Vývoj kybernetických hrozeb v době pandemie Covid-19

Lazar Slavković-Raco

Bakalářská práce
2022

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav informatiky a umělé inteligence

Akademický rok: 2021/2022

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Lazar Slavković-Raco**
Osobní číslo:	**A16446**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Softwarové inženýrství**
Forma studia:	**Prezenční**
Téma práce:	**Vývoj kybernetických hrozeb v době pandemie Covid-19**
Téma práce anglicky:	**Evolution of Cybersecurity Threats During the Covid-19 Pandemic**

Zásady pro vypracování

1. Seznamte se s základy principy kybernetické bezpečnosti.
2. Specifikujte vybrané bezpečnostní hrozby v kyberprostoru, zaměřte se při výběru na četnost jejich výskytu.
3. Vysvětlete rozdíl mezi dobou před pandemií a během pandemie Covid-19 se zaměřením na kybernetickou bezpečnost.
4. Analyzujte složení a počty kybernetických hrozeb před pandemií a při pandemii Covid-19.
5. Navrhněte vhodná opatření proti nejčastějším hrozbám.

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. DIOGENES, Yuri a Erdal OZKAYA. Cybersecurity – attack and defense strategies: infrastructure security with Red Team and Blue Team tactics. Birmingham: Packt, 2018, viii, 367 s. ISBN 9781788475297. Dostupné z: https://vufind.katalog.k.utb.cz/Record/91570
2. FRANKE, Don. Cyber security basics: protect your organization by applying the fundamentals. USA: Don Franke, 2016, 101 s. ISBN 9781522952190 Dostupné z: https://vufind.katalog.k.utb.cz/Record/100770
3. OZKAYA, Erdal. _Cybersecurity: the beginner's guide: A comprehensive guide to getting started in cybersecurity. Birmingham: Packt, 2019. ISBN 978-178-9616-194. Dostupné z: https://www.packtpub.com/product/cybersecurity-the-beginner-s-guide/9781789616194
4. GRUBB, Sam. _How cybersecurity really works: a hands-on guide for total beginners_. San Francisco: No Starch Press, [2021]. ISBN 978-171-8501-294. Dostupné z: https://nostarch.com/cybersecurityreallyworks
5. WANG, Lidong a Cheryl Ann ALEXANDER. Cyber security during the COVID-19 pandemic. _AIMS Electronics and Electrical Engineering_. 2021, **5**(2), 146-157. ISSN 2578-1588. Dostupné z: https://www.aimspress.com/article/id/6087e948ba35de2200eea776
6. LALLIE, Harjinder Singh, Lynsay A. SHEPHERD, Jason R.C. NURSE, Arnau EROLA, Gregory EPIPHANIOU, Carsten MAPLE a Xavier BELLEKENS. Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. _AIMS Electronics and Electrical Engineering_. 2021, **105**(2), 146-157. ISSN 01674048. Dostupné z: doi:10.1016/j.cose.2021.102248

Vedoucí bakalářské práce: **Ing. Lukáš Králík, Ph.D.**
Ústav počítačových a komunikačních systémů

Datum zadání bakalářské práce: **3. prosince 2021**
Termín odevzdání bakalářské práce: **23. května 2022**

doc. Mgr. Milan Adámek, Ph.D. v.r.
děkan

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

prof. Mgr. Roman Jašek, Ph.D., DBA v.r.
ředitel ústavu

Ve Zlíně dne 24. ledna 2022

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 23.05.2022

Lazar Slavković-Raco, v. p.
podpis studenta

ABSTRAKT

Tato bakalářská práce se zaměřuje na bezpečnost a ochranu kyber prostoru v různých sektorech. Konkrétně se zabývá průzkumem vývoje kyber prostoru během pandemie Covid-19 v oblastí státních nemocnic a podniků bez ohledu na velikosti firmy. V práci jsou vysvětleny základní pojmy kyber bezpečnosti, které jsou spojený s touto problematikou. Uvedeny jsou nejčastější a majoritní hrozby, které se vyskytují v kyber prostoru, společně se způsoby, jakými se lze v kyber prostoru chránit.

Klíčová slova: kyber prostor, kyber bezpečnost, bezpečnost, informační technologie, pandemie, Covid-19

ABSTRACT

This bachelor thesis focuses on the security and protection of cyberspace in various sectors. Specifically it deals with the development of cyberspace during the Covid-19 pandemic in areas of state hospitals and businesses, regardless of the size of the company. The thesis explains the basic concepts of cyber security, which are associated with this issue. The most common and major threats that occur in cyberspace are listed, along with the ways in which cyberspace can be protected.

Keywords: cyberspace, cyber security, security, information technology, pandemic, Covid-19

Poděkování, motto a čestné prohlášení, že odevzdaná verze bakalářské práce a verze elektronická, nahraná do IS/STAG jsou totožné ve znění:

Prohlašuji, že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Kybernetický prostor je jedna z oblastí dnešní doby, která se velice rychle vyvíjí společně s novými technologiemi. S přírůstkem nových technologií také přichází zločinci, kteří pracují v kybernetickém prostoru. Těm se říká hackers. S příchodem hackerů do kybernetického prostoru je potřeba nějakým způsobem chránit instituce a organizace. K tomu je kybernetická bezpečnost, která řeší ochranu infrastruktury různých organizací a institucí. Se současnou situací, kterou přinesla pandemie, se zvýšila aktivita v kybernetickém prostoru a s tím i kybernetické hrozby.

Tato bakalářská práce se zaměřuje na bezpečnost a ochranu kyber prostoru v různých sektorech. Konkrétně se zabývá průzkumem vývoje kyber prostoru během pandemie Covid-19 v oblastí státních nemocnic a podniků bez ohledu na velikosti firmy. V teoretické částí práce jsou vysvětleny základní pojmy kyber bezpečnosti, které jsou spojeny s touto problematikou a také nejčastější kybernetické hrozby. V praktické částí je uveden popis užívání kybernetického prostoru během pandemie, srovnání třech nejčastějších hrozeb před a během pandemie a doporučení na kybernetickou obranu pasivní, aktivní a reaktivní.

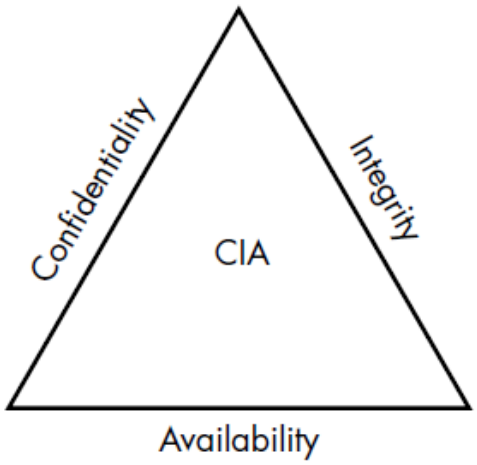
I. TEORETICKÁ ČÁST

1 KYBERNETICKÁ BEZPEČNOST

Každý rok se stávají incidenty, ve kterých dojde ke krádeži informací, a to díky neznalosti oběti. Například nemocnice mohou ztratit důležitá data a administrativní přístupy do systému, informace z firemních zařízení nebo serveru. V takových zařízeních je bezpečnost a zabezpečení digitálních infrastruktur velice důležitá a pomáhá zabránit útokům a finančním škodám.

1.1 Cíl kybernetické bezpečnosti

Kyber bezpečnost má za cíl: identifikovat kyber hrozbu v infrastruktuře, zjistit jak velké působí riziko daná zjištěna hrozba a zvládnout danou hrozbu vhodným způsobem. Hrozby lze určit všeobecným způsobem pomocí modelu Confidentiality-Integrity-Availability (CIA) trojúhelník (CIA tria v angličtině.). [1]



Obrázek 1 CIA trojúhelník [1]

CIA představuje tři základní věci: důvěrnost (confidentiality), integrita (integrity v anj.) a dostupnost (availability v anj.). *Confidentiality* představuje, jak vysoká je hrozba pro data, která jsou uchována v systému, ohrožena k vnějšku. Nejčastější způsob k ochraně důvěryhodnosti dat je zašifrování souboru nebo nastavení přístupových práv v UNIX-u. *Integrity* má za úkol ochránit data při odstranění a modifikaci souborů neoprávněným uživatelům v systému. Také zajišťuje oprávnění uživatelům, v případě, že vkládají nová data do systému nebo modifikují již existující data, která se nesmí poškodit během změn. Funkce *availability* umožňuje, aby data byla dostupná, v případě potřeby. Přístupnost dat může ovlivnit buď úmyslná sabotáž pomocí *denial-of-service* (DoS) nebo *ransomware*. Může se stát, že přístupnost k datům ovlivní živel (poškození serverů v případě zemětřesení, tornáda, …) a to

může způsobit nejen znepřístupnění dat, ale i pracovních stanic a zařízení, které poskytují komerční aplikace. Jsou několik různých řešení, ale nejčastější jsou mít záložní datové centru, kde budete dělat zálohy dat a vhodná opatření proti živlu. [1][2]

1.2 Prostředky kybernetické bezpečnosti

Bez principů kybernetické bezpečností se neobejde žádná společnost s kybernetickou infrastrukturou, pokud se bude chtít ochránit proti útokům a finančním ztrátám. Díky těmto principům jsou schopny se ochránit proti útokům a zabránit jakékoliv další finanční ztrátě.

1.2.1 Firewall

Pomocí firewallu jsme schopni hlídat síťový provoz na různých vrstvách modelu OSI. Existují různé firewally, které jsou schopny fungovat na všech vrstvách OSI. Nečastějším způsobem zabezpečení sítě je nastavit zásady brány *firewall*, která nabízí různé nastavení od zásady pro IP adresy a síťových protokolů, až po zásady založené na aktivitě v síti. *Firewall policy* se aktualizuje pravidelně na základě potřeb uvnitř síťové infrastruktury. [3][4]

1.2.2 Pokročilá správa přístupu

V dnešní době se pro přístupy do systémů používají přihlašovací údaje. Tyto přihlašovací údaje lze zjistit velice snadno, pokud je heslo přihlašovacího údaje příliš krátké nebo se opakuje vícekrát v mnoha aplikacích. Jsou různá doporučení, jak vytvořit bezpečné heslo, ale to nemusí být dostačující. Lze kombinovat přihlašovací údaje pomocí více faktorové ověřování (MFA), což nabízí další vrstvu ochrany při přihlašování do aplikace nebo do sítě. Součásti MFA může být časové jednorázové heslo (TOTP). Některé aplikace nabízejí možnost pro přihlášení pomocí TOTP, které je možné získat z jiné aplikace nebo z fyzického token generátoru. [1][3]

1.2.3 Správa uživatelského oprávnění

Každý zaměstnanec má určitá práva do systému, které potřebují k vykonávání své práce. K některým typům práce je potřeba mít větší přístupová práva do systému, což je zároveň velice rizikové pro informační bezpečnost. Takové velké množství práv je potřeba pravidelně monitorovat. [5]

1.2.4 Vzdělávání a povědomí uživatelů

Organizace musejí mít pro uživatele zásady a postupy při krizových situacích. Uživatelé musejí podstupovat pravidelná školení týkající se zásad organizace a hrozeb, které mohou ohrožovat kybernetickou bezpečnost. Specialisté kybernetické bezpečnosti v organizaci musejí být vysoce proškoleni a schopni zasáhnout v jakémkoliv okamžiku, pokud dojde k porušení bezpečností. [5]

1.2.5 Ovládací prvky vyměnitelných médií

Uživatelé by se měli vyhýbat používání vyměnitelných médií, kupříkladu USB zařízení, externích disků a klávesnic z důvodu útoku přes média. Takové útoky mohou nastat okamžitě při spojení s firemním zařízením nebo při určité aktivitě na počítači. Organizace musí nastavit pravidla pro používání vyměnitelných médií a poučit uživatele, aby omezili používání těchto médií. [5][6]

1.3 Hacking

Obrázek 2 Barvy hackerských klobouku [7]

