ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
FAKULTA BIOMEDICÍNSKÉHO INŽENÝRSTVÍ
Katedra zdravotnických oborů a ochrany obyvatelstva

Služby a prostředky zajišťující kybernetickou bezpečnost vybrané organizace

Services and resources ensuring cyber security of the selected organization

Diplomová práce

Studijní program: Civilní nouzové plánování
Autor diplomové práce: Mgr. Bc. Kamil Derfl, LL. M.
Vedoucí diplomové práce: Ing. Matej Kačic, PhD.

Kladno 2022

ZADÁNÍ DIPLOMOVÉ PRÁCE

I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení:	**Derfl**	Jméno:	**Kamil**	Osobní číslo:	**503670**
Fakulta:	**Fakulta biomedicínského inženýrství**				
Garantující katedra:	**Katedra zdravotnických oborů a ochrany obyvatelstva**				
Studijní program:	**Civilní nouzové plánování**				

II. ÚDAJE K DIPLOMOVÉ PRÁCI

Název diplomové práce:

Služby a prostředky zajišťující kybernetickou bezpečnost vybrané organizace

Název diplomové práce anglicky:

Services and Resources Ensuring Cyber Security of the Selected Organization

Pokyny pro vypracování:

V práci se bude student věnovat bezpečnosti kyberprostoru a základní charakteristice sítě Internet. V úvodu zmíní pojem kyberprostoru a vysvětlí jeho význam. Rovněž se dotkne pojmu ICT prostředků a jejich významu v komunikaci přes prostředí internetové sítě. Zároveň se bude zabývat problematikou bezpečnosti kyberprostoru v souvislosti s počítačovými viry a internetovou kriminalitou a jejími specifiky. Zmíní některá paragrafová znění, podle kterých se tato kriminalita postihuje a stání instituce, které jsou zřízeny pro ochranu kyberprostoru v ČR. V závěru práce uvede některé z možností prevence a v praktické části zpracuje výsledky provedeného zkoumání v rámci security awareness trainingu – testování reakce zaměstnanců na předem připravený phishingový útok ve firemní síti za předem stanovených podmínek. Výstupem budou anonymizovaná, ale relevantní data schopná popisu případných problémů v bezpečnosti sítě.

Seznam doporučené literatury:

[1] LUKÁŠ, Luděk, Teorie bezpečnosti , ed. 1, Zlín: Radim Bačuvčík – VeRBuM, 2017, 220 s., ISBN 978-80-87500-80-7

[2] KOLOUCH, Jan, BAŠTA, Pavel a kol., CyberSecurity, ed. 1, Praha: Edice CZ.NIC, 2019, 562 s., ISBN 978-80-88168-34-7

[3] KOLOUCH, Jan, CyberCrime, ed. 1, Praha: Edice CZ.NIC, 2016, 528 s., ISBN 978-80-88168-15-7

[4] KOŽÍŠEK, Martin, PÍSECKÝ, Václav, Bezpečně na internetu průvodce chováním ve světě online, Praha: Grada, 2016, 176 s., ISBN 978-80-247-5595-3

Jméno a příjmení vedoucí(ho) diplomové práce:

Ing. Matej Kačic, PhD.

Jméno a příjmení konzultanta(ky) diplomové práce:

Datum zadání diplomové práce: **04.10.2021**
Platnost zadání diplomové práce: **22.09.2023**

doc. Mgr. Zdeněk Hon, Ph.D.
vedoucí katedry

prof. MUDr. Jozef Rosina, Ph.D., MBA
děkan

PROHLÁŠENÍ

Prohlašuji, že jsem diplomovou práci s názvem Služby a prostředky zajišťující kybernetickou bezpečnost vybrané organizace vypracoval samostatně pouze s použitím pramenů, které uvádím v seznamu bibliografických odkazů.

Nemám závažný důvod proti užití tohoto školního díla ve smyslu § 60 zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů.

V Kladně dne 10.05.2022

.....…….

Mgr. Bc. Kamil Derfl, LL. M.

PODĚKOVÁNÍ

Touto cestou bych rád poděkoval vedoucímu práce Ing. Mateji Kačicovi, PhD. za jeho odborné vedení této diplomové práce a velmi podnětné rady a připomínky při jejím zpracování. Dále bych rád poděkoval Dominiku Kollárovi za jeho angažovanost, rady, kreativitu a ochotu pomoci.

ABSTRAKT

Tato práce se věnuje problematice bezpečnosti kyberprostoru, základní charakteristice provozu internetové sítě a možnostem jejího zabezpečení před vnějšími kybernetickými útoky. V kapitole 3 je zmíněn a vysvětlen pojem kyberprostoru a ICT, tedy informační a komunikační technologie, které mají svou nezastupitelnou funkci v době informační společnosti. V kapitole 4 je v krátkosti popsána historie vzniku sítě internet a základní charakteristika druhů a rychlostí připojení. V kapitole 5 jsou zmíněny instituce a jejich jednotlivé úkoly v souvislosti s ochranou kyberprostoru ČR před útoky, ke kterým se zneužívá internetová síť. Pojmy, které charakterizují internetovou kriminalitu a jednotlivé druhy útoků jsou probrány v kapitolách 6 a 7. Kapitola 8 se věnuje službám a prostředkům zajišťujícím kybernetickou bezpečnost vybrané organizace a současným trendům rozvoje samotného kyberprostoru a jeho ochrany včetně standardů řízení informační bezpečnosti. Kapitola 9 prezentuje metodiku zvoleného výzkumu, pro potvrzení stanovené hypotézy a v kapitole 10 jsou pak uvedeny konkrétní výsledky, které tuto hypotézu potvrzují. V kapitole 11 jsou diskutována jednotlivá opatření, která při jejich zavedení do systému ochrany významným způsobem přispějí k vyšší informační bezpečnosti a lepšímu zabezpečení kyberprostoru.

Klíčová slova

Internet; kyberprostor; ICT; počítačová kriminalita; kybernetická kriminalita; NÚKIB; ISMS; ITIL; DMARC; NIST.

ABSTRACT

This work describe the issue of cyberspace security, the basic characteristics of the operation of the Internet network and the possibilities of its security against external cyber attacks. Chapter 3 mentions and explains the concept of cyberspace and ICT, i.e. information and communication technologies, which have their irreplaceable function in the age of the information society. Chapter 4 briefly describes the history of the Internet and the basic characteristics of connection types and speeds. Chapter 5 mentions the institutions and their individual tasks in connection with the protection of the cyberspace of the Czech Republic against attacks to which the Internet network is abused. The concepts that characterize cybercrime and the various types of attacks are discussed in Chapters 6 and 7. Chapter 8 deals with the services and means of ensuring the cyber security of the selected organization and current trends in the development of cyberspace itself and its protection, including information security management standards. Chapter 9 presents the methodology of the selected research, to confirm the established hypothesis, and Chapter 10 presents the specific results that confirm this hypothesis. Chapter 11 discusses the individual measures that, when introduced into the protection system, will significantly contribute to higher information security and better security of cyberspace.

Keywords

Internet; cyberspace; ICT; computer crime; cyber crime; NÚKIB; ISMS; ITIL; DMARC; NIST.

Obsah

1 ÚVOD 9
2 CÍLE PRÁCE A HYPOTÉZY 11
3. PŘEHLED SOUČASNÉHO STAVU 14
3.1 Pojem kyberprostor 14
3.2 Information and Communication Technologies – ICT 15
3.3 Informační společnost 16
4. EXPERIMENTÁLNÍ SÍŤ – ARPANET 18
4.1 Internetová síť alias Internet 19
4.2 Druhy a rychlost připojení 20
4.3 Technologie připojení 21
5. BEZPEČNOST KYBERPROSTORU V ČR 25
5.1 Národní úřad pro kybernetickou a informační bezpečnost – NÚKIB – struktura 27
5.2 Národní úřad pro kybernetickou a informační bezpečnost– NÚKIB – úkoly 28
5.3 Národní centrum kybernetické bezpečnosti – NCKB 30
5.4 Computer Emergency Response Team – CERT (GOVCERT.CZ CSIRT.CZ) ... 31
5.5 Computer Incident Response Capability – Centrum CIRC 33
5.6 Národní agentura pro komunikační a informační technologie – NAKIT 34
6. INTERNETOVÁ KRIMINALITA 35
6.1 Kybernetická kriminalita 35
6.2 Počítačová kriminalita 36
7. KRIMINALITA PÁCHANÁ NA INTERNETU 39
7.1 Druhy počítačových útoků 40
7.2 Spam 41
7.3 DoS a DDoS útoky 43
7.4 Phishing 46
8. SLUŽBY A PROSTŘEDKY ZAJIŠŤUJÍCÍ KYBERNETICKOU BEZPEČNOST VYBRANÉ ORGANIZACE 49
8.1 Řešení ochrany kyberprostoru vybrané organizace 50
8.1.1 Systém řízení bezpečnosti informací – ISMS 53
8.2 Management bezpečnosti informací podle ITIL 55
8.3 Trendy v rozvoji řízení informační bezpečnosti – bezpečnostní rámce podle CIS a NIST 56
8.3.1 Centrum pro kybernetickou bezpečnost internetu – CIS 56

8.3.2 Národní úřad pro standardy a technologie – NIST 58
8.4 Monitoring sítě a její filtrace 60
8.5 Doporučená opatření 62
9. METODIKA 64
9.1 Popis metody testu 65
10. VÝSLEDKY 67
11. DISKUZE 69
11.1 Přijatá opatření v rámci společnosti 69
11.2 Doporučení pro infrastrukturu 70
11.3 Doporučení pro stanice a servery 71
11.4 Doporučení pro správu účtů 73
11.5 Doporučení pro správu e-mailové ochrany 74
12. ZÁVĚR 76
13. SEZNAM POUŽITÝCH ZKRATEK 78
14. SEZNAM POUŽITÉ LITERATURY 80
15. SEZNAM POUŽITÝCH OBRÁZKŮ 89
16. SEZNAM POUŽITÝCH GRAFŮ 90

1 ÚVOD

Pro vypracování této závěrečné práce padla volba na téma zabývající se bezpečností v kyberprostoru a s tím související problematiku počítačové kriminality. S rozvíjejícím se rozmachem prostředků ICT (Information and Communication Technologies) se otevírají nové možnosti jak využít stále bující kyberprostor. S rostoucím rozsahem možností kyberprostoru vzkvétá bohužel i počítačová kriminalita. Svět si problém týkající se bezpečnosti kyberprostoru dobře uvědomuje, jelikož škody způsobené tímto druhem kriminality jsou v celosvětovém měřítku obrovské. Odhadované škody napáchané ransomwarem dosáhly v roce 2021 jen v USA 623,7 milíónů USD a došlo k 495 milíónům ranwomwarových útoků, což představuje 148% nárůst oproti roku 2020. Společnosti zaznamenávají obrovské ztráty v prostojích a ztrátách produktivity nebo na platbách výkupného. Ovšem skutečná výše výkupného, která je útočníkům zaplacena, je pouhým zlomkem těchto celkových nákladů. V únoru 2020 zaplatila dánská společnost ISS po ransomwarovém útoku výkupné přes 50 miliónů USD, město New Orleans (USA) zaplatilo přes 7 miliónů USD, přepravní společnost Maersk zaplatila 200 miliónů USD zdravotnické organizace v USA stálo 92 ransomwarových útoků odhadem 21 miliard USD! Společnost Maersk je u kyberzločinců oblíbená, protože již v roce 2017 se jim povedlo globálně infikovat její síť ransomwarem NotPetya a nákaza se rozšířila tak, že se s ransomwarem potýkalo 76 přístavních doků a společnost Maersk odhadovala škodu na 300 miliónů USD. Náklady v souvislosti s počítačovou kriminalitou by, dle odhadu, měly do roku 2025 dosáhnout celosvětově 10,5 bilionů USD. Dle dostupných dat a statistik společností Enisa, Kaspersky Labs, Cybersecurity Ventures, Webroot Threat Report, Sonic Wall, Emisoft, Coveware´s atd. můžeme říci, že počítačová kriminalita je stále lukrativnější business, což ji pochopitelně činí přitažlivější pro budoucí i současné pachatele. S rostoucí sofistikovaností technologického světa lze očekávat, že i taktika, kterou kybernetičtí zločinci používají, se bude velice rychle vyvíjet [1].

Z důvodů viz výše, byla Českou republikou v únoru 2005 podepsána Úmluva o počítačové kriminalitě a následně ratifikována v srpnu 2013. Ze strany států EU bylo za účelem ochrany osobních údajů vydáno dne 27. dubna 2016 Nařízení Evropského parlamentu a Rady EU 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice

95/46/ES, s cílem posílit ochranu osobních údajů, jelikož současná právní úprava byla již nedostatečná s ohledem na prostředky, které se používají ke zpracování osobních údajů a s ohledem na samotnou architekturu procesu zpracování osobních údajů, který je dnes již mnohem sofistikovanější. Vydáním nařízení došlo k posílení práv subjektu údajů a k sjednocení právního rámce napříč státy EU.

2 CÍLE PRÁCE A HYPOTÉZY

Cílem této práce je pokusit se popsat a vysvětlit pojem kyberprostor jako takový. Dále rozebrat a zanalyzovat oblast problematiky zajištění jeho bezpečnosti, resp. bezpečnosti uživatelů sítě a poukázat na závažnost počítačové a internetové kriminality, která v posledním období dramaticky roste a nevyhýbá se nikomu. S tímto druhem kriminality měl co do činění zcela jistě každý uživatel internetové sítě. Každý by s tímto sdělením možná nesouhlasil, protože pro běžného uživatele bez patřičných zkušeností v této oblasti nemusí být nebezpečí v první chvíli jasně patrné a rozpoznatelné. Jsem ale přesvědčen o pravdivosti tohoto tvrzení, neboť by jednoduše stačilo nahlédnout do spam koše jakékoliv e-mailové schránky.

Tato práce má v úmyslu poukázat i na historické aspekty existence internetové sítě. Zmíní se o okolnostech vzniku internetu, o lidech, kteří stojí za zrodem tohoto fenoménu, jenž se během několika roků stal bezesporu nepostradatelnou součástí moderní lidské společnosti prakticky na celé planetě. Internet dokázal změnit způsob myšlení společnosti, její komunikaci a fungování. Na komunikaci po síti postupně přechází prakticky všechny subjekty, počínaje tzv. obyčejným uživatelem a konče např. státní správou. Neustále se zvyšuje procento uživatelů internetu, provozující nákupy po síti prostřednictvím různorodých e-shopů. Dostupné jsou dnes nejrůznější objednávkové systémy, ať už se jedná o nákup potravin, lístků do divadla nebo návštěvu lékaře. Bez internetu si tak současnou společnost vlastně ani nedovedeme představit. Lidstvo si tento fenomén doslova podmanil.

Přes všechna pozitiva, která internet a moderní komunikační prostředky nabízí a poskytuje, odhalí však čtenáři tato práce i stinné stránky moderních informačních technologií. Tak jako prakticky žádná oblast lidského konání, tak i svět internetu nedokáže odolat mnoha druhům podvodného jednání a kriminálních deliktů. Může se však účinně bránit, k čemuž má dostatek prostředků.

Chceme poukázat na způsoby a prostředky, které jsou k páchání internetové kriminality využívány a obeznámíme čtenáře s pravomocemi a oblastmi působnosti institucí, jejichž hlavním úkolem je dozor nad bezpečností kyberprostoru v České republice. Čtenář si tak bude moci učinit představu o tom, jak rozsáhlá je oblast této problematiky, jaké úsilí a finanční prostředky jsou vynakládány na rozvoj a udržení

bezpečného kyberprostoru ve státě a kolik institucí je do této činnosti zapojeno. Zmíním nejčastější druhy kybernetických útoků, k nimž v současnosti dochází, aby tak bylo patrno, jakých zločinů se pachatelé v kyberprostoru nebo počítačových sítích dopouštějí a co vše je za takové činy považováno. K tomuto účelu je do práce vložena přehledná infografika.

Aby bylo možno se kybernetickým útokům účinně bránit, jsou v této práci zmíněna nejčastěji používaná ochranná a bezpečnostní opatření, která přispívají ke zvýšení zabezpečení sítí a zpracovávaných dat. Tato problematika je řešena od počátku provozování internetové sítě a proto jsou zde zmíněny stěžejní právní normy a bezpečnostní rámce, podle kterých se postupuje při budování a posilování kybernetické bezpečnosti ve světě a v prostředí České republiky.

Tento přehled normativních aktů může být nápomocen všem, kteří se chtějí nebo musí orientovat ve složité problematice kybernetické bezpečnosti. V Evropě se jedná o nařízení Evropského parlamentu a Rady EU 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o směrnici Network Information Security (dále jen NIS) 2016/1148, vydaná 6. července 2016, která vznikla jako ucelený dokument, jehož cílem je zajistit společnou a vysokou míru bezpečnosti na úrovni sítí a informačních systémů a vytvořit základní požadavky, které by měly plnit všechny členské státy EU.

Tyto požadavky byly v České republice implementovány do zákona č. 181/2014 Sb., nazývaného Zákonem o kybernetické bezpečnosti (ZoKB), který upravuje pravomoci a povinnosti státu a některých dalších subjektů v oblasti kybernetické bezpečnosti a do dalších normativních právních aktů, které jsou v této práci zmíněny. Samotný zákon č. 181/2014 Sb. v současné době čeká novelizace, aby tak vyhovoval nejnovějším požadavkům Evropské unie.

Regulace v oblasti ochrany osobních údajů a nakládání s daty se stala nutností s ohledem na fakt, že informační a komunikační systémy tvoří nedílnou součást našich životů. Do značné míry zabezpečují fungování celé společnosti a v některých klíčových oblastech nebo službách se tyto systémy staly naprosto nepostradatelnými.

V závěru práce si praktickým zkoumáním ověříme hypotézu, podle které je nejslabším článkem kybernetické bezpečnosti lidský faktor. V řetězci zabezpečení kyberprostoru, je toto zabezpečení tak silné, jak je silný jeho nejslabší článek. V rámci tohoto zkoumání byl navržen a simulován phishingový útok v podobě podvrženého firemního e-mailu, jenž byl rozeslán ve firemní síti s cílem získat přihlašovací údaje zaměstnanců vybrané společnosti.

Na základě interpretace výsledků provedeného testování si společnost vyhodnotí firemní bezpečnostní politiku, úroveň zabezpečení své sítě, úroveň edukace zaměstnanců a případně přijme účinnější a sofistikovanější bezpečnostní opatření. Udržet zabezpečení kyberprostoru na maximální možné úrovni je nikdy nekončící proces a s vývojem nových technologií i finančně poměrně nákladná záležitost.

Jsme přesvědčeni, že problematika kybernetické bezpečnosti musí být v popředí zájmu všech společností, institucí, ale i jednotlivých uživatelů, má-li být zaručena ochrana a integrita dat, a že se tak bezpochyby jedná o významné celospolečenské aktivum. Případnou ztrátou dat bývá způsobena škoda v různých formách a různého rozsahu. Pro soukromého uživatele je taková situace zcela jistě velmi nepříjemná, ovšem pro běžný výrobní podnik již pouhý výpadek sítě na několik hodin představuje významné finanční ztráty.

Tato práce ve svém obsahu publikuje a doporučuje spolehlivá řešení, jejichž aplikací je riziko ohrožení nebo případné ztráty důležitých dat omezeno na minimální možnou úroveň a mohou tak být nápomocna všem, kterým na bezpečnosti kyberprostoru záleží.

3 PŘEHLED SOUČASNÉHO STAVU

Co je to kyberprostor (z anglického cyberspace)? Pro lepší představu co to kyberprostor je, se nebojím použít jako příklad film Matrix (v originálním znění "The Matrix"). Většina lidí snímek viděla, a tak je snažší tento pojem přiblížit. Kyberprostor je abstraktní svět, tvořený systémy ICT (Information and Communication Technologies) prostředků, které jsou ve vzájemném propojení, a které umožňují komunikaci v tomto virtuálním prostoru. Paradoxem je, že nám vytváří reálný časoprostor, ve kterém probíhá naše reálná komunikace s okolním světem např. prostřednictvím e-mailu, VoIP telefonie (Voice over Internet Protocol), sociálních sítí nebo si jeho prostřednictvím jednoduše objednáváme zboží či služby. Pro bezproblémové fungování v tomto virtuálním prostoru je nutné vyřešit zabezpečení dat a komunikace proti jejich zneužití. Útočníci se denně poukouší o krádež dat, prolomení hesel, neautorizované ovládnutí systému, získání citlivých údajů za účelem vydírání nebo odcizení identity atd. K tomu používají různé druhy sofistifikovaného softwaru nebo technik sociálního inženýrství. Proto je nutné si osobní a jiné citlivé údaje chránit. Bezpečnost dat a komunikace musí být priorita!

3.1 Pojem kyberprostor

Kyberprostor je přesným opakem reálného světa. Pro některé jedince lidského druhu, je to jediné místo kde jsou schopni "existovat". Kyberprostor nejsou jen samá pozitiva, ale bohužel i značná negativa, která zásadním způsobem dopadají na naši společnost víc, než jsme si schopni připustit.

Vymezení pojmu, který by jednoznačně a zcela přesně definoval kyberprostor není v současné době vůbec jednoduchý úkol, jelikož se na jednoznačném znění neshodou ani odborníci na akademické půdě. Nejširší znění pojmu kyberprostor je:

„Kyberprostor je globální a vyvíjející se doména, charakterizovaná používáním elektrických sítí a elektromagnetického spektra, jejíž smysl je vytvářet, uchovávat, upravovat, vyměňovat, sdílet, získávat, používat, vymazávat a narušovat informace.

Kyberprostor zahrnuje:

a) fyzická i telekomunikační zařízení, která umožňují spojení technologických a komunikačních systémových sítí, chápáno obecně (SCADA zařízení, smartphony/tablety, počítače, servery atd.),

b) počítačové systémy a komplementární software, který zaručuje funkčnost a konektivitu systému,

c) spojení počítačových sítí,

d) uživatelské vstupy a uzly zprostředkovatelů spojení,

e) informace – uživatelská data" [2].

Je lhostejno kolik definic kyberprostoru je zatím v různých pramenech uvedeno. Podstatné je, že se jedná o nehmotný prostor, na kterém lidstvo existenčně zavisí, ať se mu to líbí či nikoliv. Se vzrůstajícím počtem uživatelů se zároveň rozšiřuje kyberprostor a jeho možnosti. K pohybu informací jsou využívány různé technologie a prostředky, bez nichž by tento prostor byl jen prázdným místem s nevyužitým potenciálem.

3.2 Information and Communication Technologies – ICT

Zkratka ICT v sobě nese označení pro informační a komunikační technologie, ale logicky v sobě obsahuje i nástroje nebo prostředky, přes které konkrétní informace a komunikace plynou. Svým rozsahem ICT přesahuje pojem IT (Information Technologies), a vzhledem k obrovskému rozmachu komunikačních technologií a zvyklostí společnosti, vyvstává potřeba pojem IT rozšířit hlavně o pojem "komunikace" (Communication). Protože zejména díky ICT prostředkům je nám umožněno se pohybovat v kyberprostoru. Toto odvětví se tak právem řadí k nejdynamičtěji rozvíjejícím se odvětvím současnosti.

Pojmem to lze vymezit následovně: "*ICT prostředky jsou informační a komunikační technologie (někdy též uváděno IKT)...týkající se všech technologií používaných pro správu telekomunikací, vysílacích médií, inteligentních systémů správy budov, audiovizuálního zpracování a přenosových systémů a síťových řídicích a monitorovacích funkcí" [3].*

Jinými slovy můžeme říci, že ICT (informační a komunikační technologie) jsou souborem technologií a nástrojů, které lidé používají jak ke sdílení, distribuci a sběru

informací, tak i ke vzájemné komunikaci s využitím komunikačních prostředků, počítačů a vzájemně propojených počítačových sítí. Termín ICT v sobě již zahrnuje technologické inovace, informace a komunikaci.

ICT má v současné době hluboký dopad zejména na mladou generaci, jelikož se nástroje ICT stávají běžnou a můžeme říci i neoddělitelnou součástí života. Jedná se zejména o všechna zařízení, která jsou tzv. smart. Jako příklad můžeme uvést mobilní dotykové telefony, tablety, phablety, hodinky, náramky, notebooky, televize, kamery a dnes už považujeme za samozřejmost i smart pračky, susičky, myčky, chladničky, žárovky, zásuvky atd. Zmíněná zařízení dnes označujeme termínem **IoT** (Internet of Things tedy Internet věcí). Jedná se o komunikaci mezi smart zařízeními denní potřeby, a to zejména na základě bezdrátové komunikace nebo internetové sítě, do které je zapojen i člověk.

V důsledku značného pokroku v této oblasti jsou školy nuceny do výuky zařazovat smart tabule a displeje, projektory, tablety, multimediální učebnice a další moderní nástroje pro multimediální výuku. Klasickou výuku IT postupně nahrazuje výuka ICT, která vede nastupující generace k tomu, aby zvládaly používat rozvíjející se komunikační technologie a naučily se pracovat s informacemi (jak a kde je vyhledat, posoudit jejich relevantnost a umět je využít).

Jako názorný příklad výuky prostřednictvím IoT může sloužit rok 2021, kdy v důsledku šíření viru COVID–19, byly školy donuceny přejít na on-line výuku.

3.3 Informační společnost

Celá společnost touží po různých druzích informací. Na informacích stojí a padá celý svět a my žijeme v tzv. "informační společnosti". Co znamená informační společnost? Pod tímto pojmem se rozumí *společnost, ve které kvalita života, ale i perspektiva sociálních změn a ekonomického rozvoje závisí na schopnosti získat a využít informace, ty se pro takovou společnost stává alfou a omegou jejího fungování [4]*.

