Kybernetická bezpečnost vybraného subjektu

Bc. Jan Kazík

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. Jan Kazík**
Osobní číslo:	**L20196**
Studijní program:	**N1032A020002 Bezpečnost společnosti**
Specializace:	**Ochrana obyvatelstva**
Forma studia:	**Kombinovaná**
Téma práce:	**Kybernetická bezpečnost vybraného subjektu**

Zásady pro vypracování

1. Proveďte rešerši současného stavu v předmětné oblasti.
2. Zhodnoťte aktuální stav kybernetické bezpečnosti vybraného subjektu.
3. Navrhněte vhodná opatření pro zlepšení současného stavu vybraného subjektu.
4. Zpracujte příručku kybernetické bezpečnosti pro zaměstnance vybraného subjektu.

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

Seznam doporučené literatury:

1. CLARK, Robert M. a Simon HAKIM, ed. *Cyber-Physical Security.* 3rd edition. New York: Springer International Publishing, 2017. ISBN 978-3-319-32822-5.
2. DOUCEK, Petr, Martin KONEČNÝ a Luděk NOVÁK. *Řízení kybernetické bezpečnosti a bezpečnosti informací.* Praha: Professional Publishing, 2019. ISBN 978-80-88260-39-4.
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: 6.5.2022

Jméno a příjmení studenta: Bc. Jan Kazík

.....
podpis studenta

ABSTRAKT

Diplomová práce se zabývá problematikou kybernetické bezpečnosti vybraného subjektu. V teoretické části práce mapuje zdroje a shrnuje celou problematiku za účelem jejího dostatečného pochopení. Praktická část se dále zabývá identifikací rizik a následnou analýzou stavu kybernetické bezpečnosti subjektu pomocí analytických metod KARS a FMEA. Na základě zjištěných informací navrhuje příslušná opatření a je zpracována příručka pro zaměstnance subjektu za účelem zvýšení stavu vzdělanosti v dané problematice.

Klíčová slova: kybernetická bezpečnost, malware, phishing, subjekt.

ABSTRACT

The thesis deals with the issue of cyber security of a selected subject. The theoretical part of the thesis maps the sources of information and summarizes the whole issue to sufficiently understand it. The practical part focuses on further identification of risks and subsequently on the analysis of the state of cyber security of the subject using analytical methods KARS and FMEA. Based on the information obtained, it proposes appropriate measures. Also, a handbook for the entity's employees is prepared in order to increase the level of education on the given issue.

Keywords: cyber security, malware, phishing, subject.

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

OBSAH

ÚVOD

Kybernetická bezpečnost se stala obrovskou výzvou. Téměř vše, co vidíme, čeho se dotýkáme nebo co používáme, je spojeno s internetem, včetně mobilních telefonů, v podstatě nositelných zařízení, domácích spotřebičů, a dokonce už i vozidel. Internet je nástrojem pro společnost, firmy, vlády a státní instituce. Paradoxem konektivity je, čím více jsou naše počítačové systémy propojeny, tím jsou více vystaveni kybernetickým útokům za účelem ukrást data, poškodit software, narušit operace, a dokonce i fyzicky poškodit hardware a síťovou infrastrukturu. Existence oblasti kybernetické bezpečnosti je logickým krokem za účelem pochopit a působit jako obrana proti těmto útokům.

Bezpečnost v této oblasti bývá často podceňována a subjekty si neuvědomují možné ohrožení a také dopady kybernetických útoků. Z tohoto důvodu zpravidla není tato oblast důsledně řešena a nejsou nastaveny pravidla a zaměstnanci řádně proškoleni. Neznalost v této oblasti způsobuje vyšší zranitelnost a zhoršení dopadů.

Diplomová práce se zabývá kybernetickou bezpečností jednoho subjektu. Jejím obsahem všech je pokryta oblast kybernetické bezpečnosti jako celku. Zabývá se kybernetickou bezpečností a jejím stavem v České republice, legislativou s ní spojenou, typy kybernetických útoků a možnými řešeními těchto incidentů, která je řešena v teoretické části. Hlavní částí práce je praktická část, která se zabývá samotnou analýzou stavu kybernetické bezpečnosti vybraného subjektu jakožto startovní pozicí pro správnou identifikaci hrozeb. Identifikace reálných hrozeb je důležitým faktorem pro zpracování analýzy, ze které vyplývají vhodná opatření, které mají z cíl snížit riziko vzniku negativní události na minimum. Na základě návrhu vhodných opatření je zpracována příručka pro zaměstnance subjektu. Obsahem příručky je popis a postupy jakým způsobem pracovat s daty, jak s nimi nakládat a jak se chovat v kyberprostoru. Dále jakým způsobem poznat, že je systém napaden kybernetickým útočníkem, jaké jsou možnosti a jaká provádět protiopatření. Tato příručka poskytuje dostatek základních informací, není v ní však obsažena celá problematika. Je sestavena „na míru“ vybranému subjektu pro jeho potřeby.

I. TEORETICKÁ ČÁST

1 CÍLE A METODY

Hlavním cílem diplomové práce je návrh opatření pro zlepšení současného stavu kybernetické bezpečnosti vybraného subjektu. Dílčím cílem je provedení rozboru dostupných tuzemských i zahraničních zdrojů a zpracování teoretické části diplomové práce. Dalšími dílčími cíli jsou analýza kybernetické bezpečnosti, identifikace aktiv a rizik pro subjekt, která budou sloužit k další analýze, po níž bude provedeno samotné hodnocení a provedení návrhu ošetření rizik. Posledním dílčím cílem je zpracování příručky pro zaměstnance a management subjektu, která reflektuje výsledky provedených analýz.

Sběr informací byl proveden z dostupných zdrojů pomocí rešerše z důvodu hlubšího poznání sledované tématiky. Informace týkající se vybraného subjektu byly získávány kvalitativními metodami, a to řízeným rozhovorem v kombinaci s pozorováním a dalšími kontextovými otázkami. Otázky jsou zaměřeny směrem napomáhajícím určení stavu kybernetické bezpečnosti tohoto subjektu ve vztahu k fyzické bezpečnosti a bezpečnosti sítí a služeb. Základní otázky byly předem připraveny a další vyplývaly z kontextu. V průběhu pozorování byli zúčastnění průběžné dotazováni, a to poskytlo podmínky k vytvoření obrazu celého systému. Jelikož z pozice subjektu byl umožněn plný přístup ať už do jeho prostor nebo do systému, použití metody pozorování umožňovalo dlouhodobější podrobné zkoumání postupů a dějů v celém systému. Kontextový rozhovor byl veden se zaměstnanci podílejícími se na zpracování informací a pracujícími s aktivy. Hlavním představitelem této skupiny byl však jednatel, který nese zodpovědnost za celý systém. Účelem bylo stanovení stavu úrovně zabezpečení dat subjektu, které byly dále použity pro analýzu.

Při zpracovávání teoretické části byla využita metoda komparace pro srovnávání jednotlivých zdrojů a jejich vhodný výběr pro potřeby práce.

V praktické části práce byly použity vědecké metody jakožto především analýza rizik na základě vybraných metod, které jsou blíže popsány v rámci kapitoly analýza rizik. Pro identifikaci rizik byla použita metoda brainstormingu provedená s jednatelem subjektu. Jako prvotní metoda analýzy je použita metoda kvalitativní metoda analýzy KARS, která určuje vzájemnou souvztažnost jednotlivých rizik. Následně byla použita metoda analýza možného výskytu a vlivu vad (FMEA), která se zabývá určením významu, výskytu, obhajitelnosti jednotlivých vad a výpočtem finálního rizikového čísla, pomocí kterého dochází k rozdělení rizik da kategorií. Vady přestavují chyby na lidské, organizační nebo materiální úrovni.

Po každé provedené analýza následovala syntéza, pomocí které byla provedena intepretace výsledků a jejich využití pro zpracování návrhu pro jejich ošetření.

2 LITERÁRNÍ REŠERŠE

V této kapitole je zpracována literární rešerše vybraných zdrojů, které jsou použity pro porozumění, orientaci v tématu a také pro samotné zpracování diplomové práce.

2.1 Cyber-physical security

Tato kniha se zaměřuje na zranitelnost státních a místních služeb vůči kybernetickým hrozbám a navrhuje možná ochranná opatření, která by proti takovým hrozbám mohla být podniknuta. Informační a komunikační technologie (dále ICT) jsou všudypřítomné a mnoho zařízení ICT a dalších komponent jsou na sobě navzájem závislé; proto narušení jedné složky může mít negativní, kaskádový účinek na ostatní. Kybernetické útoky mohou zahrnovat odmítnutí služby, krádež nebo manipulaci s daty. Poškození kritické infrastruktury prostřednictvím kybernetického útoku by mohlo mít významný dopad na národní bezpečnost, hospodářství a živobytí a bezpečnost mnoha jednotlivých občanů. Kybernetická bezpečnost je tradičně považována za zaměřenou na hrozby vyšší úrovně, jako jsou hrozby proti internetu nebo federální vládě. (Clark a Hakim, 2017)

2.2 Cybersecurity

Kniha CyberSecurity se, jak vyplývá již z názvu, věnuje problematice kybernetické bezpečnosti. Poukazuje na základní principy, které je nutné respektovat při práci s informačními technologiemi. Kniha zároveň obsahuje také výklad právních norem týkajících se kybernetické bezpečnosti a je také využitelná odborníky na informační technologie (dále IT) jakožto zdroj informací o kybernetické bezpečnosti. (Kolouch a Bašta, 2019)

2.3 Cybercrime

Tato kniha se věnuje problematice bezpečnosti. Obsahuje důležité informace týkající se kybernetických hrozeb se zaměřením na kybernetickou kriminalitu. Zabývá s vysvětlením právních klasifikací a jednotlivých paragrafů v zákonech řešících kybernetickou kriminalitu. Vysvětluje celou řadu pojmů týkající se této oblasti a napomáhá orientaci. (KOLOUCH, 2016)

2.4 Řízení kybernetické bezpečnosti a bezpečnosti informací

Kniha poskytuje ucelený pohled na kybernetickou bezpečnost. Zabývá se řízením kybernetické bezpečnosti a bezpečnosti informací, kybernetickou bezpečností v české republice systémem řízení kybernetické bezpečnosti a realizací opatření. Představuje výsledek výzkumu autorů v oblasti kybernetické bezpečnosti a představuje návrhy jakým způsobem takový systém vytvořit a provozovat za současné legislativy. Poukazuje také na úskalí řízení kybernetické bezpečnosti u subjektu. Závěrem vysvětluje, proč podstupovat tento náročný proces, který nikdy nekončí a jaké jsou jeho přínosy. (Doucek, Konečný a Novák, 2019)

3 KYBERNETICKÁ BEZPEČNOST

Vysvětlení pojmu kybernetická bezpečnost může být problematické, jelikož představa o této problematice bývá nezřídka chybná. Tento pojem, který je v současnosti často skloňován, je často spojován pouze s odděleními informačních a komunikačních technologií. Toto je však zcela špatně. Problematika kybernetické bezpečnosti se týká každého uživatele informačních a komunikačních technologií (dále ICT) což je v dnešní době drtivá část populace. (Kolouch a Bašta, 2019)

3.1 Základní pojmy

V této kapitole budou vymezeny základní pojmy týkající se problematiky kybernetické bezpečnosti.

Kybernetická bezpečnost

Vysvětlení pojmu kybernetická bezpečnost existuje celá řada a nemá všeobecně uznávanou definici.

- Kybernetická bezpečnost představuje soubor opatření, která jsou přijata, aby byl ochráněn počítačový systém před neoprávněným přístupem či útokem. (Kolouch a Bašta, 2019)
- Kybernetická bezpečnost se komplexní opatření z hlediska práva, uspořádání technických a vzdělávacích nástrojů, které cílí k zajištění bezpečného kybernetického prostoru. (Doucek, Konečný a Novák, 2019)
- Kybernetická bezpečnost dle ISO/IEC 27100 představuje ochranu společnosti, lidí, organizací a národů před digitálními riziky. (Doucek, Konečný a Novák, 2019)

Kybernetický prostor

„Kybernetickým prostorem digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací.“ (Česko, 2014, a)

Bezpečnost

„Stav, kdy je systém schopen odolávat známým a předvídatelným (i nenadálým) vnějším a vnitřním hrozbám, které mohou negativně působit proti jednotlivým prvkům (případně celému systému) tak, aby byla zachována struktura systému, jeho stabilita, spolehlivost

a chování v souladu s cílovostí. Je to tedy míra stability systému a jeho primární a sekundární adaptace.“ (Česko, 2016)

Aktiva

Tento termín může být známý jeho použitím ve finančním kontextu. V kontextu kybernetické bezpečnosti odkazuje na jakýkoli organizační informační zdroj, který může být vystaven kybernetickému útoku, a proto potřebuje ochranu. Termín pokrývá širokou škálu jako jsou datové zdroje, software, fyzické počítačové systémy, sítě, pomocné programy, a také méně hmatatelné zdroje jako pověst, dobré jméno, důvěryhodnost, postavení společnosti. (Clark a Hakim, 2017)

Hacktivismus

Je to činnost kybernetických útočníků motivovaná občanskými nebo politickými ideály. (Kresa, 2018)

Backdoor

Tento pojem znamená v anglickém překladu zadní dveře. Tímto pojmem je nazýván škodlivý kód, který otevírá možnost pro útočníka převzít vzdáleně kontrolu nad infikovaným počítačem. (IT Slovník, © 2021)

Botnet

Jedná se o síť infikovaných počítačů, které jsou řízeny z jednoho centra za účelem provádění nežádoucí činnosti např. spamu, DDoS útoků. (IT Slovník, © 2021)

Hacking

Aktivita, při které útočník hledá chyby v systému za účelem jeho ovládnutí. Útočník se poté nazývá „Hacker“. (IT Slovník, © 2021)

Vícefaktrová autentizace

Vícefaktorová autentizace je použití více než jedné autentizace. To znamená použití dvou popřípadě více faktorů k dosažení autentizace. Faktory například heslo/PIN, něco co máte, například kryptografické identifikační zařízení nebo něco, čím jste například biometrii (otisk prstu atd.). Systém, který vyžaduje dva faktory je obecně silnější než systém vyžadující jediný faktor. (Stallings, 2019)

3.2 Principy kybernetické bezpečnosti

Tato podkapitola je věnována principům kybernetické bezpečnosti. Tyto principy jsou důležité pro předcházení negativním událostem ve vztahu ke kybernetické bezpečnosti. Jedná se o tyto triády:

- Triáda CIA.
- Prvky kybernetické bezpečnosti.
- Životní cyklus kybernetické bezpečnosti.

3.2.1 Triáda CIA

Jedná se o nejpoužívanější a nejznámější triádu kybernetické bezpečnosti. Její využití však není dostačující bez použití dalších principů, které jsou nutné pro dosažení odpovídající úrovně kybernetické bezpečnosti. Týká se ICT, ale také dat a informací během přenosu, zpracování a uchovávání. (Kolouch a Bašta, 2019)

V zahraniční literatuře je možno se setkat s principem Parkerian hexad což je v podstatě triáda CIA doplněná o další tři prvky. Po prvcích důvěrnost – Confidentality; integrita – Integrity; dostupnost – Availability je doplňen o další tři, kterými jsou: držení a kontrola – Possesion or Control; pravost – Autenticity; užitečnost – Utility (Kolouch a Bašta, 2019)

Důvěrnost (Confidentality) – tento pojem definuje skutečnost, že přístup k informacím mají pouze oprávněné osoby na základě autorizace. Pro tyto účely se provádí klasifikace informací s ohledem na jejich citlivost, hodnotu, právní požadavky a kritičnost.

Pro omezení přístupu k informacím neautorizovaným osobám musí být stanovena pravidla pro manipulaci, přístupu a ukládání těchto informací. (Kolouch a Bašta, 2019)

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 mimořádně vážnou újmu zájmům České republiky.*
- ***Tajné** (Secret) - neoprávněné nakládání s informacemi by mohlo způsobit vážnou újmu zájmům České republiky.*
- ***Důvěrné** (Confidential) - neoprávněné nakládání s informacemi by mohlo způsobit prostou újmu zájmům České republiky.*

- ***Vyhrazené*** *(Restricted) - neoprávněné nakládání s informacemi by mohlo být nevýhodné pro zájmy České republiky.“* (Česko, 2005)

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.).“* (Kolouch a Bašta, 2019)

Dále je pro klasifikaci důvěrnosti v komerční využíván Taffic light protocol (dále TPL), který využívá barev pro určení míry důvěrnosti.

Barva	Podmínky použití
TLP:RED	Informace nemůže být poskytnuta jiné osobě než té, které byla informace určena, nebudou-li výslovně stanoveny další osoby, kterým lze takovou informaci poskytnout. V případě, že příjemce považuje za důležité informaci poskytnout dalším subjektům, lze tak učinit pouze se souhlasem původce informace.
TLP:AMBER	Informace může být sdílena v rámci organizace, které byla informace poskytnuta. Dále může být poskytnuta pouze těm partnerům, kteří splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci. Jiným osobám, než výše uvedeným, nesmí být informace poskytnuta. **Původce informace může rozsah sdílení dále omezit.**
TLP:GREEN	Informace může být sdílená v rámci organizace příjemce a případně také s dalšími partnerskými subjekty příjemce, avšak nikoli skrze veřejně dostupné kanály; příjemce musí při předání zajistit důvěrnost komunikace.
TLP:WHITE	Informace může být dále poskytována a šířena bez omezení. Případné omezení na základě práva duševního vlastnictví původce a/nebo příjemce či třetích stran nejsou tímto ustanovením dotčena.

Obrázek 1 – Traffic light protocol (NÚKIB, © 2022, b)

Integrita (Integrity) – znamená nemožnost jakýmkoli způsobem zasáhnout do informací, dat, počítačových systémů mimo osob k tomu oprávněných. Je to záruka neporušenosti a celistvosti sytému. Pokud dojde k porušení integrity, nemusí být tato změna odhalena vůbec nebo až po značné době.

Dle vyhlášky číslo 82/2018 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) příloha 1 lze rozlišit stupně hodnocení integrity:

- ***Nízká –*** *aktivum nevyžaduje ochranu z hlediska integrity.*
- ***Střední –*** *aktivum může vyžadovat ochranu z hlediska integrity.*
- ***Vysoká –*** *aktivum vyžaduje ochranu z hlediska integrity. Narušení má podstatné dopady na primární aktiva.*
- ***Kritická –*** *aktivum vyžaduje ochranu z hlediska integrity. Narušení má velmi vážné dopady na primární aktiva.* (Česko, 2018)

Pro ověření integrity dat je možno využít hashovací funkce. Hashovací funkce slouží k převedení textu na číselný kód, který je jedinečný. Jedná se o jednocestný proces, tudíž není možné převést číselný kód zpět na text. Jakákoli změna v textu vyvolává změnu v číselném kódu a tím je možné ověřit integritu dat. (Kolouch a Bašta, 2019)

Dostupnost (Availability) – jedná se o garanci přístupu k informací, datům a počítačovému systému v okamžiku potřeby. Je nutno dokonale zkombinovat integritu s dostupností. Při dokonalé integritě bez možnosti přístupu k datům je systém nevyužitelný. (Kolouch a Bašta, 2019)

Dle vyhlášky číslo 82/2018 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) příloha 1 lze rozlišit stupně hodnocení dostupnosti:

- *„**Nízká –** narušení dostupnosti aktiva není důležité.*
- ***Střední –** narušení dostupnosti aktiva by nemělo překročit dobu jednoho dne.*
- ***Vysoká –** narušení dostupnosti aktiva by nemělo překročit dobu několika hodin.*
- ***Kritická –** nerušení dostupnosti aktiva není přístupné, a i krátkodobá nedostupnost vede k vážnému ohrožení.“* (Česko, 2018)

S dostupností úzce souvisí pojem redundance. Redundance je nadbytek oproti nutnosti a v oblasti IT je spojován se spolehlivostí dostupností služeb. Redundantní mohou být data, v jejich případě se jedná o ukládání dat více různých míst, infrastruktura, kde jsou zdvojovány komponenty z důvodu možné poruchy, zdroje a konektivita, kde se zdvojuje systém na sobě nezávislého napájení nebo připojení pro zajištění dostupnosti služeb. (Redundance, © 2022)

3.2.2 Prvky kybernetické bezpečnosti

Dalším principem jsou prvky kybernetické bezpečnosti. Kombinace těchto prvků zvyšuje úroveň kybernetické bezpečnosti. Jelikož naprosto bezpečný systém lze vytvořit pouze teoreticky, tak bezpečnost systému na jeho nejslabším článku (prvku). Mezi tyto prvky patří:

Lidé – představují klíčový prvek v bezpečnosti, ať už se jedná o jakýkoliv její druh. V oblasti kybernetické bezpečnosti se jejich role umocňuje, jsou nejslabším článkem a nejčastěji čelí kybernetickým útokům. V tomto systému plní zásadní role jakožto strůjce této bezpečnosti, příjemce pravidel o kybernetické bezpečnosti, subjekt nutný chránit před kybernetickými útoky, subjekt, který je třeba soustavně informovat a školit v této oblasti, a také jako zásadní hrozba pro celý systém. (Kolouch a Bašta, 2019)

Technologie – jedná se o prostředky, které uživatelům umožňují připojit se do kyberprostoru (internetu, sociálním sítím a dalším aplikacím. Uživatel zpravidla vnímá pouze koncová zařízení (PC, tablet, mobilní telefon atd.), které aktivně využívá. O další technologické vrstvy, které jsou nutné pro tuto činnost, se nezajímá.

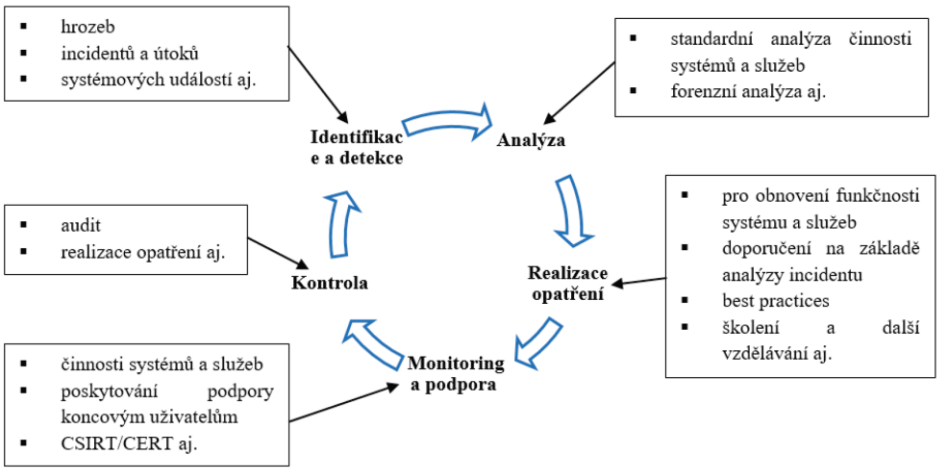
Pro organizace však technologie představují zařízení od uživatelských přes síťovou infrastrukturu až po prvky zajišťující zabezpečení. Pro zajištění kybernetické bezpečnosti je nutné provádět stálý monitoring změn a na ně reagovat. Minimálně udržováním provozuschopného systému s pravidelnou aktualizací. (Kolouch a Bašta, 2019)

Procesy – je činnost, která je nutná vynaložit, aby bylo možné technologie a s nimi spojené služby používat uživateli. Jedná se o procesy řízení aktiv a rizik, audit kybernetické bezpečnosti, autorizace a autentizace, školení, reakce na kybernetické útoky a další. (Kolouch a Bašta, 2019)

3.2.3 Životní cyklus kybernetické bezpečnosti

Při realizaci kybernetické bezpečnosti z časového hlediska je nutné uplatňovat triádu CIA a také další dílčí prvky kybernetické bezpečnosti po dobu jejího celého životního cyklu.

