Kybernetická bezpečnost v subjektu veřejné správy

Bc. Barbora Bačáková

Diplomová práce
2022

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav ochrany obyvatelstva

Akademický rok: 2021/2022

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Barbora Bačáková**
Osobní číslo:	**L20186**
Studijní program:	**N1032A020002 Bezpečnost společnosti**
Specializace:	**Ochrana obyvatelstva**
Forma studia:	**Kombinovaná**
Téma práce:	**Kybernetická bezpečnost v subjektu veřejné správy**

Zásady pro vypracování

1. Zpracujte literární rešerši vztahující se k dané problematice.
2. Zvolte subjekt veřejné správy vhodný pro posouzení kybernetické bezpečnosti.
3. Proveďte analýzu úrovně kybernetické bezpečnosti vybraného subjektu veřejné správy.
4. Navrhněte případná opatření ke zvýšení úrovně kybernetické bezpečnosti vybraného subjektu veřejné správy.

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

Seznam doporučené literatury:

1. DOUCEK, Petr, Martin KONEČNÝ a Luděk NOVÁK. *Řízení kybernetické bezpečnosti a bezpečnosti informací.* Praha: Professional Publishing, 2019. ISBN 978-80-88260-39-4.
2. FAGEL, Michael J. a Jennifer L. HESTERMAN, ed. *Soft targets and crisis management: what emergency planners and security professionals need to know.* Boca Raton: Press, Taylor & Francis Group, 2017. ISBN 9781498756327.
3. KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity.* Praha: CZ.NIC, z.s.p.o. CZ.NIC, 2019 ISBN 978-80-88168-31-7.

Další odborná literatura dle doporučení vedoucího diplomové práce.

Vedoucí diplomové práce: **Ing. Petr Svoboda, Ph.D.**
Ústav ochrany obyvatelstva

Datum zadání diplomové práce: **1. prosince 2021**
Termín odevzdání diplomové práce: **6. května 2022**

L.S.

doc. Ing. Zuzana Tučková, Ph.D.
děkanka

prof. Ing. Dušan Vičar, CSc.
ředitel ústavu

V Uherském Hradišti dne 1. prosince 2021

PROHLÁŠENÍ AUTORA
DIPLOMOVÉ PRÁCE

Beru na vědomí, že:

- diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

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

V Uherském Hradišti, dne: 5. 8. 2022

Jméno a příjmení studenta: Bc. Barbora Bačáková

.....
podpis studenta

ABSTRAKT

Diplomová práce se věnuje problematice kybernetické bezpečnosti v subjektu veřejné správy. V teoretické části práce jsou uvedena základní teoretická východiska řešené problematiky a vybrané koncepční dokumenty.

Praktická část se zabývá veřejnou správou vybraného sektoru, identifikací rizik a následnou analýzou stavu kybernetické bezpečnosti za pomoci dotazníkového šetření a metody FMEA. V závěru práce jsou na základě zjištěných informací navržena příslušná opatření pro zlepšení současného stavu.

Klíčová slova: Kybernetická bezpečnost, Kybernetické hrozby, malware, veřejná správa.

ABSTRACT

This diploma thesis is devoted to the issue of cyber security in public administration. The goal of the thesis is to provide an up-to-date picture of cyber security in the public administration environment of the selected company.
In the theoretical part, the diploma thesis describes literary sources and summarizes the range of issues for the understanding of the reader. The practical part contains the public administration of the selected sector, it deals with the identification of risks and the subsequent analysis of the state of cyber security using FMEA methods and a questionnaire survey. Based on the information found, it proposes appropriate measures.

Keywords: Cybersecurity, Cybersecurity threats, malware, Public Administration.

Chtěla bych tímto poděkovat panu Ing. Petrovi Svobodovi Ph.D. za ochotu vést tuto diplomovou práci, za vstřícný přístup, cenné rady a pomoc během jejího zpracování.

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

OBSAH

ÚVOD **9**
I TEORETICKÁ ČÁST **11**
1 CÍLE A METODY **12**
2 KONCEPČNÍ DOKUMENTY **13**
2.1 Základní pojmy 13
2.2 Základní koncepční dokumenty 13
3 ZÁKLADNÍ POJMY **15**
4 KYBERNETICKÁ BEZPEČNOST **21**
4.1 Klasifikace z hlediska kybernetické bezpečnosti 21
4.2 Principy kybernetické bezpečnosti 25
4.2.1 Triáda CIA 25
4.2.2 Prvky kybernetické bezpečnosti 34
4.2.3 Životní cyklus kybernetické bezpečnosti 37
5 TYPY ÚTOKŮ **38**
5.1 Hrozby kybernetických útoků 39
5.2 Malware 40
5.2.1 Dělení z hlediska účinků 40
5.2.2 Dělení z hlediska způsobů šíření 42
5.3 Kybernetické útoky 44
5.3.1 Phishing 44
5.3.2 Pharming 45
5.3.3 Cross-sitte scripting 45
5.4 Statistika penetrace malwaru v České republice 46
II PRAKTICKÁ ČÁST **48**
6 POPIS VEŘEJNÉ SPRÁVY **49**
7 ANALÝZA BEZPEČNOSTI SUBJEKTU VEŘEJNÉ SPRÁVY **53**
7.1 Fyzická ochrana 53
7.1.1 Fyzická bezpečnostní kontrola 53
7.1.2 Zabezpečení vnějšího perimetru (linie nemovitosti) 53
7.2 Technické prvky fyzické bezpečnosti 53
7.2.1 Poplachové zabezpečovací a tísňové systémy 54
7.2.2 Systém detekce požáru 55
7.2.3 Přístupové systémy 56
7.2.4 Mechanické zábranné systémy 57
7.3 Zabezpečení pracovních stanic a sítí 59
7.3.1 Ochrana proti malware 59
7.3.2 Zálohování 59

7.3.3 Omezení přístupu k internetu 59
7.3.4 Firmware-aktualizace 59
7.3.5 Školení zaměstnanců 60
7.4 ČÍM JE VEŘEJNÁ SPRÁVA NAPADÁNA 60
8 DOTAZNÍKOVÉ ŠETŘENÍ 62
8.1 NÁVRH OPATŘENÍ 69
9 ANALÝZA RIZIK FAILTURE MODE AND EFFECT ANALYSE (FMEA) 71
9.1 IDENTIFIKACE AKTIV 71
9.1.1 Primární aktiva 72
9.1.2 Podpůrná aktiva 73
9.2 IDENTIFIKACE HROZEB 74
9.2.1 Interní hrozby 74
9.2.2 Externí hrozby 75
9.3 SESTAVENÍ TÝMU 76
9.4 SESTAVENÍ HODNOTÍCÍ STUPNIC 76
9.5 FMEA 79
9.6 VYHODNOCENÍ ANALÝZY 86
9.7 NÁVRH OPATŘENÍ 87
ZÁVĚR 90
SEZNAM POUŽITÉ LITERATURY 92
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK 96
SEZNAM OBRÁZKŮ 97
SEZNAM TABULEK 98
SEZNAM GRAFŮ 99

ÚVOD

Na začátku 60. let lidé viděli velký potenciál v přenosu a sdílení informací mezi různými systémy se zaměřením na vědeckou a vojenskou oblast. S raným technologickým zdokonalením bylo potřeba zabezpečit citlivá data, software a aplikace, což vedlo ke vzniku kybernetické bezpečnosti. Kybernetická bezpečnost je dovedností ochrany systémů, sítí a programů před digitálními útoky. Tyto útoky jsou obvykle zaměřeny na přístup, změnu nebo zničení citlivých informací (vymáhání peněz od uživatelů nebo přerušení běžných obchodních či pracovních procesů). Zavádění účinných opatření v oblasti kybernetické bezpečnosti je dnes obzvláště náročné, protože existuje více zařízení než lidí a útočníci jsou stále inovativnější.

Informační a komunikační technologie jsou dnes využívány skoro ve všech oblastech veřejného i soukromého sektoru. Napadení jejich dosažitelnosti, důvěrnosti či narušení integrity může mít závažné dopady. Zvyšuje se důležitost hodnot kybernetické bezpečnosti, aby byla ochráněna informační a komunikační technologie před jejími zákroky. Bezpečnost je v tomto případě velice důležitá, protože i náklady na porušení kybernetické bezpečnosti rostou. Je třeba vzít v úvahu i nefinanční náklady, jako je poškození pověsti. Nové předpisy a požadavky podávání zpráv činí z dohledu nad riziky kybernetické bezpečnosti problém.

Diplomová práce se zabývá kybernetickou bezpečností v subjektu veřejné správy. Byla vybrána z hlediska aktuálních přibývajících kybernetických útoků v soukromém i veřejném sektoru či v běžném praktickém životě.

Cílem diplomové práce je poskytnutí přehledu o kybernetických hrozbách v kybernetické bezpečnosti a jejich ochrana před útočníky. Přiblížení se s danou problematikou a seznámení člověka, který se o tuto problematiku zajímá. Analýza kybernetických útoku v kybernetické bezpečnosti v prostředí veřejné správy je hlavním tématem. V práci je především zvolen normativní přístup s využitím analýzy, syntézy a komparace.

Práce je rozdělena do dvou částí. Teoretická část nám pomůže, se zorientovat v odborných názvech pomocí vybrané literatury. Zabývá se aspekty kybernetické bezpečnosti jako celku, ale také je zde upřesněn vztah kybernetické bezpečnosti k bezpečnosti informační či ke vztahu kyberprostoru. Praktická část se zabývá konkrétními aspekty právní úpravy kybernetické bezpečnosti v daném subjektu. V hlavní praktické částí práce je analýza bezpečnosti subjektu veřejné správy, kde jsou vymezeny bezpečnostní systémy a identifikace aktiv. Identifikace aktiv je důležitá pro zpracování přesné analýzy, ze kterých

jsou vyhodnocena vhodná opatření. Tyto opatření mají snížit riziko vzniku negativních událostí na minimu. Závěrečná část je věnována návrhu vhodných opatřeních pro daný subjekt.

I. TEORETICKÁ ČÁST

1 CÍLE A METODY

Hlavním cílem práce je analýza kybernetické bezpečnosti vybraného subjektu a navržení opatření na zlepšení současného stavu.
Pro splnění hlavního cíle bude nezbytné splnit dílčí cíle:

- Rešerše související problematiky.
- Provedení dotazníkového šetření pro zjištění současného stavu kybernetické bezpečnosti.
- Provedení analýzy kybernetické bezpečnosti subjektu.
- Návrh opatření pro zvýšení kybernetické bezpečnosti vybraného subjektu.

Aplikované vědecké metody

V práci je použito několik odborných metod. Literární rešerše je v práci uvedena také. K dosažení cíle a dílčích cílů byly využity sesbírané informace odborných pojmů z kybernetické bezpečnosti. Následující další aplikované vědecké metody:

- Analýza – posouzení hrozeb a rizik v subjektu veřejné správy za účelem analýzy a vyhodnocení rizik podle stanoveného stupně. V práci je analýza uvedena v praktické části.
- Deskripce – sběr informací a následné utřídění podle svých potřeb, je využito v praktické části v dotazníkovém šetření.
- Dotazníkové šetření – sesbírání informací a využité pro hodnocení v praktické části.
- Komparace – neboli komparace názorů a hypotéz jedná se o zdůvodnění vlastního názoru, v práci je využita v návrzích a opatřeních.
- Popis – seznámení vybraného subjektu v praktické části.
- Rešerše – přehled odborných literárních či elektronických zdrojů, je využita na začátku práce k přiblížení tématu.
- Syntéza – spojení jednotlivých částí do konečného celku v závěru praktické části.

2 KONCEPČNÍ DOKUMENTY

V této kapitole je zpracovaný soupis odborné literatury k vybranému tématu. Je zde vycházeno ze zdrojů, které jsou určené k porozumění problematice. Výběr koncepčních dokumentů je nesmírně důležitý pro kvalitní zpracování.

2.1 Základní pojmy

Kybernetická bezpečnost je spojována s legislativou a tvoří určité strategické dokumenty. Využívají informace k dosažení očekávaných cílů. V celé práci je vycházeno ze základních koncepčních dokumentů, díky kterým je pak práce zpracována:

- Identifikace problému.
- Vymezení předmětu kybernetické bezpečnosti.
- Základní strategické cíle.
- Rámcový popis implementace kybernetické bezpečnosti.

2.2 Základní koncepční dokumenty

Základní koncepční dokumenty obsahují strategické dokumenty či odborné informace, řešící konkrétní problematiku. Jsou zde vybrány dokumenty, které kladou jasný důraz na dané téma.

Zákon o kybernetické bezpečnosti

Tato kniha, jak již vyplívá z názvu, se zabývá Zákony o kybernetické bezpečnosti. Upravuje práva a povinnosti osob, rovněž upravuje pravomoc a působnost orgánů veřejné moci, a to vše v oblasti kybernetické bezpečnosti.
Hlavním pochopením je ochrana funkčnosti kybernetického prostoru. Jelikož vývoj moderních technologií se stále víc prohlubuje, a tím přibývá závislost společností na informačních systémech, tak tyto předpisy představují naprosto zásadní úpravu. Vydání uvádí uspořádané a přehledné podání základního předpisu s vykonávanými předpisy. (Andraško, 2018)

CyberSecurity

V této knize se dozvíme o problematice kybernetické bezpečnosti. Najdeme zde základní principy, které by každý občan, který používá informační a komunikační technologie, měl uznávat a respektovat. Napomáhá každé osobě, aby si případně obměňovala v dané

souvislosti na činnosti či účelu, za kterým tyto technologie využívá. Současně však kniha zahrnuje i dílčí vysvětlení některých právních norem, které souvisejí s problematikou kybernetické bezpečnosti. Mimo teoretické a právní části má kniha i praktickou část. Praktická část jé spíše určena pro IT odborníky, kde se mohou zabývat a vzdělávat i v problematice kybernetické bezpečnosti.

Tato kniha shrnuje názory a zkušenosti autorů, které získali v oblasti kybernetické bezpečnosti, kybernetické kriminality a vzdělání uživatelů. (Kolouch a Bašta, 2019)

CyberCrime

Autor ve své knize zhodnotil bohaté zkušenosti pedagoga, právníka i odborníka na počítačovou bezpečnost. Věnuje se tedy problematice bezpečnosti. Zabývá se kybernetickými hrozbami se specializací na kybernetickou kriminalitu. Analyzuje kybernetickou kriminalitu z pohledu jednotlivých paragrafů, a umožňuje tak čtenářům, kteří sice znají technické pojmy, ale svět právních klasifikací, paragrafů a odstavců je jim cizí a neorientují se v něm. (Kolouch, 2016)

Soft Targets and Crisis Management

Tato kniha se zabývá vnitřní bezpečnosti a nouzového managementu. Představuje převládající problémy, které dnes ovlivňují společnost vnitřní bezpečnosti. Editoři vytvářejí řád, vedou čtenáře hodnocením rizik, strategiemi a zpevňujícími opatřeními na základě skutečných příkladů, případové studie a aktuální výzkum v praxi. (Fagel a Hesterman, 2017)

3 ZÁKLADNÍ POJMY

Oblast kybernetické bezpečnosti je velmi široké a multidisciplinární téma, proto je důležité si v první kapitole přiblížit výklad některých základních pojmů se kterými bude tato práce pracovat.

Informační společnost

„Informační společnost je charakterizována podstatným využíváním digitálního zpracovávání, uchovávání a přenosu informací. Ze zpracování informací se stává významná ekonomická aktivita, která jednak prostupuje tradičními ekonomickými či společenskými aktivitami a jednak vytváří zcela nové příležitosti a činnosti, které podstatně ovlivňují charakter společnosti.“ (Basl a Blažíček, 2012)

Pro shrnutí definice je zřejmé, že podstatou informační společnosti je informace, její zpracování, uchování a přenos. Dále je patrné, že informační společnost je posilující současnými technologickými vývoji, které jsou založeny na vzájemném propojení informačních, komunikačních a masově-mediálních technologií. Jejím výsledkem je snížení prostorového a časového omezení a zvýšení přístupu k množství veřejných informací. (Basl a Blažíček, 2012)

Jednou z priorit státní informační politiky je s využitím informačních technologií zlepšovat služby poskytované občanům veřejnou správou. Současné informační systémy veřejné správy ulehčují a zdokonalují rozhodovací procesy a umožnují účinnější propojení mezi jednotlivými částmi. Veřejné informace se stávají všestranně dostupné pro občany z veřejných míst i z domova. Veřejná správa byla přepracována tak, aby byla schopna pracovat s novými informačními technologiemi jako nástroji ke zefektivnění vlastní činnosti a k poskytování lepších veřejných služeb občanům a ekonomickým subjektům. Nezávislé informační systémy státní správy jsou vzájemně propojeny do neveřejné sítě státního informačního systému, to znamená, že data jsou do systému zaváděna pouze jednou. (Vláda ČR, 2022)

Státní informační systém musí poskytovat služby i informačním systémům samosprávy. Vytvořil se tak integrovaný informační systém obsahující informační systémy veřejné správy, umožňující oprávněným osobám nezbytné informace a zároveň zajistí bezpečnost osobních dat. K vyřízení správních agend se zřídila integrovaná síť kontaktních míst veřejní správy.

K využití informačních a komunikačních technologií byla veřejná správa přeměněna a stala se tak skutečnou službou občanům a podnikatelské veřejnosti. Na sjednocené informační systémy veřejné správy jsou přes příslušná rozhraní navázány veřejně přístupné služby, ty umožní pomocí počítačových sítí kontaktovat veřejnou správu. Nutností elektronické komunikace mezi občany a veřejnou správou je možné využívání elektronického podpisu a autentizace. Pomocí formulářů lze digitálně vyplnit např. podání daňového přiznání či nejrůznější žádosti, které musí být stvrzeny podpisem. Hovoříme tedy o elektronické správě (e-Government), která nahrazuje komunikaci přes elektronickou poštou (e-mail), a snaží se odstranit byrokracii a přiblížit tak obce i stát občanům. (ISSS, 2004)

Zformulováním vzájemně komunikujících informačních systému veřejné správy, musí být i legislativně podchycen. Data, která obsahují osobní údaje musí být řádně legislativně ale i technicky chráněna proti zneužití. Z tohoto důvodu musí být zajištěn kontrolovaný přístup ke sdíleným údajům a je zřízena veřejnoprávní instituce, která kontroluje dodržování ochrany osobních dat. (ISSS, 2004)

Kyberprostor

Kyberprostor můžeme nazvat jako virtuální svět vytvořený propojením mezi počítači, internetovými zařízeními, servery, routery a dalšími prvky internetové infrastruktury. Na rozdíl od internetu samotného je však kyberprostor místem produkovaným těmito odkazy. Termín kyberprostor poprvé použil americko-kanadský autor William Gibson v roce 1982 v příběhu publikovaném v časopise Omni a poté ve své knize Neuromancer. V tomto sci-fi románu Gibson popsal kyberprostor jako vytvoření počítačové sítě ve světě plném uměle inteligentních bytostí. (Bauwens, 2010)

V populární kultuře 90. let se kyberprostor jako termín bral k popisu „místa“, ve kterém se lidé vzájemně ovlivňovali při používání internetu. Je to místo, kde se odehrávají online hry, chatovací sociálně sítě nebo online komunikace prostřednictvím rychlých zpráv. Kyberprostor se také stal také klíčovým místem pro společenskou a politickou diskusi, přičemž na konci 20. a na počátku 21. století se objevily populární webové diskusní fóra a blogy. Blogy jsou obvykle vytvářeny jednotlivci, kteří zahrnují své osobní sdělení a často nabízejí komentáře a odkazy na další místa na webu, která je podle nich zajímají.

Od vzniku internetu národní vlády a jejich analytici prokázali podstatu jak národních předpisů, tak mezinárodních dohod o charakteru kybernetického prostoru. Čínská vláda

přísně kontroluje, kdo má přístup k internetu a jaký obsah má k dispozici. Vláda USA omezuje některé online aktivity, jako je sdílení digitálních dat, prostřednictvím zákona Digital Millennium Copryricht Act a dalších právních předpisů. Spojené stát navíc vyvinuly strategii pro bezpečnost kybernetického prostoru, aby bylo možné předcházet útokům na internetovou infrastrukturu a reagovat na ně.

Kontrola kybernetického prostoru je tedy důležitá nejen kvůli jednání jednotlivých účastníků, ale také proto, že infrastruktura kybernetického prostoru je nyní zásadní pro fungování národních a mezinárodních bezpečnostních systému, obchodních sítí, tísňových služeb, základních komunikací a dalších veřejných a soukromých aktivit. Jelikož vlády vidí potenciální hrozby pro bezpečnost svých občanů vznikající v kyberprostoru, jednají tak, aby kontrolovaly přístup i obsah. (TZIMOPOULOU, 2006)

Kybernetická bezpečnost

„Kybernetická bezpečnost v posledním desetiletí získala na významu a stala se tak jednou z hlavních priorit v mnoha národních politikách. Je tomu zejména díky přesahu do jiných bezpečnostních sfér a taktéž díky incidentům, které tento pojem nechvalně proslavily a přiměly i širokou veřejnost přemýšlet o potřebě zabezpečení v kyberprostoru. S tím souvisí potřeba chránit kyberprostor tak, aby v nejvyšší možné míře byla zachována komplexní bezpečnost České republiky a zároveň práva jedinců na informační sebeurčení.“ (NUKIB, 2017)

Mnoho lidí si pod pojmem kybernetická bezpečnost představují výhradně oddělní, zabývající se informačními a komunikačními technologiemi. Tato teorie je ovšem mylnou domněnkou, neboť kybernetická bezpečnost se týká každého z nás, kdo využívá jakékoliv prvky ICT ve svém každodenním životě. (Kolouch a Bašta, 2019)

Kybernetickou bezpečnost můžeme tedy definovat několika různorodými způsoby, jelikož nemá vyhrazenou definici. Uznávané definice:

- Kybernetická bezpečnost představuje *„souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru.“* (Jirásek, Novák a Požár, 2015)

- *„Kybernetická bezpečnost představuje souhrn organizačních, politických, právních, technických a vzdělávacích opatření a nástrojů směřujících k zajištění zabezpečeného, chráněného a odolného kyberprostoru v České republice, a to jak pro subjekty veřejného a soukromého sektoru, tak pro širokou českou veřejnost.“* (Govcert, 2015)
- *„Kybernetická bezpečnost představuje soubor opatření, která jsou přijata, aby byl ochráněn počítačový systém před neoprávněným přístupem či útokem*.“ (Kolouch a Bašta, 2019)

Mezi principy kybernetické bezpečnosti se řadí tzv. triády CIA, LTP a PDR. Tato problematika je popsána v samostatné kapitole 4.