Počátky informační společnosti lze spatřovat v 80. letech 20. století, kdy se z USA do společnosti po celém světě začala v masovém měřítku šířit internetová sít (dále jen internet). Informační společnost se vyznačuje: *"...podstatným využíváním*

digitálního zpracovávání, uchovávání a přenosu informací" [5]. Informace jsou velmi cenným artiklem a ovlivňují každou oblast moderní společnosti. Kdo má ty správné informace, má náskok před konkurencí. Informace sdílené v síti hýbou ekonomikami vyspělých států, které internet implementovaly do své infrastruktury. S internetem přichází úplně nové možnosti, které svým rozsahem zcela zásadně mění společnost. Hlavně v oblasti ekonomiky a průmyslu se kola byznysu roztáčí na plné obrátky. S tím úzce souvisí překotný technologický pokrok, snad v každém technologickém odvětví, jež se vydal mílovými kroky vpřed a přináší tak výsledky v miniaturizaci konstrukčních prvků IT techniky, zejména pak u mikroprocesorů. Věda a výzkum se stává ústředním tématem pro jejich financování, a rovněž je třeba změnit systém vzdělávání. Mění se i sociokulturní chování a způsob komunikace společnosti. Padají různá společenská tabu a lidská společnost už nebude nikdy stejná jako před nástupem internetu. Je na této síti závislá a ta trvale změnila lidský svět. Zařízení implementovaná do našeho života slibují usnadnění života, komunikace, práce apod. Co se stane v případě, když dojde k dlouhodobému výpadku internetové sítě nebo elektrické sítě? Je skutečně moderní společnost schopná fungovat v případě tzv. blackoutu?

4 EXPERIMENTÁLNÍ SÍŤ – ARPANET

Prvotní počátek výzkumu a výstavby internetové sítě, tedy internetu by se mohl datovat do června roku 1945 kdy americký vědec Dr. Vannevar Bush v časopisu The Athlantic Monthly publikoval článek s názvem "As We May Think", ve kterém popsal funkci zařízení, které nazval Memex (memory extended). Toto zařízení mělo zvětšit paměťovou kapacitu lidského mozku a fungovat na obdobném principu jako lidský mozek. Tedy informaci přijmout, vyhodnotit a uložit její asociaci. V případě potřeby je informace zpětně vyvolána prostřednictvím asociace. Toto zařízení nebylo nikdy postaveno, avšak dalo by se v hrubých rysech považovat za "předchůdce PC" [6].

Milníkem pro spuštění opravdového technologického rozvoje, bylo vypuštění sovětského Sputniku 1 na oběžnou dráhu dne 4. 10. 1957. Tato událost spustila v USA vlnu strachu z toho, že USA technologicky zaostávají za Sovětským svazem v období studené války, kdy hrozilo reálné riziko zničení komunikační infrastruktury v důsledku použití jaderných zbraní. Spojené státy americké si uvědomily, že je potřeba decentralizovat řízení komunikační sítě pro počítače a pro vyřešení tohoto problému si vybraly společnost DARPA (Defense Advanced Research Projects Agency), založena roku 1958, jež pro ministerstvo obrany vedla pokročilé výzkumné projekty a jejímž hlavním posláním bylo udržet technologický náskok ozbrojených sil USA [7]. Hlavním problémem bylo mimo jiné, jak vyřešit přenos datových paketů v případě zničení komunikačních uzlů, které by zcela určitě nepřestály jaderný útok. V roce 1962 vstoupila do hry společnost Reseach and Development tzv. RAND, která měla zabezpečit komunikaci počítačítačové sítě amerického letectva v době nukleární války. V roce 1964 přišel RAND s řešením. Každý komunikační uzel by byl postaven na stejnou úroveň s ostatními komunikačními uzly a s vlastní autoritou vytváření, předávání a přijímání datových zpráv. Datové zprávy by byly rozděleny do paketů a každému paketu by byla přiřazena nezávisle na sobě adresa. Datový paket by tak odešel z komunikačního uzlu s určenou adresou cílového komunikačního uzlu. Cestu k cíli by si tak datový paket v síti hledal sám, přes komunikační uzly, které by nebyly vyřazeny z provozu v důsledku jejich zničení [8].

Skutečným zárodkem internetu však byla až experimentální sít ARPANET (Advanced Research Projects Agency NETwork), která byla instalována za účelem propojení počítačů na vybraných univerzitách USA:

– University of California Los Angeles

– Stanford Central Research Institute

– University of California Santa Barbara

– University of Utah

ARPANET byl spuštěn v roce 1969 a do Evropy se ARPANET dostal po připojení k síti Norska a Velké Británie. Možnosti této sítě rostly hlavně v rámci elektronické komunikace. S příchodem roku 1983 se změnil komunikační potokol NCP (Network Control Program) na TCP/IP (Transmission Control Protocol/Internet Protocol) a ARPANET tak zastával pouze funkci páteřní přenosové sítě a i tu později přebrala NSFNET (National Foundation Network). Definitivní ukončení provozu sítě ARPANET nastalo 3/1990 [9].

4.1 Internetová síť alias internet

Ve světě existuje mnoho pokusů o stanovení definice toho, co je to internet. Zmíním dvě, které to ve své podstatě vystihují na několika málo řádcích zcela dostatečně:

a) *Internet je globální informační systém, který je logicky vzájemně propojen globálně jedinečnými adresami založenými na Internet Protokolu (IP) nebo jeho pozdějším rozšíření či modifikaci, tento systém podporuje komunikaci založenou na skupině protokolů Transmission control Protocol/Internet Protocol (TCP/IP) nebo jiných kompatibilních IP protokolů. Poskytuje, užívá nebo zpřístupňuje, veřejně nebo soukromně, vysokoúrovňové služby založené na komunikační a související infrastruktuře popsané shora [10].*

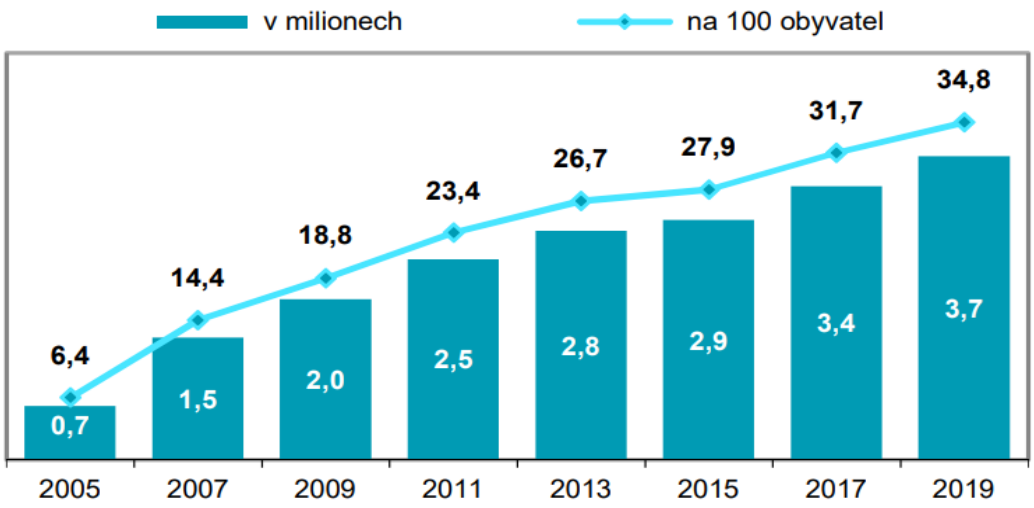
b) *„Globální systém propojených počítačových sítí, které používají standardní internetový protokol (TCP/IP). Internet slouží miliardám uživatelů po celém světě. Je to síť sítí, která se skládá z milionů soukromých, veřejných, akademických, obchodních a vládních sítí, s místním až globálním rozsahem, které jsou propojeny širokou škálou elektronických, bezdrátových a optických síťových technologií" [11, s. 49].*

Podoba internetové sítě, tak jak ji známe dnes, je dle některých pramenů informací přisuzována Vintu G. Cerfovi a Bobu Kahnovi. Ti jsou autory konceptu

podoby internetu dneška. Dave Clark je architektem internetu a Jon Postel se stal správcem síťových adres [12]. Vint Gray Cerf, Jon Postel a Steve Crockel v roce 1978 vytvořili TCP/IP protokol, což mělo zcela zásadní význam pro otevření sítě dalším uživatelům. *Protože software TCP/IP byl volně dostupný (public-domain) a základní technologie byla decentralizovaná, a ze své podstaty poněkud anarchistická, bylo obtížné zastavit lidi v invazi na síť sítí, ve skutečnosti neměl nikdo zájem bránit jim v připojování na rozšiřující se komplex sítí, který začal být všeobecně znám pod označením Internet [13].*

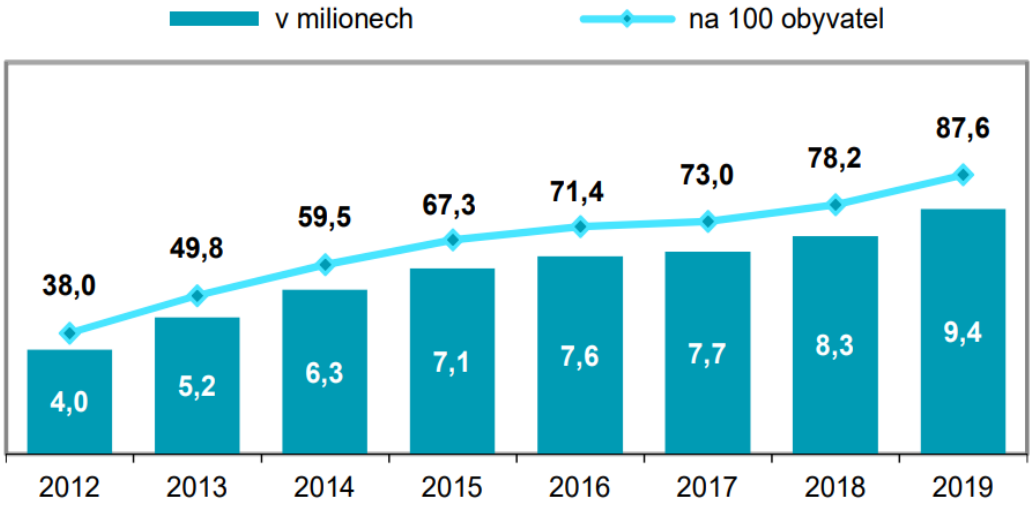
4.2 Druhy a rychlost připojení

Se skokovým nárůstem počtu uživatelů bylo samozřejmě nutné řešit i přenosovou rychlost sítě. Protože např. v roce 1985 bylo k internetu připojeno jen asi dva tisíce počítačů a o sedm let později, v roce 1992, to už bylo přes jeden milion počítačů. Tím samozřejmě dramaticky vzrostl požadavek na propustnost a rychlost přenosové soustavy. Přiložené grafy 1 a 2 ukazují nárůst počtu internetových přípojek v České republice. Z grafu 1 je patrné, že za období od roku 2005 do roku 2019 vzrostl počet pevných přípojek v ČR více než 5×. Přičemž je nutno vzít na vědomí i stoupající požadavek na mobilní připojení k internetu (viz graf 1), které se stává v poslední době téměř neodmyslitelnou součástí nabízených tarifů mobilních operátorů, kteří tak reagují na stoupající požadavky zákazníků, potažmo společnosti.



***Graf 1** – Počet přípojek pevného vysokorychlostního internetu v České republice [14]*

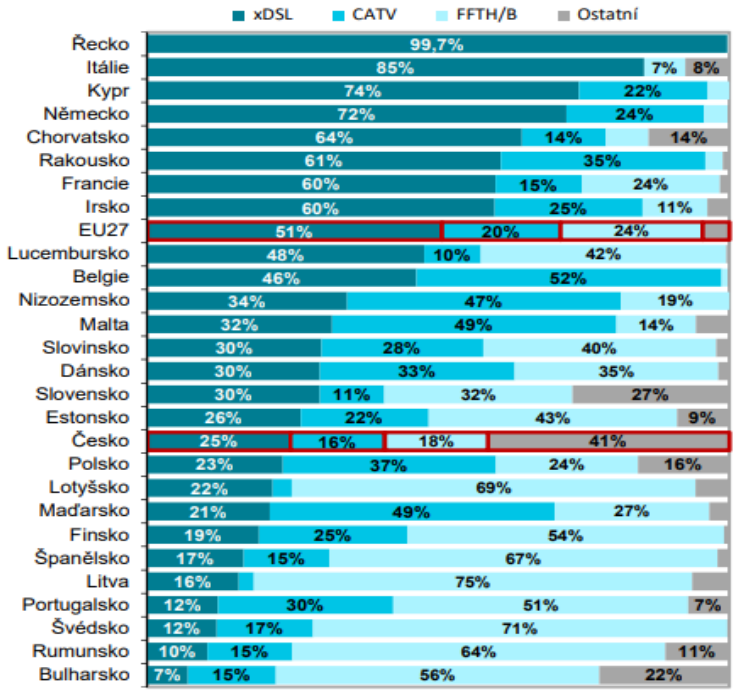
Se vzrůstající potřebou společnosti být neustále on-line a tedy ve spojení s rodinou, přáteli, klienty nebo např. s byznys partnery se změnila i preference použité technologie pro přístup k internetu. Přípojka pevného internetu tak přestávala uspokojovat tuto potřebu. Mobilní telefon už dávno neplní jen funkci telefonu, ale stal se nezbytnou součástí běžného života. Proto narůstá potřeba mobilního připojení k internetu (viz graf 2).



***Graf 2** – Počet přípojek mobilního internetu v České republice [15]*

4.3 Technologie připojení

Rozdíl v počátcích měření statistických dat mezi grafem 1 a 2 je pochopitelný, neboť v roce 2005 nebyla v České republice dostupná např. LTE (Long Term Evolution) technologie. Tato technologie opatrně nakráčela do České republiky až v roce 2012 prostřednictvím všech tří operátorů. S masovým technologickým vývojem a používáním mobilních telefonů se začalo měnit i složení preferovaných přístupových bodů k internetu dle typu (viz grafy 1 a 2). A dále s masovým využíváním digitálních masmédií, začaly stoupat nároky na přenosovou rychlost a objem přenášených dat. V závislosti na tom se mění i technologie připojení k internetu (viz graf 3), který ukazuje vývoj použitých technologií pro připojení k internetové síti v zemích EU (2019).

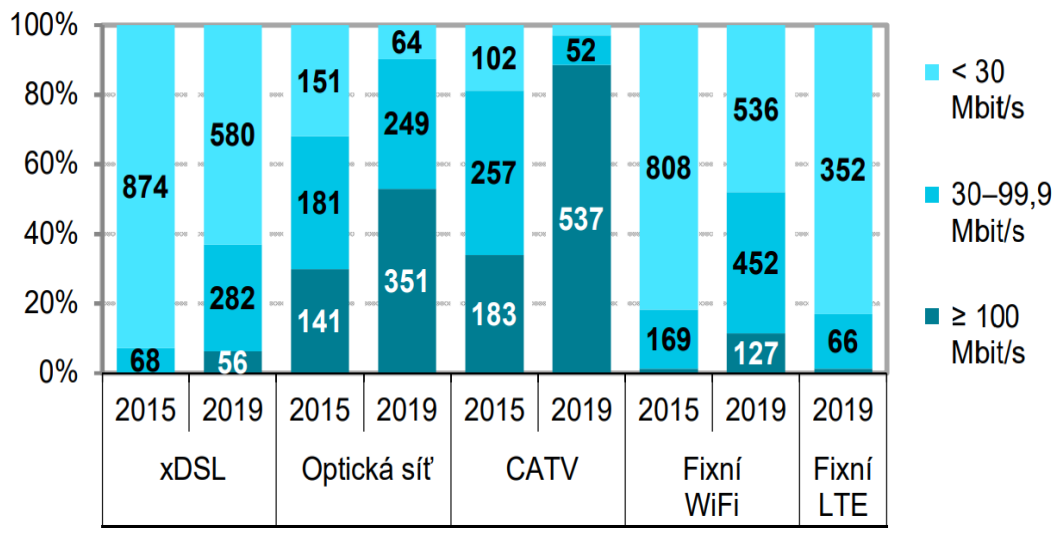


***Graf 3** – Pevný internet v zemích EU podle použité technologie [16]*

Telekomunikační infrastruktura je jedním z hlavních hledisek, podle kterého je hodnocena technologická vyspělost jednotlivých států nebo vzato globálně celého světa. Tzv. síť sítí se stala pro lidskou společnost nezbytnou součástí života a přinesla zvrat do mezilidské komunikace, meziliských vztahů, uvažování, kultury, vědy, politiky apod. [17]. Internet změnil způsob vyhledávání, předávání, uchovávání a nákládání s informacemi, a zároveň pochopitelně změnil i samotný způsob života společnosti.

Od internetu a přenosové infrastruktury očekáváme rychlý a bezpečný přenos obrovského množství dat nezbytných pro fungování celé společnosti, která je již existenčně závislá na internetu.

Tento požadavek může splnit jen správně dimenzovaná, moderní, spolehlivá komunikační a datová infrastruktura. Z grafu 4 je patrné, jak se zvyšuje požadavek na rychlost přenášených dat v síti.



***Graf 4** – Pevný internet podle technologických řešení a nabízené rychlosti [18]*

Souvisí to s potřebou společnosti přenášet stále objemnější pakety dat např. z důvodu změny způsobu komunikace, streamování videií, sledování TV a rovněž sledování zpravodajství via internet. Lidé chtějí komunikovat a sdílet své žážitky ihned prostřednictvím sítě a napříč kontinenty. K tomu je potřeba zajistit obrovskou průchodnost a rychlost sítě.

Dle Hillstroma *můžeme předpokládat, že implementace internetu do společnosti bude mít na ni stejný dopad, jako např. vynález knihtisku nebo parního stroje a svět se bude posouvat vpřed ve skocích stejně jako v období průmyslové revoluce [19].*

V současné době se společnost ve vyspělých zemích nachází na prahu průmyslové revoluce 4.0. Stroje a zařízení budou vybaveny mikročipy a pomocí vzdálené správy prostřednictvím internetu je bude možné kontrolovat, konfigurovat, diagnostikovat a opravovat řídící software. Kalkuluje se např. s tím, že automatizace výroby přinese finanční i časovou úsporu a zvýší se produktivita a efektivita výroby [20].

Neil Postman říká, že technika nás svými možnostmi svádí a ve chvíli, kdy se jí to povede, stáváme se na technice závislými. Fyzik Robert Oppenheimer zase zmínil, že vědci jsou hnáni touhou objevovat nové věci nebo postupy. Tento stav popsal slovy: *...když narazíte na něco technicky atraktivního, prostě se do toho pustíte, začnete se tím zabývat, a teprve když dosáhnete úspěchu, začnete diskutovat na téma co s tím dál, a tak to bylo i v případě atomové bomby [21].*

Cesta, kterou kráčíme v oboru umělé inteligence nebo autonomních systémů a systémů řízených nebo sledovaných počítačovými algoritmy, je jak se zdá, svádění technikou. V současném přetechnizovaném světě, je dobrovolné přenechávání samostatného rozhodování člověka na umělé inteligenci (angl. AI – Artificial Inteligence) hrozbou do budoucna. Ve společnosti je všeobecně zaužívaný názor, že technika nedělá chyby. Nedělá chyby v napsaném algoritmu, ale zatím nedovede správně a spontánně reagovat na nahodilé situace, ke kterým nenalezne algoritmus. Chybí ji schopnost cítit, je bez emocí. Právě tato chybějící schopnost je zatím pro ni limitem.

Zároveň se vždy jedná o "program", který napsal člověk a člověk má bohužel i tu schopnost, dobrovolně být sám sobě smrtelnou hrozbou. Tuto schopnost nenajdeme u žádného jiného živočišného druhu na této planetě. Vždy se najde individum či skupina individuí, kteří se z důvodu osobního prospěchu budou snažit nabourat do elektronických systémů různých společností či státních institucí. Ruku v ruce s technologickým pokrokem přicházejí i hrozby ze strany zneužití těchto těchnologií proti jednotlivci nebo společnosti. Společnost si je vědoma těchto hrozeb a proto se snaží budovat mechanizmy, které těmto hrozbám budou čelit. Česká republika si pro hlídání svého kyberprostoru ustanovila Národní úřad pro kybernetickou a informační bezpečnost, který má i zahraniční působnost v rámci předem dané spolupráce.

5 BEZPEČNOST KYBERPROSTORU V ČR

Hlavním řešitelem problematiky kybernetické bezpečnosti a autoritou v ČR v této oblasti byl v minulosti ustanoven Národní bezpečnostní úřad (dále jen NBÚ), a to na základě přijatého usnesení vlády České republiky č. 781 z 19. října 2011. S tímto usnesením zároveň vzniklo Národní centrum kybernetické bezpečnosti (dále jen NCKB) se sídlem v Brně, které se tak stalo součástí NBÚ. Ovšem s vydáním a účinností zákona č. 181/2014 Sb. zákon o kybernetické bezpečnosti vznikl zcela nový úřad a sice Národní úřad pro kybernetickou a informační bezpečnost (dále jen NÚKIB), který pod sebe přejal NCKB, jehož součástí je Vládní CERT (Computer Emergency Response Team). Tato definitivní právní úprava proběhla v roce 2017, zákonem č. 205/2017 Sb., kterým se změnil zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) dále jen ZoKB. Smyslem zákona je:

- sladit spolupráci mezi soukromým sektorem a veřejnou správou z důvodu zvýšení efektivity řešení kybernetických bezpečnostních incidentů,
- konstituovat oprávnění a povinnosti v dané oblasti s cílem zvýšit bezpečnost kybernetického prostoru,
- konstituce práv a povinností orgánu státu, jemuž je svěřena konkrétní pravomoc v oblasti zajišťování kybernetické bezpečnosti v souvislosti s právy a povinnostmi dalších orgánů státu,
- konstituce práv a povinností soukromoprávních subjektů, které v této oblasti participují.

ZoKB v § 3 ukládá povinnosti těmto subjektům:

a) poskytovatelé služby elektronických komunikací a subjekty zajišťující síť elektronických komunikací,
b) orgány nebo osoby zajišťující významnou síť,
c) správce informačního systému kritické informační infrastruktury,
d) správce komunikačního systému kritické informační infrastruktury,
e) správce významného informačního systému [22].

O přesné rozklíčování toho, jaké subjekty jsou tímto vymezením myšleny je nutné nahlédnout mimo ZoKB také do jiných právních norem. Můžeme zmínit vyhlášku

č. 82/2018 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (o kybernetické bezpečnosti).

Vyhláška č. 82/2018 Sb. vychází ze směrnice Evropského parlamentu a Rady EU 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii a pro informační systém kritické informační infrastruktury, komunikační systém kritické informační infrastruktury, významný informační systém, informační systém základní služby anebo informační systém nebo síť elektronických komunikací, které využívá poskytovatel digitálních služeb, (dále jen „informační a komunikační systém“) upravuje:

a) obsah a strukturu bezpečnostní dokumentace,
b) obsah a rozsah bezpečnostních opatření,
c) typy, kategorie a hodnocení významnosti kybernetických bezpečnostních incidentů,
d) náležitosti a způsob hlášení kybernetického bezpečnostního incidentu,
e) náležitosti oznámení o provedení reaktivního opatření a jeho výsledku,
f) vzor oznámení kontaktních údajů a jeho formu,
g) způsob likvidace dat, provozních údajů, informací a jejich kopií [23].

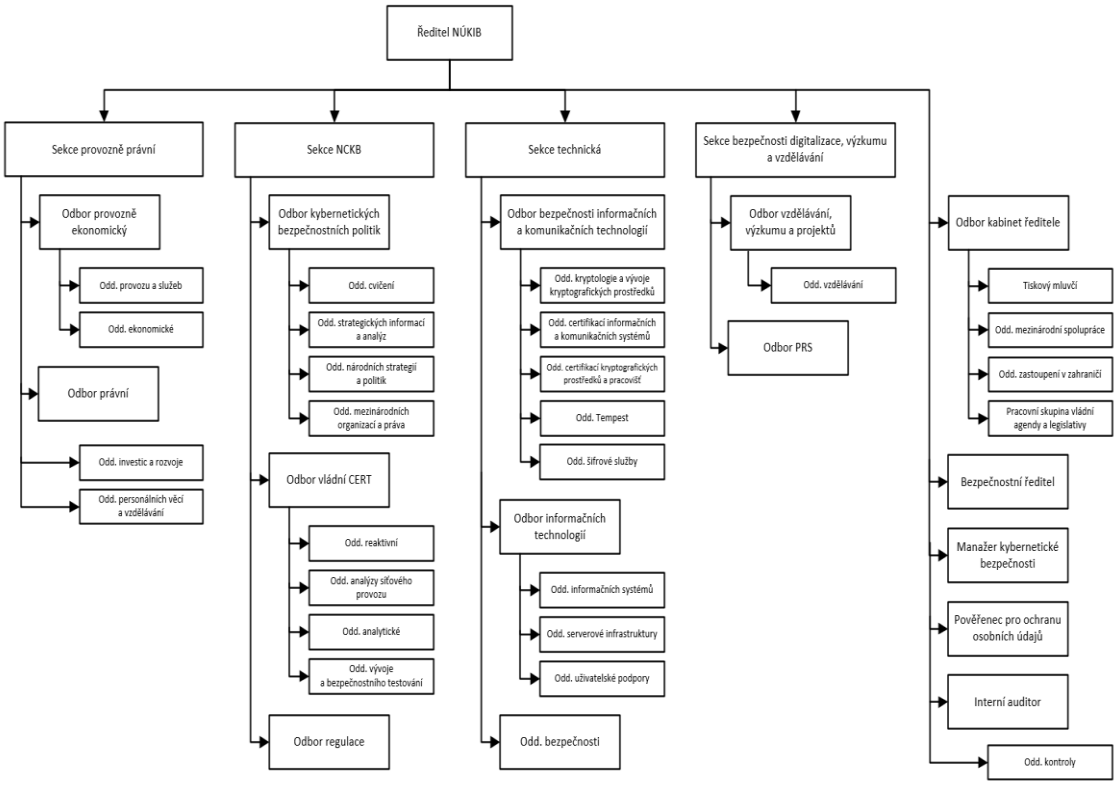
Další právní normy, které je možné vztáhnout ke kybernetické bezpečnosti potažmo k ZoKB jsou:

- zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), který upravuje podmínky podnikání, podmínky výkonu komunikační činnosti a výkon státní správy, včetně regulace trhu, v oblasti elektronických komunikací a upřesňuje subjekty působící v oblasti elektronické komunikace,
- vyhláška č. 315/2021 Sb. o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci, již z názvu právní normy můžeme dovodit, že pojednává o jednotlivých bezpečnostních úrovních (jsou 4 – nízká, střední, vysoká a kritická) pro využívání cloud computingu a zmiňuje možné dopady kybernetického bezpečnostního incidentu související s touto problematikou,
- vyhláška č. 317/2014 Sb. o významných informačních systémech a jejich určujících kritériích.