Jedná se především o prevenci, detekci a reakci na útok. Při řešení kybernetické bezpečnosti neexistuje stav nulové hrozby nebo absolutního zabezpečení. Jedná se o nekonečný proces, který má za úkol výrazně zvyšovat úroveň kybernetické bezpečnosti. (Kolouch a Bašta, 2019)



Obrázek 2 – Životní cyklus kybernetické bezpečnosti (Kolouch a Bašta, 2019)

3.3 Kybernetická bezpečnost v ČR

Kybernetická bezpečnost je dnes chápána jako významná součást celkové bezpečnosti ČR. Současná situace ukázala, co všechno je možné přesunout do kybernetického prostoru. S tím souvisí také vyšší riziko kybernetických útoků. Závislost na službách vycházejících s kyberprostoru je dnes nepopiratelná a ovlivňuje každého jednotlivce. Česká republika proto postupuje dle „Národní strategie kybernetické bezpečnosti České republiky“. Současná strategie se zabývá lety 2021-2025 a je zaměřena se především na bezpečnostní složky státu a subjekty veřejné správy.

3.3.1 Národní strategie kybernetické bezpečnosti České republiky 2021-2025

Základem strategie je vize založená na odolnosti společnosti a celkové infrastruktury ČR, sebevědomém vystupování, ale také na aktivním přístupu k řešení kybernetických hrozeb, a to za pomoci aliančních partnerů. Strategie stanovuje tři základní pilíře:

- *„Sebevědomě v kyberprostoru.*

- *Silná a spolehlivá spojenectví.*
- *Odolná společnost.“*

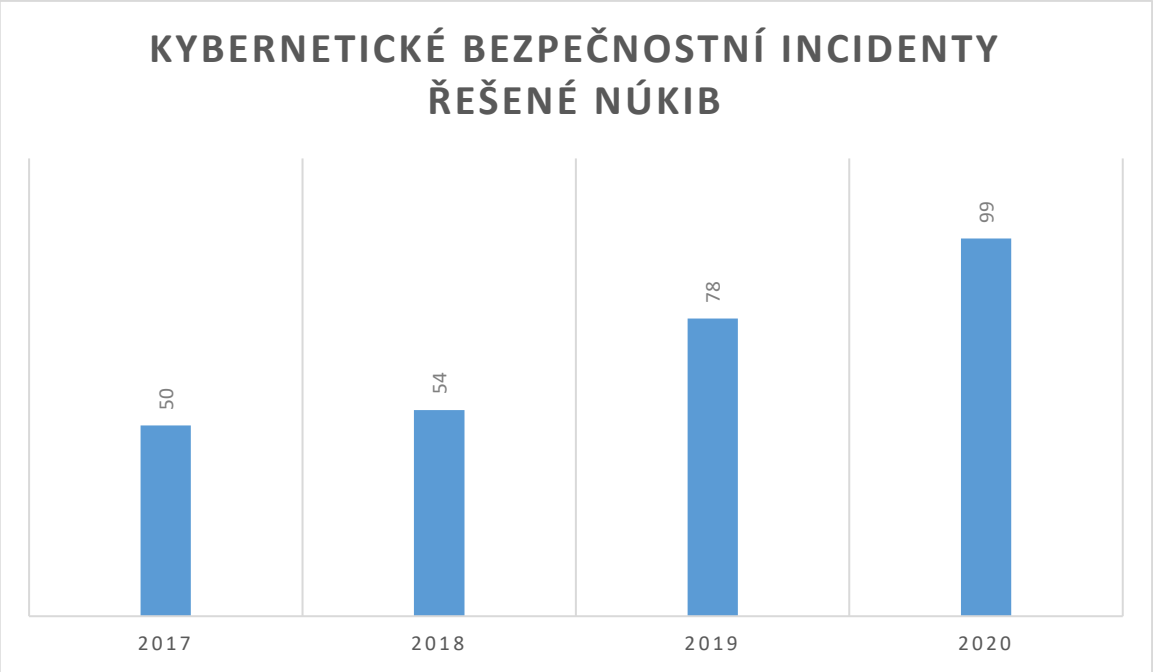
Jelikož je dnešní společnost závislá na ICT a využívá se ho ve všech odvětvích, jsou kybernetické hrozby důležitým faktorem. Hrozby mohou narušit stabilitu systému, proto je hrozbám věnována samostatná kapitola. Včasná identifikace, vyhodnocení a reakce jsou nezbytné pro zvládání kybernetických hrozeb a stabilitu bezpečnostního prostředí. (NÚKIB, 2020)

3.3.2 Akční plán k národní strategii kybernetické bezpečnosti české republiky na období let 2021 až 2025

Akční plán slouží jako harmonogram činností k naplňování cílů Národní strategie kybernetické bezpečnosti České republiky dělící odpovědnost mezi jednotlivé subjekty dle jejich kompetence ve smyslu zákona 181/2014 Sb. o kybernetické bezpečnosti. Na základě akčního plánu probíhá dle časového rámce realizace a naplňování cílů v něm stanovených. (NÚKIB, 2021, a)

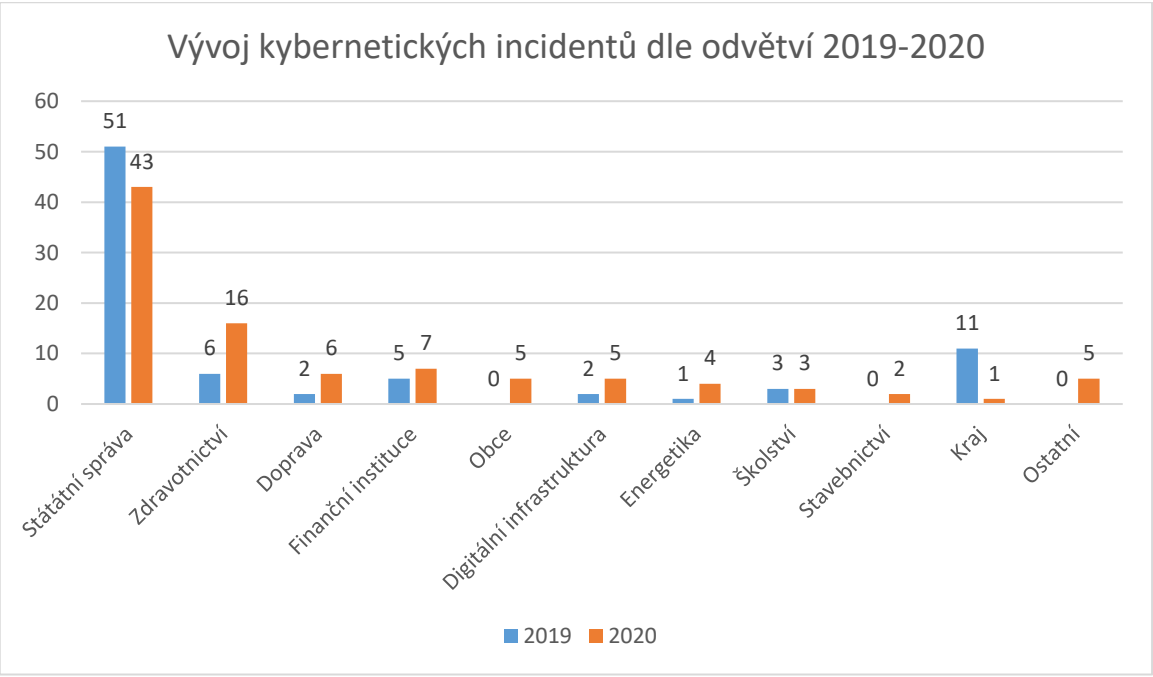
3.3.3 Zpráva o stavu kybernetické bezpečnosti české republiky za rok 2020

V roce 2020 byl zaznamenán nárůst cíleného phishingu a ransomwaru. Dle respondentů z řad českých institucí, organizací a firem byl nejčastějším typem útoku spam a po něm phishing. V roce 2020 obdržel Národní úřad pro kybernetickou a informační bezpečnost (dále NÚKIB) 468 hlášení o kybernetických bezpečnostních incidentech, z nichž přímo řešil 99 incidentů. (NÚKIB, 2021, b)



Graf 1 – Kybernetické bezpečnostní incidenty řešené NÚKIB (NÚKIB, 2021, b)

Během roku 2020 bylo NÚKIB řešeno nejvíce kybernetických incidentů v oblasti státní správy. Ve druhém nejčastějším sektoru a to zdravotnictví došlo k meziročnímu nárůstu o 267 %.



Graf 2 – Vývoj kybernetických incidentů dle odvětví 2019-2020 (NÚKIB, 2021, b)

Z grafu 2 je patrné, že dochází k meziročnímu nárůstu incidentů ve většině odvětví, proto je nutné neustále pracovat na zlepšování systémů zabezpečení jednotlivých subjektů.

3.4 Národní úřad pro kybernetickou a informační bezpečnost

Na základě potřeby k zajištění kybernetické bezpečnosti vznikl 1. srpna 2017 Národní úřad pro kybernetickou a informační bezpečnost dle zákona č. 205/2015 Sb., který měnil zákon č. 181/2014 Sb. O kybernetické bezpečnosti. NÚKIB převzal kompletně od Národního bezpečnostního úřadu (dále NBÚ) agendu Národního centra kybernetické bezpečnosti. (Doucek, Konečný a Novák, 2019)

„NÚKIB je ústředním správním orgánem pro kybernetickou bezpečnost včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany. Dále má na starosti problematiku veřejně regulované služby v rámci družicového systému Galileo. Ředitel Úřadu se též pravidelně účastní jednání Bezpečnostní rady státu (dále BRS) a je členem Výboru pro kybernetickou bezpečnost, který je stálým pracovním orgánem BRS pro koordinaci plánování opatření k zajišťování kybernetické bezpečnosti České republiky.“ (NÚKIB, 2021, c)

4 PRÁVNÍ RÁMEC KYBERNETICKÉ BEZPEČNOSTI

Tato kapitola pojednává o vybraných právních předpisech týkajících se kybernetické bezpečnosti.

4.1 Zákon o kybernetické bezpečnosti a související předpisy

Podkapitola pojednává o základních a souvisejících předpisech týkající se kybernetické bezpečnosti.

Zákon č. 181/2014 Sb. o kybernetické bezpečnosti

„Tento zákon upravuje práva a povinnosti osob a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti, zapracovává příslušné předpisy Evropské unie a upravuje zajišťování bezpečnosti sítí elektronických komunikací a informačních systémů. Nevztahuje na informační nebo komunikační systémy, které nakládají s utajovanými informacemi.“ (Česko, 2014, a)

Vznik tohoto zákona podpořily hlavně požadavky a závazky vůči mezinárodním společenstvím NATO a Evropské unii. Nemalou mírou také přispěl výskyt DDoS útoků.

Cílem zákona je vytvořit zákonné postavení státní instituce zodpovědné za zajišťování kybernetické bezpečnosti státu a také regulací klíčových subjektů. Jelikož státní moc lze uplatňovat pouze na základě zákona byl vznik zákona nevyhnutelný. (Doucek, Konečný a Novák, 2019)

Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (dále Směrnice NIS)

Cílem této směrnice je harmonizovat právní úpravu v oblasti bezpečnosti sítí a informačních systémů u členských států a zavést jednotný standard úrovně kybernetické bezpečnosti. Některé povinnosti vyplývající z této směrnice již ČR řeší v rámci zákona č. 181/2014 Sb., o kybernetické bezpečnosti. Směrnice se zabývá a rozšiřuje typy subjektů, které budou mít stanoveny povinnosti v oblasti kybernetické bezpečnosti. (NÚKIB, 2021, d)

Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti

Zpracovává Směrnici NIS a pro informační a komunikační systémy. Upravuje obsah a strukturu bezpečnostní dokumentace a bezpečnostních opatření. Rozděluje a hodnotí významnost

kybernetických incidentů, způsob a náležitosti hlášení incidentů a způsob likvidace dat, informací a provozních údajů. (NÚKIB, 2021, d)

Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích

Tato vyhláška stanovuje významné informační systémy a také kritéria pro jejich určení. V roce 2020 byla přijata novelizace této vyhlášky, která zpřesňuje kritéria významnosti informačního systému. Vyhláška bude přijímána po jednotlivých vlnách v letech a kompletně tato vyhláška nabude účinnosti v roce 2023. (NÚKIB, 2021, d)

Vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby

Tato vyhláška zpracovává směrnici NIS a upravuje odvětvová a dopadová kritéria pro určení provozovatele základní služby a vymezení významnosti dopadu narušení základní služby na zabezpečení společenských nebo ekonomických činností podle § 22a odst. 1 zákona o kybernetické bezpečnosti. Vyhláška byla zpracována NÚKIB ve spolupráci s odbornou veřejností. (NÚKIB, 2021, d)

4.2 Související právní předpisy

Podkapitola se zabývá vybranými souvisejícími právními předpisy týkající se bezpečnosti.

Ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky

Ústavní zákon stanovuje základní povinnosti státu k zajištění svrchovanosti, územní celistvosti, demokratických základů, ochrany životů, zdraví a majetkových hodnot. Definuje způsob zajištění bezpečnosti ČR a povinnosti jednotlivých státních orgánů, orgánů územních celků, právnických a podnikajících fyzických osob podílejících se na zajišťování bezpečnosti státu. (Česko, 1998)

Zákon č. 240/2000 Sb. o krizovém řízení a o změně některých zákonů (krizový zákon)

Stanovuje působnost a pravomoc veřejných institucí, práva a povinnosti právnických a fyzických osob při přípravě a řešení mimořádných událostí (dále MÚ). Zabývá se také ochranou kritické infrastruktury (dále KI) na základě Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvků KI, kde řeší mimo jiné vztah mezi KI a kritickou informační infrastrukturou. (Česko, 2000)

Zákon č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti

Zákon se zabývá klasifikováním informací jako utajovaných, stanovuje, za jakých podmínek k nim přistupovat a s tím spojených požadavků na jejich ochranu. Dále se zabývá

bezpečnostním řízením, výkonem státní správy ve vztahu k utajovaným informacím a také přestupky. (Česko, 2005)

Zákon č. 110/2019 Sb. o zpracování osobních údajů

V zákoně jsou zapracované příslušné předpisy Evropské unie a je navázán na další příslušný předpis. Upravuje práva a povinnosti při zpracování osobních údajů ve vztahu k naplnění práv na jejich ochranu. (Česko, 2019)

4.3 Normy, standardy a metodiky

Standard a norma jsou často považovány za synonyma, avšak rozdíl mezi těmito pojmy tu je. Pokud je označení ČSN ISO/IEC tak se jedná o dokument vydaný „Českou agentura pro standardizaci“ (dále ČAS). Pokud se jedná o dokument s označením ISO/IEC byl tento dokument vydán organizací „International Organization of Standardization“ (dále ISO) (ISO, 2021)

4.3.1 Česká agentura pro standardizaci

Zabývá se tvorbou, vydáváním a distribucí technických norem. Byla zřízena „Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví“ (dále ÚNMZ) podle zákona č. 265/2017 Sb., o technických požadavcích na výrobky. Od roku 2018 převzal ČAS od ÚNMZ všechny činnosti. (Agentura, © 2021)

4.3.2 Mezinárodní organizace pro standardizaci

Jedná se o nevládní organizaci se sídlem v Ženevě ve Švýcarsku. Svoji činnost zahájila již v roce 1947. Prostřednictvím svých členů sdružuje odborníky, aby sdíleli znalosti a vyvíjeli dobrovolné mezinárodní normy založené na konsensu, relevantní pro trh, které podporují inovace a poskytují řešení globálních výzev. K vytvoření standardu zapotřebí spousta lidí, kteří spolupracují. Proces hlasování je klíčem ke konsenzu. Pokud se toho dosáhne, návrh je na cestě stát se normou ISO. Pokud nedojde k dohodě, bude návrh dále upravován a znovu se o něm hlasuje. Od prvního návrhu po konečné zveřejnění trvá vytvoření standardu obvykle asi 3 roky. (ISO, 2021)

4.3.3 Normy týkající se bezpečnosti informací

Vybrané normy týkající se bezpečnosti informací pochází z množiny norem ČSN ISO/IEC 27000. Tyto normy se zabývají řízením bezpečnosti informací v rámci mezinárodní organizace pro normalizace ISO. (Doucek, Konečný a Novák, 2019)

ČSN ISO/IEC 27000:2020 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník

Jedná se o odborný slovník, jehož úkolem je definovat základní modely a pojmy používané při řízení bezpečnosti informací. Jako jediná z rodiny norem ČSN ISO/IEC 27000 je poskytována zdarma. (Doucek, Konečný a Novák, 2019)

ČSN ISO/IEC 27001:2014 Informační technologie – Bezpečnostní techniky – Systém řízení bezpečnosti informací – Požadavky

Tato mezinárodní norma určuje a specifikuje požadavky na udržování a neustále zlepšování řízení bezpečnosti informací v rámci kontextu rizik činnosti dané organizace. Zabývá se také způsobem posouzení rizik a jejich následného ošetření. Tuto normu je možné aplikovat ve všech typech organizací bez ohledu na velikost a povahu. (Seznam ČSN, © 2021)

ČSN ISO/IEC 27002:2014 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Soubor postupů pro opatření bezpečnosti informací

Norma je určena k výběru vhodných opatření v rámci procesu řízení bezpečnosti informací založeném na ČSN ISO/IEC 27001. Dále je využitelná při vývoji směrnic pro řízení bezpečnosti informací organizace s ohledem na jejich konkrétní prostředí rizik. Bezpečnost informací je dosaženo zavedením vhodné sady opatření, vhodných politik, procesů a zavedení vhodného hardwaru softwaru. (Seznam ČSN, © 2021)

ČSN ISO/IEC 27003:2018 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Pokyny k implementaci systémů řízení bezpečnosti informací

Představuje pokyny k požadavkům na systém řízení bezpečnosti informací dle specifikace v normě ČSN ISO/IEC 27001. Dále poskytuje doporučení, možnosti a oprávnění. Jejím účelem není poskytování obecných pokynů týkající se všech aspektů, ale má pouze doporučující charakter na základě specifik dané organizace. (Seznam ČSN, © 2021)

ČSN ISO/IEC 27004:2018 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Monitorování, měření, analýza a hodnocení

Poskytuje směrnice organizacím, jejich cílem je hodnotit výkonnost bezpečnosti informací a napomáhat k efektivitě systému řízení bezpečnosti informací, aby byly splněny požadavky normy ČSN ISO/IEC 27001. Stanovuje způsoby monitoringu a měření výkonnosti bezpečnosti informací. Normu mohou implementovat organizace všech typů a velikostí. (Seznam ČSN, © 2021)

ČSN ISO/IEC 27005:2019 Informační technologie Bezpečnostní techniky – Řízení bezpečnosti informací

Norma slouží k podpoře implementace bezpečnosti informací na základě přístupu k řízení k řízení přístupu. Obsahuje směrnice pro řízení rizik bezpečnosti informací. Pro její plné pochopení je třeba je nutná znalost konceptů, modelů, procesů a terminologie obsažené v normách ČSN ISO/IEC 27001 a ČSN ISO/IEC 27002. (Seznam ČSN, © 2021)

ČSN ISO/IEC 27006:2016 Informační technologie – Bezpečnostní techniky – Požadavky na subjekty poskytující audit a certifikaci systému řízení bezpečnosti informací

Norma nastavuje kritéria pro organizace zabývající se auditem a certifikací systémů řízení. Hlavním cílem je poskytnutí informací akreditačním orgánům, které se zabývají certifikací a akreditací systému řízení bezpečnosti informací. (Seznam ČSN, © 2021)

ČSN ISO/IEC 27032:2013 Informační technologie – Bezpečnostní techniky – Směrnice pro kybernetickou bezpečnost

Tato norma obsahuje doporučení ohledně zlepšení bezpečnosti kyberprostoru. Obsahuje základní bezpečnostní postupy pro oblasti, jako jsou bezpečnost informací, sítí, internetu a ochrana kritické informační infrastruktury (Seznam ČSN, © 2021)

ČSN ISO/IEC 27033 Informační technologie - Bezpečnostní techniky - Bezpečnost sítě

Norma se zabývá různými aspekty síťové bezpečnosti. Skládá se se šesti dílů:

- Přehled a pojmy.
- Směrnice pro návrh a implementaci bezpečnosti sítě.
- Referenční síťové scénáře – Hrozby, techniky návrhu a otázky řízení.
- Zabezpečení komunikace mezi sítěmi s využitím bezpečnostních bran.
- Zabezpečení komunikace napříč sítěmi použitím virtuálních privátních sítí (VPN).
- Zabezpečení přístupu k bezdrátové IP síti. (Seznam ČSN, © 2021)

4.3.4 Metodiky

Při výstavbě informačního systému je nutné klást důraz na budování bezpečnosti informací. Pro tento účel lze využívat technické standardy, které určují základní parametry v oblasti bezpečnosti informačních systémů a jejího hodnocení z pohledu certifikace, klasifikace a posuzování. Nejpoužívanější a neznámější jsou metodiky Information Technology

Infrastructure Library (dále jako „ITIL“) a Control Objectives for Information and Related Technology (dále jako „COBIT“). (Smejkal, Sokol a Kodl, 2019).

COBIT

Jedná s o soubor těch nejlepších praktik pro řízení informací k dosažení strategických cílů organizace při minimalizaci rizik. Je určen především pro výkonný management. (Smejkal, Sokol a Kodl, 2019).

ITIL

Tato metodiky představuje soubor osvědčených postupů pro poskytování IT služeb. Systematický přístup subjektům pomáhá řídit rizika a budovat stabilní prostředí IT. Poskytuje osvědčené pokyny pro správu IT po celou dobu jejího životního cyklu. (Smejkal, Sokol a Kodl, 2019).

4.4 Kyberkriminalita

Využívání výpočetní techniky je dnes více než běžné. Nalézt oblasti lidské činnosti kde nejsou využívány informační a komunikační technologie v podstatě nelze nalézt. Tím že rostou možnosti využívání těchto technologií k vědecko-technickému pokroku, tak zároveň rostou i možnosti pro páchání trestné činnosti. (KOLOUCH, 2016)

4.4.1 Klasifikace forem kyberkriminality

Klasifikace kyberkriminality dle „Úmluvy o počítačové kriminalitě“ dělí trestné činy do čtyř kategorií:

- Tresné činy proti utajování, integritě a dostupnosti dat a systémů.
- Trestné činy související s počítači.
- Trestné činy související s obsahem.
- Trestné činy související s porušováním autorských práv pomocí počítačových systémů.

„Jménem České republiky byla Úmluva podepsána ve Štrasburku dne 9. února 2005. S Úmluvou vyslovil souhlas Parlament České republiky a prezident republiky ji ratifikoval. Ratifikační listina České republiky byla uložena u generálního tajemníka Rady Evropy, depozitáře Úmluvy dne 22. srpna 2013.“ (Česko, 2014, b)

Dodatkový protokol poté definuje další kybernetické trestné činy týkající se rasizmu, xenofobie, popírání, snižování nebo ospravedlňování zločinů proti lidskosti. Existuje celá řada klasifikací kybernetické trestné činnosti např. dle Komise expertů Rady Evropy pro zločiny v kyberprostoru, eEurope+ a další. (Kolouch, 2016)

4.4.2 Prostředky trestního práva

Pokud se jedná o kyberkriminalitu, tak postih útočníka páchajícího kybernetický útok není možný, pokud tento útok není možné zařadit pod ustanovení trestního zákona. Je však možné útočníka stíhat podle prostředky správního nebo občanského práva. Jde-li o vymáhání trestního práva, tak je v roli vymahatele stát, respektive jeho orgány. Jde-li však o právo soukromé, je nutné, aby se na vymáhání práva podílela osoba dotčená nebo poškozená kybernetickým útokem.

Pokud se jedná o aplikaci práva správního, je prostředkem, který umožňuje postih protiprávního jednání, jež má povahu přestupku vizuálního zákon č. 200/1990 Sb., o přestupcích, který definuje pojem přestupku.

