chová konzistentně, ale člověk nikoliv, ať už je to chování, které způsobí nákazu ransomwarem, krádež, či únik a ztrátu informací.

PG: Takže procesní opatření jsou efektivnější než technické překážky?

RŽ: Jasně, lidé jsou velice vynalézaví. Ve chvíli, kdy vědí, že máte DLP, URL filtering nebo cokoliv jiného, tak to nebudou zkoušet prolomit, ale půjdou okolo. My jsme jednou řešili docela zajímavý případ. V podstatě jsme udělali test DLP, kdy jsme vytvořili fiktivní strategickou prezentaci firmy na příští rok. Prezentace měla být pro 40 uživatelů v dané firmě a my jsme každou prezentaci označili unikátním kódem, který byl viditelný na jednotlivý snímcích. Kolik bys řekl, že z těch 40 lidí tu prezentaci nafotilo a poslalo dál?

PG: Nepochybuji o tom, že jich bylo více, když to zmiňujete. Nedokáži říci, kolik procent.

RŽ: Bylo jich 12 – to je přes čtvrtinu. Ale síťové ani koncové DLP nezachytilo nic. Oni prezentaci prostě ofotili na mobil a pak ji poslali ke svým kamarádům a k nám se to potom dostávalo z různých zdrojů. Na základě daného kódu jsme pak byli schopni identifikovat konkrétního člověka. 12 lidí to vzalo, okopírovalo a poslalo dál. Ať už ke konkurenci, nebo k jiným účelům.

PG: Lze tomuto vůbec zabránit?

RŽ: Je to prostě riziko podnikání. Jde hodně o filozofii firmy a o míru loajality zaměstnanců. A bohužel, pokud je to ve vyšších sférách, tam je to hodně postaveno na penězích. Ve zmíněném případu to byli všechno vysoce postavení manažeři, běžný zaměstnanec tam nebyl žádný. Měli šanci něco získat a pouze to chtěli vytěžit a získat z toho peníze.

PG: Fungují tedy podle Vás lépe tvrdá preventivní opatření případně spojená s represí negativního chování nebo spíše uživatelská osvěta?

RŽ: Nejlépe funguje represe. Ve chvíli, kdy budete spoléhat na osvětu, tak obsáhnete pouze určité procento lidí. Fraud je spojený s tím, že lidé jsou nespokojení, nedocenění, chtějí se dostat dál, chtějí mít víc peněz. Zažil jsem například skupinu uživatelů, kteří si maskovali objednávání výpočetní techniky a místo toho si kupovali televize, kávovary, kola. K odhalení došlo ve chvíli, kdy jednoho ze svých kolegů přeskočili a neobjednali mu televizi. A on je udal, akorát to udělal přes interní internetovou proxy. Takže napsal e-mail zvenku, ale na našem firewallu to bylo vidět. Šlo o škodu asi za 8 milionů a fungovalo to tak 4 roky.

PG: Znamená to, že firma by se nejvíce měla bát lidí, které sama přijala?

RŽ: Z mých osobních statistik pochází 80 % problémů zevnitř

PG: Jsou to spíše lidé na vyšších postech, nebo naopak malé ryby?

RŽ: Jsou to zaměstnanci na vyšších postech, případně marketingová a obchodní oddělení. Tam je největší problém. V závěsu jsou lidé z oddělení klientské podpory. Na těchto místech dochází k rychlé rotaci osob, požadavky na přijetí jsou minimální. Mají přístup k účtům, informacím o klientech a tak dále. Navíc zde pracují lidé z různých sociálních skupin, často s negativním vlastnostmi jako alkoholismus, drogy apod. Když za nimi někdo přijde a řekne jim, že chce za pár tisíc koupit detaily o konkrétní osobě, většinou uspěje.

PG: Z médií lze nabýt dojmu, že kyberkriminalita je postavená výhradně na sofistikovaných exploitech softwaru, ale nejjednodušší cesta je často ta nejkratší. Je tomu tak?