V světe kyber bezpečností existují šest druhu hackeru, ale budeme se zaměřovat na dva hlavni druhy spektru hackeru . Na jedné straně spektra je útočník, který se dostává do systému a dopouští se zločinu. Na druhé straně je útočník, který má za cíl odhalit systémové vady a nahlásit je patřičné osobě v organizaci s podrobnostmi ohledně zjištěných vad. Útočníci mohou mít různé technické pozadí a věk, ale každá osoba si stanovuje svůj jasný cíl, jakým typem útočníka chce být. Existují i jiné klobouky, ale v této práci se nebude nutné jimi zabývat. [1]

1.3.1 Penetrační test

Cíl útočníka je zjistit bezpečnostní díry a udělat škody firmě. Kyber bezpečnostní tým dělá takzvaný *red team vs blue team*, kde hrají role útočníka versus obránce. Simulační útoky mohou nastávat buď z vnějšku firemní sítě nebo zevnitř. Cíl simulačního útoku je najít bezpečnostní díry v sítí firmy a zajistit, aby se takový útok neopakoval v budoucnu. [3]

1.3.2 White Hat

White Hat nebo etnický hacker je typ útočníka, který provádí útoky na systém dané organizace. Jeho cílem je zjistit vady v systému a pak je nahlásit patřičné osobě, která se stará o systém v organizaci. Bílý klobouk pokrývá širokou škálu kyber bezpečnosti, ale organizace zakládají své požadavky pro svou kyber bezpečnost v systému. Bílý klobouk provádí útoky podobným způsobem jako útočníci černého klobouku. [1]

1.3.3 Black Hat

Black Hat je druh útočníka, který má za cíl škodit organizacím. Takové druhy útočníků se dopouštějí trestních činů za cílem vydírání dané osoby nebo organizace, krádeži citlivých dat (například osobní údaje, rodné číslo, zdravotní karta atd.) za účelem prodeje na černém trhu. [1] [7]

Existuje několik druhů černých klobouků: script kiddies, hackitivsti, state actor a pokročilá trvalá hrozba. Každý z těchto druhů černých klobouků mají své dané cíle, když provádějí útoky v kyber prostoru. [1]

1.3.3.1 Script Kiddies

Script kiddies jsou nezkušení uživatelé v oblastí kyber prostoru. Používají softwarové nástroje, které jsou snadno přístupné na internetu. Jedná se o uživatele ve věkové hranici šestnáct až dvacet let. Útoky provádí pomocí návodu nebo dokumentací, které lze najít na a internetu a provádí útoky na náhodné cíle. Lidé, kteří se označují za s*cript kiddies*, sami sebe neoznačují za hackery a ani si neuvědomují následky provedených útoků. [1][8]

1.3.3.2 Hackitvisti

Pod názvem hacktivista si můžeme představit buď osobu nebo skupinu lidí, kteří používají své znalosti pro politické účely. Cíl hacktivisty nikdy není získat data nebo odcizovat peníze, ale tlačit na politickou agendu nebo změnu ve společnosti. Příklad útoku může být odcizení

sociálního účtu firmy, se kterou nesouhlasí. Účet využijí k tomu, aby napsali nevhodnou nebo nepravdivou zprávu a zničili reputaci dané firmy. S odcizeným účtem mohou prosazovat vlastní agendu. Nejznámější hacktivist skupiny jsou americká skupina Anonymous, běloruská skupina Cyber Partisans a turecká skupina Red Hack [1]

1.3.3.3 Nájemný hacker

Nájemný hacker je osoba, která je sponzorovaná ze strany státu. Cíle státního herce se mohou lišit stát do státu. Cílem může být provádět útoky na systém jiného státu za účelem poškodit systém, monitorovat jiné státy za účelem plánování útoku nebo získání přísně tajných informaci. Státní herec může být i bílý klobouk, pokud má za cíl poskytovat ochranu státního systému. Státní herci jsou největší hrozbou pro kyber bezpečnost z důvodu nabídky velkého množství peněz, přístupu k novějších technologií a tréninku ze strany státu. Nejznámější státy, které mají programy pro sponzorování hackerů jsou Rusko (skupina Cozy Bear, která je aktivní od roku 2008), Čína (skupina Double Dragon od roku 2012, která je známa pro mezinárodní hackovací kampaň), Irán (skupina Helix Kitten od roku 2007) a Severní Korea (skupina Lazarus Group od roku 2010). [1][9][23]

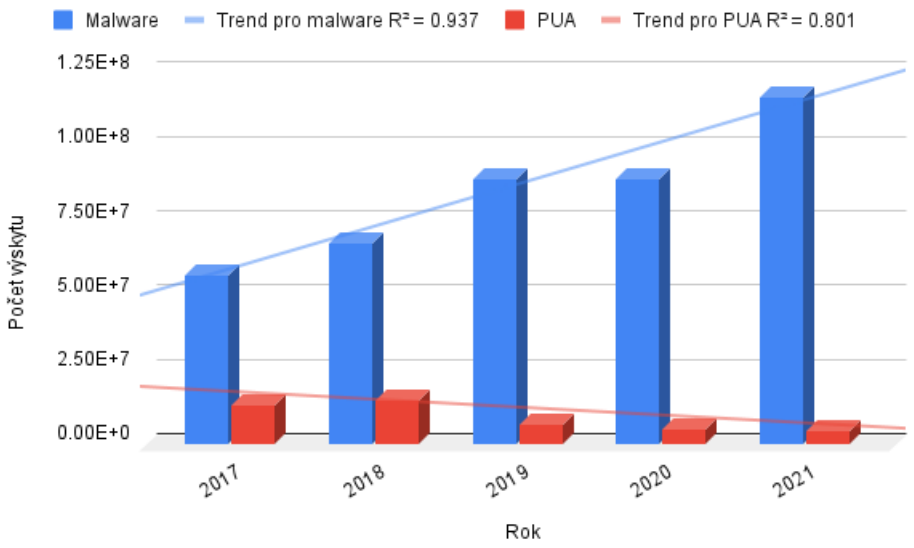
2 BEZPEČNOSTNÍ HROZBY

Dnes se technologie vyvíjí velice rychle. Svět je poháněn sociálními sítěmi, online transakcemi, cloud computingem a automatizovanými procesy. S rychlým vývojem technologií také přichází vyvíjecí se kyber útoky, kterým je potřeba rozumět a co nejlépe jim zabránit.

2.1 Malware

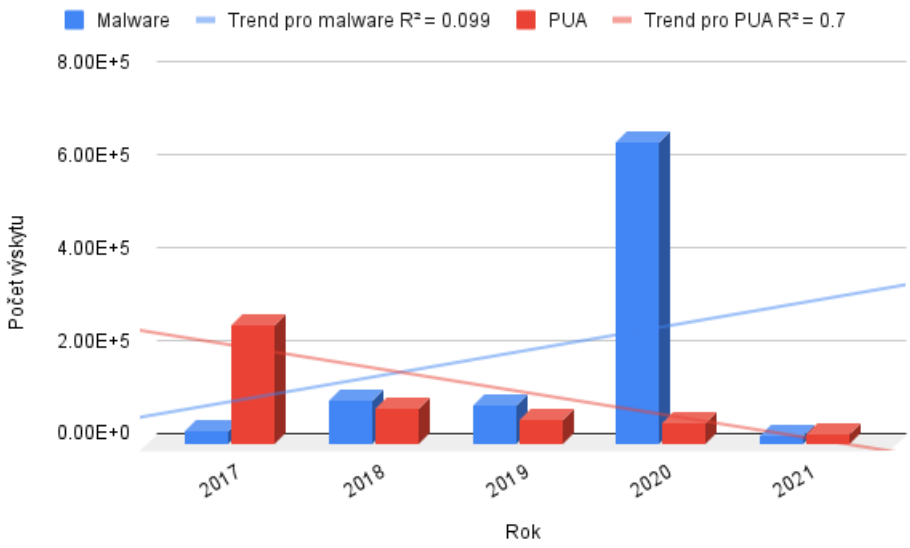
Malware je jeden z druhů škodlivých softwaru, který má za účel poškodit počítač, server nebo počítačovou síť. Existuje několik druhů malwaru, přičemž každý z nich funguje, když útočí na počítače. Malware můžeme rozdělit na: virus, trojan, worm, ransomware, spyware. [10]

Celkový součet výskytů zaregistrovaných malware a PUA (*potentionally unwanted application*) za posledních pět let můžeme vidět na následujícím obrázku. Následující obrázek zobrazuje statistiku pro operační systém Windows.



Obrázek 3 Statistika celkově nahlášených malware a PUA pro operační systém Windows [11]

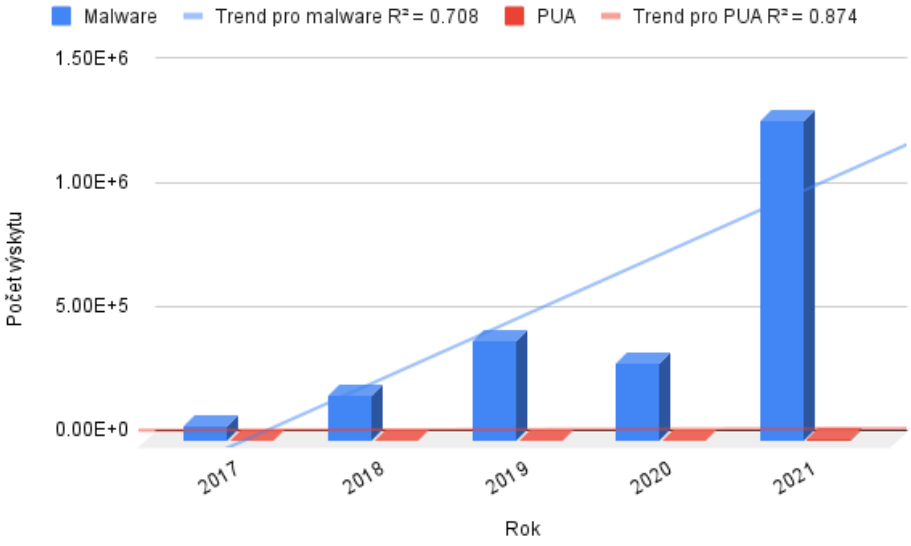
Pro rok 2021 můžeme vidět velký rozdíl oproti předchozích letech malware. Oproti roku 2019 a 2020 počet výskytu nových malware je přibližně 30 procent, mezi roce 2018 a 2019 je přibližně 24 procent. Na následujícím obrázku můžeme vidět výskyt malware a PUA pro MacOS.



Obrázek 4 Statistika celkově nahlášených malware a PUA pro operační systém Mac OS [12]

Zde můžeme vidět, že výskyt nových malware mezi rokem 2019 a 2020 se zvýšil o necelých 91 procent oproti Windows. Rozdíl nových výskytů pro Mac OS je mnohem menší než Windows, který má čísla nad 50 milionu a víc výskytů za rok. Na následujícím obrázku můžeme vidět četnost výskytů nových malware pro operační systém Linux.

Zde můžeme vidět, že Linux má podobnou situaci jako Mac OS v oblasti nových výskytů v určitém ročním období.