Kybernetická kriminalita

Kybernetická kriminalita je poměrně nový mezioborový obor, zaobírají se nezákonnými škodlivými aktivitami v kyberprostoru a může být zaměněn s termíny internetová kriminalita nebo počítačová kriminalita.

Rozdíl mezi těmito pojmy je především v prostředí, ve kterém jsou trestné činy páchány:

- Internetová kriminalita – trestné činy jsou páchány v prostředí internetu.
- Počítačová kriminalita – je páchána v prostředí počítačových systémů.
- Kybernetická kriminalita – jsou činy páchané v protřídí kyberprostoru. (Jirovský, 2007)

V dnešní moderní době se stálé více stává, že lidé sdílí své pocity, fotky, každodenní činnosti nebo soukromý život ze světa reálného do světa kyberprostoru. V současné době tedy dochází k vzestupu kybernetické kriminality mnohem rychleji a častěji, než tomu bylo před pár lety zpět.

Kyberterorismus

Jedná se o předem promyšlený, politický zapříčiněný útok proti informačním systémům, datům a programům. Kyberterorismus si můžeme představit jako terorismus, na rozdíl od klasického terorismu využívá elektronické sítě a informační technologie jako nástroj pro uskutečnění útoku. Hlavní motivací kyberteroristických útoků je poškodit oběti, nejedná se ovšem o fyzickou újmu. Místem kde dochází k činu je kyberprostor, jde o virtuální svět mezi počítači za využití internetu. (Správa sítě, 2016)

Bezpečnost

Slovo bezpečnost je jádrem kybernetické bezpečnosti. Zabezpečení je praxe, která se zabývá všemi aspekty prevence, ochrany a nápravy jakéhokoli typu poškození majetku. Zabezpečení informací je také praxí, jejímž cílem je chránit jakýkoli typ informačních aktiv. Nyní je kybernetická bezpečnost podmnožinou informační bezpečnosti, která se zaměřuje konkrétně na ochranu digitálních informačních aktiv v jejich ekosystému. Jedná se o nejnovější pilíř kybernetické bezpečnosti, kromě jednoho, jehož dopad je potenciálně nejkritičtější. Incidenty kybernetické bezpečnosti by mohly mít za následek zranění, ekologické katastrofy, a dokonce i ztráty na životech. Může se jednat o uživatele připojeného na zdravotnické zařízení, což by mohlo potenciálně vést až k smrtelnému nebezpečí, pokud je toto zařízení hacknuto, nebo může být připojený v autě, letadle či vlaku. (ČESKO, 2016) Koncept bezpečnosti přivádí teorie o kybernetické bezpečnosti čistě technický přístup více zaměřený na lidi. Zeptejme se sami sebe, jak naše rozhodnutí v oblasti kybernetické bezpečnosti přesahují bezpečnost informací a případně zahrnují prevenci fyzického poškození člověka nebo životního prostředí.

Integrita

Integrita je soubor postupů a nástrojů (kontrol) určených k ochraně, udržitelnosti a zajišťovaní přesností, tak úplností údajů pro celý jeho životní cyklus. Integrity dosáhneme provedením implementace digitálních podpisů, zápis-jednou-přečtení-mnoho mechanismus a hašovaní. (Kolouch, 2016)

Hacking

Hacking jsou nazývaný aktivity, které se snaží poškodit digitální zařízení, jako jsou chytré telefony, tablety, televize, počítače či celé sítě. Nejedná se vždy o škodlivý účel. Nyní je mnoho odkazů na hackování a hackery charakterizováno jako nezákonná činnost kyberzločinců. Motivují je finančním ziskem, shromažďování informací – špionáž, nebo jen pro zábavu. (Malwarebytes, 2022)

Hacker

Hacker je osoba s vynikající znalostí informačního systému, počítačového programování nebo technických dovedností. Nemusí se jednat vždy o kyberzločince. Většinou jde o hackera, který proniká do systému za účelem krádeže osobních dat. Nejznámější hackerské techniky:

- Práce se softwarem – nejznámější škodlivý typ softwaru – malware. Patří sem nástroje, které mají zvláštní účel pro hackerovou práci.
- Hardwarová práce – technika phreakingu nebo keyloggeru. Jelikož se může jednat o firemní monitorování zaměstnanců při své práci, není tahle technika trestná.
- Sociální inženýrství – jde o určitý druh psychologické manipulace. Děje se u phishingu nebo pharmingu. (Kolouch, 2016)

Botnet

Botnet je velká skupina zařízení a počítačů připojených k internetu infikovaných malwarem, který ovládá operátor. Útočníci využívají zadní vrátka pro budoucí zneužití. Útočníci využívají tato kompromitovaná zařízení k zahájení rozsáhlých útoků k narušení služeb, krádeži přihlašovacích údajů a získání neoprávněného přístupu ke kritickým systémům. Model příkazů a řízení botnetu umožňuje útočníkovi převzít operace těchto zařízení a ovládat je na dálku. Síla botnetu je v počtu infikovaných strojů, které obsahuje. Útočníci mohou ovládat botnety na dálku a přijímat od nich aktualizace softwaru, pomocí těchto aktualizací rychle změnit své chování. (IT Slovník, 2021)

4 KYBERNETICKÁ BEZPEČNOST

Kybernetická bezpečnost definuje procesy, technologii a design rámce, vyvinuté k ochraně zařízení, programů, dat a dalších organizací. Cenných aktivit před neoprávněným přístupem z kybernetické hrozby.

Tato část je určena k pochopení a poskytnutí základních informací o kybernetické bezpečnosti, klíčové pojmy jako riziko versus zranitelnost a různé rámce kybernetické bezpečnosti, mezi které patří 3 základní triády a ISO norma.

Následně jsou stručně popsány hrozby, aktiva a zranitelnost z pohledu, jak kybernetická bezpečnost chrání data, zařízení, sítě a systémy před útoky virů, malwaru, hackerů a úniku dat. (Clark a Hakim, 2017)
Některé pojmy, které v rámci kybernetické bezpečnosti často slyšíme jsou aktiva, zranitelnost, riziko a ohrožení.

Toto jsou klíčové pojmy, které bychom se měli naučit a znát:

- Aktiva – je to cokoliv v prostředí, které je třeba chránit jako jsou data, lidé, softwarové nástroje a procesy nezbytné pro obchodní operace.
- Zranitelnost – Slabina v organizaci či subjektu, kterou lze zneužít jako chyby v softwarovém kódu a zastaralém softwaru.
- Riziko – Pravděpodobnost nebo možnost, že hrozba úspěšně pronikla do sítí, rizikem by byla celková ztráta aktiva.
- Hrozba – Cokoliv, co se snaží znehodnotit, narušit nebo ukrást váš majetek, je hrozbu. (Ptačka, 2022)

V oblasti ICT je v nynější době Kybernetická bezpečnost pochopením různých subjektů, od obchodních společností až po orgány státní veřejné správy. V současné době se kybernetická bezpečnost týká každého jedince a je neustále v rychlém vývoji.

4.1 Klasifikace z hlediska kybernetické bezpečnosti

Kybernetická bezpečnost je obor složený z velmi různorodých typů rostoucí vědní technologií používaných k ochraně systémů před různými druhy útoků, z nichž některé jsou známé a nějaké neznámé. Vzhledem ke složitosti vyvíjejících se aspektů těchto oblastí tam

není standardní klasifikací ochranných technologií. Klasifikace kybernetiky technologie pomáhá lépe pochopit, jak tyto technologie fungují.

Klasifikace kybernetické bezpečnosti:

V následující podkapitole jsou vysvětleny klasifikace rozdělení z hlediska kybernetické bezpečnosti.

Rozdělení klasifikace z hlediska kybernetické bezpečnosti:

- Aplikovaná kybernetická bezpečnost.
- Věda o kybernetické bezpečnosti.
- Vzdělání a školení v oblasti kybernetické bezpečnosti.
- Kybernetické incidenty.
- Řízení a politika kybernetické bezpečnosti.
- Technologie kybernetické bezpečnosti.
- Lidská a sociální kybernetická bezpečnost.
- Teorie v kybernetické bezpečnosti. (Hassanien a Elhoseny, 2019)

Z praktického hlediska je jeden typ klasifikace běžně založen na druhu hrozeb a jejich zamyšlených účincích. V této kategorií jsou hrozby klasifikovány do dvou skupin:

- Útočné techniky,
- Dopady hrozeb. (Bauwens, 2010)

Další typ klasifikace je založen na typu kybernetické ochrany. Ochranná technologie pak lze rozdělit do čtyř skupin:

- Systém architektury.
- Detekční typ.
- Ekosystém.
- Datový typ. (Hassanien a Elhoseny, 2019)

Technologie kybernetické bezpečnosti lze také klasifikovat na základě komponent, z nichž každá technologie má chránit. Tato klasifikace zahrnuje následující hlavní skupiny:

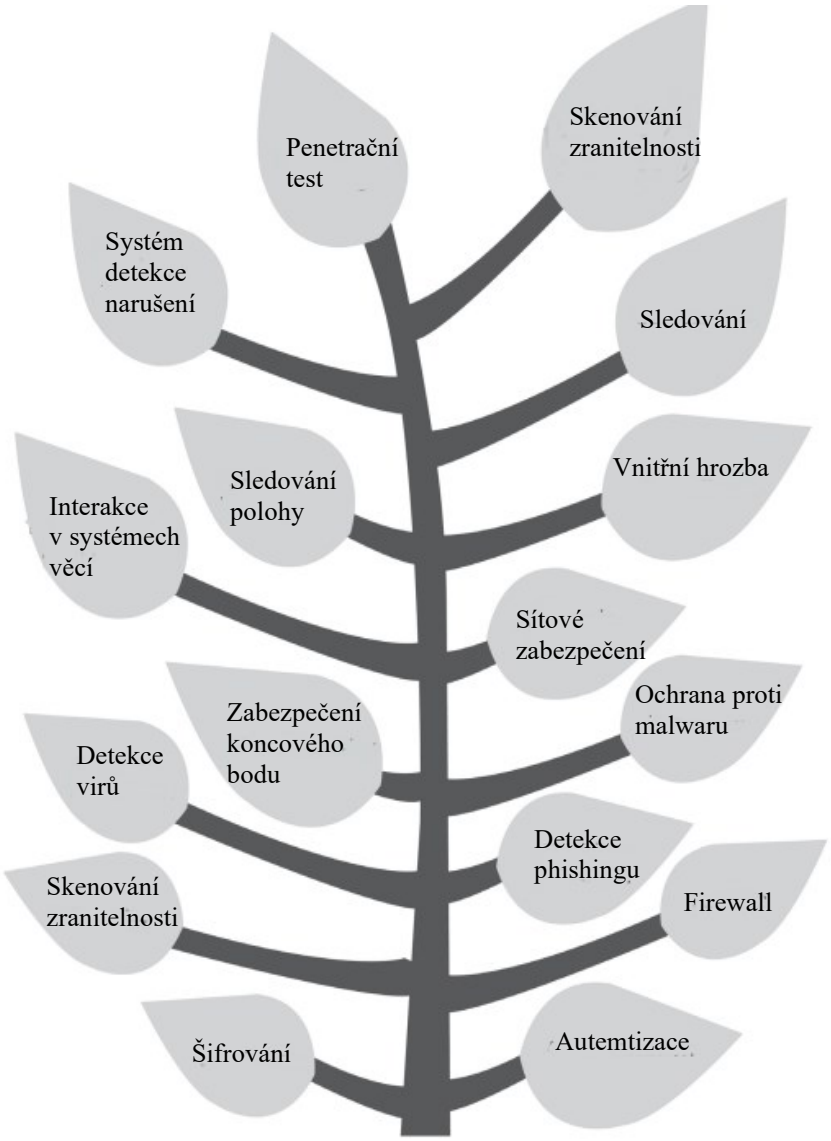
- Síť.
- Aplikace.
- koncový bod.
- Data.
- Identitu.
- Databáze.
- Infrastruktura.
- Mobilní.
- Mrak.
- Záloha. (Hassanien a Elhoseny, 2019)

Na základě řešení klasifikace je další typ založen na empirický způsob klasifikace kybernetických technologií. V této klasifikaci jsou řešení zařazena do následujících skupin:

- Správa identit a přístupu.
- Řízení rizik a dodržování předpisů.
- Šifrování.
- Prevence ztráty dat (DLP).
- Sjednocená správa hrozeb (Unified Threat Management – UTM).
- Firewall.
- Antivirová/antimalwarová řešení.
- Monitorovací systém (Intrusion Detection System – IDS).
- Obnova po havárii.
- Distribuovaný útok (Denial-of-service -DDoS).

- Filtrování webu. (Hassanien a Elhoseny, 2019)

V následující části je zobrazen stromový pohled klasifikace existujících technologických řešení, jsou seskupeny do 16 hlavních kategorií.



Obrázek 1- Klasifikace technologií kybernetické bezpečnosti na základě existujících technologických řešení.

(Zpracování (Hassanien a Elhoseny, 2019)

4.2 Principy kybernetické bezpečnosti

Při uplatňování kybernetické bezpečnosti dochází k implementaci následujících principů, které jsou také nazývány triády kybernetické bezpečnosti. (Hsu a Marinucci, 2013)

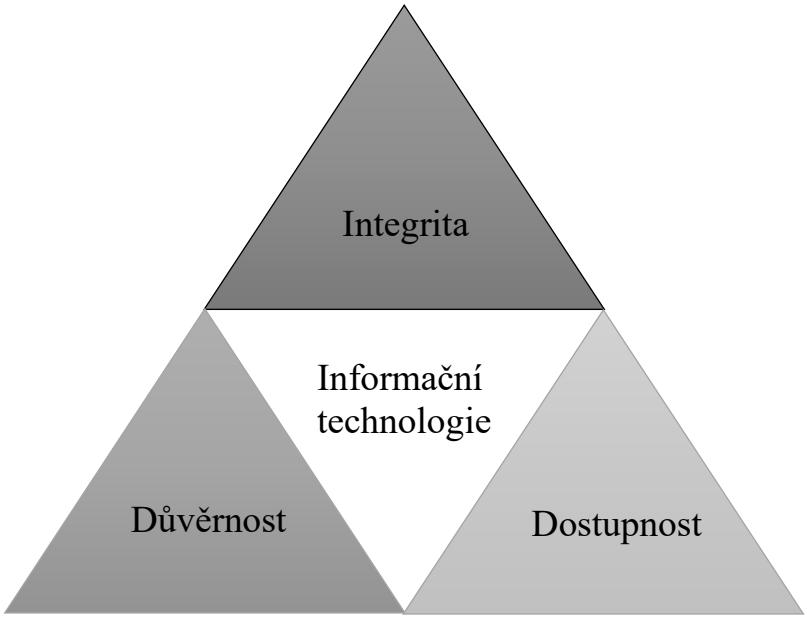
Jedná se o následující 3 triády:

1. CIA (C – Confidentality (důvěrnost), I – Integrity (celistvost), A – Availability (dostupnost)).
2. Prvky kybernetické bezpečnosti.
3. Životní cyklus kybernetické bezpečnosti. (Kolouch, 2016)

4.2.1 Triáda CIA

Nejznámější a nejpoužívanější triádou kybernetické bezpečnosti je právě triáda CIA. Triáda v kyberprostoru znamená důvěrnost, integritu a dostupnost. Tohle jsou základní pilíře kybernetické bezpečnosti, ovšem je doplněna o další tři prvky: P/C – Possession/Control (držení či kontrola), A – Authenticity (autentičnost) a U – Utility (užitečnost).

Nejjednodušší způsob jak jak uvažovat o triádě CIA, je jako bezpečnostní model který pomůže rozbalit různé bezpečnostní komponenty informačních technologií. Tento model pomáhá rozvíjet bezpečnostní politiku k identifikaci problémových oblastí v síti a zároveň poskytují vhodné řešení. (Kolouch a Bašta, 2019)



Obrázek 2 – CIA Triáda (Clark a Hakim, 2017)

Velmi často je triáda CIA vztahována jednoznačně k informacím. Informační bezpečnost se zaměřuje na ochranu informací a je pak aplikována po celý jejich životní cyklus. Informační bezpečnost je definována i normou ISO 27000.

Mezi základní normy informační bezpečnosti patří:

- ČSN ISO/IEC 27001:2014 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky.
- ČSN ISO/IEC 27002:2014 Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací. (Kolouch, 2016)

Důvěrnost

Důvěrnost zahrnuje úsilí organizace zajistit, aby data zůstala tajná nebo soukromá. Aby toho bylo dosaženo, musí být přístup k informacím kontrolován, aby se zabránilo neoprávněnému sdílení dat – ať už úmyslnému nebo náhodnému. Klíčovou součástí zachování důvěrnosti je zajistit, aby lidé bez řádného oprávnění neměli přístup k aktivům důležitým pro subjekty. A naopak, efektivní systém také zajišťuje, že ti, kteří potřebují mít přístup, mají potřebná oprávnění. (Refsdal, Solhaug a Stølen, 2015)

Bezpečnostní standardy ISO/IEC 27000 definují že:

1. *„Informace by měly být klasifikovány, a to s ohledem na jejich hodnotu, právní požadavky, citlivost a kritičnost.“*
2. *„Pro značení informací a zacházení s nimi by měly být vytvořeny a do praxe zavedeny postupy, které jsou v souladu s klasifikačním schématem přijatým organizací.“* (Sak a Mareš, 2007)

„*Pro zabránění neautorizovanému přístupu nebo zneužití informací by měla být stanovena pravidla pro manipulaci s nimi a pro jejich ukládání.“* (Kolouch a Bašta, 2019)

Příklady některých klasifikačních schémat:

Tabulka 1 - Klasifikace informací dle zákona 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti**.** (ČESKO, 2005)

1. Klasifikace informací dle zákona 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti.	
Přísně tajné (Top Secret)	*„Neoprávněné nakládání s informacemi by mohlo způsobit vyzrazení neoprávněné osobě nebo zneužití může způsobit mimořádně vážnou újmu zájmům České republiky.“*
Tajné (Secret)	*„Neoprávněné nakládání s informacemi by mohlo způsobit vyzrazení neoprávněné osobě nebo zneužití může způsobit vážnou újmu zájmům České republiky.“*
Důvěrné (Confidential)	*„Neoprávněné nakládání s informacemi by mohlo způsobit vyzrazení neoprávnění osobě nebo zneužít vyzrazení může způsobit prostou újmu zájmům České republiky.“*
Vyhrazené (Restricted)	*„Neoprávněné nakládání s informacemi by mohlo způsobit vyzrazení neoprávněné osobě nebo zneužití může být nevýhodné pro zájmy České republiky.“*

V tabulce č. 1 jsou vypsány pouze klasifikace informací dle zákona 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. V tabulce č. 2 jsou pak pospány informace podle citlivé povahy. Tyto klasifikace se může dále podrobněji dělit dle organizace, jednotlivce či zda jsou akceptovány dle právního předpisu. (Kolouch, 2016)

Tabulka 2 - Klasifikace informací (Šulc, 2018)

2. Klasifikace informací využívaná v komerční sféře.	
Chráněné	*„Neoprávněné nakládání s informacemi by mohlo způsobit závažné poškození či zničení organizace (např. únik strategických informací, zdrojových kódů, schémat zabezpečení, hesel aj.).“*
Interní	*„Neoprávněné nakládání s informacemi by mohlo způsobit poškození organizace (např. únik osobních údajů, smluv aj.).“*
Citlivé	*„Neoprávněné nakládání s informacemi by mohlo mít negativní dopad na společnost (např. dosud nezveřejněné informace o projektech, plánovaných akcích aj.).“*
Veřejné	*„Neoprávněné nakládání s informacemi by nemělo nikoho poškodit a nemělo by mít jakýkoliv dopad na společnost (např. veřejně dostupné kontakty, prezentace projektů aj.).“*

Traffil Light Protocol

Protokol TLP (Traffic Light Protocol) je protokol pro někoho, kdo sdílí informace, aby informoval veřejnost o jakýchkoli omezeních při dalším šíření těchto informací. Používá se téměř ve všech komunitách CSIRT a v některých centrech pro analýzu a sdílení informací (ISAC). TLP lze použít ve všech formách komunikace, ať už písemné nebo ústní.