Přestupky týkající se občanského soužití:

- „*Přestupku s dopustí ten:*
    - *jinému ublíží na cti tím, že ho urazí nebo vydá v posměch,*
    - *jinému ublíží na zdraví.*
- *přestupku se dopustí ten, kdo úmyslně naruší občanské soužiti tím, že:*
    - *jinému vyhrožuje újmou na zdraví,*
    - *jiného nepravdivě obviní z přestupku,*
    - *se vůči jinému dopustí schválnosti, nebo se vůči jinému dopustí jiného hrubého jednaní.*
- *Přestupku se dále dopustí ten, kdo*
    - *omezuje nebo znemožňuje příslušníku národnostní menšiny výkon práv příslušníků národnostních menšin, nebo způsobí jinému újmu pro jeho příslušnost k národnostní menšině nebo pro jeho etnický původ, pro jeho rasu, barvu pleti, pohlaví, sexuální orientaci, jazyk, víru nebo náboženství, věk, zdravotní postižení, pro jeho politické nebo jiné smýšlení, členství nebo*

> *činnost v politických stranách nebo politických hnutích, odborových organizacích nebo jiných sdruženích, pro jeho sociální původ, majetek, rod, zdravotní stav anebo pro jeho stav rodinný.*“ (Kolouch, 2016)

Při použití občanského práva lze uplatnit zejména občanský zákoník. Je to komplexní norma soukromého práva obsahující řadu ustanovení, které je možné uplatnit v reálné, ale i virtuálním světě. V ustanovení paragrafu 84 občanského zákoníku je stanoveno, že není možné zachytit jakýmkoli způsobem podobu člověka, ze které je možné určit totožnost, bez jeho svolení. Zakazuje také zasahovat do soukromí bez zákonného důvodu. (Kolouch, 2016)

5 KYBERNETICKÉ ÚTOKY

Kybernetický útok je možné definovat jako jakékoli protiprávní jednání útočníka v kyberprostoru, který je směřován proti zájmům jiné osoby za účelem poškození informačních technologií a získávání informací. Takovéto jednání nemusí mít vždy povahu trestného činu, ale může se jednat narušování běžného života napadeného. Za kybernetický útok je považována i jeho příprava nebo stádium pokusu. (Kolouch, 2016)

5.1 Nástroje kybernetických útoků

Kybernetické útoky jsou nástrojem kybernetické kriminality. Značná část kyberkriminality využívá běžné druhy protiprávního jednání, které však přenáší do kyberprostoru. Jedná se o podvody, porušování autorských práv, krádeže, šikanu atd. V tomto prostředí je možno páchat tyto trestné činy rychleji a efektivněji než prostředí reálném. (KOLOUCH, 2016)

Pro ryze kybernetické útoky je třeba použití nástrojů a metod, které útočníkovi napomáhají k úspěšnému uskutečnění jeho útoku a dosažení požadovaného cíle.

5.1.1 Malware

Škodlivý software, známý také jako malware. Je to software, jehož autor má zlomyslný úmysl. Vývojáři malwaru se snaží zabránit důvěrnosti, integritě, dostupnosti dat nebo systémů, které jej zpracovávají, přenášejí a ukládají. Autoři malwaru mohou být motivováni mnoha různými věcmi, včetně vojenská špionáže, ekonomická špionáže a hacktivismu. Malware dnes představuje většinou smíšené hrozby. Dříve se jednalo především o jeden typ hrozby – byl to buď červ, nebo a zadní vrátka, ale ne obojí. Dnes má většina malwaru několik vlastností. Analytici v antimalwarových laboratořích, kteří reverzně analyzují vzorky malwaru obvykle klasifikují malware podle primárního nebo většiny vlastností dle kterých se každý vzorek chová. Malware může například vykazovat vlastnosti červa, trojského koně nebo viru. (Rains, 2020)

Trojské koně

Jedná se o celosvětově nejrozšířenější kategorie malwaru za poslední desetiletí. Trojský kůň spoléhá na sociální inženýrství, aby byl úspěšný. Je to program nebo soubor, který se představuje jako jedna věc, i když ve skutečnosti je věcí druhou, stejně jako metafora trojského koně, na které je založen jeho název. Uživatel je oklamán, aby si jej stáhl a otevřel. Trojské koně se nešíří pomocí neopravených zranitelností nebo slabých hesel jako červi; musí spoléhat na sociální inženýrství. Backdoor je také jednou z jeho variací. Jakmile

uživatel spustí škodlivý program, tak tento umožňuje útočníkům vzdálený přístup k infikovanému systému. V tomto případě mohou potenciálně krást identity, data, softwarové a herní klíče, instalovat software a další malware dle vlastního výběru, zařadit infikovaný systém do botnetů a dalších možných zneužití systému. Toto může zahrnovat vydírání, Distributed Denial of Service (dále DDoS) útoky, ukládání a distribuce nezákonného materiálu nebo jiného využití. (Rains, 2020)

Červi

Další kategorie hrozeb, které využívají neopravené zranitelnosti, jsou červi. Červ disponuje svým vlastním vlastní doručovacím mechanismem, aby se mohl automaticky šířit ze systému do systému. Červi mohou používat unpatched zranitelnosti, chybné konfigurace zabezpečení, slabých hesel a sociálního inženýrství k vlastnímu šíření. Příkladem tohoto typu červa je Conficker. Existuje několik variant tohoto červa. Využívá neopravené chyby zabezpečení. Může se šířit prostřednictvím vyměnitelných jednotek, jako USB disky, stejně tak přes sítě. Červy je velmi je těžké odstranit z prostředí IT, jakmile se do něj dostanou, mohou se totiž „schovat“ do online i offline paměťových médií. (Rains, 2020)

Viry

Viry jsou tu už desítky let. Jedná se o samo replikující se souborové infektory. Viry se mohou šířit, když se jsou neúmyslně zkopírovány do systému. Protože infikují soubory nebo hlavní spouštěcí záznam v systému. Mohou to být velmi „hlučné“ hrozby, které lze snadno odhalit, ale těžko dezinfikovat. V poslední době se viry vrátili do módy. Moderní útočníci, kteří vyvíjejí viry, obvykle nejen infikují soubory jako to dělali jejich předchůdci před desítkami let, ale dnes jsou mnohem nápaditější. Jak již bylo zmíněno, většina hrozeb je smíšená. Moderní viry mají tu vlastnost, že jakmile infikují systém, stahují další malware, deaktivujte antimalwarový software, kradou přihlašovací údaje uložené v mezipaměti, zapínají mikrofon nebo kameru v počítači, shromažďují audio a video data, otevírají backdoor pro útočníky a odesílají ukradená data útočníkům na vzdálené servery. Viry nejsou zdaleka tak rozšířené jako trojské koně, ale počet jejich detekce není zanedbatelný. (Rains, 2020)

5.2 Metody kybernetických útoků

Mimo to, že útočníci používají nástroje, které jím pomáhají dosáhnout svých cílů, existují také metody, jakým způsobem tyto nástroje infikovat do systémů, nebo požadované informace získat přímo od uživatelů. V této podkapitole jsou vysvětleny některé vybrané metody.

5.2.1 Phishing

Phishing je technika sociálního inženýrství, která se snaží získat citlivé informace, obvykle přihlašovací údaje nebo údaje o kreditní kartě, a to pomocí maskováním jako důvěryhodná organizace. Tyto útoky obecně zahrnují e-maily, které směrují uživatele na falešnou webovou stránku, která vypadá jako skutečná. Takové stránky vyzývají uživatele k zadání svých přihlašovacích údajů nebo jiných citlivých informací, aby bylo možné informace shromáždit a použít ke krádeži identity. Často si myslíme, že tyto věci jsou tak zjevné a směšné, že by to nikdo nikdy neudělal, ale tento typ podvodu má úspěšnost a proto je tak oblíbený.

První a nejlepší způsob, jak bojovat proti phishingu, je vzdělávat uživatele. Spíše než je zahanbit za to, že jsou důvěřiví, je mnohem lepší nabídnout jednoduché způsoby jak rozpoznat rozdíl mezi skutečným a falešným e-mailem nebo webovou stránkou. Vzhled e-mailu nebo webové stránky může být klamný. Loga a vzhledy stránek neposkytují žádnou legitimitu, protože je lze snadno zfalšovat nebo zkopírovat. (Brooks, Grow, Craig Jr. a Short, 2018)

5.2.2 Ransomware

Další kategorií malwaru, která může mít potenciálně zničující důsledek je ransomware. Jakmile se ransomware dostane do systému tak zašifruje data nebo uzamkne uživatele mimo pracovní plochu systému. Zamčená plocha zobrazuje zprávu, která požaduje zaplacení výkupného a pokyny, jak ho zaplatit. Úspěšné ransomwarové útoky se dostaly do titulků po celém světě. Útočníci používají ransomware ve svých pokusech o vydírání všech druhu organizací, včetně nemocnic a všech organizací na úrovni státní správy. (Rains, 2020)

5.2.3 Pharming

Pharming je typ kybernetického útoky při kterém útočník napadá webovou stránku a manipuluje s jejím provozem. Cílem je přesměrovat uživatele na ním vytvořený falešný web za účelem sběru dat. Útočníci zpravidla vytváří falešné weby bank nebo internetových obchodů. Na rozdíl od phishingu se pharming nezaměřuje na přímo na manipulaci s uživateli, ale na DNS (Co je pharming, © 2022)

5.2.4 Scanning

Jedná se o soubor procedur pro identifikaci a vytvoření seznamu aktivních hostitelů, portů a služeb, zjišťování operačního systému a architektury cílového systému, identifikaci zranitelností a hrozeb v síti. Síťové skenování se používá k vytvoření profilu cílové organizace. Scanning bývá zpravidla prvním krokem pře zahájením útoku na cílový systém. (Co je skenování portů, © 2022)

5.2.5 Sociální inženýrství

Sociální inženýrství využívá lidské interakce k obcházení normální bezpečnosti. Tradiční zabezpečení se zlepšuje a zneužití sítě je stále obtížnější, tak se hackeři uchylují k psychologické manipulaci, aby dosáhli svých cílů. Máme tendenci tento koncept podceňovat, ale sociální inženýrství funguje překvapivě dobře, pokud je dobře promyšlené a sofistikované. Jádro problému je v tom, že lidé chybují a jsou přehnaně nápomocní a důvěřiví. Když někdo narazí na dobře promyšlený útok, bez řádného tréninku uvědomění jsou lidé až příliš důvěřivý. Některé podvody sociálního inženýrství jsou tak realistické, že je lze jen velice obtížně rozpoznat. Jedinou možnou prevencí je proto vzdělávání uživatelů v této problematice. (Brooks, Grow, Craig Jr. a Short, 2018)

5.2.6 DDoS

Distributed Denial of Service je druh útoku jehož účelem je narušit funkci některé internetové služby formou zahlcení jejich serverů. Je známo, že existuje mnoho způsobů, jak zaplavit síť nebo službu s požadavky, které mohou v konečném důsledku srazit i ty největší servery. Nejlepší, v co lze doufat, je jejich minimalizace dopadu a mít plán, jak se s nimi vypořádat. Ve skutečnosti totiž neexistuje způsob, jak být vůči nim zcela imunní. DDoS útok využívá na mnoha kompromitovaných systémech různé sítě (označované jako botnety) k zajištění útoku. Botnet systémy jsou obvykle infikovány trojským koněm, ale existuje mnoho způsobů, jak infikovat malware do počítače. Protože útok může pocházet ze stovek

nebo dokonce tisíců počítačů, je ho velice obtížné zastavit. Navíc DDoS útoky jsou tak snadno proveditelné, že je dokáže provést i průměrný útočník a tím způsobit útok, který způsobí zkázu v síti. (Brooks, Grow, Craig Jr. a Short, 2018)

5.3 Kybernetické útoky v ČR

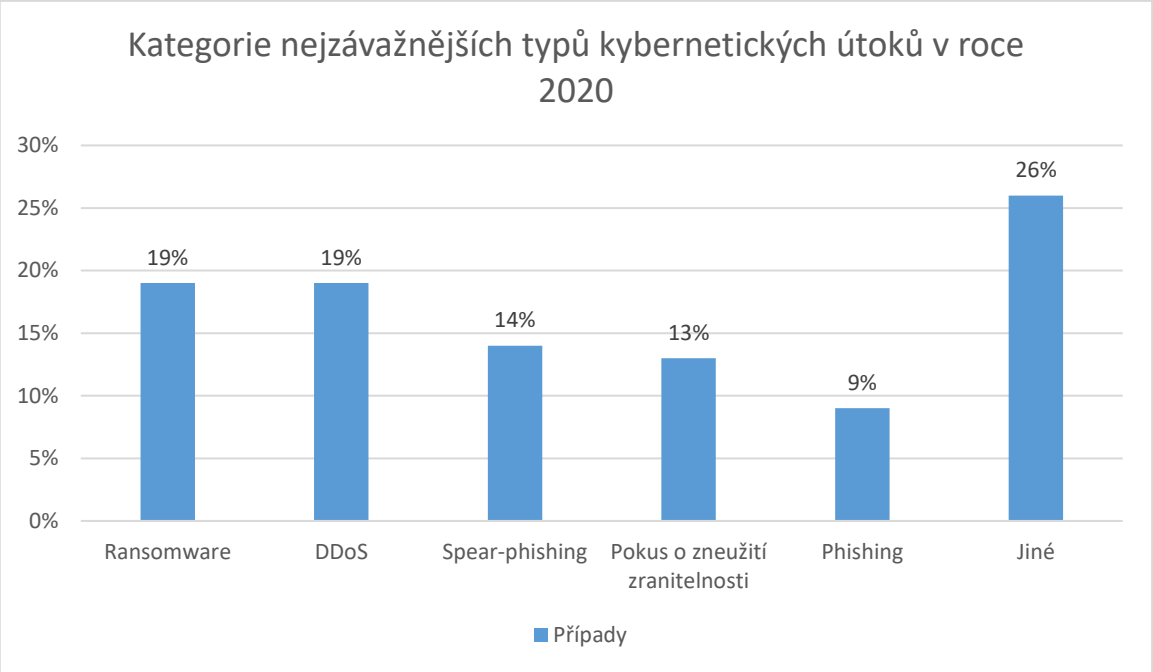
Incidenty týkající se kybernetické bezpečnosti řeší NÚKIB. Jeho účel a působnost je popsána v předcházející kapitole. Tato podkapitola se zabývá počtem a vývojem kybernetických útoků v ČR.

5.3.1 Kybernetické incidenty v ČR

V roce 2020 bylo nahlášeno 468 bezpečnostních kybernetických incidentů. Jedná se o nezanedbatelný meziroční nárůst z 219 v roce 2019. Za tímto nárůstem stojí s vysokou pravděpodobností větší množství kybernetických útoků. Řešeno bylo 99 incidentů, kde u ostatní nebyl zásah NÚKIB nutný.

Nejvýznamnějším útokem z posledních let byl ransomwarový útok na Fakultní nemocnici Brno v březnu 2020, kde došlo k zašifrování systému nemocnice. Incident způsobil výrazné omezení provozu nemocnice ve třech lokalitách. Škody způsobené tímto útokem se vyšplhaly do výše stovek milionů korun. Již v tomtéž měsíci se útok opakoval, a to na Psychiatrickou nemocnici Kosmonosy, kde s útok týkal administrativní části infrastruktura a nebyla zde narušena péče o pacienty. Třetím neméně významným incidentem se stal phishingový útok na emailové schránky strategické stání instituce. Došlo ke kompromitaci desítek emailových účtů a narušení jejich důvěryhodnosti. Došlo k nedostupnosti e-mailových služeb až na dva dny. (NÚKIB, 2021, b)

Celosvětový nárůst kybernetických útoků se potvrdil i v ČR, jak už reflektují předchozí události. Závislost na využívání ICT se v současné době stále více prohlubuje a kybernetických útoků přibývá. Je proto nutné si tuto skutečnost uvědomovat a uplatňovat zásady pro snížení pravděpodobnosti těchto útoků ať už se jedná o jednotlivce nebo společnost.



Graf 3 – Kategorie nejzávažnějších typů kybernetických útoků v roce 2020 (NÚKIB, 2021, b)

5.4 CERT a CSIRT týmy

Computer Emergency Response Team (dále CERT) a Computer Security Incidents Response Team (dále CSIRT) jsou týmy, jejichž úkolem je řešení incidentů a kybernetických hrozeb. I když jejich zkratky mají mírně odlišný význam, tak úkoly těchto týmů jsou v současnosti identické. Tyto týmy vznikají u jednotlivých organizací zprostředkovávajících internetové připojení nebo u těch co internet používají jako hlavní pole působnosti. Základním úkolem CERT/CSIRT týmů je včasně reagovat na hrozbu a spolupracovat při řešení incidentů. Hlavním rozdílem mezi CERT/CSIRT týmy a běžnými bezpečnostními týmy je, že CERT/CSIRT týmy jsou zapojeny do světové bezpečnostní infrastruktury, sdílí informace a postupují dle standardizovaných formálních postupů. Zřizování CERT/CSIRT týmů je vhodné u každého provozovatele sítí na jakékoli úrovni.

CERT/CSIRT týmy na vládní a národní úrovni jsou zvláštní formou těchto týmů. Národní CERT/CSIRT týmy jsou volbou poslední instance, jejichž úkolem je poskytovat pomoc při zásahu, pomoci a intervenci. Nemají možnost přímého zásahu, ale pouze zprostředkovat kontakt mezi napadeným a původcem. Jejich role převážně koordinační. Dále je jejich funkce vzdělávací, kde působí na veřejnost s cílem působit osvětu v této oblasti.

Vládní CERT/CSIRT týmy se zaměřují na státní správu a samosprávu a incidenty týkající se ohrožení státu a jeho služeb. Při ochraně kritické informační infrastruktury a významných informačních systémů hrají vládní CERT/CSIRT týmy zásadní roli dle zákona č. 181/2014 Sb. o kybernetické bezpečnosti. (Kolouch a Bašta, 2019)

6 DÍLČÍ ZÁVĚR

Kybernetická bezpečnost je pojem, který je v dnešní době často skloňován, avšak ne každý ví, co tato problematika skutečně obnáší. Jedná se o rozsáhlou multidisciplinární problematiku, která zasahuje do životů států, společností, ale i jednotlivců. Momentální stav ukazuje na nepředstavitelnost života bez ICT a jejich využití je všude kolem nás.

Studium této problematiky ukazuje základní principy kybernetické bezpečnosti, jaký je stav v ČR a jaké jednotlivé instituce se touto problematikou zabývají. Zabývá se typy kybernetických útoků, jakým způsobem jsou tyto útoky řešeny na národní úrovni a také v neposlední řadě legislativou, která zahrnuje postihy a klasifikace těchto útoků dle práva. Ne vždy je útok možné klasifikovat jako přestupek nebo dokonce trestný čin, a to tyto útoky tvoří ještě více nebezpečné.

Stále si ještě populace neuvědomuje, že terčem útočníka se může stát každý z nás. Ať už se jedná o otázku pracovního nebo soukromého života.

II. PRAKTICKÁ ČÁST

7 POPIS VYBRANÉHO SUBJEKTU

Jelikož se jedná o otázku kybernetické bezpečnosti, tak o zkoumaném subjektu bude stále hovořeno jak o subjektu a nebude blíže specifikován jeho název, ani přesná oblast jeho působnosti. Při dohovoru se subjektem bylo jednou z podmínek zachování jeho anonymity z důvodu bezpečnosti. Z tohoto důvodu nebude práce obsahovat přesné půdorysy, plány, fotodokumentaci, ani schémata z prostor subjektu a popis jeho činnosti bude popisován tak, aby nebylo možné subjekt přesně specifikovat.

Subjekt se zabývá stavbou přírodních koupacích biotopů a klientským servisem v této oblasti. Zpracovává data, informace a plány. Provádí také vlastní stavební činnost menšího rozsahu, výrobu a provozuje vozidla a další stroje. Lokace subjektu je v areálu, kde se nachází také další společnosti.

7.1 Identifikace aktiv subjektu

Kapitola se zabývá identifikací aktiv subjektu. V rámci bezpečnosti informací subjektu je nezbytné vytvoření seznamu aktiv a určení odpovědnosti za jejich ochranu. Dle normy ČSN/IEC 27005, příloha B dělíme aktiva na dvě základní skupiny.

7.1.1 Primární aktiva

Jedná se o informace, činnosti a procesy, při jejichž ztrátě by byla ohrožena nebo negativně ovlivněna činnost subjektu. (Seznam ČSN, © 2021)

- **Osobní informace**

  Osobní informace zaměstnanců a klientů. Jejich únik by byl měl za důsledek porušení nařízení o ochraně osobních údajů (dále GDPR), také ztrátu důvěryhodnosti a dobrého jména subjektu. Zneužití osobních údajů patří mezi významné bezpečnostní hrozby.

- **Zásadní informace důležité pro podnikatelskou činnost**

  Mezi tyto aktiva patří informace o výběrových řízeních, cenové nabídky a další informace týkající se výběrových řízení. Únik těchto aktiv ke konkurenčním společnostem by měl za následek ovlivnění hospodářské soutěže. Jelikož se subjekt podílí i státních zakázkách byla by způsobena značná škoda.

- **Strategické informace**

  Informace a plány rozvoje společnosti, rozšíření služeb a uvedení nových produktů a služeb. Tyto aktiva mají vysokou hodnotu a jejich zneužití by mělo za následek strategickou nevýhodu pro společnost na trhu a konkurenční politice.

7.1.2 Podpůrná aktiva

Do této kategorie patří software, hardware, zaměstnanci a další potřebné pro podporu primárních aktiv. (Seznam ČSN, © 2021)

Hardware

- **Mobilní zařízení**

  Každý zaměstnanec je vybaven mobilním telefonem, pomocí kterých je vedena evidence docházky a odpracované doby. Vedoucí zaměstnanci jsou vybaveni notebooky. Každé z těchto zařízeních je zabezpečeno heslem a je určeno k používání pouze zaměstnanci, který si zařízení převzal.

- **Pevné zařízení**

  Vedoucí zaměstnanci disponují osobními počítači v kancelářích společnosti. Osobní počítače jsou chráněny heslem. V sídle společnosti je umístěn server, který slouží pouze jako podpůrný prvek pro ukládání naskenovaných dokumentů, jinak je používáno placené cloudové úložiště.

- **Zpracovatelské periferie**

  Tiskárny, kopírka a skener jsou umístěny v kanceláři a nejsou zabezpečeny hesly. Tyto zařízení jsou využívána jako sdílená.

- **Elektronická media**

  Elektronická média jsou používána pouze při výběrových řízeních, pokud je požadavek zadavatele na formu odevzdání nabídky touto formou. Ostatní datový tok probíhá pouze po síti.

- **Statická média**

  Dokumentace v papírové podobě je uložena v trezoru nebo uzamykatelné kartotéce.

Software

Operační systém a další používaná software je pořízený legální cestou a pravidelně aktualizován. Administrace je povolena zaměstnancům a starají se také o údržbu, kterou jsou schopni zvládnout. V případě problému se softwarem, kterou není možné řešit vlastními silami je kontaktována specializovaná firma.

Síť

Pevná zařízení jsou připojena ethernetovým síťovým kabelem. Mobilní zařízení jsou připojena na bezdrátovou síť v kanceláři společnosti nebo pomocí poskytovatele mobilních služeb na mobilní internetové připojení.

Vozidla a technika

Společnost disponuje sedmi osobními služebními vozidly, které jsou přiděleny jednotlivým zaměstnancům. Vozidla jsou vybavena GPS lokátory pro evidenci pohybu vozidel pro zpracování knihy jízd a také jako prevence odcizení. Dále společnost disponuje dvěma bagry, nákladním vozidlem, vysokozdvižným vozíkem, smykovým nakladačem a kolovým dumperem. Tato technika je také vybavena GPS lokátory. Vozidla menších rozměrů jsou parkována ve skladovacích prostorech firmy a větší před jejím sídlem.

7.1.3 Vlastnictví aktiv

Veškerá aktiva jsou ve vlastnictví subjektu a jsou využívána dle přidělení jednotlivým zaměstnancům. Je možné je rozčlenit na trvale přidělená aktiva, jako jsou výpočetní technika a mobilní zařízení a osobní vozidla. Na dočasně přidělení, jako jsou nákladní vozidlo, bagr a smykový nakladač atd. Nakládání s aktivy je předem definováno.

7.1.4 Vracení aktiv

Dočasně přidělená aktiva se po dokončení směny, nebo popřípadě projektu, vrací zpět do sídla společnosti, je provedena údržba a uložení materiálu a techniky.

