

Scénáře narušení informační bezpečnosti subjektu ochrany obyvatelstva

Bc. Karel Kváš

Diplomová práce
2025



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: 2024/2025

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	Bc. Karel Kváš
Osobní číslo:	L23737
Studijní program:	N1032A020002 Bezpečnost společnosti
Specializace:	Ochrana obyvatelstva
Forma studia:	Prezenční
Téma práce:	Scénáře narušení informační bezpečnosti subjektu ochrany obyvatelstva

Zásady pro vypracování

- Na základě dostupných zdrojů zpracujte teoretickou část dané problematiky.
- Pojednejte o informační bezpečnosti vybraného subjektu ochrany obyvatelstva.
- Navrhněte scénáře narušení informační bezpečnosti tohoto subjektu.
- Za pomoci vhodného softwarového nástroje modelujte navržené scénáře.

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

Seznam doporučené literatury:

1. CORNISH, Paul. *The Oxford Handbook of Cyber Security*. United Kingdom: Oxford University Press, 2021. ISBN 978-0-19-880068-2.
2. PANDE, Jeetendra. *Introduction to Cyber Security*. India: Uttarakhand Open University, 2017. ISBN 978-93-84813-96-3.
3. SMEJKAL, Vladimír. *Kybernetická kriminalita*. 3. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2022. ISBN 978-80-7380-849-5.
4. SMEJKAL, Vladimír; SOKOL, Tomáš a KODL, Jindřich. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. ISBN 978-80-7380-765-8.
5. ŠULC, Vladimír. *Kybernetická bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-737-5.

Další odborná literatura dle doporučení vedoucího diplomové práce.

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

Datum zadání diplomové práce: **2. prosince 2024**
Termín odevzdání diplomové práce: **25. dubna 2025**

L.S.

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

prof. Ing. Dušan Vičar, CSc.
ředitel ústavu

V Uherském Hradišti dne 2. prosince 2024

PROHLÁŠENÍ AUTORA DIPLOMOVÉ PRÁCE

Beru na vědomí, že

- odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb., v platném znění bez ohledu na výsledek obhajoby;
- diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému a bude dostupná k nahlédnutí;
- jedno vyhotovení diplomové práce v listinné podobě bude ponecháno Univerzitě Tomáše Bati ve Zlíně k uložení;
- na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 mohu užít své dílo – diplomovou práci – nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá; neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji, že

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

V Uherském Hradišti, dne 25. 4. 2025

.....
podpis autora

ABSTRAKT

Diplomová práce se zabývá problematikou narušení informační bezpečnosti v prostředí Hasičského záchranného sboru České republiky. Cílem práce je navrhnout modelové scénáře útoků, provést jejich analýzu pomocí metody What-if a matice rizik a následně navrhnout vhodná bezpečnostní opatření. Teoretická část se věnuje právním rámcům a významu informační bezpečnosti ve veřejné správě. Praktická část obsahuje vizualizaci vybraných scénářů pomocí vývojových diagramů, jejich hodnocení a návrh řešení. Výsledkem práce je návrhový přístup, který může sloužit jako inspirace pro posílení bezpečnostní odolnosti veřejných institucí.

Klíčová slova: hasičský záchranný sbor, informační bezpečnost, kybernetická bezpečnost, scénáře narušení, subjekt ochrany obyvatelstva

ABSTRACT

This thesis addresses the issue of information security breaches within the Fire Rescue Service of the Czech Republic. The aim is to propose model threat scenarios, analyze them using the What – if method and a risk matrix, and subsequently design appropriate security measures. The theoretical part focuses on legal frameworks and the importance of information security in public administration. The practical section includes visualized scenarios using flowcharts, their assessment, and proposed solutions. The result is a conceptual approach that may serve as inspiration for strengthening the cybersecurity resilience of public institutions.

Keywords: fire rescue service, information security, cybersecurity, incident scenarios, population protection entity

Rád bych poděkoval příslušníkovi Hasičského záchranného sboru za ochotu a cenné odpovědi, které mi pomohly při zpracování praktické části této práce.

Děkuji vedoucímu práce panu Ing. Petru Svobodovi, Ph.D., za formální vedení práce.