RŽ: Nikdy jsem nezažil, že by si někdo objednal hack na míru. Buďto šlo o anonymně adresovaný malware, který někdo omylem spustil, nebo šlo o techniky, které jsou všeobecně známé. Za 20 let v oboru pro mě byl největší problém vždy vnitřní nepřítel, to znamená uživatel. Ten, který je nevyzpytatelný, u kterého nejsi schopen poznat, jestli je loajální či nikoliv. Zažil jsem interní kybernetický incident v rozmezí od škody pár stokorun až po cca 48 milionů korun. Ve srovnání největší kybernetický incident zvenčí byla nákaza ransomware, kde obnova stála cca 1 milion.

PG: Máte zkušenost i s trestním řízením jako následkem takového prohřešku?

RŽ: Ano, šlo o případy úniku telekomunikačních dat. V případě podvodů se to vždycky řešilo osobní domluvou. Zaměstnanec raději ty věci zaplatil a uznal vinu. Vždy byl problém jít k soudu, protože pro daného hříšníka by to byla stopka.

PG: Hrozí kybernetická kriminalita i soukromým osobám?

RŽ: Jedna věc jsou např. Nigerijské spamy. To je oblast, ve které propadne opravdu minimální počet lidí. Pak tu jsou incidenty, kdy může být uživateli podstrčen na stanici cryptominer, ale vzhledem k hardwarové náročnosti těžby kryptoměn se to už útočníkům nevyplatí. Stále je relevantní ransomware a další malware, ale to už není věc, která by směřovala na jednotlivce. K němu se to samozřejmě dostat může, ale primárně tyto hrozby směřují na firmy, nemocnice, státní úřady.

PG: Má smysl, aby se organizace, ve které uživatel pracuje, snažila bránit ho před kybernetickou kriminalitou i v soukromém životě?

RŽ: Nemyslím si, a ani sami uživatelé to takto nevnímají. Snaží se to mít hlavně co nejjednodušší. V práci musí zadat 10 hesel, každé musí mít 12 míst a podobně. Takže uživatel bude mít raději doma prostředí bez hesla, za co nejmenší náklady, protože počítač je pro něj věc, přes kterou se chce podívat na internet a nakoupit si něco v e-shopu. Pro útočníky jsou zajímavé skutečně korporace, velké subjekty nebo organizace, které mají vazby na státní správu.

Příloha č. 3

Textový přepis rozhovoru: Peter Gemeri – Jan Beránek (Organizace 2), 30.7.2021

PG: Jaká je Vaše historie v oboru informační bezpečnosti?

JB: V oboru informační bezpečnosti působím od roku 2010, kdy jsem nastoupil na pozici vedoucího informační bezpečnosti ve středně velké finanční instituci. Po téměř deseti letech jsem změnil působiště, nyní zastávám podobnou roli v jiné firmě.

PG: V jaké oblasti působí Váš současný zaměstnavatel?

JB: Jedná se o jednu z menších bank na českém trhu.

PG: Spadá Vaše současné působiště pod ISO27000, ZKB, GDPR, PCIDSS nebo jinou regulaci kybernetické bezpečnosti?

JB: Ano, spadá. Nad rámec výše zmíněných lze uvést například ještě požadavky na kybernetickou bezpečnost subjektů zapojených do platebního systému SWIFT, což se také typicky týká všech bank.

PG: V čem spatřujete největší kybernetické riziko současnosti pro soukromé/ právnické osoby?

JB: Nejrizikověji vnímám únik a zneužití uživatelských identit, respektive přihlašovacích údajů. Za nebezpečné považují též nedostatky v procesu správy zranitelností a obecně lidský faktor.

PG: Který druh pachatele a kybernetické trestné činnosti považujete za nejpravděpodobnější a nejnebezpečnější?

JB: Odpovědí na obě otázky je nekalá aktivita neloajálního zaměstnance.

PG: Jaké aktuální trendy v oblasti kybernetické kriminality a její prevence pozorujete?

JB: Z mojí zkušenosti jde především o specializaci rolí a kompetencí, a to jak na straně útočníků, tak security týmů. Dále se dnes v kyberbezpečnosti klade výrazně větší důraz na maturitu procesů a spolehlivost kontrolních mechanismů.

PG: Jaká preventivní opatření jsou momentálně zavedena na Vašem současném působišti a jaká opatření plánujete zavést v budoucnu?