7.2 Bezpečnost subjektu

Tato podkapitola je zaměřena na aktuálně zjištěný stav kybernetické bezpečnosti subjektu v oblasti fyzické bezpečnosti a bezpečnosti služeb a sítí. Informace byly získány na základě řízeného rozhovoru s jednatelem subjektu a pozorováním.

7.2.1 Fyzická bezpečnost

Tato kapitola se zabývá stavem fyzické bezpečnosti subjektu. Fyzická bezpečnost subjektu je řešena na několika úrovních. První je řešena v oblasti zabezpečených oblasti a druhá se týká zabezpečená samotného zařízení pro zpracování informací.

Zabezpečené oblasti

Zabezpečené oblasti jsou první úrovní při ochraně informací.

- **Fyzický bezpečnostní perimetr**

Sídlo společnost se nachází v areálu, ve kterém se nachází řada dalších firem. Areál je zabezpečen stálou službou na vjezdu a vchodu. Jelikož je na vjezdu do areálu velká fluktuace osob a automobilů, je prováděna pouze namátková kontrola vstupu a vjezdu. Tudíž ji nelze považovat za efektivní. Kanceláře a skladovací prostory společnosti nejsou zabezpečeny obvodovou ochranou a tudíž jsou volně přístupné z celého areálu.

- **Zabezpečení kanceláří, místností a vybavení**

Všechny budovy jsou zabezpečeny elektronickým zabezpečovací systém a video dohledovým systémem. Přístup k vybavení pro zpracovávání informací mají pouze určení zaměstnanci. Zabezpečení je řešeno pouze jedním generálním kódem a není možné identifikovat osobu, která deaktivovala zabezpečovací zařízení.

- **Ochrana před přírodními a vnějšími hrozbami**

Sídlo společnosti je vybaveno pouze elektrickou protipožárním zařízením. Před přírodními hrozbami ani nehodami není chráněno.

- **Práce v zabezpečených oblastech**

Společnost nemá vyčleněny zabezpečené oblasti. Do kanceláří mají však přístup pouze vyčlenění zaměstnanci. Práce zaměstnanců neprobíhá pod dohledem. Pořizování audio a video záznamů a kontrola zařízení není prováděna.

- **Oblasti pro nakládku a vykládku**

Prostory pro nakládku a vykládku jsou samostatné a odděleny od vybavení pro zpracovávání informací. Skladovací prostory jsou zabezpečeny elektronickým zabezpečovacím zařízením a video-dohledovým systémem. Kontrola materiálu před výbušninami a nebezpečnými

chemickými látkami neprobíhá. Neprobíhá evidence a registrace příchozího materiálu a příchozí a odchozí zásilky nejsou odděleny.

Zařízení

Zařízení pro zpracovávání informací je nutné chránit proti poškození, odcizení a ztrátě. Je to nutné z důvodu zabránění kompromitace aktiv, popřípadě přerušení chodu organizace.

- **Umístění zařízení a jeho ochrana**

Přístup do kanceláře mají i zaměstnanci, kteří nejsou určeni pro zpracovávání informací. Zařízení je v prostoru umístěno tak, aby nedocházelo ke sledování informací. Zařízení pro ukládání informací není umístěno v prostorech mimo neoprávněný přístup ostatních zaměstnanců. Zařízení jsou zabezpečena heslem. Bezpečnostní parametry hesel nejsou regulovány. Pravidla pro stravování a pití v blízkosti zařízení nejsou nastavena. Budova a rozvody elektřiny jsou chráněny před bleskem, ale neprobíhá monitoring vhodné vlhkosti a teploty. Nepoužívají se membránové klávesnice ani není zařízení nijak chráněno před vlivem elektromagnetického vyzařování.

- **Podpůrné služby**

Zařízení není chráněno před výpadkem napájení ani dalšími poruchami.

- **Bezpečnost kabelových rozvodů**

Pouze napájení je vedeno pod zemí, jinak kabeláž není nijak chráněna před odposlouchávánim, rušením nebo poškozením.

- **Údržba zařízení**

Doporučené servisní intervaly jsou dodržovány a servis provádí vždy autorizovaný servis. Nejsou však prováděny záznamy o podezřelých chybách ani o jejich nápravě. Servis se provádí na zařízení s informacemi a personál se neprověřuje. Před novým uvedením do provozu se zařízení neprověřuje proti neoprávněné manipulaci.

- **Přemístění aktiv**

Odpovědné osoby mají povoleno přemisťování zařízení bez časového omezení. Není vedena evidence o přemístění. Není prováděno kontrolování těchto zařízení.

- **Bezpečnost zařízení a aktiv mimo prostory organizace**

Zařízení je provozováno mimo prostory organizace jen se svolením. Není vedena historie zařízení ani všech kdo ho používají. Zřízení nesmí být ponecháváno na veřejných místech bez dozoru. Práce mimo prostory organizace není nijak omezena. Zpracování informací probíhá na mobilních zařízeních na dálku.

- **Bezpečná likvidace nebo opakované použití zařízení**

Paměťová média nejsou fyzicky ničena, ale jsou formátována tak, aby je nebylo možné obnovit.

- **Neobsluhovaná uživatelská zařízení**

Uživatelé jsou proškoleni, po ukončení relace uzamknout zařízení, odhlásit se z aplikace nebo síťových služeb. Zařízení jsou zabezpečena heslem. Není však požadován mechanismus změny hesel ve stanovených časových intervalech.

- **Zásada prázdného stolu a prázdné obrazovky**

Citlivé informace jsou uloženy v uzamykatelných kartotékách a trezoru. Zařízení ke zpracování informací jsou vždy uzamčena a odhlášena. Použití tiskárny a kopírky je volně přístupné a odebírání médií je volné, nijak nezabezpečené.

7.2.2 Bezpečnost služeb a sítí

Kapitola s zabývá stavem zabezpečení služeb a sítí subjektu, jelikož pokud je důkladně zabezpečena fyzická bezpečnost společnosti a jejich zařízení pro zpracovávání informací, existuje stále reálná hrozba vyplývající z kyberprostoru.

- **Malware**

Zařízení pro zpracování informací společnosti jsou zabezpečena proti malware pomocí antivirových programů. Software a firmware zařízení je na udržován aktualizovaný. Aktualizace provádí manuálně každý zaměstnanec na svém zařízení. Veškerá externí zařízení jsou po připojení kontrolována na přítomnost malware. Uživatelé zařízení mají plná administrátorská práva a proto je vysoké riziko nakažení při instalaci určitých typů rizikových softwarů.

- **Školení zaměstnanců v oblasti kybernetické bezpečnosti**

V této problematice společnost neprovádí školení zaměstnanců. Existuje proto hrozba narušení bezpečnosti informací plynoucí z neznalosti zaměstnance. Rizika spojená s nevyžádanou poštou nebo určitou formou phishingu, malwaru představují nezanedbatelné riziko pro informační bezpečnost společnosti.

- **Kybernetická špionáž**

Problematika kybernetické špionáže je řešena pouze pomocí antimalwarových programů. Není využíváno služeb specializovaných firem zabývajících se touto problematikou.

- **Zálohování dat**

Společnost využívá pro zálohování dat cloudová úložiště a vlastní cloudové úložiště se systémem automatického zálohování.

- **Šifrování dat**

Šifrování dat se neprovádí žádným způsobem.

8 HROZBY

Hrozba je událost náhodná nebo úmyslně vyvolaná, která může mít negativní dopad na subjekt z hlediska důvěrnosti, integrity a dostupnosti aktiv. V této kapitole budou určeny oblasti a popsán aktuální stav, který dále bude sloužit pro identifikaci hrozeb.

8.1 Identifikace hrozeb

Riziko hrozeb může být posuzováno z vícero hledisek. Může se jednat o selhání lidského faktoru úmyslně či neúmyslně, o úmyslné nebo o neúmyslné poškození organizace zvenčí nebo vlastním zaměstnancem. Dalším možnou příčinou vzniku negativního jevu je technické selhání, nebo přírodní vlivy. Selhání ze strany techniky lze předvídat a je mu možné do jisté míry předcházet údržbou a pravidelnými aktualizacemi a kontrolami. Lidský faktor je do jisté míry možné ovlivnit organizačně, ale stálé se jedná o jedno z největších rizik. Přírodní vlivy lze jen těžko předpovídat. Z aktuálního stavu uvedeného výše lze vyhodnotit hrozby, které mohou být pro subjekt rizikové a bude nutná jejich analýza.

8.1.1 Lidé

Lidský faktor je jedním z nejrizikovějších faktorů v této problematice a to, z několika důvodů:

Neúmyslné selhání

K neúmyslnému selhání dochází zpravidla z důvodu nedbalosti, neznalosti směrnic a postupů. (Kresa, 2019)

Neúmyslné lidské selhání	
Nezabezpečení pracoviště	Spuštění škodlivých kódů
Nezabezpečení pracovní stanice	Ztráta integrity dat
Ztráta technického vybavení	Neúmyslná ztráta dat
Poškození technického vybavení	Neautorizovaný používání IS
Prozrazení citlivých informací	Instalace SW z neprověřených zdrojů

Tabulka 1 – Lidské neúmyslné selhání

Neúmyslné selhání organizace

Hrozby organizačních selhání v oblasti lidských zdrojů se týkají zpravidla vědomého nezabezpečení dostatečné přípravy zaměstnanců na vykonávanou pozici, popřípadě jejich celkového nedostatku. (Kresa, 2019)

Neúmyslné selhání organizace	
Nedostatek personálu	Nízká Kvalifikace
Nedostatečné proškolení v oblasti bezpečnosti informací	Absence bezpečnostních pravidel
Nedostatečné stanovení odpovědnosti	Administrátorská práva zaměstnanců

Tabulka 2 – Neúmyslné selhání organizace

Úmyslné poškození

Tyto hrozby mohou pramenit z úmyslu vlastního zaměstnance z důvodů, které mohou být poškození organizace z osobních pohnutek, finanční nebo jiné. Hlavní hrozbou je však externí kybernetický útok na subjekt. (Kresa, 2019)

Úmyslné poškození	
Manipulace s daty	Neautorizovaný přístup do IS
Zneužití uživatelských práv	Kybernetický útok
Zneužití citlivých dat	Ransomware
Poškození HW	Phishing

Tabulka 3 – Lidské úmyslné poškození

8.1.2 Selhání technického zařízení

Využívání technických zařízení s sebou vždy přináší řadu hrozeb. Na těchto zařízení může dojít k nepředvídatelné poruše a dochází k zásadnímu narušení funkčnosti systému. Některé z těchto hrozeb je možné ošetřit relativně jednoduše a jiné pouze z vyššími náklady nebo vůbec. (Kresa, 2019)

Selhání technického zařízení	
Nezabezpečený systém	Nefunkčnost SW
Nedodržování pravidelných aktualizací	Výpadek sítě
Chybná záloha dat	Poškození datových nosičů
Porucha HW	Přerušení dodávky elektrické energie

Tabulka 4 – Selhání technického zařízení

8.1.3 Přírodní hrozby

Hrozby přírodního charakteru mohou mít sice výrazný vliv na celý systém, ale jejich výskyt je možné předpovídat a rizika ošetřit. Z hlediska kybernetické bezpečnosti vybraného subjektu nehrají zásadní roli. (Kresa, 2019)

Přírodní hrozby	
Úder blesku	Požár
Ohrožení vodou	Prach

Tabulka 5 – Přírodní hrozby

9 ANALÝZA RIZIK

Kapitola se zabývá analýzou rizik. Jedná se o proces, který hodnotí úroveň rizika pro daný subjekt. Tento proces identifikuje, hodnotí a z dosažených výstupů navrhuje opatření, které mají za úkol minimalizovat riziko. Zvoleny byly dva typy analýzy, a to metoda KARS, která určuje a hodnotí vzájemnou souvztažnosti identifikovaných rizik a analýza možných vad a jejich následků (dále FMEA), která hodnotí význam, příčiny a důsledky jednotlivých identifikovaných hrozeb. Dále je hodnotí a na výstupu stanovuje číselnou hodnotu jednotlivých rizik. Výstupy z těchto analýz slouží jako základní informace pro návrh opatření a zpracování příručky pro zaměstnance o kybernetické bezpečnosti.

9.1 Metoda KARS

Jedná s o kvalitativní metodu analýzy rizik, která je založena na principu interakce a korelace jednotlivých typů rizik. Jejím cílem je určit vzájemnou souvztažnost jednotlivých druhů nebezpečí. Metoda KARS je zvolena z důvodu určení významnosti všech typů rizik a jejich souvztažnost v rámci vybraného subjektu.

Postup provádění analýzy pomocí metody KARS je následující:

- Seznam zdrojů rizik pro subjekt.
- Výpočet koeficientů aktivity a pasivity.
- Graf souvztažnosti rizik.
- Vyhodnocení analýzy. (Jelšovská a Peterková, 2013)

9.1.1 Seznam zdrojů rizik

Základním krokem k provedení analýzy je určení seznamu zdrojů možných rizik. Tento seznam vychází z předchozí kapitoly identifikace hrozeb. Byl sestaven pomocí týmu zaměstnanců zabývajících se IT u vybraného subjektu metodou brainstormingu.

Bude sestavena tabulka souvztažnosti v podobě matice, kde počty řádků i sloupců odpovídají počtu identifikovaných rizik. Každé riziko (R_i) je porovnáno ve vztahu jinému (R_j) ve smyslu jejich souvztažnosti, za předpokladu, že dané riziko nemůže zapříčinit samo sebe.
Do tabulky dosadíme číslice „1“ a „0“, kde „1“ znamená, že riziko R_i může reálně zapříčinit riziko R_j a „0“ v případě kdy tomu tak není. (Jelšovská a Peterková, 2013)

P.č.	Riziko	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.	18.	19.	20.	$\sum K_{ARi}$
1.	Ztráta technického vybavení	0	0	0	0	0	0	1	0	0	0	0	1	1	0	0	0	1	1	1	1	**7**
2.	Selhání HW	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	**3**
3.	Selhání SW	0	1	0	1	0	0	1	0	0	0	0	1	1	1	1	0	1	1	1	1	**11**
4.	Výpadek sítě	0	0	1	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	1	0	**4**
5.	Přerušení dodávky elektrické energie	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	**4**
6.	Přírodní vlivy	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	**5**
7.	Spuštění škodlivých kódů	0	1	1	1	1	0	0	0	0	0	0	1	1	1	1	0	1	1	1	1	**12**
8.	Nedostatečné proškolení v oblasti bezpečnosti informací	1	0	0	0	0	0	1	0	0	0	1	1	1	1	1	1	1	1	1	1	**12**
9.	Nedostatečné stanovení odpovědnosti	1	0	0	0	0	0	1	0	0	0	1	1	1	1	0	0	0	1	1	1	**9**
10.	Absence bezpečnostních pravidel	0	0	1	1	0	0	1	0	0	0	1	1	1	0	0	0	1	1	1	1	**10**
11.	Zneužití uživatelských práv	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	1	1	1	1	**6**
12.	Zneužití citlivých dat	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	1	1	1	**6**
13.	Neautorizovaný přístup do IS	0	0	1	1	0	0	1	0	0	0	1	1	0	1	1	0	1	1	1	1	**11**
14.	Kybernetický útok	0	1	1	1	1	0	1	0	0	0	0	1	1	0	1	1	1	1	1	1	**13**
15.	Ransomware	0	1	1	1	1	0	1	0	0	0	1	1	1	0	0	0	1	1	1	1	**12**
16.	Phishing	0	0	1	1	1	0	1	0	0	0	1	1	1	1	1	0	1	1	1	1	**13**
17.	Odcizení dat	0	0	1	0	0	0	0	0	0	0	1	1	1	0	0	0	0	1	1	1	**7**
18.	Ztráta integrity dat	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	**2**
19.	Ztráta dostupnosti dat	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	1	0	1	**4**
20.	Ztráta důvěrnosti dat	0	0	1	0	0	0	0	0	0	0	0	1	1	0	0	0	1	1	0	0	**5**
	$\sum K_{PRi}$	**2**	**6**	**12**	**10**	**5**	**0**	**9**	**0**	**0**	**0**	**7**	**14**	**12**	**8**	**8**	**2**	**13**	**15**	**18**	**15**	

9.1.2 Výpočet koeficientů

Koeficienty aktivity a pasivity slouží ke kvalifikaci rizika. Analýza má za cíl posuzovat rizika za využití koeficientů aktivity a pasivity. Pro výpočet koeficientů je nutné provést součet rizik $R_{j,}$ v tomto případě je to x = 20 a z nich stanovit počet možných kombinací x – 1 = 19 z důvodu předpokladu, že riziko R_i nemůže vyvolat samo sebe. Výpočet je proveden dle vzorce $K_{ARi} = (\sum R_i/x\text{-}1) * 100[\%]$ a $K_{PRi} = (\sum R_i/x\text{-}1) * 100[\%]$

- **Koeficient aktivity** (K_{ARi}) – vyjádření počtu závažných rizik, které mohou být vyvolané rizikem R_i vyjádřených v procentech.
- **Koeficient pasivity (**K_{PRi}) – vyjádření počtu rizik, která mohou vyvolat působení rizika R_i vyjádřených v procentech. (Jelšovská a Peterková, 2013)

Koeficient aktivity (K_{ARi}) – výpočet

1. $KARi = \frac{\sum Ri}{x-1} * 100\ [\%] = \frac{7}{19} * 100 = 36{,}84\%$
2. $KARi = \frac{\sum Ri}{x-1} * 100\ [\%] = \frac{3}{19} * 100 = 15{,}79\%$
3. $KARi = \frac{\sum Ri}{x-1} * 100\ [\%] = \frac{11}{19} * 100 = 57{,}89\%$
4. $KARi = \frac{\sum Ri}{x-1} * 100\ [\%] = \frac{4}{19} * 100 = 21{,}05\%$
5. $KARi = \frac{\sum Ri}{x-1} * 100\ [\%] = \frac{4}{19} * 100 = 21{,}05\%$
6. $KARi = \frac{\sum Ri}{x-1} * 100\ [\%] = \frac{5}{19} * 100 = 26{,}32\%$
7. $KARi = \frac{\sum Ri}{x-1} * 100\ [\%] = \frac{12}{19} * 100 = 63{,}16\%$
8. $KARi = \frac{\sum Ri}{x-1} * 100\ [\%] = \frac{12}{19} * 100 = 63{,}16\%$
9. $KARi = \frac{\sum Ri}{x-1} * 100\ [\%] = \frac{9}{19} * 100 = 47{,}37\%$
10. $KARi = \frac{\sum Ri}{x-1} * 100\ [\%] = \frac{10}{19} * 100 = 52{,}63\%$
11. $KARi = \frac{\sum Ri}{x-1} * 100\ [\%] = \frac{6}{19} * 100 = 31{,}58\%$
12. $KARi = \frac{\sum Ri}{x-1} * 100\ [\%] = \frac{6}{19} * 100 = 31{,}58\%$

13. $KARi = \frac{\sum \mathrm{Ri}}{x-1} * 100\ [\%] = \frac{11}{19} * 100 = 57{,}89\%$
14. $KARi = \frac{\sum \mathrm{Ri}}{x-1} * 100\ [\%] = \frac{13}{19} * 100 = 68{,}42\%$
15. $KARi = \frac{\sum \mathrm{Ri}}{x-1} * 100\ [\%] = \frac{12}{19} * 100 = 63{,}16\%$
16. $KARi = \frac{\sum \mathrm{Ri}}{x-1} * 100\ [\%] = \frac{13}{19} * 100 = 68{,}42\%$
17. $KARi = \frac{\sum \mathrm{Ri}}{x-1} * 100\ [\%] = \frac{7}{19} * 100 = 36{,}84\%$
18. $KARi = \frac{\sum \mathrm{Ri}}{x-1} * 100\ [\%] = \frac{2}{19} * 100 = 10{,}53\%$
19. $KARi = \frac{\sum \mathrm{Ri}}{x-1} * 100\ [\%] = \frac{4}{19} * 100 = 21{,}05\%$
20. $KARi = \frac{\sum \mathrm{Ri}}{x-1} * 100\ [\%] = \frac{5}{19} * 100 = 26{,}32\%$

Koeficient pasivity (K_{PRi}) – výpočet

1. $KPRi = \frac{\sum \mathrm{Ri}}{x-1} * 100\ [\%] = \frac{2}{19} * 100 = 10{,}53\%$
2. $KPRi = \frac{\sum \mathrm{Ri}}{x-1} * 100\ [\%] = \frac{6}{19} * 100 = 31{,}58\%$
3. $KPRi = \frac{\sum \mathrm{Ri}}{x-1} * 100\ [\%] = \frac{12}{19} * 100 = 63{,}16\%$
4. $KPRi = \frac{\sum \mathrm{Ri}}{x-1} * 100\ [\%] = \frac{10}{19} * 100 = 52{,}63\%$
5. $KPRi = \frac{\sum \mathrm{Ri}}{x-1} * 100\ [\%] = \frac{5}{19} * 100 = 26{,}32\%$
6. $KPRi = \frac{\sum \mathrm{Ri}}{x-1} * 100\ [\%] = \frac{0}{19} * 100 = 0\%$
7. $KPRi = \frac{\sum \mathrm{Ri}}{x-1} * 100\ [\%] = \frac{9}{19} * 100 = 47{,}37\%$
8. $KPRi = \frac{\sum \mathrm{Ri}}{x-1} * 100\ [\%] = \frac{0}{19} * 100 = 0\%$
9. $KPRi = \frac{\sum \mathrm{Ri}}{x-1} * 100\ [\%] = \frac{0}{19} * 100 = 0\%$
10. $KPRi = \frac{\sum \mathrm{Ri}}{x-1} * 100\ [\%] = \frac{0}{19} * 100 = 0\%$
11. $KPRi = \frac{\sum \mathrm{Ri}}{x-1} * 100\ [\%] = \frac{7}{19} * 100 = 36{,}84\%$
12. $KPRi = \frac{\sum \mathrm{Ri}}{x-1} * 100\ [\%] = \frac{14}{19} * 100 = 73{,}68\%$

13. $KPRi = \frac{\sum \mathrm{Ri}}{x-1} * 100\ [\%] = \frac{12}{19} * 100 = 63{,}16\%$

14. $KPRi = \frac{\sum \mathrm{Ri}}{x-1} * 100\ [\%] = \frac{8}{19} * 100 = 42{,}11\%$

15. $KPRi = \frac{\sum \mathrm{Ri}}{x-1} * 100\ [\%] = \frac{8}{19} * 100 = 42{,}11\%$

16. $KPRi = \frac{\sum \mathrm{Ri}}{x-1} * 100\ [\%] = \frac{2}{19} * 100 = 10{,}53\%$

17. $KPRi = \frac{\sum \mathrm{Ri}}{x-1} * 100\ [\%] = \frac{13}{19} * 100 = 68{,}42\%$

18. $KPRi = \frac{\sum \mathrm{Ri}}{x-1} * 100\ [\%] = \frac{15}{19} * 100 = 78{,}95\%$

19. $KPRi = \frac{\sum \mathrm{Ri}}{x-1} * 100\ [\%] = \frac{18}{19} * 100 = 94{,}74\%$

20. $KPRi = \frac{\sum \mathrm{Ri}}{x-1} * 100\ [\%] = \frac{15}{19} * 100 = 78{,}95\%$

Dle určených koeficientů bude sestavena tabulka, kde je každé riziko charakterizováno koeficientem aktivity a pasivity.

