VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, Z. Ú., ČESKÉ BUDĚJOVICE

BAKALÁŘSKÁ PRÁCE

KYBERNETICKÁ BEZPEČNOST VE VEŘEJNÉ SPRÁVĚ

Autor práce: Lukáš Poskočil, DiS.

Studijní program: Bezpečnostně právní činnost

Forma studia: Kombinovaná

Vedoucí práce: RNDr. Růžena Ferebauerová

Katedra: Katedra právních oborů a bezpečnostních studií

2022

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, z. ú.
Žižkova tř. 6, 370 01 České Budějovice

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jméno a příjmení studenta: Lukáš Poskočil

Studijní program: Bezpečnostně právní činnost
Forma studia: Kombinovaná
Místo studia: Příbram

Název bakalářské práce: Kybernetická bezpečnost ve veřejné správě

Název bakalářské práce v anglickém jazyce: Cyber security in public administration

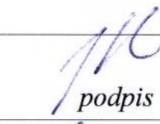
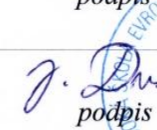
Katedra: Katedra právních oborů a bezpečnostních studií
Vedoucí bakalářské práce (jméno a příjmení, titul): RNDr. Růžena Ferebauerová

Datum zadání bakalářské práce (měsíc, rok): říjen 2021

Cíl bakalářské práce:
Cílem bakalářské práce je zhodnotit současnou bezpečnost v kybernetickém prostoru ve veřejné správě, a to zejména s ohledem na zajištění bezpečnosti veškerých dat, s kterými veřejná správa disponuje, včetně poukázáním na jednotlivá negativa a pozitiva. Na základě tohoto se autor v závěrečných pasážích své bakalářské práce pokusí nastínit úvahy eliminace možných rizik v kybernetickém prostoru s využitím získaných dat z výroční Zprávy o stavu kybernetické bezpečnosti České republiky za rok 2020.

Student: Lukáš Poskočil	19.11.21 *datum*	 *podpis*
Vedoucí práce: RNDr. Růžena Ferebauerová	19.11.21 *datum*	 *podpis*

Schvaluji zadání bakalářské práce:

Vedoucí katedry: doc. JUDr. Roman Svatoš, Ph.D.	6.12.2021 *datum*	 *podpis*
Prorektor pro studium a vnitřní záležitosti: doc. PhDr. Miroslav Sapík, Ph.D.	8.12.2021 *datum*	 *podpis*
Pověřený rektor: doc. Ing. Jiří Dušek, Ph.D.	14.12.2021 *datum*	 *podpis*

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně, na základě vlastních zjištění a s použitím odborné literatury a materiálů uvedených v seznamu použitých zdrojů.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce v elektronické podobě ve veřejně přístupné části infodisku VŠERS, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky vedoucí a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce systémem na odhalování plagiátů.

.....

Děkuji vedoucímu bakalářské práce RNDr. Růženě Ferebauerové, za cenné rady, připomínky a metodické vedení práce.

ABSTRAKT

POSKOČIL, L. *Kybernetická bezpečnost ve veřejné správě*: bakalářská práce. České Budějovice: Vysoká škoda evropských a regionálních studií, 2022. 64 s. Vedoucí bakalářské práce: RNDr. Růžena Ferebauerová.

Klíčová slova: kybernetická kriminalita, kybernetický prostor, kybernetické útoky, zabezpečení kybernetického prostoru.

Tato práce na téma „Kybernetická bezpečnost ve veřejné správě“ pojednává o aspektech a specifikách kybernetických útoků zejména na instituce Policie České republiky, Hasičského záchranného sboru a Zdravotnického záchranného systému, tudíž instituce Integrovaného záchranného systému v rámci České republiky. Práce se snaží vystihnout současné trendy kybernetické kriminality a její nejpoužívanější útoky. Kybernetická kriminalita se stala v současné době dynamicky se rozvíjející podskupinou kriminality a páchá značné finanční škody. Proto hlavním aspektem v této práci je ohrožení života, zdraví a bezpečnosti občanů České republiky, kdy tyto útoky pachatelů mají fatální následky na akceschopnost Integrovaného záchranného systému.

ABSTRACT

POSKOČIL, L. Cyber security in public administration: BechelorThesis. České Budějovice: The College of European and Regional Studies, 2022. 64 p. Supervisor: RNDr. Růžena Ferebauerová.

Key words: cyber criminal, cyberspace, cyber attacks, cybersecurity.

This work on the theme of " Cyber security in public administration " deals with aspects and specifics of cyber attacks, especially against the institutions of the Police of the Czech Republic, Fire Rescue System and Medical Rescue System, that is to say institutions of the Integrated Rescue System of the Czech Republic. The work tries to capture the current trends of cybercrime and its most commonly used attacks, given that cybercrime has now become a dynamically developing subgroup of crime and causes significant financial damage. The main aspect of this work is the threat to the life, health and safety of citizens of the Czech Republic, when such attacks have fatal consequences for the operational abilities of the Integrated Rescue System.

Obsah

Úvod

Problematika kybernetické kriminality je v současnosti více než aktuální, přičemž její význam roste úměrně s tím, jak se rychle rozvíjejí informační technologie. Stručně lze říci, kybernetická kriminalita je na vzestupu, kdy v této práci se autor bude věnovat kybernetické bezpečnosti ve veřejné správě.

V úvodních částech práce se budu věnovat otázkám věnovaných teoretickým otázkám kybernetické kriminality. Zejména půjde o vymezení pojmů, které jsou úzce spjaty s kybernetickou kriminalitou. V dalších kapitolách se budu věnovat zabezpečení kyberprostoru v rámci počítačových sítí Integrovaného záchranného systému, který v současné době propojuje svůj Intranet s Internetem, kdy se jedná o velmi složitý proces pro zabezpečení citlivých dat, kterými tyto instituce disponují.

Žijeme v informačním věku, kdy informace má vysokou hodnotu a počítače s počítačovými sítěmi zacházejí s těmito informacemi. Právě počítače a jiná mobilní zařízení poskytují mnoho výhod široké skupině lidí. Počítač skýtá nejen výhody, ale jak se počítače rozšiřovaly z velkých podniků a škol, potažmo zejména z univerzit do domácností, rostlo i procento lidí, kteří se lehce naučili zacházet s počítači. Začali se zde objevovat i určité negativní jevy, které postupem času rozrostly až do obrovských komplikací. Bohužel i tento fakt s sebou nese modernizace. Počítač se tímto stává i určitou hrozbou, i přes veškeré své výhody.

Fenomén kybernetické kriminality je v dnešní době považován za velice aktuální téma. Toto téma kybernetické kriminality bylo probíráno již v roce 1990 v rámci 8. konference OSN konané v Havaně, která byla věnována právě prevenci kriminality. Zde byla kybernetická bezpečnost označena za jednu z nejnebezpečnějších forem trestné činnosti vedle distribuce drog a organizovaného zločinu. Tento fakt je dán i určitou nedostatečnou zkušeností uživatelů v kyberprostoru, nedostatečnou prevencí právě uživatelů či institucí, určitou anonymitou pachatelů a dostupnosti zařízení, s kterými je možné páchat trestné činy v oblasti kybernetické kriminality. Od této doby uplynulo celých 31 let, kdy kybernetická kriminalita nezmizela, spíše se dále vyvinula a rozvinula v opravu velký a těžce uchopitelný problém, zejména z právního hlediska. Složitosti ve správném uchopení kybernetické kriminality spočítá v pomalé reakci zákonodárců a správců sítě na rychle se rozvíjející problematiku kybernetické kriminality. Nemožností

korektního a přesného odhadu její budoucnosti a tím také vydávání účinnějších, ve své podstatě nadčasové, právní úpravy, protože se kriminalita páchaná v kyberprostoru stále každým dnem rozrůstá a vymezuje jiným způsobem než předchozí den. Bohužel i v oblasti kybernetické kriminality platí pravidlo, že pachatel je vždy o krok napřed před našimi zákonodárci a správci sítě.

O samotné kybernetické kriminalitě a jejích specifikách je dnes k dispozici nepřeberné množství dat a informací, avšak více zdrojů pochází právě z internetu než materiálů v tištěné podobě. Tento fakt je dán zejména tím, že internetové zdroje mohou být postupem času aktualizovány, což zaručuje zejména aktuálnost, která je pro tento problém a boj proti němu velmi důležitá. Oproti monografiím, učebnicím, oficiálním policejním zprávám se stal přirozeně sám internet největším, v některých případech taky nejdůležitějším, aktuálním a primárním zdrojem informací o kybernetické kriminalitě. Internet a sběr informací, které nám poskytuje, má však jisté úskalí, které je důvěrně známé všem uživatelům. Největším problémem sběru informací na internetu je ověření právě pravdivosti a relevantnosti získaných informací.

Cílem bakalářské práce je charakterizovat současné trendy kybernetické kriminality, zhodnotit a interpretovat zabezpečení integrovaného záchranného systému v České republice v kybernetickém prostoru.

1 Cíl a metodika bakalářské práce

Bakalářská práce se bude podrobně zabývat aktuální situací v kybernetické bezpečnosti. Druhům možných útoků, kterým v současné době čelí nejen veřejný kybernetický prostor, ale celá společnost. Taktéž se v bakalářské práci autor bude věnovat druhům zabezpečení, které se v současné době využívají k zabezpečení kybernetického prostoru. Autor se bude věnovat zejména institucím Policie České republiky, Hasičským záchranným sborem a Zdravotním záchranným sborem, tudíž instituce Integrovaného záchranného systému v rámci České republiky.

Práce bude rozdělena do 2 částí. První část, kterou lze charakterizovat jako teoretickou, bude informačně bohatší a obsahově rozsáhlejší. K jejímu zpracování budou využity metody shromažďování dat, analýzy a syntézy. Druhá část, kterou lze označit jako praktická, bude věnována praktickému zabezpečení kybernetického prostoru ve veřejné správě a to konkrétně v Integrovaném záchranném systému.

V prvé kapitole budou uvedeny cíle práce a metody, které budou využity k jejímu zpracování.

Druhá kapitola bude věnována základní definici kybernetické kriminality.

Ve třetí kapitole budou popsány nejčastější útoky v kybernetickém prostoru.

Ve čtvrté části jsou vysvětleny pojmy subjekty zúčastněné v rámci kybernetické kriminality.

Pátá kapitola bude obsahovat základní zabezpečení sítě Integrovaného záchranného systému České republiky.

V šesté kapitole jsou uvedeny informace ke kybernetické bezpečnosti v České republice.

Sedmá kapitola je shrnuta zpráva o stavu kybernetické bezpečnosti České republiky za rok 2020.

V osmé kapitole je uveden rozvoj vývoje kybernetických útoků s její možností eliminace.

Těžiště práce je popisnou metodou vysvětlit základní pojmy kybernetické kriminality a její vývoj se zaměřením na Integrovaný záchranný systém s eliminací hrozeb, které kybernetickému prostředí hrozí.

2 Kybernetická kriminalita

Vzhledem k tomu, že obor kybernetické kriminality je velmi složitý a existuje mnoho náhledů na danou problematiku je těžké pojem kybernetická kriminalita nějakým stylem uchopit. Důvodem pro její obtížné vymezení je taktéž její dynamický rozvoj, který je spjat s rozvojem informačních technologií, který neustále prudce stoupá a postupně se stává součástí naší společnosti. Převážná většina zdrojů, která se týká kybernetické kriminality, se často shoduje v nepřesném vymezení kybernetické kriminality.

2.1 Pojem kybernetická kriminalita

Kybernetická kriminalita jako pojem je vymezena mnoha autory a existuje velké množství definic, které jsou více či méně podobné. Dá se tedy říci, že zcela jednoznačná definice zřejmě neexistuje. Z čistě jazykového výkladu je možné kybernetickou kriminalitu volně vymezit jako trestnou činnost, která je v přímé souvislosti s počítači. Jakkoliv toto tvrzení může primárně působit jako dobře strukturované vymezení pojmu kybernetické kriminality, při detailnějším rozebrání může vykazovat jisté nedostatky v podobě rozsahu. Neboť není přesně určeno, co konkrétně je tímto druhem kriminality myšleno, respektive, kde leží pomyslná hranice této kriminality, a taktéž není přesně určen její vztah k ostatním druhům kriminality.

Samozřejmě by bylo poněkud jednotvárné tvrdit, že se jedná pouze o trestné činy a nesmíme opomenout i jiné delikty. V užším pojetí lze do kyberkriminality řadit např. i správní delikty.

Definice, která vymezuje tento pojem zpracovalo Ministerstvo vnitra České republiky, je specificky zaměřena a konkrétně zasazena do našeho prostředí. Tuto definici je možno dohledat v materiálu s názvem „*Analýza současného stavu a trendů vývoje trestné činnosti na úseku informačních technologií a Internetu včetně návrhu řešení*“ kde je uvedeno: „*pod pojmem počítačová kriminalita je třeba chápat páchání trestné činnosti, 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 této trestné činnosti, ovšem s výjimkou majetkové trestné činnosti, nebo jako nástroj trestné činnosti.“[1]

Smejkal již v roce 1995 definoval pojem počítačová kriminalita *„jako páchání trestné činnosti, 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:*

a) *jako předmět této trestné činnosti, ovšem s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako věci movité.*
b) *nebo jako nástroj trestné činnosti.“*[2]

2.2 Specifika kybernetické kriminality

Mezi zvláštnost v rámci kybernetické kriminality můžeme považovat dostupnost, anonymitu, nízké náklady, globálnost.

„V současnosti je většina kyberkriminality spojena s internetem, ale bez významu nejsou ani další sítě (např. uzavřená firemní síť bez připojení na internet, síť řídící procesy v elektrárně atp.). Jedná se o otevřený systém bez jediného řídícího centra, naopak drtivá většina aktivit (např. zobrazení webové stránky) probíhá vždy prostřednictvím několika serverů. Přenos dat mezi zařízeními tak mnohdy prochází přes různé státy, i když se obě zařízení nachází na stejném místě. Je proto mnohdy nejasné, ve které zemi jsou uložena data a přes které státy byla transportována.“[3] Právě kýžené odhalování a dokazování kyberkriminality se proto potýká s celou řadou problémů, zejména s omezeními plynoucími z přeszahraničního charakteru, oproti tomu se vyžaduje patřičné technické vybavení i odborné schopnosti.