Obrázek 5 Statistika celkově nahlášených malware a PUA pro operační systém Linux [12]

2.1.1 Virus

Virus je jedna z podskupin malware. Tenhle druh malware je schopen se rozmnožit do vícero počítačů. Virus má většinou za cíl zničit nebo smazat důležité soubory, než „nakazí“ další počítač díky uživateli. Virus můžeme získat buď stahováním souborů z internetových stránek, připojením externích a sdílených médií. Virus se nespustí bez interakce ze strany uživatele. [14]

2.1.2 Trojan

Trojan je druh malware, pod kterým se skrývá škodlivý kód nebo program. Chová se jako legitimní, ale uživatel se nevšimne akce skrytého Trojan programu. Trojan může být navržen, aby učinil škodlivé akce buď na počítačích nebo v sítí. Je potřeba pomoc uživatele přesvědčit o tom, že soubor nebo program je legitimní, aby ho spustil on sám. Nejvíce typický Trojan malware jsou: DDoS Trojan který využívá Váš počítač pro provádění DDoS útoků na danou IP adresu, Remote Access Trojan (RAT) umožňuje vzdálený přístup na ohrožené počítače. [15]

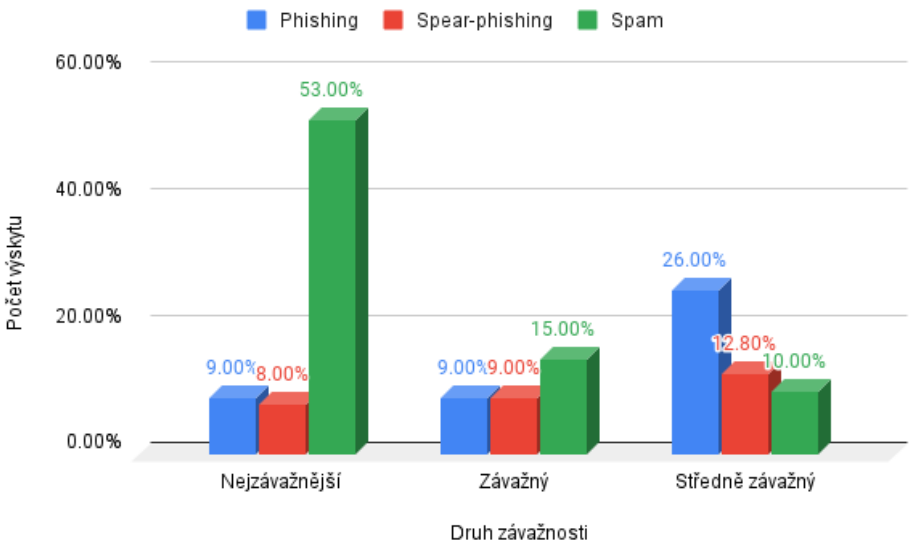
2.1.3 Ransomware

Ransomware je další druh malware, který má za cíl zašifrovat soubory na zařízení. Všechny soubory v systému cíleného zařízení se stanou nepoužitelné. Útočník je schopen vyžádat vykupne finanční hodnoty nebo data za dešifrování napadaného zařízení. Proti ransomware se velice těžko brání díky neustálému zdokonalování strategií za účelem útočit na tato zařízení. [16]

2.2 Sociální inženýrství

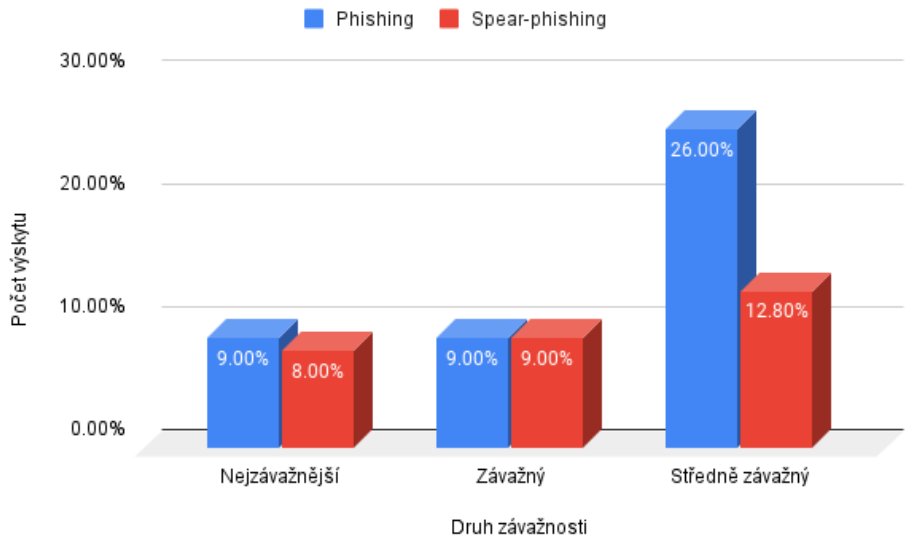
Sociální inženýrství je jeden z druhů útoků, který používá techniku zmatení oběti za účelem získání informací. Útočník může provádět útok za účelem získání hesel k internetovým účtům až po získání kontroly nad zařízení oběti. [17]

Během roku 2019 se organizace na území České republiky setkávaly s těmito nejčastějšími útoky: spam, phishing a podvodný email. Jenom třetina útoků narušila důvěrnost, integritu nebo dostupnost k informacím nebo službám. Nejvíce nahlášených incidentů pocházelo ze samosprávních celků a finančních institucí. [18]



Obrázek 6 Graf pro nejčastější typy útoků na území České republiky pro rok 2019 [18]

Nejzávažnější útoky z druhu sociálního inženýrství byly na území České republiky phishing a také druh phishing spear-phishing. Také se začaly vyskytovat podvodné telefonáty pomocí deepfake technologie, zde se jedná o útok vishing. [18]



Obrázek 7 Graf pro nejzávažnější typy útoků na území České republiky pro rok 2019 [18]

2.2.1 Phishing

Phishing je druh útoku, kde útočník posílá falešnou zprávu na všeobecný cíl a domáhá se přístupových údajů k danému účtu nebo spuštění daného malware na zařízení pro další učinění škody. Phishing útoky začínají být více sofistikované a nahlášených útoků je o dvojnásobek více než jiných způsobů kybernetických útoků. Existuje několik situací, dojde k phishing: pokud dostaneme hlášení o tom, že účet byl napaden; žádost o změnu hesla; žádost o bankovní transakci; příspěvek charitě. [19]

Phishing byl v roce 2020 nejčastějším druhem kybernetického útoku. Tato data byla ohlášena americkou vládní organizaci Federální úřad pro vyšetřování (FBI) z oddělení Centrum pro stížnosti na internetovou kriminalitu. [20]

2.2.2 Spear-phishing

Spear-phishing je druh útoku, který je podobný běžnému phishing. Zatímco phishing provádí útok na všeobecný cíl, spear-phishing útočí na specifickou danou osobu nebo skupinu osob v organizaci. Obvyklé jsou cíle, které mají přístup k důležitým datům nebo přístupová práva k infrastruktuře. Útočník provádí sběr informací o daném cíli, který bude obětí spear-phishingu. Až útočník nasbírá dostatečné informace o určeném cíli, útok bude nastaven dostatečně, aby cíl nepoznal, že se jedná o kybernetický útok. [21]

2.2.3 Vishing

Vishing je hlasový phishing útok, který se provádí přímým hovorem mezi útočníkem a cílem. Cílem útočníka je získat od cíle přístupové údaje buď k bankovnímu účtu nebo k přístupovým právům do infrastruktury sítě. Útočník provádí sběr dat o daném cíli, aby zhodnotil, jakou identitu bude zfalšovat při hovoru. Útočník se po telefonu může vydávat za osobu z organizace. Například zaměstnanec z banky, osoba s vyšší pozicí v dané organizaci nebo přesvědčí cíl, že vyhrál cenu a je potřeba zaplatit administrační poplatek. [22]

2.3 Man-in-the-middle útok

Man-in-the-middle (MITM) útok je způsob, jak odposlouchávat spojení mezi serverem a uživatelem. Takové útoky většinou probíhají buď v aplikace na mobilním zařízení nebo spojení přes bankovní rozhraní. Útočník je schopen nastavit sám sebe do středu datového spoje. Díky tomu je útočník schopen přijímat informace z jedné strany datového průtoku a posílat škodlivé odkazy nebo informace druhé straně. Lze používat tento útok k odposlouchávání

průtoku informací, kde útočník vede individuální spojení s oběma stranami a posílá zprávy. [24][25]

Je několik způsobů techniky pro MITM útoky, ale tyto jsou nejvíce typické: spoofing, e-mail hijacking, únos spojení a odposlouchávaní Wi-Fi. [26]

2.3.1 Spoofing

Spoofing je jedna z technik, kdy se útočník představuje pod jinou falešnou identitu pomocí dat. Při spoofing nelze dostatečně ověřit v mnoha TCP protokolech kdo byl zdroj ani cíl zprávy. Spoofing může být proveden předstíráním daného zařízení využitím jeho IP adresy, oklamáním prohlížeče použitím HTTPS protokolu nebo přesměrováním na jinou falešnou stránku, kde útočník nasbírá data od obětí. [27]

2.3.2 E-mail hijacking

E-mail hijacking je jedna z technik při man-in-the-middle útoku, kde útočník dostane přístup k dané e-mail adrese. Pro přistup k cílené e-mailové adrese je potřeba oklamat majitele e-mailové adrese pomocí phishing nebo sociální inženýrství, kde majitel zadá přístupová data k účtu. Díky tomu útočník může monitorovat e-mail na přicházející zprávy. [28]

2.3.3 Únos spojení

Jiný způsob, jak se dostat k přihlašovacím údajům je vzít takzvaně cookies od prohlížeče. Prohlížeče ukládají data o aktuálním spojení mezi webovou službou a uživatelem na prohlížeči. Útočník může vzít data a dešifrovat je, aby zjistil přihlašovací údaje k dané webové službě. [29]

2.3.4 Odposlouchávaní Wi-Fi

Wi-Fi odposlouchávaní je další způsob, jak získat informace od uživatele pomocí sestavené Wi-Fi ze strany útočníka. Útočník sestaví další Wi-Fi spojení pod podobným jménem lokace, kde se nachází útočník. Lidé, kteří budou hledat spojení k Wi-Fi, si tak budou myslet, že se připojují k důvěryhodnému Wi-Fi spojení. Útočník je schopen monitorovat průtok datové informace ze strany oběti. [30]

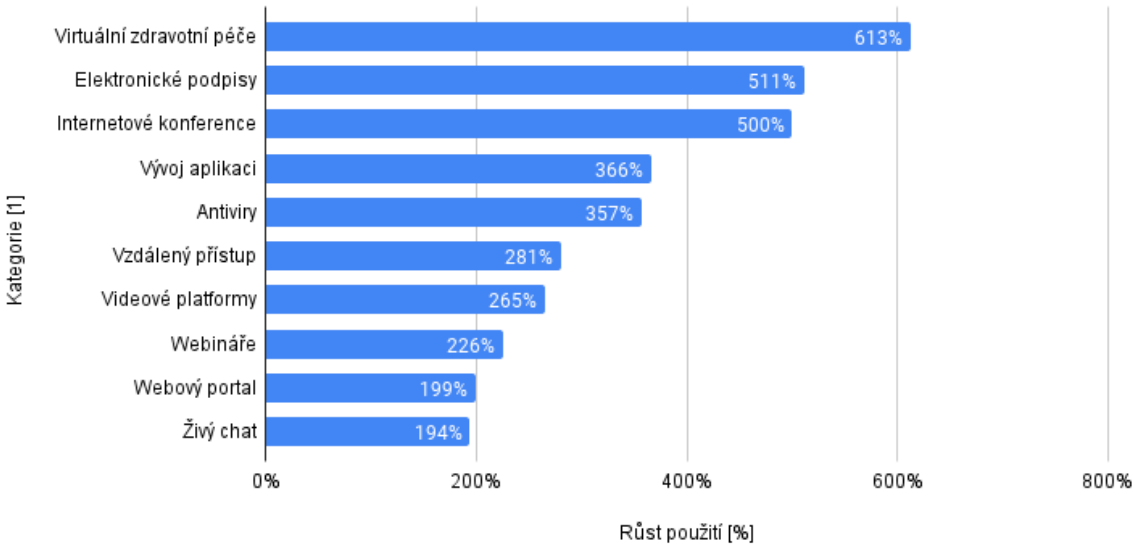
II. PRAKTICKÁ ČÁST

3 POPIS STAVU PŘED A BĚHEM PANDEMIE

Na začátku pandemie se začala několikanásobně zvyšovat aktivita v kybernetickém prostoru díky omezení fyzického kontaktu. Lidé začali více používat aplikace v kybernetickém prostoru, které jím umožnily komunikovat, objednávat si jídlo nebo nakupovat, používat sociální sítě a podobně. Následující data, které budou popsána, jsou převážně platná pro USA. Nicméně můžeme očekávat podobné výsledky dat i ve zbytku světa.