Dále bych vyjádřil vděčnost své přítelkyni za podporu, pochopení a pomoc, kterou mi poskytovala v období stresu a vypětí. V neposlední řadě děkuji také své rodině a blízkým, kteří o práci projevovali zájem a byli mi po celou dobu oporou.

OBSAH

ÚVOD.....	11
CÍLE A POUŽITÉ METODY.....	12
I TEORETICKÁ ČÁST.....	14
1 INFORMAČNÍ BEZPEČNOST	15
1.1 KYBERNETICKÁ BEZPEČNOST.....	17
1.1.1 Význam kybernetické bezpečnosti.....	17
1.1.2 Prvky kybernetické bezpečnosti.....	18
1.1.3 Vícevrstvá ochrana a řízení přístupu.....	20
1.1.4 Rozdíl mezi kybernetickou bezpečnostní událostí a incidentem a postup při jejich řešení	20
1.1.5 Síťové zabezpečení	21
1.1.6 Počítačové zabezpečení.....	22
1.2 FYZICKÁ BEZPEČNOST	23
1.2.1 Prostředky fyzické bezpečnosti.....	23
1.2.2 Integrace fyzické a kybernetické bezpečnosti.....	24
2 PRÁVNÍ NORMY	26
2.1 EVROPSKÁ LEGISLATIVA A MEZINÁRODNÍ NORMY	27
2.2 NÁRODNÍ INSTITUCE A BEZPEČNOSTNÍ TÝMY	28
3 HROZBY A ÚTOKY NA INFORMAČNÍ BEZPEČNOST.....	30
3.1 KYBERNETICKÉ ÚTOKY	30
3.1.1 Hacking	31
3.1.2 Sociální inženýrství.....	31
3.1.3 Malware.....	32
3.1.4 Další příklady kybernetických útoků	34
3.2 FYZICKÉ HROZBY INFORMAČNÍ BEZPEČNOSTI	35
4 OCHRANA OBYVATELSTVA	37
4.1 HLAVNÍ SUBJEKTY OCHRANY OBYVATELSTVA	37
4.2 OSTATNÍ DŮLEŽITÉ SUBJEKTY	39
DÍLČÍ ZÁVĚR.....	42
II PRAKTICKÁ ČÁST.....	43
5 INFORMAČNÍ BEZPEČNOST SUBJEKTU OCHRANY OBYVATELSTVA.....	44
5.1 ANALÝZA SOUČASNÉHO STAVU VYBRANÉHO ÚZEMNÍHO ODBORU V OLOMOUCKÉM KRAJI	44
5.2 BEZPEČNOSTNÍ RÁMEC INFORMAČNÍCH SYSTÉMŮ VE VEŘEJNÉ SPRÁVĚ.....	46
5.3 NÁVRHY SCÉNÁŘŮ NARUŠENÍ INFORMAČNÍ BEZPEČNOSTI.....	47
5.4 DŮVODY VÝBĚRU JEDNOTLIVÝCH SCÉNÁŘŮ	48

