Hrozba Ransomware v prostředí ochrany obyvatelstva

Milan Kučera

Bakalářská práce
2024

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

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

Akademický rok: 2023/2024

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Milan Kučera**
Osobní číslo:	**L21613**
Studijní program:	**B1032A020002 Ochrana obyvatelstva**
Forma studia:	**Prezenční**
Téma práce:	**Hrozba Ransomware v prostředí ochrany obyvatelstva**

Zásady pro vypracování

1. Na základě provedené rešerše zpracujte teoretický vstup do dané problematiky.
2. Seznamte se s problematikou ransomwaru jakožto hrozby v kontextu ochrany obyvatelstva.
3. Analyzujte opatření přijímaná subjekty v souvislosti s hrozbou ransomwaru.
4. Navrhněte scénáře dopadů hrozby ransomware v oblasti ochrany obyvatelstva.

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

Seznam doporučené literatury:

1. GRIMES, Roger A. *Ransomware protection playbook*. Hoboken, New Jersey: Wiley, 2021. ISBN 978-1-119-84912-4.
2. KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o., 2019. ISBN 978-80-88168-31-7.
3. SMEJKAL, Vladimír, Tomáš SOKOL a Jindřich KODL. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019 ISBN 978-80-7380-765-8.

Další odborná literatura dle doporučení vedoucího bakalářské práce.

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

Datum zadání bakalářské práce: **1. prosince 2023**
Termín odevzdání bakalářské práce: **3. května 2024**

L.S.

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

prof. Ing. Dušan Vičar, CSc.
ředitel ústavu

V Uherském Hradišti dne 4. prosince 2023

PROHLÁŠENÍ AUTORA
BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že:

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

Prohlašuji,

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

V Uherském Hradišti, dne: 3.5.2024

Jméno a příjmení studenta: Milan Kučera

.....
podpis studenta

ABSTRAKT

Bakalářská práce zkoumá problematiku kybernetické bezpečnosti v konkrétním subjektu. Práce má strukturu teoretické a praktické části. První část se zabývá teoretickým pozadím této problematiky, včetně základní terminologií, principy kybernetické bezpečnosti a legislativním rámcem. Druhá část se zaměřuje na konkrétní charakteristiku zkoumaného subjektu a provádí analýzu jeho vnitřního a vnějšího prostředí, pomocí metody SWOT. Na základě výsledků této analýzy je identifikována strategie subjektu, která je odvozena od silných stránek, slabý stránek, příležitostí a hrozeb. Dále se práce zaměřuje na aplikaci metody "What – if", s cílem prozkoumat a zmapovat možné důsledky různých hypotetických scénářů dané problematiky. Na základě takto získaných poznatků je pak navržen soubor opatření, pro efektivní řešení daných problémů.

Klíčová slova: Analýza, kybernetická bezpečnost, kyberprostor, legislativa, ransomware

ABSTRACT

The bachelor thesis examines the issue of cyber security in a specific entity. The thesis has a structure of theoretical and practical part. The first part deals with the theoretical background of this issue, including basic terminology, principles of cyber security and legislative framework. The second part focuses on the specific characteristics of the studied entity and performs an analysis of its internal and external environment, using the SWOT method. Based on the results of this analysis, the entity's strategy is identified, which is derived from strengths, weaknesses, opportunities and threats. Furthermore, the work focuses on the application of the "What – if" method, in order to explore and map the possible consequences of various hypothetical scenarios of the issue. On the basis of the knowledge obtained in this way, a set of measures is then proposed for the effective solution of the given problems.

Keywords: Analysis, Cybersecurity, cyberspace, legislation, ransomware

Chtěl bych poděkovat panu Ing. Petru Svobodovi, Ph.D. za odborné vedení, jeho cenné rady a čas, který mi věnoval při zpracování této bakalářské práce. Dále bych chtěl poděkovat jednatelům daného subjektu za materiály pro zpracování.

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

OBSAH

ÚVOD

V dnešní digitální době se informační technologie staly nedílnou součástí našeho života. Závisíme na nich v mnoha oblastech včetně komunikace, práce, vzdělávání a zábavy. Bohužel s rostoucím používáním informačních technologií roste i riziko kybernetických útoků. Jedním z nejzávažnějších typů kybernetických útoků je ransomware. Ransomware je typ malwaru, který ukradne a zašifruje soubory oběti a požaduje výkupné za jejich dešifrování. Útočníci vyvíjí dodatečný nátlak tím, pokud výkupné nebude zaplaceno, že data zveřejní nebo prodají na černém trhu. Tento typ útoku může mít zničující dopad na jednotlivce i organizace. Proto je důležité si uvědomovat rizika kybernetických útoků a přijímat nezbytné kroky k ochraně proti nim.

V oblasti ochrany obyvatelstva představuje ransomware mimořádnou hrozbu. Záchranné složky, nemocnice a další kritická infrastruktura jsou na svých IT systémech silně závislé a jejich narušení může vést k fatálním následkům. Například v roce 2017, ransomware WannaCry zaútočil na stovky nemocnic po celém světě, čímž způsobil rozsáhlé narušení provozu a ohrozil zdraví místních pacientů.

V současné době je situace ohledně ransomwaru stále závažnější a vyžaduje neustálou pozornost a snahu o zlepšení ochrany. Příkladem může být i poslední velký útok z února roku 2024, kdy údajně ruská skupina hackerů, napadla největší společnost zabývající se zdravotním pojištěním v Severní Americe, UnitedHealth Group Incorporated, kdy společnost byla nucena zaplatit 22 milionů dolarů ve formě Bitcoinu jak výkupné a další náklady, které dosahují astronomické výše 3 miliard dolarů.

Jelikož jsou tyto kybernetické hrozby globální, je potřeba mezinárodní spolupráce v boji proti této kybernetické hrozbě. Ransomware útoky jsou často prováděny útočníky ze zahraničí, kteří cílí na oběti v jiných zemích. Díky internetu a globálnímu propojení jsou útoky schopny rychle překročit národní hranice a zasáhnout cíle na celém světě. Boj proti ransomware vyžaduje koordinovanou mezinárodní reakci, včetně výměny informací, spolupráce při vyšetřování a provádění právních opatření proti útočníkům. Organizace jako Europol, Interpol a další mezinárodní instituce hrají klíčovou roli, při koordinaci těchto aktivit.

Budoucí výzvy a trendy v oblasti ransomwaru představují důležitý aspekt, kterým by se měli odborníci zabývat. Útočníci neustále vyvíjejí nové metody a techniky, aby obešli bezpečnostní opatření a zvyšovali úspěšnost svých útoků. S rostoucí důležitostí dat

a zvýšením citlivosti údajů se může očekávat, že útočníci budou požadovat vyšší výkupné za odblokování dat. S nástupem nových technologií, jako je umělá inteligence a blockchain, mohou útočníci využít nové možnosti k provádění ransomware útoků nebo zvýšení jejich účinnosti.

Hlavním cílem práce je provést analýzu možných dopadů ransomware na vybraný subjekt ochrany obyvatelstva. Ke splnění tohoto cíle byly stanoveny dílčí cíle, které jsou: pojednat o teoretických východiscích práce, analyzovat dopady současných verzí ransomware, vytvořit scénáře těchto negativních dopadů na vybraný subjekt ochrany obyvatelstva a navrhnout opatření ke zmírnění těchto negativních dopadů.

I. TEORETICKÁ ČÁST

1 ZÁKLADNÍ NÁZVOSLOVÍ

V úvodní části bakalářské práce je popsána základní terminologie vybraných odvětví. Tyto pojmy jsou důležité pro pochopení praktické části bakalářské práce.

1.1 Kyberprostor

Abychom mohli porozumět kybernetické bezpečnosti a kybernetickým útokům, je třeba definovat prostředí, ve kterém se tyto akce odehrávají. Pojem kyberprostor poprvé vymyslel spisovatel William Gibson v roce 1982. Gibsonova původní myšlenka, která nabyla popularity v době vzestupu cyberpunku v osmdesátých letech, poskytla inspiraci nejen pro tvůrce počítačových systémů a uživatelských rozhraní, ale také pro další autory pohybující se v oblasti cyberpunku. I když Gibson později vyjádřil kritiku vůči termínu "kyberprostor", označil ho za "sugestivní a v podstatě nesmyslný". Pojem se v průběhu let pevně zakořenil v oblasti IT, internetu a sítí, zejména díky počítačovým subkulturám. V průběhu let se však jeho definice stala zastaralou a proto je možné najít v nových slovnících definici, jak například říká tato, od Oxford dictionary *„fiktivní prostředí, ve kterém dochází ke komunikaci skrze počítačové sítě.“* (Kolouch, Bašta 2019)

Česká legislativa podle zákonu č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů uvádí definici pojmu kybernetický prostor jako: *„kybernetickým prostorem [se rozumí] digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací“.* (Zákon č. 181/2014 Sb.)

Kolouch uvádí, že kyberprostor je virtuální svět, který je otevřený, globalizovaný a plný informací. Uživatelé v něm mohou interaktivně komunikovat a ovlivňovat mínění ostatních. Technologie a na ně navázané služby jsou v kyberprostoru dominantní. V poslední době se ukazuje, že události ve virtuálním světě mohou mít dopady na svět reálný. (Kolouch 2016)

V současnosti se nejčastěji popisuje kyberprostor takto: *„Kyberprostor je globální a vyvíjející se doména popisovaná užíváním elektrických sítí a elektromagnetického spektra, jejíž smysl je vytvářet, uchovávat, upravovat, vyměňovat, sdílet, vybírat, používat či vymazávat informace.“* Kyberprostor zahrnuje:

- *„Fyzická i telekomunikační zařízení, která umožňují spojení technologií a komunikaci sítí systému, chápáno obecně (smartphony/tablety, počítače, servery, atd...) “.*
- *„Počítačové systémy a komplementární software, který zaručuje spojení a funkčnost systému“.*
- *„Spojení počítačových sítí“.*
- *„Uživatelské vstupy a uzly zprostředkovatelů spojení“.*
- *„Informace – uživatelská data“.* (Mayer et al., 2014)

1.2 Kybernetická bezpečnost

Koncept kybernetické bezpečnosti nemá jednotně přijatou obecnou definici. Dle Jiráska a kol. představuje kybernetická bezpečnost *„souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru“.* (Jirásek, Požár a Novák, 2015)

Relativně obdobně je kybernetická bezpečnost definována i v Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020. V této strategii je uvedeno, že: *„Kybernetická bezpečnost představuje* ***souhrn*** *organizačních, politických, právních, technických a vzdělávacích* ***opatření a nástrojů směřujících k zajištění zabezpečeného, chráněného a odolného kyberprostoru v České republice****, a to jak pro subjekty veřejného a soukromého sektoru, tak pro širokou českou veřejnost.“* (Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020, 2015)

Dále by se dala kybernetická bezpečnost definovat jako ochrana počítačových systémů, sítí a souvisejících dat před neoprávněným přístupem, použitím, změnou nebo zničením. (Sanders 2023)

Cílem kybernetické bezpečnosti je zajistit, aby byly tyto systémy a data bezpečné a dostupné pouze oprávněným uživatelům. Kybernetické útoky jsou stále častější, sofistikovanější a mohou zahrnovat:

- Hacking: Neoprávněný přístup k počítačovým systémům nebo sítím.
- Malware: Škodlivý software, který může způsobit poškození nebo ztrátu dat.

- Útoky na sociální inženýrství: Pokusy o získání citlivých informací od uživatelů podvodnými prostředky. (Sanders 2023)
- Phishing: Útok pomocí technik sociálního inženýrství, kdy se útočník snaží získat důvěrná data oběti nebo spustit na zařízení oběti škodlivý kód.
- Botnet: Rozsáhlá síť kompromitovaných zařízení (tzv. zombies) ovládaných kybernetickými útočníky.
- DDoS: Útoky, které mají za cíl přetížit systém nebo síť, aby byly nedostupné. (Porter 2023)

1.3 Principy kybernetické bezpečnosti – Triáda CIA

Při zavádění opatření kybernetické bezpečnosti se provádí implementace základních principů, které jsou rovněž označovány jako triáda kybernetické bezpečnosti (CIA).

Triáda CIA

Triáda kybernetické bezpečnosti známá jako CIA (C – **Confidentiality** (důvěrnost); I – **Integrity** (celistvost); A – **Availability** (dostupnost) je nejvíce rozšířená a používaná, avšak pouhé používání těchto základních principů bez zahrnutí dalších nedostačuje k udržení dostatečné úrovně kybernetické bezpečnosti v dnešní době. Dnes se například poukazuje i na uplatňování **Parkerian hexad**, což je de facto triáda CIA, která je doplněna o další tři prvky: **P/C – Possession/Control** (držení či kontrola), **A – Authenticity** (autentičnost) a **U – Utility** (užitečnost). (Hsu a Marinucci, 2013)

Obrázek 1 CIA – Parkerian hexad (Khasayeva, 2023)

Často se triáda CIA přisuzuje zejména oblasti informací.

Toto užší pojetí vychází z konkrétní definice informační bezpečnosti, která zdůrazňuje ochranu informací. Během této ochrany není důležité, na jakém médiu (např. papír, elektronická média) nebo v rámci jakého systému jsou informace zpracovávány. Koncept informační bezpečnosti se pak týká ochrany informací po celou dobu jejich životního cyklu. (Kolouch, Bašta 2019)

Normy ISO 27000 poskytují definice a směrnice pro informační bezpečnost. Mezi klíčové normy v oblasti informační bezpečnosti patří:

- ČSN ISO/IEC 27001:2023 Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Systémy managementu informační bezpečnosti – Požadavky. (Česká agentura pro standardizaci, 2023)
- ČSN ISO/IEC 27002:2023 Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Opatření informační bezpečnosti. (Česká agentura pro standardizaci, 2023)

Důvěrnost (Confidentiality)

Koncept důvěrnosti stanoví, že pouze oprávněné subjekty mají přístup k informacím, datům nebo informačním a komunikačním technologiím (ICT). S ohledem na rozsáhlý objem zpracovávaných informací je užitečné implementovat některou z klasifikací informací. Tuto klasifikaci lze následně rozšířit i na ostatní prvky kybernetické bezpečnosti a regulovat přístup k nim. (Kolouch, Bašta 2019).