[1] ČESKO. MINISTERSTVO VNITRA. *Analýza současného stavu a trendů vývoje trestné činnosti na úseku informačních technologií a Internetu včetně návrhu řešení.* [cit. 2021-12-05]. Dostupné z: <http://www.mvcr.cz/soubor/informacni-pdf.aspx>.
[2] SMEJKAL, V. *Kriminologie*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015. 640 s. ISBN 978-80-7478-615-3.
[3] GŘIVNA, T., POLČÁK, R., *Kyberkriminalita a právo*. Praha: Aufitorium, 2008. s 336. ISBN 978-80-9037-867-3.

První specifický znak kybernetické kriminality spočívá v dostupnosti, „*ve které kyberprostor existuje nezávisle na vůli jednotlivce 24 hodin 7 dní v týdnu. Každý okamžik se mění v data v něm obsažená a mohou probíhat škodlivé útoky.*“[4] V současné době je kybernetická kriminalita dostupná velkému okruhu společnosti. Kolem nás je všude dostupný internet, zařízení i softwary. Lze říci, že každý v této digitální době vlastní telefon, který je připojený a internet a počítač, jak přenosný tak popřípadě nepřenosný. Vzhledem k těmto možnostem, se můžeme připojit na internet kdykoliv a kdekoliv z těchto zařízení, kdy můžeme přijímat a taktéž odesílat jakékoliv data do sítě internetu.

Náklady, které jsou dalším specifikem kybernetické kriminality, můžeme považovat za poměrnou veličinu, protože v mnoha případech nám stačí pouze počítač či mobilní telefon, ale v dalších případech se jedná o nákladné částky k pořízení výkonných počítačů, různých softwaru a dalších součástek, které jsou potřeba k páchání kybernetické kriminality. Poukázal bych na publikaci Gřivny, kde se zaměřuje pouze na nízké náklady spojené se získáním velkého vlivu nebo způsobení velké škody. Pachateli podle *Gřivny „stačí pouze získat přístup k internetu (či k jiné požadované síti) a mít určitou uživatelskou schopnost.“*[5] V této definici nezahrnuje náklady na pořízení zařízení k páchání této kriminality.

Zejména globálnost kyberprostoru podle Gřivny *„vede často také k problematickému postihu prostřednictvím tradičního trestního systému založeného na státní suverenitě“*[6] a proto je dalším specifikem kybernetické kriminality.

Kyberprostor nemá hmotnou podstatu, je imaginární. Přesto jsou ale jeho vznik a existence závislé na světě reálném. *„Jde o nové sociálně interaktivní prostředí, jehož specifikum spočívá především v neexistenci časových a prostorových bariér, mnohonásobné konektivitě, anonymitě a možnostech změny on-line identity, což vytváří*

[4] GŘIVNA, T., SCHEINOST, M., ZOUBKOVÁ, I. *Kriminologie*. Praha: Wolters Kluwer, a.s, 2015. Sv. 4. vyd. 336 s. ISBN 978-80-7478-614-3.
GŘIVNA, T., SCHEINOST, M., ZOUBKOVÁ, I. *Kriminologie*. Praha: Wolters Kluwer, a.s, 2015. Sv. 4. vyd. 336 s. ISBN 978-80-7478-614-3.
[6] GŘIVNA, Tomáš; SCHEINOST, Miroslav; ZOUBKOVÁ, Ivana. *Kriminologie*. Praha: Wolters Kluwer, a.s, 2015. Sv. 4. vyd. 334 s. ISBN 978-80-7478-614-3.

nové formy a zákonitosti závadného jednání, které jsou kvalitativně odlišné od jiných druhů kriminality.“[7]

Dalším specifikem, které v kybernetické kriminalitě často uvádíme, je anonymita v prostředí, která „*je pouze zdánlivá, pachatel zanechává stopy, např. v podobě IP nebo MAC adresy zařízení, ze kterého vede svůj útok, v praxi však takovéto stopy nemusejí být využitelné.“*[8] V tomto případě bude pachateli stačit návštěva internetové kavárny, kterých je nejen v České republice bezpočet a je jednoduché použít k páchání kyberkriminality veřejně dostupný počítač. Nicméně taktéž existují programy, které zvládnou vaši IP nebo MAC adresu skrýt nebo dokonce přepsat na úplně jinou adresu, atd.

V poslední řadě pachateli hraje do karet latence, kterou je specifická kyberkriminalita. *„Oběť mnohdy ani netuší, že je cílem útoku, např. proto, že neodhalí ve svém zařízení tzv. spyware4 nebo neví, že dané jednání je trestné. Jindy poškozený nechce oznámit orgánům činným v trestném řízení napadení svých zařízení (např. z obavy ztráty důvěryhodnosti e-shopu či služby elektronického bankovnictví). K vysoké latenci přispívá též bezprostřední neviditelnost způsobených následků (oproti např. vloupání) a v některých případech i zpochybňována společenská škodlivost.“*[9]

[7] ŠÁMAL, P. a kol. Trestní zákoník II. §140 až 421. Komentář. 2. vydání. Praha: C. H. Beck, 2012, s. 845. ISBN 978-80-7400-428-5.
[8] GŘIVNA, T., SCHEINOST, M., ZOUBKOVÁ, I. *Kriminologie*. Praha: Wolters Kluwer, a.s, 2015. Sv. 4. vyd. 337 s. ISBN 978-80-7478-614-3.
[9] GŘIVNA, T., SCHEINOST, M., ZOUBKOVÁ, I. *Kriminologie*. Praha: Wolters Kluwer, a.s, 2015. Sv. 4. vyd. 338 s. ISBN 978-80-7478-614-3.

3 Nejčastější útoky v kybernetickém prostoru

V současnosti se dá hovořit, že přelom 20. a 21. století je přelom „starých“ a „nových“ forem kybernetické kriminality. V minulosti byla převážná většina trestné činnosti z podvodů, porušování autorských práv, které je často označováno, avšak nepříliš vhodně, jako počítačové pirátství. Dále útoky na funkčnost počítačových systémů, nejdříve fyzicky, následně častěji na dálku a to zejména pomocí virů. Neoprávněné nakládání s osobními údaji, neoprávněné užívání počítačů a dalších zařízení, jakož i různé druhy skutkových podstat spojených s šířením informacích (pornografie, nebezpečné vyhrožování a pronásledování, nekalá soutěž). Od „soukromých“ hackerů a útoků na peníze jsme se posunuli k útokům „státním“ a útokům na kritickou infrastrukturu anebo útokům ideologický a propagačním. Dnes se setkáváme především s těmito skutkovými podstatami, přičemž očekáváme jejich další vývoj a hlavně nárůst:

1. **kyberterorismus** v podobě útoků na funkčnost počítačových systémů a elektronických komunikací (zejména tzv. DoS a DDoS útoky, malware a spyware, elektromagnetické útoky atd.), vedoucí k naplnění skutkových podstat trestných činů jako jsou obecné ohrožení, poškození a ohrožení provozu obecně prospěšného zařízení, sabotáž,

2. **útoky na obsah počítačových systémů a předávaných zpráv** (vyzvědačství, ohrožení utajované informace),

3. **šíření informací** ve prospěch útočníka a/nebo v neprospěch protivníka, případně ovlivňující třetí strany.[10]

[10] SMEJKAL, V.. *Kriminologie*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015. 157 s. ISBN 978-80-7478-615-3.

Útoky v rámci kyberkriminality jsou různorodé a nejčastěji rozlišujeme podle Úmluvy o kybernetické kriminalitě na:

a) útoky proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů,
b) útoky spočívající ve vytváření a šíření škodlivého (tj. nelegálního nebo nežádoucího) obsahu,
c) útoky spočívající v porušování práv duševního vlastnictví,
d) tradiční kriminalita v novém kabátě – v širším pojetí, než zastává Úmluva, hovořící pouze o padělání a podvodu.[11]

3.1 Útoky proti důvěryhodnosti, integritě a dostupnosti počítačových dat a systémů

„Velká část kyberkriminality spočívá v malwaru, neboli škodlivém softwaru a tzv. sociálním inženýrstvím. Obvyklým postupem bývá průnik do systému, oklamání uživatele a poté použití získaných dat.“ [12]

V současné době využívají pachatelé důvěryhodné webové portály zaměřené na prodej zboží (market place, sbazar, bazos). Prodávajícímu zašlou pod vymyšlenou legendou internetový odkaz, který se tváří jako odkaz přepravních firem (DPD, Zásilkovna, Česká pošta). Tyto odkazy jsou velmi důvěryhodné. Do tohoto odkazu prodávající vyplní své údaje ke kreditní kartě včetně CVV/CVC (Card Verification Value - speciální trojmístné číslo, které slouží k autorizaci online plateb kartou), kdy si prodávající myslí, že mu částka za zboží bude následně připsána na bankovní účet. Poté, ale pachatel provede transakce na bankovním účtu, který je spjatý s kreditní kartou, ke které mu prodávající poslal všechny údaje, a odčerpá finanční hotovost.

[11] ETS No.:185, Convection of Cybercrime
[12] GŘIVNA, T., SCHEINOST, M., ZOUBKOVÁ, I. *Kriminologie*. Praha: Wolters Kluwer, a.s, 2015. Sv. 4. vyd. s. 340. ISBN 978-80-7478-614-3.

3.1.1 Průnik do systému a oklamání uživatele

„Průnik do systému může být cílem i prostředkem. Spočívá v překonání překážky, nejčastěji v podobě překonání softwarové ochrany nebo hesla (pomocí sociálního inženýrství nebo softwaru či hardwaru), případně oklamáním uživatele.“[13]

3.1.2 Prolamování hesel

„Prolomení je dle Výkladového slovníku kybernetické bezpečnosti charakterizováno jako neoprávněné proniknutí do systému.“[14] V tomto případě hovoříme o nejčastějším způsobu útoku proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů. Tuto kyberkriminalutu značí poměrně jednoduché zadávání a zkoušení hesel ke konkrétnímu účtu, které si uživatel sám nastavil při registraci, či zakládání.

„Při využívání sociálního inženýrství k prolomení hesla či získání přístupových údajů (např. k elektronickému bankovnictví) pachatel využívá psychické manipulace k ovlivnění jednání uživatele tak, aby ho přiměl k dobrovolnému sdělení hesla či jiné důvěrné informace.“ [15]

Prolamovač hesel je definován ve Slovníku kybernetické bezpečnosti *„jako program určený k luštění hesel, a to buď metodou Brute force attack nebo Dictionary attack.“*[16] Útok s použitím hrubé síly (anglicky Brute force attack) *„je metoda k zjišťování hesel, kdy útočící program zkouší jako možné heslo všechny existující kombinace znaků, dokud nezjistí skutečné heslo. Tento způsob je časově velmi náročný. Jeho úspěšnost je závislá na délce hesla, složitosti hesla a na výpočetním výkonu*

[13] GŘIVNA, T., SCHEINOST, M., ZOUBKOVÁ, I. *Kriminologie*. Praha: Wolters Kluwer, a.s, 2015. Sv. 4. vyd. s. 340. ISBN 978-80-7478-614-3.
[14] JIRÁSEK, P., NOVÁK. L., POŽÁR. J., Výkladový slovník kybernetické bezpečnosti. Praha: Policejní akademie České republiky v Praze, 2015. s. 92. ISBN 978-80-7251-436-6.
[15] GŘIVNA, T., SCHEINOST, M., ZOUBKOVÁ, I. *Kriminologie*. Praha: Wolters Kluwer, a.s, 2015. Sv. 4. vyd. s. 340. ISBN 978-80-7478-614-3.
[16] JIRÁSEK, P., NOVÁK. L., POŽÁR. J., Výkladový slovník kybernetické bezpečnosti. Praha: Policejní akademie České republiky v Praze, 2015. s. 92. ISBN 978-80-7251-436-6.

použitého počítače.“[17] *„Dictionary atack (neboli slovníkový útok) je metoda zjišťování hesel, kdy crackovací program zkouší jako možné heslo všechna slova ve slovníku. Jedná se o metodu poměrně rychlou, záleží to na velikosti slovníku a na tom, zda oběť používá jednoduchá hesla.“* [18]

3.1.3 Keylogger

Keylogger je software, který „*umožňuje automatické zaznamenávání všech stisků kláves (psaný text, hesla apod.), navštívených www stránek, chatů a diskuzí přes ICQ, MSN apod., spouštěných aplikací, screenshotů práce s počítačem, práce uživatele se soubory a další. Často se používá pro utajený monitoring všech aktivit na PC, jenž je pro ostatní uživatele neviditelný a chráněný heslem. Zaznamenaná data mohou být skrytě odesílána emailem.“* [19]

Gřivna uvádí, že k ochraně uživatele před prolomením hesla*, „záleží pouze na něm, jak silné heslo si zvolí, protože se rychlost prolomení se pohybuje v závislosti na schopnostech prolamovače od několika sekund u čtyř znaků až po několik let u osmi a více znaků.“* [20]

3.1.4 Phishing

Phishing neboli rybaření, házení udic, rhybaření. „*Jedná se o podvodnou metodu, usilující o zcizování digitální identity uživatele, jeho přihlašovacích jmen, hesel, čísel bankovních karet a účtu apod. za účelem jejich následného zneužití (výběr hotovosti z konta, neoprávněný přístup k datům atd.).“*

[17] JIRÁSEK, P., NOVÁK. L., POŽÁR. J., Výkladový slovník kybernetické bezpečnosti. Praha: Policejní akademie České republiky v Praze, 2015. s. 122. ISBN 978-80-7251-436-6.
[18] JIRÁSEK, P., NOVÁK. L., POŽÁR. J., Výkladový slovník kybernetické bezpečnosti. Praha: Policejní akademie České republiky v Praze, 2015. s. 105. ISBN 978-80-7251-436-6.
[19] JIRÁSEK, P., NOVÁK. L., POŽÁR. J., Výkladový slovník kybernetické bezpečnosti. Praha: Policejní akademie České republiky v Praze, 2015. s. 62-63. ISBN 978-80-7251-436-6.
[20] GŘIVNA, T., SCHEINOST, M., ZOUBKOVÁ, I. *Kriminologie*. Praha: Wolters Kluwer, a.s, 2015. Sv. 4. vyd. 340 s. ISBN 978-80-7478-614-3.

