Kybernetické hrozby a ochrana v kyberprostoru

Štěpánka Čechová

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:	**Štěpánka Čechová**
Osobní číslo:	**L21356**
Studijní program:	**B1032A020002 Ochrana obyvatelstva**
Forma studia:	**Kombinovaná**
Téma práce:	**Kybernetické hrozby a ochrana v kyberprostoru**

Zásady pro vypracování

1. Vymezte základní pojmy a historický vývoj v předmětné oblasti.
2. Proveďte analýzu kybernetických hrozeb a následnou diskuzi nad jejími výsledky.
3. Na základě zjištěných dat navrhněte opatření pro prevenci a reakci proti těmto hrozbám.

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

Seznam doporučené literatury:

1. KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o., 2019. ISBN 978-80-88168-31-7.
2. SEGAL, Adam. *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*. New York: PublicAffairs, 2017. ISBN 978-1-61039-872-5.
3. ŠULC, Vladimír. *Kybernetická bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-737-5.

Další odborná literatura dle doporučení vedoucího bakalářské práce.

Vedoucí bakalářské práce: **Ing. Pavel Tomášek, 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: Štěpánka Čechová

.....
podpis studenta

ABSTRAKT

Tato bakalářská práce se zaměřuje na analýzu kybernetických hrozeb a navržení opatření k ochraně vybraných organizací v kyberprostoru. Práce začíná vymezením základních pojmů a genezí kybernetických hrozeb. Metodologie zahrnuje analýzu SWOT, analýzu rizik pomocí metodiky NÚKIB a podrobnou analýzu pomocí Fraud Risk Assessment. Pro identifikaci zranitelností a hodnocení aktiv CIA byla provedena komplexní analýza. K dalšímu zaměření návrhu opatření bylo provedeno dotazníkové šetření zaměřené na zálohování a ochranu dat. V závěru práce jsou prezentována doporučení a návrhy opatření pro organizace v oblasti kybernetické bezpečnosti. Výsledkem provedených opatření byla implementace kultury kybernetické bezpečnosti v těchto organizacích.

Klíčová slova: Analýza rizik, kybernetická bezpečnost, kybernetické hrozby

ABSTRACT

This bachelor thesis focuses on the analysis of cyber threats and proposes measures to protect selected organizations in cyberspace. The thesis begins by defining basic concepts and the genesis of cyber threats. The methodology includes SWOT analysis, risk analysis using the NUKIB methodology, and a detailed analysis using Fraud Risk Assessment. A comprehensive analysis was conducted to identify vulnerabilities and assess CIA assets. To further focus on the proposal of measures, a questionnaire survey focused on data protection backup was conducted. In conclusion, the thesis presents recommendations and measures for organizations in the field of cybersecurity. The result of the measures implemented was the establishment of a cybersecurity culture within these organizations.

Keywords: Cyber security, cyber threats, risk analysis

Tímto bych chtěla poděkovat vedoucímu mé bakalářské práce Ing. Pavlu Tomáškovi, Ph.D. za odborné rady, rychlé reakce a vedení práce.

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

OBSAH

ÚVOD

V dnešní době se stále více činností přesouvá do digitálního prostředí kyberprostoru, proto se ochrana před kybernetickými hrozbami dostává do popředí priorit jak jednotlivců, tak organizací. Typické kybernetické útoky, které známe už mnohá léta dostávají stále novou masku a útočníci hledají lepší způsoby k napadení. Řešení kybernetické bezpečnosti se pro mnohé stále zdá nedůležitá, ovšem do chvíle, kdy se také nestanou obětí jednoho z útoků.

"Kyberprostor významně mění všechny historické zkušenosti". Jde o oblast, kde nejistota roste a kde se státní autorita může stát nejasnou, což zvyšuje potřebu zabezpečení a prevence proti kybernetickým útokům (Segal, 2017).

V digitálním světě se potýkáme s neviditelnými hrozbami, proto je nutné dbát o ochranu aktiv komplexně. Aktiva se vyskytují v různých podobách, mohou jimi být datové systémy, hardware, software, lidské zdroje. Ochrana těchto aktiv je nutná z důvodu zachování integrity, důvěrnosti a dostupnosti (Friedrich Nietzsche , 2023).

Analýza kybernetických hrozeb byla provedena ve spolupráci se dvěma organizacemi, které se nachází v jedné obci: místní knihovna a obecní úřad. Organizace vyjádřily svůj požadavek se zachováním anonymity.

Práce se zaměřuje na problematiku kybernetických hrozeb a ochranu kyberprostoru. Teoretická část se bude věnovat vymezení základních pojmů z oblasti kyberprostoru, kybernetické bezpečnosti a kyberkriminality. Dále zde bude rozebrána geneze kybernetických hrozeb, historické aspekty a aktuální trendy v kyberkriminalitě.

Hlavní částí práce bude praktická část, kde bude provedena analýza a návrh opatření. Na začátku praktické části bude provedena analýza SWOT, která by měla pomoci organizacím identifikovat jejich silné a slabé stránky a nastavit SWOT strategii, ta by měla minimalizovat slabé stránky a hrozby. V práci bude využita metodika Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB) k ohodnocení primárních aktiv organizací pomocí hodnocení důvěrnosti (Confidentiality), integrity (Integrity) a dostupnosti (Availability) - CIA.

Další část práce se bude zabývat celkovou analýzou rizik, identifikací zranitelností a hrozeb. Analýza bude provedena podle postupů doporučených NÚKIB. Dále bude využita metodika Fraud Risk Assessment, kterou poskytla fakulta, aby se identifikovaly nejzávažnější rizika hrozící organizacím. Tato komplexní analýza pomůže lépe porozumět hrozbám, zranitelnostem a rizikům, se kterými se organizace potýkají v kybernetickém prostředí. Výsledkem práce by měl být návrh opatření a proti těmto hrozbám. Pro lepší zaměření tohoto

návrhu opatření a doporučení bylo vytvořeno dotazníkové šetření zaměřené na zálohování a ochranu dat. Výsledky dotazníku by měly odpovědět na otázky týkající zálohování, bezpečnosti dat.

V práci byla pro analýzu použita kvalitativní analýzu SWOT, kde byly identifikovány síly (Strenghts), slabosti (Weaknesses), Příležitosti (Opportunities) a hrozby (Threats). Další výzkumnou metodou byla kvalitativí metoda Fraud Risk Assessment. Pro identifikaci aktiv byl vytvořen řízený rozhovor, který naleznete v Příloze P X: Řízený rozhovor. Na závěr byla použita kvantitativní metoda dotazníkového šetření.

V analytické části bude úkolem vytvořit přehled o současném stavu kybernetických hrozeb a rizik v těchto organizacích a v návrhové části vytvořit konkrétní opatření a reakce na tyto hrozby. Dalšími dílčími úkoly bylo vymezení základních pojmů v této oblasti a geneze kybernetických hrozeb.

I. TEORETICKÁ ČÁST

1 KYBERPROSTOR

Kyberprostor, jakožto pojmový komplex s různými interpretacemi a významy, nám otevírá brány do digitálního světa, který prorůstá naší každodenní realitou. I když mnohé slovníky mohou definovat kyberprostor jako abstraktní virtuální sféru propojených informačních systémů, jeho skutečný význam a rozsah mohou být mnohem širší.

Tato kapitola se bude věnovat prostředí, ve kterém se kybernetické hrozby odehrávají. Na úvod by se pojem kyberprostor dal vyjádřit podle této definice:

„Kyberprostor si lze představit jako středověkou krajinu, která se skládá z nechráněných vesnic, opevněných hradišť, menších hrádků a hradů, a nakonec z velkých královských měst, která byla velmi dobře opevněna a střežena,“ (Zelinka, 2018).

Kyberprostor si lze představit mnoha způsoby. V současné chvíli neexistuje shoda na jedné ucelené definici, nicméně autoři vybrali jednu z definic, která by měla situaci objasnit: *“Kyberprostor je časově závislá sada propojených informačních systémů a lidských uživatelů, kteří s těmito systémy interagují,“* (Ottis, a další, 2010). Z takového pojetí lze pochopit, co se v kyberprostoru děje. Následující podkapitola bude hlouběji zkoumat tento základní termín a představí nám jeho bližší podobu.

1.1 Vymezení pojmu kyberprostor

Klíčovou roli ve zviditelnění tohoto pojmu ve veřejné sféře představuje dokument z roku 1996 *„Deklarace nezávislosti kyberprostoru,“* od Johna Perry Barlowa, po vydání se definice kyberprostoru stala široce známou. Tato deklarace zdůrazňuje, že národní vlády by neměly hrát žádnou roli v řízení kyberprostoru. John také argumentoval, že *„komunita v kyberprostoru by měla vytvořit svá vlastní pravidla a řešit konflikty nezávisle na zákonech a soudnictví jakéhokoli konkrétního státu. Důraz je kladen zejména na ochranu svobody projevu a výměny mezi „beztělesnými“ osobnostmi kyberprostoru. Tento pohled nabývá zvláštní relevance v případě možnosti skrýt fyzickou polohu a identitu osoby účastnící se aktivity v „kyberprostoru,“* (Barlow, 1996).

Slovník Oxford Dictionary uvádí cyberspace jako *„fiktivní prostředí, ve kterém dochází ke komunikaci skrze počítačové sítě,“* (Dictionary, (bez data)). Blíže uvádí Český Výkladový slovník kybernetické bezpečnosti definici kyberprostoru, *„Digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací.“* (Jirásek, a další, 2015). Nebo také *„Počítačová síť sestávající*

z celosvětové sítě počítačových sítí, které používají síťové protokoly TCP / IP k usnadnění přenosu a výměny dat," z anglického slovníku (Vocabulary, 2024).

Definice vyplývající ze zákona zní: *„kybernetický prostor jako digitální prostředí, umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy a sítěmi elektronických komunikací.*" Tato definice je teoreticky neměnná a aplikovatelná v jakémkoliv kontextu, což nám poskytuje jistotu a přesnost. Vychází ze „*zákona č. 181/2014 Sb. Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů kybernetické bezpečnost,"* (Epravo, 2024).

Jiným způsobem by se dalo říct, že kyberprostor je tím, co si z ně společnost vytvoří. Kdekoliv zúčastněné strany zakládají virtuální prostory, tam vidíme existenci kyberprostoru. Jakkoliv se využívá internetu, lze říct, že vytváří kyberprostor. Podle mnoha odborníků na informační technologie, včetně F. Randalla Farmera a Chipa Morningstara, získal kyberprostor popularitu jako prostředek sociální interakce, spíše než díky své technické exekuci a implementaci. Hnací silou kyberprostoru se tak stala společenská interakce na úkor jeho technických aspektů (Rouse, 2023).

Kyberprostor není jednotným prostorem, ale skládá se z mnoha dílčích prostorů nebo světů, z nichž každý má vlastní pravidla a zákonitosti. V každém z těchto prostředí je zkušenost formována odlišně, a má jiná pravidla ve srovnání s profesními světy a jinými prostředími (Dodge, a další, ©2021).

Další pojetí kyberprostoru podtrhuje jeho politickou a sociální moc. Jedná se o entitu, která umožňuje šíření kultury bez ohledu na hranice a současně využívá prostředí s omezeným právním regulováním (Lessig, 2006).

Kyberprostor je tak místem, kde se prolínají politické a sociální vlivy, což otevírá prostor pro nové formy interakce a sdílení informací. Jeho schopnost šířit se bez legislativních bariér může mít dopad na globální politiku a sociální dynamiku (Černý, 2020).

Jak chápat a využívat tento pojem, závisí spíše na nás a na kontextu, ve kterém se pohybujeme. Každá definice nám poskytuje jiný pohled na tuto složitou realitu.

1.2 Co tvoří kyberprostor

V předchozí podkapitole je uvedena teoretická podoba kyberprostoru a diskuse o jeho virtuálním nebo abstraktním charakteru. Následující odstavec se bude věnovat jeho fyzické podobě.

Jak bylo předesláno, kyberprostor není pouhým virtuálním konceptem, ale má svůj hmotný základ. Tento základ spočívá v síťové infrastruktuře, zahrnující fyzické prvky, jako jsou dráty, počítače, kabely, servery a routery. Tato infrastruktura poskytuje zázemí pro existenci kyberprostoru. Skutečným stavebním materiálem jsou však informace, které se projevují formou kódu. Kód je vyjádřen symboly, znaky nebo instrukcemi a je vázán na pravidla. Tvoří základní stavební kámen kyberprostoru, zejména ve formě binární reprezentace jedniček a nul (Schmidt, 2012).

Další možné rozdělení popisuje Koncept plánu schopností kybernetických operací 2016-2028, který kyberprostor rozděluje do tří vrstev – fyzické, logické a sociální.

V logické vrstvě je identifikována technická logická síťová složka, zahrnující propojení mezi jednotlivými uzly sítě. Jinak řečeno, v této vrstvě je struktura, která definuje logická spojení mezi různými body v síti. Fyzická vrstva kyberprostoru zahrnuje geografické a fyzické sítě. Geografická složka se vztahuje k reálné poloze prvků sítě, zatímco fyzická síťová složka zahrnuje veškeré hardwarové vybavení a infrastrukturu. Jinými slovy, tato vrstva se týká umístění a technického zázemí síťových prvků. Poslední sociální vrstva se zaměřuje na lidské a kognitivní aspekty. Tato část zahrnuje *„kyberosobnost“* a osobnostní složku, která obsahuje identifikaci a individuální charakteristiky jednotlivců působících na síti. To znamená, že se věnuje lidským a mentálním prvkům, včetně online identit a charakteristiky uživatelů (ARMY’S, 2010).

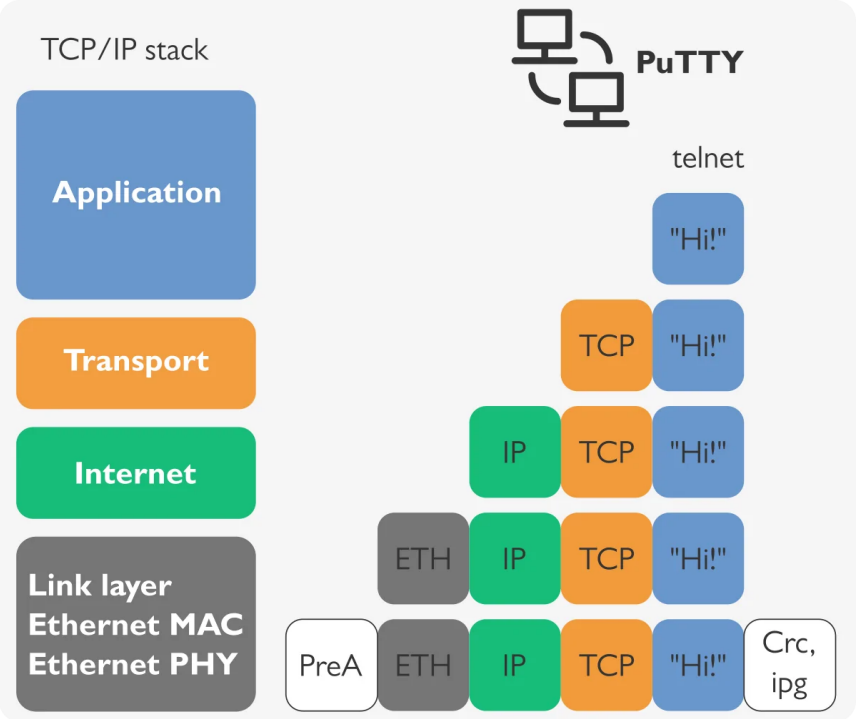
Kyberprostor není pouze abstraktním pojmem, ale má reálný vliv na fyzický svět a vzájemně ovlivňuje lidské myšlení a aktivity (Bastl, a další, 2013).

Transmission Control Protocol

Jinak také protokol řízení přenosu, je standard, který stanovuje postup pro inicializaci, udržování komunikace v síti a umožňující aplikacím vzájemnou výměnu dat (Lutkevich, a další, 2023).

Patří mezi hlavní protokoly internetové sady protokolů. Nachází se mezi aplikačními, síťovými vrstvami a slouží k poskytování spolehlivých doručovacích služeb. TCP spolupracuje s Internet Protocol (IP), který implementuje techniku odesílání datových paketů mezi počítači (GeeksforGeeks, 2020).

Obrázek, který bude následovat ilustruje proces přenosu dat pomocí protokolu TCP/IP nad Ethernetem na základě použití programu PuTTY. Zobrazuje, jak data putují od uživatele, přes různé vrstvy síťového modelu až k jejich cílovému zařízení (Xipera, 2020).



Obrázek 1- Ukázka provozu TCP/IP nad Ethernetem (Xiphera, ©2020)

Internet Protocol address

IP adresa je speciální číslo, které identifikuje zařízení na internetu nebo v místní síti. Zkratka "IP" znamená "internetový protokol" a označuje pravidla, která upravují, jak jsou data odesílána přes internet nebo místní síť.

IP adresy jsou důležité pro umožnění zařízením komunikovat ve síti, poskytují informace o poloze a umožňují vzájemnou interakci mezi zařízeními. Tyto adresy jsou nezbytné pro internet, který potřebuje způsob, jak rozlišit mezi počítači, směrovači a webovými stránkami. Celkově řečeno, IP adresy jsou klíčové pro fungování internetu a umožňují správné směrování a komunikaci mezi zařízeními v síti (Kaspersky, 2022).

Certifikát SSL

Tento certifikát slouží k zabezpečení komunikace přes protokol SSL, chrání před odposlechem a ověřuje identitu komunikujících stran. Zajišťuje šifrování dat přenášených mezi uživateli a webovými stránkami.

Proces fungování SSL certifikátu začíná tím, že když uživatel nebo webový server chce navštívit zabezpečenou webovou stránku, prohlížeč nebo server se pokusí připojit k této stránce, která je chráněna SSL certifikátem. Prohlížeč se pokusí připojit na stránku, požádá webový server o identifikaci. Webový server pošle prohlížeči kopii svého SLL certifikátu. Následně prohlížeč zkontroluje platnost SSL certifikátu a zda mu důvěřuje. Pokud je certifikát platný a prohlížeč mu důvěřuje, oznámí to webovému serveru. Webový server vrátí potvrzení o zahájení šifrované relace SLL. Poté jsou mezi webovým prohlížečem a serverem sdílena šifrovaná data (Švec, 2024).

Šifrování citlivých dat při přenosu poskytuje uživatelům jistotu v komunikaci. Webové stránky s SSL certifikátem jsou identifikovatelné díky začátku adresy https://, což zdůrazňuje bezpečnost a vylepšuje viditelnost ve vyhledávačích (Forpsi, 2020).

Většina uživatelů pravidelně využívá tuto oblast internetu, kde se nacházejí webové prezentace firem, portály veřejné správy, zpravodajské portály, blogy a části některých sociálních sítí (přestože ne všechny jsou indexovány a dostupné pro veřejnost).

1.2.1 Surface Web

Surface web, jinými slovy *„viditelný web“* představuje veřejně dostupnou část internetu, která zahrnuje webové stránky indexované vyhledávači a snadno přístupné prostřednictvím standardního webového prohlížeče. Většina uživatelů pravidelně využívá tuto oblast internetu, kde se nacházejí webové prezentace firem, portály veřejné správy, zpravodajské portály, blogy a části některých sociálních sítí (Cyberprotection, 2023).

1.2.2 Deep Web

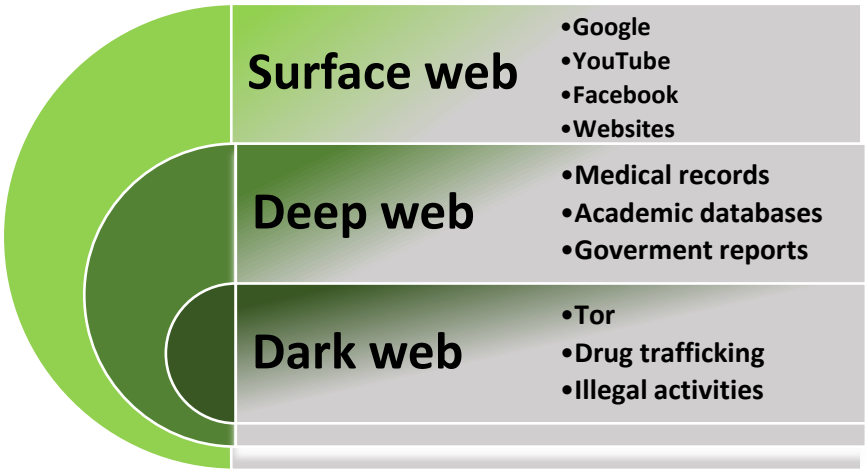
Jedná se o další vrstvou internetového prostoru. Tato vrstva už není dostupná standartními vyhledávači. Tato oblast zahrnuje obsah skrytý za přihlašovacími formuláři s nutností přihlašovacích údajů, veřejné databáze, které vyžadují specifické vyhledávací dotazy, a placený obsah v digitálních knihovnách, online časopisech a zpravodajských kanálech, vyžadující registraci a poplatek (Khelghati, a další, 2023).

1.2.3 Dark Web

Dark web reprezentuje nejhlubší vrstvu internetu, k níž lze přistupovat pouze prostřednictvím speciálního softwaru, například prohlížeče TOR (The Onion Router) (Řešetková, 2021).Na rozdíl od většiny obsahu na Deep webu, se Dark web zaměřuje na

nezákonné aktivity a služby. Tento prostor poskytuje anonymitu uživatelů, jelikož jejich identita je chráněna šifrovací technologií (Čihák, 2022).

Na obrázku jsou uvedeny příklady toho, co můžeme v jednotlivých webech najít.



Obrázek 2 - Ukázka příkladů z jednotlivých webů (zdroj: vlastní zpracování)

Nejčastěji vyhledávaná část internetu je Surface web, která je snadno dostupná pomocí běžných vyhledávačů. Jsou zde stránky, které využíváme denně. Deep web, na rozdíl od toho, obsahuje neindexované webové stránky, jako jsou firemní intranety nebo databáze chráněné heslem. K těmto stránkám se nedostaneme běžnými vyhledávači a vyžadují speciální přístupové údaje.

Nejtajnější částí internetu a obsahuje nelegální a anonymní obsah. Zahrnuje ilegální trhy, fóra hackerů a další podzemní aktivity. Přístup k Dark webu vyžaduje speciální software pro anonymní prohlížení.

2 KYBERNETICKÁ BEZPEČNOST

V moderní době, kdy počítače, internet a digitální technologie pronikly do všech oblastí našeho života, od komunikace a zábavy po dopravu, nakupování a medicínu, se kybernetická bezpečnost stala nezbytnou praxí. Specializuje se na ochranu systémů, sítí a programů před digitálními útoky s cílem odhalovat neoprávněný přístup, manipulaci a destrukci citlivých informací. Tato oblast také zahrnuje obranu před různými formami kybernetických útoků, jako jsou snahy o vydírání peněz pomocí ransomware nebo narušení běžných obchodních procesů (Siemens, 2023).

Kybernetická bezpečnost je klíčový prvek v digitálním prostředí, ve kterém je zaměřena na ochranu citlivých informací, udržení důvěrnosti dat, zjištění dostupnosti digitálních informací a prevenci kybernetických útoků (Cisco, 2022).

„*Kybernetická bezpečnost se týká každého z nás, kdo využívá jakékoliv prvky ICT ve svém každodenním životě,“* (Kolouch, a další, 2018).

S rostoucím počtem a dynamickým vývojem útočnických metod čelí kybernetická bezpečnost výzvám. Ochrana informačních technologií se stává klíčovým prvkem pro udržení integrity a dostupnosti dat (Kaspersky, 2019).

V současné digitalizované společnosti přinášejí pokročilé programy kybernetické obrany výhody pro jednotlivce, organizace a klíčovou infrastrukturu. Výzkumníci v oblasti kybernetického výzkumu hrají klíčovou roli při identifikaci nových hrozeb, zdokonalování nástrojů a šíření povědomí o klíčovosti kybernetické bezpečnosti. Jejich práce přispívá k vytváření bezpečnějšího prostředí pro všechny uživatele (CISA, 2021).

Mezi preventivní opatření patří např.:

- Softwarová ochrana sítí.
- Ochrana dat a informací.
- Zabezpečení databáze infrastruktury.
- Školené kybernetické bezpečnosti.
- Zálohování dat.
- Obnova dat po útoku.

Existuje rozmanitá paleta opatření, která jsou věnována oblasti kybernetické bezpečnosti, a tyto stránky jsou podrobně analyzovány v rámci informační bezpečnosti, jak bude podrobně

popsáno v následující podkapitole. Je však klíčové zdůraznit, že každý z těchto přístupů se soustředí na odlišné hlediska zabezpečení. Organizace a firmy, jež investují do bezpečnostních strategií, by měly lépe porozumět rozdílům mezi těmito dvěma oblastmi (BOZP, 2021).

1.3 Pojem kybernetická bezpečnost

Pojem "kybernetická bezpečnost" nelze jednoduše definovat. Existují mnohé definice, následující pochází z cizojazyčných slovníků.

Tento pojem lze definovat podle následující definice od americké služby Merriam-Webster: „*Opatření přijatá k ochraně počítače nebo počítačového systému (jako na internetu) před neoprávněným přístupem nebo útokem,"* (Merriam-webster, 2023).

Slovník University Camridge definuje kybernetickou bezpečnost jako*:*

„Věci, které jsou prováděny k ochraně osoby, organizace nebo země a jejich informací na počítači před zločinem nebo útoky provedenými pomocí internetu," (Dictionary, 2023).

Autor Michal Štusák ve své práci uvádí výstižnou definici kybernetické bezpečnosti, která vychází z *„Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020"*. Tato definice zní*: „Kybernetická bezpečnost představuje souhrn organizačních, politických, právních, technických a vzdělávacích opatření a nástrojů směřujících k zajištění zabezpečeného, chráněného odolného kyberprostoru v České republice, a to jak pro subjekty veřejného a soukromého sektoru, tak pro širokou českou veřejnost"* (Štusák, 2020), (NBÚ, 2015).

Termín "kyberbezpečnost" spojuje dvě klíčová slova: "kybernetika," která se týká nebo je charakteristická pro kulturu počítačů, informační technologie a virtuální reality, a "bezpečnost," což označuje stav bezpečí bez hrozby nebo nebezpečí. Kybernetika se zabývá studiem řízení, komunikace a informací v systémech, zatímco bezpečnost se zaměřuje na ochranu před nebezpečím a zachování integritu (Cs.bab.la, (bez data)).

Tyto dva prvky dohromady tvoří komplexní oblast. Pojem bezpečnost bude dále vymezen v následující kapitole.