Bezpečnostní standardy ISO/IEC 27000 definují že:

- *„Informace by měly být klasifikovány, a to s ohledem na jejich hodnotu, právní požadavky, citlivost a kritičnost.“*
- *„Pro značení informací a zacházení s nimi by měly být vytvořeny a do praxe zavedeny postupy, které jsou v souladu s klasifikačním schématem přijatým organizací.“*
- *„Pro zabránění neautorizovanému přístupu nebo zneužití informací by měla být stanovena pravidla pro manipulaci s nimi a pro jejich ukládání.“* (Kolouch, Bašta 2019).

Příklady některých klasifikačních schémat:

1) Klasifikace informací dle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti:
    - **Přísně tajné** – neoprávněná manipulace s informacemi by mohla přinést mimořádně vážné poškození zájmům České republiky.
    - **Tajné** – nekompetentní zacházení s informacemi by mohlo vážně poškodit zájmy České republiky.
    - **Důvěrné** – neoprávněné zacházení s informacemi by mohlo způsobit prostou újmu zájmům České republiky.
    - **Vyhrazené** – nekompetentní manipulace s informacemi by mohla být nevýhodná pro zájmy České republiky. (Zákon č. 412/2005 Sb.)
2) Hodnocení informací používané v oblasti podnikání:
    - **Chráněné** – nekompetentní manipulace s informacemi by mohla vést k závažnému poškození nebo zničení organizace, jako například únik strategických informací, zdrojových kódů, schémat zabezpečení nebo hesel.
    - **Interní** – neoprávněná manipulace s informacemi by mohla způsobit škodu organizaci, jako například únik osobních údajů nebo smluv.
    - **Citlivé** – nekompetentní zacházení s informacemi by mohlo mít nepříznivý vliv na společnost, jako například uvolnění dosud nezveřejněných informací o projektech nebo plánovaných akcích.
    - **Veřejné** – neoprávněná manipulace s informacemi by neměla způsobit žádnou škodu a neměla by mít žádný vliv na společnost, například při zveřejnění veřejně dostupných kontaktů nebo prezentací projektů. (Šulc, 2018)
3) Traffic Light Protocol

V rámci komunity kybernetické bezpečnosti vznikla potřeba sdílet citlivé informace a data, zejména týkající se kybernetických útoků. K tomu byl vytvořen na začátku 21. století protokol TLP (Traffic Light Protocol) v National Infrastructure Security Coordination Centre. Cílem tohoto protokolu je urychlit výměnu informací mezi zúčastněnými subjekty a zároveň stanovit pravidla pro zacházení s poskytnutými informacemi. Zdroj informací

vždy označuje informaci specifickou barvou, která udává pravidla pro manipulaci s informacemi ze strany příjemce. (Kolouch, Bašta 2019)

Tato tabulka ilustruje základní barvy TLP 2.0 (aktualizován v roce 2022) a jejich příslušné popisy, které indikují úroveň citlivosti a rozsah sdílení informací. (Národní úřad pro kybernetickou a informační bezpečnost, 2022)

Tabulka 1 Traffic Light Protocol 2.0. Zdroj: (NÚKIB, 2022)

Barva	Popis
Červená	Informace může být sdělena pouze osobě, pro niž byla původně určena, pokud nejsou explicitně stanoveny další osoby, kterým lze takovou informaci předat.
Oranžová + striktní	Informace smí být sdílena pouze uvnitř příslušné organizace, a to pouze osobám, které splňují need-to-know a jsou nezbytní pro řešení uvedeného problému nebo hrozby.
Oranžová	Informace smí být sdílena uvnitř příslušné organizace a jejím partnerům, a to pouze osobám, které splňují need-to-know a jsou nezbytní pro řešení uvedeného problému nebo hrozby.
Zelená	Informace může být sdílena s vybranými partnery nebo skupinami, avšak nikoli skrze veřejně dostupné kanály; příjemce musí při předání zajistit důvěrnost komunikace.
Bezbarvá	Bez omezení – sdílet s jakýmkoli subjektem nebo veřejností. Případné omezení na základě práva duševního vlastnictví původce a/nebo příjemce či třetích stran.

Integrita (Integrity)

Dle Výkladového slovníku kybernetické bezpečnosti je **integrita** definována jako *„vlastnost přesnosti a úplnosti.“* **Integrita** dat je pak ve stejném slovníku definována jako *„jistota, že data nebyla změněna. Přeneseně označuje i platnost, konzistenci a přesnost dat, např. databází nebo systémů souborů. Bývá zajišťována kontrolními součty, hašovacími funkcemi, samoopravnými kódy, redundancí, žurnálováním atd. V kryptografii a v zabezpečení informací všeobecně integrita znamená platnost dat.“* **Integrita systému** pak je *„vlastnost,*

že systém vykonává svou zamýšlenou funkci nenarušeným způsobem, bez záměrné nebo náhodné neautomatizované manipulace se systémem.“ (Jirásek, Požár a Novák, 2015)

Integrita tedy znamená, že pouze oprávněná osoba má možnost manipulovat s informacemi, daty, počítačovými systémy a jejich nastavením, a nikdo jiný nemá právo do těchto prvků zasahovat. Integrita rovněž zabezpečuje neporušenost systému, informací a dat, poskytující jakousi záruku nedotčenosti. (Kolouch, Bašta 2019)

V situaci, kdy dochází k narušení integrity, je důležité si uvědomit, že nechtěné změny dat nemusí být okamžitě odhaleny, a může uplynout značný čas, než je porušení integrity objeveno.

Příloha č. 1 k vyhlášce o kybernetické bezpečnosti obsahuje také referenční měřítko pro posouzení integrity:

Nízká – integrita tohoto aktiva nepotřebuje být chráněna, ať už z hlediska oprávněných zájmů subjektu nebo jakékoliv jiné potřeby. Ochrana není nutná. (Vyhláška č. 82/2018 Sb.)

Střední – integrita tohoto aktiva může vyžadovat ochranu, protože narušení integrity může způsobit škodu oprávněným zájmům subjektu a projevit se menšími dopady na hlavní aktiva. Standardní nástroje, jako například omezení přístupových práv pro zápis, jsou používány k ochraně integrity. (Vyhláška č. 82/2018 Sb.)

Vysoká – aktivum vyžaduje ochranu z hlediska integrity. Porušení integrity tohoto aktiva způsobuje škodu oprávněným zájmům subjektu s výraznými dopady na primární aktiva. K zajištění integrity jsou používány specifické metody, které umožňují sledovat historii provedených změn a identifikovat osobu, která tyto změny provedla. Bezpečnost integrity informací přenášených komunikačními sítěmi je zajištěna pomocí kryptografických prostředků. (Vyhláška č. 82/2018 Sb.)

Kritická – integrita tohoto aktiva vyžaduje efektivní ochranu. Narušení integrity způsobuje mimořádně závažné poškození oprávněných zájmů subjektu s bezprostředními a výrazně vážnými důsledky na klíčová aktiva. K zajištění integrity se využívají speciální prostředky pro jednoznačnou identifikaci osoby, která provádí změnu, například pomocí digitálního podpisu. (Vyhláška č. 82/2018 Sb.)

Dostupnost (Availability)

Dle Výkladového slovníku kybernetické bezpečnosti je dostupnost definována jako *„vlastnost přístupnosti a použitelnosti na žádost oprávněné entity.“* (Jirásek, Požár a Novák, 2015)

Dostupnost může být interpretována jako záruka možnosti získání informací, dat nebo přístupu k počítačovému systému v daný okamžik. I ten nejperfektnější systém, který zabezpečuje integritu a umožňuje přístup k systému, datům nebo informacím, není užitečný, pokud nedokáže spolehlivě zajistit přístup podle potřeby. (Kolouch, Bašta 2019)

Stupnice hodnocení dostupnosti je obsažena v příloze č. 1 k vyhlášce o kybernetické bezpečnosti.

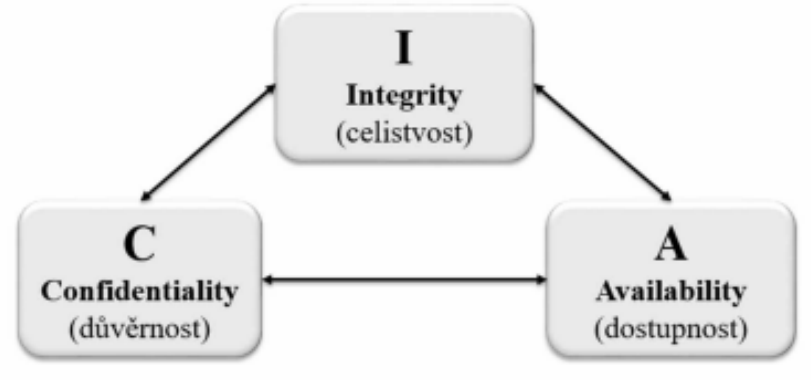
Nízká – narušení dostupnosti aktiva není důležité a v případě výpadku je obvykle tolerováno delší období na opravu (přibližně do jednoho týdne). Pro zajištění dostupnosti postačuje pravidelné zálohování. (Vyhláška č. 82/2018 Sb.)

Střední – přerušení dostupnosti tohoto aktiva by nemělo přesáhnout pracovní den, a pokud by bylo delší, mohlo by to představovat potenciální riziko pro oprávněné zájmy subjektu. Pro zajištění dostupnosti se běžně využívají standardní postupy zálohování a obnovy. (Vyhláška č. 82/2018 Sb.)

Vysoká – narušení dostupnosti tohoto aktiva by nemělo přesáhnout několik hodin. Každý výpadek je třeba okamžitě řešit, neboť představuje přímé ohrožení oprávněných zájmů subjektu. Tato aktiva jsou považována za velmi klíčová. K zajištění dostupnosti se využívají záložní systémy, a obnovení poskytování služeb může vyžadovat zásah personálu nebo výměnu technických prostředků. (Vyhláška č. 82/2018 Sb.)

Kritická – narušení dostupnosti tohoto aktiva je nepřípustné a i krátkodobá nedostupnost (v řádu několika minut) představuje vážné riziko pro oprávněné zájmy subjektu. Tato aktiva jsou považována za kritická. Pro zajištění dostupnosti jsou využívány záložní systémy, a obnova poskytování služeb je krátkodobá a automatizovaná. (Vyhláška č. 82/2018 Sb.)

Grafická reprezentace Triády CIA bývá často používána k lepšímu pochopení vzájemných vztahů a atributů této koncepce. Z tohoto důvodu je zde prezentováno typické vizuální znázornění Triády CIA.



Obrázek 2 Triáda CIA (Kolouch, Bašta 2019)

1.4 Legislativa kybernetické bezpečnosti

V roce 2000 Ministerstvo vnitra ČR vydalo koncepci boje proti trestné činnosti v oblasti informačních technologií. Tato koncepce se primárně zaměřovala na potírání trestné činnosti, ale také na vytvoření podmínek pro systémový přístup státu k této problematice. Kromě potírání kybernetické trestné činnosti se tento dokument také zabývá otázkami kybernetické bezpečnosti protože se v něm uvádí, že *„je zapotřebí vytvořit prostředí pro vzájemnou osvětu a informační výměnu mezi subjekty, získávajícími poznatky o jednotlivých bezpečnostních aspektech, spojených s používáním nových technologií. Je úlohou státních orgánů vytvářet stabilní a bezpečné prostředí, které dává občanům oprávněně pocit právní jistoty při využívání moderních informačních a komunikačních prostředků“*. (Ministerstvo vnitra ČR, 2000).

„K získaným poznatkům o jednotlivých obecných i konkrétních bezpečnostních rizicích by měla mít bezprostřední přístup i veřejnost. K tomuto úkolu je třeba přistoupit aktivně, tedy průběžně provádět preventivně cílenou informační kampaň ve spolupráci všech odpovědných resortů a za účinné participace dalších zainteresovaných subjektů“ (Ministerstvo vnitra ČR, 2000).

Koncepce boje proti trestné činnosti v oblasti informačních technologií stanovila několik konkrétních opatření, která měla přispět k zajištění kybernetické bezpečnosti. Mezi tato opatření patřilo:

- Vypracování projektu hlásného systému pro trestnou činnost v oblasti informačních technologií, který by umožnil rychle a efektivně shromažďovat a vyhodnocovat informace o kybernetických útocích.

- Iniciování a podpora vzniku a činnosti skupin typu CERT (Central Emergency Response Team), které by poskytovaly podporu a pomoc při řešení kybernetických incidentů. (Ministerstvo vnitra ČR, 2000)

Gestorem této problematiky byl odbor bezpečnostní politiky Ministerstva vnitra ČR, který spolupracoval s dalšími odbory ministerstva, Policejním prezidiem, Úřadem vyšetřování, Kriminalistickým ústavem, Policejní akademií ČR a dalšími subjekty. (Ministerstvo vnitra ČR, 2000)

1.4.1 Směrnice Evropského parlamentu a Rady (EU) 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii.

Tímto návrhem směrnice se předkládá rozsáhlý soubor opatření zaměřených na zvýšení úrovně bezpečnosti sítí a informačních systémů s účelem zabezpečit klíčové služby pro ekonomiku a společnost v rámci Evropské unie. Směrnice má za cíl zajistit, že členské země EU budou adekvátně připraveny a schopny účinně řešit kybernetické útoky a reagovat na ně prostřednictvím:

- Určení příslušných orgánů.
- Zřízení bezpečnostních týmů typu CSIRT (Computer Security Incident Response Team).
- Přijetí národní strategie pro kybernetickou bezpečnost.

Také ustanovuje spolupráci na úrovni Evropské unie a to jak na strategické, tak na technické úrovni. V neposlední řadě nařizuje, aby poskytovatelé základních a digitálních služeb přijímali adekvátní bezpečnostní opatření a informovali příslušné národní orgány o významných bezpečnostních incidentech. (Směrnice EU 2016/1148 – kybernetická bezpečnost sítí a informačních systémů, 2018)

1.4.2 Zákon č. 181/2014 Sb., o kybernetické bezpečnosti

Právními předpisy v oblasti kybernetické bezpečnosti se zabývá zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů. Zákon upravuje práva a povinnosti osob a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti. (Zákon č. 181/2014 Sb.)

