Specifikace řešení kybernetických bezpečnostních incidentů

Bc. Lukáš Papšík

Diplomová práce
2022

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav elektroniky a měření

Akademický rok: 2021/2022

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Lukáš Papšík**
Osobní číslo:	**A20703**
Studijní program:	**N1032A020003 Bezpečnostní technologie, systémy a management**
Specializace:	**Bezpečnostní management**
Forma studia:	**Kombinovaná**
Téma práce:	**Specifikace řešení kybernetických bezpečnostních incidentů**
Téma práce anglicky:	**Specification for Solving Cyber Security Incidents**

Zásady pro vypracování

1. Vypracujte literární rešerši na dané téma.
2. Analyzujte právní rámec předmětné problematiky.
3. Popište účel a strukturu organizace z hlediska kybernetické bezpečnosti.
4. Definujte a srovnejte modely řešení kybernetické bezpečnosti.
5. Realizujte aplikace vybraného bezpečnostního modelu.

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

Seznam doporučené literatury:

1. LUKÁŠ, Luděk. Teorie bezpečnosti I. Zlín: Radim Bačuvčík ? VeRBuM, 2017. ISBN 978-80-87500-89-7.
2. LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management V. Zlín: Radim Bačuvčík ? VeRBuM, 2015. ISBN 978-80-87500-67-5.
3. ČAPEK, Jan, Miloslav HUB, Radim ROUDNÝ, Hana KOPÁČKOVÁ, Jan FUKA a Martin IBL. Vybrané aspekty kybernetické bezpečnosti. Pardubice: Univerzita Pardubice, 2015. Monografia. ISBN 978-80-7395-953-1.
4. KOLOUCH, Jan a Pavel BAŠTA. CyberSecurity. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88168-31-7.
5. MCCARTHY, N. K. The computer incident response planning handbook: executable plans for protecting information at risk. New York: McGraw-Hill, 2012. ISBN 978-0-07-179039-0.
6. SMEJKAL, Vladimír, Tomáš SOKOL a Jindřich KODL. Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. ISBN 9788073807658.

Vedoucí diplomové práce: **doc. Ing. Martin Hromada, Ph.D.**
Ústav bezpečnostního inženýrství

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

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

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

Ing. Milan Navrátil, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 7. února 2022

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně;
- byl/a jsem seznámen/a s tím, že 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;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- beru na vědomí, že 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 totožné.

Ve Zlíně, dne …….

Lukáš Papšík v. r.

ABSTRAKT

Tato diplomová práce pojednává o problematice řešení kybernetických bezpečnostních incidentů. Teoretická část definuje specifika řešení incidentů kybernetické bezpečnosti. Cílem praktické části bylo definovat, zhodnotit a vytvořit modely řešení bezpečnostního incidentu a následné vybrat nejlepší model. Na tento model posléze aplikoval reálný bezpečnostní incident a tím ověřit jeho funkcionalitu.

Klíčová slova: kybernetická bezpečnost, kybernetická obrana, kybernetický útok, riziko, hrozba, řízení, organizace

ABSTRACT

This diploma thesis deals with the issue of solving cyber security incidents. The theoretical part defines the specifics of solving cyber security incidents. The aim of the practical part was to define, evaluate and create models for dealing with a security incident and then select the best model. He later applied a real security incident to this model and thus verify its functionality.

Keywords: Cyber Security, Cyber Defense, Cyber-attack, Risk, Threat, Control, Organization

Nejprve bych rád poděkoval doc. Ing. Luďkovi Lukášovi, CSc. za první nasměrování ve tvorbě diplomové práce a zároveň bych rád poděkoval doc. Ing. Martinovi Hromadovi, Ph.D. za vedení, korekturu a podněty k mé diplomové práci.

Dále bych rád poděkoval mé manželce a mým dětem za podporu během studia a klid, který mi dopřály pro tvorbu diplomové práce.

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

OBSAH

ÚVOD

Žijeme v době, kdy se počet kybernetických útoku zvyšuje. Tyto útoky stále častěji ať už přímo či nepřímo ovlivňují naše životy. Nemalý podíl na tom má snaha co nejvíce věci digitalizovat. Cílem útoků se stávají státní ale i nestanní organizace. Lidská společnost se na tyto útoky připravuje pomocí legislativy, organizačních a technických prostředku, ale také procesem jak útok odrazit.

Pracuji na pozici, kde probíhá výměna a předávání všech informaci, technických i netechnických, při řešení kybernetického bezpečnostního incidentu. V rámci pozice, kterou zastávám, řešíme neustále otázky koho informovat, jaký může být dopad, o jaký typ útoku se jedná apod. Otázky vznikají ze způsobu, jakým je kybernetický útok vedený. Na kybernetický útok nelze zcela reagovat klasickým způsobem řízení incidentu. A proto se někdy stává, že daný útok by byl zastaven dříve, kdybychom k němu přistupovali jiným způsobem. Svoji diplomovou práci jsem zaměřil na seznámení s legislativním rámcem, kybernetickými útoky, základní kybernetickou analýzou a úlohou organizační struktury organizace při řešení incident.

Cílem práce je definovat a srovnat modely možných řešení kybernetického bezpečnostního incidentu a na vybraný model aplikovat kybernetický incident a dokázat tak jeho funkčnost.

I. TEORETICKÁ ČÁST

1 KYBERNETICKÁ BEZPEČNOST, ÚVOD DO PROBLEMATIKY A DEFINICE ZÁKLADNÍCH POJMŮ

Tato kapitola se bude snažit vymezit základní právní rámce kybernetické bezpečnosti a povinnosti plynoucí ze zákona zejména pro osoby povinné. Budou zde uvedeny nejpodstatnější definice a názvosloví z oboru kybernetické bezpečnosti. Jednotlivé definice a právní základ je zde uveden v míře, která je nutná pro řešení kybernetických bezpečnostních incidentů a jejich specifika, která jsou cílem této diplomové práce. Cílem této kapitoly není zpracovat komplexní náhled na kybernetickou bezpečnost z pohledu práva.

1.1 Právní rámce kybernetické bezpečnosti

Z pohledu práva je kybernetická bezpečnost chápána v užším slova smyslu především na úrovni státu tedy jako ochranu národního zájmu před hrozbami, které se mohou negativně projevit v národním měřítku. Na nižší úrovni je kybernetická bezpečnost řešena pomocí standartních nástrojů českého práva trestního, správního nebo civilního[1].

Legislativní dokumenty, které řeší problematiku kybernetické bezpečnosti přímo nebo nepřímo jsou:

- Usneseni č.2/1993 Sb. – Listina základních práv a svobod.
- Ústavní zákon č.110/1998 Sb. – Ústavní zákon o bezpečnosti České republiky.
- Zákon č.181/2014 Sb. – Zákon o kybernetické bezpečnosti.
- Zákon č. 127/2005 Sb. – Zákon o elektronických komunikacích.
- Zákon č. 150/2021 Sb. – Zákon o vojenském zpravodajství.
- Zákon č. 240/2000 Sb. – Krizový zákon.
- Zákon č. 412/2005 Sb. – Zákon o ochraně utajovaných informací a bezpečnostní způsobilosti.
- Vyhláška č. 82/2018 Sb. – Vyhláška o kybernetické bezpečnosti.
- Vyhláška č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci.

[1] GOGELA, Robert, 2011. *Pracovní příručka bezpečnostního manažera*. Praha: Policejní akademie ČR v Praze. ISBN 978-80-7251-364-2.

- Vyhláška č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu.
- Vyhláška č. 317/2014 Sb. – Vyhláška o významných informačních systémech a jejich určujících kritériích.
- Nařízení vlády č. 315/2014 Sb. – Nařízení vlády, kterým se mění nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury.

1.1.1 Zákon a vyhláška kybernetické bezpečnosti

V tomto odstavci se budeme v krátkosti zabývat dvěma důležitými legislativními dokumenty upravující činnost při řešení kybernetických bezpečnostních incidentů.

Zákon o kybernetické bezpečnosti začal vznikat na půdě Národního bezpečnostního úřadu v roce 2013. Cílem nově vznikajícího zákona byla ochrana informačních systému, komunikačních systému a kritické infrastruktury. Byly definovány povinnosti subjektu (osob) a povinnost detekovat kybernetické bezpečnostní incidenty pro tyto subjekty.

Novinkou a novým bezpečnostním stavem v ČR, se dnem vstupu zákona o kybernetické bezpečnosti stal *stav kybernetického nebezpečí.* Tento stav vyhlašuje ředitel Národního úřadu pro kybernetickou a informační bezpečnost. Vyhlašuje ho na nezbytně dlouhou dobu, nejdéle však 7 dní a může být rozhodnutím ředitele prodloužen až na dobu 30 dní. Pokud ani do 30 dnů od vyhlášení, stav kybernetického nebezpečí trvá, může tento stav přejit do nouzového stavu.

Cíle ZoKB lze shrnout do následujících tvrzení:

- Cílem je stanovit základní úroveň bezpečnostních opatření.
- Cílem je zlepšit detekci kybernetických bezpečnostních incidentů.
- Cílem je zavést systém hlášení o kybernetických bezpečnostních incidentech.
- Cílem je zavést systém opatření na kybernetické bezpečnostní incidenty.
- Stanovit činnost pracovišť národní CERT a vládní CERT[2].

Vyhláška o kybernetické bezpečnosti začala vznikat na popud směrnice Evropského parlamentu a Rady (EU) 2016/1148[3]. Některé požadavky této směrnice byly zapracovány již

[2] Legislativa KB. In: *Nukib.cz* [online]. Brno [cit. 2022-04-27]. Dostupné z: https://nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/

do ZoKB. Hlavní devízou vyhlášky je zaměření na věci z praxe, do přesnění některých termínů a ukázka praktických příkladů.

Cíle VoKB lze shrnout do následujících tvrzení:

- Cílem je stanovit obsah a strukturu bezpečnostní dokumentace.
- Cílem je stanovit obsah a rozsah bezpečnostních opatření.
- Cílem je stanovit kategorie a hodnocení významnosti kybernetických bezpečnostních incidentů.
- Cílem je stanovit způsob a náležitosti hlášení o kybernetickém bezpečnostním incidentu.
- Cílem je stanovit náležitosti hlášení o provedení reaktivního opatření a jeho výsledku na kybernetický bezpečnostní incident.
- Cílem je stanovit způsob likvidace dat, provozních údajů, informaci a jejich kopií[4].

1.1.2 Povinnosti odpovědných osob

Zákon o kybernetické bezpečnosti stanovuje vcelku jasná a přesná pravidla pro osoby, které jsou povinné z tohoto zákona podle § 3 zákona č. 181/2014 Sb.

Jistým záporem ZoKB, je stanovení povinností pouze pro správce a provozovatele systému, pokud není správce a provozovatel zároveň poskytovatelem, subjektem, orgánem nebo osobou a pokud ano, tak i tito jsou povinni podle zákona.

Výše uvedené osoby podle § 6 vyhlášky č. 82/2018 Sb. musí určit osoby zastávající role:

- manažera kybernetické bezpečnosti,
- architekta kybernetické bezpečností,
- garanta aktiva,
- auditora kybernetické bezpečnosti.

---

[3] Směrnice evropského parlamentu a rady (EU) 2016/1148, 2016. In: *EUR-Lex.europa.eu* [online]. LUXEMBOURG [cit. 2022-04-27]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32016L1148&from=EN

[4] Legislativa KB. In: *Nukib.cz* [online]. Brno [cit. 2022-04-27]. Dostupné z: https://nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/

V mnoha organizacích jsou určení další architekti, manažeři, kteří svým způsobem mohou ovlivnit daný systém natolik, že dle daného zákonu bude muset být konáno. Veškerá odpovědnost za tuto činnost spadá na správce nebo provozovatele.

Mohou se objevit i rozsáhlé organizace povinné ze ZoKB, které navenek mají jednoho provozovatele svých informačních nebo komunikačních systému, ale vnitřním členěním zde vznikají další pozice správců a provozovatelů, kteří v zákoně již nejsou na rozdíl od hlavního provozovatele definování.

Povinné osoby pak musí hlásit narušení dostupnosti, důvěryhodnosti a integrity informaci. Musí implementovat, pokud je zákoně vyžadováno, nařízení Národního úřadu pro kybernetickou a informační bezpečnost[5].

1.2 Definice pojmů

V kybernetické bezpečnosti stejně jako v jiných druzích bezpečnosti je velmi důležité definovat názvosloví a pojmy, aby nedocházelo k záměně významů a shodnému chápaní jednotlivých výrazů.

Sjednocení terminologie v oblasti informačních a komunikačních technologií není jednoduché ať už z důvodu rychlého rozvoje oboru, tak z důvodu možného duplicitního pojmenovávání stejných výrazů nejenom samotnými techniky, ale také manažery, kteří do oblasti informačních a komunikačních technologií vstupují stále častěji.

1.2.1 Kybernetická bezpečnost

Bezpečnost je základním pojmem bezpečnostní terminologie v řadě společenskovědních, přírodovědných a technických oborů. Jejím synonymem, tak jak je uvedeno ve slovníku spisovné češtiny, je jistota a spolehlivost[6]. Všeobecně je pojem bezpečnost vymezován v negativním významu ve vztahu k hrozbám.

---

[5] SMEJKAL, Vladimír, Tomáš SOKOL a Jindřich KODL, 2019. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk. ISBN 978-807-3807-658.

[6] ČERVENÁ, Vlasta, FILIPEC, Josef, ed., 2003. *Slovník spisovné češtiny pro školu a veřejnost s Dodatkem Ministerstva školství, mládeže a tělovýchovy České republiky*. Vyd. 3., opr. Praha: Academia. ISBN 80-200-1080-7.

Pojem kybernetická bezpečnost ve srovnání s „klasickými“ druhy bezpečnosti jako jsou fyzická bezpečnost, administrativní bezpečnost a další druhy bezpečnosti, nelze jednoznačné definovat. Kybernetická doména tedy místo, kde kybernetická bezpečnost působí, můžeme rozdělit například na doménu fyzickou a doménu virtuální z hlediska působení hrozby. Důležité je zmínit, že hranice kybernetické domény nejsou limitovány podobně jako u klasických druhů bezpečnosti a může tak působit kdekoliv, kdykoliv a jakkoliv.

Jednoduše a s přihlédnutím na aktuálně platné zákony můžeme kybernetickou bezpečnost definovat jako soubor opatření vedoucí k zajištění dostupnosti, důvěryhodnosti a integrity informaci[7].

1.2.2 Kybernetický prostor

Diplomová práce přibližuje problematiku řešení kybernetických bezpečnostních incidentů, proto se musí nejprve vymezit onen kybernetický prostor, kde tyto incidenty probíhají. V kyberprostoru samozřejmě dochází k další činnosti, k obraně, útoku, k ochraně digitální dat apod. Komplexnost tohoto prostoru však přináší problém v jeho definici[8]. Podle encyklopedie Britannica je kyberprostor: beztvarý virtuální svět, bez vnitřní struktury, který je vytvořen propojenými počítači, servery, routery a dalšími internetovými zařízeními do celosvětové internetové infrastruktury. Na rozdíl od Internetu samotného je však kyberprostor místem, kde se tyto propojení vytvářejí[9]. Pokud se budeme držet legislativních definic, můžeme použít znění § 2 písm. a) zákona č. 181/2014 Sb., kde je uvedeno, že “*kybernetickým prostorem je digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací*“.

Je vidět, že definovat kyberprostor je složité a to nejenom z důvodu, že si mnoho lidí myslí, že Internet je kyberprostor a naopak. Proto zde použiji podle mého názoru definice jasnější a to, že kyberprostor je místo (data, informace, služby), které nelze běžně dostupnými prostředky vyhledat v Internetu[10].

---

[7] LUKÁŠ, Luděk, 2017. *Teorie bezpečnosti I*. Zlín: Radim Bačuvčík - VeRBuM. ISBN 978-80-87500-89-7.
[8] KOLOUCH, Jan a Pavel BAŠTA, 2019. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o. CZ.NIC. ISBN 978-808-8168-348.
[9] BUSSELL, Jennifer, 2013. *Cyberspace* [online]. In: . Encyclopedia Britannica [cit. 2022-04-27]. Dostupné z: https://www.britannica.com/topic/cyberspace. Překlad autora.
[10] KOLOUCH, Jan a Pavel BAŠTA, 2019. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o. CZ.NIC. ISBN 978-808-8168-348.

1.2.3 Aktivum

Aktivum je v kybernetické bezpečnosti myšleno, jako soubor technického a programového vybavení tzv. hardware, software, procesy a lidské zdroje, které jsou nezbytné k dané funkci informačního nebo komunikačního systému.

Na základě toho lze dělit aktiva na:

- Primární aktiva – informace nebo služba.
- Podpůrná aktiva – lidské zdroje, dodavatelé.
- Technická aktiva – technické vybavení, software apod.[11]

1.2.4 Kybernetická bezpečnostní událost

Zákon o kybernetické bezpečnosti definuje kybernetické bezpečnostní události jako události, které mohou způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikacích[12].