P. č.	**Riziko**	**K_{ARi} [%]**	**K_{PRi} [%]**
1.	Ztráta technického vybavení	36,84	10,53
2.	Selhání HW	15,79	31,58
3.	Selhání SW	57,89	63,16
4.	Výpadek sítě	21,05	52,63
5.	Přerušení dodávky elektrické energie	21,05	26,32
6.	Přírodní vlivy	26,32	0
7.	Spuštění škodlivých kódů	63,16	47,38
8.	Nedostatečné proškolení v oblasti bezpečnosti informací	63,16	0
9.	Nedostatečné stanovení odpovědnosti	47,38	0
10.	Absence bezpečnostních pravidel	52,63	0

11.	Zneužití uživatelských práv	31,58	36,84
12.	Zneužití citlivých dat	31,58	73,68
13.	Neautorizovaný přístup do IS	57,89	63,16
14.	Kybernetický útok	68,42	42,11
15.	Ransomware	63,16	42,11
16.	Phishing	68,42	10,53
17.	Odcizení dat	36,84	68,42
18.	Ztráta integrity dat	10,53	78,95
19.	Ztráta dostupnosti dat	21,05	94,74
20.	Ztráta důvěrnosti dat	26,32	78,95

Tabulka 6 – Tabulka koeficientů aktivity a pasivity

9.1.3 Graf souvztažnosti rizik

Pro přehledné zpracování koeficientů je možné využití grafického řešení analýzy. Na osu x budou vyneseny koeficienty aktivity (K_{ARi}) a na osu y koeficienty pasivity (K_{PRi}). Dále je nutné provést výpočet os, které nám rozdělují graf na čtyři oblasti, které stanovují význam rizika. Pomocí grafu budou určeny nejvýznamnější rizika z pohledu jejich vzájemné souvztažnosti. Tyto nejvýznamnější rizika s stanoví pomocí jejich poloze v jednotlivých oblastech:

- *„Oblast primárně i sekundárně nebezpečných rizik.*
- *Oblast sekundárně nebezpečných rizik.*
- *Oblast primárně nebezpečných rizik.*
- *Oblast relativně bezpečná.“*

Do těchto oblastí bude graf rozdělen pomocí os O_1 a O_2. Osa O_1 je kolmicí k ose x a osa O_2 je kolmicí k ose y. Jejich polohu vypočítáme pomocí níže uvedených vzorců. Dříve než budou polohy os vypočítány, je nutné stanovit procentuální pokrytí daných rizik. Obecně je pro tuto analýzu doporučeno pokrytí 80 % z hodnocených rizik. Z toho vyplývá, že

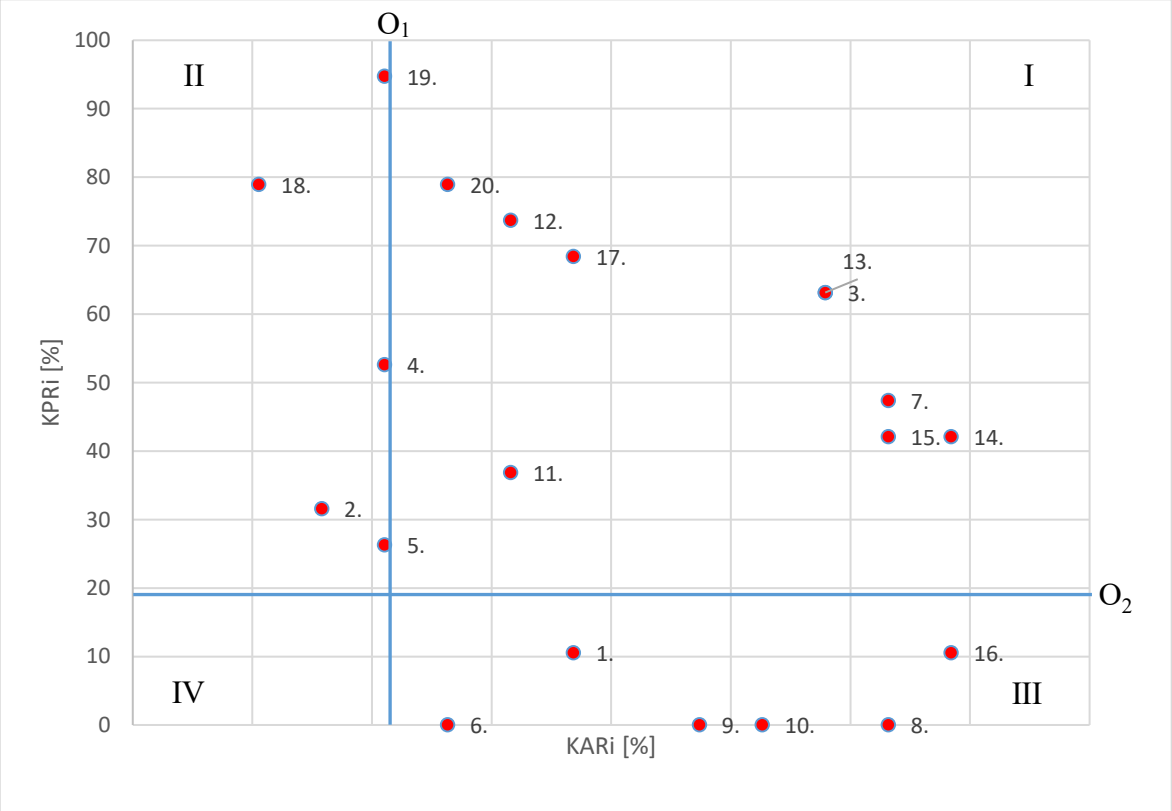
do oblasti primárně a sekundárně nebezpečných rizik dostaneme 80 % rizik analyzovaných. (Jelšovská a Peterková, 2013)

Výpočet os O_1 a O_2:

- $O_1 = K_{Amax} - \frac{K_{Amax} - K_{Amin}}{100} * 80\ [\%] = 68{,}42 - \frac{68{,}42 - 10{,}53}{100} * 80 = 22$

- $O_2 = K_{Pmax} - \frac{K_{Pmax} - K_{Amin}}{100} * 80\ [\%] = 94{,}74 - \frac{94{,}74 - 0}{100} * 80 = 19$

Pomocí těchto výsledků bude sestrojen síťový graf souvztažnosti, s jehož pomocí boudou rizika rozdělena do čtyř oblastí.



Graf 4 – Graf souvztažnosti rizik

9.1.4 Vyhodnocení analýzy

Cílem této analýzy je určení potencionálně nebezpečných rizik v závislosti na jejich souvztažnosti. Jedná se o nebezpečná rizika, která spouští další negativní jevy a způsobují rizika další. Pomocí grafu rozděleného na 4 oblasti je možné tyto rizika vyhodnotit dle jejich závažnosti.

P. č.	Riziko	Kvadrant	Doporučená opatření
1.	Ztráta technického vybavení	III	Evidence vynášení technického zařízení
2.	Selhání HW	II	Servis a pravidelná kontrola
3.	Selhání SW	I	Údržba, kontrola, aktualizace
4.	Výpadek sítě	II	Redundance, údržba
5.	Přerušení dodávky elektrické energie	II	Použití záložního zdroje
6.	Přírodní vlivy	III	Pojištění
7.	Spuštění škodlivých kódů	I	Školení, zamezení administrátorských práv
8.	Nedostatečné proškolení v oblasti bezpečnosti informací	III	Školení, příručka
9.	Nedostatečné stanovení odpovědnosti	III	Stanovení odpovědnosti
10.	Absence bezpečnostních pravidel	III	Zavést systém bezpečnostních pravidel
11.	Zneužití uživatelských práv	I	Přidělení odpovědnosti za svěřená aktiva
12.	Zneužití citlivých dat	I	Přidělení odpovědnosti za svěřená aktiva, kontrola záznamových zařízení
13.	Neautorizovaný přístup do IS	I	Zabezpečení systému
14.	Kybernetický útok	I	Zabezpečení systému
15.	Ransomware	I	Zálohování dat
16.	Phishing	III	Školení, příručka
17.	Odcizení dat	I	Stanovení odpovědnosti

18.	Ztráta integrity dat	II	Použití hashovací funkce
19.	Ztráta dostupnosti dat	II	Zálohování dat a jejich kontrola
20.	Ztráta důvěrnosti dat	I	Kontrola systému, evidence práce s daty

Tabulka 7 – Vyhodnocení analýzy KARS

I. Oblast primárně a sekundárně nebezpečných rizik

V této oblasti jsou rizika, které představují největší nebezpečí. Jelikož se jedná o rizika spouštějící další rizika a mohou působit jako spouštěč stavu, který může způsobit fatální škody subjektu. Do této oblasti spadají selhání softwaru, spuštění škodlivého kódu, zneužití uživatelských práv, zneužití citlivých dat, neautorizovaný přístup do informačního systému, kybernetický útok a Ransoware, Odcizení dat a ztráta důvěrnosti dat. Je patrné, že většina těchto rizik je způsobena lidským faktorem a to úmyslně či neúmyslně. Proti těmto rizikům je velice obtížné se bránit a je možné pouze působit preventivně, formou vzdělávaní v oblasti kybernetické bezpečnosti i v oblasti možných postihů.

II. Oblast sekundárně nebezpečných rizik

Jedná se o rizika, která nenesou závažné riziko spouštění dalších negativních jevů, avšak sama jsou také závažnými sekundárními riziky. Do této oblasti byli zařazeny rizika týkající se výpadku datové sítě, přerušení dodávky elektrické energie, selhání hardwaru, ztráta integrity a dostupnosti dat. Vzhledem k tomu, že subjekt ke svému provozu potřebuje dostupná a celistvá data, může jejich nedostupnost a to i z důvodů výpadku energie nebo sítě způsobit závažné problémy chodu subjektu a také možné finanční ztráty.

III. Oblast primárně nebezpečných rizik

V této oblasti jsou zařazena rizika, jejichž projev může být odhalen až v určitém čase. Jedná se o rizika, která působí v delším časovém horizontu a jejich odhalení může být komplikované. Tato rizika však mohou subjektu způsobit závažné škody. Do této kategorie patří ztráta technického vybavení, působení přírodních vlivů, nedostatečné školení zaměstnanců v oblasti bezpečnosti informací, nedodatečné stanovení odpovědnosti, absence bezpečnostních pravidel a phishing.

IV. Oblast relativně bezpečná

Do této oblasti nebylo zařazeno žádné z hodnocených rizik.

9.2 Failture mode and effects analysis (FMEA)

Analýza možných vad a jejich následků je analytická technika, která má za cíl identifikovat možné poruchy nebo vady v systému. Její historie sahá již do šedesátých let, kde byla vyvinuta během vesmírného programu APOLLO. Tato analýza se nejčastěji používá ve výrobě, je možné ji však využít i pro jiné potřeby. Metoda vyžaduje zkušený tým pro správnou identifikaci možných rizik a vad. Tato analýza hodnotí rizika z pohledu výskytu, dopadu a odhalitelnosti vady. K tomuto účelu slouží hodnotící pomocné tabulky, pomocí kterých dochází k finálnímu výpočtu celkového rizika. (Analýza možností vzniku vad a jejich následků, 2019)

9.2.1 Předmět analýzy

Předmětem analýzy je samotný subjekt a jeho kybernetická bezpečnost. Obecně se jedná o subjekt využívající IS jakožto zásadní pro fungování celého systému. K využití analýzy budou využita data z kapitoly identifikace rizik a tyto rizika budou dále analyzována.

9.2.2 Výběr týmu

Jako tým pracující na identifikaci, analýze a samotném hodnocení dat byl sestaven tým z jednatele subjektu, který zároveň zastává pozici správce IS a má největší přehled o celém fungování. Dále asistentky jednatele, která pracuje s IS a má dostatečnou orientaci v celém systému. V poslední řadě také ze zpracovatele této diplomové práce. Tento tým má něj lepší možný předpoklad správně identifikovat a také hodnotit rizika týkající se vybraného subjektu. Analyzovány budou proces fungování systému při výskytu určité vady (rizika).

9.2.3 Tabulky hodnocení

Tabulky hodnocení slouží ke klasifikaci závažnosti, výskytu a odhalitelnosti poruch a vad v systému. Pomocí hodnotících tabulek bude vypočítáno výsledné riziko, které bude sloužit jako výstupní hodnota jeho závažnosti.

Význam – Vz

Sotva postřehnutelný	Je nepravděpodobné, že by chyba mohla mít účinek na systém	1
Nepatrný	Význam chyby vyvolá v systému jen nepatrnou disfunkci/ohrožení	2-3
Středně závažný	Způsobí ohrožení systému	4-6
Velký	Zásadní význam, který ohrožuje významně funkci systému	7-8
Mimořádně závažný	Mimořádně vysoký význam, který může mít fatální následky pro systém	9-10

Tabulka 8 – Význam chyby

Výskyt – Vy

Nepravděpodobná	Chyba je podstatě vyloučena	1	1 z 1000000
Nepatrná	Proces je pod kontrolou, výskyt chyby jen ojediněle	2	1 z 20000
		3	1 z 4000
Malá	Proces je pod kontrolou, v malém rozsahu jdou chyby myslitelné	4	1 z 1000
		5	1 z 400
		6	1 z 80
Velká	Proces není pod kontrolou, častý výskyt chyb	7	1 z 40
		8	1 z 20
Velmi vysoká	Chybě v podstatě není možné zabránit	9	1 z 8
		10	1 z 2

Tabulka 9 – Výskyt chyby

Odhalení – Od

Vysoká	Metody zabezpečení sytému odhalí s vysokou pravděpodobností možnou chybu (automaticky)	1
Mírná	Zabezpečení systému může odhalit možnou chybu	2 - 5
Malá	Zabezpečení systému s určitou pravděpodobnosti odhalí chybu	6 - 8
Velmi malá	Zabezpečení systému může pouze sotva zjistit chybu	9
Nepravděpodobná	Zabezpečení systému nezjistí nebo nemůže zjistit potencionální chybu	10

Tabulka 10 – Pravděpodobnost odhalení chyby

9.2.4 FMEA

Současný stav									Budoucí stav					
Prvek procesu	Možná vada	Možné následky	Význam (1-10)	Možné příčiny	Výskyt (1-10)	Stávající opatření k odhalení	Odhalitelnost (1-10)	Rizikové číslo (RN)	Opatření	Zodpo-vědnost	Význam (1-10)	Výskyt (1-10)	Odhalitelnost (1-10)	Rizikové číslo (RN)
Neúmyslné lidské selhání	Nezabezpečení pracoviště	Odcizení dat	7	Nedůslednost zaměstnance	2	Mobilní aplikace k zabezpečovací mu systému	2	28	Automatické hlášení zabezpečovacího systému	jednatel	7	2	1	14
	Nezabezpečení pracovní stanice	Neautorizovan ý přístup do IS	9	Absence pravidel bezpečnosti	2	Ne	8	144	Zavedení pravidel pro uživatele	jednatel	9	1	5	45
	Ztráta technického vybavení	Odcizení dat	7	Nedůslednost zaměstnance	1	Ne	1	7	Poučení zaměstnance	Jednatel	7	1	1	7
	Poškození technického vybavení	Nedostupnost dat	2	Nešikovnost zaměstnance	1	Ne	1	2	Poučení zaměstnance	jednatel	2	1	1	2
	Prozrazení citlivých informací	Finanční ztráta	8	Nedostatečné školení	1	Ne	9	72	Logování	jednatel	8	1	3	24
Neúmyslné lidské selhání	Spuštění škodlivého kódu	Kybernetický útok	10	Neznalost	3	Ne	7	210	Zamezení administrátorský ch práv uživatelů, školení	jednatel	10	1	7	70

Akceptovatelné riziko RN ≤10

Významné riziko 10 < RN ≤ 100

Nepřijatelné riziko RN > 100

Současný stav									Budoucí stav					
Prvek procesu	Možná vada	Možné následky	**Význam (1-10)**	Možné příčiny	**Výskyt (1-10)**	Stávající opatření k odhalení	**Odhalitelnost (1-10)**	**Rizikové číslo (RN)**	Opatření	Zodpo-vědnost	**Význam (1-10)**	**Výskyt (1-10)**	**Odhalitelnost (1-10)**	**Rizikové číslo (RN)**
Neúmyslné lidské selhání	Ztráta integrity dat	Finanční ztráta	8	Chyba při vkládaní dat	1	Ne	10	80	Použití hashovací funkce	jednatel	8	1	1	8
	Neúmyslná ztráta dat	Finanční ztráta	8	Zneužití dat	2	Ne	1	16	Zákaz používání přenosných medií	jednatel	8	1	1	8
	Neautorizované používání IS	Odcizení dat	10	Nedbalost zaměstnance	2	Ne	1	20	Školení v oblasti bezpečnosti informací	jednatel	10	1	1	10
	Instalace SW z neprověřených zdrojů	Kybernetický útok	10	Administrátor-ská práva uživatele	5	Ne	1	50	Odebrání administrátorských práv	jednatel	10	1	1	10
Neúmyslné selhání organizace	Nedostatečné proškolení v oblasti informační bezpečnosti	Spuštění škodlivého kódu	8	Problematika není subjektem řešena	3	Ne	1	24	Školení v oblasti informační bezpečnosti	jednatel	8	1	1	8
	Nedostatečné stanovení odpovědnosti	Zneužití dat	5	Zaměstnanec nenese odpovědnost za data	2	Ne	9	90	Stanovit odpovědnost za zpracovávaná data	jednatel	5	1	5	25

Akceptovatelné riziko
RN ≤10

Významné riziko
10 < RN ≤ 100

Nepřijatelné riziko
RN > 100

Současný stav									**Budoucí stav**					
Prvek procesu	Možná vada	Možné následky	**Význam (1-10)**	Možné příčiny	**Výskyt (1-10)**	Stávající opatření k odhalení	**Odhalitelnost (1-10)**	**Rizikové číslo (RN)**	Opatření	Zodpo-vědnost	**Význam (1-10)**	**Výskyt (1-10)**	**Odhalitelnost (1-10)**	**Rizikové číslo (RN)**
Neúmyslné selhání organizace	Nízká kvalifikace	Neúmyslné prozrazení citlivých informací	8	Nízká klasifikace zaměstnance/ ovlivnění z třetí strany	2	Ne	9	144	Zlepšit systém výběrového řízení	jednatel	8	1	9	72
	Absence bezpečnostních pravidel	Neautorizovaný přístup do IS	8	Problematika není subjektem řešena	2	Ne	10	160	Zavést bezpečnostní pravidla	jednatel	8	1	10	80
	Administrátorská práva uživatelů	Instalace SW z neprověřených zdrojů/napadení systému	9	Problematika není subjektem řešena	4	Ne	7	252	Zamezení administrátorských práv uživatelům	jednatel	9	1	2	18
Úmyslné poškození	Manipulace s daty	Ztráta integrity/důvěrnosti dat	8	Úmysl poškození subjektu/ obohacení	2	Ne	10	160	Zálohování dat/kontrola integrity	jednatel	4	1	1	4
	Zneužití uživatelských práv	Odcizení dat/zneužití dat	7	Úmysl poškození subjektu/ obohacení	2	Ne	8	112	Zavedení systému kontrol přístupu k citlivým datům	jednatel	5	1	1	5

Akceptovatelné riziko
RN ≤10

Významné riziko
10 < RN ≤ 100

Nepřijatelné riziko
RN > 100

Současný stav									Budoucí stav					
Prvek procesu	Možná vada	Možné následky	**Význam (1-10)**	Možné příčiny	**Výskyt (1-10)**	Stávající opatření k odhalení	**Odhalitelnost (1-10)**	**Rizikové číslo (RN)**	Opatření	Zodpo-vědnost	**Význam (1-10)**	**Výskyt (1-10)**	**Odhalitelnost (1-10)**	**Rizikové číslo (RN)**
Úmyslné poškození	Zneužití citlivých dat	Finanční ztráta	7	Úmysl poškození subjektu/obohacení	2	Ne	9	126	Zavedení systému kontrol přístupu k citlivým datům	jednatel	5	1	1	5
	Poškození HW	Ztráta dostupnosti dat	5	Záměrné poškození	1	Pojištění	1	5	Ne		5	1	1	5
	Neautorizovaný přístup do IS	Zneužití citlivých dat/finanční ztráty	10	Kybernetický útok	2	Antivirový program/ pravidelné aktualizace	4	80	Konzultace zabezpečení s odbornou firmou	jednatel	10	1	1	10
	Kybernetický útok	Zneužití citlivých dat/finanční ztráty	10	Spuštění škodlivého kódu/neautorizovaný přístup do IS	5	Antivirový program/ pravidelné aktualizace	3	150	Konzultace zabezpečení s odbornou firmou	jednatel	10	2	1	20
	Ransomware	Finanční ztráta	10	Kybernetický útok	3	Antivirový program/ pravidelné aktualizace	3	90	Konzultace zabezpečení s odbornou firmou/zálohování dat	jednatel	4	2	1	8
	Phishing	Odcizení dat	10	Kybernetický útok	4	Ne	5	200	Školení zaměstnanců	jednatel	10	1	1	10

Akceptovatelné riziko
RN ≤10

Významné riziko
10 < RN ≤ 100

Nepřijatelné riziko
RN > 100

Současný stav									Budoucí stav					
Prvek procesu	Možná vada	Možné následky	**Význam (1-10)**	Možné příčiny	**Výskyt (1-10)**	Stávající opatření k odhalení	**Odhalitelnost (1-10)**	**Rizikové číslo (RN)**	Opatření	Zodpo-vědnost	**Význam (1-10)**	**Výskyt (1-10)**	**Odhalitelnost (1-10)**	**Rizikové číslo (RN)**
Selhání technickéh o zařízení	Nezabezpečený systém	Kybernetický útok	10	Nedostatečné technické zabezpečení	2	Antivirový program	5	100	Konzultace zabezpečení s odbornou firmou	jednatel	5	1	2	10
	Nedodržování pravidelných aktualizací	Oslabení bezpečnosti IS	5	Absence údržby systému	4	Antivirový program	4	80	Nastavení administrátorské kontroly aktualizací systému	jednatel	3	1	1	3
	Chybná záloha dat	Nedostupnost dat	6	Selhání systému/ jednotlivce	1	Pouze osobní kontrola	3	18	Automatický systém zálohování s notifikací	jednatel	4	1	1	4
	Porucha HW	Nedostupnost dat	6	Nedostatečná údržba/ neprobíhá v pravidelných intervalech	2	Pojištění	3	36	Zavedení systému pravidelných revizí HW	jednatel	5	1	1	5
	Nefunkční SW	Nedostupnosti dat/ oslabení bezpečnosti IS	8	Nepravidelná údržba SW	3	Ne	3	72	Zavedení systému pravidelných kontrol SW a jeho údržby	jednatel	5	1	1	5

Akceptovatelné riziko
RN ≤10

Významné riziko
10 < RN ≤ 100

Nepřijatelné riziko
RN > 100

Současný stav									Budoucí stav					
Prvek procesu	Možná vada	Možné následky	**Význam (1-10)**	Možné příčiny	**Výskyt (1-10)**	Stávající opatření k odhalení	**Odhalitelnost (1-10)**	**Rizikové číslo (RN)**	Opatření	Zodpo-vědnost	**Význam (1-10)**	**Výskyt (1-10)**	**Odhalitelnost (1-10)**	**Rizikové číslo (RN)**
Selhání technickéh o zařízení	Výpadek datové sítě	Nedostupnost dat	4	Nepravidelná údržba HW/SW	2	Ne	2	16	Zavedení systému pravidelných kontrol SW/HW a jeho údržby	jednatel	4	1	1	4
	Poškození datových nosičů	Nedostupnost dat	4	Stáří komponentů	2	Zálohování	2	16	Obměna datových nosičů	jednatel	4	1	1	4
	Přerušení dodávky elektrické energie	Nedostupnost dat/ztráta dat	3	Technické selhání	1	Záložní zdroj	1	3	Ne		3	1	1	3
Přírodní hrozby	Úder blesku	Poškození HW/požár	5	Přírodní vlivy	2	Pojištění	1	10	Ne		5	2	1	10
	Požár	Poškození HW	5	Porucha elektroinstalace	1	Požární hlásiče/pojištění	1	5	Ne		5	1	1	5
	Voda	Poškození HW vybavení	5	Havárie vody /přírodní vlivy	1	Pojištění	1	5	Ne		5	1	1	5
	Prach	Poškození HW	5	Prašné prostředí	1	Pojištění	1	5	Ne		5	1	1	5

Tabulka 11 – Analýza možného výskytu a vlivu vad

Akceptovatelné riziko
RN ≤10

Významné riziko
10 < RN ≤ 100

Nepřijatelné riziko
RN > 100

9.2.5 Vyhodnocení analýzy FMEA

Výsledky analýzy zobrazují nejnebezpečnější rizika z pohledu jejich významu, pravděpodobného výskytu a také možnosti jejich odhalení. Hodnocena jsou pouze rizika považována za nejzásadnější. Riziková čísla byla vypočítána pomocí vzorce RN = Vz * Vy * Od. V tabulce níže je uvedeno shrnutí s rizikovými čísly v aktuální situaci a v situaci po zahrnutí následných opatření.

