VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

INFORMAČNÍ A KYBERNETICKÉ HROZBY V ROCE 2019
INFORMATION AND CYBER THREATS IN 2019

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE
AUTHOR

Bc. Jonatán Bača

VEDOUCÍ PRÁCE
SUPERVISOR

Ing. Petr Sedlák

BRNO 2020

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Student:	**Bc. Jonatán Bača**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Informační management
Vedoucí práce:	**Ing. Petr Sedlák**
Akademický rok:	2019/20

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává diplomovou práci s názvem:

Informační a kybernetické hrozby v roce 2019

Charakteristika problematiky úkolu:

Úvod
Cíle práce, metody a postupy zpracování
Teoretická východiska práce
Analýza současného stavu
Vlastní návrhy řešení
Závěr
Seznam použité literatury
Přílohy

Cíle, kterých má být dosaženo:

Analyzovat informační a kybernetické hrozby za určité časové období a vytvořit prevenci pro společnosti.

Základní literární prameny:

ČSN ISO/IEC 27001, Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky. Praha: Český normalizační institut, 2014.

ČSN ISO/IEC 27002, Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnostiinformací - Soubor postupů. Praha: Český normalizační institut, 2014.

DOUCEK, P., L. NOVÁK a V. SVATÁ. Řízení bezpečnosti informací. Praha: Professional Publishing, 2008. ISBN 80-86898-38-5.

ONDRÁK, V., P. SEDLÁK a V. MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: CERM, Akademické nakladatelství, 2013. ISBN 978-80-7204-872-4.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2019/20

V Brně dne 29.2.2020

L. S.

doc. RNDr. Bedřich Půža, CSc. ředitel	doc. Ing. et Ing. Stanislav Škapa, Ph.D. děkan

Abstrakt

Diplomová práca sa zameriava na informačné a kybernetické hrozby v roku 2019. Práca pozostáva z teoretických východísk, ktoré slúžia pre lepšie pochopenie danej problematiky. Následne práca popisuje analýzu súčasného stavu poskladanú z viacerých analýz zameraných primárne na české spoločnosti. V poslednej časti je vytvorený návrh opatrení spojený s vytvorením predikcií a preventívnych opatrení a odporúčaní pre spoločnosti.

Kľúčové slová

analýza, informačná a kybernetická bezpečnosť, zraniteľnosti, bezpečnostné hrozby, kybernetické útoky, predikcie, preventívne opatrenia

Abstract

Diploma thesis focuses on information and cyber threats in 2019. It comprises theoretical basis for better understanding of the issue. Afterward the thesis describes the analysis of the current situation which combined several analyses primarily aimed on Czech companies. In the last part draft measures is created which contain predictions and preventive actions and recommendations for companies.

Key words

analysis, information a cyber security, vulnerabilities, security threats, cyberattacks, predictions, preventive actions

Bibliografická citácia

BAČA, Jonatán. Informační a kybernetické hrozby v roce 2019 [online]. Brno, 2020 [cit. 2020-05-07]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/127732. Diplomová práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Petr Sedlák.

Čestné prehlásenie

Prehlasujem, že predložená diplomová práca je pôvodná a spracoval som ju samostatne. Prehlasujem, že citácie použitých prameňov sú úplné, že som vo svojej práci neporušil autorské práva (v zmysle Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brne dňa 6. mája 2020

_____

podpis študenta

Poďakovanie

Moje veľké poďakovanie patrí pánovi Ing. Petrovi Sedlákovi za vedenie mojej diplomovej práce, za poskytnutie užitočných a odborných rád. Rovnako veľké poďakovanie patrí pánovi Bc. Michalovi Mezerovi MSc. za vykonanú oponentúru, odborné konzultácie, trpezlivosť a venovaný čas. Ďakujem takisto Bc. Jakubovi Mazalovi za cenné rady ohľadom služby ThreatGuard. V neposlednej rade patrí moje poďakovanie rodine, priateľke a kamarátom za veľkú podporu pri písaní tejto práce.

OBSAH

ÚVOD

V kybernetickom priestore sú každú sekundu vykonané desiatky až stovky kybernetických útokov. Každý deň tak vo svete prebehnú státisíce až milióny útokov. Jedná sa o rôzne typy sieťových útokov, zneužívanie zraniteľností, webové hrozby, spamové e-maily a mnohé ďalšie. Predstava, že by vo večerných správach boli zmieňované státisíce až milióny fyzických útokov na ľudí v jednej krajine je desivá a zastrašujúca. Avšak kyberpriesoru nie je kladený veľký záujem širokej verejnosti a neupriamuje sa naň veľká pozornosť.

Keď už však niekto venuje svoju pozornosť a pochopenie kyberpriestoru, môže sa strácať v obrovskom množstve dát a informácií, ktoré tento priestor poskytuje. Selektovanie a prípadná analýza je pre takýto dynamický celok časovo náročná. Častokrát aj selektovaných a kategorizovaných informácií býva veľké množstvo. Všetky tieto informácie je potrebné ďalej filtrovať či už podľa regiónu, závažnosti, alebo iného zvoleného kritéria. V takomto prípade môže nastať ucelený pohľad na danú problematiku, s ktorým je možné ďalej pracovať.

Preto je potrebné, pre lepšiu informovanosť okolia, pracovať s týmito údajmi, z ktorých v konečnom dôsledku môžu vzniknúť zaujímavé analýzy, na základe ktorých je možné vyvodiť isté závery. Z analýz dokážeme získať prehľad o určitom, vopred vymedzenom období, ale takisto môžeme v analýzach sledovať určitý trend, z ktorého sme schopní vytvoriť preventívne opatrenia na budúce časové obdobie. A práve v tejto diplomovej práci budú takéto analýzy vykonané.

VYMEDZENIE PROBLÉMU A CIELE PRÁCE

Ako už bolo naznačené v úvode diplomovej práce, spracovanie a analýza informácií bude súčasťou tejto práce. Konkrétne hlavným cieľom práce je analyzovanie informačných a kybernetických hrozieb za určité časové obdobie, v tomto prípade to bude rok 2019. Pre zvýšenie adekvátnosti tejto analýzy, budú spracovávané informácie z viacerých zdrojov. Tieto zdroje budú navyše ďalej filtrované pomocou zvolených kritérií. Kritéria tejto analýzy budú primárne zamerané na české spoločnosti. Pre výber ďalších kritérií bude nápomocná analýza reportov zo služby ThreatGuard od spoločnosti COMGUARD. Viac informácií o tejto službe nájdete v analytickej časti diplomovej práci. Analýzy budú doplnené o reporty informačno-kybernetických hrozieb Kaspersky Lab a o najzávažnejšie mediálne správy roku 2019, týkajúce sa kybernetických útokov, ktoré zasiahli Českú republiku.

Okrem analýzy súčasného stavu, diplomová práca pozostáva z teoretických východísk a vlastného návrhu riešenia. Teoretické východiská slúžia na lepšie pochopenie problematiky diplomovej práce a vytvoria potrebný základ práce. Na analýzu súčasného stavu a zistených informácií z tejto kapitoly nadviaže návrhová časť práce pozostávajúca z vytvorených možných predikcií a preventívnych opatrení pre spoločnosti na nasledujúci rok 2020.

1 TEORETICKÉ VÝCHODISKÁ PRÁCE

Prvá kapitola diplomovej práce bude venovaná teoretickým východiskám práce. Na základe tejto časti bude možné lepšie pochopiť ostatné kapitoly tejto práce.

1.1 ZÁKLADNÉ POJMY

Obsahom tejto podkapitoly sú základne pojmy, ktoré je potrebné nevyhnutne poznať pre absolútne pochopenie problematiky preberanej v tejto diplomovej práci. Tieto pojmy sa v práci vyskytujú niekoľkonásobne.

IT (Information Technology) – informačné technológie [1]
ICT (Information Communication Technology) – informačné a komunikačné technológie [1]
IS (Information System) – informačný systém [1]

Dáta sú spracovávané určitým spôsobom tak, aby vytvorili a napĺňali informáciu, ktorou sa však nemusia nutne stať. Dátami môže byť sekvencia znakov, text, čísla, obraz atď. Sú získavané výpočtom, čítaním, pozorovaním, meraním a inými spôsobmi. Dáta sú vhodné pre komunikáciu, spracovanie a vyhodnocovanie [1; 2].

Pod **citlivými dátami** chápeme dáta, ktoré majú pre chod organizácie zásadný význam. Zneužitím, vyzradením, nedostupnosťou alebo neautorizovanou zmenou týchto dát by vznikla škoda pre organizáciu, prípadne by nemohla riadne plniť svoje poslanie. Jedná sa predovšetkým o personálne dáta a dáta týkajúce sa chodu organizácie [2; 8].

Informácie sú poznatky vytvorené a pozostávajúce z dát, ktoré znižujú neurčitosť a neznalosť a dávajú príjemcovi význam. V informatike sú informácie tvorené kódovanými dátami [1; 2].

Citlivé informácie sú informácie, ktoré na základe rozhodnutia príslušnej autority musia byť chránené, pretože ich zmena alebo strata by viedla k výraznej ujme a škode [8].

Aktívum je čokoľvek, čo má pre vlastníka aktíva nejakú hodnotu. Aktíva základne rozdeľujeme na hmotné a nehmotné. Medzi hmotné aktíva môžeme zaradiť hardware, ako napríklad servery, počítačové koncové stanice, sieťové zariadenia atď. Do

nehmotných aktív zaraďujeme software, ako napríklad programy, operačné systémy atď., dáta a informácie [2; 3; 4].

Informačný systém je definovaný ako systém, ktorého väzby sú definované ako informácie a jeho prvky (hardware, procesy, služby, aplikácie atď.) ako miesta spracovania či transformácie dát a informácií [2; 4].

Pojem **sieťová infraštruktúra** chápeme ako súhrn všetkých zariadení a sieťových prvkov, ktoré sú použité pri realizácii ICT prostredia a slúžia k vytváraniu a podpore informačného systému [1].

Súčasťou sieťovej infraštruktúry je **počítačová sieť**, ktorá slúži k realizácii komunikačného prostredia medzi užívateľmi siete [1].

Zraniteľnosť je slabá stránka, úmyselná chyba alebo neúmyselný nedostatok vo výpočtovej logike (napr. v kóde) zistená v softwarových alebo hardwarových komponentoch, ktorá predstavuje potencionálne bezpečnostné riziko zneužiteľné útočníkom pre škodlivú činnosť. Ak je zraniteľnosť zneužitá, vedie k negatívnemu vplyvu na dôvernosť, integritu a dostupnosť. Zraniteľnosti sú buď známe a publikované, ale výrobcom neošetrené, alebo skryté a neobjavené [5; 6; 8].

Zneužitie (**exploit**) je kód alebo software, ktorý využíva zraniteľnosť operačného systému alebo aplikácie a spôsobuje ich nežiadúce správanie alebo neočakávaný a nepovolený spôsob používania programov, počítačov alebo systémov [5; 8].

Hrozby definujeme ako zneužitie zraniteľností aktív za účelom vytvorenia škody. Hrozba je akákoľvek potencionálna okolnosť alebo udalosť, ktorá môže mať nepriaznivý vplyv na aktíva prostredníctvom neoprávneného prístupu, zničenia, zverejnenia, modifikácii alebo vymazania údajov alebo nedostupnosti služby [1; 7; 8].

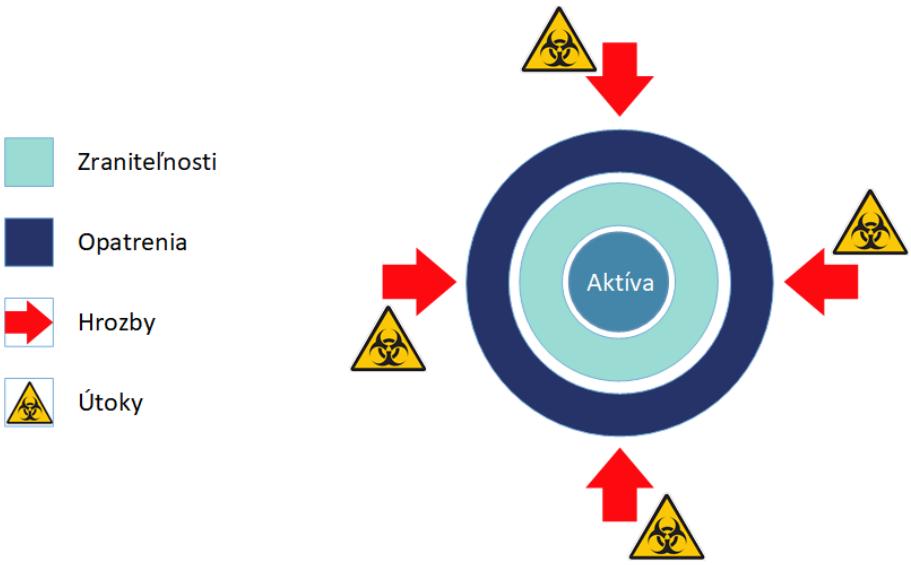
Viac informácií o hrozbách a ich rozdelení nájdete v ďalších častiach.

Opatrenie je proces alebo aktivita, ktorá vedie k zníženiu rizika vybraných hrozieb pre zaistenie bezpečnostných požiadaviek kladených na systém [1; 8].

Preventívne opatrenie je opatrenie, ktoré slúži k odstráneniu potencionálnej nezhody alebo hrozby [1].

Riziko je možnosť, že zraniteľnosť aktíva bude zneužitá určitou hrozbou, ktorá následne spôsobí škodu pre vlastníka aktíva [1; 8].

Dopad je následok pôsobenia hrozby a vznik určitej škody [1].



Obrázok 1: Prvky rizika
Zdroj: Vlastné spracovanie podľa [9]

Bezpečnostná udalosť je identifikovaný stav systému, služby alebo siete, ktorý môže spôsobiť alebo viesť k porušeniu pravidiel definovaných k ochrane – bezpečnostnej politiky – alebo k zlyhaniu bezpečnostných opatrení [1; 8].

Bezpečnostný incident označuje neštandardnú bezpečnostnú udalosť, ktorá vedie k narušeniu bezpečnostných politík, pravidiel alebo zásad v organizácii [1; 8].

1.1.1 Informačná bezpečnosť

Informačná bezpečnosť alebo takisto aj bezpečnosť informácií rieši ochranu informácií pred ich stratou, zničením, alebo krádežou a rovnako sa zameriava na zachovanie a zaistenie dôvernosti, integrity a dostupnosti informácií. Informačná bezpečnosť môže chrániť aj vlastnosti ako nepopierateľnosť, autentickosť, zodpovednosť a spoľahlivosť [1; 4; 8].

Je potrebné zmieniť pojmy ***bezpečnosť organizácie*** a ***bezpečnosť IS/ICT***, ktoré sú vo vzájomnou vzťahu s informačnou bezpečnosťou [1].

Úlohou **bezpečnosti organizácie** je zabezpečenie objektu a takisto majetku organizácie. Vo vzťahu s informačnou bezpečnosťou a bezpečnosťou IS/ICT je bezpečnosť organizácie nadradená a tým pádom zahŕňa tieto dva pojmy [1].

Bezpečnosť IS/ICT zabezpečuje len aktíva informačného systému, ktoré sú podporované informačnými a komunikačnými technológiami [1].

Obrázok 2: Jednotlivé úrovne bezpečností v organizácii
Zdroj: Vlastné spracovanie podľa [1]

V definícii termínu informačná bezpečnosť sú zmienené tri základné atribúty, ktoré majú byť zaistené – dôvernosť, integrita a dostupnosť. Tieto atribúty sú známe ako CIA triáda (Confidentiality, Integrity, Availability) [2; 10].

Dôvernosť sa týka obmedzenia prístupu k informáciám a ich sprístupnenie iba oprávneným používateľom, ako aj zabránenie prístupu neoprávneným používateľom [6].

Integrita sa týka správnosti, kompletnosti a pravdivosť informácií [6; 10].

Dostupnosť sa vzťahuje na dostupnosť informačných zdrojov a informácií ako takých pre autorizovaných používateľov. Dostupnosť ovplyvnenej komponenty znižujú útoky spotrebúvajúce šírku pásma siete, cykly procesorov alebo miesto na disku [6; 10].

1.1.2 Kybernetická bezpečnosť

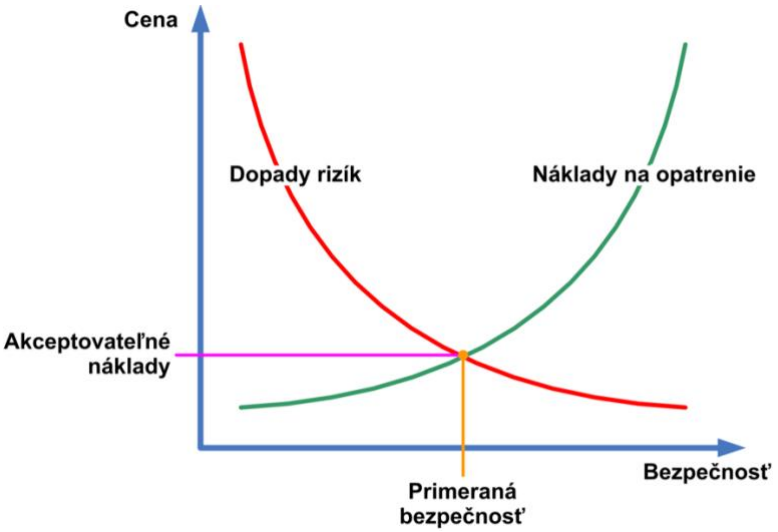
Kybernetická bezpečnosť je schopnosť brániť alebo chrániť používaný kybernetický priestor pred kybernetickými útokmi. Rovnako je možné kybernetickú bezpečnosť

definovať ako komplex právnych, technických, organizačných a vzdelávacích prostriedkov, ktoré zaisťujú ochranu kybernetického priestoru. Rozdiel oproti informačnej bezpečnosti sa nachádza v perimetri. Zatiaľ čo informačná bezpečnosť sa týka organizácie ako celku, do ktorej zahŕňame fyzickú, personálnu, komunikačnú a organizačnú bezpečnosť, kybernetická bezpečnosť sa týka celého kybernetického priestoru [8; 10; 11].

Kybernetický priestor môžeme nazvať ako globálnu doménu v informačnom prostredí, ktorá pozostáva zo vzájomne prepojenej siete infraštruktúr informačných systémov, telekomunikačných sietí, počítačových systémov a zabudovaných procesorov a radičov. Je to digitálne prostredie, ktoré umožňuje vznik, spracovanie a výmenu informácií pomocou siete Internet [8; 11; 12].

Útok je akákoľvek škodlivá činnosť či pokus o získanie neoprávneného prístupu k systémovým službám, zdrojom alebo informáciám či pokus o vystavenie hrozbe, zmenu, odcudzenie alebo zničenie informácií alebo aktív so snahou o narušenie integrity systému [8; 11].

Z **kybernetický útok** považujeme útok prostredníctvom kybernetického priestoru. Je zameraný na IT podnikovú infraštruktúru a jej využívanie kybernetického priestoru. Účelom kybernetického útoku je narušenie, deaktivácia, zničenie alebo škodlivé riadenie IT podnikovej infraštruktúry alebo poškodenie a získanie citlivých dát a informácií [8; 11].



Obrázok 3: Graf primeranej bezpečnosti za akceptovateľné náklady
Zdroj: Vlastné spracovanie podľa [10]

1.2 BEZPEČNOSTNÉ HROZBY

Definícia bezpečnostných hrozieb je uvedená v predošlej časti. V tejto podkapitole sa nachádza rozdelenie bezpečnostných hrozieb podľa prednášky *Bezpečnostné hrozby* od Ing. Viktora Ondráka PhD. a rozdelenie typov bezpečnostných hrozieb podľa dokumentu *Threat Landscape and Good Practice Guide for Internet Infrastructure* od Agentúry Európskej únie pre bezpečnosť sietí a informácií (súčasný názov: Agentúra Európskej únie pre kybernetickú bezpečnosť) – ENISA. Táto podkapitola bude medzistupňom ku podkapitole, ktorá nasleduje ihneď za ňou – *Typy kybernetických útokov*.

1.2.1 Rozdelenie bezpečnostných hrozieb

Bezpečnostné hrozby môžeme posudzovať z veľkého množstva hľadísk a prakticky nie je možné dosiahnuť úplného vymenovania [13].

Jedným z možných rozdelení podľa určitých kritérií môže byť nasledovné:

- **podľa zdroja pôsobenia**:
  - vnútorné,
  - vonkajšie:
    - spôsobené ostatnými aktívami,
    - z vnútra vlastnej organizácie,
    - z okolitého sveta,
- **podľa úmyslu**:
  - náhodné,
  - neúmyselné,
  - úmyselné,
- **podľa pôvodu**:
  - prírodné,
  - spôsobené človekom,
  - spôsobené iným zariadením,
- **podľa toho, na aké druhy aktív pôsobia**:
  - na hardware,
  - na počítačovú sieť,
  - na operačný systém,

    - na aplikácie,
    - na informácie,
    - na užívateľa,
- **podľa smerovania na bezpečnostné atribúty**:
    - dostupnosť,
    - integrita,
    - dôvernosť,
- **podľa motivácie útočníka**:
    - za účelom získania finančného prospechu,
    - za účelom získania konkurenčnej prevahy,
    - za účelom dokázania schopností,
    - za účelom odplaty
    - z dôvodu neplnenia povinností [13].

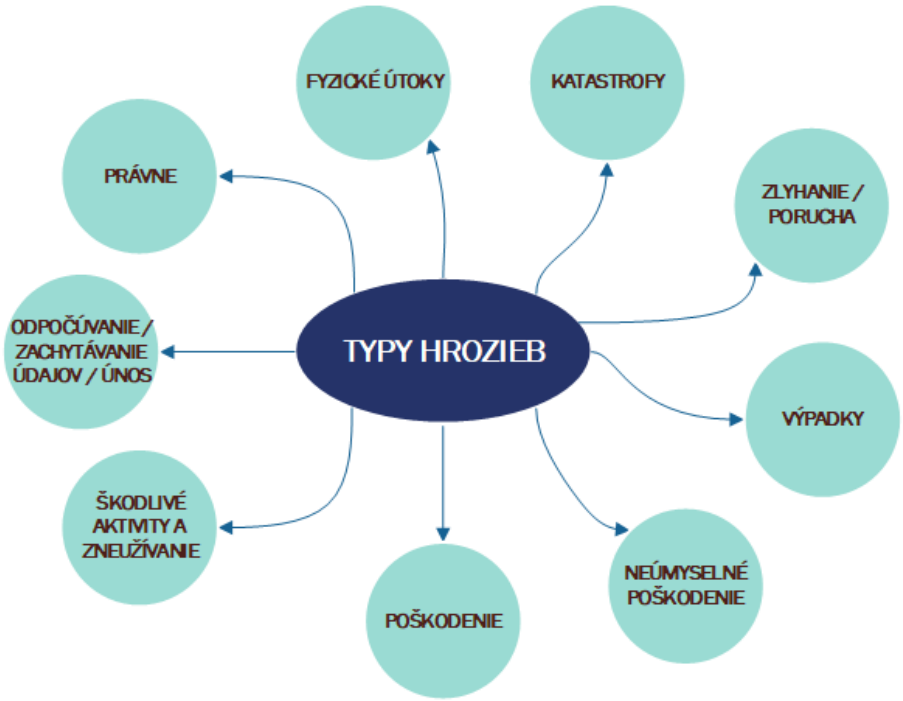
1.2.2 Typy bezpečnostných hrozieb

Bližšie sa v tejto diplomovej práci budem zaoberať typmi bezpečnostných hrozieb podľa agentúry ENISA. Navyše časť *Škodlivé aktivity a zneužívanie* bude potrebným medzistupňom k prechodu do ďalšej podkapitoly.

Rozdelenie typov hrozieb z vybranej štúdie je zamerané prevažne na hrozby kybernetickej bezpečnosti. Rovnako však toto rozdelenie počítať aj s bezchybnou prevádzkou, na ktorú sú potrebné aj fyzické aktíva a preto predpokladá toto rozdelenie aj niekoľko špecifických hrozieb, ktoré sa netýkajú informačných technológií. Každý typ hrozby predstavuje zdrojovú príčinu hrozby [7].

Typy hrozieb boli rozdelené do hlavných kategórií, ktoré sú rozšírené o ďalšie podkategórie. Hlavnými kategóriami sú **fyzické útoky**, **katastrofy**, **zlyhanie** alebo **porucha**, **výpadky**, **neúmyselné poškodenie**, **poškodenie**, **škodlivé aktivity** a **zneužívanie**, **odpočúvanie**, **zachytávanie údajov** a **únos**, **legálne hrozby** [7].

Ku každej kategórii bude uvedený stručný popis a vybrané príklady. Pri niektorých kategóriách bude opis detailnejší. Vyššie zmienené typy hrozieb môžete vidieť na obrázku na nasledujúcej strane.



Obrázok 4: Typy hrozieb
Zdroj: Vlastné spracovanie podľa [7]

Prvou kategóriou sú **fyzické útoky**. Tieto útoky chápeme ako úmyselné ofenzívne akcie, ktorých cieľom odhaliť, odcudziť, zmeniť, deaktivovať, zničiť alebo získať neoprávnený prístup k fyzickým aktívam. Medzi fyzické aktíva môžeme zaradiť hardware, sieťové a komunikačné prvky alebo celú infraštruktúru. Tento typ hrozby je aplikovateľný pre všetky druhy infraštruktúr. Medzi tento typ útokov môžeme zaradiť krádež , vandalizmus, únik informácií, neautorizovaný fyzický prístup apod. [7]

Katastrofy môžeme považovať za vážne narušenie fungovania nie len organizácií, ale aj celej ľudskej spoločnosti. Katastrofy môžeme rozdeliť na dve hlavné časti – prírodné katastrofy, ktoré nie sú priamo vyvolané človekom a environmentálne katastrofy zapríčinené človekom. Tieto druhy sa týkajú ktorýchkoľvek aktív. Medzi katastrofy môžeme zaradiť povodne, požiare, zemetrasenia, znečistenie, prach alebo korózie [7].

Zlyhania alebo **poruchy** sú jednými z hlavných podmienok nefunkčnosti aktív sieťovej infraštruktúry. Častými zlyhaniami alebo poruchami chyby softwaru, chyby konfigurácie alebo zlyhania a poruchy sieťových zariadení, komunikačných liniek a systémov [7].

Ďalšou typom hrozby sú **výpadky**. Výpadky chápeme ako neočakávané prerušenie služieb alebo pokles kvality pod požadovanú úroveň. To môže zahŕňať všetky druhy

aktív, vrátane ľudských zdrojov. Zaraďujeme sem sieťové výpadky, výpadky chladenia, strata energie alebo prepätie, ale aj nedostatok zdrojov (napr. kapacita úložísk) [7].

Neúmyselným poškodením sa vzťahuje na spôsobenie ujmy, zničenie alebo škoda na majetku či osobe v dôsledku nepredvídanej udalosti alebo neúmyselnej nehody. Zvyčajne býva spôsobené neznalosťou, neopatrnosťou alebo neplnením povinnosti. Môžeme sem zaradiť úniky dát a informácií, nesprávne používanie alebo správu zariadení a systémov, používanie informácií z nespoľahlivých zdrojov alebo neúmyselné zmeny údajov v informačných systémoch [7; 13].