Zjednodušeně se jedná o možné narušení bezpečnosti, tedy o možný kybernetický útok. Příkladem uveďme phishingový e-mail, který obsahuje škodlivý odkaz vedoucí ke stažení malwaru. Až v případě přistoupení na daný odkaz a stáhnutím malware nastává kybernetický bezpečnostní incident, viz níže.

1.2.5 Kybernetický bezpečnostní incident

Zákon o kybernetické bezpečnosti definuje kybernetický bezpečnostní incident jako narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikacích[13].

---

[11] ČESKO. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) - znění od 1. 9. 2021. In: *Zákony pro lidi.cz* [online]. © AION CS 2010-2022 [cit. 27. 4. 2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181#f5278849

[12] ČESKO. § 7 odst. 1 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) - znění od 1. 9. 2021. In: *Zákony pro lidi.cz* [online]. © AION CS 2010-2022 [cit. 31. 1. 2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181#p7-1

[13] ČESKO. § 7 odst. 2 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) - znění od 1. 9. 2021. In: *Zákony pro lidi.cz* [online]. © AION CS 2010-2022 [cit. 31. 1. 2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181#p7-2

Zjednodušeně se tedy jedná o narušení bezpečností, které aktuálně probíhá nebo již proběhlo. A to z důvodu, že v kybernetické bezpečnosti jsou některé útoky detekované tzv. ex-post.

1.2.6 Kybernetický útok

Cílená snaha poškodit referenční objekt využitím zranitelností v informačním nebo komunikačním systému a tím tomuto referenčnímu objektu způsobit újmu.

Útoky, které nejsou vedeny jednorázově a využívají pokročilých technik a jsou vedeny jednotlivci nebo skupinami, se souhrnně označují anglickým výrazem Advance Persistent Threat[14].

1.2.7 Kybernetická hrozba

Cílená aktivita jednotlivce nebo skupiny s cílem způsobit újmu nebo poškodit informační nebo komunikační systém nebo těchto systému využít pro další škodlivou činnost. Dále může být hrozba definována jak entita schopná narušit pořádek, řádný stav IS nebo KS.

V bezpečnostní strategii České republiky z roku 2003 je hrozba definována jako "jakýkoli fenomén, který má schopnost potencionálně poškodit zájmy ČR[15]".

1.2.8 Kybernetická zranitelnost

Úmyslná nebo neúmyslná chyba v informačním nebo komunikačním systému, která může být zneužita útočníkem.

Zranitelnosti dělíme na základě znalosti na:

- známe,
- neznámé.

Známé zranitelnosti jsou výrobcem publikované, ale výrobce daného softwaru nevydal nebo nezná účinnou bezpečnostní záplatu. Avšak výrobce udává, jakým způsobem lze da-

---

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

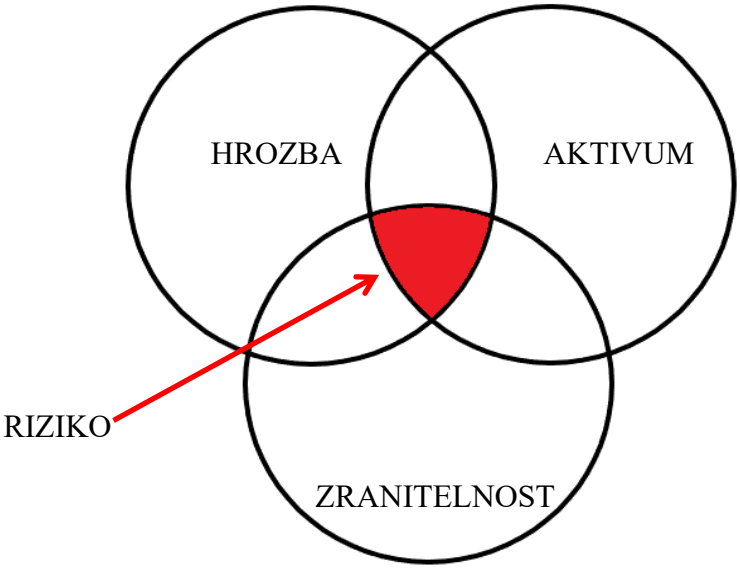
[15] *Bezpečnostní strategie ČR (2003)* [online], 2003. PRAHA: Ministerstvo pro místní rozvoj ČR [cit. 2022-04-27]. Dostupné z: https://www.dataplan.info/img_upload/7bdb1584e3b8a53d337518d988763f8d/bezpecnostni-strategie-cr.pdf

nou zranitelnost zneužít a jaké kroky může vlastník aktiv provést, aby tyto zranitelnosti minimalizoval.

U neznámých zranitelností záleží na tom, zda je výrobce, analytik nebo kdokoliv jiný objeví dříve, než útočník dokáže těchto zranitelností zneužít.

1.2.9 Riziko

Pojem riziko v kybernetickém prostoru významně souvisí s výše uvedenými pojmy KBU, KBI, hrozba, zranitelnost a aktivum. Výkladový slovník kybernetické bezpečnosti definuje riziko jako:



Obrázek 1 Znázornění vztahu riziko, hrozba, zranitelnost a aktivum
[zdroj: Vlastní tvorba]

- Nebezpečí, možnost škody, ztráty, nezdaru.
- Účinek nejistoty na dosažení cílů.
- Možnost, že určitá hrozba využije zranitelnosti aktiva nebo skupiny aktiv a způsobí organizaci škodu[16].

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

V obecnější rovině můžeme o riziku tvrdit, že se jedná o stav, kdy hrozba, jedna nebo více může zneužít zranitelnosti a tím způsobit újmu aktivům. Tento proces je znázorněn na obrázku 1. Riziko však lze definovat i matematickým vztahem

$$R = H \times A \times Z,$$

kde R je míra rizika, H je hodnota hrozby, A je hodnota aktiva a Z je hodnota zranitelnosti. Aktivum lze také vyjádřit mírou dopadu na tři základní pilíře kybernetické bezpečnosti dostupnosti, důvěryhodnosti a integrity informací. Riziko je pak definováno vtahem

$$R = H \times D \times Z,$$

kde D je hodnota dopadu na aktivum[17].

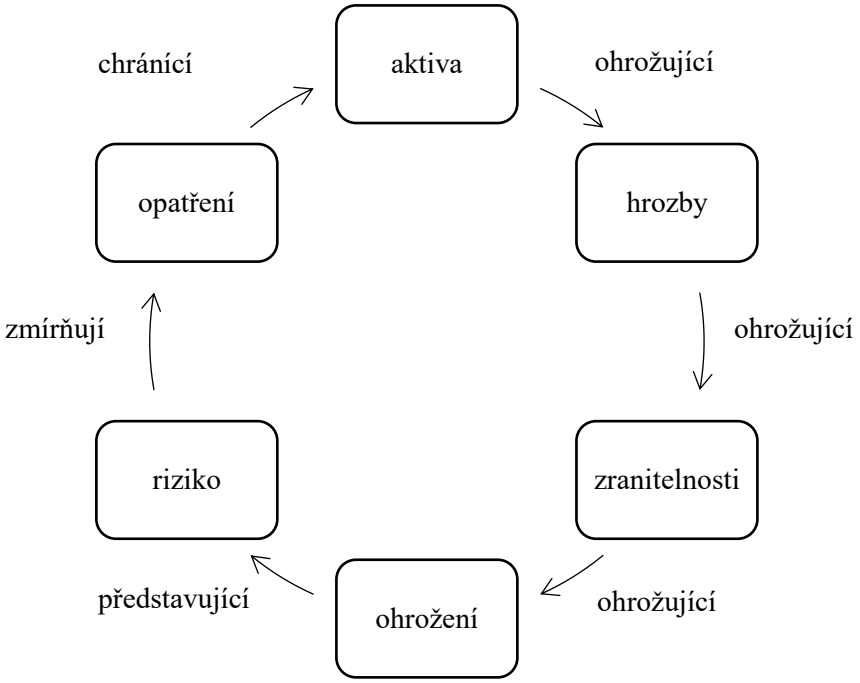
1.3 Závěr kapitoly

Kybernetická bezpečnost jak z pohledu legislativy, tak z pohledu definic prochází obdobím velkých změn. Některé instituce, lidé spojují kybernetickou bezpečnost pouze s fyzickými předměty a proto v tomto pohledu může kybernetická bezpečnost působit trochu jako filozofie. Doufám, že se Vám jako čtenářům v této kapitole dostalo základních odpovědí, kde kybernetická bezpečnost působí a čím může být narušena jako i definice základních pojmů.

[17] ČESKO. Příloha č. 2 vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) - znění od 28. 5. 2018. In: *Zákony pro lidi.cz* [online]. © AION CS 2010-2022 [cit. 27. 4. 2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/2018-82#f6228918

2 ANALÝZA KYBERNETICKÝCH RIZIK

V této kapitole bude následovat analýza kybernetických rizik z pohledu teorie. Bude vysvětleno jak určit dopad, jak identifikovat a analyzovat hrozbu a nakonec identifikace a analýza zranitelnosti.



Obrázek 2 Schéma analýzy rizik [zdroj: Miroslav Čermák]

2.1 Metoda analýzy rizik

Vyhláška č. 82/2018 Sb. kybernetické bezpečnosti ve svých přílohách pomáhá povinným osobám stanovit hodnotu aktiva, dopadu, zranitelnosti a hrozby. Další pomůckou pro analýzu kybernetických rizik je mezinárodní norma ISO 27001 neboli systém řízení bezpečností informací.

Kompletní proces analýzy je znázorněn graficky na obrázku 2.

2.2 Analýza dopadu

V kybernetické bezpečnosti je nejtěžším úkolem hodnocení dopadu. Dopad se určuje pro každé aktivum zvlášť a tím zároveň určuje důležitost aktiva. Vzhledem k tomu, že dopad ovlivňuje bezpečnost informací v IS nebo KS, respektive jaký dopad by mělo nerušení bezpečnosti informací, lze pro hodnocení využít tří pilířů tzv. CIA triády, tedy důvěrnosti,

dostupnosti a integrity. Základní pomůckou může být tabulka 1 pro ohodnocení dopadu, která je přílohou č. 1 k vyhlášce č. 82/2018 Sb.[18]

Tabulka 1 Hodnocení aktiva[19]

Úroveň	Popis důvěrnosti	Popis dostupnosti	Popis integrity
Nízká	Aktiva jsou veřejně dostupná nebo byla určená ke zveřejnění.	Narušení dostupnosti aktiva není důležité a v případě výpadku je běžně tolerováno delší časové období pro nápravu (cca do 1 týdne).	Aktivum nevyžaduje ochranu z hlediska integrity. Narušení integrity aktiva neohrožuje oprávněné zájmy povinné osoby.
Střední	Aktiva nejsou veřejně přístupná a tvoří know-how povinné osoby, ochrana aktiva není vyžadována žádným právním předpisem nebo smluvním ujednáním.	Narušení dostupnosti aktiva by nemělo překročit dobu pracovního dne, dlouhodobější výpadek vede k možnému ohrožení oprávněných zájmů povinné osoby.	Aktivum může vyžadovat ochranu z hlediska integrity. Narušení integrity aktiva může vést k poškození oprávněných zájmů povinné osoby a může se projevit méně závažnými dopady na primární aktiva.
Vysoká	Aktiva nejsou veřejně přístupná a jejich ochrana je vyžadována právními předpisy, jinými předpisy nebo smluvními ujednáními (například obchodní tajemství, osobní údaje).	Narušení dostupnosti aktiva by nemělo překročit dobu několika hodin. Jakýkoli výpadek je nutné řešit neprodleně, protože vede k přímému ohrožení oprávněných zájmů povinné osoby. Aktiva jsou považována za velmi důležitá.	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity aktiva vede k poškození oprávněných zájmů povinné osoby s podstatnými dopady na primární aktiva.
Kritická	Aktiva nejsou veřejně přístupná a vyžadují nadstandardní míru ochrany nad rámec předchozí kategorie (například strategické ob-	Narušení dostupnosti aktiva není přípustné a i krátkodobá nedostupnost (v řádu několika minut) vede k vážnému ohrožení oprávněných zájmů	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity vede k velmi vážnému poškození oprávněných zájmů povinné osoby s

[18] ČESKO. Příloha č. 1 vyhlášky č. 82/2018 Sb., vyhláška o kybernetické bezpečnosti - znění od 28. 5. 2018. In: *Zákony pro lidi.cz* [online]. © AION CS 2010-2022 [cit. 17. 2. 2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/2018-82#f6228907

[19] Taktéž

	chodní tajemství, zvláštní kategorie osobních údajů)	povinné osoby. Aktiva jsou považována za kritická.	přímými a velmi vážnými dopady na primární aktiva.

2.3 Identifikace a analýza hrozeb

Abychom mohli hrozby analyzovat, musíme je nejdříve identifikovat. K identifikaci hrozeb nám může pomoci příloha č. 3 k VoKB, kde jsou uvedeny vybrané typy hrozeb. Konkrétní identifikace hrozeb je odpovědností povinné osoby.

Ve své podstatě mohou být hrozby náhodné nebo úmyslné, přírodní nebo antropogenní. Povinná osoba na základě katalogu hrozeb, vlastních zkušeností nebo průzkumu s přihlédnutím k povaze organizace, kde je prováděna identifikace a analýza hrozeb tyto hrozby zhodnotí a ohodnotí. K hodnocení může být použita i tabulka 2, která je přílohou VoKB.

Tabulka 2 Stupnice pro hodnocení hrozeb[20]

Úroveň	**Popis**
Nízká	Hrozba neexistuje nebo je málo pravděpodobná. Předpokládaná realizace hrozby není častější než jednou za 5 let.
Střední	Hrozba je málo pravděpodobná až pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 roku do 5 let.
Vysoká	Hrozba je pravděpodobná až velmi pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 měsíce do 1 roku
Kritická	Hrozba je velmi pravděpodobná až víceméně jistá. Předpokládaná realizace hrozby je častější než jednou za měsíc.

2.4 Identifikace a analýza zranitelností

K identifikaci zranitelností můžeme použít stejnou přílohu jako v případě identifikace hrozeb. Platí přitom stejná pravidla pro povinnou osobu.

[20] ČESKO. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) - znění od 1. 9. 2021. In: *Zákony pro lidi.cz* [online]. © AION CS 2010-2022 [cit. 27. 4. 2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181#f5278849

Tabulka 3 Stupnice pro hodnocení zranitelností[21]

Úroveň	**Popis**
Nízká	Zranitelnost neexistuje nebo je zneužití zranitelnosti málo pravděpodobné. Jsou zavedena bezpečnostní opatření, která jsou schopna včas detekovat možné zranitelnosti nebo případné pokusy o jejich zneužití.
Střední	Zneužití zranitelnosti je málo pravděpodobné až pravděpodobné. Jsou zavedena bezpečnostní opatření, jejichž účinnost je pravidelně kontrolována. Schopnost bezpečnostních opatření včas detekovat možné zranitelnosti nebo případné pokusy o překonání opatření je omezena. Nejsou známé žádné úspěšné pokusy o překonání bezpečnostních opatření.
Vysoká	Zneužití zranitelnosti je pravděpodobné až velmi pravděpodobné. Bezpečnostní opatření jsou zavedena, ale jejich účinnost nepokrývá všechny potřebné aspekty a není pravidelně kontrolována. Jsou známé dílčí úspěšné pokusy o překonání bezpečnostních opatření.
Kritická	Zneužití zranitelnosti je velmi pravděpodobné až víceméně jisté. Bezpečnostní opatření nejsou realizována nebo je jejich účinnost značně omezena. Neprobíhá kontrola účinnosti bezpečnostních opatření. Jsou známé úspěšné pokusy překonání bezpečnostních opatření.

2.5 Závěr kapitoly

Kapitola popisuje analýzu kybernetických rizik. Vzhledem k existenci VoKB je pro osoby povinné ze zákona jednoduší provést analýzu rizik a to z důvodu, že ve vyhlášce jsou uvedeny praktické příklady, které může nejedna organizace využít ve své analýze rizik.

[21] ČESKO. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) - znění od 1. 9. 2021. In: *Zákony pro lidi.cz* [online]. © AION CS 2010-2022 [cit. 27. 4. 2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181#f5278849

3 KYBERNETICKÉ ÚTOKY

V současné době dochází stále častěji k útokům na prvky připojené do sítě Internet. Globalizace naučila lidstvo používat online svět stejně často jako svět reálný. Vždyť i jednotlivé státy jdou tomuto trendu naproti a snaží se co nejvíce státní sféru digitalizovat. O to víc jsme jako lidstvo náchylnější na útoky na tyto prvky, infrastrukturu. A aby se stát, populace či jedinec mohli účinně před těmito útoky chránit, je nutné nejprve porozumět jednotlivým typům kybernetických útoků a jakých zranitelností útočníci využívají.

Avšak rozdělit kybernetické útoky do typových kategorií je velmi obtížné a to nejenom z důvodu, že je téměř každý den objevena jedna nebo více zranitelností, ale také z důvodu, že ve většině případů je kybernetický útok složený z více dílčích útoku. Pokusíme se tedy ty nejznámější typy útoků v této kapitole popsat a zároveň uvést jaké zranitelnosti útočníci zneužívají.