Protokol je v zásadě snadno použitelný. Sdílející informace označí informace barvou. Označení informací sestává jednoduše z přidání „TLP: COLOUR“ (v tabulce č. 3) na dokument nebo jeho část. Význam barvy označuje možnosti dalšího šíření informace. V průběhu let se objevila různá znění TLP, ale komunita CSIRT se nedávno pokusila TLP objasnit. (Cyberblog, 2022)

Tabulka 3 - Protokol semaforu (TLP) (ČESKO, 2018)

3. Trafiic Light Protovol		
Barva	**Význam**	**Příklad**
TPL: RED Neurčeno k zveřejnění pouze pro účastníky	*„Zdroje mohou používat TLP: RED, pokud s informacemi nemohou účinně jednat další strany, a pokud by byly zneužity, mohlo by to mít dopad na soukromí, pověst nebo operace strany. Příjemci nesmějí sdílet informace s žádnými stranami mimo konkrétní výměnu, schůzku nebo konverzaci, ve které byly původně zveřejněny. Například v souvislosti se schůzkou jsou informace TLP: RED omezeny na osoby přítomné na schůzce. Ve většině případů by měla být vyměněna ústně nebo osobně.“*	*„Informace sdílené s lidi na schůzce, přímý e-mail.“*
TPL: AMBER Omezené zveřejnění, omezené na organizace účastníků	*„Zdroje mohou používat TLP: AMBER, když informace vyžadují podporu, aby bylo možné s nimi efektivně jednat, a přesto s sebou nesou rizika pro soukromí, pověst nebo operace, pokud jsou sdíleny mimo zúčastněné organizace. TLP: AMBER pouze se členy své vlastní organizace a s klienty nebo zákazníky, kteří potřebují znát informace, aby se ochránili nebo zabránili dalšímu poškození. Zdroje mohou svobodně specifikovat další zamyšlené limity sdílení: ty musí být dodrženy.“*	*„Sdílení ukazatelů kompromisu (IoC) s CSIRT organizace. Ty by mohli být předělány SOC k dalšímu opatření.“*
TPL: GREEN Omezena zveřejnění, omezené na komunitu	*„Zdroje mohou použít TLP: GREEN, pokud jsou informace užitečné pro informovanost všech zúčastněných organizací a také u kolegů v rámci širší komunity nebo sektoru. Příjemci mohou sdílet informace s kolegy a partnerskými organizacemi v rámci svého sektoru nebo komunity, ale ne prostřednictvím veřejně přístupných kanálů. Informace v této kategorii mohou být široce*	*„Sdílení analýzy malwaru s konkrétním průmyslovým sektorem.“*

	šířeny v rámci konkrétní komunity. Informace nesmí být zveřejněny mimo komunitu.“	
TPL: WHITE	*„Zdroje mohou používat TLP: WHITE, pokud informace nesou minimální nebo žádné předvídatelné riziko zneužití, v souladu s platnými pravidly a postupy pro zveřejnění. V souladu se standardnímu pravidly autorských práv mohou být informace distribuovány bez omezení.“*	*„Poradenství veřejné bezpečnosti.“*

Na protokol TLP je kladen důraz urychlit výměnu informací mezi zúčastněnými subjekty. Subjekty předávají informace a vždy musí označit informaci určitou barvou.

Tabulka 4 - Stupnice pro hodnocení důvěrnosti (ČESKO, 2018)

4. Hodnocení důvěrnosti dle vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat		
Úroveň	**Popis**	**Příklady požadavků**
Nízká	*„Aktiva jsou veřejně přístupná nebo byla určena ke zveřejnění. Narušení důvěrnosti aktiv neohrožuje oprávněné zájmy povinné osoby.* *V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle tzv. traffic light protokolu (dále jen „TLP“) je využíváno označení TLP: WHITE.“*	*„Není vyžadována žádná ochrana.* *Likvidace/mazání aktiva na úrovni Nízká.“*
Střední	*„Aktiva nejsou veřejně přístupná a tvoří know-how povinné osoby, ochrana aktiv není vyžadována žádným právním předpisem nebo smluvním ujednáním.*	*„Pro ochranu důvěrnosti jsou využívány prostředky pro řízení přístupu.“*

	V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení TLP: GREEN nebo TLP: AMBER.“	
VYSOKÁ	*„Aktiva nejsou veřejně přístupná a jejich ochrana je vyžadována právními předpisy, jinými předpisy nebo smluvními ujednáními (například obchodní tajemství, osobní údaje). V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení TLP: AMBER.“*	*„Pro ochranu důvěrnosti jsou využívány prostředky, které zajistí řízení a zaznamenávání přístupu. Přenosy informací komunikační sítí jsou chráněny pomocí kryptografických prostředků.“*
KRITICKÁ	*„Aktiva nejsou veřejně přístupná a vyžadují nadstandardní míru ochrany nad rámec předchozí kategorie (například strategická obchodní tajemství, zvláštní kategorie osobních údajů). V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení TLP: RED nebo TLP: AMBER.“*	*„Pro ochranu důvěrnosti jsou využívány prostředky, které zajistí řízení a zaznamenávání přístupu. Dále metody ochrany zabraňující zneužití aktiv ze strany administrátorů. Přenosy informací jsou chráněny pomocí kryptografických prostředků.“*

Integrita

Integrita dat je koncept a proces, který zajišťuje přesnost, úplnost, konzistenci a platnost dat organizace. Dodržováním tohoto procesu organizace nejen zajistí integritu dat, ale zaručí, že budou mít ve své databázi přesná a správná data.

Důležitost integrity dat se zvyšuje s tím, jak objemy dat stále exponenciálně rostou. Velké organizace jsou stále více závislé na integraci dat a schopnosti přesně interpretovat informace, aby mohly předvídat chování spotřebitelů, vyhodnocovat aktivitu trhu a zmírňovat potenciální rizika zabezpečení dat. To je pro vytahování dat zásadní, takže datoví vědci mohou pracovat se správnými informacemi. V tabulce č. 5 je popsána stupnice pro hodnocení integrity. (Jirásek, Novák a Požár, 2015)

Tabulka 5 - Stupnice pro hodnocení integrity (ČESKO, 2018)

1. Vyhláška o kybernetické bezpečnosti představuje také stupnici pro hodnocení integrity.		
Úroveň	**Popis**	**Příklady požadavků**
Nízká	*„Aktivum nevyžaduje ochranu z hlediska integrity. Narušení integrity aktiva neohrožuje oprávněné zájmy povinné osoby.“*	*„Není vyžadována žádná ochrana.“*
Střední	*„Aktivum může vyžadovat ochranu z hlediska integrity. Narušení integrity aktiva může vést k poškození oprávněných zájmů povinné osoby a může se projevit méně závažnými dopady na primární aktiva.“*	*„Pro ochranu integrity jsou využívány standardní nástroje (například omezení přístupových práv pro zápis).“*
Vysoká	*„Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity aktiva vede k poškození oprávněných zájmů povinné osoby s podstatnými dopady na primární aktiva.“*	*„Pro ochranu integrity jsou využívány speciální prostředky, které dovolují sledovat historii provedených změn a zaznamenat identitu osoby provádějící změnu. Ochrana integrity informací přenášených*

		komunikačními sítěmi je zajištěna pomocí kryptografických prostředků.“
Kritická	*„Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity vede k velmi vážnému poškození oprávněných zájmů povinné osoby s přímými a velmi vážnými dopady na primární aktiva.“*	*„Pro ochranu integrity jsou využívány speciální prostředky jednoznačné identifikace osoby provádějící změnu (například pomocí technologie digitálního podpisu).“*

Dostupnost

I když jsou data důvěrná a jejich integrita zachována, jsou často k ničemu, pokud nejsou k dispozici těm v organizaci a zákazníkům, kterým slouží. To znamená, že systémy, sítě a aplikace musí fungovat tak, jak mají a kdy mají. Také jednotlivci s přístupem ke konkrétním informacím musí mít možnost je využít, když to potřebují, a dostat se k datům by nemělo zabrat nepřiměřeně dlouho. Pro lepší porozumění jsou stupnice dostupnosti popsány v tabule 6.

Tabulka 6 - Stupnice pro hodnocení dostupnosti (ČESKO, 2018)

1. Vyhláška o kybernetické bezpečnosti pro hodnocení dostupnosti		
Úroveň	**Popis**	**Příklady požadavků na ochranu aktiva**
Nízká	*„Narušení dostupnosti aktiva není důležité a v případě výpadku je běžně tolerováno delší časové období pro nápravu (cca do 1 týdne).“*	*„Pro ochranu dostupnosti je postačující pravidelné zálohování.“*

Střední	*„Narušení dostupnosti aktiva by nemělo překročit dobu pracovního dne, dlouhodobější výpadek vede k možnému ohrožení oprávněných zájmů povinné osoby.“*	*„Pro ochranu dostupnosti jsou využívány běžné metody zálohování a obnovy.“*
Vysoká	*„Narušení dostupnosti aktiva by nemělo překročit dobu několika hodin. Jakýkoli výpadek je nutné řešit neprodleně, protože vede k přímému ohrožení oprávněných zájmů povinné osoby. Aktiva jsou považována za velmi důležitá.“*	*„Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb může být podmíněna zásahy obsluhy nebo výměnou technických aktiv.“*
Kritická	*„Narušení dostupnosti aktiva není přístupné, a i krátkodobá nedostupnost (v řádu několika minut) vede k vážnému ohrožení oprávněných zájmů povinné osoby. Aktiva jsou považována za kritická.“*	*„Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb je krátkodobá a automatizovaná.“*

4.2.2 Prvky kybernetické bezpečnosti

Další podkapitola pojednává o třech prvcích, které na sebe vzájemně působí a ulehčují vytvořit kybernetickou bezpečnost:

1. Lidé.
2. Technologie.
3. Procesy.

Lidé

V dnešní době používají kybernetičtí útočníci vysoce sofistikované metody cílení na zaměstnance v první linii, a dokonce i na generální ředitele. To je důvod, proč je většina narušení bezpečnosti obviňována z lidské chyby, což dokazuje, že lidé jsou nejslabším článkem kybernetické bezpečnosti. Správnými procesy a školicími programy je však lze

proměnit v LIDSKÝ FIREWALL, který nám nesmírně pomůže při řešení kybernetických bezpečnostních hrozeb. Pokud si koupíme nejlepší technologii, a implementujeme ji špatně nebo ji neumíme efektivně spravovat, je k ničemu. Měli bychom tedy pochopit, že lidé jsou velmi důležitým pilířem v každé organizaci. Každý v podnikání potřebuje, abychom si byli vědomi své role při prevenci a snižování kybernetických hrozeb, kybernetická bezpečnost je obchodní záležitostí a každý má svou roli.

Důležité body týkajících se lidí:

- Manager kybernetické bezpečnosti.
- Pracovník pro ochranu osobních údajů.
- Program a proces řízen dovedností lidí k identifikaci znalostí o kybernetické bezpečnosti.
- Povědomí o kybernetické bezpečnosti a školení pro zaměstnance aj.

Dodržování bezpečnostních zásad a osvědčených postupů ze strany uživatelů je podpořeno vizí organizace, kulturou zabezpečení a závazkem vrcholového managementu. Konzistence, jednotné prosazování zásad u všech zaměstnanců, aniž by byly podřízeny seniorům v hierarchii. Největším rizikem jsou lidé, ale při správných procesech nemusí být. (Techrepublic, 2022)

Technologie

Existuje celá řada technologií, které mohou bezpečnostní týmy implementovat za účelem vrstvení své obrany. K dosažení robustní a bezpečné informační struktury by organizace měly vybudovat rámec pro výběr technologií, který je v souladu s podnikovou technologií a architekturou zabezpečení.

Příklad některých technologií:

- Obvodové zabezpečení.
- Zabezpečení sítě.
- Zabezpečení koncového bodu.
- Zabezpečení aplikací.
- Zabezpečení dat.

- Bezpečnostní operace.
- Zabezpečení cloudu. (Smejkal, Sokol a Kodl, 2019)

Procesy

Procesy jsou klíčové pro implementaci efektivní strategie kybernetické bezpečnosti. Tento pilíř kybernetické bezpečnosti zajišťuje, že jejich kybernetická bezpečnost má zavedeny strategie, jak proaktivně předcházet a rychle a efektivně reagovat v případě kybernetického bezpečnostního incidentu.

V kybernetické bezpečnosti existuje mnoho procesů a programů:

- Plánování strategie kybernetické bezpečnosti.
- Program řízení bezpečnosti informací.
- Hodnocení pozice kybernetické bezpečnosti a analýza mezer.
- Strategie hodnocení rizik kybernetické bezpečnosti.
- Politika a postup kybernetické bezpečnosti aj.

Tyto tři pilíře kybernetické bezpečnosti – lidé, procesy a technologie – by všechny měly spolupracovat na vybudování silné obranné sítě. Když však organizace efektivně vyvažuje lidi, procesy a technologie, je možné vytvořit synergický rámec, který plně podporuje kybernetickou bezpečnost. (Kolouch, 2016)

4.2.3 Životní cyklus kybernetické bezpečnosti

Obrázek 3 – Životní cyklus kybernetické bezpečnosti (Kybez, 2021)

Životní cyklus kybernetické bezpečnosti je mnohdy zobrazován do různých diagramů. Kvůli časové posloupnosti je potřeba uplatňovat triádu CIA i jednotlivé prvky kybernetické bezpečnosti, a to v průběhu celého životního cyklu. Zaměřuje se na prevenci, detekci a reakci na útok. (Hub, 2013)

5 TYPY ÚTOKŮ

Existuje nespočet klasifikací kybernetických útoků. Zde je několik hlavních slovních pojmů, ty nejpoužívanější a ty, ve kterých slyšíme o diskuzích kybernetické bezpečnosti:

- **Advanced persistent threat – APT (Pokročilá trvalá hrozba)** – říká, co dělá a dělá to, co říká. Je to koordinovaný, vytrvalý, odolný a adaptivní útok proti cíli. APT se primárně používá ke krádeži dat. Provádění výzkumu, plánování a koordinace trá poměrně dlouho ale když uspějí, jsou často zničující.
- **Brute force attack (Útok hrubou silou) –** Pokud je v háčkovacím systému nějaká elegance, pak tato metoda ji postrádá. Útok hrubou silou, podobně jako brutální, se nepoužívá žádný mozek pouze síla – v tomto případě výpočetní síla. Tedy, kdybychom chtěli uhádnout své heslo útokem hrubé síly, použili bychom velmi rychlí počítač a vyzkoušeli každou jednotlivou možnou kombinaci čísla – a úkol, který může zabrat hodně času nebo překvapivě krátkou dobu v závislosti na složitosti hesla.
- **Denial of Service – DoS (Útok odmítnutí služby) –** DoS útoky přicházejí ve dvou variantách: jedno zdrojové a distribuované. K jedno – zdrojovému útoku dojde, když je jeden počítač použit k utopení jiného počítače, aby cílový nemohl fungovat, zatímco distribuovaný útok dosahuje stejného výsledku prostřednictvím mnoha počítačů. Při DDoS útocích jsou počítače obvykle pod koordinovanou kontrolou botnetu. V poslední době je tento typ útoků stále více a více využíván, protože místo použití kompromitovaných počítačů jako součást botnet, hackeři používali jakékoli digitální zařízení (např. chůvy, termostaty), která jsou připojena k internetu. Většina těchto zařízení postrádá i to nejzákladnější zabezpečení a příliš mnoho uživatelů se neobtěžuje měnit výchozí heslo. Přispívají tedy ke snadnému zneužívání těchto zařízení a chovají se jako roboti.
- **Man-in-the-Middle attack („Člověk uprostřed“) -** Při tomto typu útoku hacker zachytí komunikaci mezi dvěma systémy a nahradí ji svou vlastní, což nakonec vede k jeho získání kontroly nad oběma systémy. Lze použít k získání přístupu k přihlašovacím údajům a následně k předstírání normálních operací, zatímco útočník poškozuje cíl.

- **Phishing attack (Phishingový útok)** – Phishig a spear phising jsou útoky, které využívají sociální inženýrské sítě. Sociální inženýrství je v tomto kontextu pouhou fantazií slovo pro lhaní. Hackeři přesvědčují oběť, že útočník je důvěryhodný subjekt (přítel, zavedená firma, instituce nebo vládní agentura) a oklamat oběť, aby se dobrovolně vzdala svých dat. Cílem těchto útoků je získat důvěru, abychom vyzradili citlivé informace útočníkovi. Míra propracování takových útoků se liší, od známého nigerijského prince na e-maily, které se zdají být od bank nebo státních agentur až po extrémně sofistikované nevýhody, které mohou oklamat i nejlépe připravenou a skeptickou oběť. (Oliveira, Hrubec a Sobottka, 2018)

5.1 Hrozby kybernetických útoků

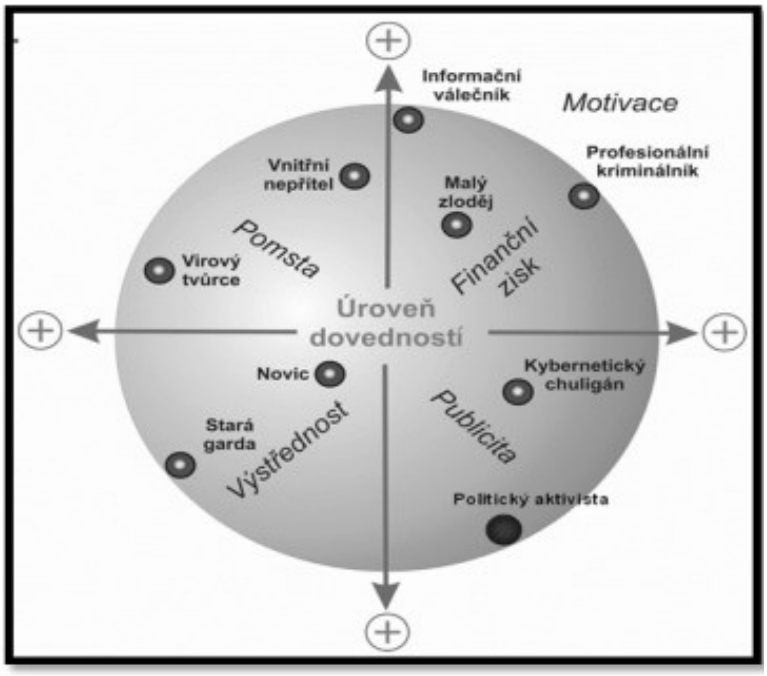
Hrozby sociálního inženýrství bývají plánovány s dostatečným předstihem. Útočník získává informace o cíli z veřejných dostupných zdrojů (sociální sítě, profesní sítě, firemní weby, veřejné záznamy, dokonce i agregátory dat) a poté tyto informace jsou použity k předstírání identity a poškozují cíl. Čím více veřejných informací máme veřejně dostupné a přístupné na internetu, tím snáz je dostaneme. (Kolouch a Bašta, 2019)

V dnešní době nepřestávají být útoky na počítače, softwary, data či samotné sítě nic neobvyklého. Útoky jsou stále rafinovanější, promyšlenější, účinnější, díky chybějící trestněprávní ochraně před novými protiprávními jednáními. Za Hrozbu můžeme považovat jednání, které směřuje ke změně informace, aplikace či systému samotného. (Jirovský, 2007)

Podle Jirovského jsou vymezeny čtyři skupiny základních hrozeb a zároveň charakterizuje jejich vztah:

- Únik informace – *„je stav, kdy dojde k vyzrazení chráněné informace neautorizovaného subjektu.“*
- Narušení integrity – „*představuje poškození, změnu, či vymazání dat.“*
- Potlačení služby – *„znamená úmyslné bránění v přístupu k informacím, aplikacím, či systému.“*
- Nelegitimní použití – *„je užití informací neautorizovaným subjektem či neoprávněným způsobem.“* (Jirovský, 2007)

Je jisté, že všechny hrozby pochází od jistých útočníků, které je možné klasifikovat z různých hledisek.



Obrázek 4 - Členění útočníků v kyberprostoru podle motivace (JANOUŠEK, 2006)

5.2 Malware

Za malware můžeme označit škodlivý software a je používán z anglického názvu. Toto slovo vzniklo složením anglických slov *„malicious software“* v překladu „zákeřný software.“ Jedná se o jakýkoliv software využitý k narušení nebo napadení běžné činnosti počítačového systému, získání dat, informací či získání přístupu do systémů. Jediný malware může poškodit více počítačů najednou. (Kolouch a Bašta, 2019) Dělíme jej dle hlediska účinků (podkapitola 5.2.1) a postupu šíření (podkapitola 5.2.2).

5.2.1 Dělení z hlediska účinků

Malware má více než jednu podobu i více druhů, které jsou propojený dle činnosti provedení. Níže jsou vysvětleny alespoň ty nejhlavnější účinky týkající se malware.

- Adware.
- Spyware.
- Ransomware.

Adware

Software podporující reklamu. Jedná se o nejméně nebezpečnou nežádoucí nebo škodlivou reklamu. Ovšem tato forma je nejvíce výnosná, protože adware zobrazuje reklamy

počítačových systémech nebo na webových stránkách, což ovlivňuje snížení výkonu počítače. Uživatel si tento malware může stáhnout neúmyslně. (Dočekal, 2022)

Obrázek 5 – Příklad reklam (Avast, 2018)

Spyware

Spyware je typ malwaru, který shromažďuje citlivá data z počítačového sytému bez souhlasu uživatele, a aniž by o tom uživatelé věděli. Po instalaci monitoruje aktivity uživatelů na počítači a internetu a poté předává podrobnosti zlomyslným aktérům. Tento škodlivý software může dokonce ukrást přihlašovací jméno, heslo a informace o kreditní kartě. Spyware může také narušit uživatelskou kontrolu nad počítačem instalací dalšího softwaru neb přesměrováním webových prohlížečů. Některý spyware může změnit nastavení počítače, což může mít za následek zpomalení rychlosti připojení k internetu, neoprávněné změny v nastavení prohlížeče nebo změny nastavení softwaru. (Avast, 1988-2022)

Obrázek 6 – Spyware (Itportal.io, 2021)

Ransomware

Je typ malwaru, který brání v přístupu k počítači (nebo k datům, která jsou v něm uložena). Počítač samotný se může zamknout nebo data na něm mohou být ukradena, smazána nebo zašifrována. Některý ransomware se také pokusí rozšířit na další stroje. Obvykle jsme požádáni, abychom útočníka kontaktovali prostřednictvím anonymní e-mailové adresy nebo se řídili pokyny na anonymní webové stránce a provedli platbu. Platba je vždy požadována v kryptoměně, jako je bitcoin, za účelem odemknutí počítače nebo přístupu k našim datům. Nicméně, i když zaplatíme výkupné, neexistuje žádná záruka, že získáte přístup ke svému počítači nebo souborům. (MALWAREBYTES, 2022)

Ransomware můžeme do počítače získat pomocí: malspam, malvertising, spear phishing, sociální inženýrství.