„Phishing spočívá ve vytvoření podvodné zprávy, šířené většinou elektronickou poštou, jež se snaží zmíněné údaje z uživatele vylákat. Dané zprávy mohou být maskovány tak, aby co nejvíce imitovaly důvěryhodného odesílatele. Může jít například o padělaný dotaz banky, jejíchž služeb uživatel využívá, se žádostí o zaslání čísla účtu a PIN pro kontrolu.“ [21]

Gřivna uvádí jako přiklad v publikaci Kriminologie. *„Pachatel například zašle na tisíce adres e-mail zdánlivě odcházející od důvěryhodné instituce (např. konkrétní banka) požadující ověření přístupových údajů k elektronickému bankovnictví z důvodu množících se útoků na ně.“* [22]

K této metodě je i přes častou informovanost uživatelů stále efektivní. Často se prezentují informace o dalších phishing útocích, avšak uživatelé jsou důvěřivý a metoda je stále úspěšná.

3.1.5 Pharming

Tuto metodu řadíme mezi *„podvodné metody používané na Internetu k získávání citlivých údajů od obětí útoku. Principem Pharmingu je napadení DNS a přepsání IP adresy, což způsobí přesměrování klienta na falešné stránky* internetbankingu, e-mailu, *sociální sítě, atd. po zadání URL do prohlížeče. Tyto stránky jsou obvykle k nerozeznání od skutečných stránek banky a ani zkušení uživatelé nemusejí poznat tuto záměnu na rozdíl od příbuzné techniky phishingu.“* [23]

Gřivna uvádí, že za *„útok pomocí Pharmingu může zejména nepozornost uživatele, kdy webová stránka pouze napodobuje důvěryhodný web (stejné logo, barvy,*

[21] JIRÁSEK, P., NOVÁK. L., POŽÁR. J., Výkladový slovník kybernetické bezpečnosti. Praha: Policejní akademie České republiky v Praze, 2015. s. 83. ISBN 978-80-7251-436-6.
[22] GŘIVNA, T., SCHEINOST, M., ZOUBKOVÁ, I. *Kriminologie*. Praha: Wolters Kluwer, a.s, 2015. Sv. 4. vyd. s. 340. ISBN 978-80-7478-614-3.
[23] JIRÁSEK, P., NOVÁK. L., POŽÁR. J., Výkladový slovník kybernetické bezpečnosti. Praha: Policejní akademie České republiky v Praze, 2015. s. 83. ISBN 978-80-7251-436-6.

rozložení obsahu atp.) URL adresa se však drobně liší – např. vynechává či přidává písmeno nebo je pod jinou doménou (např. „vláda.cz“ namísto „vlada.cz“).“ [24]

3.1.6 Další techniky a nástroje

„Cross site scripting, označovaný jako XSS, funguje na podobném principu jako Pharming, oproti Pharmingu, kdy se jedná o podvodnou „napodobeninu“ webové stránky, pachatel vloží do zdrojového kódu dané webové stránky vlastní kód, čímž může jednak změnit použití dialogového okna, předstírajícího, že je oknem banky – tzv. spoofing obsah stránek, jejich funkčnost atp., ale také získat přístup k osobním údajům uživatelů.“

„Za určitou formu průniku do systému lze považovat i tzv. Sniffing. Pachatel prostřednictvím speciálního softwaru či hardwaru zachycuje data probíhající v síti. Zneužití získaných dat je omezeno jejich případným šifrováním a jeho složitostí. „

Gřivna uvádí také fakt, *„že pachatelé se mohou ovšem spolehnout i na čistě technické prostředky průniku do systému a využití bezpečnostní chyby v programu. Hackeři tak činí za účelem potěšení z vlastních schopností, odhalení chyb a vylepšení daného systému, zatímco tzv. crackeři, o kterých se mylně v médiích hovoří jako o hackerech, za účelem dosažení neoprávněného prospěchu.“* [25]

3.1.7 Malware

Ve slovníku kybernetické bezpečnosti se definuje malware jako *„obecný název pro škodlivé programy. Mezi škodlivý software patří počítačové viry, trojské koně,*

[24] GŘIVNA, T., SCHEINOST, M., ZOUBKOVÁ, I. *Kriminologie*. Praha: Wolters Kluwer, a.s, 2015. Sv. 4. vyd. s. 340. ISBN 978-80-7478-614-3.
[25] GŘIVNA, T., SCHEINOST, M., ZOUBKOVÁ, I. *Kriminologie*. Praha: Wolters Kluwer, a.s, 2015. Sv. 4. vyd. s. 341. ISBN 978-80-7478-614-3.

červy, špionážní software.“ [26]Křivna k této problematice uvádí, že *„malware je hojně využíván k zásahům do počítačů a jiných zařízení. Předpokladem pro postižení tímto škodlivým programem zařízení je nainstalování nakaženého softwaru do cílového zařízení, což je učiněno obvykle nevědomky právě samotným uživatelem.“* [27]

3.1.8 Počítačové viry a červy

Vir je „typ malware, který se šíří z počítače na počítač tím, že se připojí k jiným aplikacím. Následně způsobuje tento typ škodlivého softwaru nežádoucí a nebezpečnou činnost.“ [28]

3.1.9 Trojský kůň

Dle Jirovského „*trojské koně patří mezi neoblíbenější hackerský nástroj současnosti. Jedná se o program, který plní na první pohled nějakou užitečnou funkci, ale ve skutečnosti má ještě nějakou skrytou škodlivou funkci. Trojský kůň se sám nereplikuje, šíří se díky viditelně užitné funkci, kterou poskytuje.“*[29] Trojské koně se používají na nejrůznější účely, od pouhého monitorování činnosti cílového počítače až po zneužití pro útok DoS.

Dále Jirovský uvádí další variantu trojských koní tzv. *„dataminery“ „neboli programy, které po nainstalování monitorují činnost uživatele a zajímavé údaje odesílají do sběrného místa. Ty poté rozlišuje podle předem známých kritérií, např. při přihlašování k účtu v bance zaznamená stisknuté klávesy, a tak prozradí hackerovi přístupové kódy k manipulaci s účtem.“*[30]

JIRÁSEK, P., NOVÁK. L., POŽÁR. J., Výkladový slovník kybernetické bezpečnosti. Praha: Policejní akademie České republiky v Praze, 2015. s. 115. ISBN 978-80-7251-436-6.

[27] GŘIVNA, T., SCHEINOST, M., ZOUBKOVÁ, I. *Kriminologie*. Praha: Wolters Kluwer, a.s, 2015. Sv. 4. vyd. s. 341. ISBN 978-80-7478-614-3.

[28] JIRÁSEK, P., NOVÁK. L., POŽÁR. J., Výkladový slovník kybernetické bezpečnosti. Praha: Policejní akademie České republiky v Praze, 2015. s. 125. ISBN 978-80-7251-436-6.

[29] JIROVSKÝ, Václav. Kybernetická kriminalita. 2007. Praha: Geada Publishing a.s. s. 67. ISBN 978-80-247-1561-2.

[30] JIROVSKÝ, Václav. *Kybernetická kriminalita*. Praha: Geada Publishing a.s., 2007. s. 67. ISBN 978-80-247-1561-2.

3.1.10 Spyware

„Program skrytě monitorující chování oprávněného uživatele počítače nebo systému. Svá zjištění tyto programy průběžně (např. při každém spuštění) zasílají subjektu, který program vytvořil, respektive distribuoval. Takové programy jsou často na cílový počítač nainstalovány spolu s jiným programem, například s počítačovou hrou, s jehož funkcí však nesouvisí.“[31]

Spyware dle Gřivny *„se snaží zůstat co nejdéle mimo pozornost uživatele, neboť sleduje jeho činnost a mapuje obsah uložených souborů, údaje následně odesílá pachateli. Získaná data jsou rozmanitá, od navštívených internetových stránek, přes „Data Mining“ – dolování dat, techniky pro vyhledávání souvislostí v rozsáhlých databázích přihlašovací údaje a soubory, jejich obsahem mohou být takové údaje, veškeré osobní údaje, e-mailové kontakty atp., až po průmyslovou špionáž.“*[32]

3.1.11 DoS, DDoS útoky

„DoS neboli odmítnutí služby je technika útoku na internetové služby nebo stránky, při níž dochází k přehlcení požadavky a k pádu nebo nefunkčnosti a nedostupnosti systému pro ostatní uživatele a to útokem jednotlivce.“[33]

„DDoS neboli distribuované odmítnutí služby je technika útoku na internetové služby nebo stránky, při níž dochází k přehlcení požadavky a k pádu nebo nefunkčnosti a nedostupnosti systému pro ostatní uživatele a to útokem mnoha koordinovaných útočníků.“[34]

[31] JIRÁSEK, P., NOVÁK. L., POŽÁR. J., Výkladový slovník kybernetické bezpečnosti. Praha: Policejní akademie České republiky v Praze, 2015. s. 111. ISBN 978-80-7251-436-6.
[32] GŘIVNA, T., SCHEINOST, M., ZOUBKOVÁ, I. *Kriminologie*. Praha: Wolters Kluwer, a.s, 2015. Sv. 4. vyd. s. 342. ISBN 978-80-7478-614-3.
[33] JIRÁSEK, P., NOVÁK. L., POŽÁR. J., Výkladový slovník kybernetické bezpečnosti. Praha: Policejní akademie České republiky v Praze, 2015. s. 78. ISBN 978-80-7251-436-6.
[34] JIRÁSEK, P., NOVÁK. L., POŽÁR. J., Výkladový slovník kybernetické bezpečnosti. Praha: Policejní akademie České republiky v Praze, 2015. s. 40. ISBN 978-80-7251-436-6.

3.2 Útoky spočívající ve vytváření a šíření škodlivého obsahu

Na internetu mimo níže popsaných útoků lze pozorovat i z hlediska škodlivého obsahu stránky, které poskytují návody ke spáchání útoku, jak vyrobit nástroj k páchání trestného činu atp. Dle Gřivny *„jsou některé návody v některých případech úmyslně nesprávné s cílem poškodit osobu postupující podle nich. Právě tento fakt se stává v dnešní době velmi kritický, kdy se různé organizace snaží radikalizovat své členy, pro takového člověka není nic snazšího, než si najít návod k přípravě např. výbušniny a poté ji použít.“*[35]

3.2.1 Dětská pornografie

Článek č. 9 Úmluvy o kybernetické kriminalitě zahrnuje pod škodlivý obsah na internetu problematiku dětské pornografie, tj. takové, která zobrazuje nebo jinak využívá dítě (osoba mladší 18 let) nebo osobu, jež se jeví dítětem.

„Trestním zákonem je postihováno jakékoli nakládání s dětskou pornografií, od prostého přechovávání po výrobu a distribuci.“[36] Dětská pornografie se stala celosvětovým problémem, protože je lehce rozšiřitelná, právě pomocí internetu.

Trestné činy, kde figuruje dítě nebo osoba nezletilá jsou vždy o to závažnější, protože tyto osoby obvykle neví, jak se bránit či dokonce toto chování považují za zcela normální. Pachateli pouze postačí získat důvěru dítěte či mladistvého nebo je přinutí násilím.

Dále Gřivna uvádí *„spojitost dětské pornografie s dětskou prostitucí, často dobrovolnou v podobě tzv. sextingu (zasílání vlastních sexuálně laděných portrétů) nebo zveřejňování tzv. selfie.“*[37]

[35] GŘIVNA, T., SCHEINOST, M., ZOUBKOVÁ, I. *Kriminologie*. Praha: Wolters Kluwer, a.s, 2015. Sv. 4. vyd. s. 345. ISBN 978-80-7478-614-3.
[36] GŘIVNA, T., SCHEINOST, M., ZOUBKOVÁ, I. *Kriminologie*. Praha: Wolters Kluwer, a.s, 2015. Sv. 4. vyd. s. 343. ISBN 978-80-7478-614-3.
[37] GŘIVNA, T., SCHEINOST, M., ZOUBKOVÁ, I.. *Kriminologie*. Praha: Wolters Kluwer, a.s, 2015. Sv. 4. vyd. s. 344. ISBN 978-80-7478-614-3.

3.2.2 Extremismus a násilí

Otázky soužití odlišných kultur, míra vzájemné tolerance a jejich mezí patří mezi nejpalčivější společenská témata euroatlantické civilizace. V dnešním globalizovaném světě, kde se stále více střetávají rozličné kultury, národy a národnosti, dochází i k útokům vůči „těm jiným“, vůči těm, kteří se nějak odlišují od majoritní společnosti. „*Jedná se o trestné činy motivované společenskými předsudky vztahujícími se k rase, náboženství, pohlaví a sexuální orientaci, národnostní a etnické příslušnosti či jiné odlišnosti.“*[38]

„Až dodatek Úmluvy o kybernetické kriminalitě rozšířil postih škodlivého obsahu o problematiku rasové a xenofobní nenávisti. V kyberprostoru se pohybuje řada skupin využívajících internet k šíření svých názorů, skryté komunikaci mezi sebou a získávání nových příznivců.“[39] V praxi se často můžeme setkat s extremismem a násilím na internetu, důvodem může být již zmiňovaná anonymita, kterou poskytuje kyberprostor.

3.2.3 Kybergrooming

Kybergrooming dle Slovníku Kybernetické bezpečnosti *„spočívá v nebezpečném chování uživatelů internetových komunikačních prostředků (chat, Facebook, atd.), kteří se snaží získat důvěru dítěte s cílem ho zneužít, zejména sexuálně či zneužít k nelegálním aktivitám.“*[40] Gřivna ve své publikaci Kriminologie uvádí Kybergrooming *„jako psychickou manipulaci oběti prostřednictvím informačních a komunikačních technologií s cílem jejího sexuálního využití.“*[41]

[38] GŘIVNA, Tomáš; POLČÁK, R. Kyberkriminalita a právo. Praha: Aufitorium, 2008. s. 144-145. ISBN 978-80-9037-867-3.
[39] GŘIVNA, T., SCHEINOST, M., ZOUBKOVÁ, I. *Kriminologie*. Praha: Wolters Kluwer, a.s, 2015. Sv. 4. vyd. s. 344. ISBN 978-80-7478-614-3.
[40] JIRÁSEK, P., NOVÁK. L., POŽÁR. J., Výkladový slovník kybernetické bezpečnosti. Praha: Policejní akademie České republiky v Praze, 2015. s. 69. ISBN 978-80-7251-436-6.
[41] GŘIVNA, T., SCHEINOST, M., ZOUBKOVÁ, I.. *Kriminologie*. Praha: Wolters Kluwer, a.s, 2015. Sv. 4. vyd. s. 344. ISBN 978-80-7478-614-3.