3.1 Kdo útočí

V kapitole 1.2.6 jsme mluvili o definici kybernetického útoku. Než začneme popisovat ty nejznámější útoky, pojďme si říci kdo je nebo může být útočníkem. V dnešní době může být útočníkem v podstatě kdokoli. Ať už se jedná o státem podporované skupiny, APT, profesionály nebo jednice. Dnes nemusíte být počítačovým programátorem, ale stačí si stáhnout jednoduchý, volně dostupný program a můžete útočit. Samozřejmě, že tento typ útoku nebude tak komplexní jako profesionální útok a většina prvků v síti tento útok odhalí a zastaví, ale vy jste se stali oním útočníkem. Na Internetu lze naleznout nepřeberné množství návodů na kybernetický útok. Důležité je zmínit, že většina těchto návodů je postavena tak, abychom mohli otestovat a zabezpečit vlastní systém před podobným typem útoku.

Na druhou stranu dnešní útočníci nemusí používat ani tak komplexní útoky, jako spojení jednoho nebo více jednodušších útoků a za pomoci velké skupiny lidí mohou odstavit, znepřístupnit či jinak poškodit systém, na který útočí.

3.2 DoS, DDoS

Cílem tohoto útoku je odepření, znemožnění uživatelům využívat služby Internetu nebo webových stránek. Proti útoku neexistuje stoprocentní obrana a to z důvodu principu fungování Internetu.

Útok lze přirovnat například k vykoupení všech lístků na koncert a tím ostatním posluchačům znemožnit jeho poslech.

3.3 Phishing

Kybernetický útok, při kterém je využito technik sociálního inženýrství za účelem získání citlivých údajů oběti. Těmito údaji jsou hesla, čísla kreditních karet apod. Podle způsobu kompromitace můžeme dělit formy phishingu na:

- Spam nebo spear phishing,
- vishing
- smishing.

Spam je všeobecné označení nevyžádaného sdělení většinou ve formě elektronické pošty. Spam se snaží vylákat citlivé informace nebo údaje od uživatele tím, že mu například oznámí, že jeho e-mailová schránka je plná a musí se přihlásit svými údaji na níže uvedeném odkaze, jinak nebude moci nadále přijímat e-maily. Další způsob je vylákání peněz od uživatele tím, že se útočník vydává například za Českou poštu[22].

Spear phishing je velice podobný klasickému spamu, na rozdíl od něho zde útočník klade větší důraz na svoji oběť, o které se snaží zjistit co nejvíce informaci a na jejich základech přizpůsobit obsah zprávy. Takto vytvořená zpráva pak působí důvěryhodněji.

Slovo vishing vychází z anglického *voice phishing* a jedná se tedy o phishing za pomocí telefonu. Útočník se snaží, aby mu jeho oběť poskytla například přihlašovací údaje do internetového bankovnictví včetně potvrzovací sms[23].

Smishing je velmi podobný vishingu, ale namísto volání je zde použit jako vektor útoku SMS zpráva. NA vzestupu jsou, ale i ostatní formy komunikace na podobném principu, kde se vyměňují nejenom textové zprávy, jako příklad lze uvést takové služby jako what-

[22] Historie podvodných e-mailů a SMS, © 2022. In: *Ceskaposta.cz* [online]. Praha: Česká pošta, s.p. [cit. 2022-02-23]. Dostupné z: https://www.ceskaposta.cz/o-ceske-poste/historie-podvodnych-e-mailu
[23] Vishing a spoofing, © 2021. In: *Policie.cz* [online]. Policejní prezidium ČR [cit. 2022-02-23]. Dostupné z: https://www.policie.cz/clanek/vishing-a-spoofing.aspx

sapp, messenger apod. Útočníci se opět snaží vylákat citlivé údaje nebo přinutit oběť ke stáhnutí malwaru[24].

Ve všech případech phishingu neexistuje účinná obrana. Tyto útoky jsou velice jednoduché a útočník nemusí využít speciálních prostředku, ale běžně dostupných nástrojů. Jedinou aktuálně účinnou obranou proti těmto útokům je zvyšování bezpečnostního povědomí uživatelů a zdravý selský rozum.

3.4 SQL útoky

Útoky, které zneužívají bezpečnostních chyb vyskytujících se v databázové vrstvě aplikace[25]. Útočníci využívají jazyka SQL, který se používá pří správě a dotazování v databázích. Bezpečnostní chyba umožňuje útočníkům infiltraci do databáze vložením vlastního SQL příkazu. Záměrem je většinou získání citlivých údajů nebo změna struktura databáze.

Podobným typem útoku je XSS neboli cros-site scripting. Útočník se snaží vložením vlastního kódu do webové aplikace, získat citlivé údaje uživatele nebo se snaží o poškození webové stránky.

3.5 Zero day

V kybernetické bezpečnosti se jedná o formu útoku nebo hrozby, kdy se útočník snaží zneužít zranitelnosti používaného softwaru. Taková zranitelnost není dosud známa nebo pro ni výrobce softwaru nevydal bezpečnostní aktualizaci, a proto pro útočníka představují značnou výhodu.

K provedení útoku využívají chyby v programu tak zvané exploity. Ty umožňují pomocí příkazové sekvence, kódu nebo speciálního programu spustit neočekávané, nepovolené chování instalovaného softwaru na počítači nebo serveru uživatele a tím nad nimi získat plnou kontrolu nebo je zneužít pro další činnost např. těžení kryptoměn[26].

---

[24] HODAČOVÁ, Veronika, © 2021. Smishing. In: *Policie.cz* [online]. Policie ČR [cit. 2022-02-23]. Dostupné z: https://www.policie.cz/clanek/preventivni-informace-smishing.aspx

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

[26] Taktéž

Zneužití zero day útoku je možné do doby než výrobce softwaru provede bezpečnostní aktualizaci a tím napraví chybu v programu. Do doby vydání bezpečnostní aktualizace může výrobce softwaru navrhnout kroky k minimalizaci zneužití zranitelnosti.

3.6 Malware

Je všeobecným názvem pro škodlivé programy vytvořené za účelem poškození uživatele, počítače, serveru apod. Podle jejich účelu je můžeme dělit:

- Spyware neboli program, který slouží ke špehování uživatele nebo počítače, serveru. Zjištěná data pak odesílá zpět útočníkovi.
- Adware neboli program, který zejména uživateli zobrazuje nechtěné reklamy nebo jiná sdělení. Tyto programy dokáží například měnit výchozí stránku v prohlížeči.
- Ransomware tedy program, který může zašifrovat data a pro jejich obnovení požaduje po uživateli zaslání peněžních prostředku, nejčastěji kryptoměn.
- Viry neboli zákeřný program, který se dokáže šířit bez vědomí uživatele. Modifikuje softwarové vybavení počítače nebo serveru.
- Červi neboli škodlivý program, který je schopen autonomně vytvářet své kopie a rozesílat je do dalších počítačových systému. Primárně slouží jako nositel dalších zde výše uvedených programů.

Z výše uvedeného je tedy patrné, že tyto škodlivé programy se ve většině případu instalují na počítače nebo servery.

3.7 MITM

V případě tohoto útoku, zachycuje útočník komunikaci uživatele a serveru bez jejich vědomí. Útočník se nachází uprostřed komunikace a řídí ji. Cílem útoku je možnost kontrolovat, číst, zneužít atd. informace v rámci této komunikace[27].

3.8 Závěr kapitoly

Tato kapitola byla věnována nejběžnějším typům kybernetických útoku, se kterými je možné se setkat. U každého útoku byl popsán nejběžnější vektor útoku, tedy jak se útočník

[27] MITM (Man In The Middle), 2016. In: *ManagementMania.com* [online]. Wilmington (DE) 2011-2022 [cit. 2022-04-27]. Dostupné z: https://managementmania.com/cs/mitm-man-in-the-middle

může dostat do počítače, serveru apod. V dnešní době je důležité uvědomit si, že útočníci utočí stále komplexněji. Používají techniky sociálního inženýrství a tím vzbuzují u obětí pocit důvěryhodnosti. Útočí na nejslabší článek v systému a tím je bohužel uživatel.

4 ZPŮSOBY ZAJIŠTĚNÍ KYBERNETICKÉ BEZPEČNOSTI

Zajištění kybernetické bezpečnosti můžeme rozdělit podle toho, kdo kybernetickou bezpečnost poskytuje vlastní síly nebo jiné síly nebo podle toho jakou kybernetickou bezpečnost poskytuje pasivní nebo aktivní.

4.1 Kdo poskytuje kybernetickou bezpečnost

Organizace, které si zajišťují kybernetickou bezpečnost vlastními silami, ji nejčastěji záměrně slučují s dalšími druhy bezpečnosti, nejčastěji s fyzickou a informační potažmo administrativní bezpečností, pokud je nutné chránit utajované informace. Organizace mohou tvořit samostatná oddělení NOC nebo SOC, spravující jeden nebo více informačních nebo komunikačních systému organizace.

Dalším způsobem poskytování kybernetické bezpečnosti je její poskytování jako služby. Nezávislá organizace na základě smlouvy mezi poskytovatelem služby a jejím uživatelem, spravuje informační nebo komunikační systém podle předem stanovených postupů, odpovědností a podpory.

Vyhláška o kybernetické bezpečnosti nestanovuje přesný způsob zajištění kybernetické bezpečnosti pouze její legislativní rámec. Je však důležité mít na paměti, že v případě povinných osob, nejsou tyto osoby zbaveny odpovědnosti a naopak se zvyšují nároky např. na řízení dodavatelů, bezpečnost lidských zdrojů atd.

4.2 Jak zajistit kybernetickou bezpečnost

Kybernetickou bezpečnost lze zajistit pasivně nebo aktivně. Prakticky se využívá obou přístupů, jelikož ani jeden není schopen plně kybernetickou bezpečnost plnit.

Mezi pasivní prvky kybernetické bezpečnosti patří zejména prvky daného informačního systému, které můžeme souhrnně nazývat bezpečnostními technologiemi. Aktivní prvky jsou zde myšleny IT technici, analytici a další bezpečnostní pracovníci IS nebo KS.

4.3 Pasivní prvky kybernetické bezpečnosti

Jak již bylo uvedeno v předchozím odstavci, pasivní prvky tvoří prvky IS nebo KS, které souhrnně nazýváme bezpečnostními technologiemi tak, aby při jejich provozu nemuselo docházet k interakci s člověkem.

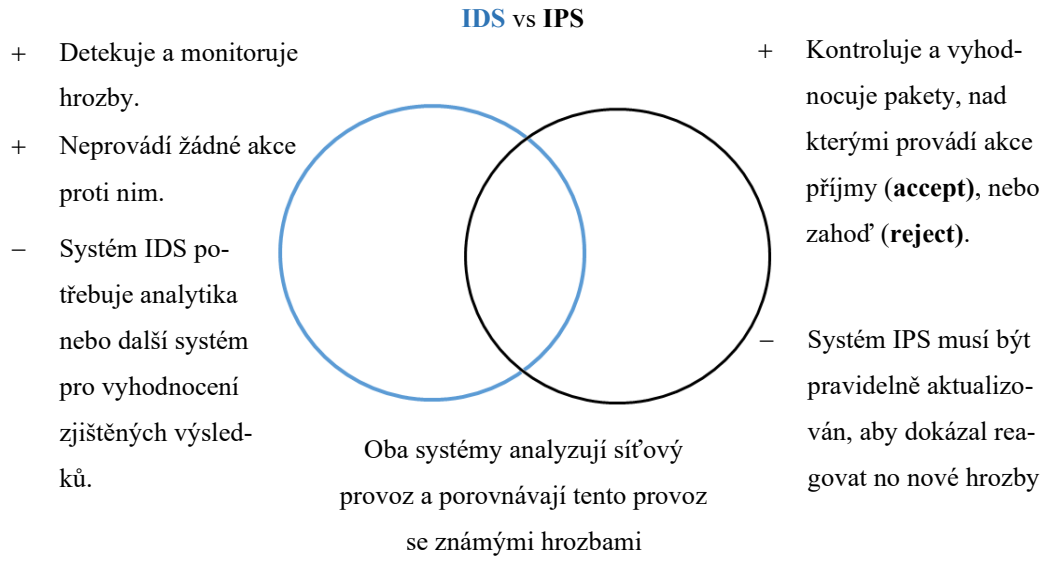
Smysl těchto technologií je tedy bez vnějšího zásahu automaticky vytvářet akce proti bezpečnostním hrozbám na základě předem definovaných pravidel. Příkladem pravidla může být maximální počet přihlášení na firemní e-mailovou schránku, kdy například po třech, špatných přihlášení dojde k automatické akci a to zablokování dané e-mailové schránky.

Většina těchto bezpečnostních pravidel umožňuje práci s dvojicí pravidel. První dvojice pravidel, jsou pravidla vytvářena a aktualizována výrobcem technologie. Druhá dvojice pravidel je pak vytvářena technikem pracujícím s danou bezpečnostní technologií. Obě skupiny pravidel mají své výhody i nevýhody a konečné nastavení je nutné optimalizovat na danou organizaci respektive daný IS nebo KS.

Mezi tyto prvky řadíme IDS/IPS systémy, systémy chránící před únikem data tzv. DLP systémy, firewally další generace tzv. NGFW a další prvky. U NGFW se ve většině případů jedná o klasický firewall, který v sobě integruje více zařízení a více služeb. NGFW jsou třetí generací firewallu po firewallu „paketovém“ a „stavovém“.

4.3.1 IDS/IPS systémy

Tedy systémy na detekci průniku nebo na prevenci průniku. Rozdíl mezi systémem IPS a IDS nejlépe vystihuje níže vyobrazený obrázek 3 a také tvrzení, že systém IDS je pasivní a systém IPS je aktivní. Oba systémy mají své výhody a nevýhody. Nasazení systému IDS nebo IPS tak záleží na konkrétním případu IS. Jeden z faktorů může být například propust-



Obrázek 3 Porovnání IDS vs IPS [zdroj: Vlastní tvorba]

nost systému, kdy v případě IPS může být propustnost sítě limitována.

Oba systémy detekují tzv. stav „false positive“ a „false negative“ události a oba mohou blokovat regulérní provoz stejně, jako mohou propustit do systému skutečnou hrozbu[28].

Oba systémy pro své fungování potřebuji někde tzv. „běžet“. Možností jsou:

- IPS/IDS jako softwarové řešení,
- IPS/IDS jako přídavná karta do HW nebo jako
- IPS/IDS jako samostatný HW (sonda).

4.3.2 DLP Systémy

Systémy DLP (*Data Loss Prevention*) chrání a monitoruji především data organizace před jejich zneužitím. DLP umožnuje např. sledovat jaká data si jednotlivý uživatele nahrávají na USB disky, na jaké data v systému přistupují apod. Dále dokáží monitorovat e-mailovou komunikaci a přenos FTP, HTTP nebo HTTPS.

DLP systémy jsou umístěny na uživatelských stanicích jako tzv. endpointy tak i na síti, buď jako samostatný prvek i když dnes se již nejčastěji slučuji například se systémem IPS nebo IDS. IPS/IDS systém pak detekuje například nadměrný tok dat ze sítě organizace a DLP systém analyzuje, o jaká data se jedná[29].

Systém například může detekovat, že v rámci datového toku je nalezen vzorek, který může obsahovat rodná čísla, která jsou odesílaná z organizace ven. Systém v tomto případě samozřejmě není všemocný a řetězec znaků například RČ může být vytržen z kontextu celkového datového toku a proto musí být zapojen lidský prvek například analytika, který tuto událost příjme, zanalyzuje a potvrdí nebo vyvrátí únik dat.

4.3.3 Firewally další generace

Firewally další generace tedy zařízení, které mimo klasického FW sdružují například i možnosti IPS systému nebo stále častěji SD-WAN.

---

[28] IDS Vs IPS, ©1994 - 2022. In: *Checkpoint.com* [online]. [cit. 2022-05-17]. Dostupné z: https://www.checkpoint.com/cyber-hub/network-security/what-is-an-intrusion-detection-system-ids/ids-vs-ips/#CheckPointsolution

[29] What Is DLP and How Does It Work?, © 2022. In: *Trellix.com* [online]. Musarubra US [cit. 2022-05-17]. Dostupné z: https://www.trellix.com/en-us/security-awareness/data-protection/how-data-loss-prevention-dlp-technology-works.html

Tyto FW pracují s aplikační vrstvou, tak dokáží systém chránit dokonaleji než předchozí generace. Oproti klasickým stavovým FW, které povolují nebo blokují provoz podle předem daných pravidel na základě stavu, portu a protokolu. Mohou tak být levným a zároveň základním zabezpečením sítě.

4.3.4 Vyhodnocovací systémy

Pomyslným pojítkem mezi pasivními a aktivními prvky je systém, který událost ze všech pasivních prvků sbírá a tyto informace v reálném čase poté zobrazuje a prezentuje analytikům. Tyto systémy se nazývají SIEM. Zástupcem je například QRadar od společnosti IBM[30]. Mezi hlavní vlastnosti SIEM systému patří:

- agregace dat,
- korelace,
- přehledové statistiky a informační panely,
- compliance reporty – shody,
- uchovávání dat tzv. logů.