1.4 Bezpečnost

Bezpečnost je obvykle chápána jako schopnost společnosti nebo státu zabránit konkrétním rizikům překročit bezpečné hranice. Subjekt odpovědný za bezpečnost, jako například stát

nebo mezinárodní organizace, aktivně připravuje účinná opatření pro zvládání možných hrozeb s cílem zajistit bezpečnost v různých oblastech, jako je ochrana obyvatelstva, udržení svrchovanosti státu, zachování vnitřního pořádku, majetku, životního prostředí a plnění mezinárodních bezpečnostních závazků.

Realizace bezpečnosti zahrnuje širokou škálu opatření, strategií a akcí směřujících k zajištění vnitřní, vnější a mezinárodní bezpečnosti jednotlivců, států nebo celého mezinárodního společenství, a to jak v běžném stavu, tak i v době krizových situací (Souček, a další, 2005).

"Vlastnost prvku (např. informační systém), který je na určité úrovni chráněn proti ztrátám, nebo také stav ochrany (na určité úrovni) proti ztrátám. Bezpečnost IT zahrnuje ochranu důvěrnosti, integrity a dosažitelnosti při zpracování, úschově, distribuci a prezentaci informací," (Jirásek, a další, 2015) .

Tato definice zdůrazňuje, že jde o vlastnost prvku, například informačního systému, který je chráněn na určité úrovni proti ztrátám. Tato definice se shoduje s definicí o stavu bezpečnosti, která je definována jako minimální omezení hrozeb pro objekt, typický národní stát nebo mezinárodní organizaci. Tento termín je vyjádřen v *„České bezpečnostní terminologii: Výkladu základních pojmů,“* a zní: „stav*, kdy jsou nejnižší možnou mírou limitovány hrozby pro objekt (zpravidla národní stát, popř. mezinárodní organizace) a jeho zájmy a tento objekt ke k eliminaci stávajících i potencionálních hrozeb efektivně vybaven a ochoten při ní spolupracovat,"* (Zeman, 2002).

1.5 Triáda CIA

V jádru tří pojmů, jež budou následně podrobně analyzovány, se nachází kybernetická bezpečnost. Triáda CIA, opírající se o principy důvěrnosti, neporušenosti a dostupnosti, představuje základní koncept v oblasti informační bezpečnosti. Tato koncepce zohledňuje zásadní stavební prvek pro ochranu dat a informací v organizacích, a také umožňuje zaměstnancům efektivně plnit každodenní úkoly, včetně sběru dat, poskytování zákaznického servisu a obecné správy (Coursera, 2023).

V rámci standardu ISO 27001, mezinárodní normy pro správu informační bezpečnosti, zaujímá CIA triáda významné postavení. Díky její aplikaci organizace dosahují optimální úrovně bezpečnosti, aniž by to omezovalo efektivnost běžných pracovních procesů (Irwin, 2023).

Znění Triády CIA každého pojmu zvlášť zní:

- **Důvěrnost (Confidentiality):** Důvěrnost představuje opatření na ochranu osobních informací s cílem zabránit neoprávněnému přístupu Ilustrace: Při odesílání e-mailu se snažíte zajistit, aby ho viděl pouze zamýšlený příjemce. Bezpečnostní prvky, jako jsou hesla a zámky, slouží k udržení obsahu e-mailu soukromého.
- **Neporušenost (Integrity):** Neporušenost znamená, že data zůstávají přesná a nedochází k neoprávněným změnám. Veřejně prezentovaná data musí být spolehlivá, aby si lidé mohli být jisti důvěryhodností informací poskytovaných organizací.
- **Dostupnost (Availability):** Dostupnost znamená, že oprávněné osoby mají možnost snadno přistupovat k datům, aniž by to narušilo jejich důvěrnost nebo neporušenost (Coursera, 2023).

1.5.1 Informační bezpečnost

Následující podkapitola bude věnována informační bezpečnosti. Avšak pro plné porozumění tématu je nezbytné nejprve definovat samotné slovo "informace".

Informace

Informace je složená z dat, která získávají význam a interpretaci pro subjekt, který je přijímá. Data samotná mohou být neupravená a nemusí automaticky nesehrávat významnou roli, ale jakmile jsou interpretována a organizována, transformují se v informace.

„Informace jsou data, kterým rozumíme, mají pro nás nějaký smysl," (Bigyzr, 2020). Zde je zdůrazněno, že informace vznikají v okamžiku, kdy dat získají význam pro konkrétního jedince. Pro organizace i jednotlivce strategické aktivum, a proto je nezbytné zajistit jejich komplexní ochranu po celou dobu jejich životního cyklu. Od fáze tvorby až po fázi zničení musí být informace chráněny před neoprávněným přístupem, zneužitím, modifikací či ztrátou (Šulc, 2018).

Infosec neboli informační bezpečnost zahrnuje opatření, jejichž účelem je zajištění bezpečnosti elektronických dat proti neoprávněnému přístupu a potenciálním hrozbám.

Hlavním záměrem je udržet důvěrnost, integritu a dostupnost informací v kontextu s kybernetickou bezpečností, jež se specializuje na ochranu všech aktiv v oblasti informačních

technologií. Důležitou roli v rámci informační bezpečnosti hrají síťové a aplikované zabezpečení. Infosec je nezbytný pro organizace využívající informační technologie (Fruhlinger, 2020).

Informační bezpečnostní politika, jako součást tohoto rámce, detailně stanovuje pravidla s cílem zabezpečit informační aktiva. Těmito pravidly jsou omezené přístupy pouze pro autorizované subjekty. Dále politika minimalizuje potenciální dopady na ohrožená informační aktiva a také řeší stížnosti a dotazy v oblasti kybernetických rizik (Tunggal, 2023).

Organizační opatření se snaží vytvořit interní jednotku specializovanou na informační bezpečnost a integrovat tuto oblast do povinností vybraných zaměstnanců ve všech odděleních organizace. Lidská opatření zahrnují školení uživatelů, kde je kladen důraz na správné postupy a zvýšení povědomí o bezpečnostních hrozbách. Fyzická opatření se zaměřují na kontroly přístupu, což naznačuje, že bezpečnostní opatření nejsou relevantní pouze pro digitální sféru, ale ovlivňují také fyzický přístup k prostorům a zařízením (Fruhlinger, 2020).

1.5.2 Klasifikace informací

Podle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů, v § 4 Stupně utajení jsou informace klasifikovány do čtyř stupňů utajení podle následujících kritérií:

- **Přísně tajné** – v případě, že vyzrazení neoprávněné osobě nebo zneužití může způsobit mimořádně vážnou újmu zájmům České republiky.
- **Tajné** – pokud vyzrazení neoprávněné osobě nebo zneužití může způsobit vážnou újmu zájmům České republiky.
- **Důvěrné** – v situaci, kdy vyzrazení neoprávněné osobě nebo zneužití může způsobit prostou újmu zájmům České republiky.
- **Vyhrazené** – když vyzrazení neoprávněné osobě nebo zneužití může být nevýhodné pro zájmy České republiky (NBÚ, 2025).

2 GENEZE KYBERNETICKÝCH HROZEB

Následující kapitola se bude věnovat genezi kybernetických hrozeb, která představí počátky i aktuální trendy v oblasti kyberkriminality, její vývoj, a bude se také věnovat pojmům z této oblasti. Zkoumání tohoto vývoje nám umožňuje lépe chápat, jak a proč kybernetické hrozby vznikají, mění se a přizpůsobují se v průběhu času.

Termín "geneze″ v tomto kontextu označuje komplikovaný proces, jak se kybernetické hrozby vyvíjejí historicky. Důkladné porozumění tohoto evolučního procesu je klíčové pro účinné řešení současných i budoucích výzev v oblasti kybernetické bezpečnosti (Bagge, 2015).

Tato kapitola se zaměřuje na analýzu různých etap, faktorů a proměnných, které formují různé formy kybernetických hrozeb, od malwaru po sofistikované útoky nebo techniky sociálního inženýrství. Vliv technologického vývoje, změn v sociálním chování, ekonomických faktorů a dalších determinantů na genezi kybernetických hrozeb je klíčový pro úspěšnou analýzu.

Studium geneze kybernetických hrozeb poskytuje základ pro porozumění povaze a dynamice těchto hrozeb, což umožňuje vytvářet efektivní strategie v oblasti kybernetické bezpečnosti a prevence (Costigan, 2014).

2.1 Vymezení pojmu kyberkriminalita

Problematice kybernetické kriminality, známé též jako "kyberkriminalita," v dnešní době velmi aktuálním tématem, které se zabývá nezákonnými činnostmi provedenými pomocí počítačů či internetu (Cobb, 2021).

Z doslovného překladu anglického názvu "Cybercrime," pak překlad "kyberkriminalita" není přesný, neboť doslovný překlad tohoto spojení dvou slov je možné přeložit jako "kyber zločin" (případně trestný čin) (Kolouch, 2016).

Termín "kybernetická kriminalita" reflektuje široký dosah, kde počítače mohou působit samostatně nebo ve vzájemné kombinaci v rámci trestné činnosti. Odborníci poukazují na změnu terminologie, kde místo pojmu *„počítač“* se v dnešní době používá spíše výraz „*informační a komunikační technologie“ (*Information and Communication Technology – ICT*), resp. „trestné činy v ICT,“* (Požár, 2005).

Vzhledem ke snaze o definování pojmu kybernetické kriminality je vhodné využít Úmluvu Rady Evropy č. 185 o kybernetické kriminalitě ze dne 23. listopadu 2001. Tato

úmluva však vlastní pojem kyberkriminality nevymezuje. Definuje pouze opatření, která by měla být přijata ratifikující stranou na vnitrostátní úrovni (Kolouch, 2016).

„Trestná činnost, kdy jsou služby nebo aplikace v kybernetickém prostoru nástrojem nebo cílem útoku, případně trestná činnost v rámci, které je kybernetický prostor zdrojem, nástrojem, cílem nebo místem trestného činu.“, je klíčovým prvkem této problematiky (Požár, a další, 2022).

2.1.1 Kybernetické a ICT právo

V kontextu s kyberkriminalitou je nutné zmínit také legislativní rámec v oblasti kybernetické bezpečnosti. Globálně lze hovořit o právu hovořící za informační a komunikační technologie (ICT).

Právo ICT, též známé jako právo informační technologie nebo právo IT, se stalo samostatným a klíčovým oborem právní odbornosti, který zahrnuje prvky z různých odvětví, zahrnuje různé právní úvahy od smluvního po právo ochrany spotřebitele, trestní právo, patentové právo, autorské právo, ochranu obchodních značek, duševní vlastnictví, bankovní právo, až po práva týkající se ochrany soukromí, svobody projevu, daní, telekomunikací, pracovního práva a práva důkazního (Lawinsider, 2017).

V digitálním věku roste význam práva ICT jako ochranného mechanismu, který zajišťuje přizpůsobení právních rámů neustále se měnícímu prostředí technologie a poskytuje stabilní základ pro etické a právní chování podniků a vlád v digitálním prostoru (Michalsons, 2016).

Úvodní sekce zákona přesně vymezuje práva, povinnosti jednotlivců a pravomoci orgánů veřejné moci působících v oblasti kybernetické bezpečnosti. Nezanedbatelným prvkem je rovněž adaptace na evropské směrnice, s důrazem na transpozici směrnice NIS. *„NIS (Network Information Security) je první směrnice vytvořená EU jako komplexní dokument, jehož cílem je zajistit jednotnou a vysokou úroveň bezpečnosti na úrovni sítí a informačních systémů v členských státech EU,“* (Utb.cz, 2016).

2.1.2 Pojmy z oblasti kyberkriminality

Základní pojmy z této oblasti budou obsaženy v praktické části. V této oblasti se vyskytuje mnoho pojmů týkající se kybernetických hrozeb, útoků a ochrany. Zde budou zmíněna alespoň ta základní, která by měla postačit pro pochopení hlavní části práce. Mezi hlavní pojmy patří bezpečnostní hrozba, riziko, zranitelnost a aktiva.

Bezpečnostní hrozba

Bezpečnostní hrozba, v kontextu bezpečnosti, reflektuje situaci, kdy se identifikuje potenciální vyžití existující zranitelnosti k ohrožení integrity, dostupnosti nebo důvěrnosti systému či datových aktiv. Její následky mohou zahrnovat finanční ztráty, poškození reputace, nebo ztrátu důvěryhodnosti systému (It-slovnik, 2024).

Riziko

Riziko lze definovat jako pravděpodobnost vzniku nežádoucí události v určitém časovém období nebo za daných podmínek. Tato pravděpodobnost je charakterizována kombinací pravděpodobnosti samotné události a jejích potenciálních dopadů. Je tedy chápáno jako ve vztahu s očekávanou ztrátou (Bernatík, 2016).

Nebezpečí

Je vlastnost nebezpečné látky nebo situace, která může vést k vážné havárii. Jedná se o skrytou vlastnost objektu, která může způsobit neočekávané škody. Tato vlastnost se projevuje ve chvíli, kdy jsme ji vystaveni, nebo jsme s ní v kontaktu (Bernatík, 2016).

Zranitelnost

Zranitelnost je vlastnost nebo slabina na úrovni fyzické, logické nebo administrativní bezpečnosti, která může být zneužita hrozbou. Je to stav nebo vlastnost systému, procesu nebo jednotlivce, která je citlivá nebo náchylná k újmě, poškození nebo útoku. Díky nedostatečné ochraně, nebo chybám umožňuje zranitelnost pomoci hrozbám k proniknutí, poškození, nebo narušení integrity, dostupnosti nebo důvěrnosti daného systému nebo subjektu (Acresia, 2020).

Aktivum

Aktiva jsou prvky organizačního prostředí, které představují zdroje s ekonomickou hodnotou či potenciálem dosažení cílů organizace. Tyto aktiva se také dělí na:

- Primární aktiva – tyto aktiva jsou nezbytné pro provoz a fungování organizace. Jsou jimi informační systémy a služby.
- Podpůrná aktiva – tyto aktiva slouží k podpoře a optimalizaci provozu primárních aktiv. Zde můžeme zařadit technické vybavení, programové vybavení, lidské zdroje a dodavatele zapojené do provozu.

V oblasti řízení rizik je podstatné tyto aktiva umět rozlišit a ohodnotit (Kresa, 2023).

Bezpečnostní opatření

Bezpečnostní opatření jsou souborem kroků, jejichž účelem je chránit bezpečnost informací v informačních systémech, zajišťovat dostupnost a spolehlivost služeb a sítí elektronických komunikací v kybernetickém prostoru. Jsou jimi technické, administrativní a fyzické prvky, které mají minimalizovat rizika spojená s možnými hrozbami a zajistit ochranu a integritu prostředí organizace (Lewik, 2015).

Bezpečnostní incident

K bezpečnostnímu incidentu, též nazývanému "Security Incident" dochází v momentě, kdy dochází k ohrožení informací nebo porušení bezpečnostních pravidel. Příčinou může být jak chyba v bezpečnostních opatřeních, tak i nedodržování bezpečnostní politiky ze strany uživatelů. Jednoduše řečeno, za bezpečnostní incident se považuje neúspěšný pokus o narušení bezpečnosti (ManagementMania, 2018).

2.2 Počátky kyberkriminality

První doložený kybernetický incident, který proběhl ve Francii v roce 1834, představuje pokus o neoprávněné získání informací na finančním trhu prostřednictvím kompromitace telegrafního systému. Tato událost, zahrnující první národní datovou síť na světě v rámci mechanického telegrafu, může být chápána jako první kybernetický útok s důrazem na přenos informací na vzdálenost.

Přestože termín "kyber" obvykle odkazuje na počítačové sítě, tento historický příklad zdůrazňuje jeho relevanci v kontextu současných kybernetických hrozeb, jež překračují rámec pouhé krádeže informací (Monroecollege, 2023).

Počátky šedesátých let představovaly převážně velké sálové systémy umístěné v kontrolovaných prostředích a s omezeným přístupem. Omezená dostupnost a vysoké náklady bránily jednotlivcům s programátorskými dovednostmi v plném rozsahu těchto zařízení. Během této doby se termín *„hackování“* začal formovat, zejména ve spojitosti s neoprávněným přístupem k vlakovým soupravám MIT Tech Model Railroad Club. Tento vývoj poukazuje na adaptaci konceptu „*hackování*“ v rámci počítačových systémů.

S postupem 60. let a zejména v roce 1962 přinesl další vývoj první počítačový virus, známý jako Creeper, na ARPANETu, což iniciovalo postupný nárůst kybernetické kriminality. V roce 1971 Allen Scherr zahájil významný kybernetický útok proti MIT, kde neoprávněně získal hesla prostřednictvím děrné karty, zahajujíc tak éru významných kybernetických

událostí. Toto období ilustruje, jak se kybernetická kriminalita vyvinula od prvního počítačového viru k významným útokům, představovaným Allenem Scherrem (Davies, 2021).

V několika desetiletích se kybernetická kriminalita vyvíjela. V roce 1981 došlo k prvnímu odsouzení za počítačovou kriminalitu. Následoval významný kybernetický útok "Morris Worm" v roce 1988 a výzvy v oblasti kybernetické bezpečnosti, kterým čelil Kevin Mitnick v 90. letech. Jeho inovativní přístupy, včetně sociálního inženýrství, přinesly nový rozměr kybernetické bezpečnosti, aktuální i v současných výzvách přesahujících digitální rámec.

V 80. letech se výrazně zvyšoval počet významných kybernetických útoků, dokumentovaných incidenty v Národní laboratoři CSS, AT&T a Los Alamos. Film "Válečné hry" z roku 1983 ilustruje, jak zlovolný počítačový program přejímá formu hry a ovládá jaderné raketové systémy.

V té době byly uvedeny pojmy *„Trojan Horse“* a *„počítačový virus“*. Během studené války rostlo riziko kybernetické špionáže. V současném desetiletí kybernetická kriminalita pokračuje ve svém vývoji, stává se tak významnou kapitolou v historii (Wolf, 2022).

2.3 Aktuální trendy v kyberkriminalitě

V této kapitole budou zmíněny typy kybernetických útoků, které jsou v aktuální době vyskytovány nejčastěji.

Artificial Intelligence

V oblasti kybernetické bezpečnosti nové technologické pokroky v umělé inteligenci ovlivňují strategie a taktiky útoků. Generativní umělá inteligence umožňuje útočníkům nalézt nové způsoby útoků na cloudové systémy a využít geopolitické napětí.

I přes určitou ochranu, kterou nástroje jako ChatGPT poskytují proti vytváření škodlivého kódu, odborníci dokážou využít chytrých technik k obejití těchto ochran a vytvoření sofistikovaného malwaru. Nástroje AI mohou napomoct ke tvorbě automatizovaných malware, k phishingovým a jiným pokročilým útokům.

Odborníci varují před riziky v oblasti ochrany soukromí v důsledku možného úniku dat a zneužití AI k sledování uživatelů (Malwarebytes, 2024).

Technologie *„deepfake“* umožňuje vytváření autentických falešných videí a zvukových záznamů, což umožňuje kyberzločincům manipulovat s jednotlivci v phishingových útocích a získávat citlivé informace.

Navíc phishingové útoky využívající AI jsou stále složitější a obtížněji odhalitelné, přičemž kyberzločinci využívají AI k vytváření věrohodných falešných e-mailů a webových stránek, které jsou těžko odlišitelné od těch legitimních. Potenciál AI sahá i k usnadnění sofistikovanějších útoků na odmítnutí služby (DoS) a ransomwarové útoky, které jsou vysoce personalizované a dynamické, což umožňuje kyberzločincům vyhnout se tradičním bezpečnostním opatřením (Devoteam, 2024).

Remote Desktop Protocol

RDP je komunikační protokol, který umožňuje uživatelům přístup a správu počítače odkudkoli na světě přes bezpečné a spolehlivé spojení. Uživatel má možnost sledovat a ovládat počítač na dálku, jako by byl fyzicky přítomen. Tato virtuální spojení umožňují uživatelům navigovat v rozhraní vzdáleného počítače, spustit licencovaný software, získat uložené soubory, a dokonce *„streamovat“* zvuková data, vše pomocí síťového spojení (Vaideeswaran, 2023).

Tento protokol přináší do světa kyberbezpečnosti hrozby v podobě potenciálně slabých míst, která mohou být zneužita útočníky k neoprávněnému přístupu a útokům. Zranitelnost je jako mezera v zámku na předních dveřích domu – poskytuje cestu pro zloděje, kteří se chtějí dostat dovnitř.

V protokolu jsou dvě významné zranitelnosti, těmi jsou:

1. Slabé přihlašovací údaje.
2. Neomezený přístup k portům.

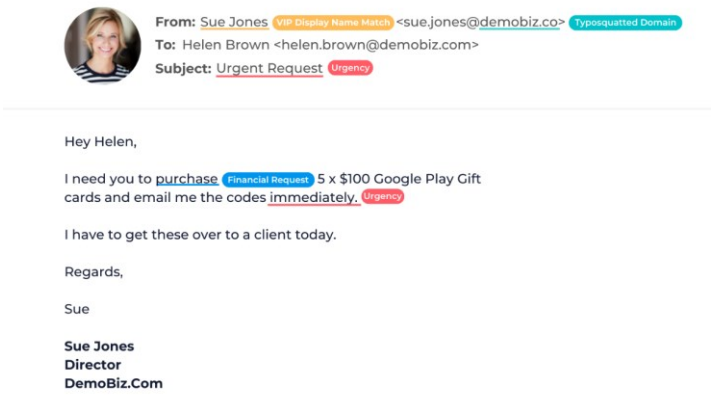
Připojení pomocí RDP se téměř vždy odehrává na portu 3389*. Útočníci mohou předpokládat, že tento port je používán, a zaměřit se na něj k provedení útoků na cestě nebo jiných (Cloudflare, 2024).

Business Email Compromise

BEC je sofistikovaná forma útoku, která spadá do kategorie phishingových útoků. Cílem je podvést vedoucí pracovníky nebo osoby odpovědné za finanční rozhodování, aby převedli peníze nebo poskytli citlivé informace útočníkům.

Útočníci využívají e-maily, které vypadají věrohodně a přesvědčivě. Jsou cílené a zaměřené na konkrétní jednotlivce nebo organizace, což činí jejich detekci ještě obtížnější. BEC útoky jsou tedy významnou hrozbou pro organizace všech velikostí (NCSC, 2020).

Na snímku je vysvětlen příklad, na kterém lze vidět vyjádření slov, která mají působit na zaměstnance. Těmito slovy jsou např. ihned nebo nutně.



Obrázek 3 - Příklad BEC útoku (zdroj: Pottrel, ©2024)

Supply chain attack

Tento typ kybernetického útoku cílí na důvěryhodného dodavatele třetí strany, který poskytuje služby nebo software nezbytné pro dodavatelský řetězec. Do aplikace vkládají škodlivý kód s cílem infikovat všechny uživatele aplikace.

Softwarové dodavatelské řetězce jsou náchylné k rizikům způsobeným tím, že moderní software skládá z mnoha hotových komponent, včetně API třetích stran, open source kódu a vlastního kódu od dodavatelů softwaru, místo toho, aby byl psán zcela od začátku (Lenaerts-Bergmans, 2023).

Cyberactivism

Cyberaktivismus je proces využívání internetových sociálních sítí a komunikačních technik k organizaci a propagaci různých forem aktivismu. Tento přístup umožňuje jednotlivcům i organizacím využívat online platformy k mobilizaci, sdílení informací a prosazování určitých zájmů či cílů.

Základ je podobný jako u tradičního fyzického aktivismu, kdy je vytvořeno hnutí směřující k dosažení specifického cíle. Cyberaktivisté využívají různé online platformy, jako jsou

sociální sítě typu Twitter nebo Facebook, k šíření informací a interakci s uživateli internetu (Rouse, 2017).

Social engineering

Sociální inženýrství je metoda, kterou útočníci využívají k manipulaci s lidským chováním a důvěrou, s cílem získat citlivé informace nebo finanční prostředky. Tento druh útoků se často provádí prostřednictvím různých triků, jako jsou phishingové e-maily, falešné telefonáty nebo vydávání se za jinou osobu, objevuje se jak v online, tak i v offline prostředí. Velkou roli zde hraje již zmíněná umělá inteligence, která může provádět manipulace pomocí chatbotů. Tyto útoky mohou mít vážné důsledky pro jednotlivce i organizace (Koren, 2023).

Cryptojacking

Při této formě útoku dochází k neoprávněnému využívání výpočetních zařízení jednotlivců nebo organizací k těžbě kryptoměn. Útočníci jsou motivováni finančním ziskem, ale na rozdíl od jiných hrozeb je záměrem zůstat úplně skrytý před obětí.

Cryptojacking se využívá k vniknutí do cílového zařízení, kde následně využívá jeho výpočetních zdrojů pro těžbu kryptoměn. Právě kryptoměna je digitální forma peněz, která existuje pouze elektronicky a nemá fyzické základy (Kaspersky, 2023).

Ransomware

Jde o formu malware, která uzamkne a šifruje data, soubory, zařízení nebo systémy obětí, čímž se stanou nedostupnými, dokud útočník neobdrží výkupné. Původní verze ransomware využívaly pouze šifrování k zabránění obětem v přístupu k jejich souborům a systémům, avšak útočníci začali používat také taktiky kybernetického vydírání a častěji cílí na zálohy obětí (Irei, a další, 2023).

Ransomware má značné dopady na široké spektrum organizací a odvětví, včetně zdravotnických institucí, vzdělávacích zařízení, maloobchodních subjektů a energetických distribučních sítí. Tři hlavní metody, jak ransomware proniká do systémů obětí, zahrnují sociální inženýrství a phishing, využívání protokolu Remote Desktop Protocol (RDP) a zneužívání přístupových údajů, a využití zranitelností softwaru (Kelley, 2023).

Jedním z hlavních trendů v oblasti ransomware jsou útoky tzv. "triple extortion", kde útočníci nejen šifrují data, ale také je vykrádají a hrozí jejich zveřejněním, pokud nebudou zaplaceny. (RaaS) je další trend, který umožňuje útočníkům využívat platformy poskytující

ransomware kód a infrastrukturu pro spuštění a udržování ransomwarových kampaní. Nakonec, útočníci i nadále využívají phishingové e-maily jako cestu k infikování organizací (Kerner, 2024).

DDoS

Tento kybernetický útok se projevuje zahlcením webového serveru zahlcením služby velkým počtem nelegitimních požadavků. Účinky těchto útoků jsou různorodé, a záleží na konkrétním případu napadení. Nejčastější dopady jsou zejména ty finanční, pokles produktivity, nebo jiné poškození, které může mít také dopad na důvěryhodnost organizace (Microsoft, 2020).