Pachatel neboli Kybergroomer „ *kontaktuje předem vybranou osobu, s níž obvykle pod (alespoň částečně) změněnou identitou dlouhodobě udržuje a prohlubuje vztah. Snaží se izolovat oběť od okolí a podporuje ji i drobnými dárky. Postupně mámí z oběti pornografické materiály až do její emoční závislosti. Kybergroomer poté požaduje po oběti osobní setkání, při kterém zpravidla oběť dál sexuálně využije.“*[42]

3.2.4 Kyberšikana

Kyberšikana je druhem šikany*, „který využívá elektronické prostředky, jako jsou mobilní telefony, e-maily, pagery, internet, blogy a podobně, k zasílání obtěžujících, urážejících či útočných mailů a SMS, vytváření stránek a blogů dehonestujících vybrané jedince nebo skupiny lidí.“*[43]

Kyberšikana se stala fenoménem dnešní doby, zejména u dětí je tato technika hojně využívaná k potřebě vědomě či nevědomě ublížit dané oběti. V souvislosti s kyberkriminalitou se hovoří zejména o psychické šikaně, která je mnohem hůře odhalitelná. Díky kyberprostoru je možnost šikanovat oběti mnohem lehčí, než šikanování v tváři tvář oběti. Dále se do šikanování může zapojit více lidí, a proto se šikanování stává více údernější a více zraňuje oběť šikany. Kyberprostor nabízí agresorům v některých případech tolik potřebnou anonymitu, protože by neměli tolik potřebnou odvahu šikanovat oběť tváří v tvář.

3.2.5 Hoax

„Neboli poplašná zpráva se snaží svým obsahem vyvolat dojem důvěryhodnosti. Informuje například o šíření virů nebo útočí na sociální cítění adresáta. Může

[42] GŘIVNA, T., SCHEINOST, M., ZOUBKOVÁ, I.. *Kriminologie*. Praha: Wolters Kluwer, a.s, 2015. Sv. 4. vyd. s. 344. ISBN 978-80-7478-614-3.
[43] JIRÁSEK, P., NOVÁK. L., POŽÁR. J., Výkladový slovník kybernetické bezpečnosti. Praha: Policejní akademie České republiky v Praze, 2015. s. 85. ISBN 978-80-7251-436-6.

obsahovat škodlivý kód nebo odkaz na internetové stránky se škodlivým obsahem.“[44] Cílem Hoax je nastolení chaosu a strachu, který je ve své podstatě neopodstatněný.

Dle Gřivny „*jsou nepravdivé zprávy jiným typem útoků, které šíří nežádoucí obsah, za cíl poškodit určitou fyzickou osobu, a to v rámci internetových diskusí, na sociálních sítích, webech atp. oproti tomu jsou hoaxy, které např. varují před domnělým nebezpečím, virem atp. takové zprávy uživatele obtěžují, snižují důvěru v obsah internetu a zatěžují síť, podobně jako spam, nevyžádaná obchodní sdělení.“*[45]

[44] JIRÁSEK, P., NOVÁK. L., POŽÁR. J., Výkladový slovník kybernetické bezpečnosti. Praha: Policejní akademie České republiky v Praze, 2015. s. 88. ISBN 978-80-7251-436-6.
[45] GŘIVNA, T., SCHEINOST, M., ZOUBKOVÁ, I.. *Kriminologie*. Praha: Wolters Kluwer, a.s, 2015. Sv. 4. vyd. s. 345. ISBN 978-80-7478-614-3.

4 Subjekty zúčastněné v rámci kybernetické kriminality

„Počítače a telekomunikační sítě umožňují pachatelům provádět útoky na obětí na dálku. Historie prvních online útoků nás zavede do Spojených států, zpět do osmdesátých let dvacátého století, do doby, kdy internet ještě neexistoval. Přesněji řečeno, koncept kyberútoků tak, jak jej vnímáme dnes, tvořil neoddělitelnou část procesu vytváření internetu.“[46]

4.1 Pachatel

Dle Završnika „*se pro pachatele kybernetické kriminality používá název počítačový hacker. Výraz byl vymyšlen studeny Massachusetts Institute of Technology, kde byl paradoxně i vybudován první moderní počítačový systém (Levy, 1984).“*[47] Gřivna dále charakterizuje typy pachatelů kybernetické kriminality, neboli hackerů:. „*Z hlediska charakteristiky pachatele záleží vždy na druhu či typu trestné činnosti, které se dopouští, neexistuje typický pachatel kyberkriminality, předpokladem je pouze základní uživatelská znalost kyberprostoru.“*[48] Vysoká anonymita internetu navíc má za příčinu pocit neodhalitelnosti u hackerů a i v téhle době poměrně nízký stupeň vnímání viktimizace a způsobených škod, které znamenají pro pachatele menší sociální tlak odrazující od protiprávního jednání.

Musíme mít ale na paměti, že hackerství dle Završnika *„z počátku nevedlo k negativním konotacím, ani destruktivním či vandalským činnostem. Při budování sítí šlo o běžný a žádoucí přístup části skupin, které se zabývaly programováním.“*[49] A v některých případech pracovali i pro stejnou společnost, pro kterou byl program či software navrhnut a vytvořen. „*Útočník, nebo pachatel pracuje v globálním prostředí, může se v kyberprostoru velmi rychle a nepozorovaně pohybovat, měnit identity nebo i mizet. Může vytvářet, předstírat nebo realizovat různé hrozby a vždy bude o krok*

[46] GŘIVNA, T., POLČÁK, R. Kyberkriminalita a právo. Praha: Aufitorium, 2008. s. 35. ISBN 978-80-9037-867-3.
[47] ZÁVRŠNÍK, A. *Kyberkriminalita*. Praha:Wolters Kluwer a.s. 2017. 128 s., ISBN 978-80-7552-758-5.
[48] GŘIVNA, T., SCHEINOST, M., ZOUBKOVÁ, I. *Kriminologie*. Praha: Wolters Kluwer, a.s, 2015. Sv. 4. vyd. 338 s. ISBN 978-80-7478-614-3.
[49] ZÁVRŠNÍK, A. *Kyberkriminalita*. Praha:Wolters Kluwer a.s. 2017. 128 s., ISBN 978-80-7552-758-5.

napřed. Může využívat variability předpisů v různých jurisdikcích nebo nedostatků ve vyšetřovacím procesu.“[50]

„Hackery lze v neposlední řadě dělit i na pachatele amatéry a profesionály. Důvodem se stávají některé typy útoků, které vyžadují hlubší znalosti práce s moderními komunikačními zařízeními – například DDoS, malware atp. Pro amatéry se jeví jednoduchost v páchání činů například v Naopak tzv. tradiční kriminalitě v novém kabátě, kde nejsou potřeba obvykle zvláštní schopnosti. Někdy je oddělována i zvláštní skupina – teroristé, které budou předmětem diskursu v budoucnosti, protože můžeme spatřovat velký trend právě v terorismu vedený přes internet.“[51]

4.2 Oběť

Je na místě zkoumat kybernetickou kriminalitu a její důsledky i z pohledu viktimologie (věda, nauka o oběti). Tyto získané poznatky mohou pomoci v prevenci, v další práci s obětmi nebo i s vyvíjením antivirových a bezpečnostních programů pro naše zařízení. Jak již bylo výše zmíněno, oběť mnohdy ani netuší, že se stala cílem útoku kybernetického charakteru. V dnešní době má běžný uživatel internetu několik e-mailových schránek, několik účtů na sociálních sítí, bankovnictví si může spravovat on-line, dostáváme se do doby, kdy si můžete víceméně vše, na co si vzpomenete zařídit během pár minut, bez toho, aniž byste museli vycházet z tepla domova. Podle doporučení by si takový běžný uživatel měl určit a nastavit ke každému svému účtu odlišné heslo, neměly by se v něm objevovat lehce zjistitelné údaje, jako je rok narození či telefonní číslo, ale přes to by mělo být dlouhé a v jisté míře složité. V tom se stává ten problém, v dnešním uspěchaném světě je více než nekomfortní mít pro všechny své účty odlišná hesla, proto se kybernetické útoky staly pro pachatele velmi jednoduchými a lehce proveditelnými. Oproti tomu tu stojí fakt, který uvádí Gřivna*, „že většina stižených subjektů (podniky a organizace) nemá zájem na zveřejnění útoku, který utrpěla, protože by to odhalilo jejich zranitelnost a omylnost. Zveřejnění by mohlo*

[50] JIROVSKÝ, V. *Kybernetická kriminalita*. Praha: Geada Publishing a.s., 2007. s. 19. ISBN 978-80-247-1561-2.
[51] GŘIVNA, Tomáš; SCHEINOST, Miroslav; ZOUBKOVÁ, Ivana. *Kriminologie*. Praha: Wolters Kluwer, a.s, 2015. Sv. 4. vyd. 338-339 s. ISBN 978-80-7478-614-3..

poškodit ekonomický úspěch těchto obětí, protože by zvýšilo nedůvěru v bezpečnost jejich služeb a tím snížilo důvěru veřejnosti.“[52]

[52] GŘIVNA, T., SCHEINOST, M., ZOUBKOVÁ, I. *Kriminologie*. Praha: Wolters Kluwer, a.s, 2015. Sv. 4. vyd. s. 36. ISBN 978-80-7478-614-3.

5 Základní zabezpečení sítě Integrovaného záchranného systému

5.1 Demilitarized zone servery

DMZ (anglicky *demilitarized zone*) je v počítačové bezpečnosti fyzická nebo logická podsíť, která je z bezpečnostních důvodů oddělena od ostatních zařízení. Jsou v ní umístěny služby, které jsou k dispozici většinou z celého Internetu. Účelem DMZ je přidání další bezpečnostní vrstvy v LAN (lokální sítě). To znamená, že případný útočník získá přístup pouze k zařízení, které je v DMZ, ale zbytek lokální sítě je v bezpečí. Jméno je odvozeno z termínu „demilitarizovaná zóna“, což je oblast mezi státy, ve které nejsou povoleny žádné vojenské akce.

V počítačové síti jsou nejvíce náchylní k útoku ti, kteří poskytují služby uživatelům mimo lokální síť, jako je e-mail, webové služby a DNS (Domain Name System). Vzhledem ke zvýšené pravděpodobnosti útoků na tyto poskytovatele, jsou jejich služby umístěny ve vlastních podsítích s cílem ochránit zbytek sítě před případně úspěšným útokem.

Počítače v DMZ mají omezené připojení k vybraným počítačům ve vnitřní síti, komunikace s ostatními počítači v DMZ může být omezena a s venkovní sítí je povolena. To umožňuje počítačům v DMZ poskytovat služby jak pro vnitřní, tak i pro vnější sítě, zatímco firewall kontroluje provoz pouze mezi servery v DMZ a klienty vnitřní i venkovní sítě.

DMZ jsou obvykle zabezpečené před útoky zvenčí, ale nemají vliv na vnitřní útoky, jako je odchytávání komunikace přes paketový analyzátor (např. Wireshark). [53]

[53] ANDRESS, J. *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice* (2nd ed.). 2014. s.241. Elsevier Science. ISBN 978-01-2800-812-6.

5.1.1 Služby poskytované v DMZ

Jakákoli služba, která je poskytována uživateli přes externí síť, může být umístěna do DMZ. Nejčastěji to jsou tyto služby:

- Webový server
- Mail Transfer Agent (MTA, přeprava elektronické pošty)
- File Transfer Protocol (FTP, SFTP, FTPS servery)
- VoIP brána

Webové servery, které komunikují s vnitřní databází, vyžadují přístup k databázovému serveru, který by neměl být veřejně přístupný a může obsahovat citlivé informace. Webové servery mohou komunikovat s databázovým serverem, ať už přímo, nebo z bezpečnostních důvodů prostřednictvím firewallu.

E-mailové zprávy jsou obvykle uloženy na serverech, které nejsou přístupné z Internetu (alespoň ne nezabezpečeným způsobem), ale lze používat SMTP, POP3 servery, které jsou z internetu přístupné.

Pro zabezpečení firemního prostředí, dodržování právních předpisů a monitorovacích důvodů, umísťují některé firmy proxy servery do DMZ nebo interní sítě. To má tyto důsledky:

- Zavazuje interní uživatele (obvykle zaměstnance) používat proxy k získání přístupu do Internetu.
- Umožňuje společnostem snížit rychlostní požadavky přístupu do Internetu, protože některý webový obsah může být uložen v mezipaměti proxy serveru.
- Zjednodušuje zaznamenávání (logování) uživatelských aktivit a blokovat určitý webový obsah, který nesplňuje politiku dané firmy.

Existuje mnoho způsobů, jak navrhnout síť s DMZ. Nejzákladnější metody jsou pomocí jednoho nebo dvou firewallů. Tyto architektury mohou být rozšířeny k vytvoření složitějších architektur v závislosti na síťových požadavcích. [54]

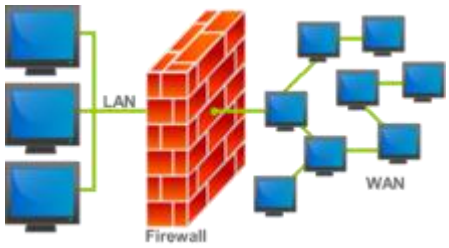
[54] ANDRESS, J. *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice* (2nd ed.). 2014. Elsevier Science. ISBN 978-01-2800-812-6.