Typy ransomwaru: scareware, screenokers, šifrování ransomwaru.

5.2.2 Dělení z hlediska způsobů šíření

Jak už je uvedeno v předchozí kapitole malware je dělen do dvou podkapitol. Ovšem kdybychom ho chtěli dělit podrobněji, tak zapadá do více kategorií. Zde jsou uvedeny některé typy způsobu šíření:

- Viry.
- Červi.
- Trojské koně.
- Backdoor.
- Rootkity. (Kolouch, 2016)

Viry

Počítačový program, který se může zkopírovat a infikovat počítač bez povolení nebo vědomí uživatele. Virus může poškodit nebo odstranit data v počítači, použít e-mailové programy k šíření do jiných počítačů nebo dokonce vymazat vše na pevném disku. Virus se rozšíří v okamžiku, dojde ke spuštění tohoto softwaru nebo otevření infikované dokumentu.
Příznaky můžou být:

- Vyskakovací okna.
- Hromadné emaily odesílaný ze soukromého účtu.

- Přechod domovské stránky v prohlížeči.
- Výpadky operačního systému.
- Zpomalený výkon počítače.
- Cizí programy, které se spouštějí po zapnutí počítače aj. (Avast, 1988-2022)

Červi

Počítačoví červi mohou infikovat mnoho počítačů v síti během velmi krátí doby. Dokáže se rychle rozšířit z jednoho systému do druhého a nepotřebují k tomu žádného hostitele, tedy žádný spustitelný soubor, šíří se tedy zpravidla samostatně. Červi mohou proniknout do počítačových systémů a pozměnit nebo zničit data. Mají také schopnost instalovat škodlivý software. Každý počítačový červ má svůj vlastní cíl.

Některé jsou vytvořeny aby, se replikovaly, zatímco jiné jsou určeny ke spotřebě systémových prostředků:

- Dochází ke ztrátě, když se systém náhle zhroutí.
- Automatické otevírání a zavírání počítačových programů, které byly nainstalovány.
- Nepravidelně je ovlivněn výkon webového prohlížeče.
- Neočekávané chování počítače.
- Firewall vysílá mnoho varování.
- Soubory mohou chybět nebo jsou upravovány.
- Operační systém zobrazuje chybová upozornění.
- Bez našeho vědomí se e-maily rozesílají mnoha příjemcům. (Brooks et al., 2018)

Trojské koně

Trojské koně jsou druh malwaru, který je maskováním ověřeného nebo legitimního softwaru. Je to druh softwaru, který je škodlivý a je vyvíjen vetřelci nebo hackery pro získání přístupu do systému oběti. Primární záměr návrhu trojského viru je spojen s poškozením, narušením, krádeží a vyvoláním akcí, které jsou škodlivé pro síť nebo data. Trojan je virus, který se chová jako aplikace, která je bonafide nebo soubory, takže oklamat oběť je snadné. Snadno oklame oběť ve dvou aspektech, kterými jsou spuštění a načtení malwaru do

zařízení. Po instalaci trojského softwaru není jednání pro hackery vůbec obtížné. Ve většině případů jsou trojské koně zaváděny prostřednictvím příloh e-mailu. Tyto e-maily jsou maskovány způsobem, který se jeví jako autentický. Poté, co uživatel stáhne soubor, který je připojen, a připraví se ke spuštění, nastane čas, kdy data začnou poškozovat systém. (Eset, 2022)

Backdoor

Ve světě kybernetické bezpečnosti se zadními vrátky rozumí jakákoli metoda, pomocí které jsou autorizovaní a neoprávnění uživatelé schopni obejít běžná bezpečnostní opatření a získat vysoký uživatelský přístup počítačovému systému, síti nebo softwarové aplikaci. Jakmile se kyberzločinci dostanou dovnitř, mohou pomocí zadních vrátek ukrást osobní a finanční data, nainstalovat další malware a unést zařízení.

Zadními vrátky se rozumí jakákoli metoda, pomocí které jsou autorizovaní a neoprávnění uživatelé schopni obejít běžná bezpečnostní opatření a získat vysoký uživatelský přístup (neboli root přístup) k počítačovému systému, síti nebo softwarové aplikaci. (MALWAREBYTES, 2022)

Rootkity

Rootkit je program nebo sbírka škodlivých softwarových nástrojů, které poskytují aktérům hrozby vzdálený přístup a kontrolu nad počítačem nebo jiným systémem. Ačkoli tento typ softwaru má určité legitimní využití, jako je poskytování vzdálené podpory koncovým uživatelům. Rootkity se často pokoušejí zabránit detekci škodlivého softwaru deaktivací antimalwaru a antivirového softwaru koncových bodů. (Kolouch a Bašta, 2019)

5.3 Kybernetické útoky

Kybernetické útoky lze definovat jako jakékoli úmyslné konání útočníka v kyberprostoru. Útočník si obvykle vyhledá nějaký druh útoku a naruší tak sítě oběti. Před tyto útoky se musíme čím dál více chránit a být na pozoru, jelikož se tato oblast stává stále více dynamičtější. Nejedná se o útoky na jednotlivce, ale jsou určeny spíše proti velkým organizacím. Nejznámější kybernetické útoky na organizace. (Clark a Hakim, 2017)

5.3.1 Phishing

Phishingové útoky jsou praktiky zasílání podvodných zpráv, které vypadají, že pocházejí z důvěryhodného zdroje. Obvykle se provádí prostřednictvím e-mailu. Cílem je ukrást

citlivá data, jako jsou kreditní karty a přihlašovací údaje, nebo nainstalovat malware do počítače oběti. Phishing je běžný typ kybernetického útoku, o kterém by se měl každý dozvědět, aby se ochránil. Phishing začíná podvodným e-mailem nebo jinou komunikací, která má nalákat oběť. Zpráva vypadá, jako by přišla od důvěryhodného odesílatele. Pokud to oběť oklame, je přemluvena, aby poskytla důvěrné informace – často na podvodné webové stránce. Někdy je malware také stažen do cílového počítače.

Kyberzločinci začínají tím, že identifikují skupinu jedinců, na které se chtějí zaměřit. Poté vytvoří e-mailové a textové zprávy, které se zdají být legitimní, ale ve skutečnosti obsahují nebezpečné odkazy, přílohy nebo návnady, které přimějí jejich cíle k provedení neznámé, riskantní akce. (Jirásek, Novák a Požár, 2015)

5.3.2 Pharming

Pharming je typ kybernetického útoku zahrnujícího přesměrování webového provozu z legitimního webu na falešný web za účelem krádeže uživatelských jmen, hesel, finančních údajů a dalších osobních údajů. (Kolouch a Bašta, 2019)

5.3.3 Cross-sitte scripting

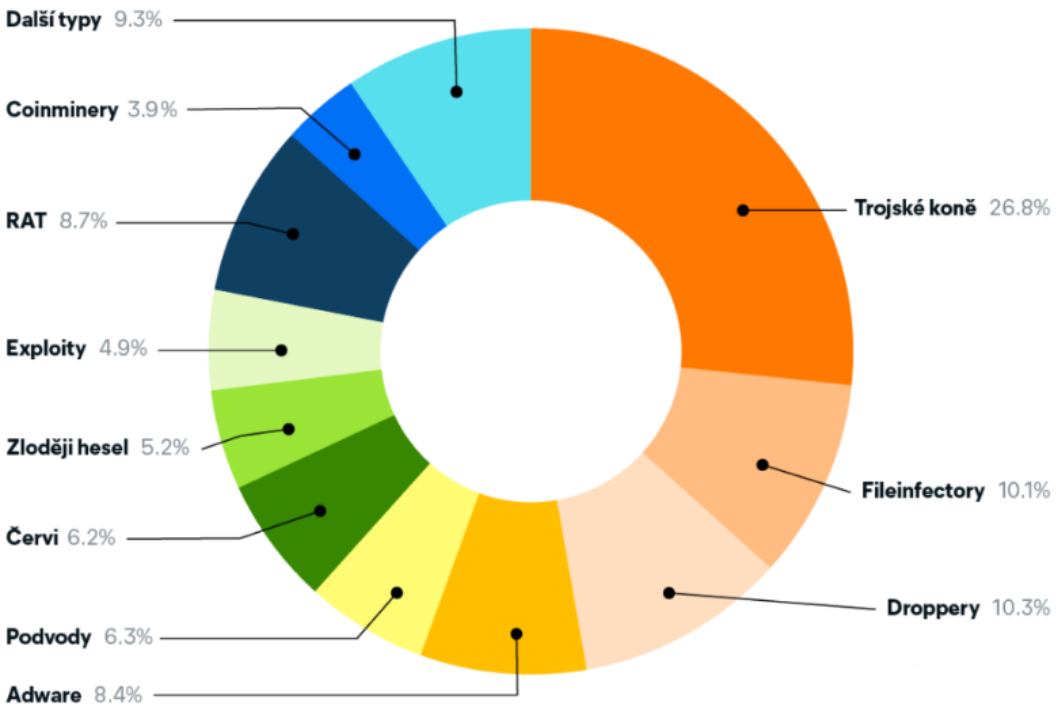
Útoky Cross-sitte scripting (XSS) jsou typem injekce, při které jsou škodlivé skripty vpravovány do jinak neškodných a důvěryhodných webových stránek. K útokům XSS dochází, když útočník použije webovou aplikaci k odeslání škodlivého kódu, obvykle ve formě skriptu na straně prohlížeče, jinému koncovému uživateli. Chyby, které umožňují těmto útokům uspět, jsou poměrně rozšířené a vyskytují se všude, kde webová aplikace používá vstup od uživatele v rámci výstupu, který generuje, aniž by jej ověřovala nebo kódovala. Útočník může použít XSS k odeslání škodlivého skriptu nic netušícímu uživateli. Prohlížeč koncového uživatele nemá žádný způsob, jak zjistit, že skriptu nelze důvěřovat, a skript spustí. Protože se domnívá, že skript pochází z důvěryhodného zdroje, může škodlivý skript přistupovat ke všem souborům cookies, tokenům relace nebo jiným citlivým informacím, které prohlížeč uchovává a používá s tímto webem. Tyto skripty mohou dokonce přepsat obsah HTML stránky.

5.4 Statistika penetrace malwaru v České republice

Dle statistiky je za posledních pár let nejrozšířenějším typem malwaru v ČR trojské koně. Statky se provádí každý a registruje se přes 450 000 škodlivých hrozeb. Tyto hrozby jsou zkontrolovány a následně klasifikovány dle jejich vlastností. Pomocí speciálních programů jsou pak tyto hrozby převedeny do grafů a vytváří aktuální statistiky.

K nejčastějším hrozbám v ČR za rok 2021 patří:

- Trojské koně pro vzdálený přístup (RAT).
- Adware.
- Červi.
- Malware ke krádeži dat.
- Fileinfectory.
- Droppery.
- Podvody.
- Zloději hesel.
- Exploity.
- Coinminery.
- Další typy. (Cyberblog, 2022)



Graf 1- Nejčastější hrozby v Česku za rok 2021 (Cyberblog, 2022)

V grafu č.1 jsou za největší hrozby považovány trojské koně (26,8 %), na druhém místě jsou droppery (10,3 %) škodlivé programy určené k nainstalování viru. Třetí hrozbou byly fileinfectory (10,1 %) jedná se o malware napadající soubory a trvale je poškodit či šířit v systému.

II. PRAKTICKÁ ČÁST

6 POPIS VEŘEJNÉ SPRÁVY

Cílem praktické části je aplikovat požadavky na kybernetickou bezpečnost v oblasti veřejné správy. V úvodu praktické části bude nejprve popsána veřejná správa a dále analyzovány rizika kybernetické bezpečnosti v subjektu veřejné správy a definovány tyto rizika z pohledu ochrany aktiv, které organizace využívá.

Definice pro veřejnou správu existuje mnoho, avšak můžeme říct, že se jedná o správní činnost související s poskytováním veřejných služeb. Řídí veřejné záležitosti na místní i centrální úrovni a zajišťuje záležitosti ve veřejném zájmu. (Lochmannová, 2020) Mimo jiné je veřejná správa označována též jako správní orgán, do tohoto orgánu zahrnujme především úřady. Jedná se určité druhy, které veřejnou správu vykonává:

- Činnosti (funkce).
- Instituce orgánu.

Veřejná správa je rozdělená na státní správu a samosprávu. Státní správa je bezprostředně orgánem státu v rámci jejího systému. Samospráva se ještě rozděluje na územní, zájmovou a profesní. Veřejná správa je činností orgánu státu nebo jiného subjektu veřejné moci, ovšem mimo státní orgány, které vykonávají zákonodárství, soudnictví nebo vládu. Při výkonu svých činností můžou používat jen takové prostředky a formy regulace, které jsou určeny zákonem. (Vrabková, 2016)

Organizace veřejné správy je upravována právními předpisy:

- Ústavní zákon č. 1/1993 Sb., ve znění pozdějších ústavních zákonů.
- Zákon č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy České republiky, ve znění pozdějších předpisů.
- Zákon č. 347/1997 Sb., o vytvoření vyšších územních samosprávných celků, ve znění pozdějších ústavních zákonů. (Vrabková, 2016)

Subjekty veřejné správy jsou povinny nést odpovědnost za plnění veřejných úkolů. Příklady některých subjektů veřejné správy:

- Stát.
- Státní fondy, veřejné ústavy a veřejné podniky.
- Zájmová a profesní společenství.
- Nadace a nadační fondy.

Mezi orgány veřejné správy patří Ústava, hlava III., která upravuje moc výkonnou. Jedná se o postupy vlády jako vytvářet, rozhodovat a působit. Vykonavateli jsou:

- Prezident ČR.
- Vláda.
- Ministerstva.
- Jiné ústřední správní úřady.
- Jiné správní úřady (řízené ministerstvy a podřízené jiným správním úřadům).
- Orgány samosprávy (obcí, krajů a zřízených zvláštními zákony s přesně vymezenou působností.
- Orgány vysokých škol.
- Veřejné bezpečnostní sbory (ozbrojené nebo neozbrojené). (Lochmannová, 2020)

6.1 Popis daného subjektu

Z důvodu zachování mlčenlivosti nebude popis subjektu obsahovat detailní informace o informačních systémech, plánech a fotodokumentací, tak aby subjekt nebylo možné přesně identifikovat. Subjekt veřejné správy se zabývá správou veřejných záležitostí ve veřejném zájmu. Organizace provádí výběr poplatků spojených s obchodem a její činnost podléhá specifickému zákonu, který upravuje obchodně-politické dění. Na základě charakteru činnosti organizace se jedná o kritickou infrastrukturu, která spravuje důležité informace. Subjekt je tedy součástí kritické bezpečnostní infrastruktury státu a v objektech jsou nainstalována bezpečnostní a síťová infrastruktura.

Současný model a podoba kybernetické infrastruktury a informačních systémů je zformována na základě skutečnosti, že transformace informací a požadavky na komunikační technologie představují výzvy, které má veřejná správa povinnost zajišťovat. Synchronizace činností jednotlivých subjektů státní správy a na druhé straně řízení složité komunikační sítě je důležité přizpůsobit novým technologiím, ale také zajistit optimální ochranu před potenciálními riziky, která by ohrozily náklady a bezpečnost státu. (Smejkal a Rais, 2013)

Organizace subjektu má dvě základní rozdělení:

- Generální ředitelství sídlící v Praze.
- Úřady, kterých je v ČR patnáct.

Úřady jsou v krajských městech a jeden sídli na v Praze. Nadřízeným orgánem je Ministerstvo financí. Veřejná správa v současné době disponuje vlastním informačním systémem, který zajišťuje rozvoj činností v oblasti výběrů daní, specifických poplatků apod. Informační systém organizace splňuje požadavky principů ČSN ISO 20 000 a ČSN ISO 27 001, které představují rámec certifikace kybernetické bezpečnosti informací pro subjekty zabývající se obchodem. Organizace má v současnosti téměř 4.500 zaměstnanců.

Personální systém

Personální systém je vybavena funkcemi, které zajišťují především následující činnosti a jsou nepostradatelné pro mzdovou a personální agendu:

- Řízení lidských zdrojů.
- Evidence osobních údajů, informace o dovolených, absence, přesčasů a odměn.
- Evidence údajů pro zdravotní a sociální pojišťovnu.
- Kalkulace a výpočet mezd, mzdové podklady-výplatní pásky, roční zúčtování mezd.

Systém evidence dotací

Systém evidence dotací slouží jako centrální databáze a evidence poskytnutých dotací, které byly vyplaceny ze státního rozpočtu. V evidenci lze nalézt údaje jako jsou příjemci dotací, výše a účel poskytnutých grantů, termíny vyplacených finančních částek apod. Systém evidencí dotací zajišťuje především tyto služby:

- Vykazování dat o správě dotací dle jednotlivých resortů v návaznosti na politiku Evropské unie v oblasti strukturálních fondů.
- Zlepšení evidence a předávání informací.
- Zlepšení úplnosti a správnosti dat.

Webové aplikace

Webové aplikace představují především Internetové stránky (prezentace informací týkající se činnosti organizace a komunikace s třetími stranami) a Intranetové stránky (komunikace uvnitř společnosti, která je omezena jen pro zaměstnance státní správy).

Internetové stránky zejména zajišťují tyto činnosti:

- Komunikace s fyzickými, právnickými osobami a elektronické formuláře ke stažení.
- Kontakty na jednotlivá územní pracoviště.

- Seznam poplatků, které spadají pod působnost správy.
- Vymezení hlavních kompetencí správy.

Intranetové stránky zejména zajišťují tyto činnosti:

- Usnadňovat komunikaci se zaměstnanci.
- Řídit konferencí a vztahy se zaměstnanci.
- Zvýšit produktivitu pracovních sil.

7 ANALÝZA BEZPEČNOSTI SUBJEKTU VEŘEJNÉ SPRÁVY

Tato kapitola je zaměřena na analýzu fyzické bezpečnosti subjektu a cílem je podat obraz o aktuální kybernetické bezpečnosti, která se přímo vztahuje k budově, ve které subjekt trvale sídlí. Fyzická kybernetická bezpečnost budovy by měla spojovat takové aspekty, které vycházejí z technických, právních a organizačních požadavků. Smyslem je tedy získat dané požadavky a získat informace prostřednictvím rozhovoru s generálním ředitelem.

7.1 Fyzická ochrana

Fyzická bezpečnost budovy představuje řešení, které zajistí schopnost čelit novým hrozbám a výzvám z vnějšího okolí. Sídlo společnosti disponuje rozsáhlým portfoliem bezpečnostních řešení, které jsou vzájemně kombinovány. Vstupní část budovy je chráněna prostřednictvím fyzické ochrany, velkými vstupními vraty a dále při vstupu do budovy jsou instalovány fyzické bezpečnostní kontroly, které fungují na principu kontroly fyzické bezpečnosti a jejich smyslem je přidat další prvek k zásadě kybernetické bezpečnosti organizace. Kontroly fyzické bezpečnosti (systém fyzického zabezpečení) je důležitý, jelikož společnost sídlí v centru města, kde se pohybuje velké množství osob a návštěvníků.

7.1.1 Fyzická bezpečnostní kontrola

Smyslem je držet mimo prostory budovy osoby, kterým není povolen vstup do objektu. Kontrola funguje na principu kartiček s elektronickými čidly, která jsou vydávány návštěvníkům a zaměstnancům. Cílem těchto zařízení je především odstrašit a detekovat. Detekce slouží jako senzor, který je schopen zaznamenat nepovolené v pohyby na místech, která jsou vysoká z bezpečnostního hlediska.

7.1.2 Zabezpečení vnějšího perimetru (linie nemovitosti)

Budova je chráněna prostřednictvím extrémnějších forem zabezpečení nemovitosti vnějšího prostředí a zadní a okolní linie budovy jsou chráněny ostnatými dráty.

7.2 Technické prvky fyzické bezpečnosti

Smyslem kamerových systémů je zpravidla prevence a odhalení trestné činnosti a prevence, a to nejen ve venkovních prostorech, ale i uvnitř objektu a v bezprostředním okolí veřejných objektů. Kamerové systémy plní svůj účel a chrání soukromý majetek lidí a jejich sousedství.