5.1 Národní úřad pro kybernetickou a informační bezpečnost – NÚKIB – struktura

V čele Národního úřadu pro kybernetickou a informační bezpečnost (dále jen NÚKIB) stojí ředitel, kterého jmenuje po projednání ve výboru Poslanecké sněmovny příslušném ve věcech bezpečnosti vláda, která ho též odvolává. Ředitel NÚKIB, je odpovědný předsedovi vlády nebo pověřenému členovi vlády [24]. Financování NÚKIB je řešeno samostatnou kapitolou státního rozpočtu.

Tento úřad je rozčleněn do 4 sekcí a 10 odborů. NÚKIB pod sebe rovněž přejal sekci NCKB, pod kterou patří vládní bezpečnostní tým, tzv. Vládní CERT České republiky (zkr. GovCERT.CZ). Dále tak spolupracuje s ostatními CERT a CSIRT bezpečnostními týmy v ČR, ale i ve světě. NÚKIB se podílí na přípravě národních bezpečnostních standardů v oblasti kyber bezpečnosti a stanovuje bezpečnostní standardy pro informační systémy, pro tzv. kritickou informační infrastrukturu, která je důležitá pro chod České republiky. Dále zastává funkci tzv. "příslušného orgánu PRS" (anglicky Competent Public Regulated Service Authority), jehož hlavním úkolem je implementace služby PRS (Public Regulated Service) navigačního systému Galileo v ČR (Veřejná regulovaná služba programu Galileo). Vytváří a v mezinárodním přesahu hájí pozice ČR v oblasti kybernetické bezpečnosti. Dále vytyčuje národní strategie kybernetické bezpečnosti a připravuje zákony a podzákonné normy v oblasti kybernetické bezpečnosti. Provádí vlastní výzkum a vývoj pro kybernetickou a informační bezpečnost ČR [25].



***Obrázek 1** – Organizační struktura NÚKIB [26]*

5.2 Národní úřad pro kybernetickou a informační bezpečnost – NÚKIB – úkoly

NÚKIB má celou řadu úkolů, které musí plnit, aby byla zajištěna bezpečnost kyberprostoru České republiky. Těmito úkoly jsou:

a) stanoví bezpečnostní opatření,

b) vydává opatření,

c) plní stanovené úkoly ve vybraných oblastech ochrany utajovaných informací,

d) vede evidence podle tohoto zákona a podle zákona o ochraně utajovaných informací,

e) ukládá správní tresty za nedodržení povinností stanovených tímto zákonem a zákonem o ochraně utajovaných informací a o bezpečnostní způsobilosti,

f) působí jako koordinační orgán ve stavu kybernetického nebezpečí,

g) spolupracuje s orgány a osobami, které působí v oblasti kybernetické bezpečnosti a kybernetické obrany, zejména s veřejnoprávními korporacemi, výzkumnými a vývojovými pracovišti a s ostatními pracovišti typu CERT a s orgány a osobami, které působí ve vybraných oblastech ochrany utajovaných informací,

h) zajišťuje mezinárodní spolupráci v oblasti kybernetické bezpečnosti a ve vybraných oblastech ochrany utajovaných informací,

i) sjednává a uzavírá smlouvy o mezinárodní spolupráci v oblasti kybernetické bezpečnosti a ve vybraných oblastech ochrany utajovaných informací,

j) zajišťuje prevenci, vzdělávání a metodickou podporu v oblasti kybernetické bezpečnosti a ve vybraných oblastech ochrany utajovaných informací,

k) zajišťuje výzkum a vývoj v oblasti kybernetické bezpečnosti a ve vybraných oblastech ochrany utajovaných informací,

l) uzavírá veřejnoprávní smlouvu s provozovatelem národního CERT,

m) zasílá podle krizového zákona Ministerstvu vnitra návrh prvků kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti, jejichž provozovatelem je organizační složka státu,

n) určuje podle krizového zákona prvky kritické infrastruktury v odvětví komunikačních a informačních systémů v oblasti kybernetické bezpečnosti, pokud nejde o prvky uvedené v písmenu m),

o) ověřuje každé 2 roky aktuálnost určení prvků kritické infrastruktury podle písmen m) a n),

p) určuje provozovatele základní služby a informační systém základní služby,

q) zpracovává a vládě ke schválení předkládá národní strategii kybernetické bezpečnosti a akční plán k jejímu naplňování a tuto strategii aktualizuje nejméně každých 5 let,

r) je jednotným kontaktním místem pro zajištění přeshraniční spolupráce v oblasti kybernetické bezpečnosti v rámci Evropské unie,

s) je příslušným orgánem v České republice a plní informační povinnosti vůči Evropské komisi a skupině pro spolupráci podle příslušného předpisu Evropské unie,

t) informuje veřejnost o kybernetickém bezpečnostním incidentu podle § 12 odst. 3,

u) provádí analýzu a monitoring kybernetických hrozeb a rizik,

v) vykonává působnost v oblasti veřejné regulované služby Evropského programu družicové navigace Galileo,

w) vydává Věstník Úřadu, který zveřejňuje na svých internetových stránkách,

x) plní další úkoly v oblasti kybernetické bezpečnosti stanovené tímto zákonem a ve vybraných oblastech ochrany utajovaných informací podle zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti [27].

5.3 Národní centrum kybernetické bezpečnosti – NCKB

Národní centrum kybernetické bezpečnosti (dále jen NCKB) je **výkonnou sekcí** Národního úřadu pro kybernetickou a informační bezpečnost. NCKB zejména zajišťuje:

a) činnost Vládního CERT České republiky,

b) prevenci před kybernetickými hrozbami proti:

- prvkům kritické informační infrastruktury,
- informačním systémům základní služby,
- významným informačním systémům a vybraným informačním systémům veřejné správy,

c) řešení a koordinaci kybernetických bezpečnostních incidentů u subjektů kritické infrastruktury, provozovatelů základní služby a orgánů veřejné správy,
e) spolupráci s národními i mezinárodními organizacemi podílejícími se na zajišťování bezpečnosti kybernetického prostoru,
f) vyhodnocování rizik v oblasti kybernetické bezpečnosti a přijímaní příslušných nápravných a preventivních opatření,
g) komunikační strategii NÚKIB v oblasti kybernetické bezpečnosti ve spolupráci s ostatními organizačními celky NÚKIB,
h) výzkum a vývoj v oblasti kybernetické bezpečnosti,
i) zastupování České republiky v orgánech mezinárodních organizací působících v oblasti kybernetické bezpečnosti,
j) plnění mezinárodních závazků a spolupráci na mezinárodní úrovni při realizaci předpisů vyplývajících z členství České republiky v NATO a členství v EU a členství v jiných mezinárodních organizacích [28].

5.4 Computer Emergency Response Team – CERT (GOVCERT.CZ a CSIRT.CZ)

Mezi vrcholná dohledová centra pro Českou republiku v rámci dohledu na bezpečnost našeho kyberprostoru jsou stanovena dvě hlavní centra, jejichž úlohou je zároveň působit jako prvotní zdroj bezpečnostních informací a pomoci pro orgány státu, organizace, ale i občany. Rovněž se podílejí na zvyšování vzdělanosti v oblasti bezpečnosti na internetu a na tvorbě bezpečnostních standardů. Těmito centry jsou:

a) **Vládní CERT** (GOVCERT.CZ) – provozován pod NCKB – **<u>státní instituce:</u>**

- zastává zásadní roli při ochraně *kritické informační infrastruktury* a významných *informačních systémů* dle zákona č. 181/2014 Sb. ZoKB a o změně souvisejících zákonů, přijímá údaje od provozovatele národního CERT a tyto údaje vyhodnocuje,

- spolupracuje zejména s bezpečnostními složkami a úřady státní správy, vyhodnocuje údaje o kybernetických bezpečnostních událostech a kybernetických bezpečnostních incidentech z kritické informační infrastruktury, informačního systému základní služby, významných informačních systémů a dalších informačních systémů veřejné správy,

- poskytuje podle § 9 odst. 4 zák. č. 181/2014 Sb. provozovateli národního CERT, orgánům vykonávajícím působnost v oblasti kybernetické bezpečnosti v zahraničí a jiným osobám působícím v oblasti kybernetické bezpečnosti, údaje z evidence incidentů, plní roli týmu CSIRT (Computer Security Incident Response Team) podle příslušného předpisu Evropské unie a spolupracuje s týmy CSIRT jiných členských států.

- všechny země, které mají své kritické systémy připojeny do internetu, musí být schopny rychle, efektivně a účinně čelit bezpečnostním hrozbám a incidentům a reagovat na ně, spolupracovat na mezinárodní úrovni a koordinovat činnosti při řešení těchto událostí a účelně jim předcházet.

Do působnosti Vládního CERT spadají orgány a osoby, na které se vztahuje zákon o kybernetické bezpečnosti a jsou uvedeny v **§ 3 písm. c) až g)**, od kterých zároveň přijímá oznámení kontaktních údajů a hlášení o kybernetických bezpečnostních

incidentech a tyto údaje eviduje, uchovává, vyhodnocuje a informuje o nich NÚKIB [29].

b) **Národní CERT** (CSIRT.CZ) – **<u>právnická osoba soukromého práva:</u>**

- je provozován sdružením CZ.NIC na základě uzavřené veřejnoprávní smlouvy a zákona č. 181/2014 Sb. Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů, jehož působnost je v rámci celé České republiky, tzn. uživatelé a sítě nacházející se v České republice, ale které svým charakterem nespadají pod Vládní CERT,
- udržuje zahraniční vztahy s ostatními tými CERT/CSIRT a dalšími organizacemi, které s těmito týmy spolupracují, spolupracuje s dalšími subjekty v rámci ČR, poskytovateli obsahu, bankami, akademickým sektorem apod.,
- poskytuje proaktivní služby v oblasti řešení a koordinace bezpečnostních incidentů a v oblasti osvětové a školící činnosti,
- národní CERT nebo-li CSIRT.CZ je členem mezinárodních uskupení CSIRT/CERT týmů a od roku 2011 je akreditovaný u Trusted Introducer a od roku 2015 je rovněž členem organizace FIRST.

Do působnosti Národního CERT spadají orgány a osoby, na které se vztahuje zákon o kybernetické bezpečnosti, a jsou uvedeny v **§ 3 písm. a) a b)**, od kterých zároveň přijímá oznámení kontaktních údajů a hlášení o kybernetických bezpečnostních incidentech, tyto údaje eviduje, uchovává, vyhodnocuje a informuje o nich Vládní CERT [30].

	2018	2019	2020	2021
Sensor Network*	18 435	14 911	16 217	10 284
Phishing	518	483	738	1 281
Spam	144	128	216	165
Malware	135	85	109	141
Other	58	85	86	54
Probe	171	141	68	66
Trojan	0	0	0	0
DOS	7	16	16	11
Botnet	20	4	2	1
Virus	0	0	0	0
Portscan	16	3	29	7
Pharming	10	9	3	0
Celkem	**1 079**	**954**	**1 267**	**1 726**

* Sensor Network není započten do celkového počtu

***Obrázek 2** – Statistika bezpečnostních incidentů řešených týmem CSIRT [31]*

5.5 Computer Incident Response Capability – Centrum CIRC

Ministerstvo obrany si svůj kyberprostor hlídá speciálním útvarem Computer Incident Response Capability, tzv. Centrem CIRC (dále jen CIRC). Tento prvek je organizačně začleněn pod Agenturu komunikačních a informačních systémů tzv. AKIS. Působnost CIRC je v rámci celého rezortu MO.

Hlavním úkolem CIRC je identifikace bezpečnostních hrozeb a incidentů nepřetržitým monitoringem důležitých segmentů datových sítí resortu Ministerstva obrany (dále jen MO). CIRC analyzuje a následně vyhodnocuje bezpečnostní hrozby a incidenty. O výsledcích informuje oprávněné partnery.

Z důvodu rychlé reakce na bezpečnostní hrozby, CIRC připravuje protiopatření, opravné postupy a nástroje a šíří povědomí o bezpečnosti mezi uživateli a správci informačních a komunikačních systémů. Zaměřuje se na ochranu informací a dat, která jsou uložena v informačních systémech a dále se zabývá ochranou technických prostředků pro velení a řízení resortu MO. Zabezpečuje a provádí nasazení, provoz, správu a údržbu bezpečnostních technologií CIRC [32].

Úzce spolupracuje s odbornými orgány při šetření počítačových bezpečnostních incidentů a jejich původců, zejména pak s Ministerstvem vnitra a Národním úřadem pro kybernetickou a informační bezpečnost a v rámci NATO např. s NCI Agency Cyber Security. Ta je odpovědná za celou oblast činností kybernetické bezpečnosti NATO, a to zejména při navrhování, implementaci a provozu informačních a komunikačních systémů, technickou podporu a údržbu, jejich stálou kontrolu a monitoring bezpečnostních incidentů v rozsahu 24/7/365. Dále má na starosti získávání a předávání vědeckých a technických znalostí a jejich využití v oblasti prevence [33].

5.6 Národní agentura pro komunikační a informační technologie – NAKIT

Národní agentura pro komunikační a informační technologie (dále jen NAKIT) byla založena 1. února 2016 jako servisní organizace Ministerstva vnitra České republiky a zároveň je i strategickým partnerem státu zajišťující komunikační a informační služby pro záchranné a bezpečnostní složky a veřejnou správu. Ke své činnosti využívá více než 40 regionálních pracovišť.

Statut agentury vymezuje široký rozsah činností a předurčuje NAKIT k vybudování nových kompetencí umožňujících např. informační a komunikační technologie nejen provozovat a udržovat, ale zároveň je dlouhodobě rozvíjet v souladu s potřebami jejich uživatelů. Zajišťuje koncepční rozvoj kritické komunikační infrastruktury a bezpečné řešení sdílených služeb státu a dohlíží na bezpečnost digitálních služeb a komunikací. V dané oblasti spolupracuje s nejvyššími autoritami a bezpečnostními týmy na kybernetickou bezpečnost v České republice [34].

6 INTERNETOVÁ KRIMINALITA

Kyberprostor nabízí možnosti jak zůstat do značné míry nebo zcela anonymní, ovšem pouze za určitých okolností s využitím speciálního sofwaru a hardwaru a s tím souvisí i nemalá rizika. Přes jeho jednoznačná pozitiva, bohužel zároveň vytváří podhoubí pro rychle se rozvíjející kyberkriminalitu, která je páchána **pouze** v kyberprostoru prostřednictvím internetové sítě. Samotná internetová síť tak představuje **způsob páchání** takového trestného činu, nebo se jedná o takovou trestnou činnost, u které je internetová síť, potažmo samotný kyberprostor, objektem pachatelova útoku.

Internetová kriminalita je tak chápána jako poddruh počítačové kriminality. *Internetová kriminalita je součástí počítačové kriminality, protože trestná činnost páchaná v prostředí internetu se děje výlučně prostřednictvím výpočetní techniky nebo je přímo výpočetní technika cílem trestné činnosti. Ale ne všechna kriminalita spáchaná výpočetní technikou je spáchána na internetu nebo jeho prostřednictvím [35].* Z této definice se dá dovodit, že každý trestný čin spáchaný v internetové síti, je možno označit jako poddruh počítačové kriminality, obráceně to však nelze, protože např. krádež dat z notebooku v kanceláři bude označována na základě některých definic stále jako počítačová kriminalita. **Internetová kriminalita** se *„…od **počítačové kriminality** odlišuje zejména tím, že vyjma počítače jako objektu útoku nebo nástroje pro spáchání trestného činu, vyžaduje propojení počítačů lokálními i vzdálenými sítěmi a následně využití internetu [36].*

6.1 Kybernetická kriminalita

Internetovou trestnou činnost spojuje **fakultativní znak** objektivní stránky skutkové podstaty trestného činu, a sice **způsob spáchání** trestného činu. Způsobem rozumíme **využití internetové sítě** nebo **jiných veřejně přístupných počítačových sítí** [37]. Někteří autoři považují kyberkriminalitu a počítačovou kriminalitu za **synonymum**. Jiného názoru je však P. Šámal a kol. který uvádí, že *o synonymum se však nejedná, protože kybernetická kriminalita se odvozuje nikoliv od pojmu kybernetika, ale od pojmu kybernetický prostor [38].* Pojem kyberkriminality, který je v širší právní rozpravě příjímán je definován takto: *„Kybernetickým trestným činem je:*

a) trestný čin ohrožující ICT – informační a síťovou bezpečnost (trestný čin proti počítačové integritě nebo také trestný čin v úzkém pojetí),

b) trestný čin využívající ICT ke spáchání tradičních trestných činů (trestný čin vztahující se k počítačům),

c) trestný čin vztahující se k obsahu, jako například dětská pornografie, pomluva a porušení práv k duševnímu vlastnictví (trestný čin vztahující se k obsahu počítačových dat)" [39, s. 15].

International Criminal Police Organization (tzv. INTERPOL) je mezinárodní organizace, která zabezpečuje spolupráci na kriminálně-policejní úrovni a ta člení kyberkriminalitu do následujících skupin:

- útoky proti počítačovému hardwaru a softwaru (např. malware),
- finanční trestné činy (např. online podvody, phishing),
- zneužívání a vykořisťování (např. cybergrooming) [40].

6.2 Počítačová kriminalita

Optikou **kriminalistiky** vidíme počítačovou kriminalitu jako *skupinu trestných činů páchaných prostředky výpočetní techniky v podmínkách komunikačních sítí, systémů, programového vybavení anebo databází výpočetní techniky [41].*

Policie České republiky chápe pojem počítačové kriminality jako trestnou činnost *"...v níž figuruje určitým způsobem počítač, jako souhrn technického a programového vybavení (včetně dat), nebo pouze některá z jeho komponent, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď jako předmět zájmu této trestné činnosti (s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako věci movité) nebo jako prostředí (objekt) nebo jako nástroj trestné činnosti. Často se pojem počítačová kriminalita používá i pro tradiční formy kriminality, u níž byly počítače nebo počítačové sítě použity, aby ji usnadnily. Určujícím operacionálním elementem je přitom vždy způsob zneužití výpočetní techniky, vzhledem k jejím specifickým vlastnostem a dominantnímu postavení mezi věcnými komponentami způsobu páchání konkrétního trestného činu" [42, s. 1].*

Pojmem počítačové kriminality se na mezinárodní úrovni zabývali odborníci z komise pro zločin v kyberprostoru, která je organizačně začleněná pod Radou Evropy a ta ustanovila pojem počítačové kriminality v roce 2000 jako: *„Trestný čin namířený proti integritě, dostupnosti nebo utajení počítačových systémů nebo trestný čin v tradičním slova smyslu, při kterém je použito moderních informačních a komunikačních technologií“ [43, s. 33].*

Rovněž **Organizace spojených národů** v dokumentu „Manuál pro prevenci a kontrolu počítačového zločinu“ ustanovila pojem počítačové kriminality v tomto znění: *„Počítačovou kriminalitu představují jednak tradiční zločinecké aktivity jako krádež, podvod nebo padělání, tedy činy, které jsou trestné ve většině zemí světa. K tomu se přidružují nové způsoby zneužití počítačů, které jsou, nebo by měly být trestnými“ [44, s. 4–5].*

Autor několika publikací **J. Kuchta** vnímá počítačovou kriminalitu jako: “*...trestná jednání, jejichž společným jmenovatelem je, že v nich vystupuje počítač jako souhrn hardwarového a softwarového vybavení a dat, a to buď jako předmět útoku nebo jako nástroj pachatele“[45, s. 603].* Dále pak tento autor počítačovou kriminalitu dělí do 6 skupin:

- krádež počítače, programu, dat, komunikačního zařízení,
- neoprávněné užívání počítače nebo komunikačního zařízení,
- neoprávněný přístup k datům, získání utajovaných nebo jiných informací,
- neoprávněná změna v programech a datech,
- útoky na počítače, programy, data, komunikační zařízení,
- zneužívání počítačových prostředků k páchání jiné trestné činnosti [46].

Výše zmiňovaná kriminalita se samozřejmě liší od klasické kriminality páchané v reálném světě a to několika znaky, které uvádí J. Kuchta. Jedná se zejména o následující výčet:

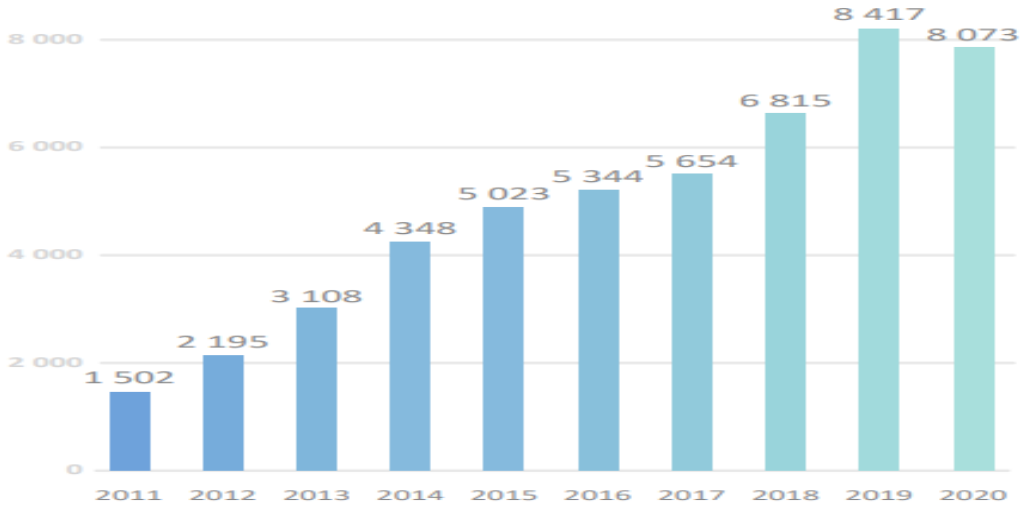
- značně vysoká míra diskrétnosti a latence,
- motivy i cíle pachatelů mohou být zištné, ale i dosud netradiční (ochrana nezávislosti kyberprostoru),
- je páchána intelektuálně vyspělými, teoreticky i prakticky vzdělanými pachateli,

- způsoby odhalování, dokazování a dokumentování jsou značně složité,
- často má mezinárodní charakter,
- dá se předpokládat značný podíl organizovanosti pachatelů.
- pro boj s ní doposud neexistuje dostatek právních, režimových a organizačních prostředků,
- do budoucna se dá očekávat její rozvoj vzhledem k přibývajícímu počtu počítačů, uživatelů internetu apod.,
- jejím následkem vznikají značné škody, které na jedné straně lze obtížně kvantifikovat, ale na druhé straně mohou mít až katastrofický rozměr,
- prevence je více záležitostí příslušných vlastníků informačních a komunikačních systémů a poškozených než orgánů činných v trestním řízení [47].

7 KRIMINALITA PÁCHANÁ NA INTERNETU

Nejčastějšími trestnými činy, které jsou páchány v kyberprostoru jsou:

- porušení práva na ochranu osobnosti,
- trestné činy proti lidské důstojnosti v sexuální oblasti,
- trestné činy proti rodině a dětem,
- trestné činy proti majetku apod.



***Graf 5** – Nápad trestné činnosti – kybernetická kriminalita [48]*

V celkovém nápadu trestné činnosti v prostředí internetu byly nejčastěji zastoupené různé formy podvodného jednání, nicméně v porovnávaném období byl pozorován vzrůstající trend u trestných činů v oblasti hackingu. Namátkou zde uvádím statistiku množiny trestných činů spojovaných s **hackingem**: § 230 Neoprávněný přístup k počítačovému systému a nosiči informací, § 231 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat a § 232 Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti.

2021 – počet spáchaných TČ 1 866, objasněno 158, tj. 8,5 %,
2020 – počet spáchaných TČ 1 287, objasněno 155, tj. 12 %,
2019 – počet spáchaných TČ 1 092, objasněno 208, tj. 19,1 %,
2018 – počet spáchaných TČ 893, objasněno 231, tj. 25,9 %,
2017 – počet spáchaných TČ 76, objasněno 6, tj. 7,9 % [49].
Za období 5ti let se jedná o nárůst o neuvěřitelných 2 455 %!