Útočníci, známí jako "threat actors", neustále vylepšují své techniky a reagují na změny v prostředí kybernetických hrozeb, včetně politických událostí, jako je konflikt na Ukrajině. Tato prostředí poskytují útočníkům příležitosti k provádění DDoS útoků a těžení z jejich účinků, což představuje značnou výzvu pro ochranu před těmito hrozbami (Microsoft, 2023).

Phishing

Je to praktika útoků prostřednictvím podvodných komunikací, které se zdají být legitimní, s cílem získat citlivé informace nebo nainstalovat malware. Tato taktika útoků je charakterizována různými strategiemi manipulace, jako je vyvolání strachu, zvědavosti či naléhavosti, které mají za účel přimět oběť k interakci s podvodným obsahem, například kliknutím na odkazy či otevřením příloh. Zprávy často vypadají velmi důvěryhodně, často jako od známých, nebo vámi navštěvovaných společností.

Jelikož již jeden jediný úspěšný útok může vést ke kompromitaci celé sítě a odcizení důležitých dat, je nezbytné, aby uživatelé byli obezřetní a pečlivě zvažovali své kroky před jakoukoliv interakcí s podezřelými zprávami nebo odkazy (Cisco, 2024).

Jako příklad pro tento útok byl vybrán úspěšný phishingový útok, který za pouhých 5 dní obelhal stovky lidí. Cílem byli uživatelé e-mailových schránek u centrum.cz a centrum.sk. Útok začal e-mailem, který tvrdil, že jejich e-mailové účty jsou omezeny. Útočníci instruovali oběti, aby ručně rozeslaly e-mail ze serverů centrum.cz, aby obešly antispamové a antivirové filtry třetí strany od virusfree.cz, které centrum.cz používá od roku 2018. Tento případ ukazuje, jak útočníci využili důvěryhodnosti e-mailových domén k vytvoření zdánlivě legitimního podvodu.

Obrázek 4 - Příklad phishingového e-mailu (Málek©2022)

Uživatel, který klikl na odkaz *"ÄKTUALIZÄCE"* byl zaveden na podvodnou stránku, která vypadala jako obvykle. V této doméně byla nezašifrovaná cizí doména.

Útočník posílal shromážděné údaje a přenášel je na svůj Gmail účet. Současně využíval aplikaci v Telegramu k jejich distribuci a archivaci. Tyto informace byly též zaznamenávány do logů na serveru. Po získání přístupových údajů se pokusil o nasazení podvržené platební stránky s názvem "Peníze nebudou strženy jen za účelem ověření účtu". Navzdory tomu, že útok zaznamenal pokles úspěšnosti, někteří jednotlivci se stále stali oběťmi a poskytli útočníkovi údaje svých platebních karet.

Útočník posílal shromážděné údaje a přenášel je na svůj Gmail účet. Po získání přístupových údajů se pokusil o nasazení podvržené platební stránky s názvem "Peníze nebudou strženy jen za účelem ověření účtu". Navzdory tomu, že útok zaznamenal pokles úspěšnosti, někteří jednotlivci se stále stali oběťmi a poskytli útočníkovi údaje svých platebních karet (Málek, ©2022).

Malware

Tento škodlivý software, který je navržen k infikování počítačových systémů a získání neoprávněného přístupu, představuje klíčovou složku současné kybernetické hrozby. Mezi typy malware zahrnujeme: adware, spyware, viry, botnety, trojany, červy, rootkity a ransomware a jiné.

Přičemž jejich společným cílem je narušit bezpečnost a integritu počítačových systémů. Tyto hrozby se často šíří prostřednictvím různých kanálů, včetně infikovaných odkazů v e-mailech, nelegitimních webových stránek, torrentů a dokonce i prostřednictvím textových zpráv.

Díky široké dostupnosti zdrojového kódu malwaru na temném webu mají i běžní kybernetičtí zločinci snadný přístup k těmto nástrojům, což zvyšuje riziko kybernetických útoků (Belcic, 2023).

Man in the Middle

MITM útok je situace, kdy někdo tajně sleduje komunikaci mezi dvěma lidmi nebo zařízeními online. Útočník může zachytit citlivé informace, jako jsou hesla nebo bankovní údaje, a použít je bez vědomí uživatele. Útočníci využívají malware k infiltraci datových transakcí a online komunikace. Tím, že se útočníci vkládají do středu komunikace mezi dvěma stranami, získávají kontrolu nad přenášenými daty a mohou tak získat citlivé informace, jako jsou přihlašovací údaje či finanční informace (Vaněk, 2023).

Tyto útoky jsou zejména problematické pro online bankovnictví a e-commerce platformy, které vyžadují bezpečnou autentizaci. Útočníci využívají techniky jako data *„interception“* a *„decryption“* k tomu, aby klamali uživatele a servery, čímž umožňují únik citlivých informací a potenciální finanční ztráty uživatelů (Yasar, a další, 2022).

SQL injection

SQLi je metoda kybernetického útoku, při které se útočník pokouší využít zranitelností vstupních polí webové aplikace k manipulaci s databází SQL a získání neoprávněného přístupu k datům. Tento typ útoku je starým problémem, který se vyskytuje již od konce 90. let minulého století, ale stále představuje závažnou hrozbu díky své rozšířené aplikaci.

Útoky SQL injection mohou nastat, když webová aplikace nesprávně ověřuje uživatelský vstup, což umožňuje útočníkovi vložit do vstupních polí kód, který může poškodit databázi nebo získat citlivá data. Zranitelnost vůči SQL injection je velmi rozšířená, protože mnoho webových stránek a serverů používá SQL databáze (Kaspersky, 2022).

Advanced Persistent Threat

APT je pokročilá hrozba, která je cílená na konkrétní osobu nebo organizaci. Tyto útoky mohou být:

- Pokročilé: V tomto případě útočník vyhledává zranitelnosti, aby mohl proniknout do systému. Využívá při tom různé metody jako exploit, zero-day, ale také sociální inženýrství.
- Trvalé: V takovém případě se útočník snaží získávat informace, nebo kompromitovat systémy po delší dobu.

Tyto způsoby útoku se vyznačují čtyřmi fázemi. V přípravné fázi útočník sbírá data, analyzuje systém oběti a skenuje dostupnost systému. Druhou fází je průnik. V této fázi se

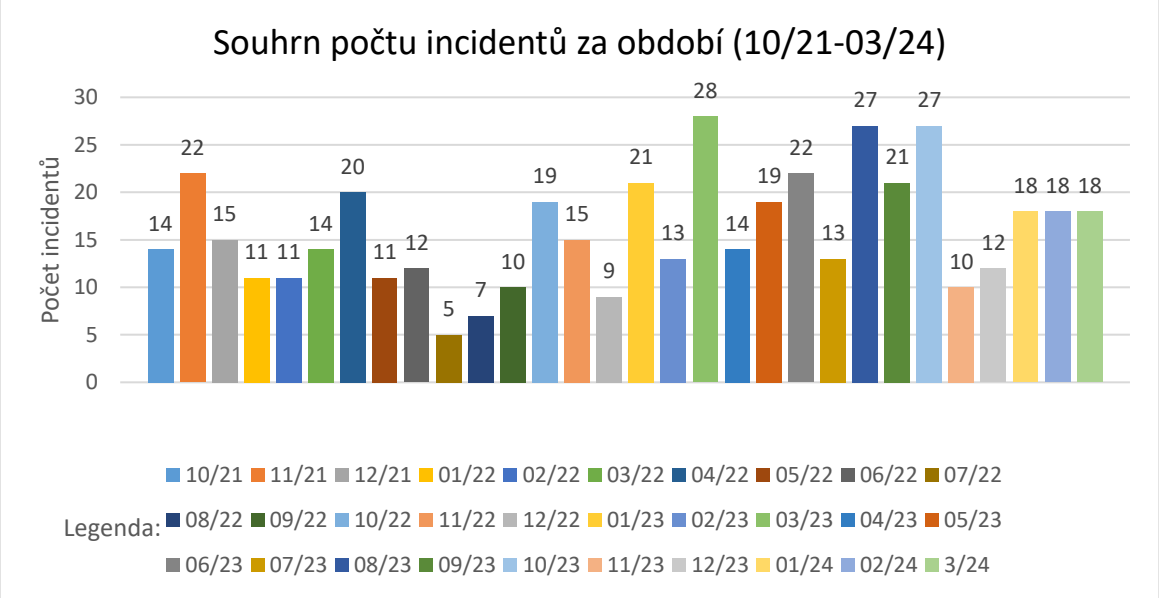
útočník pokouší proniknout do systému a napadnout ho vybraným způsobem. V třetí fázi, kompromitace, útočník již operuje v systému. Po činnostech, které útočníkovi pomohly získat požadované informace, následuje poslední fáze, dokončení. To znamená, že systém může být kompletně napaden, a je na útočníkovi, jak s ním naloží (Šulc, 2018).

2.3.1 Souhrn incidentů za určité období

Kybernetických útoků je velké množství a mnoho jich probíhá v jedné chvíli. Tyto útoky lze sledovat v reálném čase na stránkách https://cybermap.kaspersky.com/.

NÚKIB pravidelně zpracovává analýzy hlášených incidentů v oblasti kybernetické bezpečnosti, které se týkají České republiky. V těchto analýzách jsou zaznamenány různé typy útoků, včetně způsobů útoku a cílů, na které byly zaměřeny. Následující graf, konkrétně na období od října 2021 do března 2024 poskytuje ucelenější pohled na vývoj kybernetických hrozeb v České republice.

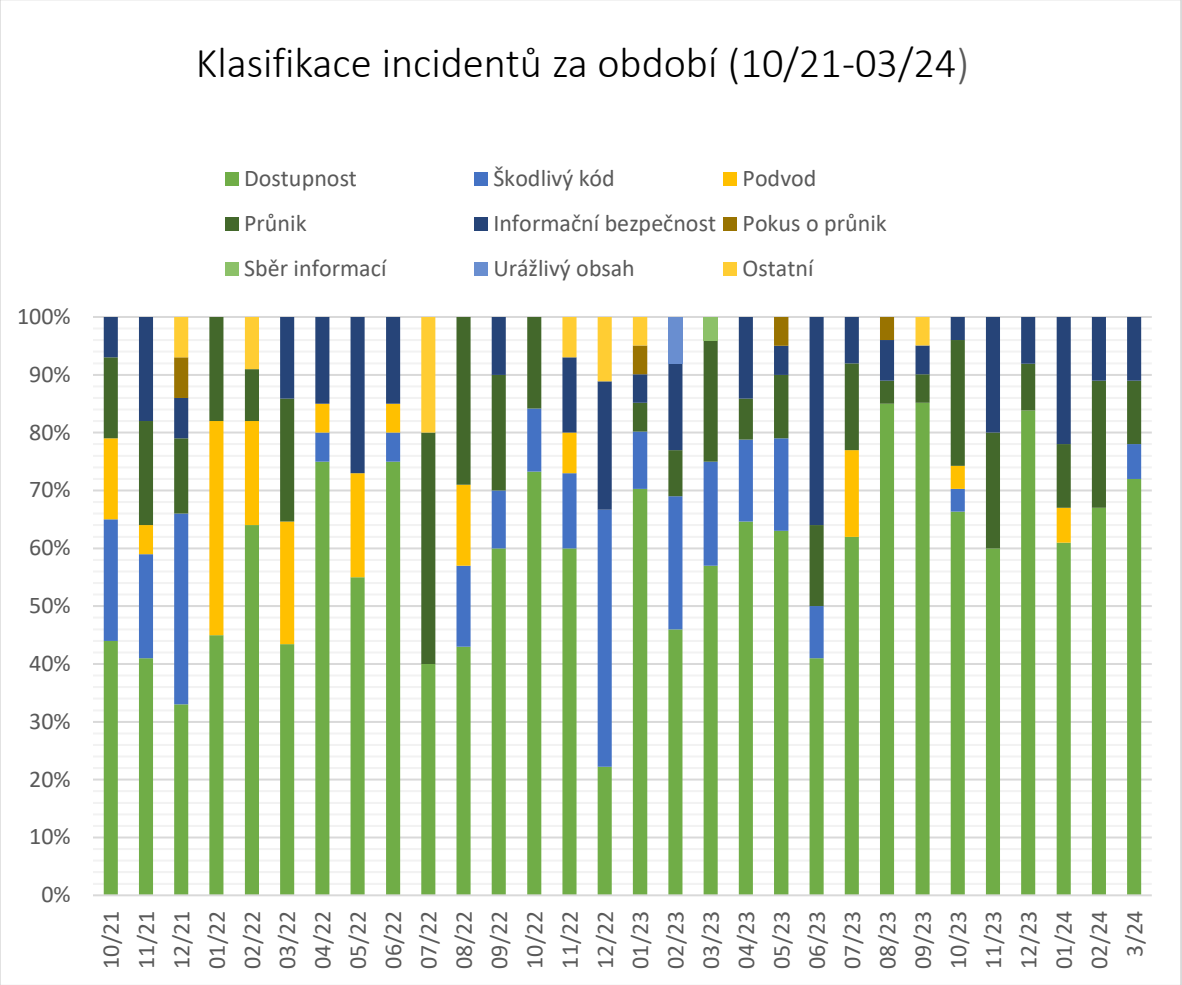
Tento časový rozsah umožňuje sledovat trendy a změny v kybernetickém prostředí v České republice. Zároveň je v této tabulce znázorněn počet incidentů, které byly nahlášeny na NÚKIB, ať už se jedná o phishing, ransomware, DDoS útoky nebo jiné formy kybernetických útoků.



Graf 1 - Souhrn incidentů z NÚKIB za období (10/21-03/24), (zdroj: NÚKIB), (vlastní zpracování)

V dalším grafu se nachází klasifikaci těchto incidentů. Data také pocházejí z pravidelných analýz kybernetických incidentů provedených NÚKIB. Tento graf poskytne detailnější

pohled na různé typy kybernetických útoků, které byly identifikovány a klasifikovány během sledovaného období.



Graf 2 - Klasifikace incidentů za období (10/21-03/24), (zdroj: NÚKIB), (vlastní zpracování)

Během celého sledovaného období přetrvává dlouhodobý trend, kdy incidenty spojené s nedostupností, jako jsou DDoS útoky, dominují. Dalším nejčastějším typem incidentů je průnik do systému, následovaný problémy spojenými s informační bezpečností. Také se zaznamenává významný počet incidentů spojených se škodlivým kódem. Naopak, sběr informací a obsah považovaný za urážlivý jsou za sledované období nejméně častými typy incidentů.

2.4 Dílčí závěr

V teoretické části práce byl představen koncept v oblasti kybernetické bezpečnosti. Byly zde probrány základní pojmy týkající se kyberprostoru, včetně jeho vymezení. Dále byla práce

zaměřena na oblast kybernetické bezpečnosti, triádu CIA a základní principy ochrany informací.

Následně byla probrána témata problematiky kybernetických hrozeb, kybernetické a ICT právo, byla definována kyberkriminalita a část byla věnována její historii a současným trendům. Dále byly zmíněny běžné metody kybernetických útoků a na základě dat z NÚKIB bylo zpracováno stručné shrnutí nahlášených kybernetických incidentů v České republice.

Tato teoretická část sloužila jako základní úvod do problematiky kybernetické bezpečnosti, poskytující náhled do základních konceptů.

Následující část se zaměří na analýzu kybernetických hrozeb několika organizací, pro které bude také vytvořeno opatření proti těmto hrozbám. Na závěr bude vedena diskuse, která se bude věnovat závěrům, které z analýzy vyšly.

II. PRAKTICKÁ ČÁST

3 CHARAKTERISTIKA ORGANIZACÍ

Pro spolupráci na této analýze byly vybrány malé organizace. Jejich velikost a omezené aktivity často vedou k mylnému přesvědčení, že nemohou být terčem kybernetických útoků, protože nemají co nabídnout.

V rámci bakalářské práce se naskytla příležitost spolupracovat s různými organizacemi, zahrnujícími knihovnu, obecní úřad. Každá z těchto institucí poskytla jedinečné možnosti spolupráce, přičemž informace získané od každé z nich se lišily v množství a dostupnosti. Pro provedení analýzy byla v každé organizaci vytvořena malá analytická skupina, s kterou bylo provedeno vyhodnocování.

Je důležité zdůraznit, že v souladu s principem důvěrnosti a ochranou citlivých informací byly tyto organizace anonymizovány na základě vzájemné dohody. V této kapitole budou organizace stručně představeny, včetně popisu jejich cílů, poskytovaných služeb a charakteristik vybraných respondentů, kteří se účastnili analýzy.

3.1 Představení organizace č.1 Knihovna

Tato knihovna se nachází v malé vesnici s přibližně 400 obyvateli, kde kromě ní fungují ještě další dvě organizace. Jako knihovna působí téměř 140 let, avšak během tohoto období prošla několika změnami. Její budova není pouze místem pro půjčování knih, ale také slouží jako centrum volnočasových aktivit. Uvnitř budovy najdete dětský klub, komunitní centrum a učebnu pro neformální vzdělávání. Počet návštěv kulturních, komunitních a volnočasových akcí se pohybuje kolem 387 návštěv za měsíc, přičemž na vzdělávacích akcí je 72 návštěv za měsíc. Kromě toho sem chodí dalších 1 218 návštěvníků, kteří se účastní akcí, jež nejsou přímo pořádané knihovnou, ale probíhají i v jejích prostorách.

3.1.1 Rozsah a školení

Rozsah a hranice systému knihovny jsou definovány pouze na úrovni místní knihovny, která spadá pod okresní město. Školení o kybernetické bezpečnosti je součástí auditu bezpečnosti práce, který probíhá v rámci školení zaměstnanců. V rámci bezpečnostního školení zaměstnanců v oblasti kybernetické bezpečnosti jsou zaměstnanci seznámeni s obecnými zásadami dodržování bezpečnosti, jako je používání služebních zařízení, zákaz neoprávněných zásahů do operačních systémů a softwarů, a dodržování zásady uzamčené obrazovky (Win+L). Zaměstnancům je dále doporučováno, aby nedůvěřovali neznámým e-

mailům a neotvírali podezřelé přílohy či odkazy. Přičemž poslední školení v této oblasti proběhlo v roce 2022.

3.1.2 Cíle a služby knihovny

Knihovna nabízí služby jako půjčování knih z vlastního fondu pro děti, mládež i dospělé, a také z výměnného fondu. Financování provozu knihovny pochází z rozpočtu obce a využívá se pro regionální programy knihoven, které jsou realizovány pověřenou knihovnou.

Knihovna se snaží oslovit široké spektrum návštěvníků, a proto má vyhrazené dny pro dospělé i děti. Dodržuje knihovní řád, který byl schválen obecním zastupitelstvem a je v souladu se zákonem o knihovnách.

Správou osobních údajů registrovaných uživatelů knihovny se zabývá obec. Zpracovávání osobních údajů je prováděno v souladu smluvními podmínkami, které uzavřel uživatel s knihovnou, a v souladu s GDPR. Knihovna používá pro uchování osobních údajů počítačovou databázi Tritius.

3.1.3 Výběr respondentů a struktura organizace

Při výběru respondentů byla zohledněna omezenost výběru. V případě zpracování údajů týkajících se knihovny a obecního života byl vybrán místní pracovník knihovny. Jeho účast umožňuje získat detailní pohled na provozní a organizační aspekty knihovny z perspektivy pracovníka na první linii.

Co se týče vrcholového vedení, je složeno z místního obecního starosty a pověřeného knihovníka, který poskytuje strategické a rozhodovací perspektivy, zatímco metodické vedení nabízí rámec pro standardní postupy a směry ve vedení knihoven v rámci města.

3.2 Představení organizace č. 2 Obecní úřad

Obecní úřad v této obci, založený v roce 1990 krátce po sametové revoluci, hrál klíčovou roli ve zlepšování životních podmínek občanů. Za dobu své existence prošel mnoha změnami, ale jeho základní poslání sloužit občanům zůstalo stále stejné.

3.2.1 Služby a povinnosti obecního úřadu

Obecní úřad zajišťuje širokou škálu služeb v oblasti správy obce, matriky, školství a kultury a životního prostředí. Kromě poskytování služeb má úřad i řadu povinností, daných

zákonem, jako je zajišťování bezpečnosti a pořádku, práva majetku obce a zajišťování základních služeb pro občany.

Jeho rozpočet se pohybuje okolo 10 500 000 Kč, které jsou používány na financování těchto služeb a povinností. Činnost obecního úřadu upravena v řadě zákonů a předpisů, které se týkají specifických oblastí jeho působnosti (Tříska, 2018)**.**
Činnost obecního úřadu je upravena v široké škále zákonů a předpisů. Základními dokumenty jsou zákon č. 128/2000 Sb., o obcích (obecní zřízení) a zákon č. 500/2004 Sb., správní řád. Další relevantní legislativa se týká specifických oblastí působnosti úřadu, jako je ochrana životního prostředí, správa majetku obce apod.

Příklady služeb:

- Podpora školství a kulturního života.
- Zajištění svozu odpadu.
- Zásobování vodou a elektřinou.
- Podpora a rozvoj spolků.

Příklady povinností:

- Správa majetku obce.
- Zajišťování základních služeb pro občany.

3.2.2 Výběr respondentů

Do výzkumu byli zapojeni hlavní pracovníci z různých oddělení obecního úřadu, starosta a zaměstnanec úřadu, kteří měli nejlepší znalosti v konkrétních oblastech fungování obce. Na základě jejich odpovědí byla provedena analýza dat a hodnocení všech oblastí analýzy.

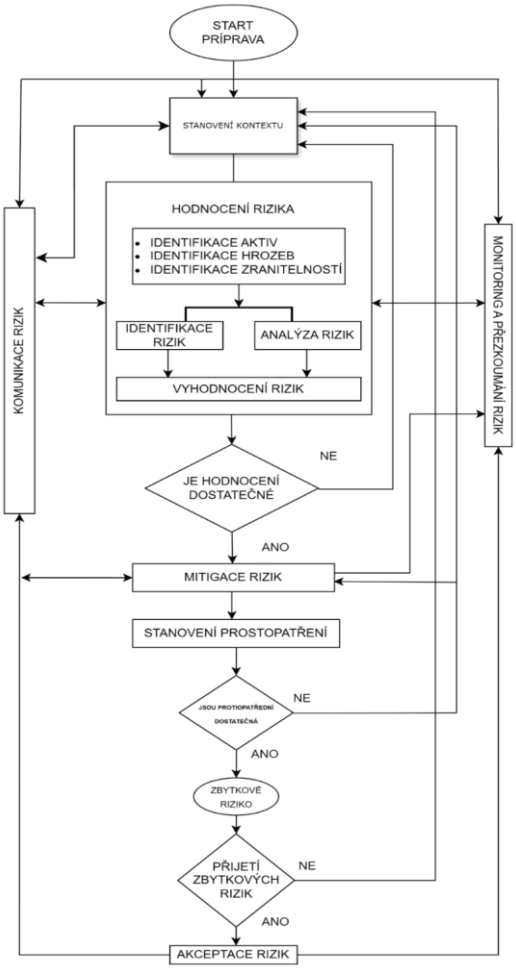
4 ANALYTICKO-METODOLOGICKÁ ČÁST

V minulé části byly představeny dvě organizace, ve kterých bude provedena analýza hrozeb. V této části bude následovat analýza ve vybraných organizacích.

Prvním krokem je identifikace různých aspektů, které mohou představovat hrozby. Následuje samotná analýza, během které se podrobně zkoumají možné scénáře a jejich dopady. Poté je nezbytné stanovit opatření, která mají minimalizovat nebo eliminovat tyto hrozby. Po stanovení opatření následuje jejich aplikace a implementace v organizaci.

Nakonec je důležité ověřit funkčnost těchto opatření prostřednictvím monitorování a komunikace rizik. Vzhledem k tomu, že žádná z těchto organizací neposkytla možnost testování, tento úkol bude ležet na samotných organizacích.

Nyní bude následovat vývojový diagram, který znázorní postup řízení rizik. Diagram systému řízení rizik poskytuje vizuální reprezentaci jednotlivých kroků a procesů.



Obrázek 5 - Vývojový diagram zobrazující postup při analýze rizik (zdroj: vlastní zpracování)

4.1 Stanovení kontextu

Stanovení kontextu nebo hranic v systému řízení rizik je charakterizováno definováním prostředí, ve kterém organizace působí, a určením rozsahu a limitů, v nichž se rizika vyskytují. V této fázi lze lépe pochopit vnitřní a vnější faktory, které mohou ovlivnit bezpečnostní postupy a strategie organizace a které je třeba brát v úvahu při identifikaci a hodnocení řízení rizik.

4.1.1 SWOT Analýza

Pro lepší představu o vnitřním a vnějším prostředí organizace byla vytvořena SWOT analýza. Ta zkoumá silné stránky (Strengths), slabé stránky (Weaknesses), příležitosti (Opportunities) a hrozby (Threats), které ovlivňují organizaci. Na závěr analýzy budou na základě výsledků vytvořené strategie SWOT.

SWOT analýza knihovny

Ve spolupráci s respondenty byly vypracovány SWOT analýzy, tito respondenti také doprovázejí celý zbytek analýzy. Pro analýzu bylo využito nástrojů umělé inteligence, kterou knihovna i obecní úřad používají pro svoji SWOT analýzu. Je třeba si však uvědomit, že SWOT analýza poskytuje pouze obecný pohled na hrozby organizace.

Na základě výsledků bylo zjištěno, že pro knihovnu bude nejlepší strategie spojenectví. Výsledky této analýzy lze najít v Příloze P I: Výsledek analýz SWOT. Tato strategie byla zakomponována do komplexní analýzy SWOT. Společně s umělou inteligencí byly navrženy konkrétní kroky pro zlepšení atributů knihovny. Analýzu SWOT nalezneme v tabulce, která byla vyplněna na základě dotazníku pro respondenty.

Z analýzy lze vyčíst, že pro knihovnu je podstatné hledat další finanční zdroje, aby mohla financovat lepší bezpečnostní prostředí. Hledat spolupráci s místními organizacemi a aktivně zapojovat komunitu do společných akcí. Tuto tabulku lze najít v Příloze P IV: Analýzy SWOT organizací. Dalším krokem je vylepšení bezpečnostního prostředí, jako jsou kamery a prostředky pro ochranu před fyzickou krádeží. Tabulky strategií se nachází v Příloze P V: Strategie SWOT analýzy.