3.1 Pandemicky úspěšné aplikace

Když se celý svět přesunul do kybernetického prostoru, aplikace různých kategorií začaly nabírat značný nárust užívání oproti předchozím letům. Díky této větší aktivitě některé kategorie aplikací začaly pozorovat větší nárust stahování kvůli přesunu zaměstnání z kanceláře domů, výuky z domova nebo kvůli velice omezenému přístupu k úředním institucím. Na následujícím obrázku můžeme vidět nárust užívání aplikací dle kategorie na začátku pandemie. [31] [32]



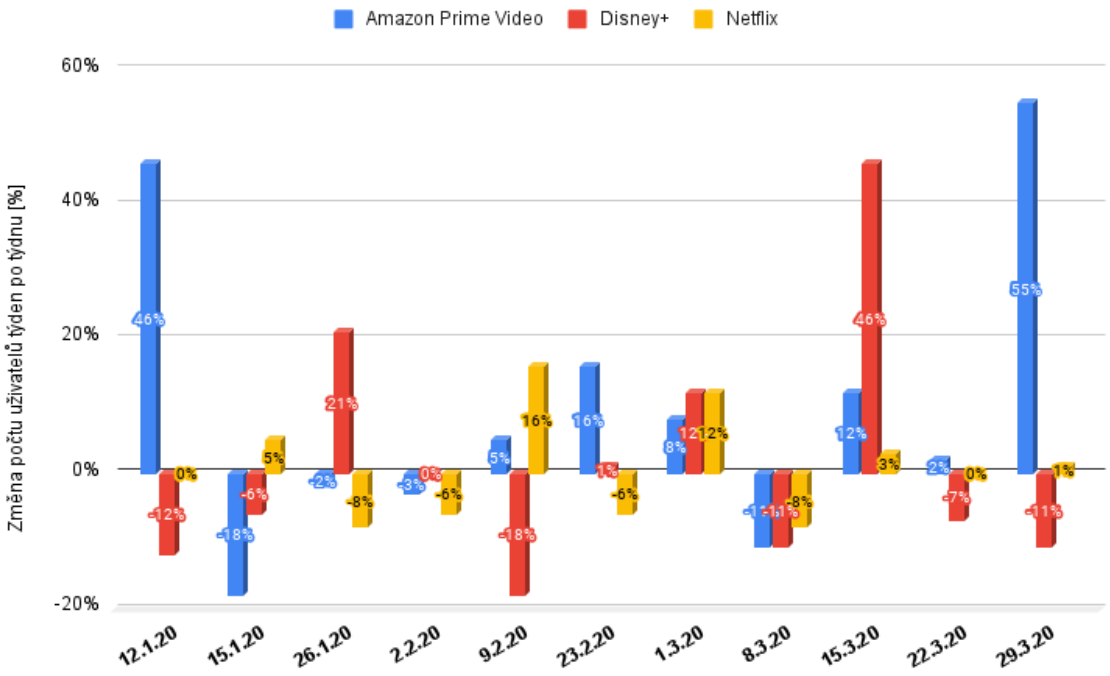
Obrázek 8 Růst použití aplikací dle kategorií na začátku pandemie v roce 2020 [32]

Zde můžeme vidět nárust používaní aplikací dle kategorie. Virtuální zdravotní péče, služby elektronických podpisů a internetové konference mají největší nárust v použití během začátku pandemie. Další kategorií aplikací, které získaly značný nárust použití, jsou například pro vývoj aplikací, antiviry nebo aplikace, které používají vzdálený přístup. Další kategorie

aplikací, která není zmíněna v obrázku 8 jsou například finanční aplikace, které dosáhly nárustu až 55 procent.

3.2 Média a zábava

Během pandemie se dalo očekávat, že se objeví značný růst užívání aplikací pro média a zábavu. Služby, které nabízejí média v kategorii filmy a seriály, zaznamenaly značný nárůst v počtu uživatelů na začátku pandemie. Nárůst počtu uživatelů vzrostl přibližně o 25 procent od ledna 2020 až do konce dubna 2020. Na následujícím obrázku je znázorněn růst uživatelů ve službách Amazon Prime Videos, Disney+ a Netflix. Její nárůst je označován v procentech. [31] [33]



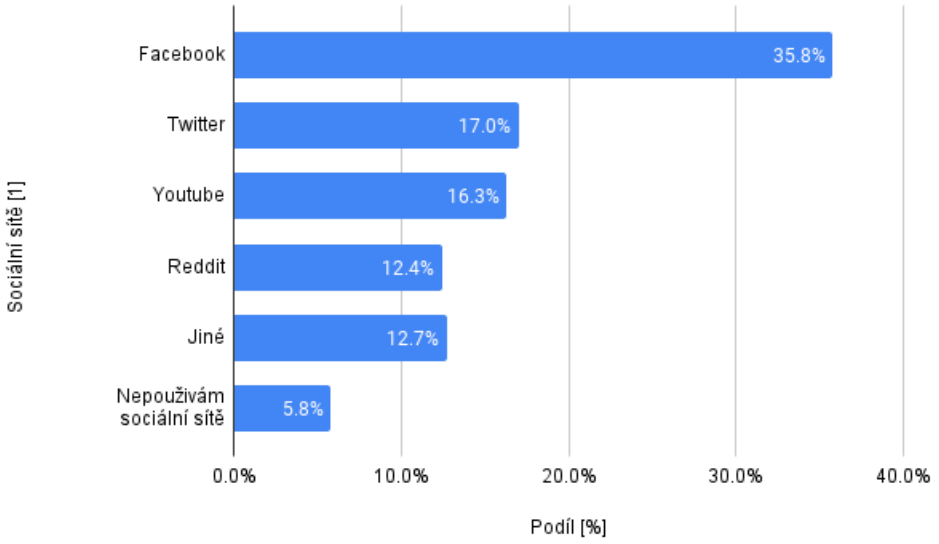
Obrázek 9 Průběh počtu nových uživatelů od ledna 2020 do konce dubna 2020 [33]

Na obrázku 9 můžeme vidět data, na kterých lze pozorovat počty uživatelů za každý týden. Největší převrat v počtu nových uživatelů zaznamenal Amazon Prime Videos, který při nejvyšším nárustu dosáhl až o 55 procent více nových uživatelů.

3.3 Sociální sítě

Sociální sítě měly během pandemie problém zabránit vlny dezinformačních zpráv ohledně Covid-19. Sociální sítě byly jedním z hlavních zdrojů informací ohledně situace s Covid-19.

S velkým nárustem používání sociálních sítí se také začaly se ve velkém množství objevovat články, které šířily nepravdivé informace ohledně Covidu-19. Na následujícím obrázku můžeme vidět, jaký podíl měly sociálních sítě jako hlavní zdroj na šíření informací ve spojitosti s Covid-19. [31] [34]

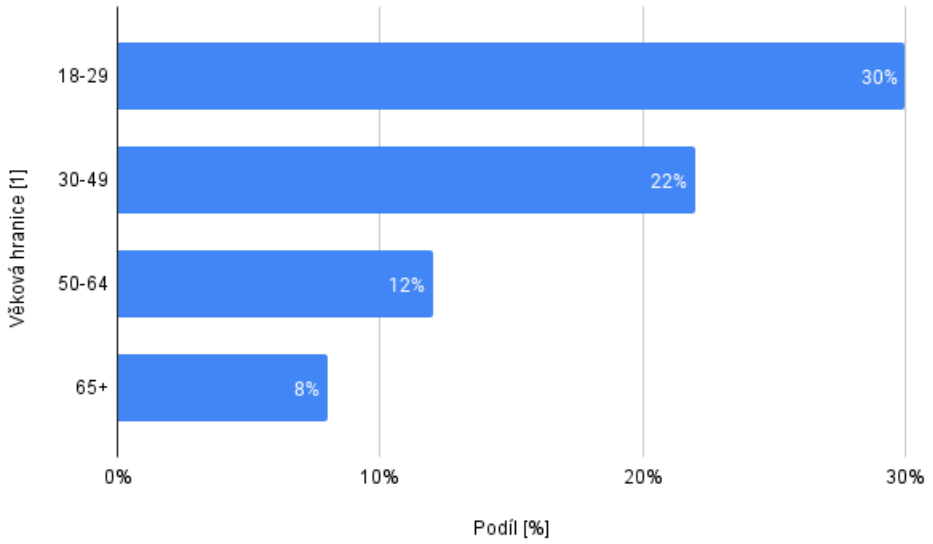


Obrázek 10 Podíl sociálních sítí jako hlavní zdroj informací pro Covid-19 [34]

Zde můžeme vidět podíl nejvýznamnějších sociálních sítí. Facebook byl hlavním zdrojem informací pro Covid-19 a následuje Twitter. Facebook má od začátku pandemie problém bojovat s dezinformacemi na své platformě. Hlavními dezinformátory na této platformě jsou většinou skupiny založené anti-vaxery a internetové bulváry. [35]

3.4 Zdraví a fitness

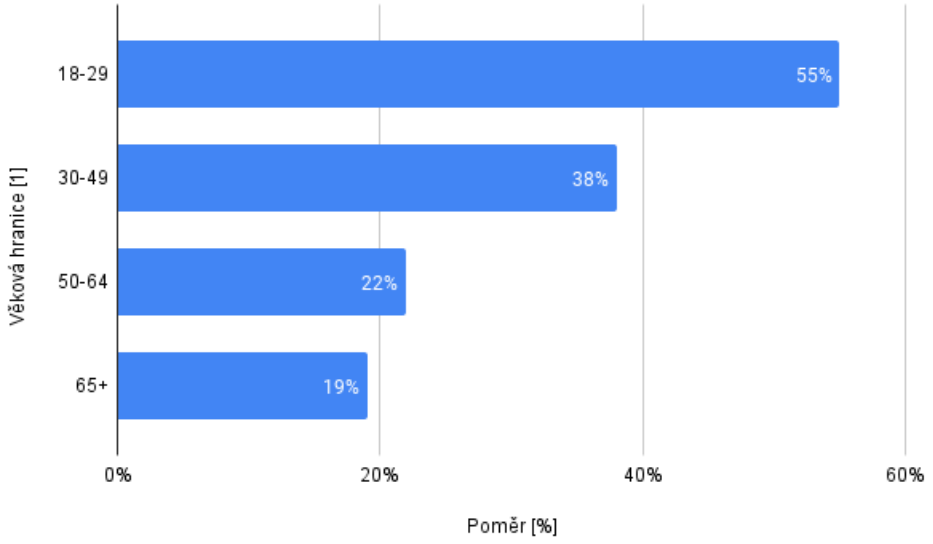
Opatření proti pandemii zabránilo přístupu k posilovnám, fitnessovým centrům a různým fitness studiím. Kvůli těmto opatřením lidé začali používat aplikace pro fitness, aby mohli cvičit doma. Cvičení probíhalo buď pomocí online hodin nebo výukových videí. Na následujícím obrázku je zobrazeno užívání fitness aplikací dle věkových kategorii. [36]



Obrázek 11 Podíl užívání fitness aplikací dle věku [36]