Výše znatelný vzestup můžeme přisuzovat tomu, že se aktivity člověka stěhují z reality do abstraktního světa "nul a jedniček". Minimálně v poslední dekádě byl lidský svět výrazně poznamenán a změněn, snad v každém ohledu, v důsledku rozvoje ICT prostředků a kyberprostoru.

S výrazným technologickým rozvojem miniaturizace a ICT prostředků a stejně tak i s překotným rozvojem internetu, výrazně stoupá riziko hackerských útoků (viz statistika výše), které mimo jiné způsobují i značné finanční ztráty.

7.1 Druhy počítačových útoků

Počítačový útok můžeme charakterizovat jako soustavu **5 kroků**, které na sebe navazují:

- **footprinting** (jedná se o modelování a mapování kompletního profilu cíle pachatele a sběr informací o něm),
- **scanning** (zjišťování technických parametrů koncových systémů),
- **enumeration** (hledání mezer ve zjištěných technických parametrech systémů),
- **využití nalezených mezer** k provedení samotného útoku,
- **zahlazení stop**.

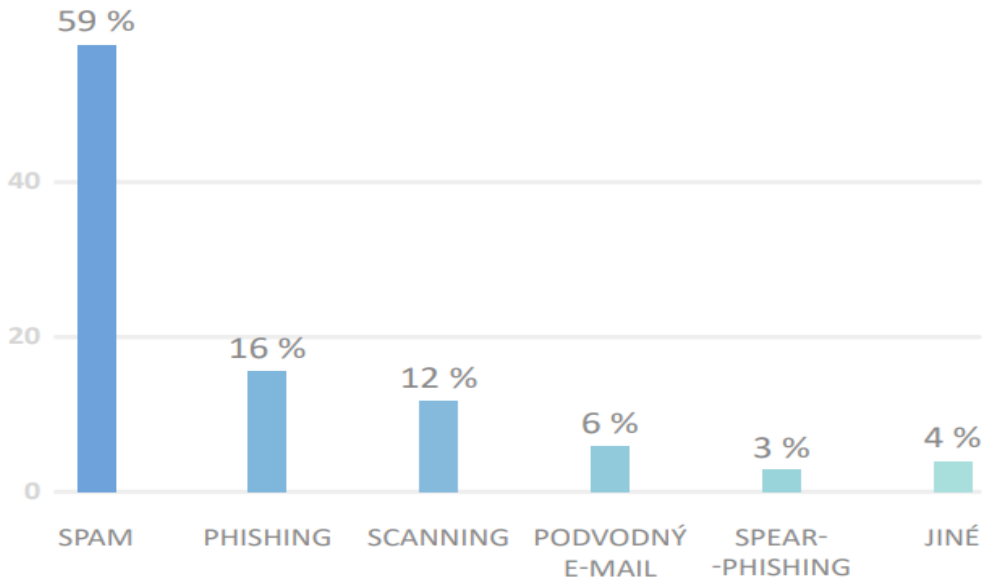
V případě, že se zaměříme na technický způsob provedení kybernetického útoku, tak můžeme mluvit o dvou základních fázích:

a) **automatizovaná** – v této fázi útočník pomocí "robotů" (např. vytvořeným malware) vyhledává potencionální cíle nebo automatizovaně skenuje již předem vybrané cíle za účelem získat konkrétní informace o uživateli (hesla, osobní údaje, chování na internetu apod.)

b) manuální – v této fázi už útočník sám zneužívá nelegálně získané informace o oběti nebo mezer v použitých technologiích a systémech za účelem získání přístupu k datům, svůj útok poté eskaluje tak, aby dosáhl svého cíle [50].

Začneme-li se zabývat konkrétními druhy kybernetických útoků, možná každého napadne **hacking/cracking**. Jedná se o neoprávněný průnik do konkrétního informačního systému, provedený z vnějšku. Můžeme zmínit i tzv. **defacement**, který

představuje průnik do webových serverů oběti a nahrazení jeho internetových stránek obsahem, který byl vytvořen útočníkem [51]. Široké veřejnosti je dobře znám spam. Nejčastěji se jedná o druh počítačového útoku ve formě nevyžádaného e-mailu (ve spojení s reklamou), ale postupným vývojem, tento fenomén postihl i ostatní druhy elektronické komunikace, např. diskuzní fóra, komentáře nebo instant messaging. I podle NÚKIB patří spam k nejčastějšímu typu kybernetického útoku (viz graf 6).



Graf 6 *– Nejčastější typy kybernetických útoků v roce 2020 (% respondentů) [52]*

7.2. Spam

Spam je nevyžádaná reklamní pošta, nebo jiné nevyžádané sdělení, masově šířené internetem. **Spam** můžeme rozdělit na:

a) **scam 419** (nigerijské dopisy) – jedná se o specifický druh podvodu, kdy se podvodník snaží vylákat ze své oběti peníze pod různorodými záminkami, veškerá komunikace probíhá pouze na dálku přes dopisy nebo e-maily a k přímému kontaktu mezi podvodníkem a obětí vůbec nedojde, často je zneužita vytipovaná osoba (bílý kůň – mules), např. pro výběr, předání nebo převod finančních prostředků.

b) **phishing** – jeho zdokonalenou formou je **spear pharming** nebo **SMShing** – jedná se o podvodnou techniku tzv. sociálního inženýrství používanou k získání citlivých údajů v elektronické komunikaci. Cílem je získat přihlašovací jména, hesla, čísla kreditních

karet apod. Nebo se jedná o činnost usilující o krádež digitální identity apod. Vzhledem k aktuálnosti problematiky phishingu je této problematice věnována samostatná kapitola 7.4. [53]

c) **malware** – souhrnný pojem pro jakýkoliv software, který při svém spuštění zahájí činnost ke škodě systému, ve kterém se nachází. Malware můžeme rozdělit na:

- **ransomware** – software, který blokuje počítačový systém nebo šifruje data zapsaná na pevném disku, za zpřístupnění je vyžadováno výkupné, příkladem lze uvést:
    - krypto–malware – šifruje soubory, s počítačem se může i nadále pracovat, avšak soubory jsou již zašifrované (ransomware **WannaCry**),
    - doxware – přenáší vaše citlivé soubory do útočníkova počítače a útočník poté požaduje výkupné za nezveřejnění ukradených dat (ransomware **Ransoc**),
    - scareware – oznamuje, že ve vašem počítači nalezl problémy a za jejich opravu požaduje peníze, může vaši obrazovku zaplavit vyskakovacími okny či výstrahami nebo vám dokonce může uzamknout počítač, dokud nezaplatíte výkupné (ransomware **SystemSecurity**) [54].
- **adware** – cílem je doručení reklamního sdělení i proti vůli uživatele systému (prostřednictvím instalačního balíčku),
- **spyware** – skrytě monitoruje chování uživatele počítače nebo systému a provedená zjištění průběžně zasílá subjektu, který program vytvořil, respektive za tím účelem distribuoval,
- **trojský kůň** – software implantovaný do systému bez vědomí oprávněného uživatele, monitorující specifické činnosti, o které útočník projevil zájem, software zaznamenává např. znaky, které uživatel stiskl na klávesnici nebo stránky, které navštívil a tyto údaje předává útočníkovi k dalšímu zpracování,
- **worm** – samostatně fungující software, vytvářející své identické klony, které rozesílá do dalších počítacových systémů, dodržuje naprogramovanou činnost a slouží převážně k hledání bezpečnostních skulin v systémech,

- **redial-software** – přesměruje uživatele na určité stránky namísto těch, které původně chtěl navštívit a na takových stránkách dochází k instalaci dalšího crimeware (viru),
- **logical bombs** – software, který se tajně vkládá do aplikací nebo do operačního systému, kde za předem určených podmínek (např. přesné datum a hodina) spustí destruktivní aktivity (logickou bombu) [55],
- **PC viry** – software, který se dokáže množit a šířit sám bez vědomí uživatele, ale je zavislý na přenosu hostitelem (např. z PC do PC), množením se rozumí proces, kterým se virus vkládá do jiných spustitelných souborů či dokumentů, software/vir se chová podobně jako biologický virus, který se šíří vkládáním svého kódu DNA do živých buněk, a proto se analogicky někdy takovému procesu šíření viru říká nákaza/infekce a napadenému souboru hostitel [56].

Zdánlivě neškodný spam v podobě různých reklam, může při špatně nastaveném zabezpečení systému a e-mailového účtu (spam filtru), tvořit dle odhadu až polovinu elektronické komunikace a tím neúměrně zatěžuje servery pro elektronickou poštu a způsobuje pokles jejich výkonnosti. Malware se může šířit nejen e-mailem, ale jako carrier může sloužit i URL adresa nebo instalační softwarový balíček.

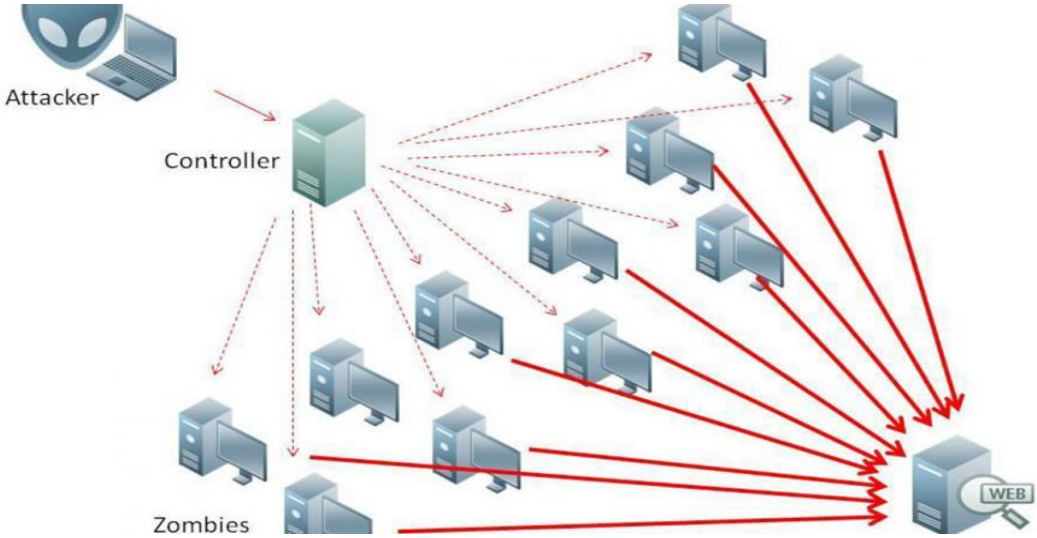
7.3 DoS a DDoS útoky

Dalším nebezpečným kybernetickým útokem, který dokáže oběti napáchat velké finanční škody nebo dokonce znemožnit činnost, jsou útoky typu DoS (Denial of Service) nebo DDoS (Distributed Denial of Service). Princip útoku je poměrně jednoduchý, přičemž cílem je *jednotlivá připojená zařízení nebo celou síť udělat nedostupnými pro právoplatného uživatele [57]*. Datové pakety jsou vysílané na cílový informační a komunikační systém v enormním množství, které tento systém není schopen zpracovávat. DoS/DDoS směřuje k vyčerpání síťové kapacity (bandwidth), nebo k max. vytížení CPU (Central Processing Unit) či RAM (Random–Access–Memory) apod., v důsledku toho dojde k přehlcení systému a jeho následné nefunkčnosti. Pokud vysílá pakety jeden zdroj, mluvíme o DoS útoku, pokud je k vysílání datových paketů použito více zdrojů (za pomoci více PC v síti tzv. botnetu), mluvíme o DDoS útoku. DoS/DDoS útoky necílí jen na web servery, ale i na

směrovače, firewally, IPS a rovněž na aplikační prostředky, např. protokol HTTP (Hypertext Transfer Protocol), HTTPS (HTTP Secure), DNS (Domain Name System), SMTP (Simple Mail Transfer Protocol) apod. Útoky jsou cíleny na slabá místa spuštěných služeb v aplikační vrstvě modelu TCP/IP [58]. DoS útoky lze rozdělit dle jejich intenzity:

a) **záplavové** – **"floods"** – zahlcení cíle obrovským množstvím specifickými požadavky na přenos paketů za sekundu (pps) nebo objemem datového toku (Mbps)

b) **pomalé** – **"low and slow"** – předmětem útoku jsou slabiny komunikačního protokolu TCP, jehož prostřednictvím útočník naváže komunikaci s obětí útoku a tento útok se pak tváří jako legální provoz, což je velice těžké odhalit a následně se mu bránit [59].



Obrázek 3 *– Schéma DDoS útoku [60]*

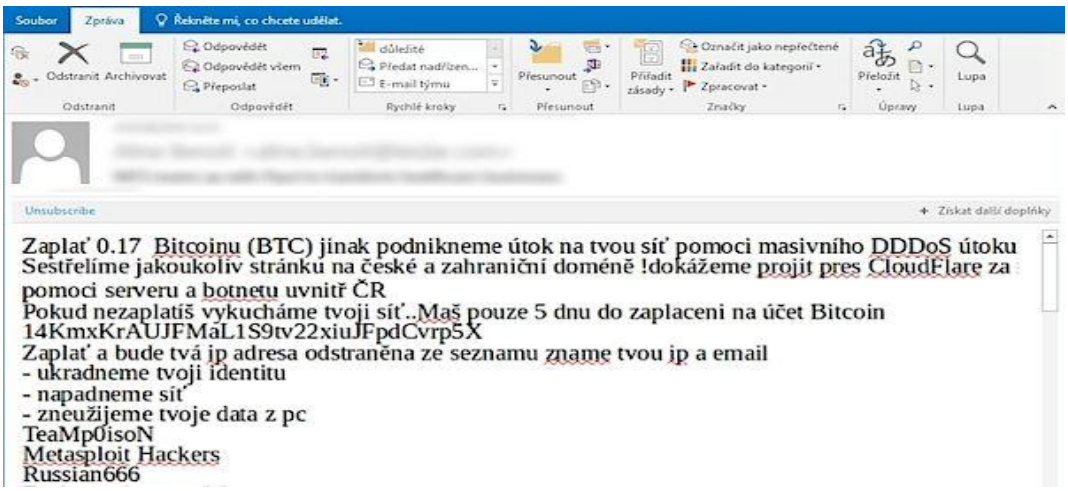
Obrana proti takovému útoku není jednoduchá. Základem je co nejdříve identifikovat o jaký druh útoku se jedná (jestli o DoS nebo DDoS) a zahájit např. blokaci širšího spektra IP adres. Pokud tento útok cílí na více úrovní ISO/OSI síťových vrstev (Inernational Standards Organization/Open System Interconnection), je obrana už podstatně složitější a vyžaduje hloubkovou analýzu provozu systému v jednotlivých síťových vrstvách za použití monitorovacích nástrojů. Úkolem každé vrstvy je poskytovat služby následující vyšší vrstvě. V případě, že je tento proces narušen, stává se síť z části nebo zcela nefunkční. Architektura vrstev je členěna viz obrázek 4.

Vrstva OSI	Využívaný protokol a služby	Příklad techniky útoku	Mitigace uvedeného příkladu
Aplikační vrstva	FTP, DNS, DHCP, POP3, SMTP, SSH, Telnet, TFTP	HTTP get/post - přihlašování do aplikace, upload videa, zasílání komentářů	monitorováni aplikace, CAPTCHA. Vzhledem k tomu, že na této vrstvě útoky „napodobují" lidské konání, obrana je náročnější
Prezentační vrstva	komprimace, šifrování, konvertování	útok pomocí upravených SSL dotazů	přesměrování SSL dotazů z původní infrastruktury přes nějaký jiný zdroj
Relační vrstva	zahájení a ukončení relačního spojení	omezení služeb jinak přístupných přes Telnet	útok je možný v důsledku zranitelnosti, která může byt updatem odstraněná
Transportní vrstva	TCP, UDP	SYN flood, Smurf attack. Omezuje počet síťových připojení na zařízeních	informování o blackholingu u svého poskytovatele připojení
Síťová vrstva	směrování a síťové adresování	ICMP flooding	stanovení limitu na ICMP
Linkova vrstva	switche a přepínače	MAC flooding	omezení počtu MAC adres které mohou porty přijmout
Fyzická vrstva	síťové kabely	fyzická manipulace s vedením	omezení fyzického přístupu

Obrázek 4 *– Rozdělení síťových vrstev [61]*

Konkrétní obranu můžeme provádět buď **filtrací síťového provozu** nebo pravidelnou údržbou dat na HDD (Hard Drive Disk) – **scrubbing.** Kontroluje se stav úložiště a cesty k souborům na úložišti. V případě potřeby obnovy dat, je tato obnova snažší, jelikož systém ví, kde přesně se data nachází a jaké cesty k nim vedou.

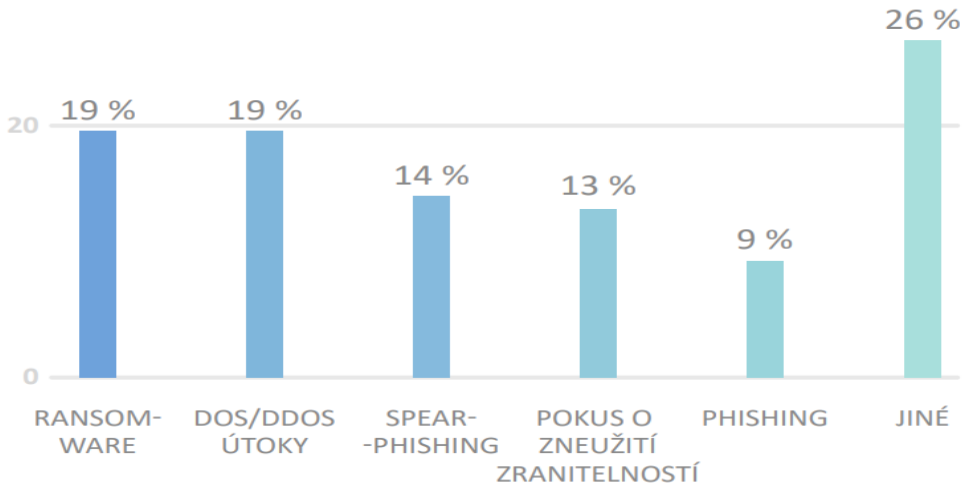
S exponenciálním nárůstem objemu dat na celosvětové síti dochází ke stále většímu počtu útoků typu DDoS. Pro každou obchodní společnost je rozhodování o struktuře a zabezpečení sítě otázkou, která je úzce spojena s úspěšným byznysem. I krátkodobý výpadek sítě, vyvolaný DDoS útokem by těmto společnostem způsobil škody v řádech desítek tisíc, nemluvě o povinnosti chránit citlivé údaje svých zákazníků. Velké společnosti, VIP osoby ale i jednotlivé úřady státní správy apod., jsou denně po celém světě cílem např. vyděračských kyber útoků.



Obrázek 5 *– Ukázka spamu hrozícího DDoS (distributed denial of service) útokem [62].*

7.4 Phishing

Tato kriminální metoda je založena na tzv. sociálním inženýrství. Používá se k získání citlivých údajů nejčastěji cestou elektronické komunikace. V hledáčku útočníků jsou přihlašovací jména a hesla, čísla kreditních karet nebo digitální identita oběti apod. Propracovanější formou phishingu je **spear phishing**, tedy tzv. cílený phising, který využívá již předem získané informace o oběti a je cílen na konkrétní obět (chování oběti je cíleně po nějaký čas sledováno). V tom se liší od obecného phishingu, který je cílen na kohokoliv [63]. Nepřebernou knihovnou informací a osobních údajů je např. služba Facebook (Meta), Instagram, Twitter apod. Kyberprostoru tak vědomě svěřujeme svá nejcenější **aktiva** (osobní údaje, digitální identitu, peníze apod.). Tato aktiva jsou motivací a cílem pachatelů kyberkriminality. O některých jedincích se dá zjistit na internetu téměř vše. Zneužití získaných informací je u spear phishingu vyšší než v případě obecného phishingu, jelikož útočník může např. převzít digitální identitu dobrého přítele oběti a touto podvodně získanou identitou vést komunikaci apod. Jedná se o třetí nejzávažnější typ kybernetického útoku (viz graf 7).



***Graf 7** – Nejzávažnější typy kybernetických útoků v roce 2020 (% respondentů) [64]*

Phishingovým útokům jsou vystaveni mimo jiné i klienti významných bank nebo dalších finančních institucí, inzertních portálů (domácích i zahraničních), populárních sociálních sítí nebo úřadů státní správy apod. Jedná se o sofistifikované podvodné jednání. Padělaná webová stránka se tváří, že pochází z důvěryhodného zdroje nebo od IT administrátorů. Tyto stránky často vyzývají adresáta k zadání osobních údajů na padělané stránce, jejíž podoba je takřka identická s tou oficiální.

Stránka může napodobovat přihlašovací okno internetového bankovnictví a uživatel, který do něj zadá své přihlašovací jméno a heslo, tím tyto údaje prozradí útočníkům, kteří jsou následně schopni z účtu oběti vykrást peníze nebo jeho ukradenou digitální identitu zneužijí k dalším podvodům (viz obrázek 6).

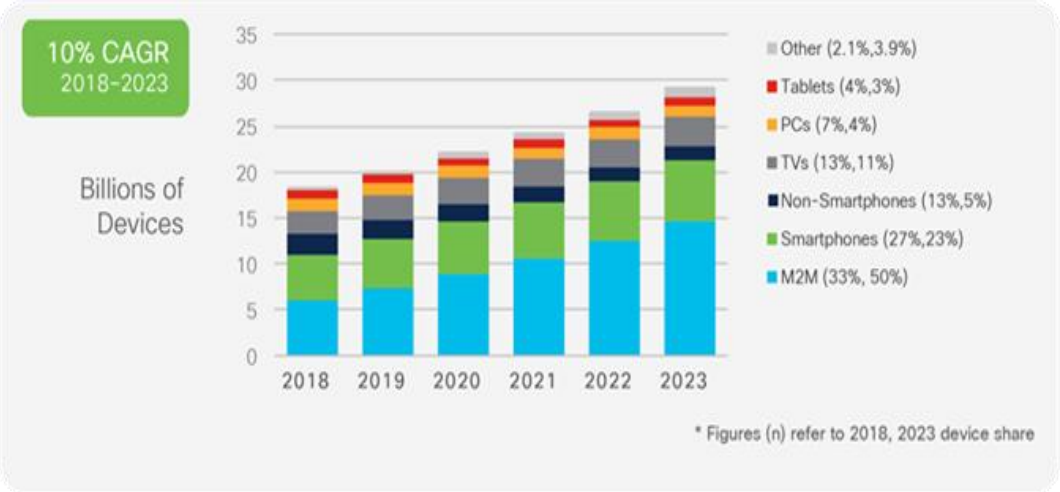
Obrázek 6 *– Ukázka phishingového útoku zaměřeného na klienty ČS, a.s. [65]*

Phishing se nevyhýbá ani významným univerzitám a výzkumným ústavům po celém světě. Zájmem hackerů jsou data významných projektů, výsledky výzkumné činnosti, patenty nebo i nepublikované vědecké práce. V nedávné minulosti útočila na univerzitní prostředí hackerská skupina Cobalt Dickens, jejímž cílem na konci roku 2018 bylo 17 výše zmiňovaných institutů.[66]. Mnohdy se pachatelé přesunuli do kyberprostoru kvůli větší efektivitě. Zejména pak páchání trestných činů se sexuálním podtextem se stalo jednodušší. Pro dokreslení jaké další trestné činy se páchájí prostřednictvím internetu a jsou vyšetřovány OČTŘ uvádím jejich stručný výčet:
§ 182 – Porušení tajemství dopravovaných zpráv, § 183 – Porušení tajemství listin a jiných dokumentů uchovávaných v soukromí, § 184 – Pomluva, § 186 – Sexuální nátlak, § 187 – Pohlavní zneužívání, § 191 – Šíření pornografie, § 192 – Výroba a jiné nakládání s dětskou pornografií, § 193b – Navazování nedovolených kontaktů s dítětem, § 209 – Podvod, § 230 – Neoprávněný přístupu k počítačovému systému a nosiči informací, § 231– Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat, § 232 – Poškození záznamu

v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti, § 270 – Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi, § 287 – Šíření toxikomanie, § 345 – Křivé obvinění, § 348 – Padělání a pozměnění veřejné listiny, § 354 – Nebezpečné pronásledování, § 355 – Hanobení národa, rasy, etnické nebo jiné skupiny osob, § 356 – podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod, § 403 – Založení, podpora a propagace hnutí směřujícího k potlačení práv a svobod člověka, § 404 – Projev sympatií k hnutí směřujícímu k potlačení práv a svobod člověka, § 405 – Popírání, zpochybňování, schvalování a ospravedlňování genocidia [67].

8 SLUŽBY A PROSTŘEDKY ZAJIŠŤUJÍCÍ KYBERNETICKOU BEZPEČNOST VYBRANÉ ORGANIZACE

Vzhledem k exponenciálnímu nárůstu počtu připojených zařízení do internetové sítě a složitosti problematiky kyberkriminality není a nebude lehkým úkolem udržet kyberprostor bezpečný. Společnost CISCO odhaduje, že v roce 2023 bude počet zařízení připojených do internetové sítě dosahovat 30 miliard (graf 8).