SIEMy dokáží sbírat data nejenom z bezpečnostních prvků sítě, ale také například z uživatelských stanic, serveru nebo například z webových stránek. Jsou tedy doopravdy univerzálním nástrojem pro správu kybernetické bezpečnosti.

4.4 Aktivní prvky kybernetické bezpečnosti

Aktivní prvky proti kybernetickým útokům můžeme definovat jako systematickou činnost analytiků, kteří reagují na události, analyzují hrozby a vytvářejí tak další bezpečnostní úroveň proti kybernetickým hrozbám. Aktivně pracují se získanými daty a vyhodnocují je. Na základě svých zjištěni pak mohou nastavovat bezpečnostní technologie.

4.4.1 Analytik

Analytici ve většině organizaci zastávají definované role, které odpovídají jejich zkušenostem a zaměření. V jednoduchosti je lze rozdělit na analytiky, kteří v provozu na síti vyhod-

[30] IBM Security QRadar SIEM, ©1994- 2021. *Ibm.com* [online]. IBM Corporation [cit. 2021-11-03]. Dostupné z: https://www.ibm.com/products/qradar-siem

nocují a vyhledávají odlišnosti, které pak podrobují analýze a na specialisty, kteří již řeší konkrétní zjištění problém, kterým může být:

- exploit,
- malware,
- zranitelnost,
- počítačová forenzní věda a další.

První skupinu analytiků lze nazvat jako skupinu bezpečnostních analýz. Jejich náplní práce je reagovat na události z dohledového systému, vytvářet nová pravidla a co nejvíce minimalizovat falešné poplachy. Jsou první linií obrany. Na základě jejich prvotního úsudku a z analýzy provozu se rozhodují, zda se jedná o škodlivou činnost nebo o běžný síťový provoz.

Druhá skupinou analytiků jsou specialisti. Ti už se při své analýze zaměřují na obory, které si zvolili. Například analytik řešící malware, hledá ve škodlivém kódu C&C servery, na které pak tento malware komunikuje a nejenom to. Své zjištění pak předá první skupině a ti jsou schopni na základě jeho analýzy nastavit bezpečnostní technologie tak, aby technologie byly schopny detekovat danou komunikaci na síti. Dalším příkladem je analytik, který sleduje zranitelnosti, které v systému vyhledává. Nejde přitom pouze o zranitelnosti nainstalovaného SW, ale také o zranitelnosti v HW např. špatně nastavené porty atd.

4.4.2 NOC

Z anglického termínu *Network Operations Center*, v překladu bychom mohli mluvit o středisku síťových operací. V širším slova smyslu můžeme hovořit o technickém dohledu sledující stav síťové infrastruktury se všemi jejími prvky[31].

Z pohledu kybernetické bezpečnosti je NOC první linií obrany a to z důvodu, že jeho hlavním úkolem je udržovat prvky na prvních třech vrstvách modelu ISO/OSI aktuální a nastavené dle bezpečnostní politiky organizace. Sledují a vyhodnocují stav sítě a reagují na výkyvy – odlišnosti od běžného provozu.

[31] Network Operations Center (NOC), 2018. In: *Cesnet.cz* [online]. Praha: © 1996–2021 CESNET, z. s. p. o. [cit. 2022-04-27]. Dostupné z: https://www.cesnet.cz/sluzby/noc/

4.4.3 SOC

Z anglického termínu *Security Operations Center*, tedy v překladu centrum bezpečnosti. Pokud v případě NOCu hovoříme, že tvoří kybernetickou bezpečnost zejména správným nastavením bezpečnostních technologií respektive prvků síťové infrastruktury, tak v případě SOCu jde o aktivní vyhledávání kybernetických hrozeb, rizik a zranitelností a reakcí na ně.

Analytici SOCu někdy též označovaní jako L3 nebo level 3 support, jsou experti v daných oblastech svého působení. V případě kybernetické bezpečnosti je jejich úkolem především reakce na incident a proaktivní přístup při vyhledávaní slabých míst infrastruktury. Nedílnou součástí jejich práce je také komunikace s externími partnery. Na základě výsledků jejich zjištění, by měl bezpečnostní manažer organizace aktualizovat bezpečnostní politiku organizace.

4.4.4 OSINT

Open source Intelligence[32] neboli zpravodajství z otevřených zdrojů. Získávání informaci v dnešním digitálním světě již není doménou pouze zpravodajských služeb, špionáže atd. Každý uživatel, který kdy něco napsal, vložil nebo se registroval kdekoli na internetu po sobě zanechal nesmazatelnou stopu tzv. digitální stopu. Takto dohledatelné informace získané za pomocí OSINT jsou zcela legální.

OSINTové nástroje jsou dnes volně a zdarma přístupně široké veřejnosti. Ty lepší si jako kdekoli musíte zaplatit. Tyto nástroje nám mohou najít informace o útočníkovi nebo nám poskytnou detaily škodlivého kódu. Dokonce nám mohou dát ucelený obraz útoku a také odpověď na otázku důvodu útoku na naši organizaci. Nástroji OSINTu není pouze Internet, ale také média, různé reporty atd. Jednoduchým příkladem OSINTu může být vyhledávání fotky pomocí prohlížeče GOOGLE. Lze si tak například ověřit skutečný původ fotky, kde a kým byla pořízena.

Vyhledávácí strategii OSINTu jsou odpovědi na otázky kdo, co, proč, kdy a kde?

---

[32] NORDINE, Justine. OSINT Framework. In: *Osintframework.com* [online]. [cit. 2022-05-17]. Dostupné z: https://osintframework.com

4.5 Kybernetická ochrana a obrana

Pojmy ochrana a obrana zní velmi podobně a většinou je cíl obou pojmů společný. Avšak v kybernetické bezpečnosti na úrovni státu a organizací jsou oba pojmy mírně rozdílné. Pokud budeme vycházet z toho, že kybernetickou ochranu České republiky zaštiťuje Národní úřad pro kybernetickou a informační bezpečnost, vyplívajíc z toho je ochrana civilní záležitostí, tak kybernetická obrana České republiky je záležitostí Ministerstva obrany. Obrannou linii tvoří Vojenské zpravodajství, které má legislativní pravomoc provádět aktivní zásah.

V kybernetické bezpečnosti tak ochrana je souborem opatřeni k zajištění bezpečnosti. Většinou ve smyslu minimalizovat riziko plynoucí z hrozeb

Obrana je pak činností Vojenského zpravodajství vedoucí k zajištění kybernetické obrany státu. Z tohoto titulu může provést opatření k odvrácení kybernetických útoků a hrozeb. Aktivní zásah VZ, za splnění zákonných podmínek, bude použit jako krajní řešení národní sebeobrany.[33]

Pro účely diplomové práce bude k oběma pojmům přistupováno jako k rovnocenným.

4.6 Závěr kapitoly

V této kapitole byly uvedeny základní způsoby zajištění kybernetické bezpečnosti a prvky, které se v kybernetické bezpečnosti používají. Je nutné si uvědomit, že podíl kybernetických hrozeb celosvětově stoupá s tím, jak stoupá používání celosvětové sítě Internet. Vzestup je nejvíce patrný i díky celosvětové pandemii COVID-19 a rozšíření práce z domova.

Významným faktorem je, že na poli kybernetické bezpečnosti jsou útočníci stále o krok napřed a proto pro správné zajištění kybernetické bezpečnosti musíme přemýšlet jako útočníci a hledat ve vlastních IS nebo KS slabiny a ty následně opravit a reportovat.

[33] Novela zákona o Vojenském zpravodajství. In: *Vzcr.cz* [online]. Praha [cit. 2022-04-27]. Dostupné z: https://vzcr.cz/novela-zakona-o-vojenskem-zpravodajstvi-151

5 ÚČEL A STRUKTURA ORGANIZACE Z HLEDISKA KYBERNETICKÉ BEZPEČNOSTI

V této kapitole se v krátkosti zaměříme na základní typy organizačních struktur společnosti, jelikož jejich komplexnost hraje při řešení incidentu nemalou roli. Pro každou organizační strukturu budou uvedeny její výhody a nevýhody a krátké shrnutí řešení kybernetického bezpečnostního incidentu.

Určitě zde nebudou zmíněné všechny typy možných organizačních struktur. Důvodem je, že všechny organizační struktury nejsou vzhledem k zaměření práce zcela relevantní a v některých nelze ani princip řešení bezpečnostního incidentu realizovat z povahy jejich struktury např. výrobková organizační struktura apod.

5.1 Účel organizace

Cíl jakékoli organizace z pohledu kybernetické bezpečnosti se neliší od cílů ostatních organizaci. Cílem organizace není jenom zvyšování majetku, hodnoty organizace, byť v některých případech je vydělávání peněz jediným a hlavním záměrem. V 21. století většina organizací prošla nebo prochází změnou a do popředí vstupují nové cíle, jako jsou ekologie, udržitelnost, globálnost, bezpečnost a mnoho dalších.

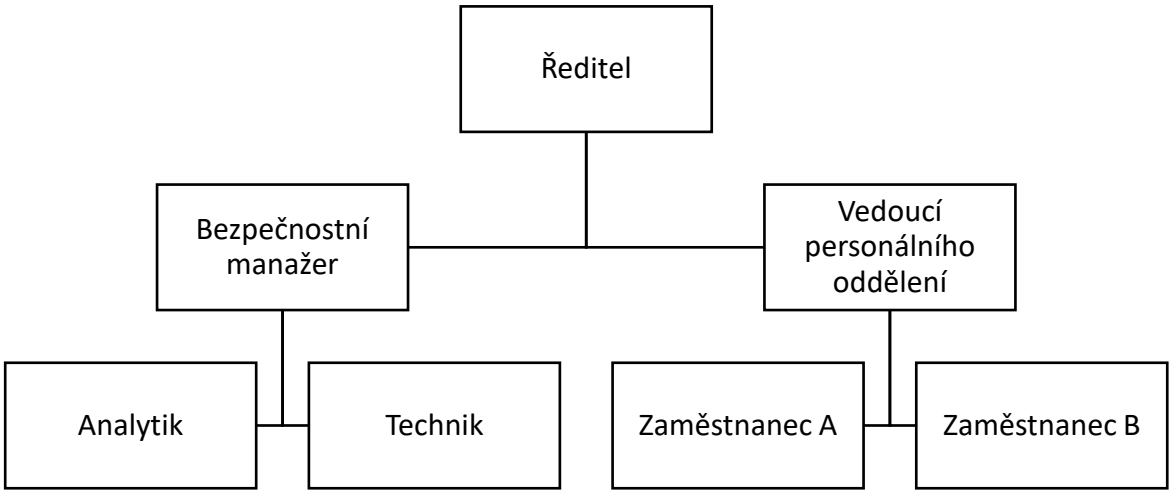
Kybernetická bezpečnost jako cíl organizace zvyšuje svoji popularitu a to nejenom z důvodu, že v dnešním globálním prostředí, lze produkty, služby a další věci nabízet téměř kdekoli, ale také hrozba – útok může přijít odkudkoli.

Účelem organizace z hlediska kybernetické bezpečnosti by tedy mělo být především vytváření takového prostředí organizace, technického vybavení, softwarového vybavení, personálního obsazení, které je schopno úspěšně čelit těmto negativním kybernetickým jevům.

5.2 Struktura organizace

Struktura organizace z pohledu kybernetické bezpečnosti se výrazně neliší od struktury klasické organizace. Jde o hierarchické uspořádání vztahů, které se nejčastěji vytváří na základě rozhodovacích pravomocí mezi jednotlivými organizačními prvky.

Z pohledu kybernetické bezpečnosti jde především o pravomoc zasahovat do informačního nebo komunikačního systému organizace v míře nutné pro jejích bezpečný chod bez zbytečných odkladů.



Obrázek 4 Liniová organizační struktura [Zdroj: Vlastní tvorba]

5.2.1 Liniový typ

Nejstarším typem organizační struktury je liniový typ, který je zároveň vhodný pro organizaci do 50 zaměstnanců. Vztah nadřízený – podřízený je orientován vertikálně. Organizační struktura z pohledu kybernetické bezpečnosti je znázorněna na obrázku 4.

Výhody liniové organizační struktury:

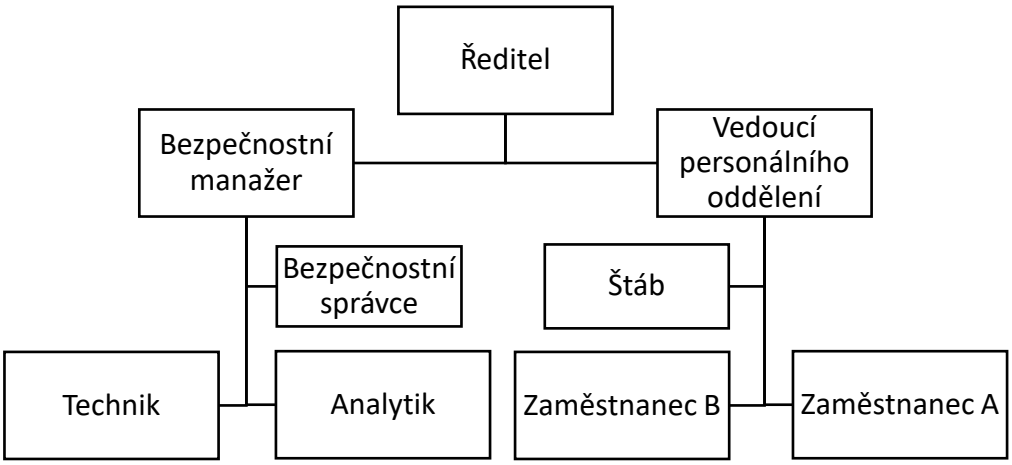
- Jednoznačnost pravomocí.
- Jednoduchost organizačních vztahu.
- Nadřízený pracovník může jednoduše kontrolovat podřízené pracovníky.

Nevýhody liniové organizační struktury:

- Dlouhé cesty mezi jednotlivými řídícími pracovníky.
- Pomalá reakce na změny, těžkopádnost.
- Vysoké nároky na vedoucí pracovníky.

5.2.2 Kybernetická bezpečnost v liniovém typu

Kybernetická bezpečnost v liniovém typu je řešena neefektivně z hlediska času a složitosti tou informací. V případě zjištění porušení kybernetické bezpečnosti u zaměstnance A, analytikem je tok informací následující: analytik, bezpečnostní manažer, ředitel, vedoucí personálního oddělení, zaměstnanec A.



Obrázek 5 Štábní organizační struktura [Zdroj: Vlastní tvorba]

5.2.3 Štábní typ

Štábní typ respektive liniově-štábní organizační struktura je rozšířením liniového typu o štábní útvary. Štábní útvary pak přijímají nebo je na ně částečně delegována rozhodovací pravomoc. Jsou tvořeny odborníky specializující se na různé oblasti řízení a zároveň podporují řídící činnost liniového vedoucí

Výhody štábní organizační struktury:

- Zlepšení kvality rozhodování a řízení.
- Odlehčení rozhodování liniovým vedoucím.

Nevýhody štábní organizační struktury:

- Možné zdvojení pravomocí, konflikty mezi linií a štábem.
- Nárůst organizace o štábní útvary.

5.2.4 Kybernetická bezpečnost ve štábním typu

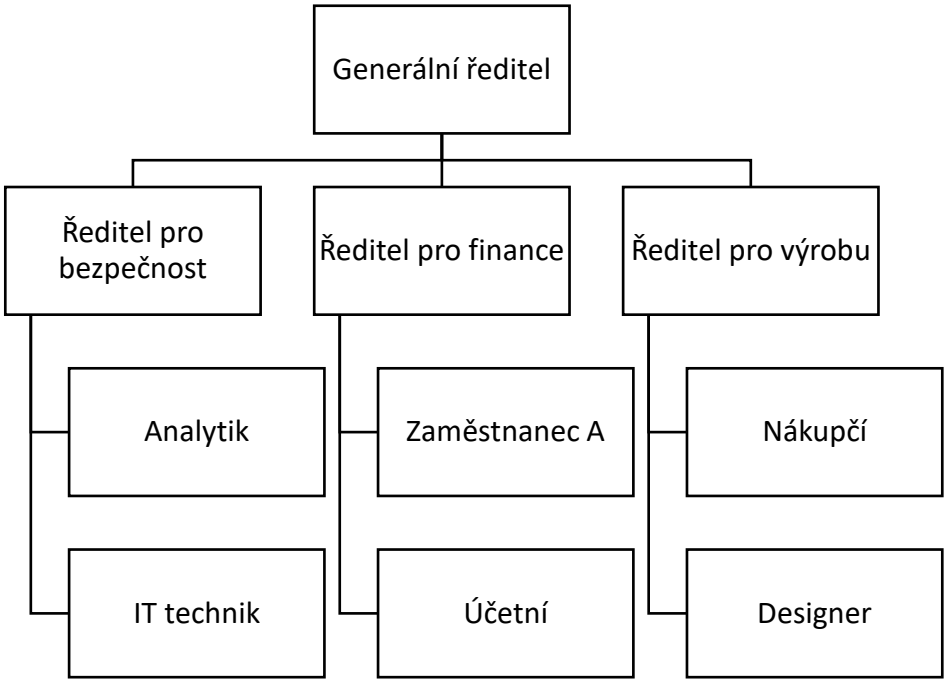
Z pohledu kybernetické bezpečnosti je štábní typ téměř srovnatelný s liniovým typem a v některých případech může dokonce docházet ještě k většímu zpoždění při řešení porušení kybernetické bezpečnosti. Na druhou stranu štábní útvary zde mohou převzít část odpovědnosti za řešení problému. Zatímco liniový vedoucí řeší problém u svého zaměstnance stejně jako v případě liniového typu, může štáb vedoucího personálního oddělení řešit tento problém s ostatními podřízenými zaměstnanci a tím reaktivně nebo proaktivně reagovat na nastalou situaci.