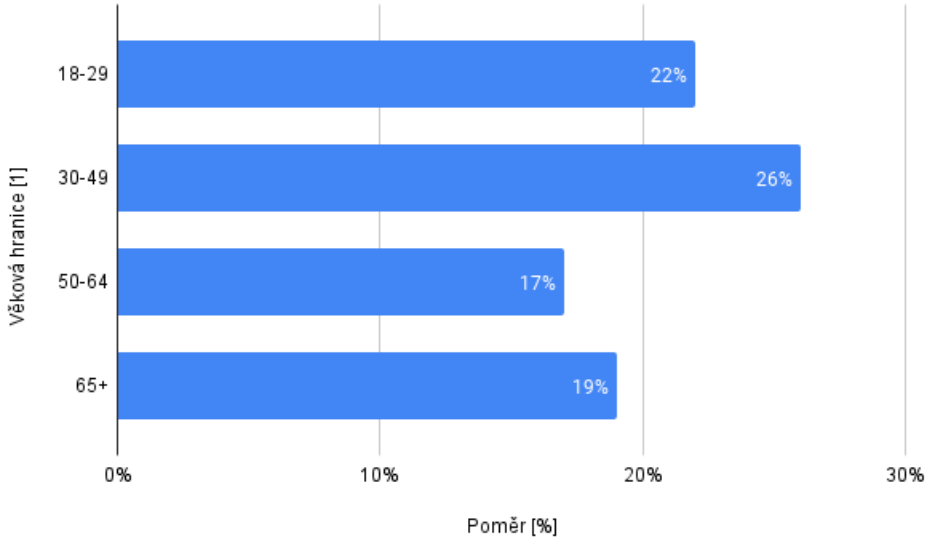
3.5 Online objednávky a dovoz

Mnoho restaurací a obchodních značek v supermarketech mělo problém s velkými nákupními frontami. Mnoho lidí také mělo obavy z přenosu Covid-19 v nákupních centrech. Hodně restaurací začalo používat aplikace pro doručení jídla jako jsou například pro Českou republiku DámeJídlo, Wolt, Bolt nebo Pádim. Dále můžeme vidět na obrázku které věkové kategorie objednávaly jídla nejčastěji přes mobilní aplikace. [31]



Obrázek 12 Rozložení věkových kategorií, které objednávaly jídlo přes aplikace [31]

Největšími dodavateli nákupu jsou aktuálně Rohlík.cz a Košík.cz, kteří používají místní farmáře a někdy obchodní řetězce. Některé obchodní řetězci vytvořili svou vlastní službu, ve které lze doručit nákup, jako jsou například Albert. Dále můžeme vidět na obrázku které věkové kategorie nejvíce využívaly doručení nákupu přes mobilní aplikace nebo webové služby. [31]



Obrázek 13 Rozložení věkových kategorií, které objednávaly nákup přes aplikaci nebo přes webové služby [31]

4 SROVNÁNÍ KYBER HROZEB PŘED A BĚHEM PANDEMIE

Pro jejich porovnání můžeme kyber hrozby rozdělit do tří nejpopulárnějších trendů: malware, ransomware a phishing. Trendy budeme porovnávat před pandemií od roku 2017 až do roku 2020 a během pandemie od roku 2020 do začátku roku 2022. V každém porovnání je uvedena vhodná obrana proti dané kyber hrozbě a data týkající se tohoto období.

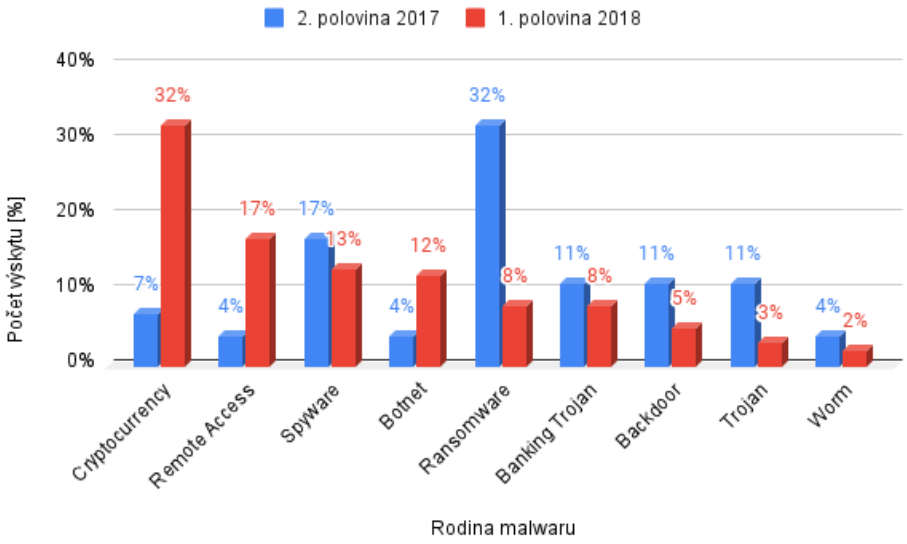
4.1 Malware

Malware je jeden z nejvíce zaznamenaných kybernetických útoku a nejvíce rostoucí útok za posledních pár let. Díky zvýšené aktivity v kybernetickém prostoru se začalo objevovat další trendy pro malware jako jsou například použití PowerShell pro provádění útoku nebo nabízení malwaru jako služba.

4.1.1 Před pandemií

Uživatel může dostat malware přes internetové odkazy z e-mailu nebo z falešných e-mailových inzerátů, spam e-mail a tak podobně. Existují způsoby ochrany proti malware, ale největší důvod útoku je neznalost uživatele. Je potřeba učinit školení o zásadách bezpečnosti pro zaměstnance, nejlépe každý rok, aby se snížila šance útoku. Pokud by se dostal malware do infrastruktury, je potřeba postupovat dle bezpečnostních pravidel. Tyto pravidla se budou týkat všech příslušných pozic, vedoucích a koncových uživatelů. V dnešní době je možno zajistit anti-malware software, aby se zabránilo jakémukoliv spuštění malware v systému. Takové software nabízí testy, které zhodnotí, v jakém stavu je ochrana v daném zařízení. [37] [38]

Nejčastějším útočným vektorem je phishing pomocí podvodných e-mailu, který činí 90 až 95 procent všech úspěšných útoku. Na následujícím obrázku můžeme vidět rozdělení malwarových rodin mezi rokem 2017 a 2018. Dále můžeme vidět velké změny v malwarových trendech, jako jsou například velký úpadek ransomware nebo velké množství kryptoměnových těžařů. [37] [38]



Obrázek 14 Složení malwaru mezi rokem 2017 a 2018 [38]

4.1.2 Během pandemie

Doporučení proti malware jsou téměř totožná jako před pandemií, ale přidala se k nim další vhodná doporučení z důvodu větší aktivity v kybernetickém prostoru. Je potřeba povolit firewallu kontrolu přenosu dat za pomocí protokolu SSL/TLS. Díky tomu jsme schopni monitorovat přenášené informace tam i zpět z webových stránek, e-mailové komunikace a mobilních aplikací. Hodně malwaru začíná používat PowerShell, aby mohli obejít anti-malware obrany. Proto se doporučuje buď úplně zakázat použití PowerShell nebo jej do určité míry omezit. [39] [40]

Během pandemie začal vznikat nový trend, kdy se malware začal nabízet jako služba (MaaS) a poskytuje zákazníkovi cestu, jak konat kybernetické zločiny. Takové služby lze použít ve formě poplatku ze zisku při použití MaaS. Poskytovatel nabídne zákazníkovi infrastrukturu a sadu nářadí pro učinění kybernetického útoku. [40]

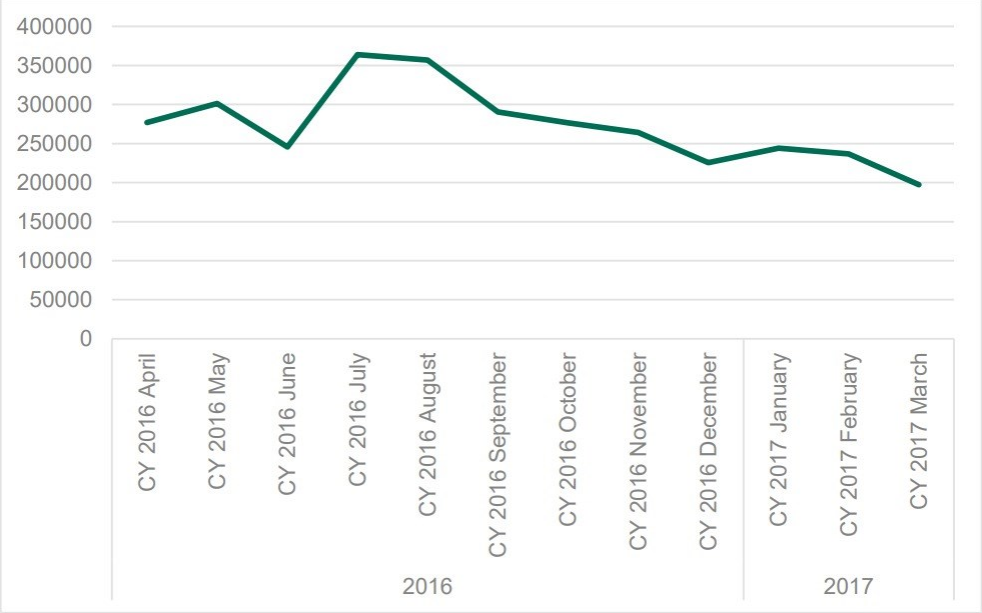
4.2 Ransomware

Ransomware je jeden z útoků, který patřil mezi trendy kybernetických útoků již před pandemií. Ransomware je schopný způsobovat velké škody, pokud není dostatečně ošetřena ochrana infrastruktury. Díky zvýšené aktivitě v kybernetickém prostoru se začaly objevovat další trendy pro ransomware jako jsou například nabízení ransomware jako služba.

4.2.1 Před pandemii

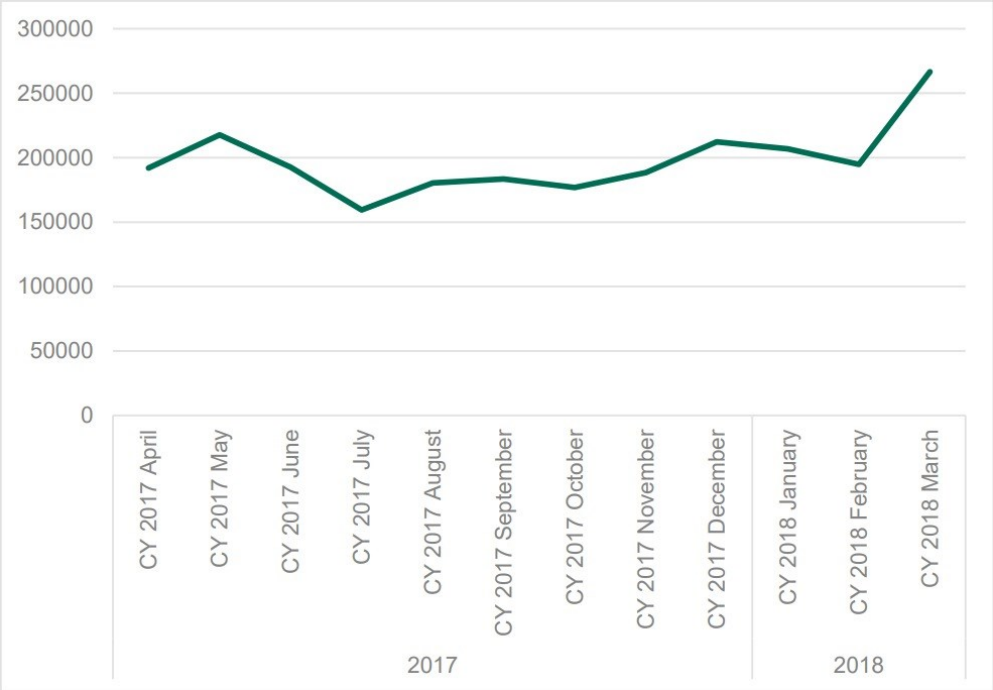
Doporučení proti ransomware jsou různá, ale tyto jsou nejvíce typické. Organizace by měla vytvořit zálohy, které nebudou přístupné pomocí internetového spojení. Pro takové zálohovací řešení je potřeba zajistit, aby se data obnovila včas. Ransomware lze spustit ze složek, kde se dočasně ukládají soubory. Doporučuje se nastavit pravidlo pro operační systém, aby se nespouštěly žádné soubory z dočasných složek (Temp ve Windows 10 a /tmp v Linux/Mac OS). Ransomware se může taky dostat do infrastruktury díky externímu zařízení jako je například USB flash disk nebo mobilní zařízení. Je potřeba nastavit pravidla pro spojení jakéhokoliv externího zařízení do zařízení v infrastruktuře. Pro uživatele je potřeba investovat do školení, jak se bezpečně chovat při prohlížení na internetu. [37] [38]

Nejčastějším útočným vektorem je napadení pomocí phishingových útoku. Většina phishingových útoku pochází z e-mailu, které předstírají již existující službu, jakou jsou například pošta, e-mailové služby. Na následujících obrázcích můžeme vidět průběhy výskytů ransomware, se kterými uživatelé střetnuli alespoň jedenkrát od dubna 2016 až do března 2017. [37] [38]



Obrázek 15 Počet uživatelů, kteří se alespoň jednou setkali s ransomwarem, v období od dubna 2016 až březen 2017 [39]

Na následujícím obrázku vidíme pokračování obr. 9, který zobrazuje data od dubna 2017 až do března 2018.