Poškodenie je v tomto kontexte brané podobne ako neúmyselné škody, avšak prikladá sa určitý úmysel. Poškodenie má za následok chybu, zlyhanie alebo zníženie užitočnosti. Primárne je tento typ hrozby zameraný na aktíva informačných technológií. Pri poškodení hrozí strata integrity citlivých informácií, s ňou spojená možná strata reputácie, zničenie záloh a zariadení apod. [7]

Ďalším typom hrozieb sú **právne hrozby**. Môžu to byť predpokladané, zamýšľané alebo práve prebiehajúce kroky tretích strán (zmluvné alebo iné), ktorých cieľom je zakázať konanie alebo nahradiť škodu na základe uplatniteľného práva. Medzi tento typ hrozieb radíme porušovanie zákonov, súdnych príkazov a nedodržiavanie zmluvných požiadaviek, ktoré vykonávajú poskytovatelia služieb sieťovej infraštruktúry alebo sú im pripisované [7].

Odpočúvanie, **zachytávanie** a **únos**. Tieto typy hrozieb sa vzťahujú na skupinu akcií, ktorých cieľom je počúvať, prerušovať alebo ovládať komunikáciu tretích strán bez akéhokoľvek súhlasu. Vieme sem zaradiť zachytávanie informácií spojené s útokmi, ako napr. man-in-the-middle alebo rôzne „injection“ sieťové útoky [7].

Posledným a pre túto diplomovú prácu najdôležitejším typom hrozby sú **škodlivé aktivity** a **zneužívanie**. Sú to úmyselné činnosti, ktoré sa zameriavajú na systémy informačných a komunikačných technológií (ICT), infraštruktúru a počítačové siete s cieľom zmeniť, ukradnúť alebo zničiť určitý cieľ. Do tejto kategórie zaraďujeme hrozby, ktoré sú všeobecne označované ako kybernetické útoky a k ním súvisiace aktivity. Patria sem nežiadané e-mailové správy, malware a vírusy potencionálne nežiadúci software (napr. adware), zneužitie úniku citlivých dát a informácií, neautorizované aktivity, útoky nedostupnosti služby (DoS a DDoS), sociálne inžinierstvo

(napr. phishing), vzdialené škodlivé aktivity, zneužívanie softwarových chýb (chyby jadra systému alebo vyrovnávacej pamäte), zneužívanie validačných chýb (SQL injection, Cross site scripting, Cross site request forgery) a mnohé ďalšie [7].

O týchto a mnohých ďalších podobných škodlivých aktivitách a kybernetických útokoch bude popísané v nasledujúcej podkapitole.

1.3 TYPY KYBERNETICKÝCH ÚTOKOV

Súčasťou tejto podkapitoly je súhrn škodlivých aktivít a kybernetických útokov, ktoré sú obsiahnuté v ostatných častiach diplomovej práce. Ich znalosť uľahčí pochopiť problematiku preberanú v tejto práci.

Vektor útoku chápeme ako cestu či techniku, pomocou ktorej útočníci získajú neautorizovaný prístup k zariadeniu alebo sieti na škodlivé účely. Sú zneužívané nedostatky, chyby a zraniteľnosti v systéme alebo sieti, vrátane ľudských prvkov. Príkladom vektoru útoku môže byť zneužite zraniteľnosti webového prehliadača cez vyskakovacie okná alebo aj e-mailové prílohy [1; 14].

Útoky nultého dňa (zero-day attacks) sú kybernetické útoky proti zraniteľnosti aplikácie alebo operačného systému, ktorá nie je známa alebo je nenahlásená. Názov tohoto útoku pochádza zo skutočnosti, že samotný útok začal „nultým dňom“ verejného povedomia a častokrát ešte skôr, ako si to samotný vendor uvedomil. Útoky nultého dňa sú veľmi účinné, pretože môžu zostať nezistené po dlhú dobu. Zvyčajne to býva niekoľko mesiacov až niekoľko rokov. Dokonca aj potom, ako je útok identifikovaný a vendor informovaný, náprava zraniteľnosti môže trvať niekoľko dní až týždňov [15].

Škodlivý software alebo kód (Malicious software – Malware) je všeobecný pojem pre akýkoľvek druh počítačového softwaru so škodlivým úmyslom. Škodlivým úmyslom rozumieme narušenie dôvernosti, integrity a dostupnosti údajov, aplikácií alebo operačného systému alebo poškodenie či narušenie činnosti počítača, prebratie kontroly nad počítačovým systémom, vypnutie určitých funkcií a zhromažďovanie či ukradnutie citlivých informácií. Všeobecne ide o spôsobenie škody. Medzi malware môžeme zaradiť počítačové vírusy a červy, Trojské kone, ransomware, rootkity, spyware a mnohé ďalšie [5; 11; 15; 16].

Pre vysvetlenie a urovnanie si znalostí, budú ďalej zmienené aj počítačové vírusy a červy.

Počítačový vírus je typ škodlivého kódu alebo súbor počítačových inštrukcií, ktorý sa šíri vložením svojej kópie do iného počítačového súboru alebo programu, aby sa následne mohol replikovať a šíriť ďalej z jedného počítača na druhý. Takmer všetky vírusy sú pripojené k tzv. spustiteľnému súboru, čo znamená, že síce môže v systéme existovať, avšak nebudú aktívne až po interakciu užívateľa (interakciou rozumieme spustenie alebo otvorenie škodlivého súboru alebo programu). Následne môže spôsobiť nežiadúcu nebezpečnú činnosť spojenú napríklad s poškodením alebo odstránením údajov alebo softwaru v počítači. Vírusy sa šíria keď je dokument, súbor alebo software, ku ktorému sú pripojené, prenesený z jedného počítača na druhý pomocou siete, disku alebo infikovaných e-mailových príloh [5; 8; 11; 15; 17].

Počítačový červ je veľmi podobným druhom malwaru ako počítačový vírus. Replikuje sa sám, zvyčajne prostredníctvom zraniteľností v operačných systémoch, z počítača na počítač bez potreby akejkoľvek intervencie zo strany užívateľa. Súhrnne môžeme počítačový červ označiť ako autonómny program, ktorý sa rozmnožuje a replikuje sám. Pokročilejšie červy využívajú šifrovacie a ransomware technológie na poškodenie vybraných cieľov [5; 11; 15; 17].

Trojský kôň je program, ktorý sa javí, že vykonáva užitočnú funkciu, ale namiesto toho vykonáva skrytú, častokrát škodlivú funkciu. Na rozdiel od vírusov a červov, nemá Trojský kôň replikačnú funkciu a preto sa nemôže voľne šíriť do iných zraniteľných počítačov. Trojské kone sa šíria prostredníctvom interakcie používateľa (interakciou rozumieme otvorenie e-mailovej prílohy, stiahnutie alebo spustenie súboru z internetu). Tento druh malwaru zvykne vytvárať alebo zahŕňať tzv. **zadné vrátka (backdoor)**, ktoré poskytujú útočníkom obídenie bežných bezpečnostných prístupových opatrení či dokonca kontrolu nad cieľovým zariadením s administrátorskými oprávneniami. To môže viesť k vymazaniu súborov, úniku informácií alebo k aktivácii a šíreniu iného škodlivého softwaru. To všetko bez akéhokoľvek súhlasu alebo vedomia užívateľa [5; 15; 16; 17].

Ransomware je typ škodlivého softwaru, ktorý má za úlohu zablokovať prístup k údajom obete, zašifrovať ich alebo hroziť zverejnením týchto údajov a teda vydierať obeť. Za obnovenie prístupu k údajom alebo ich dešifrovaniu je vyžadované výkupné od obete. Zaplatenie výkupného nezaručuje, že údaje budú sprístupnené alebo dešifrované [5; 17].

Rootkit je typ škodlivého softwaru, ktorý umožňuje útočníkovi získať privilegovaný prístup k systému s najvyššími oprávneniami na úrovni „root“. Je využívaný na skrytie určitých objektov a aktivít v systéme, ako napríklad skrytie existencie škodlivého softwaru, súborov, služieb, ovládačov sieťových pripojení a iných systémových komponentov. Existujú pre operačné systémy Windows, Linux a MacOS X [5; 11; 17].

Spyware je druh škodlivého softwaru, ktorá slúži na monitorovanie užívateľskej činnosti a na získavanie a zhromažďovanie informácií o osobe alebo organizácii bez ich súhlasu a vedomia. Tieto informácie môžu byť zaslané inému subjektu bez akéhokoľvek súhlasu a môžu byť zneužité. Na rozdiel od predchádzajúcich typov malwaru, spyware nepoškodzuje operačný systém, programy alebo súbory [5; 17; 18].

Stalkerware je druh spywaru, ktorý je používaný ako nástroj rodičovskej kontroly na sledovanie detí, ale aj príbuzných alebo kolegov. Stalkerware býva nainštalovaný bez súhlasu používateľa alebo vlastníka zariadenia a poskytuje odosielanie osobných údajov obete – geolokačných údajov, obrázkov a videí apod. – na príkazový server. Predstavuje preto riziko zneužitia a úniku osobných údajov pre tretie strany a preto je jeho distribúcia prostredníctvom legitímnych obchodov s aplikáciami zakázaná, za nedodržiavanie etických noriem [18].

Sociálne inžinierstvo je útočná metóda, ktorú využívajú útočníci na manipulovanie a prinútenie obetí k vykonaniu činnosti (napr. stiahnutiu a otvoreniu škodlivých súborov), ktorá môže viesť k odhaleniu informácií (napr. heslá) alebo neoprávnenému prístupu k systémov. Jedná sa skôr o netechnické narušenie bezpečnosti, ktoré spolieha na interakciu užívateľa (napr. kliknutie na infikovanú e-mailovú prílohu alebo na odkaz na kompromitovanú stránku) [11; 17; 18].

Phishing je jednou z techník sociálneho inžinierstva. Jedná sa o podvodnú metódu, ktorej cieľom je získanie osobných informácií od obete pomocou klamlivých počítačových prostriedkov. Zaslaný e-mail sa javí legitímne, aby bola zvýšená úspešnosť interakcie užívateľa. Kliknutím na odkaz vložený do e-mailu alebo otvorenie škodlivej prílohy spôsobí stiahnutie exploitu alebo malwaru. Inou možnosťou je, že vložený odkaz presmeruje obeť na škodlivú webovú stránku, na ktorej má zadať osobné informácie, ako napríklad prihlasovacie údaje, heslá, PIN atď. [5; 11]

Spear phishing je sofistikovanejšia verzia útoku phishing. Jedná sa o cielený pokus, ktorý využíva informácie o obeti, ktoré boli dopredu získané alebo využíva e-mail, ktorý pôsobí, že bol odoslaný od jednotlivca (napr. kolegu) alebo organizácie, ktorú obeť pozná. Tým sa javí spreaphishingový útok dôveryhodnejšie a preto má vyššiu pravdepodobnosť na úspech [5; 8].

1.3.1 Kybernetické útoky a škodlivé aktivity uvedené v analýze portálu ThreatGuard

Ako už názov podkapitoly naznačuje, informácie v nej uvedené budú odkazovať na kapitolu analytickej časti diplomovej práce *Analýza reportov z portálu ThreatGuard*, ktorej súčasťou je analýza reportov tejto služby za rok 2019. K jednotlivým hrozbám, respektíve útokom, budú uvedené preklady, krátky alebo detailnejší popis.

Information Exposure (Odhalenie informácií).

Arbitrary Code Execution (Spustenie ľubovoľného kódu) – táto hrozba zahŕňa v analýze lokálne aj vzdialené spustenie ľubovoľného kódu a rovnako útoky code a command injection (doslova „vstrekovanie“ (vloženie) kódu alebo príkazu).

Code / Command injection sa týka manipulovania zraniteľného programu s cieľom vykonať ľubovoľný škodlivý kód, ktorý je „vstreknutý“ do bežiaceho procesu tohoto programu. To je možné, ak program využíva napríklad techniku, pri ktorej sú príkazy operačného systému predávané priamo na server. To môže umožniť útočníkovi umiestniť vytvorený škodlivý vstup (kód alebo príkaz), ktorý bude spustený v bezpečnostnom kontexte procesu webového servera, ktorý je častokrát dostatočne výkonný na to, aby útočník mohol kompromitovať celý server [18; 19].

Authentication Bypass (Obídenie autentifikácie). Proces, ktorým pristupuje aplikácia k úložisku, je zvyčajne rovnaký, bez ohľadu na to, či bol tento vstup vyvolaný akciami správcu aplikácie alebo neoprávneného útočníka. Webová aplikácia funguje ako riadenie prístupu k údajom a na základe typu používateľského účtu, vytvára dotazy na získavanie, pridávanie alebo úpravu údajov v dátovom úložisku. Úspešný „vstrekovací“ útok, ktorý modifikuje dotaz, môže následne obísť riadenie prístupu a získať neoprávnený prístup [19].

Buffer Overflow (Pretečenie vyrovnávacej pamäte) je chyba v programe, ktorá sa vyskytne pri pokuse o umiestnenie vstupu (bloku údajov) do pamäte, ktorý však prevyšuje množstvo priestoru (pridelenú kapacitu), ktorý je naň vyhradený a môže potencionálne dôjsť k prepísaniu a poškodeniu údajov v pamäti. Útočníci využívajú túto chybu na zlyhanie systému (napr. DoS – odmietnutie služby) alebo na vloženie špeciálne vytvoreného kódu, ktorý je spustený s rovnakými právami ako aplikácia a ktorý im umožňuje získať kontrolu nad systémom [11; 18].

Cross-site scripting (XSS) je zraniteľnosť či typ útoku, ktorá umožňuje útočníkom, po nájdení bezpečnostnej chyby, vložiť škodlivý kód na webovú stránku. Vložené skripty môžu ohroziť dôvernosť a integritu dátových prenosov medzi webovou stránkou a klientom. Škodlivý kód vložený na webovej stránke sa spustí na zariadení obete v tom momente, keď užívateľ otvorí danú stránku a následne ho pripojí na webový server útočníka. Ak webové stránky zobrazujú údaje dodané užívateľom na základe žiadostí alebo formulárov, môže dôjsť k získaniu osobných údajov užívateľov alebo obsahu databázy či dokonca k obídeniu bezpečnostných prvkov webovej aplikácie [8; 11; 18].

Cross-site Request Forgery (CSRF) je typ útoku, pri ktorom kybernetickí zločinci používajú obmedzenia HTTP protokolu. Útočník vytvorí na prvý pohľad neškodnú webovú stránku, ktorá ma za úlohu, aby po otvorení tejto stránky webový prehliadač používateľa odoslal žiadosť priamo zraniteľnej aplikácii, ktorá následne vykoná neplánovanú akciu, ktorú útočník môže použiť pre svoj účel. Ak je obeťou bežný používateľ, úspešný útok CSRF môže prinútiť používateľa vykonať žiadosť o zmenu stavu, ako napríklad zmenu e-mailovej adresy na prihlásenie. Ak je obeťou administrátorský účet, CSRF môže ohroziť celú webovú aplikáciu [18; 19, 20].

Deserialization of untrusted data (Deserializácia nedôveryhodných údajov). Deserializácia je rekonštrukcia pôvodného objektu zo sekvencie bitov získaných serializáciou, ktorá sa zvyčajne používa na prenos multidimenzionálnych dátových polí vo forme jednorozmerného poľa – textového alebo binárneho súboru. Deserializácia nedôveryhodných údajov nastáva vtedy, keď aplikácia deserializuje nedôveryhodné údaje (údaje kontrolované útočníkom) bez dostatočného overenia, či výsledné údaje budú platné. To môže umožniť útočníkom vykonávať neoprávnené činnosti, ako napríklad

zneužívanie aplikačnej logiky, odmietnutie služby alebo vykonanie ľubovoľného kódu [18; 20; 21].

Denial of Service (DoS – Nedostupnosť služby) je útok určený na preťaženie sieťovej prevádzky a následnú nedostupnosť fungovania webovej stránky, servera alebo iného sieťového prvku. Základom tohoto útoku sú falošné dotazy kladené serveru, na ktoré musí server odpovedať, čim zahlcuje linku, na ktorú sa mu vracajú neustále ďalšie pakety [1; 18].

Distributed Denial of Service (DDoS – Distribuovaná nedostupnosť služby) sa líši od útoku DoS jedine v tom, že škodlivý sieťový útok je vykonávaný pomocou viacerých počítačov súčasne [1; 18].

Out-of-bounds read / write (Čítanie / zápis mimo hranice) je vykonávané vtedy, keď software zapisuje / číta údaje pred začiatkom alebo za koncom učenej vyrovnávacej pamäte. Zápis mimo hranice môže mať za následok poškodenie údajov, zlyhanie softwaru alebo spustenie kódu. Čítanie mimo hranice zvyčajne umožňuje útočníkom čítať citlivé údaje z iných miest pamäte alebo spôsobiť zlyhanie softwaru [21].

Privilege Escalation (Eskalácia privilégií) chápeme ako zvýšenie úrovne prístupu k zdrojom systému dosiahnuté zneužitím zraniteľnosti v systéme alebo sieti (napr. nesprávna konfigurácia). Útočníci túto zraniteľnosť využívajú na získanie povolení na vyššej úrovní, ktoré im umožnia kompromitovať údaje alebo využívať výpočtovú silu zariadenia obete [18; 22].

SQL Injection je útok, ktorým je „vstrekovaný“ škodlivý kód do dotazu SQL zaslaného cieľovému zariadeniu. SQL injection je bežný spôsob kompromitovania internetových zdrojov a aplikácií, ktoré používajú databázy. Tento typ útoku umožňuje útočníkom infiltrovať neoprávnené znaky do SQL príkazov autorizovaného užívateľa, čo následne umožní získať neoprávnený prístup k citlivým údajom z databázy, upravovať databázové údaje (funkciami Insert / Update / Delete) alebo vykonávať administrátorské operácie (napr. vypínanie DBMS – systému riadenia bázy dát) [8; 18; 20].

1.4 TYPY ÚTOČNÍKOV

V poslednej podkapitole *Typy útočníkov* budú zmienené jedno z možných rozdelení kybernetických aktérov. Podkapitola bude takisto obsahovať rozdelenie hackerov.

1.4.1 Rozdelenie útočníkov

Hacker je osoba, ktorá sa zaoberá preskúmavaním detailov programových systémov, počítačov a počítačových sietí [8; 23].

Cracker je osoba, ktorá zneužíva svoje znalosti k tomu, aby sa pokúsila získať neoprávnený prístup k informačnému systému, za účelom odhalenia citlivých informácií, čím tak porušuje zákon [8; 23].

Insider je osoba s autorizovaným a legálnym prístupom, v rámci bezpečnostnej domény, do informačného alebo komunikačného systému organizácie (väčšinou zamestnanec), ktorá má potenciál na poškodenie týchto systémov alebo organizácie. Takáto osoba môže zničiť, odcudziť, zverejniť alebo modifikovať citlivé dáta a informácie alebo spôsobiť nedostupnosť služby [8; 11].

Hacktivist (Haktivista = Hacker + aktivista) je osoba, ktorá využíva počítačové technológie ako prostriedok slúžiaci na protest, podporu alebo popularizáciu sociálne orientovaných nápadov. Haktivisti dodržujú etické princípy a nenarúšajú počítačové systémy, neporušujú právo ľudí na prístup k informáciám a ani nešíria strach a nenávisť [15; 18].

Cyber criminal (Kybernetický zločinec) je osoba, ktorá nezákonne kradne údaje z počítača obete za účelom osobného finančného zisku [15].

Cyber terrorist (Kybernetický terorista) je osoba, ktorá pácha trestnú činnosť s využitím IT prostriedkov s cieľom vyvolať strach a nenávisť. Kontext útokov je častokrát extrémistický, nacionalistický a politický [8].

State-sponsored threat actor (Štátom sponzorovaný aktér hrozby) je osoba, kybernetický zločinec, ktorého zamestnáva štát, aby vykonával kybernetické útoky proti nepriateľom štátu, väčšinou na politicky motivované účely [15].

1.4.2 Druhy hackerov

V tejto časti podkapitoly *Typy útočníkov* sa nachádza rozdelenie hackerov do skupín podľa ich činností.

White hat, tiež nazývaný **etický hacker**, je osoba, IT odborník, ktorý sa dostáva do počítačových systémov a skúma ich, aby našiel zraniteľné miesta. Svoje zistenia a nájdené bezpečnostné chyby následne hlási vývojárom alebo osobe, ktorá si ho zmluvne najala a spolupracujú na opravení nájdených chýb. Motiváciou týchto osôb môže byť ako finančná odmena, tak aj altruizmus [18].

Black hat tiež nazývaný **cracker**, je osoba, ktorá zneužíva svoje vedomosti a zručnosti na vykonávanej trestnej činnosti. Trestnou činnosťou rozumieme vytváranie hackerských programov alebo webových stránok, zničenie alebo krádež údajov, šifrovanie informácií alebo vyradenie siete z prevádzky pre ostatných užívateľov. Motivácia týchto osôb je materiálny zisk alebo verejné uznanie [18; 23].

Grey hat je osoba, ktorá je kombináciou medzi White hat a Black hat, pretože zneužíva bezpečnostných chýb systémov alebo produktov k ich prieniku. Účelom týchto prienikov je upozornenie na zraniteľnosť administrátora a prípadne ponúknutie opravy chýb za finančnú odmenu. Pri tomto type hackera môže však hroziť aj k zverejneniu získaných citlivých informácií, čo môže byť príležitosťou pre páchanie trestnej činnosti [8; 23].

Blue hat je externá osoba alebo firma, ktorá sa zaoberá počítačovou bezpečnosťou a ktorá je najímaná pre otestovanie systému pred jeho spustením a uvedením na trh [23].

2 ANALÝZA SÚČASNÉHO STAVU

Obsahom kapitoly *Analýza súčasného stavu* je prehľad informačných a kybernetických hrozieb za rok 2019. Pre adekvátnosť výsledkov a získaných informácií z jednotlivých analýz, bude v tejto časti diplomovej práce porovnanie viacerých zdrojov a reportov, ktoré sú zamerané ako na malé, tak na stredné až veľké spoločnosti.

Prvou v poradí bude analýza informačno-kybernetických hrozieb z portálu ThreatGuard za rok 2019. Analýzou týchto hrozieb, získame výsledky a informácie predovšetkým pre české a slovenské spoločností. Je potrebné podotknúť, že ThreatGuard si nekladie ciel popísať všetky hrozby, ale informovať o tých dôležitých, aktuálne využiteľných a hlavne najrizikovejších, s vysokou závažnosťou, predovšetkým v regióne Českej a Slovenskej republiky. V tejto službe nie sú uvádzané teoretické a ťažko uplatniteľné postupy, ale závažné hrozby typicky s verejne známym exploitom apod. Podrobnejšej o tejto analýze a zdroji informácií bude popísané v podkapitole nižšie.

Pre širší záber výsledkov a pre doplnenie informácií, budú použité a následne zrovnávané reporty informačno-kybernetických hrozieb Kaspersky Lab, od výrobcu Kaspersky.

V reportoch tohto výrobcu sú spracovávané hrozby, ktoré boli identifikované veľkou škálou jeho produktov. Spektrum kategórií zákazníkov a hrozieb pôsobiacich na ich aktíva sa vďaka týmto dokumentom rozšíri od jednotlivca až po veľké, svetové spoločnosti. Pre účely tejto práce bude skupina *jednotlivci* nebraná v úvahu. Fúziou výsledkov analýz vznikne ucelený prehľad o informačných a kybernetických hrozbách za rok 2019.

Pre doplnenie informácií a rozšírenie pohľadu na danú problematiku budú v poslednej podkapitole analytickej časti uvedené najzávažnejšie mediálne správy roku 2019, týkajúce kybernetických útokov, ktoré sa objavili v českých médiách a zasiahli Českú republiku.

Na základe výsledkov a zistených informácií z tejto kapitoly bude vypracovávaná návrhová časť diplomovej práce, ktorá bude obsahovať predikcie a preventívne opatrenia pre spoločnosti na nasledujúci rok.

2.1 ANALÝZA REPORTOV Z PORTÁLU THREATGUARD

Na úvod podkapitoly je dôležité vytvoriť slovník výrazov, ktoré budú v tejto časti používané. Jedná sa o skratky a anglické výrazy, ktoré sú buď v službe ThreatGuard pravidelne používané, alebo je ich anglický ekvivalent vhodnejší použiť, pretože pri preklade do slovenského jazyka stratia technický a významový zmysel.

Zoznam výrazov:

vendor – predajca,

exploit – je kód alebo software, ktorý využíva zraniteľnosť operačného systému alebo aplikácie a spôsobuje ich nežiadúce správanie alebo neočakávaný a nepovolený spôsob používania programov, počítačov alebo systémov,

newsfeed – webová stránka alebo obrazovka, ktorá sa často aktualizuje (mení), aby zobrazovala najnovšie správy alebo informácie,

CSIRT – Computer Security Incident Response Team – je kyberbezpečnostná jednotka, ktorej cieľom je zabezpečiť primeranú úroveň ochrany a zabezpečenia verejnej správy a jej informačných systémov,

report – správa, oznam, hlásenie,

sandbox – bezpečnostné simulované prostredie slúžiace na oddelenie spustených programov, zvyčajne v snahe zmierniť zlyhanie systému alebo šírenie softwarových zraniteľností.

V tejto podkapitole analytickej časti diplomovej práce sa nachádza predstavenie a cieľ služby ThreatGuard. Následne bude zmienený spôsob selekcie a následného spracovania informácií na tomto portáli a taktiež ukážka tvorby jedného reportu pomocou jednotlivých zadávaných častí na portáli. V podkapitole bude takisto vysvetlené hodnotenie závažnosti zraniteľností pomocou CVSS skóre. Na záver podkapitoly sa nachádza sumárna analýza jednotlivých reportov vytvorený v tejto službe za rok 2019, ktorá je rozdelená na päť čiastkových analýz – analýza hrozieb (tretí a štvrtý kvartál), analýza najviac ohrozených (zraniteľných) vendorov a analýza najviac ohrozených

vendorov spoločne so skupinou ostatní, analýza aktív za rok 2019 s vyzdvihnutím posldených dvoch kvartálov v poslednej analýze.

V analýze bolo spracovávaných celkovo 333 reportov zo služby ThreatGuard za rok 2019. Výsledky analýz sa nachádzajú v nasledujúcich častiach tejto kapitoly.