Cílem zákona je zajištění bezpečnosti informačních systémů, služeb a sítí elektronických komunikací v kybernetickém prostoru. Kybernetický prostor je definován jako virtuální prostor, který je tvořen informačními systémy, službami a sítěmi elektronických komunikací. Zákon se vztahuje na všechny orgány veřejné moci, právnické osoby a fyzické osoby, které provozují informační systémy nebo služby a sítě elektronických komunikací. Osoby a orgány veřejné moci jsou povinny přijmout bezpečnostní opatření, která zajistí ochranu jejich informačních systémů, služeb a sítí elektronických komunikací před kybernetickým nebezpečím. Kybernetickým nebezpečím se rozumí stav, ve kterém je ve velkém rozsahu ohrožena bezpečnost informací v informačních systémech nebo bezpečnost služeb elektronických komunikací anebo bezpečnost a integrita sítí elektronických komunikací. (Zákon č. 181/2014 Sb.)

Orgány veřejné moci jsou povinny v případě vzniku kybernetického bezpečnostního incidentu, který může mít významný dopad na veřejné zájmy, informovat Národní úřad pro kybernetickou bezpečnost (NÚKIB). NÚKIB je orgánem veřejné moci, který má za úkol koordinovat a zajišťovat kybernetickou bezpečnost v České republice. Zákon upravuje také povinnosti orgánů veřejné moci a osob v oblasti vzdělávání, výzkumu a vývoje v oblasti kybernetické bezpečnosti. (Zákon č. 181/2014 Sb.)

Zákon rovněž stanovuje opatření a povinnosti týkající se ochrany kritické infrastruktury.

Zákon definuje KI jako *"informační systémy, sítě elektronických komunikací a další informační a komunikační technologie, jejichž narušení nebo zničení by mohlo mít závažný dopad na fungování státu, hospodářství nebo společnosti."* Zákon dále rozlišuje mezi kritickou informační infrastrukturou (KII) a významnými informačními systémy (VIS). KII zahrnuje systémy v odvětvích jako energetika, doprava, bankovnictví, zdravotnictví a další kritické sektory. VIS zahrnuje systémy, které sice nejsou tak kritické jako KII, ale jejich narušení by mohlo mít také značný dopad. (Zákon č. 181/2014 Sb.)

Dále zákon ukládá provozovatelům kritické infrastruktury řadu povinností, jejichž cílem je chránit tyto systémy před kybernetickými útoky. Mezi tyto povinnosti patří:

- Provádění rizikové analýzy a hodnocení kybernetické bezpečnosti svých systémů.
- Zavádění adekvátních bezpečnostních opatření na základě provedeného hodnocení.
- Hlášení kybernetických bezpečnostních incidentů Národnímu úřadu pro kybernetickou a informační bezpečnost (NÚKIB).

- Spolupráce s NÚKIB a dalšími orgány státní správy v oblasti kybernetické bezpečnosti. (Zákon č. 181/2014 Sb.)

NÚKIB má pravomoc provádět u provozovatelů KI kontroly a ukládat jim sankce v případě zjištění porušení zákona. Zákon si dává za cíl v oblasti KI zvýšit tuto odolnost proti kybernetickým útokům a zmírnit dopady případných incidentů. Toho dosahuje zavedením výše uvedených povinností pro provozovatele KI a posílením pravomocí orgánů dohledu. (Zákon č. 181/2014 Sb.)

Zákon byl novelizován v roce 2022. Novela zavádí nové povinnosti pro orgány veřejné moci a osoby v oblasti kybernetické bezpečnosti, zejména v oblasti:

- Posílení spolupráce orgánů veřejné moci a osob v oblasti kybernetické bezpečnosti.
- Zpřísnění povinností orgánů veřejné moci a osob v oblasti vzdělávání, výzkumu a vývoje v oblasti kybernetické bezpečnosti.
- Zjednodušení postupů při řešení kybernetických bezpečnostních incidentů. (Zákon č. 181/2014 Sb.)

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

Tato vyhláška zapracovává příslušný předpis Evropské unie pro informační systém kritické infrastruktury, komunikační systém kritické infrastruktury, významný informační systém, informační systém základní služby anebo informační systém nebo síť elektronických komunikací, které využívá poskytovatel digitálních služeb a upravuje:

a) Obsah a strukturu bezpečnostní dokumentace.
b) Typy, kategorie a hodnocení významnosti kybernetických bezpečnostních incidentů,
c) Způsob likvidace dat, provozních údajů, informací a jejich kopií. (Vyhláška č. 82/2018 Sb.)

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

Vyhláška stanovuje, které informační systémy se v České republice považují za významné informační systémy (dále jen VIS) a jaká kritéria musí splňovat, aby do této kategorie spadaly. VIS je informační systém, jehož narušení nebo zničení by mohlo mít závažný dopad

na fungování státu, hospodářství, obyvatelstva nebo životního prostředí. (Vyhláška č. 317/2014 Sb.)

Vyhláška stanovuje 3 typy určujících kritérií, které musí VIS splňovat:

- Odvětvová kritéria: Tato kritéria se vztahují na specifické odvětví, jako je například energetika, doprava nebo zdravotnictví.
- Dopadová kritéria: Tato kritéria posuzují dopad, který by mohlo mít narušení nebo zničení VIS na různé aspekty, jako je lidské zdraví, bezpečnost nebo hospodářství.
- Kritéria pro informační systémy orgánů veřejné moci: Tato kritéria se vztahují na informační systémy orgánů veřejné moci a posuzují jejich důležitost pro fungování daného orgánu. (Vyhláška č. 317/2014 Sb.)

Správci VIS musí splnit řadu povinností, včetně:

- Provedení posouzení, zda jejich informační systém splňuje kritéria VIS.
- Implementace bezpečnostních opatření na ochranu VIS před kybernetickými hrozbami.
- Ohlášení VIS Národnímu úřadu pro kybernetickou a informační bezpečnost.
- Pravidelné provádění kontrol a auditů bezpečnosti VIS. (Vyhláška č. 317/2014 Sb.)

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

Zákon upravuje zásady pro stanovení informací jako informací utajovaných, podmínky pro přístup k nim a další požadavky na jejich ochranu, zásady pro stanovení citlivých činností a podmínky pro jejich výkon a s tím spojený výkon státní správy. Zákon se zabývá těmito oblastmi:

a) Zákon stanovuje, co to jsou utajované informace a jak jsou kategorizovány podle úrovně citlivosti. Informace mohou být veřejné, interní nebo tajné.

b) Zákon upravuje, na jaké subjekty se vztahuje. To zahrnuje státní orgány, vojenské organizace, a další subjekty, které mají přístup k utajovaným informacím nebo vykonávají činnosti, které jsou spojeny s bezpečnostní způsobilostí.

c) Zákon stanovuje podmínky pro získání a udržení bezpečnostní způsobilosti. Bezpečnostní způsobilost je schopnost fyzické nebo právnické osoby zajistit ochranu utajovaných informací.

d) Zákon stanovuje různé povinnosti pro subjekty, které mají přístup k utajovaným informacím. To může zahrnovat oznamování bezpečnostních incidentů, spolupráci s bezpečnostními orgány a dodržování určitých postupů.

e) Zákon stanovuje sankce a postihy za porušení jeho ustanovení. Tyto sankce mohou zahrnovat pokuty, ztrátu bezpečnostní způsobilosti nebo trestní stíhání. (Zákon č. 412/2005 Sb.)

1.4.6 Zákon č. 110/2019 Sb., o zpracování osobních údajů (Adaptační zákon)

Zákon upřesňuje a doplňuje některá ustanovení Obecného nařízení o ochraně osobních údajů (GDPR), aby lépe odpovídala českému právnímu prostředí. Zákon obsahuje zvláštní ustanovení o ochraně osobních údajů při zpracování za účelem předcházení, vyhledávání nebo odhalování trestných činů a při zajišťování obrany a bezpečnosti ČR. (Zákon č. 110/2019 Sb.)

Mezi tyto ustanovení se řadí:

- Povinnosti správce a zpracovatele osobních údajů při zpracování osobních údajů pro účely výzkumu, statistiky a archivace.
- Pravidla pro nakládání s citlivými kategoriemi osobních údajů, jako jsou údaje o rasovém či etnickém původu, politických názorech nebo náboženském vyznání.
- Způsoby, jakými mohou subjekty údajů uplatňovat svá práva týkající se ochrany osobních údajů. (Zákon č. 110/2019 Sb.)

Zákon č. 111/2019 Sb., zákon, kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů.

Zároveň s Adaptačním zákonem č. 110/2019., „*o zpracování osobních údajů“* vešel v účinnost také zákon č. 111/2019., „*kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů“*. Zákon č. 111/2019 upravuje způsob, jakým soudy a orgány činné v trestním řízení zpracovávají osobní údaje, stanovuje povinnosti pro advokáty a notáře v oblasti ochrany osobních údajů a upřesňuje pravidla pro zpracování osobních údajů ve zdravotnictví a sociálních službách. (Zákon č. 111/2019 Sb.)

2 RANSOMWARE

Ransomware je typ malwaru, který zneužívá oběti tím, že jim ukradne soukromá data a následně vyhrožuje, že pokud nebude zaplaceno výkupné, tak odcizená data zveřejní, prodá nebo zašifruje. V minulosti se ransomware obvykle zaměřoval na jednotlivce, ale v poslední době se stává větší a obtížněji odvratitelnou hrozbou ransomware řízený lidmi, který se zaměřuje na organizace. Tento typ ransomwaru využívá tým útočníků, kteří spolupracují, aby získali přístup do podnikových sítí organizací. Některé útoky tohoto druhu jsou tak sofistikované, že útočníci nastavují cenu výkupného na základě informací, které se jim podařilo získat z interních dokumentů organizací. (Microsoft, 2023)

Kybernetičtí útočníci mají schopnost napadnout téměř jakékoliv chytré zařízení, které je připojeno k internetu. V roce 2017 došlo k jednomu z incidentů, kdy skupina hackerů pronikla do kasina v Las Vegas prostřednictvím chytrého teploměru, umístěného v jednom z akvárií. Proběh i experiment, kde byl využit chytrý kávovar k proniknutí do firemní sítě. (Fawkes, c 2014-2024)

2.1 Jak útoky pomocí ransomware fungují

Ransomware využívající sociální inženýrství je v dnešní době častým typem útoku. Kyberzločinci používají k šíření ransomware phishingové útoky, které využívají podvodů. V těchto útocích se útočník vydává za legitimní společnost nebo web a oběť přesvědčuje, aby klikla na odkaz nebo otevřela přílohu, která do jejího zařízení nainstaluje ransomware. Útoky často obsahují alarmující zprávy, které mají oběť vyděsit. Například kyberzločinec se může vydávat za banku a poslat příjemci e-mail, že jeho účet byl zablokován kvůli podezřelé aktivitě. E-mail obsahuje odkaz, na který by měl příjemce kliknout, aby problém vyřešil. Po kliknutí na odkaz se nainstaluje ransomware. (Microsoft, 2023)

Ransomware řízený lidmi je komplexní útok, který vyžaduje důkladnou přípravu a znalosti. Útočníci nejprve získají přístup do sítě organizace odcizením přihlašovacích údajů. Poté se pomocí ukradeného účtu dostanou k informacím o dalších účtech s vyššími oprávněními. Tyto informace použijí k získání přístupu k citlivým datům a klíčovým firemním systémům. Na tyto systémy pak nainstalují ransomware, který data zašifruje, ukradne a vyvíjí nátlak na společnost, že pokud nezaplatí výkupné, tak data zveřejní nebo prodají. Platby obvykle požadují v kryptoměně, aby se chránili před vypátráním. (Microsoft, 2023)

Tyto skupiny se zaměřují na velké organizace, protože mohou zaplatit vyšší výkupné než běžný jednotlivec. Někdy požadují miliony dolarů. Vzhledem k tomu, že narušení podnikové sítě může mít pro organizaci vážné důsledky, mnoho organizací se rozhodne raději výkupné zaplatit, než aby riskovalo únik citlivých dat nebo další útoky kyberzločinců. (Microsoft, 2023)

2.2 Typy ransomwarových útoků

Vyskytují se především dva druhy ransomwaru: kryptografický ransomware a blokovací (locker) ransomware. (Microsoft, 2023)

Kryptografický ransomware

Kyberzločinci, kteří využívají kryptografický ransomware, šifrují citlivá data nebo soubory oběti tak, aby byla nedostupná. Poté je oběť nucena zaplatit výkupné, aby získala šifrovací klíč a opět získala přístup ke svým datům. I při zaplacení výkupného neexistuje žádná jistota, že kyberzločinec skutečně poskytne šifrovací klíč nebo zcela uvolní kontrolu nad daty. Doxware představuje variantu kryptografického ransomwaru, která šifruje data a často vyhrožuje zveřejněním citlivých osobních údajů oběti, což by jí mohlo způsobit škodu. Hlavním cílem je rovněž dosažení zaplacení výkupného. (Microsoft, 2023)

Blokovací ransomware

Blokovací ransomware znefunkční zařízení oběti tak, že se do něj nemůže přihlásit. Oběti se na obrazovce zobrazí výzva k zaplacení výkupného, které je nutné uhradit, aby byl obnoven přístup k zařízení. Tato varianta ransomwaru obvykle nezahrnuje šifrování, což znamená, že poté, co oběť opět získá přístup ke svému zařízení, má také přístup ke svým citlivým souborům a datům. (Microsoft, 2023)

Double extortion ransomware

Metoda útok, která vylepšuje klasický ransomware o další nástroj nátlaku. Klasický ransomware šifruje data oběti, čímž jsou pro ni nepřístupná. Útočník pak požaduje výkupné za dešifrování. Double extortion k tomu přidává ještě krádež dat.

Útok probíhá tak, že:

1. Útočník se dostane do systému oběti.
2. Nainstalují ransomware, který zašifruje data.

3. Současně s tím ukradne citlivé informace (například finanční data, osobní údaje zákazníků nebo obchodní tajemství).
4. Potom oběť informuje, že data jsou zašifrovaná a navíc budou zveřejněny, prodány na černém trhu nebo jinak zneužity, pokud nebude zaplaceno výkupné.