SWOT analýza obecního úřadu

Pro obecní úřad byla vytvořena SWOT analýza, která slouží k systematickému hodnocení jeho silných stránek, slabých stránek, příležitostí a hrozeb. Tato analýza byla prováděna za účasti respondentů, kteří poskytli své názory a informace. Těmito respondenty byl pracovník

úřadu a starosta obce. Kromě toho byla využita i umělá inteligence, která přispěla k objektivnímu zhodnocení dat a k identifikaci klíčových oblastí pro zlepšení. SWOT analýza poskytuje obecný přehled o stavu obecního úřadu a jeho okolí, což umožňuje lépe porozumět jeho silným a slabým stránkám.

Výsledek ukázal, že vhodnou strategií pro obecní úřad je defenzivní strategie. Na základě výsledku byly vytvořeny kroky pro zlepšení vnitřního a vnějšího prostředí. Výsledek pro tuto analýzu lze najít v Příloze P I: Výsledek analýz SWOT.

Tato strategie by měla být zaměřena na posílení bezpečnosti, efektivity a zlepšení služeb poskytovaných místní komunitě. Zároveň se strategie soustředí na posílení bezpečnostních opatření, jako je informování občanů o kybernetických hrozbách a zajištění dostupnosti zálohovaných dat.

4.1.2 Závěr analýzy SWOT

Pro každou organizaci byly identifikovány hodnotné atributy a na základě toho byla navržena specifická strategie. Pro knihovnu byla doporučena strategie spojenectví. Pro obecní úřad byla navržena strategie defenzivní.

4.2 Identifikace aktiv

Tato kapitola se bude věnovat hodnocení aktiv a také hodnocení na základě CIA. Každá složka tohoto hodnocení představuje důležitý prvek:

- Důvěrnost (Confidentiality).
- Integrita (Integrity).
- Dostupnost (Availability).

Toto hodnocení bylo provedeno podle metodiky CIA, založené na Metodice stanovení požadavků na bezpečnost informačního systému (IS). Pro tento proces byla využita Příloha č.4 - Souhrnné analytické zprávy poskytovaná Národním úřadem pro kybernetickou a informační bezpečnost (NÚKIB).

Seznam primárních aktiv byl poskytnut a následně ohodnocen. Tato metodika slouží jako vodítko pro správce IS, kteří určují úroveň bezpečnostních opatření, jež je třeba zajistit interně nebo prostřednictvím služeb eGC (elektronického Government Cloud) (NÚKIB, 2018).

Každé aktivum bylo ohodnoceno na základě interview s respondenty, kteří zodpovídali otázky týkající se reálných scénářů nejhoršího případu. Jako vodítko pro toto hodnocení byla použita dopadová tabulka, která je součástí Metodiky k vodítkům pro hodnocení dopadů (NÚKIB, 2018).

Byly vytvořeny katalogy primárních aktiv, které byly společně s respondenty pečlivě vybrány. Každé z těchto primárních aktiv bylo ohodnoceno pomocí principů důvěrnosti, integrity a dostupnosti (CIA). Tento proces vycházel z Průvodce řízením aktiv a rizik dle vyhlášky o kybernetické bezpečnosti (NÚKIB, 2022).

V knihovně byly identifikovány aktiva se zaměřením na digitální prvky. Tabulku se všemi aktivy naleznete v Příloze P II: Tabulky aktiv. Jako primární aktivum knihovny byl vybrán Portál Tritius, kterým je správcem nadřízená knihovna a který zajišťuje půjčování knih.

Tabulka 1 - Katalog primárních aktiv knihovny (zdroj: vlastní zpracování)

KATALOG PRIMÁRNÍCH AKTIV KNIHOVNY						
ID	**Systém/aplikace/přístup**	**Popis**	**Kategorie**	**Priorita**	**Záloha**	**Osobní údaje**
S1	Portál Tritius	Knihovna	Služba	nízká	správce/nadřízená knihovna	ano

V této tabulce byly identifikovány dvě primárná aktiva, kterými jsou služby, jenž obecní úřad používá pro své každodenní fungování.

Tabulka 2 - Katalog primárních aktiv obecního úřadu (zdroj: vlastní zpracování)

KATALOG PRIMÁRNÍCH AKTIV OBECNÍ ÚŘAD						
ID	**Systém/aplikace/přístup**	**Popis**	**Kategorie**	**Priorita**	**Záloha**	**Osobní údaje**
S1	KEO 4.	Ekonomika	Služba	kritická	1x měsíčně. Plná	ano
S2	TACITUS NG	Správa	Služba	nízká	1x měsíčně. Plná	ano

4.3 Hodnocení aktiv CIA

V této kapitole proběhne hodnocení aktiv CIA. Hodnotící kritéria jsou navržena s využitím podpůrných materiálů poskytovaných NÚKIB. Každá analýza je upravena dle specifických potřeb organizace. V tabulkách níže bude uvedeno hodnocení aktiv a výsledná tabulka.

Po vytvoření katalogů aktiv byla provedena zhodnocení všech aktiv pomocí dopadové tabulky, která je k dispozici v Příloze P III: Dopadová tabulka. Tato tabulka poskytuje strukturovaný přehled o potenciálním dopadu různých hrozeb a incidentů na jednotlivá aktiva. Zjednodušená dopadová tabulka se nachází níže.

Tabulka 3 - Základní hodnocení úrovně dopadu (zdroj: vlastní zpracování)

Úroveň dopadu	
0	nerelevantní
1	nízká
2	střední
3	vysoká
4	kritická

Tabulka 4 – Hodnocení primárních aktiv Knihovny (zdroj: vlastní zpracování)

CIA HODNOCENÍ AKTIV KNIHOVNY																							
Hodnocení narušení bezpečnosti dat a informací na		Dostupnost										Ztráta						Důvěrnost			Integrita		
Respondent	Kategorie dat a informací	Nedostupnost 15 min.	Nedostupnost 1h.	Nedostupnost 4h.	Nedostupnost 8h.	Nedostupnost 16h.	Nedostupnost 1 den.	Nedostupnost 2 dny.	Nedostupnost 1 týden.	Nedostupnost 14 dní.	Nedostupnost měsíc a více.	Ztráta dat od zálohy (1hod.)	Ztráta dat od zálohy (4hod.)	Ztráta dat od zálohy (8hod.)	Ztráta dat od zálohy (16hod.)	Ztráta dat od zálohy (14 dní.)	Úplná ztráta dat	Prozrazení v rámci organizace.	Prozrazení smluvním partnerem.	Prozrazení vně organizace.	Modifikace dat malého rozsahu.	Modifikace dat velkého rozsahu.	Úplná modifikace.
Pověřený pracovník knihovny	A. Bezpečnost a zdraví osob	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	B. Ochrana osobních údajů.	1	1	1	1	1	1	1	2	2	3	1	1	1	2	3	3	1	2	2	2	2	2
	C. Zákonné a smluvní povinnosti	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	D. Trestně-právní řízení	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	E.Veřejný pořádek	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	F.Mezinárodní vztahy	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	G.Řízení a provoz organizace	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1	2
	H. Ztráta důvěryhodnosti	1	1	1	1	1	1	1	1	2	2	1	1	1	1	1	1	1	1	1	1	1	1
	I. Finanční ztráty	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	J. Zajišťování nezbytných služ	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	3	1	1	1	1	1	2
	Komentář k dopadům.	Ttitius je software pro půjčování knížek. Je zde riziko napadení výpůjčního systému, kde mohou uniknout osobní data čtenářů, nebo přihlašovací údaje do e-mailu knihovny nebo údaje do zařízení, která využívají. Co se týče naší knihovny, výpadek by neměl takový význam, jen v případě, že by unichly osobní data. Knihovna dokáže pracovat i bez systému, svoji činnost může nahradit manuálním zapisováním.Únik osobních údajů je v rámci knihovny rizikovější, co se týče dat, zálohování není pravidelné tudíž úplná ztráta dat by mohla být větším problémem.																					

Tabulka 5- Výsledné hodnocení primárního aktiva (Tritius), (zdroj: vlastní zpracování)

Software Tritius		Hodnota
Výsledná hodnocení primárního aktiva (nejvyšší hodnoty jednotlivých atributů)	**Dostupnost**	1
	Ztráta	3
	Důvěrnost	2
	Integrita	2

Obecní úřad si pro své hodnocení primárních aktiv vybral softwary, které používá ke své každodenní činnosti. TACITUS NG a KEO 4. TACITUS NG slouží k digitalizaci a obsahuje osobní údaje. KEO 4. je software zabezpečující správy peněz.

Tabulka 6 – Hodnocení primárního aktiva Obecního úřadu (KEO), (zdroj: vlastní zpracování)

CIA HODNOCENÍ AKTIV OBECNÍ ÚŘAD																						
Hodnocení narušení bezpečnosti dat a informací na		Dostupnost										Ztráta						Důvěrnost			Integrita		
Respondent	Kategorie dat a informací	Nedostupnost 15 min.	Nedostupnost 1h.	Nedostupnost 4h.	Nedostupnost 8h.	Nedostupnost 16h.	Nedostupnost 1 den.	Nedostupnost 2 dny.	Nedostupnost 1 týden.	Nedostupnost 14 dní.	Nedostupnost měsíc a více.	Ztráta dat od zálohy (1hod.)	Ztráta dat od zálohy (4hod.)	Ztráta dat od zálohy (8hod.)	Ztráta dat od zálohy (16hod.)	Ztráta dat od zálohy (14 dní.)	Úplná ztráta dat	Prozrazení v rámci organizace.	Prozrazení smluvním partnerem.	Prozrazení vně organizace.	Modifikace dat malého rozsahu.	Modifikace dat velkého rozsahu.	Úplná modifikace.
Starosta obce	A. Bezpečnost a zdraví osob	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	B. Ochrana osobních údajů.	1	1	1	1	1	1	1	1	1	1	1	1	2	2	3	4	2	2	2	2	2	2
	C. Zákonné a smluvní povinnosti	1	1	1	1	1	1	2	2	2	3	1	1	2	2	2	3	1	1	1	2	2	3
	D. Trestně-právní řízení	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	E.Veřejný pořádek	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	F.Mezinárodní vztahy	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	G.Řízení a provoz organizace	1	1	1	2	2	3	3	3	4	4	1	1	1	1	2	2	1	1	1	2	2	3
	H. Ztráta důvěryhodnosti	1	1	1	1	2	1	1	1	3	3	1	1	1	1	1	2	1	1	2	1	1	2
	I. Finanční ztráty	2	2	2	2	3	3	3	3	3	3	1	1	1	2	2	4	2	2	2	2	2	2
	J. Zajišťování nezbytných služeb	1	1	1	2	2	2	3	3	4	4	1	1	1	2	2	3	1	1	1	3	3	4
	Komentář k dopadům.	KEO je software, který využíváme pro správu peněz. Jeho nedostupnost sebou nese mnoho rizik. Pokud tento systém vypadne, není možné vykonávat běžnou činnost, pokud by výpadek trval déle mohl by ohrozit fungování obce a zajišťování bezpečnosti obyvatel. Při ztrátě dat porušujeme GDPR a je je narušena důvěrnost. Únik dat by mohl mít velký vliv na ztrátu peněz. V případě nečinnosti systému je v mnoha věcech nezastupitelný.																				

Tabulka 7 – Výsledné hodnocení primárního aktiva (KEO 4.), (zdroj: vlastní zpracování)

Software KEO 4.		Hodnota
Výsledná hodnocení primárního aktiva (nejvyšší hodnoty jednotlivých atributů)	Dostupnost	4
	Ztráta	4
	Důvěrnost	2
	Integrita	3

Tabulka 8 – Hodnocení primárního aktiva Obecního úřadu (TACITUS NG), (zdroj: vlastní zpracování)

CIA HODNOCENÍ AKTIV OBECNÍ ÚŘAD																						
Hodnocení narušení bezpečnosti dat a informací na		Dostupnost										Ztráta						Důvěrnost			Integrita		
Respondent	Kategorie dat a informací	Nedostupnost 15 min.	Nedostupnost 1h.	Nedostupnost 4h.	Nedostupnost 8h.	Nedostupnost 16h.	Nedostupnost 1 den.	Nedostupnost 2 dny.	Nedostupnost 1 týden.	Nedostupnost 14 dní.	Nedostupnost měsíc a více.	Ztráta dat od zálohy (1hod.)	Ztráta dat od zálohy (4hod.)	Ztráta dat od zálohy (8hod.)	Ztráta dat od zálohy (16hod.)	Ztráta dat od zálohy (14 dní.)	Úplná ztráta dat	Prozrazení v rámci organizace.	Prozrazení smluvním partnerem.	Prozrazení vně organizace.	Modifikace dat malého rozsahu.	Modifikace dat velkého rozsahu.	Úplná modifikace.
Zaměstnanec obecního úřadu	A. Bezpečnost a zdraví osob	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	B. Ochrana osobních údajů.	1	1	1	1	1	1	1	1	1	2	1	1	1	2	2	3	2	2	3	2	3	3
	C. Zákonné a smluvní povinnosti	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	D. Trestně-právní řízení	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	E.Veřejný pořádek	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	F.Mezinárodní vztahy	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	G.Řízení a provoz organizace	1	1	1	1	1	2	2	2	2	3	1	1	1	2	2	2	1	1	1	2	2	3
	H. Ztráta důvěryhodnosti	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1	2	1	1	1	1	1	1
	I. Finanční ztráty	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	J. Zajišťování nezbytných služ	1	1	1	1	1	1	1	1	1	2	1	1	1	1	2	3	1	1	1	1	1	2
	Komentář k dopadům.	Software TACITUS NG používáme pro pomoc při digitalizaci. Jsou v něm osobní údaje, to znamená že jejich ztráta přináší rizika. Pokud nejsou data dostupná omezuje to činnost obecního úřadu.																					

Tabulka 9 – Výsledné hodnocení primárního aktiva (TACITUS NG), (zdroj: vlastní zpracování)

Software TACITUS NG		Hodnota
Výsledná hodnocení primárního aktiva (nejvyšší hodnoty jednotlivých atributů)	Dostupnost	2
	Ztráta	2
	Důvěrnost	2
	Integrita	3

4.4 ANALÝZA RIZIK

Další částí práce je analýza kybernetických hrozeb, která bude provedena ve třech fázích:

1. **Analýza typových zranitelností a hrozeb.**
2. **Fraud Risk Assessment (FRA).**
3. **Dotazníkové šetření.**

V prví části analýzy byl vytvořen katalog rizik, kde se pracovalo s primárními aktivy. Tato analýza neobsahuje žádná hodnocení, pouze identifikuje možné spojení hrozeb a zranitelností.

4.4.1 Analýza typových zranitelností a hrozeb

Pro tuto analýzu byly vybrány relevantní hrozby a zranitelnosti z katalogu NÚKIB a navrženy konkrétní kroky k minimalizaci rizika. Tato analýza se zaměřuje pouze na vybrané typové hrozby a zranitelnosti. Neposkytuje ale komplexní přehled všech kybernetických rizik.

Tabulka 10 – Katalog rizik (zdroj: vlastní zpracování)

KATALOG RIZIK						
ID	**Organizace**	**Aktivum**	**Zranitelnost**	**Hrozba**	**Způsob zvládání rizika**	**Návrh opatření**
S1	Knihovna	Portál Tritius	4. Nedostatečné bezpečnostní povědomí lidských zdrojů	11.Pochybení ze strany zaměstnanců a administrátorů	Redukce	Poskytnout zaměstnancům a administrátorům pravidelná školení ohledně bezpečnostních postupů, politik a procedur, aby byli lépe informováni o správných postupech a rizicích.
S1	Obecní úřad	KEO4.	8.Nedostatečná ochrana aktiv	9.Ztráta, odcizení nebo poškození aktiva	Redukce	Provádět pravidelné bezpečnostní audity a penetrační testy k identifikaci možných slabých míst a zranitelností v ochraně aktiv. Vypracovat a pravidelně aktualizovat incidentní plány pro rychlou reakci v případě ztráty, odcizení nebo poškození aktiv, aby se minimalizovaly škody a obnovila normální činnost.
S2	Obecní úřad	TACITUS NG	11.Nedostatek zaměstnanců s potřebnou odborností	11.Pochybení ze strany zaměstnanců a administrátorů	Redukce	Poskytnout existujícím zaměstnancům možnosti rekvalifikace a školení, aby získali potřebné odborné dovednosti a znalosti. Provést aktivní rekrutaci nových zaměstnanců s potřebnou odborností.

4.4.2 Fraud Risk Assessment

Tato analýza identifikovala a hodnotila kybernetická rizika v kontextu dané organizace. Proběhlo zde také hodnocení současného opatření, přičemž zároveň bylo poskytnuto nové opatření pro zmírnění rizik.

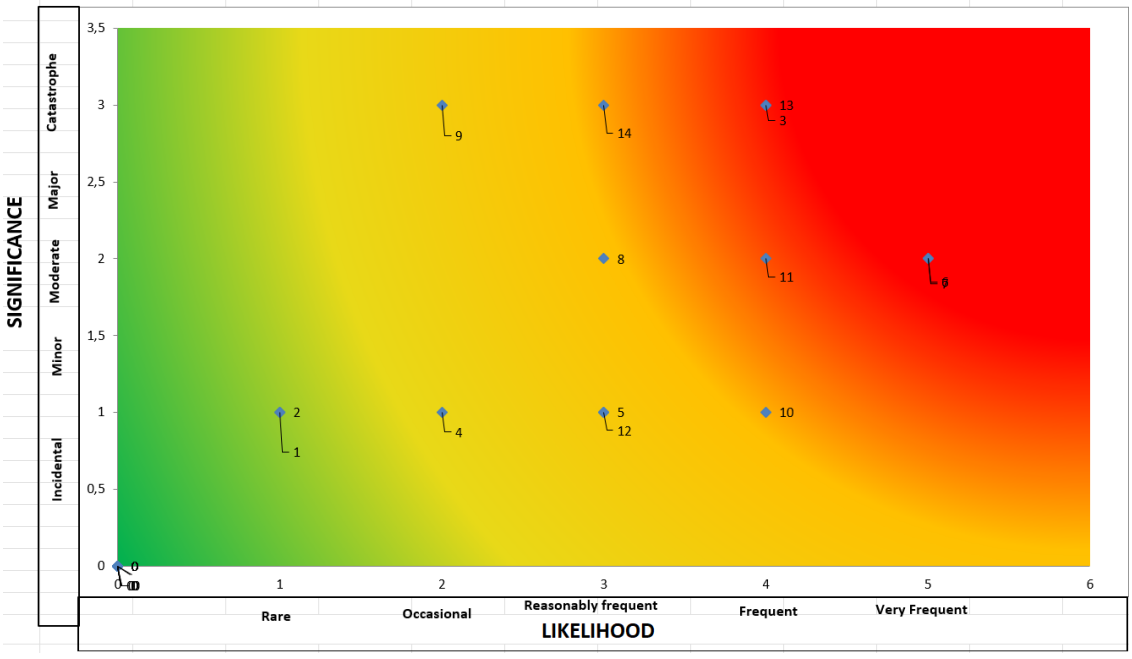
Obsah analýzy FRA byl upraven a zkrácen pro potřeby organizace. V této analýze lze nalézt jak identifikaci zranitelností, tak hrozeb. Tato analýza ovšem navíc poskytuje hodnocení pravděpodobnosti, významu a hodnocení účinnosti kontrol. Kritéria pro toto hodnocení lze

nalézt v Příloze P VII: Kritéria pro hodnocení analýzy Fraud Risk Asseeement. Hodnocení bylo vypracováno společně s respondenty. Analýza byla zaměřena na identifikaci klíčových nedostatků, které by mohly představovat největší hrozby pro organizaci.

Pro zobrazení výsledků používá tato analýza vizuální nástroj Heat mapu, která pomocí barevných odstínů zobrazuje různé úrovně hodnocených rizik. Tyto odstíny barev slouží k rychlému a snadnému pochopení, které oblasti jsou nejvíce ohroženy nebo vystaveny určitým rizikům, podobně jako v dopadové matici.

Tabulka 11 – Zdroje rizik pro knihovnu (zdroj: vlastní zpracování)

ZDROJE RIZIK: KNIHOVNA			
1	Chybějící VPN	**8**	Chybějící opatření proti fyzické krádeži
2	Chybějící VPN	**9**	Chybějící opatření proti fyzické krádeži
3	Nízká úroveň ochrany proti spamu	**10**	Mezery při využívání WI-FI hotspot
4	Zaměstnanci jsou zároveň obyvateli obce	**11**	Mezery při využívání WI-FI hotspot
5	Příchozí excelové tabulky	**12**	Nepravidelná aktualizace
6	Nezabezpečený vstup externích disků	**13**	Nepravidelné zálohování
7	Nezabezpečený vstup externích disků	**14**	Nepravidelné zálohování



Obrázek 6 – Heat mapa knihovny (zdroj: vlastní zpracování)

Mapa rizik identifikuje **5 oblastí**, které představují pro knihovnu nejvyšší kybernetická rizika:

a) 6. Nezabezpečený vstup externích disků: Uživatelé mohou do notebooků knihovny připojovat nekontrolovaná externí zařízení, čímž se do knihovní sítě dostávají potenciální hrozby. Knihovna postrádá bezpečnostní opatření pro regulaci vstupu externích zařízení.

b) 9. Nedostatečná fyzická ochrana: Knihovna nemá žádné bezpečnostní prvky kromě dveří, které by mohly zabránit neoprávněnému přístupu a krádeži zařízení.

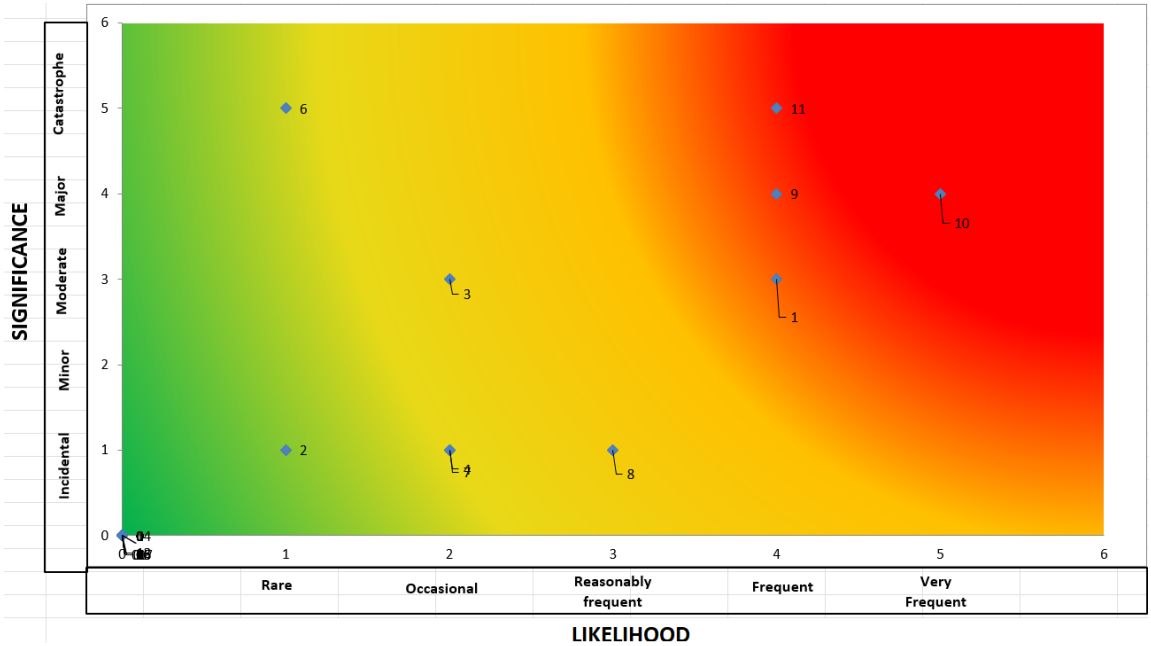
c) 13.Nepravidelné zálohování: Knihovna neprovádí pravidelné a dostatečné zálohování dat, čímž riskuje jejich ztrátu v případě havárie systému nebo krádeže zařízení. Zálohování na externí disky je nespolehlivé a v případě ztráty disku se data ztrácejí.

d) 3. Nízká úroveň ochrany proti spamu: Knihovna používá e-mailovou komunikaci, která je náchylná k phishingovým útokům a šíření malwaru.

e) 11. Mezery v zabezpečení Wi-Fi hotspotu: Knihovna používá Wi-Fi hotspot, který je náchylný k bezpečnostním zranitelnostem. Knihovna by měla sledovat aktualizace od výrobce a instalovat dostupné opravy.

Tabulka 12 - Zdroje rizik pro Obecní úřad (zdroj: vlastní zpracování)

ZDROJE RIZIK: OBECNÍ ÚŘAD	
1	Odklad aktualizací
2	Falešné přístupové body
3	Odcizení externího disku
4	Nezabezpečené webové stránky
6	Chybějící ochrana plat. terminálů
7	Nesprávná konfigurace systému TACTIKUS NG
8	Příchozí excelové tabulky
9	Nízká úroveň ochrany proti spamu
10	Nepravidelné zálohování
11	Chybějící ochrana plat. terminálů



Obrázek 7 – Heat mapa obecního úřadu, (zdroj: vlastní zpracování)

Mapa rizik identifikuje **3 oblastí**, které představují pro Obecní úřad nejvyšší kybernetická rizika:

a) 10. Ztráta dat by mohla mít pro Obecní úřad řadu negativních důsledků. Prvním z nich je narušení chodu úřadu, kdy ztráta dat znemožní plnění úkolů, které byly uloženy zastupitelstvem nebo radou obce. Dále by došlo k ohrožení důvěrnosti osobních údajů, protože ztráta dat s citlivými informacemi o občanech by mohla vést k porušení jejich soukromí a ohrozit jejich bezpečnost.

b) 9. Nedostatečné povědomí o kybernetických hrozbách je dalším problémem, se kterým se Obecní úřad potýká. Zaměstnanci nemusí být plně informováni o rizicích spojených s phishingovými útoky a dalšími hrozbami v e-mailu.

c) 1. Zanedbávání aktualizací softwaru je dalším problémem, se kterým se Obecní úřad potýká. Starší a neaktualizovaný software obsahuje známé chyby a zranitelnosti, které mohou útočníci zneužít k napadení systémů.

4.4.3 Dotazníkové šetření

Ve všech organizacích bylo provedeno dotazníkové šetření na téma zálohování a ochrana dat. Na dotazník odpovědělo celkem 108 respondentů. Dotazník obsahoval celkem 17 otázek. Respondenti odpovídali zcela anonymně. Vyhodnocení otázek, které sloužily k potvrzení nebo vyvrácení hypotéz, bude uvedeno následně. Obsah otázek lze nalézt v Příloze

P VIII: Dotazníkové šetření. Výsledky a odpovědi tohoto dotazníku lze najít v Příloze P IX: Výsledky dotazníkového šetření.