6	POPIS SCÉNÁŘU NARUŠENÍ INFORMAČNÍ BEZPEČNOSTI.....	51
6.1	MODELOVÝ SCÉNÁŘ SPEAR – PHISHING S MALWAREM.....	52
6.1.1	What-if analýza – spear-phishing.....	53
6.1.2	Reakční plán – IRP.....	54
6.2	MODELOVÝ SCÉNÁŘ DDOS ÚTOKU NA TÍSŇOVOU LINKU HZS.....	56
6.2.1	What-if analýza – DDoS útok	57
6.2.2	Reakční plán – IRP.....	58
6.3	MODELOVÝ SCÉNÁŘ: FYZICKÉ NAPADENÍ SERVEROVNY NOVÝM ZAMĚSTNANCEM S IMPLEMENTACÍ RANSOMWARE NA USB DISKU	59
6.3.1	What-if analýza – serverovna.....	60
6.3.2	Reakční plán – IRP.....	61
7	MODELOVÁNÍ JEDNOTLIVÝCH SCÉNÁŘŮ	63
7.1	MODEL SPEAR-PHISHINGOVÉHO ÚTOKU S MALWAREM.....	64
7.2	MODEL DDoS ÚTOKU NA TÍSŇOVOU LINKU HZS.....	66
7.3	MODEL FYZICKÉHO NAPADENÍ SERVEROVNY NOVÝM ZAMĚSTNANCEM HZS S IMPLEMENTACÍ RANSOMWARE NA USB DISKU	68
8	VYHODNOCENÍ A ANALÝZA VÝSLEDKŮ MODELOVÁNÍ.....	70
8.1	IDENTIFIKOVANÉ SLABINY NAPŘÍČ SCÉNÁŘI.....	70
8.2	SHRNUTÍ VÝSLEDKŮ V MATICI RIZIK	71
9	NÁVRHY OPATŘENÍ KE ZMÍRNĚNÍ IDENTIFIKOVANÝCH RIZIK	74
9.1	PREVENCE SPEAR-PHISHINGOVÉHO ÚTOKU.....	74
9.2	OPATŘENÍ PROTI DDoS ÚTOKU NA TÍSŇOVOU LINKU	75
9.3	OPATŘENÍ PROTI FYZICKÉMU NAPADENÍ SERVEROVNY A VNITŘNÍMU AKTÉROVI.....	76
	ZÁVĚR.....	79
	SEZNAM POUŽITÉ LITERATURY	80
	SEZNAM OBRÁZKŮ	86
	SEZNAM TABULEK.....	87
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK	88
	SEZNAM PŘÍLOH.....	89

ÚVOD

Informace jsou důležitou součástí každého jedince i organizace. Tím, že se nacházíme v digitální době, tak se i informace zpracovávají elektronicky, což má své výhody, ale i nevýhody. S příchodem digitalizace se stávají se více ohroženými a zranitelnými. Informační systémy s sebou přináší rychlejší a přehlednější zpracování informací, ale zároveň jsou terčem pro kybernetické útoky. Je proto důležité tyto informace chránit, ať už se jedná o informace jako takové, citlivá data nebo jiné důležité informace. Jejich ztráta, krádež nebo zničení by mohli ohrozit nejen jedince nebo organizace, ale i například celý stát, pokud by se jednalo o subjekty kritické infrastruktury. Současný stav ukazuje, že hrozby kybernetických útoků jsou stále intenzivnější a napadené subjekty nejsou už jen soukromé firmy, ale také subjekty veřejné správy, které jsou důležité pro ochranu obyvatelstva. Proto je důležité, aby byly všechny instituce připraveny na tyto útoky a zodpovědně řešili svou bezpečnost informací.

Subjekty ochrany obyvatelstva, jako je například Hasičský záchranný sbor ČR, ke své činnosti potřebují informační technologie a v dnešní době na tyto technologie celkem spoléhají. Může se jednat o databáze, komunikační nebo krizové systémy a další. Pokud by došlo k jejich výpadku, může to ovlivnit fungování celého informačního systému, a to by byl pro obyvatelstvo velký problém.

Informační bezpečnost tak dnes není jen o tom mít kvalitní antivirový program nebo silné heslo. Jde o celkovou připravenost organizace – schopnost reagovat, předcházet a přemýšlet nad tím, co by se mohlo stát. Zejména u subjektů, které zajišťují ochranu obyvatelstva, je důležité přistupovat ke kybernetickým hrozbám stejně zodpovědně jako k těm fyzickým. Útok může přijít kdykoli a často bez varování.

Při rostoucí intenzitě kybernetických útoků je proto klíčové, aby se subjekty ochrany obyvatelstva aktivně věnovaly ochraně svých informačních systémů. Nestačí pouze reagovat na incidenty, ale je potřeba jim předcházet – pomocí vhodných technických, organizačních a personálních opatření. Mezi ty patří například pravidelné zálohování dat anebo školení zaměstnanců. Jen dobrá připravenost na možné scénáře narušení informační bezpečnosti mohou zjistit, že služby pro veřejnost zůstanou zachovány i případě krizové situace.