***Graf 8** – Odhad vývoje připojených zařízení do internetové sítě [68]*

S růstem populace poroste počet připojení do internetové sítě. Odhad je, že 2/3 světové populace budou mít přístup k internetu do roku 2023. To představuje 5,3 miliardy uživatelů (66 % celosvětové populace). S tím souvisí technologická náročnost na rychlost a propustnost internetové sítě, z důvodu narustajícího objemu dat, která jsou internetovou sítí posílána.

V roce 2018 byla průměrná rychlost připojení mobilní (celulární) sítě 13,2 Mbps a z dosavadního vývoje se odhaduje, že v roce 2023 bude více než trojnásobná. Ten samý nárůst zrychlení se očekává i u Wi-Fi, kterou vytváří mobilní zařízení. V globálním měřítku se u Wi-Fi předpokládá nárůst rychlosti v roce 2023 na 92 Mbps (průměr v roce 2018 činil 30,3 Mbps). S ekonomickým, technologickým a průmyslovým rozvojem společnosti vyvstavala potřeba ještě více zrychlit mobilní přenost dat. Proto byla vyvinuta nová síť s označením 5G, která je schopna reálně překročit hranici > 10 Gbps při latenci méně než 1 ms. To představuje desetinásobný nárůst rychlosti proti současné 4G síti (max. 150 Mbps) [69]. V České republice se

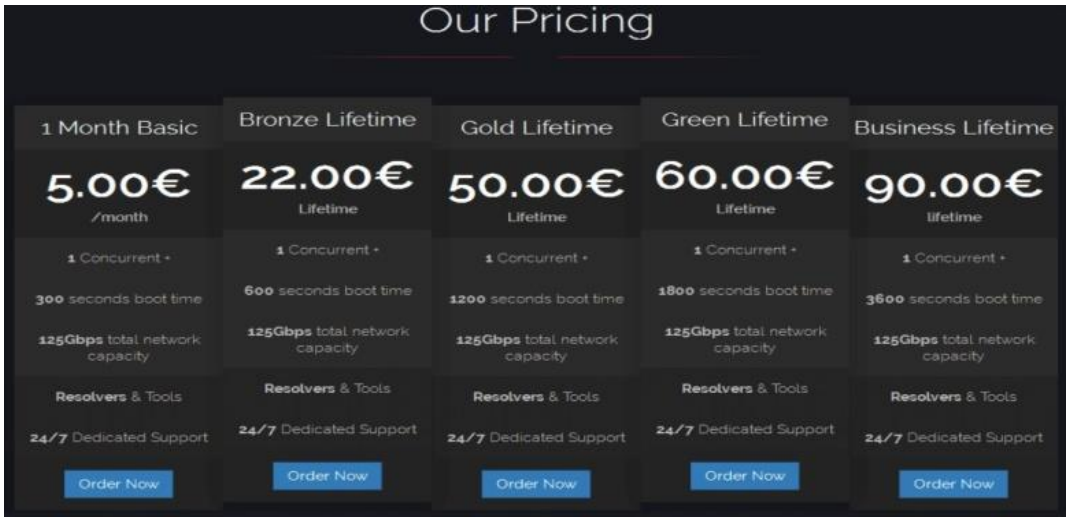
zatím tato síť testuje ve vybraných městech Praha, Brno, Karlovy Vary, Ústí nad Labem a Jeseník. Česká republika je první země Evropy, ve které společnost Vodafone spustila 5G síť a to v pražském metru.

Wi-Fi sítě se svou základní podstatou přenosu dat liší od sítí kabelových, označovaných jako ethernet. Tyto sítě, mají z hlediska bezpečnosti jednu nevýhodu vycházející právě z její podstaty fungování. Nejsme totiž schopni zabezpečit dostatečné omezení rozsahu vysílání signálu wi-fi sítě a chránit tak přenos dat před útokem zvenčí. U ethernetové sítě je to pro útočníka težší, protože útočník se musí připojit k fyzické vrstvě sítě, aby mohl zachytávat probíhající komunikaci. V případě wi-fi sítě, se útočníkovi stačí dostat do prostoru dosahu jejího signálu, který je přístupný všem v jeho dosahu. Aby útočníci zjistili informace o vytipované wi-fi síti, používají k tomuto účelu zařízení na určení přesné GPS polohy, silné antény pro zachytávání signálu, vysoce citlivé síťové karty apod. Jejich cílem je zachytit komunikaci v síti a zjistit SSID (Service Set Identifier), způsob zabezpečení a šifrování. Abychom se vyhnuli nebezpečí neoprávněnému zachytávání komunikace, je nutné přenosový signal šifrovat [70].

Současným a zatím posledním standardem v šifrování je IEEE (Institute of Electrical and Electronics Engineers) 802.11i, známý též jako WPA2, který používá standardizovaný pokročilý algoritmus šifrování AES (Advanced Encryption Standard). Tento algoritmus rozdělí komunikaci do datových rámců a ty jsou šifrovány a dešifrovány podle stejného klíče. Tato metoda nazývaná CCMP (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol) je v současnosti považovaná za nejvyšší úroveň zabezpečení, integrity, dostupnosti a důvěryhodnosti dat [71].

8.1 Řešení ochrany kyberprostoru vybrané organizace

S technologickým pokrokem přibývají i bezpečnostní hrozby. Od roku 2006 všechna zařízení připojovaná do sítě, která chtějí mít certifikaci Wi-Fi, musí podporovat standard WPA2. Zařízení, která jsou připojená do sítě internet a mají zastaralý firmware nebo slabé zabezpečení, jsou snadným cílem pro jejich ovládnutí nebo zneužití k útoku na vybraný cíl [72]. DoS/DDoS útoky se dají koupit či pronajmout jako služba za pár dolarů (konkurenční boj), stejně tak celé botnetové sítě nebo ransomware a při špatné ochraně sítě, je snadné celou síť úplně zahltit nebo odstavit.



***Obrázek 7**– Ukázka cenové nabídky za DDoS útok [73]*

Prioritou pro společnost, která nám umožnila nahlédnout do jejího systému ochrany kyberprostoru a provést nám testování jejich zaměstnanců prostřednictvím její sítě musí být bezpečnost uchovávaných dat s ohledem na jejich charakter. Tato společnost zvolila komplexní ochranu vybudovanou a navrženou jedním dodavatelem. Pravidelně obnovuje síťové prostředky, které vykazují morální zastaralost nebo poruchovost a které jsou začleněny do kybernetické ochrany jejího síťového perimetru. Stejnou pozoronost věnujě i dalším periferiím, které se připojují do sítě (ugrade a update) a dále se pochopitelně provádí pravidelné aktualizace používaných operačních a databázových systémů a jejich zálohování.

Společnost si k základní ochraně perimetru (sítě na centrále, pobočkách a v data centrech) zvolila sadu nástrojů a zařízení od společnosti FortiGate. Zařízení jsou vyráběna americkou firmou FortiNet, a vyznačují se vysokou spolehlivostí, nadstandardní úrovní ochrany a snadným způsobem správy za optimální cenu. Do ochrany jsou začleněny FortiFirewally NGFW – next generation firewall, které spolupracují se systémem pro detekci a prevenci průniku tzv. IDPS. Tento systém trvale monitoruje celou sít a vyhledává znaky podezřelých aktivit (anomálií v provozu sítě). Analyzuje přenosový síťový protokol, včetně přenosového protokolu firemních bezdrátových sítí. V případě, že systém v síťovém protokolu nalezne anomálii spustí příslušnou nadefinovanou akci. Tyto firewally spolupracují na přenosu paketů a komunikují s přístupovými body (AP – access point). Pro jejich nastavení a správu je

využíván nástroj FortiAP / FortiWifi s podporou standardu Wi-Fi 5 (IEEE 802.11ac) a nejnovějšího Wi-Fi 6 (IEEE 802.11ax).

Dále jsou tato zařízení vybavena podporou funkcí jako FortiASIC (zrychluje VPN, podporuje multi-gigabitové rychlosti, specifická obsahová kontrola paketů), Antivirus Gateway (zastaví viry, spyware, červy atd. ještě před jejich vniknutím do sítě, nástroj kontroluje přílohy příchozích a odchozích e-mailů, provoz přístupu na domény, upload / download, má přístup v reálném čase do celosvětové databáze antivirových signatur a aktualizační sítě FDN (FortiGuard Distribution Network), FortyOS (antispam – aktualizuje seznam zakázaných a povolených domén, IP a také emailových adres, traffic shaping – kontroluje provoz, aby udržel a optimalizoval výkon provozu sítě, minimalizuje čekací dobu na přenos, třídí a řadí pakety do fronty, směrováním reguluje přetížení atd.), FortiGuard (web filtering – kontroluje a testuje veškerý webový obsah a hledá známé nežádoucí URL adresace v kategorizovaných stránkách FortiNetu).

Vzdálené připojení do interní sítě střeží FortiClient VPN (software provádí ověření uživatele, šifruje data, spravuje relace) a ve spolupráci s dalšími komponenty jako jsou FortiGate, FortiAnalyzer, FortiSandbox apod. má tento nástroj ucelený přehled provozu na připojených koncových bodech a může tak zabezpečit vynucování a dodržování pravidel a naprostou kontrolu nad provozem sítě. Pro ochranu datacentra a extranetových aplikací společnost využívá nástroj FortiWeb a pro ochranu cloudového uložiště nástroj FortiGate Cloud. Pro chráněný přístup k aplikacím přes mobilní zařízení používá O365 Intune, což je cloudová služba, která je zaměřena na správu mobilních zařízení a správu mobilních aplikací. Přes tento nástroj lze řídit používání zařízení společnosti jako jsou např. notebooky, tablety, mobilní telefony apod. Zároveň lze nakonfigurovat konkrétní pravidla řízení aplikací (zákaz posílání e-mailů osobám mimo společnost). Další výbornou možností O365 Intune je, že dokáže v zařízení izolovat data společnosti od osobních dat.

Všechny výše uvedené nástroje jsou svedeny a připojeny do jednoho místa, kde je přehledně a pohodlně umožněna jejich centrální správa. Ta se provádí za pomoci nástroje FortiManager, ve kterém si správce může nastavit a spravovat naprosto vše co je potřeba pro správu sítě. Od řízení přístupu do jednotlivých účtů, přes reporty z anylýz antiviru až po definování lokální nebo globální bezpečnostní politiky společnosti.

8.1.1 Systém řízení bezpečnosti informací – ISMS

Ochrana bezpečnosti kyberprostoru u vybrané organizace má i svůj ucelený **systém řízení bezpečnosti informací** (ISMS – Information Security Management System) podle základní normy ČSN EN ISO/IEC 27000:2020, pod kterou jsou podřazeny další normy upravující tuto problematiku (viz dále). Úkolem tohoto systému je řešit řízení a správu aktiv (informace/data), management, analýzu a eliminaci bezpečnostních rizik. Výstupem z tohoto řetězce činností je:

a) **identifikace aktiv,** která mají být chráněna

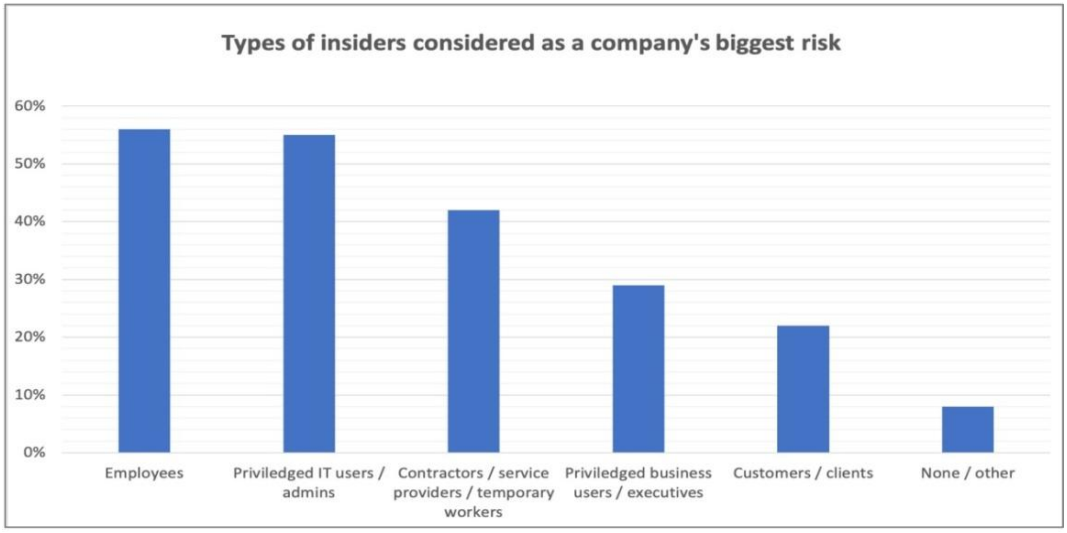
- primární aktiva – informace, služby,
- podpůrná aktiva – sítě, počítače, software,

b) **identifikace hrozeb** (vnější a vnitřní) a **zranitelnost systému** (technická, organizační, personální apod.),

c) **zavedení opatření** k eliminaci rizik a dopadů,

d) **management kontroly** dodržování opatření [74].

Stanovená bezpečnostní rizika jsou pak vždy posuzována na základě vztahu **chráněná aktiva** x **úroveň zranitelnosti systému** x **pravděpodobnost** a **dopad hrozby** na sledovaný systém. Nikdy se nebudeme moci bránit rizikům na 100 %, ale vždy je snaha učinit taková opatření, která budou riziko snižovat na minimální nebo alespoň přijatelnou úroveň.



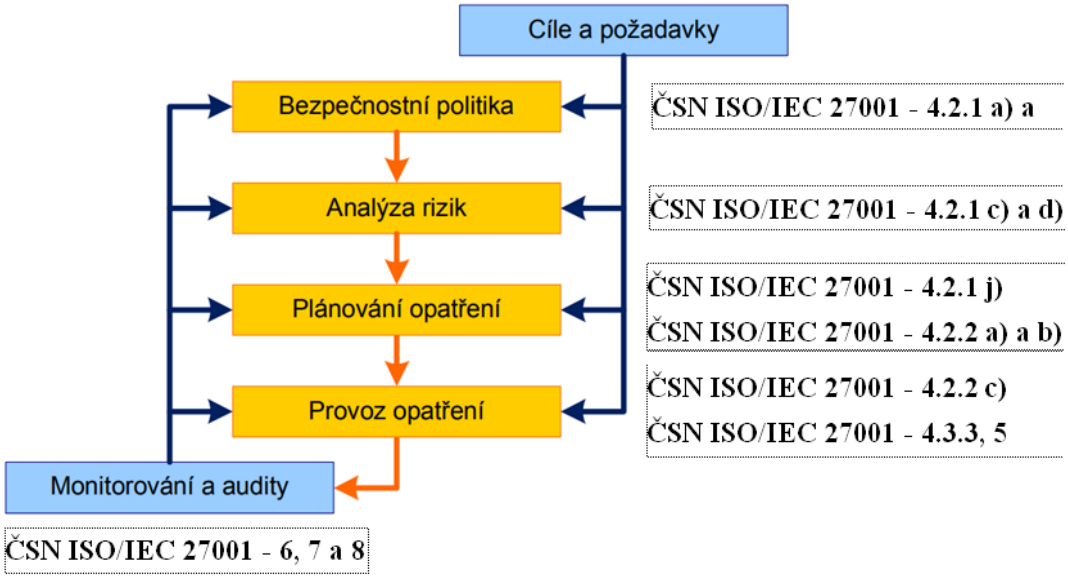
***Graf 9** – Ohrožení dat a bezpečnosti informačního systému ze strany insiderů [75]*

Graf názorně ukazuje přehled tzv. personálního rizika dle typu insiderů pohybujících se uvnitř společnosti nebo instituce. Největší bezpečnostní riziko představují sami **zaměstnanci**, **privilegovaní IT uživatelé** nebo **správci systému**. Druhou skupinu tvoří poskytovaelé služeb, dodavatelé a dočasní pracovníci (např. brigádníci) a rovněž zaměstnanci ve vedení společnosti. Z této interpretace vyplývá, že nejslabším článkem v řetězci bezpečnosti systému je **člověk**.

V případě velkých společností je výstavba, zabezpečení a monitoring sítě včetně připojených IT prostředků daleko složitější a komplexnější problematika. Bezvýznamnou není ani finanční náročnost, kterou musí společnost kalkulovat a zvažovat celkové náklady na její výstabu, provoz, údržbu a zabezpečení s ohledem na důležitost a povahu chráněných dat. Při hledání způsobu zajištění bezpečnosti se nikdy nepovede dosáhnout hranici 100% zabezpečení, ale můžeme aplikovat bezpečnostní opatření a takové způsoby zabezpečení, které se ve vhodné kombinaci a uspořádání, této hranici alespoň přiblíží a zároveň budou přiměřené k hodnotě chráněných aktiv (informací), jež jsou primárním předmětem ochrany. Při hledání vhodného způsobu ochrany by měla panovat přímá úměra mezi hodnotou, kterou mají informace pro daný subjekt a bezpečností prostředků, které slouží k tvorbě, přenosu a uchování informací.

8.2 Management bezpečnosti informací podle ITIL

Pro názornost a snažší orientaci v managementu bezpečnosti informací vycházející z **ITIL** (Information Technology Infrastructure Library) uvádíme toto schéma včetně normy, kterou se tato problematika řídí.



***Obrázek. 8** – Základní schéma procesů řízení bezpečnosti informací dle ITIL* [76]

- **Bezpečnostní politika** – vytyčení požadavků na úroveň zabezpečení sítě a stanovení cílů (kdo, co a jakým způsobem);
- **Analýza rizik** – stanovení aktiv, která mají být chráněna, určení a posouzení hrozeb, zranitelností systému a možných následků při selhání (ztráta dostupnosti a integrity aktiv, poškození pověsti atd.);
- **Plánování opatření** – ucelený přehled rozhodnutí, která stanoví řešení pro omezení nebo eliminaci identifikovaných rizik a stanoví zdroje, priority, odpovědnosti a činnosti pro řešení rizik narušení bezpečnosti informací;
- **Provoz opatření** – stanoví způsob provádění přijatých opatření a vedení záznamů, které objektivně prokazují způsob provozu zavedeného ISMS (způsob správy úkolů a procesy schvalování);
- **Monitorování a audity** – pravidelná kontrola a vyhodnocování efektivity a funkcionality přijatých opatření v závislosti na výsledcích zvládání řešení bezpečnostních incidentů a auditů, posouzení podnětů a návrhů participujících stran, aktualizace přijatých opatření ve vztahu k stanoveným cílům [77, 78].

8.3 Trendy v rozvoji řízení informační bezpečnosti – bezpečnostní rámce podle CIS a NIST

alší bezpečnostní normy (rámce), které řeší kybernetickou bezpečnost jsou CIS (**C**enter for **I**nternet **S**ecurity) a NIST (**N**ational **I**nstitute of **S**tandards and **T**echnology). V současné době se jedná o nejpoužívanější standardy bezpečnostních rámců zejména v USA. Pochopení a aplikace norem NIST i CIS v systému ochrany kyberprostoru organizace znamená, že taková organizace má podstatně větší šanci účinně čelit jakékoliv kybernetické hrozbě. Jednou z výhod bezpečnostních rámců podle NIST a CIS je jejich vzájemná kompatibilita a kompatibilita s normou ČSN ISO/IEC 27001, která je aplikována zejména v Evropě a Asii.

8.3.1 Centrum pro kybernetickou bezpečnost internetu - CIS

CIS existuje od roku 2000, využívající globální standardy a uznávané postupy pro zabezpečení IT systémů a dat proti nejrozšířenějším útokům. Tyto standardy a postupy jsou neustále vylepšovány a aktualizovány profesionály z oboru bezpečnosti IT v závislosti na vývoji bezpečnostních hrozeb. Cílem této organizace je zavádět a podporovat standardizované protokoly kybernetické bezpečnosti a rovněž podporovat komunity, které se věnují dalšímu rozvoji a výzkumu v oblasti kybernetické bezpečnosti. Z dosavadních zkušeností, a na základě vývoje technologií IT vypracoval CIS soubor 20 kritických bezpečnostních kontrol rozdělených do 3 skupin:

a) základní:

- inventarizace a kontrola hardwarových aktiv,
- inventarizace a kontrola softwarových aktiv,
- průběžná správa zranitelností,
- řízené používání administrativních oprávnění,
- zabezpečená konfigurace hardwaru a softwaru na mobilních zařízeních, noteboocích, pracovních stanicích a serverech,
- údržba, monitorování a analýza protokolů auditu,

b) základní - rozšířená:

- ochrana e-mailu a webového prohlížeče,
- ochrana proti malwaru,
- omezení a kontrola síťových portů, protokolů a služeb,

- možnost obnovy dat,
- zabezpečená konfigurace pro síťová zařízení, jako jsou brány firewall, směrovače a přepínače,
- ochrana perimetru sítě,
- ochrana dat,
- řízený přístup založený na potřebě vědět,
- bezdrátové řízení přístupu,
- monitoring a kontrola uživatelských účtů,

c) organizační:

- implementovat školení za účelem zvyšování povědomí o kyberbezpečnosti,
- zabezpečení aplikačního softwaru,
- kontrola reakce na incidenty a řízení,
- provádět penetrační testy a cvičení u oddělení IT [79].

Kromě obecných bezpečnostních kontrol poskytuje CIS další návody pro širší spektrum specifických nástrojů (CIS Controls, CIS Benchmarks, CIS Secure Suite), které jsou přizpůsobeny konkrétním zařízením nebo platformám. Jejich obsahem je například IoT – Internet of Things Security Companion Guide, kde jsou zmíněna slabá místa v zařízeních, obecně nazývaných jako smart (tablety, telefony, hodinky apod.), která jsou v popředí zájmu hackerů. Tato příručka aplikuje ovládací prvky CIS na současná i budoucí zařízení IoT.

Jiným nástrojem je průvodce CIS Controls Cloud Companion, který řeší problematiku bezpečnosti dat v externím uložišti – cloudu. Toto prostředí, představuje jedinečnou bezpečnostní výzvu, jak už se v minulosti nejednou ukázalo (únik dat známých osobností). K útoku na iCloud úložiště známých osobností v roce 2014 byl použit škodlivý software “iBrute” (dostupný na GitHub). Společnost Apple učinila kroky k tomu, aby se tento případ již neopakoval (např. omezila počet možností zadání hesla pro přihlášení do iCloud).

Ačkoli mnohé z hlavních bezpečnostních problémů řeší standardní CIS Controls, mohlo by být obtížné aplikovat jednotlivá doporučení univerzálně. Je to proto, že různé cloudové systémy fungují na základě různých bezpečnostních protokolů.

8.3.2 Národní úřad pro standardy a technologie – NIST

Národní institut pro standardy a technologie je neregulační agentura, která je součástí Ministerstva obchodu USA. NIST se mimo jiné zabývá výzkumem v oblasti průmyslu, s cílem posílit pozici USA jako technologicko-ekonomického lídra. Bezpečnostní rámec NIST Cybersecurity Framework (NIST CSF), který byl uveden v roce 2014 je známý zejména v USA a pomáhá organizacím porozumět, organizovat a spravovat zabezpečení informací. Patří mezi nejvíce používané bezpečnostní standardy vládními agenturami, dodavateli a je povinným standardem pro federální agentury USA. V roce 2018 byl aktualizován. výše jmenovaným organizacím poskytuje komplexní pohled na jejich data, personál, zařízení, cíle, zúčastněné strany a další systémové podrobnosti, aby lépe porozuměly rizikům kybernetické bezpečnosti a tomu, jak je řídit. NIST Cybersecurity Framework se člení na 3 základní části:

a) **The NIST Framework Core Function - základní funkce bezpečnostního rámce**, který je složen z 5 vzájemně spolupracujících prvků s cílem:

- **identifikovat** zdroje, které podporují nejdůležitější funkce vaší organizace, související rizika s kybernetickou bezpečností a další úkoly zahrnující hodnocení rizik, řízení a analýzu podnikatelského prostředí,
- **chránit** cíle podnikání organizace implementací správných bezpečnostních opatření, aby byl ochráněn kontinuální provoz nejkritičtějších infrastrukturních služeb, dále implementací školení o kyberbezpečnosti nebo používání ochranných technologií,
- **detekovat** události ohrožující kebernetickou bezpečnost organizace implementací vhodných detekčních procesů nebo softwaru pro monitorování, vyhodnocování a uchovávání záznamů o provozních anomáliích,
- **reagovat** adekvátním způsobem na události ohrožující kebernetickou bezpečnost organizace (mít vypracován plán reakce na bezpečnostní incident, stanovenou bezpečnostní politiku organizace),
- **obnovit** funkčnost klíčových procesů a dat a chod organizace vrátit do stavu normálního provozu.