Dotazník sloužil pro upřesnění zaměření návrhové části, kde se zabýváme zálohováním a bezpečností dat. Dotazník měl odpovědět na následující hypotézy:

1) V organizaci obec a knihovna se aktivně starají o bezpečnost dat, mají proškolený personál a dbají o pravidelné aktualizace.
2) Přestože organizace má proškolený personál, pravidelně zálohuje a aktivně se stará o bezpečnost svých dat, může stále existovat riziko pro únik dat důvodu nedostatečného povědomí kybernetických hrozbách.

Výsledky vybraných otázek říkají že: (41,7 %) respondentů nezálohuje nikdy svá data. Překvapivě (20,4 %) respondentů provádí zálohy týdně. Nejmenší část, pouze (9,3 %) respondentů, zálohuje svá data denně. Téměř polovina respondentů (48,5 %) zálohuje svá data pomocí cloudových úložišť a podobných služeb, zatímco další polovina (28,8 %) využívá externí disky k zálohování. Téměř polovina respondentů (48,1 %) se spoléhá na antivirovou ochranu. Menší, ale stále významná část respondentů, uvádí, že používá silná hesla (41,7 %). Další významná část respondentů (25 %) pravidelně aktualizuje svůj software. Avšak 15,7 % respondentů neprojevuje žádnou péči o bezpečnost svých dat. Další otázka č.8 zaměřená na bezpečnost dat se zabývala způsoby, jakými respondenti pečují o bezpečnost svých dat. Největší procento odpovědí se odkazovalo na dvoufaktorové ověření (42,6 %). Další významné procento (31,5 %) respondentů uvedlo fyzické zabezpečení jako způsob ochrany svých dat.

Z otázky č.6 se zjistilo, že tři čtvrtiny respondentů (75 %) odpovědělo že neví, jak by postupovali v případě obnovy svých dat ze zálohy. Souhrn odpovědí na tuto ověřovací otázku lze nalézt v Příloze P IX: Výsledky dotazníkového šetření.

Výsledek hypotéz

Z výsledků, které poskytlo dotazníkové šetření se zjistilo, že první hypotéza byla nepotvrzena pouze částečně. Otázky zaměřující se na povědomí organizací na zabezpečení svých dat se potvrdilo, že rizika stále existují.

Zaměstnanci a uživatelé nejsou dostatečně proškoleni v oblasti kybernetické bezpečnosti. V tom případě byla hypotéza č.1 nepotvrzena. Druhá hypotéza byla na základě odpovědí respondentů potvrzena. Zjištěné nedostatky budou řešeny v návrhové části této práce.

4.5 Diskuse

Analytická část práce měla za cíl analyzovat kybernetické hrozby organizací. Pro celkovou analýzu byla využita metodika hodnocení rizik poskytovanou NÚKIB. Tato metodika zahrnovala identifikaci hrozeb, zranitelností a hodnocení aktiv, která byla identifikována prostřednictvím řízených rozhovorů. Identifikované hrozby se ohodnotili pomocí katalogu zranitelností, přičemž hrozby s nimi související byly přiřazeny z katalogu hrozeb. Tyto katalogy vytvořil NÚKIB a obsahují typové hrozby a zranitelnosti.

Podrobnější analýza pomocí metody Fraud Risk Assessment zahrnovala hodnocení pravděpodobnosti, významu a stávajících opatření. V této analýze byly identifikovány oblasti, které organizacím představují největší nebezpečí. Následně bylo provedeno vyhodnocení dotazníku, který byl poskytnut zaměstnancům a návštěvníkům těchto organizací, a podařilo se získat 108 respondentů. Dotazníkové šetření mělo za úkol potvrdit nebo vyvrátit stanovené hypotézy.

Existují akademické práce, které se zabývají podobnému tématu. V diplomové práci Jana Kazíka z roku 2022 měl student za úkol navrhnout příručku kybernetické bezpečnosti pro vybraný subjekt. Pro analýzu zvolil analytickou analýzu KARS a FMEA (Kazík, 2022). Stejně jako v této práci je jméno organizace anonymizováno. Celkově lze říct, že malé podniky a organizace se kybernetickou bezpečností téměř nezabývají. Proto může být analýza rizik provedená v těchto pracích pro tyto organizace přínosná.

Otázkou však zůstává, jak obecně tyto organizace přimět k budování kultury kybernetické bezpečnosti. Dalším problémem může být finanční stránka podniků a organizací, které nemají finanční prostředky na potřebnou ochranu a prevenci.

Analýza kybernetických hrozeb a návrhy opatření k jejich zmírnění prezentované v této práci poskytují cenné poznatky v oblasti kybernetické bezpečnosti. Použitím metodologií jako je analýza rizik a provedením komplexní analýzy nabízí studie praktický přístup k identifikaci zranitelností a hrozeb. Porovnání s podobnými studiemi a identifikace otevřených otázek, budoucích směrů přispívá k probíhající diskusi o kybernetické bezpečnosti v organizacích. Poskytnutá doporučení mohou sloužit jako směrnice pro organizace, které si přejí zlepšit svá postavení v oblasti kybernetické bezpečnosti, zejména pro ty, které nemají finanční prostředky na rozsáhlé investice do bezpečnostních opatření.

5 OCHRANA V KYBERPROSTORU

Návrhová část práce se zaměřuje na návrh opatření pro jednotlivé organizace. Jednotlivé části navrženého opatření a doporučení byly pečlivě vybrány na základě nejlepších znalostí a porozumění kybernetické bezpečnosti.

Tyto znalosti vycházejí z odborné literatury, komunikace s odborníky v oboru kybernetické bezpečnosti a studia relevantní legislativy a doporučení. Pro každou organizaci bude navrženo řešení, které se zaměří především na identifikovaná rizika, s důrazem na ochranu v kyberprostoru.

5.1 Návrh opatření pro knihovnu

Návrh pro knihovnu se bude zaměřovat na zlepšení fyzické bezpečnosti prostředí, ochranu externích disků, pravidelné zálohování dat, bezpečnosti modemu k eliminaci potenciálních bezpečnostních mezí využívání WI-FI hotspotů a ochrany zařízení.

Fyzická bezpečnost

Knihovna se nachází mezi dalšími subjekty, avšak budova není zcela chráněna obvodovou ochranou. Před knihovnou je umístěna kamera, která má za úkol sledovat vstupní prostor do zahrady knihovny a nástěnku knihovny.

Abychom zlepšili fyzickou bezpečnost, doporučuji ohradit vstupní prostor. To zahrnuje: kamerový systém, navrhuji zaměřit kameru především na vstup do knihovny, aby byl vstupní prostor co nejlépe monitorován. Fyzická kontrola vstupu do budovy bude zajištěna pomocí kamerového systému, protože identifikace návštěvníků pomocí ID není z finančních důvodů možná.

Co se týče ochrany zařízení, je důležité vést evidenci půjčování notebooků. To usnadní zpětné vyhledávání případných problémů. Externí disky by měly být bezpečně uloženy např. v archivu a jejich půjčování by mělo být také evidováno. Archiv by měl být umístěn tak, aby nebyl veřejnosti přístupný, případně by měl být zamčen a klíč by měla mít osoba zodpovědná za archivaci (Čermák, 2023).

Ochrana zařízení

Další částí fyzické ochrany je ochrana zařízení. Silové a datové kabely budou chráněny před poškozením a vzájemným rušením. Zařízení zpracovávající kritické nebo citlivé informace budou umístěny v zabezpečeném prostoru, a zajištěna bude ochrana proti blesku. Opravy a

servis zařízení budou prováděny pouze oprávněnými osobami, a o všech podezřelých chybách budou vedeny záznamy.

Firewall ochrana modemu

Pro knihovny je nezbytné chránit modem desktopovým firewallem. Firewall slouží jako bariéra mezi modemem a internetem. Blokuje přístup k počítači neoprávněným uživatelům a škodlivému softwaru, čímž chrání knihovní síť před viry, trojskými koni a jinými hrozbami, filtruje příchozí a odchozí internetový provoz a blokuje nevyžádané dotazy, čímž snižuje riziko zahlcení sítě a kybernetických útoků. Desktopový firewall umožňuje uživateli kontrolovat, které aplikace se mohou připojovat k internetu. To je důležité pro omezení přístupu k potenciálně škodlivým webům a aplikacím a pro ochranu citlivých dat knihovny.

Několik důležitých bodů o nastavení firewallu zahrnuje správnou konfiguraci firewallu, jeho ochranu, nastavení a pomoc při luštění hlášení. Firewall by měl být odolný proti pokusům malwaru o odstranění či deaktivaci a měl by být integrován hluboko do operačního systému, aby kontroloval veškerý provoz v síti na nejnižších vrstvách modelu OSI. Nastavení firewallu je důležité a často složité, a proto je nutné věnovat mu pečlivou pozornost. Firewall se může často ptát, zda má povolit připojení nějakého programu k internetu, a je proto doporučeno hledat informace o daném programu na internetu. Hardwarové firewally poskytují další úroveň ochrany proti útokům z internetu, avšak i tyto firewally mají svá rizika, a je proto důležité je správně nastavit a aktualizovat (Arnold, 2008).

Antivirová ochrana

Knihovna by měla využívat antivirový software z důvodu ochrany proti škodlivému softwaru, jako jsou viry a malware. Antivirový software provádí skenování zařízení a sítě s cílem detekovat, blokovat a odstranit viry a malware. Využívá k tomu různé metody, včetně skenu souborů, heuristiky, kontroly velikosti souborů a kontrolních součtů, aby identifikoval potenciálně nebezpečný software. Tím pomáhá chránit knihovní systémy a uživatele před možnými kybernetickými hrozbami a zabezpečuje bezpečné prostředí pro práci s digitálními zdroji.

Vzhledem k omezeným finančním prostředkům knihovny je vhodné hledat alternativy antivirového programu, které jsou zdarma, ale přesto poskytují spolehlivou ochranu. Mezi takové antivirové programy patří například Avast Free Antivirus, AVG Antivirus Free nebo

Avira Free Antivirus. Tyto programy nabízejí základní ochranu proti virům a malware bezplatně a jsou dobrým řešením pro knihovny s omezeným rozpočtem. Doporučuji vyhradit prostředky pro kompletní antivirový program, jako je Microsoft Defender, Bitdefender apod. které jsou pro tento rok hodnoceny jako nejlepší. Linux je obecně považován za bezpečný operační systém, protože se vyznačuje minimálním rizikem virů a malware (Glamoslija, 2024).

Používání antivirového programu v Linuxu je obvykle zbytečné pro ochranu samotného systému. Doporučené antivirové programy jsou např. ClamAV, Chkrookit nebo Bitdefender Antivirus for Unices (Davison, 2024).

Ochrana externích disků

Pro ochranu externích disků je důležité zvážit heslování, nebo zašifrování dat. Použití heslem chráněného nebo zašifrovaného disku může výrazně snížit riziko úniku dat. Běžní uživatelé nebudou mít přístup k datům, a také zkušení hackeři budou mít přístup k citlivým informacím ztížen. Doporučuji knihovně, aby si zašifrovala své flash disky pomocí softwaru BitLocker a VeraCrypt (dříve TrueCrypt).

Dále je důležité vypnout funkci *„autorun“* v systému Windows, která automaticky spouští programy z externích disků. To zabrání spuštění škodlivého softwaru, který by se mohl nacházet na disku (Grabowska, 2024).

Školení o vzdělávání v oblasti kybernetické bezpečnosti

Vzdělávání zaměstnanců v oblasti kybernetické bezpečnosti je klíčové pro ochranu organizace před hrozbami. Pro knihovnu je důležité nabídnout zaměstnancům a uživatelům efektivní školení a zdroje, které jim pomohou lépe porozumět kybernetickým hrozbám, kybernetické bezpečnosti a naučit se, jak se jim úspěšně bránit.

Doporučuji knihovně nabídnout zaměstnancům kurzy a e-learningové materiály, které jsou dostupné zdarma a poskytují základní znalosti kybernetické bezpečnosti. Mezi takové zdroje patří například kurz "Dávej kyber", který se zaměřuje na základy kybernetické bezpečnosti. Kromě toho knihovna může využít materiály od ESET zaměřené na ochranu firemních dat před kybernetickými útoky nebo techniky obrany proti phishingovým útokům. Tyto materiály jsou poskytovány zdarma a stačí pouze přihlášení k odběru (NÚKIB, 2022).

Dalším krokem by mohlo být proškolení zaměstnanců v identifikaci a kontrole e-mailů jako preventivní opatření proti phishingovým útokům. To by mohlo zahrnovat školení

zaměstnanců v rozpoznávání podezřelých e-mailů, včetně znaků phishingu a správného postupu při jejich identifikaci a nahlášení. Školení by mohlo významně přispět ke zlepšení bezpečnostní kultury v knihovně a snížení rizika úspěšných kybernetických útoků.

Pro hlášení kybernetických incidentů doporučuji se seznámit s metodikou "Hlášení kybernetického bezpečnostního incidentu". Tato metodika je základním nástrojem k plnění povinností podle „zákona č. 181/2014 Sb., o kybernetické bezpečnosti“. Poskytuje podrobné pokyny, jak identifikovat, dokumentovat a hlásit kybernetické incidenty. Seznámení se s touto metodikou umožní knihovně řádně plnit své povinnosti v oblasti kybernetické bezpečnosti (NÚKIB, 2024).

Zavedení bezpečnostní politiky

Zde jsou některá opatření, která mohou pomoci omezit rizika spojená s chováním uživatelů na internetu a jejich administrátorskými právy:

- **Omezení administrátorských práv:** Administrátorská práva by neměla být přidělována všem uživatelům. Místo toho by měla být přidělována pouze těm, kteří je skutečně potřebují pro svou práci.
- **Zásady pro otevírání souborů:** Uživatelé by měli být obeznámeni s pravidly pro otevírání souborů. Neprověřené přílohy e-mailů by neměly být otevírány, pokud uživatel nemá jistotu o jejich původu.

I když Tritius slouží k uchovávání různých informací, nejen o půjčování knih, samotný proces půjčování knih probíhá manuálním zápisem a následným zápisem do softwaru.

5.2 Návrh opatření pro Obecní úřad

Pro Obecní úřad byla navržena opatření, která se budou zaměřovat na:

- Nepravidelné zálohování.
- Nízkou úroveň proti spamu.
- Pravidelné aktualizace.

Zálohovací strategie pro Obecní úřad

Pro ochranu dat obecního úřadu a zajištění bezpečnosti datového úložiště je důležité implementovat efektivní zálohovací plán. Zde jsou klíčové kroky, které by měl takový plán zahrnovat:

- **Automatizace zálohování:** Zálohování by mělo být nastaveno tak, aby probíhalo automaticky bez nutnosti manuálního zásahu. Tímto způsobem se zajistí konzistence a minimalizuje se riziko lidských chyb.
- **Bezpečné uchovávání záloh:** Zálohy by měly být uchovávány na bezpečném místě mimo pracoviště, aby byly chráněny před fyzickými hrozbami, jako jsou požáry, povodně nebo krádeže.
- **Testování obnovy dat:** Pravidelné testování obnovy dat ze záloh je nezbytné pro ověření, že data lze úspěšně obnovit v případě potřeby.
- **Diferencované zálohování:** Použití různých metod a úrovní zálohování (např. inkrementální, diferenciální, plné zálohování) pro různé typy dat a systémů (Elhenický, 2012).

Doporučená softwarové řešení zdarma:

- AOMEI Backupper Standard.
- EaseUS Todo Backup Free.
- FBackup.

Doporučená placená softwarová řešení:

- Acronis True Image.
- Ashampoo.
- EaseUS Todo Backup Home (Popescu, 2024).

Doporučená softwarová řešení open source:

- UrBackup
- Bacula (Saashub, 2018).

Archivace

Archivace slouží pro dlouhodobé uchování dat, u kterých není potřebná rychlá obnova. Pro archivaci je nutné zvolit vhodné místo a vhodná média. Doporučuji použít klasické HDD disky. Ve skladovaných prostorách by se měla uchovávat nejlépe stabilní teplota.

Ochrana proti spamu

Pro Obecní úřad doporučuji následující doporučení:

- Nastavení antispamových filtrů na e-mailovém serveru, které automaticky identifikují a blokují nevyžádané e-maily. Dále je důležité nastavit filtrování e-mailů na základě klíčových slov, adres odesílatele a dalších parametrů.
- Zaměstnanci by měli být školeni v rozpoznávání podezřelých e-mailů a charakteristických znaků phishingu, například neznámý odesílatel či žádosti o citlivé informace. Dále je důležité vzdělávat zaměstnance o bezpečném chování na internetu, aby byli obezřetní při klikání na neznámé odkazy a nedávali do e-mailů citlivé informace, jako jsou hesla či čísla kreditních karet.
- Procvičení zaměstnanců v rozpoznávání phishingových e-mailů pomocí poskytnutí falešných phishingových e-mailů a sledování reakcí zaměstnanců (Microsoft, 2016).

Politika aktualizace

Pravidelné opakování procesu a aktualizace nástrojů jsou nezbytné pro udržení bezpečnosti. Zde jsou uvedené body, které by měly obecnímu úřadu pomoci s pravidelnou aktualizací:

- Definujte plán aktualizací softwaru, který určí četnost a postup aktualizace pro všechny používané aplikace a systémy.
- Nastavte automatické aktualizace pro veškerý používaný software tam, kde to je možné. Tím minimalizujete riziko zranitelností spojených s neaktuálním softwarem.
- Využijte centrálního správce aktualizací, který umožňuje sledovat a řídit aktualizace všech softwarových aplikací z jednoho místa.
- Školte zaměstnance o důležitosti pravidelné aktualizace softwaru a o postupech pro aktualizaci jejich pracovních prostředků.
- Pravidelně kontrolujte dostupnost nových aktualizací.

Zákaz automatického otevírání maker v excelových tabulkách

V Microsoft Excel je možné nastavit zabezpečení tak, aby se makra nespouštěla automaticky. Toto opatření lze provést změnou nastavení v Centru zabezpečení aplikace. Lze využít pro Excel 2021, 2019, 2016, 2013. Uživatelé by měli vždy ověřit zdroj souboru nebo dokumentu před jeho otevřením, zejména pokud pochází z e-mailu nebo internetu (Microsoft, ©2024).

Školení zaměstnanců

Využijte e-learning, poskytované materiály např. od NÚKIB či ESET, nebo udělejte pravidelná školení, která budou zvyšovat povědomí vašich zaměstnanců a vytvořte doporučení pro návštěvníky. Můžete se nechat inspirovat materiály z NÚKIB. Doporučené vzdělávací kurzy najdete na stránce: https://www.nukib.cz/cs/infoservis/doporuceni/

5.3 Obecná doporučení pro ochranu v kyberprostoru

Kromě hlavních doporučení týkajících se analýzy rizik zde bude uvedeno pár preventivních doporučení, na které se mohou zaměřit jak knihovna, tak obecní úřad, ale také uživatelé respektive návštěvníci.

Investice do testovacího softwaru

Jako první věc, která je doporučena pro všechny, nejen tyto organizace, je investování do testovacího softwaru, který poskytuje organizacím nástroje k identifikaci a simulaci různých typů kybernetických útoků a hrozeb. Další výhodou testovacích softwarů je neustálý monitoring. Díky softwaru je možné provádět pravidelné analýzy a testovat nová opatření.

Metody zálohování

Nespoléhejte na zálohování na externí disky nebo na Cloudové úložiště, tyto způsoby jsou v organizacích použity nejvíce. Zálohování nebo také *„backup“* je při napadení hackerem možná poslední možnost, kdy je možné získat zpět svá data. U externího úložiště může dojít k hardwarovému poškození. Zvažte například jednu z metod zálohování:

- **Mirroring (RAID)**

  Jedná se o jeden ze způsobů zálohování, kdy je možné spojit několik pevných nebo jiných disků do jednoho logického úložiště. Přičemž každá jednotka je optimalizována na konkrétní situaci.

- **Replikační zálohování**

  Zálohovaná data ukládá do trezorů, které poskytují různé možnosti replikace pro zajištění redundance dat. Standardními možnostmi jsou:

  a) Místně redundantní úložiště (LRS).

  b) Geograficky redundantní úložiště (GRS).

  c) Zónově redundantní úložiště (ZRS).

  Zálohovat můžete např:

1) Místní zálohy a virtuální počítače.
2) SQL Server – databáze spuštěné na virtuálních počítačích (Microsoft, 2024).

- **Zálohování metodou 3-2-1**

Tato metoda je jedna z nejúčinnějších způsobů zálohování dat, doporučovaný odborníky na kybernetickou bezpečnost i vládou USA.

Princip pravidla spočívá v tom, že si máte udělat 3 kopie dat, ty rozdělit na 2 média a 1 z nich umístit na jinou lokalitu. Tak máte jistotu, že budete mít vždy alespoň jeden nepoškozený soubor dat.

Pravidlo 3-2-1 uvádí:

a) **3 kopie dat:** Udělejte si alespoň 3 zálohy dat.
b) **2 různá média:** Ukládejte soubory na 2 různé typy úložišť.
c) **1 kopie mimo pracoviště:** Udržujte jednu kopii mimo pracoviště, abyste zabránili ztrátě dat v důsledku selhání na konkrétním pracovišti (Ko, 2023).

Ochrana před Scam útoky

Jedná se o podvodné útoky označující pokus o získání něčeho hodnotného od oběti pomocí klamání a podvodu. Mezi hlavní znaky těchto útoků patří přílišné naléhání, nabízení podezřele výhodné nabídky, neočekávané ověření účtu ale také věrohodná zpráva od blízkého. Jakými způsoby se můžeme chránit:

a) Dvoufaktorové ověření.
b) Kontrolujte adresy URL, nebo předčíslí volajícího.
c) Neklikejte na náhodné odkazy a ověřujte si pravost zdroje.
d) Udržujte svoje zařízení aktualizované.

Určení administrátora a jeho práv a povinností

Pro každou organizaci doporučuji zvolení administrátora, který bude zodpovídat za infrastrukturu účty apod. Doporučení pro administrátory doporučuji nastudovat z materiálů od NÚKIB, konkrétně NIS2 Nejnovější legislativu EU pro oblast kybernetické bezpečnosti, kde poslední straně dokumentu najdete Bezpečnostní doporučení NÚKIB pro administrátory 4.0 (Walgaard, a další, 2023).

5.4 Reakce na hrozby

Reakce na hrozby v kyberprostoru je klíčovým prvkem každé kybernetické strategie. Tyto hrozby můžou ohrozit jak soukromé osoby, tak i celé organizace a státy. Reakce na hrozby zahrnuje soubor strategií a opatření, které mají za cíl:

- **Identifikovat** kybernetické hrozby a jejich potenciální dopady.
- **Analyzovat** zranitelnosti a rizika v kyberprostoru.
- **Prevence** na kybernetické útoky a minimalizovat jejich dopady.
- **Reagovat** na kybernetické incidenty a obnovit narušené systémy.
- **Zajišťovat** kontinuitu provozu a odolnost vůči kybernetickým hrozbám (Evropská rada, 2023).

Základní principy při reakci na hrozbu:

1. Odpojte počítač k zamezení odesílání nebo stahování.
2. Počítat vypněte, pokud je to možné.
3. Změňte hesla pro všechny své online účty.
4. Zkontrolujte bankovní a kreditní karty.
5. Naskenujte počítač antivirovým, nebo antispyware programem.
6. Nahlaste útok, pokud se stanete obětí phishingového e-mailu nebo jiného kybernetického útoku, měli byste to nahlásit (Matesvaprava, 2022).

Další postupy mohou být:

- Odpojení sítě.
- Zablokování platebních karet.
- Odpojení od účtu.
- Zabezpečte webovou kameru.

Důležitost reakce na kybernetické útoky často závisí na závažnosti útoku a typu organizace, ve které se incident odehrává. Zatímco menší útoky mohou být rutinně zvládnuty bez větších následků, větší útoky mohou mít značný dopad na činnost organizace. Každá organizace má odlišnou politiku týkající se hlášení kybernetických incidentů. Zatímco některé organizace mohou preferovat otevřenost a rychlé hlášení všech incidentů, jiné mohou mít zavedené postupy, které stanovují, které incidenty musí být nahlášeny a jakým způsobem.

ZÁVĚR

Cílem bylo vylepšení kybernetické bezpečnosti ve vybraných organizacích. Těmito organizacemi byla místní knihovna a obecní úřad. V každé z těchto organizací bylo nutné zjistit na jaké úrovni kybernetické bezpečnosti se nachází. Pro organizace byly vytvořeny strategie SWOT, které vycházely z poskytnutých analýz. Poté byla zahájena analýza rizik. Prvně bylo nutné zjistit, jaká aktiva se v každé organizaci nacházejí a určit primární aktiva. Po identifikaci aktiv, které bylo vypracováno společně s respondenty následovalo hodnocení aktiv, pro které byla použita metodu CIA, kteří byla hodnocena podle aspektů dostupnosti, ztráty a integrity. Jakmile byla aktiva ohodnocena byla vytvořena analýza rizik pomocí typových hrozeb a zranitelností, které poskytuje NÚKIB. Následná analýza měla identifikovat širší škálu hrozeb. Pro tuto analýzu byla vybrána analýza Fraud Risk Assesment. V obou z těchto analýz bylo navrženo opatření, které mělo vylepšit dosavadní úroveň opatření.

Pro knihovnu byly identifikovány jako nejnebezpečnější rizika nezabezpečený vstup externích disků, mezery při používání WI-FI hotspot, nedostatečná fyzická ochrana, nepravidelné zálohování a nízká úroveň proti spamu. U obecního úřadu se vyskytl jako největší problém nepravidelné zálohování, nedostatečné povědomí o kybernetických hrozbách a zanedbávání aktualizací.

Na základě identifikovaných rizik bylo navrženo opatření proti hrozbám pro každou organizaci zvlášť a také obecná doporučení pro ochranu v kyberprostoru. Na závěr návrhové části byl vytvořen krátký přehled doporučení pro reakce na kybernetické útoky.

Z výsledů dotazníkového šetření se návrhy opatření zaměřily na slabá místa, kterými bylo zálohování a bezpečnost dat.

V teoretické části bylo za úkol vymezit základní pojmy z této oblasti. Proto byly jako hlavní témata vybrány kyberprostor a kyberkriminalita. Dalším bodem v teoretické části bylo pojednat o historii kybernetických hrozeb do které byly zahrnuty i aktuální trendy.