Tímto pádem útočník oběť vydírá hned dvakrát:

- Oběť přijde o přístup ke svým datům.
- Oběti hrozí poškození reputace, finanční ztráta nebo právní problémy kvůli úniku citlivých dat.

Double extortion je nebezpečnější než klasický ransomware, protože oběť má větší motivaci zaplatit, aby se zabránilo zveřejnění dat. (SentinelOne, c2024)

Triple extortion ransomware

Tento typ zahrnuje další vrstvu útoku nad šifrováním souborů a krádeží dat. V závislosti na typu ransomwaru může mít různou podobu. Jedním z oblíbených vektorů útoku je narušení služeb (například útok DDoS). Oběť kromě ztráty a ohrožení dat čelí i narušení kritických operací. (PaloaltoNETWORKS, c2024)

Další vrstvou útoku, jejíž popularita mezi skupinami útočníků roste, jsou útoky přidružených třetích stran. V tomto případě, hrozby a požadavky na výkupné útočník rozšiřuje i na klienty, dodavatele nebo jiné spolupracovníky původní oběti. (PaloaltoNETWORKS, c2024)

2.3 Historie ransomwaru

Počátky ransomwaru sahají do roku 1989, kdy byl vytvořen trojan AIDS. Tento trojan se šířil pomocí disket a e-mailů a uživatelům nabízel databázi lidí nakažených AIDS. V pozadí však počítal spuštění počítače a po dosažení 90 spuštění zašifroval disk a požadoval zaplacení licenčního poplatku ve výši 189 dolarů. Autorem trojanu byl Dr. Joseph Popp, který byl nakonec prohlášen za duševně nemocného a zproštěn viny. (Peterka et al., 2017)

Dále se v roce 2005 objevilo velké množství tzv. scareware programů. Jedná se o typ ransomwaru, který má za úkol uživatele vyděsit. Zneklidňuje ho pomocí mnoha frází jako, „KRITICKÁ CHYBA“ nebo „DŮLEŽITÉ SYSTÉMOVÉ VAROVÁNÍ“, s cílem přesvědčit uživatele, že na jeho počítači dochází k problémům, které je třeba urgentně vyřešit. Vzápětí mu však nabízí nástroj, který slibuje řešení všech jeho problémů za nízkou cenu, obvykle kolem 50 dolarů. Jedním z příkladů může být SpySheriff. (Peterka et al., 2017)

Obrázek 3 Ransomware SpySheriff (Peterka et al., 2017).

Zdatnější uživatelé se však mohli ransomwaru zbavit poměrně snadno. Stačilo, aby počítač spustili v bezpečném režimu a vymazali specifický klíč z registrů. (Peterka et al., 2017)

Rok 2006 byl bohatý pro nově vynalezené typy ransomwaru, kdy došlo k vypuštění malwaru Archievus. Poprvé byl zde k zašifrování souborů použit algoritmus RSA – tedy šifrování s veřejným klíčem. Obecně je Archievus také považován za první ransomware, který využil asymetrické šifrování. Archievus tedy využíval na svou dobu velmi pokročilou metodu šifrování. Zajímavostí však bylo, že šifroval pouze soubory uložené ve složce *Moje dokumenty*. V té době většina uživatelů svých počítačových zařízení ukládala veškeré své soubory právě do této složky, což znamenalo úplnou ztrátu svých souborů. (Peterka et al., 2017)

O několik let později, v letech 2011 až 2013, se začal šířit ransomware pracující na podobném principu jako již zmíněné varianty scarewaru. Tentokrát se však snažil ransomware vyděsit uživatele tím, že jim vyhrožoval problémem v systému, který by mohl vést k sankcím ze strany úřadů. Tento ransomware byl pravděpodobně prvním svého druhu výrazně rozšířeným i u nás v České republice a říkalo se mu policejní vir. Tento druh ransomwaru se jmenoval Reveton a uživateli sděloval, že je obviněn z nelegální činnosti, za což mu dle trestního zákoníku ČR hrozí až několik let vězení. (Peterka et al., 2017)

2.3.1 CryptoLocker

Cryptolocker je považován za přelomový druh ransomwaru, jehož vznik se datuje k datumu 5. září roku 2013. Jednalo se o první kryptografický ransomware, jehož distribuce probíhala skrz webové stránky nebo e-mailové přílohy mířené nejčastěji na firmy. E-mailová příloha obsahovala spustitelný soubor, který vypadal jako obyčejné PDF. Ransomware využil funkci Windows, která ve výchozím nastavení uživatele nerozptylovala tím, že by mu ukazovala o jakou příponu se jednalo. (Peterka et al., 2017)

Po spuštění se škodlivý kód nainstaloval do registrů a pokusil se spojit s jedním ze svých serverů, na kterém byl následně vytvořen 2048bitový pár RSA klíčů. Vyžádání platby výkupného ve výši přibližně 400 dolarů nebo eur bylo standardní podmínkou, pro získání privátního klíče, nezbytného k dešifrování souborů. Časový limit pro provedení platby byl stanoven na obrazovce kde i probíhal stresující odpočet. Zhruba 1,3 % postižených osob údajně výkupné zaplatilo. I přes toto relativně nízké procento byl předpokládaný zisk pachatelů odhadován na 3 miliony dolarů. (Peterka et al., 2017)

2.3.2 WannaCry

WannaCry je zkratka pro WannaCrypt a odkazuje na skutečnost, že WannaCry je crypto-ware. Přesněji řečeno, je to cryptoworm, schopný se replikovat a šířit automaticky. WannaCry byl mimořádně účinný především díky svému způsobu šíření. Na rozdíl od využívání podvodů typu phishing, či stahování z infikovaných stránek botnetů, využíval WannaCry inovativní metodu. Tento ransomware se zaměřoval na známé zranitelnosti v operačních systémech počítačů Windows. Byl naprogramován tak, aby prohledával sítě a identifikoval počítače, které používaly starší verze Windows Server s již známými bezpečnostními chybami. Jakmile infikoval jeden počítač v síti, rychle identifikoval další zařízení s touto chybou. Tento automatizovaný a rychlý postup přispěl k rychlému šíření WannaCry a jeho masovému dopadu. (Fawkes, c 2014-2024)

Zarážející byl ovšem fakt, že zranitelnost WannaCry, využívaná v systémech Windows, byla identifikována před několika lety americkou národní bezpečnostní agenturou (NSA). Místo upozornění světa na tuto hrozbu se NSA rozhodla mlčet a vytvořila svůj vlastní nástroj pro zneužívání této slabiny, která poté sloužila jako kybernetická zbraň. To znamená, že WannaCry vycházel ze systému vyvinutého státní bezpečnostní agenturou. (Fawkes, c 2014-2024)

2.4 Budoucnost ransomwaru

S ohledem na rapidní nárůst zisků, které kybernetičtí zločinci dosahují díky ransomwaru se očekává, že se tato forma útoku bude v budoucnosti objevovat mnohem častěji. Úspěch WannaCry, který využíval automaticky se replikující technologie a zaměřoval se na známé zranitelnosti systémů, pravděpodobně stanovil trend pro většinu útoků v krátkodobé perspektivě. Je ovšem velmi nepravděpodobné předpokládat, že tvůrci ransomwaru již nepřemýšlejí o nových metodách infikování, šíření a monetizaci tohoto malwaru. (Fawkes, c 2014-2024)

Stále častěji se v dnešní době objevují v domácnostech a firmách chytré zařízení, která mají v sobě zabudovanou možnost připojit se k internetu. Útočníci mohou např. uzamknout automobil na dálku, blokovat chytré televize, znemožnění funkčnosti termostatu ústředního vytápění, proniknutí do sítě domácnosti skrze chytrého robota a podobně. S rostoucím používáním technologií a propojením světa se otevírá rozsáhlý prostor, ve kterém mohou kyberzločinci operovat. Tímto způsobem bude schopnost ransomwaru ovlivňovat náš každodenní život stále více narůstat. (Fawkes, c 2014-2024)

Další hrozby, kterým v budoucnu budeme muset pravděpodobně čelit:

- **Zvýšená sofistikovanost útoků:** Očekává se, že útočníci budou stále sofistikovanější a budou využívat pokročilé techniky, aby obešli bezpečnostní opatření a šifrovali nebo kradli cílová data. Náklady na ochranu proto budou stále narůstat.
- **Cílené útoky na velké organizace:** Útočníci mohou upřednostňovat cílené útoky na velké organizace a instituce, kde mohou získat vyšší výkupné nebo způsobit větší škody.
- **Zneužívání umělé inteligence:** Útočníci by mohli začít využívat umělou inteligenci ke zlepšení útoků a přizpůsobení se obranným opatřením. (Fawkes, c 2014-2024)

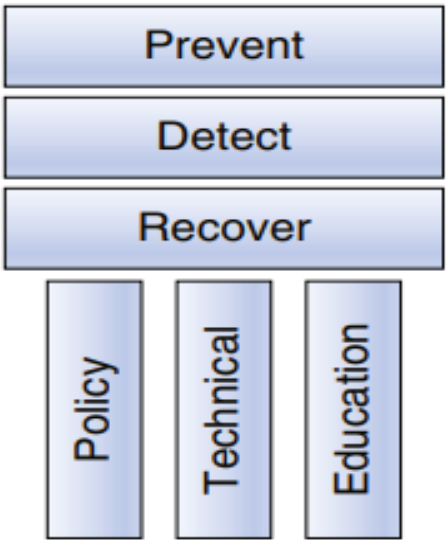
2.5 Jak se proti ransomwaru bránit

Jakmile hacker nebo malware získá počáteční přístup do zařízení nebo prostředí, je podstatně obtížnější minimalizovat další škody, než tomu bylo doposud. Zabezpečení celé infrastruktury podniku bývá velmi složité, obtížně proveditelné a nákladné, ale i tak je tento přístup stále levnější a jednodušší, než řešit následky, když už nastane nějaký průnik do systému. (Grimes, 2021)

Nejtěžší částí každého kybernetického útoku je první, počáteční přístup. Poté může většina útočníků snáze využít jeden napadený program nebo zařízení a dostat se do mnoha dalších. Mnohé studie ukazují, že sofistikovaní útočníci mohou přejít od jednoho kompromitovaného zařízení k mnoha dalším, počínaje již za méně než 19 minut. (Grimes, 2021)

Zabránění hackerům a škodlivému softwaru získat prvotní vstup do systému a využívat jej jako "operační základnu", by mělo být hlavním cílem každého odborníka na kybernetickou bezpečnost. Bohužel se v praxi stává, že rada "Dobře zálohujte!", je často prvním a někdy i jediným "preventivním" doporučením týkající se ransomwaru. Zálohování není prevence. Zálohování je minimalizace škod. Grimes říká, že pokud používáte zálohu, abyste se ochránili, vaše preventivní kontroly již dávno selhaly a ransomware má přístup do vašeho prostředí. Ransomware prokázal, že je zdatný v obcházení detekce, jakmile je spuštěn v prostředí. Jeden z průzkumů odhalil, že 86 % napadených obětí mělo nainstalovanou nejnovější antivirovou detekci. Podle některých dalších údajů, antivirová a jiná řešení pro detekci zastaví ransomware až v 50 % případů, ale je jasné, že kdyby byla detekce ransomwaru antivirovými produkty lepší, nebyl by ransomware tak velkým problémem, jakým je dnes. (Grimes, 2021)

Grimes říká, že každá obrana se skládá nejméně ze tří hlavních typů kontrol, zaměřených na tři různé cíle. Nazývá je 3x3 Security Control Pillars (SCP), ale často jsou popisovány s více fázemi a kontrolními typy od jiných kybernetických odborníků. Grimes minimalizoval tyto typy kontrol a cíle, aby byly jednodušší na pochopení. Tyto kontroly probíhají ve třech hlavních fázích: preventivní, detekční a obnovovací. (Grimes, 2021)



Obrázek 4 3x3 SCP. (Grimes, 2021)

Preventivní kontroly jsou všechny činnosti, které systém provádí, aby zabránil tomu, že se něco stane – v tomto konkrétním případě ransomware.

Detekční kontroly jsou vše, co systém dělá, aby zjistil, že hrozba úspěšně prošla všemi preventivními kontrolami a získala neoprávněný přístup do prostředí (nebo brání ostatním v získání legitimního přístupu). Právě zde je důležité dosáhnout včasného varování. Pokud se nedá zabránit tomu, aby se něco špatného stalo, další nejlepší věcí je včasné varování, abychom mohli rychle reagovat a v ideálním případě minimalizovat škody.

Poslední skupinou kontrolních opatření je vše, co se dá udělat, pro rychlé zotavení ze škodlivé události, kvůli minimalizaci odstávky a nákladů. (Grimes, 2021)

Každý typ kontroly se skládá ze tří složek: zásady, technická obrana a vzdělávání.