CÍLE A POUŽITÉ METODY

Hlavním cílem této diplomové práce bylo na základě vytvořených modelových scénářů narušení informační bezpečnosti subjektu Hasičského záchranného sboru České republiky, konkrétně se jedná Hasičský záchranný sbor v územním odboru v Olomouckém kraji, a navrhnout vhodná opatření ke zmírnění rizik. Práce se soustředí na upozornění na možné hrozby, které mohou ohrozit fungování organizace.

Pro dosažení hlavního cíle byly stanoveny následující dílčí cíle:

Bod 1: Seznámení se s teoretickými východisky informační bezpečnosti.

Bod 2: Pojednat o informační bezpečnosti vybraného subjektu ochrany obyvatelstva.

Bod 3: Navrhnout scénáře narušení informační bezpečnosti tohoto subjektu.

Bod 4: Za pomoci vhodného softwarového nástroje modelovat navržené scénáře.

V diplomové práci byly použité tyto metody:

- Syntéza – informace byly v teoretické části z různých odborných zdrojů spojeny do uceleného přehledu. Tato metoda pomohla vytvořit teoretický rámec práce propojením legislativních, technických i organizačních aspektů informační bezpečnosti v prostředí veřejné správy.
- Analýza – v rámci návrhu a popisu jednotlivých scénářů narušení informační bezpečnosti byla použita metody analýzy. Scénáře byly rozebrány na jednotlivé fáze a zkoumány z hlediska dopadů a průběhu incidentu.
- Dedukce – scénáře vycházely z obecných trendů a poznatků v oblasti kybernetických hrozeb a byly aplikovány na specifický kontext HZS ČR. Obecné informace byly tedy deduktivně.
- Modelování – v praktické části byla využita metoda modelování, kde byly navrženy a modelově znázorněny hypotetické scénáře narušení pomocí nástroje Microsoft Visio.
- Metoda what-if – byla použita v části vyhodnocení scénářů, kde se zkoumá, co by se stalo, kdyby došlo ke konkrétnímu incidentu. Tato metoda pomáhá identifikovat rizika a slabá místa v systému řízení informační bezpečnosti.

- Riziková analýza – pro každý scénář bylo provedeno posouzení rizik pomocí rizikové matice (pravděpodobnost x dopad). Na základě výsledků byly navrženy vhodné bezpečnostní opatření.

Omezení práce

Při zpracování praktické části nebylo možné získat podrobnější technické informace od IT specialistů HZS z důvodu důvěrnosti. Pokus o konzultaci s IT specialistou územního odboru tedy nebyl úspěšný a krajské ředitelství HZS odmítlo sdílet informace s odkazem na jejich chráněný charakter. Praktická část proto vychází z veřejně dostupných zdrojů a neformálního rozhovoru se zaměstnancem HZS, který poskytl rámcový vhled do provozního fungování informačních systémů. Tyto informace byly následně nezávisle potvrzeny druhým zaměstnancem z jiného územního odboru, čímž se zvýšila důvěryhodnost základních východisek pro návrh modelových scénářů.

I. TEORETICKÁ ČÁST

1 INFORMAČNÍ BEZPEČNOST

Informační bezpečnost je ochrana důležitých informací před neoprávněným přístupem, zveřejněním, použitím, změnou nebo narušením. Pomáhá zajistit, aby citlivá data organizace byla dostupná oprávněným uživatelům, zůstala důvěrná a zachovala si svou integritu (Kyriazoglou, 2024).

Informační bezpečnost je úzce spjata s kybernetickou bezpečností. Hlavními pilíři jsou zachování důvěrnosti, dostupnosti a integrity, také zvané jako CIA triáda. Profesionálové v oblasti informační bezpečnosti, kteří vytvářejí zásady a postupy (často označené jako modely správy), musí při vytváření plánu na ochranu počítačového systému zohlednit každý z těchto cílů. (Merkow a Breithaupt, 2014).

Kybernetická bezpečnost řeší mnoho kybernetických incidentů pomocí činností, které se právě dotýkají i samotné informační bezpečnosti (Doucek et al., 2019).

Tyto pilíře se snaží řešit alespoň jeden ze tří cílů:

- ochrana důvěrnosti dat,
- zachování integrity dat,
- podpora dostupnosti dat pro autorizované použití (Merkow a Breithaupt, 2014).



Obrázek 1 Triáda CIA.