5.2 Firewall

Firewall je síťové zařízení, které slouží k řízení a zabezpečování síťového provozu mezi sítěmi s různou úrovní důvěryhodnosti a zabezpečení. Zjednodušeně se dá říct, že slouží jako kontrolní bod, který definuje pravidla pro komunikaci mezi sítěmi, které od sebe odděluje. Tato pravidla historicky vždy zahrnovala identifikaci zdroje a cíle dat (zdrojovou a cílovou IP adresu) a zdrojový a cílový port, což je však pro dnešní firewally už poměrně nedostatečné – modernější firewally se opírají přinejmenším o informace o stavu spojení, znalost kontrolovaných protokolů a případně prvky IDS. Firewally se během svého vývoje řadily zhruba do následujících kategorií:

- Paketové filtry
- Aplikační brány
- Stavové paketové filtry
- Stavové paketové filtry s kontrolou známých protokolů a popř. kombinované s IDS [55]

Obr. 1: Firewall hlídající provoz mezi lokální sítí (LAN) a „zbytkem světa“ (WAN)



5.2.1 Historie

Pojem firewall označoval původně protipožární zeď, která sloužila pro oddělení ohně v budově tak, aby se již dále nešířil. Později se pojem používal pro podobná využití, tentokrát se však jednalo o kovovou desku oddělující motorový prostor auta nebo letadla od prostoru pro pasažéry.

[55] 11. ŽOLTA, L. Firewall. [online]. [cit. 2022-03-25]. Dostupné z: <http://lucie.zolta.cz/index.php/pocitace-a-site/178-stavovy-firewall>.

Technologie firewallu ve výpočetní technice se poprvé objevovala koncem osmdesátých let, kdy byl Internet, co se týče celosvětového použití, poměrně mladou technologií.

Předchůdci dnešních firewallů byly tenkrát routery používané právě koncem osmdesátých let, které sloužily pro zabezpečení sítě. [56]

5.2.2 První generace: filtrování paketů

Prvním typem síťového firewallu byl paketový filtr, který sledoval síťové adresy a porty paketu, aby zjistil, zda má být tento paket povolen nebo zablokován. První dokument publikovaný o technologii firewall byl v roce 1988, kdy inženýři společnosti Digital Equipment Corporation (DEC) vyvinuli filtrační systémy známé jako brány firewall pro paketové filtry. Tento poměrně základní systém byl první generací toho, co je dnes hojně užívaná technická funkce internetového zabezpečení. V laboratořích AT&T Bell pokračoval ve výzkumu filtrování paketů Bill Cheswick a Steve M. Bellovin, kteří vyvinuli pracovní model pro svou vlastní firmu založený na původní architektuře první generace. Význam firewallu zásadně vzrostl s rozšířením internetu a následně prvními úspěšným šířením virů a jiných hrozeb.[57]

Obr. 1: Vlastní zdroj

[56] CHESWICK, W. R., BELLOVIN, S. M., RUBIN, A. D., "Google Books Link". *Firewalls and Internet Security: repelling the wily hacker* [online]. 2003, [cit. 2021-12-14]. Zdroj: https://books.google.com/

[57] CHESWICK, W. R., BELLOVIN, S. M.., RUBIN, A. D., "Google Books Link". *Firewalls and Internet Security: repelling the wily hacker* [online]. 2003, [cit. 2021-12-14]. Zdroj: https://books.google.com/

5.2.3 Druhá generace: stavové filtry

V letech 1989-1990 tři kolegové z laboratoře AT&T Bell, Dave Presotto, Janardan Sharma a Kshitij Nigam vyvinuli druhou generaci firewallů a nazvali ji circuit-level brány.

Brány firewall druhé generace vykonávají práci svých předchůdců z první generace, ale pracují až do 4. vrstvy (transportní vrstva) modelu OSI. To je dosaženo uchováváním paketů, dokud není k dispozici dostatek informací k posouzení stavu. Známá pod termínem stavová kontrola paketů zaznamenává všechna připojení, procházející skrze síť a určuje, zda je paket začátkem nového připojení, nebo součástí stávajícího spojení, nebo není součástí žádného spojení. Přestože statická pravidla jsou stále používaná, tato pravidla mohou nyní obsahovat stav připojení jako jedno z jejich kritérií testování.

Určité DOS útoky bombardují firewall tisíci falešnými pakety s pokusem o jeho přetížení tím, že přehltí jeho vyrovnávací paměť. [58]

5.2.4 Třetí generace: aplikační vrstva

Marcus Ranum, Wei Xu a Peter Churchyard vyvinuli aplikační firewall známý jako Firewall Toolkit (FWTK). V červnu 1994 Wei Xu rozšířil FWTK o kernel zdokonalení, obsahující IP filtru a transparentní socket. Tento firewall byl znám jako první transparentní aplikační firewall, uvedený coby komerční produkt Gauntlet firewallu ve společnosti Trusted Information Systems. Gauntlet firewall byl v letech 1995-1998 hodnocen jako jeden z nejlepších firewallů.

Klíčová výhoda filtrování aplikační vrstvy spočívá v tom, že může "rozumět" určitým aplikacím a protokolům (například FTP, Domain Name System (DNS) nebo Hypertext Transfer Protocol (HTTP)). Je to užitečné, protože dokáže rozpoznat, zda se

[58] CHESWICK, W. R.. BELLOVIN, S. M., RUBIN, A. D., "Google Books Link". *Firewalls and Internet Security: repelling the wily hacker* [online]. 2003, [cit. 2021-12-14]. Zdroj: https://books.google.com/

nežádoucí aplikace nebo služba nepokouší obejít bránu firewall pomocí protokolu na povoleném portu nebo zjistit, zda není protokol zneužíván ke špatným účelům.

Od roku 2012 není takzvaný firewall další generace (NGFW) ničím jiným než "širší" nebo "hlubší" kontrolou v aplikačním zásobníku.[59]

5.2.5 Kategorie firewallů

Podle umístění lze firewally dělit na:

- Síťový firewall – samostatné hardwarové řešení pro ochranu počítačové sítě
- Personální firewall – realizován na koncových stanicích (počítačích)[60]

5.2.6 Jeden firewall

Jeden firewall s alespoň třemi síťovými rozhraními může být použit k vytvoření síťové architektury obsahující DMZ. Externí síť je na prvním síťovém rozhraní vytvořena mezi ISP a firewallem, místní síť je tvořena druhým síťovým rozhraním a DMZ je tvořen ze třetího. Firewall se takto stane jediným bodem, kde může síť selhat a musí být schopen ustát všechen provoz směřující jak do DMZ, tak do interní sítě. Zóny se obvykle označují barvami, například fialová pro LAN, zelená pro DMZ a červená pro Internet. [61]

[59] CHESWICK, W. R., BELLOVIN, S. M., RUBIN, A. D., "Google Books Link". *Firewalls and Internet Security: repelling the wily hacker* [online]. 2003, [cit. 2021-03-14]. Zdroj: https://books.google.com/

[60] CHESWICK, W. R., BELLOVIN, Steven M., RUBIN, A. D., "Google Books Link". *Firewalls and Internet Security: repelling the wily hacker* [online]. 2003, [cit. 2021-03-14]. Zdroj: https://books.google.com/

[61] CHESWICK, W. R., BELLOVIN, S. M., RUBIN, A. D., "Google Books Link". *Firewalls and Internet Security: repelling the wily hacker* [online]. 2003, [cit. 2021-03-14]. Zdroj: https://books.google.com/

5.2.7 Dvojitý firewall

Mnohem bezpečnější je použít dva firewally k vytvoření DMZ. První firewall (označovaný jako „front-end“ firewall) musí být nakonfigurován tak, aby kontroloval provoz pouze pro DMZ. Druhý firewall (označovaný jako „back-end“ firewall) kontroluje provoz mezi DMZ a vnitřní sítí. Některé firewally se dodávají jako jedno zařízení, které v sobě obsahuje 2 a více virtuálních firewallů.

Toto nastavení lze považovat za bezpečné, protože jinak mohou být ohrožována oboje zařízení. Pokud se použije každé zařízení od jiného výrobce, tak se bezpečnost dále zvyšuje, protože je nepravděpodobné, aby trpěly stejnými bezpečnostními chybami. Pro příklad: při náhodné konfiguraci je nepravděpodobné, že by se útočník dostal do sítě přes stejnou bezpečnostní chybu u obou zařízení vyrobených jinými výrobci. Tato architektura je samozřejmě více nákladná. Používání různých firewallů od různých výrobců je někdy popisováno jako „hloubková obrana“. [62]

5.2.8 Paketové filtry

Nejjednodušší a nejstarší forma firewallování, která spočívá v tom, že pravidla přesně uvádějí, z jaké adresy a portu na jakou adresu a port může být doručen procházející paket, tj. kontrola se provádí na třetí a čtvrté vrstvě modelu síťové komunikace OSI.

Výhodou tohoto řešení je vysoká rychlost zpracování, proto se ještě i dnes používají na místech, kde není potřebná přesnost nebo důkladnější analýza procházejících dat, ale spíš jde o vysokorychlostní přenosy velkých množství dat.

Nevýhodou je nízká úroveň kontroly procházejících spojení, která zejména u složitějších protokolů (např. FTP, video/audio streaming, RPC apod.) nejen nedostačuje ke kontrole vlastního spojení, ale pro umožnění takového spojení vyžaduje otevřít i por-

[62] CHESWICK, W. R., BELLOVIN, S. M., RUBIN, A. D., "Google Books Link". *Firewalls and Internet Security: repelling the wily hacker* [online]. 2003, [cit. 2021-03-14]. Zdroj: https://books.google.com/

ty a směry spojení, které mohou být využity jinými protokoly, než bezpečnostní správce zamýšlel povolit.

Mezi typické představitele paketových filtrů patří např. tzv. ACL (Access Control Lists) ve starších verzích operačního systému IOS na routerech spol. Cisco Systems, popř. JunOS spol. Juniper Networks, starší varianty firewallu v linuxovém jádře (ipchains). [63]

5.2.9 Aplikační brány

Jen o málo později, než jednoduché paketové filtry, byly postaveny firewally, které na rozdíl od paketových filtrů zcela oddělily sítě, mezi které byly postaveny. Říká se jim většinou Aplikační brány, někdy také Proxy firewally. Veškerá komunikace přes aplikační bránu probíhá formou dvou spojení – klient (iniciátor spojení) se připojí na aplikační bránu (proxy), ta příchozí spojení zpracuje a na základě požadavku klienta otevře nové spojení k serveru, kde klientem je aplikační brána. Data, která aplikační brána dostane od serveru, pak zase v původním spojení předá klientovi. Kontrola se provádí na sedmé (aplikační) vrstvě síťového modelu OSI (proto se těmto firewallům říká aplikační brány).

Jedním vedlejším efektem použití aplikační brány je, že server nevidí zdrojovou adresu klienta, který je původcem požadavku, ale jako zdroj požadavku je uvedena vnější adresa aplikační brány. Aplikační brány díky tomu automaticky působí jako nástroje pro překlad adres (NAT), nicméně tuto funkcionalitu má i většina paketových filtrů.

Výhodou tohoto řešení je poměrně vysoké zabezpečení známých protokolů.

Nevýhodou je zejména vysoká náročnost na použitý HW – aplikační brány jsou schopny zpracovat mnohonásobně nižší množství spojení a rychlosti, než paketové filtry a mají mnohem vyšší latenci. Každý protokol vyžaduje napsání specializované proxy,

[63] CONWAY, R. *Code Hacking: A Developer's Guide to Network Security.* Hingham, Massachusetts: Charles River Media. 2004. s. 183. ISBN 1-58450-314-9.

nebo využití tzv. generické proxy, která ale není o nic bezpečnější, než využití paketového filtru. Většina aplikačních bran proto uměla kontrolovat jen několik málo protokolů (obyčejně kolem deseti). Původní aplikační brány navíc vyžadovaly, aby klient uměl s aplikační branou komunikovat a neuměly dost dobře chránit svůj vlastní operační systém; tyto nedostatky se postupně odstraňovaly, ale po nástupu stavových paketových filtrů se vývoj většiny aplikačních bran postupně zastavil a ty přeživší se dnes používají už jen ve velmi specializovaných nasazeních.[64]

5.2.10 Stavové paketové filtry

Stavové paketové filtry provádějí kontrolu stejně jako jednoduché paketové filtry, navíc si však ukládají informace o povolených spojeních, které pak mohou využít při rozhodování, zda procházející pakety patří do již povoleného spojení a mohou být propuštěny, nebo zda musí znovu projít rozhodovacím procesem. To má dvě výhody, jednak se tak urychluje zpracování paketů již povolených spojení, jednak lze v pravidlech pro firewall uvádět jen směr navázání spojení a firewall bude samostatně schopen povolit i pakety odpovědí a u známých protokolů i další spojení, která daný protokol používá. Například pro FTP tedy stačí nastavit pravidlo, ve kterém povolíte klientu připojení na server pomocí FTP a protože se jedná o známý protokol, firewall sám povolí navázání řídícího spojení z klienta na port 21 serveru, odpovědi z portu 21 serveru na klientem použitý zdrojový port a po příkazu, který vyžaduje přenos dat, povolí navázání datového spojení z portu 20 serveru na klienta na port, který si klient se serverem dohodli v rámci řídícího spojení a pochopitelně i pakety odpovědí z klienta zpět na port 20 serveru. Zásadním vylepšením je i možnost vytváření tzv. virtuálního stavu spojení pro bez stavové protokoly, jako např. UDP a ICMP. [65]

K největším výhodám stavových paketových filtrů patří jejich vysoká rychlost, poměrně slušná úroveň zabezpečení a ve srovnání s výše zmíněnými aplikačními branami a jednoduchými paketovými filtry řádově mnohonásobně snazší konfigurace a

[64] CONWAY, R. *Code Hacking: A Developer's Guide to Network Security.* Hingham, Massachusetts: Charles River Media. 2004. s. 187. ISBN 1-58450-314-9.
[65] CONWAY, R. *Code Hacking: A Developer's Guide to Network Security.* Hingham, Massachusetts: Charles River Media. 2004. s. 187. ISBN 1-58450-314-9.

díky zjednodušení konfigurace i nižší pravděpodobnost chybného nastavení pravidel obsluhou.