V našem případě tak štáb může například proškolit zaměstnance B, aby neopakoval chybu zaměstnance A.

5.2.5 Funkční typ

Vychází z definice, že každá organizace vytváří hodnoty, které předává zákazníkům, a proto je vhodné soustředit zaměstnance, kteří plní nebo pracují na podobných úkolech do skupin, viz obrázek 6. Tento typ organizační struktury je vhodný pro středě velké podniky.

Z pohledu kybernetické bezpečnosti se jedná o velmi dobrou organizační struktura a to z důvodu, že ředitel pro bezpečnost je primárně odpovědný za zajištění kybernetické bez-



Obrázek 6 Funkční organizační struktura [Zdroj: Vlastní tvorba]

pečnosti v celé organizaci.

Výhody funkční organizační struktury:

- Efektivní využití zdrojů.
- Centralizovaná struktura a strategické rozhodování shora.
- Respektuje princip pracovní specializace.

Nevýhody funkční organizační struktury:

- Pomalé rozhodování a nejasná otázka odpovědnosti.
- Přílišné zaměření a úzká specializace klíčových zaměstnanců.

- Pomalá adaptace na změny.

5.2.6 Kybernetická bezpečnost ve funkčním typu

Kybernetická bezpečnost ve funkčním typu organizace je vzhledem předchozím dvou typů asi nejlepší řešení. V této struktuře se nachází specializované oddělení, které v ideálním případě řídí a rozhoduje o všech otázkách, které se vztahují ke kybernetické bezpečnosti. V tomto případe je v pravomoci ředitele pro bezpečnost přijmout nezbytná opatření u zaměstnance A, aby byla zabezpečena bezpečnost organizace.

5.3 Závěr kapitoly

Cílem této kapitoly nebylo, jak již bylo napsáno v úvodu, porovnat všechny organizační struktury, ale upozornit na některé úskalí jednotlivých typů. Ve většině případů je největším úskalím v kybernetické bezpečnosti čas a rychlost. Ve většině organizací bude kybernetická bezpečnost řešena samostatným oddělením nebo jednotlivými zaměstnanci. Důvodem je, že kybernetická bezpečnost je příliš specifická proto, aby mohla být spojena s jinou činností zaměstnance.

DÍLČÍ ZÁVĚR TEORETICKÉ ČÁSTI

V teoretické části byly nastíněny podstatné faktory, které jsou při řešení kybernetických bezpečnostních incidentů nutné vzít v potaz. Ať už se jedná o legislativu, která udává právní rámec problematiky a v některých případech dokonce přikazuje, co musí být splněno a uděláno, tak po analýzu kybernetických rizik, kdy si musíme říci co je pro náš IS, KS nebo organizace důležité, co považujeme za aktiva a jak by na ně mohli útočníci zaútočit.

Do řešení incidentů vstupuje, ale také samotná struktura organizace, vedení a řízení lidí. To jak má nebo bude daná organizace tvořit skupinu odborníku, která se bude zabývat kybernetikou. Zda bude interní nebo externí a jaké pravomoci budou mít.

Poslední nedílné součásti při řešení incidentů jsou samotné útoky, jejich typy a možná intenzita. Pro zdárný proces řešení je nejprve nutné tyto útoky nebo pokusy identifikovat. Jak už bylo v teoretické části zmíněno, existuje mnoho bezpečnostních technologií, ale ty nefungují sami o sobě. Ke své činnosti potřebují odborníky, kteří dokáží vypozorovat a odhalit zdánlivé odchylky „běžného“ datového provozu.

II. PRAKTICKÁ ČÁST

6 MODELOVÁ ORGANIZACE

V diplomové práci vystupuje reálna organizace, která si přeje zůstat v anonymitě. Organizace spadá pod působnost zákona o kybernetické bezpečnosti se všemi povinnostmi vyplívající z tohoto zákona. Pro potřeby této práce bude společnost fiktivně nazvaná jako SEaP a.s. Organizace provozuje více informačních systému, které na sobě nejsou závislé a pro účely diplomové práce zde budou uvedeny dva IS.

6.1 Účel a struktura organizace

Účelem akciové společnosti Státní elektřina a plyn je výroba, distribuce a skladování komoditních surovin zejména elektřiny a plynu.

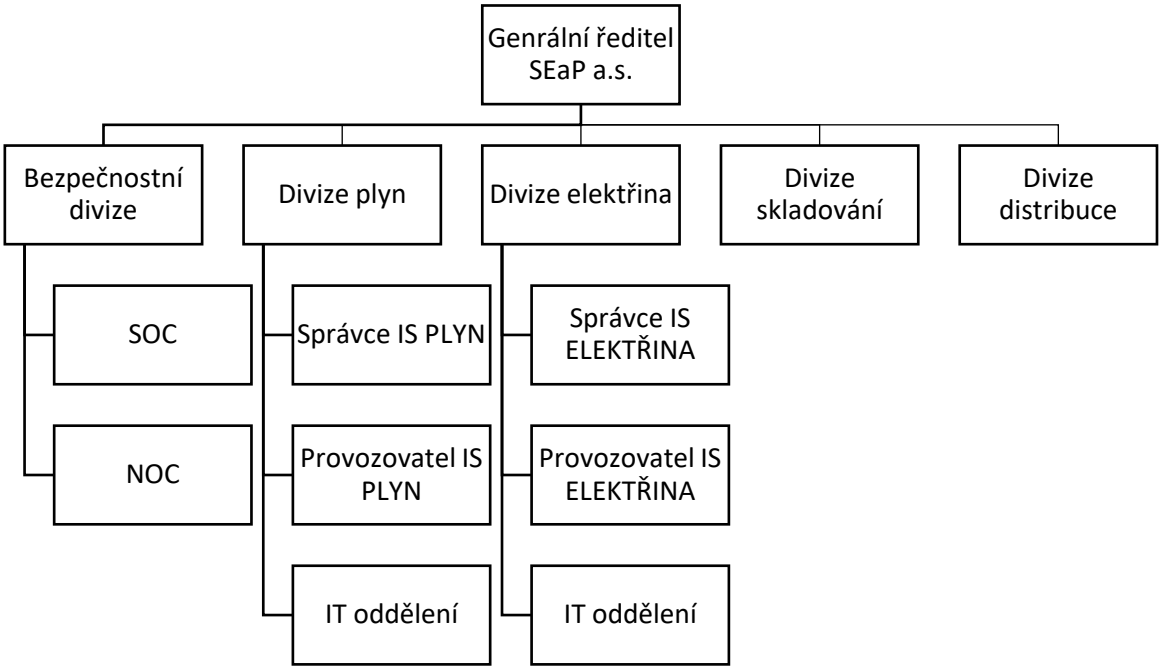
Mezi hlavní priority společností patří, poskytnou svým zákazníkům bezpečnou přepravu, distribuci výše uvedených komodit, zajištění bezpečnosti aktiv IS a dodržovat všechna opatření jako bezpečnost práce a zdraví na pracovišti, požární bezpečnost. Cílem výše uvedených činností je splňovat požadavky dané zákonem.

6.2 Struktura organizace

Z pohledu diplomové práce bude struktura organizace zjednodušena na nezbytné prvky tak, aby byla zabezpečena funkční struktura pro řešení kybernetických bezpečnostních událostí. Vypuštěny jsou tak z organizační struktury organizace prvky jako finanční oddělení, personální oddělení, logistika a tak dále.

Důležitým prvkem organizace je její bezpečnostní divize, přesněji její SOC, který je uveden na obrázku 7. SOC je samostatnou součástí celé organizace a nemá tak přímou kontrolu nad řízením jednotlivých informačních systémů. Její úkolem je poskytovat kybernetickou bezpečnost jako službu své vlastní organizaci. Z pohledu ZoKB, tak pro SOC neplyne žádná povinnost.

Jednotlivé IS tedy IS PLYN a IS ELEKTŘINA, mají své provozovatele s vlastní bezpečnostní politikou, která je různá pro oba. Cílem obou je udržovat IS a technické vybavení na úrovni tak, aby byla splněna minimální hladina bezpečnosti. Oba IS spadají pod ZoKB.



Obrázek 7 Zjednodušené schéma organizace [Zdroj: Vlastní tvorba]

6.3 Bezpečnostní politika organizace

Vedení společnosti SEaP a.s. vyhlašuje zásady bezpečnosti organizace. Bezpečnostní politika je závazná pro celou organizaci, její zaměstnance a pro všechny spolupracující subjekty. Cílem je vytvářet bezpečné pracovní prostředí nad rámec požadavků zákona.

Hlavním cílem bezpečnostní divize SEaP a.s. je chránit informace a infrastrukturu před kybernetickými útoky a zajišťovat její chod. Kontinuálně se podílí na analýze zejména kybernetických rizik a přijímá potřebná opatření k minimalizaci rizik. Divize je odpovědná zá nákup HW a SW od prověřených dodavatelů a jejich řízení podle VoKB. Nedílnou součásti je také řešení kybernetických bezpečnostních incidentů ve společnosti.

6.4 Informační systém organizace

Společnost SEaP a.s. provozuje dva na sobě nezávislé IS. Oba IS (IS PLYN a IS ELEKTŘINA) jsou systémy kritické informační infrastruktury dle zákona[34]. Společnost SEaP a.s. své IS provozuje ve vlastních datových centrech v lokalitách Praha a Brno. Pro-

[34] ČESKO. Zákon č. 240/2000 Sb. krizový zákon. § 2 písm. g) zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon). In: *Zákony pro lidi.cz* [online]. © AION CS 2010-2022 [cit. 5. 1. 2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-240#p2-1-g

pojení IS mezi datovými centry je zabezpečeno prostřednictvím veřejné sítě Internet a záložní dedikovanou linkou. Tyto spojení jsou tunelována a šifrována.

6.4.1 Informační systém PLYN

Informační systém PLYN monitoruje a zabezpečuje kontrolu plynu v plynovodech a v zásobnících plynu společnosti. Další funkcí je dálkový odečet množství odebraného plynu z odběratelských míst zákazníků.

Funkčnost systému z pohledu udržení systému v chodu zabezpečuje IT oddělení divize plyn. Hlavní náplní je udržovat systém v provozu 24/7 a optimalizovat síťové a jiné prvky infrastruktury IS PLYN.

Jako aktiva IS PLYN byly identifikovány:

- Hardwarova aktiva (servery, síťové prvky, počítače).
- Datová aktiva (databáze, dokumentace, smlouvy).
- Softwarova aktiva (aplikační software, řídící software)

6.4.2 Informační systém ELEKTŘINA

Informační systém ELEKTŘINA monitoruje a řídí stav napětí v přenosové soustavě na území České republiky. Systém umožňuje spuštění systémů, které reagují na výkyvy v přenosové soustavě.

Funkčnost systému z pohledu udržení systému v chodu zabezpečuje IT oddělení divize elektřina. Hlavní náplní je udržovat systém v provozu 24/7 a optimalizovat síťové a jiné prvky infrastruktury IS ELEKTŘINA.

Jako aktiva IS ELEKTŘINA byly identifikovány:

- Hardwarova aktiva (servery, síťové prvky, počítače).
- Datová aktiva (databáze, dokumentace, smlouvy).
- Softwarova aktiva (aplikační software, řídící software)

6.5 Kybernetické hrozby společnosti SEaP

Na základě aktuální geopolitické situace, válečný konflikt na Ukrajině, společnost přepracovala svůj katalog hrozeb, aby více odpovídal aktuální trendům. Rozsáhlé útoky útočníků byly nahrazeny útoky, které jsou komplexnější a sofistikovanější. Zároveň se útoky svým

rozsahem přesouvají s národního do globálního měřítka. Cílem těchto útoku je napadaný IS vyřadit z provozu natrvalo nebo způsobit velmi rozsáhlé škody.

6.5.1 Identifikace hrozeb

Aktiva informačního systému se vyskytují v prostředí, kde se vyskytuje nespočet druhů hrozeb. Tyto hrozby mohou být úmyslné nebo neúmyslné, vnitřní nebo vnější apod. Identifikace pak musí být relevantní k danému aktivu.

Ve společnosti SEaP a.s. byla provedena identifikace hrozeb řízeným a dokumentovaným procesem na základě, kterého vznikl katalog hrozeb.

6.5.2 Katalog kybernetických hrozeb

V katalogu kybernetických hrozeb společnosti SEaP a.s., který pracuje s úrovní hrozeb, budou uvedeny pouze hrozby, které mohou poškodit aktiva společnosti skrze kybernetický prostor. Uvedené hrozby jsou totožné pro oba informační systémy. Tabulka je vypracována zjednodušené pro účely této diplomové práce.

V tabulce 4 jsou uvedeny tyto parametry:

- Zdroj hrozby – původce úmyslné změny stavu, jehož cílem je poškodit IS.
- Hrozba – úmyslná změna stavu, která je vyvolána zdrojem hrozby.
- Úroveň – pravděpodobnost s jakou se hrozba vyskytne.
- Ohrožená aktiva – aktiva, která mohou být hrozbou poškozena nebo zničena.

Zdroje hrozeb lze dělit podle typů útočníka například na:

- APT,
- státem podporované skupiny,
- hackeři,
- kyberkriminálnící a další.

Pro účely této práce nebudou výše uvedené zdroje hrozeb rozděleny a to z důvodu, že zde neřeším právní problematiku, kdy důležitým faktorem je, kdo je útočníkem. Neřeším ani způsob jak řešit kybernetický bezpečnostní incident na národní úrovni, kdy důležitým faktorem je odkud zdroj hrozby útočí, zda z vnitřního bezpečnostního prostředí státu nebo z vnějšího.

Tabulka 4 Katalog hrozeb [Zdroj: Vlastní tvorba]

Zdroj hrozby	Hrozba	Úroveň	Ohrožená aktiva
APT Státem sponzorované skupiny Hackeři Kyberkriminálníci	Zničení dat	Vysoká	Hardwarová aktiva Datová aktiva Softwarová aktiva
	Krádež dat	Vysoká	
	Phishing	Kritická	
	Malware	Vysoká	
	Útok na webové stránky/aplikace	Vysoká	
	DoS, DDoS	Vysoká	
	Únik informací	Střední	
	Spam	Kritická	
	Ransomware	Střední	
	Špionáž	Střední	
	Fyzické škody	Vysoká	
	Bezpečnostní díry	Vysoká	

6.6 Kybernetická rizika

V této kapitole budeme na základě katalogu hrozeb stanovovat úroveň rizika pro jednotlivé hrozby. Analýza kybernetických rizik se významně neliší od klasické analýzy rizik. Stanovíme si hodnoty, subjektivně nebo objektivně, pro jednotlivé parametry a provedeme jejich zhodnocení[35].

6.6.1 Analýza rizik

Hodnota parametru pro hrozbu v tabulce odpovídá těmto parametrům:

- Nízká – hrozba téměř neexistuje, výskyt jednou za 5 let.
- Střední – hrozba je málo pravděpodobná, výskyt je od 1 roku do 5 let.

[35] LUKÁŠ, Luděk, 2015. *Bezpečnostní technologie, systémy a management V*. Zlín: Radim Bačuvčík - VeRBuM. ISBN 978-80-87500-67-5.

- Vysoká – hrozba je pravděpodobná, výskyt od 1 měsíce do 1 roku.
- Kritická – hrozba je velmi pravděpodobná, výskyt je častěji než jednou za měsíc[36].

Hodnota parametru pro dopad v tabulce odpovídá těmto parametrům:

- Nízký – téměř bez dopadu na IS.
- Střední – méně významný dopad na IS.
- Vysoký – významný dopad na IS.
- Kritický – velmi významný dopad na IS[37].

Hodnota parametru pro zranitelnost v tabulce odpovídá těmto parametrům:

- Nízká – zneužití je téměř neexistuje,
- Střední – zneužití je málo pravděpodobné,
- Vysoká – zneužití je pravděpodobné,
- Kritická – zneužitá je velmi pravděpodobné, nelze realizovat bezpečnostní opatření[38].