Zásady jsou jakákoliv pravidla, předpisy nebo doporučení, která jsou zavedena a sdělována za účelem minimalizace rizik. Například nikdy nesdělujte své heslo od e-mailu, ani nespouštějte program nebo neotvírejte dokument, který přijde v neočekávaném e-mailu. Nikdy nepoužívejte stejné heslo pro různé stránky nebo služby. Zásady mohou být podobné jako pilíř vzdělávání, ale mohou mít odlišné zaměření a přístup. Mezi zásady patří také postupy ("způsob, jak věci dělat") a standardy ("co se musí udělat nebo co se musí používat"). Zásady mohou znít například takto: "Všechny soubory musí být při přenosu šifrovány pomocí průmyslově přijímaných kryptografických standardů a klíčů.". (Grimes, 2021)

Technická obrana jsou všechny nástroje, které pomáhají předcházet, odhalovat, zmírnit nebo reagovat na hrozby a rizika. Do technické obrany v kybernetické bezpečnosti patří například antivirový software, software pro detekci koncových bodů a reakci na ně (EDR), firewally, zabezpečené konfigurace, filtrování obsahu, filtry proti phishingu atd. Bez ohledu na to, jak kvalitní jsou zásady a technická ochrana, je pravděpodobné, že se určité množství špatností dostane ke koncovému uživateli, který bude konfrontován s jejich pozorováním a zpracováním. (Grimes, 2021)

Vzdělávání se snaží naučit koncové uživatele, jak rozpoznat škodlivý kód, když se k nim dostane, a jak s ním zacházet, aby se minimalizovaly škody. V ideálním případě se koncoví uživatelé učí, jak ohlašovat pokusy o zneužití a jak je mazat nebo ignorovat. Jak však ukázala historie, sociální inženýrství, použité proti koncovým uživatelům, je vedlo k nesprávnému zacházení se škodlivými jevy, což je důvodem číslo jedna pro úspěšné narušení bezpečnosti. Často popisované metaforické dogma "obrana do hloubky" říká to, že každý systém by měl

usilovat o vytvoření co nejlepšího, vrstevnatého souboru preventivních, detekčních a obnovovacích kontrol s využitím několika vzájemně se překrývajících zásad, technických ochran a vzdělávání. Obvykle jsou žádoucí překrývající se kontroly a složky, protože snižují riziko vyplývající ze selhání jednotlivých kontrol. Jedna může zachytit to, co ostatním unikne. Je důležité vytvořit co nejlepší, hloubkovou obranu, vrstvenou sadu kontrol, abychom zabránili úspěchu ransomwaru. (Grimes, 2021)

Obecné postupy a rady k zvýšení resilience vůči ransomwaru

Zde je několik obecných rad, jak zvýšit resilienci vůči ransomwaru:

- Neklikat na přílohy v e-mailech od neznámých zdrojů a ignorovat e-maily, které působí podezřele. Útočníci často využívají různé metody sociálního inženýrství a nátlaku.
- Zajistěte bezpečnost svého počítače a mobilního zařízení instalací kvalitního antivirového programu a firewallu. Firewall slouží jako bariéra mezi zařízením a internetem, proto je důležité pravidelně aktualizovat, abyste měli ochranu proti nejnovějším hrozbám.
- Pravidelně provádějte aktualizace softwaru, vývojáři průběžně vydávají opravy, které řeší možná bezpečnostní rizika. Proto se nedoporučuje odkládat aktualizaci softwaru, i když přijde v nevhodný okamžik.
- Nepodceňujte důležitost zálohování dat – pravidelné vytváření záloh klíčových dat je základním opatřením k ochraně před kybernetickými útoky. V případě útoku pak můžete obnovit data ze zálohy.
- Omezte využívání vzdáleného ovládání pracovní plochy – měli byste buďto zcela zakázat tuto funkci nebo ji povolit pouze ve firemní síti, případně přes bezpečné připojení pomocí VPN.
- Školení svých zaměstnanců je klíčové, aby byli seznámeni s možnými hrozbami a byli schopni je identifikovat.
- Sledování podezřelé aktivity může zmírnit dopady ransomwaru, kvůli jeho rychlejší identifikaci. (ESET, c1992 – 2024)

3 DÍLČÍ ZÁVĚR TEORETICKÉ ČÁSTI

V teoretické části práce jsou nejprve v jednotlivých kapitolách definovány klíčové pojmy jako je kyberprostor, kybernetická bezpečnost a jsou zde popsány základní principy kybernetické bezpečnosti, včetně Triády CIA – konceptu zajišťujícího důvěrnost, integritu a dostupnost dat. Dále je pozornost věnována legislativě v oblasti kybernetické bezpečnosti, včetně relevantních zákonů a vyhlášek. Následně je analyzován samotný vir ransomware, včetně jeho fungování, historie, vývoje a také případy známých ransomwarových útoků jako je WannaCry. Prostor je kladen i tématu budoucnosti ransomwaru a jsou zde i zmíněny možné trendy, v oblasti kybernetických hrozeb. V závěrečné kapitole teoretické části této práce jsou představeny strategie a postupy, pro ochranu a zvýšení resilience, před infikování ransomwarem, včetně obecných rad a doporučení, pro uživatele a organizace. Teoretická část práce nastiňuje problematiku viru ransomware a nabízí vysvětlení jeho funkčnosti, pro pochopení praktické části práce.

II. PRAKTICKÁ ČÁST

4 POPIS ZVOLENÉHO SUBJEKTU

Subjekt, který byl pro zpracování v rámci bakalářské práce vybrán, je městský úřad v Otrokovicích. Jedná se o obec s rozšířenou působností, pod kterou spadají obce, jako jsou Napajedla, Tlumačov, Spytihněv a jiné.

4.1 Historie a současnost

Město Otrokovice se nachází ve Zlínském kraji na východě České republiky. Historie města sahá až do 13. století, kdy se první písemná zmínka o obci objevuje v listinách olomouckého biskupa Bruna ze Schauenburku z roku 1261. Postupně se rozvíjela jako zemědělská oblast s typickou osadnickou strukturou. Největší změna v historii města přišel ve 20. století, kdy se Otrokovice staly důležitým průmyslovým centrem. V roce 1919 zde zakládá Tomáš Baťa svou první továrnu na obuv, což položilo základy pro rozvoj města a vytvořilo podmínky pro vznik jednoho z nejvýznamnějších podnikatelských subjektů v Československu. Během své historie bylo město Otrokovice svědkem mnoha proměn. Po roce 1989 byly podniky znárodněny a privatizovány. To vedlo k mnoha změnám v místní ekonomice a společnosti obecně. Dnes jsou Otrokovice moderním městem s rozvinutou průmyslovou základnou a širokou škálou společenských, kulturních a rekreačních zařízení. Tomáš Baťa a jeho odkaz stále ovlivňují město a jeho obyvatele, a to nejen v ekonomickém smyslu, ale také ve smyslu architektonického dědictví a firemní kultury. Díky své poloze se zde setkávají charakteristiky tří regionů: Valašska, Slovácka a Hané. Dnes má město téměř 17 tisíc obyvatel a patří mezi šest největších měst Zlínského kraje, slouží jako centrum mikroregionu, který zahrnuje obce s celkovým počtem téměř 35 000 obyvatel. Městem se prolínají důležité silniční a železniční spojení a tak jsou Otrokovice považovány za vstupní bránu do Zlínského kraje.

4.2 Struktura subjektu a jednotlivé odbory a oddělení

Městský úřad v Otrokovicích je zodpovědný za poskytování různých veřejných služeb obyvatelům města. To zahrnuje vydávání občanských průkazů, evidence obyvatel, vydávání stavebního povolení, správu komunálního majetku, plánování a řízení územního rozvoje města v souladu s platnými zákony a předpisy. Úřad rovněž přijímá a spravuje rozpočet města a je zodpovědný za sběr daní, výběr poplatků, alokaci finančních prostředků na různé projekty a služby a řízení městských financí. Dále úřad spolupracuje s místními bezpečnostními složkami, jako jsou policie a hasiči, na zajištění veřejné bezpečnosti

a pořádku ve městě. To zahrnuje monitorování kriminality, poskytování bezpečnostních služeb a řešení místních problémů spojených s veřejným pořádkem. Úřad disponuje celkem 41 odbory a odděleními. V každém případě, je potřeba u těchto oddělení provést kybernetické zabezpečení a školení osob, pracujících pod těmito odděleními. O tyto záležitosti se stará oddělení informatiky, které zabezpečuje ochranu proti kybernetickým hrozbám. Pod tímto oddělením pracuje 6 osob a toto oddělení má za úkol zajistit správu a rozvoj informačních technologií a informačních systémů, které podporují efektivní fungování města a poskytování veřejných služeb. Činnosti informačního oddělení zahrnují:

- Správa a údržba IT infrastruktury
    - Oddělení se stará o provoz a údržbu počítačových sítí, serverů, hardwaru a softwaru potřebného pro běžný chod městského úřadu.
- Vývoj a správa informačních systémů
    - Oddělení zajišťuje vývoj a údržbu informačních systémů používaných různými odděleními městského úřadu pro správu dat a automatizaci procesů, jako je evidence obyvatelstva, účetnictví, správa majetku, a další.
- Bezpečnost IT
    - Oddělení zabezpečuje ochranu dat a informací městského úřadu proti hrozbám z internetu, včetně kybernetických útoků, malware a dalších bezpečnostních hrozeb.
- Podpora uživatelů
    - Oddělení poskytuje technickou podporu a školení zaměstnancům městského úřadu při používání IT systémů a aplikací.
- Digitalizace služeb
    - Oddělení podporuje digitalizaci veřejných služeb, která zahrnuje poskytování elektronických formulářů, online platby, elektronickou komunikaci s občany a další digitální iniciativy.

5 EXPERTNÍ ROZHOVOR S VEDOUCÍM ODDĚLENÍ INFORMATIKY MĚSTSKÉHO ÚŘADU OTROKOVICE

Za účelem zkoumání a hodnocení opatření přijímaných subjektem, ohledně hrozby ransomwaru, došlo k rozhovoru s vedoucím oddělení informatiky na Městském úřadu v Otrokovicích. Během tohoto rozhovoru byly předloženy předem připravené otázky, na které dotyčná osoba odpovídala.

5.1 Rozbor odpovědí

Tato část je věnována rozboru odpovědí, které poskytl vedoucí oddělení informatiky na městském úřadu.

1. Jaká je Vaše pozice na městském úřadu?

    - Vedoucí IT oddělení.

    Z odpovědi vyplývá, že respondent zastává klíčovou pozici v oblasti informačních technologií na městském úřadě. Z tohoto titulu lze odhadnout, že má odpovědnost za řízení a správu všech IT operací a projektů. Můžeme předpokládat, že je zodpovědný za strategické plánování IT, správu IT infrastruktury, implementaci nových technologií a poskytování technologické podpory ostatním oddělením městského úřadu. Jelikož je vedoucím oddělení, pravděpodobně má také manažerské povinnosti, jako je řízení týmu, hodnocení výkonu a rozvoj IT personálu. Tato odpověď naznačuje, že respondent má v IT oblasti rozsáhlé zkušenosti a odborné znalosti a hraje klíčovou roli ve vedení a rozvoji IT strategií organizace.

2. Zabývají se kybernetickou bezpečností i jiné osoby na úřadu? Pokud ano, má každá osoba jinou oblast zaměření?

    - Ano, kybernetickou bezpečností se zabývá více osob a každá má svou oblast zaměření.

    Z této odpovědi lze zjistit, že na městském úřadě se zabývá kybernetickou bezpečností více osob, což je pozitivní z hlediska zajištění bezpečnosti informačních systémů. Také je významné, že každá z těchto osob má svou vlastní oblast zaměření, což by mohlo znamenat specializaci na konkrétní aspekty kybernetické bezpečnosti, jako jsou síťová bezpečnost, správa hesel, monitorování hrozeb, ochrana dat atd. Tato

organizovanost a specializace může přispět k efektivnějšímu zajištění bezpečnosti a ochrany dat na úřadu.

3. Účastníte se Vy, jakožto odborník/ci na kybernetickou bezpečnost, například konferencí nebo seminářů,k prohloubení znalostí v této oblasti?

    - Ano, pravidelné vzdělávání je nezbytné.

    Z odpovědi vyplývá, že respondent považuje pravidelné vzdělávání v oblasti kybernetické bezpečnosti za nezbytné. To naznačuje, že si uvědomuje důležitost udržování aktuálních znalostí a dovedností v rychle se měnícím prostředí kybernetických hrozeb a technologií. Účast na konferencích a seminářích může respondentovi poskytnout příležitost se dozvědět o nejnovějších trendech, postupech a nástrojích v oblasti kybernetické bezpečnosti a rozšířit si své znalosti. Takové aktivity naznačují zájem o profesní růst a schopnost reagovat na aktuální bezpečnostní výzvy.

4. Probíhají pravidelná školení zaměstnanců úřadu k rozvoji identifikace kybernetických hrozeb? Pokud ano, jak často?

    - Ano probíhají. Termín není pevně stanoven, odvíjí se většinou od vážnosti aktuálních hrozeb, na které se školení následně zaměřuje.

    Na úřadu probíhají pravidelná školení zaměstnanců k rozvoji identifikace kybernetických hrozeb. Je však důležité poznamenat, že termín těchto školení není pevně stanoven a závisí na vážnosti aktuálních hrozeb. To znamená, že úřad pravděpodobně pružně reaguje na aktuální situaci a prioritizuje školení v reakci na nové nebo zvýšené hrozby. Tato strategie umožňuje úřadu lépe odpovídat na aktuální bezpečnostní výzvy a efektivněji budovat povědomí o kybernetických hrozbách mezi zaměstnanci.

5. Jsou na úřadu vypracovány interní dokumenty, jak postupovat v případě infikace malwarem/ransomwarem?

    - Ano.

    Odpověď udává, že na úřadu jsou vypracovány interní dokumenty, které popisují postupy v případě infikace malwarem nebo ransomwarem. Důležité je, aby tyto dokumenty byly pravidelně aktualizovány a zaměstnanci byli řádně školeni v jejich používání.

6. Myslíte si, že je městský úřad dostatečně připraven čelit kybernetickým hrozbám i v budoucnosti?

    - Ne. Jedná se neustálý proces, reagující na aktuální hrozby.

    Z odpovědi vyplývá, že respondent považuje tuto oblast za neustále se měnící a z praxe většinou vyplívá, že kyberzločinci mají co se týká nových technologií a postupů vždy navrch. Tato oblast vyžaduje pružnou reakci na aktuální hrozby. To naznačuje, že úřad možná bude v budoucnu potřebovat investovat do dalších opatření a zlepšení, aby lépe reagoval na stále se měnící kybernetické hrozby.

7. Jaké jsou podle Vás obvyklé motivace za útoky ransomwarem na veřejné instituce, jako je městský úřad?

    - Finance či informace.

    Odpověď poukazuje na to, že obvyklé motivace za útoky na veřejné instituce jsou primárně finanční zisk a získání citlivých informací. Útočníci mohou chtít buď přímo získat peníze od úřadu nebo využít šifrovaná data k vydírání za účelem získání finančního prospěchu nebo získání citlivých informací.

8. Jaké jsou klíčové prvky plánu obnovy po útoku ransomwarem a jakým způsobem by městský úřad měl tuto oblast zahrnout do svých bezpečnostních opatření?

    - Jednotlivé postupy v rámci plánu obnovy jsou zakomponovány do strategických dokumentů.