Každý prvek v sobě obsahuje řadu funkcí a úkolů, jejichž cílem je vyšší a komplexnější kybernetická ochrana.

b) **The Framework Implementation Tiers – implementace úrovní bezpečnostního rámce** berou v úvahu současné postupy řízení rizik organizace, prostředí hrozeb, požadavky na dodržování předpisů a obchodních zvyklostí, aby bylo možné určit, úroveň kybernetické bezpečnosti s ohledem na podnikání organizace a ty by měly zvážit postup na vyšší úroveň, pokud je to pro ně nákladově efektivní v komparaci se snížením bezpečnostního rizika. Tyto úrovně obsahují:

- **úroveň 1 – částečná** – na této úrovni nejsou strategie kybernetické bezpečnosti formalizovány a rizika jsou řízena tzv. ad hoc,
- **úroveň 2 – informace o riziku** – na této úrovni má organizace zavedeny určité postupy řízení rizik, ale nejsou formalizovány a standardizovány napříč organizací,
- **úroveň 3 – opakovatelná** – na této úrovni existuje formalizovaná strategie kybernetické bezpečnosti pro celou organizaci, bezpečnostní zásady jsou definovány, implementovány a pravidelně revidovány,
- **úroveň 4 – adaptivní** – na této úrovni organizace projevuje sofistikovaný přístup ke kybernetické bezpečnosti, který se opírá o předchozí zkušenosti a prediktivní indikátory hrozeb.

c) **The Framework Profil – rámcový profil** kombinuje obchodní cíle a prostředí hrozeb s veškerými požadavky a kontrolami kybernetické bezpečnosti. Je odrazem sladění organizačních požadavků, řízení rizik a zdrojů. Skládá se z aktuálních (požadovaných) aktivit v oblasti kybernetické bezpečnosti reflektující základní funkce bezpečnostního rámce. Na základě toho organizace identifikuje svou úroveň a poté porovná svůj profil, aby zjistila, co ještě musí splnit, aby dosáhla požadovaného cílového stavu. Rámcové profily pomohou odhalit mezery ve strategii nebo slepá místa v cílech řízení rizik. Jsou rovněž silným výchozím bodem při formalizaci zásad a postupů v celé organizaci [80, 81].

8.4 Monitoring sítě a její filtrace

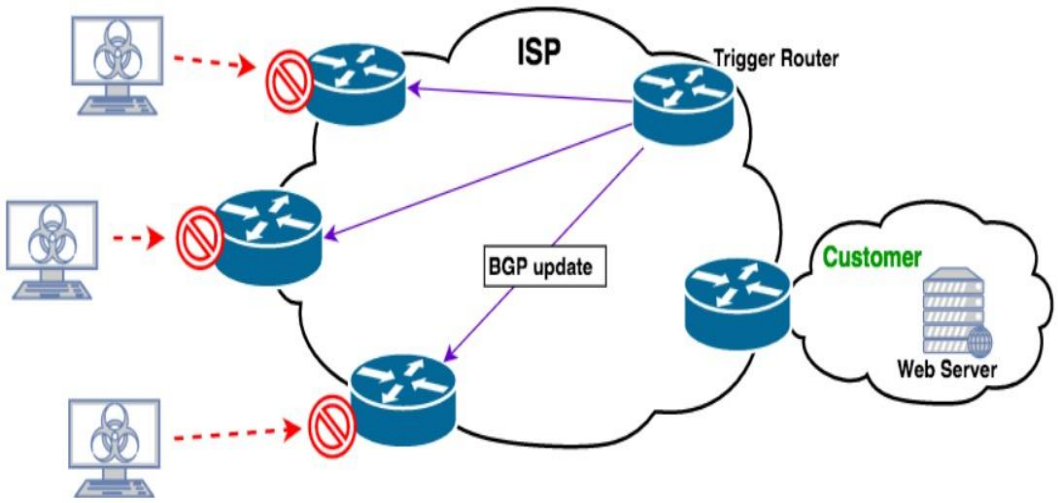
V době, kdy se v soukromých, ale i státních organizacích rozmáhá výkon práce z jiného než obvyklého místa (sídla) výkonu práce (práce z domova vzdáleným přístupem), vzrostla potřeba rozšířit ochranu firemní sítě i za její fyzické hranice uvnitř působiště. K tomu účelu slouží systém **EDR** (Endpoint Detection and Response), který monitoruje činnost aplikací a systému připojených koncových stanic (desktop, laptop, tablet, smartphone, IoT zařízení apod.), jejich vzájemnou interakci a interakci se síťovými prostředky zařazených v jednotlivých síťových vrstvách. EDR sleduje, detekuje, analyzuje a vyhodnocuje podezřelé (neobvyklé) aktivity v systému, a na základě výsledků označí hrozbu. Analytický modul v reálném čase podle nastavených algoritmů vyhodnocuje a koreluje velké objemy dat, ve kterých hledá stejné nebo podobné vzory chování systému. Tato činnost je podpořena forenzními nástroji, které umožňují hledat shody ve způsobech narušení a chování malware, zaznamenaných v historii chodu systému zařízení. Záznamy se analyzují pro lepší pochopení toho, jak malware funguje a jak pronikl do systému. Jedná se velice složitý algoritmus instrukcí, který je řízen k tomu účelu naprogramovanou sofistikovanou **AI** (Artificial Inteligence). Nástroj EDR má 3 základní součásti:

a) **software pro scan a sběr dat** – jeho úkolem je monitorovat činnost koncového zařízení a o této činnosti shromažďovat informace (spouštěné procesy, připojování k síti, objem vykazované aktivity a přenosu dat,

b) **software pro automatickou odezvu** – obsahuje předkonfigurované algoritmy, které dokáží rozpoznat pokud, příchozí data vykazují známé typy chování při narušení bezpečnosti, a v tomto případě se spustí naprogramovaný algoritmus automatické odpovědi systému (odeslání výstrahy uživateli nebo správci systému, odhlášení koncového zařízení, zamezení dalšího přístupu apod.),

c) **software pro analýzu dat a forenzní nástroje** – analyzuje chování koncového zařízení v reálném čase, nástroji pro rychlou diagnostiku hrozeb, které zcela neodpovídají předem nakonfigurovaným pravidlům, a zároveň využívá forenzní nástroje pro hlubší analýzu a vyhledávání stop po narušení bezpečnostního systému, které po sobě malware zanechal [82].

K rozpoznání anomálií v chodu systému a provozu v síti slouží speciální monitorovací sotware, jehož charakteristika zde byla uvedena. Sledování provozu lze provádět i pasivním monitorováním sítě na směrovačích (routerech) pomocí protokolu NetFlow/sFlow. Tento nástroj umožňuje zaznamenat informace o provozu od zdrojové adresy k cílové adrese a od zdrojového portu k cílovému portu, využitého protokolu nebo času všech proběhlých operací. Tato zaznamenaná data jsou důležitá pro zpětnou identifikaci útoku a proces filtrace. [83]. V případě jednoduchých sítí, které obsahují jeden směrovač, není řešení složité. Filtrace/blokace je realizována přímo na směrovači, který zajišťuje konektivitu do sítě internet a zároveň i směrování interní sítě. V případě složitější architektury sítě, kde je implementováno více směrovačů (routerů), lze využít filtrace (blokace) za pomoci protokolu BGP (Border Gateway Protocol) v součinnosti s RTHB (Remotely Triggered Black Hole).



***Obrázek 9** – Implementace RTHB směrovačů [84]*

Prostřednictvím protokolu BGP lze definovat, který provoz směřující do koncové sítě je nelegitimní a má být zahozen již páteřní sítí, aniž by zatěžoval přístupovou linku účastníka. Velice jednoduchou jednorázovou konfigurací protokolu BGP si zajistíme spojení s uzlem RTHB. Protokol BGP pomáhá směrovat datové pakety mezi autonomními systémy, přičemž každá nechtěná IP adresa šířená prostřednictvím protokolu BGP skrz RTBH uzel je sdělena všem ostatním směrovačům sítě, které tuto IP adresu začnou ihned blokovat. Tím odpadá nutnost manuálního výběru a konfigurace filtrů na síti. Správce sítě má pak jistotu, že datový paket blokované IP adresy bude zahozen již prvním síťovým směrovačem (routerem) [85]. Díky jeho poměrně snadné

automatizaci můžeme RTBH uzel zapojit do vlastního portfolia mechanizmů obranné strategie počítačové sítě.

8.5 Doporučená opatření

Nízké povědomí společnosti o bezpečném chování v kyberprosotru přináší řadu problémů. V tomto směru je potřeba se zaměřit na vzdělávání v oblasti bezpečného chování v kyberprostoru již od primárního stupně systému vzdělávání. Stále dokonalejší formy kybernetických útoků, používání umění sociálního inženýrství nebo i šíření jakéhokoliv malware je značně nebezpečné, obtěžující a způsobuje nemalé finanční ztráty. Předmětem útoku malware už dávno nejsou jen významní jednotlivci, ale především velké národní a nadnárodní společnosti, finanční a vzdělávací instituce, orgány státní správy atd. Malware pronikl i do průmyslových válek a průmyslové špionáže. Můžeme zmínit, že vědečtí pracovníci společnosti ESET objevili malware **Industroyer**, který byl zaměřen na průmyslové elektrárenské kontrolní systémy a pravděpodobně stál za výpadkem dodávek elektrické energie na Ukrajině v roce 2015 a 2016 [86]. Velké oblibě útočníků se těší tzv. "**kryptominery**", jejichž cílem jsou počítačové sítě společností a institucí, které jsou pak zneužívány k těžbě kryptoměn. Malware **Cryptoloose** a modulární trojan **Emotet** postihly celosvětově 6 % společností. V České republice se do popředí prodral kryptominer **JSEcoin,** který měl dopad na 38 % domácích společností [87].

Pro bezpečnost systému lze ze strany běžného uživatele učinit některá opatření, která významně napomohou zvýšení kybernetické bezpečnosti a jsou všobecně známá:

a) pravidelně aktualizovat operační systém a další dostupný firmware do používaných zařízení,

b) používat jen legální software,

c) používat kvalitní antivirový program,

d) začlenit do sítě firewall,

e) chránit připojené prostředky silným heslem:

- směrovač (router)
- wi-fi síť
- počítač
- operační systém

- mobilní zařízení (telefon, phablet, tablet atd.

f) pravidelně měnit hesla,

g) nepoužívat stejná hesla pro více služeb nebo připojovaných prostředků,

h) hesla nebo přihlašovací údaje nikdy nikomu nesdělovat,

i) v případě možnosti používat pro přihlášení do systému elektronický klíč,

j) navštěvovat jen dobře prověřené stránky,

k) stahovat data jen z důvěryhodných zdrojů,

l) neotvírat e-maily od neznámých adresátů nebo s nebezpečným obsahem,

m) nesdělovat své citlivé údaje např. e-mailem, po telefonu apod. (takové žádosti vždy velice pečlivě zvážit),

n) sledovat a zvažovat udělení oprávnění pro stahované aplikace do IoT.

Oblast kybernetické bezpečnosti je rychle se rozvíjející oblast, která je plná nových myšlenek a přístupů. Velká část útoků ze strany kyberzločinců je založena na neznalosti, podceňování situace, omylech, pochybeních nebo docela obyčejné lidské lenosti. To, jestli se staneme obětí kyberzločinu, záleží na momentálních okolnostech i kontextu dané situace, ovšem je nutno zmínit, že do značné míry to ovlivňujeme my sami. Nebojme se hlásit bezpečnostní incidenty, a to ani ty, které zrovna způsobíme. Zodpovědnou autoritou za technologické vybavení a bezpečnost sítě v každé instituci je IT oddělení, které je nutné vyrozumět včas, když lze hrozbu ještě v počátcích zastavit.

Abychom ověřili všeobecně prezentovaný názor, že nejslabší článek v bezpečnosti sítě je lidský faktor, provedl jsem praktický výzkum, zaměřený na chování člověka, který se stane terčem spear phishingového útoku.

9 METODIKA

Abychom ověřili všeobecně prezentovaný názor, že nejslabší článek v bezpečnosti sítě je lidský faktor, byl proveden praktický výzkum, zaměřený na chování člověka, který se stane terčem spear phishingového útoku. Zcela v souladu s bezpečnostní firemní politikou, souhlasem vedení společnosti a ve spolupráci s ředitelem odělení IT této společnosti, byl vypracován scénář spear phishingového útoku v rámci awareness trainingu, jehož cílem byla kontrola **povědomí zaměstnanců o kybernetické bezpečnosti** a **kontrola dodržování zásad bezpečnostní politiky společnosti**.

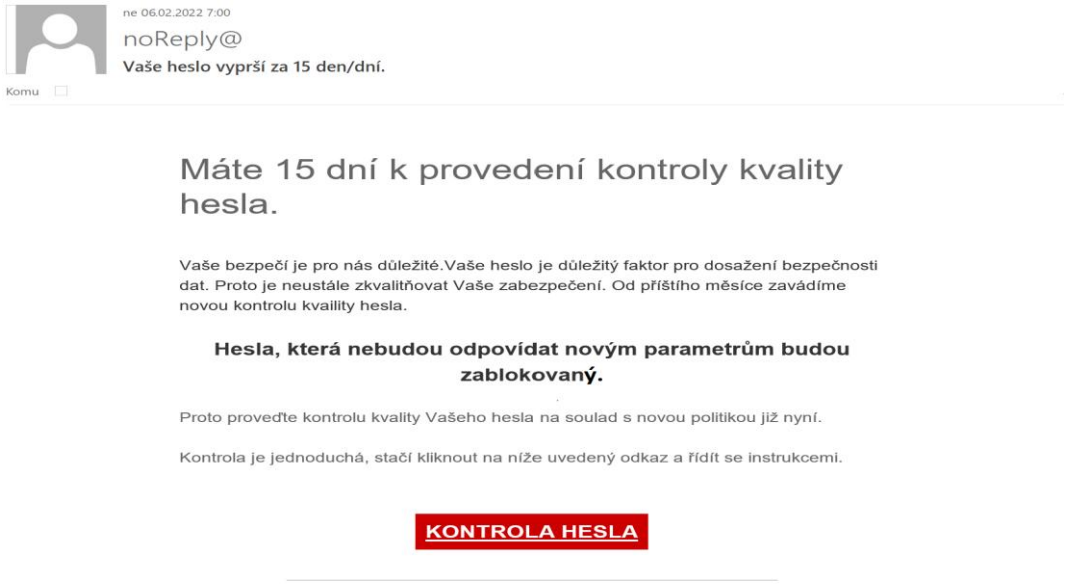
Před samotným provedením připraveného phishingového útoku se kmenoví zaměstnanci a externí spolupracovníci společnosti zúčastnili e-learningového školení zabývajícího se tématikou kybernetické bezpečnosti. Školení bylo zaměřeno právě na problematiku phishingových útoků a v jeho průběhu byly zaměstnancům prezentovány různé druhy a podoby phishingových útoků, kterými si prošla například Česká spořitelna, nemocniční zařízení v Benešově nebo Brně. Byly rovněž zmíněny a prezentovány markanty, které by mohly být vodítkem pro to, aby si člověk uvědomil, že by se v daném případě mohlo jednat o podvodné jednání. Nezapomnělo se ani na zmínku o bezpečném přihlašování do firemní sítě, o parametrech silného hesla a jeho zadávání do systému. Zaměstnanci byli rovněž upozorněni, že ani jejich kolegové z IT oddělení by po nich nikdy jejich heslo nevyžadovali. V případě, že by z nějakého důvodu zaměstnanci potřebovali nové přístupové heslo, je to řešeno cestou tzv. self-service, kdy je na žádost uživatele odesláno dočasné heslo do předem ověřeného firemního e-mailu uživatele. Tato služba je přístupná 24 h 7 dnů v týdnu. Na závěr byli zaměstnanci poučeni o tom, že nikomu nemají vyzrazovat své zvolené heslo, zejména je-li jakýmkoliv způsobem žádáno vzdáleným přístupem neznámou osobou, případně se neprodleně obrátit na kolegy z IT oddělení s žádostí o spolupráci.

Tento test společnosti poskytl možnost ověřit si, jaká je “náchylnost” (personální riziko) k social engeneeringu mezi zaměstnanci a externími spolupracujícími osobami. Rovněž si management ověřil, jaký vliv mají prováděná školení na dodržování bezpečnostní politiky pro zaměstnance a jakou míru zodpovědnosti vykazují zaměstnanci v přístupu k bezpečnostní politice.

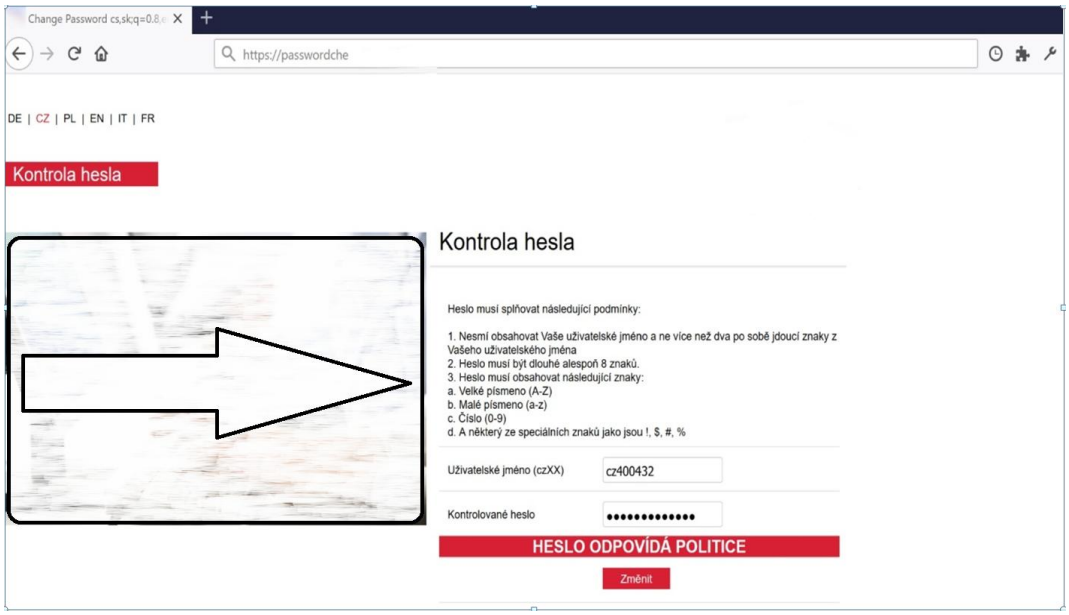
9.1 Popis metody testu

Jako kontrolně-výzkumná metoda byla zvolena rozesílka předem připraveného phishingového e-mailu ve vnitropodnikové síti (intranetu). V e-mailu byl uveden odkaz na fiktivní formulář pro zadání osobních údajů. Formulář byl koncipován tak, aby co nejvěrněji kopíroval vzhled firemního e-mailu a na první pohled se zaměstnancům jevil jako by byl rozeslán z oddělení IT. V začátku textu předmětného formuláře byla zmíněna doba, kterou má zaměstnanec určenou pro "kontrolu hesla". Poté se e-mail druhou větou snaží vzbudit důvěru navozením pocitu, že se IT oddělení stará o jejich bezpečnost, a z toho důvodu je kontaktovalo. Dále následují věty, které byly napsány s nejasnou formulací a gramatickými chybami tak, aby zaměstnancům vyslaly signál, že není vše úplně v pořádku. Věta s fontem "**bold**" a s použitím velkého písma už měla jasné varovné sdělení s tím, že pokud zaměstnanec nenastaví heslo dle nových parametrů, bude mu po vypršení lhůty zablokován přístup. Jasně a zřetelně je mu touto cestou sdělováno, že "nemá jinou volbu", byl použit psychologický nátlak a uživatel je nepřímo tlačen k rozhodnutí jednat. Následuje věta, která dotyčného vyzývá a nutí k tomu, aby s kontrolou neotálel a provedl ji, pokud možno, hned. To vše bylo sestavováno s cílem vytvořit na uživatele tlak, aby nevěnoval tolik pozornosti zaslanému formuláři. V takovém případě se předpokládalo, že uživatel bude chtít mít celou akci rychle splněnou a rutinně bude klikat podle návodu a ztratí ostražitost.

V případě, že uživatel klikl na odkaz pro kontrolu hesla, byl přesměrován na druhý připravený formulář, který byl již bez gramatických chyb a s jasnými instrukcemi pro zadání hesla. Bylo zvoleno jedno, ne zcela vhodné slovo, a to "POLITICE" místo "PARAMETRŮM". Pokud bylo heslo zadáno správně a systémem vyhodnoceno jako vyhovující, byl uživatel ujištěn o správném nastavení hesla zprávou v červeném poli: "HESLO ODPOVÍDÁ POLITICE". Nutno podotknout, že po grafické stránce byl phishingový e-mail shodný s originální verzí e-mailu, který je ve firmě běžně používán. Ovšem záměrně obsahoval nejasné formulace vět, nevhodný pořádek slov ve větě, nespisovná nebo chybějící slova. Při větší nepozornosti obeslaných uživatelů se tyto zjevné markanty daly skutečně přehlédnout, ovšem u pozorného čtenáře by takové znění e-mailu mělo vzbudit minimálně podezření, a v takovém případě se očekávalo, že osoba bude kontaktovat oddělení IT s žádostí o vysvětlení.



Obrázek 10 *– Ukázka podvodného e-mailu s odkazem na kontrolu hesla*



Obrázek 11 *– Ukázka podvodného formuláře pro zadání osobních údajů*

10 VÝSLEDKY

Hlavním cílem provedeného awarness testu bylo zjistit kolik zaměstnanců vybrané společnosti podlehne simulovanému phishingovému útoku. Vedlejším cílem bylo sledování chování a reakcí dotčených osob na tento phishingový e-mail, respektive, zda se s žádostí o informace nebo pomoc obrátí na IT oddělení nebo jejich nadřízené. V této souvislosti se sledovalo i chování a reakce zaměstnanců IT oddělení při zachycení indícií o pokusu infiltrace do sítě. Zároveň se sledovala jejich komunikace se zaměstnanci a externími spolupracovníky, v případě, že se tyto osoby na IT oddělení obrátí s žádostí o informace nebo pomoc.

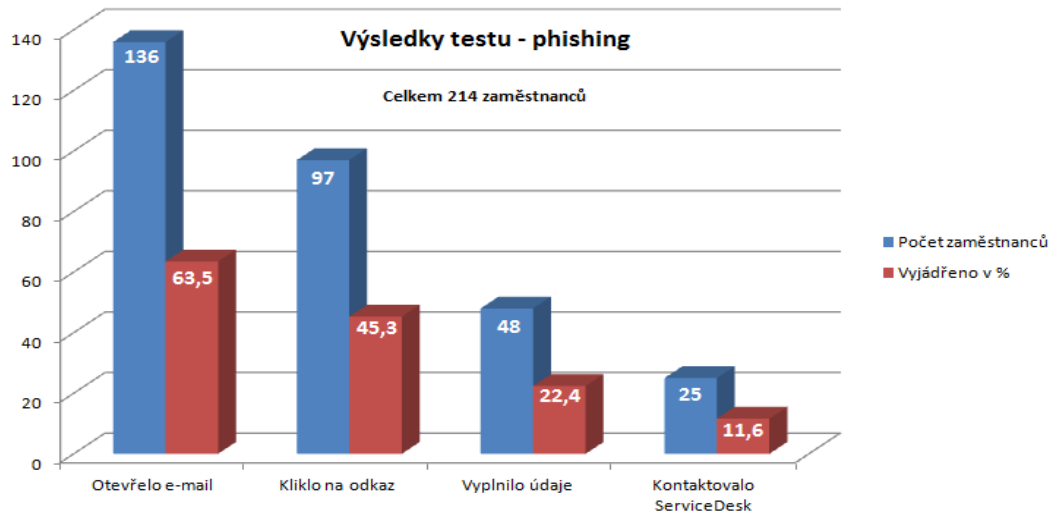
Systémově se sledovalo:

a) kolik osob doručený e-mail otevře k přečtení,

b) kolik osob kliknutím na odkaz v e-mailu otevře podvrženou stránku,

c) kolik osob vyplní citlivé údaje,

d) kolik osob kontaktuje oddělení ServiceDesk.



Graf 10 *– Vyhodnocení testu*

Při vyhodnocení reakcí zaměstnanců IT oddělení po obdržení vzorku spear phishingového e-mailu jsme došli k závěru, že tito zareagovali podle očekávání a správně určili, že se jedná o podvodný e-mail a zahájili hloubkový scan sítě, aby se pokusili najít stopy po jejím případném nestandardním chování a započali kroky

k eliminaci hrozících škod. Rovněž ihned informovali své nadřízené a v tuto chvíli byli zastaveni vedoucím pracovníkem oddělení IT, který je informoval o celém pozadí testu.

Podle našeho názoru, **výsledek testu potvrdil hypotézu**, že selhání lidského faktoru je skutečně tím nejslabším článkem řetězu v oblasti kyberbezpečnosti a má **významný vliv na selhání systémové ochrany informací a bezpečnost kyberprostoru**. V našem názoru nás podpořil i vedoucí pracovník IT, pro něhož výsledek testu nebyl až tak překvapivým, protože nikterak nevybočoval z výsledků, které vzhledem k jeho dosavadní dlouholeté praxi v IT viděl.

Opět musíme zopakovat, že největším rizikem v řetězci bezpečnosti je selhání člověka, tedy jím způsobená chyba, úmyslná nebo neúmyslná. Úmyslné chybě se nedá zabránit, ale ty neumyslné můžeme potlačit správným nastavením celého systému, soustavnou edukací a trénováním všech uživatelů systému. Ani nejlépe chráněný systém s perfektně nastavenou segregací přístupu do systému na principu need-to-know, nedokáže eliminovat riziko úmyslného škodlivého jednání, tzv. fraudu.

Základem pro řešení problémů, které by mohly být generovány uživateli v oblasti kybernetické bezpečnosti je edukace i v oblasti informační bezpečnosti. Tou rozumíme ochranu informací ve všech jejich podobách a po celou dobu jejich životního cyklu a neodmyslitelně jde ruku v ruce s počítačovou gramotností, kterou se z obecného pohledu myslí způsobilost k ovládání a využívání osobního počítače. Aby se do budoucna zlepšila situace v oblasti kybernetické bezpečnosti a informační bezpečnosti u této společnosti, rozhodl se management posílit vzdělávání svých zaměstnanců v těchto oblastech a klást na to patřičný důraz.