Výsledkem analytické části bylo vytvoření analýzy kybernetických hrozeb pro obě organizace. V návrhové části na základě zjištěných rizik navrhnou opatření a reakce na tyto hrozby. Dalšími dílčími úkoly bylo vymezení pojmů z oblasti kyberprostoru, kyberkriminality, kybernetické bezpečnosti a následovná geneze kybernetických hrozeb.

Analýza kybernetických hrozeb malých organizací může přinést pohled pro další malé podniky, které se nachází v podobné situaci, s podobnými aktivy, nebo podobnou úrovní zabezpečení.

Práce na analýze kybernetických hrozeb mě vtáhla do nového odvětví kyberprostoru a tento směr se mi zalíbil. Proto jsem se také rozhodla v této oblasti dále pohybovat.

SEZNAM POUŽITÉ LITERATURY

ACRESIA, 2020. *Analýza rizik*. Online. In: Acresia.com. Dostupné z: https://acresia.com/index.php/sluzby/69-analyza-rizik. [cit. 2024-04-18].

ARCTIC WOLF, 2022. *A Brief History of Cybercrime*. Online. In: Arcticwolf.com. Dostupné z: https://arcticwolf.com/resources/blog/decade-of-cybercrime/. [cit. 2024-04-19].

ARNOLD, Arne, 2008. *Vše, co potřebujete vědět o firewallech*. Online. In: Computerworld.cz. Dostupné z: https://www.computerworld.cz/clanky/vse-co-potrebujete-vedet-o-firewallech/. [cit. 2024-04-27].

BAGGE, Daniel P., 2015. *BSS469 Kybernetická bezpečnost: Historické aspekty kybernetické bezpečnosti*. Online. In: Is.muni.cz. Dostupné z: https://is.muni.cz/el/fss/podzim2015/BSS469/um/BSS469_6.10.pdf. [cit. 2024-04-18].

BARLOW, Perry, 1996. *A Declaration of the Independence of Cyberspace*. Online. In: Eff.org. Dostupné z: https://www.eff.org/cyberspace-independence. [cit. 2024-04-18].

BASTL, Martin a GRUBEROVÁ, Zuzana, 2013. *Kyberprostor jako „pátá doména"? Vojenské rozhledy*. Roč. 22 (54), č. 4, s. 10-21. ISSN ISSN 1210-3292.

BELCIC, Ivan, 2023. *What Is Malware and How to Protect Against Malware Attacks: What is Malware?* Online. In: Avast.com. 25.10.2023. Dostupné z: https://www.avast.com/c-malware. [cit. 2024-04-18].

BERGMANS, Bart Lenaerts, 2023. *What is a supply chain attack?* Online. In: Crowdstrike.com. Dostupné z: https://www.crowdstrike.com/cybersecurity-101/cyberattacks/supply-chain-attacks/. [cit. 2024-04-19].

BERNATÍK, Aleš, 2016. Analýza nebezpečí a rizik. Online. In: Ostrava, s. 20. Dostupné z: https://www.fbi.vsb.cz/export/sites/fbi/cs/.content/galerie-souboru/U3V/studijni-materialy/U3V_Analyza_nebezpeci_a_rizik.pdf. [cit. 2024-04-18].

BEZPECNOSTPRACE, 2021. *Kybernetická a informační bezpečnost: Legislativa, povinnosti a typy kybernetických útoků*. Online. In: Bezpecnostprace.info. Dostupné z: https://www.bezpecnostprace.info/kybernetika-informace/kyberneticka-bezpecnost-legislativa-povinnost/. [cit. 2024-04-18].

BIGYZR, 2018. *1. Informace, data, informatika*.Online. In: Dostupné z: https://www.bigyzr.cz/shared/clanky/2893/ICT-Pripravy/IS4-Pripravy_informace.pdf. [cit. 2024-04-18].

BRUSH, Kate a COBB, Michael, 2024. *Cybercrime*. Online. In: Techtarget.com. Dostupné z: https://www.techtarget.com/searchsecurity/definition/cybercrime. [cit. 2024-04-18].

CISA, 2021. *What is Cybersecurity?* Online. In: Cisa.gov. Dostupné z: https://www.cisa.gov/news-events/news/what-cybersecurity. [cit. 2024-04-18].

CISCO, 2022. *What Is Cybersecurity?* Online. In: Cisco.com. Dostupné z: https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html. [cit. 2024-04-18].

CISCO, 2024. *What Is Phishing?* Online. In: Cisco.com. Dostupné z: https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html. [cit. 2024-04-18].

CLOUDFLARE, 2024. *What are the security risks of RDP? | RDP vulnerabilities*. Online. In: Cloudflare.com. Dostupné z: https://www.cloudflare.com/learning/access-management/rdp-security-risks/. [cit. 2024-04-18].

COSTIGAN, Sean S., 2014. *Cybersecurity, the internet of things, and the role of government*. Online. In: Diplomaticourier.com. Dostupné z: https://www.diplomaticourier.com/posts/cybersecurity-the-internet-of-things-and-the-role-of-government. [cit. 2024-04-26].

COURSERA, 2023. *What Is the CIA Triad?* Online. In: Coursera.org. Dostupné z: https://www.coursera.org/articles/cia-triad. [cit. 2024-04-18].

CS.BAB.LA, (bez data). *Jaký je překlad "security" v Česku?* Online. In: Cs.bab.la. Dostupné z: https://cs.bab.la/slovnik/anglicky-cesky/security. [cit. 2024-04-19].

ČERMÁK, Miroslav, 2023. *Kybernetická bezpečnost: základní fyzická bezpečnostní opatření*. Online. In: Cleverandsmart.cz. Dostupné z: https://www.cleverandsmart.cz/kyberneticka-bezpecnost-zakladni-fyzicka-bezpecnostni-opatreni/. [cit. 2024-04-27].

ČERNÝ, Michal, 2020. *Nové pojetí multikulturality jako klíče k bytí "onlife." Sociální pedagogika/Social Education*. S. 8(2), 10–28. ISSN 1805-8825.

ČIHÁK, Lukáš, 2022. *Co je to Dark Web, jak se na něj dostat a kam se na něm vydat?* Online. In: Cdr.cz. Dostupné z: https://cdr.cz/clanek/co-je-dark-web-jak-se-na-nej-dostat-kam-se-na-nem-vydat. [cit. 2024-04-18].

DAVIES, Vikki, 2021. *The history of cybersecurity*. Online. In: Cybermagazine.com. Dostupné z: https://cybermagazine.com/cyber-security/history-cybersecurity. [cit. 2024-04-18].

DAVISON, Kate, 2024. *5 nejlepších antivirů pro Linux v roce 2024*. Online. In: Cs.safetydecectives.com. Dostupné z: https://cs.safetydetectives.com/best-antivirus/linux/. [cit. 2024-04-28].

DEVOTEAM, 2023. *Dangers and Challenges of AI in Cybersecurity. Are You Prepared?* Online. In: Devoteam.com. Dostupné z: https://www.devoteam.com/expert-view/dangers-and-challenges-of-ai-in-cybersecurity/. [cit. 2024-04-18].

DICTIONARY.CAMBRIDGE, 2023. *Cybersecurity*. Online. In: Dictionaru.Cambridge.org. Dostupné z: https://dictionary.cambridge.org/dictionary/english/cybersecurity. [cit. 2024-04-18].

DODGE, Martin a KITCHIN, Rob, ©2021. *Mapping Cyberspace*. Milton: Routledge.

ELHENICKÝ, Jan, 2012. *Návrh zálohování dat pro městský úřad v Trutnově*. Bakalářská práce. Brno: Vysoké učení technické v Brně.

EPRAVO, 2024. *Kyberkriminalita a její vliv na obchodní společnosti*. Online. In: Epravo.cz. Dostupné z: https://www.epravo.cz/top/clanky/kyberkriminalita-a-jeji-vliv-na-obchodni-spolecnosti-117898.html. [cit. 2024-04-29].

EVROPSKÁ RADA, 2023. *Kybernetická bezpečnost: jak EU řeší kybernetické hrozby*. Online. In: Consilium.europa.eu. Dostupné z: https://www.consilium.europa.eu/cs/policies/cybersecurity/. [cit. 2024-04-26].

FORPSI, 2017. *Co je SSL certifikát*. Online. In: Forpsi.com. Dostupné z: https://www.forpsi.com/ssl/. [cit. 2024-04-18].

FRUHLINGER, John, 2020. *What is information security? Definition, principles, and jobs*. Online. In: Csoonline.com. Dostupné z: https://www.csoonline.com/article/568841/what-is-information-security-definition-principles-and-jobs.html. [cit. 2024-04-18].

GEEKSFORGEEKS, 2024. *What is Transmission Control Protocol (TCP)?* Online. In: Geeksforgeeks.org. 26.2.2024. Dostupné z: https://www.geeksforgeeks.org/what-is-transmission-control-protocol-tcp/. [cit. 2024-04-18].

GLAMOSLIJA, Katarina, 2024. *9 nejlepších antivirů pro Windows 2024 (ZCELA ZDARMA)*. Online. In: Cs.safetydetectives.com. 24.04.2024. Dostupné z: https://cs.safetydetectives.com/blog/nejlepsich-opravdu-zdarma-antiviru-pro-windows/. [cit. 2024-04-27].

GRABOWSKA, Karolina, 2024. *Jak zaheslovat externí disk nebo flashdisk*. Online. In: Premocz.eu. Dostupné z: https://www.premocz.eu/jak-zaheslovat-externi-disk. [cit. 2024-04-27].

IRWIN, Luke, 2023. *Demystifying the CIA Triad: Why It's Crucial for Cyber Security*. Online. In: Itgovernance.co.uk. Dostupné z: https://www.itgovernance.co.uk/blog/what-is-the-cia-triad-and-why-is-it-important. [cit. 2024-04-18].
ISBN 978-0-415-19884-4.

IT-SLOVNIK, (bez data). *Co je to Bezpečnostní hrozba? Zdroj: https://it-slovnik.cz/pojem/bezpecnostni-hrozba/?utm_source=cp&utm_medium=link&utm_campaign=cp*. Online. In: Itslovnik.cz. Dostupné z: https://it-slovnik.cz/pojem/bezpecnostni-hrozba. [cit. 2024-04-18].

JIRÁSEK, Petr; NOVÁK, Luděk a POŘÁR, Josef, 2015. *Výkladový slovník kybernetické bezpečnosti*. Online. In: Nukib.gov.cz. Dostupné z: https://nukib.gov.cz/download/publikace/podpurne_materialy/Vkladov%20slovnk_5.ver.pdf. [cit. 2024-04-19].

JIRÁSEK, Petr; NOVÁK, Luděk a POŽÁR, Josef, 2022. *Výkladový slovník kybernetické bezpečnosti*. Online. In: Cybersecurity.cz. Dostupné z: https://www.cybersecurity.cz/data/Slovnik_523el.pdf. [cit. 2024-04-26].

KASPERSKY, 2022. *What is an IP Address – Definition and Explanation*. Online. In: Kaspersky.com. Dostupné z: https://www.kaspersky.com/resource-center/definitions/what-is-an-ip-address. [cit. 2024-04-18].

KASPERSKY, 2022. *What is Cryptojacking and how does it work?* Online. In: Kaspersky.com. Dostupné z: https://www.kaspersky.com/resource-center/definitions/what-is-cryptojacking. [cit. 2024-04-18].

KASPERSKY, 2022. *What is Cybersecurity? Types, Threats and Cyber Safety Tips*. Online. In: Kaspersky.com. Dostupné z: https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security. [cit. 2024-04-18].

KASPERSKY, 2022. *What is SQL injection? Definition and explanation*. Online. In: Kaspersky.com. Dostupné z: https://www.kaspersky.com/resource-center/definitions/sql-injection. [cit. 2024-04-18].

KAZÍK, Jan, 2022. *Kybernetická bezpečnost vybraného subjektu*. Diplomová práce. Uherské Hradiště: Univerzita Tomáše Bati ve Zlíně.

KELLEY, Diana, 2023. *Top 3 ransomware attack vectors and how to avoid them*. Online. In: Techtarget.com. Dostupné z: https://www.techtarget.com/searchsecurity/tip/Top-3-ransomware-attack-vectors-and-how-to-avoid-them. [cit. 2024-04-18].

KERNER, Sean Michael, 2024. *Ransomware trends, statistics and facts heading into 2024*. Online. In: Techtarget.com. Dostupné z: https://www.techtarget.com/searchsecurity/feature/Ransomware-trends-statistics-and-facts. [cit. 2024-04-18].

KHELGHATI, Mohammadreza; HIEMSTRA, Djoerd a KEULEN, Maurice van, 2012. *Deep web entity monitoring*. Online. In: Research.utwente.nl. Dostupné z: https://research.utwente.nl/en/publications/deep-web-entity-monitoring-2. [cit. 2024-04-18].

KHERA, Varin, 2020. *The Web Layers: Introduction to Surface, Deep and Darknet*. Online. In: Cyberprotection-magazine.com. Dostupné z: https://cyberprotection-magazine.com/the-web-layers-introduction-to-surface-deep-and-darknet. [cit. 2024-04-18].

KO, Matias, 2023. *Řešení zálohování dat s pravidlem 3-2-1*. Online. In: Msi.com. Dostupné z: https://cz.msi.com/blog/a-backup-solution-for-you-with-3-2-1-data-backup-rule. [cit. 2024-04-22].

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

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

KOREN, Miroslav, 2023. *Sociální inženýrství: Aktuální hrozby a budoucí výzvy*. Online. In: Linkedin.com. Dostupné z: https://www.linkedin.com/pulse/soci%C3%A1ln%C3%AD-in%C5%BEen%C3%BDrstv%C3%AD-aktu%C3%A1ln%C3%AD-hrozby-budouc%C3%AD-v%C3%BDzvy-miroslav-koren/. [cit. 2024-04-19].

KRESA, Dan, 2023. *Analýza bezpečnosti #2: Co jsou aktiva a jak je evidovat?* Online. In: Kybez.cz. Dostupné z: https://kybez.cz/analyza-bezpecnosti-2-co-jsou-aktiva-a-jak-je-evidovat/. [cit. 2024-04-19].

LÁTAL, Jaroslav, 2016. *Zálohovací strategie a plán obnovy v malých firmách a organizacích*. Online. In: Linkedin.com. Dostupné z: https://www.linkedin.com/pulse/z%C3%A1lohovac%C3%AD-strategie-pl%C3%A1n-obnovy-v-mal%C3%BDch-firm%C3%A1ch-jaroslav-l%C3%A1tal/. [cit. 2024-04-26].

LAWINSIDER, 2019. *ICT Law definition*. Online. In: Lawinsider.com. Dostupné z: https://www.lawinsider.com/dictionary/ict-law. [cit. 2024-04-19].

LESSIG, Lawrence, 1999. *Code and Other Laws of Cyberspace*. New York: Basic Books. ISBN 0-465-03912-X.

LEWIK, 2015. *Bezpečnostní opatření (zákon o kybernetické bezpečnosti, § 4 - 6)*. Online. In: Lewik.org. Dostupné z: https://www.lewik.org/term/13376/bezpecnostni-opatreni-zakon-o-kyberneticke-bezpecnosti-4-6/. [cit. 2024-04-26].

MÁLEK, Zdeněk, ©2022. *Foto: Opravdu takto primitivně může vypadat úspěšný phishingový e-mail*. Online. In: Webdesign-karlovyvary.cz. Dostupné z: https://webdesign-karlovyvary.cz/down/202205/centrum-phishing.jpg. [cit. 2024-04-22].

MÁLEK, Zdeněk, 2022. *Jak funguje phishing a je stále úspěšný? Příklad z praxe*. Online. In: Webdesign-karlovyvary.cz. Dostupné z: https://webdesign-karlovyvary.cz/jak-funguje-phishing-a-je-stale-uspesny-priklad-z-praxe.html. [cit. 2024-04-26].

MALWAREBYTES, 2023. *AI in Cyber Security: Risks of AI*. Online. In: Malwarebytes. Dostupné z: https://www.malwarebytes.com/cybersecurity/basics/risks-of-ai-in-cyber-security. [cit. 2024-04-19].

MANAGEMENTMANIA, 2018. *Bezpečnostní Incident (Security Incident)*. Online. In: Managementmania.com. 17.02.018. Dostupné z: https://managementmania.com/cs/bezpecnostni-incident. [cit. 2024-04-19].

MATESVAPRAVA, 2022. *Byl/a jsem napaden, co mám dělat?* Online. In: Matesvaprava.cz. Dostupné z: https://matesvaprava.cz/byla-jsem-napadena-co-mam-delat. [cit. 2024-04-22].

MERRIAM-WEBSTER.COM, 2024. *Cybersecurity noun*. Online. In: Merriam-webster.com. 19.04.2024. Dostupné z: https://www.merriam-webster.com/dictionary/cybersecurity. [cit. 2024-04-19].

MICROSOFT, ©2024. *Změna nastavení zabezpečení maker v Excelu*. Online. In: Support. Microsoft.com. Dostupné z: https://support.microsoft.com/cs-cz/office/zm%C4%9Bna-nastaven%C3%AD-zabezpe%C4%8Den%C3%AD-maker-v-excelu-a97c09d2-c082-46b8-b19f-e8621e8fe373. [cit. 2024-04-28].

MICROSOFT, 2016. *Blokovat nebo povolit (Nastavení nevyžádané pošty)*. Online. In: Support. Microsoft.com. Dostupné z: https://support.microsoft.com/cs-cz/topic/blokovat-nebo-povolit-nastaven%C3%AD-nevy%C5%BE%C3%A1dan%C3%A9-po%C5%A1ty-48c9f6f7-2309-4f95-9a4d-de987e880e46. [cit. 2024-04-28].

MICROSOFT, 2023. *2022 in review: DDoS attack trends and insights*. Online. In: Microsoft.com. Dostupné z: https://www.microsoft.com/en-

us/security/blog/2023/02/21/2022-in-review-ddos-attack-trends-and-insights/. [cit. 2024-04-19].

MICROSOFT, 2023. *What is a DDoS attack?* Online. In: Microsoft.com. Dostupné z: https://www.microsoft.com/en-us/security/business/security-101/what-is-a-ddos-attack. [cit. 2024-04-19].

MICHALSONS, 2016. *What is IT law, ICT law or Cyber law?* Online. In: Michalsons.com. Dostupné z: https://www.michalsons.com/blog/what-is-it-law-ict-law-or-cyber-law/286. [cit. 2024-04-19].

MONROECOLLEGE, 2023. *Cybersecurity history: hacking & data breaches.* Online. In: Monroecollege.edu. Dostupné z: https://www.monroecollege.edu/news/cybersecurity-history-hacking-data-breaches. [cit. 2024-04-18].

NBÚ, 2005. *Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů*. Online. In: Nbu.cz. Dostupné z: https://www.nbu.cz/cs/pravni-predpisy/1089-zakon-c-4122005/. [cit. 2024-04-19].

NBÚ, 2015. *Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020*. Online. In: Nbú.cz. Dostupné z: https://www.govcert.cz/cs/informacni-servis/strategie-akcni-plan/. [cit. 2024-04-19].

NCSC, ©2020. *Business email compromise: Dealing with targeted phishing emails*. Online. In: Ncsc.gov.uk. Dostupné z: https://www.ncsc.gov.uk/files/Business-email-compromise-infographic.pdf. [cit. 2024-04-19].

NIETZSCHE, Friedrich, 2023. *Citáty slavných osobností*. Online. In: Citaty.net. Dostupné z: https://citaty.net/citaty/270083-friedrich-nietzsche-ten-jenz-bojuje-s-monstry-by-si-mel-dat-pozor-a/. [cit. 2024-04-22].

NÚKIB, 2018. *Metodika k varování ze dne 17. prosince 2018*. Online. In: Nukib.gov.cz. 04.01.2019. Dostupné z: https://nukib.gov.cz/download/publikace/podpurne_materialy/2019_01_04_metodika_k_varov%C3%A1n%C3%AD_z_17-12-2018_v1.0.pdf. [cit. 2024-04-19].

NÚKIB, 2018. *Metodika k vodítkům hodnocení dopadů*. Online. In: Nukib.gov.cz. Dostupné z: https://nukib.gov.cz/download/publikace/podpurne_materialy/Metodika_k_voditkum_pro_hodnoceni_dopadu_NUKIB_v.1.2_s_prilohou.pdf. [cit. 2024-04-19].

NÚKIB, 2022. *Průvodce řízením aktiv a rizik dle vyhlášky o kybernetické bezpečnosti: https://nukib.gov.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/.*

Online. In: Nukib.gov.cz. Dostupné z: https://nukib.gov.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/. [cit. 2024-04-19].

NÚKIB, 2022. *Průvodce řízením aktiv a rizik dle vyhlášky o kybernetické bezpečnosti*. Online. In: Nukib.gov.cz. Dostupné z: https://nukib.gov.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/. [cit. 2024-04-19].

NÚKIB, 2022. *NÚKIB spouští aktualizovanou verzi on-line kurzu „Dávej kyber!“*. Online. In: Nukib.gov.cz. Dostupné z: https://nukib.gov.cz/cs/infoservis/aktuality/1841-nukib-spousti-aktualizovanou-verzi-on-line-kurzu-davej-kyber/. [cit. 2024-04-27].

NÚKIB, 2024. *Hlášení incidentů*. Online. In: Nukib.gov.cz. Dostupné z: https://nukib.gov.cz/cs/kontakty/hlaseni-incidentu/. [cit. 2024-04-27].

OTTIS, Rain a PEETER, Lorents, 2010. *Cyberspace: Definition and Implications*. Online. In: Proquest.com. Dostupné z: https://dumitrudumbrava.wordpress.com/wp-content/uploads/2012/01/cyberspace-definition-and-implications.pdf. [cit. 2024-04-18].

OXFORD, (bez data). *Cyberspace noun*. Online. In: Oxfordlearnersdictionaries.com. Dostupné z: https://www.oxfordlearnersdictionaries.com/definition/english/cyberspace. [cit. 2024-04-26]. POTTRELL, ©2024. *What is business email compromise?* Online. In: Meshsecurity.io. Dostupné z: https://www.meshsecurity.io/business-email-compromise. [cit. 2024-04-22].

POPESCU, Vladimír, 2024. *Software pro zálohování obrazu Windows 11: 5 nejlepších v roce 2024*. Online. In: Mspoweruser.com. 02.01.2024. Dostupné z: https://mspoweruser.com/cs/windows-11-image-backup-software/. [cit. 2024-04-28].

POŽÁR, Josef, 2005. *Informační bezpečnost*. Plzeň: Aleš Čeněk. ISBN 80-86898-38-5.

ROUSE, Margaret, 2017. *Cyberactivism*. Online. In: Technopedia.com. Dostupné z: https://www.techopedia.com/definition/27973/cyberactivism. [cit. 2024-04-19].

ROUSE, Margaret, 2023. *What Does Cyberspace Mean?* Online. In: Technopedia.com. Dostupné z: https://www.techopedia.com/definition/2493/cyberspace. [cit. 2024-04-19].

ŘEŠETKOVÁ, Dagmar, 2021. *Deep a Dark Web: Temné a neviditelné strany internetu*. Online. In: Abicko.cz. Dostupné z: https://www.abicko.cz/clanek/precti-si-technika/25986/deep-a-dark-web-temne-a-neviditelne-strany-internetu.html. [cit. 2024-04-19].

SAASHUB, 2018. *UrBackup VS Bacula*. Online. In: Saashub.com. Dostupné z: https://www.saashub.com/compare-urbackup-vs-bacula. [cit. 2024-04-28].

SEGAL, Adam, 2017. *The Hacker World Order: How Nations Fight, Maneuver, and Manipulate in the Digital Age*. New York: PublicAffairs™. ISBN 978-1-61039-872-5.

SHEA, Sharon a IREI, Alissa, 2023. *What is ransomware? How it works and how to remove it*. Online. In: Techtarget.com. Dostupné z: https://www.techtarget.com/searchsecurity/definition/ransomware. [cit. 2024-04-18].

SCHMIDT, Richard, 2012. *Memy a normativita kyberprostoru*. Online, Diplomová práce, vedoucí JUDr. Radim Polčák, PhD. Brno: Právnická fakulta Masarykovy univerzity. Dostupné z: https://is.muni.cz/th/nvl07/Kyberprostor_diplomka.pdf. [cit. 2024-04-19].

SIEMENS, 2023. *Kybernetická bezpečnost ve výrobě: Již to není téma jen pro specialisty*. Online. In: Visionmag.cz. Dostupné z: https://www.visionsmag.cz/kyberneticka-bezpecnost-ve-vyrobe-jiz-to-neni-tema-jen-pro-specialisty. [cit. 2024-04-19].

SOUČEK, Vladimír; STAŇOVÁ, Eva a LINHART, Martin, 2005. *Vnitřní bezpečnost a veřejný pořádek: Krizové řízení*. Online. In: Mvcr.cz. Dostupné z: https://www.mvcr.cz/clanek/prirucky-a-metodicke-pomucky.aspx?q=Y2hudW09Ng%3D%3D. [cit. 2024-04-26].

ŠTUSÁK, Michal, 2020. *Kybernetické hrozby proti kritické informační infrastruktuře v ČR*. Online, Bakalářská práce. Praha: Fakulta biomedicínského inženýrství. Dostupné z: https://theses.cz/id/36lcvb. [cit. 2024-04-19].

ŠULC, Vladimír, 2018. APT. In: *Kybernetická Bezpečnost*. Plzeň: Aleš Čeněk, s. 56–61. ISBN 978-80-7380-737-5.

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

ŠVEC, Jan, 2024. *Proč je důležité mít na webu SSL certifikát*. Online. In: Unifer.cz. Dostupné z: https://unifer.cz/jak-dulezite-je-miti-ssl-certifikat/. [cit. 2024-04-24].

THE UNITED STATES ARMY'S, 2010. *awatiations Concept Capability Plan 2016-2028*. Online. In: Irp.fas.org. Dostupné z: https://irp.fas.org/doddir/army/pam525-7-8.pdf. [cit. 2024-04-19].

TŘÍSKA, Tomáš, 2018. *Metodické doporučení k činnosti územních samosprávných celků.* Online. In: Mvcr.cz. Dostupné z: https://www.mvcr.cz/soubor/metodicke-doporuceni-k-cinnosti-uzemne-samospravnych-celku-obecni-urad.aspx. [cit. 2024-04-19].

TUNGGAL, Abi Tyas, 2023. *What is an Information Security Policy?* Online. In: Upguard.com. Dostupné z: https://www.upguard.com/blog/information-security-policy. [cit. 2024-04-19].