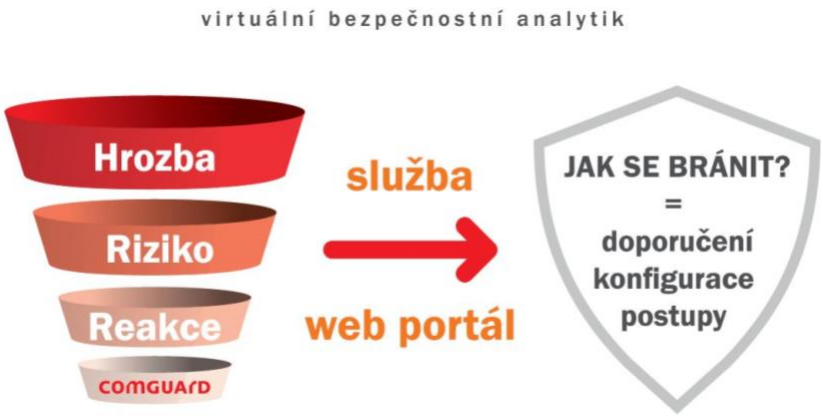
2.1.1 Predstavenie a cieľ služby ThreatGuard

Služba ThreatGuard je poskytovaná a prevádzkovaná českou spoločnosťou COMGUARD a.s., ktorá pôsobí v oblasti IT bezpečnosti a primárne sa zaoberá distribúciou s pridanou hodnotou. K spoločnosti COMGUARD a ich službe som sa dostal vďaka dlhodobej spolupráci Fakulty podnikateľskej VUT v Brne. Dostal som možnosť spracovávať údaje nachádzajúce sa v tejto službe a vytvoriť z nich ročnú analýzu a report, ktorých údaje nájdete v nasledujúcich častiach tejto práce. Analýza údajov navyše poskytne spoločnosti COMGUARD cenné informácie pri vývoji novej verzie služby ThreatGuard.

Je potrebné opäť podotknúť, že ThreatGuard si nekladie ciel popísať všetky hrozby, ale informovať o tých dôležitých, aktuálne využiteľných a hlavne najrizikovejších, s vysokou závažnosťou, predovšetkým v našom regióne. V tejto službe nie sú uvádzané teoretické a ťažko uplatniteľné postupy, ale závažné hrozby typicky s verejne známym exploitom apod.

Samotná služba je dostupná ako webová aplikácia sledujúca aktuálny vývoj IT hrozieb s optimalizáciou aj pre mobilné telefóny. Spoločnosť ju uvádza ako virtuálneho bezpečnostného analytika či ako stále dostupnú, aktuálnu a štruktúrovanú databázu hrozieb a opatrení. Tieto hrozby a opatrenia sú sumarizované a vyhodnocované tímom expertov, ktorý vyhodnocuje informácie z rôznych zdrojov. Medzi tieto zdroje patria *webové stránky, databázy exploitov, sociálne siete, newsfeed vendorov, CSIRT tímy* a ďalšie *verejné a neverejné médiá* a *aktuálne riešené incidenty v regióne*.

Výsledné reporty sprostredkúvané službou ThreatGuard sú zameriavané na malé, stredné a veľké spoločnosti. Spoločnosť COMGUARD má zákazníkov predovšetkým z Českej a Slovenskej republiky, avšak informácie nachádzajúce sa na ich webovom portáli dokážu vyriešiť problém takisto spoločnostiam mimo vyššie zmienených krajín, keďže obsahom analýzy hrozieb sú zraniteľnosti a vendori s globálnym pôsobením.



Obrázok 5: Doporučená architektúra
Zdroj: [24]

Z predchádzajúceho vyobrazeného obrázku vyplýva, že služba ThreatGuard nie je len že spravuje a filtruje bezpečnostné hrozby, ale takisto vydáva k daným hrozbám odporučenia a návody, ako danú hrozbu riešiť, napraviť či odstrániť.

2.1.2 Selekcia a spracovanie údajov v službe ThreatGuard

Ako už bolo zmienené v predchádzajúcej časti, služba ThreatGuard pracuje a vyhodnocuje informácie z rôznych zdrojov, ktorými sú *webové stránky*, *databázy exploitov*, *sociálne siete*, *newsfeed vendorov*, *CSIRT tímy* a ďalšie *verejné a neverejné médiá* a *aktuálne riešené incidenty v regióne*. Avšak takýchto zdrojov je veľký počet a úlohou služby ThreatGuard je tieto zdroje filtrovať.

K relevantnosti zistených hrozieb dopomáha odborný tím ThreatGuard, ktorý z uvedených zdrojov efektívne selektuje tie hrozby, ktoré sú adekvátne pre firemné prostredie predovšetkým v Českej a Slovenskej republiky. Do tohoto výberu spadajú vendori, zariadenia (informačné aktíva) a typy hrozieb relevantné pre dané prostredie. Všetky tieto kategórie sú triedené podľa vytvorených zoznamov odborníkmi spoločnosti COMGUARD, ktoré vznikli na základe viac ako 10 ročného pôsobenia a toho vyplývajúcich vedomostí a know-how tejto spoločnosti na trhu. V zoznamoch sa nachádzajú vendori a zariadenia, ktoré vznikli na základe analýz a komunikácie so svojimi zákazníkmi.

Hrozby typu *phishing*, *malware* a *ransomware* sú posudzované ako z hľadiska ich závažnosti, tak aj z regionálneho hľadiska. Pri týchto typoch hrozieb hrá veľkú rolu *geolokácia*, keďže sú spracovávané pre určitý región. Z toho vyplýva, na portáli

nenájdeme napríklad phishingový útok v cielený na Čínu, pretože tento útok nemá dopad pre náš región. Aj v takomto prípade sa preukazuje dôležitosť selekcie každej hrozby.

Dôležitým kritériom pri filtrovaní informácií je pridelená CVSS závažnosť, o ktorej bude detailnejšie zmienené v ďalšej časti diplomovej práce. Do služby ThreatGuard sú vyberané bezpečnostné hrozby, ktoré majú CVSS skóre v kvalitatívnom rozmedzí *stredný, vysoký* a *kritický*.

2.1.3 Tvorba reportu a súhrn jednotlivých častí

Na úvod je potrebné uviesť, že reporty sú v službe ThreatGuard spracovávané v troch jazykových variantoch – českom, slovenskom a v anglickom. Z dôvodu neodhalenia kompletne celej služby, nebudú v tejto časti diplomovej práce vymenované všetky súčasti služby, ktoré sú jej súčasťou a ktoré slúžia pre vypracovanie reportov.

Prvou časťou a dôležitým smerovačom pre zákazníka je uvedenie typu hrozby. Súčasná verzia služby pracuje s piatimi typmi hrozieb. Patria sem *ransomware, phishing, malware, DoS* (Denial of Service – nedostupnosť služby) a *vulnerabilty* (zraniteľnosť). O týchto hrozbách a ich podskupinách sa dočítate viac v teoretickej časti diplomovej práce.

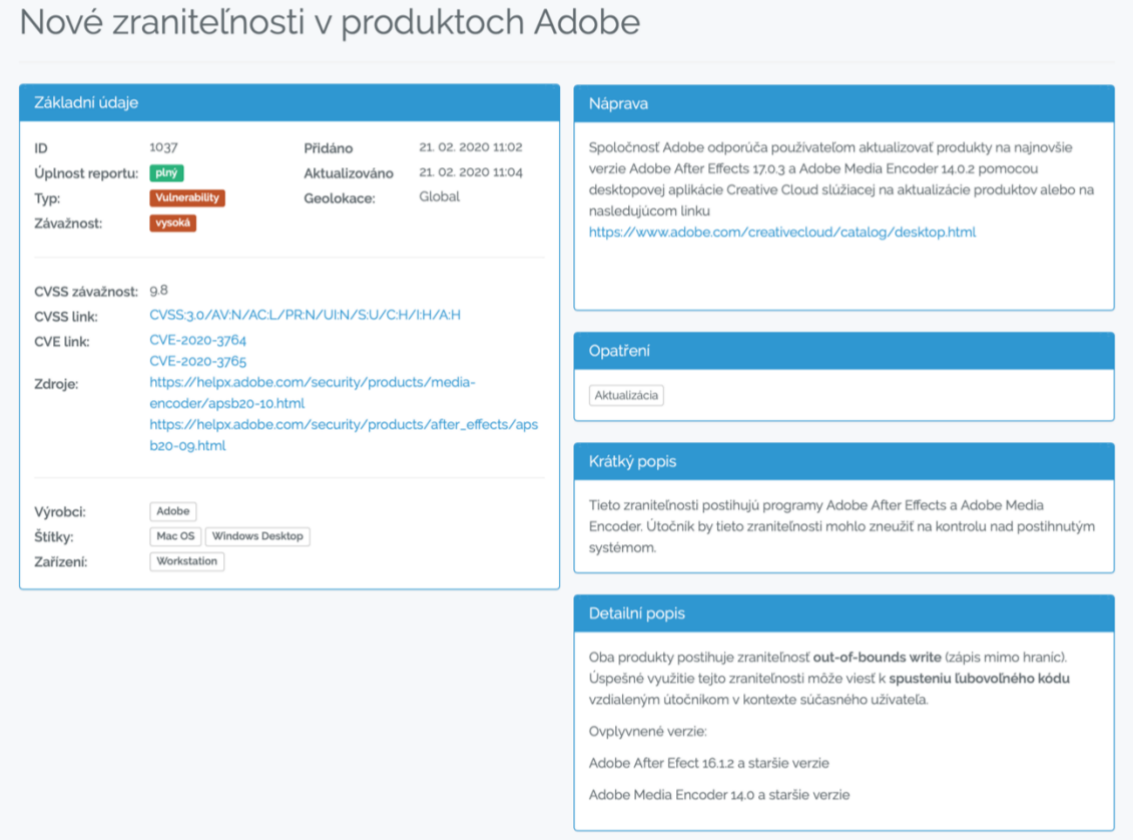
Ďalšou časťou je závažnosť hrozby. Služba ThreatGuard pracuje s tromi úrovňami závažností – *vysoká, stredná* a *upozornenie*. Kategória závažnosti *upozornenie* sa prevažne využíva pri hrozbách typu *ransomware*, *phishing* a *malware*, kde sa nevyskytuje CVSS skóre, ktoré je smerodajné pri určovaní závažnosti zraniteľností. V podkapitole *Hodnotenie závažnosti zraniteľností pomocou CVSS* budú úrovne závažností rozdelené trochu inak, avšak služba ThreatGuard si prispôsobila túto stupnicu podľa vlastných potrieb.

Časť portálu, ktorá zlepší orientáciu a z ktorej je zákazník schopný vyvodiť dôležitosť reportu pre jeho organizáciu, je rozsah pôsobnosti hrozby. V tejto časti sú určovaní vendori, ktorých produkty daná hrozba postihuje, štítky, ktoré dopomáhajú rozšíriť informácie o reporte a zariadenia, ktoré môžu byť daným typom hrozby napadnuté.

Pokiaľ predošlé časti zaujmú zákazníka, viac informácií zo služby získa v textovej časti reportu. Táto časť pozostáva z *názvu, krátkeho* a *detailného popisu* a *nápravy*. Náprava častokrát obsahuje odporúčanie vendora, ale takisto aj postup, ako zraniteľnosť napraviť

či odporučenie od odborníkov spoločnosti COMGUARD, ako pristupovať k danej hrozbe a aké činnosti je vhodné vykonať k zníženiu alebo úplnému predídeniu touto hrozbou.

Report obsahuje takisto kvantitatívne ohodnotenie v podobe vyššie zmieneného CVSS skóre. Viac informácií o tomto hodnotení je uvedených v nasledujúcej podkapitole.



Obrázok 6: Report vypracovaný v službe ThreatGuard - pohľad používateľa
Zdroj: [25]

Na obrázku možno vidieť stručnejší, avšak úplne vyplnený report vhodný pre ilustráciu do diplomovej práce. V takejto podobe ho môže vidieť zákazník (používateľ), ktorý je schopný v portáli, okrem prehliadania reportov, aj filtrovať reporty podľa svojho vlastného záujmu a to podľa kategórií *vendor*, *zariadenie*, *štítky*, *úplnosť reportu*, *závažnosť*, *typ hrozby*, *geolokácia* či *overenosť*.

2.1.4 Hodnotenie závažnosti zraniteľností pomocou CVSS

Common Vulnerability Scoring System (Spoločný systém hodnotenia zraniteľností), ďalej iba CVSS, je otvorený rámec na určovanie závažnosti zraniteľností softwaru. CVSS poskytuje spôsob, ako zachytiť základné charakteristiky zraniteľnosti a následne vytvoriť

ich premenu na číselné skóre. Numerické skóre je možné pretransformovať do kvalitatívnej reprezentácie, čo pomáha organizáciám správne posúdiť a uprednostniť svoje procesy riadenia zraniteľnosti. Kvalitatívnymi reprezentáciami sú hodnoty *nízka*, *stredná*, *vysoká* a *kritická* [6; 26].

Služba ThreatGuard, ako už bolo zmienené, pracuje pri filtrácii s hodnotami závažnosti zraniteľností *stredná*, *vysoká* a *upozornenie*, pričom kvalitatívnu hodnotu *nízka* vynecháva z dôvodu zamerania služby na spracovávanie závažnejších zraniteľností a hrozieb. Rovnako táto služba spája hodnoty *vysoká* a *kritická* do jednej a jednotne ju nazýva *vysoká* závažnosť zraniteľnosti. Kategória závažnosti *upozornenie* sa prevažne využíva pri hrozbách typu *ransomware*, *phishing* a *malware*, kde sa nevyskytuje CVSS skóre.

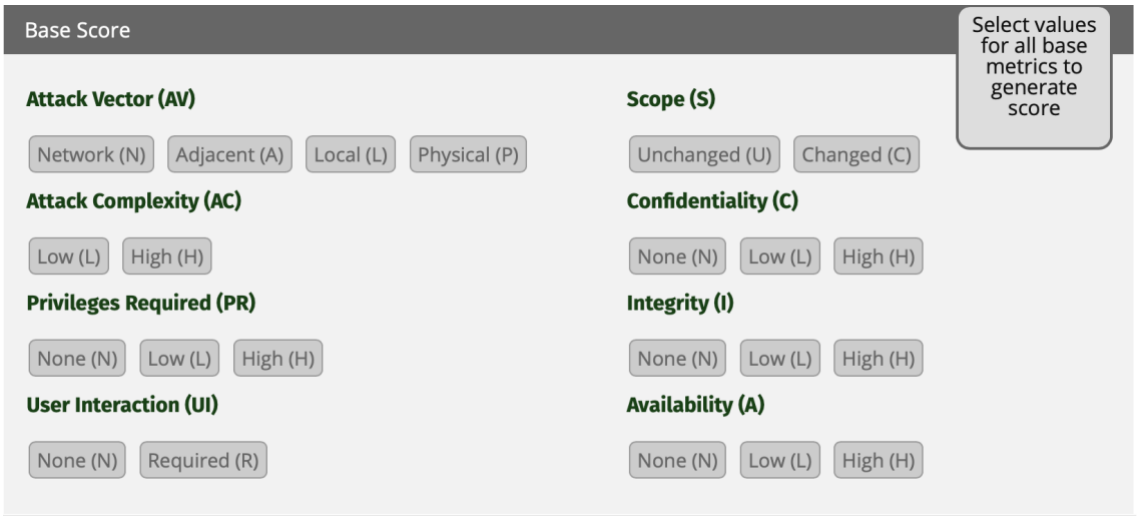
Tabuľka 1: Kvalitatívne a kvantitatívne hodnotenie závažnosti zraniteľnosti
Zdroj: Vlastné spracovanie podľa [6]

Závažnosť	Rozsah skóre
Žiadna	0.0
Nízka	0.1 – 3.9
Stredná	4.0 – 6.9
Vysoká	7.0 – 8.9
Kritická	9.0 – 10.0

2.1.5 Jednotlivé časti potrebné k zostaveniu CVSS skóre

CVSS skóre nie je vytvorené odhadom a aby mohlo byť pridelené k danej zraniteľnosti, musí byť vyskladané z niekoľkých metrík, ktoré ovplyvňujú celkovú závažnosť. Týchto metrík je celkovo 8 a sú súčasťou tzv. Base Score (základného skóre), ktoré je možné zostaviť a vypočítať pomocou online kalkulačky. K reportom v službe ThreatGuard je používaná kalkulačka od organizácie FIRST (Forum of Incident Response and Security Teams) vo verzii 3.0. V tejto podkapitole budú zmienené a porovnávané jednotlivé metriky a ich časti spoločne s ich vplyvom na celkové CVSS skóre.

Na nasledujúcom obrázku je zobrazené prostredie online kalkulačky od organizácie FIRST a pod obrázkom sú porovnané jednotlivé metriky a ich časti.



Obrázok 7: Online kalkulačka (verzia 3.0) od organizácie FIRST slúžiaca na zostavenie kvantitatívneho skóre závažnosti zraniteľnosti

Zdroj: [26]

Vektor útoku je prvá metrika, ktorá odráža kontext, v ktorom je možné zneužitie zraniteľnosti. Základné skóre je zvyšované logickou a fyzickou vzdialenosťou útočníka, z ktorej môže zneužiť zraniteľnú súčasť. Najvyššiu váhu má v tomto prípade *Network* (sieťový vektor útoku), kde útočník dokáže vzdialene zneužiť zraniteľnosť cez 3. vrstvu OSI modelu (sieťovú vrstvu). Ďalším v poradí je *Adjacent* (priľahlý sieťový vektor), u ktorého je útok obmedzený na rovnakú zdieľanú fyzickú alebo logickú sieť (napr. IEEE 802.11, Bluetooth atď.) a ktorý nemôže byť vykonaný cez hranice 3. vrstvy OSI modelu (napr. router). Tretím v poradí je lokálny prístup útočníka (*Local*), kde cesta útočníka spočíva cez schopnosti read/write/execute, ktorými je schopný získať povolenia alebo prístupové práva na napadnutom zariadení. Posledným v poradí je *Physical* (fyzický vektor útoku), ktorým je myslený fyzický prístup útočníka k zariadeniu (dotyk alebo manipulácia). Príkladom môže byť pripojenie zariadenia k systému.

Komplexnosť (zložitosť) útoku rozdeľujeme na nízku a vysokú. Pri nízkej komplexnosti neexistujú špeciálne podmienky prístupu alebo poľahčujúce okolnosti. Pri vysokej komplexnosti je vyžadované úsilie útočníka do prípravy alebo k vykonaniu aktivity smerujúcej na zraniteľný komponent (napr. pripraviť cieľové prostredie na zvýšenie spoľahlivosti zneužitia).

Požadované oprávnenia sú ďalšou súčasťou základného skóre. Rozdeľujeme ich do 3 skupín na žiadne, nízke a vysoké. Pokiaľ nie sú požadované oprávnenia od útočníka, na vykonanie útoku nie je vyžadovaný prístup k nastaveniam alebo súborom, útočníka

označujeme ako neautorizovaného. Pre nízke požadované oprávnenia platí, že útočník je autorizovaný oprávneniami, ktoré poskytujú základné používateľské funkcie, ktoré by normálne mohli ovplyvniť iba nastavenia a súbory vlastnené používateľom a nemajú vplyv na citlivé údaje. Vysokými požadovanými oprávneniami rozumieme také oprávnenia, ktoré poskytujú významnú (napr. administratívnu) kontrolu nad zraniteľným komponentom a ktoré by mohli ovplyvniť jeho nastavenia a súbory.

Pokiaľ nie je **interakcia užívateľa** požadovaná, zraniteľný systém je možné zneužiť bez akejkoľvek interakcie od akéhokoľvek používateľa. Požadovanie interakcie užívateľa znamená, že pre úspešné zneužitie zraniteľnosti, je požadovaná nejaká akcia užívateľa (napr. kliknutie, otvorenie webovej stránky alebo e-mailovej prílohy).

Pri metrike **rozsah** je hlavný rozdiel v rovnosti zraniteľnej a postihnutej zložky. Ak sú tieto dve zložky rovnaké, rozsah je nezmenený a zneužitá zraniteľnosť môže ovplyvniť prostriedky spravované rovnakými oprávneniami. Naopak pri odlišnosti zraniteľnej a postihnutej zložky, môže zneužitá zraniteľnosť ovplyvniť prostriedky nad rámec autorizačných oprávnení určených zraniteľným komponentom.

Metrika rozsahu súvisí priamo aj s poslednými tromi metrikami **dôvernosti**, **integrity** a **dostupnosti**. Ak úspešný útok ovplyvní nie len zraniteľnú zložku, ale aj iné zložky, musí to byť u týchto troch metrík zohľadnené.

2.1.6 Analýza hrozieb z portálu ThreatGuard za tretí a štvrtý kvartál roku 2019

Ako už bolo na začiatku podkapitoly zmienené, analýza reportov zo služby ThreatGuard pozostáva z piatich čiastkových analýz. Prvou v poradí je analýza bezpečnostných hrozieb za tretí a štvrtý kvartál roku 2019. Jednotlivé hrozby budú uvedené v anglickom jazyku pre ich presnejší technický význam.

Dôvod výberu posledných dvoch kvartálov roku 2019 má niekoľko dôvodov. Prvý z nich je kvalita spracovania reportov v službe. Keďže služba sa kontinuálne vyvíja, úplnosť a kvalita reportov počas roka 2019 bola takisto menená. Prvý polrok boli reporty spracovávané bez niektorých parametrov a nebol kladený dôraz na ich kompletné spracovanie. To si spoločnosť uvedomila a v druhej polovici roka bol kladený vyšší dôraz na úplnosť reportov. Jednotlivé informácie o reportoch boli ucelenejšie a vhodnejšie pre vytvorenie analýzy.

Druhým dôvodom je vyššia výpovedná hodnota výsledkov. Pre vyvodenie záverov a návrhov pre spoločnosti je zdôraznenie posledných 2 kvartálov roku, v dynamickom prostredí, vhodnejší a akurátnejší, pretože je očakávaný väčší predpoklad pôsobenia týchto hrozieb aj v roku 2020.

Dôležité je podotknúť, že rozdelenie typov hrozieb v službe má všeobecný charakter. Z tohoto dôvodu sa v reportoch prevažne vyskytovali *Vulnerabilities (Zraniteľnosti)*, takmer v 85 % prípadov. Kvôli lepším znalostiam z výsledkov analýz som sa rozhodol pre rozšírenie kategórií typu hrozieb a jednotlivé reporty som doplnil o presnejšie informácie o typu hrozby.

Vzniknutých kategórií po prvej analýze bolo väčšie množstvo a preto som sa rozhodol v druhej analýze zjednotiť tieto kategórie podľa vecného a významového hľadiska a tým vytvoriť všeobecnejšie kategórie. Jednotlivé informácie som dohľadal v zdrojových odkazoch k danej hrozbe. Tento krok spôsobil aj vyššiu prehľadnosť výsledkov analýz a zjednodušil tvorbu grafov.

Napríklad do hrozby *Arbitrary Code Execution (Spustenie ľubovoľného kódu)* som zaradil podkategórie hrozieb Local (lokálne) a Remote (vzdialené) Code Execution, Command a Code Injection a Action Execution (vykonanie určitej lokálnej alebo vzdialenej akcie na napadnutom zariadení). Ďalšou sumárnou kategóriou je kategória *Other (Ostatné)*. Táto kategória bola vytvorená pre vyššie zmienenú prehľadnosť analýz. Do tejto kategórie boli zahrnuté hrozby, ktorých počet výskytov bol nízky až zanedbateľný pre analýzu. Do tejto kategórie spadajú hrozby ako CSFR (Cross-Site Request Forgery, ktorá umožňuje útočníkovi podnietiť používateľov, aby vykonávali činnosti/akcie, ktoré nemajú v úmysle vykonať), XSS (Cross-Site Scripting), Open Redirect, Bypassing Sandbox Protection a mnohé ďalšie.

Údaje v nasledujúcich tabuľkách sú radené abecedne, prípadne, pre prehľadnosť grafu, je poradie údajov zmenené.

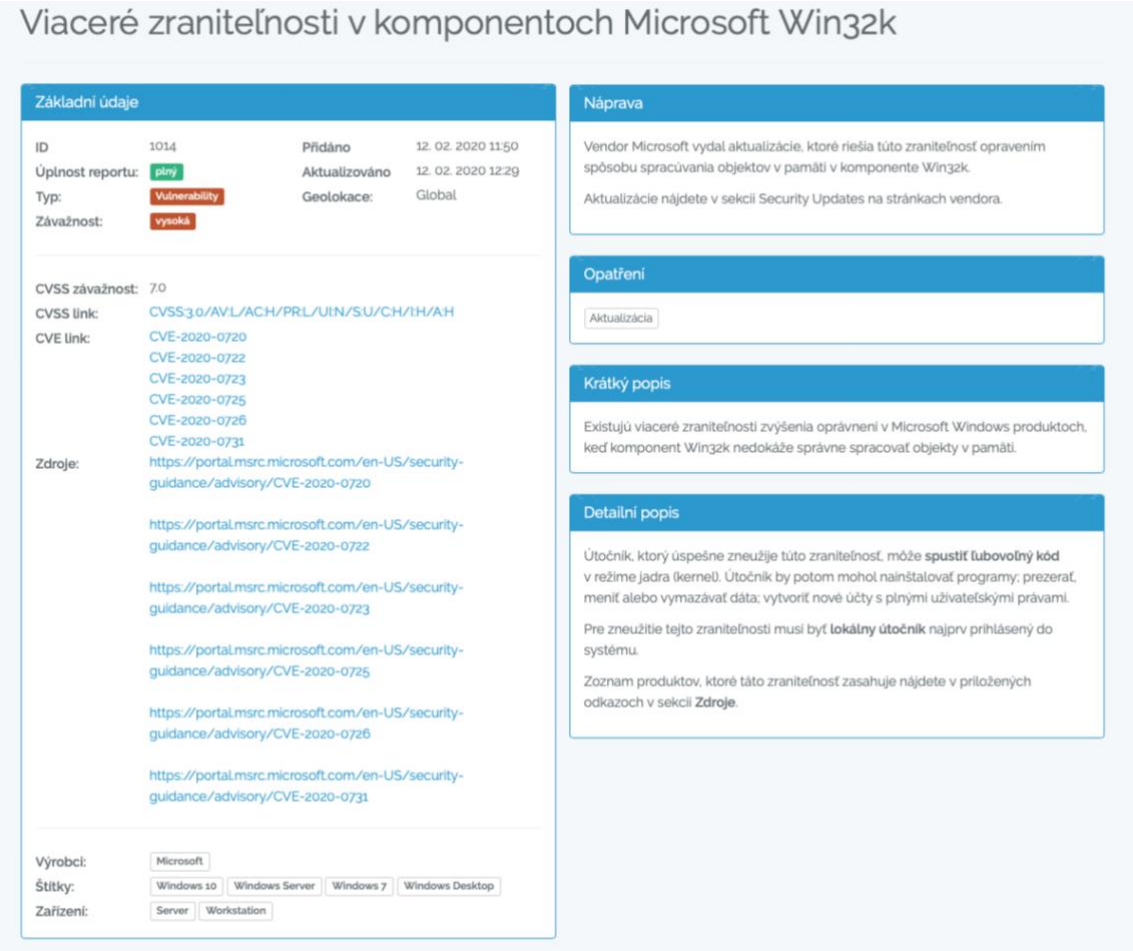
Tabuľka 2: Hrozby zaznamenané službou ThreatGuard za 3. a 4. kvartál roku 2019
Zdroj: Vlastné spracovanie

Hrozba	Počet výskytov
Arbitrary Code Execution	95
Authentication Bypass	12
Buffer Overflow	12
Denial of Service	38
Information Exposure	15
Out-of-bounds Read / Write	21
Privilege Escalation	24
SQL Injection	4
Other	32
Celkový súčet	**253**

Z tabuľky možno vyvodiť nasledujúci záver. Celkový počet hrozieb zaznamenaných službou ThreatGuard za posledné dva kvartály roku 2019 je 253. Tento počet však nie je úplne presný. V službe sú spracovávané takisto reporty, ktoré obsahujú viac hrozieb. Vyplýva to z toho, že častokrát vendor vydá balíček opatrení pre skupinu hrozieb, ktoré postihovali určitú skupinu zariadení. Aby nedošlo k neprehľadnosti služby a aby sa nevyskytovali na portáli hrozby postihujúce podobné zariadenia od jedného vendora, služba ThreatGuard spracováva reporty, ktoré zahŕňajú jednu alebo niekoľko podobných hrozieb. Následne je týmto reportom pridelená hodnotenie závažnosti zraniteľnosti s najvyšším skóre, ktoré sa vyskytlo pomedzi jednotlivé hrozby.