    Z této odpovědi vyplývá, že klíčové prvky plánu obnovy po útoku ransomwarem jsou zakomponovány do strategických dokumentů úřadu. To naznačuje, že městský úřad má strukturovaný plán, který obsahuje konkrétní postupy a opatření, která by měla být provedena v případě útoku ransomwarem. Tyto postupy mohou zahrnovat opatření k obnově dat, obnovení systémů a aplikací, komunikaci s dotčenými stranami a další důležité kroky pro minimalizaci dopadů útoku.

9. Setkal se Váš úřad někdy v minulosti s kybernetickým útokem typu ransomware?

    - Naštěstí ne.

    Pozitivní zprávou je, že úřad se v minulosti ještě nesetkal s kybernetickým útokem typu ransomware. Toto naznačuje, že úřad měl štěstí, že nebyl dosud obětí takového

útoku. Důležité je si uvědomit, že absence minulých útoků neznamená, že neexistuje riziko budoucích rizik. Městský úřad by měl nadále zůstat obezřetný a pokračovat v posilování svých kybernetických obranných mechanismů a připravenosti na případné útoky v budoucnosti.

10. Jakými způsoby může městský úřad spolupracovat s jinými institucemi a organizacemi na ochraně před ransomwarem a sdílení informací o těchto hrozbách?

    - Neocenitelná je výměna informací, ať už o způsobu provedení útoku, tak i o způsobu řešení konkrétní situace.

    Respondent považuje výměnu informací s jinými institucemi a organizacemi za klíčový prvek v ochraně před ransomwarem. Tento přístup naznačuje, že úřad uznává důležitost spolupráce a sdílení znalostí a zkušeností s dalšími subjekty v oblasti kybernetické bezpečnosti.

11. Spolupracuje městský úřad s externími dodavateli softwaru a služeb na zajištění bezpečnosti systémů a aplikací před ransomware útoky?

    - Ano.

    Městský úřad spolupracuje s externími dodavateli softwaru a služeb na zajištění bezpečnosti systémů a aplikací před ransomware útoky. Tato spolupráce ukazuje důležitost využití specializovaných technologií a služeb od externích dodavatelů k posílení své kybernetické obrany. Úřad by měl nadále spolupracovat s těmito dodavateli a využívat jejich odborné znalosti a zkušenosti k identifikaci a odvrácení kybernetických hrozeb. Je důležité, aby úřad pečlivě vybíral své dodavatele a udržoval s nimi pravidelný dialog a aktualizace, aby zajistil nejvyšší možnou úroveň bezpečnosti svých systémů a aplikací.

12. Jaké technické nástroje a software jsou nezbytné pro detekci, prevenci a reakci na ransomware útoky na městský úřad?

    - Na tuto otázku záměrně neodpovím.

    Respondent se rozhodl nezodpovědět otázku o konkrétních technických nástrojích a softwaru nezbytných pro detekci, prevenci a reakci na ransomware útoky. Toto může být způsobeno různými důvody, jako je například obava z možného odkrytí

interních postupů nebo technologií, ochrana citlivých informací nebo snaha o zachování bezpečnostních opatření.

13. Myslíte si, že nové technologie, jako je umělá inteligence a strojové učení mohou pomoci městskému úřadu v prevenci a detekci ransomware útoků?

    - Doufáme v to. Tyto technologie pomáhají útočníkům, tak by mohly snad pomoci i s obranou. Prozatím jsme to ale nevyzkoušeli.

    Respondent uvádí že vidí potenciál v nových technologiích, jako je umělá inteligence a strojové učení, v prevenci a detekci ransomware útoků. Existuje možnost toho, že tyto technologie mohou být užitečné pro posílení kybernetické obrany. Nicméně, zároveň je zde uvedeno, že úřad zatím tyto technologie nevyzkoušel, což znamená, že dosud nemá konkrétní zkušenost s jejich použitím v praxi.

14. Přijal městský úřad vzhledem k stále narůstajícímu počtu kybernetických útoků v ČR v tomto roce nějaká nová softwarová opatření nebo doporučení například ze strany NÚKIBU?

    - V tomto roce plánujeme zavést další z technologií a postupů k posílení zabezpečení vůči kybernetickým útokům. Konkrétní záměrně nebudu.

    Z odpovědi vyplývá, že městský úřad plánuje v tomto roce zavést další technologie a postupy k posílení zabezpečení proti kybernetickým útokům. Nicméně, konkrétní detaily těchto plánovaných opatření nebyly sděleny z důvodu bezpečnosti.

15. Monitoruje Vaše oddělení situaci ohledně kybernetických hrozeb v ČR nebo se tímto odvětvím nezabýváte?

    - Ano, sledujeme aktuální vývoj.

    Oddělení monitoruje situaci ohledně kybernetických hrozeb v České republice a sleduje aktuální vývoj v tomto odvětví. To naznačuje, že je důležité mít povědomí o kybernetických hrozbách v oblasti kybernetické bezpečnosti. Sledování aktuálního vývoje může pomoci včasné identifikaci nových hrozeb a přijetí odpovídajících opatření k ochraně před kybernetickými útoky.

16. Měl by podle Vás městský úřad komunikovat s veřejností v případě úspěšného ransomware útoku? Pokud ano, jak by měl řídit mediální obraz a krizovou komunikaci?

    - Hovořím za sebe, ne za úřad. Dle mého by měl úřad k veřejnosti komunikovat o tom, co proběhlo, jaké byly napáchány škody a kdy je předpoklad opětovného zprovoznění služeb.

    Podle respondentova názoru by bylo vhodné komunikovat s veřejností v případě úspěšného ransomware útoku. Komunikace by měla zahrnovat informace o tom, co se stalo, jaké škody byly způsobeny a odhadovaný časový rámec pro obnovení provozu služeb. To je důležité pro udržení transparentnosti a důvěryhodnosti úřadu vůči veřejnosti.

17. Máte povědomí, o čem pojednává nová směrnici EU, o kybernetické bezpečnosti „NIS2“, která má vyjít v platnost v roce 2025 a jakých okruhů se týká? Pokud ano, plánuje se úřad na tyto změny dopředu připravit?

    - Ano, zabýváme se i touto směrnicí, podstatné je pro nás, jak se směrnice EU promítnou do naší legislativy.

    Z odpovědi je zřejmé, že úřad má povědomí o nové směrnici EU o kybernetické bezpečnosti nazvané „NIS2“, která má být zavedena v roce 2025. Směrnice se týká regulace v oblasti kybernetické bezpečnosti a může mít vliv na právní rámec a požadavky týkající se kybernetické bezpečnosti pro úřady a organizace v České republice. Plánování a příprava na tyto změny je důležitá, protože nová směrnice může vyžadovat úpravu interních postupů, politik a technických opatření pro zajištění souladu s novými požadavky. Úřad by měl provést analýzu dopadů a zhodnotit, jaké kroky jsou nezbytné k dosažení souladu s novou legislativou. To zahrnuje nejen úpravu procesů a procedur, ale také investici do technologií a školení zaměstnanců.

5.2 SWOT analýza

SWOT analýza je nástroj pro systematické hodnocení silných stránek, slabých stránek, příležitostí a hrozeb, které ovlivňují subjekt, firmu či organizaci. Tento analytický framework umožňuje podrobně prozkoumat interní faktory, jako jsou vlastní zdroje, schopnosti a omezení, stejně jako externí faktory, jako jsou tržní trendy, konkurence

a regulace. Používá se k identifikaci klíčových oblastí, které je třeba posílit, a k zvážení možných strategií pro růst a úspěch. Následující SWOT analýza je zaměřena na zhodnocení vnitřního a vnějšího prostředí subjektu aby poskytla ucelený pohled na jeho současnou pozici a budoucí perspektivu.

Tabulka 2 SWOT analýza. Zdroj: (vlastní)

SWOT analýza		
Vnitřní prostředí	**Silné stránky**	**Slabé stránky**
	Pravidelné školení zaměstnanců	Nezkušenost s ransomware útokem
	Počet odborníků na více oblastí	Neflexibilita veřejné instituce
	Proaktivní přístup k bezpečnosti	Omezené finanční zdroje
	Spolupráce s externími subjekty	Zákonem daná opatření
	Zájem o nové technologie	Implementace nařízení EU
Vnější prostředí	**Příležitosti**	**Hrozby**
	Implementace nových technologií	Podcenění nebezpečí
	Robustnější zabezpečení subjektu	Nedbalá správa systémů
	Hlubší spolupráce s externisty	Selhání zaměstnanců
	Účast na seminářích a konferencích	Nové formy ransomwaru
	Doporučení ze strany NÚKIBU	Ztráta triády CIA

5.2.1 Silné stránky

Z výše uvedených silných stránek městského úřadu vyplývá, že subjekt disponuje dobrými zdroji a strategiemi, které mu umožňují efektivně reagovat na výzvy a příležitosti ve svém prostředí. Pravidelné školení zaměstnanců podporuje neustálý růst jejich odborných schopností a znalostí, což zvyšuje bezpečnost celého úřadu. Počet odborníků pokrývajících různé oblasti je zárukou komplexního a kvalitního systému obrany, neboť umožňuje úřadu reagovat na širokou škálu požadavků. Proaktivní přístup k bezpečnosti signalizuje, že městský úřad bere ochranu svých dat a infrastruktury vážně, což posiluje důvěru občanů a dalších zúčastněných subjektů v jeho činnost. Spolupráce s externími subjekty poskytuje

možnost sdílení informací a zkušeností a umožňuje využít synergie mezi různými organizacemi pro dosažení společných cílů. Zájem o nové technologie dokládá, že městský úřad je ochoten a schopen inovovat a využívat moderní technologické nástroje ke zlepšení efektivity a kvality svých služeb. Tím se zvyšuje připravenost na budoucí výzvy.

5.2.2 Slabé stránky

Nezkušenost s ransomware útokem může znamenat jen teoretické znalosti, nikoliv praktické, jak postupovat v případě výskytu tohoto viru což může mít vážné důsledky pro bezpečnost a provoz úřadu. Neflexibilita veřejné instituce může vést k obtížím při přijímání rychlých rozhodnutí, což může brzdit reakci při výskytu ransomwaru. Omezené finanční zdroje mohou snížit možnosti investic do rozvoje infrastruktury a poskytování služeb, což může zpomalit růst a inovace v rámci úřadu. Zákonem daná opatření a implementace nařízení EU mohou vytvářet administrativní zátěž a omezovat flexibilitu a autonomii městského úřadu při rozhodování a provádění politik a programů. Tyto slabé stránky naznačují potřebu zlepšení ve smyslu připravenosti na kybernetické hrozby, zvýšení flexibility a schopnosti reagovat na měnící se podmínky, a hledání způsobů, jak efektivněji využít dostupné finanční zdroje a zvládat administrativní výzvy spojené s legislativou.

5.2.3 Příležitosti

Příležitosti naznačují několik klíčových oblastí, které mohou městskému úřadu pomoci v jeho rozvoji a posílení jeho schopnosti reagovat na současné výzvy a budoucí potřeby. Implementace nových technologií představuje možnost využít moderního digitálního prostředí k zefektivnění procesů a zlepšení obranyschopnosti celé infrastruktury úřadu. Robustnější zabezpečení subjektu umožňuje vytvoření více vrstev k posílení ochrany proti kybernetickým hrozbám, což je klíčové v době, kdy digitální bezpečnost hraje stále důležitější roli. Hlubší spolupráce s externisty otevírá možnosti sdílení zkušeností, zdrojů a know-how s externími partnery, což může vést k novým inovacím a synergickým projektům. Účast na seminářích a konferencích nabízí příležitost k neustálému vzdělávání a získávání nových informací o aktuálních trendech a nejlepších postupech v oboru, což může podpořit profesionální rozvoj. Doporučení ze strany NÚKIBU mohou poskytnout podněty pro zlepšení kybernetické bezpečnosti městského úřadu.

5.2.4 Hrozby

Hrozby mohou být v extrémních případech likvidační pro danou instituci nebo subjekt. Podcenění nebezpečí signalizuje možnost nedostatečného vnímání potenciálních hrozeb a nedostatečného připravení na krizové situace, což může zvýšit riziko nežádoucích událostí a ztráty dat. Nedbalá správa systémů představuje riziko pro kybernetickou bezpečnost, protože zanedbání správy a údržby informačních systémů může vést k zranitelnostem a útokům ze strany kybernetických útočníků. Selhání zaměstnanců může být důsledkem nedostatečného školení, nekompetentnosti, úmyslného nebo neúmyslného chování, což může vést k úniku citlivých informací, narušení integrity dat nebo dalším bezpečnostním incidentům. Nové formy ransomwaru představují stále se vyvíjející hrozbu pro kybernetickou bezpečnost, která může městský úřad ohrozit šifrováním dat a vydíráním za jejich obnovení, což může mít značné finanční a provozní dopady. Ztráta triády CIA může nastat v důsledku úspěšného kybernetického útoku, který ohrožuje důvěrnost, integritu nebo dostupnost dat a služeb městského úřadu, což může vést k vážným následkům pro jeho fungování a důvěryhodnost.