Úrovně jednotlivých parametrů jsou pak vyjádřeny procentuálně v

Tabulka 5 Úroveň parametrů [Zdroj: Vlastní tvorba]

Úroveň	**Procentuální hodnota**
Nízká	0 % - 25 %
Střední	26 % - 50 %
Vysoká	51% - 75 %
Kritická	76 % - 100 %

V tabulce 6 jsou uvedeny tyto parametry:

- Aktivum – nezbytný HW, SW a další prvek nutný pro funkci IS.

[36] ČESKO. Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) - znění od 28. 5. 2018. In: *Zákony pro lidi.cz* [online]. © AION CS 2010-2022 [cit. 27. 4. 2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/2018-82#f6228374
[37] Taktéž
[38] Taktéž

- Hrozba – z katalogu hrozeb.
- Zranitelnost – představuje parametr odolnosti proti hrozbě, tedy jak lehce může hrozba systém ohrozit.
- Dopad – představuje parametr, který udává, jaký dopad může mýt hrozba na systém v případě zneužití zranitelnosti.

Tabulka 6 Analýza rizik [Zdroj: Vlastní tvorba]

Aktivum	**Hrozba** [%]	**Zranitelnost** [%]	**Dopad** [%]	**Riziko** [%]
Nezbytný HW, SW a další prv-ky nutné pro funkci IS	Zničení dat 65	Vysoká 65	Kritická 100	Kritické 76,7
	Krádež dat 50	Vysoká 60	Kritický 80	Vysoké 63,4
	Phishing 90	Střední 50	Vysoký 55	Vysoké 65
	Malware 90	Střední 70	Vysoký 75	Kritické 78,4
	Útok na webové stránky/aplikace 80	Nízká 5	Střední 30	Střední 38,4
	DoS, DDoS 75	Nízká 5	Nízký 5	Střední 28,4
	Únik informací 26	Střední 26	Vysoký 51	Střední 34,4
	Spam 90	Nízká 10	Nízký 10	Střední 36,7
	Ransomware 30	Střední 45	Vysoký 75	Střední 50

	Špionáž 5	Nízká 5	Vysoký 55	Nízké 21,7
	Bezpečnostní díry 68	Vysoká 55	Vysoký 70	Vysoké 64,4

6.7 Kybernetická bezpečnost v modelové organizaci

V modelové společnosti je zabezpečována kybernetická bezpečnost vlastním oddělením ve struktuře organizace. Bezpečnostní divizi tvoří Network Operations Centre a Security Operations Centre které poskytuje vlastní organizaci tyto základní služby:

- Detekci – kontinuálním monitoringem v reálném čase zjišťuje výskyt škodlivých kódů, zranitelností nebo potencionálně škodlivé chování v systému.
- Analýzu – zabezpečuje rozlišení na kybernetickou bezpečnostní událost nebo kybernetický bezpečnostní incident. Dále zkoumá celý kybernetický bezpečnostní incident zejména vektor útoku nebo kompromitace a snaží se určit dopad na IS.
- Reakci – zabezpečuje okamžitou reakci na kybernetický bezpečnostní incident a tím se snaží minimalizovat negativní dopad.

Mezi další služby SOCu patří:

- Zranitelnosti – aktivní skenování vlastní sítě a vyhledávaní zranitelností HW a SW prvků.

Bezpečnostní oddělení respektive SOC není správcem ani provozovatelem žádného IS společnosti. Informace o kybernetických bezpečnostních hrozbách získává nejenom vlastním monitoringem, ale také z veřejně dostupných zdrojů.

Oddělení NOC spravuje svěřené hardwarové prvky a nastavuje bezpečnostní politiku na těchto prvcích na základě doporučené oddělení SOC. Zaměstnanci NOC sledují a vyhodnocují stav sítě a nestandartní chování postupují na SOC.

6.8 Technická opatření kybernetické bezpečnosti

Technická opatření kybernetické bezpečnosti vycházejí na základě analýzy rizik. Společnost jednotlivá rizika přijmula a přijala opatření k minimalizaci těchto rizik. Rizika v tabulce 6 již nelze bez vynaložení enormních finančních a technických prostředku minimalizovat nebo by tyto prostředky finančně převýšila hodnotu rizika vyjádřenou v penězích.

Níže jsou uvedeny jednotlivá opatření k hrozbám na základě analýzy rizik.

6.8.1 Fyzická bezpečnost

Ve společnosti SEaP a.s. jsou jednotlivá pracoviště vedená jako režimová pracoviště s elektronickou kontrolou vstupu. Datová centra společnosti mají vybudovanou aktivní perimetrickou ochranu napojenou na PCO.

Fyzická bezpečnost představuje ochranu před hrozbou *únik informací, špionáž.*

6.8.2 Ochrana před škodlivým kódem

Ochrana před škodlivým kódem je řešena ve společnosti v několika stupních. Prvním stupen je šifrování počítačů zaměstnanců nástrojem *BitLocker* a pravidelná aktualizace HW a SW. Aktualizaci HW a SW mají na starost jednotlivé divize IS. SOC může jednotlivým provozovatelům nebo správcům IS poskytnout informace o aktuálnosti respektive neaktuálnosti HW a SW.

Druhým stupněm je pravidelné zálohování serveru společnosti. Z části jsou zálohovaný i počítače zaměstnanců, kde se zálohuje specifická složka na těchto počítačích na dedikovaný server. Počítače zaměstnanců jsou zálohovány, pouze pokud jsou připojeny v interní síti společnosti.

Třetím stupněm je NGFW, který detekuje podezřelou činnost, kterou SOC vyhodnocuje a analyzuje v rámci svých služeb.

Ochrana před škodlivým kódem představuje hrozby *malware, ransomware.*

6.8.3 Ochrana před odepřením služby

Ochrana před odepřením služby poskytuje prvek Anti-DDoS, který se učí chování sítě a dokáže tak reagovat na nestandartní chování. Tento prvek chrání před útoky typu *UDP floods, ICMP floods, SYN floods, Ping of Death* a další podobné.

Ochrana před odepřením služby představuje hrozby *DoS, DDoS.*

6.8.4 Zálohování

Společnost zálohuje servery v pravidelných intervalech mimo hlavní pracovní dobu. Pro zálohování je použita metoda „*Grandfatjer-Father-Son*“. Metoda spočívá ve vytvoření třech media setu denní –„*Son*“, týdenní – „*Father*“ a měsíční –„*Grandfather*. Jako zálohovací média jsou použita LTO pásky, které se ukládají mimo data centrum.

Denní set je tvořen 4 páskami pro zálohu probíhající v pondělí až čtvrtek, kde každá z pásek je přepsána jednou týdně a probíhá na ně inkrementální záloha.

Týdenní set je tvořen 5 páskami pro zálohu probíhající v pátek, kde každá z pásek je přepsána jednou za 4 až 5 týdnů v závislosti na počtu celých týdnu v měsíci. Na tyto pásky se provádí plná záloha.

Měsíční set je tvořen 12 páskami pro zálohu probíhající poslední pátek v daném měsíci, kde každá z pásek je přepsána jednou za rok. Na tyto pásky se provádí plná záloha.

Z důvodu, že obnova z pásek je časově náročná nejenom z hlediska přenosu a obnovy dat, ale také z hlediska fyzického doručení pásek do data centra. Proto je u virtuálních serverů použita záloha ve formě obrazu virtuálního serveru, která je uložena na diskovém poli přímo v data centru. Tato záloha je v režimu pouze pro čtení (*read-only*).

Zálohování představuje ochranu proti hrozbám z*ničení da, malware, ransomware.*

6.8.5 Ochrana před nevyžádanou poštou

Oba informační systémy společnosti mají vlastní poštovní servery pro komunikaci se zákazníky, dodavateli a uvnitř společnosti. Příchozí pošta je filtrována pomocí antispamového řešení, dedikovaného serveru vyhodnocující příchozí poštu. Antispam vyhodnocuje příchozí poštu automaticky na základě nastavených filtrů a algoritmů nebo lze blokovat ručním zadáním konkrétního odesílatele, předmět a další položky nacházející se v elektronické poště.

Princip automatického vyhodnocování pracuje s online databází odesílatelů, blacklistů atd. Pokud je otisk, který nese informaci o obsahu elektronické pošty, nalezen v některé z databází nebo blacklistu je označen jako SPAM a podle nastavení doručen příjemci nebo je

uložen rovnou do karantény na serveru[39]. I v případě tohoto nastavení, ale dochází k propuštění jednotek nevyžádané pošty příjemci.

Ochrana před nevyžádanou poštou představuje ochranu proti hrozbám *SPAM, Phishing*.

6.8.6 Ochrana před útokem SQL Injection

Společnost při návrhu respektive programování aplikací, kde může hrozit nebezpečí útoku SQL Injection přijala tyto bezpečnostní opatření při jejich návrhu:

- Použití tzv. prepared statements a validace vstupů.
- Použití objektového programování.
- Ošetření přístupových práv.
- Escapovaní nebezpečných znaků.

Nad tyto „programátorské“ ochrany společnost využívá i bezpečnostních technologií v podobě sond, které jsou umístěny v infrastruktuře společnosti. Sondy jsou schopné detekovat pokus o útok SQL Injection a reakci aplikace na tento útok. V případě nestandartní odpovědí aplikace je notifikováno bezpečnostní oddělení.

Ochrana před SQL Injection představuje ochranu proti hrozbám *únik informací, krádež dat, zničení dat a útok na webové stránky/aplikace*.

6.8.7 Ochrana před útokem XSS

Společnost, obdobně jako v případě ochrany před útokem SQL Injection, při návrhu a realizaci webových stránek implementuje bezpečnostní mechanizmy, aby stránky byly proti těmto útokům odolné. Jedná se zejména o:

- Validaci vstupů.
- Pravidelná aktualizace komponent webových stránek nebo redakčního systému
- Escapovaní nebezpečných znaků.

Stejně jako v ochraně před útokem SQL Injection jsou zde sondy nastaveny na detekci pokusu o útok a následné odpovědi webové stránky na tento pokus.

---

[39]Using Anti-Spam and Mail, 2022. In: *Sc1.checkpoint.com* [online]. © 2020 Check Point Software Technologies [cit. 2022-04-27]. Dostupné z: https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_ThreatPrevention_AdminGuide/Topics-TPG/Using_Anti_Spam_and_Mail.*htm*

Ochrana před útokem XSS představuje ochranu proti hrozbám *únik informací, krádež dat, zničení dat a útok na webové stránky/aplikace*.

6.8.8 Phishing

Společnost si je vědoma jak lehce lze zneužít důvěru zaměstnanců a proto proti phishingovému útoku nasadila tyto technická řešení:

- Dvou faktorová autentizace.
- Zákaz spouštění maker v programech.
- Antispamový filtr.
- Antivirové řešení na koncových stanicích.

Ochrana před phishingem představuje ochranu proti hrozbám *phishing, spam, malware, únik a krádež dat*.

6.8.9 ZERODAY

V kapitole 3.5 byla tato zranitelnost vysvětlena, a tedy z její povahy nelze IS nebo KS do vydání aktualizace nebo opravy účinně chránit. Výrobce však může vysvětlit jak je zranitelnost využívaná nebo jak pokus o zneužití detekovat. Těchto informací bezpečnostní oddělení používá pro nastavení bezpečnostních technologií k její detekci. Dále lze aktiva, která trpí touto zranitelností odpojit od sítě do doby vydání bezpečnostní záplaty, pokud je to u nich možné.

Ochrana před ZERODAY představuje ochranu proti hrozbám *bezpečnostní díry*.

6.8.10 Kryptografické prostředky

Kryptografické prostředky nejsou ve společnosti použity.

6.9 Bezpečnostní divize v modelové organizaci

Bezpečnostní divize řeší kybernetické bezpečnostní incidenty na základě stanov bezpečnostní politiky společnosti. Je tvořena klasickým 3 stupňovým dělením:

- Level 1 – tvořen zaměstnanci NOCu.
- Level 2 – tvořen zaměstnanci SOCu.
- Level 3 – tvořen zaměstnanci SOCu.

Level 1 tedy NOC je odpovědný za nastavování prvků v infrastruktuře společnosti na základě její bezpečností politiky. Sledují a vyhodnocují události nebo logy ze sond a dohledových systémů. Všechny zjištění nestandartního chování informačních systémů společnosti, které se souhrnně označují jako události, postupují na Level 2.

Level 2 je složen ze specialistů se všeobecným zaměřením, kteří provádí základní analýzu zjištěných událostí. Navrhují prvotní bezpečnostní opatření a v případě podezření na KBI, eskalují událost na Level 3.

Level 3 je složen z expertů - specialistů v daných oblastech, například specialista na malware, specialista na zranitelnosti apod. Provádí detailní analýzu události a v rámci svého šetření se soustředí na nalezení vektoru útoku a reaktivní opatření. Závěrečná zpráva týmu L3 by měla obsahovat informace o tom, jak útok proběhnul a jak nastavit bezpečnostní technologie pro prevenci podobných útoků.

Celý proces řešení kybernetického bezpečnostnímu incidentu popisuje proces tzv. *Incident Handling Process*.

6.10 Řešení kybernetických bezpečnostních incidentu

Ve společnosti je řešení kybernetických bezpečnostních incidentů, jak bylo zmíněno výše, řešeno plánem tzv. *Incident Handling Proces*, který můžeme přeneseně nazvat řízení reakce na incident. Zahrnuje v sobě několik činností jako například plán zvládání incidentu, vyčlenění lidských zdrojů, komunikace s partnery apod.[40]

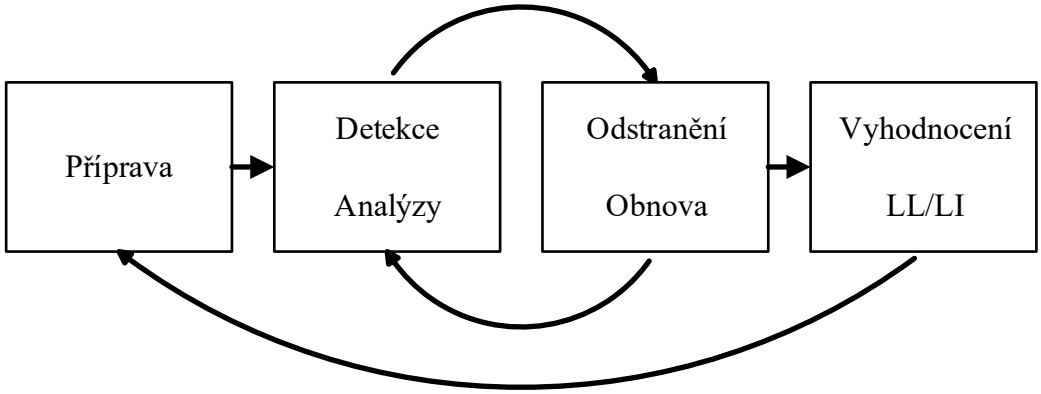
Tento proces se příliš neliší od přístupu, který je definován ve frameworku ITIL®. U obou přístupů je hlavním cílem obnovení služeb. Na rozdíl však od klasického *Incident Managementu* neboli česky řízení incidentu, jde pří řešení kybernetického bezpečnostního incidentu o nalezení vektoru útoku tedy, kudy se útočník dostal do IS společnosti a jak tomu příště zabránit. Současně s tím musí proběhnout analýza možného úniku informací.

6.10.1 Plán zvládání incidentu

Společnost SEaP a.s. má připraven základní plán zvládání kybernetického incidentu. Plán se sestává z několika dílčích částí, jak je vidět na obrázku 8.

[40] MCCARTHY, N. K., 2012. *The computer incident response planning handbook: executable plans for protecting information at risk.* New York: McGraw-Hill. ISBN 978-0-07-179039-0.

První části je příprava a společnost na základě analýzy rizik implementovala do infrastruktury sondy IDS, které vyhodnocují informační tok a vytvářejí události, které zpracovává



Obrázek 8 Životní cyklus incidentu [Zdroj: NIST.gov]

L1. Součástí přípravy je tak udržování systémů, aplikace a prvků infrastruktury na jejich aktuálních verzích a podle zásad bezpečnostní politiky.

Druhou částí je detekce a analýza. Detekce událostí, které mohou potencionálně znamenat kybernetický bezpečnostní incident, přichází ze sond IDS nebo z dohledového systému SIEM v podobě logů nebo informací, které zpracuje a vyhodnotí L1 nebo L3. Následnou analýzu již provádí L2, který na základě svých schopností rozhodne o podezření na KBI nebo všechny zjištěné informace eskaluje na L3. Mezi hlavní výsledky v případě KBI této části plánu patří:

- Zjištění vektoru útoku.
- Analýza incidentu a jeho dokumentace.
- Priorita řešení incidentu
- Informování o incidentu.

Třetí část odstranění a obnova. V této časti L2 a L3 spolupracují a snaží se zabránit dalšímu šíření incidentu a předkládají návrhy bezpečnostních opatření. Mezi hlavní výsledky v případě KBI této části plánu patří:

- Identifikace útočníka.
- Odstranění napadení a obnova služeb, systému apod.
- Dokumentace všech zjištěných informaci, kterými mohou být IP, MAC adresy, délka trvání útoku apod.