Riziko	**RN (aktuální)**	**RN (budoucí)**
Nezabezpečení pracoviště	28	14
Nezabezpečení pracovní stanice	144	45
Ztráta technického vybavení	7	7
Poškození technického vybavení	2	2
Prozrazení citlivých informací	72	24
Spuštění škodlivého kódu	210	70
Ztráta integrity dat	80	8
Neúmyslná ztráta dat	16	8
Neautorizované používání IS	20	10
Instalace SW z neprověřených zdrojů	50	10
Nedostatečné proškolení v oblasti informační bezpečnosti	24	8
Nedostatečné stanovení odpovědnosti	90	25
Nízká kvalifikace	144	72
Absence bezpečnostních pravidel	160	80
Administrátorská práva uživatelů	252	18
Manipulace s daty	160	4
Zneužití uživatelských práv	112	5
Zneužití citlivých dat	126	5

Poškození HW	5	5
Neautorizovaný přístup do IS	80	10
Kybernetický útok	150	20
Ransomware	90	8
Phishing	200	10
Nezabezpečený systém	100	10
Nedodržování pravidelných aktualizací	80	3
Chybná záloha dat	18	4
Porucha HW	36	5
Nefunkční SW	72	5
Výpadek datové sítě	16	4
Poškození datových nosičů	16	4
Přerušení dodávky elektrické energie	3	3
Úder blesku	10	10
Požár	5	5
Voda	5	5
Prach	5	5

Tabulka 12 – Hodnocení rizik

9.2.6 Oblasti nepřijatelných rizik

Podle výpočtu rizikového čísla byla jako nejrizikovější vyhodnoceno:

- Nezabezpečení pracovní stanice.
- Spuštění škodlivého kódu.
- Nízká kvalifikace zaměstnance.
- Absence bezpečnostních pravidel.
- Administrátorská práva uživatelů.
- Manipulace s daty.

- Zneužití uživatelských práv.
- Zneužití citlivých dat.
- Kybernetický útok.
- Phishing.

Jak už bylo analyzováno pomocí analýzy KARS, rizika spolu úzce souvisí a jsou sebou následně vyvolávány. V této kategorii se objevují rizika převážně způsobena lidským faktorem, ať už s úmyslem nebo bez něj. Jako zásadní se dále projevily problémy s nastavením bezpečnostních pravidel subjektu, jejich kontrola a vymáhání. Jako další zásadní hrozba je kybernetický útok, který může být zapříčiněn i jakožto primární cílený, ale také jako sekundární důsledek některé z uživatelských chyb.

I když se z hlediska výskytu těchto hrozeb nejedná o vysoké číslo, tak z hlediska významu a ve většině případů velice komplikované odhalitelnosti jedná o hrozby přímo ohrožující subjekt z finančního hlediska, ale také z hlediska know-how a konkurenční výhody na trhu.

9.2.7 Oblasti významných rizik

Do této oblasti byli dle výpočtu rizikového čísla zařazeny:

- Nezabezpečení pracoviště.
- Prozrazení citlivých informací.
- Ztráta integrity dat.
- Neautorizované používání IS.
- Nedostatečné proškolení v oblasti bezpečnosti informací.
- Nedostatečné stanovení odpovědnosti.
- Neautorizovaný přístup do IS.
- Ransomware.
- Nezabezpečený systém.
- Nedodržování pravidelných aktualizací.
- Chybná záloha dat.

- Porucha HW.
- Nefunkční SW.
- Výpadek datové sítě.
- Poškození datových nosičů.

V této kategorii se objevují rizika, která jsou považována za významná, i když dle tabulky 12 je možné určit rozsah a závažnost jednotlivých z nich. Jako nejzásadnější rizika, která na hranici s riziky z kategorie nepřijatelných jsou ztráta integrity dat, nedostatečné stanovení odpovědnosti, neautorizovaný přístup do IS a nedodržování pravidel aktualizací. Tyto rizika je nutno v této kategorii ošetřovat prioritně a s ohledem na jejich dopad na subjekt. Další rizika v této oblasti však nejsou také zanedbatelná, jelikož souvztažnost těchto rizik byla prokázána další analýzou, proto mohou vést k rizikům nepřijatelným. Stále se objevují významné pochybení na straně organizace a jednotlivých uživatelů s výjimkou technických závad na zařízeních a případných kybernetických útoků a infikace ransomwaru do IS.

9.2.8 Oblast akceptovatelných rizik

Do oblasti akceptovatelných rizik dle analýzy vyplynulo:

- Ztráta technického vybavení.
- Poškození technického vybavení.
- Neúmyslná ztráta dat.
- Poškození HW.
- Veškeré přírodní hrozby.

Do této oblasti spadají rizika, která je subjekt schopný akceptovat a již zpravidla má tyto rizika nějakým způsobem ošetřena. Některá rizika týkající se úmyslu nebo náhodného poškození lze ošetřit pouze transferem rizika a to pojištěním.

10 NAVRHOVANÁ OPATŘENÍ PRO SUBJEKT

V kapitole jsou detailněji rozpracována vybraná navrhovaná opatření vycházející z předchozích analýz týkající se zvýšení kybernetické bezpečnosti subjektu.

Dle rozhovorů, analýz a pozorování chodu subjektu byly identifikovány a vyhodnoceny skutečnosti, které subjekt splňuje na dostatečné a odpovídající úrovni. Tyto body není třeba zlepšovat. Převážná většina však vykazuje zjevné nedostatky a je nutné provést neodkladná opatření. Opatření jsou navrhována dle výsledků analýz KARS z oblasti primárně a sekundárně nebezpečných rizik a FMEA z oblasti nepřijatelných a hraničních významných rizik. Dále jsou navrhována opatření i pro oblasti, které nebyly podrobeny podrobné analýze. Cílem opatření naplnění podmínek normy ISO 27001, ale zlepšení stavu kybernetické bezpečnosti subjektu. Zahrnutí navrhovaných opatření je předmětem jednání managementu subjektu v závislosti na finanční náročnosti jednotlivých opatření.

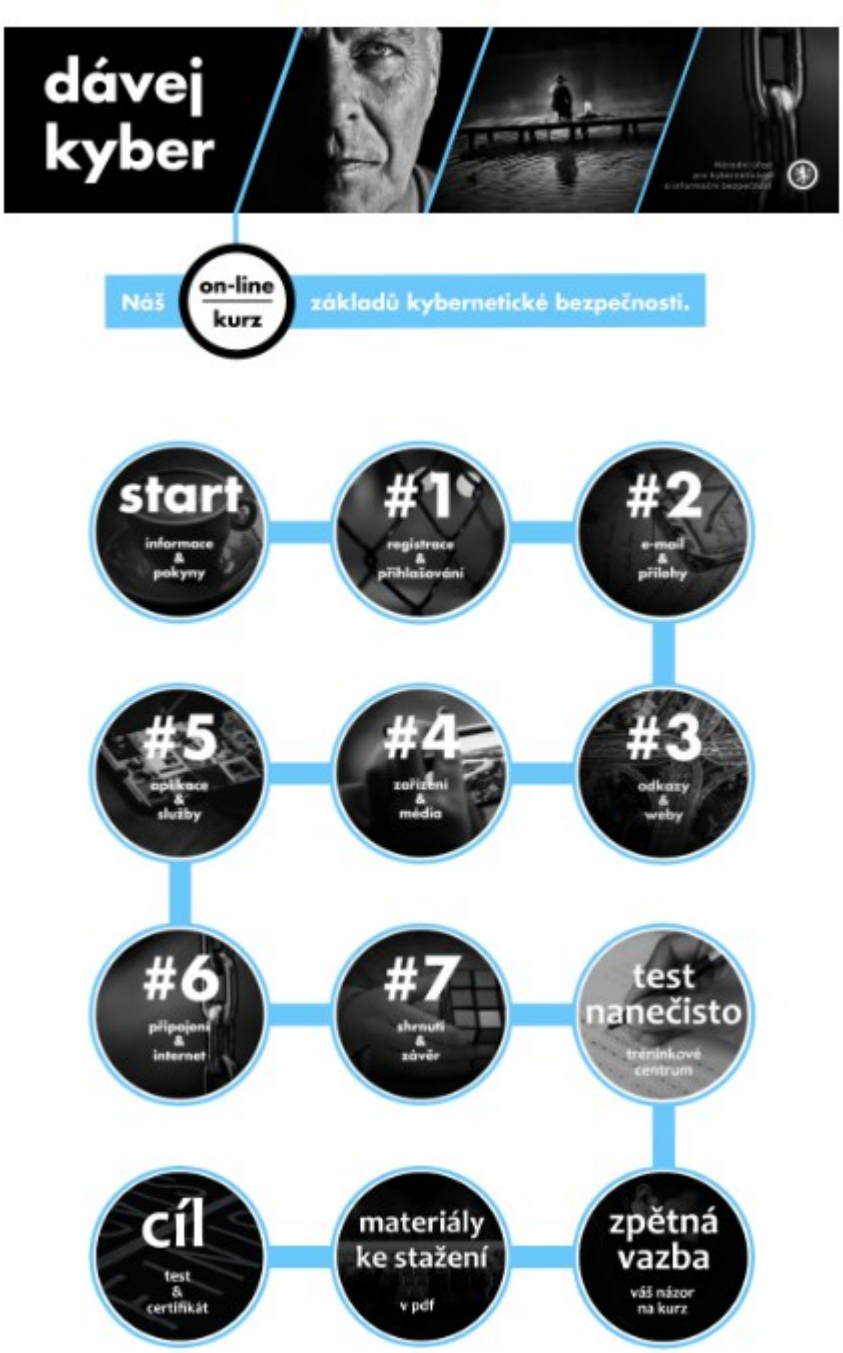
10.1 Organizační opatření

U subjektu nejsou stanovena bezpečnostní pravidla využívání IS. Jako prioritní navrhuji určení nebo zřízení nové pozice odpovědného zaměstnance za kybernetickou bezpečnost. Odpovědnost za tuto oblast musí být přesně definována a musí být vynucováno dodržování bezpečnostních pravidel.

Vzdělávání se v oblasti kybernetické bezpečnosti

Informace v oblasti kybernetické bezpečnosti je jednou z nejdůležitějších věcí, které by měl uživatel znát. Neznalost v tomto oboru nese vysoké riziko. Nedostatečně vzdělaný uživatel se stává pro útočníka snadným cílem. Proti hrozbám jako phishing, pharming nebo ransomware je jedinou obranou znalost problematiky a stylu těchto útoků. Vzdělanost v této oblasti je u subjektu na velmi nízké úrovni. Riziko s tím spojená jsou na kritické úrovni. Navrhuji proto zpracovat příručku pro zaměstnance subjektu, která bude sestavena na míru potřebám subjektu a poskytne informace a nabídne možné postupy při setkání s některou z forem kybernetického útoku. Také navrhuji sestavit sérii odborných zaměstnání na témata kybernetické bezpečnosti a zvýšit povědomí zaměstnanců v této problematice. Jako počáteční školení doporučuji využití e-learnigového kurzu poskytovaným NÚKIB „Základy kybernetické bezpečnosti“, který je poskytován zdarma. Popřípadě využít služby firmy zabývající se problematikou odborných školení na témata týkající se kybernetické bezpečnosti a zajištěním nejnovějších informací, jelikož se tento obor dynamicky vyvíjí.

Vzdělávání v této oblasti výrazně snižuje rizika úspěšnosti kybernetického útoku na subjekt a tím neohrožuje jeho činnost.



Obrázek 3 – Kurz základů kybernetické bezpečnosti (NÚKIB, © 2022, c)

Odpovědnost za aktiva

Navrhuji zavést systém odpovědnosti jednotlivých zaměstnanců za svěřená aktiva s ukládáním veškeré historie nakládání s aktivy a tím redukovat možnost zneužití citlivých informací, uživatelských práv, odcizení dat a případně jinou manipulací

s daty. Systém musí obsahovat možnosti přidělení přístupů odpovědného zaměstnance pouze ke svěřeným aktivům. Dále provést nastavení automatické instalace aktualizací a provádět pravidelné kontroly HW a SW vybavení subjektu.

Zásada prázdného stolu

Citlivé informace v papírové podobě jsou uloženy v uzamykatelných kartotékách a trezoru. Zařízení ke zpracování informací by měla být vždy uzamčena a odhlášena. Tím je z části zabezpečen také přístup do systému. Zabezpečení pracovní stanice však není subjektem vyžadováno a administrátorsky kontrolováno. Jako další výraznou hrozbu lze vnímat nedostatečnou sílu hesla, která je spojena s politikou hesel subjektu. Uživatelé často používají hesla snadno prolomitelná, spojená s jejich osobními údaji, která výrazně usnadňují útočníkovi práci. Je proto nutné zavést vyžadování uzamčení pracovní stanice a provádění kontroly. Navrhuji systém, který vyžaduje změny hesel v pravidelných 3měsíčních intervalech a vyžadování používání hesel o 12 znacích v kombinaci malých a velkých písmen, čísel a znaků, popřípadě vícefaktorvou autentizaci. Dále nastavit automatické uzamykání pracovní stanice po 3 minutách bez činnosti.

Bezpečnost zařízení a aktiv mimo prostory organizace

Práce mimo prostory organizace není nijak omezena. Zpracování informací probíhá na mobilních zařízeních na dálku. Není však vedena žádná historie. Jako riziko lze považovat použití nezabezpečených sítí, možnost ponechání zařízení na veřejných místě a jeho případné zneužití. Navrhuji zavedení systému evidence a systém povolení vynášení zařízení mimo prostory subjektu cestou odpovědného zaměstnance.

Administrátorská práva uživatelů

Subjekt žádným způsobem neomezuje práva uživatelů pracovních stanic a umožnuje plná administrátorská práva všem uživatelům. Z tohoto pramení vysoké riziko používání tohoto zařízení jakožto „polosoukromého“. S tímto je spojeno instalování dalšího SW, který může pocházet s neprověřených zdrojů a způsobit napadení zařízení některým druhem malware. Toto nese vysoké riziko následného kybernetického útoku na subjekt. Navrhuji přiřadit uživatelům pouze uživatelská práva a tím zamezit výše uvedeným rizikům zneužití zařízení. Opatření vyžaduje minimální investici s výrazným zvýšením úrovně kybernetické bezpečnosti.

Otevírání souborů z neprověřených zdrojů

Jedním z nejčastějších zdrojů nákazy jsou soubory, často se jedná o přílohy posílané emailem, které uživatel otevře a stáhne do systému. Tvůrci jsou vynalézavý a vytvoří malware, který vypadá jako textový dokument, nebo obrázek. Proto je důležité neotevírat soubory přiložené k emailům, které uživateli nic neříkají nebo nemají jasného odesílatele. Stejná pravidla platí i při prohlížení internetových stránek, nebo při stahování obrázků. Některé antivirové programy už poskytují automatické zablokování webové stránky, která je potencionálně nebezpečná a tím uživatele chrání před napadením. S tímto úzce souvisí vzdělanost v oblasti kybernetické bezpečnosti. Navrhuji provést školení na téma kybernetické bezpečnosti.

10.2 Technická opatření

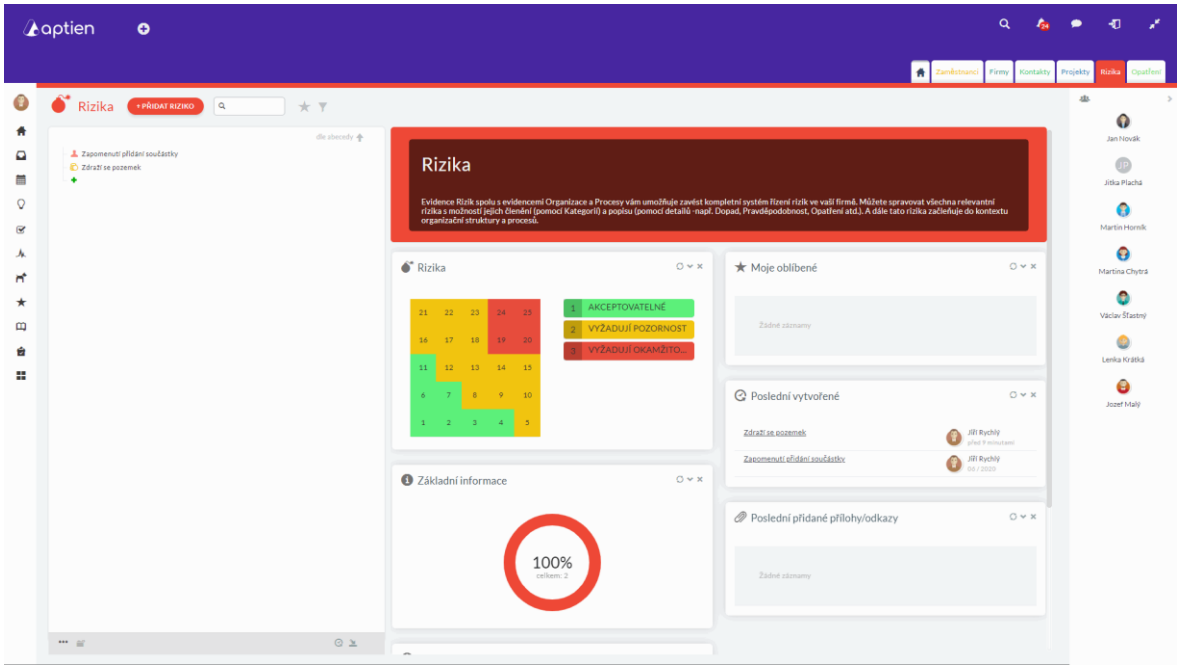
Podkapitola technická opatření zahrnuje řešení fyzické bezpečnosti subjektu a také technická řešení zabezpečení sítí a služeb.

10.2.1 Softwarové produkty

Podkapitola se zabývá možnými softwarovými produkty pro řízení bezpečnosti subjektu.

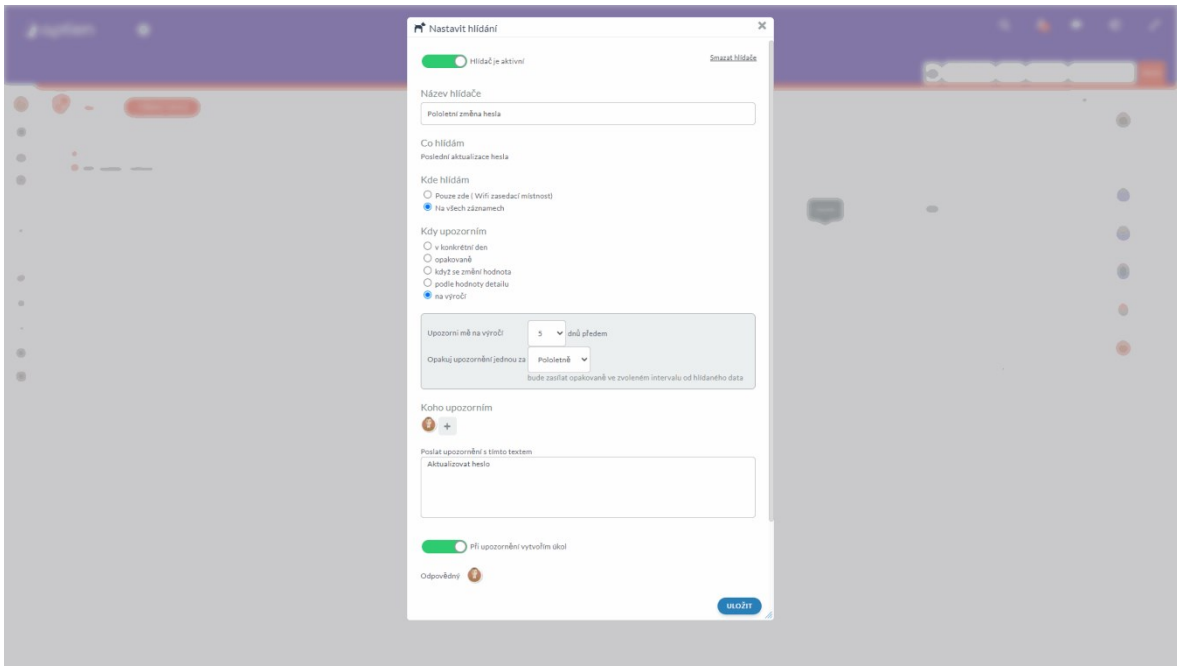
Aptien

Z technických opatření týkajících sítí a služeb je vhodné navrhnout použití softwarových nástrojů pro řízení evidence a bezpečnosti subjektu. Tyto opatření umožnuje ošetřit softwarový produkt firmy Aptien. Je to software určený pro řešení firemní administrativy od evidence majetku a zařízení, personálu, vedení administrativy, projektů atd. Zaměřuje se také na řízení rizik firmy, správu hesel, evidenci bezpečnostních incidentů a evidence oprávnění a přístupů zaměstnanců. Aplikaci je možné si přizpůsobit na všechny typy firemních rizik nevyjímaje dle ISO 27000. Aplikace je dostupná v testovací bezplatné verzi. (Systém na řízení rizik ve firmě, © 2022)



Obrázek 4 – Evidence rizik subjektu (Systém na řízení rizik ve firmě, © 2022)

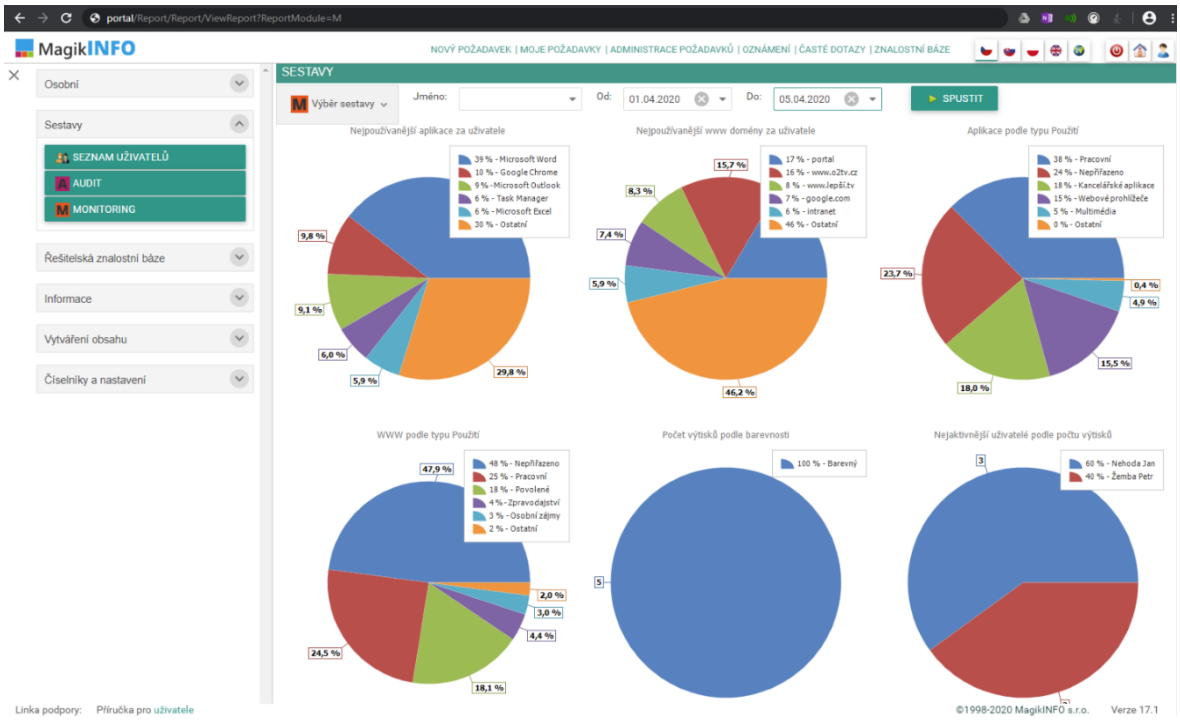
V případě správy hesel umožnuje hlídání výročí změny a také jejich evidenci.