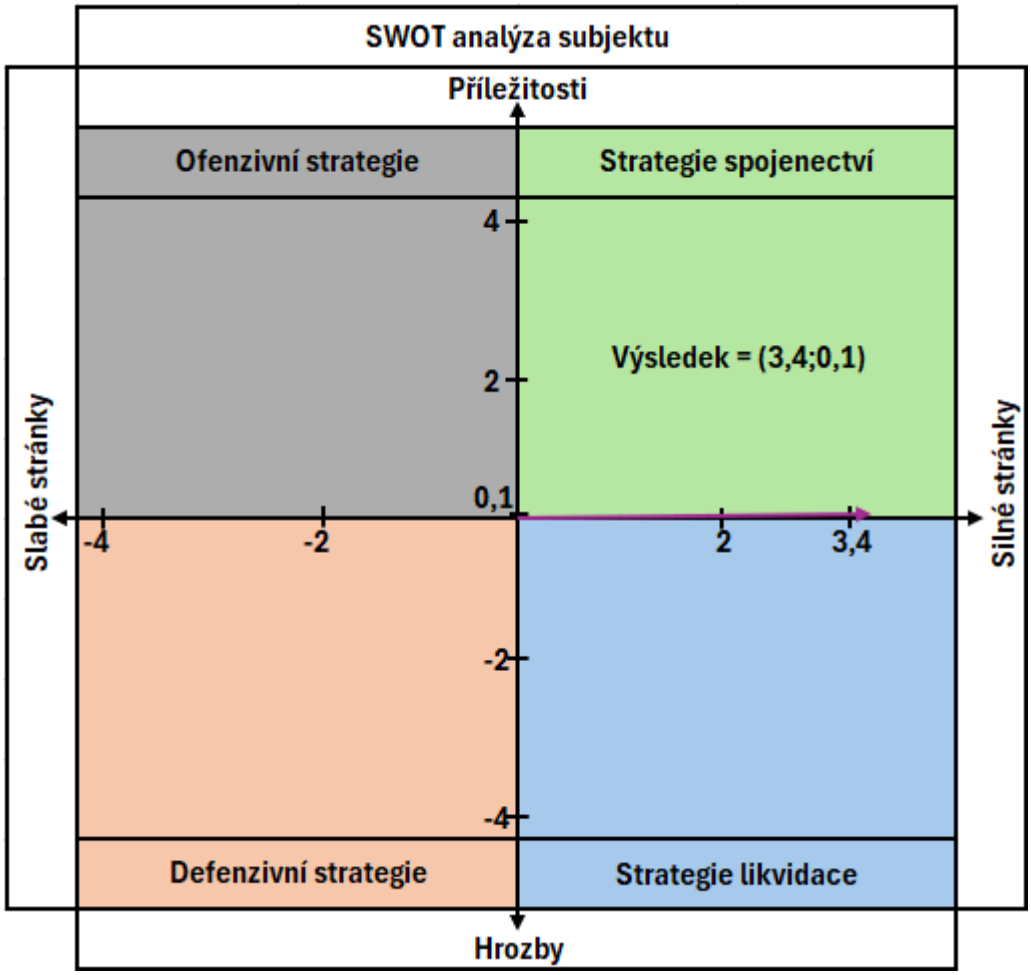
5.3 Vyhodnocení SWOT analýzy

Vyhodnocení SWOT analýzy je klíčovým krokem, který pomáhá identifikovat hlavní zjištění a strategické směry na základě analýzy silných stránek, slabých stránek, příležitostí a hrozeb. Jednotlivé složky jsou hodnoceny pomocí váhy v rozmezí mezi 1 až 10, přičemž se zaměřují na pozitivní aspekty jako silné stránky a příležitosti. Slabé stránky a hrozby jsou naopak hodnoceny v rozsahu mezi -1 až -10. Každá složka má své přiřazené hodnocení a součet těchto vah musí být roven 1. Výsledné skóre je získáno násobením váhy daného faktoru s jeho hodnocením a je zaznamenáno ve sloupci "Výsledný součin". Celková strategie je pak získána součtem hodnot vnitřního a vnějšího prostředí. Dle níže uvedeného schématu, strategie vyplívající ze SWOT analýzy udává, že výsledek analýzy vnějšího a vnitřního prostředí se pohybuje v rozmezí prvního kvadrantu. Tento kvadrant reprezentuje strategii spojenectví, kdy subjekt využívá své silné stránky k dosažení stanovených cílů.

Tabulka 3 SWOT analýza – hodnocení složek. Zdroj: (vlastní)

Typ	Složka	Váha	Hodnocení	Výsledný součin	Výsledný součet
Silné stránky	Pravidelné školení zaměstnanců	9	0,3	2,7	8,5
	Počet odborníků na více oblastí	7	0,2	1,4	
	Proaktivní přístup k bezpečnosti	8	0,1	0,8	
	Spolupráce s externími subjekty	6	0,1	0,6	
	Zájem o nové technologie	10	0,3	3	
Slabé stránky	Nezkušenost s ransomware útokem	-5	0,3	-1,5	-5,1
	Neflexibilita veřejné instituce	-6	0,2	-1,2	
	Omezené finanční zdroje	-7	0,2	-1,4	
	Zákonem daná opatření	-5	0,1	-0,5	
	Implementace nařízení EU	-5	0,1	-0,5	
Příležitosti	Implementace nových technologií	10	0,4	4	8,5
	Robustnější zabezpečení subjektu	8	0,2	1,6	
	Hlubší spolupráce s externisty	7	0,1	0,7	
	Účast na seminářích a konferencích	7	0,2	1,4	
	Doporučení ze strany NÚKIBU	8	0,1	0,8	
Hrozby	Podcenění nebezpečí	-7	0,1	-0,7	-8,4
	Nedbalá správa systémů	-7	0,1	-0,7	
	Selhání zaměstnanců	-9	0,3	-2,7	
	Nové typy ransomwaru	-9	0,3	-2,7	
	Ztráta triády CIA	-8	0,2	-1,6	
Vnitřní prostředí		3,4			
Vnější prostředí		0,1			

Z analýzy vyplývá, že subjekt má dobrou východní pozici a nachází se v pozitivní situaci, jelikož silné stránky převažují nad slabými a zároveň existují i příležitosti, kterých může subjekt využít. To umožňuje se úřadu zaměřit na strategii spojenectví, kdy využije své silné stránky k dosažení cílů ve spolupráci s externími partnery.



Obrázek 5 Graf SWOT analýzy. Zdroj: (vlastní)

5.4 Návrh strategie spojenectví pro subjekt

Strategie spojenectví ve SWOT analýze odkazuje na možnosti využití externích partnerů, aby se zvýšila konkurenceschopnost a úspěšnost organizace nebo veřejné instituce. Tato strategie se zaměřuje na využití silných stránek externích subjektů, jako jsou dodavatelé, distributoři nebo dokonce konkurenti, ke zlepšení vlastní situace. Strategie spojenectví může poskytnout organizaci konkurenční výhodu tím, že umožní efektivnější využití zdrojů a posílení tržního postavení prostřednictvím synergických vztahů s externími partnery.

K výše zmíněné strategii, sedí především využití silných stránek a příležitostí. Toho bylo dosaženo díky kontinuálnímu vzdělávání personálu, který si udržuje nejnovější znalosti

a dovednosti. Městský úřad tak může lépe reagovat na měnící se požadavky a výzvy. Široká škála znalostí a zkušeností v rámci týmu umožňuje úřadu komplexně řešit i složité problémy a nacházet inovativní řešení. Vzájemná spolupráce a sdílení poznatků mezi experty vedou k efektivnějšímu a rychlejšímu dosažení cílů. Městský úřad se aktivně snaží předcházet kybernetickým útokům a dalším bezpečnostním hrozbám, čímž chrání důležitá data a své systémy. Implementace preventivních opatření a osvědčených postupů minimalizuje rizika a zajišťuje stabilní a bezpečný provoz úřadu.

Návrhy

- Strategické partnerství s externími organizacemi, jako jsou univerzity, výzkumná centra a soukromé firmy by mělo být v povědomí odpovědných osob, které na úřadu pracují. To by umožnilo úřadu sdílet informace, čerpat z jejich expertízy a učit se z osvědčených postupů. Tento přístup by vedl k efektivnějšímu řešení problémů a zavádění inovací.
- Navázání kontaktu s odborníky v daném oboru v době krize, vytvoření efektivního a srozumitelného systému pro zvládání krizových situací, inspirace z postupů ostatních subjektů a aktivní snaha o sjednocení postupů.
- Využití doporučení Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB) může vést k výraznému posílení kybernetické bezpečnosti úřadu. NÚKIB poskytuje odborné rady a konzultace v oblasti kybernetické bezpečnosti a pomáhá organizacím implementovat efektivní bezpečnostní opatření.
- Není prakticky možné eliminovat všechny hrozby a slabé stránky. Naopak není z finančních důvodů ani možné využít všechny příležitosti, které jsou navrženy. Je důležité dát prostor a šanci novým příležitostem a uznat, že existují různé přístupy k jejich využití. Nepochybně jsou již na úřadu zavedeny jisté postupy, které vycházejí z nejlepšího přesvědčení osob, které se na jejich implementaci podílejí.

5.5 Metoda What – if

Metoda What – if je systematický přístup k analýze a plánování, který se používá k posouzení různých scénářů a jejich potenciálních dopadů na rozhodování. Základní princip metody spočívá v tom, že se lidé ptají na otázky typu "Co kdyby..." a poté zkoumají různé možné scénáře a jejich důsledky. Tímto způsobem je možné identifikovat potenciální rizika, příležitosti nebo nečekané události, které by mohly ovlivnit jejich cíle. Metoda What – if je

užitečný nástroj pro řízení rizik, strategických plánování a podporu inovací a kreativity. Je flexibilní a může být použita v mnoha různých kontextech, jako je například podnikání, vědecký výzkum, projektový management nebo krizové plánování. Použití této metody umožňuje předcházet neočekávaným událostem a překvapením a pomáhá lidem připravit se na nejistotu a zlepšuje schopnost rychle reagovat na změny.

Tabulka 4 Metoda What – if. Zdroj: (vlastní)

Číslo	Problém	Dopad	Návrh opatření
1	Co kdyby vznikl nedostatek financování?	Nutnost implementace starších nebo levnějších technologií, snížení stavu personálu.	Minimalizace nákladů, zajištění dotací, najít nové možnosti získání prostředků.
2	Co kdyby úředníci městského úřadu otevřeli podezřelý e-mail, obsahující ransomware?	Prověření, zda se ransomwaru podařilo prolomit ochranu, zjištění o jaký typ se jedná, přijmout adekvátní řešení pro danou situaci.	Poskytnout pravidelné školení zaměstnanců ohledně bezpečnosti informací, včetně identifikace podezřelých e-mailů a příloh. Zjištění, zda už neexistuje zdarma řešení pro odblokování konkrétního typu ransomwaru např. pomocí stránky nomoreransom.org.
3	Co kdyby se ransomware úspěšně dostal do systému a zašifroval důležité soubory a dokumenty?	Přerušení činnosti úřadu, nutnost spolupracovat s externími odborníky, ztráta citlivých informací, možná finanční újma.	Implementovat nové technologie, mít vytvořené zálohy, citlivé údaje by měli být odděleny od primární infrastruktury, revidovat systém zabezpečení. Využití stránky nomoreransom.org pro zjištění, zda konkrétní typ ransomwaru už nebyl prolomený.
4	Co kdyby byl městský úřad nucen zaplatit výkupné?	Finanční ztráta, možná podpora kriminálních aktivit, reputační ztráta a riziko, že data nebudou vráceny, nezveřejněny nebo odblokovány i po zaplacení výkupného.	Snažit se problém vyřešit bez nutnosti výkupné zaplatit, informovat NÚKIB, spolupracovat se subjekty zabývající se vytvářením bezpečnostního softwaru.

Číslo	Problém	Dopad	Návrh opatření
5	Co kdybychom odmítli platit výkupné a rozhodli se pro obnovu dat ze zálohy?	Následky by mohly zahrnovat časovou prodlevu, ztrátu nedostatečně aktualizovaných záloh, dodatečné náklady na obnovu, narušení provozu úřadu a riziko prodeje citlivých dat na černém trhu.	Zajišťovat pravidelný stav záloh, šifrovat důležité a utajené informace, provozovat tyto údaje na oddělených účtech.
6	Co kdybychom zaplatili výkupné, ale útočníci nám data nevrátili?	Finanční ztráta a navíc ztráta dat, riziko přilákání dalšího ransomware útoku, v horších případech může být dopad likvidační pro podnik. I při zaplacení může vzniknout problém, že obdržíme špatný klíč nebo že soubory budou poškozené.	Zvážit zda je opravdu nutné výkupné zaplatit. V 50 % případů se podaří data získat bez zaplacení, odpovědět si na otázky jako „nemůžeme obnovit data ze zálohy?, jak rychle potřebujeme naše data obnovit?, bude pro nás likvidační pokud data nezískáme zpátky?, je etické zaplatit výkupné?“. Kontaktovat příslušné úřady, zvážit profesionální pomoc.
7	Co kdyby útočníci vydali výhružky na veřejném fóru nebo sociálních médiích?	Panika veřejnosti, ztráta důvěry v městský úřad, šíření dezinformací a poškození pověsti města.	Proaktivní přístup města vydáním stanoviska o situaci pro veřejnost, zjištění stavu ochrany, spolupráce s externími subjekty.
8	Co kdyby útočníci získali citlivé informace během útoku?	Porušení ochrany osobních údajů, možné pokuty a soudní žaloby, ztráta důvěryhodnosti a riziko prodeje citlivých dat na černém trhu.	Zjistit o jaké údaje se jedná, pravidelně zálohovat důležitá data a informace na externí úložiště mimo síť, navázání spolupráce s kybernetickými bezpečnostními experty, šifrovat data.
9	Co kdyby se našla zranitelnost v operačním systému?	Zranitelnost systému, útočníci mohou využít k instalaci škodlivého softwaru, jako je ransomware, finanční ztráty, ztráta důvěryhodnosti.	Pravidelně aktualizovat antivirový software, firewall a další bezpečnostní nástroje a softwarové aktualizace, aby byla minimalizována zranitelnost systému vůči ransomwaru.

Číslo	Problém	Dopad	Návrh opatření
10	Co kdybychom se setkali s novým typ ransomwaru?	Zpochybnění stávajících opatření, zvýšená finanční zátěž na prevenci, aktualizování plánu reakce na kybernetické incidenty.	Implementace systémů monitorování a detekce hrozeb, které mohou identifikovat podezřelou aktivitu a varovat před potenciálními útoky ransomwarem, aktualizovat bezpečnostní software, školení zaměstnanců.