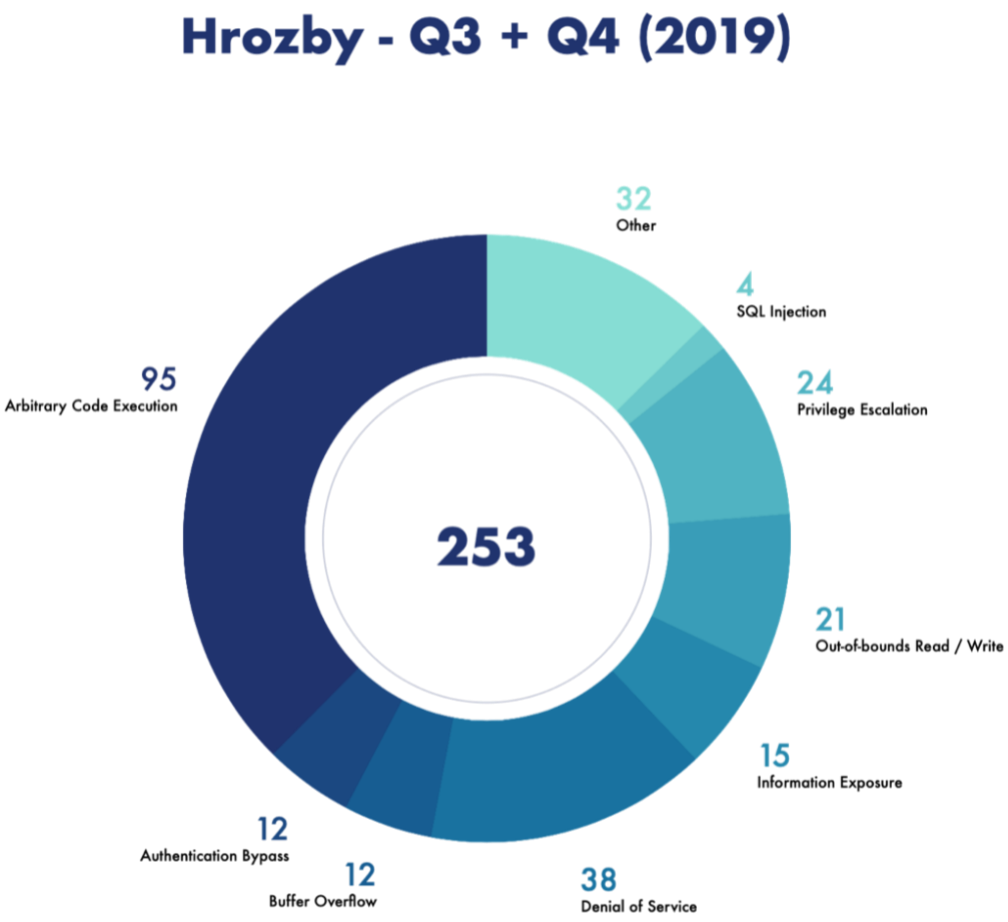
Ďalším dôvodom nižšieho celkového súčtu hrozieb je už zmienené kritérium filtrácie obsahu reportov podľa hodnotenia závažnosti. Do úvahy sú brané hrozby so strednou, vysokou a kritickou závažnosťou.

Pre vhodnosť a vyššiu prehľadnosť diplomovej práce je použitý obrázok, ktorý ilustruje report s vyšším počtom hrozieb. Pozn. tieto reporty sú častokrát rozšírenejšie, avšak nemá zmysel poukázať na kvantitu, ale zobraziť názorný príklad.



Obrázok 8: Report s vyšším počtom hrozieb vypracovaný v službe ThreatGuard - pohľad používateľa
Zdroj: portál ThreatGuard

Z výsledkov analýzy vieme ďalej vyvodiť najčastejšie sa vyskytujúce typy hrozieb v posledných dvoch kvartáloch roku 2019. Najväčší podiel tvorí kategória hrozieb *Arbitrary Code Execution (Spustenie ľubovoľného kódu)* približne, prepočtom na percentá, s 37,5 % výskytu. Druhou najčastejšie sa vyskytujúcou hrozbou bola *Denial of Service (Odmietnutie služby)* s približne 15 % výskytu. Približne 12,7 % zaznamenala sumárna kategória *Other (Ostatné)* a aj napriek vyššiemu podielu na výsledku uprednostním na tretie miesto *Privilege Escalation (Eskalácia privilégií)* s približne 9,5 % výskytu. Najmenší výskyt bol nameraný u typu hrozby *SQL Injection* s 1,6 %. Tento typ hrozby, aj napriek nízkemu výskytu, som nezaradil do kategórie *Other (Ostatné)*, pretože dopad tohoto typu hrozby je častokrát vysoký a to zvyšuje jej samotný význam.



Graf 1: Hrozby v 3. a 4. kvartáli roku 2019
Zdroj: Vlastné spracovanie

2.1.7 Analýza vendorov z portálu ThreatGuard za rok 2019 (bez ostatných)

Druhou v poradí je analýza vendorov za rok 2019. S týmto časovým obdobím som pracoval kvôli tomu, že väčšina reportov malo jasne prideleného vendora. S údajmi som ďalej pracoval a po dokončení prvej analýzy som usúdil, že bude vhodné rozdeliť túto analýzu na dve časti. Prvá časť bude obsahovať vytvorenú analýzu najviac ohrozených vendorov. Kategóriu „Najviac ohrozených“ je nutné definovať. Z prvej analýzy vyplynulo, že pre prehľadnosť a adekvátnosť výsledkov sa spodná číselná hranica počtu výskytov stanoví na čísle 5. To znamená, že najviac ohrození vendori za rok 2019 sa v reportoch vyskytli aspoň 5 krát. Opäť treba brať v úvahu, že jednotlivé reporty obsahovali viacero hrozieb, ktoré boli pridelené k vendorom a že celkový počet výskytov sa odvíja z počtu reportov a nie počtu hrozieb.

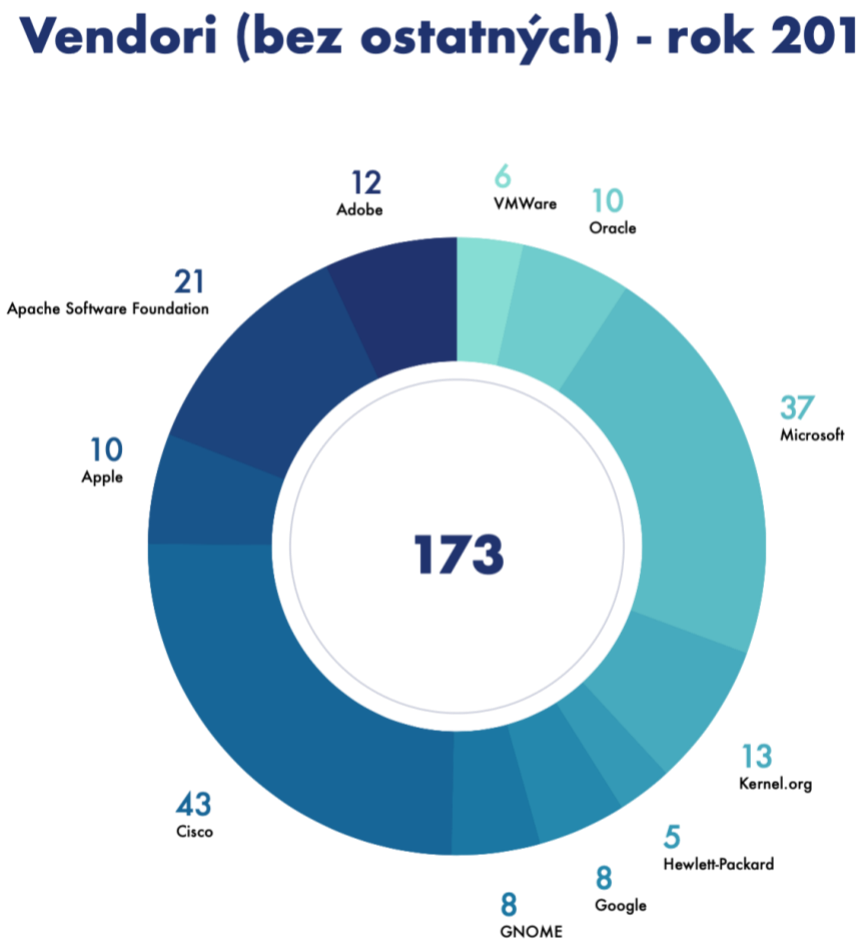
Údaje v nasledujúcich tabuľkách sú radené abecedne, prípadne, pre prehľadnosť grafu, je poradie údajov zmenené.

Tabuľka 3: Selektovaní vendori zo služby ThreatGuard a ich počet výskytov
Zdroj: Vlastné spracovanie

Vendor	Počet výskytov
Adobe	12
Apache Software Foundation	21
Apple	10
Cisco	43
GNOME	8
Google	8
Hewlett-Packard	5
Kernel.org	13
Microsoft	37
Oracle	10
VMWare	6
Celkový súčet	**173**

Do užšieho zoznamu, podľa vyššie zmieneného filtra, sa dostalo 11 vendorov, ktorí zaznamenali celkový počet výskytov na čísle 173. Z analyzovaných informácií vyplýva, že najviac ohrození zaznamenala spoločnosť Cisco s počtom výskytov 43, čo je takmer štvrtina z celkového počtu. Len o 6 výskytov menej zaznamenala spoločnosť Microsoft. Do prvej trojky najohrozovanejších vendorov roku 2019 radíme organizáciu Apache Software Foundation s počtom výskytov 21. V rozmedzí od 10 do 20 výskytov sa nachádzajú 4 vendori – Adobe, Apple, Kernel.org a Oracle. Najmenej výskytov, v intervale od 5 do 10, zaznamenali 4 vendori – GNOME, Google, Hewlett-Packard a VMWare.

Tento typ analýzy bude vhodnejší a účinnejší pre vytvorenie návrhov, kvôli vyšším a významnejším výsledným hodnotám počtu výskytov.

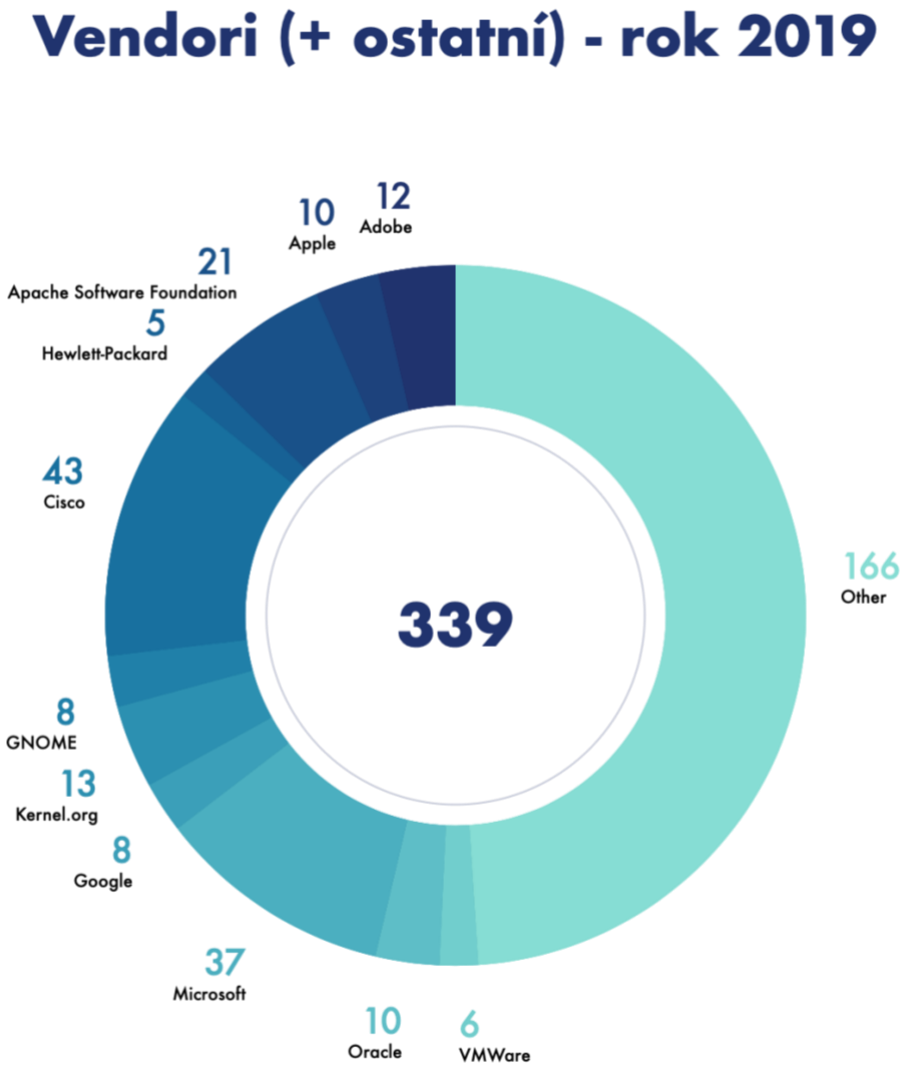


Graf 2: Analýza vendorov (bez ostatných) za rok 2019
Zdroj: Vlastné spracovanie

2.1.8 Analýza vendorov z portálu ThreatGuard za rok 2019 (s ostatnými)

Druhá časť analýzy vendorov za rok 2019 zohľadňuje aj kategóriu *Other (Ostatní)*. Do tejto kategórie som zaradil vendorov, ktorí sa vyskytli v reportoch menej ako 5 krát. Dôvodom mohlo byť ich priradenie v skoršom vývoji služby a následné nespracovávanie reportov o nich. Služba sa neustále vyvíja a administrátor môže v určitý okamih posúdiť ako vhodné vložiť vendora do zoznamu pre budúce účely. V zozname sa potom nachádzajú vendori, ktorí prestanú byť využívaní, ale takisto môže nastať, že v zozname sa určitý výrobca nevyskytuje. Všetky tieto možnosti sú zohľadnené v kategórii *Other (Ostatní)*.

So započítaním ostatných vendorov do celkovej analýzy, vzrástol celkový počet výskytov na hodnotu 339. Skupina *Other* tvorí zo zoznamu takmer polovicu výskytov. Spoločnosť bude riešiť túto odchýlku v novej verzii.



Graf 3: Analýza vendorov (s ostatnými) za rok 2019
Zdroj: Vlastné spracovanie

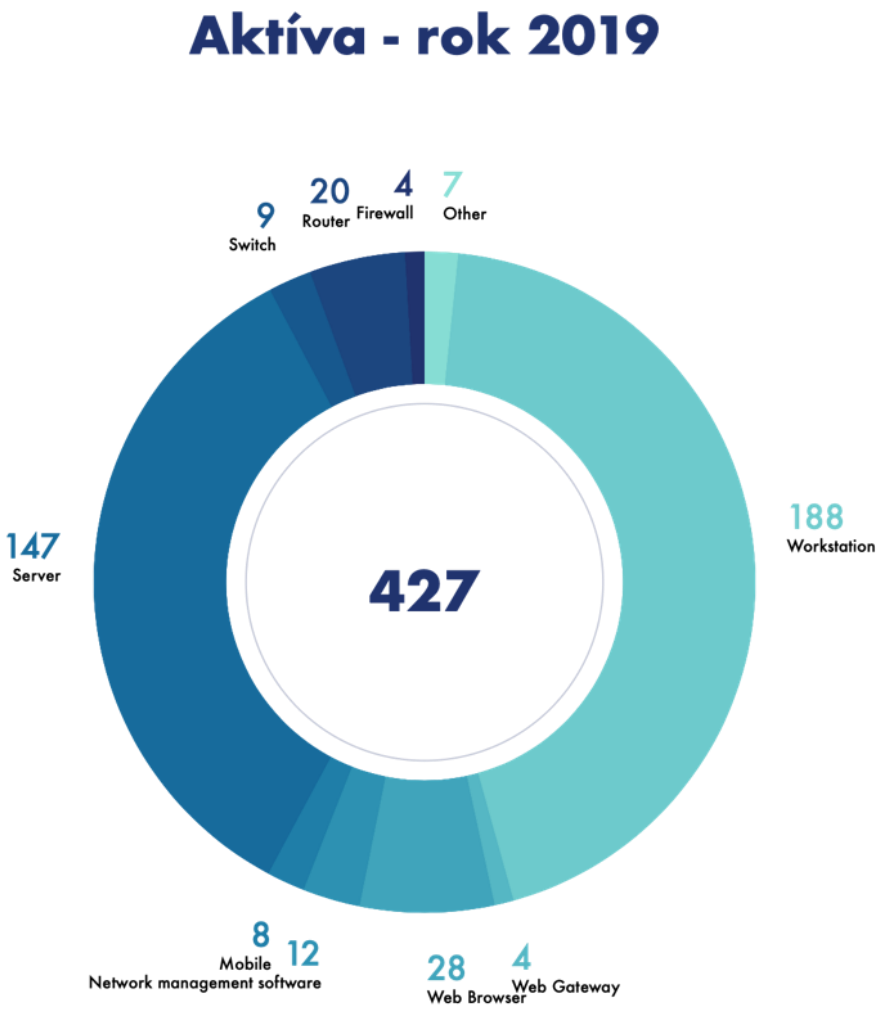
2.1.9 Analýza aktív z portálu ThreatGuard za rok 2019

Posledné analýzy budú venované informačným aktívam (zariadeniam), ktoré mohli byť potencionálne ohrozené v roku 2019. Ako analýza vendorov, tak aj analýza aktív bude rozdelená na 2 časti. Je to z dôvodu zistenia a zdôraznenia zmien, ktoré mohli nastať počas roka 2019. Prvou časťou bude analyzovaný celý rok 2019. Druhá časť zas bude zdôrazňovať posledné 2 kvartáli tohoto roku.

Celkový počet aktív, ktoré boli uvedené v jednotlivých reportoch a ktoré boli ohrozené v roku 2019 bol 427. Najviac výskytov zaznamenali útoky na *Workstation* (pracovnú počítačovú stanicu), nasledované zariadením *Server*, do ktorého bolo započítané aj zariadenie *Web Server* zo zoznamu zariadení služby ThreatGuard. Týmto 2 typom

zariadení dokopy patrí vyše ¾ celkových výskytov v zozname – 78,5 %. Zo zvyšných aktív mali najvyššie výskyty *Web Browser* (webový prehliadač), *Router* a *Network management software* (software na správu siete).

Aj pre túto analýzu som vytvoril skupinu *Other*, do ktorej boli zaradené aktíva s počtom výskytov 1 resp. 2 za celé obdobie.

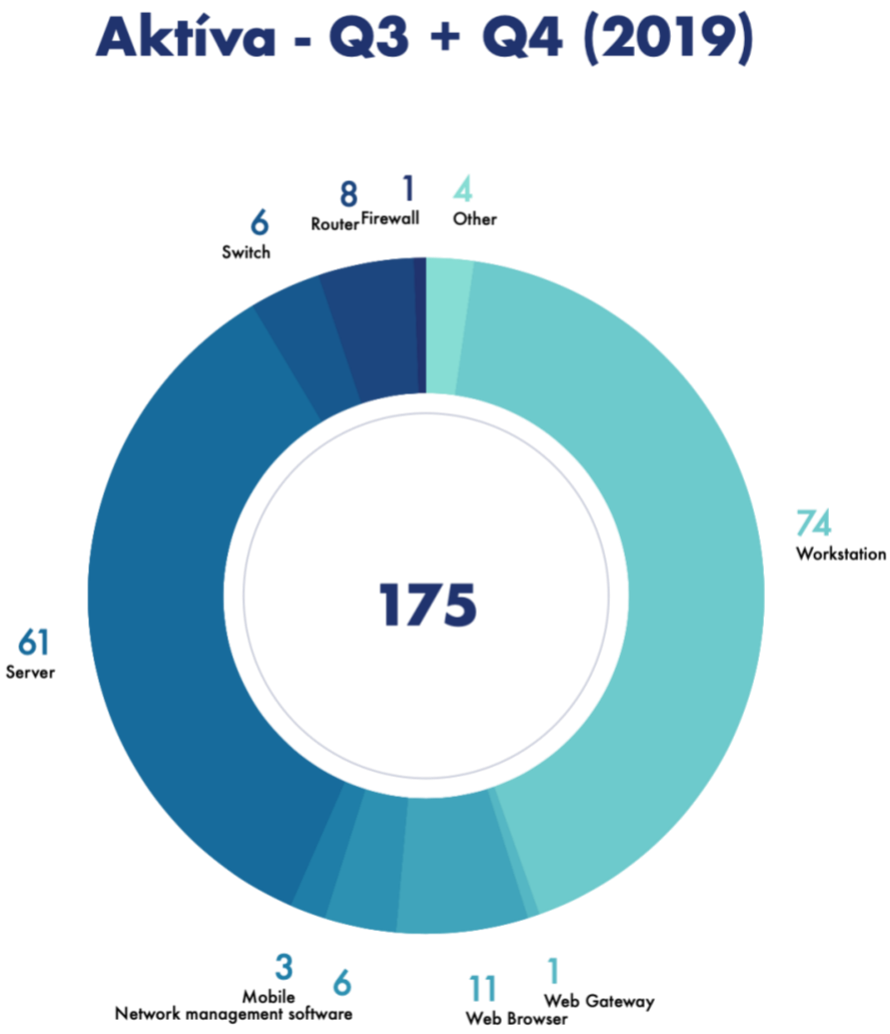


Graf 4: Analýza aktív za rok 2019
Zdroj: Vlastné spracovanie

2.1.10 Analýza aktív z portálu ThreatGuard za tretí a štvrtý kvartál roku 2019

Prvým porovnateľným údajom je počet výskytov. V druhej polovici roka bol tento ukazovateľ nižší ako v tej prvej, s percentuálnou hodnotou približne 41 %. Môžeme to odôvodniť tým, že frekvencia hrozieb je v letným mesiacoch a v mesiaci december nižšia, ako ostatné mesiace v roku.

Ohrozenia zariadení *Server* a *Workstation* zaznamenali aj v tomto období viac ako ¾ výskytov – približne 77 % – a jasne prevyšujú všetky ostatné zariadenia. Celkom zásadný pokles nastal u zariadenia *Web Browser*, keď počet jeho výskytov klesol zo 17 na 11 výskytov v tomto období. Takisto len ¼ z celkového počtu výskytov v roku zaznamenali zariadenia *Firewall* a *Web* Gateway. Naopak dvojnásobný nárast výskytov nastal v posledných dvoch kvartáloch pri zariadení Switch. Ostatné aktíva sa nachádzajú na približne polovici výskytov, čo je ekvivalentné časovému obdobiu.

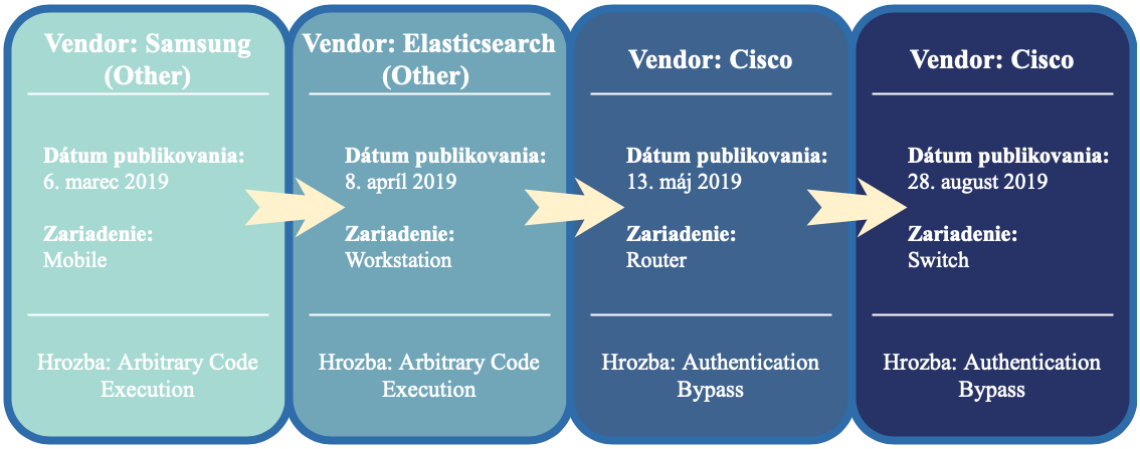


Graf 5: Analýza aktív za 3. a 4. kvartál roku 2019
Zdroj: Vlastné spracovanie

2.1.11 Najzávažnejšie zraniteľnosti z portálu ThreatGuard za rok 2019

V poslednej časti analýzy reportov z portálu ThreatGuard budú zmienené najzávažnejšie zraniteľnosti za rok 2019. Závažnosť bude posudzovaná podľa CVSS skóre a do tohoto

výberu budú vybrané hrozby s najvyšším možným skóre 10. V zozname reportov portálu ThreatGuard je počet výskytov hrozieb s týmto skóre celkovo 4. Jednotlivé hrozby budú zoradené chronologicky a bude k ním vytvorená grafická vizualizácia.



Obrázok 9: Najzávažnejšie zraniteľnosti z portálu ThreatGuard za rok 2019|
Zdroj: Vlastné spracovanie

Z analýzy vyplýva, že sa po 2 razy vyskytli rovnaké typy hrozieb – spustenie ľubovoľného kódu a obídenie autentifikácie. Oba typy hrozieb mohli byť zneužité vzdialeným útočníkom, bez nutnosti autentifikácie.

U prvej hrozby bola zraniteľná inštalácia programu na zariadení Samsung Galaxy S9 vo verziách starších ako 1.4.20.2. Chyba existovala v rámci manipulácie s aktualizačným mechanizmom GameServiceReceiver.

Druhá hrozba zasiahla vizualizačný nástroj Timelion v softwarovom programe Kibana vo verziách 5.6.15 až 6.6.1, ktorý nesprávne spracovával vstup zadaný užívateľom. Útočník s prístupom k aplikácii Timelion mohol poslať žiadosť, ktorá umožnila spustiť ľubovoľný kód JavaScript v hostiteľskom systéme.