Vzhledem k tomu, že výsledek testu nedopadl na požadované úrovni, nebyl vysloven souhlas od vedení společnosti ke zveřejnění obchodního názvu společnosti, nicméně k prezentování výsledků pod rouškou anonymity ano.

11 DISKUZE

11.1 Přijatá opatření v rámci společnosti

Jak bylo zmíněno v předchozí kapitole, provedeným testem a jeho následným vyhodnocením se potvrdila hypotéza, že nejslabším článkem v řetězci ochrany informačního systému je v tomto případě člověk. Toto zjištění je v souladu se závěrem, který je uveden v dokumentu Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2020, kterou vypracoval NÚKIB. V této zprávě se uvádí, že nejslabším článkem kybernetické bezpečnosti bývají lidé [88]. Ačkoliv byli zaměstnanci před útokem školeni v dané problematice, přesto nadpoloviční většina zaměstnanců zaslaný phishingový mail otevřela a požadované údaje sdělila.

Po diskuzi s vedením společnosti o výsledcích provedeného testu se management rozhodl, vyčlenit 1 zaměstnance z oddělení IT, který se bude věnovat edukaci se zaměřením na bezpečné chování v kyberprostoru. Oddělení IT dostalo za úkol vypracovat roční plán vzdělávání, který bude rozdělen na jednotlivá čtvrtletí a každé čtvrtletí bude obsahovat 2 témata týkající se problematiky kybernetické a informační bezpečnosti podle kterých budou provedena on-line školení formou powerpointové prezentace. Aby se ověřila funkčnost tohoto systému vzdělávání, 2× v roce si zaměstnanci projdou on-line testem zaměřeným na zmíněné problematiky. Do on-line školení budou rovněž zahrnuty informace o aktuálních rizicích a zásadách v oblasti kybernetické a informační bezpečnosti, které budou prezentovány prostřednictvím powerpointové prezentace. 1× za 2 měsíce vyčleněný IT specialista rozešle zaměstnancům krátký report o aktuálním dění a hrozbách v oblasti kyberbezpečnosti s doporučením čemu věnovat zvýšenou pozornost a jakému rizikovému chování se v oblasti kyberbezpečnosti vyhnout.

Při pracovních poradách bude určený zástupce oddělení IT informovat vedení společnosti o aktuálním stavu edukace a výsledcích uskutečněných testů. Bylo stanoveno, že podobný typ testu bude prováděn min. 2× ročně. Vedení společnosti toto zjištění vzalo zcela vážně a plně si uvědomilo, že bezpečnosti dat je potřeba věnovat mimořádnou pozornost.

11.2 Doporučení pro infrastrukturu

Aby byla zachována maximální možná ochrana sítě a dat, měli by administrátoři respektovat několik následujících doporučení, která vycházejí z několikaletých praktických zkušeností NÚKIB:

a) rozdělit síť na menší celky a nastavit uživatelská práva odpovídající stanovené hierarchii, za účelem oddělení citlivých informací a kritických služeb a vytvoření zón s různou bezpečnostní úrovní s odpovídajícími bezpečnostními omezeními,

b) sledovat síťový provoz určenými síťovými prvky mezi servery a klienty, komunikaci směrem do internetu, na perimetru sítě a vzájemnou komunikaci mezi servery a tuto komunikaci pak vyhodnocovat a snažit se identifikovat hrozby,

c) uchovávat záznamy o síťovém provozu, a to směrem do, i z kritickým pracovních stanic/serverů, a rovněž i provoz jdoucí za perimetr sítě, z důvodu dohledávání neoprávněného průniku do systémů a sítě,

d) instalovat systémy detekce a prevence průniku (IDS/IPS) sloužící k identifikaci anomálií v provozu systémů a sítě, ale i v komunikaci mezi prostředky za perimetrem sítě,

e) blokovat podezřelé domény a IP adresy na úrovni brány a vytvářet pro tyto účely tzv. blacklisty, čímž se eliminuje hrozba již v počátku,

f) pro domény společnosti volit jednoduché názvy, aby bylo jasně na první pohled vidět, zda s názvem domény bylo manipulováno (volžená nebo jinak pozměněná sada písmen) v případech phishingového útoku,

g) kontrolovat příchozí i odchozí elektronickou poštu a blokovat podezřelé nebo podvržené zprávy za pomoci nástrojů Sender ID, Sender Policy Framework, Domain Keys Identified Mail, Domain Based Message Authentication apod.,

h) šifrovat spojení mezi mail servery a kontrolovat obsah zpráv po jejich dešifrování, k takovému účelu lze využít nástroj DNS Based Authentication of Named Entities,

ch) implementovat automatizovanou dynamickou analýzu obsahu e-mailů a webů, která se spustí v sandboxu za účelem nalezení podezřelých aktivit ukazující na úpravy

v uložených souborech, nově vznikající soubory, změny ve stávajících konfiguracích apod.,

i) kontrolovat certifikáty a elektronické klíče pro SSH autentizaci, která zabezpečuje šifrování dat při přenosu v síti, šifrovanou komunikaci používat pokud možno všude tam, kde je to relevantní,

j) zpracovat plán obnovy sítě ze zálohy pro případ jejího destruktivního napadení z vnějšího perimetru, tzv. "disaster recovery plan – DRP", ve kterém budou mimo jiné uvedeny telefonní a mailové kontakty na ostatní administrátory, management společnosti a CERT/CISRT podpůrné týmy,

k) do systému implikovat anti-DDoS technologie pokrývající celou škálu rozsahu IP adres společnosti, které pomohou s analýzou projevu kybernetického útoku nebo poskytnou cenná data pro poskytovatele internetového připojení [89].

11.3 Doporučení pro stanice a servery

I u pracovních stanic nebo serverů platí zásady pro zachování bezpečnosti provozu a to zejména:

a) instalovat a provozovat pouze legální a aktualizovaný operační systém, jelikož aktualizace zabezpečí implementaci nejnovějších bezpečnostních záplat proti zranitelnostem, ten samý přístup platí i pro pro provozovaný software a firmware,

b) instalovat bezpečnostní a antivirové programy, které sledují a analyzují systém a zabraňují spouštění nebezpečných aplikací vyjma aplikací s jasně udělenými výsadami,

c) instalovat servery a pracovní stanice podle předem stanovených a nastavených konfigurací (SOE – Standard Operating Enviroment), ve kterých budou zapnuty jen ty funkcionality, které jsou nutné pro správné fungování,

d) ověřovat identitu souborů a aplikací, po ověření identity je povolena činnost jen důvěryhodným souborům včetně skriptů, DLL knihoven apod.) a jen rozsahu udělených oprávnění, v prostředí Windows je lze použít aplikace Device Guard nebo AppLocker,

e) kontrolovat obsah e-mailů se zaměřením na nebezpečné druhy elektronických příloh, hloubkové analýze zasílaných souborů e-mailem, nastavit povolení pouze pro takové formáty příloh, které jsou v rámci společnosti využívány, ostatní formáty příloh zablokovat, rovněž kontrolovat označení přípony souboru s jeho skutečným formátem,

f) kontrolovat přenosná média, kterým se v systému povolí připojení přes preferovaný vstup instalovaný ve stanici a následně monitorovat interakci mezi přenosným médiem, stanicí a sítí, nastavit podmínky pro jejich evidenci, ukládání, mazání nebo likvidaci,

g) využívat kryptografický software (TPM – Trusted Platform Module) pro tvorbu a ukládání hesel, ale i kryptografických klíčů, šifrovat i pevné disky včetně centrální evidence klíčů,

h) nastavit unikátní heslo pro každou provozovanou stanici v BIOSu (Basic Input Output System) nebo v UEFI (Unified Extensible Firmware Interface) pokud je provozována centrální správa hesel,

ch) využívat ke spouštění operačního systému funkci Secure Boot (moderní PC s UEFI), která při spouštění operačního systému ověřuje, že všechny nezbytné systémové soubory jsou opatřeny digitálním podpisem a jsou v nezměněném stavu, tzn. že nedojde ke spuštění podvrženého zavaděče škodlivého sofwaru (mallware),

i) zálohovat veškerá důležitá data mimo provozovanou síť, systémové databáze, konfigurace spouštěných služeb, obsah webového rozhraní, zálohovaná data testovat z pohledu funkčnosti obnovy,

j) implementovat proces hardeningu konfigurace aplikací umístěných na serveru, jako personální databáze (HR database), zákaznická databáze (CRM database), účetní systémy apod., tento systém zvyšování bezpečnosti je založen na analýze a kontrole aktualizací systému, bezpečnostních politik (management, vyhodnocování, audit, aktualizace, dodržování), nastavených procesů a technických předpisů, implementaci nástroje automatizované kontroly nastavení systému apod.,

k) implementovat proces hardeningu uživatelských aplikací, povolováním jen té funkcionality, která je nezbytná pro bezproblémovou práci uživatelů, další funkce povolovat pouze je-li to nezbytné (makra sady MS Office, Java, Flash atd.),

l) implementovat systém pro detekci a prevenci průniku (IPS – Intrusion Prevention Systems), který monitoruje jak provoz na síti, tak i aktivity operačního systému, které by mohly vést k narušení bezpečnosti, systém je implementován přímo do síťové cesty, proto může aktivně blokovat identifikovaný nebezpečný nebo nežádoucí provoz na síti (načítání neverifikovaných ovladačů, detekce aktivity klávesnice, pokusy o změnu systémových registrů apod.,

m) využívat přístup chráněného režimu virtuální paměti při nakládání se soubory pracovních stanic, za využití módu Protected Mode, čímž se zamezí tomu, aby spuštěný software zasahoval do jiných procesů nebo do jádra systému, než je mu dovoleno, tím nedochází ke vzájemnému ovlivňování spuštěných úloh, úlohy běží v režimu multitasking,

n) připojovat se přes VPN (Virtual Private Network) z důvodu zabezpečeného šifrovaného spojení mezi uživatelem a sítí nebo mezi sítěmi a i nadále kontrolovat, zda nedochází k přesměrování připojení mimo síť společnosti,

o) nastavit podmínky pro fyzickou bezpečnost provozovaných stanic [90].

11.4 Doporučení pro správu účtů

Z důvodu kontroly a dohledatelnosti pohybu ve firemní síti je nutné každému účastníku přidělit jeho vlastní účet s přednastavenými oprávněními. Pro administraci účtů uvádíme několik doporučení:

a) aplikovat centrální správu uživatelských účtů a jejich oprávnění, nastavit jednotnou bezpečnostní politiku, účtům u kterých to není potřeba odbrat některá oprávnění, zakázat úpravu registrů, spouštění skriptů nebo instalaci softwaru atd.,

b) pro správu jednotlivých systémů přidělit každému administrátorovi unikátní heslo k jeho účtu a nesdílet účty,

c) každé lokální stanici přidělit heslo, pod OS Windows lze použít LAPS (Local Administrator Password Solution),

d) pro běžné pracovní aktivity používat neprivilegovaný účet, pro správu domén vytvořit privilegovaný účet doménového administrátora, ale s tímto účtem nepřistupovat na klientské stanice nebo servery,

e) pravidelně kontrolovat oprávnění u lokálních, ale i centrálně spravovaných uživatelských účtů,

f) používat silná hesla, která se nebudou opakovat, vynucovat změnu hesel v pravidelných intervalech,

g) v případě správy akcí, které jsou privilegovány, mají vyšší úroveň oprávnění nebo se jedná o kritické operace (přístup k citlivým údajům, vzálený přístup apod.) vyžadovat vícefaktorovou autentizaci [91].

11.5 Doporučení pro správu e-mailové ochrany

Pro zabezpečení e-mailových klientů proti spamu, phishingu, spoofingu, malwaru atd. lze využít nástroj DMARC (Domain-based Message Authentication Reporting and Conformance), který na základě nastavených TXT záznamů v DNS provede ověření platnosti, tedy validity e-mailu a umožňuje tak uživateli domény zabezpečit jeho elektronickou komunikaci a daleko lépe jej chrání před elektronickou poštou, která cílí na zneužití jeho domény. Pro správné fungování celého nástroje, je nutné nejdříve nastavit záznam SPF (Sender Policy Framework) a DKIM (Domain Keys Identified Mail). Nástroj DMARC kontroluje a v rámci nastavených parametrů porovnává:

- SPF alignment (shodnost domén odesílatele a obálkového odesílatele v SMTP komunikaci) – jedná se o nástroj, který se ověřuje platnost elektronické pošty a slouží jako ochrana proti spamu. Poštovní server ověří odchozí IP adresu elektronické zprávy srovnáním se seznamem serverů, které jsou autorizovány k odesílání elektronických zpráv z domény odesílatele a jsou zveřejněny ve speciálním DNS záznamu (pro bezproblémový chod, zde musí být zahrnuty všechny servery, které z domény uživatele elektronickou poštu odesílají).

- DKIM aligment (shodnost domény uvedené v DKIM podpisu s doménou odesílatele uvedenou v hlavičce zprávy) – jedná se o metodu, která ověřuje zda nedošlo k pozměnění elektronické zprávy při cestě mezi odesílatelem

a příjemcem. Před odesláním eletkronické zprávy je tato opatřena DKIM podpisem, pokud je zpráva označena za ověřenou, potvrzuje, že je odeslána autoritou, která má právo doménu používat. Zpráva může být útočníkem přečtena, ovšem nemůže ji nijak pozměnit ani podvrhnout.

Přednost nástroje DMARC spočívá v tom, že:

- je zde vysoká pravděpodobnost nedoručení falešných (podvodných) e-mailů do schránky nebo do spam koše, protože pokud není e-mail ověřen (validován), je automaticky vyřazen a to díky nástroji SPF,
- je pod kontrolou seznam povolených poštovních serverů, které mohou posílat e-maily jménem majitele domény,
- pokud je použit DKIM nemůže být manipulováno s obsahem zaslaného e-mailu [92].

Zavedení nástroje DMARC umožňuje chránit doménu před neoprávněným použitím. DMARC je rovněž účinnou ochranou před podvodnými e-maily typu BEC (Business Email Compromise), známými též jako Man-in-the-Email, kdy útočníci využívají technik sociálního inženýrství, aby oklamali nic netušící zaměstnance různých společností. Při těchto pokusech prostřednictvím e-mailu se nejčastěji pokouší vydávat za generálního ředitele společnosti nebo jinou vysoce postavenou osobu z managementu společnosti. Útočníci umí věrně napodobit vzhled e-mailu, který se běžně používá pro komunikaci ve společnosti a tento e-mail se i jeví, jakoby přišel z e-mailové adresy např. generálního ředitele. Účelem těchto e-mailů je přimět pečlivě vytipovanou osobu, nejčastěji s oprávněním pro finanční operace k převodu finančních prostředků na útočníkův účet. Protože tyto podvodné e-maily neobsahují žádné škodlivé odkazy nebo přílohy, mohou se útočníci vyhnout dohledání podle zanechaným digitálních stop [93].

Výše zmíněná opatření neochrání síť a připojené prostředky na 100 %, ale významě sníží rizika hrozeb pro síť. Po implementaci těchto bezpečnostních opatření se bude síť snáze spravovat, chránit před neoprávněným vniknutním, sledovat její provoz a data, která jsou po síti transportována. Získané přehledy o provozu sítě poslouží pro hloubkovou analýzu provozu a odhalení případných zranitelností, které je potřeba eliminovat.

12 ZÁVĚR

Před trestnými činy páchanými v kyberprostoru není v plné míře chráněn žádný stát. Útoků v kyberprostoru stále přibývá a útoky směřují nejen na soukromé společnosti, ale i proti státním a vzdělávacím institucím, které fungují v kyberprostoru, zejména to jsou odvětví kritické infrastruktury jako energetika, doprava, průmysl, finance, zdravotnictví apod. Díky digitální transformaci v celosvětovém měřítku se nejen tato odvětví stávají stále závislejšími na digitálních technologiích. S rostoucí implementací digitálních nástrojů roste i množství vytvořených dat. Světová banka odhaduje, že do konnce roku 2022 se celkový internetový provoz zvýší asi o 50 % oproti úrovni z roku 2020 a dosáhne objemu dat 4,8 zettabytů. Pokud byste na nosiče DVD uložili 4,8 zettabytů, stoh těchto nosičů by šestkrát omotal Zemi [94]. Můžeme říci, že na digitálních technologiích stojí a padá národní hospodářství, ale i lidská společnost. V krizovém období COVID–19 se to potvrdilo. Dozvuky této krize přetrvávají i dnes, zejména v důsledku výpadků průmyslové výroby (např. nedostatek čipů pro automobilový průmysl).

Zdá se, že preventivní opatření určená ke kontrole internetové kriminality nejsou dostatečná. Mladší generace se již zásadám bezpečného užívání internetu učí rychleji, ovšem někdy až z vlastních chyb. V důsledku prostupování internetu do života lidí bude nutné začít s osvětou už v útlém věku. Doposud si mnoho lidí neuvědomuje, jak nebezpečno může být v kyberprostoru. Vzpomeňme např. problém kyberšikany, který způsobuje nemalé problémy např. v životě žactva, ale i pedagogického sboru.

Tehdejší séf společnosti Google Eric Schmidt v roce 2013 prohlásil, že každý člověk na planetě bude připojen k internetu do roku 2020 [95]. Tato predikce se nevyplnila. V roce 2015 byl Eric Schmidt tázán na budoucnost internetu a na otázku odpověděl: *"Odpovím velice jednoduše, a sice že internet zmizí, ...bude zde velké množství IP adres, ...mnoho zařízení, senzorů, věcí které nosíte, věcí se kterými komunikujete a ani o tom nevíte"* [96]. Mýlil se v jedné věci, internet nezmizel, a jak se zdá, ani nezmizí. Pomalu, ale jistě svěřujeme své životy a identitu zařízením napojených na kyberprostor. Dobrovolně se vzdáváme uvažování a rozhodování ve prospěch virtuálního světa. Eric Schmidt dále poznamenává, že internet bude součástí přítomnosti každého jedince a vyvstane tak velmi personalizovaný, vysoce interaktivní a velmi, velmi zajímavý svět.

Proto je v nejvyšším zájmu České republiky, aby neustále posilovala zabezpečení a odolnost síťové infrastruktury a implementovaných ICT prostředků do těchto sítí. Zároveň musí zkvalitňovat procesy bezpečnostních standardů v IT systémech, které provozuje veřejná správa.

Neméně důležité je neustálé kvalitní proškolování zaměstnanců v oblasti bezpečnosti KIS (komunikačních a informačních systémů), a také zabezpečení kvalitního a vzdělaného personálu, který se stará o funkčnost infromačních a komunikačních systémů a ICT prostředků. Jedině tak je možné minimalizovat hrozící rizika a úspěšně čelit kybernetickým útokům např. spear phishingu. Doba se mění a jednotlivé státy mezi sebou nevedou otevřené konflikty na bojištích, ale v kyberprostoru (např. špionáž, defamace, dezinterpretace apod.)

Mezi nejaktivnější kyberšpionážní kampaně patřila ruská kampaň APT28/Sofacy. Ta necílila jen na data samotná, ale s velkou intenzitou se zaměřuje na krádeže osobních údajů a přihlašovacích údajů do informačních a komunikačních systémů, které mohou být dále využity k pozdějším sofistikovaným spear phishingovým útokům. APT28/Sofacy využívala k útokům proti českým cílům zahraniční počítačovou infrastrukturu (botnety). V souvislosti s touto kampaní bylo odhaleno několik útoků proti českým vojenským cílům, z nichž k nejzávažnějším patřily kompromitace několika soukromých emailových účtů patřících osobám spojeným s Ministerstvem obrany, Armádou ČR a kompromitace IP adresy patřící MO ČR/AČR malwarem známým pod názvem X–Agent. Ačkoliv útočníci tímto útokem s nejvyšší pravděpodobností nezískali žádné utajované informace, získali řadu osobních informací a citlivých údajů, které mohou být dále zneužity pro další útoky či nelegitimní aktivity. Vlna spear phishingových emailů cílila především na osoby z oblasti vojenské diplomacie a zbrojařské společnosti působící v Evropě [97].

Nacházíme se v době, kdy je velmi těžké rozeznat co je pravda, polopravda nebo lež. S informacemi se manipuluje a kupčí, některé státy si platí hackery, aby páchali zlo a tím financovali státní kasy (Severní Korea) [98], velké společnosti si objednávají kyber útoky na konkureci, zakládají se falešné digitální identity a ty pravé se kradou. Zodpovědný přístup jednotlivce, ale i jednotlivých států k otázce bezpečnosti kyberprostoru začíná u osvěty, vzdělání a končí u uvědomění si, že jednoznačnou prioritu v kyberprostoru musí být bezpečnost a ochrana dat.

11. SEZNAM POUŽITÝCH ZKRATEK

AES – Advanced Encryption Standard

AI – Artificial Inteligence

ARPANET – Advanced Research Projects Agency NETwork

BEC – Business Email Compromise

BGP – Border Gateway Protocol

CCMP – Counter Cipher Mode with Block Chaining Message Authentication Code Protocol

CERT – Computer Emergency Response Team

CIRC – Computer Incident Response Capability

CIS – Center for Internet Security

CPU – Central Processing Unit

DARPA – Defense Advanced Research Projects Agency

DDoS – Distributed Denial of Service

DKIM – Domain Keys Identified Mail

DNS – Domain Name System

DMARC – Domain-based Message Authentication Reporting and Conformance

DoS – Denial of Service

EDR – Endpoint Detection and Response

GPS – Global Position System

HHD – Hard Drive Disk

HTTP – Hypertext Transfer Protocol

HTTPS –HTTP Secure

ICT – Information and Communication Technologies

IDS/IPS – Intrusion Detection System/Intrusion Prevention System

IEEE – Institute of Electrical and Electronics Engineers

IKT – informační a komunikační technologie (ekvivalent k ICT)

INTERPOL – International Criminal Police Organization

IoT – Internet of Things

IP – Internet Protokolu

ISMS – Information Security Management System

ISO/OSI – Inernational Standards Organization/Open System Interconnection

IT – Information Technologies

ITIL – Information Technology Infrastructure Library

KII – kritická informační infrastruktura

KIS – komunikační a informační systémy

LAPS – Local Administrator Password Solution

LTE – Long Term Evolution

MO – Ministerstvo obrany ČR

NAKIT – Národní agentura pro komunikační a informační technologie

NBÚ – Národní bezpečnostní úřad

NCKB – Národní centrum kybernetické bezpečnosti

NCP – Network Control Program

NIST – National Institute of Standards and Technology

NSFNET – National Foundation Network

NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost

OČTŘ – orgány činné v trestním řízení

PRS – Public Regulated Service

RAM – Random Access Memory

RTHB – Remotely Triggered Black Hole

SMTP – Simple Mail Transfer Protocol

SOE – Standard Operating Enviroment

SPF – Sender Policy Framework

SSID – Service Set Identifier

TCP/IP – Transmission Control Protocol/Internet Protocol

TPM – Trusted Platform Module

UEFI – Unified Extensible Firmware Interface

VoIP – Voice over Internet Protocol

VPN – Virtual Private Network

12. SEZNAM POUŽITÉ LITERATURY

1. ZAHARIA, Andra. *300+ Terrifying Cybercrime and Cybersecurity Statistics (2022 EDITION)* [online]. February 22, 2022 [cit. 2021-03-25]. Dostupné z: https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/

2. MAYER, Marco, Luigi MARTINO, Pablo MAZURIER a Gergana TZVETKOVA. *How would you define Cyberspace?* [online]. Akademia.edu, 2014 [cit. 2021-11-25]. Dostupné z: https://www.academia.edu/7096442/How_would_you_define_Cyberspace

3. Information and Communications Technology (ICT): Techopedia Explains Information and Communications Technology (ICT). *Techopedia.com: Dictionary* [online]. August 18, 2020 [cit. 2021-11-27]. Dostupné z: https://www.techopedia.com/definition/24152/information-and-communications-technology-ict

4. DYTRT, Z., MIKULECKÝ, P., NEJEZCHLEBA, M., PRILLWITZ, G., ROUDNÝ, R. (editoři): *Etika podnikání a veřejné správy: Informační společnost – etická výzva pro 21. století*. Sborník z 2. mezinárodní konference, Hradec Králové, 18. – 20. 5. 1999, Vyd. VUSTE ENVIS Praha, 1999. ISBN 80–902356–5–4.

5. ZLATUŠKA, P. *Informační společnost*. Zpravodaj ÚVT MU. ISSN 1212–0901, 1998, roč. VIII, č. 4, [online]. [cit. 2021-11-27]. Dostupné z: http://webserver.ics.muni.cz/bulletin/articles/122.html

6. BUSCH, Vannevar. *AS WE MAY THINK*. In: Theatlantic.com [online]. Washington, D. C.: The Atlantic, JULY 1945 [cit. 2021-11-28]. Dostupné z: https://www.theatlantic.com/magazine/archive/1945/07/as-we-may-think/303881/

7. DARPA. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 8. 3. 2022 v 01:33 [cit. 2021-11-28]. Dostupné z: https://cs.wikipedia.org/wiki/DARPA

8. BARTOŠEK, M. *Krátce z historie Internetu* [online]. Zpravodaj ÚVT MU, 1995, roč. V, č. 3, [cit. 2021-11-28]. ISSN 1212-0901. Dostupné z: http://webserver.ics.muni.cz/bulletin/articles/22.html

9. ARPANET. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 19. 12. 2021 v 20:00 [cit. 2021-11-28]. Dostupné z: https://cs.wikipedia.org/wiki/ARPANET

10. *FNC Resolution: Definition of "Internet"* [online]. Federal Networking Council (FNC) October 24, 1995. [cit. 2021-12-02]. Dostupné z: https://www.nitrd.gov/historical/fnc/internet_res.pdf

11. JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník Kybernetické bezpečnosti: Cyber Security Glossary* [online]. 3. aktualizované vydání. Praha: PA ČR a

česká pobočka AFCEA, 2015 [cit. 2021-12-02]. ISBN 978-80-7251-436-6. Dostupné z: https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/podpurne-materialy/

12. MCCULLOUGH, Brian. *How the Internet happened: from Netscape to the iPhone*. New York: Liveright Publishing Corporation, 2018. ISBN 978-1631493072.