Obrázek 5 – Hlídání hesel (Systém na řízení rizik ve firmě, © 2022)

MagikMONITOR

Pro kontrolu práce zaměstnanců na přidělených zařízení je vhodné použití softwaru pro monitoring práce uživatelů a to například Magicmonitor. Slouží k monitorování aktivit uživatelů na pracovišti a také mimo něj. Sleduje návštěvy webových stránek, připojování přenosných médií a využívání aplikací. Zaznamenává a zobrazuje detailní časovou práce uživatele. Umožňuje srovnávat uživatele dle efektivity využívání pracovní doby. Poskytuje přehled o tisku na lokálních i síťových tiskárnách a tím umožnuje určení efektivity a snížení nákladů. Pomocí aplikace Magikmonitor je možné provádět restrikce a notifikace a tím omezovat vybrané webové stránky, aplikace nebo připojení externího úložiště. (Magikmonitor, © 2022)



Obrázek 6 – Monitorování aktivit (Magikmonitor, © 2022)

10.2.2 Ostatní technická opatření

Podkapitola reflektuje ostatní opatření technická opatření týkající se fyzická bezpečnosti, přírodních vlivů a zabezpečení dat.

Zálohování dat

Zálohování dat je prováděno na několika úrovní a tedy riziko jejich ztráty není vysoké. Je využíváno cloudových úložišť a jejich zabezpečení je v odpovědnosti poskytovatele služby. Není však zabezpečen záložní poskytovatel připojení a tudíž při ztrátě připojení

dochází ke ztrátě dostupnosti dat. Navrhuji nastavení notifikace při dokončení pravidelné zálohy z důvodu kontroly a použití hashovací funkce pro zajištění integrity dat. Pokud by došlo k chybné záloze dat vlivem SW nebo HW poruchy, mohlo by dojít při dlouhodobé chybné záloze ke ztrátě dat. Při ransomwarovém útoku je nezávislá záloha dat zásadní a pokud by uživatel neměl pořízené zálohy je zde vysoké riziko ztráty všech dat.

Fyzický bezpečnostní perimetr

Sídlo subjektu se nachází v areálu, kde sousedí s řadou dalších subjektů. Kontrola vstupu do areálu není prováděna na požadované úrovni a sídlo subjektu není chráněno obvodovou ochranou. Jako opatření je nutné zabezpečit obvodovou ochranou samotné budovy subjektu. Navrhuji opocení sídla a ostatních staveb subjektu oplocení výšky 2 metry opatřenou ostnatým drátem pro zamezení překonání. Realizace tohoto opatření nevyžaduje stavební povolení, není finančně náročná a sníží cenu za pojištění.

Pro zvýšení bezpečnosti zajistit evidenci vstupu a vjezdu do areálu, popřípadě pro vyšší bezpečnost systémem povolení vstupu as vjezdu do areálu. Toto opatření závisí na jednání jednotlivých subjektu nacházejících se v areálu.

Zabezpečení kanceláří, místností a vybavení

Kvalitní zabezpečení je jedním se základních podmínek ochrany informací. Jelikož je samotný objekt zabezpečen elektronickým zabezpečovacím systémem a video dohledovým systémem je tento bod považován za dostatečný pro tento typ subjektu. Jelikož u subjektu je používán jeden společný kód pro odblokování elektronického zabezpečovacího systému je nutné doporučit přidělení jednotlivých účtů a vlastních kódů pro možnou identifikaci pracovníka, který vstupuje na pracoviště. Dále nastavení automatické notifikace signalizující manipulaci s elektronickým zabezpečovacím systémem pro informování o vstupu na pracoviště a stavu zabezpečení.

Nezabezpečené oblasti

Subjekt nemá rozděleny prostory na zabezpečené a nezabezpečené oblasti. Z tohoto důvodu může docházet k neoprávněnému přístupu k informacím. Stavebně tento problém není možné vyřešit. Pro rozdělení oblastí by muselo dojít k výstavbě dalších prostor.

Neoprávněný přístup ostatních zaměstnanců

S předchozím bodem úzce souvisí přístup ostatních zaměstnanců do prostor, kde dochází ke zpracování informací. Ideální variantou je tyto prostory separovat. Z důvodu nedostatku prostoru a ekonomického hlediska tato však separace není možná.

Přírodní hrozby

V oblasti ochrany subjektu pře přírodními hrozbami je subjekt chráněn pomocí automatických hlásičů požáru, jsou prováděny pravidelné revizi elektroinstalace a spotřebičů a veškerý movitý i nemovitý majetek je pojištěn. Z tohoto pohledu je ochrana před riziky ze strany přírody na dostatečné úrovni.

10.3 Shrnutí

Dle výše zpracovaný analýz bylo zjištěno, že bezpečnostní opatření proti neoprávněnému přístupu externím útočníkům není subjekt dostatečně zabezpečen. Je vybaven kvalitním softwarovým vybavením, avšak nevyužívá dostupné softwarové nástroje pro řízení bezpečnosti informací. Zabezpečovacím systémem a data jsou zálohována dostatečným způsobem. Zabezpečit po dohovoru s představiteli ostatních subjektů v areálu důkladnou kontrolu osob vstupujících a vést jejich evidenci. Je třeba však vhodným způsobem vyřešit nepovolaný vstup ostatních zaměstnanců subjektu do prostor kde dochází ke zpracovávání informací. Implementovat systém vyžadování uzamčení pracovní stanice při opuštění pracoviště a vynutit používání silných hesel, popřípadě vícefaktorovou autentizaci. Provést revizi a určit systém přidělení odpovědnosti zaměstnanců za svěřená aktiva a jednoznačně odebrat uživatelům administrátorka práva. Provádět pravidelnou kontrolu HW a SW vybavení s důrazem na provedené aktualizace systémů a používaného SW. Jelikož subjekt vykazuje značné nedostatky, doporučuji konzultaci se společností zabývající se zabezpečením kybernetické bezpečnosti.

Největším problémem se dle analýzy jeví však nedostatečná vzdělanost zaměstnanců v oblasti kybernetické bezpečnosti. Tato neznalost oblasti způsobuje neakceptovatelná rizika a cesta vzdělávání v této oblasti je relativně snadnou cestou k dosažení vyšší míra bezpečnosti. Jako výrazné hrozby byly identifikovány možnost pracovníků nakládat se zařízením pro zpracování informací s právy administrátora, otvírání souborů z nezabezpečených zdrojů, síla hesel a neznalost malwaru a jiných nástrah kybernetického prostoru. Toto vše úzce souvisí se vzdělaností v oblasti a politikou kybernetické bezpečnosti subjektu.

Celkově se zkoumaný subjekt vykazuje, že kybernetická bezpečnost není v zásadě řešena a to z důvodu neznalosti této problematiky a reálných hrozeb. Hodnocení subjektu v oblasti kybernetické bezpečnosti považuji za nedostatečné, a proto navrhuji tyto návrhy na opatření:

- Určit odpovědnou osobu za bezpečnost v oblasti kybernetické bezpečnosti.
- Zorganizovat systém vzdělání zaměstnanců v oblasti kybernetické bezpečnosti.
- Zavést systém vyžadování uzamčení pracovní stanice a provádět kontroly.
- Zavést systém odpovědnosti jednotlivých zaměstnanců za svěřená aktiva.
- Provádět pravidelnou kontrolu HW a SW vybavení subjektu a důrazem na aktualizace.
- Definovat a nastavit politiku hesel ve společnosti.
- Odebrat administrátorská práva uživatelům.
- Navrhnou systém evidence a systém povolení vynášení zařízení mimo prostory subjektu, popřípadě využít možnosti vícefaktorové autentizace.
- Provést nastavení notifikace při dokončení pravidelné zálohy.
- Zajistit evidenci vstupu a vjezdu do areálu, popřípadě pro vyšší bezpečnost systémem povolení vstupu as vjezdu do areálu.
- Rozdělit prostory na zabezpečené a nezabezpečené oblasti.
- Zpracovat příručku kybernetické bezpečnosti pro subjekt.

11 PŘÍRUČKA KYBERNETICKÉ BEZPEČNOSTI SUBJEKTU

Příručka je určena všem zaměstnancům subjektu na všech úrovních. Zabývá se problematikou kybernetické bezpečnosti a poskytuje informace jakým způsobem se chovat v kyberprostoru. V první části příručky jsou řešena bezpečností opatření z úrovně managementu organizace a druhá část se bude věnovat převážně koncovým uživatelům.

11.1 Cíl

Cílem této příručky je zvýšit úroveň znalostí uživatelů v oblasti kybernetické bezpečnosti. Poskytnou návod, jakým způsobem se chovat ve vybraných situacích a tím zvýšit úroveň bezpečnosti. Dále také nastínit možná řešení a organizaci opatření pro podporu kybernetické bezpečnosti. Příručka je sestavena cíleně pro vybraný subjekt a obsahuje pouze výčet informací o kybernetické bezpečnosti jeho se týkajících.

11.2 Zásady kybernetické bezpečnosti subjektu

Tato kapitola obsahuje zásady pro bezpečnou činnost subjektu ve vztahu ke kybernetické bezpečnosti a také doporučení pro její zaměstnance, jak se chovat a správně pracovat s IS a svěřeným zařízením. Jedná se o cílené informace na základě identifikovaných hrozeb pro subjekt a také zjištění z analýz.

11.2.1 Bezpečnostní opatření

Západním pravidlem je vždy se řídit pokyny určeného specialisty. Pokud nevíte, jakým způsobem se zachovat v dané situaci, tak kontaktujte tuto osobu. Za tím to účelem by každý subjekt měl mít minimálně určeného zaměstnance, zabývajícího se touto problematikou, i kdyby to měla být jeho sekundární funkce. Tato osoba musí být obeznámena s touto problematikou a měla by být v této oblasti vzdělávána. Tato osoba má na starost bezpečnost subjektu. (NÚKIB, © 2022, a)

„Vždy respektuj pokyny specialisty.“

11.2.2 Práce se svěřeným zařízením

Při práci s firemním počítačem je nezbytně nutné zařízení vždy uzamknout při jakémkoli vzdálení. Odemknuté zařízení bez dozoru dává potencionálnímu útočníkovi prostor k manipulaci s daty a zařízením samotným. Je nutné toto mít na paměti vždy, a především

na veřejných místech. Zamknutí u zařízení používající systém Windows se provádí zkratkou WIN+L. (Doporučení a návody, © 2022)

„Vždy uzamkni pracní stanici (WIN+L).“

Soukromá zařízení, které nejsou pod správou subjektu nelze požívat pro pracovní účely. Tyto zařízení nejsou zpravidla dostatečně zabezpečena a jsou sdílena s dalšími cleny domácnosti. (NÚKIB, © 2022, a)

„Nikdy nepoužívej soukromé zařízení k pracovním účelům.“

11.2.3 Online účty a hesla

Každý uživatel využívá v současné době spoustu účtů. Kombinace pracovních a soukromých online účtů není doporučována za důvodu, že soukromé účty nejsou pod kontrolou subjektu. Zde je zvýšené riziko zanesení škodlivého kódu do firemní sítě.

„Nikdy nepoužívej pracovní účty soukromě a obráceně.“

Veškeré přístupy k právním účtům je nutné chránit hesly. Pro každý účet je nutné zvolit jiné heslo. Při prozrazení hesla jednoho účtu nebude mít útočník přístup do všech. (NÚKIB, © 2022, a)

„Každý účet vlastní heslo.“

Přihlašovací údaje nikdy nesdělujte jiné osobě, každý zaměstnanec subjektu by měl mít vlastní, pokud má mít přístup do daného účtu nebo pracovní stanice. Toto jednání může mít závažná následky, za které ponesete odpovědnost vy.

„Nikomu nesděluj své přihlašovací údaje.“

Pokud je to možné tak využívej vícefaktorovou autentizaci. Především do oblastí, kde by prolomení hesla znamenalo neakceptovatelné riziko. Tento způsob autentizace výrazně zvyšuje bezpečnost.

Administrátorské účty jsou určeny pouze pro správce systému. Běžní uživatelé tyto práva nepotřebují a při jejich vlastnictví vzniká vyznané riziko zanesení škodlivých kódů do zařízení. (NÚKIB, © 2022, a)

„Administrátorská práva pouze pro správce systémů. “

Nastavujte vždy jedinečná hesla, která neobsahují vaše osobní údaje jako je jméno nebo datum narození atd. Heslo musí být dlouhé, čím delší tím lepší. Vždy používejte kombinaci znaků malých a velkých písmen, číslic a symbolů. Tím zabezpečíte vyšší odolnost proti útoku. Hesla s nikým nikdy nesdílejte a nezapisujte si je do zápisníku ani si je neukládejte do počítače. Nejbezpečnější je pořízení správce hesel. (Doporučení a návody, © 2022)

„Heslo: kombinace znaků, co nejdelší, nikdy nesdílej."

Zkontrolujte si, zda vaše přihlašovací údaje figurují na seznamech uniklých či ukradených účtů. Pokud ano okamžitě změňte heslo nebo účet zrušte. (Doporučení a návody, © 2022)

„haveibeenpwned.com"

11.2.4 Datové nosiče

Pro přenos dat ve firemní síti používat pouze zařízení k tomu určená a nikdy je nepožívat soukromě a nepřipojit mimo určené pracovní stanice.

Připojení neznámých zařízení ne zařízeních soukromých do právní stanice může zanést infekci do firemní sítě. V případě nevyhnutelnosti provést antivirovou kontrolu. (NÚKIB, © 2022, a)

„Nikdy nepřipojuj neznámé nebo soukromé paměťové zařízení."

11.2.5 Odkazy a neznámé zdroje

Instalace SW z neprověřených zdrojů nese významné riziko pro uživatele. SW z těchto zdrojů může obsahovat škodlivé kódy a způsobit oslabení bezpečnosti systému proti kybernetickému útoku. Instalaci SW vždy provádějte z oficiální a prověřených zdrojů a instalujte pouze SW, který je podporován a jsou dostupné aktualizace.

„SW vždy z ověřených zdrojů."

Při klikání na odkaz vždy zkontroluj, zda nevede na podezřelou URL adresu. Skutečná adresa se zobrazí po umístění kurzoru myši na odkaz bez jeho rozkliknutí. Pokud toto nelze ověřit tak na odkaz nikdy neklikej. (NÚKIB, © 2022, a)

„Nikdy neklikej na podezřelý odkaz."

11.2.6 Aktualizace

Aktualizace SW a operačních systémů hlavně ty bezpečnostní jsou velice důležité. Pokud výrobce vydává aktualizaci tak tím upozorňuje potencionálního útočníka na chyby, které mohou být zneužity. Proto jen nutné udržovat všechny využívané SW nástroje a operační systém vždy aktualizovaný. Ideálně nastavit provádění aktualizací automaticky. (Kilián, 2021)

„Aktualizuj."

11.2.7 Záloha

Na začátku je nutné si neplést zálohu s archivem. Archivace je obraz celého systému, zatímco záloha je rozdílová záloha systémových oddílů a databází od poslední archivace.

Dělejte tři kopie záloh. Dvě zálohy na místních, ale rozdílných zařízeních a minimálně jedna mimo subjekt. Základem je pravidelnost, archivace alespoň jedenkrát za půl roku a jednou týdně plnou zálohu a každý den zálohu nových dat. Dbejte na to a kontrolujte, zda je možné zálohu obnovit. (Doporučení a návody, © 2022)

„Zálohuj pravidelně."

11.2.8 Veřejná bezdrátová síť

Využívání veřejné bezdrátové sítě nese vysoké riziko a představuje relativně jednoduchý možnost přístupu útočníka do vašeho zařízení. Tím se mu otevírají dveře ke všem vašim činnostem, ale hlavně k vašim přihlašovacím údajům a heslům. Jedná se hlavně o nezabezpečený bezdrátové sítě nebo s veřejně dostupným heslem na veřejných místech. Bezpečnější je použití mobilního internetu. (Doporučení a návody, © 2022)

„Nepoužívej veřejné WIFI."

11.2.9 Bezpečná komunikace

Ověřujte si totožnost osoby, se kterou komunikujete. Vždy je tu riziko, že osoba se kterou komunikujete se může vydávat za někoho jiného. Pokud si nejste jisti tak raději komunikaci ukončete. Nesdělujte touto formou žádné citlivé informace a dobře zvažte, zda je nutné zveřejnovat určité informace osobní. Tyto informace pak mohou být zneužity například při spear-phishingu. (NÚKIB, © 2022, a)

„Ověř si, s kým komunikuješ."

11.3 Phishing

Jedná se o druh kybernetické kriminality, kdy se terčem stávají osoby. Cílem je získání cenných osobních informací nebo doručení malware do vašeho zařízení. Provádí se formou e-mailu, SMS, zprávy na sociálních sítích nebo telefonickým hovorem s úmyslem vyvolat obavy, dostat osobu so stresové situace a vylákat informace. Provádí se cestou odkazu na webové stránky s vyplněním přihlašovacích údajů, zaslání přihlašovacích údajů atd.

11.3.1 Phishingové výzvy

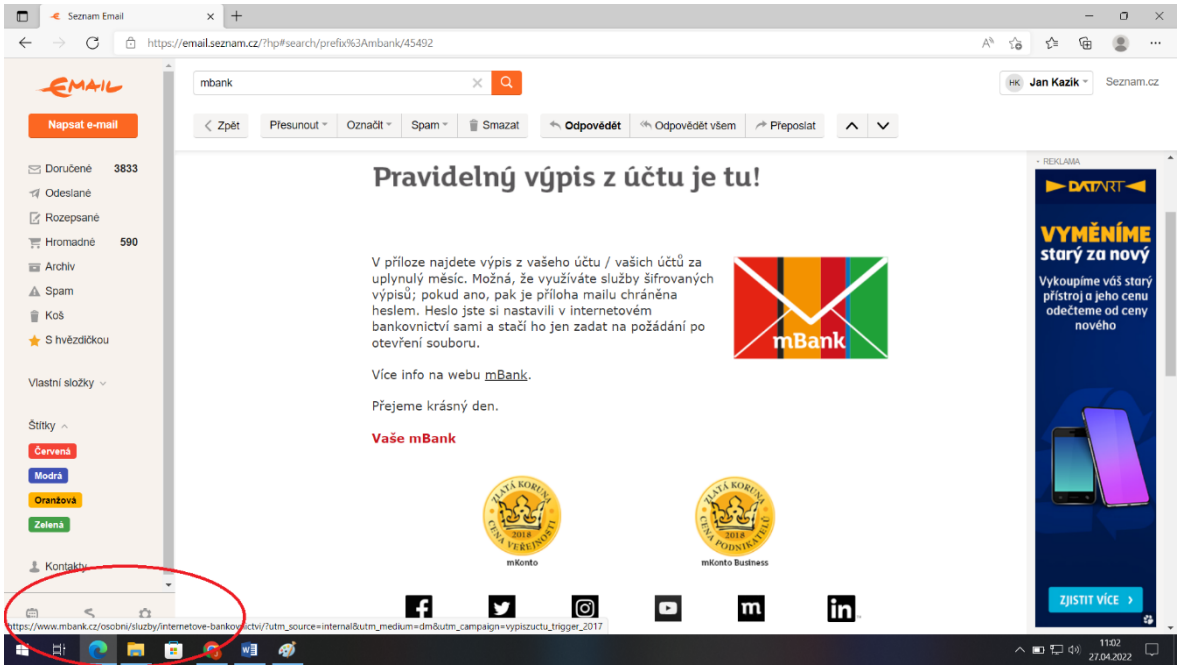
- Přihlášení do online bankovnictví.
- Aktualizace osobních údajů.
- Restart účtu.
- Potvrzení převzetí zásilky.
- Žádost o platbu.
- Zaslání daňového přiznání.
- Pomoc s bankovním převodem. (Doporučení a návody, © 2022)

11.3.2 Jak poznat podvodný e-mail

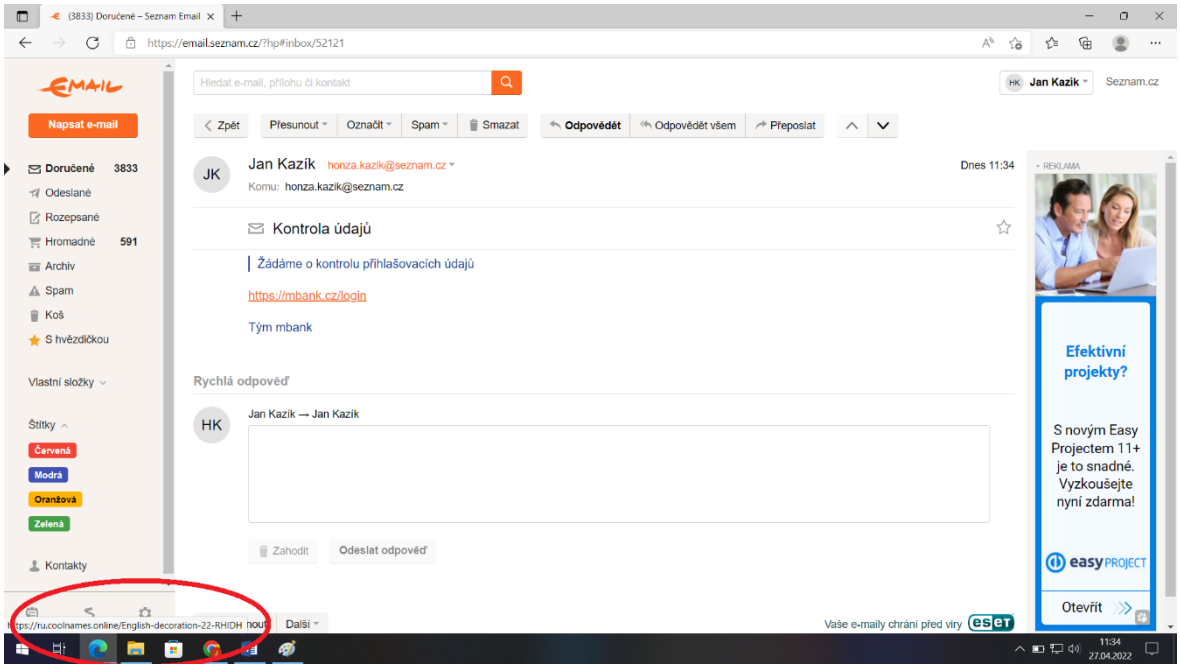
Základem je kontrola odesílatele a zda je email očekávaný. Je nutné si všímat detailů, zda je v komunikaci nebo v emailu něco podezřelého. Bude daná organizace řešit problém pomocí jiné společnosti? Pravděpodobně ne. Všímejte si tvaru e-mailových adres, nemělo by se jednat o free mail, zdánlivých překlepů, záměny písmen, tvaru URL a kdo je odesílatel. Pokud se vám některý z těchto aspektů zdá podezřelý nebo nekoresponduje tak nikdy

neklikejte na odkaz nebo neotvírejte přílohu. Uvědomte si, citlivé informace o vás nikdo nemůže chtít touto formou.

Po umístění kurzoru na odkaz nabízený v e-mailu uvidíte v levém spodním rohu reálnou URL adresu. Je nutné ji pečlivě přečíst, zda není podezřelá a neodkazuje na jiné weby. (Doporučení a návody, © 2022)

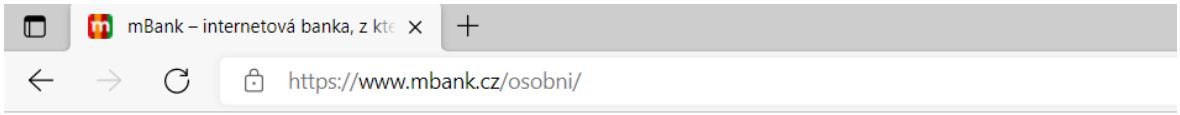


Obrázek 7 – Důvěryhodný odkaz

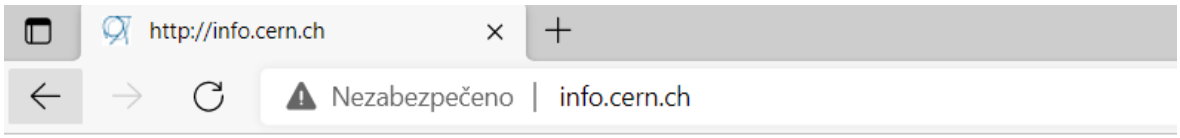


Obrázek 8 – Podezřelý odkaz

Proveďte kontrolu, zda neobsahuje zaměněné znaky nebo jinou doménu např. mmbank.cz, mbenk.cz, ebank.cz apod. Dále zkontrolujte zda se jedná o zabezpečené připojení a pouze v tom případě zadávejte své uživatelské přihlašovací údaje. Pokud v předponě „https“ chybí „s“ jedná se o nezabezpečené stránky. Lze rozeznat také podle ikony zámku. V tomto případě žádné údaje nezadávejte.