Posledné dve hrozby sa týkali produktov vendora Cisco, konkrétne ich programovacieho prostredia aplikácií, ktoré umožňuje vývojárom vytvárať softwarové aplikácie. Bezpečnostnou chybou bolo nesprávne schvaľovanie požiadaviek. Útočník to mohol zneužiť zaslaním škodlivých požiadaviek na systém a úspešným zneužitím chyby mohol zaviesť vlastný kód s administrátorskými právami.

2.2 ANALÝZA REPORTOV SPOLOČNOSTI KASPERSKY

Táto kapitola analytickej časti diplomovej práce obsahuje základné informácie o zdroji pre analýzu od spoločnosti Kaspersky. V kapitole je zdôvodnený výber jednotlivých súčastí reportov použitých pre analýzu. V poslednej časti sa nachádza samotná analýza. Táto časť rozšíri skupiny používateľov od jednotlivcov (ktorí nie sú braní v úvahu) až po veľké spoločnosti.

2.2.1 Základné informácie o reportoch Kaspersky

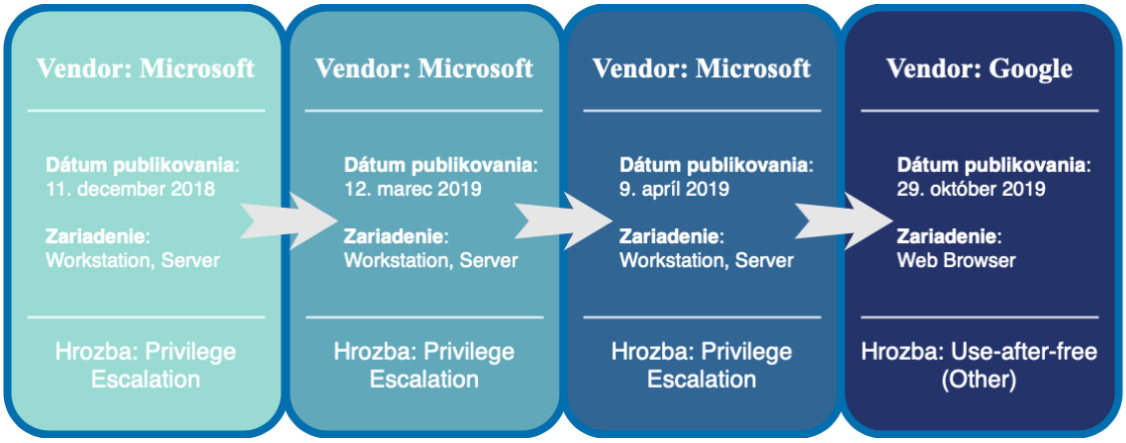
Od spoločnosti Kaspersky sa v analytickej časti zameriam na 2 reporty, ktoré nadviažu na predošlú kapitolu s analýzou reportov zo služby ThreatGuard. Prvým reportom bude ročný, súhrnný report s názvom *Kaspersky Security Bulletin ’19 Statistics*. Tým druhým bude ročný súhrnný report zameraný na mobilné zariadenia *Mobile malware evolution 2019*. Z oboch reportov vyselektujem časti, ktoré súvisia a rozvíjajú analytickú časť diplomovej práce.

Všetky štatistiky použité v týchto reportoch boli získané pomocou Kaspersky Security Network (KSN), distribuovanej antivírusovej siete, ktorá pracuje s rôznymi komponentmi ochrany pred škodlivým softwarom. Údaje boli zhromaždené od používateľov KSN, ktorí súhlasili s ich poskytnutím. Ide o milióny používateľov produktov spoločnosti Kaspersky z 203 krajín a teritórií na celom svete. Štatistiky z reportu *Kaspersky Security Bulletin ’19 Statistics* boli zbierané v období od novembra 2018 do októbra 2019. Štatistiky z *Mobile malware evolution 2019* zohľadňujú dlhšie časové obdobie, kvôli ukážke vývoja hrozieb postihujúcich mobilné zariadenia.

2.2.2 Analýza zraniteľných aplikácií

V súhrnnom ročnom reporte *Kaspersky Security Bulletin ’19 Statistics* sa nachádza analýza zraniteľných aplikácií, ktoré sú cieľom kybernetických útokov. Podľa spoločnosti Kaspersky narástol, s porovnaním s minulým rokom, celkový počet aktívne zneužívaných exploitov nultého dňa. Presný počet spoločnosť neudáva. Pre informáciu, riešenia spoločnosti Kaspersky, v roku 2019, odrazili celkovo 975 491 360 útokov spustených online zdrojov umiestnených po celom svete.

Spoločnosť vo svojom reporte udáva 4 zraniteľnosti, ktoré boli odhalené ich odborníkmi. Jednotlivé zraniteľnosti budú zoradené chronologicky a bude k ním vytvorená grafická vizualizácia, ako tomu bolo v podkapitole *Najzávažnejšie hrozby z portálu ThreatGuard za rok 2019*.



Obrázok 10: 4 zraniteľnosti odhalené odborníkmi Kaspersky
Zdroj: Vlastné spracovanie

Prvá zistená zraniteľnosť umožnila získať systémové oprávnenia a vykonať kód na úrovni jadra vo všetkých verziách Windows. Navyše sa táto zraniteľnosť nachádzala v ovládači Kernel Transaction Manager, čo umožnilo zneužitie obídenia sandboxov webového prehliadača.

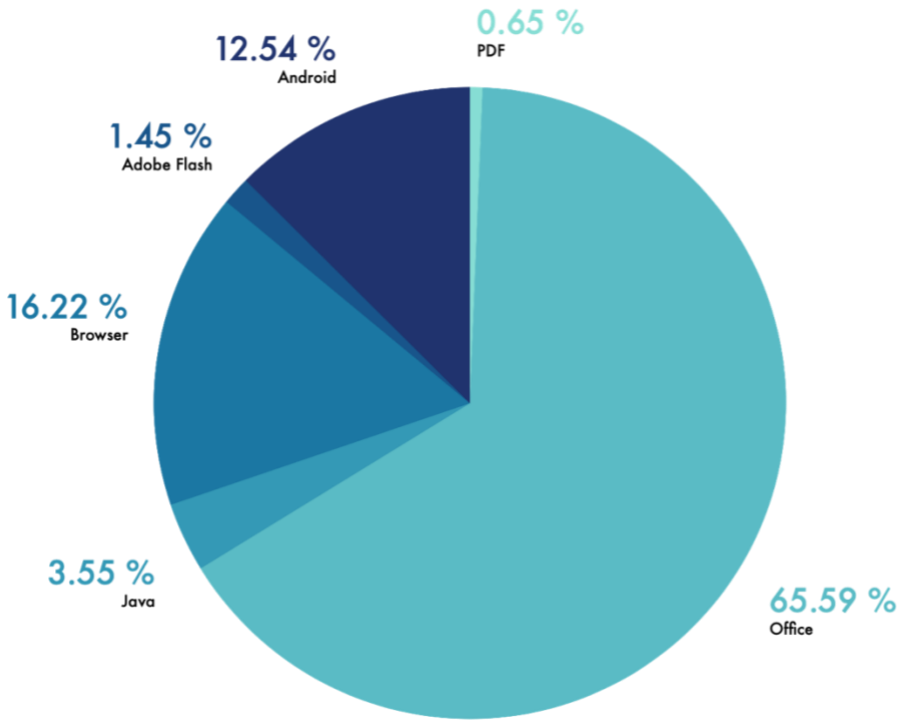
Druhá zraniteľnosť v poradí sa stala štvrtou aktívne zneužívanou zraniteľnosťou nultého dňa, zistenou spoločnosťou Kaspersky, počas prvých 6 mesiacov roku 2019. Hrozba vyplývajúca z tejto zraniteľnosti bola rovnaká, ako u prvej zmienenej zraniteľnosti. Zraniteľným komponentom bol ovládač win32k.sys zodpovedný za grafiku a rozhranie.

Ďalšia aktívne zneužívaná zraniteľnosť vendora Microsoft umožňovala zvýšenie užívateľských práv prostredníctvom ďalšej chyby ovládača win32k.sys. Zaujímavosťou pri tejto zraniteľnosti bolo payload (súkromné textové pole, ktoré vykonáva škodlivú akciu) so shellcode (malý kus kódu pri zneužívaní softwarovej zraniteľnosti), ktoré indikovali, že exploit bol mierený na finančný sektor.

Poslednou v zozname bola zraniteľnosť objavená po sérii útokov na nové verzie prehliadača Google Chrome. Kaspersky nazval tieto útoky ako Operation WizardOpium, pretože nebol schopný získať jasné spojenie s inými skupinami.

Report od spoločnosti Kaspersky ponúka náhľad aj na škodlivé exploity, ktoré rozdelila podľa typu cieľových aplikácií na Office, Browser, Android, Java, Adobe Flash a PDF. Tieto výsledky je možné porovnať s tými minuloročnými.

Až u piatich typov cieľových aplikácií došlo k poklesu percent voči minulému roku. Najväčší pokles zaznamenal Android s 5,38 %, nasledovaný Browser s 3,57 % a Adobe Flash s 1,06 %, ktorému končí podpora koncom roku 2020. Naopak výrazný rast, 10,9 % napadnutých používateľov, pozorujeme u exploitoch Microsoft Office, aj napriek tomu, že pri najviac zneužívaných zraniteľnostiach nenastali veľké zmeny.



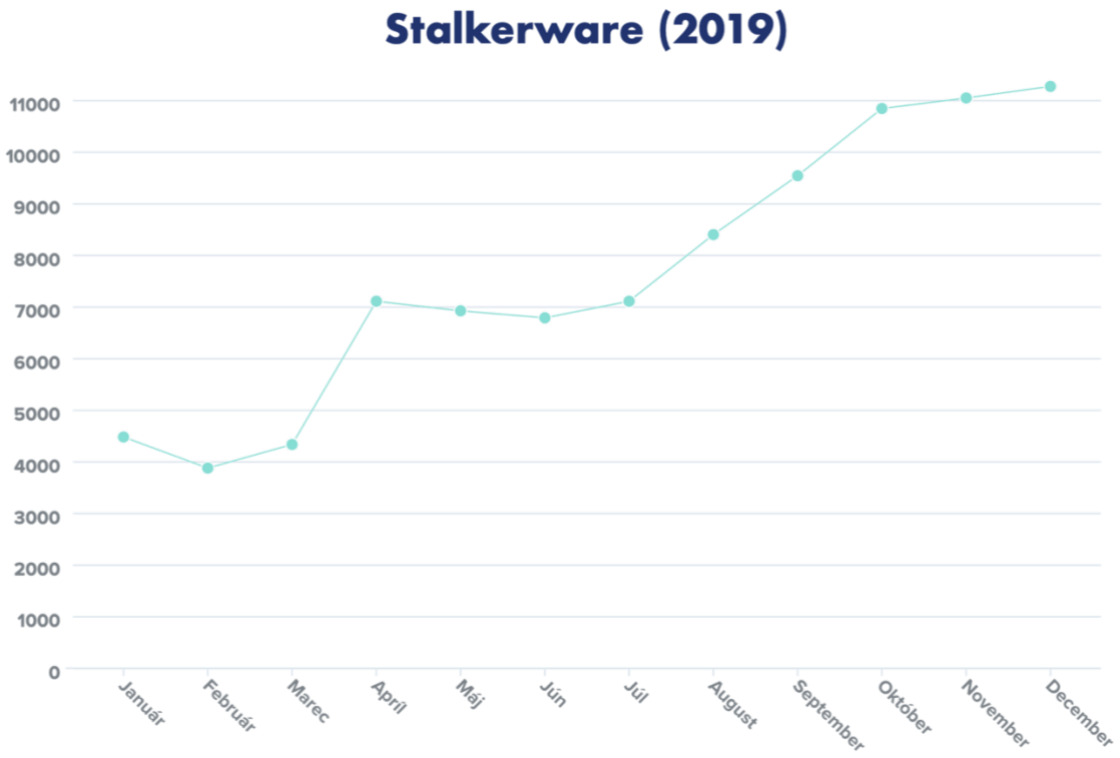
Obrázok 11: Škodlivé exploity rozdelené podľa typu cieľovej aplikácie
Zdroj: Vlastné spracovanie

Podľa odborníkov spoločnosti Kaspersky zostávajú sieťové útoky jedným z najbežnejších typov útokov. Tento zoznam je doplnený rôznymi zneužitiami SMB (Service Message Block) protokolu, známym ako EternalBlue, EternalRomance, atď. Veľká časť škodlivého sieťového prenosu pochádza z dotazov „ťažby“ hesiel, ktoré sú cielené na populárne sieťové služby a servery ako Remote Desktop Protocol a Microsoft SQL.

V roku 2019 sa takisto objavilo viacero zraniteľností v subsystéme vzdialenej plochy v rôznych verziách operačného systému Windows, ktoré dostali označenia BlueKeep

a DejaBlue. V súčasnosti však nie sú rozsiahle zneužívané, čo môže byť spojené s komplexnosťou procesu.

Často využívaným informačným aktívom sú mobilné telefóny. A s ním sú spájané aj hrozby, ktoré budú zhrnuté grafmi s vlastným spracovaním podľa reportu *Mobile malware evolution 2019* od spoločnosti Kaspersky. Dôležitým poznatkom z tohoto reportu je zvyšovanie frekvencie útokov na osobné dáta, nazývaných stalkerware. Na nasledujúcom grafe sa nachádza trendová krivka, ktorá zobrazuje počet jedinečných užívateľov napadnutých stalkerwarom za rok 2019. Januárový počet výskytov 4 483 narástol do decembra na 11 277 výskytov.

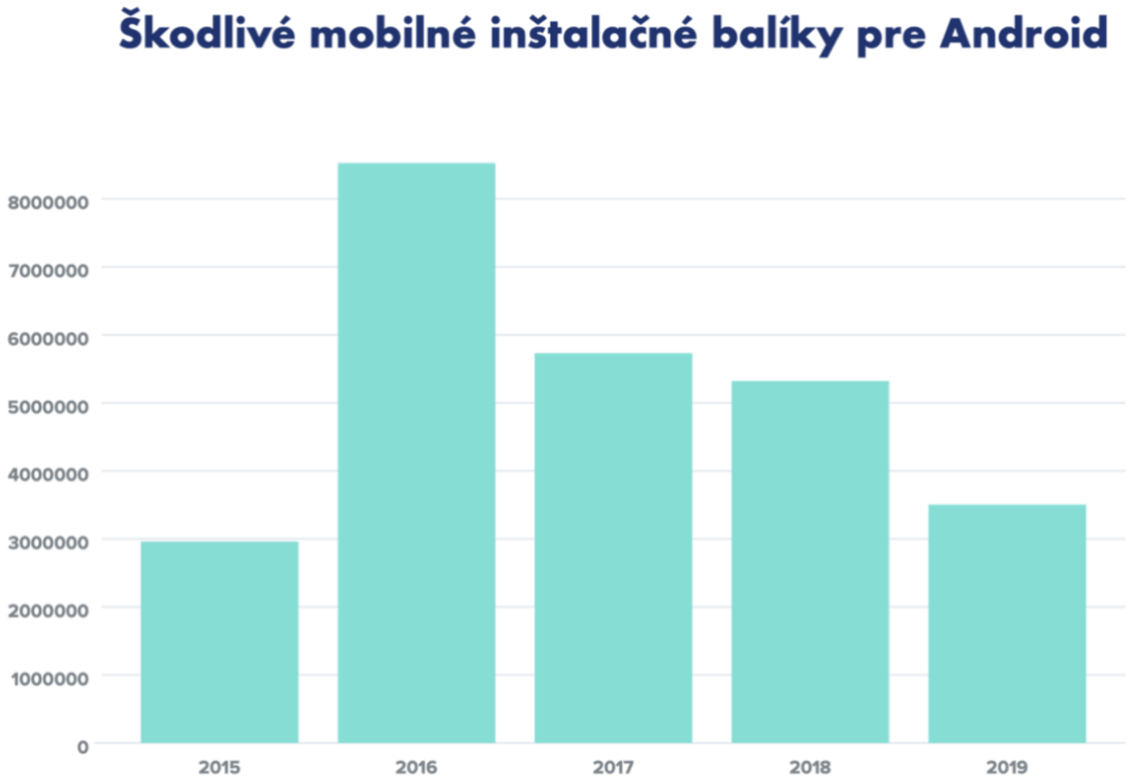


Graf 6: Nárast počtu útokov stalkerware
Zdroj: Vlastné spracovanie podľa [27]

Rovnako rastúci trend, oproti roku 2018, má celkový počet odhalených inštalačných balíkov adware. Celkový počet narástol z 440 098 výskytov na 764 265.

Pozitívny trend Androidu, ktorý bol naznačený pri opise grafu zobrazujúcom percentuálne rozdelenie škodlivých exploitov rozdelených podľa typu cieľových aplikácií, potvrdzuje graf, ktorý vyjadruje počet škodlivých mobilných inštalačných balíkov pre Android od roku 2015 po rok 2019. Tento obraz do značnej miery závisí od

konkrétnych kybernetických trestných kampaní: niektoré sa stali menej aktívnymi, iné úplne zanikli a noví „hráči“ sa musia ešte len rozbehnúť. Tento trend je pozitívny najmä z toho dôvodu, že počet firemných mobilných zariadení a práce na diaľku narastá.



Graf 7: Škodlivé mobilné inštalačné balíky pre Android - vývoj v čase
Zdroj: Vlastné spracovanie podľa [27]

2.3 MEDIÁLNE SPRÁVY ZA ROK 2019

V poslednej podkapitole *Analýzy súčasného stavu* budú uvedené najzávažnejšie mediálne správy roku 2019, týkajúce kybernetických útokov, ktoré sa objavili v českých médiách a zasiahli Českú republiku.

V médiách otriasli Českou republikou v roku 2019 dve veľké správy týkajúce sa kybernetických útokov. Obe tieto správy boli uverejnené v decembri tohoto roku a oba útoky boli pravdepodobne spôsobené rovnakým typom hrozby. Jedná sa o kybernetické útoky na nemocnicu Rudolfa a Stefanie v Benešove a na spoločnosť OKD, producenta čierneho uhlia v Českej republike.

O týchto dvoch incidentoch bolo písané a hovorené v niekoľkých českých médiách, avšak pre podobnosť článkov a reportáží som sa rozhodol použiť ako zdroje iRozhlas.cz, BENEŠOVSKÝ.deník.cz a radio.cz.

Cieľom tejto časti bude selekcia informácií, ktoré nebudú odbočovať od určitej línie tejto diplomovej práce. Je nutné podotknúť, že o oboch incidentoch sa stále nenachádzajú kompletné informácie.

2.3.1 Kybernetický útok – nemocnica Benešov

V čase spracovávania údajov práce nebolo známe, kedy prenikol vír do počítačovej siete. Odhaduje sa obdobie niekoľko týždňov až mesiacov pred samotným incidentom.

Nahlásenie problému: 11. december, 2:50 hod.

Detekcia útoku: 11. december, 3:20 hod.

Vypnutie siete IT oddelením nemocnice: 11. december, 3:30 hod.

Podľa prvých údajov nebolo možné spustiť počítačovú sieť, na ktorej chrbticovú časť boli pripojené zdravotnícke prístroje a iné zariadenia. Takisto nebola možná výmena informácií (komunikácia) s inými nemocnicami. Odstupom času boli ako napadnuté zariadenia označené všetky servery, vyše 600 koncových IT staníc (Wokstation z predošlej podkapitoly), röntgenové, ultrazvukové a laboratórne prístroje, CT prístroj a prístroj na magnetickú rezonanciu. Na väčšine týchto zariadení bol preinštalovaný software. Nemocnica mala vytvorené zálohy a tie, ktoré neboli napadnuté, boli použité k obnoveniu dát.

Podľa slov Polície Českej republiky bol ako typ hrozby uvedený ransomware Ryuk. Ryuk je pripisovaný ruským zločineckým skupinám Wizard Spider a CryptoTech a jeho prvý výskyt sa datuje na august 2018. Zameriava sa prevažne na veľké organizácie s cieľom dosiahnuť vysoké výkupné. Za úlohu má zašifrovanie dát.

V tejto informácii však dochádza k nezhode. Na jednej strane za výpadok počítačovej siete môže ransomware, ktorého znakom je vyžadovanie výkupného a na druhej strane je vyhlásenie hajtmanky Stredočeského kraja, Jaroslavy Pokornej Jermanovej, ktorá uviedla, že za odblokovanie zašifrovaných dát nepožiadal nikto výkupné. Existuje takisto

informácia, že pri odšifrovaní napadnutých zariadení bola v systéme nájdená podozrivá šifrovaná e-mailová adresa, ktorá bola predaná Polícii Českej republiky. Predpokladá sa, že bola využitá prvej fázy útoku, kde sa malo jednať o masívnu spamovú a phishingovú kampaň. V podozrivej e-mailovej správe sa mala nachádzať príloha s falošnou faktúrou, ktorá sa tvárila ako od dôveryhodného odosielateľa. Pri kliknutí na faktúru sa mal spustiť malware Emotet, ktorý umožnil stiahnutie ransomwaru na infikované zariadenie.

Nemocnica sa dostala do plnej prevádzky v priebehu januára 2019. Avšak s následkami tohoto incidentu sa bude nemocnica vysporiadať ďalších 5 až 6 mesiacov.

Škoda bola odhadnutá na 38 miliónov českých korún. K tomu je však potrebné pripočítať ďalšie 2 milióny za preinštalovanie softwaru. Nemocnica navyše nedostávala po dobu 3 týždňoch platby od zdravotných poisťovní, kvôli uzavretiu oddelení. Údajná čiastka, ktorú mala zinkasovať nemocnica za deň bola 3 milióny českých korún. Na to sa však nemocnica odvolala ako na zásah vyššej moci. Nemocnica dostala od Stredočeského kraja dotácie vo výške 30 miliónov českých korún.

2.3.2 Kybernetický útok – OKD

Prvý útok: 20. december 2019

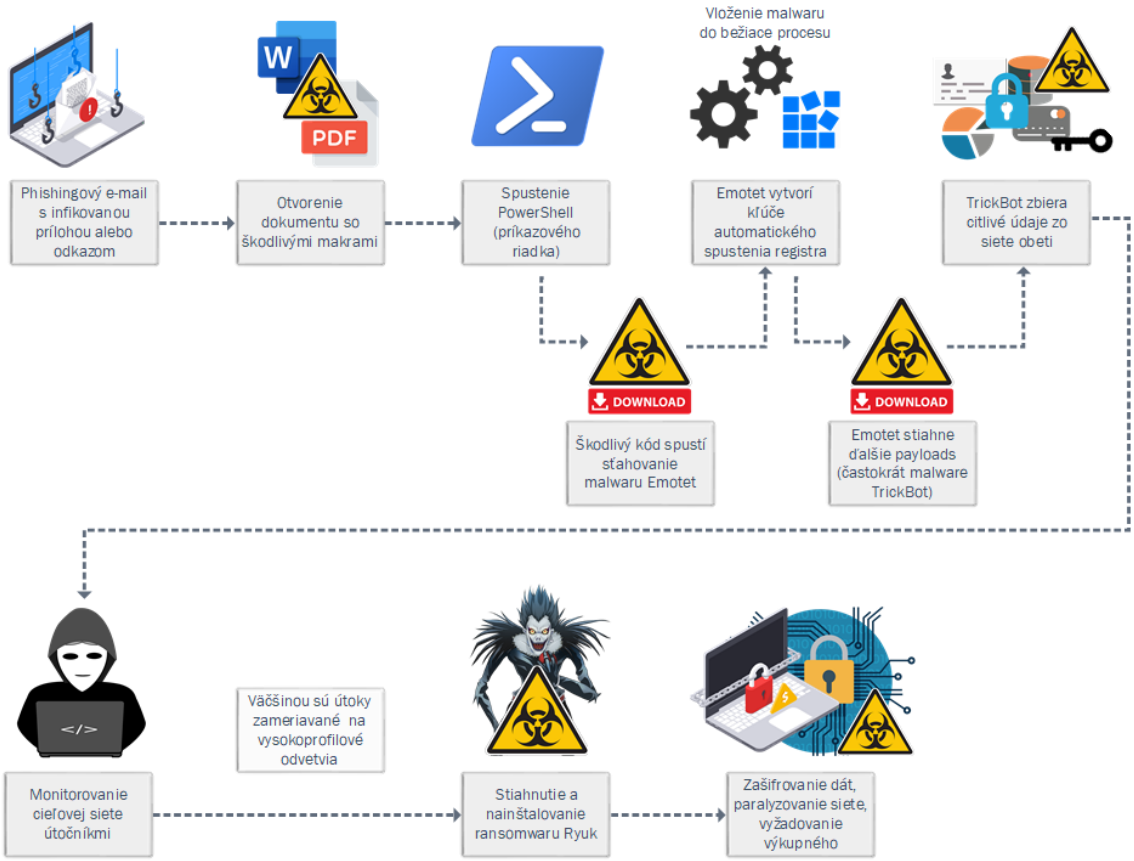
Hlavný útok: 22. december 2019, okolo 22:00

V čase spracovávania údajov práce neboli známe presnejšie informácie, ako sú uvedené v texte nižšie.

Rovnako ako v prípade nemocnice v Benešove, tak aj v tomto prípade bol za daný incident nahlásený ransomware Ryuk. Jedno sa opäť o komplexný útok, kde škodlivý kód napadol a ochromil celú infraštruktúru spoločnosti (celá sieť a všetky jej servery). IT pracovníci spoločnosti sa ihneď pustili do preinštalovania najdôležitejších staníc a obnovy systému a po útoku vytvorili oddelenú internú sieť, ktorá bude monitorovať počet zamestnancov v baniach a bude ovládať vybrané stroje v podzemí.

Podľa hovorcu spoločnosti OKD má obnova primárnej siete a kompletná obnova dát trvať niekoľko týždňov a mesiacov, pretože infraštruktúra OKD je zložitejšia ako v nemocnici Rudolfa a Stefanie v Benešove.

Na obrázku nižšie môžeme vidieť mnou vytvorenú schému najčastejšie sa vyskytovaných krokov infikovania počítačovej siete ransomwarom Ryuk.



Obrázok 12: Najčastejšie kroky pri infekcii ransomwarom Ryuk
Zdroj: Vlastné spracovanie podľa [28; 29; 30]

Celý proces infikovania začína zaslaním phishingového e-mailu obsahujúceho škodlivú prílohu alebo odkaz na webovú stránku, kde sa automaticky stiahne dokument. V e-mailovej prílohe sa častokrát nachádzajú súbory s koncovkami .docx, .xlsx, .pdf alebo .zip. Tieto súbory obsahujú škodlivé makrá, ktoré po stiahnutí a otvorení dokumentu spustia škodlivý kód v prostredí príkazového riadka PowerShell. Škodlivý kód následne spustí sťahovanie malwaru Emotet, ktorý následne vytvorí kľúče automatického spustenia registra. Už v tejto fáze môže nastať zbieranie citlivých údajov o systéme. Malware Emotet následne stiahne do systému malware Trickbot, ktorý začne vykonávať škodlivé akcie ako zbieranie citlivých údajov z napadnutej siete. Všetky citlivé údaje sú preposielané útočníkom, ktorí tak môžu monitorovať napadnutú sieť. Útočníci sa väčšinou zameriavajú na vysokoprofilové odvetvia, väčšinou odvetvia kritickej infraštruktúry, napr. zdravotníctvo. Pokiaľ útočníci usúdia, že infikovaná cieľová sieť je

pre nich atraktívna, stiahnu a nainštalujú do nej ransomware Ryuk. Tento ransomware následne zašifruje všetky dáta, paralyzuje sieť a následne vyžaduje výkupné od obete. Výkupné je väčšinou vyžadované v kryptomenách ako Bitcoin a podobne.