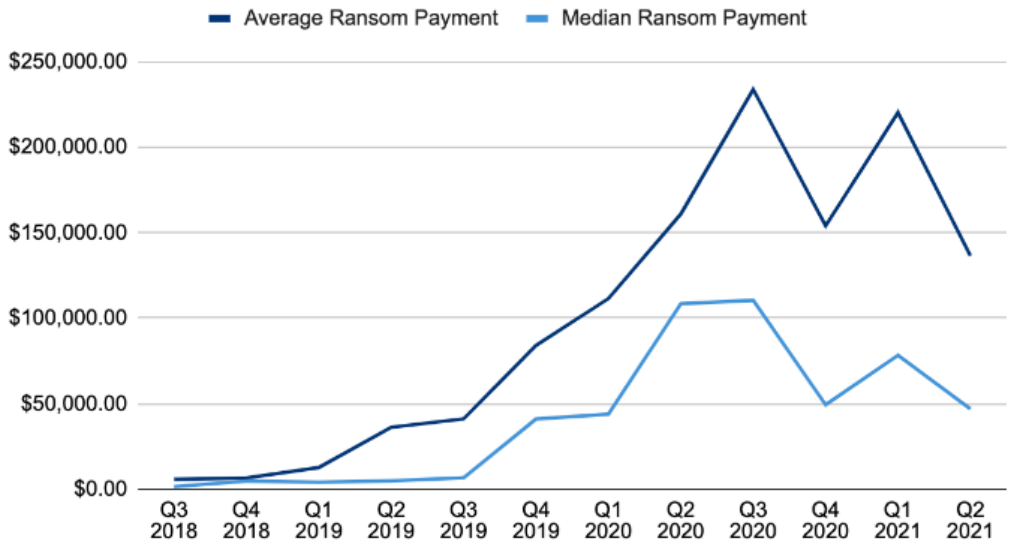


Obrázek 16 Počet uživatelů, kteří se alespoň jednou setkali s ransomwarem, v období od dubna 2017 až březen 2018 [39]

4.2.2 Během pandemie

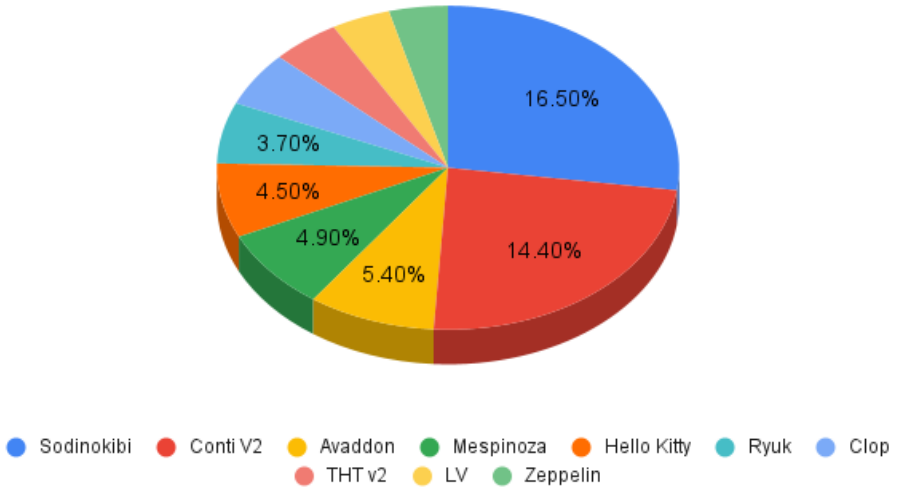
Doporučení proti ransomware jsou totožná jako s těmi před pandemii, pouze jedno doporučení se změnilo kvůli vyššímu zabezpečení. Pro tvorbu zálohy dat se doporučuje sledovat pravidlo 3-2-1. Znění tohoto pravidla je: udělat tři kopie zálohy ve dvou různých formátech, kde alespoň jedna kopie bude přístupná off-line. [40][42]

Po zvýšení aktivity v kybernetickém prostoru se množství výkupného začalo zvyšovat v druhé polovině 2020. Průměrná částka za výkupné pomocí ransomware byla v roce 2019 přibližně 90,000 amerických dolarů. V roce 2020 průměrná částka za výkupné se zdvojnásobila přibližně na 170,000 amerických dolarů. Na následujícím obrázku je znázornění grafu výkupného. [40]



Obrázek 17 Výše požadovaného výkupného skrze ransomware rozloženo po kvartálech od roku 2018 až do 2021 [43]

Dále můžeme rozdělit které ransomware na druhy, které získávaly tržní podíl na začátku roku 2021. Druh ransomware Mespinoza s tržním podílem 4.9 % a Hello Kity s tržním podílem 4.5 % jsou mezi novými ransomware s největším podílem. [40]



Obrázek 18 Podíl trhu druhů ransomware během pandemie [40]

Během pandemie začal vznikat nový trend, kdy se ransomware začal nabízet jako služba (RaaS) a poskytuje zákazníkovi cestu, jak konat kybernetické zločiny. Takové služby lze použít ve formě poplatku ze zisku při použití RaaS. Poskytovatel nabídne zákazníkovi infrastrukturu a sadu nářadí pro učinění kybernetického útoku. [40]

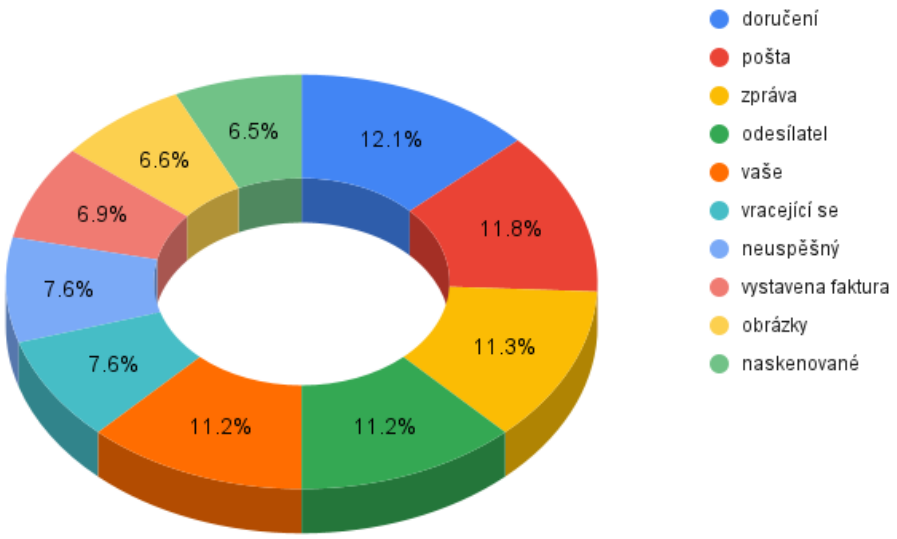
4.3 Phishing

Phishing začal v posledních letech figurovat v útočných vektorech nejčastěji. Útočníci začali zlepšovat způsoby phishingu tak, že již nebývá jednoduché rozeznat škodlivý e-mailu a legitimního.

4.3.1 Před pandemií

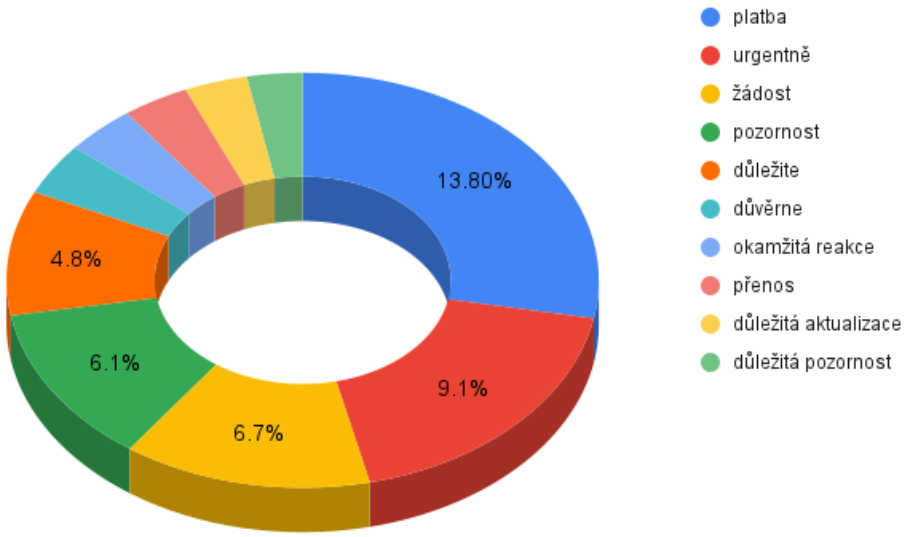
Existuje několik doporučení na obranu proti phishing. Jedno z hlavních doporučení je provést školení pro lepší odhalení padělaných a škodlivých e-mailů. Doporučuje se jednou za rok provádět školení pro zaměstnance organizace. Během roku by se měla provést simulace phishing útoku, aby se zjistil stav infrastruktury a reakce jejích zaměstnanců. Organizace by měla zařídit pro svou e-mailovou službu bezpečnostní bránu s danými filtry, které budou filtrovat škodlivý obsah od neškodlivého. [37] [38]

V e-mailech za účelem phishing se mohou vyskytovat klíčová slova, u kterých bude uživatel věřit jejich legitimnosti. Na následujícím obrázku je složení nejčastěji používaných slov ve phishingových e-mailech. Tato slova se nejčastěji vyskytují ve všeobecných phishingových e-mailech. [38]



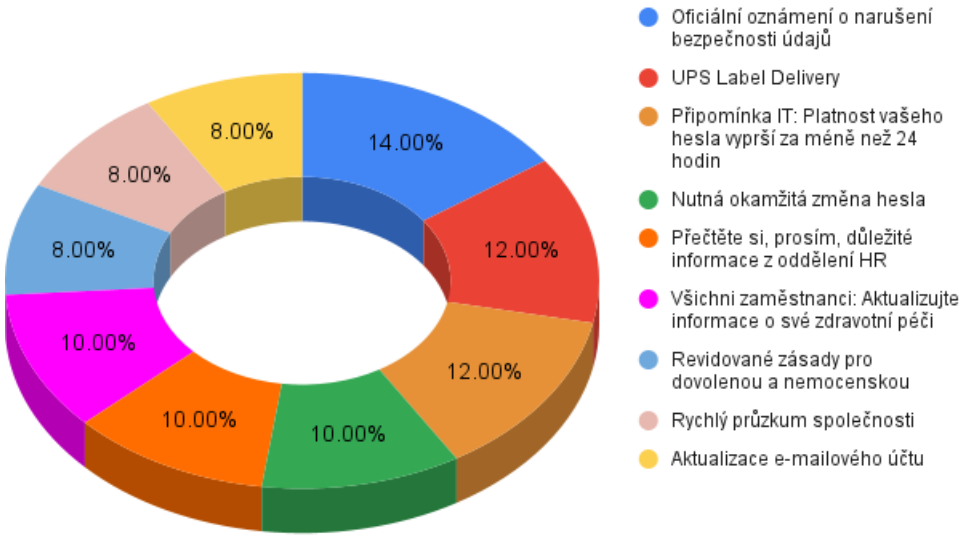
Obrázek 19 Nejčastěji používaná slova ve phishingových e-mailech v obecném prostředí [38]