JB: Vzhledem k tomu, že chápu kybernetickou bezpečnost jako skládání vícero obranných vrstev, nepovažuji za účelné uvádět jmenný seznam. Ve zkratce pokrýváme oblasti podle best practice tak, jak je stanoveno např. v ISO 27000. Aktuálně se ale důrazně soustředíme na oblast uživatelských oprávnění. Zavádíme nový systém na centrální správu všech identit v bance, tzv. IDM a v blízké budoucnosti budeme začínat s projektem na centrální řízení privilegovaných přístupů (Privilege access management).

PG: Co je podle Vás nejdůležitějším preventivním opatřením v politice kybernetické bezpečnosti?

JB: Z těch technických je to sandboxing veškeré příchozí komunikace. Dále je důležitý výběr zaměstnanců, nejlépe se zahrnutím screeningu.

PG: Co naopak z Vaší zkušenosti nepřináší slibovanou přidanou hodnotu?

JB: Myslím, že hlavně z pozic vyššího managementu se nepřiměřeně velké naděje vkládají do DLP systémů. DLP řeší jen následky způsobené dřívějšími příčinami v řetězci – nekvalitní výběr uživatelů, nedostatečné bezpečnostní povědomí a další chybějící procesy.

PG: Jaký prostor je z Vaší zkušenosti věnován kybernetické bezpečnosti v každodenním chodu právnických osob?

JB: Domnívám se, že stále relativně malý, ale s výrazně rostoucím trendem.

PG: Máte zkušenost s trestním řízením jako následkem kybernetické kriminality?

JB: Za svou kariéru jsem se s tím ještě nesetkal, takže nemám.

PG: Používáte v rámci bezpečnostní politiky frameworky nebo standardy třetích stran?

JB: Ano, používáme jak obecně známé standardy typu NIST či ANSSI, tak interní metodiky vypracované pro konkrétní účely třetí stranou, jako například standardy pro bezpečnost vývoje interních aplikací.

Criminological aspects of cybercrime

Abstract (EN)

This thesis is a study of specific aspects of cybercrime in regards to banking and non-banking financial institutions in Czech republic. By comparing results of third-party analytical resources and own findings obtained by strategically performed interviews with personnel in leading positions in cyber-security careers, the thesis describes causes and results of cyber-attacks and related preventive measures with emphasis on their respective place and priority in the cybersecurity policy of the organization. The main finding is that the biggest risk to the organization seems to be its own employees. That is why the entity cannot simply trust in the security of its perimeter by protecting only its border, but has to also consider its internal part.

An equally important finding is the fact that mechanisms for the prevention of cybercrime take a large number of non-mutually exclusive forms, and in order to maintain the highest possible level of security, it is appropriate to layer these measures into complex units.

Keywords

Cybercrime, cybersecurity, criminology, financial organizations, cybercrime prevention

Kriminologické aspekty kybernetické kriminality

Abstrakt (CZ)

Práce se věnuje specifickým aspektům kybernetické kriminality páchané na bankovních a nebankovních poskytovatelích finančních služeb na českém trhu. Metodou srovnání analytických zdrojů a vlastních zjištění z rozhovorů s osobami na vedoucích pozicích v oblasti kybernetické bezpečnosti jsou hledány příčiny a následky kybernetických útoků a doporučeny navazující preventivní opatření včetně jejich postavení a prioritizace v konceptu politiky informační bezpečnosti organizace. Hlavním zjištěním je, že největší míru kybernetického rizika s sebou nese pro organizaci její zaměstnanec. Organizace proto nemůže spoléhat při zabezpečení svých informačních systémů pouze na ochranu svého perimetru na jeho hranici, ale také uvnitř něj. Neméně významným nálezem je také fakt, že mechanismy pro prevenci kybernetické kriminality mají velkou řadu vzájemně se nevylučujících forem, a v zájmu zachování co nejvyšší míry zabezpečení je vhodné tyto opatření vrstvit do komplexních celků.

Klíčová slova

Kyberkriminalita, kybernetická bezpečnost, kriminologie, finanční organizace, prevence kybernetických útoků