(zdroj: Merkow a Breithaupt, 2014)

Principy informační bezpečnosti – Důvěrnost, integrita a dostupnost jsou velmi důležité pro jakoukoli studii nebo praxi v této oblasti. Často se označují jako CIA triáda a slouží jako základní pilíře ochrany informací. Tento koncept se běžně využívá ve výzkumu i praxi informační bezpečnosti (Merkow a Breithaupt, 2014).

Důvěrnost: Tento pojem označuje stav, kdy jsou informace zpřístupněny výhradně osobám s oprávněním k jejich použití. Pokud dojde k neautorizovanému přístupu či úniku dat, jedná se v oblasti informační bezpečnosti o narušení důvěrnosti informací

Integrita: Integrita představuje udržení správnosti a úplnosti dat. Jakákoli neoprávněná změna informací je v z pohledu informační bezpečnosti vnímána jako narušení jejich integrity.

Dostupnost: Tento princip zajišťuje, že informace jsou oprávněným uživatelům k dispozici tehdy, kdy je potřebují. (Šulc, 2018).

Životní cyklus informací

Informace musí být chráněny během svého cyklu, a to jak v úložišti, přenosu tak i použití, protože zde hrozí narušení důvěrnosti, integrity a dostupnosti. Proto by měla každá informace stanovovat svého vlastníka, který provádí její klasifikaci a určuje přístup k těmto informacím (Šulc, 2018).

Vztahy mezi počítačovou, datovou, informační a kybernetickou bezpečností

Informační bezpečnost se skládá z několika vzájemně propojených oblastí, které se liší svým zaměřením a rozsahem ochrany. Informační bezpečnost představuje nejširší rámec, jehož cílem je chránit informace ve všech formách – digitálních i fyzických. Kybernetická bezpečnost je její podmnožinou a soustředí se na ochranu informací v digitálním prostředí, zejména před kybernetickými hrozbami. Počítačová bezpečnost se zaměřuje na ochranu samotných systémů, tedy hardwaru, softwaru a sítí, které informace zpracovávají (Communication Team, 2024).

Datová bezpečnost, někdy považovaná za součást kybernetické bezpečnosti, se věnuje ochraně digitálních dat. Zahrnuje opatření jako šifrování řízení přístupu či zálohování.

Vzájemná provázanost těchto oblastí znamená, že každá úroveň zabezpečení přispívá k ochraně informací jako celku. Informační bezpečnost určuje strategické zásady, kybernetická bezpečnost chrání digitální celek, počítačová zajišťuje fyzickou a technickou ochranu systémů a datová bezpečnost zabezpečuje samotný obsah proti neoprávněnému

přístupu nebo manipulaci. Dalo by se tedy říct že tyto oblasti lze chápat jako vrstvy komplexního systému ochrany informací, kde informační bezpečnost tvoří hlavní rámec, kybernetická bezpečnost se zaměřuje na digitální hrozby, počítačová bezpečnost chrání samotné systémy a datová bezpečnost se stará o ochranu konkrétních dat (Marshal, 2023).

1.1 Kybernetická bezpečnost

Pod pojmem kybernetická bezpečnost si mnoho lidí představuje oblast informačních a komunikačních technologií (dále v textu jen „ICT“), což může být problém, protože kybernetickou bezpečnost využíváme každý den a lidstvo je v podstatě její součástí. Pokud si tento fakt nepřiznáme, tak se pravděpodobnost kybernetických útoku zvyšuje (Kolouch a Bašta, 2019).

Tato bezpečnost představuje jistou podmnožinu bezpečnosti jako takové. Jeho definice není jednoznačná. Lze ale vycházet z již ustálených definic: Kybernetická bezpečnost představuje soubor opatření, která jsou přijata, aby byl ochráněn počítačový systém před neoprávněným přístupem či útokem. Podle Koloucha a Bašty (2019) je kybernetická bezpečnost definována jako: *„Souhrn právních, organizačních, technických a vzdělávacích prostředků, které směřují k zajištění ochrany počítačových systémů a dalších prvků ICT, aplikací, dat a uživatelů, schopnost počítačových systémů a využívaných služeb reagovat na kybernetické hrozby či útoky a jejich následky, jakož i plánování obnovy funkčnosti počítačových systémů a služeb s nimi spojených.“*