Phishing se může taktéž dotknout i pracovního prostředí. Zaměstnanec může také uvěřit tomu, že se jedná o pracovní e-mail z intranetu. Na následujícím obrázku je složení slov, jejichž phishingové e-maily byly určeny pro firmy. [37] [38]



Obrázek 20 Nejčastější používaná slova ve phishingových e-mailech v pracovním prostředí [38]

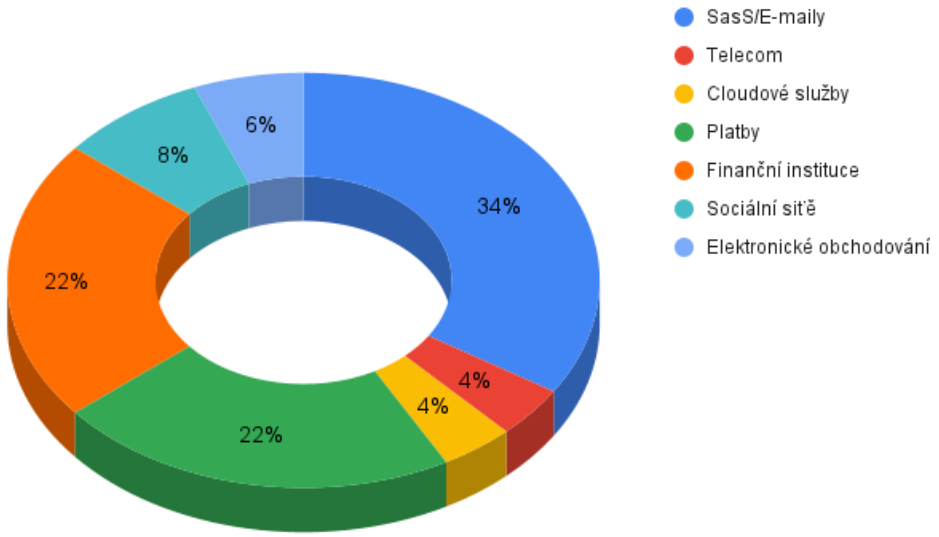
Každý phishingový e-mail obsahuje předmět, který přitáhne uživatele tím, že ho otevře. Takové předměty mohou znít jako „vyprší heslo“, „vyzvednutí balíku“ a podobně. Na následujícím obrázku je rozložení nejvíce otevíraných phishingových e-mailů dle předmětu.



Obrázek 21 Nejčastěji předměty ve phishingových e-mailech v všeobecném prostředí [38]

4.3.2 Během pandemie

Doporučení proti phishing jsou totožná jako před pandemií, ale je potřeba si dávat větší pozor z důvodu menšího výskytu gramatických chyb a také proto, že se vydávají za cizí organizace. Útočníci využili pandemické situace pro zasílání e-mailů, kde se vzdávali za zdravotní organizace nebo univerzity. Předmět tohoto e-mailu oznamoval případy infekčnosti v pracovním prostředí nebo zdravotnický názor profesionálů. E-maily obsahovaly odkazy, které obsahovaly malware software. Takové e-maily činily přibližně 2 %. Phishing stránky začaly adoptovat protokoly HTTPS, kde mohly vypadat na první pohled jako důvěryhodná stránka. Je potřeba zkontrolovat odkaz, zda se skutečně jedná o ten, který to má být, jako například Facebook nebo Amazon. Na následujícím obrázku můžeme vidět podíl služeb, na které bylo zaútočeno phishingem. [39] [44] [45]



Obrázek 22 Rozdělení phishingových útoků na dané služby [44]

Během pandemie začal vznikat nový trend, kdy se phishing začal nabízet jako služba (PaaS), která poskytuje phishing kit zákazníkovi za účelem kybernetických zločinů. Takovou službu je schopna použít i osoba bez technických znalosti. Dle statistik existuje již takových služeb přes 5000, které nabízejí své unikátní phishingové kity. Taková služba je velice finančně nákladově nízká, může stát v rozmezí 50 až 80 amerických dolarů. Část PaaS je hostována na legitimní cloud službě s doménovým jménem a certifikátem. [44]

5 KYBERNETICKÁ OBRANA

Doporučení pro kybernetickou obranu se mohou zcela lišit v závislosti na druhu kybernetického útoku. Některé obrany mají minimální až nulovou interakci s uživatelem, jiné vedou velice aktivní interakce v důležitých částech infrastruktury. Kybernetická obrana lze rozdělit na tři kategorie: pasivní, aktivní a reaktivní.

5.1 Pasivní

Pasivní obrana je druh obrany, kde je minimální až žádná interakce uživatele s nastavenou kybernetickou obranou. Pasivní obrana může začínat na nastavení dostatečně silného hesla a sahat až k firewallu.

5.1.1 Uživatelský účet

Při tvorbě uživatelského účtu je potřeba vytvořit dostatečně silné heslo, nejlépe 16 až 24 znaků. Také je vhodné, aby obsahovalo speciální znaky a čísla. Pro zesílení ochrany účtu je doporučeno využít více faktorové ověření. Toto ověření nabízí další vrstvu ochrany, pokud útočník odhalil heslo. Více faktorové ověření je dostupné ve více formách buď jako aplikace (Google Authenticator) nebo ve formě fyzického klíče, který je mnohem bezpečnější. Zcela se nedoporučuje používat více faktorové ověření pomocí SMS. Velké množství přihlašovacích údajů lze kompletně nahradit pomocí jednorázovému přihlášení (SSO), které umožní uživateli přistoupit k několika aplikacím pod jednou sítí. [37] [38]

5.1.2 DDoS

Je vhodné najít poskytovatele internetu, který již nabízí ochranné prostředky proti útokům typu DDoS. Tím se odkloní část zodpovědnosti za ochranu od organizace a předá se internetovému poskytovateli. Metody, které může poskytovatel používat jsou různé a každá z nich má benefity i cenové náklady. Příklad techniky pro prevenci DDoS útoku je blackholing nebo scrubbing. Dále je vhodné nastavit bezpečnostní plán v případě útoku DDoS, například mít plán pro kritické aplikace a zadržovat administrativní přístup během útoku. [37] [38] [46]

5.1.3 Webový útok

Je vhodné nastavit webový aplikační firewall (WAF), který filtruje internetový provoz HTTP protokolu mezi webovou aplikací a internetem. WAF je schopen se bránit proti cross-

site skriptování, cross-site request forgery (XSRF) a SQL injekcím a mnoho dalším. Tato ochrana je nastavena na 7. vrstvě modelu OSI. Další možnost ochrany je zařazení určité webové adresy, webového obsahu nebo souborů do blacklistu. Díky blacklistu zabráníme nežádoucímu přístupu. [37] [38] [47]

5.2 Aktivní

Při používání aplikací v prostoru organizace je potřeba monitorovat chování dané aplikace, abychom se vyhnuli útoku. Takové aplikace mohou být například plug-in pro webové prohlížeče. Pravidelné aktualizace operačního systému nebo aplikací snižují riziko útoku na uživatele. Použití antiviru pomáhá nejen chránit se před škodlivými soubory i útoku na dané zařízení, ale také nabízí skenování zařízení, na kterém je nainstalovaný antivir. Stránky, které jsou redakční systémy (CMS), je potřeba co nejčastěji aktualizovat a co nejméně používat add-on nebo plug-in třetí strany kvůli bezpečnosti. Je potřeba pravidelně kontrolovat externí zařízení připojené ke strojům, které uživatel nejčastěji používá nebo malá neznámá zařízení v kritických místech uvnitř budovy organizace. Taková zařízení mohou obsahovat keylogger na sběr stisknutých kláves nebo minipočítač na vzdálený útok, aniž by útočník byl v blízkosti. Pravidelné školení ohledně zásad kybernetické bezpečnosti a zásadních pravidel každoročně pomáhá snížit pravděpodobnost útoku na organizaci a snižuje finanční škody. [37] [38] [40]

5.3 Reaktivní

Pokud by nastal útok na organizaci, je potřeba udělat několik kroků na zjištění útoku: omezení, vyšetřování, nahlášení a náprava.

5.3.1 Omezení útoku

Když nastane útok, je potřeba zjistit které zařízení jím jsou ovlivněny. Po zjištění, která zařízení jsou ovlivněna, je potřeba odpojit jakýkoliv přístup a zařízení odpojit ze sítě organizační struktury. V případě, kdy se nezjistí, která zařízeni jsou ovlivněna útokem, je nejlepším řešením odpojení všech zařízení ze sítě. Dalším postupem bude změna hesel k účtům, které jsou na těchto ovlivněných zařízení, za nové, silné heslo. Posledním postupem je aktualizovat veškerý software na zařízení. [48]

5.3.2 Vyšetřování útoku

V dalším kroků je potřeba zjistit rozsáhlost útoku na organizaci. Je potřeba zjistit, kdo se podílel na útoku do organizace. Na útoku se mohou podílet i zaměstnanci organizace nebo některé softwary, které organizace používá. Zjistit časovou osu útoku a kdy útok na organizaci začal. Útok mohl proběhnout i měsíce před odhalením. Podívat se do systému, zda byly některé soubory odstraněny, upraveny nebo byly přidány soubory do sítě organizace. Je potřeba posoudit škody útoku na základě rozsáhlosti útoku. Pro kontrolu úspěšnosti vyšetření výsledku útoku je nejlepší nechat případ prošetřit třetí stranou pomocí auditu. [48]

5.3.3 Nahlášení

V případě útoku by se situace měla řešit s právníkem organizace. Také by se mělo vyhodnotit, kdo může být tímto útokem ovlivněn. Ovlivněné osoby mohou být zaměstnanci, zákazníci nebo prodejci. Také je potřeba tuto událost nahlásit zúčastněným stranám pro transparentnost. Především je nutné událost nahlásit právním složkám jako je například policie České republiky. [48]

5.3.4 Náprava

Po vyšetření je potřeba vytvořit detailní report ohledně kybernetickému útoku. Reportu by měl obsahovat popis toho, co se přesně stalo, kdy se to stalo, proč se to stalo, kdo to učinil a kdo je ovlivněn tímto útokem. Také by měl obsahovat jaké kroky by se měly podniknout, aby se útoku zabránilo v budoucnu. Díky tomuto reportu jsme schopni upravit bezpečností pravidla, ochranné vrstvy a taky prozkoumat software, který zvýší ochranu proti danému útoku do budoucna. [48]

ZÁVĚR

Cílem této práce bylo seznámit čtenářem se situací v kybernetickém prostoru během pandemie, seznámit se se základními pojmy, seznámit se s druhy kybernetických útoků a jejich srovnání před a během pandemie, doporučení kybernetické obrany pasivní, aktivní a reaktivní.

V teoretické části byl čtenář seznámen se základy kybernetické bezpečnosti a jaký má cíl. Vysvětlení prostředků, které osoba v kybernetické bezpečnosti používá k ochranně organizace nebo uživatele. Seznámení s druhy kybernetických útoků a jejich rozdělení.

V praktické části je popsáno použití kybernetického prostoru během pandemie a nárůst používání aplikací buď přes webový prohlížeč nebo za použití chytrého telefonu. Srovnání nejčastějších kybernetických útoku před pandemií od roku 2017 až do 2020 a během pandemie s doporučením, jak bojovat proti nim. Doporučení na kybernetickou bezpečnost pasivním, aktivním a reaktivním způsobem.