Obrázek 9 – Zabezpečené připojení



Obrázek 10 – Nezabezpečené připojení

11.3.3 Bezpečné chování

Nikdy své citlivé údaje nezasílejte třetí straně. Důvěryhodné společnosti nebudou nikdy žádat tyto informace touto formou. Na e-maily, které toto vyžadují nikdy neodpovídejte. Soubory připojené k podezřelým e-mailům neotvírejte. Pokud si chcete informace ověřit, tek kontaktujte zákaznické centrum dané společnosti.

Pokud bude chování uživatele bezpečné, bude pracovat s rozvahou, všímat si detailů a budete se řídit pokyny z kapitoly 11.2, tak pokud dojde k napadení zařízení nebo uživatelských účtů bude toto z největší pravděpodobnosti způsobeno chováním uživatele. (Doporučení a návody, © 2022)

11.4 Ransomware

Je typ malwaru, který uzamkne nebo zašifruje obsah napadeného zařízení za účelem požadování výkupného. (Doporučení a návody, © 2022)

11.4.1 Vznik infekce

Ransomware se do zařízení může dostat několika způsoby. Do systému se může dostat pomocí phishingové zprávy, pomocí prohlížeče, rizikovým nelegálním stahováním, z pornografických stránek, instalací pluginů do prohlížečů, kliknutím na falešnou reklamu a další. (Doporučení a návody, © 2022)

11.4.2 Když dojde k napadení

Prvním krokem je kontaktovat IT správce nebo jinou odpovědnou osobu.
Řešením je odpojit zařízení ze sítě a tím ochránit další zařízení. Je možné se pokusit odstranit ransomware pomocí antivirového programu, vaše data vám to však nevrátí. Existuje možnost najít dešifrovací klíč na internetu. Asi nejúčinnější je kompletní zformátování, nová instalace a obnovení zálohy. Proto je velmi důležité provádět pravidelnou zálohu dat.

Platit výkupné se nedoporučuje z důvodu motivace zločinců k dalším podvodům a také neexistuje záruka vrácení dat. (Doporučení a návody, © 2022)

11.4.3 Bezpečné chování

Zda platí jako zásadní provádět pravidelné zálohy. Riziko napadení ransomwarem nikdy nelze dokonale eliminovat, a tudíž se nadá vyloučit. Pokud se však budeme řídit zásadami kybernetické bezpečnosti, můžeme toto riziko výrazně snížit. (Doporučení a návody, © 2022)

11.5 Jak poznat, že se do počítače nabourał hacker

Útočníci se nezaměřují pouze na velké společnosti a bohaté lidi. Terčem jejich útoku s může stát kdokoli. Zde je několik způsobů, jak poznat, že se vám do vašeho zařízení dostal hacker. (Doporučení a návody, © 2022)

11.5.1 Útočník vás kontaktuje

Pokud se útočníkovi zdaří útok na vaše zařízení tak vás kontaktuje. Jeho činnost je velice jednoduchá. Odcizí nebo zašifrují vám data a vyžadují výkupné za návrat vašich dat do normálu. Nejčastěji tuto činnost vykonávají pomocí ransomware. Po zaplacení výkupného není garance návratu dat. (Doporučení a návody, © 2022)

11.5.2 Nový panel v prohlížeči

Pokud s vám ve vašem prohlížeči objeví nový panel nástrojů a není to vaše práce, tak vaše zařízení bylo infikováno. Pomocí panelu nástrojů je možné zaznamenávat vaši činnost v prohlížeči včetně zadávání přihlašovacích údajů a hesel. (Doporučení a návody, © 2022)

11.5.3 Samovolná změna hesla

Pokud se vám nedaří se přihlásit do vašeho účtu a po ověření jste zjistily, že služba je funkční a nemá výpadek, tak vám byl pravděpodobně zcizen účet a útoční změnil heslo. (Doporučení a návody, © 2022)

11.5.4 Nový software v počítači

Pokud se vám ve vašem zařízení objeví nový SW nebo aplikace, a přitom jste žádnou neinstalovali tak s může jednat o napadení. Některé druhy malware se totiž mohou tvářit jako běžné aplikace nebo programy. (Doporučení a návody, © 2022)

11.5.5 Samovolný pohyb kurzoru

Pokud dochází k samovolnému pohynu kurzoru na vaší obrazovce, nejdříve ověřte, zda s nejedná o problém s HW. Pokud s však kurzor pohybuje a je veden na přesná místa a dochází ke klikání. Může se jednat o vzdálené přihlášení administrátora k vašemu zařízení nebo také o kybernetický útok. (Doporučení a návody, © 2022)

11.5.6 Vypnutý firewall

Váš obranný SW a antivir je mimo provoz a nelze ho opětovně zapnout znamená to, že vaše zařízení bylo nakaženo malwarem. (Doporučení a návody, © 2022)

11.5.7 Nevysvětlitelné aktivity

Jelikož kybernetická kriminalita je prováděna převážně za účelem obohacení, snaží se pomocí přístupu do vašeho zařízení dostat k vašemu online bankovnictví. Přihlašování v neobvyklých časech, v noci, nebo velké přesuny naznačují, že jste možná byli napadeni kybernetickým útokem. (Doporučení a návody, © 2022)

11.5.8 Jak se bránit

Stoprocentní bezpečnost neexistuje, ale pokud s budete řídit radami v předchozí kapitole 11.2, můžete riziko na úspěšné provedení kybernetického útoku výrazně snížit.

11.6 Shrnutí

Příručka slouží jako možný návod pro bezpečné chování v kyberprostoru. Poukazuje na zásady a prevenci proti kybernetickým útokům a jejích případné řešení. Nezahrnuje však

všechny možné situace a postupy. Pro lepší pochopení celé oblasti je nutné další studium dostupných materiálů a školení.

ZÁVĚR

Studium této oblasti je nikdy nekončící proces, jelikož se kybernetická bezpečnost stále vyvíjí je nutné se stále vzdělávat. Kybernetická bezpečnost se doslala do popředí je jedním se základních aspektů bezpečnosti. V dnešním světě je otázka kybernetické bezpečnosti tématem, které je vidět všude kolem a tvrdit, že se nás to netýká by bylo velice krátkozraké. Stále však se existují subjekty, které otázku kybernetické bezpečnosti odsouvají na zadní příčky pomyslného žebříčku priorit a domnívají se, že se jich tato otázka netýká. S tím souvisí i vzdělanost společnosti v této oblasti, která stále není na odpovídající úrovni. Všichni přitom používáme různé typy chytrých zařízení tudíž se můžeme stát terči útočníků. Práce zmapovala dostupné zdroje a podklady zabývající kybernetickou bezpečností. Počet zdrojů je nepřeberný a byly vybrány ty, které odpovídají potřebám práce a jsou přijímány odbornou veřejností. Studiem zdrojů jsou zodpovězeny základní otázky důležité pro pochopení celé problematiky a systému kybernetické bezpečnosti, druhy možných útoků a také možnosti řešení. Také nejzávažnějšími útoky, které postihli instituce v České republice. Je provedeno zmapování stavu kybernetické bezpečnosti vybraného subjektu a pomocí zjištěných informací jsou identifikována nejzávažnější možná rizika pro subjekt. Zjištění aktuálního stavu ukázalo, že opatření jsou značně podceněna. Pomocí identifikovaných rizik a jejich analýzy pomocí metod analýzy KARS a FMEA byly určeny nezávažnější rizika a jejich příčiny a také důsledky. Tyto výstupy jsou využity pro nutné ošetření rizik a zpracování návrhu opatření. Jednotlivá navrhovaná opatření definují, jakým způsobem zvýšit úroveň kybernetické bezpečnosti subjektu.

Jako zásadní je vyhodnocena nevzdělanost uživatelů v oblasti kybernetické bezpečnosti. Nevzdělanost v této oblasti nese vysoké riziko, protože uživatel je pro útočníka vstupní branou do IS. Proto je zpracována příručka jakožto prvotní materiál sloužící ke zvýšení povědomí zaměstnanců subjektu, která se zabývá nejzásadnějšími problémy v oblasti kybernetické bezpečnosti obecně tak i specifiky vybraného subjektu. Smyslem příručky je poskytnout okamžité informace o této problematice a tím snížit riziko možných kybernetickým útokům prostřednictvím uživatelů.

Přínos práce vidím především v navrhovaných opatřeních navržených na základě provedených analýz a pozorování stavu kybernetické bezpečnosti vybraného subjektu. Dále v příručce pro zaměstnance, která je sestavena pro potřeby subjektu. V neposlední řadě také

v otevření tohoto tématu již při zpracovávání práce, sbírání podkladů a informací, které už samo o sobě zapříčinilo zvýšení povědomí a subjekt s touto otázkou začal zabývat.
Cíle práce byli splněny a realizace vybraných navržených opatření je na programu jednání managementu subjektu.

SEZNAM POUŽITÉ LITERATURY

Agentura, © 2021. *Česká agentura pro standardizaci* [online]. [cit. 2021-11-21]. Dostupné z: https://www.agentura-cas.cz/o-nas/agentura/

Analýza možností vzniku vad a jejich následků: příručka FMEA : FMEA návrhu produktu, FMEA procesu, doplňková FMEA monitorování a odezvy systému, 2019. Přeložil Stanislav KŘEČEK. Praha: Česká společnost pro jakost. ISBN 978-80-02-02885-7.

BROOKS, Charles J., Christopher GROW, Philip A. CRAIG Jr., Donald SHORT, 2018. *Cybersecurity Essentials*. Indianapolis: John Wiley & Sons. ISBN: 978-1-119-36239-5.

CLARK, Robert a Simon HAKIM, ed., 2017. *Cyber-Physical Security*. 3rd edition. New York: Springer International Publishing. ISBN 978-3-319-32822-5.

Co je pharming, © 2022. *Ssl.com* [online]. Houston [cit. 2022-4-13]. Dostupné z: https://www.ssl.com/cs/blogy/co-je-pharming/

Co je skenování portů, © 2022. *Avast* [online]. [cit. 2022-04-12]. Dostupné z: https://www.avast.com/cs-cz/business/resources/what-is-port-scanning#pc

ČESKO, 1998. Ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky. In: *Sbírka zákonů České republiky*. Dostupné také z: https://www.zakonyprolidi.cz/cs/1998-110

ČESKO, 2000. Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon). In: *Sbírka zákonů České republiky*. Dostupné také z: https://www.zakonyprolidi.cz/cs/2000-240

ČESKO, 2005. Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. In: *Sbírka zákonů České republiky*. Dostupné také z: https://www.zakonyprolidi.cz/cs/2005-412

ČESKO, 2005. *Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti*. In: . Praha: Česká republika, ročník 2005, 143/2005, 412/2005 Sb. Dostupné také z: https://www.zakonyprolidi.cz/cs/2005-412

ČESKO, 2014, a. *Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)*. In: . Praha: Česká republika, ročník 2015, 75/2014, 181/2014 Sb. Dostupné také z: https://www.zakonyprolidi.cz/cs/2014-181

ČESKO, 2014, b. Sdělení č. 104/2013 Sb. m. s., Sdělení Ministerstva zahraničních věcí o sjednání Úmluvy o počítačové kriminalitě. In: *Sbírka zákonů České republiky*. Dostupné také z: https://www.zakonyprolidi.cz/ms/2013-104

ČESKO, 2016. *Terminologický slovník pojmů z oblasti krizového řízení, ochrany obyvatelstva, environmentální bezpečnosti a plánování obrany státu*. In: . Praha: Česká republika, ročník 2016, Dostupné také z: https://www.mvcr.cz/soubor/terminologicky-slovnik-mv-verze-ke-stazeni.aspx

ČESKO, 2018. *Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)*. In: . Praha: Česká republika, ročník 2018, 43/2018, 82/2018 Sb. Dostupné také z: https://www.zakonyprolidi.cz/cs/2018-82

ČESKO, 2019. Zákon č. 410/2019 Sb., o zpracování osobních údajů. In: *Sbírka zákonů České republiky*. Dostupné také z: https://www.zakonyprolidi.cz/cs/2019-110

Doporučení a návody, © 2022. *Computer Incident Response Capability* [online]. [cit. 2022-3-17]. Dostupné z: https://www.circ.acr/doporuceni-a-navody

DOUCEK, Petr, Martin KONEČNÝ a Luděk NOVÁK, 2019. *Řízení kybernetické bezpečnosti a bezpečnosti informací*. Praha: Professional Publishing. ISBN 978-80-88260-39-4.

ISO, 2021 *International Organization of Standardization* [online]. Geneva, 2021 [cit. 2021-11-21]. Dostupné z: https://www.iso.org/what-we-do.html

IT Slovník, © 2021. *Počítačový slovník* [online]. Jihlava [cit. 2021-12-22]. Dostupné z: https://it-slovnik.cz/

JELŠOVSKÁ, Katarína a Andrea PETERKOVÁ, 2013. *Řešení krizových situací - metody a jejich aplikace* [online]. Opava [cit. 2022-02-27]. Dostupné z: https://www.slu.cz/file/cul/67f86af0-d484-45dc-87cf-52b7d488c52a. Studijní opory. Slezská univerzita v Opavě.

KILIÁN, Karel, 2021. Ignorování aktualizací není typické jen pro uživatele Windows. *Živě* [online]. Praha: CZECH NEWS CENTER, 2021 [cit. 2022-03-17]. Dostupné z: https://www.zive.cz/clanky/ignorovani-aktualizaci-neni-typicke-jen-uzivatele-windows-sve-o-tom-vi-i-autori-linuxu-mint/sc-3-a-208705/default.aspx

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

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

KRESA, Dan, 2018. Co je hacktivismus. *KYBEZ* [online]. [cit. 2022-02-15]. Dostupné z: https://www.kybez.cz/co-je-hacktivismus-/

KRESA, Dan, 2019. Analýza kybernetické bezpečnosti. *KYBEZ* [online]. [cit. 2022-02-15]. Dostupné z: https://www.kybez.cz/analyza-kybernetic ke-bezpecnosti-3-identifikace-hrozeb-a-zranitelnosti/

Magikmonitor, © 2022. *Magikinfo* [online]. [cit. 2022-04-26]. Dostupné z: https://www.magikinfo.cz/magikmonitor

NÚKIB, © 2022, a. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. [cit. 2022-3-16]. Dostupné z:

https://www.nukib.cz/download/publikace/doporuceni/Zakladni_bezpecnostni_opatreni_pro_vrcholove_vedeni_brozura_barevna.pdf

NÚKIB, © 2022, b. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. [cit. 2022-4-13]. Dostupné z: https://www.nukib.cz/cs/infoservis/doporuceni/1593-doporuceni-k-pouzivani-protokolu-tlp-ke-sdileni-chranenych-informaci/

NÚKIB, © 2022, c. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. [cit. 2022-4-25]. Dostupné z: https://osveta.nukib.cz/course/view.php?id=67

NÚKIB, 2020. *Národní strategie kybernetické bezpečnosti České republiky na období let 2021-2025*. In: *NÚKIB* [online]. Brno: NÚKIB [cit. 2021-11-20]. Dostupné z: https://www.nukib.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2020-2025_%20cr.pdf

NÚKIB, 2021, a. *Akční plán k Národní strategie kybernetické bezpečnosti České republiky na období let 2021-2025*. In: *NÚKIB* [online]. Brno: NÚKIB [cit. 2021-11-21]. Dostupné z: https://www.nukib.cz/download/publikace/strategie_akcni_plany/akcni_plan_2021-2025.pdf

NÚKIB, 2021, b. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2020*, 2021. In: *Národní úřad pro kybernetickou a informační bezpečnost* [online]. NÚKIB [cit. 2021-11-20]. Dostupné z: https://nukib.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_KB_2020.pdf

NÚKIB, 2021, c. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. [cit. 2021-11-20]. Dostupné z: https://nukib.cz/cs/o-nukib/

NÚKIB, 2021, d. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. [cit. 2021-11-20]. Dostupné z: https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/

RAINS, Tim, 2020. *Cybersecurity Threats, Malware Trends, and Strategies*. Birmingham: Packt Publishing Ltd. ISBN 978-1-80020-601-4.

Redundace, © 2022. *MasterDC – Specialisté na firemní IT infrastrukturu* [online]. Brno [cit. 2022-4-13]. Dostupné z: https://www.master.cz/help/slovnik/redundance/

Seznam ČSN, © 2021. *Česká agentura pro standardizaci* [online]. [cit. 2021-11-21]. Dostupné z: http://seznamcsn.agentura-cas.cz/Vysledky.aspx

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 978-80-7380-765-8.

STALLINGS, William, 2019. *Effective Cybersecirity*. 1st edition. Boston: Addison-Wesley Professional. ISBN 978-0-13-477280-6.
Systém na řízení rizik ve firmě, © 2022. *Aptien* [online]. [cit. 2022-04-25]. Dostupné z: https://aptien.com/cs/system-rizeni-rizik#product_hero

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

BRS	Bezpečnostní rada státu
CERT	Computer Emergency Response Team
COBIT	Control Objectives for Information and Related Technology
ČAS	Česká organizace pro standardizaci
ČR	Česká republika
EU	Evropská unie
FMEA	Failure Mode and Effects Analysis
GDPR	General Data Protection Regulation
ICT	Informační a komunikační technologie
ISO	International Organization of Standardization
IT	Informační technologie
ITIL	Information Technology Infrastructure Library
KI	Kritická infrastruktura
MÚ	Mimořádná událost
NBÚ	Národní bezpečnostní úřad
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
SCIRT	Computer Security Incidents Response Team
TLP	Taffic light protocol
ÚNMZ	Úřad pro technickou normalizaci, metrologii a státní zkušebnictví
URL	Uniform Resource Locator
VPN	Virtual Private Network

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM GRAFŮ

SEZNAM PŘÍLOH

PŘÍLOHA P I: ŘÍZENÝ ROZHOVOR

Otázky pro určení stavu kybernetické bezpečnosti s jednatelem subjektu.

Jaké jsou vaše primární aktiva, která by ohrozila nebo poškodila vaši firmu?

Jsou to údaje klientů a některých obzvlášť. Někteří naši klienti to mají dokonce ve smlouvě pod velkou pokutou. Občas jsou i zaplombovány kamery na mobilních telefonech našich zaměstnanců při práci u těchto klientů. Samozřejmě bychom ztratily důvěryhodnost, a to by nás velice poškodilo.

Dále jsou to cenové nabídky a další informace o výběrových řízeních, kde by nám při úniky vznikla značná škoda. A informace o dalším rozvoji firmy a zavádění nových služeb.

Dále s vás zeptám na podpůrná aktiva. Co vaši zaměstnanci potřebují při práci?

Zaměstnanci v managementu společnosti používají stolní počítače a laptopy při práci z domova. Každý zaměstnanec má služební chytrý mobilní telefon, pomocí kterých se dorozumíváme a také evidujeme docházku. V kanceláři je ještě scanner a tiskárna.

Jaký operační systém využíváte?

Všechno běží na Windows 10 a mobily Android. Jenom já mám iOS.

Tiskárnu máte zabezpečenou?

Ne tiskárnu máme sítovou, a tak je dostupná pro všechny**.**

Mate zabezpečena statická média?

Ano jdou uložena v zamykatelných kartotékách a trezoru.

Jakým způsobem máte vyřešeno připojení?

Máme zřízeno pevné připojení k internetu kabelem a v kanceláři máme wifi router. V každém chytrém telefonu je předplacený mobilní internet.

Máte ještě nějaká další podpůrná aktiva?

Pokud se to za ně pokládá tak máme sedm služebních osobních vozidel, dva bagry, nákladní vozidlo, vysokozdvižný vozík, nakladač a dumper. Ve všech máme GPS, abychom mohli sledovat jejich pohyb.

A co se týká vlastnictví aktiv?

Všechny vlastníme. Osobní auta jsou přidělena stabilně a ostatní aktiva dle momentální potřeby.

Máte ve vaší společnosti osobu odpovědnou za kybernetickou bezpečnost?

Doteď jsem to nijak neřešili, takže nemáme. Asi to budu já.

Plánujete zabezpečit společnost obvodovou ochranou?

Jsme v areálu, který je obvodově zabezpečen a je, zda ostraha v podobě vrátného, ale plánujeme do budoucna.

Vede se evidence vstupu do areálu nebe existuje systém povolení k vstupu?

Nic takového pustí vlastně každého.

Máte zabezpečené kanceláře, místnosti a vybavení?

Ano, máme zabezpečovací systém a kamerový systém.

Kdo má přístup do kanceláří?

Pouze zaměstnanci k tomu určení.

Každý zaměstnance má svůj vlažní kód?

Ne máme jeden, který používají všichni.

Chráníte se proti přírodním hrozbám?

Ano máme požární čidla a pojištění.

Říká vám něco pojem zabezpečená oblast.

Ano, ale nevím přesně.

Máte oddělené prostory pro osoby zpracovávající informace a ostatní zaměstnance?

Ano máme odděleny kanceláře od šaten a skladovacích prostorů. Ale pokud je to potřeba tak vstupují i ostatní zaměstnanci.

Jakým způsobem řešíte ochranu zařízení?

Máme je umístěné v zabezpečené kanceláři a jsou zaheslované.

Máte nastavenou politiku hesel a jeho kontrolu?

Zařízení musí být zaheslováno, ale nemáme žádné požadavky na délku atak. Žádnou kontrolu neděláme.

Provádíte pravidelné aktualizace?

Ano každý uživatel si aktualizuje svoje přidělené zařízení.

Používáte nějaký náhradní způsob napájení?

Ne, nemáme nic.

Jakým způsobem řešíte bezpečnost kabelových rozvodů?

Jsou pod zemí jinak nijak.

Jakým způsobem je prováděna údržba zařízení?

Máme nasmlouvanou firmu. Někdy závadu nebo údržbu řeší na místě a někdy si počítač odvezou a pak ho zase vrátí.

Prověřujete, jestli nemanipulovali s daty po opravě?

Ne.

Je u vaší společnosti možné pracovat z domova?

Ano, stalo se to jakýmsi pravidlem. Zaměstnanci této možnosti využívají poměrně často.

Vedete evidenci provozu zařízení mimo prostory organizace?

Evidenci ani žádné záznamy nevedeme, ale zařízení mohou vynášet pouze se svolením. I když svolení mají momentálně všichni.

Jakým způsobem likvidujete paměťová media?

V podstatě žádné nepoužíváme a pokud ano tak pouze pokud to vyžaduje výběrové řízení. Potom se zařízení naformátuje.

Jakým způsobem řešíte ochranu citlivých informací?

Máme trezor a uzamykatelné kartotéky. Tiskárna je volně, pro všechny. Počítače by měli být vždy zaheslovány, ale nikdo to nekontroluje.

Jakým způsobe, řešíte ochranu proti malware?

Máme antivirové programy, které si platíme. Používáme McAfee.

Mají uživatelé administrátorká práva?

Ano nijak to neomezujeme jak na počítačích, tak na telefonech.

Provádíte pravidelnou zálohu dat?

Ano používáme cloudová úložiště OneDrive, která máme předplacené.

Provádíte kontrolu záloh?

Ne, ale zatím nebyl problém.

A co šifrování dat?

Neřešíme, nešifrujeme.

Školíte nebo vzděláváte vaše zaměstnance v oblasti kybernetické bezpečnosti?

Nic takového neprovádíme, ale asi by to nebylo na škodu.

Setkal jste se s pojmy phishing, ransomware?

Phishing s tím už jsem se setkal, ale ransomware přesně nevím.

Co si přestavujete pod pojmem kybernetický útok?

Krádež dat, zformátování počítače nebo vykradení účtu.

Myslíte si, že je nutné začít kybernetickou bezpečnost řešit?

Teď už ano, po tomto rozhovoru. Ani jsem si neuvědomoval, jak je to všechno provázané a jak je to nebezpečné. Začneme to určitě řešit.