1.1.1 Význam kybernetické bezpečnosti

V moderní společnosti hraje kybernetická bezpečnost důležitou roli, hlavně kvůli rostoucí digitalizaci, která pronikla do všech aspektů života – od ochrany kritické infrastruktury po zabezpečení osobních dat. Historicky se první kybernetické hrozby objevily spolu s rozvojem internetu, což umožnilo rychlé šíření virů a zneužití systémů. Tento vývoj vedl k vytvoření obranných mechanismů, jako jsou firewally a šifrování, které dnes patří mezi základní bezpečnostní opatření (Singer a Friedman, 2014).

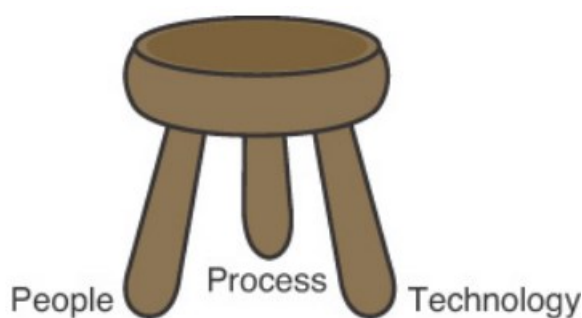
Kybernetická bezpečnosti uplatňuje ve své funkčnosti 3 základní triády, které jsou taky známé jako triády kybernetické bezpečnosti:

- 1) Již zmiňovaná CIA,
- 2) klíčové prvky kybernetické bezpečnosti – zahrnují lidi, technologie a procesy, přičemž každý z těchto prvků přispívá k celkovému zabezpečení organizace,

- 3) životní cyklus kybernetické bezpečnosti – skládá se ze tří hlavních fází: prevence, detekce a reakce. Tyto fáze umožňují organizacím efektivně řídit kybernetická rizika (Kolouch a Bašta, 2019).

1.1.2 Prvky kybernetické bezpečnosti

Lidé, procesy a technologické kontroly jsou zásadními prvky v několika oblastech praxe v oblasti bezpečnosti informačních technologií, včetně bezpečnosti provozu, bezpečnosti vývoje aplikací, fyzické bezpečnosti a kryptografie. Tyto tři pilíře bezpečnosti jsou často znázorněny jako trojnohá stolička (Merkow a Breithaupt, 2014).



Obrázek 2 Pilíře bezpečnosti.

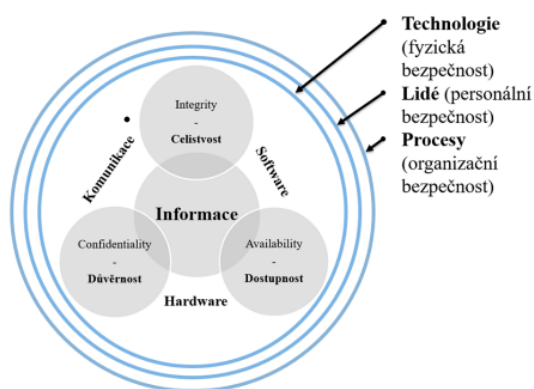
(zdroj: *Merkow a Breithaupt, 2014*)

Lidé: Lidský faktor hraje významnou roli v ochraně informačních systémů. Zahrnuje odborníky jako manažery kybernetické bezpečnosti, architekty bezpečnosti, auditory, administrátory a další odpovědné osoby, které zajišťují implementaci a správu bezpečnostních opatření (Stallings a Brown, 2024).

Technologie: Technologická opatření zahrnují širokou škálu nástrojů, které pomáhají identifikovat, eliminovat a předcházet hrozbám. Mezi základní technologie patří:

- Firewally – brání neoprávněnému přístupu do sítě a regulují síťový provoz na základě bezpečnostních pravidel.
- Systémy detekce a prevence narušení (IDS/IPS) - sledují síťový provoz a identifikují podezřelé aktivity, případně automaticky blokuje.
- Šifrování dat – klíčová metoda ochrany citlivých informací před neoprávněným přístupem.
- Zálohovací a obnovovací systémy – pomáhají minimalizovat dopady kybernetických incidentů tím, že umožňují rychlou obnovu kritických dat (Stallings a Brown, 2024).