2.4 SUMARIZÁCIA ANALÝZY SÚČASNÉHO STAVU

Kapitola *Analýza súčasného stavu* pozostávala z troch hlavných analýz, ktoré boli rozpracované na ďalšie čiastkové analýzy. Hlavnými analýzami boli *Analýza reportov z portálu ThreatGuard*, *Analýza reportov spoločnosti Kaspersky* a analýza *mediálnych správ za rok 2019*. Cieľom analýz bolo získať užitočné sumárne informácie o existujúcich hrozbách, zraniteľnostiach a typoch útokov. Výsledné informácie boli primárne zamerané na malé až veľké spoločnosti, pôsobiace na území Českej republiky, doplnené globálnymi informáciami.

Analýza reportov z portálu ThreatGuard pozostávala 5 čiastkových častí – boli to analýza hrozieb za 3. a 4. kvartál roku 2019, analýza vendorov za rok 2019, ktorá bola porovnávaná s analýzou vendorov doplnených o skupinu ostatných vendorov, ktorá vznikla podľa určitých pravidiel uvedených v texte a analýzy aktív za rok 2019, respektíve za posledné dva kvartáli roku 2019. Z jednotlivých analýz vyplýva nasledovné: vo všetkých analýzach sa nachádzali 2 atribúty, ktoré spoločne mali vysoký počet percent výskytu – v analýze hrozieb mali 2 najviac vyskytované typy hrozieb (*Spustenie ľubovoľného kódu* a *Denial of Service*) približne 52,57% podiel na celom grafe, v analýze vendorov mali 2 najviac ohrození vendori (*Cisco* a *Microsoft*) približne 46,24% podiel na celom grafe a najväčší percentuálny podiel zaznamenali aktíva *Server* a *Workstation* v analýze aktív za rok 2019 a to 75,52 %.

Najzávažnejšie zraniteľnosti na portáli ThreatGuard, s CVSS skóre závažnosti 10, boli celkovo 4. Ohrozenými vendormi boli *Samsung*, *Elasticsearch* a dvakrát *Cisco* a zariadenia, v rovnakom poradí, *Mobile*, *Workstation*, *Router* a *Switch*. Dvakrát bol ako typ hrozby uvedené *Spustenie ľubovoľného kódu* a ostatné dva razy *Authentication Bypass* (*Obídenie overovania*).

Ďalšou hlavnou analýzou bola *Analýza reportov spoločnosti Kaspersky*. Tá pozostávala z 2 čiastkových analýz reportov od tejto spoločnosti. Z týchto reportov vyplýva nasledovné:

- došlo k nárastu počtu aktívne zneužívaných exploitov nultého dňa,
- najbežnejším typom útokov zostali sieťové útoky, nasledované zneužitím SMB protokolu (slúžiacemu ku komunikácii medzi sieťovými uzlami) alebo dotazy „ťažby“ hesiel, ktoré boli cielené na populárne sieťové služby a servery (napr. Remote Desktop Protocol a Microsoft SQL),
- nárast počtu útokov na osobné dáta označených ako stalkerware,
- pokles škodlivých mobilných inštalačných balíkov pre Android,
- najviac škodlivých exploitov zaznamenali aplikácie Office (65,59 %) a Browser (16,22 %).

Spoločnosť Kaspersky vo svojich ročných reportoch uviedla 4 zraniteľnosti odhalené jej odborníkmi. Tri z tých zraniteľností sa týkali vendora *Microsoft*, jedna vendora *Google*. Rovnako trikrát boli zraniteľnými zariadeniami zároveň *Server* a *Workstation* a zvyšný raz *Webový prehliadač*. Ten istý pomer zaznamenali aj typy hrozieb – trikrát to bola *Eskalácia privilégií* a raz *Use-after-free*.

Posledná v poradí bola analýza *Mediálnych správ za rok 2019*. Vyberané boli mediálne správy týkajúce sa kybernetických útokov, ktoré zasiahli Českú republiku. Dva takéto medializované útoky sa vyskytli na konci roka 2019. Jednalo sa o útoky na nemocnicu Rudolfa a Stefanie v Benešove a na spoločnosť OKD, producenta čierneho uhlia v Českej republike. Oba incidenty sú spájané s ransomwarom Ryuk a u oboch incidentoch boli napadnuté servery a koncové počítačové stanice.

3 VLASTNÝ NÁVRH RIEŠENIA

Súčasťou tejto kapitoly diplomovej práce budú dve hlavné časti, ktoré budú rozdelené do ďalších podčastí. Prvá časť bude pozostávať s vytvorenia predikcií na rok 2020, ktoré budú vecne nadväzovať na analytickú časť. Druhou hlavou časťou tejto kapitoly bude vytvorenie opatrení a odporúčaní na základe analytickej časti a takisto aj možných predikcií.

Úlohou a cieľom tejto kapitoly je vytvoriť dokument resp. brožúru, ktorá bude užitočná pre malé, stredné, ale aj veľké spoločnosti v roku 2020 v oblasti ICT bezpečnosti. Tento dokument bude obsahovať informácie dôležité pre IT bezpečnostné oddelenia, ako aj pre správcov sietí alebo manažérov spoločností.

3.1 PREDIKCIE PRE ROK 2020

Predikcie pre rok 2020 sú prvou hlavnou časťou návrhovej časti diplomovej práce. Budú zostavené na základe trendov vychádzajúcich z fúzie analýz reportov zo služby ThreatGuard, spoločnosti Kaspersky a sčasti aj mediálnych správ o kybernetických útokov na české objekty, kde by mala trend naznačiť trendová krivka roku 2019 vybraných analýz. Ďalšie predikcie budú pozostávať zo selektovaných informácií, ktoré sú obsiahnuté v predikciách nachádzajúcich sa v dokumentoch vendorov alebo na webových stránkach.

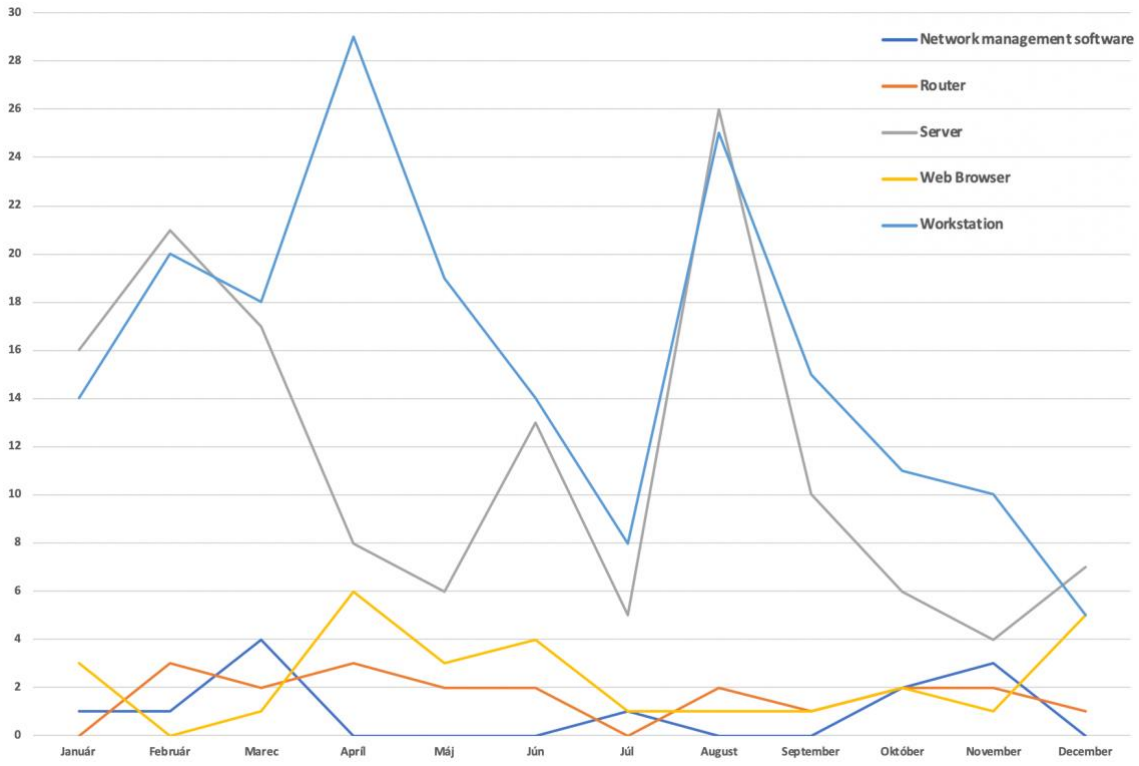
Súčasťou tejto podkapitoly budú informácie, ktoré nadväzujú na analytickú časť po vecnej stránke, ako aj prichádzajúce a rozvíjajúce sa technológie a riziká pre spoločnosti s nimi spojené.

3.1.1 Predikcie podľa analytickej časti práce

Z analýz dát portálu ThreatGuard boli v predchádzajúcej kapitole vytvorené grafy a komentáre, ktoré poukazujú stav informačnej a kybernetickej bezpečnosti určený istými kritériami, ktoré vytvorila spoločnosť COMGUARD a jej IT odborníci. Spracované reporty v danej službe sú vytvárané zo selektovaných zdrojov, ktorých miera závažnosti zraniteľností je podľa hodnotenia CVSS skóre stredná, vysoká a kritická. Takisto sú brané

do úvahy zdroje, ktorých obsah sa týka a zasahuje prevažne českých a slovenských zákazníkov tejto služby.

Aby sme určili predikcie podľa tohoto zdroja, je potrebné stanoviť spôsob, podľa ktorého bude môcť vytvoriť určitý trend. Zvolený spôsob bude analyzovanie druhej polovice roku 2019, tretieho a štvrtého kvartálu alebo vykreslenie trendových kriviek pozostávajúcej z piatich najviac vyskytovaných údajov vo vybranej analýze, ako je tomu na obrázku nižšie..



Graf 8: Trendové krivky piatich najviac ohrozených aktív za rok 2019
Zdroj: Vlastné spracovanie

Na obrázku vyššie sú vytvorené trendové krivky vytvorené podľa jednotlivých mesiacov. Krivky naznačujú trend piatich najviac vyskytovaných zariadení v reportoch ThreatGuard, ktoré boli ohrozené počas celého roku 2019. V práci už bolo zmieňované, že počas letných a zimných mesiacov dochádza k poklesu výskytu zraniteľností a hrozieb, ako aj spracovaných reportov. Preto vidíme na grafe, ako sa všetky krivky približujú v mesiaci december k jednému bodu. Aj napriek prevažne klesajúcej tendencii vyššie uvedených zariadení, môžeme predikovať, že pozíciu najviac ohrozených zariadení si aj v roku 2020 udržia *Server* a *Workstation*. Tieto zariadenia sú najzraniteľnejšími z dôvodu ich vlastnenia v takmer každej organizácii. Navyše pri

zariadení *Workstation*, je vysoké potenciálne riziko interakcie používateľa tohoto aktíva. Práve vďaka interakcii používateľa dochádza k najčastejšie k zraniteľností. Navyše aj pri hrozbe ransomwaru je častým prvým krokom infikovania celej siete interakcia užívateľa pri otváraní škodlivej e-mailovej prílohy alebo zistenie administrátorského hesla po nevhodnej interakcii užívateľa (škodlivý odkaz, otvorenie alebo stiahnutie súboru). Predpokladom teda je, že sieťové útoky budú v roku 2020 stále najčastejšie sa vyskytujúcimi typom útokov.

Naspäť k ransomwaru. Z analyzovaných reportov služby ThreatGuard sa typ hrozby ransomware objavil len trikrát v roku 2019. Avšak všetky tri výskyty sa nachádzajú v poslednom štvrtom kvartáli roku. Tento údaj sa zhoduje aj s analýzou mediálnych správ týkajúcich sa kybernetickej bezpečnosti. Oba prípady, ako nemocnica v Benešove, tak aj kybernetický útok na OKD, ktorých príčinou bol ransomware, sa vyskytli v decembri roku 2019. Môžeme teda očakávať, že tento typ hrozby bude postihovať české spoločnosti aj v roku 2020.

To potvrdzuje aj prípad z 13. marca 2020, keď bol vykonaný kybernetický útok na Fakultnú nemocnicu v Brne, ktorého príčinou bol ransomware. Problémom nemocnice sú zašifrované dáta, nedostupnosť databáz a záloh a napadnuté všetky koncové stanice, ktorých počet je približne 2300. Navyše nemocnici hrozí strata všetkých doterajších údajov o pacientoch, pretože záloha dát v tomto objekte bola nedostatočná.

Porovnaním cieľových aplikácií z reportu ThreatGuard a z reportu Kaspersky môžeme predikovať, že hrozby týkajúce sa webových prehliadačov budú pokračovať aj do roku 2020 v pomerne vysokých číslach. V trendovej krivke analýzy ThreatGuard možno vyčítať, že počet výskytov zraniteľností vo webových prehliadačoch rástol a takmer sa dostal na maximálnu hodnotu celého roku, ktorá bola 6 výskytov v mesiaci apríl. Z reportu Kaspersky vyplýva, že aj napriek miernemu poklesu oproti predchádzajúcemu roku, z vybraných analyzovaných cieľových aplikácií, sú exploity na aplikácie *Browser* druhé najviac sa vyskytujúce po exploitoch na aplikácie *Office*. Práve tieto aplikácie sú pravdepodobne najviac využívanými medzi spoločnosťami a určite by nemali byť nepovšimnuté pri vytváraní opatrení pre rok 2020.

3.1.2 Predikcie spracované z iných zdrojov

Tieto predikcie budú pozostávať zo selektovaných informácií, ktoré sú obsiahnuté v predikciách nachádzajúcich sa v dokumentoch vendorov alebo na ich webových stránkach. Informácie budú získavané z dokumentov *Kaspersky Security Bulletin – Advanced threat predictions for 2020* a *The new norm – Trend Micro Security Predictions for 2020* a z webových stránok obsahujúcich predikcie od McAfee – *McAfee Labs 2020 Threat Predictions Report* a Check Point – *2020 Vision: Check Point's cyber-security predictions for the coming year*.

Týmito zdrojmi bude zvýšená adekvátnosť, ako aj presnosť predikcií, pre nasledujúci rok. Informácie vybrané a spracované v tejto časti môžu byť kvalitným smerovačom pre spoločnosti.

3.1.3 Ransomware v roku 2020

Ransomware je stále najúčinnejším nástrojom na získanie finančného zisku od obetí. V posledných dvoch rokoch zaznamenávame zameriavanie sa útočníkov na určité oblasti a organizácie. Toto cielené prenikanie do podnikových sietí nazývame ako takzvaný **cielený ransomware**. Zameriavanie útokov má svoje opodstatnenie. Útočníci cielia častokrát svoje útoky na organizácie, pri ktorých sa predpokladá, že bude zaplatená vyššia čiastka výkupného pre získanie dát späť. Jedná sa prevažne o veľké spoločnosti, štátne a miestne samosprávne orgány, systémy priemyselnej kontroly alebo, ako to bolo za posledné obdobie, dvakrát, v Českej republike, zdravotnícke organizácie. Jedná sa o odvetvia a organizácie, ktoré nemôžu fungovať s akýmikoľvek výpadkami. Dôvod je jasný, takéto organizácie vlastnia pomerne veľký objem citlivých dát.

Nárast **cieleného ransomwaru** vytvoril takisto rastúci dopyt po ohrozených podnikových sieťach. Tento dopyt je uspokojovaný zločincami, ktorí sa špecializujú naraz na prenikanie do podnikových sietí a predaj úplného prístupu do siete. Preto pravdepodobným budúcim vývojom v roku 2020 bude ďalší nárast **cieleného ransomwaru** na exfiltráciu citlivých podnikových dát. Predpokladajú sa však agresívnejšie pokusy o vydieranie peňazí. Útočníci sa budú usilovať okrem nepoužiteľnosti súborov aj o hrozbu zverejnenia údajov. To bude možné realizovať **dvojfázovým vydieracím útokom**, kde v prvej fáze počítačový zločinci začnú

s ochromujúcim ransomware útokom, ktorým budú vydierať obete, aby dostali svoje súbory späť. Po predpokladanom odmietnutí zaplatenia výkupného za dáta by nastala druhá fáza. V tejto fáze sa zločinci zamerajú na zotavujúce sa obete ransomware útoku znova vydieračským útokom. Avšak tentoraz budú hroziť, že zverejnia citlivé údaje ukradnuté pred ransomware útokom. Druhou fázou sa zvýši pravdepodobnosť zaplatenia výkupného a prípadne aj jeho navýšenie.

Okrem tejto zmeny, je možné, že útočníci sa pokúsia o **diverzifikáciu svojich útokov**. Okrem bežne napádaných klientskych staníc alebo serverov, môže nastať rozšírenie na iné typy zariadení, napríklad na cloud. Práve servery a údaje spoločností sú presúvané na túto platformu. Preto môže v roku 2020 dôjsť k snahe smerovať ransomware práve na túto službu, ktorá obsahuje veľké množstvo dôležitých a citlivých údajov.

Posledným smerom, ktorým ransomware útoky môžu v roku 2020 smerovať, je **zničenie záloh**. Zničením záloh sa zároveň zvyšuje percento obetí, ktoré zaplatia výkupné. Týka sa to najmä organizácií spoliehajúcich sa na zálohovanie a obnovovanie dát, namiesto preventívnej a rýchlej neutralizácie hrozieb. Týmto krokom sa vystavujú riziku, ktorým sa nebudú môcť zotaviť z útoku ransomware.

3.1.4 Cloudové aplikácie a platformy bez serverov

Podľa dokumentu Českého štatistického úradu, Využívanie informačných a komunikačných technológií v podnikateľskom sektore, za rok 2019 až 82 % firiem s počtom zamestnancov 10 a viac využívalo na zálohovanie firemných dát samostatné/externé úložisko (vrátane zálohovania do cloudu). Na základe tohoto údaju je vhodné vytvoriť predikciu k zariadeniam cloud a platformám bez serverov.

Očakávam prírastok kompromitovaných sietí, kvôli slabým stránkam (zraniteľnostiam) cloudových služieb. Týmito slabými stránkami sú nesprávne konfigurácie v cloudových úložiskách, nedostatočné obmedzenia prístupu, nesprávne spracované kontroly povolení, zastarané zdieľané knižnice a mnohé ďalšie. Kvôli takýmto zraniteľnostiam môže dôjsť k hrozbe spustenie škodlivého kódu a to priamo do kódu alebo prostredníctvom knižnice tretej strany (ktorú užívateľ stiahne a následne dôjde k spusteniu škodlivého kódu), čo môže mať za následok odpočúvanie alebo prevzatie kontroly nad užívateľskými súbormi a informáciami v cloude. Následne existuje možná hrozba prieniku do podnikových sietí.

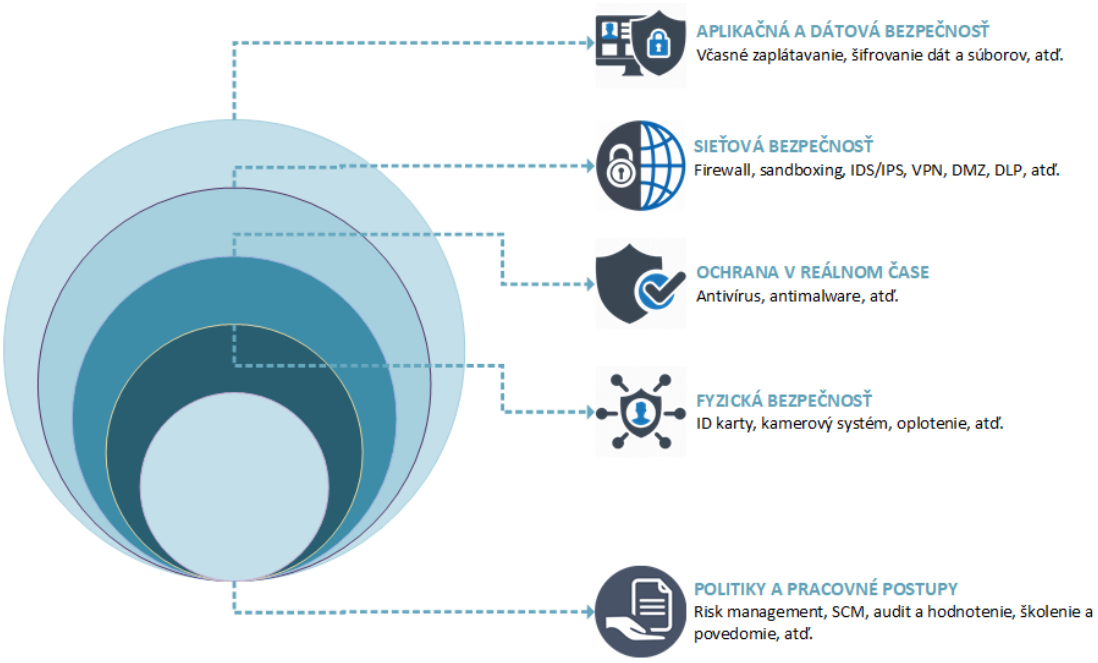
Hlavne open-source platformy bez serverov poskytujú bezstavové funkcie (znamená to, že neexistujú žiadne záznamy o predchádzajúcich interakciách a každá žiadosť o interakciu sa musí byť spracovaná výlučne na základe informácií, ktoré sú s ňou dodávané). Preto by malo byť v roku 2020 dôležité zamerať sa na monitorovanie povolení a ukladanie citlivých údajov, spojených so zlepšovaním procesov a dokumentácie pracovných postupov. *To všetko je spojené s vytvorením bezpečnostných nástrojov a nasadením konkrétnych funkcií.*

Je potrebné brať v úvahu jednoduchú rovnicu, čím viac firemných údajov sa nachádza v cloude, tým je väčší záujem útočníkov.

3.1.5 Predikcie ohľadne Covid-19

Využívanie mobilných zariadení a vzdialených (mobilných) zamestnancov je posledné roky na vzostupe. Práca na diaľku, resp. práca z domu, tiež známa ako home office, má za úlohu zvýšiť produktivitu a znížiť pocit vyhorenia u zamestnancov. V dobe pandémie sa tento typ práce rozšíril a spopularizoval medzi mnohými spoločnosťami v Českej, ako aj Slovenskej republike a pre mnohých sa stal takmer každodenným rituálom. Spoločnosti navyše zredukovali svoje náklady. Je takmer isté, že v roku 2020 rapídne stúpne trend a celkový počet zamestnancov pracujúcich z domu resp. na diaľku.

Spoločnosti by si však mali rovnako uvedomiť, aké riziká práca na diaľku prináša. Tento typ práce môžeme rovnako nazvať ako práca mimo bezpečnostný perimeter spoločnosti. To znamená, že pracovník prišiel o niekoľko vrstiev bezpečnostnej ochrany, ktorá by mala byť súčasťou väčšiny spoločností. Do týchto vrstiev môžeme zaradiť napríklad firemné politiky a pracovné postupy, fyzickú bezpečnosť, sieťovú bezpečnosť, aplikačnú a dátovú bezpečnosť. Viac informácií môžeme vidieť na obrázku nižšie.



Obrázok 13: Vrstvy bezpečnostnej ochrany
Zdroj: Vlastné spracovanie

Okrem toho môžu mobilné zariadenia maskovať kontrolné znaky phishingových útokov alebo iných bezpečnostných hrozieb. Ďalším problémom môže byť slabé zabezpečenie domácej Wi-Fi siete, ako je zdieľaný alebo verejný pracovný priestor. Otvorená sieť ponecháva citlivé súbory a informácie na dosah ostatným užívateľom v tej istej sieti. Slabé zabezpečenie siete môže spôsobiť napadnutie vzdialeného zariadenia škodlivým softwarom, čo môže mať za následok eskaláciu oprávnení až do podnikovej siete a únik citlivých informácií.

Iným problémom môže byť používanie viacerých zariadení, pomocou ktorých sa zamestnanec pripája a získava prístup ku cloudovým aplikáciám a komunikačnému softwaru.

S globálnou pandémiou sú spojené aj iné predikcie. Zvyšuje sa pravdepodobnosť nárastu zraniteľností a hrozieb pre aplikácie na vykonávanie videohovorov, ako je Zoom, Microsoft Teams alebo Skype. Problém môže nastať pri sťahovaní inštalačných balíčkov z neoficiálnych centier sťahovania vendorov, respektíve ich oficiálnych stránok. V súboroch stiahnutých z iných webových stránok sa môže nachádzať škodlivý inštalačný súbor. Ďalším nebezpečenstvom pre možné infikovanie vzdialených zariadení môžu byť škodlivé spamové phisingové e-maily, ktoré môže obsahovať škodlivé súbory alebo URL odkazy na škodlivé stránky, ktoré môžu obsahovať napríklad malware.

3.1.6 Častejšie zneužívanie zraniteľností s vysokou závažnosťou

Do zraniteľností s vysokou závažnosťou budú zaradené dve dôležité chyby zabezpečenia, ktoré sa vyskytovali v predošlých rokoch, ale tento rok by mal počet útokov na tieto zraniteľnosti rásť. Prvá chyba má anglický prívlastok „wormable“, ktorého význam je nasledovný – jediným zneužitím zraniteľnosti sa malware, väčšinou sa jedná o vzdialené spustenie kódu, rýchlo šíri zariadeniami, bez potreby akejkoľvek interakcie od správcov sietí alebo používateľov. Dňa 14. mája 2019 bola opravená kritická zraniteľnosť vzdialeného spustenia kódu od Microsoftu v aplikácii Microsoft Remote Desktop, používaný na administráciu vzdialenej plochy, nazývaná ako BlueKeep. Od tej doby vendor zverejňuje podobné aktualizácie zraniteľností týkajúce sa služieb vzdialenej pracovnej plochy v systéme Windows.

V roku 2020 bude častejšie zneužívanou práve zraniteľnosť BlueKeep, ku ktorej sa pridajú pokusy o zneužitie ďalších známych zraniteľností s vysokou závažnosťou, ktoré budú ohrozovať nechránené systémy cez široko používané protokoly, ako napríklad Server Message Block (SMB) a Remote Desktop Protocol (RDP). Navyše kombinácia zraniteľnosti BlueKeep a RDP protokolu je bežným vstupným vektorom pre ransomware útok.