SEZNAM POUŽITÉ LITERATURY

[1] GRUBB, Sam. *How cybersecurity really works: a hands-on guide for total beginners.* San Francisco: No Starch Press, [2021]. ISBN 978-171-8501-294. Dostupné z: https://nostarch.com/cybersecurityreallyworks

[2] *What is the CIA Triad and Why is it important?* [online]. Fortinet [cit. 2022-01-17]. Dostupné z: https://www.fortinet.com/resources/cyberglossary/cia-triad

[3] SCAFORNE, Karen a Paul HOFFMAN. *Guidelines on Firewalls and Firewall Policy: Recommendations of the National Institute of Standards and Technology*. USA: National Institute of Standards and Technology, 2009, (1), 48. Dostupné také z: https://www.govinfo.gov/content/pkg/GOVPUB-C13-f52fdee3827e2f5d903fa8b4b66d4855/pdf/GOVPUB-C13-f52fdee3827e2f5d903fa8b4b66d4855.pdf

[4] *The Six Principles of Cyber Security* [online]. USA: Neos IT [cit. 2022-01-18]. Dostupné z: https://blog.neosit.com/en/the-six-principles-of-cyber-security

[5] PEDAMKAR, Priya. *Cyber Security Principles* [online]. Educba [cit. 2022-01-24]. Dostupné z: https://www.educba.com/cyber-security-principles/

[6] WALTERS, Pennie. *The Risks of Using Portable Devices* [online]. Carnegie Mellon University, 2012, 5 [cit. 2022-01-25]. Dostupné z: https://www.cisa.gov/uscert/sites/default/files/publications/RisksOfPortableDevices.pdf

[7] HANNA, Katie Terrell a Taina TERAVAINEN. *Black hat hacker* [online]. TechTarget, November 2021 [cit. 2022-01-29]. Dostupné z: https://www.techtarget.com/searchsecurity/definition/black-hat

[8] LEMOS, Robert. *Script kiddies: The Net's cybergangs: Call them clueless. Call them ankle-biters. Call them what you want. The Internet's teen vandals aren't going away* [online]. ZDNet, July 13, 2020 [cit. 2022-02-01]. Dostupné z: https://www.zdnet.com/article/script-kiddies-the-nets-cybergangs/

[9] *State-Sponsored Hacking Explained* [online]. CyberPolicy [cit. 2022-02-05]. Dostupné z: https://www.cyberpolicy.com/cybersecurity-education/state-sponsored-hacking-explained

[10] MOIR, Robert. *Defining Malware: FAQ* [online]. Microsoft, 04/01/2009 [cit. 2022-02-14]. Dostupné z: https://docs.microsoft.com/en-us/previous-versions/tn-archive/dd632948(v=technet.10)?redirectedfrom=MSDN

[11] *Total amount of malware and PUA under Windows* [online]. AV-Atlas [cit. 2022-02-17]. Dostupné z: https://portal.av-atlas.org/malware/statistics

[12] *Total amount of malware and PUA under MacOs* [online]. AV-Atlas [cit. 2022-02-17]. Dostupné z: https://portal.av-atlas.org/malware/statistics

[13] *Total amount of malware and PUA under Linux* [online]. AV-Atlas [cit. 2022-02-17]. Dostupné z: https://portal.av-atlas.org/malware/statistics

[14] *What Is Malware?* [online]. CISCO [cit. 2022-02-14]. Dostupné z: https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-malware.html#~7-types-of-malware

[15] JOHANSEN, Alison Grace. *What is a Trojan? Is it a virus or is it malware?* [online]. July 24, 2020 [cit. 2022-02-19]. Dostupné z: https://us.norton.com/internet-security-malware-what-is-a-trojan.html

[16] *Ransomware 101* [online]. Cybersecurity and Infrastructure Security Agency [cit. 2022-02-22]. Dostupné z: https://www.cisa.gov/stopransomware/ransomware-101

[17] *What is Social Engineering?: Examples & Prevention Tips* [online]. Webroot [cit. 2022-02-26]. Dostupné z: https://www.webroot.com/us/en/resources/tips-articles/what-is-social-engineering

[18] *Zpráva o stavu kybernetické bezpečnosti ČR - 2019* [online]. NÚKIB, 2019, 18.09.2020, 33 [cit. 2022-02-26]. Dostupné z: https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/zpravy-o-stavu-kb/

[19] *What is phishing? Learn how this attack works* [online]. Youtube, Aug 28, 2019 [cit. 2022-02-26]. Dostupné z: https://www.youtube.com/watch?v=Y7zNlEMDmI4

[20] *Internet Crime Report 2020* [online]. Federal Bureau of Investigation, 2021, 30 [cit. 2022-02-26]. Dostupné z: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

[21] *What is Spear Phishing | Difference from Phishing and Whaling* [online]. Youtube, May 19, 2020 [cit. 2022-02-26]. Dostupné z: https://www.youtube.com/watch?v=JzoJeJBdhuI

[22] *Vishing: Jak ho rozeznat a vyhnout se mu?* [online]. Eset, 25. 08. 2021 [cit. 2022-02-28]. Dostupné z: https://www.eset.com/cz/blog/hrozby/vishing-jak-ho-rozeznat-a-vyhnout-se-mu/

[23] MIKALAUSKAS, Edvardas. *The world's most dangerous state-sponsored hacker groups* [online]. Cyber News, 16 February 2021 [cit. 2022-02-28]. Dostupné z: https://cybernews.com/editorial/the-worlds-most-dangerous-state-sponsored-hacker-groups/

[24] WANG, Le a Alexander M. WYGLINSKI. *Detection of man-in-the-middle attacks using physical layer wireless security techniques: Man-in-the-middle attacks using physical layer security*. Wireless Communications and Mobile Computing, 2014, 19. Dostupné z: doi:10.1002/wcm.2527

[25] *Man in the Middle (MITM) Attack: Learn About Man-in-the-Middle Attacks, Vulnerabilities, and How to Prevent MITM Attacks* [online]. VeraCode [cit. 2022-03-03]. Dostupné z: https://www.veracode.com/security/man-middle-attack

[26] GEORGESCU, Elena. *Man-in-the Middle (MITM) Attack: Learn What Is a Man-in-the-Middle Attack, How It Works, and How to Protect Your Company* [online]. Heimdal Security, 27.08.2021 [cit. 2022-03-05]. Dostupné z: https://heimdalsecurity.com/blog/man-in-the-middle-mitm-attack/

[27] JINDAL, Keshav, Surjeet DALAL a Kamal Kumar SHARMA. *Analyzing Spoofing Attacks in Wireless Networks*. IEEE, 07 April 2014n. l., 5. ISSN 2327-0632. ISBN: 978-1-4799-4910-6. Dostupné z: doi:10.1109/ACCT.2014.46

[28] *Email hijacking* [online]. Double Octopus [cit. 2022-03-06]. Dostupné z: https://doubleoctopus.com/security-wiki/threats-and-tools/email-hijacking/

[29] *Cookie Theft* [online]. Techopedia [cit. 2022-03-09]. Dostupné z: https://www.techopedia.com/definition/24633/cookie-theft

[30] GUPTA, Deepak. *Wi-Fi Eavesdropping: what is it and how to avoid this problem* [online]. TechUnwrapped, July 18, 2021 [cit. 2022-03-12]. Dostupné z: https://techunwrapped.com/wi-fi-eavesdropping-what-is-it-and-how-to-avoid-this-problem/

[31] *Software Bugs Don't Shelter in Place: What app usage and error data reveal during COVID-19* [online]. Bugsnag [cit. 2022-05-04]. Dostupné z: https://www.bugsnag.com/covid-19-app-usage-error-data-report?fbclid=IwAR2TFG00OUb-JFPP5Xahzr5VbJC_3_0EaXxVr-tF8WQ6ivNjxgPa9F5oksg

[32] *COVID-19 Software Industry Statistics* [online]. TrustRadius, April 9th, 2020 [cit. 2022-05-04]. Dostupné z: https://www.trustradius.com/vendor-blog/covid-19-software-industry-data-and-statistics

[33] *Americans Are Turning To Apps For Entertainment During COVID-19* [online]. InMobi, May 18, 2020 [cit. 2022-05-05]. Dostupné z: https://www.inmobi.com/blog/2020/05/18/americans-are-turning-to-apps-for-entertainment-during-covid-19

[34] HUTCHINSON, Andrew. *Facebook is the Leading Social Platform for News During COVID-19 [Infographic]* [online]. Social Media Today, April 29, 2020 [cit. 2022-05-06]. Dostupné z: https://www.socialmediatoday.com/news/facebook-is-the-leading-social-platform-for-news-during-covid-19-infograph/576962/

[35] GALLAGHER, Fergal. *Facebook 'failing' to tackle COVID-19 misinformation posted by prominent anti-vaccine group, study claims: Researchers claim Facebook isn't enforcing policies on COVID-19 misinformation.* [online]. ABC News, 3 December 2021 [cit. 2022-05-07]. Dostupné z: https://abcnews.go.com/Technology/facebook-failing-tackle-covid-19-misinformation-posted-prominent/story?id=81451479

[36] VOGELS, Emily A. *From virtual parties to ordering food, how Americans are using the internet during COVID-19* [online]. Pew Research Center, April 30, 2020 [cit. 2022-05-08]. Dostupné z: https://www.pewresearch.org/fact-tank/2020/04/30/from-virtual-parties-to-ordering-food-how-americans-are-using-the-internet-during-covid-19/

[37] *ENISA Threat Landscape Report 2017* [online]. ENISA, January 15, 2018, 114 [cit. 2022-03-26]. Dostupné z: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017

[38] *ENISA Threat Landscape Report 2018* [online]. ENISA, January 28, 2019, 114 [cit. 2022-03-26]. Dostupné z: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

[39] *KSN Report: Ransomware and malicious cryptominers 2016-2018* [online]. Kaspersky, 2018, 34 [cit. 2022-04-22]. Dostupné z: https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2018/06/27125925/KSN-report_Ransomware-and-malicious-cryptominers_2016-2018_ENG.pdf

[40] *ENISA Threat Landscape 2021* [online]. ENISA, October 27, 2021, 116 [cit. 2022-04-03]. Dostupné z: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

[41] *ENISA Threat Landscape 2020 - Malware* [online]. ENISA, October 20, 2020, 24 [cit. 2022-04-03]. Dostupné z: https://www.enisa.europa.eu/publications/malware

[42] *ENISA Threat Landscape 2020 - Ransomware* [online]. ENISA, October 20, 2020, 26 [cit. 2022-04-03]. Dostupné z: https://www.enisa.europa.eu/publications/ransomware

[43] *Q2 Ransom Payment Amounts Decline as Ransomware becomes a National Security Priority* [online]. CoveWare, July 23, 2021 [cit. 2022-04-23]. Dostupné z: https://www.coveware.com/blog/2021/7/23/q2-ransom-payment-amounts-decline-as-ransomware-becomes-a-national-security-priority

[44] *ENISA Threat Landscape 2020 - Phishing* [online]. ENISA, October 20, 2020, 24 [cit. 2022-04-03]. Dostupné z: https://www.enisa.europa.eu/publications/phishing

[45] *Phishing Activity Trends Report: Activity October-December 2019* [online]. Anti-Phishing Working Group, February 24, 2020, 13 [cit. 2022-05-01]. Dostupné z: https://docs.apwg.org/reports/apwg_trends_report_q4_2019.pdf

[46] *Denial of Service (DoS) guidance: Guidance to help organisations understand and mitigate DoS attacks.* [online]. Velká Britanie: National Cyber Security Center, 16 March 2016, 19 November 2020 [cit. 2022-05-11]. Dostupné z: https://www.ncsc.gov.uk/collection/denial-service-dos-guidance-collection/preparing-denial-service-dos-attacks1/response-plan

[47] *What is a WAF?: Web Application Firewall explained* [online]. CloudFlare [cit. 2022-05-11]. Dostupné z: https://www.cloudflare.com/en-gb/learning/ddos/glossary/web-application-firewall-waf/

[48] ELGAN, Mike. *Reactive Cybersecurity: How to Get it Right* [online]. SecurityIntelligence, January 20, 2022 [cit. 2022-05-12]. Dostupné z: https://securityintelligence.com/articles/reactive-cybersecurity-get-it-right/

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

CIA	Confidentiality-Integrity-Availability
DoS	Denial of Service
DDoS	Distributed Denial of Service
OSI	Open System Internconnection
MFA	Multi-Factor Authentication
TOTP	Time-based one-time password
PUA	potentionally unwanted application
MaaS	Malware jako služba
RaaS	Ransomware jako služba
PaaS	Phishing jako služba
RAT	Remote Access Trojan
SSO	Jednorázové přihlášení
CMS	Redakční systém

SEZNAM OBRÁZKŮ