Výhodou kamerových systémů je bezpochyby schopnost zajistit důkazy v případě spáchání trestné činnosti a zároveň slouží jako odstrašující prostředek. (Honzík, 2020)
Kamerové systémy společnost využívá zejména za účelem ochrany svého majetku a zajištění bezpečnosti a ochrany lidí, které vstupují do monitorovaného areálu, ať už jsou to zaměstnanci, klienti nebo veřejnost. Kamerové systémy, byly instalovány v budově zhruba před čtyřmi lety na základě doporučení z kybernetické národní rady, a to z důvodu, že dříve musela organizace čelit vniknutí do budovy a detekovat vetřelce. Bylo nezbytně nutné vyřešit i otázku, jak chránit tato zařízení před vandalismem a poškozením. Také bylo důležité informovat prostřednictvím informačních tabulí osoby, že se nacházejí ve střeženém prostoru, který je monitorován. První podmínkou při nákupu těchto systémů bylo, aby kamery příliš nezasahovaly do soukromí osob. Bylo nutné respektovat zásady a práva osob na ochranu svého soukromí. Záznamy ze soukromí osob pořízené kamerami bylo možné jen využít v souvislosti s kdy došlo ke spáchání trestné činnosti a jiné důkazy nejsou k dispozici. Dále společnost stanovila ve spolupráci s oddělením rizik lhůtu, po kterou bude možné dané záznamy objektu uchovávat. Lhůta vycházela z podstaty, že dané záznamy a snímky budou archivovány jen na dobu nezbytnou pro kterou nahrávky slouží ke stanovenému účelu.

7.2.1 Poplachové zabezpečovací a tísňové systémy

Poplachové zabezpečovací a tísňové systémy (PZTS) *„nejen v prostředí veřejné správy slouží jako doplněk k opatřením kontroly vstupu osob do objektu a tyto bezpečnostní systémy působí tak, aby posílily vnitřní bezpečnost a poskytly adekvátní prostředky k ochraně majetku vyšší hodnoty a ochránili operace či činnosti citlivých na bezpečnost ve vybraných objektech. Tyto technologie zabezpečují ochranu v jednotlivých místnostech a chrání majetek, v neposlední řadě a poskytují záchranářům a policii specifické informace pro případnou reakci v případě řešení nepovoleného vstupu do objektu.“* (Burda, 2017)

Prostory budovy jsou chráněny robustnějšími a komplexnějšími poplachovými a tísňovými systémy (PZTS), jelikož prostory jsou rozsáhlejší oproti jiným budovám a jsou uzpůsobeny pro účely ochrany majetku jak hmotného a nehmotného na více místech. PZTS systémy, které jsou využívány v subjektu představují elektronické systémy, které disponují čidly a detektory, aby spolehlivě a průběžně monitorovaly pohyby ve střežených prostorech.

Na základě řízeného rozhovoru lze definovat následující poplachové zabezpečovací a tísňové systémy (PZTS*):*

Alarmy proti narušení a nepovolenému vstupu

Tyto alarmy slouží k nepovolenému vstupu do budovy a jsou umístěny v prostorách na základě nejvyšší pravděpodobnosti potenciálního rizika vstupu. Detektory pohybu monitorují vstup budovy a místností, kde se nacházejí cenná aktiva společnosti. Dále detekují pohyby u místností, kde se nachází cenné vybavení a nákladná technika a trezory. Signály senzorů jsou bezdrátové a jsou posílány do centrálního, řídícího centra. Tímto je zajištěna ochrana a bezpečnost záznamů, které alarmy detekují. Jednotlivé aktivity, které jsou zaznamenány čidly monitorují zaměstnanci externí firmy a jejich úkolem je mobilizovat pomocné síly v případě ohrožení a zachování bezpečnosti. Konkrétní alarmy proti narušení, které jsou instalovány v prostorách jsou pasivní infračervená čidla, která jsou napojena na elektronický zabezpečovací systém.

Systém prevence kriminality

Systém prevence kriminality představuje detekci rozbití skla. Detektor rozbití skla upozorní v případě, že dojde k rozbití skla v oknech nebo rozbití skla ve dveřích. Detektory rozbití skla byly využity, tak aby byla zajištěna komplexní a důležitá vrstva bezpečnosti. Snímače rozbití skla jsou umístěny bezprostředně na sklech dveří a oknech. V konkrétním případě byly zvoleny nárazové detektory, které jsou zaměřeny na vibrace v případě nárazu a rozbití skel. Jak uvedl dotazovaný nejvyšším přínosem je extra forma zabezpečení. Ovšem téměř ve většině případů se jedná o falešné poplachy, které způsobuje i silnější dovírání dveří.

7.2.2 Systém detekce požáru

Systémy detekce požáru slouží jako součást kybernetické bezpečnosti. Oheň může zasáhnout a poškodit informační bezpečnost, jak uvedl respondent. Respondent se vyjádřil konkrétně k systému detekce požáru takto: *„V prostorách orgánu státní správy se nachází hardware a média, které je nutné třeba chránit, a to nejen před fyzickými útoky, ale i před přírodními živly.“*

Dále respondent uvedl, že požární a detekční systémy jsou alokovány nejen v místech, které dle zákona je nutné zabezpečit požárními systémy, ale navíc i v rizikových prostorech. Alarmy, které detekují požár obsahují akustické signály a je zajištěn 24hodinový provoz těchto alarmů pomocí náhradních zdrojů. Společnost využívá klasická systémy, které jsou napojeny na centrální ústřednu, která má v kompetenci identifikovat poplach a vyslat požární

ochranu na rizikové místo. Rizikové prostory jsou dále rozděleny do tzv. požárních zón, které jsou pod dohledem.

7.2.3 Přístupové systémy

Přístupové systémy jsou jedním ze způsobu, jak chránit majetek a bezpečí osob. Přístupové systémy fungují na principu, že po identifikaci osob umožní vstup do chráněných prostor. Přístupové systémy můžeme dělit na tři typy:

- Centrálně řízené.
- Autonomně řízené.
- Kombinovaně.

Výhodou přístupových systémů je, že v případě ztráty klíčů nemusíme řešit náhradní a dochází jen k odblokování uživatele v systému. Nejpodstatnějšími výhodami přístupových systémů oproti zamykacím zařízením jsem tato:

- *„Zavedením přístupových systémů se omezí volný a nekontrolovatelný pohyb osob v určitých prostorách objektů.*
- *Pohyb osob je možno omezit v čase.*
- *Nahradí mnoho klíčů jednou kartou nebo čipem.*
- *Zvýší komfort ovládání.*
- *Umožní přístup pouze vybraným skupinám omezí se pohybu vozidel v areálu“.*
  (Z-WARE, 2022)

Přístupové systémy jsou považována za jednu z nejdůležitějších a nejbezpečnějších systému, které se nacházejí v komplexu. Na základě této skutečnosti byly zpracovány odborné expertní návrhy nejefektivnějších přístupových systémů. Cílem přístupových systémů je zabezpečení především citlivých dat a informací. Řízení přístupů je jedním z nejsložitějších a nejnákladnějších bezpečnostních systémů a správa je zajištěna prostřednictvím IT externí společnosti. Tyto systémy jsou řízeny softwarem, který zajišťuje správu celého komplexního systému. Přístupové systémy jsou dále využívány i k omezení či udělení práv uživatelům a personálu ke konkrétním informacím a datům. Jedním z typů přístupových systémů, které jsou využívány je docházkový systém. Docházkový systém zaznamenává tzv. průchodová data pomocí terminálů. Terminály jsou nastaveny tak, aby dokázali identifikovat osoby

a byly schopny rozlišit noční a denní směny apod. Docházkový systém je významným pomocníkem pro zpracování mezd, umožňuje kontrolu docházky.

Řízení přístupu do budovy

Řízení přístupu je akt selektivního povolení nebo omezení přístupu do budovy a prostorů v této budově. Prvním typem je Monitorování zaměstnanců u vchodů za účelem kontroly ID nebo pověřen**:** jedná se o manuální kontrolu zaměstnanců a personálu prostřednictvím fyzické osoby, která průběžně kontroluje vstup do budovy. Kontrola probíhá na základě ID karty a systémů evidence zaměstnanců v počítači.

Elektronický přístupový systém je součást integrovaného přístupového systému. Sídlo je vybaveno jen online elektronickým přístupovým systémem, který zabezpečuje rizikové oblasti pracovišť a umožňují vstup jen určitým osobám a zaměstnancům, kteří mají povolený vstup do místnosti. Sledování pohybu zajišťuje počítač. Elektronická kontrola přístupu je realizována pomocí ID karet.

Kontrola fyzického přístupu do budovy je zajištěna umístěním turniketů do vstupní části budovy a venkovní turnikety monitorují přístup do jednotlivých areálů budovy. Překážka ke vstupu funguje na principu turniketu a je opět na pojena na centrální systém a v případě poruchy umožňuje systém odblokování vstupu.

Posledním typem zabezpečení, jež tvoří řízení kontroly přístupu do budovy jsou bezpečnostní zámky a uzamykací systémy. Uzamykací systémy jsou k dispozici u místností, které jsou označeny jako vysoce rizikové a přístup k nim mají jen konkrétní osoby. Uzamykací systémy představují důmyslný systém s několika zamykacími systémy na dveřích.

7.2.4 Mechanické zábranné systémy

Mechanické zábranné systémy jsou zařízení, které chrání okolí budovy před vstupem. Zábrany tak umožňují nejen zastavovat osoby v budově, ale i navádějí návštěvníky kudy je možné vstoupit do komplexu. Oproti ostatním zabezpečovacím systémům v budovách je pro tato zařízení, že vynikají vyšší odolností proti nárazu, mechanickému poškození apod. Většina z nich je konstruována, tak aby nebylo možné systém poškodit mechanicky. Možnosti, jak mechanické systémy využít v budově jsou velké a společnost je plně využila a můžeme je zařadit do systému nejvyšší ochrany. Tato ochrana se využívá především pro obvodovou ochranu budov a pro zpomalení potencionálního narušitele bezpečnosti. Ve své

podstatě konkrétní systém mechanické zábrany byl vybrán, aby zvýšil fyzickou ochranu a zajistil technickou ochranu. (Burda, 2017)

Bezpečnostní brána

Automatická bezpečnostní brána je určena pro vozidla a osoby a smyslem je neumožnit vstup nežádoucím subjektům. Bezpečnostní brána je vybavena závorou a bez ID karty není možné se dostat do budovy. Respondent ocenil zejména rychlost a vysokou efektivitu vstupní brány. Dále uvedl že fungování závory obsluhuje sofistikovaný systém, který řídí a monitoruje každý pohyb v okolí brány. Dále z rozhovoru vyplynulo, že bezpečnostní brána je nejen efektivní, ale i šetří náklady společnosti. Dalším benefitem je, že vstupní zařízení i odrazuje v noci potenciální narušitele, jelikož je vybavena led světly a je i z delší vzdálenosti viditelná. Neposledním přínosem je i zlepšení logistiky v areálu a průchody, kterých je 6 lze ovládat jen jedinou závorou.

Plotový systém

Bezpečnostní plotový systém je dalším systémem detekce pohybu, který má specifickou konstrukci plotu, který nelze přelézt, rozlomit či naštípnout. (Burda, 2017)Tento plot, který je situován po venkovním obvodu celé budovy je ze silného a kvalitního materiálu, který je obtížné narušit či poškodit. Jelikož je bezpečnost prioritou veřejného sektoru, investoval subjekt do plotového systému vyšší finanční prostředky, a to na základě skutečnosti, že venkovní ochranu považuje za jednu z nejklíčovějších a nejbezpečnějších postupů, jak eliminovat rizikové vniknutí. Konkrétní plotové řešení je navíc vybaveno bezpečnostním zařízením a kamerami, které snadno identifikují a zaznamenají rizikové chování osob. Kamery a detektory dokáží ihned lokalizovat sebemenší pokus o narušení. Z rozhovoru vyplynulo že plotový systém je víceúčelovým prostředkem sloužící k ochraně archivu, vnější fasády budov, zajišťuje stín a chrání datové centrum. Kromě samotného oplocení bylo nejtěžší vymyslet vchody pro zaměstnance. Konečné rozhodnutí reflektovalo náklady a v plotovém systému jsou vybudovány tři vstupy pro zaměstnance pomocí detekce ID kódu. Nevýhodou však je, jak dotazovaný uvedl, že se jedná o důležitou bezpečnostní infrastrukturu, která vyžaduje revizi a údržba zařízení, a především časté kontroly, který je nákladný. Nicméně i přes úskalí a nevýhody ocenil výhodu vyšší bezpečnosti a kvalitu plotového systému.

Bezpečnostní skla

Bezpečnostní skla byly nakoupena jen pro určitou, nejohroženější část budov a konkrétně byly využity v nižších částech budovy k zabránění rozbití skla a vniknutí pachatele do rizikových a ohrožených prostor.

7.3 Zabezpečení pracovních stanic a sítí

Tato kapitola pojednává o tom, jaký je stav zabezpečení sítí v konkrétním podniku, tak aby co nejlépe dokázala čelit kybernetickým útokům, které v dnešním globálním prostředí jsou aktuálním tématem. Správná implementace v podniku účinných opatření v oblasti kybernetické bezpečnosti je dnes obzvláště důležitá, protože útočníci jsou stále inovativnější.

7.3.1 Ochrana proti malware

Ochrana proti malware (škodlivý software) je řešena takovými nástroji, které mají dvě podoby, a to osobní ochrana a ochranné prostředky. Osobní ochrana zahrnuje školení zaměstnanců. Ochrannými prostředky je kvalitní antivirová ochrana, která byla navržena pro konkrétní účely. Ochrana proti malware zahrnuje robustnější způsob ochrany, který má chránit údaje o finančních datech. Finanční ochrana dat je zabezpečena aplikačními nástroji pro správu hesel.

7.3.2 Zálohování

Zálohování dat je dalším nástrojem k ochraně sítí. Zálohovací struktura je oddělena od hlavní infrastruktury, tak aby v případě kybernetického útoků nebyly zničeny či ztraceny nenávratně veškerá data. Aby nedocházelo k nebezpečí v podobě k přístupu k těmto zálohám je přístup posílen více faktorovým ověřením.

7.3.3 Omezení přístupu k internetu

Omezení přístupu k internetu vychází z myšlenky, že veškerá zařízení, která jsou v budově by měla být co nejméně připojena k internetu. Vedoucí pracovníci jsou školeni, aby bylo zajištěno minimálního připojení zařízení k internetu.

7.3.4 Firmware-aktualizace

Firmware jsou využívány zpravidla pro řízení bezdrátového Wi-Fi. Firmware slouží jako nástroj pro snížení pravděpodobnosti kybernetického útoku. Pro správnou funkčnost je

zapnuta automatická aktualizace. Dále jsou prováděny pravidelné opravy zabezpečení. V neposlední řadě jsou systémové sítě chráněny novými, aktuálními antivirovými programy a antimalwerovými opatřeními.

7.3.5 Školení zaměstnanců

Kybernetická bezpečnost tvoří podstatnou úlohu na základě skutečnosti, že ochrana předmětu činnosti subjektu je klíčová. Na základě této skutečnosti je i kybernetická bezpečnost a školení zaměstnanců v popředí zájmů. Témata školení zahrnují širokou škálu oblastí, které a kladou důraz na rozsáhlou škálu zranitelných míst. Smyslem edukačního plánu je naučit osoby, aby sami dokázali rozpoznat sofistikované metody útoků a adekvátně na ně reagovat. Dále je cílem naučit zaměstnance, kteří mají přístup k internetu jak správně a bezpečně navštěvovat webové stránky.

7.4 Čím je veřejná správa napadána

Jak uvádí Jirovský ve své publikaci Kybernetická kriminalita: *Jedním z hlavních důvodu kybernetických útoků je nejčastěji politická motivace a s tím i vzrůstající její propracovanost a složitost.“* (Jirovský, 2007)

Dnes je veřejná správa čím dál více ohrožena častěji než v minulých letech, a to díky faktu, že roste digitalizace veřejné správy a čímž se vynořují nové hrozby kybernetických útoků. Vliv pandemie také zesílil hrozby kyberútoků, jelikož mnoho společností a organizací muselo uzpůsobit svou činnost na dálku a zvýšil se počet pracujících z domova. (Vlada.cz, 2021)

Podle agentury ENISA (Evropská unie pro kybernetickou bezpečnost) v současné době existuje devět hlavních hrozeb:

- *„Ransomware – útočníci šifrují data organizace a za obnovení přístupu vyžadují zaplacení výkupného.*
- *Cryptojacking – kyberzločinci tajně využívají výpočetní výkon oběti ke generování kryptoměny.*
- *Hrozby spojené s osobními daty – narušení/únik dat.*
- *Malware – software, který spouští proces ovlivňující systém.*
- *Dezinformace/zavádějící informace – šíření zavádějících informací.*
- *Neškodné hrozby – lidské chyby a chybná konfigurace systému.*

- *Hrozby v dostupnosti a integritě – útoky, které brání uživatelům systému v přístupu k jejich informacím.*
- *Hrozby pro dodavatelský řetězec – útoky (například na poskytovatele služeb) za účelem získání přístupu k datům zákazníka.“* (Vlada.cz, 2021)

E-goverment se dnes snaží splnit očekávání, která jsou na společnost kladena v podobě přístupnosti informací a dat, transparentnosti a celkově zvýšenému přístupu k veřejným informacím. Tyto trendy však zvyšují problémy se zabezpečením. Právě veřejný sektor dnes digitalizuje procesy a transformuje je do požadované podoby a důsledky těchto aktivit mohou být problematické. Právě vedoucí pracovníci si musí být vědomi důsledků těchto aktivit a měli by být s předstihem připraveni aplikovat maximálně bezpečnou ochranu. (European Commission, 2017)

V roce 2018 byla významně ovlivnila úroveň bezpečnosti informací napříč zeměmi Evropské unie zavedením směrnice Evropské Unie GDBP, které významně omezila přístup k veřejným informacím, které by mohly být zneužity. Ovšem i přes tuto skutečnost jsme svědky útoků na mezinárodní ale i regionální úrovni. Je důležité si uvědomit, že informační bezpečnost dnes ovlivňuje řada faktorů jako je konkurence, regulační tlaky apod.

8 DOTAZNÍKOVÉ ŠETŘENÍ

Cílem empirické části je zjištění skutečné situace prevence a způsobů ochrany ve vybraném podniku. Pro dosažení maximálně relevantních dat byly v praktické části zvoleny dva způsoby provedení analýz:

- Dotazníkové šetření.
- Analýza rizik FMEA.

Dotazník byl koncipována na základě tří tematických okruhů:

- Přístup k informacím.
- Kontrola zabezpečení a odpovědnost.
- IT školení.

Dotazník měl podobu 6 otázek a byl určen pro zaměstnance ve věkové skupině 22-55 let. Dále se vycházelo, že někteří respondenti nemají počítačovou gramotnost a soubor znalostí, schopností zaměřených nejen na ovládání a počítače, ale ani neznají vybavení IT bezpečnosti. Při výběru relevantního vzorků respondentů pro zvolený dotazník byly vybírány kompetentní osoby, které denně užívají programové vybavení společnosti.

Cílem výzkumné části bylo verifikovat znalost a prevenci počítačové kriminality. Výsledky výzkumu byly rovněž zpracovány v grafickém podobě pro maximální přehlednost. Výzkumné šetření probíhalo pomocí online dotazování, které distribuovalo personální oddělení. Účast na výzkumu byla povinná pro zajištění adekvátní návratnosti a validity šetření.

Přístup k informacím

1. Můžete identifikovat data, které jsou citlivé ve Vašem zaměstnání?

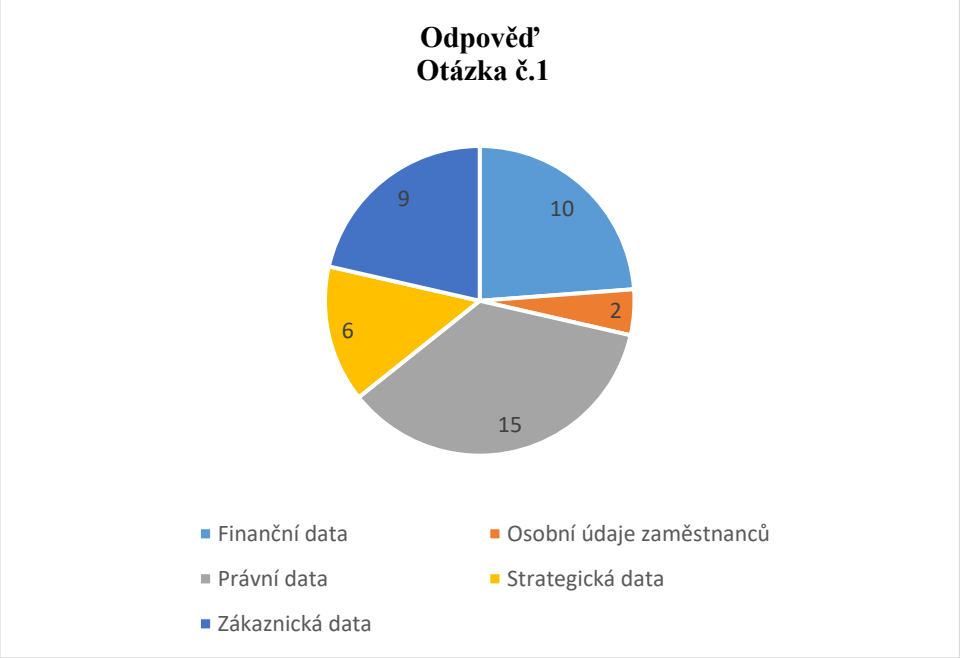
Respondenti interpretovali celkem spolehlivě data, která jsou relativně citlivá. Ovšem někteří respondenti považovali za méně citlivá taková data, která jsou obecně veřejně známé nebo údaje, která nesouvisela s předmětem činnosti podniku. Výčet jednotlivých kategorií dat a jejich specifikace samotnými účastníky výzkumu byl celkem pochopitelný a rozumný. Vesměs byly uváděny odpovědi, kdy citlivost považovali za důležitou v souvislosti s právními, strategickými činnostmi. Jako významné údaje pro společnost vybíraly údaje,

které mají význam pro podnikání jako údaje o zakázkách, zákaznicích, obchodních případech apod.