Druhou chybou, ktorá by mohla byť pre spoločnosti veľkým problémom, je chyba v deserializácii nedôveryhodných údajov. Keď je táto zraniteľnosť zneužitá, dochádza k modifikácii dát alebo k možnému spusteniu kódu kontrolovaného útočníkom. To umožňuje útočníkom pomerne jednoduché získanie vzdialeného prístupu.

3.2 OPATRENIA A ODPORÚČANIA PRE SPOLOČNOSTI

Druhou hlavou časťou kapitoly *Vlastný návrh riešenie* bude vytvorenie opatrení a odporúčaní na základe analytickej časti a takisto aj predikcií zmienených v predošlej časti. Táto časť bude obsahovať všeobecné údaje, ktoré budú obsahovať štatistiky Českého štatistického úradu za rok 2019 týkajúce sa bezpečnosti ICT, o ktorých bude popísané viac v nasledujúcej podčasti. Zvyšné časti budú pozostávať z opatrení a odporúčaní pre spoločnosti pre jednotlivé časti firemnej infraštruktúry, ktoré vecne nadväzujú na predošlé kapitoly diplomovej práce. Všetky nižšie zmienené opatrenia

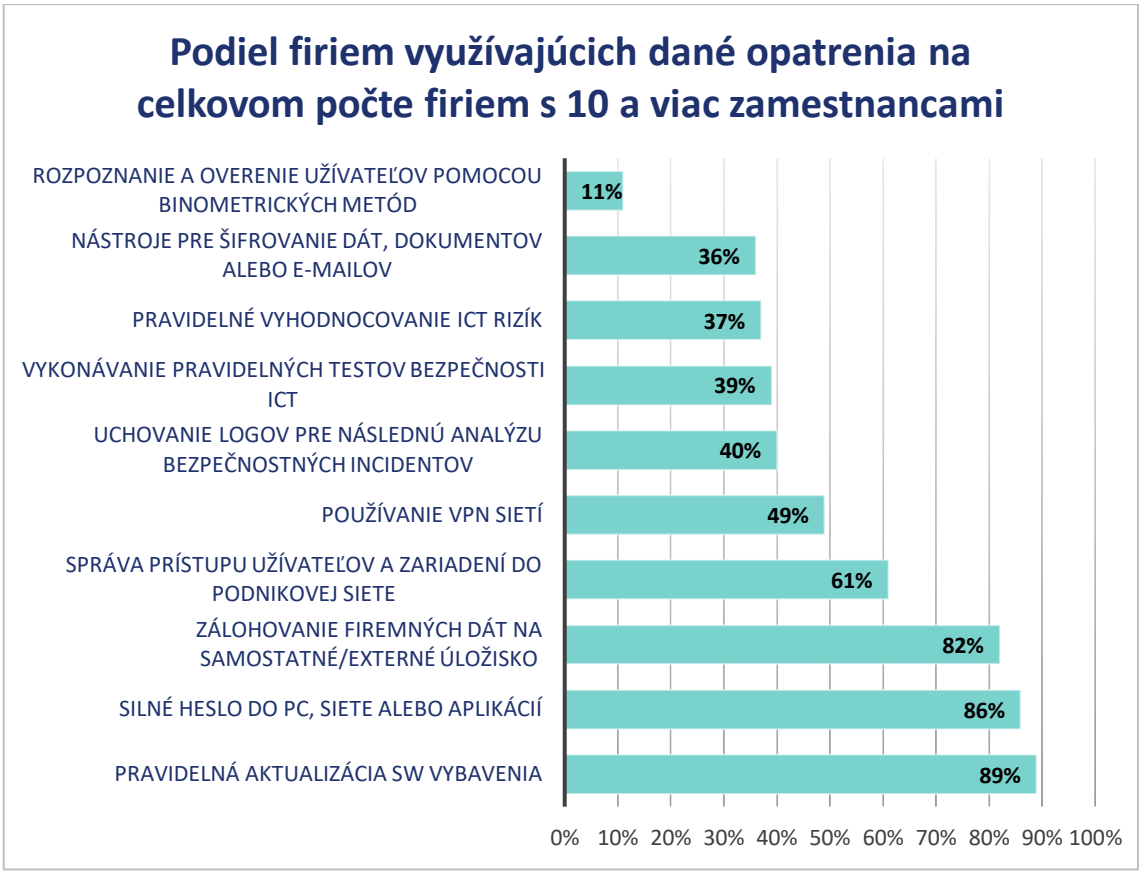
a odporúčania sú dôležité pre všeobecnú bezpečnosť informačných a komunikačných technológií a zároveň sú potrebnou prevenciou proti ransomware útokom.

Na úvod budú zmienené štatistiky Českého štatistického úradu (ďalej iba ČSÚ) za rok 2019. Dáta, z ktorých boli spracované štatistiky uvedené nižšie vychádzajú z výsledkov ročných štatistických šetrení ČSÚ o využívaní informačných a komunikačných technológií v podnikateľskom sektore v Českej republike. Pre účely tejto diplomovej práce bol vybraný graf z kapitoly *Bezpečnosť ICT*. Tento graf akurátne poukazuje na situáciu medzi spoločnosťami v Českej republiky a ich prístupu k zabezpečeniu informačných a komunikačných technológií, ktorým spoločnosti pristupujú k znížení rizika napadnutia a zneužitia získaných informácií. V praxi to znamená ochranu pred neoprávnenou fyzickou manipuláciou so zariadeniami, zabezpečenie prístupu k elektronickým dátam a ochranu pred ich neoprávnenou manipuláciou, šifrovanie vzájomnej komunikácie a uložených dát a ich pravidelné zálohovanie.

Z vybraného grafu vyplývajú nasledujúce zistenia. Najviac využívanými opatreniami k zaisteniu bezpečnosti informačných a komunikačných technológií (ďalej iba ICT) boli pravidelná aktualizácia softwarového vybavenia, používanie silného hesla do počítača, siete alebo aplikácií a zálohovanie firemných dát na samostatné alebo externé úložisko. Všetky zmienené opatrenia využívajú spoločnosti s 10 a viac zamestnancami vo viac ako 80 % prípadov. Vo viac ako polovici prípadov spoločnosti používajú riadenie prístupov užívateľov a zariadení do podnikovej siete. To zahŕňa kontrolu oprávnenia prístupov do objektu alebo k firemným dátam.

Následne medzi 35 – 50 % sa nachádza 5 opatrení, medzi ktoré patria používanie VPN sietí, uchovanie logov pre následnú analýzu bezpečnostných incidentov, vykonávanie pravidelných testov bezpečnosti ICT, pravidelné vyhodnocovanie ICT rizík a nástroje pre šifrovanie dát, dokumentov alebo e-mailov. Z toho vyplýva, že pravidelné aktivity týkajúce sa bezpečnosti ICT nie sú veľmi populárnymi medzi spoločnosťami v Českej republike.

Najmenej rozšíreným opatrením medzi českými spoločnosťami je využívanie rozpoznávania a overovania užívateľov pomocou biometrických metód. Medzi takéto metódy môže patriť rozpoznávania tváre, otlačok prsta alebo ruky, rozoznávanie dúhovky oka, rozoznávanie hlasu a iné fyziologické a behaviorálne merania.



Graf 9: Podiel firiem využívajúcich dané opatrenia
Zdroj: Vlastné spracovanie podľa [31]

3.2.1 Pre sieťovú infraštruktúru

Pri implementácii bezpečnostných opatrení by sa malo začať zabezpečením nastavení siete, databáz a klientskeho rozhrania. Zabezpečenie siete zahŕňa správu topológie, izoláciu siete, a obmedzenie sieťových služieb a protokolov. Na záver tejto podčasti bude uvedená odporúčaná schéma siete.

Vhodné je logické rozdelenie siete na menšie celky, tzv. segmentácia a takisto oddelenie užívateľských práv jednotlivých užívateľov, tzv. segregácia, kde bude prístup priraďovaný na základe rolí alebo polohy užívateľov. Segmentáciou budú umiestnené kritické podnikové systémy, ako aj citlivé informácie do oddelenej siete. Jednou z možností môže byť rozdelenie siete na internú zónu, intranet, vonkajšiu zónu, internet a vytvorenie tzv. demilitarizovanej zóny, v ktorej budú prebiehať procesy autentifikácie, kontrola proti známym internetovým útokom, validácia vstupov a výstupov do/zo siete a mnohé ďalšie bezpečnostné obmedzenia.

Jednotlivé segmenty siete je vhodné oddeliť zariadením firewall. Na firewalloch oddeľujúcich siete, ako aj na aplikačnom firewalle umiestnenom, napríklad, v demilitarizovanej zóne, je vhodné využiť tzv. whitelist. Jedná sa o povolenie len žiadúcich užívateľov, služieb, autorizovaného softwaru a štandardnej prevádzky. Tým možno dosiahnuť, že k určitému zariadeniu má prístup iba konkrétna IP adresa alebo rozsah IP adries. Je to efektívnejšia technika ako tzv. blacklist, v ktorej má prístup každý užívateľ/služba okrem blokovaných. Vhodným riešením by bolo využitie Next Generation Firewallov (NGFW). Oproti bežným firewallom, ktoré majú za úlohu staticky kontrolovať a blokovať porty a protokoly, NGFW disponuje funkciami ako kontrola na úrovní aplikácií, integrovaná prevencia proti prienikom alebo schopnosť blokovať pokročilé útoky malwaru.

Avšak „firewally novej generácie“ majú vysokú obstarávaciu cenu. Preto väčšine spoločností bude vyhovovať doplniť klasický firewall o IDS – Intrusion Detection System (detekčný systém prienikov) alebo IPS – Intrusion Prevention System (prevenčný systém prienikov) systémov. Systémy slúžia na sledovanie sieťovej prevádzky a identifikáciu podozrivých aktivít v rámci prevádzky siete. IDS dokáže útoky len detekovať a následne ich ohlásiť, ale IPS dokáže útoky aj blokovať. Je odporúčané blokovať hrozby už na perimetri.

Ďalším dôležitým bodom je sledovanie a uchovávanie sieťovej prevádzky. Sieťovú prevádzku je možné monitorovať pomocou sieťových prvkov, ako napríklad firewall alebo router. Následne je možné sledovať komunikáciu medzi klientami a servermi, klientov do internetu, komunikáciu medzi servermi a prevádzku na perimetri siete. Identifikované prevádzkové a bezpečnostné problémy je následne vhodné uchovať pre prípadné budúce skúmanie, keď nastane incident preniknutia do siete a systémov alebo iný incident ohrozujúci sieťovú infraštruktúru.

V neposlednej rade je vhodné zaviesť centrálne zaznamenávanie logov sieťových udalostí a ich automatické vyhodnocovanie. To je potrebné pre porozumenie organizácie o existujúcich, vznikajúcich a historických bezpečnostných udalostiach, ktoré súvisia s bezpečnostnými incidentami. Rovnako je potrebné vytvoriť jednotnú stratégiu na zaznamenávanie a koreláciu týchto udalostí. Táto stratégia musí využívať logovanie zo všetkých sieťových zariadení.

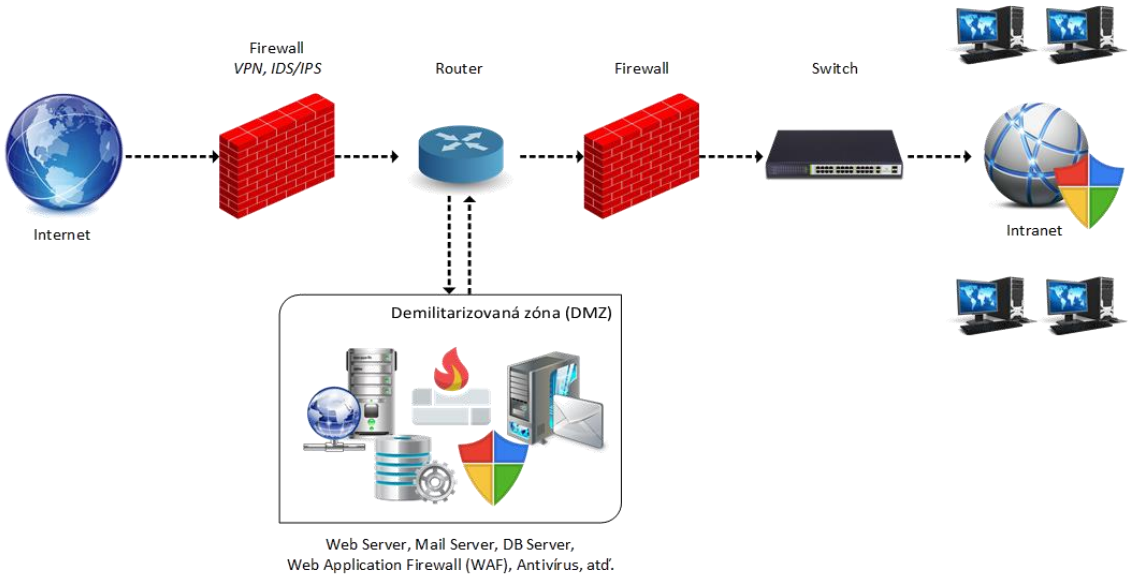
Následne je na samotnej spoločnosti, aký štruktúrovaný prístup vyvinie k analýze logov a sledovaniu incidentov. Môže sa jednať o jednoduchý prístup, ale až o dôsledné preskúmavanie údajov doplnené o pokročilú analýzu so stanovenými pravidlami. Riešením centrálneho umiestnenia logov a ich informácií je vzdialený syslog server. Samotný server ako aj prenos informácií na tento server by mal byť šifrovaný.

Kde je možné, použite šifrovanú komunikáciu. Pôjde predovšetkým o šifrovanú internú komunikáciu klient/server, šifrovanie dát alebo autentifikačných údajov pomocou protokolu Secure Sockets Layer (SSL) alebo Transport Layer Security (TLS). Pre šifrovanie dát je vhodné používať algoritmus AES-256. Takisto šifrujte disky počítačov, predovšetkým tých prenosných.

Odporúčam vypracovať Disaster Recovery Plan (DRP) alebo plán obnovy po havárii. Ide o dokument, ktorý zhromažďuje procesy, politiky a postupy týkajúce sa prípravy na zaistenie prevádzky technologickej infraštruktúry kritických pre organizáciu po prírodnom alebo človekom vyvolanom incidente či katastrofe.

Používanie virtuálnej súkromnej siete (VPN) pripojenia, ktoré umožní vzdialeným používateľom, prípadne aj pobočkám spoločností, zabezpečený prístup do sieťovej infraštruktúry, ku konkrétnym aplikáciám a zdrojom. Aby bola zabezpečená bezpečnosť, musí byť vytvorené súkromné sieťové point-to-point spojenie pomocou šifrovaného protokolu, ktorý vytvorí akýsi tunel medzi uzlami sietí. Používatelia VPN potom používajú na získanie prístupu autentifikačné metódy, ako sú heslá alebo certifikáty.

Na obrázku nižšie sa nachádza odporúčaná schéma IT podnikovej infraštruktúry vytvorená podľa odporúčaní a opatrení zmienených v predošlých riadkoch.



Obrázok 14: Zjednodušená odporúčaná schéma IT podnikovej infraštruktúry
Zdroj: Vlastné spracovanie

Pre ďalšie zvýšenie bezpečnosti infraštruktúry a celej siete odporúčam pravidelne kontrolovať otvorené porty a blokovať nepoužívané. Pravidelná kontrola zabezpečí, aby sa do siete nedostával škodlivý kód, Trojské kone alebo červy. Takisto pri pomerne častých zmenách v sieti, nezabúdajte na pravidelnú kontrolu vstupných bodov do siete, aby ste predišli a zabránili prieniku nechcených súborov a aplikácií a rovnako úniku citlivých informácií.

3.2.2 Pre e-mailovú komunikáciu

Odporúčania a opatrenia pre e-mailovú komunikáciu sú ďalšou podčasťou. Pretože veľké množstvo hrozieb pre spoločnosti prechádza do siete práve cez e-mailovú komunikáciu, je potrebné vyčleniť pre ňu samotnú časť. Otvorením alebo stiahnutím škodlivej prílohy, kliknutím na škodlivý odkaz alebo odpovedaním dôvernými údajmi môže byť vykonaný až ransomware útok na systém. Rovnako aj praktiky sociálneho inžinierstva, ako phishingové e-mailové správy, sú veľmi častou hrozbou pre spoločnosti. V tejto časti budú vymenované niektoré odporúčania, ktoré by mali redukovať zraniteľnosti a hrozby e-mailovej komunikácie.

Prvým odporúčaním je kontrolovať prichádzajúce, ako aj odchádzajúce e-mailové správy a následné blokovanie nežiadúcich správ. Existuje na to pomerne veľké množstvo mechanizmov, ako napríklad autentifikačný protokol DMARC (Domain-based Message

Authentication, Reporting and Conformance), ktorý overuje legitímnych odosielateľov a zabraňuje škodlivým e-mailom alebo neovereným zdrojom, aby dostali do priečinku doručenej pošty zamestnancov a takisto reportuje zlyhania autentifikácie doménových mien odosielateľov.

Ďalším odporúčaním je filtrovanie a blokovanie e-mailov podľa typu súborov nachádzajúcich sa v ich prílohách. Je potrebné prepúšťať len relevantné druhy príloh pre danú spoločnosť. Každá spoločnosť dokáže rozhodnúť, aké typy súborov využívajú jej zamestnanci. Vhodné je takisto limitovanie veľkosti e-mailových príloh alebo skenovanie kľúčových slov v správach. Zaistenie karantény a nápravy pre podozrivé e-mailové správy je takisto dôležité.

Pokiaľ chceme mať naozaj zabezpečený e-mail, tak je nutnosťou pokročilá analýza e-mailov, príloh a URL pomocou analýzy v sandboxe alebo podobnej pokročilejšej technológii. Neustále sa objavujú nové možnosti, ako pridať malware do súborov, ktoré nie sú vo väčšine spoločností blokované, ako napríklad dokumenty Office.

Dôležité je zabezpečiť šifrovanie správ, aby ich mohol prečítať len určený príjemca pomocou súkromného kľúča. Rovnako ako správy, je odporúčané šifrovať spojenie medzi mailovými servermi, pomocou TLS.

V rámci phishingových e-mailov je vhodné voliť jednoduché doménové názvy pre viditeľné prípadné zámeny písmen v týchto e-mailoch. V neposlednej rade je potrebné zaistiť pravidelné školenie zamestnancov na zistenie regulárnych phishingových útokov.

3.2.3 Pre servery a klientske stanice a ich software

Veľmi podstatným odporučením a opatrením pre tieto typy zariadení je ich udržiavanie v aktuálnom stave a pravidelne aplikovať ich bezpečnostné aktualizácie. Operačný systém, ako aj softwarové aplikácie by mali byť aktualizované a zaplátané včas a často. Mali by ste sa uistiť, že ste použili aj základné bezpečnostné konfigurácie, ktoré sú poskytované vendormi vášho softwaru. Rovnako je potrebné dať si pozor na verzie použitých doplnkov a tiež ich pravidelne aktualizovať. Dôležité je používať len dôveryhodný software, od dôveryhodných vendorov a s tým spojené sťahovanie inštalátorov len z oficiálnych (hlavných) webových stránok softwarových aplikácií alebo

z obchodu s aplikáciami. Mnoho súborov je možné sťahovať z viacerých umiestnení na internete, preto je potrebné zamerať sa na tie zabezpečené.

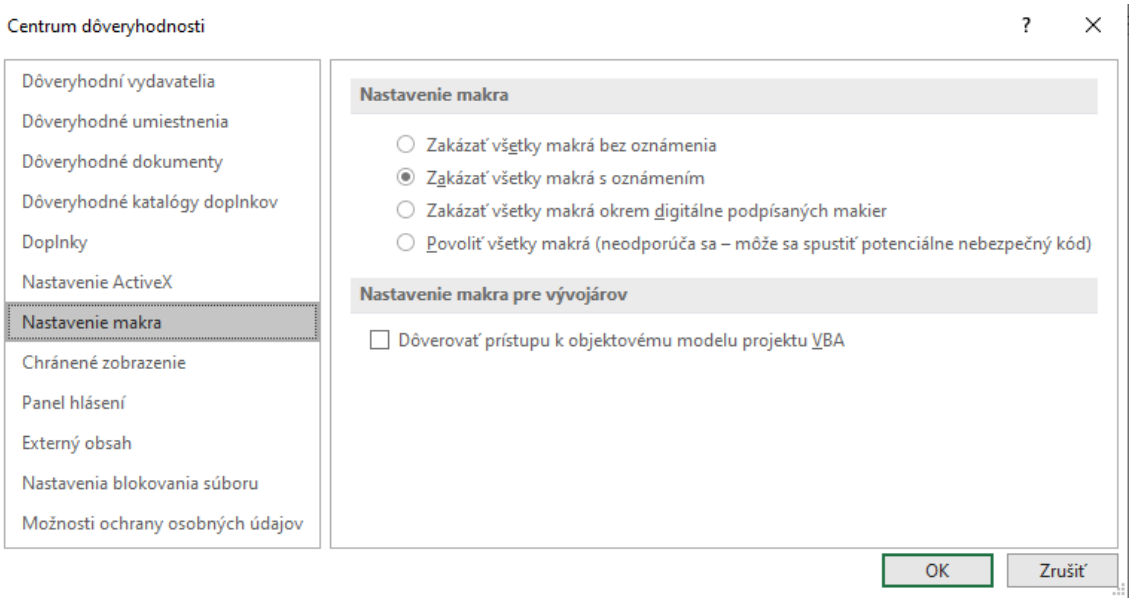
So sťahovaním súborov je spojené nastavenie práv užívateľom, ktorí v spoločnosti môžu a potrebujú sťahovať súbory a aplikácie z webových stránok. Je vhodné zvážiť povolenia len pre dôveryhodných používateľov, ktorí sú povinní sťahovať súbory v rámci svojej každodennej práce a zabezpečte, aby boli títo zamestnanci poučení o bezpečnom sťahovaní súborov. Je takisto vhodné sťahovať súbory cez kontrolovaný kanál, kde bude prebiehať kontrola súborov, ako napríklad web gateway.

So softwarom a súbormi je spojené aj nepoužívanie nepodporovaných produktov. To sa v roku 2020 bude týkať pluginu Adobe Flash Player, keďže koncom tohoto roka skončí podpora tohoto produktu. Ukončením podpory bude skončené vydávanie aktualizácií a distribúcie tohoto produktu. Vhodnou prípadnou náhradou môžu byť štandardy ako HTML5, WebGL alebo WebAssembly.

Pokým to však nie je nevyhnutné, je vhodné zakazovať funkcionality týchto doplnkov a povoliť len vyžadované funkcionality pre prácu používateľov. Tieto odporúčania sa týkajú aj produktov Microsoft Office. Vhodné je povoliť makrá len ak je to nevyhnutné a odporúča sa hľadať potencionálne škodlivé anomálie v dokumentoch Microsoft Office. Makrá automatizujú často vykonávané činnosti a šetria čas strávený písaním na klávesnici a ovládaním myši. Sú častokrát vytvárané vo Visual Basic for Applications (VBA) a sú písané vývojármi softwaru. Niektoré makrá však môžu predstavovať potencionálne riziko pre zabezpečenie. Hackeri môžu do súborov zaviesť deštruktívne makro, ktoré môže do klientskej stanice alebo do siete organizácie rozšíriť vírus. Pokiaľ sú makrá povolené, tak by mali byť kontrolované a mala by byť obmedzená ich činnosť. Makro by nemalo mať povolenú komunikáciu do internetu alebo spúšťanie ďalších procesov. Takéto zmeny je možno vykonať pomocou Host IPS.

Odporučil by som zmeniť odporúčané nastavenia makier a zabránil používateľom v ich akejkoľvek budúcej zmene. Dôležité je nastaviť makrá pre všetky aplikácie Office. Zmenu nastavení makier je možné vykonať v Centrum zabezpečenia v českých verziách alebo v Centrum dôveryhodnosti v slovenských verziách. Postup pre operačné systémy Windows je nasledovný:

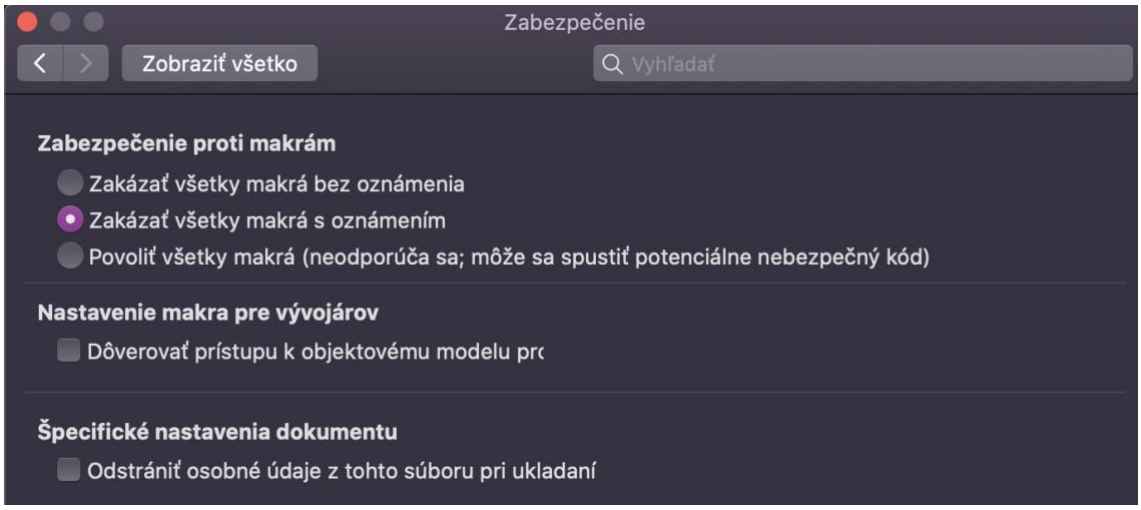
1. Kliknite na kartu **Súbor**.
2. Kliknite na tlačidlo **Možnosti**.
3. Kliknite na položku **Centrum zabezpečenia/ Centrum dôveryhodnosti** a potom kliknite na položku **Nastavenia centra zabezpečenia/ Nastavenia centra dôveryhodnosti**.
4. V okne **Centrum zabezpečenia/ Centrum dôveryhodnosti** kliknite na položku **Nastavenia makra**.
5. Vyberte požadované nastavenie.
6. Kliknite na tlačidlo **OK**.



Obrázok 15: Centrum dôveryhodnosti – nastavenie makra (operačný systém Windows)
Zdroj: Snímka obrazovky

Postup pre operačné systémy macOS:

1. Kliknite na ponuku **Word**, **Excel** alebo **PowerPoint** v ľavom hornom rohu, podľa potreby.
2. Kliknite na položku **Predvoľby** alebo použite skratku *command* + , .
3. Kliknite na položku **Zabezpečenie**.
4. Vyberte požadované nastavenie.