13. BARTOŠEK, M. *Krátce z historie Internetu* [online]. Zpravodaj ÚVT MU, 1995, roč. V, č. 3 [cit. 2021-12-02]. ISSN 1212-0901. Dostupné z: http://webserver.ics.muni.cz/bulletin/articles/22.html

14. *INFORMAČNÍ SPOLEČNOST V ČÍSLECH 2021: ČESKÁ REPUBLIKA A EU* [online]. Praha: Český statistický úřad, © březen 2021 [cit. 2021-12-15]. ISBN 978-80-250-3083-7. Dostupné z: https://www.czso.cz/documents/10180/143060187/06100421.pdf/e115d5fc-ea3f-4c4e-a4fd-e789648e6615?version=1.14

15. *INFORMAČNÍ SPOLEČNOST V ČÍSLECH 2021: ČESKÁ REPUBLIKA A EU* [online]. 1. Praha: Český statistický úřad, © březen 2021 [cit. 2021-12-15]. ISBN 978-80-250-3083-7. Dostupné z: https://www.czso.cz/documents/10180/143060187/06100421.pdf/e115d5fc-ea3f-4c4e-a4fd-e789648e6615?version=1.14

16. *INFORMAČNÍ SPOLEČNOST V ČÍSLECH 2021: ČESKÁ REPUBLIKA A EU* [online]. 1. Praha: Český statistický úřad, © březen 2021 [cit. 2021-12-18]. ISBN 978-80-250-3083-7. Dostupné z: https://www.czso.cz/documents/10180/143060187/06100421.pdf/e115d5fc-ea3f-4c4e-a4fd-e789648e6615?version=1.14

17. WALLACE, P. *The Psychology of the Internet*. Cambridge: Cambridge University Press, 2001. ISBN 0521797098

18. *INFORMAČNÍ SPOLEČNOST V ČÍSLECH 2021: ČESKÁ REPUBLIKA A EU* [online]. 1. Praha: Český statistický úřad, © březen 2021 [cit. 2021-12-28]. ISBN 978-80-250-3083-7. Dostupné z: https://www.czso.cz/documents/10180/143060187/06100421.pdf/e115d5fc-ea3f-4c4e-a4fd-e789648e6615?version=1.14

19. HILLSTROM, Kevin. *The Internet Revolution (Defining Moments)*. Detroit: Omnigrafics, August 30, 2005. ISBN 978-0780807679.

20. HOLANOVÁ, Tereza. *Nová průmyslová revoluce. Nezaspěte nástup Práce 4.0*. Aktuálně.cz [online]. 2015–07–29 [cit. 2021-12-29] Dostupné z: https://zpravy.aktualne.cz/ekonomika/nova–prumyslova–revoluce–nezaspete–nastup–prace–40/r~97fa2490353311e593f4002590604f2e/?redirected=1550521689

21. LATIFF, Robert H. *Války budoucnosti: Příprava na nové globální bojiště*. CPress, 2018. ISBN 978-80-264-2138-2.

22. ČESKÁ REPUBLIKA. Zákon č. 181/2014 Sb.: zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: Sbírka zákonů. 2014, částka 75, číslo 181. Dostupné také z: https://www.zakonyprolidi.cz/cs/2014-181/zneni-20210901

23. ČESKÁ REPUBLIKA. Vyhláška č. 82/2018 Sb.: vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti). In: *Sbírka zákonů*. 2018, částka 43, číslo 82. Dostupné také z: https://www.zakonyprolidi.cz/cs/2018-82

24. ČESKÁ REPUBLIKA. Zákon č. 181/2014 Sb.: zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: Sbírka zákonů. 2014, částka 75, číslo 181. Dostupné také z: https://www.zakonyprolidi.cz/cs/2014-181/zneni-20210901

25. O úřadu. *Nukib.cz* [online]. Brno: Národní úřad pro kybernetickou a informační bezpečnost [cit. 2021-12-29]. Dostupné z: https://www.nukib.cz/cs/o-nukib/o-uradu/

26. Organizační struktura úřadu. *Nukib.cz* [online]. Brno: Národní úřad pro kybernetickou a informační bezpečnost [cit. 2021-12-29]. Dostupné z: https://www.nukib.cz/cs/o-nukib/organizacni-struktura-uradu/

27. ČESKÁ REPUBLIKA. Zákon č. 181/2014 Sb.: zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: Sbírka zákonů. 2014, částka 75, číslo 181. Dostupné také z: https://www.zakonyprolidi.cz/cs/2014-181/zneni-20210901

28. Kybernetická bezpečnost. *Nukib.cz* [online]. Brno: Národní úřad pro kybernetickou a informační bezpečnost [cit. 2021-12-30]. Dostupné z: https://www.nukib.cz/cs/kyberneticka-bezpecnost/

29. Národní centrum kybernetické bezpečnosti. *Govcert.cz* [online]. Brno: Národní úřad pro kybernetickou a informační bezpečnost [cit. 2021-12-29]. Dostupné z: https://www.govcert.cz/cs/vladni-cert/govcert-cz/

30. O nás. Csirt.cz: Služby [online]. Praha: CZ.NIC [cit. 2021-12-30]. Dostupné z: https://www.csirt.cz/cs/o-nas/sluzby/

31. Zpráva o činnosti CSIRT.CZ (národního CSIRT ČR) za rok 2021. In: *Csirt.cz: o nás* [online]. Praha: 2021 [cit. 2022-12-30]. Dostupné z: https://csirt.cz/media/filer_public/b8/97/b897d087-6854-4c69-8e99-3bb90561e6b7/220302_csirt_vyrocni_zprava_2021.pdf

32. O nás. *Circ.army.cz* [online]. Praha: © 2004-2014 Ministerstvo obrany [cit. 2021-12-14]. Dostupné z: http://www.circ.army.cz/o-nas

33. About. *Ncirc.nato.int* [online]. Mons: © 2021 - NCSC [cit. 2021-12-14]. Dostupné z: http://www.ncirc.nato.int/Home/About

34. Služby. *Nakit.cz* [online]. Praha: Národní agentura pro komunikační a informační technologie, s. p. [cit. 2021-12-14]. Dostupné z: https://nakit.cz/sluzby/

35. VÁLKOVÁ, Helena, Josef KUCHTA a Jana HULMÁKOVÁ. *Základy kriminologie a trestní politiky*. 3. vydání. Praha: C.H. Beck, 2019. Beckovy mezioborové učebnice. ISBN 978-80-7400-732-3.

36. VÁLKOVÁ, Helena, Josef KUCHTA a Jana HULMÁKOVÁ. *Základy kriminologie a trestní politiky*. 3. vydání. Praha: C.H. Beck, 2019. Beckovy mezioborové učebnice. ISBN 978-80-7400-732-3.

37. JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník Kybernetické bezpečnosti: Cyber Security Glossary* [online]. 3. aktualizované vydání. Praha: PA ČR a česká pobočka AFCEA, 2015 [cit. 2021-12-15]. ISBN 978-80-7251-436-6. Dostupné z: https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/podpurne-materialy/

38. ŠÁMAL, Pavel et al. *Trestní zákoník*. 2. vydání. Praha: C. H. Beck, 2012. ISBN 978-80-7400-428-5,

39. POLČÁK, Radim a Tomáš GŘIVNA. *Kyberkriminalita a právo*. 1. vyd. Praha: AUDITORIUM, 2008. ISBN 978-80-903786-7-4,

40. Crimes/Cybercrime. *Interpol.int* [online]. © Interpol.int, 2019 [cit. 2021-12-30]. Dostupné z www: https://www.interpol.int/Crimes/Cybercrime,

41. HOLCR, Květoň et al. *Kriminológia*. 1. vydanie. Bratislava: Iura Edition spol s r.o., 2008. ISBN 978-80-8078-206-1,

42. *Základní definice, vztahující se k tématu kybernetické bezpečnosti.* MVCR.CZ. [online]. Praha 2009 [cit. 2022-01-04]. Dostupné z www: http://www.mvcr.cz/soubor/cyber-vyzkum-studie-pojmy-pdf.aspx,

43. KOLOUCH, Jan. *CyberCrime* [online]. Praha: CZ.NIC, z. s. p. o., 2016 [cit. 2022-01-04]. ISBN 978-80-88168-18-8. Dostupné z: https://knihy.nic.cz/files/edice/cybercrime.pdf,

44. GREGUŠOVÁ, D. *Počítačové právo*. Brno: Institut dalšího vzdělávání, 2002. ISBN 80-86629-04-X,

45. VÁLKOVÁ, Helena, Josef KUCHTA a Jana HULMÁKOVÁ. Základy kriminologie a trestní politiky. 3. vydání. Praha: C.H. Beck, 2019. ISBN 978-80-7400-732-3,

46. VÁLKOVÁ, Helena, Josef KUCHTA a Jana HULMÁKOVÁ. Základy kriminologie a trestní politiky. 3. vydání. Praha: C.H. Beck, 2019. ISBN 978-80-7400-732-3,

47. VÁLKOVÁ, Helena, Josef KUCHTA a Jana HULMÁKOVÁ. Základy kriminologie a trestní politiky. 3. vydání. Praha: C.H. Beck, 2019. ISBN 978-80-7400-732-3,

48. Zpráva o stavu kybernetické bezpečnosti české republiky za rok 2020. In: *Nukib.CZ: zprávy o stavu KB* [online]. Brno: 2021 [cit. 2022-01-05]. Dostupné z: https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/zpravy-o-stavu-kb/,

49. Statistiky. In: *Policie.cz* [online]. © 2021 Policie ČR. [cit. 2022-01-05]. Dostupné z: https://www.policie.cz/clanek/policie-cr-web-informacni-servis-statistiky-statisticke-prehledy.aspx,

50. MCCLURE, Stuart, Joel SCAMBRAY a George KURTZ. *Hacking Exposed 7: Network Security Secrets & Solutions*. 7th Edition. New York: McGraw-Hill, 2012. ISBN-13: 978-0-07-178028-5,

51. GOLDSMITH, Jack, WU, Tim. *Kdo řídí internet: Iluze o světě bez hranic*. 1. vydání. Praha: Argo a Dokořán, 2008. ISBN 978-80-7363-184-0,

52. Zpráva o stavu kybernetické bezpečnosti české republiky za rok 2020. In: *Nukib.CZ: zprávy o stavu KB* [online]. Brno: 2021 [cit. 2022-01-05]. Dostupné z: https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/zpravy-o-stavu-kb/,

53. JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník Kybernetické bezpečnosti: Cyber Security Glossary* [online]. 3. aktualizované vydání. Praha: PA ČR a česká pobočka AFCEA, 2015 [cit. 2021-01-06]. ISBN 978-80-7251-436-6. Dostupné z: https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/podpurne-materialy/,

54. EMPEY, Charlotte. Vše, co potřebujete vědět o ransomwaru a jak se před ním ochránit. In: *Avast.com: Rady a tipy* [online]. 1988 - 2022 Copyright © Avast Software, 5 BŘE 2018 [cit. 2022-01-06]. Dostupné z: https://blog.avast.com/cs/co-je-ransomware,

55. Základní definice, vztahující se k tématu kybernetické bezpečnosti. In: *Mvcr.cz*. [online]. Praha: 2009 [cit. 2022-01-04]. Dostupné z www: http://www.mvcr.cz/soubor/cyber-vyzkum-studie-pojmy-pdf.aspx,

56. *Trestní právo: odborný časopis pro trestní právo a obory související* [online]. Praha: Nakladatelství Orac, 2011, **15** (1), 11-20 [cit. 2022-01-07]. ISSN 1211-2860.,

57. KAČIC, Matej. *Analýza útoků na bezdrátové sítě*. Brno, 2017. Disertační práce. Vysoké učení technické v Brně. Fakulta informačních technologií 2017. Ústav inteligentních systémů,

58. GRABOVSKÝ, Štěpán, Vlastimil ČLUPEK, Milan ŠVEHLÁK a Jan KLIMEŠ. *Sítový generátor DoS útoků*. Elektrorevue, 2018, roč. 20, č. 3, 69. ISSN: 1213-1539,

59. OWOKADE, Adeolu. *How to configure Remotely Triggered Black Hole routing to protect from DDOS attacks (with bonus)*. Routerfreak.com [online]. © 2008-2022

RouterFreak [cit. 2022-01-07]. Dostupné z: https://www.routerfreak.com/remotely-triggered-black-hole-routing-ddos-attacks/,

60. *Schéma DDoS útoku*. Ct24.ceskatelevize.cz [online]. © 2019 [cit. 2022-01-10]. Dostupné z: https://ct24.ceskatelevize.cz/sites/default/files/styles/file-video_16x9/public/images/2010118-ddos-attack-ex.jpg?itok=KLq0-WNU,

61. DURAČINSKÁ, Zuzana a Pavel BAŠTA. *DDoS – sofistikovaný útok nebo služba na objednávku?* In: *Nic.cz* [online]. Praha, 24. 5. 2015 [cit. 2022-01-10]. Dostupné z: https://www.nic.cz/files/nic/doc/IT_Security_DDoS_042015.pdf,

62. Vlastní archiv,

63. *Spear-phishing a jak se před ním chránit*. Nukib.CZ, Infoservis, Doporučení [online]. Brno: 9. duben 2020 [cit. 2022-01-11]. Dostupné z: https://www.nukib.cz/cs/infoservis/doporuceni/1514-spear-phishing-a-jak-se-pred-nim-chranit/,

64. Zpráva o stavu kybernetické bezpečnosti české republiky za rok 2020. In: *Nukib.CZ: zprávy o stavu KB* [online]. Brno: 2021 [cit. 2022-01-11]. Dostupné z: https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/zpravy-o-stavu-kb/,

65. *NOVINKY Z BEZPEČNOSTI: není to naše nabídka, ale phishing*. In: Csas.cz: Zprávy z banky [online]. 15 PRO 2021 [cit. 2022-01-15]. Dostupné z: https://www.csas.cz/cs/zpravy-z-banky/2021/12/15/neni-to-nase-nabidka-phishing#,

66. *Varování: vědecké informace v zájmu podvodníků*. CSIRT.MUNI.CZ, Aktuálně [online]. Brno: Masarykova univerzita, 17. 9. 2018 [cit. 2022-01-15]. Dostupné z: https://csirt.muni.cz/about-us/news/phish_sci,

67. ČESKÁ REPUBLIKA. Zákon č. 40/2009 Sb.: trestní zákoník. In: Sbírka zákonů. 2009, částka 11, číslo 40. Dostupné také z: https://www.zakonyprolidi.cz/cs/2009-40/zneni-20220201,

68. *Cisco Annual Internet Report (2018–2023) White Paper*. Cisco.com [online]. San José: March 9, 2020 [cit. 2022-01-16]. Dostupné z: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html?dtid=osscdc000283,

69. CHETTRI, Lalit a Rabindranath BERA. *A Comprehensive Survey on Internet of Things (IoT) Toward 5G Wireless Systems.* IEEE Internet of Things Journal [online]. 2020, 7 (1), 16-32 [cit. 2022-01-16]. ISSN 2327-4662. DOI: 10.1109/JIOT.2019.2948888. Dostupné z: https://ieeexplore.ieee.org/document/8879484,

70. KAČIC, M. *Analýza útoků na bezdrátové sítě*. Brno, 2017. Disertační práce. Vysoké učení technické v Brně. Fakulta informačních technologií 2017. Ústav inteligentních systémů.

71. KAČIC, M. *Analýza útoků na bezdrátové sítě*. Brno, 2017. Disertační práce. Vysoké učení technické v Brně. Fakulta informačních technologií 2017. Ústav inteligentních systémů.

72. *Strategie kybernetické obrany ČR: 2018 - 2022*. Vzcr.cz [online]. Praha: Národní centrum kybernetických operací, 2018 [cit. 2022-01-17]. Dostupné z: https://www.vzcr.cz/uploads/46-Strategie-kyberneticke-obrany-CR.pdf,

73. KRČMÁŘ, Petr. *Kolik stojí DDoS? Základní přijde na pár dolarů, pokročilý na stovky*. Root.cz [online]. Praha: 7. 4. 2017, Internet Info, s.r.o. [cit. 2022-01-17]. Dostupné z: https://www.root.cz/clanky/kolik-stoji-ddos-zakladni-prijde-na-par-dolaru-pokrocily-na-stovky/,

74. ČSN EN ISO/IEC 27000. *Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2020, 54 s. Třídící znak 36 9790,

75. *ENISA Threat Landscape Report 2018: 15 Top Cyberthreats and Trends* [online]. Heraklion, Greece: European Union Agency for Network and Information Security, JANUARY 2019 [cit. 2022-04-27]. ISSN 2363-3050. Dostupné z: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018,

76. GOGELA, Robert. *Standardy a definice pojmů bezpečnosti informací*. Cybersecurity [online]. 2020, s. 4 [cit. 2022-01-19]. Dostupné z: https://www.cybersecurity.cz/data/Gogela.pdf,

77. GOGELA, Robert. *Standardy a definice pojmů bezpečnosti informací*. Cybersecurity [online]. 2020, s. 4 [cit. 2022-01-019]. Dostupné z: https://www.cybersecurity.cz/data/Gogela.pdf,

78. ČSN EN ISO/IEC 27000. *Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014, 151 s. Třídící znak 36 9797,

79. WHAT IS THE CENTER FOR INTERNET SECURITY (CIS)?. In: *Rsisecurity.com: blog* [online]. San Diego, CA: RSI Security, July 13, 2020 [cit. 2022-03-05]. Dostupné z: https://blog.rsisecurity.com/what-is-the-center-for-internet-security-cis/

80. An Introduction to the Components of the Framework. In: *Nist.gov: cyberframework* [online]. Gaithersburg: NIST, May 14, 2021 [cit. 2022-03-07]. Dostupné z: https://www.nist.gov/cyberframework/online-learning/components-framework

81. *Framework for Improving Critical Infrastructure Cybersecurity: version 1.1* [online]. Gaithersburg: NIST, April 16, 2018 [cit. 2022-03-07]. Dostupné z: doi: https://doi.org/10.6028/NIST.CSWP.04162018

82. *What Is Endpoint Detection and Response (EDR)?* Mcafee.com [online]. ©□ 2022 [cit. 2022-01-20]. Dostupné z: https://www.mcafee.com/enterprise/en-us/security-awareness/endpoint/what-is-endpoint-detection-and-response.html,

83. DURAČINSKÁ, Zuzana a Pavel BAŠTA. *DDoS – sofistikovaný útok nebo služba na objednávku?* In: *Nic.cz* [online]. Praha, 24. 5. 2015 [cit. 2022-01-20]. Dostupné z: https://www.nic.cz/files/nic/doc/IT_Security_DDoS_042015.pdf

84. OWOKADE, Adeolu. *How to configure Remotely Triggered Black Hole routing to protect from DDOS attacks (with bonus)*. Routerfreak.com [online]. © 2008-2022 [cit. 2022-01-20]. Dostupné z: https://www.routerfreak.com/remotely-triggered-black-hole-routing-ddos-attacks/,

85. KRČMÁŘ, Petr. *DDoS útoky: jak se účinně bránit?* Root.cz [online]. Praha: 16. 5. 2016, Internet Info, s.r.o. [cit. 2022-01-22]. Dostupné z: https://www.root.cz/clanky/ddos-utoky-jak-se-ucinne-branit/,

86. *Malware*. Eset.com: malware [online]. Praha: ESET, © 1992 – 2022 [cit. 2022-01-22]. Dostupné z: https://www.eset.com/cz/malware/,

87. WOLF, Karel. Kryptominery stále mezi nejrozšířenějšími škodlivými kódy. In: *Lupa.cz* [online]. Praha, 3. 5. 2019 [cit. 2022-01-23]. Dostupné z: https://www.lupa.cz/aktuality/kryptominery-stale-mezi-nejrozsirenejsimi-skodlivymi-kody/,

88. Zpráva o stavu kybernetické bezpečnosti české republiky za rok 2020. In: *Nukib.CZ: zprávy o stavu KB* [online]. Brno: 2021 [cit. 2022-02-10]. Dostupné z: https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/zpravy-o-stavu-kb/

89. Bezpečnostní doporučení NÚKIB pro administrátory 4.0. In: *Nukib.cz: publikace ke vzdělávání* [online]. Brno: Národní úřad pro kybernetickou a informační bezpečnost, 2. 7. 2020 [cit. 2022-02-10]. Dostupné z: https://www.nukib.cz/download/publikace/doporuceni/Doporuceni_admin_4.0_brozura_cb.pdf,

90. Bezpečnostní doporučení NÚKIB pro administrátory 4.0. In: *Nukib.cz: publikace ke vzdělávání* [online]. Brno: Národní úřad pro kybernetickou a informační bezpečnost, 2. 7. 2020 [cit. 2022-02-10]. Dostupné z: https://www.nukib.cz/download/publikace/doporuceni/Doporuceni_admin_4.0_brozura_cb.pdf,

91. Bezpečnostní doporučení NÚKIB pro administrátory 4.0. In: *Nukib.cz: publikace ke vzdělávání* [online]. Brno: Národní úřad pro kybernetickou a informační bezpečnost, 2. 7. 2020 [cit. 2022-02-10]. Dostupné z: https://www.nukib.cz/download/publikace/doporuceni/Doporuceni_admin_4.0_brozura_cb.pdf,

92. Nesnášíte spam? Zaklínám tě SPF a DKIM. In: Antstudio.cz: blog [online]. Plzeň: ANT studio, © 2006 - 2022 [cit. 2022-05-01]. Dostupné z: https://www.antstudio.cz/blog/spam-spf-a-dkim/,

93. Business Email Compromise (BEC). In: Trendmicro.com: security: definition [online]. Irving, Texas: Trend Micro Incorporated, © 2022 [cit. 2022-05-01]. Dostupné z: https://www.trendmicro.com/vinfo/us/security/definition/business-email-compromise-(bec),

94. BISSELL, Kelly a Algirde PIPIKAITE. What you need to know about cybersecurity in 2022. In: *Weforum.org* [online]. Geneva, 18 Jan 2022 [cit. 2022-02-26]. Dostupné z: https://www.weforum.org/agenda/2022/01/cyber-security-2022-global-outlook/,

95. GROSS, Doug. Google boss: Entire world will be online by 2020. In: *Cnn.com* [online]. Atlanta, April 15, 2013 [cit. 2022-02-26]. Dostupné z: https://edition.cnn.com/2013/04/15/tech/web/eric-schmidt-internet/index.html,

96. PRIGG, Mark. Google's Eric Schmidt claims the 'internet will disappear' as everything in our life gets connected. In: *Dailymail.co.uk* [online]. London, 22 January 2015 [cit. 2022-03-02]. Dostupné z: https://www.dailymail.co.uk/sciencetech/article-2922460/Google-s-Eric-Schmidt-claims-internet-disappear-life-gets-connected-says-robots-WON-T-world.html,

97. Výroční zpráva Bezpečnostní informační služby za rok 2020. In: *Bis.cz: výroční zprávy* [online]. Praha, 23. 11. 2021 [cit. 2022-03-05]. Dostupné z: https://www.bis.cz/vyrocni-zpravy/,

98. North Korean Regime-Backed Programmer ... Multiple Cyber Attacks and Intrusions: north Korean Hacking Team Responsible for ... and Other Malicious Activities. In: *Justice.gov: department of Justice* [online]. Washington, DC, Thursday, Semptember 6, 2018 [cit. 2022-03-05]. Dostupné z: https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and.

13. SEZNAM POUŽITÝCH OBRÁZKŮ

Obrázek 1 - Organizační struktura NÚKIB

Obrázek 2 - Statistika bezpečnostních incidentů řešených týmem CSIRT

Obrázek 3 - Schéma DDoS útoku

Obrázek 4 - Rozdělení síťových vrstev

Obrázek 5 - Ukázka spamu hrozícího DDoS (distributed denial of service) útokem

Obrázek 6 - Ukázka phishingového útoku zaměřeného na klienty ČS, a.s.

Obrázek 7 - Ukázka cenové nabídky za DDoS útok

Obrázek. 8 - Základní schéma procesů řízení bezpečnosti informací dle ITIL

Obrázek 9 - Implementace RTHB směrovačů

Obrázek 10 - Ukázka podvodného e-mailu s odkazem na kontrolu hesla

Obrázek 11 - Ukázka podvodného formuláře pro zadání osobních údajů

14. SEZNAM POUŽITÝCH GRAFŮ

Graf 1 - Počet přípojek pevného vysokorychlostního internetu v České republice

Graf 2 - Počet přípojek mobilního internetu v České republice

Graf 3 - Pevný internet v zemích EU podle použité technologie

Graf 4 - Pevný internet podle technologických řešení a nabízené rychlosti

Graf 5 - Nápad trestné činnosti - kybernetická kriminalita

Graf 6 - Nejčastější typy kybernetických útoků v roce 2020 (% respondentů)

Graf 7 - Nejzávažnější typy kybernetických útoků v roce 2020 (% respondentů)

Graf 8 - Odhad vývoje připojených zařízení do internetové sítě

Graf 9 - Ohrožení dat a bezpečnosti informačního systému ze strany insiderů

Graf 10 - Vyhodnocení testu