Tabulka 7 – Identifikace citlivých dat (zpracování vlastní)

Nejcitlivější data ve společnosti	Počet respondentů
Finanční data	10
Osobní údaje zaměstnanců	2
Právní data	15
Strategická data	6
Zákaznická data	9
Celkem	**42**

Dle grafu č.2 respondenti nejčastěji uvedli, právní a finanční data, jako nejcitlivější data ve společnosti. Méně se však shodli nad strategickými a zákaznickými daty, nejméně pro osobní údaje zaměstnanců.



Graf 2 – Identifikace citlivých dat (zpracování vlastní)

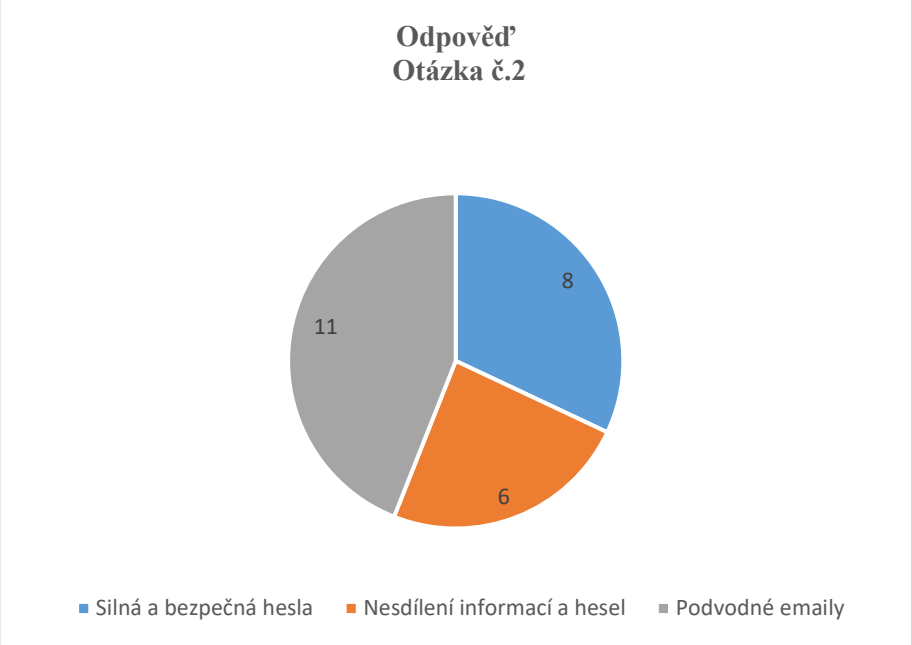
2. Znáte bezpečnostní pravidla pro ochranu údajů ve firmě?

Z velké části odpověděli zaměstnanci, že bezpečnostní pravidla probíhají pomocí nastavení hesel, které v pravidelných intervalech musí měnit a dále v síle hesel, které mají být bezpečná. Další podoba ochrany spočívala dle výsledků otázky v nesdílení informací a hesel a podvodné emaily.

Tabulka 8 – Znalost bezpečnostních pravidel (vlastní zpracování)

Znalost bezpečnostních pravidel	Počet respondentů
Silná a bezpečná hesla	8
Nesdílení informací a hesel	6
Podvodné emaily	11
Celkem	**25**

Dle grafu č.3 většina respondentů uvedla, jako riziko pro ochranu údajů ve firmě podvodné emaily, avšak i přesto, že je zcela nezbytně nutné zásadně dodržovat ochranu hesel a nesdílet informace mimo potřebný okruh subjektů.



Graf 3 – Znalost bezpečnostních pravidel (vlastní zpracování)

Kontrola zabezpečení a odpovědnost

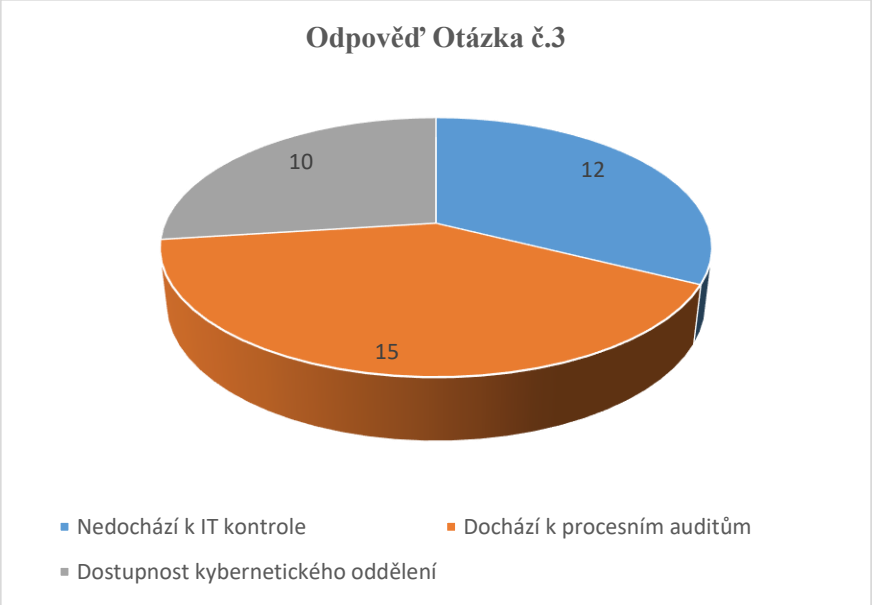
3. Domníváte se, že je dostatečná kontrola bezpečnosti ve firmě?

Reakce na tuto otázku byli poměrně negativní. Výsledkem je, že má personál nízké povědomí o tom, zdali se provádí kontrolu bezpečnosti IT pracovníky. Na druhé straně je velké povědomí o procesních auditech v organizaci. Jako nejčastější kontrolu IT bezpečnosti byla zaznamenána IT infolinka a kontakt na zaměstnance, kteří se zabývají kybernetickou kontrolou. Kybernetické oddělení dle výsledku zjištění slouží k nahlášení incidentů.

Tabulka 9 – IT kontrola bezpečnosti (vlastní zpracování)

IT kontrola bezpečnosti	Počet respondentů
Nedochází k IT kontrole	12
Dochází k procesním auditům	15
Dostupnost kybernetického oddělení	10
Celkem	**37**

Dle grafu č.4, můžeme poukázat na dostupnost informací respondentů v rámci kybernetického oddělení.



Graf 4 – Znalost IT kontroly bezpečnosti (vlastní zpracování)

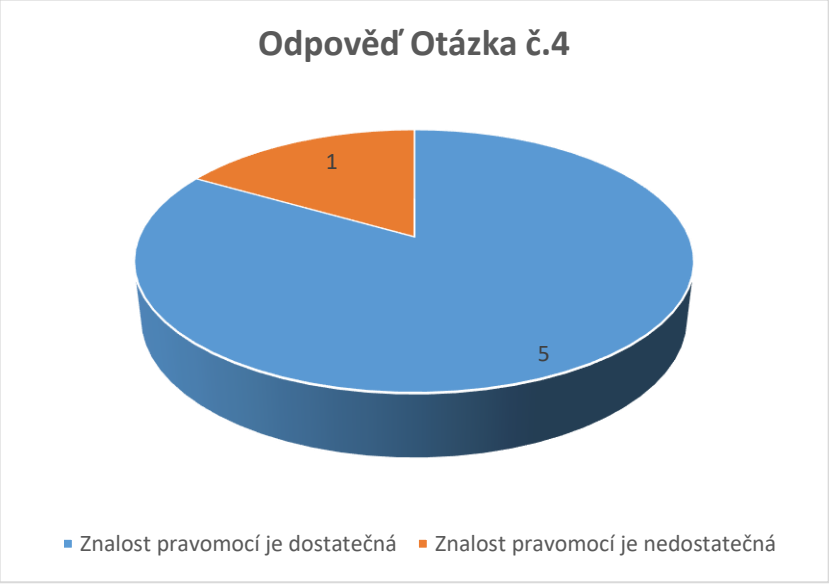
4. Znáte odpovědné osoby za kybernetickou bezpečnost?

Odpovědné osoby za kybernetickou bezpečnost byli spolehlivě identifikovány. Delegace pravomocí a odpovědností za technickou a softwarovou péči je rozdělena vhodně a všichni mají dostatečné informace o kompetencích a odpovědnosti IT oddělení.

Tabulka 10 – Rozdělení pravomocí (vlastní zpracování)

Kompetence a odpovědnost	**Počet respondentů**
Znalost pravomocí je dostatečná	5
Znalost pravomocí je nedostatečná	1
Celkem	**6**

Dle grafu č.5 můžeme poukázat na dostačující znalost respondentů kteří se shodují ve znalosti pravomocí dostatečně. Pouze 1 % respondentů se neshodlo a znalosti pravomocí jim není známá.



Graf 5 – Rozdělení kompetencí (vlastní zpracování)

IT školení

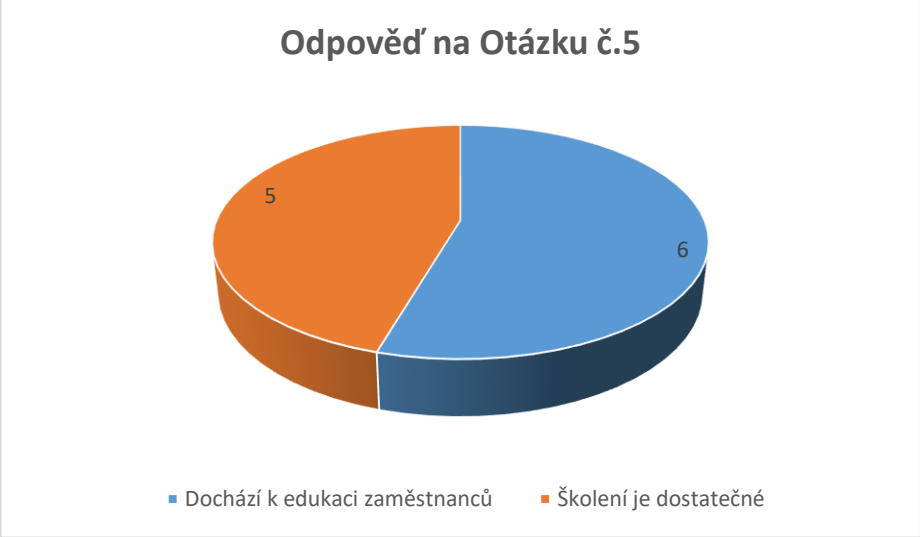
5. Probíhá IT školení bezpečnosti pravidelně ve Vašem zaměstnání?

Školení bezpečnosti je nastaveno na kvartální bázi, které je pro účastníky povinné. Bylo zaznamenáno, že školení je úplné a komplexní a zahrnuje širokou škálu témat a okruhů. Výhodu spatřují osoby především i v online kurzech kybernetické bezpečnosti, kdy účast je povinná a v závěru se ověřují získané poznatky.

Tabulka 11 – Realizace IT školení (vlastní zpracování)

Výukový program bezpečnosti	Počet respondentů
Dochází k edukaci zaměstnanců	6
Školení je dostatečné	5
Školení je nedostatečné	1
Celkem	**12**

Dle grafu č.6 vidíme, jak neadekvátně je nastaveno školení IT bezpečnosti a pro respondenty jsou nutné pravidelné školení kvůli jejím nedostačujícím znalostem.



Graf 6 – Realizace IT školení (vlastní zpracování)

6. Získáte praktické dovednosti v rámci školení?

Školení obsahuje i části na procvičení praktických dovedností, což velice bylo příznivě hodnoceno. Přínosem úkolů s praktickými činnostmi je dle názoru účastníků dotazníkového šetření v tom, že takto koncipovaný trénink jim přinesl řadu nových poznatků a umožnil pochopení bezpečnostních zásad. Dále díky tomuto prvku výuky dokázali pochopit, jak jednotlivé procesy probíhají ve firmě, což je dokáže připravit na kritickou situaci.

Tabulka 12 – Praktická výuka IT bezpečnosti (vlastní zpracování)

Praktické dovednosti v krizových situacích	Počet respondentů
Probíhá praktická výuka	6
Neprobíhá praktická výuka	0
Celkem	**6**

Dle grafu č.7, si můžeme všimnout, že se všichni respondenti se shodli v praktické výuce v krizových situacích ze školení a jsou hodnoceny jako pozitivní přínos.

Graf 7 – Praktická výuka v IT bezpečnosti (vlastní zpracování)

8.1 Návrh opatření

Ve vybraném podniku je kybernetika bezpečnosti významně propracovaná. Na základě výsledků je nutné, aby si podnik uvědomil nebezpečí, která představují především selhání lidského faktoru a neznalost rozsahu citlivých dat. Je samozřejmostí, že žádná společnost dnes nemůže fungovat bez vlastních zaměstnanců, avšak každodenní práce osob s citlivými daty je největším předpokladem pro šíření a přístupu ke kybernetické kriminalitě.

Odpověď č. 1 nám jednoznačně poskytla zjištění, která potvrzují neznalost rozsahu problémových míst. Lidské jednání by mělo být prioritou a hlavním nástrojem budování trvalé bezpečné kultury.

Otázka č. 2 verifikuje skutečnost, že zaměstnanci jsou ostražití a dobře informování, avšak varianta odpovědi *„Nesdílení informací a hesel“* byla zastoupena nejméně. Uskutečněná školení v budoucnu by měla být více posunuta směrem k upevňování ostražitosti. V praktické části školení je vhodné směrovat úkoly k uvědomování si vlastní odpovědnosti zaměstnanců a zvýšit povědomí o únikových místech.

Otázka č. 3 dokládá, že kontrola bezpečnosti je propracována, avšak existují stále nedostatky, které by měly být řešeny. Na variantu odpovědi „*Dostupnost kybernetického oddělení“* kladně odpovědělo nejméně osob a potvrdila nám, že je nutné více posunout zmiňované oddělení do podvědomí lidí napříč všemi pracovními úseky, jelikož včasné nahlášení incidentů a včasný zásah jsou zásadním předpokladem pro boj proti vniknutí do systému.

Otázka č. 5 která měla zjistit přístup ke vzdělávání zaměstnanců můžeme označit realizaci školení jako uspokojivé, avšak byla navržena v rámci této kapitoly vhodná doporučení v oblasti koncepce výukových programů.

Otázka č. 6 jednoznačně potvrdila aplikaci praktické výuky. Doporučení, jež mohou v oblasti školení být navržena je více reálné úkoly zaměřovat na odpovědnost zaměstnanců a nastínění rozsahu škod, které mohou způsobit.

V závěru můžeme zhodnotit, že faktem činností související s kybernetickou bezpečností tvoří informace (o povaze či četnosti kybernetických bezpečnostních incidentů, o možných příštích útocích, o trvání potencionálních zranitelností). Tyto informace by měli být z hlediska kybernetické bezpečnosti prioritou pro zaměstnance daného subjektu, a jejich

strohé znalosti by měli být doplněny a neustále obnovovány. V subjektu musí být dodrženy kroky s principy publicity a přehledností informacemi, ale zároveň musí některé informace chránit, aby nedošlo k jakémukoliv ohrožení uvnitř. Zmírnění rizik kybernetické bezpečnosti, v organizaci je náročné, avšak při menší snaze mít kontrolu nad znalostmi a chováním zaměstnanců či zabezpečením zařízení může vést ke zlepšení. Efektivní přístup musí zahrnovat celou IT infrastrukturu a musí být založen na pravidelném hodnocení rizik. Dalším efektivním řízení kybernetické bezpečnosti musí vycházet z vrcholu organizace. Masivní kultura kybernetické bezpečnosti, posílena pravidelnými školeními, zajistí, že každý zaměstnanec uzná bezpečnost jako svou odpovědnost a instinktivně se za ní staví. Dobré zabezpečení a efektivní pracovní postupy musí jít ruku v ruce. Zabezpečení sítě je taktéž velice důležité a zahrnuje řešení omezení zranitelnosti operačních systému, síťovou architekturu, včetně serverů a hostitelů, firewallů a bezdrátových přístupových bodů a síťových protokolů. Pomoci může i zabezpečení takzvané *„Internet of Thnigs“* to zahrnuje zabezpečení chytrých zařízení a sítí připojených k internetu věcí. Mezi tyto zařízení, které se připojují k internetu bez lidského zásahu jsou:

- Chytré požární hlásiče.
- Světla.
- Termostaty.
- Zabezpečovací systémy.
- Dveřní systémy.
- Přístupové systémy.

V rámci osobní návštěvy v subjektu veřejné správy bych doporučila školení na „*plánování reakce na incidenty“*. Kybernetické útoky a únik dat jsou nevyhnutelné, takže rychlost, kterou na porušení reaguje, je kritická. Kyberzločincům stačí najít pouze jednu slabinu, aby mohli proniknout do systémů, takže je nezbytné být připraveni, když dojde k narušení.

9 ANALÝZA RIZIK FAILTURE MODE AND EFFECT ANALYSE (FMEA)

Analýza režimu a možnosti selhání je technikou, která prolíná na rozdíl od ostatních technik aspekty zabezpečení. FMEA je metodou příčin-následků. Prostřednictvím analýzy Failture Mode and effect analyse (FMEA) je využíváno znalostí a zkušeností expertů, kteří společně aplikují tuto metodu v týmu. Podstatou je vytvoření týmu pracovníků, kteří se nejvíce podílejí na přidané hodnotě v podniku a všemi osobami, které jsou nositeli informací. Takto koncipovány tým z pracovníků by měl být veden zkušeným moderátorem, který řídí a moderuje daný tým. Samozřejmostí je, že tým by měl být sestaven z osob, které jsou nejblíže dané problematice, která se vyhodnocuje. Tým by měl pravidelně vyhodnocovat jednotlivé kroky, postupy a závěry, tak aby se došlo k požadovanému výsledku. (Franke, 1993)

Výsledky dílčích závěrů se zaznamenávají do formuláře, kde jsou jednotlivé položky detailně popsány. Tento postup a koncept analýzy FMEA je jen ilustrativní a každý podnik si může způsob provedení analýzy FMEA uzpůsobit jejím konkrétním potřebám. (Plura, 2001)

9.1 Identifikace aktiv

Tato kapitola se zabývá identifikací aktiv vybraného subjektu. V rámci řízení bezpečnosti je nezbytné nejprve identifikovat dílčí aktiva ve společnosti a uvést odpovědné osoby za jejich správu a péči. Identifikace aktiv je jedním z kroků a postupů analýzy rizik. Společnost by měla posuzovat aktiva na základě jejich hodnoty a měl by být proveden soupis s uvedením a vyčíslením hodnoty majetku. Hodnota majetku by měla být posuzována v souvislosti s dopadem na bezpečnost při ztrátě či zničení. Dále je důležité hodnotit dané aktivum z pohledu jedinečnosti, dostupnosti a nahraditelnosti.

Pojem aktivum si zjednodušeně můžeme představit jako něco co je pro objekt hodnotné a cenné. Toto aktivum se právě může zmenšovat působením rizika.

Při hodnocení aktiva bychom měli zohlednit tyto hlediska:

- Veškeré náklady spojené s nákupem a pořízením daného aktiva.
- Význam aktiva pro samotný subjekt (vliv na existenci a dopad na změny chování).

- Náklady spojené s odstraněním škod ze ztráty aktiva.
- Doba odstranění škod.
- Specifická hlediska, která jsou typická pro konkrétní aktivum. (Smejkal a Rais, 2013)

Vyjadřuje vše, co má pro objekt hodnotu, která se zmenšuje působením hrozby. Aktiva můžeme dělit na hmotná (movitá), nehmotná a nemovitá. Aktivum může být ale také sám subjekt, protože na celou jeho existenci může působit hrozba.

Při hodnocení aktiva bereme v potaz především tato hlediska:

- *Pořizovací náklady či jiná hodnota aktiva.*
- *Důležitost aktiva pro existenci či chování subjektu.*
- *Náklady na překlenutí případné škody na aktivu.*
- *Rychlost odstranění případné škody na aktivu.*
- *Jiná hlediska (mohou být specifická případ od případu).* (Smejkal a Rais, 2013)

Aktiva můžeme členit na základě základních charakteristik na hmotná a nehmotná, primární a podpůrná. Hmotná aktiva zahrnují taková aktiva, na které si lze fyzicky sáhnout, oproti tomu nehmotná aktiva jsou například duševní vlastnictví, know-how. Na straně primárních aktiv identifikujeme základní obchodní činnosti a procesy. Podpůrná aktiva souvisí s primárními aktivy a slouží k zajištění primárních aktiv. Neméně podstatnou charakteristikou aktiva je pak klasifikace aktiv na základě hodnoty, kterou lze vyjádřit jako subjektivní a objektivní hodnotu mnoha způsoby. Objektivní hodnocení je takové hodnocení, které vychází ve finančním ohodnocení, subjektivní hodnota vychází z vlastní hodnoty, která je pro každého jedinečná a subjektivní. (Smejkal, 2015)

9.1.1 Primární aktiva

Primární aktiva zahrnují především informace, které v případě narušení či odcizeny společnost nemůže splnit své poslání. Dalšími primárními aktivy jsou přístupy k finančním prostředkům a informacím o bankovních účtech. Zneužití či odcizení údajů patří bezesporu mezi významné hrozby společnosti.

Podnikové informace

Mezi zásadní podnikové informace můžeme zařadit údaje o dotacích, dotační tituly, evidence dotací, cenové nabídky. Dalšími zásadními informacemi o výběrech poplatků, kde jsou důležité informace o pohybu komodit a záznamy z dohledu nad ním. Jelikož se veškeré informace týkají státního rozpočtu byla bych jejich ztráta fatální.