Poslední částí je vyhodnocení incidentu. Mezi hlavní výsledky v případě KBI této části plánu patří:

- Leassons Learned.
- Využití zjištěných dat a informací z incidentu.

6.11 Závěr kapitoly

V této kapitole byla popsaná modelová organizace, její organizační struktura, infrastruktura a základní popis kybernetického zabezpečení. Veškeré informace této kapitoly mají základ v reálné organizaci, která jak již bylo řečeno, je zde prezentována společnost SEaP a.s. Je důležité si uvědomit, že ochrana proti hrozbám, kybernetickým útokům je kontinuální činnost a proto se i metody obrany mohou v čase měnit.

7 MODELY ŘEŠENÍ KYBERNETICKÉHO BEZPEČNOSTNÍHO INICDENTU

V této kapitole budou navrhnuty tři modely pro řešení kybernetického bezpečnostního incidentu. Pro návrh těchto modelů budou stanoveny objektivní i subjektivní kritéria rozhodovacího procesu, které vycházejí jednak z požadavků zákona, tak z požadavků naší modelové organizace.

7.1 Stanovení kritérií

V tomto odstavci budou stanovena kritéria, která jsou těmi nejdůležitějšími v modelové organizaci. Je důležité zmínit, že aktuálně není v modelové společnosti stanoveno, které kritérium je více či méně důležité. Zvládání incidentu je tak ad hoc řešeno podle povahy kybernetického bezpečnostního incidentu. Jednotlivé ohodnocení kritérií bylo stanoveno subjektivně s přihlédnutím k objektivním skutečnostem, které incident provází.

7.1.1 Kritérium – rychlost

Rychlost (RYC) je kritérium stanovené objektivně ze zákona a udává, jak rychle se musí incident začít řešit. Kritérium nestanovuje dobu, za jak dlouho musí být incident vyřešen, ale jak rychlá musí být reakce nutná k zahájení řešení incidentu. Příkladem uveďme například současný výpadek webových stránek a výpadek řadiče domény. Jelikož řadič domény je odpovědný za autentizaci, způsobí jeho výpadek větší problém společnosti než výpadek webových stránek. V tomto případě je nutné co nejvíce zdrojů soustředit na obnovu řadiče za co nejkratší dobu. Kritérium je udávané v minutách podle významností KBI ve třech hodnotách:

- 1 – méně významný, kde reakce na incident musí proběhnout do 120 minut.
- 2 – významný, kde reakce na incident musí proběhnout do 90 minut.
- 3 – velmi významný, kde reakce na incident musí proběhnout do 30 minut.

7.1.2 Kritérium – dostupnost

Dostupnost (DOS) je kritérium stanovené zákonem a udává, jak dlouho může být dané aktivum nedostupné. Kritérium je udávané v minutách. Příkladem pro použití kritéria je výpadek webových stránek organizace a jak dlouho můžou být stránky nedostupné, než nastane nějaký problém.

Čím je hodnota nedostupnosti vyšší, tím je aktivum pro organizaci důležitější. Kritérium nabývá hodnot 1 až 4:

- 1 – výpadek aktiva do 1 týdne.
- 2 – výpadek aktiva do 1 dne.
- 3 – výpadek aktiva do 1 hodiny.
- 4 – výpadek aktiva v řádu minut.

7.1.3 Kritérium – posloupnost

Posloupnost (POS) je kritérium stanovené subjektivně a udává ideální posloupnost řízení kybernetického incidentu. Navazuje na kritérium RYC, jelikož v některých případech je nutné přeskočit v posloupnosti řízení incidentu, některé stupně a kontaktovat dotčený subjekt napřímo. Tato situace bývá nutná povětšinou z povahy kybernetického bezpečnostního incidentu.

Příklad použití kritéria je například infikování počítače v organizaci. Ve chvíli zjištění je důležitější tento počítač co nejrychleji odpojit od informačního systému organizace než incident eskalovat k nadřízeným. Je nutné zdůraznit, že se nejedná o činnost, kdy dochází k obcházení nadřízených stupňů, ale o činnost směřující k co nejrychlejšímu zastavení škodlivé činnosti. Nadřízení jsou informováni až po tomto zásahu.

Hodnocení tohoto kritéria je 1 až 3. Platí, že:

- 1 – znamená přímý kontakt subjektu.
- 2 – je přímý kontakt subjektu a nadřízeného.
- 3 – je kontakt pouze nadřízeného.

7.1.4 Kritérium – typ

Typ (TYP) je kritérium stanovené subjektivně a udává, o jaký útok na infrastrukturu společnosti se jedná. V jednoduchosti lze kritérium přirovnat k nebezpečnosti útoku respektive jeho komplexnosti. V přeneseném slova smyslu může být chápáno jako míra rizika. Kritérium má hodnoty 1 až 3 kde:

- 1 – nízká úroveň rizika (SPAM, skenování apod.).
- 2 – střední úroveň rizika (Phishing, DoS apod.).
- 3 – vysoká úroveň rizika (kompromitace zařízení, infrastruktury, Malware apod.).

7.1.5 Kritérium – dopad

Dopad (DOP) je kritérium vycházející ze zákona a určuje, jaký dopad může mít kybernetický útok na chod společnosti. Hodnota kritéria vzrůstá s tím, jak stoupá dopad kybernetického útoku. Kritérium nabývá hodnot 1 až 4:

- 1 – méně závažný dopad.
- 2 – závažný dopad.
- 3 – velmi závažná dopad.
- 4 – kritický dopad (narušení celistvosti systému).

7.2 Stanovení vah

Váhy v první sloupci byly stanoveny na základě profesionálního subjektivního hodnocení odborníka, který koordinuje činnost pří řešení kybernetických incidentů.

Váhy v druhém sloupci, byly zpracovány na základě anonymního dotazníku, který je přílohou této diplomové práce, v modelové organizaci respektive v jeho bezpečnostním oddělení.

Váhy na základě dotazníku byly stanoveny takto:

Tabulka 7 Váhy jednotlivých kritérií [Zdroj: Vlastní tvorba]

Kritérium	Váhy - diplomant	Váhy - dotazník
RYC	**0,33**	0,23
DOS	0,13	0,15
POS	0,07	0,18
TYP	0,2	0,2
DOP	0,27	**0,25**

Ze stanovení vah je vidět mírná odlišnost mezi hodnocením odborníka a z dotazníkového šetření. Rozdíl je u určení hlavního kritéria tedy rychlost nebo dostupnost. Model bude pracovat s kritérii odborníka, jelikož vztah mezi kritérii rychlost a dostupnost je nepřímo úměrný. Z hlediska procesu řešení platí, že čím rychleji bude incident řešen, tím se zmenšuje dopad incidentu na infrastrukturu a naopak čím větší dopad útoku na infrastrukturu

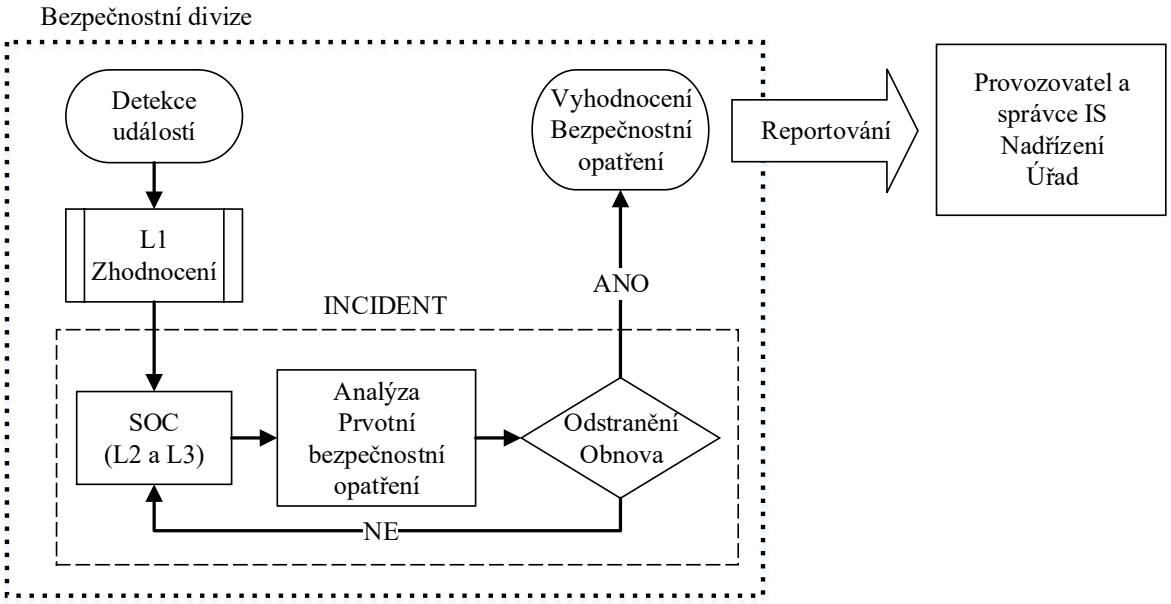
tím musí být reakce rychlejší. Zároveň platí, že čím vyšší hodnota váhy, tím je kritérium významnější.

7.3 Návrh modelů

Vzhledem k výše uvedenému bude v diplomové práci rozebrán detailně pouze jeden model a to model, kde je nejdůležitějším kritériem rychlost. Tento model se pro účely této diplomové práci nazývá modelem rychlostním. U zbylých modelů bude pouze nastíněn proces řešení. Návrh modelu je vztažen na modelovou organizaci a její strukturu, která je uvedena na obrázku 7.

7.3.1 Rychlostní model

Úkolem SOCu v modelové organizaci je řešit vzniklý kybernetický incident co nejrychleji. Rychlost je rozhodujícím faktorem a tedy i model bude zaměřen na tento parametr.



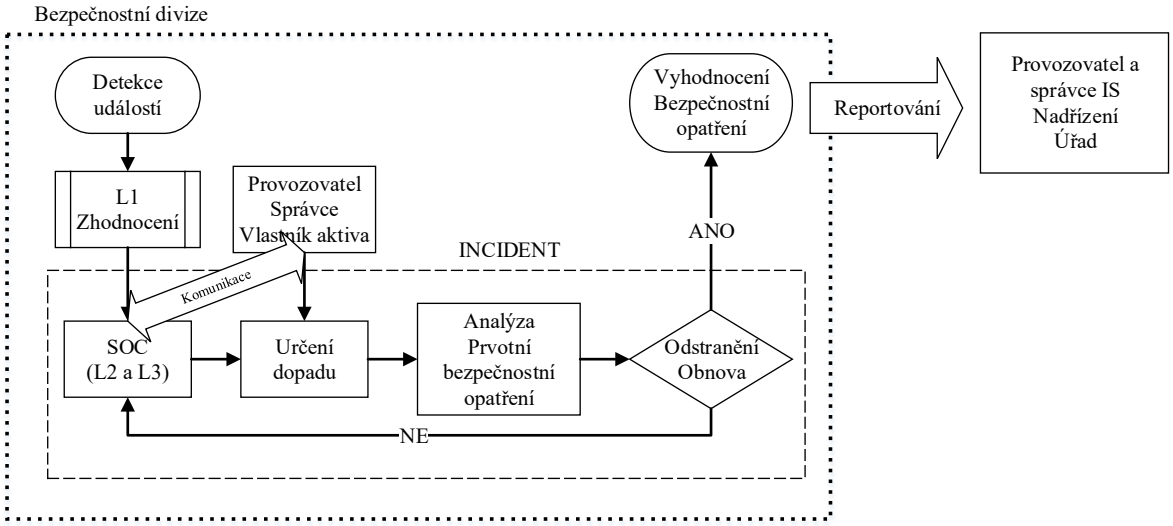
Obrázek 9 Rychlostní model [Zdroj: Vlastní tvorba]

Jak je z obrázku 9 vidět SOC provede prvotní analýzu incidentu a navrhne i prvotní bezpečnostní opatření. Může se jednat o odpojení zařízení, segmentu sítě, vypnutí služby apod. Model se plně soustředí na co nejrychlejší reakci a minimalizaci škod.

7.3.2 Dopadový model

Úkolem SOCu v modelové organizaci je řešit kybernetický incident na základě dopadu. Dopad musí nejprve určit na základě informací, o jaké aktivum se jedná, jak je významné a z toho plynoucí dopad na organizaci.

U modelu je již na první podhled vidět místo kde se proces řešení bude zpomalovat. Tím místem je práce určení dopadu, kdy SOC není vlastníkem, provozovatelem ani správcem IS. V tomto případě se na ně musí obrátit, aby dokázal z jejich pomoci na základě vyhodnocení situace určit dopad.



Obrázek 10 Dopadový model [Zdroj: Vlastní tvorba]

7.4 Vyhodnocení zvolených modelů

Z pohledu kybernetické bezpečnosti je a bude nejdůležitějším parametrem rychlost řešení kybernetického bezpečnostního incidentu. V rámci úvahy je lepší funkčnost systému dočasně omezit, než poskytovat útočníkům cenné minuty pro jejich škodlivou činnost. Proto s porovnání modelů vychází jako nejlepší model rychlostní. Proces řešení incidentu je téměř bez prodlev.

V případě dopadového modelu je prodleva v komunikaci mezi SOC a provozovatele, správcem nebo vlastníkem aktiva. Určení dopadu nelze jednoduše určit bez předchozí analýzy nebo porozumění co se v systému děje. Tento model je tak v reálné situaci použitelný, ale s určitými omezeními. Aby se eliminovala prodleva, musely by se pro každý typ útoku na dané aktivum určit dopady. To je v reálné situaci téměř nemožné ať už z důvodu, že útočník většinou použije více technik útoku tak proto, že minimálně zranitelnosti HW nebo

SW se objevují téměř každý den a tak by se musel dopad vždy podle zranitelnosti aktualizovat.

7.5 Závěr kapitoly

Navzdory všemu je zřejmé, že v kybernetické bezpečnosti musíme při řešení přeskočit některé fáze i proti vůli nadřízených. Ve fázi útoku je důležité, aby analytik dostatečně rychle analyzoval situaci a přijal bezpečnostní opatření. Ty nemusí být vždy správná, ale to je již úkolem fáze vyhodnocení, aby zlepšovala a zrychlovala proces řešení incidentu.

V této kapitole jsme si tak stanovily váhy, na základě kterých se můžeme rozhodovat v procesu řešeni kybernetického bezpečnostního incidentu. Podle mého odborného úsudku byly vybrány taková kritéria, která jsou v procesu řešení nejčastěji řešena.

8 APLIKACE VYBRANÉHO MODELU

V této závěrečné části budeme aplikovat rychlostní model z předchozí kapitoly do reálné situace. Budou popsané jednotlivé kroky plánu zvládání incidentu vztaženému k vybranému modelu.

8.1 Vznik incidentu

Útočníci si vybrali modelovou organizaci s cílem poškodit její reputaci, získat data a poškodit co nejvíce její infrastrukturu. Použili relativně jednoduchý útok podvodným e-mailem, tedy útok typu *spear-phishing*. Tento typ nevyžádané pošty byl doručen více zaměstnancům. Neobsahoval přílohu, pouze text s hypertextovým odkazem, a proto nebyl bezpečnostními technologiemi označen jako „SPAM“ ani zahozen. Pro uživatele se tak jevil jako legitimní e-mail, avšak text e-mailu upozorňoval uživatele, že jejich schránka je plná a pokud si nenavýší její limit, bude dočasně pozastavena její funkčnost. Jeho důvěryhodnost zvyšovalo i to, že byl velice podobný e-mailu, který dostávají od svého správce poštovního serveru.

Útok nebyl veden proti konkrétní osobě jako proti organizaci. Zaměstnanec, budeme ho značit jako “Bob“, e-mail obdržel a na odkaz pro zvýšení limitu schránky přistoupil a následně vyplnil své jméno a heslo. Následovalo přesměrování na skutečné schránky a tak Bob neměl podezření. Avšak útočnicí ukradli Bobovi přihlašovací údaje a ty následně použily k infiltraci IS PLYN společnosti SEaP a.s.

Jakmile útočnici infiltrovali systém, použili poštovní server společnosti k rozesílání různých sdělení jak jejím zákazníkům tak i vládním a nadnárodním organizacím v ČR i mimo ni. Společnost má nastavené bezpečnostní technologie, které upozorní v případě, kdy počet odeslaných e-mailů překročí hranici 30 za minutu.

Cílem odstavce není polemizovat proč uživatel na e-mail reagoval nebo ukázat jak takový e-mail vypadá a to z toho důvodu, že jsme každý tento typ e-mailu nejednou obdrželi jak do svých soukromých, tak i pracovních e-mailů, ale také proto, že není cílem řešit důvody infiltrace jako takové, ale její vyřešení.

8.2 Řízení incidentu

Na následujících řádcích bude popsána činnost společnosti respektive SOCu na kybernetický bezpečnostní incident podle rychlostního modelu.