Nevýhodou je obecně nižší bezpečnost, než poskytují aplikační brány.[66]

5.2.11 Stavové paketové filtry s kontrolou protokolů a IDS

Moderní stavové paketové filtry kromě informací o stavu spojení a schopnosti dynamicky otevírat porty pro různá řídící a datová spojení složitějších známých protokolů implementují něco, co se v marketingové terminologii různých společností nazývá nejčastěji Deep Inspection nebo Application Intelligence. Znamená to, že firewally jsou schopny kontrolovat procházející spojení až na úroveň korektnosti procházejících dat známých protokolů i aplikací. Mohou tak například zakázat průchod http spojení, v němž objeví indikátory, že se nejedná o požadavek na WWW server, ale tunelování jiného protokolu, což často využívají klienti P2P sítí (ICQ, gnutella, napster, apod.), nebo když data v hlavičce e-mailu nesplňují požadavky RFC (technické požadavky pro řízení služby) apod.

Nejnověji se do firewallů integrují tzv. in-line IDS (Intrusion Detection Systems – systémy pro detekci útoků). Tyto systémy pracují podobně jako antiviry a pomocí databáze signatur a heuristické analýzy jsou schopny odhalit vzorce útoků i ve zdánlivě nesouvisejících pokusech o spojení, např. skenování adresního rozsahu, rozsahu portů, známé signatury útoků uvnitř povolených spojení apod.

Výhodou těchto systémů je vysoká úroveň bezpečnosti kontroly procházejících protokolů při zachování relativně snadné konfigurace, poměrně vysoká rychlost kontroly ve srovnání s aplikačními branami, nicméně je znát významné zpomalení (zhruba o třetinu až polovinu) proti stavovým paketovým filtrům.

Nevýhodou je zejména to, že z hlediska bezpečnosti designu je základním pravidlem bezpečnosti udržovat bezpečnostní systémy co nejjednodušší a nejmenší. Tyto typy fi-

[66] CONWAY, R. *Code Hacking: A Developer's Guide to Network Security.* Hingham, Massachusetts: Charles River Media. 2004. s. 188. ISBN 1-58450-314-9.

rewallů integrují obrovské množství funkcionality a zvyšují tak pravděpodobnost, že v některé části jejich kódu bude zneužitelná chyba, která povede ke kompromitování celého systému. [67]

5.3 Webový aplikační firewall

Webový aplikační firewall (WAF) je zařízení, které poskytuje rychlou a účinnou eliminaci rizik spojených s provozováním webových aplikací.

Jde o typ firewallu, který eliminuje útoky vedené na aplikační úrovni, nejčastěji pomocí protokolů HTTP/HTTPS (7. vrstva OSI modelu), z veřejného internetu na webové aplikace, portály či webové služby. Doplňkem může být i ochrana protokolů FTP a SMTP či možnost propojení s externím antivirovým systémem.

WAF zvyšuje celkovou úroveň bezpečnosti, dokáže zabránit útokům dříve, než zasáhnou vlastní webovou aplikaci. Poskytuje ochranu před velkou škálou útoků, nabízí monitorování provozu a jeho analýzu v reálném čase. To vše s minimálním dopadem na existující infrastrukturu. WAF poskytuje ochranu tam, kde jsou běžné paketové firewally a IPS neúčinné.

Klíčové vlastnosti WAF:

- Detekce a prevence útoků na webové aplikace
- Ochrana před DoS a DDoS
- Logování provozu
- Maskování serverů, aplikací a dat
- Rychlé řešeni existujících chyb - aplikace „workaround“ řešeni
- Centralizované zabezpečení infrastruktury webových aplikací a aplikací webových služeb

[67] CONWAY, R. *Code Hacking: A Developer's Guide to Network Security.* Hingham, Massachusetts: Charles River Media. 2004. s. 188. ISBN 1-58450-314-9.

- Zajištění bezpečnosti tam, kde není zajištěna logikou aplikace (např. doplnění o více faktorovou autentizaci)
- Snížení nákladů na řešení bezpečnosti na úrovni úpravy kódu aplikace
- Eliminace rizik u „starých aplikací“, kde již mnohdy není ani samotný kód k dispozici
- Efektivnější proces nasazení nových verzí aplikací
- Snížení času a nákladů za účelem zajištění souladu s požadavky standardu, např. Kybernetický zákon, PCI DSS.
- Rychlý a názorný přehled o útocích na aplikace

WAF lze typicky pořídit jako samostatnou apliance provozovanou na speciální hardwarové platformě anebo jako Virtuální appliance provozovanou nad VMware, Microsoft Hyper-V, Citrix nebo KVM. [68]

5.4 Next generation firewall

Společnost Gartner zveřejnila na konci roku 2009 výzkumnou zprávu: Definování firewallu nové generace, ve které se uvádí, že měnící se podnikatelské procesy, nové technologie, které podniky zavádějí a také nové hrozby, které se objevují, jsou hnacím motorem nových požadavků na zabezpečení sítě. Gartner upozorňuje, že pokud chceme splnit tyto úkoly, firewally se musí vyvíjet směrem, který Gartner označuje jako nová generace firewallů – Next Generation Firewall (NGFW). [69]

[68] Webový aplikační firewall. [online]. Autocont, 2019, [cit. 2021-12-14]. Dostupné z : https://www.autocont.cz/aktuality/openspace/ochrana-webovych-aplikaci/webovy-aplikacni-firewall

[69] Next generation firewall [online]. Praha: www.sands.cz, 2019 [cit. 2021-12-20]. Dostupné z: http://www.sands.cz/sluzby-produkty/bezpecnost-ict/next-generation-firewall

5.4.1 Přínosy využití systému

- All-in-One funkcionalitu: NGFW může spojovat funkci tradičního firewallu s funkcí IPS, antivirové ochrany a filtrování protokolu.
- Větší přehled a kontrolu: NGFW nabízí jemnější granularitu kontroly podle IP adresy a uživatele nejen webových aplikací a obsahu, ale také starších aplikací a obsahu.
- Zjednodušená správa: Zatímco starší firewally byly řízeny individuálně a konfigurovány ručně, můžeme NGFW sledovat a aktualizovat z jediné konzole bez přerušení provozu.
- Lepší zabezpečení: Nová generace firewallů kontroluje obsah také jako prevenci úniku dat a zastavení hrozeb pomocí detailní inspekce datového provozu. Mnohé NGFW poskytují zabezpečení založené na bezpečnostních politikách a rolích.
- Nižší celkové náklady na vlastnictví: protože nová generace firewallů sníží počet potřebných bezpečnostních zařízení, snižují se investiční a provozní náklady. Úspory jsou také v oblasti snížení časové náročnosti správy a konfigurace těchto zařízení.[70]

5.5 Segmentace

Segmentace sítě v počítačových sítích je úkon nebo praxe rozdělení počítačové sítě do podsítí, přičemž každá je síťovým segmentem. Výhody takového rozdělení jsou primárně pro zvýšení výkonu a zlepšení zabezpečení.

Když počítačový zločinec získá neoprávněný přístup k síti, může segmentace nebo „zónování“ poskytnout účinnou kontrolu omezující další pohyb po síti. PCI-DSS (Payment Card Industry Data Security Standard) a podobné standardy poskytují pokyny pro vytváření jasného oddělení dat v síti, například oddělení sítě pro autorizaci platebních karet od oprávnění pro Point-of-Service nebo zákazníka wi-fi provozu. Dobrá politika

[70] Next generation firewall [online]. Praha: www.sands.cz, 2019 [cit. 2021-12-20]. Dostupné z: http://www.sands.cz/sluzby-produkty/bezpecnost-ict/next-generation-firewall

zabezpečení zahrnuje segmentaci sítě do několika zón s různými požadavky na zabezpečení a důsledné vynucování zásad v tom, jaká je povelena komunikace mezi zónami.

5.5.1 Kontrola přístupu externích uživatelů

Třetí strany (dodavatelé, outsoursing) jsou obvykle odděleni a mají mít svůj vlastní segment s různými administračními hesly do sítě, přístup k jednotlivým prvkům. Serverům nebo službám by měl být zprostředkován nástrojem PIM/PAM (Privileg access management). [71]

5.6 Internet věcí

Internet věcí (anglicky Internet of Things, zkratka IoT) je v informatice označení pro síť fyzických zařízení, vozidel, domácích spotřebičů a dalších zařízení, která jsou vybavena elektronikou, softwarem, senzory, pohyblivými částmi a síťovou konektivitou, která umožňuje těmto zařízením se propojit a vyměňovat si data. Každé z těchto zařízení je jasně identifikovatelné díky implementovanému výpočetnímu systému, ale přesto je schopno pracovat samostatně v existující infrastruktuře internetu. Experti odhadují, že Internet věcí bude v roce 2021 zahrnovat přibližně 35 miliard zařízení. Hodnota trhu se odhaduje na 100 miliard dolarů.[72]

[71] Network Segment Definition [online]. 2005 [cit. 2021-09-03].
Dostupné z: https://www.cisco.com/c/en/us/products/security/what-is-network-segmentation.html

[72] KRAUSOVÁ, V. *Internet věcí (Internet of Things) a jeho bezpečnost.* Brno, 2014. 37 s., 9 nečísl. s. Bakalářská diplomová práce. Ved. práce PhDr. Michal Lorenz, Ph.D. Masarykova univerzita, Filozofická fakulta, Ústav české literatury a knihovnictví, Kabinet informačních studií a knihovnictví, Informační studia a knihovnictví. Přístup také z: https://is.muni.cz/th/d0hvz/

5.6.1 Charakteristika

Internet věcí umožňuje zařízením, aby byla zjištěna či vzdáleně kontrolována pomocí existující infrastruktury (počítačová síť, Internet, mobilní síť, atd.), která umožňuje lepší integraci fyzických zařízení do počítačově řízených systémů, a tedy vyšší účinnost, přesnost a ekonomičnost i nižší nároky na uživatele. Pokud jsou v zařízení umístěna čidla či akční členy, technologie se stává částí více obecné kategorie kyber-fyzických systémů, která zahrnuje technologie, jako jsou chytré sítě, chytré domácnosti, a inteligentní přepravu, či též chytrá města. Roli hrají rovněž logistické systémy, integrované logistické řetězce a cykly v globální struktuře.[73]

Pojmem „věci" v oblasti IoT (Internet of Things) může být definována škála zařízení, jako jsou např. srdeční implantáty k měření srdečního tepu, biočipové senzory na farmách, kamery vysílající živé záběry divokých zvířat, automobily se zabudovanými senzory, přístroje na analýzu DNA nebo terénní zařízení, která pomáhají hasičům v pátracích a záchranných operacích. Lidé pracující v justici doporučují posuzovat tyto „věci" jako jednotný mix hardwaru, softwaru, dat a služeb.

Tato zařízení sbírají potřebná data s pomocí rozličných existujících technologií a poté samostatně rozesílají tato data mezi ostatními zařízeními. Rychlý vývoj a expanze Internetu věcí by také mělo znamenat produkci velkého množství dat z různých oblastí a následnou potřebu rychlého zařazení dat a zvýšení potřeby na indexování, ukládání a zpracovávání dat efektivněji. V posledních letech, spolu s masivním růstem globálních kybernetických hrozeb, se také objevuje výrazný růst zneužívání Internetu věcí k páchání kybernetických zločinů.

Termín „Internet věcí" vytvořil Kevin Ashton z Procter & Gamble, později MIT Auto-ID Center v roce 1999. [74]

[73] WEBER, R. H., WEBER, R. *Internet of Things: Legal Perspectives.* Berlin: Springer, 2010. 129 s. ISBN 978-3-642-11709-1.
[74] KRAUSOVÁ, V. *Internet věcí (Internet of Things) a jeho bezpečnost.* Brno, 2014. 37 s., 9 nečísl. s. Bakalářská diplomová práce. Ved. práce PhDr. Michal Lorenz, Ph.D. Masarykova univerzita, Filozofická fakulta, Ústav české literatury a knihovnictví, Kabinet informačních studií a knihovnictví, Informační studia a knihovnictví. Přístup také z: https://is.muni.cz/th/d0hvz/

5.6.2 Bezpečnost internetu věcí

Inteligentní systémy automaticky znamenají zvýšení zranitelnosti (Hypponenův zákon).

Bezpečnostní problémy internetu věcí jsou podobné jako problémy běžných serverů, osobních počítačů a smartphonů. Ovšem u zařízení s podstatně menším výpočetním výkonem jsou stěží použitelná bezpečnostní řešení jako firewall, antimalware a bezpečnostní update (výrobci ve velmi malé míře reagují na zveřejněné zranitelnosti jejich zařízení). V současnosti se tedy technické řešení bezpečnosti týká zabezpečení sítě, i když se objevují čipy pro koncová zařízení, která používají kryptografické metody k ověření identifikace.

5.6.3 Ověřování uživatelů

Pro plnou kontrolu přístupu uživatele, musí být nejprve autentizován systémem uživatelská identita. Nejčastěji lze ověřit identitu uživatele na základě toho:

a) co zná,
b) co vlastní,
c) čím je.

a) Nejběžnější je autentizace uživatele ve formě hesla (určitého řetězce znaků) na základě toho, co uživatel zná. Uživatel obvykle zadává heslo na výzvu systému. Zadané heslo je pak porovnáno s heslem uživatele, které bylo dříve v systému uloženo. Uživatel, pokud se hesla shodují, se přihlásí a uživatel získá přidělená oprávnění.

   Výhodou hesel je, že se snadno používají a snadno implementují do systému. Avšak čím je heslo složitější či kvalitnější, tím hůře si ho uživatelé zapamatují. Nevýhodou hesel je, že je možné zadávání sledovat a následně heslo dále šířit.

b) Autentizace uživatele na základě vlastnictví předmětu se obvykle dosahuje držením tokenu uživatele (např. čipová karta, klíče atd.). Tuto funkci může dnes převzít kupříkladu mobilní telefon. Nevýhodou validace na základě vlastnictví předmětu je fakt, že zařízení může být předáno, odcizeno nebo ztraceno. Navíc je toto využití pro autentizaci uživatele a je spojeno s výrazně vyššími náklady než při ověření na základě toho, co uživatel zná.

c) Autentizace uživatele na základě toho čím je se zabývá biometrie, která rozpoznává jedinečné biologické charakteristiky daného uživatele. Existuje několik charakteristik, u nichž se předpokládá nebo je matematicky prokázáno, že jsou pro každého člověka jedinečné. Tyto charakteristiky často využívají i jiné vědní obory, jako je například kriminalistika. Uživatele je možné ověřovat podle otisku prstů, obličeje, hlasu, oční duhovky, atd. Nevýhodou autentizace uživatele představuje nutnost pořízení speciálního hardwaru, nemožnost změnit používané charakteristiky, či možnost napodobení některých biometrických údajů.