Obrázok 16: Centrum dôveryhodnosti - nastavenie makra (opračný systém macOS)
Zdroj: Snímka obrazovky

Microsoft Office pre operačné systémy Windows má funkcionalitu navyše v podobe *Zakázať všetky makrá okrem digitálne podpísaných makier*. Podľa vendora sú makrá zakázané, ale v prítomnosti makra sa zobrazí upozornenie zabezpečenia. Ak je však makro digitálne podpísané dôveryhodným vydavateľom, môže sa spustiť, ak bol vydavateľ zaradený medzi dôveryhodných vydavateľov. Ak nebol vydavateľ zaradený medzi dôveryhodných vydavateľov, zobrazí sa upozornenie, na základe ktorého môžete povoliť podpísané makro a zaradiť vydavateľa medzi dôveryhodných. Tento variant funkcionality môže byť prácnejším, ale v konečnom dôsledku môže byť najbezpečnejším. Odporučil by som minimálne zváženie tejto možnosti.

Ďalším bezpečnostným odporúčaním a opatrením zároveň je používanie antivírusového softwaru. To zabezpečí zákaz spustenia nebezpečných webových stránok a aplikácií. Takisto bude slúžiť ako nástroj, ktorý bude chrániť systém v dobe, kedy nebudú k dispozícii iné bezpečnostné aktualizácie. Dbajte na to, aby bol takisto aj tento software vždy aktualizovaný a platený.

Pravidelne zálohujte dôležité a citlivé dáta a informácie. Používajte metódu 3-2-1 pre svoje najdôležitejšie údaje. Táto metóda znamená, aby ste mali vytvorené 3 zálohy svojich dát na dvoch rôznych typoch úložísk a najmenej na jednom samostatnom externom úložisku, mimo pracoviska spoločnosti, kde je rovnako potrebné mať zabezpečenú zmluvnú zodpovednosť spoločnosti za zálohy. Pravidelne kontrolujte stav,

funkčnosť a konzistenciu vašich záloh a možnosť obnovenia ich dát. Je to najúčinnejšia prevencia nie len proti ransomware útoku.

Vykonávajte kontrolu prenosných médií, do ktorej zahrniete zoznam povolených zariadení, ich šifrovanie, skladovanie, mazanie a likvidáciu.

Pokúste o zavedenie viacfaktorovej autentifikácia pre vyššie úrovne oprávnení alebo tam, kde hrozí únik citlivých informácií. Môže sa jednať o e-mailovú aplikáciu, vzdialený prístup apod. Viacfaktorová autentifikácia pridáva ďalšiu vrstvu ochrany tým, že vyžaduje, aby užívateľ poskytol bezpečnostný token, ako napríklad kód prijatý notifikáciou alebo biometrické overenie.

V prípade klientskych staníc (Workstation) a serverov (Server) s operačnými systémami Windows, ktoré nevyžadujú vzdialený prístup a Server Message Block (SMB), môžete zastaviť túto službu, aby ste zabránili vzdialeným pripojeniam zo škodlivých alebo kompromitovaných zariadení (pre prichádzajúce spojenia). Je to možné vykonať manuálne pomocou modulu „Services“ (Services.msc), pomocou PowerShell Set-Service cmdlet alebo pomocou preferencie skupinovej politiky. Po zastavení a zakázaní týchto služieb, SMB už nebude môcť nadviazať odchádzajúce spojenie alebo prijímať prichádzajúce pripojenie.

Preto nesmiete zakázať službu Server na radičoch domény alebo na súborových serveroch. Žiadny klient by následne nemohol uplatňovať skupinovú politiku, ani by sa nemohol pripojiť k svojím údajom. Je možné však obmedziť prístup k nim z dôveryhodných rozsahov IP adries a zariadení. Rovnako by mali byť obmedzené na profily doménových alebo súkromných brán firewall a nemali by povoliť prenos hosť/verejnosť. Službu Workstation nesmiete zakázať na počítačoch, ktoré sú členmi domény Active Directory, pretože nebudú môcť naďalej uplatňovať skupinovú politiku.

Podobné opatrenia a odporúčania, ako pre SMB, platia aj pre Remote Desktop Protocol (RDP). Pokým nie je vzdialene prístupný RDP absolútne nevyhnutným protokolom na používanie, nepoužívajte ho. V posledných rokoch sa ukázal ako jedným z hlavných zo vstupných vektorov pre útoky rodiny ransomwaru Ryuk. Ak však úplne spoliehate na tento protokol, existuje zopár možností, ktorými ho lepšie zabezpečiť.

Prvým odporúčaním je používanie tohoto protokolu spoločne s VPN. Aj s komplexnou politikou hesiel a viacfaktorovou autentifikáciou môžete byť zraniteľní voči hrozbe

odmietnutiu služby (Denial of Service) alebo uzamknutiu používateľského účtu, z dôvodu, že RDP je otvorenou službou. Viac o VPN nájdete popísané v podčasti *Pre sieťovú infraštuktúru*. Avšak nezabúdajte ani na používanie komplexných hesiel, ani na používanie viacfaktorovej autentifikácie.

Používajte heslá, ktoré obsahujú aspoň 8 znakov, z ktorých aspoň jedným je písmeno abecedy, malé aj veľké, číslo a znamienka interpunkcie alebo iné znaky dokopy.

Odporúčané je aj obmedzenie alebo blokovanie používateľov a IP adries s veľkým počtom neúspešných pokusov o prihlásenie. Častokrát je to znak útokov „hrubou silou". Každý neúspešný pokus o prihlásenie je zaznamenaný pod *Windows Event ID 4625*. Prihlasovanie RDP spadá pod prihlasovací typ 10. Následne hranicu blokovania účtu, počet neúspešných pokusov, je možné určiť v lokálnej skupinovej politike v nastaveniach *Politiky účtu (Account Policies)*. Následne je dôležité logovať ako neúspešné, tak aj úspešné prihlásenia. Potrebné je takisto povoliť špecifickú bezpečnostnú vrstvu pre pripojenia RDP. Ak tak neurobíte, nebudete schopní povedať, že pokus o prihlásenie prešiel cez protokol RDP alebo nebude možné vidieť zdrojovú IP adresu.

Ďalším dôležitým odporúčaním je obmedzenie používateľov, ktorí sa môžu prihlásiť pomocou RDP protokolu. Vzdialený prístup by mal byť obmedzený len pre účty, ktoré ho vyžadujú. Je potrebné mať na pamäti, že všetky správcovské účty môžu predvolene používať RDP. Je vhodné usilovať sa o maximálne jeden účet lokálneho správcu, ktorý bude primerane zabezpečený. Dôvodom je, že po získaní prístupu útočníkom do systému, lokálne administrátorské účty poskytujú vektor útoku. Preto je potrebné sa uistiť, že lokálne tieto účty sú jedinečné. To znamená, že lokálne administrátorské účty sa nesmú zhodovať z účtami v iných systémoch v serverovej internej sieti. Vendor Microsoft riešenie v podobe *Local Administrator Password Solution (LAPS)*, ktoré slúži na centrálnu správu jedinečných poverení lokálneho správcu.

V neposlednej rade si je potrebné dať pozor na účty skupiny správcov domén. Tieto účty patria do administrátorskej skupiny pre všetky radiče domény, pracovné stanice a členské servery domény. Pokiaľ by bolo poverenie pre účet správcu domény získané zo servera RDP, útočník by mal úplnú kontrolu nad celou doménou. Preto by mal byť znížený, rovnako ako počet lokálnych správcov, aj počet správcov domén. Takisto je potrebné

vyhnúť sa prístupu k serveru RDP alebo iným externe exponovaným systémom prostredníctvom týchto účtov, aby sa predišlo neúmyselnému sprístupneniu poverení pre tento typ účtu.

Posledným odporúčaním je šifrovanie. RDP podporuje štyri úrovne šifrovania, ktoré sú nakonfigurované na serveri vzdialenej plochy (Remote Desktop): nízka, kompatibilná s klientom, vysoká a kompatibilná s FIPS (Federal Information Processing Standards). Je to možné ďalej vylepšiť použitím rozšírenej RDP bezpečnosti, ktorá poskytuje šifrovanie a autentifikáciu servera implementovanými externými bezpečnostnými protokolmi, ako napr. TLS.

3.2.4 Pre ransomware Ryuk

V tejto podčasti sa nachádzajú odporúčania a opatrenia pre ransomware Ryuk, vrátane malwaru Emotet a TrickBot, ktoré sú dôležitou súčasťou celého procesu infikovania systému / podnikovej siete týmto ransomwarom. V tejto časti sa budú nachádzať informácie, ktoré už možno boli zmienené v predošlom texte, ale je potrebné dať tieto informácie pod jednu časť.

Na úvod začneme preventívnymi opatreniami pre ransomware Ryuk. Prvým a zaiste veľmi dôležitým opatrením je vykonávanie pravidelného zálohovania systému a jeho častí. Aplikujte metódu 3-2-1, ktorou majú byť vytvorené 3 zálohy dát na dvoch rôznych typoch úložísk a najmenej na jednom samostatnom externom úložisku, mimo pracoviska spoločnosti. Viacero iterácií záloh vám pomôže pri obnove záloh, keďže hrozí, že niektoré vaše zálohy budú obsahovať infikované súbory alebo budú šifrované. Pravidelne kontrolujte stav, funkčnosť, integritu a konzistenciu vašich záloh a možnosť obnovenia ich dát. Je to najúčinnejšia prevencia nie len proti ransomware útoku.

Ďalšími dôležitými krokmi opatrení sú včasné a časté aktualizovanie všetkých operačných systémov, aplikácií a iného softwaru, vrátane antivírusového softwaru, aby bolo zmiernené potencionálne zneužitie zraniteľností útočníkmi. Pred aplikovaním je vhodné testovanie týchto aktualizácií. Je potrebné vykonávať segmentáciu siete a používať kontroly prístupu medzi jednotlivými segmentami. Viac o segmentácií siete nájdete v podkapitole odporúčaní a opatrení *Pre sieťovú infraštruktúru*. V rámci sieťovej infraštruktúry a aktívnych prvkov využívajte tzv. whitelist. Jedná sa o povolenie len

žiadúcich užívateľov, služieb, autorizovaného softwaru a štandardnej prevádzky. Všetky položky, mimo whitelist, budú blokované. Pokúste sa prevádzkovanie užívateľskej politiky, ktorá bude zahŕňať čo najviac obmedzený prístup používateľov k systému a teda čo najmenšie privilégiá. Zároveň zaistite, aby používatelia dodržiavali politiku hesiel, v ktorej bude zahrnuté vytvorenie komplexných hesiel a obsah ich znakov, pravidelná zmena hesiel alebo uschovávanie hesiel. Obmedzte aj administrátorské poverenia na čo najmenší počet.

Veľké množstvo počiatočných infikovaní sa dostáva do systémov a počítačových sietí cez škodlivé e-mailové prílohy, dokumenty alebo odkazy na stránky. Preto je potrebné zabezpečiť e-mailovú komunikáciu ako po systémovej stránke, tak aj po užívateľskej stránke. Systémová stránka zabezpečenia e-mailovej komunikácie by mala poskytnúť filtrovanie a blokovanie e-mailov na základe určitých identifikátorov. Týmito identifikátormi sú nežiadúce typy súborov v prílohách e-mailov, nadmerná dátová veľkosť týchto príloh, nežiadúce kľúčové slová v obsahu správ, podozrivé e-mailové a IP adresy a iné. Všetky podozrivé e-maily by mali byť blokované, umiestnené do karantény a automaticky oznamované IT bezpečnostnému oddeleniu spoločnosti. V rámci užívateľskej stránky zabezpečenia e-mailovej komunikácie, dbajte na školenie zamestnancov. Naučte ich rozoznávať podozrivé e-maily, e-mailové adresy a odkazy na stránky a prízvukujte im, aby v prípade neistoty kontaktovali IT bezpečnostné oddelenie. Používatelia by mali mať povedomie o bezpečnostných rizikách spojených s e-mailovou komunikáciou, phishingových e-mailov a sociálneho inžinierstva.

Rovnako je potrebné dať pozor na vzdialený prístup používateľov. Ako už bolo pár krát v práci zmienené, používajte VPN pre vzdialené pripojenie sa k sieti, respektíve k určitému zariadeniu. Pokým používateľ nepotrebuje vzdialený prístup, zamedzte tejto možnosti. Takéto obmedzenie je vhodné aplikovať aj pre Remote Desktop Protocol (RDP, predvolený port 3389) a Server Message Block (SMB, predvolený port 445). Pokiaľ to nie je nevyhnutné, uzavrite tieto porty a obmedzte používanie týchto služieb. Viac informácií o obmedzení týchto služieb nájdete v časti *Pre servery a klientske stanice a ich software*. Zaveďte centrálne zaznamenávanie logov sieťových udalostí a ich automatické vyhodnocovanie. O tejto problematike je písané viac v časti *Pre sieťovú infraštruktúru*.

Čo robiť po identifikovaní infekcie ransomwarom Ryuk? Pokiaľ dodržíte aspoň opatrenie zálohovania a jeho zabezpečenia, tak máte napoly vyhrané. Ransomware od vás bude pýtať výkupné na dešifrovanie údajov, neodporúča sa platiť ho, pretože nemáte istotu, že údaje budú naozaj dešifrované a častokrát obnova zo záloh alebo aj kúpa nových komponentov vyjde ekonomicky výhodnejšie. Prvým krokom je izolovanie infikovaného systému. Vypnite a odpojte všetky sieťové zariadenia, koncové počítačové stanice a iné potencionálne napadnuté zariadenia. Prepnite sieť do režimu offline. Pokiaľ je to možné, umiestnite napadnuté komponenty na jedno miesto a označte, že sa jedná o zašifrované zariadenia. Následne skontrolujte vaše zálohované údaje pomocou antivírového programu, ak je to možné. Zaistíte tým, že vo vašich zálohách sa nenachádza malware.

V ďalších krokoch resetujte a zmeňte všetky heslá lokálnych a doménových správcovských účtov a heslá k jednotlivých účtom a aplikáciám. Pre opätovné zostavenie systému, využite nové inštalácie alebo overené a bezpečné zálohy. Pri nových inštaláciách a nasadeniach, zmeňte predvolené nastavenia.

Následne prejdite na investigatívnu činnosť za pomoci odborníkov a pokúste sa identifikovať zdroj infekcie a vektor útoku.

3.2.5 Pre malware Emotet a Trickbot

Malware Emotet býva častokrát prvým krokom k úplnému infikovaniu ransomwaru Ryuk. Infikovanie nastáva po otvorení alebo kliknutí na škodlivý odkaz na stiahnutie, PDF alebo Microsoft Word dokument so škodlivými makrami. Následne sa Emotet šíri počítačovou sieťou a sťahuje do infikovaných systémov iný malware, častokrát TrickBot. V tejto podčasti sa nachádzajú odporúčania a opatrenia pre predídenie infikovania týmto malwarom.

Na úvod sú to opatrenia, ktoré boli v práci spomenuté a preto budú zmienené len stručne. Jedná sa o včasné a časté aktualizovanie všetkých operačných systémov, aplikácií a iného softwaru, vrátane antivírusového softwaru, aby bolo zmiernené potencionálne zneužitie zraniteľností útočníkmi. Pred aplikovaním je vhodné testovanie týchto aktualizácií. Zabezpečte čo najviac obmedzený prístup a zároveň čo najmenšie privilégiá používateľov k systému. Rovnako obmedzte aj administrátorské poverenia len na určených správcov.

Keďže malware Emotet infikuje systém častokrát cez e-mailovú komunikáciu, dbajte na opatrenia, ktoré boli vymenované v predošlej časti, ako aj v časti *Pre e-mailovú komunikáciu*. K týmto odporúčaniam a opatreniam by som dodal označenie externých e-mailov pre následnú kontrolu odosielateľa. V rámci blokovaných e-mailových príloh dajte pozor hlavne na prípony súborov .exe, .doc, .docx, .pdf, .xls, .xlsx, .vbs, .scr, .rtf a .zip. V prípade neistoty používateľa, odporučte kontaktovanie IT bezpečnostného oddelenia. V rámci školenia užívateľov im prízvukujte, aby svoje citlivé údaje, používateľské mená a heslá nezverejňovali online alebo ich neposkytovali ako odpoveď na nevyžiadanú žiadosť. Takisto je potrebné, aby používatelia pred kliknutím na odkaz umiestnili kurzor myši na odkaz a overili cieľ. Zvážte implementáciu mechanizmu DMARC, o ktorom nájdete viac detailov v časti *Pre e-mailovú komunikáciu*.

Obmedzte prichádzajúcu komunikáciu použitím objektov skupinovej politiky nastavených na bráne firewallu. Štruktúra objektov skupinovej politiky je nasledovná:

- cesta k súborovému systému počítača,
- cesta k adresárovej službe počítača,
- cesta k systému súborov používateľa,
- cesta k adresárovej službe používateľa.

Malware TrickBot býva častokrát stiahnutý do systému malwarom Emotet. Funkcia TrickBotu je zbieranie citlivých údajov zo siete obete a napomáha monitorovaniu cieľovej siete útočníkmi. Niektoré moduly malwaru TrickBot zneužívajú SMB protokol na šírenie škodlivého softwaru po sieti obete. Odporúčania a opatrenia na vykonanie prevencie zabezpečenia sú pre tento malware takmer identické ako pre malware Emotet. Zabezpečenie e-mailovej komunikácie je možno doplniť o implementáciu štandardov SPF (Sender Policy Framework) a DKIM (DomainKeys Identified Mail). Tieto štandardy slúžia na kontrolu a blokovanie prichádzajúcej a odchádzajúcej komunikácie. Jedná sa o autentifikačné metódy určené na zisťovanie falošných adries odosielateľov.

V rámci protokolu SMB, zakážte používanie SMBv1 a miesto toho využívajte SMBv2 alebo SMBv3, pre vylepšenie služieb proti šíreniu modulov po sieti, ktoré používa TrickBot.

ZÁVER

Hlavným cieľom práce bolo analyzovanie informačných a kybernetických hrozieb za určité časové obdobie, v tomto prípade to bol rok 2019. Na základe vykonaných analýz boli následne vytvorené predikcie a preventívne opatrenia na nasledujúci rok. Táto problematika je prebraná v celom obsahu práce pozostávajúcom s troch hlavných kapitol.

Úvod práce bol venovaný spracovaniu teoretických východísk, ktoré poslúžili na porozumenie danej problematiky. V tejto kapitole boli preberané základné pojmy, od ktorých sa ďalej odvíjalo spracovanie teórie o bezpečnostných hrozbách, typoch kybernetických útokov a typoch útočníkov.

Na teoretický základ pre celú prácu nadviazala analýza súčasného stavu. Už ako cieľ diplomovej práce naznačuje, táto kapitola je pre celú prácu veľmi dôležitá. Analýza súčasného stavu pozostávala z troch hlavných častí. Cieľom analýz bolo získať užitočné sumárne informácie o existujúcich hrozbách, zraniteľnostiach a typoch útokov. Výsledné informácie boli primárne zamerané na malé až veľké spoločnosti pôsobiace na území Českej republiky, doplnené globálnymi informáciami. Prvou časťou bolo analyzovanie reportov z portálu ThreatGuard. V tejto časti bola popísaná samotná služba a jej cieľ, ako aj selekcia a spracovanie údajov v tejto službe či popis vedľajších činností vykonávaných pri spracovávaní údajov. Samotná analýza reportov bola rozdelená do ďalších 6 častí, podľa typu analyzovanej kategórie.

Druhou časťou analytickej časti bola analýza reportov spoločnosti Kaspersky. Touto analýzou bolo docielené rozšírenie spektra zákazníkov od malých až po veľké, svetové spoločnosti. Takisto bolo dosiahnuté určite globalizácie, ktorá je spojená s potencionálnymi hrozbami, ktoré netreba vylúčiť od českých spoločností.

Tretia časť analýzy slúži pre doplnenie a rozšíreniu pohľadu na danú problematiku. Jej obsahom sú spracované najzávažnejšie mediálne správy roku 2019, týkajúce sa kybernetických útokov, ktoré sa objavili v českých médiách a zasiahli Českú republiku. Zmienené boli kybernetické útoky na nemocnicu v Benešove a Ostravsko-karvinské doly, ktorých spoločným znakom bolo pôsobenie útoku ransomware.

Posledná hlavná kapitola, *Vlastný návrh riešenia*, nadväzovala priamo na analýzu súčasného stavu. Na základe analýzy boli vytvorené predikcie a opatrenia spoločne

s odporúčaniami pre spoločnosti na nasledujúci rok. Predikcie boli vytvorené ako na základe analytickej časti práce, tak aj na základe spracovania iných zdrojov, v ktorých odborníci predikujú rok 2020 v oblasti informačných a kybernetických hrozieb a ktoré boli selektované pre účely tejto práce. V druhej časti vlastného návrhu riešenia boli vytvorené opatrenia a odporúčania, ktoré boli rozdelené podľa vybraných častí firemnej infraštruktúry, ktoré vecne nadväzovali na predošlé kapitoly diplomovej práce.

Vďaka jednotlivým kapitolám tejto diplomovej práce dostane čitateľ ucelený pohľad na danú problematiku a rovnako užitočné rady ohľadom informačnej a kybernetickej bezpečnosti pre rok 2020.

ZOZNAM POUŽITÝCH ZDROJOV

[1] ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice*. 1. vydání. Brno: Akademické nakladatelství CERM, 2013. ISBN 978-80-7204-872-4.

[2] POŽÁR, Josef a kolektiv. *Základy teorie informační bezpečnosti*. 1. vydání. Praha: Vydavatelství PA ČR, 2007. ISBN 978-80-7251-250-8.

[3] ISO/IEC 27000. *Information technology – Security techniques – Information security management systems – Overview and vocabulary*. 5. vydanie. Švajčiarsko: Medzinárodná organizácia pre normalizáciu, 2018.

[4] DOUCEK, Petr. *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM.* 2. rozšířené vydání. Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.

[5] MILLER, L. *Ochrana údajov pre malé a stredné firmy* [online]. ESET, spol. s r.o. 2017. ISBN 978-80-570-1006-7. Dostupné z: https://www.eset.com/sk/firemna-it-bezpecnost/ochrana-udajov-pre-firmy-ekniha-zadarmo/

[6] NIST. *National vulnerability database* [online]. Gaithersburg: National Institute of Standards and Technology 2020 [cit. 2020-04-20]. Dostupné z: https://nvd.nist.gov

[7] LÉVY-BENCHETON, C., L. MARINOS, R. MATTIOLI, T. KING, CH. DIETZEL and J. STUMPF. *Threat Landscape and Good Practice Guide for Internet Infrastructure* [online]. ENISA. 2015. ISBN 978-92-9204-098-7. Dostupné z: https://www.enisa.europa.eu/publications/iitl

[8] JIRÁSEK, Petr, Luděk NOVÁK, Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti – Cyber Security Glossary*. 3. aktualizované vydání. Praha: Policejní akademie ČR v Praze a Česká pobočka AFCEA pod záštitou Národního centra kybernetické bezpečnosti České republiky, Národního bezpečnostního úřadu České republiky., 2015. Dostupné taktiež z: https://www.govcert.cz/download/aktuality/container-nodeid-665/slovnikkb-cz-en-1505.pdf

[9] MARTIN, A.D., L. MARINOS, E. REKLEITIS, G. SPANOUDAKIS, N. PETROULAKIS. *Threat Landscape and Good Practice Guide for Sotware Defined Networks/5G* [online]. ENISA. 2015. ISBN 978-92-9204-161-8. Dostupné z: https://www.enisa.europa.eu/publications/sdn-threat-landscape

[10] SEDLÁK, Petr. *Management informační bezpečnosti – Úvod a základní pojmy*. Brno, 2019.

[11] NISTIR 7298. *Glossary of Key Information Security Terms*. 2. revízia. Gaithersburg: National Institute of Standards and Technology, 2013.

[12] SEDLÁK, Petr. *Kybernetická bezpečnost – Obecně*. Brno, 2019.

[13] ONDRÁK, Viktor. *Bezpečnostní hrozby*. 2017.

[14] TECHOPEDIA. *Techopedia* [online]. © 2020 [cit. 2020-04-20]. Dostupné z: https://www.techopedia.com

[15] PIPER S. *Definitive Guide to Advanced Threat Protection – Defeating Your Cyber Enemies With Unified Advanced Threat Protection Defenses* [online]. CyberEdge Group, LLC. 2014. ISBN 978-0-9888233-7-2. Dostupné z: https://cyber-edge.com/wp-content/uploads/2016/08/Definitive-Guide-to-ATP.pdf

[16] MALWAREBYTES. *Malwarebytes* [online]. © 2020 [cit. 2020-04-22]. Dostupné z: https://www.malwarebytes.com

[17] CISCO. *Cisco* [online]. 2020 [cit. 2020-04-22]. Dostupné z: https://tools.cisco.com/security/center/resources/virus_differences

[18] KASPERSKY. *Encyclopedia by Kaspersky* [online]. © 2020 [cit. 2020-04-25]. Dostupné z: https://encyclopedia.kaspersky.com

[19] STUTTARD Dafydd and Marcus PINTO. *The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, Second Edition* [online]. 2. edícia. Indianapolis: Wiley Publishing, Inc., 2011. ISBN 978-1-118-02647-2.

[20] OWASP. *Owasp* [online]. © 2020 [cit. 2020-04-25]. Dostupné z: https://owasp.org

[21] MITRE. *Common Weakness Enumeration* [online]. © 2006-2020 [cit. 2020-04-30]. Dostupné z: https://cwe.mitre.org

[22] MITRE. *Att&ck* [online]. © 2015-2020 [cit. 2020-04-30]. Dostupné z: https://attack.mitre.org

[23] SEDLÁK, Petr. *Bezpečnost informací – Fenomén Hacking*. Brno, 2019.

[24] COMGUARD. *COMGUARD* [online]. © 2020 [cit. 2020-04-30]. Dostupné z: https://www.COMGUARD.cz

[25] COMGUARD. *ThreatGuard* [online]. 2020 [cit. 2020-04-30]. Dostupné z: https://portal.threatguard.cz

[26] FIRST. *First: Improving Security Together* [online]. © 1995-2020 [cit. 2020-05-01]. Dostupné z: https://www.first.org

[27] KASPERSKY. *Securelist* [online]. © 2020 [cit. 2020-05-01]. Dostupné z: https://securelist.com

[28] NCKB. *Národní centrum kybernetické bezpečnosti* [online]. 2020 [cit. 2020-05-01]. Dostupné z: https://www.govcert.cz

[29] CISA. *Cybersecurity and infrastructure security agency* [online]. 2020 [cit. 2020-05-01]. Dostupné z: https://www.us-cert.gov

[30] CYBEREASON. *Cybereason* [online]. © 2019 [cit. 2020-03-28]. Dostupné z: https://www.cybereason.com

[31] *Odbor statistik rozvoje společnosti. Využívání informačních a komunikačních technologií v podnikatelském sektoru: za rok 2019* [online]. Praha: Český statistický úřad. 2020. ISBN 978-80-250-2967-1. Dostupné z: https://www.czso.cz/documents/10180/90577049/06200519.pdf/1e5277d9-f01c-456f-a182-9e6fd68e7317?version=1.0

ZOZNAM POUŽITÝCH OBRÁZKOV

ZOZNAM POUŽITÝCH TABULIEK

ZOZNAM POUŽITÝCH GRAFOV