8.2.1 Detekce a analýza

Bezpečnostní technologie zaznamenali překročení limitu odeslaných e-mailů a byla sepnuta událost. L1 přijmul událost a podle stanovených pravidel vyhodnotil, že se nejedná o standartní chování poštovního serveru a postoupil událost na L2.

L2 provádí prvotní analýzu, stahuje logy informačního systému a také analyzuje samotný e-mail, jeho znění a komu je posílán. Do 10 minut od přijmutí události konstatuje, že se jedná o kompromitaci poštovního serveru, nejenom na základě znění e-mailu, ale také na základě příjemců, kde většina z nich není zákazníkem společnosti. Přijímá bezpečnostní opatření a dočasně pozastavuje funkčnost poštovního serveru.

L2 pokračuje v bezpečnostní analýze a zjišťuje, že pro odesílání je využit účet uživatele Bob. Účet uživatele okamžitě blokuje a zároveň pracovní počítač uživatele vzdáleně odpojuje od firemní sítě. Na základě odborných zkušeností lze konstatovat, že v tomto případě se jedná o činnost, kterou lze vyřešit do 30 minut od přijmutí události.

Aktuálně stále kromě zaměstnanců SOCu není o tomto incidentu nikdo notifikován. Veškerá činnost je zaměřena na co nejrychlejší řešení.

8.2.2 Odstranění a obnova

V této časti řešení incidentu, budou již notifikovány další osoby např. nadřízený Boba, provozovatel a správce IS PLYN apod. L2 může předat řešení L3, který provádí detailní analýzu incidentu. Výsledkem jeho práce je odstranění neodeslané pošty z poštovního serveru a obnova všech služeb.

8.2.3 Vyhodnocení

Tato část řešení incidentu bude a je u všech modelů stejná. L3 by ve spolupráci s nižšími stupni měl sestavit časovou osu incidentu.

Dalším neméně důležitým faktorem je identifikovat nedostatky a zhodnotit fáze postupu a tím vylepšovat plán zvládaní incidentu. V této části se také provozovatel a správce musí rozhodnout o klasifikaci incidentu a jeho reportování či nereportování nadřízeným a v případě, že systém spadá pod zákon, tak i Úřadu.

8.3 Vyhodnocení incidentu

Incident typu *spear-phishing* je velice rozšířený a neexistuje proti němu účinná obrana ve formě bezpečnostních technologií. Jedinou obranou v tomto případě je edukace a vlastní uvažovaní uživatelů. Je důležité zmínit, že podobný incident v modelové organizaci proběhnul, ale nebyl řešen zvoleným rychlostním modelem ale jiným způsobem, který způsobil značné zpoždění v zastavení šíření nevyžádané pošty a způsobil také značné poškození reputace organizace.

Právě čas, který byl rozhodujícím kritériem, umožnil L2 dočasně pozastavit funkčnost služeb v našem případě onoho poštovního serveru. Na rozdíl od dopadového modelu nemusel řešit dopad incidentu, jelikož z jeho pozice jako nevlastní dané aktivum a nemůže tak adekvátně posoudit dopad incidentu. Tím by docházelo k prodloužení doby reakce a dopad a veškeré negativní účinky proti chráněnému zájmu by se zvyšovaly.

Na základě vybraného rychlostního modelu, zkušeností analytiků si troufám tvrdit, že potřebný čas prvotní reakce nepřekročí dobu 30 minut od detekce události. V kybernetické bezpečnosti je vždy důležité vzít na vědomí, že útočník mohl systém napadnout mnohem dříve, skryt uvnitř systému a prozatím nebyl úspěšně detekován bezpečnostními technologiemi. Právě proto je čas při zvládání incidentu rozhodujícím faktorem.

8.4 Závěr kapitoly

V kapitole jsme úspěšně aplikovali vybraný model řešení kybernetického bezpečnostního incidentu na reálný kybernetický útok. Součástí řešení incidentu byly jednotlivé kroky nutné pro řešení incidentu, které dále popisovaly činnost v těchto krocích. V posledním odstavci pak byl incident a vybraný model vyhodnocen a ověřena jeho teoretická i praktická funkcionalita použitelná pro proces řešení kybernetického bezpečnostního incidentu.

DÍLČÍ ZÁVĚR PRAKTICKÉ ČÁSTI

V praktické části jsme se věnovali modelové organizaci. V ní jsme popsali organizační strukturu a v krátkosti jsme zmínili také její bezpečnostní politiku zaměřenou na kybernetickou bezpečnost. Následovala analýza rizik v modelové organizaci, jejich vyhodnocení. Na základě analýzy byly popsány technická opatření řešící jednotlivé hrozby. Bylo zmíněno, jak modelová organizace řeší svoji kybernetickou bezpečnost, kdo ji realizuje a jak je dělena odpovědnost. V praktické části modelové organizace bylo na závěr popsáno zvládání incidentu z pohledu životního cyklu incidentu.

Následovala kapitola, kde jsme navrhovali modely řešení incidentu pro naši modelovou organizaci. Na začátku jsme si stanovily kritéria, která jsou v procesu řešení kybernetického bezpečnostního incidentu těmi nejdůležitějšími a přiřadily jim váhy. Z vyhodnocení kritérií jsme poté vtvořily a vyhodnotily model vhodný pro řešení incidentu.

V poslední části jsme vybraný model aplikovaly a modelovou organizaci a nechali jsme tento model projít procesem řešení reálného kybernetického bezpečnostního incidentu. Závěrem jsme vyhodnotily jeho vhodnost a použitelnost pro řešení reálných incidentů.

ZÁVĚR

V diplomové práci jsem se snažil přiblížit specifika, která do procesu řešení kybernetických bezpečnostních incidentu vstupují a navrhnout model řešení kybernetického bezpečnostního incidentu na základě vybraných kritérií.

V diplomové práci jsem vysvětlil specifika řešení, která do procesu stupují napřímo legislativou a z toho pramenící specifické povinnosti a základní pojmy kybernetické bezpečnosti. Jako jedno specifikum zopakujme provozovatele nebo správce, kteří jsou z pohledu zákona za vše odpovědní. Nemusejí být však vlastníky systému a nemusí nebo nemohou rozhodovat o finanční stránce potřebné pro plnění povinnosti. Prvky poskytující kybernetickou ochranu jsou drahé a jejich použití přichází až v případě kybernetického útoku.

V dalších částech jsem vysvětlil základní typy kybernetických útoků, jakým způsobem může být kybernetická bezpečnost zajištěna a také jak v jednotlivých typech organizačních struktur řešit kybernetický incident. Tyto části diplomové práce dokreslují celkový pohled, který vzniká při řešení kybernetického bezpečnostního incidentu. Poukazuje na to, že do procesu vstupují různé proměněné. Cílem bylo vytvořit teoretické základy pro praktickou část a komplexněji ukázat čím vším se v kybernetické bezpečnosti musíme zabývat, a že vždy nejde jenom o technickou stránku věci.

Pří pokusu ve výběru modelů jsem narazil na to, že se mi nepodařil vybrat model podle některého multikriteriálního hodnocení a to z důvodu, že jednotlivá kritéria tak, jak byla stanovena, výběr nakonec neumožňovala. Pří řešení tohoto problému jsem však pochopil a ujasnil si, že nejdůležitějším a nejvýznamnějším kritériem při řešení kybernetického bezpečnostního incidentu je rychlost. Rychlost tak přímo determinuje ostatní kritéria, která jsem v práci vybral. Determinuje kritérium dostupnost tím, že včasným řešením je nedostupnost co nejkratší bez ohledu na důležitost nedostupného aktiva. Posloupnost determinuje tím způsobem, že v kybernetické bezpečnosti vzhledem k tomu jak probíhá kybernetický útok, nelze postupovat jenom vertikálně, ale je třeba postupovat především horizontálně v organizační struktuře a řešit incident na místě, kde vzniknul. V tomto případě není účel obcházení nadřízených, ale nadřízení by měli mít důvěru ve své podřízené a nechat jim volné ruce při řešení a minimalizaci dopadu kybernetického útoku. Následná náprava pak již může být v režii nadřízených, ale nejdůležitější je co nejrychleji kybernetický útok řešit. Další kritérium, které určuje je typ. Z mého pohledu je téměř jedno o jaký typ kybernetického útoku se jedná, ale o to jak rychle ho odvrátit. Posledním kritériem, které jsem

řešil a rychlost ho nepřímo určuje, je dopad. Pro vztah dopad s rychlostí platí nepřímá úměra, čím rychleji je incident vyřešen tím menší je dopad a naopak. Chtěl bych zároveň říci, že i když to tak může z diplomové práce vypadat, jsou i tyto kritéria velmi důležitá. Kritéria přichází na řadu ve chvíli kdy je na systém vedeno vícero útoku a nelze je řešit souběžně. Musí se určit priority, ale pokud se opět vrátíme k nejvýznamnějšímu kritériu a to rychlosti, opět platí, že čím rychleji je první problém vyřešen, tím rychleji mohu řešit další. Aplikoval jsem tak rychlost na reálný příklad kybernetického incidentu a ověřil jsem si správnost svého tvrzení.

Závěrem bych rád zopakoval, že cíle diplomové práce byly naplněny jak v teoretické části tak hlavně v praktické části, kde byla ověřena a modelově ukázána situace řešení kybernetického bezpečnostního incidentu.

SEZNAM POUŽITÉ LITERATURY

[1] BUSSELL, Jennifer, 2013. *Cyberspace* [online]. In: Encyclopedia Britannica [cit. 2022-04-27]. Dostupné z: https://www.britannica.com/topic/cyberspace

[2] ČAPEK, Jan et al., 2015. Vybrané aspekty kybernetické bezpečnosti. Pardubice: Univerzita Pardubice. ISBN 978-80-7395-953-1.

[3] ČERVENÁ, Vlasta, FILIPEC, Josef, ed., 2003. Slovník spisovné češtiny pro školu a veřejnost s Dodatkem Ministerstva školství, mládeže a tělovýchovy České republiky. Vyd. 3., opr. Praha: Academia. ISBN 80-200-1080-7.

[4] ČESKO. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) - znění od 1. 9. 2021. In: Zákony pro lidi.cz [online]. © AION CS 2010-2022 [cit. 27. 4. 2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181#f5278849

[5] ČESKO. Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) - znění od 28. 5. 2018. In: Zákony pro lidi.cz [online]. © AION CS 2010-2022 [cit. 27. 4. 2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/2018-82#f6228374

[6] ČESKO. § 7 odst. 1 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) - znění od 1. 9. 2021. In: Zákony pro lidi.cz [online]. © AION CS 2010-2022 [cit. 31. 1. 2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181#p7-1

[7] ČESKO. § 7 odst. 2 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) - znění od 1. 9. 2021. In: Zákony pro lidi.cz [online]. © AION CS 2010-2022 [cit. 31. 1. 2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181#p7-2

[8] ČESKO. Příloha č. 1 vyhlášky č. 82/2018 Sb., vyhláška o kybernetické bezpečnosti - znění od 28. 5. 2018. In: Zákony pro lidi.cz [online]. © AION CS 2010-2022 [cit. 17. 2. 2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/2018-82#f6228907

[9] ČESKO. Příloha č. 2 vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) - znění od 28. 5. 2018. In: Zákony pro lidi.cz [online]. © AION CS 2010-

2022 [cit. 27. 4. 2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/2018-82#f6228918

[10] GOGELA, Robert, 2011. Pracovní příručka bezpečnostního manažera. Praha: Policejní akademie ČR v Praze. ISBN 978-80-7251-364-2.

[11] HODAČOVÁ, Veronika, 2021. Smishing. In: Policie.cz [online]. Policie ČR [cit. 2022-02-23]. Dostupné z: https://www.policie.cz/clanek/preventivni-informace-smishing.aspx

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

[13] KOLOUCH, Jan a Pavel BAŠTA, 2019. CyberSecurity. Praha: CZ.NIC, z.s.p.o. CZ.NIC. ISBN 978-808-8168-348.

[14] LUKÁŠ, Luděk, 2017. Teorie bezpečnosti I. Zlín: Radim Bačuvčík - VeRBuM. ISBN 978-80-87500-89-7.

[15] LUKÁŠ, Luděk, 2015. Bezpečnostní technologie, systémy a management V. Zlín: Radim Bačuvčík - VeRBuM. ISBN 978-80-87500-67-5.

[16] MCCARTHY, N. K., 2012. The computer incident response planning handbook: executable plans for protecting information at risk. New York: McGraw-Hill. ISBN 978-0-07-179039-0.

[17] NORDINE, Justine. OSINT Framework. In: Osintframework.com [online]. [cit. 2022-05-17]. Dostupné z: https://osintframework.com

[18] SMEJKAL, Vladimír, Tomáš SOKOL a Jindřich KODL, 2019. Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk. ISBN 978-807-3807-658.

[19] Historie podvodných e-mailů a SMS, © 2022. In: Ceskaposta.cz [online]. Praha: Česká pošta, s.p. [cit. 2022-02-23]. Dostupné z: https://www.ceskaposta.cz/o-ceske-poste/historie-podvodnych-e-mailu

[20] Bezpečnostní strategie ČR (2003) [online], 2003. PRAHA: Ministerstvo pro místní rozvoj ČR [cit. 2022-05-17]. Dostupné z: https://www.dataplan.info/img_upload/7bdb1584e3b8a53d337518d988763f8d/bezpecnostni-strategie-cr.pdf

[21] IBM Security QRadar SIEM, ©1994- 2021. Ibm.com [online]. IBM Corporation [cit. 2021-11-03]. Dostupné z: https://www.ibm.com/products/qradar-siem

[22] What Is DLP and How Does It Work?, © 2022. In: Trellix.com [online]. Musarubra US [cit. 2022-05-17]. Dostupné z: https://www.trellix.com/en-us/security-awareness/data-protection/how-data-loss-prevention-dlp-technology-works.html

[23] IDS Vs IPS, ©1994 - 2022. In: Checkpoint.com [online]. [cit. 2022-05-17]. Dostupné z: https://www.checkpoint.com/cyber-hub/network-security/what-is-an-intrusion-detection-system-ids/ids-vs-ips/#CheckPointsolution

[24] Legislativa KB. In: Nukib.cz [online]. Brno [cit. 2022-04-27]. Dostupné z: https://nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/

[25] Směrice evropského parlamentu a rady (EU) 2016/1148, 2016. In: EUR-Lex.europa.eu [online]. LUXEMBOURG [cit. 2022-04-27]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32016L1148&from=EN

[26] Using Anti-Spam and Mail, 2022. In: Sc1.checkpoint.com [online]. © 2020 Check Point Software Technologies [cit. 2022-04-27]. Dostupné z: https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_ThreatPrevention_AdminGuide/Topics-TPG/Using_Anti_Spam_and_Mail.htm

[27] Novela zákona o Vojenském zpravodajství. In: Vzcr.cz [online]. Praha [cit. 2022-04-27]. Dostupné z: https://vzcr.cz/novela-zakona-o-vojenskem-zpravodajstvi-151

[28] Network Operations Center (NOC), 2018. In: Cesnet.cz [online]. Praha: © 1996–2021 CESNET, z. s. p. o. [cit. 2022-04-27]. Dostupné z: https://www.cesnet.cz/sluzby/noc/

[29] MITM (Man In The Middle), 2016. In: ManagementMania.com [online]. Wilmington (DE) 2011-2022 [cit. 2022-04-27]. Dostupné z: https://managementmania.com/cs/mitm-man-in-the-middle

[30] Vishing a spoofing, © 2021. In: Policie.cz [online]. Policejní prezidium ČR [cit. 2022-02-23]. Dostupné z: https://www.policie.cz/clanek/vishing-a-spoofing.aspx

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

APT	Advanced persistent threat
CIA	Confidentiality Integrity Availability
DoS	Denial of Service
DDoS	Distributed Denial of Service
IS	Informační systém
ISO	International Organization for Standartization
ITIL	Information Technology Infrastructure Library
KBU	Kybernetická bezpečnostní událost
KBI	Kybernetický bezpečnostní incident
KS	Komunikační systém
LTO	Linear Tape Open
OSINT	Open Source Intelligence
PCO	Pult centrální ochrany
SQL	Structured Query Language
NGFW	Next Generation Firewall
VoKB	Vyhláška o kybernetické bezpečnosti
ZoKB	Zákon o kybernetické bezpečnosti

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: DOTAZNÍK KE STANOVENÍ VAH

Dobrý den,

Pro svoji diplomovou práci bych Vás rád požádal o přiřazení vah jednotlivým kritériím, která jsou určující při řešení kybernetického bezpečnostního incidentu.

Váhy mohou nabývat hodnot 1 až 10, nemusí být použity všechny hodnoty a hodnota 10 znamená, že kritérium je nejvýznamnější. Cílem je subjektivní zhodnocení a seřazení kritérií podle Vašeho uvážení.

Kritérium	Popis	Váha
Rychlost	Jak rychle se musí reagovat na incident.	
Dostupnost	Jak dlouho může být aktivum nedostupné.	
Posloupnost	Komu předávat informace, koho informovat.	
Typ	O jaký typ kybernetického útoku se jedná.	
Dopad	Jaký dopad má kybernetický útok na organizaci.	