Pro většinu aplikací a systémů, můžeme označit za vhodné využívání dvou a výše uvedených způsobů, kde se kombinuje například znalost hesla s vlastnictvím zařízení, či biometrickými údaji. V tomto případě ověření označujeme jako dvoufaktorovou autentizaci. Nejběžnějším příkladem dvoufaktorové autenzizace je výběr peněz z bankomatu, kdy uživatel vlastní platební kartu, ale zároveň musí znát i příslušný PIN kód.[75]

[75] KOLOUCH, J., BAŠTA, P., KROPÁČOVÁ, A., KUNC, M., *CYBERSECURITY*, 1. vydání. Praha, 2019, s. 463 – 464. ISBN 978-80-88168-34-8.

6 Kybernetická bezpečnost

Kybernetická bezpečnost představuje souhrn organizačních, politických, právních, technických a vzdělávacích opatření a nástrojů směřujících k zajištění zabezpečeného, chráněného a odolného kyberprostoru v České republice, a to jak pro subjekty veřejného a soukromého sektoru, tak pro širokou českou veřejnost. Kybernetická bezpečnost pomáhá identifikovat, hodnotit a řešit hrozby v kyberprostoru, snižovat kybernetická rizika a eliminovat dopady kybernetických útoků, informační kriminality, kyberterorismu a kybernetické špionáže ve smyslu posilování důvěrnosti, integrity a dostupnosti dat, systémů a dalších prvků informační a komunikační infrastruktury. Hlavním smyslem kybernetické bezpečnosti je pak ochrana prostředí k realizaci informačních práv. Stěžejním orgánem státní správy pro oblast kybernetické bezpečnosti je Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB).

6.1 Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB)

NÚKIB je ústředním správním orgánem pro kybernetickou bezpečnost včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany. Dále má na starosti problematiku neveřejné služby v rámci družicového systému Galileo. Vznikl 1. srpna 2017 na základě zákona číslo 205/2017 Sb., kterým se změnil zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).

Hlavní oblasti činnosti NÚKIB:

- provozovat Vládní CERT České republiky (GovCERT.CZ)
- spolupráce s ostatními národními CERT® týmy a CSIRT týmy
- spolupráce s mezinárodními CERT® týmy a CSIRT týmy
- příprava bezpečnostních standardů pro informační systémy KII a VIS

- osvěta a podpora vzdělávání v oblasti kybernetické bezpečnosti
- výzkum a vývoj v oblasti kybernetické bezpečnosti
- ochrana utajovaných informací v oblasti informačních komunikačních systémů
- kryptografická ochrana
- národní kontaktní místo PRS – jedna ze služeb evropského satelitního systému Galileo (NCPRS)[76]

6.2 Bezpečnostní týmy v ČR

Jedním z prvků boje proti kyberkriminalitě jsou bezpečnostní týmy typu CERT (Computer Emergency Response Team) nebo CSIRT (Computer Security Incident Response Team). Každá z těchto zkratek má trochu jiný význam a hlavně trochu jinou historickou genezi, ve skutečnosti je dnes za oběma zkratkami možno chápat stejný typ týmu – tým, který je ve svém jasně definovaném poli působnosti zodpovědný za řešení bezpečnostních incidentů, z pohledu uživatelů nebo jiných týmů tedy místo, na které se mohou obrátit se zjištěným bezpečnostním incidentem nebo i jen podezřením.

[76] ČESKO. MINISTERSTVO VNITRA. *Kyberkriminalita*. [online]. © 2020 Ministerstvo vnitra České republiky. [cit. 2021-12-15]. Dostupné z: <https://prevencekriminality.cz/prevence-kriminality/kyberkriminalita/rozcestnik-kyberkriminality/>.

7 Shrnutí Zprávy o stavu kybernetické bezpečnosti České republiky za rok 2020

Rok 2020 se vyznačoval nárůstem počtu kybernetických útoků proti českým institucím, organizacím a firmám ve všech sektorech. V roce 2020 bylo NÚKIB nahlášeno 468 incidentů oproti 217 incidentům v roce 2019. Téměř třetinu z řešených incidentů nahlásily neregulované subjekty. Za tímto nárůstem stojí velmi pravděpodobně vyšší počet kybernetických útoků i větší povědomí o existenci a aktivitách NÚKIB. Vzrostla také závažnost incidentů, jak ukazují útoky proti Fakultní nemocnici Brno nebo Psychiatrické nemocnici Kosmonosy. Nejčastějšími typy útoků byly v roce 2020 spam, phishing a scanning. Mezi nejvážnější hrozby pro kybernetickou bezpečnost ČR dlouhodobě patří kybernetická kriminalita. V roce 2020 byla nejvíce vidět u ransomwarových útoků, které zasáhly český zdravotnický sektor. Nárůst útoků proti nemocnicím lze do velké míry přisoudit probíhající pandemii i zacílení kyberkriminálních skupin na konkrétní instituce s vyšší pravděpodobností zaplacení výkupného. I přesto považují tři čtvrtiny zdravotnických zařízení finance k zajištění kybernetické bezpečnosti za nedostatečné. NÚKIB ve spolupráci s Úřadem vlády a Ministerstvem zahraničních věcí uspořádal v září 2020 druhý ročník dvoudenní Prague 5G Security Conference, předního světového fóra pro diskusi o rizicích spojených s budováním 5G infrastruktury. Stejně jako minulý rok proběhla pod záštitou předsedy vlády ČR Andreje Babiše. Přestože se konference s ohledem na situaci spojenou s covid-19 poprvé konala virtuálně, vystoupilo na ní přes 50 řečníků z Evropy, USA, Jižní Koreje, Izraele, Austrálie, Indie a dalších zemí. Hlavním výstupem druhého ročníku bylo představení a spuštění tzv. Prague 5G Security Repository, virtuální knihovny určené ke sdílení legislativních, strategických a dalších nástrojů, které státy v uplynulém roce v oblasti bezpečnosti 5G sítí přijaly.

V roce 2020 NÚKIB pokračoval ve vzdělávání zaměstnanců státní správy a v rámci e-learningového kurzu Dávej kyber! proškolil více než 18 209 zaměstnanců státní správy, 214 pracovníků Armády ČR a 2 000 pracovníků Fakultní nemocnice Na Bulovce. Odborný kurz „Bezpečně v kyber“, který zaměstnance seznamuje se situacemi ze školního prostředí, absolvovalo 1 690 pracovníků prevence. V roce 2020 se řada dotazovaných organizací potýkala s nedostatkem odborníků a nedostatečnými rozpočty

v oblasti kybernetické bezpečnosti. Tato situace byla citelnější v sektoru státní správy než u soukromých společností. Téměř žádný z respondentů neměl obsazené všechny pozice v oblasti kybernetické bezpečnosti. Více než polovina organizací za hlavní faktor uvedla nedostatečné mzdové podmínky. NÚKIB vydal v reakci na dění v průběhu pandemie několik doporučení, upozornění, varování i reaktivních opatření. Patří mezi ně například upozornění na rizika online konferenčních služeb, doporučení Bezpečná práce na dálku, příručka Videokonference bezpečně nebo dokument Minimální bezpečnostní standard pro zabezpečení menších organizací, které vznikly ve spolupráci s NAKIT (Národní agentura pro komunikační a informační technologie). Navzdory pandemickým opatřením proběhlo i v roce 2020 mezinárodní cvičení kybernetické bezpečnosti Cyber Coalition, pořádané Severoatlantickou aliancí, poprvé ve virtuální formě. Česká republika tak opět maximálně přispěla do jednoho z největších mezinárodních cvičení kybernetické bezpečnosti.[77]

[77] https://www.nukib.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_KB_2020.pdf

8 Rozvoj vývoje kybernetických útoků s její možností eliminace

U kriminality páchané v kyberprostoru, která tvoří cca 6,2 % celkové registrované kriminality, je dle statistických dat trend setrvale stoupající (meziročně o 17,9 %), a to bez ohledu na pandemii covid-19 a následná opatření. Pro představu je přiložena komparační tabulka registrovaných skutků v ČR za období leden až prosinec 2019-2021 „spáchaných internetem“ a „ostatními počítačovými sítěmi“ (kyberkriminality).

Tab. 1: Porovnání kybernetické kriminality České republice[78]

	2019	2020	2021
Počet registrovaných skutků kyberkriminality	8 417	8 073	9 518
Spácháno internetem	8 177	7 828	9 276
Spácháno ostatními počítačovými sítěmi	240	245	242

Podle poznatků NCOZ SKPV v oblasti kybernetické kriminality je již dlouhodobě evidován stálý růst nápadu této registrované trestné činnosti, kdy meziročně stoupl počet skutků tzv. „hackingu“ o 45 %. V posledním kvartálním období byl zároveň zaznamenán zvyšující se procentuální podíl této trestné činnosti (v srpnu byl meziroční nárůst zhruba 37 %). Konkrétně bylo do konce prosince 2020 evidováno 1 160 skutků, přičemž do konce prosince 2021 bylo evidováno již 1 682 skutků. Nutno podotknout, že určitá část protiprávního jednání spočívá souběhově i v napadení emailových účtů, resp. jejich přístupových údajů, případně v napadení přístupových

[78] ČESKO. POLICIE ČESKÉ REPUBLIKY. Vývoj registrované kriminality v roce 2021 [online]. © 2022 Policie ČR. [cit. 2022-03-20]. Dostupné z: <https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2021.aspx>.

údajů sociálních sítí. Potvrzuje se předpokládaný trend, a to postupný přesun trestné činnosti jako takové do kyberprostoru. Taktéž se meziročně snižuje objasněnost případů, kde roli sehrála kybernetická kriminalita nebo ostatní kriminalita páchaná v kyberprostoru, neboť jak statistiky ukazují, v roce 2020 byla objasněnost v daných problematikách 30 %, nicméně v roce 2021 klesla související objasněnost na hodnotu 24,7 %.

Kazuistika: Severoamerická společnost Superior Plus, která představuje předního distributora a prodejce propanu, destilátů a s tím souvisejících produktů a služeb, se stal ve druhé polovině prosince 2021 terčem ransomwarového útoku. Superior Plus obsluhuje více než 780 000 zákaznických lokací v USA a Kanadě. Společnost se ihned snažila zmírnit dopady na provoz společnosti, zabezpečit své systémy, a proto musela na útok reagovat vypnutím některých počítačových systémů a aplikací. Společnost pracuje na obnovení provozu zasažených systémů a útok vyšetřuje. Dosud pouze uvedla, že nedisponuje žádnými důkazy o narušení bezpečnosti, ohrožení osobních údajů zákazníků apod., ale vyšetřování nadále probíhá. I takovýchto útoků může na území Evropy a ČR v souvislosti s případnou eskalací bezpečnostní krize na územích bývalého SSSR, příp. energetickou krizí, přibývat.[79]

8.1 Trendy v kybernetické kriminalitě a ostatní kriminalitě páchané v kyberprostoru

Údaje o dílčích útocích nejsou ještě v době vytvoření zprávy k dispozici, ale dle vývoje v období leden až listopad lze předpokládat, že i v roce 2021 bude zaznamenán větší počet dílčích útoků v rámci jednoho trestného činu než v roce 2020. I přes částečný pokles celkového nápadu trestných činů pomocí internetu nebo ostatních počítačových sítí, který byl zaznamenán v roce 2020, je dlouhodobý trend viditelně vzrůstající a nepochybně bude pokračovat.

Stejně jako v roce 2020, tak i v roce 2021 je stále nejrozšířenější oblastí trestných činů v rámci kybernetické kriminality majetková trestná činnost, nejčastěji různá

[79] ČESKO. POLICIE ČESKÉ REPUBLIKY. Vývoj registrované kriminality v roce 2021 [online]. © 2022 Policie ČR. [cit. 2022-03-20]. Dostupné z: <https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2021.aspx>.

jednání kvalifikovaná jako podvod (§ 209 trestního zákoníku). Dále ve větším množství byly páchány trestné činy pomocí internetu v oblasti poškozování a zneužití záznamu na nosiči informací (§ 230, 231 a 232 trestního zákoníku), v oblasti mravnostních trestných činů a v oblasti neoprávněného držení platebního prostředku a dále trestných činů v oblasti porušování autorského práva a porušování práv k autorské známce (§ 155 trestního zákoníku).

Vzhledem k nejednotnému výkladu, rozdílnému přístupu k trestněprávní kvalifikaci a často i souběhovému jednání je obtížné objektivně určovat přesnější trendy v oblasti kybernetické kriminality na základě pouhého statistického porovnání dle sdělované právní kvalifikace jednotlivých skutků.

Charakteristické pro současná nejčastější podvodná jednání je skutečnost, že se jedná o činy, které již vyžadují vyšší míru technických znalostí a znalostí internetového provozu a služeb v něm poskytovaných. Jde především o mnohokrát opakující se vlny podvodných falešných mailových zpráv, případně zpráv v rámci jiných komunikačních kanálů, především různé messengery, pomocí nichž se pachatelé snaží vylákat citlivé, osobní nebo jinak zájmové údaje od adresátů nebo do cílových zařízení nainstalovat škodlivý software. Zde je nejčastěji problém v koncových uživatelích, kteří nerespektují základní bezpečností opatření v rámci elektronických komunikací a používají stejné přihlašovací údaje do různých služeb, bez ohledu na jejich možné zneužití. Pro tyto tzv. vlny je typické, že trvají velmi krátce, nejčastěji okolo dvou, třech dnů a mají poměrně široký dosah. V současné době není možné předem blokovat podobné hromadné emaily, neboť útočníci neustále mění technické prostředky pro odesílání závadových zpráv.

V roce 2021 výrazně stoupl počet útoků na majetek, kdy oběti sami vydají útočníkům svoje přihlašovací údaje do např. elektronických bankovních systémů nebo v mnoha případech oběti sami provedou příslušné podvodné převody dle instrukcí útočníků. Pachatelé, mnohdy zcela špatně označovaní jako „hackeři“, využívají a zneužívají často lehkovážný přístup svých obětí k těm nejcitlivějším bezpečnostním údajům, jako jsou údaje osobní nebo právě zmiňované přístupové údaje do různých chráněných elektronických systémů. Valné většině takového protiprávního jednání by šlo snadno zabránit, pokud by oběti přistupovaly k zveřejňování svých citlivých dat a informací obezřetněji. Tento trend lze očekávat i v následujících letech.