9.1.2 Podpůrná aktiva

Podpůrná aktiva, jak již bylo zmíněno výše slouží k zabezpečení primárních aktiv. Podpůrná aktiva hrají podstatnou roli, jelikož odcizení konkrétních aktiv by také významně narušilo průběh činnosti.

Hardware

Počítači disponují téměř všichni zaměstnanci. K ochraně dochází prostřednictvím dvoufázové ho zabezpečení, a to pomocí vstupního hesla a vyplnění hesla, který identifikuje počítač. Toto heslo je potřeba zadat před samotným přihlášením do systému.

Software

Přístup k softwaru je opět zabezpečen heslem. Operační systém je zálohován a správu zajišťuje IT oddělení. Software je provozován jednak pomocí lokální sítě a také pomocí sítě na dálku u zaměstnanců pracujících z domova. Síť na dálku je zabezpečena pomocí VPN.

Mobilní telefony

Někteří zaměstnanci vlastní mobilní telefony, kde uchovávají informace, které nejsou citlivé, ale i přes tuto skutečnost jsou zaměstnanci vybaveni telefony, které jsou přístupné jen po otisku prstu.

Automobily

Společnost vlastní několik automobilů, které jsou parkována na firemním parkovišti. Možnost zapůjčení vozů pro soukromé účely není možné a vozidla jsou pojištěna.

Dokumenty

Dokumenty v papírové formě jsou uzamčeny ve skříních, od kterých mají klíče jen určité osoby. Veškeré dokumenty se skenují a ukládají do počítače na externí uložiště a lokální uložiště.

Server

Server je umístěn v místnosti, ke které má přístup jen skupina vybraných pracovníků. Dále je nad serverovnou umístěna kamera a je zvýšená fyzická ochrana této místnosti.

Veškerá aktiva jsou průběžně inventarizována, a to na čtvrtletní a roční bázi. Členové inventarizační komise jsou pravidelně obměňovány. Po každé inventuře je vyhotoven inventární protokol a vyčísleny případné rozdíly, ztráty, manka a škody.

9.2 Identifikace hrozeb

Identifikace hrozeb v této kapitole slouží k definování hlavních rizikových faktorů, které můžou ovlivnit či narušit průběh činnosti podniku. Smyslem je daná rizika kvantifikovat dle interních a externích faktorů, a to na základě skutečnosti, že některé hrozby může společnost ovlivnit, která nejčastěji mají podobu interních rizik a na taková, která ovlivnit nemůže, ale znalost těchto potenciálních hrozeb umožní podniku dostatečně se připravit na tyto podněty zvenčí. Dále je důležité dané hrozby klasifikovat podle účinku jejich dopadu, společnost může v případě nižšího dopadu dané riziko podstoupit, v opačném případě, kdy nastane situace, kdy riziko významně ovlivní aktivity v podniku je nutné dané riziko odvrátit.

9.2.1 Interní hrozby

Lidé – zaměstnanci představují významné ohrožení. I přes fakt, že výběr zaměstnanců probíhá na základě propracované výběrového řízení, kde se ověřuje minulost a trestní rejstřík osob nadále firma považuje své zaměstnance za významný rizikový potenciál.

Jak konkrétně mohu zaměstnanci ovlivnit rizika pro organizaci jsou následující:

- Lidská chyba zaměstnanců – to zahrnuje neúmyslné odeslání citlivých informací nebo osobních údajů nesprávnému příjemci. Kromě toho existuje problém chybné konfigurace systému, kde citlivé informace nejsou řádně zabezpečeny, šifrovány nebo chráněny heslem, což může vést k neoprávněnému přístupu.
- Nepoctiví zaměstnanci – jedná se o nepoctivé jednání, kdy mohou zaměstnanci vyzradit přístupové údaje, citlivé informace, poškodit hardware, nasazení škodlivého malware, zneužití informací o dotacích.

Technické zařízení

IT infrastruktura je vysoce hodnotný cíl. Riziko pro provoz, a především integritu dat, které může být způsobeno narušením je vážné a způsobí vysoké ztráty z hlediska času, finančních výdajů a v neposlední řadě poškozuje dobré jméno společnosti a důvěru občanů. Následné narušení provozu může vést ke zpoždění při poskytování služeb pro organizaci, zpomalení průběhu výběru poplatků apod.

Technické zařízení může být poškozeno z těchto důvodů: nesprávným zacházením, špatnou správnou hardware apod.

Fyzická krádež dat

Fyzická krádež dat může vzniknout nepozorností zaměstnanců, kteří nezabezpečí v době nepřítomnosti svůj počítač. Dalším rizikem je vzdálený přístup zaměstnanců, kdy kontrola zabezpečení počítačů v době nepřítomnosti je zvýšená. Také může dojít k odcizení notebooků, mobilních telefonů a USB. Notebooky jsou šifrovány a odstraňuje se tímto možnost snadnému přístupu lupiči k údajům a jejich zneužití. Zaměstnanci pracující z prostředí domova mají povinnost odcizení neprodleně nahlásit.

Absence bezpečnostní pravidel

Absence bezpečnostních pravidel jsou významným faktorem a potenciálem, jelikož zpravidla je cílem kybernetických útoků samotný uživatel. Absence bezpečnostních pravidel může být vysoká především u managementu firmy, jelikož disponují důležitými přístupy, které vyžadují nejvyšší zabezpečení. Také je podstatné vzdělání a školení zaměstnanců, a to nejen všech zaměstnanců, ale především pracovníků z IT oddělení. Pracovníci, kteří spravují sítě a starají se o hardware a mají nedostatečné znalosti a zkušenosti mohou představovat významný, rizikový potenciál pro společnost. Neznalost bezpečnostní pravidel je jedna z možných způsobů narušení pravidel, dalším způsobem je, že zaměstnanci znají směrnice a jsou proškoleni v oblasti IT bezpečnosti, ale odmítají vědomě tyto restrikce a přístupy dodržovat. Jeden z dalších způsobů, který absenci bezpečnostních pravidel způsobuje je, že tyto pravidla jsou propracovány na nízké úrovni či jsou nevhodně aplikovány a nejsou striktně kontrolovány. Bezpečnostní školení mohou také být prezentována nesrozumitelně a neadekvátně, či se věnují hlavním hrozbám jen okrajově a jsou nedostatečná.

9.2.2 Externí hrozby

Regulační riziko

Regulační riziko spočívá v nedostatečné znalosti uchovávání citlivých údajů v souvislosti se zpracováním údajů o dotačních titulech a průbězích výběrů poplatků.

Požár

Požár může značně poškodit či zpomalit činnosti, které jsou podstatné pro zajištění činností, které vyplívají ze zákona a orgán veřejné správy je povinen tyto činnosti vykonávat. Požár může vzniknout na základě těchto skutečností:

- Kouření zaměstnanců.

- Nesprávné zacházení s elektrickými spotřebiči v prostorách budovy.
- Úmyslně založený požár zvenčí.
- Únik pohonných hmot z automobilů na parkovišti a v suterénu budovy.

9.3 Sestavení týmu

Před samotným sestavení týmu, jež představuje první krok analýzy FMEA bylo složení týmu diskutováno s ředitelem IT oddělení. Cílem bylo sestavit relevantní tým, který může snadno ovlivnit faktory rizika. V následné analýze kybernetické bezpečnosti bylo stanoveno postupovat napříč jednotlivými odděleními tak, abychom byli schopni identifikovat a odhalit zásadní problémy, které mohou nastat při běžném provozu. Tým se tedy zabýval IT řešením, ale zároveň sestával i z osob na vedoucí pracovní pozici, kteří mají dostatečný přehled o aktivitách podřízených a dokáží identifikovat přesně činnosti na svěřených pracovištích. Vzájemnou interakci a komunikaci mezi týmy zastřešoval ředitel IT oddělení. Celkem byly sestaveny čtyři tým k provádění analýzy.

9.4 Sestavení hodnotící stupnic

Hodnotící stupnice slouží k ohodnocení závažnosti rizika, a především je nástrojem, který má usnadnit odhalení vad a potenciálních hrozeb. Hodnocení poruch a vad nevycházelo jen na základě tabulky s hodnotícími kritérii, ale zároveň byl reflektován individuální názor každého z členu týmu pro zajištění maximální efektivnosti. Jako podklad pro hodnocení byly sestaveny 3 tabulky kritérií. Jako RZ rizikové číslo bylo stanoveno 120.

Tabulka 13 – Pravděpodobnost výskytu (vlastní zpracování)

Význam	Charakteristika	Hodnocení
Velmi vysoký	Vada je velmi závažná a má nízkou kontrolu.	9-10
Vysoký	Vada se může vyskytovat opakovaně, vady jsou pod kontrolou.	8
Průměrný	Vady se vyskytují v menším rozsahu a nepravidelně, existuje kontrola.	6-7
Malý	Vady jsou ojedinělé a v malém rozsahu, monitoring procesů.	3-5
Velmi malý	Rizika a vady jsou téměř nepravděpodobné, existuje pravidelná kontrola.	1-2

Tabulka 14 – Význam dopadu rizika (vlastní zpracování)

Význam -	Charakteristika	Hodnocení
Vysoce závažný	Napadení má velký dopad na procesy a může způsobit závažné ohrožení a negativně ovlivnit výsledky.	9-10
Velmi závažný	Způsobuje nemožnost využívat systém/ohrožení je vysoké.	8
Středně závažný	Některé činnosti budou ohroženy a výsledky budou ovlivněny jen zčásti.	6-4
Málo závažný	Procesy budou ovlivněny jen z malé části.	3
Nezávažný	Riziko nemá dopad na činnost podniku.	1-2

Tabulka 15 – Odhalení rizika (vlastní zpracování)

Význam -	Charakteristika	Hodnocení
Vysoce pravděpodobné	Potenciální riziko nelze vůbec odhalit a dokáže způsobit fatální následky.	10
Velmi pravděpodobné	Potenciální riziko lze odhalit minimálně a dokáže způsobit fatální následky.	9
Středně pravděpodobné	Potenciální riziko je možné pravděpodobně odhalit a následky jsou středně závažné.	8
Téměř pravděpodobné	Potenciální riziko je lze odhalit velmi často a následky nejsou závažné.	7-4
Nepravděpodobné	Potenciální riziko se objeví samo bez nutnosti zásahu.	3-1

9.5 FMEA

Původ poruchy	Potenciální vada	Potenciální následky vady	Následky vady	FF	Odpovědná osoba	Opatření	Význam dopadu rizika (1-10)	Pravděpodobnost výskytu (1-10)	Odhalení rizika (1-10)	Hodnocení RZ
Kdo/ co je původcem poruchy?	**Jakými způsoby může vada uškodit?**	**Jaký je dopad na společnost, když nebudou provedeny preventivní kroky?**	**Jak se projeví vady?**	**Frekvence výskytu v průběhu roku?**	**Kdo je odpovědný za odstranění problému?**	**Jaká budou provedena preventivní opatření?**				
Úmyslné zavinění zaměstnanců	Zneužití informací a dat	Soudní spor – poškození třetích stran	Odcizení finančních prostředků, zneužití informací třetích stran	1	IT ředitel oddělení	Vyšší zabezpečení přístupů k citlivým datům	10	1	3	30
	Odcizení hardware	Soudní spor-poškození třetích stran	Nabourání se do systému a krádež informací	3	Vedoucí pracovníci oddělení	Inventarizace	9	3	5	135
	Phisnihg	Poškození dobrého jména společnosti, přerušení činnosti, finanční ztráta	Ztráta hesel, přístup k bankovním účtům	4	IT oddělení	Trénování uživatelů	7	1	1	7
	Social engineering	Soudní spor-finanční náhrada poškozené osobě	Shromáždění údajů o určité osobě	3	IT ředitel oddělení	Oddělení citlivých informací, konzultace	9	4	3	108

Původ poruchy	Potenciální vada	Potenciální následky vady	Následky vady	FF	Odpovědná osoba	Opatření	**Význam dopadu rizika (1-10)**	**Pravděpodobnost výskytu (1-10)**	**Odhalení rizika (1-10)**	**Hodnocení RZ**
Kdo/ co je původcem poruchy?	**Jakými způsoby může vada uškodit?**	**Jaký je dopad na společnost, když nebudou provedeny preventivní kroky?**	**Jak se projeví vady?**	**Frekvence výskytu v průběhu roku?**	**Kdo je odpovědný za odstranění problému?**	**Jaká budou provedena preventivní opatření?**				
Úmyslné zavinění zaměstnanců	Malware	Nepovolené výběry finančních prostředků	Zneužití přístupových práv, citlivých informací	2	IT ředitel oddělení	Vyšší zabezpečení přístupů k citlivým datům	8	4	6	192
	Ransomware	Kryptové vydírání, soudní spor	Šifrování dat oběti	3	Vedoucí pracovníci oddělení	Aktualizace antivirového programu	7	2	6	84
	Neautorizovaný přístup k dotacím	Poškození dobrého jména společnosti, finanční ztráta, soudní spor	Zveřejnění citlivých informací	2	IT oddělení/Vedoucí pracovníci oddělení	Školení zaměstnanců	4	2	1	8
	Odposlouchávání	Finanční ztráta	Detekce informací při přenosu v síti, získání hesel	1	IT ředitel oddělení	Školení zaměstnanců	6	2	4	48

Původ poruchy	Potenciální vada	Potenciální následky vady	Následky vady	FF	Odpovědná osoba	Opatření	Význam dopadu rizika (1-10)	Pravděpodobnost výskytu (1-10)	Odhalení rizika (1-10)	Hodnocení RZ
Kdo/ co je původcem poruchy?	**Jakými způsoby může vada uškodit?**	**Jaký je dopad na společnost, když nebudou provedeny preventivní kroky?**	**Jak se projeví vady?**	**Frekvence výskytu v průběhu roku?**	**Kdo je odpovědný za odstranění problému?**	**Jaká budou provedena preventivní opatření?**				
Neúmyslné zavinění zaměstnanci	Krádež hardware	Poškození činnosti podniku	Únik informací	4	Vedoucí pracovníci oddělení/HR-školení zaměstnanců	Školení zaměstnanců	7	10	2	140
	Nedodržování pravidel	Přerušení činnosti podniku	Únik informací, ztráta dat, poškození hardware	6	Vedoucí pracovníci oddělení	Kontrola vedoucími pracovníky	8	8	2	128
	Instalace vlastních software do PC	Ztráta důvěry třetích stran, poškození dobrého jména	Kybernetický útok, detekce citlivých údajů	10	IT oddělení/Vedoucí pracovníci oddělení	Školení zaměstnanců	6	6	3	108
	Poskytnutí přístupových hesel kolegům	Finanční ztráta, poškození dobrého jména společnosti	Kybernetický útok, detekce citlivých údajů	2	Vedoucí pracovníci/HR-školení	Školení zaměstnanců/Stanovení odpovědnosti	6	1	4	24

Původ poruchy	Potenciální vada	Potenciální následky vady	Následky vady	FF	Odpovědná osoba	Opatření	**Význam dopadu rizika (1-10)**	**Pravděpodobnost výskytu (1-10)**	**Odhalení rizika (1-10)**	**Hodnocení RZ**
Kdo/ co je původcem poruchy?	**Jakými způsoby může vada uškodit?**	**Jaký je dopad na společnost, když nebudou provedeny preventivní kroky?**	**Jak se projeví vady?**	**Frekvence výskytu v průběhu roku?**	**Kdo je odpovědný za odstranění problému?**	**Jaká budou provedena preventivní opatření?**				
Technické riziko	Nevhodný antivirový program	Poškození činnosti podniku	Zneužití informací	2	IT oddělení	Školení IT zaměstnanců	8	2	3	48
	Selhání hardware	Zpomalení činnosti v podniku	Ztráta přístupu k informacím	7	IT oddělení	Pravidelná revize zařízení	7	6	2	84
	Chybné fungování zařízení	Zpomalení činnosti v podniku	Ztráta přístupu k informacím	6	IT oddělení	Pravidelná revize zařízení/analýza nákupu IT techniky	6	6	3	108
	Nedostatečný servis	Zpomalení činnosti v podniku	Ztráta přístupu k informacím	3	IT oddělení	Školení zaměstnanců/Výběr externí firmy	7	2	3	42

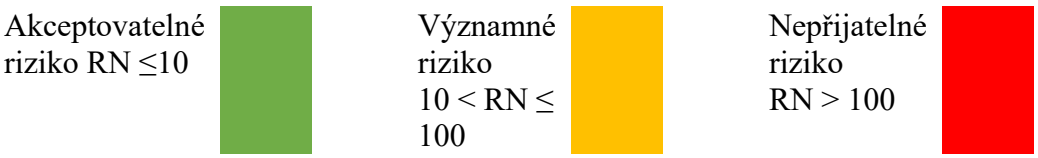
Původ poruchy	Potenciální vada	Potenciální následky vady	Následky vady	FF	Odpovědná osoba	Opatření	**Význam dopadu rizika (1-10)**	**Pravděpodobnost výskytu (1-10)**	**Odhalení rizika (1-10)**	**Hodnocení RZ**
Kdo/ co je původcem poruchy?	**Jakými způsoby může vada uškodit?**	**Jaký je dopad na společnost, když nebudou provedeny preventivní kroky?**	**Jak se projeví vady?**	**Frekvence výskytu v průběhu roku?**	**Kdo je odpovědný za odstranění problému?**	**Jaká budou provedena preventivní opatření?**				
Požár	Nesprávné zacházení s elektrickými spotřebiči	Poškození činnosti podniku	Ztráta techniky, software	2	HR/BOZP ochrana	Školení zaměstnanců/kontrola	8	4	3	96
	Úmyslně založený požár	Poškození činnosti podniku	Ztráta techniky, software	1	Ochranka	Zvýšení počtu protipožárních opatření	8	1	3	24
	Kouření zaměstnanců	Poškození činnosti podniku	Ztráta techniky, software	6	HR/BOZP ochrana	Penalizace	8	5	3	120
	Problémy s PHM v parkovacím areálu	Poškození činnosti podniku	Ztráta techniky, software	3	HR/BOZP ochrana	Školení zaměstnanců	8	2	3	48

Původ poruchy	Potenciální vada	Potenciální následky vady	Následky vady	FF	Odpovědná osoba	Opatření	**Význam dopadu rizika (1-10)**	**Pravděpodobnost výskytu (1-10)**	**Odhalení rizika (1-10)**	**Hodnocení RZ**
Kdo/ co je původcem poruchy?	**Jakými způsoby může vada uškodit?**	**Jaký je dopad na společnost, když nebudou provedeny preventivní kroky?**	**Jak se projeví vady?**	**Frekvence výskytu v průběhu roku?**	**Kdo je odpovědný za odstranění problému?**	**Jaká budou provedena preventivní opatření?**				
Absence bezpečnostních pravidel	Narušování pravidel	Soudní spor, poškození jména společnosti, finanční ztráty	Riziko kybernetického útoku	4	IT ředitel oddělení	Sankce	6	7	4	168
	Nedostatečné IT školení	Soudní spor, poškození jména společnosti, finanční ztráty	Riziko kybernetického útoku	2	IT ředitel oddělení	Plán školení-HR oddělení	4	3	4	48
	Nevhodná koncepce školení	Soudní spor, poškození jména společnosti, finanční ztráty	Riziko kybernetického útoku	1	IT ředitel oddělení	Plán školení-HR odděleními oddělení	4	1	1	4
	Neposkytnutí zpětné vazby/ověření znalostí	Soudní spor, poškození jména společnosti, finanční ztráty	Riziko kybernetického útoku	3	IT ředitel oddělení	Plán školení-HR oddělení	2	1	1	2

Původ poruchy	Potenciální vada	Potenciální následky vady	Následky vady	FF	Odpovědná osoba	Opatření	**Význam dopadu rizika (1-10)**	**Pravděpodobnost výskytu (1-10)**	**Odhalení rizika (1-10)**	**Hodnocení RZ**
Kdo/ co je původcem poruchy?	**Jakými způsoby může vada uškodit?**	**Jaký je dopad na společnost, když nebudou provedeny preventivní kroky?**	**Jak se projeví vady?**	**Frekvence výskytu v průběhu roku?**	**Kdo je odpovědný za odstranění problému?**	**Jaká budou provedena preventivní opatření?**				
Regulace	Neznalost IT norem	Poškozený pověsti firmy	Možnost kybernetického útoku	3	IT ředitel oddělení	Plán školení-HR oddělení	4	6	4	96
	Zveřejňování nepovolených informací	Poškozený pověsti firmy	Možnost kybernetického útoku	1	IT ředitel oddělení	Plán školení-HR oddělení	4	4	4	64
	Neznalost likvidace hardware	Poškozený pověsti firmy	Únik informací	3	IT ředitel oddělení	Plán školení-HR oddělení	2	1	1	2
	Neznalost mezinárodních standardů	Poškozený pověsti firmy	Globální únik informací	3	IT ředitel oddělení	Plán školení-HR oddělení	2	1	1	2

9.6 Vyhodnocení analýzy

Výsledky analýzy jsou shrnuty v následující tabulce a hodnoceny na základě tří kritérii viz. Kapitola 8.4. Jednotlivá rizika jsou řazena od nejzávažnějších (červená barva), středně závažné (žlutá barva) a nejméně závažné (modrá barva).