UTB, 2016. *Směrnice NIS*. Online. In: Utb.cz. Dostupné z: https://www.utb.cz/cybersecurity/nis/. [cit. 2024-04-19].

VAIDEESWARAN, Narendran, 2023. *What Is the Remote Desktop Protocol (RDP)?* Online. In: Crowdstrike.com. Dostupné z: https://www.crowdstrike.com/cybersecurity-101/remote-desk-protocol-rdp/. [cit. 2024-04-19].

VANĚK, Jiří, 2023. *Co je to útok zvaný Man in the Middle*. Online. In: Blog.jiriskrivanek.eu. Dostupné z: https://blog.jirivanek.eu/cs/2023/07/28/co-je-to-utok-zvany-man-in-the-middle/. [cit. 2024-04-19].

VOCABULARY, 2024. *Cyberspace*. Online. In: Vocabulary.com. 19.4.2024. Dostupné z: https://www.vocabulary.com/dictionary/cyberspace. [cit. 2024-04-19].

WALGAARD, Saranda a LAMERIAS, Andre, 2023. *NIS2: Nejnovější legislativa EU pro oblast kybernetické bezpečnosti*. Online. In: Eset.com. Dostupné z: https://www.eset.com/cz/prirucka-o-nis2/. [cit. 2024-04-22].

XIPHERA, 2020. *Example of TCP/IP operation over Ethernet*. Online. In: Xiphera.com. Dostupné z: https://xiphera.com/example-of-tcp-ip-operation-over-ethernet/. [cit. 2024-04-19].

XIPHERA, 2020. *Example of TCP/IP operation over Ethernet*. Online. In: Xiphera.com. Dostupné z: https://xiphera.com/wp-content/uploads/2023/09/xiphera_macsec_blog_3.png. [cit. 2024-04-22].

YASAR, Kinza a COBB, Michael, 2022. *Man-in-the-middle attack (MitM)*. Online. In: Techtarget.com. Dostupné z: https://www.techtarget.com/iotagenda/definition/man-in-the-middle-attack-MitM. [cit. 2024-04-19].

YASAR, Kinza a LUTKEVICH, Ben, 2020. *Transmission Control Protocol (TCP)*. Online. In: Techtarget.com. Dostupné z: https://www.techtarget.com/searchnetworking/definition/TCP. [cit. 2024-04-19].

ZEMAN, Petr, 2002. *Česká bezpečnostní terminologie: Výklad základních pojmů*. Online. In: Moodle.unob.cz. Dostupné z: https://moodle.unob.cz/pluginfile.php/11277/course/section/3043/%C4%8Cesk%C3%A1%20bezpe%C4%8Dnostn%C3%AD%20terminologie.pdf. [cit. 2024-04-26].

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AI	Artificial Intelligence
APT	Advanced Persistent Threat
BEC	Business Email Compromise
CISA	Certified Information Systems Auditor
CSS	Cascading Style Sheets
DDoS	Distributed Denial of Service
DoS	DoS Denial of Service
eGC	Electronic Governance Committee
EU	Evropská unie
FRA	Fraud Risk Aaaessment
GDPR	General Data Protection Regulation
GRS	Geographical Redundancy Storage
ICT	Informační a komunikační technologie
ID	Identity
INFOSEC	Information Security
IP	Internet Protocol
IS	Informační systém
IT	Informační technologie
LAN	Local Area Network
LRS	Long Range Surveillance
MAN	Metropolitan Area Network
MIMT	Man-in-the-middle útok
MIT	Massachusetts Institute of Technology
NCSC	National Cyber Security Centre

NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
OSI	Open Systems Interconnection
RaaS	Ransomware as a service
RAID	Redundant Array of Independent Disks
RDP	Remote Desktop Protocol
SQL	Structured Query Language
TCP	Transmission Control Protocol
TOR	The Onion Router
URL	Uniform Resource Locator
USA	United States of America
VPN	Virtual Private Network
WI-FI	Wireless Fidelity
WLAN	Wireless Local Area Network
ZRS	Zone Redundancy Storage

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM GRAFŮ

SEZNAM PŘÍLOH

PŘÍLOHA P I: VÝSLEDEK ANALÝZ SWOT

SWOT KNIHOVNA			
Silné stránky	Váha	Hodnocení	Výsledek
Lokální podpora	0,65	5	3,25
Personalizovaný servis	0,2	5	1
Omezená konkurence	0,15	2	0,3
Součet	1		4,55
Slabé stránky			
Omezený rozpočet	0,4	-5	-2
Omezený výběr	0,3	-2	-0,6
Omezené tech. možnosti	0,3	-4	-1,2
Součet	1		-3,8
Příležitosti			
Spolupráce	0,3	3	0,9
Online přítomnost	0,1	1	0,1
Granty a dotace	0,6	4	2,4
Součet	1		3,4
Hrozby			
Fyzické zabezpečení	0,2	-4	-0,8
Zastaralé technologie	0,1	-2	-0,2
Omezený zájem	0,7	-4	-2,8
Součet	1		-3,8
Interní		0,75	
Externí		-0,4	
Výsledek		0,35	

(zdroj: vlastní zpracování)

SWOT OBECNÍ ÚŘAD			
Silné stránky	Váha	Hodnocení	Výsledek
Lokální znalost	0,3	3	0,9
Osobní spojení	0,5	4	2
Flexibilita	0,2	1	0,2
Součet	1		3,1
Slabé stránky			
Omezené zdroje	0,05	-3	-0,15
Omezený personál	0,8	-5	-4
Omezený vliv	0,15	-3	-0,45
Součet	1		-4,6
Příležitosti			
Granty a dotace	0,75	4	3
Digitalizace	0,2	2	0,4
Partnerství s firmami	0,05	2	0,1
Součet	1		3,5
Hrozby			
Nízká zabezpečení	0,45	-3	-1,35
Politická nejistota	0,3	-2	-0,6
Ekonomická nestabilita	0,25	-1	-0,25
Součet	1		-2,2
Interní		-1,5	
Externí		1,3	
Výsledek		-0,2	

(zdroj: vlastní zpracování)

PŘÍLOHA P II: TABULKY AKTIV

Seznam aktiv knihovna				
Komunikační zařízení	**Datová média**	**Prostory a objekty**	**Technická zařízení**	**Hardware**
Internet,WIFI-hotspot	Flash disk	Knihovna 89 m2		Multifunkční tiskárna
Soukromý telefon	Externí disk	Kancelář 10 m2		
Modem	DVD, CD			Router
Firewall	SD karty			Notebooky
Word				Klávesnice
Excel				
ThunderBird				Projektor
Software	**Komunikační prostředky**	**Zásoby**	**Informace**	**Aplikace**
OS-Windows	Facebook	Spotřební materiál	Osobní informace	Tritius
OS-Linux	Webové stránky		GDPR prostřednictvím pověřence	
Portál Tritius	Nástěnka			
IPS				
Antivirový program Avast				
Grafické software				
Ovladače a software 3D tisk				
MS Office				
Záznamová média	**Bezpečnostní prvky**	**Personál**	**Ostatní**	**Vývoj**
FLASH Disk	GDPR nadřazená knihovna	Vrcholové vedení		Facebook
Externí disk		Pověřený pracovník knihovník		Webové stránky
DVD, CD		Uživatelé-čtenáři		Nástěnka

(zdroj: vlastní zpracování)

Seznam aktiv obecní úřad

Komunikační zařízení	Datová média	Prostory a objekty	Technická zařízení	Hardware
Internet, modem	Flash disk	prostor kanceláře obce 25 m2		Stolní PC
Soukromý telefon	Externí disk			Router
pevná linka	DVD, CD			Klávesnice
Firewall	SD karty			
Czech point				
Registr obyvatel				
Datová schránka				
Software	**Komunikační prostředky**	**Zásoby**	**Informace**	**Aplikace**
KEO 4.	Webové stránky	Spotřební materiál	Osobní informace	TACTIKUS NG
TACTIKUS NG	Nástěnka		GDPR prostřednictvím pověřence	
MS Office	Místní rozhlas			
Antivirový program Avast				
OS-Windows				
Záznamová média	**Bezpečnostní prvky**	**Personál**	**Ostatní**	**Vývoj**
FLASH Disk	GDPR – správce	Vrcholové vedení		
Externí disk		Pověřený pracovník – účetní a matrikářka v jedné osobě		
DVD, CD				

(zdroj: vlastní zpracování)

PŘÍLOHA P III: DOPADOVÁ TABULKA

Úroveň dopadu		0	1	2	3	4
		Nerelevantní	nízká	střední	vysoká	kritická
Vodítka pro určení závažnosti dopadů narušení bezpečnosti informací (dostupnost, důvěrnost, integrita)	A. Bezpečnost a zdraví osob		Žádné vodítko	Může vést k újmě (ohrožení osobní svobody nebo zranění) jedné nebo několika osob.	Může vést k újmě (ohrožení osobní bezpečnosti, svobody nebo zranění) větší skupiny osob, nebo ohrožení na životě jednotlivců.	Může vést k přímému ohrožení či ztrátě života skupiny osob.
	B. Ochrana osobních údajů		Může způsobit porušení etických, nikoli však právních předpisů vedoucí k negativním osobním dopadům na jednotlivce nebo skupinu osob.	Může způsobit porušení právních předpisů vedoucí k negativním dopadům na jednotlivce (pokuta až 10 mi. EUR nebo 2 % celkového ročního obratu - viz. Čl. 83/4 GDPR).	Může způsobit porušení právních předpisů vedoucí k negativním dopadům na velkou skupinu osob (pokuta až 20 mil. EUR nebo 4 % celkového ročního obratu - viz. Čl. 83/5 GDPR).	Žádné vodítko
	C. Zákonné a smluvní povinnosti		Může zapříčinit porušení interních předpisů a postupů, nikoli však porušení zákonných a smluvních povinností.	Může zapříčinit správní nebo občanskoprávní řízení vedoucí k pokutě nebo k náhradě škody.	Může zapříčinit porušení právních předpisů vedoucí k zahájení trestního stíhání.	Žádné vodítko
	D. Trestně-právní řízení		Žádné vodítko	Může vytvořit podmínky pro páchání trestné činnosti nebo může ztížit její vyšetřování.	Může vést k narušení vyšetřování trestné činnosti nebo soudní řízení (méně závažní kriminalita, krátkodobě, v jednotlivých případech).	Může vést k závažnému, dlouhodobému narušení schopnosti vyšetřovat trestnou činnost, popřípadě zpochybnění soudních čízení a rozhodnutí (závažná kriminalita, celkové zpochybnění systému).
	E. Veřejný pořádek		Žádné vodítko	Může zapříčinit rozsahem, formou nebo místem omezené protesty (lokální nepokoje).	Může zapříčinit rozsahem, formou nebo místem omezené protesty na úrovni významné části správního území obce s rozšířenou působností, jejichž řešení si může vyžádat aktivaci krizového řízení na úrovni kraje.	Může zapříčinit hromadné nepokoje, např. generální stávku, nebo jinak závažně narušit veřejný pořádek s celostátními dopady.
	F. Mezinárodní vztahy		Žádné vodítko	Může vytvářet negativní obraz ČR v jednom teritoriu, popř. v jednom státě.	Může vytvářet negativní obraz ČR ve světě.	Může negativně ovlivnit nebo poškodit diplomatické vztahy a tím způsobem nevýhodu pro zájmy ČR.

Vodítka pro určení závažnosti dopadů narušení bezpečnosti informací (dostupnost, důvěrnost, integrita)					
	G. Řízení a provoz organizace	Naruší řádné řízení nebo fungování části nebo celé organizace.	Může omezit provádění důležitých činností organizace.	Může způsobit dočasné zastavení nebo podstatné narušení důležitých činností organizace nebo poškodit rozvoj nebo prosazování cílů a zájmů organizace.	Může závažně a dlouhodobě ovlivnit vztahy s jinými organizacemi nebo veřejností s následkem celostátní či nadnárodní negativní publicity.
	H. Ztráta důvěryhodnosti	Může negativně ovlivnit vztahy s jinými částmi organizace, nebo jinými organizacemi nebo vztahy s veřejností, negativní publicita bude ale omezena na bezprostřední okolí a nebude mít dlouhé trvání.	Může negativně ovlivnit vztahy s jinými organizacemi nebo veřejností, negativní publicita se ale bude omezené zájmové skupiny nebo bude široká, avšak krátkodobá.	Může závažně ovlivnit vztahy s jinými organizacemi nebo veřejností s následkem celostátní negativní publicity.	Závažně a dlouhodobě ovlivní vztahy s jinými organizacemi nebo veřejností s následkem celostátní, či nadnárodní publicity, s dlouhodobými účinky a požadavky přijetí politické odpovědnostmi.
	I. Finanční ztráty	Může přímo nebo nepřímo vést ke ztrátám menším než 0,05 % ročního rozpočtu, popř. obratu organizace (v závislosti na typu organizace).	Může přímo nebo nepřímo vést ke ztrátám mezi 0,05 % a 2 % ročního rozpočtu, popř. obratu organizace (v závislosti na typu organizace).	Může mít přímo nebo nepřímo vést ke ztrátám vyšším než 2 ˇa nižším či rovným 10 % ročního rozpočtu, popř. obratu organizace). Pozn, v případě PZS je hranice ztráty stanovena na 0,25 % HDP.	Může přímo nebo nepřímo vést ke ztrátám přesahujícím 10 % ročního rozpočtu, popř. obratu organizace).
	J. Zajišťování nezbytných služeb	Žádné vodítko	Může způsobit závažné omezení či narušení nezbytných služeb pro malé množství osob.	Může způsobit závažné omezení či narušení nezbytných služeb pro více než 25 000 osob (v rámci kategorie provozovatelů základních služeb se může lišit dle právní úpravy pro jednotlivá odvětví viz. Vyhláška č. 437/2017 Sb.).	Může způsobit rozsáhlé omezení poskytování nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího více než 125 000 osob.

(zdroj: NÚKIB), (vlastní zpracování)

PŘÍLOHA P IV: ANALÝZY SWOT ORGANIZACÍ

Analýza SWOT knihovny

Základní faktory ovlivňující silné stránky podniku jsou:	Příklady slabých stránek podniku jsou:
• Malá knihovna může mít silné propojení s komunitou a získat podporu od místních obyvatel. • Možnost poskytovat osobní služby a poradenství pro čtenáře. • Bezdrátové připojení k internetu. • Firewall.	• Malé knihovny mohou mít omezené finanční zdroje pro nákup nových knih a modernizaci. • Malý počet čtenářů může omezovat diverzitu knižního fondu. • Nízký rozpočet. • Knihovna stojí na jednom člověku.
Příležitosti podle oboru podnikaní jsou:	**Hrozby podniku:**
• Vytvoření partnerství s místními školami pro podporu vzdělávacích programů. • Rozšíření knihovních služeb online, aby oslovila širší publikum. • Hledání a získávání grantů a dotací pro rozšíření knižního fondu a modernizaci knihovny.	• Rostoucí popularita elektronických knih a online knihkupectví může ovlivnit fyzické výpůjčky. • Omezený zájem veřejnosti. • Absence ochrany před fyzickou krádeží. • Bez VPN.

(zdroj: vlastní zpracování)

Analýza SWOT obecního úřadu

Základní faktory ovlivňující silné stránky podniku jsou:	Příklady slabých stránek podniku jsou:
• Obecní úřad má hluboké znalosti o potřebách a specifikách místní komunity. • Možnost navázání osobních vztahů s občany a vytvoření důvěry. • Flexibilita: Schopnost rychle reagovat na místní problémy a potřeby občanů.	• Omezené zdroje. • Nedostatečně zabezpečené prostory nebo zařízení mohou vést k fyzickému přístupu k datům a zařízením obecního úřadu. • Slabá správa hesel. • Nedostatečné zálohování dat.
Příležitosti podle oboru podnikaní jsou:	**Hrozby podniku:**
• Pravidelné auditování. • Spolupráce s externími odborníky. • Pravidelná aktualizace a upgrade softwaru a hardwaru. • Pravidelné zálohování dat a jejich ukládání na externí nebo cloudové úložiště může chránit úřad před ztrátou dat v důsledku havárie systému nebo útoku ransomware.	• Malware a ransomware mohou zablokovat přístup k datům a poškodit soubory. • Phishingové e-maily. • Fyzické bezpečnostní hrozby zahrnují krádež nebo poškození zařízení obsahující citlivá data, ať už záměrně nebo neúmyslně. • Pokud obecní úřad nedělá pravidelné zálohy svých dat, může dojít k nenávratné ztrátě důležitých informací při výpadku systému nebo poškození dat.

(zdroj: vlastní zpracování)

PŘÍLOHA P V: STRATEGIE SWOT ANALÝZ

<table>
<tr><th colspan="4">KNIHOVNA – Strategie spojenectví</th></tr>
<tr><th colspan="2" rowspan="2">SWOT Analýza</th><th colspan="2">Analýza vnitřního prostředí</th></tr>
<tr><th>Silné stránky</th><th>Slabé stránky</th></tr>
<tr><td rowspan="2">Analýza vnějšího prostředí</td><td>Příležitosti</td><td>• Vytvoření programů a služeb zaměřených na individuální potřeby čtenářů.
• Nabídka osobního poradenství a doporučení knih na základě zájmů a preferencí jednotlivých členů.
• Aktivní zapojení do komunity prostřednictvím pořádání kulturních a společenských událostí.
• Vytvoření dlouhodobých strategických partnerství s místními autoritami a institucemi pro posílení pozice na trhu.</td><td>• Hledání alternativních zdrojů financování, jako jsou granty, sponzorství od místních podniků nebo crowdfundingové kampaně, které umožní knihovně získat další finanční prostředky pro nákup nových knih a modernizaci.
• Spolupráce s místními organizacemi a komunitními skupinami s cílem rozšířit diverzitu knižního fondu.
• Zavedení online platformy pro půjčování e-knih a audioknih.
• Vyhledávání grantů a dotací zaměřených na modernizaci knihovny a zdokonalení technologických možností.</td></tr>
<tr><td>Hrozby</td><td>• Aktivní angažovanost knihovny v komunitě a poskytování osobních služeb a poradenství pro čtenáře může posílit vztahy s místními obyvateli a zvýšit jejich loajalitu ke knihovně.
• Využití monopolu na poskytování knihovnických služeb k posílení vlastního postavení a diferenciaci od online platforem.
• Nabídka speciálních služeb nebo programů, které nelze nahradit online prostředím.
• Organizace pravidelných setkání a akcí, které budou reflektovat potřeby a zájmy komunity a poskytovat prostor pro diskusi a interakci.</td><td>• Poskytnout kurzy a workshopy zaměřené na digitální gramotnost, aby se čtenáři naučili využívat elektronické knihy a online zdroje.
• Hledat granty a jiné finanční zdroje pro modernizaci technologií v knihovně, včetně zlepšení internetového připojení a přístupu k digitálním zdrojům.
• Zavést bezpečnostní opatření, jako jsou bezpečnostní kamery a vylepšené systémy dohledu.
• Zvážit investici do softwarových a hardwarových řešení pro ochranu dat a soukromí uživatelů.</td></tr>
</table>

(zdroj: vlastní zpracování)

OBECNÍ ÚŘAD – Defenzivní strategie			
SWOT analýza		**Analýza vnitřního prostředí**	
		Silné stránky	**Slabé stránky**
Analýza vnějšího prostředí	**Příležitosti**	• Vytvoření programů a služeb, které budou reflektovat specifické potřeby a hodnoty místní komunity, na základě hluboké znalosti oblasti. • Aktivní zapojení občanů do procesů rozhodování a plánování, aby byla zachována transparentnost a respektovány individuální potřeby. • Propojení digitalizace s flexibilitou a znalostmi místní komunity pro efektivní implementaci moderních informačních technologií, které budou přinášet reálnou hodnotu občanům.	• Vyhledávání grantů a dotací pro financování projektů a infrastruktury, které umožní rozšíření kapacit a zlepšení poskytovaných služeb. • Vytvoření strategických aliancí a partnerství s většími institucemi, nevládními organizacemi nebo sousedními obcemi k posílení politické váhy obecního úřadu a zvýšení jeho vlivu. • Využití grantů a dotací k investicím do digitalizace a modernizace infrastruktury, což umožní zlepšení efektivity a komunikace v rámci obecního úřadu a s občany.
	Hrozby	• Využití hlubokých znalostí o místní komunitě pro vytvoření vzdělávacích programů zaměřených na prevenci kybernetických hrozeb. • Poskytování informací občanům o bezpečnostních rizicích, jako jsou malware, phishingové e-maily a fyzické bezpečnostní hrozby. • Aktivní zapojení občanů do bezpečnostních opatření a podpora spolupráce při detekci a hlášení podezřelých aktivit. • Zajištění dostupnosti zálohovaných dat pro rychlou obnovu v případě úniku dat nebo poškození souborů v důsledku kybernetického útoku.	• Přidělení finančních prostředků na vylepšení fyzického zabezpečení prostor a zařízení obecního úřadu, včetně instalace kamer, kontrolních přístupových systémů a bezpečnostních alarmů. • Implementace politiky silných hesel, která vyžaduje složitá hesla s kombinací písmen, číslic a speciálních znaků a pravidelnou změnu hesel pro všechny zaměstnance. • Nasazení automatického systému zálohování dat na externí úložiště, který pravidelně zálohuje veškerá důležitá data obecního úřadu a zajišťuje jejich rychlou obnovu v případě potřeby. • Pravidelné monitorování a hodnocení účinnosti bezpečnostních opatření a politik s cílem identifikovat a odstranit slabiny a zlepšit celkovou úroveň kybernetické bezpečnosti.

(zdroj: vlastní zpracování)

PRÍLOHA P VI: FRAUD RISK ASSESSMENT

Fraud Risk Assessment as of [30.3.2024] KNIHOVNA											
ID	Zdroj rizika (Zranitelnosti)	Identifikace hrozeb	Pravděpodobnost [1-5]	Význam [1-5]	Fraud hodnocení rizika	Hodnocení účinnosti kontrol [1-5]	Existující opatření	Preventivní/Detekční opatření	Reziduální rizika (Vysoká, Střední,Nízká)	Fraud Response (Navrhnutá opatření)	Preventivní/Detekční opatření
1	Chybějící VPN	Odposlech dat: Bez použití VPN jsou data přenášená po internetu obvykle otevřená a mohou být snadno odposlechnuta útočníky, kteří se nacházejí v síti, kterou	1	1	1	4	Používání Firewall.	Preventivní	Nízká	Šifrování dat (HTTPS), Segmentace sítě (VLAN)	Preventivní
2	Chybějící VPN	Sledování aktivity: Poskytovatel internetového připojení nebo další osoby v síti mohou sledovat aktivity uživatelů, včetně webových stránek, které navštěvují, a komunikace, kterou provádějí.	1	1	1	5	Používání Firewall.	Preventivní	Nízká	Šifrování komunikace, pravidelné aktualizace systému.	Preventivní
3	Nízká úroveň ochrany proti spamu	Phishingové e-maily: Pokud knihovna nepoužívá účinné filtry proti spamu, mohou být uživatelé zaplavováni podvodnými e-maily, což zvyšuje riziko, že některý z nich bude kliknout na phishingový odkaz.	4	3	12	1	Antivirový program Avast.	Detekční	Střední	Filtrace spamu, Zavedení politiky společnosti.	Preventivní
4	Zaměstnanci jsou zároveň obyvateli obce	Sociální inženýrství: Útočníci často využívají psychologických triků a manipulace, aby přiměli zaměstnance k provádění nebezpečných akcí, což je v případě známosti zaměstanance snadnější.	2	1	2	5	Školení zaměstnanců.	Nedefinované	Nízká	Kontrola identity a přístupt, Přeškolení zaměstnanců.	Preventivní/Detekční
5	Příchozí excelové tabulky	Otevírání maker: Některé verze softwaru pro zpracování dokumentů mohou obsahovat zranitelnosti v implementaci makrojazyka, což může být využito k úniku dat nebo k infikování počítače škodlivým kódem.	3	1	3	2	Knihovna se vyhýbá otevírání maker.	Preventivní	Střední	Zákázání automatického spouštění maker, Ověření zdroje před	Preventivní
6	Nezabezpečený vstup externích disků	Ztráta dat: Pokud jsou externí disky používány pro zálohování důležitých dat knihovny a nejsou řádně zabezpečeny, mohou být tyto data snadno ztracena nebo poškozena náhodným odstraněním, poškozením disku nebo útokem malwarem.	5	2	10	1	Antivirový program Avast.	Detekční	Vysoká	Fyzická ochrana disků, Pravidelné zálohování.	Preventivní
7	Nezabezpečený vstup externích disků	Infekce malwarem: Externí disky mohou obsahovat škodlivý software (malware), jako jsou viry, trojské koně nebo ransomware. Pokud jsou externí disky připojeny k počítači bez dostatečného zabezpečení, může se malware snadno šířit do počítačové sítě knihovny a infikovat další zařízení.	5	2	10	1	Antivirový program Avast.	Detekční	Střední	Testování obnovy dat, Pravidelné zálohování.	Preventivní/Detekční

(zdroj: vlastní zpracování)