Vyšetřování podobné trestné činnosti je zdlouhavé a nákladné. Drtivá většina finančních prostředků pocházející z kybernetické majetkové trestné činnosti je přeposílaná do zahraničních peněžních institucí nebo okamžitě převedena na některou z kryptoměn, nejčastěji na Bitcoin.

Za uplynulé období lze pozorovat masivní využívání virtuálních měn (kryptoměny) jako prostředek k zametení stop a současně i k legalizaci výnosů z trestné činnosti. Nejčastěji využívanou virtuální měnou pro kriminální činnosti je v tuto chvíli jednoznačně Bitcoin. Pro pachatele trestné činnosti je kryptoměna Bitcoin zajímavá také svým neustále rostoucím směnným kurzem. Tato virtuální měna je z principu v podstatě nedohledatelná a nyní není možné jednoznačně určit platební cesty při použití této, ale i jiných, kryptoměn. To orgánům činným v trestním řízení velmi znesnadňuje nejen vystopování pachatelů trestné činnosti pomocí trasování platebních cest, ale i celkově objasňovat nezákonné platební machinace při využívání virtuální měny.

Další větší skupinou protiprávního jednání na internetu zůstává dlouhodobě trestná činnost mravnostního charakteru. Zde se nejčastěji jedná o šíření nebo držení dětské pornografie, navazování kontaktu s dětmi s cílem od nich vylákat erotické materiály a v menší míře také sexuální nátlak. Komunikace mezi dětmi a pachateli probíhá velmi často v uzavřených diskuzních fórech, na zahraničních komunikačních službách nebo na šifrovaných mobilních platformách, což velmi ztěžuje přesné zadokumentování důkazních materiálů, ale často také samotné odhalení takového jednání.

Podle některých zjištění byl v roce 2021 omezen přísun bezpečnostních upozornění na mravnostní trestnou činnost ze zahraničních sborů, kdy v minulých letech tyto informace byly velmi cenným zdrojem poznatků při vyhledávání online mravnostní trestné činnosti.

Lze předpokládat, že protiprávní jednání v rámci internetového prostředí bude mít také v dalších letech vzrůstající charakter. Je více než pravděpodobné, že se určité typy závadového chování budou stále výrazněji přesouvat do kyberprostoru.

S rozšiřováním tzv. internetu věcí lze předvídat zacílení útoků právě na tato koncová zařízení. S tím souvisí i zvýšené nebezpečí útoků na osobní data či citlivé údaje občanů, jako je například zdravotní dokumentace, trasování denního pohybu osob nebo útoků na bankovní data na straně klienta. S nástupem vysokorychlostního mobilního Internetu lze

předpokládat, že v nejbližší budoucnosti se začne v masivní míře využívat šifrování nejen obsahu uživatelských dat, ale především celého datového toku. Vzhledem k faktu, že online šifrování provozu je technicky téměř nemožné prolomit, předpokládá se, že zajišťování datové komunikace a obsahu koncových zařízení se stane naprosto bezpředmětným. Pokud také přihlédneme k faktu, že již nyní se často uživatelé staví k bezpečnostním pravidlům velmi nezodpovědně a lehkomyslně, lze předpokládat, že počet útoků bude narůstat.

Závěr

V předchozích kapitolách jsme si stručně nastínili nejčastější formy kybernetické kriminality páchané v současnosti. S odkazem na samotný úvod, informační technologie suplují člověka v množství jeho činností. Bonusem se stává následné ulehčení, které nám tyto technologie umožňují. Právě počítačová technologie vykazuje rozvíjející se trend, který má vysoké tempo růstu. Bohužel s tímto rychlým růstem techniky jde v ruku v ruce kriminalita páchaná v rámci kyberprostoru. Kybernetická kriminalita stejně jako počítačové technologie zaznamenává také veliký posun vpřed. Tento posun můžeme pozorovat zejména v rozvíjejících se formách kybernetické kriminality. Postupné zdokonalování, ale i nové formy jednání pachatelů kriminality na internetu, která by nikdy nevznikla bez informačních technologií.

Co se týče budoucích trendů vývoje kybernetické kriminality, lze říci, že v současné době jsou na vzestupu různá podvodná jednání v podobě poplašných zpráv, phishingových, spear-phishingových i podvodných e-mailů z hlediska počtu i sofistikovanosti. Kvalitativní posun byl patrný zejména z používání dokonalejší češtiny, propracovanějších formátů e-mailů a různorodosti. Také bych uvedl, že výrazný milník bylo uvedení chytrých zařízení na trh. V současné době může být ovládáno prakticky cokoliv pomocí chytrého zařízení, od zabezpečovacích systémů, po domácnost. Ušetření času skýtá v těchto technologiích velké riziko v podobě relativně jednoduchého napadení jinou osobou.

Tímto se kybernetická kriminalita, obzvláště ta, která je motivována ekonomickou, politickou či mocenskou sílou, stává reálnou každodenní hrozbou každého z nás.

Pevně doufám, že skutečnosti, které vznikli v roce 2019 v síti Benešovské nemocnice, byl milník, kdy si osoby, které rozhodují o financování a zabezpečení sítí integrovaného záchranného systému, uvědomili, že kybernetická kriminalita a kyberprostor není zanedbatelné riziko, kde se dá ušetřit a které se těchto institucí netýká, a poskytli dostatečné finanční prostředky, které jsou nedílnou součástí modernizace a zabezpečení těchto sítí. Největším rizikem těchto sítí je propojení vnitřní sítě Intranetu s venkovní, vnější sítí Internetu. To znamená modernizovat vnitřní síť Intranetu v takovém rozměru, aby propojení s Internetem bylo bezpečné. Zejména

pokud by došlo k pokusu dostat se z venkovních sítí do „uzavřené“ vnitřní sítě, aby byl systém dostatečně zabezpečen. Toto samozřejmě znamená velké množství finančních prostředků, ale také se nesmí zapomenout na správce, či administrátory, kteří se o vnitřní sít musí pravidelně starat a hlavně aktualizovat bezpečnostní systémy. Taktéž by mělo být samozřejmostí, aby uživatelé byli řádně proškoleni, protože špatným zacházením na uživatelském rozhraní může docházet k nevědomému oslabení zabezpečení a k případnému napadení vnitřní sítě integrovaného záchranného systému. Toto je samozřejmě velice časově náročné, ale nesmírně důležité. Informovat uživatele o správném zacházení s počítačem uvnitř sítě, jak pevného zapojeného počítače k intranetu, tak i přenosných notebooků, které případně uživatelé doma připojují na domovský Internet, či se dokonce vzdáleně připojují do vnitřní sítě instituce.

Co se týká pramenů, práce byla vypracována zejména za použití odborné literatury a elektronických zdrojů, přičemž posledně zmiňované převažovaly, avšak nikoliv razantním způsobem. Jak je z práce patrné, stěžejními odbornými díly pak byly díla Gřivny, Závršníka a Jirovského, jenž se prolíná hlavně v prvních kapitolách. Elektronické zdroje naopak spíše dokreslovaly obecné informace nebo byly zdrojem příkladů, avšak její využití jsem se snažil omezit z toho důvodu, že ne vždy se musí jednat o relevantní informace.

Vzhledem k účelu a k předpokládanému rozsahu bakalářské práce je zjevné, že tato práce nemohla detailně postihnout komplexní problematiku kybernetické kriminality. Nicméně, dle názoru autora, nabízí ucelený přehled, a to v relativně aktualizované podobě. Relativně aktualizované proto, že oblast informačních technologií je neustále se rozvíjející oblast, přičemž se rychlost rozvoje neustále zvyšuje.

Seznam použitých zdrojů

Literární zdroje

1. ANDRESS, J. *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice* (2nd ed.). 2014. Elsevier Science. ISBN 978-01-2800-812-6.
2. BURIAN, P. *Internet inteligentních aktivit*. Praha: Grada, 2014. ISBN 978-80-247-5137-5.
3. CONWAY, R. *Code Hacking: A Developer's Guide to Network Security.* Hingham, Massachusetts: Charles River Media. 2004. 281 s. ISBN 1-58450-314-9.
4. GŘIVNA, T., POLČÁK, R., *Kyberkriminalita a právo*. Praha: Aufitorium, 2008. 220 s. ISBN 978-80-9037-867-3.
5. GŘIVNA, T., SCHEINOST, M., ZOUBKOVÁ, I. *Kriminologie*. Praha: Wolters Kluwer, a.s, 2015. Sv. 4. vyd. 530 s. ISBN 978-80-7478-614-3.
6. JIRÁSEK, P., NOVÁK. L., POŽÁR. J., Výkladový slovník kybernetické bezpečnosti. Praha: Policejní akademie České republiky v Praze, 2015. 242 s. ISBN 978-80-7251-436-6.
7. JIROVSKÝ, V. *Kybernetická kriminalita*. Praha: Geada Publishing a.s., 2007. 288 s. ISBN 978-80-247-1561-2.
8. LOWE, S. *Mistrovství ve VMware vSphere 5: kompletní průvodce profesionální virtualizací*. Brno: Computer Press, 2013. ISBN 978-80-251-3774-1.
9. MATOUŠEK, P. *Síťové aplikace a jejich architektura*. Brno: VUTIUM, 2014. ISBN 978-80-214-3766-1.
10. KABELOVÁ, A., DOSTÁLEK, L. *Velký průvodce protokoly TCP/IP a systémem DNS. 5.*, aktualiz. vyd. Brno: Computer Press, 2008. ISBN 978-80-251-2236-5.
11. KOLOUCH, J., BAŠTA, P., KROPÁČOVÁ, A., KUNC, M., *CYBERSECURITY*, 1. vydání. Praha, 2019, 562 s. ISBN 978-80-88168-34-8.
12. SMEJKAL, V,. *Kriminologie*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015. 640 s. ISBN 978-80-7478-615-3.
13. ŠÁMAL, P. a kol. Trestní zákoník II. §140 až 421. Komentář. 2. vydání. Praha: C. H. Beck, 2012, 2150 s. ISBN 978-80-7400-428-5.

14. WEBER, R., H., WEBER, R. *Internet of Things: Legal Perspectives.* Berlin: Springer, 2010. 129 s. ISBN 978-3-642-11709-1.
15. ZÁVRŠNÍK, A. *Kyberkriminalita*. Praha: Wolters Kluwer a.s. 2017. 148 s., ISBN 978-80-7552-758-5.

Elektronické zdroje

1. Bezpečnost provozu intranetu [online]. Brno: CCB, spol., 2003 [cit. 2021-12-01]. Dostupné z: <https://goo.gl/NGZKiQ>.
2. ČESKO. MINISTERSTVO VNITRA. *Analýza současného stavu a trendů vývoje trestné činnosti na úseku informačních technologií a Internetu včetně návrhu řešení.* [online]. © 2020 Ministerstvo vnitra České republiky. [cit. 2021-11-05]. Dostupné z: <http://www.mvcr.cz/soubor/informacni-pdf.aspx>.
3. ČESKO. MINISTERSTVO VNITRA. [online]. © 2020 Ministerstvo vnitra České republiky [cit. 2021-03-14]. Dostupné z: <http://www.mvcr.cz/>.
4. ČESKO. MINISTERSTVO VNITRA. *Kyberkriminalita*. [online]. © 2020 Ministerstvo vnitra České republiky. [cit. 2021-03-15]. Dostupné z: <https://prevencekriminality.cz/prevence-kriminality/kyberkriminalita/rozcestnik-kyberkriminality/>.
5. ČESKO, NÁRODNÍ ÚŘAD PRO BYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Zpráva o stavu kybernetické bezpečnosti ČR - 2020*. [online]. Praha: NUKIB, 2021, [cit. 2021-03-15]. Dostupné z: <https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/zpravy-o-stavu-kb/>.
6. ČESKO. PARDUBICKÝ KRAJ. *ZZS PAK Smlouva o dílo* [online]. Průmyslová 450,530 03 Pardubice: Zdravotnická záchranná služba Pardubického kraje, 2020 [cit. 2021-03-14]. Dostupné z: <https://www.zakazky.pardubickykraj.cz>.

7. ČESKO. POLICIE ČESKÉ REPUBLIKY. *Vývoj registrované kriminality v roce 2021* [online]. © 2022 Policie ČR. [cit. 2022-03-20]. Dostupné z: <https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2021.aspx>.
8. CHESWICK, W. R., BELLOVIN, S. M., RUBIN, A. D. "Google Books Link". *Firewalls and Internet Security: repelling the wily hacker* [online]. 2003, [cit. 2021-03-14]. Dostupné z: <https://books.google.com/>.
9. Intranety. [online]. Brno: cognito.cz, 2017 [cit. 2020-12-01]. Dostupné z: <goo.gl/pfgfUa>.
10. KRAUSOVÁ, V. *Internet věcí (Internet of Things) a jeho bezpečnost.* [online]. Brno, 2014. 37 s., 9 nečísl. s. Bakalářská diplomová práce. Ved. práce PhDr. Michal Lorenz, Ph.D. Masarykova univerzita, Filozofická fakulta, Ústav české literatury a knihovnictví, Kabinet informačních studií a knihovnictví, Informační studia a knihovnictví. Přístup také z: https://is.muni.cz/th/d0hvz/
11. ŽOLTA, L. Firewall. [online]. [cit. 2022-03-25]. Dostupné z: <http://lucie.zolta.cz/index.php/pocitace-a-site/178-stavovy-firewall>.
12. Next generation firewall [online]. Praha: www.sands.cz, 2019 [cit. 2021-03-20]. Dostupné z: <http://www.sands.cz/sluzby-produkty/bezpecnost-ict/next-generation-firewall>.
13. *Network Segment Definition* [online]. 2005 [cit. 2010-09-03]. Dostupné z: <https://www.cisco.com/c/en/us/products/security/what-is-network segmentation.html >.
14. Webový aplikační firewall [online]. Autocont, 2019, [cit. 2021-03-14]. Dostupné z: <https://www.autocont.cz/aktuality/openspace/ochrana-webovych-aplikaci/webovy-aplikacni-firewall>.

Zdroje obrázků

Zdroj tabulek