Tabulka 16 – Vyhodnocení analýzy FMEA (vlastní zpracování)

Původ poruchy	Potenciální vada	Hodnocení RZ
Úmyslné zavinění zaměstnanců	Malware	192
	Ransomware	84
	Neautorizovaný přístup k dotacím	8
	Odposlouchávání	48
Neúmyslné zavinění zaměstnanci	Krádež hardware	140
	Nedodržování pravidel	128
	Instalace vlastních software do PC	36
	Poskytnutí přístupových hesel kolegům	24

Technické riziko	Nevhodný antivirový program	48
	Selhání hardware	84
	Chybné fungování zařízení	36
	Nedostatečný servis	42
Požár	Nesprávné zacházení s elektrickými spotřebiči	96
	Úmyslně založený požár	24
	Kouření zaměstnanců	120
	Problémy s PHM v parkovacím areálu	48
Absence bezpečnostních pravidel	Narušování pravidel	168
	Nedostatečné IT školení	48
	Nevhodná koncepce školení	4
	Neposkytnutí zpětné vazby/ověření znalostí	2
Regulace	Neznalost IT norem	96
	Zveřejňování nepovolených informací	64
	Neznalost likvidace hardware	2
	Neznalost mezinárodních standardů	2

9.7 Návrh opatření

Na základě provedené analýzy byla vypočtená jako nejrizikovější hrozba subjektu úmyslné zavinění zaměstnanců, hodnota rizikového faktoru činila RZ 192. Šíření malware, které probíhá nejčastěji prostřednictvím sítě internetu. Nejrozšířenějším a oblíbeným je šíření

malwaru e-mailem s bezpečně se tvářící přílohou, nebo ukrytí malwaru do navštěvovaných internetových stránek, programů a her.

Jako preventivní opatření byly přijaty a navrženy tyto kroky:

- Automaticky pravidelné zálohovaní potřebných dat na firemní zabezpečenou sít.
- Časový limit pro přístupové hesla, která se musí v určitých intervalech měnit a nesmí se opakovat.
- Přísný zákaz zaměstnanců otevíraní neověřených adres, odkazů a webových stránek.
- Instalaci potřebných aplikaci ve firemních zařízení může provádět jen zaměstnanec z oddělení IT.

Při správném dodržení těchto zásad je šance zmenšení nakazí malwarem výrazně nižší. Druhým nejzásadnějším problémem s hodnotou RZ 168 představovalo porušování a absence pravidel zásad bezpečného zacházení s technikou.

Jako preventivní opatření byly přijaty a navrženy tyto kroky:

- Přísnější a složitější školení řidičů, referentů, které je součásti pravidelného školení BOZP.
- Zavedeny finanční postihy za nedodržování zásad BOZP.

Při správné motivaci zaměstnanců můžeme eliminovat absenci a porušování pravidel. Třetím nejrizikovějším faktorem s hodnotou RZ 140 je neúmyslné zavinění zaměstnanci-krádež hardware, tady může jít často o součinnost externího a interního pachatele i nevědomě ze strany některého zaměstnance napadeného subjektu.

Jako preventivní opatření byly přijaty a navrženy tyto kroky:

- Instalace vhodného softwaru pro sledovaní samostatného zařízení.
- Doplnění možnosti vzdáleného přístupu k datům a možnosti vzdáleného mazání.
- Bez hlavního zadání hesla v zařízení nemožnost uvedení do továrního stavu.
- Vyšší zabezpečení k citlivým datům a aktualizace zabezpečení.
- Krádež hardware v případě vzdáleného přístupu – zvýšit školení zaměstnanců v oblasti správy svěřeného majetku a přijetí odpovědnosti.

Poslední oblastí s nedostatečnou ochranou bylo kouření zaměstnanců na pracovišti. Jako preventivní opatření byly přijaty a navrženy tyto kroky:

- Kouření zaměstnanců na pracovišti-finanční postihy.
- Zákaz kouření v celém areálu a v okolí areálu.

Dále bylo doporučeno komplexně zvýšit školení napříč všemi pozicemi a kontrolovat dodržování předpisů, včetně možných postihů za úmyslné nedodržování postupů.

Nejméně závažnými oblastmi byli tyto:

- Absence bezpečnostní pravidel (RZ 2 neposkytnutí zpětné vazby/ověření znalostí z absolvovaného edukačního kurzu RZ 4 nevhodná koncepce školení.
- RZ2 – neznalost mezinárodních standardů, neznalost likvidace hardware).

Tyto rizika byly označeny jako bezvýznamná, zanedbatelná rizika se souhlasem vedení společnosti. Byli zváženy náklady na řešení a v závěru bylo rozhodnuto provést technická a jiná opatření ke snížení dopadu na podnikatelský subjekt. Zpravidla však vhodná opatření budou realizována především v případě, že v rámci rozpočtu budou dostupné zdroje. Nejčetnějšími oblastmi rizik byly mírné a střední rizika, které byly klasifikovány jako méně významná rizika.

Nejvíce byla identifikována:

- Technická rizika.
- Úmyslná zavinění zaměstnanců.
- Požár.
- Regulace.

Identifikované zdroje nebezpečí budou aktivně eliminována.

ZÁVĚR

Cílem této písemné diplomové práce byla identifikovat rizika kybernetického útoku na vybraný veřejný sektor a nastínit dopad možnost úniku informací. Během práce byl zájem obírat se mimo jiné i o specifické kybernetické zájmy v orgánu veřejné správy.

Diplomová práce je rozdělena na teoretickou a praktickou část. V teoretické části jsou popsány teoretické poznatky nutné pro pochopení daného tématu, dostupné zdroje a podklady, které se zabývají kybernetickou bezpečností.

Empirická část obsahuje dvě analýzy pro zajištění maximálního prověření dané situace a identifikaci předpokladů počítačové kriminality.

Analýza FMEA byla zaměřena na specifikaci kybernetických hrozeb, a to v členění na interní hrozby (ovlivnitelné) a externí (neovlivnitelné). Interní hrozby, které byly stanoveny představovaly: úmyslné a neúmyslné selhání zaměstnanců, selhání techniky, absence bezpečnostních pravidel a fyzická krádež. Analýza FMEA potvrdila předpoklad domněnky největšího rizika lidského faktoru, které mohou být činitelem ke spuštění kybernetických hrozeb. Externí faktory zahrnovaly legislativní a právní regulaci, požár. Požár (nejvyšší RZ hodnota) byl opět výsledkem absencí odpovědného chování zaměstnanců a nedodržování pravidel a zákazů. Jak již bylo zmíněno empirická část nám dopomohla rozšířit znalosti o zabezpečení a uvědomit si lidský faktor jako významný atribut pro zajišťování spolehlivosti v budoucnu.

Dotazníkové šetření bylo tematicky zaměřeno na tři okruhy: informovanost o citlivých datech, kvality a rozsahu IT školení a IT kontrole bezpečnosti a odpovědnosti. Výsledky zkoumání specifikují pozitivní skutečnost a je jasným signálem, že vzdělávání a zabezpečení je propracované, přesto byly navrženy případné změny a zlepšení, která by pomohly potenciálním chybám předejít a omezit zneužívání systémových sítí.

Hlavní cíl práce i dílčí cíle byly splněny. Přínosem práce je získání všeobecných znalostí v oblasti kybernetické bezpečnosti, avšak je třeba se na tyto poznatky zaměřit a neustále se zdokonalovat v této problematice, protože tyhle hrozby kybernetických útoku mohou nabývat s dobou.

Závěrem lze říct, že je chybou se domnívat, že nás kybernetické útoky nezajímají. Každý, kdo je připojen k internetu, potřebuje kybernetickou bezpečnost. Je to proto, že většina kybernetických útoků je automatizovaná a jejich cílem je zneužít běžnou zranitelnost spíše než konkrétní webové stránky nebo organizace.

Provádění hodnocení hrozeb vyžaduje dovednosti a odborné znalosti, které nejsou snadno dostupné. Vyžadují aktuální přístup k informacím o hrozbách a vyžadují pochopení chování hrozby. Lidí budou vždy největším aktivem i největší hrozbou kybernetické bezpečnosti.

SEZNAM POUŽITÉ LITERATURY

ANDRAŠKO, Jozef, 2018. *Zákon o kybernetickej bezpečnosti č. 69/2018 Z. z.: komentár*. Prvé vydanie. Bratislava: Wolters Kluwer. ISBN 978-80-8168-905-5.

Avast: Adware [online], 2018. [cit. 2022-06-17]. Dostupné z: https://www.digitalnipevnost.cz/viki/adware

Avast: Co je počítačový virus [online], 1988-2022. Praha [cit. 2022-07-24]. Dostupné z: https://www.avast.com/cs-cz/c-computer-virus

Avast: Spyware [online], 1988-2022. [cit. 2022-06-24]. Dostupné z: https://www.avast.com/cs-cz/c-spyware

BASL, Josef a Roman BLAŽÍČEK, 2012. *Podnikové informační systémy: podnik v informační společnosti*. 3., aktualiz. a dopl. vyd. Praha: Grada. Management v informační společnosti. ISBN 978-80-247-4307-3.

BAUWENS, Michael, 2010. *What is cyberspace?: Computers in Libraries* [online]. In: . Academic Search Complete, EBSCOhost [cit. 2022-07-23]. ISSN 10417915. Dostupné z: https://www.ebsco.com/products/ebscohost-research-platform

BROOKS, Charlej et al., 2018. *Cybersecurity essentials* [online]. Indianapolis: John Wiley & Sons [cit. 2022-07-24]. ISBN 978-1-119-36239-5. Dostupné z: https://www.wiley.com/en-us/search?pq=%7Crelevance%7Cauthor%3ACharles+J.+Brooks

BURDA, Karel, 2017. *Základy elektronických zabezpečovacích systémů*. Vydání první. Brno: Akademické nakladatelství CERM. ISBN 978-80-7204-967-7.

CLARK, Robert a Simon HAKIM, 2017. *Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level*. 1st ed. 2017. Imprint: Springer,. Protecting Critical Infrastructure, 3. ISBN 978-3-319-32822-5.

Cyberblog: Nejrozšířenějším typem malwaru v Česku jsou trojské koně [online], 2022. Praha: Cyber Security Solutions s.r.o. [cit. 2022-08-02]. Dostupné z: https://cyberblog.cz/nejrozsirenejsim-typem-malwaru-v-cesku-jsou-trojske-kone/

ČESKO: In: Sbírka zákonů České republůiky [online], 2005. In: . Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnosti. [cit. 2022-05-20]. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-412

ČESKO: Terminologický slovník pojmů z oblasti krizového řízení, ochrany obyvatelstva, environmentální bezpečnosti a plánování obrany státu, 2016. In: *MVCR* [online]. Praha: Ministerstvo vnitra české republiky [cit. 2022-07-23].

ČESKO: Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) [online], 2018. In: . Ročník 2018 82/2018 Sb. Praha [cit. 2022-06-16]. Dostupné z: https://www.zakonyprolidi.cz/cs/2018-82

DOČEKAL, Daniel, 2022. *Lupa: Google: Adware napadá miliony zařízení a poškozuje inzerenty, weby i uživatele* [online]. [cit. 2022-07-24]. Dostupné z: https://www.cisa.gov/tlp *Eset: Trojský kůň* [online], 2022. [cit. 2022-07-24]. Dostupné z: https://www.eset.com/cz/trojsky-kun/

European Commission: KVALITA VEŘEJNÉ SPRÁVY [online], 2017. [cit. 2022-08-02]. Dostupné z: https://ec.europa.eu/info/sites/default/files/file_import/european-semester_thematic-factsheet_quality-public-administration_cs.pdf

FAGEL, Michael a Jennifer HESTERMAN, ed., 2017. *Soft targets and crisis management: what emergency planners and security professionals need to know*. Boca Raton: CRC Press, Taylor & Francis Group. ISBN 9781498756327.

FRANKE, Wolf D., 1993. *FMEA: Analýza možností vzniku vad a jejich následků*. Praha: Česká společnost pro jakost. ISBN 80-020-0968-1.

Govcert: Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020 [online], 2015. In: . [cit. 2022-06-23].

HASSANIEN, Aboul a Mohamed ELHOSENY, ed., 2019. *Cybersecurity and secure information systems: challenges and solutions in smart environments*. Cham: Springer. Advanced sciences and technologies for security applications. ISBN 978-3-030-16839-1.

HONZÍK, Petr, 2020. *Provozní kniha: bezpečnostní a technické systémy*. 1. vydání. Praha: ČIP Trading s.r.o. ISBN 9788027079162.

HSU, Frank a Dorothy MARINUCCI, 2013. *Advances in Cyber Security: Technology, Operations, and Experiences* [online]. Fordham University Press [cit. 2022-07-23]. ISBN 978-0-8232-4459-1. Dostupné z: https://doi.org/10.2307/j.ctt13x07xx. Accessed 23 Jul. 2022

HUB, Miloslav, 2013. *Bezpečnost a ochrana informací v prostředí internetu*. Vyd. 1. Pardubice: Univerzita Pardubice. ISBN 978-80-7395-701-8.

ISSS: Komunikační prostředí [online], 2004. In: . Praha [cit. 2022-05-23]. Dostupné z: www.isss.cz/archiv/2004

IT Slovník: Počítačový slovník [online], 2021. Jihlava [cit. 2022-06-01]. Dostupné z: https://it-slovnik.cz/

Itportal.io: Spyware [online], 2021. [cit. 2022-07-24]. Dostupné z: https://itportal.io/spyware/

JANOUŠEK, Michal, 2006. *Obrana a strategie: Kyberterorismus: terorismus informační společnosti* [online]. In: . [cit. 2022-08-01]. Dostupné z: file:///C:/Users/HP/Downloads/janousek_2_06.pdf

JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR, 2015. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze. ISBN 978-80-7251-436-6.

JIROVSKÝ, Václav, 2007. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada. ISBN 978-80-247-1561-2.

KOLOUCH, Jan, 2016. *CyberCrime*. 1. vydání. Praha: CZ.NIC, z.s.p.o. CZ.NIC. ISBN 978-80-88168-15-7.

KOLOUCH, Jan a Pavel BAŠTA, 2019. *CyberSecurity*. 1. vydání. Praha: CZ.NIC, z.s.p.o. CZ.NIC. ISBN 978-80-88168-31-7.

Kybez: Základní pojmy [online], 2021. Praha: Gordic spol.s.r.o. [cit. 2022-06-23]. Dostupné z: https://www.kybez.cz/zakladni-pojmy/

MALWAREBYTES: Co jsou zadní vrátka [online], 2022. [cit. 2022-08-03]. Dostupné z: https://www.malwarebytes.com/backdoor

Malwarebytes: Hacking definition: What is hacking? [online], 2022. [cit. 2022-05-20]. Dostupné z: https://www.malwarebytes.com/hacker

MALWAREBYTES: Vše o ransomwarových útocích [online], 2022. [cit. 2022-08-03]. Dostupné z: https://www.malwarebytes.com/ransomware

NUKIB, 2017. In: *NUKIB: Zpráva o stavu kybernetické bezpečnosti za rok 2017* [online]. Praha [cit. 2022-06-02].

OLIVEIRA, Nythamar, Marek HRUBEC a Emil SOBOTTKA, ed., 2018. *From social to cyber justice: critical views on justice, law, and ethics*. Prague: Filosofia. ISBN 978-80-7007-515-9.

PLURA, Jiří, 2001. *Plánování a neustále zlepšování jakosti: metodické postupy, metody QFD, FMEA, FTA, hodnocení způsobilosti procesů, systémy měření, sedm základních a sedm nových nástrojů managementu jakosti, praktické příklady*. 1. vyd. Praha: Computer Press. ISBN 80-7226-543-1.

PTAČKA, Roman, 2022. *NUKIB: KONCEPTUÁLNÍ A TEORETICKÉ ASPEKTY KYBERNETICKÉ BEZPEČNOSTI* [online]. In: . [cit. 2022-07-23]. Dostupné z: https://docplayer.cz/124556304-Konceptualni-a-teoreticke-aspekty-kyberneticke-bezpecnosti-phdr-roman-packa.html

REFSDAL, Atle, Bjørnar SOLHAUG a Ketil STøLEN, 2015. *Cyber-Risk Management*. 1st ed. 2015. Imprint: Springer,. SpringerBriefs in Computer Science. ISBN 978-3-319-23569-1.

SAK, Petr a Jiří MAREŠ, 2007. *Člověk a vzdělání v informační společnosti*. Vyd. 1. Praha: Portál. ISBN 978-80-7367-230-0.

SMEJKAL, Vladimír, 2015. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk. Pro praxi. ISBN 9788073805012.

SMEJKAL, Vladimír a Karel RAIS, 2013. *Řízení rizik ve firmách a jiných organizacích*. 4., aktualiz. a rozš. vyd. Praha: Grada. Expert (Grada). ISBN 978-80-247-4644-9.

SMEJKAL, Vladimír, Tomáš SOKOL a Jindřich KODL, 2019. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o. ISBN 9788073807658.

Správa sítě: Co je kyberterorismus? [online], 2016. Praha: Aira GROUP, s.r.o. [cit. 2022-06-21]. Dostupné z: https://www.sprava-site.eu/kyberterorismus/

ŠULC, Vladimír, 2018. *Kybernetická bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o. ISBN 978-80-7380-737-5.
Techrepublic: The CIA Triad [online], 2022. [cit. 2022-05-18]. Dostupné z: https://www.techrepublic.com/article/revil-gang-member-arrests-strike-fear-among-cybercriminals-on-the-dark-web/

TZIMOPOULOU, Sofia, 2006. *The virtuality of the digital: Intelligent Environments* [online]. **1**(2) [cit. 2022-07-23]. ISSN 0537-9989.

Vláda ČR: Informační společnost [online], 2022. Praha [cit. 2022-03-06]. Dostupné z: https://www.vlada.cz/cz/clenove-vlady/historie-minulych-vlad/statni-informacni-politika---cesta-k-informacni-spolecnosti---dokument-2089/

Vlada.cz: Kyberprostor a kybernetická bezpečnost ČR [online], 2021. Praha: Úřad vlády české republiky [cit. 2022-08-02]. Dostupné z: https://www.vlada.cz/assets/evropske-zalezitosti/aktualne/Digitalni_Cesko_FINAL-ONLINE-VERSION.pdf

Z-WARE: Přístupové systémy [online], 2022. [cit. 2022-08-02]. Dostupné z: https://www.z-ware.cz/pristupove-systemy

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

APT – advanced persistent threat

CIA – confidentiality, integrity, availability

CSIRT – computer security incident response team

ČR – Česká republika

DDoS – distributed denial of service

DLP – prevence ztráty dat

DNS – domain name system

DoS – denial of service

ENISA – evropská unide pro kybernetickou bezpečnost

FMEA – Failure Mode and Effects Analysis

ICT – informační a komunikační technologie

ID – identita

IDS – intrusion detection systém

ISAC – international scientific advisory committee

IT – informační technologie

LTP – prvky kybernetické bezpečnosti (lidé, technologie, procesy)

MZS – mechanické zábranné systémy

PDR – životní cyklus kybernetické bezpečnosti (prevence, detekce, reakce)

PZTS – poplachové zabezpečovací a tísňové systémy

RAT – malware typu RAT

TLP – traffic light protocol

USA – United state of America

UTM – unified threat management

VPN – virtuální privátní síť

XSS – ceoss site scripting

SEZNAM OBRÁZKŮ

Obrázek 1- Klasifikace technologií kybernetické bezpečnosti na 24
Obrázek 2 – CIA Triáda (Clark a Hakim, 2017) 25
Obrázek 3 – Životní cyklus kybernetické 37
Obrázek 4 - Členění útočníků v kyberprostoru podle motivace (JANOUŠEK, 2006) 40
Obrázek 5 – Příklad reklam (Avast, 2018) 41
Obrázek 6 – Spyware (Itportal.io, 2021) 41

SEZNAM TABULEK

Tabulka 1 - Klasifikace informací dle zákona 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti**.** (ČESKO, 2005) 27
Tabulka 2 - Klasifikace informací (Šulc, 2018) 28
Tabulka 3 - Protokol semaforu (TLP) (ČESKO, 2018) 29
Tabulka 4 - Stupnice pro hodnocení důvěrnosti (ČESKO, 2018) 30
Tabulka 5 - Stupnice pro hodnocení integrity (ČESKO, 2018) 32
Tabulka 6 - Stupnice pro hodnocení dostupnosti (ČESKO, 2018) 33
Tabulka 11 – Identifikace citlivých dat (zpracování vlastní) 63
Tabulka 12 – Znalost bezpečnostních pravidel (vlastní zpracování) 64
Tabulka 13 – IT kontrola bezpečnosti (vlastní zpracování) 65
Tabulka 14 – Rozdělení pravomocí (vlastní zpracování) 66
Tabulka 15 – Realizace IT školení (vlastní zpracování) 67
Tabulka 16 – Praktická výuka IT bezpečnosti (vlastní zpracování) 68
Tabulka 7 – Pravděpodobnost výskytu (vlastní zpracování) 77
Tabulka 8 – Význam dopadu rizika (vlastní zpracování) 77
Tabulka 9 – Odhalení rizika (vlastní zpracování) 78
Tabulka 10 – Vyhodnocení analýzy FMEA (vlastní zpracování) 86

SEZNAM GRAFŮ

Graf 1- Nejčastější hrozby v Česku za rok 2021 (Cyberblog, 2022)..... 47
Graf 2 – Identifikace citlivých dat (zpracování vlastní)..... 63
Graf 3 – Znalost bezpečnostních pravidel (vlastní zpracování)..... 64
Graf 4 – Znalost IT kontroly bezpečnosti (vlastní zpracování)..... 65
Graf 5 – Rozdělení kompetencí (vlastní zpracování)..... 66
Graf 6 – Realizace IT školení (vlastní zpracování)..... 67
Graf 7 – Praktická výuka v IT bezpečnosti (vlastní zpracování)..... 68