Fraud Risk Assessment as of [30.3.2024] OBECNÍ ÚŘAD										
ID	Zdroj rizika (Zranitelnosti)	Identifikace hrozeb	Pravděpodobnost [1-5]	Význam [1-5]	Fraud hodnocení rizika	Hodnocení účinnosti kontrol [1-5]	Existující opatření	Preventivní/Detekční opatření	Reziduální rizika (Vysoká, Střední,Nízká)	Fraud Response (Navrhnutá opatření)	Preventivní/Detekční opatření
1	Odklad aktualizací	Pokud není program aktualizován, útočníci mohou využít identifikované zranitelnosti.	4	3	12	2	Školení v rámci autitu.	Preventivní	Střední	Vytvořte plán správy zranitelností, který zahrnuje identifikaci, hodnocení a řešení zranitelností včetně pravidelných aktualizací.	Detekční
2	Falešné přístupové body	Při využívání Wi-Fi hrozí, že se návštěvníci připojí k nelegitimní Wi-Fi a útočník získá citlivé informace.	1	1	1	1	Doporučení (Připojovat se jen k důvěryhodným sítím).	Preventivní	Nízká	Detekce falešných bodů.	Detekční
3	Odcizení externího disku	Pokud není externí disk zabezpečen, mohou se ztratit citlivá data a mít tak dopad na důvěryhodnost obecního úřadu.	2	3	6	3	Ukládání disků na nedostupné místo.	Preventivní	Střední	Omezení přístupu k externím diskům. Šifrování dat na externích discích.	Preventivní/Detektivní
4	Nezabezpečené webové stránky	Při špatném zabezpečení mohou útočníci vyhledat chybu v kódu a zneužít této zranitelnosti.	2	1	2	5	Nedefinováno(ve správě Galileo corporation)	Nedefinované	Nízká	1.Bezpečnostní testování pro identifikaci zranitelností.2. Odstranění chyb v kódu.	Detekční
6	Chybející ochrana plat. Terminálů	Pokud útočníci získají fyzický přístup k platebnímu terminálu, mohou provést úpravy nebo instalovat škodlivý hardware, což umožní krádež platebních údajů.	1	5	5	4	Omezený přístup k terminálu.	Preventivní	Vysoká	Zabezpečení terminálu proti volnému přístutpu osob. Aktualizace a patche.	Preventivní/Detektivní
7	Nesprávná konfigurace systému TACTIKUS NG	Špatná konfigurace může způsobit bezpečnostní problémy, jako je nedostatečné šifrování dat, nevhodné oprávnění uživatelů nebo nedostatečné monitorování aktivit.	2	1	2	4	Firewall, Antivirový program Avast.	Preventivní/Detektivní	Nízká	Využijte automatizované nástroje pro správu konfigurace, které umožňují centralizovanou správu a sledování konfigurace všech zařízení a systémů v organizaci	Preventivní
8	Příchozí excelové tabulky	Otevírání maker: Některé verze softwaru pro zpracování dokumentů mohou obsahovat zranitelnosti v implementaci makrojazyka, což může být využito k úniku dat nebo k infikování počítače škodlivým kódem.	3	1	3	4	Firewall.	Preventivní	Střední	Zákázání automatického spouštění maker, Ověření zdroje před otevřením.	Preventivní/Detektivní
9	Nízká úroveň ochrany proti spamu	Útoky phishingem mohou způsobit i přímé finanční ztráty v důsledku podvodných transakcí, změn v platebních údajích nebo dalších finančních manipulacích provedených na základě podvodného e-mailu.	4	4	16	4	Antivirový program Avast.	Detekční	Vysoká	Filtrace spamu. Školení zaměstnanců zahrnující simulaci phishingových e-mailů.	Preventivní
10	Nepravidelné zálohování	Porušení bezpečnosti a soukromí: Bez pravidelného zálohování dat může organizace čelit vyššímu riziku porušení bezpečnosti a soukromí. Pokud jsou data ztracena nebo odcizena, mohou být náchylnější k neoprávněnému přístupu, zneužití nebo zveřejnění.	5	4	20	3	Zálohování na základě GDPR. (Nedefinované)	Preventivní	Střední	Zálohování by mělo probíhat automatizovaně a zálohy by měly být uchovávány na bezpečném místě mimo pracoviště.	Preventivní
11	Nepravidelné zálohování	Nedodržení povinnosti uchovávat určitá data kvůli zákonným požadavkům a jejich	4	5	20	3	Zálohování na základě GDPR. (Nedefinované)	Preventivní	Střední	Diferencované a pravidelné zálohování. Testování obnovy dat.	Preventivní/ Detektivní

(zdroj: vlastní zpracování)

PŘÍLOHA P VII: KRITERIA PRO HODNOCENÍ ANALÝZY FRAUD RISK ASSESEMENT

Likelihood				
Rating	Based on Annual Frequency		Based on Annual Probability of	
	Descriptor	Definition	Descriptor	Definition
5	Very frequent	More than twenty times per year	Almost certain	>90% chance of occurrence
4	Frequent	Six to twenty times per year	Likely	65% to 90% chance of occurrence
3	Reasonably frequent	Two to five times per year	Reasonably possible	35% to 65% chance of occurrence
2	Occasional	Once per year	Unlikely	10% to 35% chance of occurrence
1	Rare	Less than once per year	Remote	< 10% chance of occurrence

Significance		
Rating	Descriptor	Definition
5	Catastrophic	• Financial loss to company in excess of $10 million • International, long-term media coverage • Widespread employee morale issues and loss of multiple • Required to report incident to authorities, resulting in
4	Major	• Financial loss to company between $100,000 and $10 • National, long-term media coverage • Widespread employee morale problems and turnover • Required to report incident to authorities, resulting in
3	Moderate	• Financial loss to company between $10,000 and $100,000 • Short-term, regional or national media coverage • Widespread employee morale problems • Required to report incident to authorities and take
2	Minor	• Financial loss to company between $1,000 and $10,000 • Limited, local media coverage • General employee morale problems • Incident is reportable to authorities, but no follow-up
1	Incidental	• Financial loss to company less than $1,000 • No media coverage • Isolated employee dissatisfaction • Event does not need to be reported to authorities

Control Effectiveness	
Control Risk Rating	Description
5	Very effective (reduces 81–100% of the risk)
4	Effective (reduces 61–80% of the risk)
3	Moderately effective (reduces 41–60% of the risk)
2	Marginally effective (reduces 21–40% of the risk)
1	Not effective (reduces 0–20% of the risk)

(zdroj: UTB)

PŘÍLOHA P VIII: DOTAZNÍKOVÉ ŠETŘENÍ

Dotazník o zálohování a ochraně dat

Dobrý den, jsem studentka Univerzity Tomáše Bati, Fakulty logistiky a krizového řízení a momentálně se zabývám psaním své bakalářské práce, která se zaměřuje na problematiku kybernetických hrozeb.
Cílem dotazníku je zjistit, jak často a jakým způsobem respondenti zálohují svá data a jak ochraňují své informace. Zároveň se snažím ověřit jejich znalosti o obnově dat, bezpečnostních opatřeních a jejich postupu při zacházení s externími médii, jako jsou USB disky.
Dotazník také zohledňuje životní situaci respondentů, jako je jejich pracovní status, abychom lépe pochopili jejich individuální potřeby a kontext práce s daty. Na závěr bych chtěla zdůraznit, že dotazník je anonymní.

Předem děkuji za váš čas,

Štěpánka Čechová

Případné dotazy směřujte na uvedenou adresu:
s_cechova@utb.cz

* Označuje povinnou otázku

1. Určete pohlaví. Vyberte z nabízených možností. *

Označte jen jednu elipsu.

- ◯ Muž
- ◯ Žena
- ◯ Jiné: _____

2. Jaká je vaše aktuální životní situace? *

Označte jen jednu elipsu.

- ◯ Student
- ◯ Zaměstnanec
- ◯ Důchodce
- ◯ Žák (6-15let)
- ◯ Nezaměstnaný
- ◯ OSVČ
- ◯ Jiné: _____

3. Do jaké věkové kategorie spadáte? *

Označte jen jednu elipsu.

- ◯ 6-15 let
- ◯ 15-26 let
- ◯ 26-45
- ◯ 45-60
- ◯ 60-80
- ◯ 80+

4. Jak často zálohujete svá data? *

Označte jen jednu elipsu.

- ◯ Denně
- ◯ Týdně
- ◯ Měsíčně
- ◯ Jednou za rok či méně
- ◯ Nikdy

5. Pokud ano, jakým způsobem zálohujete svá data? (Můžete vybrat více odpovědí)

Zaškrtněte všechny platné možnosti.

- [ ] Záloha na externím disku
- [ ] Cloudová záloha (např. Google Drive, Dropbox)
- [ ] Záloha na vlastní server
- [ ] Jiné: _____

6. Víte, jak obnovit zálohovaná data v případě ztráty? *

Označte jen jednu elipsu.

- ◯ ANO
- ◯ NE

7. Pokud jste v předchozí otázce odpověděli ANO, popište krátce postup při obnově dat.

_____

_____

_____

_____

_____

8. Jak pečujete o bezpečnost svých dat? (Můžete vybrat i více odpovědí) *

Zaškrtněte všechny platné možnosti.

- [ ] Používám silná hesla
- [ ] Aktualizuji pravidelně software
- [ ] Využívám antivirovou ochranu
- [ ] Používám VPN
- [ ] Nijak
- [ ] Jiné: _____

9. Jaké opatření podnikáte pro ochranu citlivých dat? (Můžete vybrat i více odpovědí) *

Zaškrtněte všechny platné možnosti.

- [ ] Dvoufaktorová autentizace
- [ ] Šifrování
- [ ] Fyzické zabezpečení zařízení
- [ ] Žádná
- [ ] Jiné: _____

10. Jak přistupujete k externím diskům vlastním či služebním (např. USB)? *

Zaškrtněte všechny platné možnosti.

- [ ] Používám externí disky
- [ ] Externí disky nepřipojuji
- [ ] Externí disky odmítám
- [ ] Externí disk nevlastním
- [ ] Jiné: _____

11. Účastnili jste se školení týkajícího se kybernetické bezpečnosti? *

Označte jen jednu elipsu.

- ANO
- NE

12. Byli jste někdy svědkem nebo obětí kybernetického útoku? *

Označte jen jednu elipsu.

- Ano
- Ne

13. Máte povědomí o zabezpečení sítě ve veřejných institucích, které navštěvujete? *

Označte jen jednu elipsu.

- Ano
- Ne
- Částečně

14. Máte povědomí o základních principech, na kterých je internet postaven? *

Označte jen jednu elipsu.

- Ano
- Ne
- Částečně

15. Jak byste popsal/a internet a jeho základní funkce?

16. Kde nejvíce internet využíváte? (Můžete vybrat i více odpovědí) *

Zaškrtněte všechny platné možnosti.

- [ ] V práci
- [ ] Na svém osobním zařízení u sebe doma
- [ ] Na veřejných místech (např. knihovna, kavárna)
- [ ] Nevyužívám internet
- [ ] Jiné:

17. Pokud ano, jak často využíváte internet? Vyberte odpověď, která se nejvíce blíží skutečnosti.

Označte jen jednu elipsu.

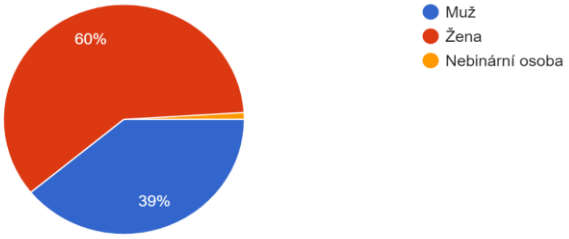
- Denně
- 1-2 krát za týden
- Několikrát za měsíc
- Téměř vůbec

(zdroj: vlastní zpracování)

PŘÍLOHA P IX: VÝSLEDKY DOTAZNÍKOVÉHO ŠETŘENÍ

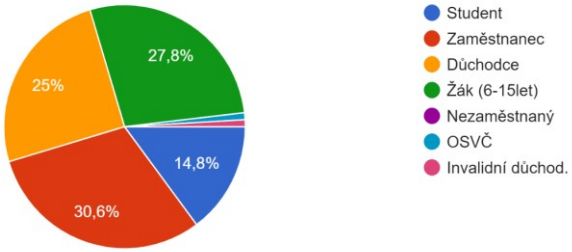
1.Určete pohlaví. Vyberte z nabízených možností.

105 odpovědí



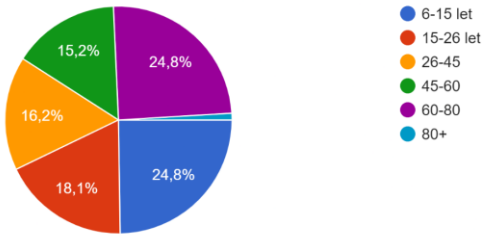
2.Jaká je vaše aktuální životní situace?

108 odpovědí



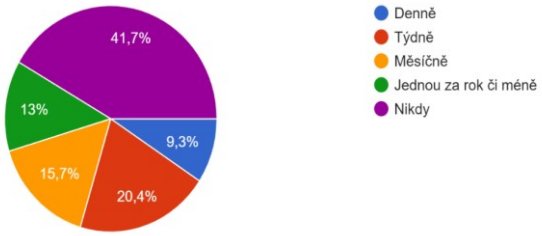
3.Do jaké věkové kategorie spadáte?

105 odpovědí



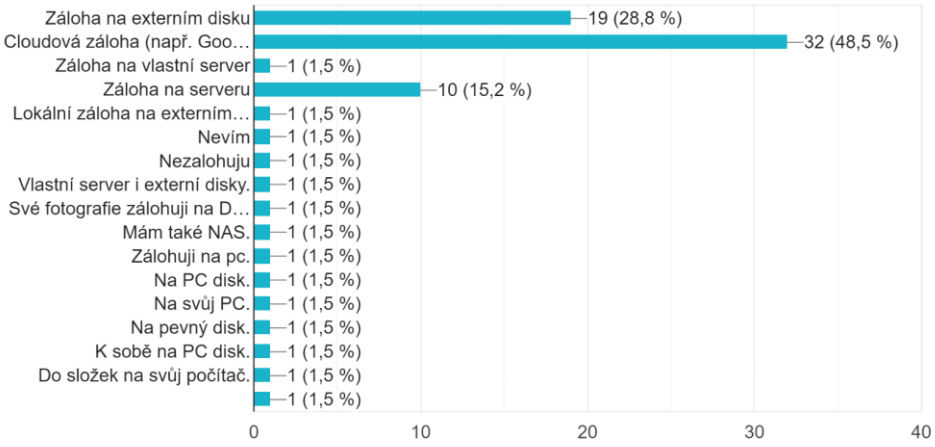
4.Jak často zálohujete svá data?

108 odpovědí



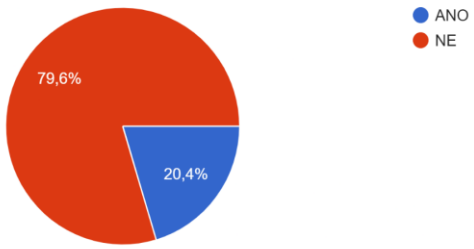
5.Pokud ano, jakým způsobem zálohujete svá data? (Můžete vybrat více odpovědí)

66 odpovědí

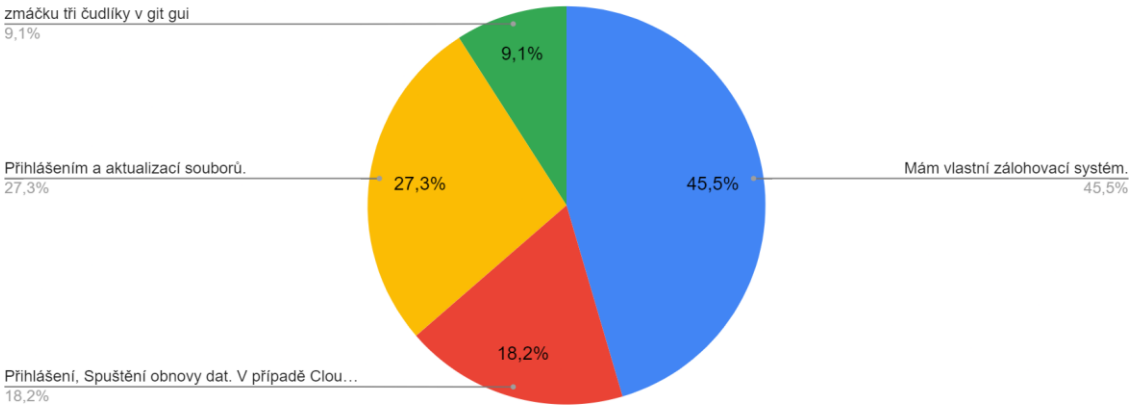


6.Víte, jak obnovit zálohovaná data v případě ztráty?

108 odpovědí

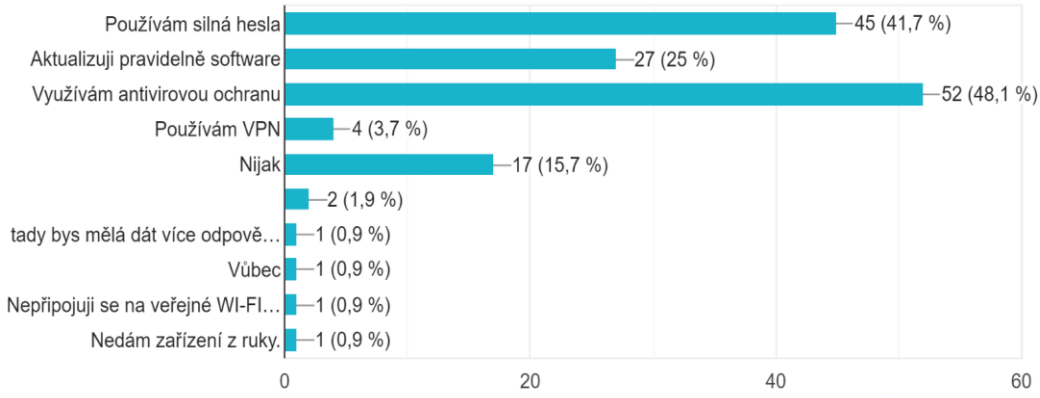


7. Pokud jste v předchozí otázce odpověděli ANO, popište krátce postup při obnově dat.



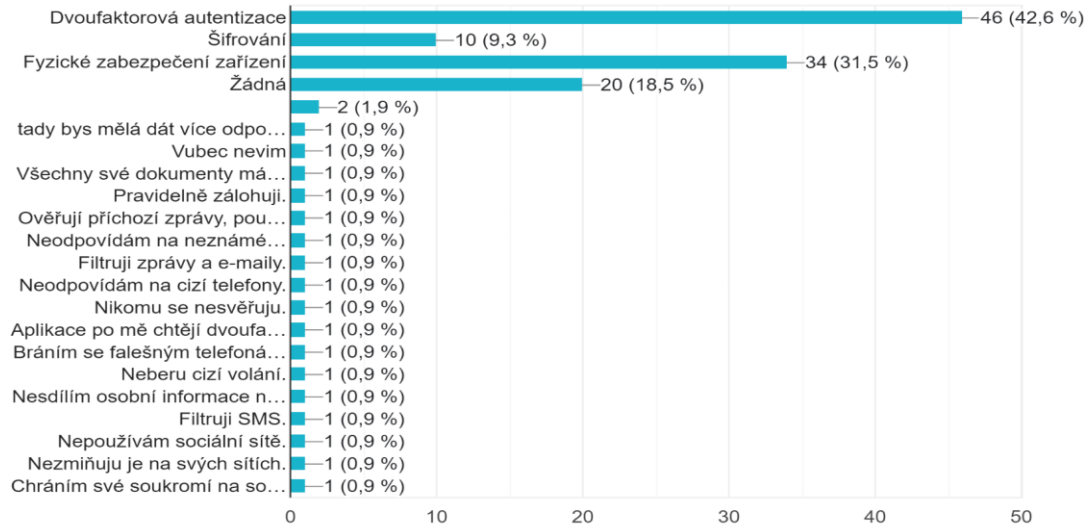
8.Jak pečujete o bezpečnost svých dat? (Můžete vybrat i více odpovědí)

108 odpovědí

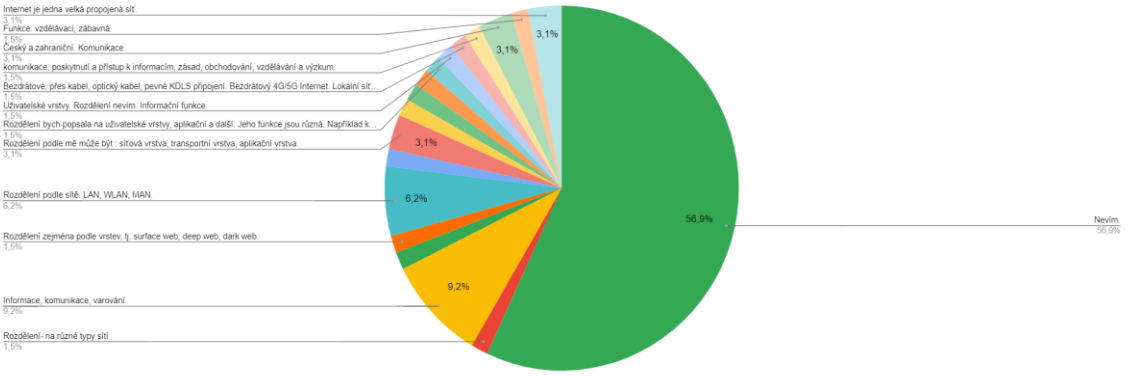


9.Jaké opatření podnikáte pro ochranu citlivých dat? (Můžete vybrat i více odpovědí)

108 odpovědí

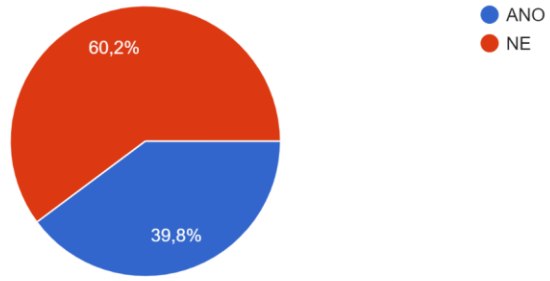


10.Jak byste popsal/a internet a jeho základní funkce?



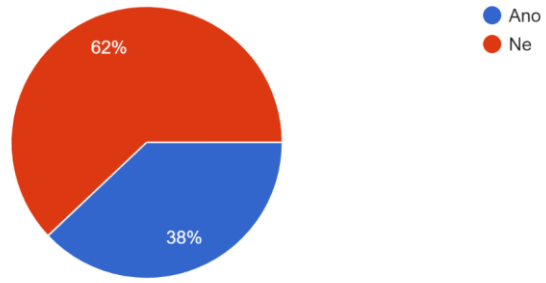
11.Účastnili jste se školení týkajícího se kybernetické bezpečnosti?

108 odpovědí

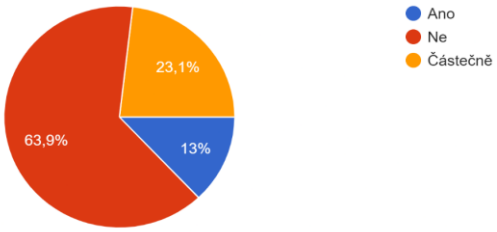


12.Byli jste někdy svědkem nebo obětí kybernetického útoku?

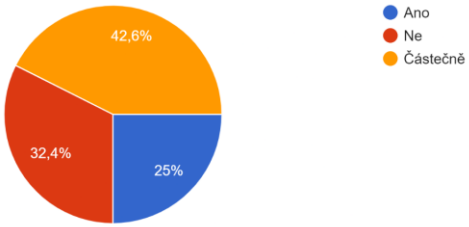
108 odpovědí



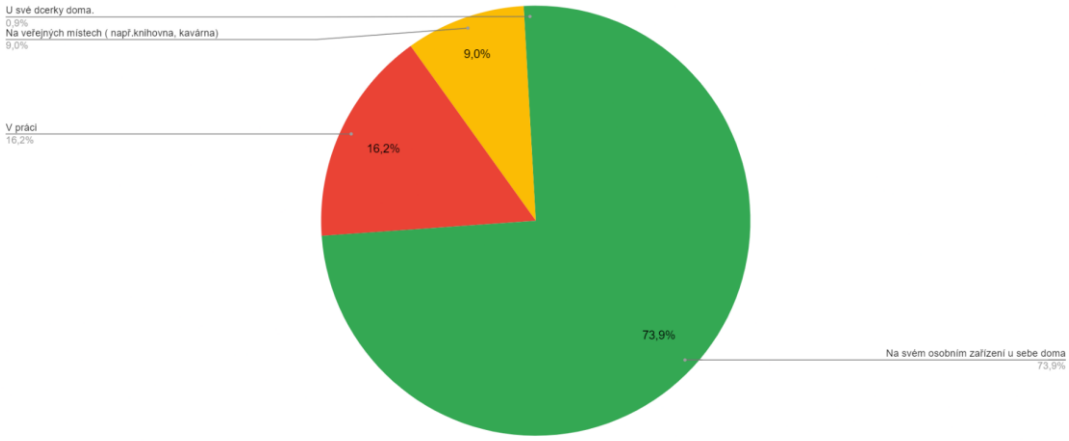
13.Máte povědomí o zabezpečení sítě ve veřejných institucích, které navštěvujete?
108 odpovědí



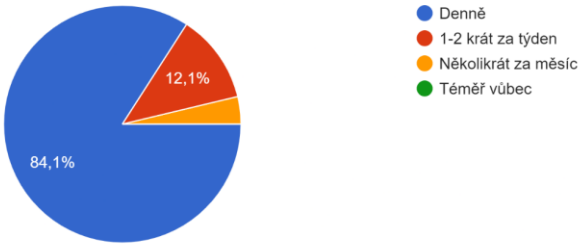
14.Máte povědomí o základních principech, na kterých je internet postaven?
108 odpovědí



16. Kde nejvíce internet využíváte? (Můžete vybrat i více odpovědí)



17.Pokud ano, jak často využíváte internet? Vyberte odpověď, která se nejvíce blíží skutečnosti.
107 odpovědí



(zdroj: vlastní zpracování)

PŘÍLOHA P X: ŘÍZENÝ ROZHOVOR

Knihovna
Kdo se stará o kyberbezpečnost ve vaší organizaci?
knihovník
Jaké operační systémy využíváte?
Windows + Linux zero
Jakým způsobem řešíte internetové připojení?
WI-FI hotspot
Je vedena evidence návštěvníků?
Ano, ale anonymní.
Je prováděna kontrola externích disků, které návštěvníci připojují k zařízení?
Ne, notebooky pro návštěvníky jsou jiné než pracovní.
Je prováděna jejich údržba?
Ano, pravidelně.
Je ve vaší organizaci prováděno školení kybernetické bezpečnosti?
Ano, pravidelně.
Provádíte kontrolu zálohování?
ano
Provádíte kompletní aktualizace na všech zařízeních?
ano
Jsou zaměstnanci ve vaší organizaci proškolení ohledně kybernetické bezpečnosti?
Částečně
Jakým způsobem jsou zabezpečené externí disky?
Zamčeny v šuplíku.
Obecní úřad
Kdo se stará o kyberbezpečnost ve vaší organizaci?
Externí firma
Jaké operační systémy využíváte?
Windows
Jakým způsobem řešíte internetové připojení?
WI-FI hotspot
Je vedena evidence návštěvníků?
ne
Je prováděna kontrola externích disků, které návštěvníci připojují k zařízení?
ano
Je prováděna jejich údržba?
ano
Je ve vaší organizaci prováděno školení kybernetické bezpečnosti?
ano
Provádíte kontrolu zálohování?
Externí firma
Provádíte kompletní aktualizace na všech zařízeních?
ano
Jsou zaměstnanci ve vaší organizaci proškolení ohledně kybernetické bezpečnosti?
Ano
Jakým způsobem jsou zabezpečené externí disky?
Uschovány v uzavřené místnosti

(zdroj: vlastní zpracování)