5.6 Hrozby pro vybraný subjekt

Hrozby, zmíněné ve SWOT analýze, nezahrnují výčet všech možných nebezpečí pro subjekt. Toto je přehled dalších z nich:

- Útočníci se mohou zaměřovat na systémy prvků kritické infrastruktury, které jsou pro chod města naprosto nezbytné, jako jsou systémy pro distribuci vody a energie. Napadení těchto systémů může vést k rozsáhlým výpadkům a značným škodám.
- Dvojité vydírání nám říká, že kromě požadavku na výkupné za dešifrování dat útočníci zneužívají ukradená data k dalšímu vydírání obětí. Mohou například zveřejnit citlivé informace nebo je prodat na černém trhu.
- Útočníci aktivně vyhledávají a zneužívají zranitelnosti v softwaru a systémech veřejných institucí k proniknutí do jejich sítí a nasazení ransomwaru a taktéž rozesílají phishingové e-maily s nakaženými přílohami nebo odkazy, které osoby lákají k otevření a spuštění ransomwaru v jejich zařízeních.
- Požadavky na zaplacení výkupného se neustále zvyšují a můžou se pohybovat v částkách, které většina veřejných institucí nebude schopná ze svých zdrojů pokrýt.

Hrozby, zmíněné v kapitole pro metodu What – if nastiňují jakým problémům může úřad čelit a jaké scénáře se mohou vyskytnout. Dopad reflektuje, jak se dané hrozby projevují a jaké jsou následky. Návrh opatření nám udává, jak by se v dané situaci mohlo postupovat a jaké kroky by měli být podniknuty.

ZÁVĚR

V této bakalářské práci byla řešena problematika hrozby Ransomware v prostředí ochrany obyvatelstva.

Z této práce vyplývá, že ochrana obyvatelstva před ransomwarem vyžaduje komplexní přístup, který zahrnuje technologická opatření, prevenci, vzdělávání a spolupráci. Analýza současné situace ukazuje, že ransomware útoky jsou stále sofistikovanější a rozmanitější, s cílem maximalizovat zisky pro útočníky a způsobit maximální škody obětem. Zároveň je zřejmé, že tato hrozba není omezena na jednotlivé země či sektory, ale má globální charakter, což vyžaduje mezinárodní spolupráci a koordinaci v boji proti ní.

SWOT analýza práce nám udává, že strategie, které by se měl úřad držet, je strategie spojenectví. Analýza odkazuje na možnosti využití externích partnerů, aby se zvýšila konkurenceschopnost a úspěšnost organizace nebo veřejné instituce. Tato strategie se zaměřuje na využití silných stránek externích subjektů ke zlepšení vlastní situace. Strategie spojenectví může přinést organizaci konkurenční výhodu tím, že umožní lepší využití zdrojů a posílení pozice na trhu díky synergickým vztahům s vnějšími partnery.

V tomto případě, subjekt dosahuje těchto závěrů, jak sám zmiňuje odpovědný pracovník, pomocí pravidelného školení zaměstnanců, kdy termín školení se odvíjí od aktuálnosti hrozeb anebo nových témat, které je potřeba probrat. Aktivní přístup, motivovaní pracovníci a zájem o nové technologie hrají také důležitou roli, zájem o téma kterému se profesně věnují znamená, že se sami budou učit a získávat nové poznatky, postupy a strategie. Doplnění o konference, které pro ně zařizuje úřad, jsou také nedílnou součástí získání nových obzorů. Spolupráce s externími organizacemi, úřady nebo firmami je pro subjekt klíčová. Nejaktuálnější opatření, zprovoznění a pravidelná kontrola celého serverového systému je nezbytná pro plynulé fungování. Implementace nových technologií, ať už vlivem nařízení nebo dobrovolně, také ukazuje, že úřad prevenci před virem ransomware nepodceňuje. Vzhledem k povaze subjektu nebylo možné, ze strany odpovědného pracovníka, poskytnout odpovědi, které se týkají konkrétních softwarových bezpečnostních opatřeních, z důvodu bezpečnosti.

Výše zmíněné pozitivní stránky ovšem zahrnují velké úsilí, čas a finanční prostředky. Úřad musí i nadále v těchto bodech pokračovat a neměl by dojít do situace, kdy zůstane stát technologicky na místě.

Hrozby, které se dotýkají i tohoto úřadu, jsou například méně kvalifikovaný personál. Pokud úřad nebude schopný v budoucnu zajistit přijímání takto kvalifikovaného personálu, může se to projevit i v přijímaných opatřeních. Moderní a nové technologie stojí stále více peněz, je proto nutné, aby vedení úřadu zajišťovalo kapitál ve formě dotací, výběru daní a provádělo investice do své vlastní bezpečnosti a nenechalo oddělení kybernetické bezpečnosti podfinancované. Na úřadu je zřízeno několik desítek odborů a oddělení, ve kterých pracují nižší stovky lidí. Vzhledem k vysokému počtu osob, a tedy i vyšší možné míře lidského selhání je nutné, aby pracovníci, jak bylo zmíněno výše, procházeli stále alespoň základním "kurzem", kde jim bude sděleno co a jak dělat, na co si dát pozor a čemu se naopak vyvarovat. Podle odpovědí je zřejmé, že si tuto důležitost uvědomují i na městském úřadu a berou tuto oblast školení zaměstnanců vážně.

Otázky kladené v metodě what – if a jejich řešení se opírají o strategii spojenectví. Úřad, jelikož není sám o sobě tvůrcem ani vývojářem bezpečnostních opatřeních nebo postupů, přejímá tyto informace od specializovaných firem, národního úřadu pro kybernetickou a informační bezpečnost nebo skrz nařízení Evropské unie. Opatření, která se doporučují, jsou mít vytvořené zálohy, zajišťovat pravidelný stav záloh, citlivé údaje by měli být odděleny od primární infrastruktury serveru, šifrovat důležité a utajené informace, provozovat tyto údaje na oddělených účtech, pravidelně aktualizovat antivirový software, firewall a další bezpečnostní nástroje a softwarové aktualizace, aby byla zvýšená resilience systému vůči ransomwaru, implementace systémů monitorování a detekce hrozeb, které mohou identifikovat podezřelou aktivitu ještě v brzkém stádiu. Pokud se vyskytne nějaký bezpečností incident, městský úřad je povinen toto zjištění hlásit NÚKIBU. Při vážnějším problému se odborníci z tohoto úřad osobně začnou tímto incidentem zabývat a mohou kontaktovat i jiné firmy, které se v tomto prostředí pohybují.

Vzhledem k obsahu práce seznávám, že stanovené cíle byly naplněny.

SEZNAM POUŽITÉ LITERATURY

Datto2018_*StateOfTheChannel_RansomwareReport.* In: THORNTON, Katie. DATTO. Datto a Kasey company [online]. [cit. 2024-02-27], 2007. Dostupné z: https://www.datto.com/resource-downloads/Datto2018_StateOfTheChannel_RansomwareReport.pdf

ČESKÁ AGENTURA PRO STANDARDIZACI. *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Systémy managementu informační bezpečnosti – Požadavky*, 2023. Brusel: Škop.

ČESKÁ AGENTURA PRO STANDARDIZACI. *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Opatření informační bezpečnosti*, 2023. Brusel: Škop.

ESET. Co je to ransomware a jak se proti němu bránit? ESET.Progress.Protected. [online]. [cit. 2024-02-28], c1992 – 2024. Dostupné z: https://www.eset.com/cz/ransomware/

FAWKES, Guy. *Historie ransomware hrozeb: jak to bylo, je a bude*. VPNMENTOR. VpnMentor Keeping You Safe Online [online]. [cit. 2024-02-26], c2014-2024. Dostupné z: https://cs.vpnmentor.com/blog/historie-ransomware-hrozeb-minulost-soucasnost-budoucnost/#section-1

GRIMES, Roger A. *Ransomware protection playbook*. Hoboken, New Jersey: Wiley, 2021. ISBN 978-1-119-84912-4.

HSU, Frank a Dorothy MARINUCCI. *Advances in Cyber Security: Technology, Operations, and Experiences*. Lincoln: Fordham University Press, 2013. ISBN 978-0-8232-4459-1.

JIRÁSEK, Petr, Josef POŽÁR a Luděk NOVÁK, *Výkladový slovník kybernetické bezpečnosti*. [online]. 5. aktualiz. vyd. Praha: AFCEA, s. 69. [online], 2015. [cit. 03. 03. 2024]. Dostupné z: https://www.govcert.cz/download/slovnik/vykladovy_slovnik_KB_3_vydani.pdf

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

KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z. s. p. o., 2016. ISBN 978-80-88168-18-8.

MINISTERSTVO VNITRA ČR. *Koncepce boje proti trestné činnosti v oblasti informačních technologií.* [online]. [cit. 2023-12-31], 2000. Dostupné z:

https://www.mvcr.cz/volby/clanek/o-nas-bezpecnost-a-prevence-dokumenty-bezpecnost-a-prevence-dokumenty-kyberneticke-hrozby.aspx

MICROSOFT. *Co je ransomware?* MICROSOFT. Zabezpečení od Microsoftu [online]. [cit. 2023-12-31], c2023. Dostupné z: https://www.microsoft.com/cs-cz/security/business/security-101/what-is-ransomware

MAYER, Marco et al. *How would you define Cyberspace?* [Online, PDF], 2014. Mayer.NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Doporučení k používání protokolu TLP ke sdílení chráněných informací* [online]. [cit. 2024-04-23], 2022. Dostupné z: https://nukib.gov.cz/cs/infoservis/doporuceni/1862-doporuceni-k-pouzivani-protokolu-tlp-ke-sdileni-chranenych-informaci-2/

Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020 [Online], 2015. Národní centrum kybernetické bezpečnosti.

PALOALTONETWORKS. *What is Multi-Extortion Ransomware?* [online]. [cit. 2024-04-30], c2024. Dostupné z: https://www.paloaltonetworks.com/cyberpedia/what-is-multi-extortion-ransomware

PORTER, Evan. *Co je DDoS útok a jak mu zabránit v roce 2024* [online]. [cit. 2023-12-31], 2023. Dostupné z: https://cs.safetydetectives.com/blog/co-je-ddos-utok-a-jak-mu-zabranit/

PETERKA, Martin et al. *Historie ransomwaru*. CSIRT.CZ. LUPACZ [online]. [cit. 2023-12-31], 2017. Dostupné z: https://www.lupa.cz/clanky/historie-a-vyvoj-ransomwaru-vsechno-to-zacalo-s-aids/

SENTINELONE. Double extortion ransomware [online]. [cit. 2024-04-23], c2024. Dostupné z: https://www.sentinelone.com/cybersecurity-101/what-is-double-extortion/

SANDERS, Andrew. *Co je sociální inženýrství a proč je to hrozba v roce 2024?* [online]. [cit. 2023-12-31], 2023. Dostupné z: https://cs.safetydetectives.com/blog/co-je-socialni-inzenyrstvi-a-proc-je-to-takova-hrozba/

Směrnice Evropského parlamentu a Rady (EU) 2016/1148 *o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii* [Online], 2018. Úřad pro publikace Evropské unie.

ŠULC, Vladimír, 2018. *Kybernetická bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk. ISBN 978-80-7380-737-5.

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)*

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

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

Zákon č. 111/2019 Sb., *zákon, kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů*.

Zákon č. 181/2014 Sb., *o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)*

Zákon č. 412/2005 Sb., *o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů*

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

CIA	Confidentiality, Integrity, Availability
ČSN	Československé státní normy
DDoS	Distributed Denial-of-Service
EDR	Endpoint Detection and Response
EU	Evropská unie
ICT	Information and Communication Technologies
IEC	International Electrotechnical Commission
IT	Informační Technologie
ISO	International Organization for Standardization
KI	Kritická infrastruktura
KII	Kritická informační infrastruktura
NSA	National Security Agency
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
P/C	Possession/Control
PDF	Portable Document Format
RSA	Rivest, Shamir, Adleman
RaaS	Ransomware as a service
SCP	Security Control Pillars
TLP	Traffic Light Protocol
VIS	Významné informační systémy
VPN	Virtual Private Network

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: OTÁZKY EXPERTNÍHO ROZHOVORU

1. Jaká je Vaše pozice na městském úřadu?
2. Zabývají se kybernetickou bezpečností i jiné osoby na úřadu? Pokud ano, má každá osoba jinou oblast zaměření?
3. Účastníte se Vy jakožto odborník/ci na kybernetickou bezpečnost například konferencí nebo seminářů k prohloubení znalostí v této oblasti?
4. Probíhají pravidelná školení zaměstnanců úřadu k rozvoji identifikace kybernetických hrozeb? Pokud ano, jak často?
5. Jsou na úřadu vypracovány interní dokumenty, jak postupovat v případě infikace malwarem/ransomwarem?
6. Myslíte si, že je městský úřad dostatečně připraven čelit kybernetickým hrozbám i v budoucnosti?
7. Jaké jsou podle Vás obvyklé motivace za útoky ransomwarem na veřejné instituce, jako je městský úřad?
8. Jaké jsou klíčové prvky plánu obnovy po útoku ransomwarem a jakým způsobem by městský úřad měl tuto oblast zahrnout do svých bezpečnostních opatření?
9. Setkal se Váš úřad někdy v minulosti s kybernetickým útokem typu ransomware?
10. Jakými způsoby může městský úřad spolupracovat s jinými institucemi a organizacemi na ochraně před ransomwarem a sdílení informací o těchto hrozbách?
11. Spolupracuje městský úřad s externími dodavateli softwaru a služeb na zajištění bezpečnosti systémů a aplikací před ransomware útoky?
12. Jaké technické nástroje a software jsou nezbytné pro detekci, prevenci a reakci na ransomware útoky na městský úřad?
13. Myslíte si, že nové technologie, jako je umělá inteligence a strojové učení mohou pomoci městskému úřadu v prevenci a detekci ransomware útoků?
14. Přijal městský úřad vzhledem k stále narůstajícímu počtu kybernetických útoků v ČR v tomto roce nějaká nová softwarová opatření nebo doporučení například ze strany NÚKIBU? Pokud můžete uvést nějaký postup nebo opatření pro konkretizaci tak prosím uveďte.

15. Monitoruje Vaše oddělení situaci ohledně kybernetických hrozeb v ČR nebo se tímto odvětvím nezabýváte?
16. Měl by podle Vás městský úřad komunikovat s veřejností v případě úspěšného ransomware útoku? Pokud ano, jak by měl řídit mediální obraz a krizovou komunikaci?
17. Máte povědomí o čem pojednává nová směrnici EU o kybernetické bezpečnosti „NIS2“, která má vyjít v platnost v roce 2025 a jakých okruhů se týká? Pokud ano, plánuje se úřad na tyto změny dopředu připravit?