Procesy: Jedná se o činnosti, které umožní lidem používat danou technologii. Do procesů patří zejména řízení aktiv a rizik, implementace ICT a aplikací, správa uživatelů a rolí, autorizace a autentizace, údržba systémů a služeb, testování zabezpečení počítačových systémů a služeb, analýza nápravných opatření, realizace nápravných opatření. Dále také audity, detekce kybernetických útoků a jejich reakce, školení a cvičení (Kolouch a Bašta, 2019).

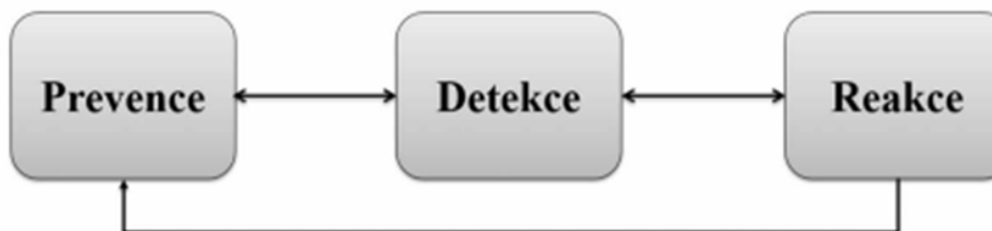


Obrázek 3 Triáda CIA doplněná o technologie, lidi a procesy.

(Kolouch a Bašta, 2019)

Životní cyklus kybernetické bezpečnosti

Při zavádění kybernetické bezpečnosti je důležité průběžně pracovat jak s triádou CIA, tak i s jednotlivými prvky kybernetické bezpečnosti podle potřeby během jejich celého životního cyklu. Hlavními kroky jsou prevence, detekce a reakce na útoky. Pro přesnost se životní cyklus znázorňuje pomocí diagramů (Kolouch a Bašta, 2019).



Obrázek 4 Zjednodušené zobrazení životního cyklu kybernetické bezpečnosti.

(zdroj: Kolouch a Bašta, 2019)

1.1.3 Vícevrstvá ochrana a řízení přístupu

K ochraně dat a systému je zapotřebí mnoho typů opatření. Mezi tyto opatření patří například: organizační, technické, systémové nebo také tzv. „security in depth“, což zahrnuje preventivní, detekční, reaktivní a další opatření. Bezpečnostní opatření je možné kombinovat různými způsoby. Pokud je jedno z opatření prolomeno, mělo by být zajištěno, že ostatní opatření stále dokážou ochránit systém. Tento přístup se nazývá „defense in depth“ neboli vícevrstvá bezpečnost. A to znamená, že bezpečnostní ochrany jsou vrstveny tak, aby v případě prolomení jedné vrstvy další vrstvy stále zajišťovaly ochranu. Toto pojetí však nezahrnuje lidi a prostory, ve kterých se informační systém nachází. Opatření se dále dělí na identifikaci, autentizaci, autorizaci, auditing a monitoring, zálohování a archivace, antimalware, šifrování a hashování. (Šulc, 2018).

Identifikace – Tento proces spočívá v přiřazení jedinečného identifikátoru uživateli nebo zařízení. Identifikátor umožňuje systémům rozpoznat a zaznamenat, kdo nebo co se pokouší o přístup. (Šulc, 2018).

Autentizace – následuje po identifikaci a zajišťuje, že subjekt skutečně odpovídá své identitě. Mezi běžné metody autentizace patří:

- Něco, co subjekt umí (odpověď na dotaz),
- Něco, co subjekt zná (heslo, pin),
- něco, co subjekt má (bezpečnostní karta),
- něco, čím subjekt je (otisk prstu, rozpoznání obličeje) (Šulc, 2018).

Autorizace – Po úspěšné autentizaci je subjektu přiděleno příslušné oprávnění k přístupu k datům nebo funkcím systému. Principem autorizace je minimalizace přístupu, takže uživatel by měl mít přístup pouze k těm informacím a prostředkům, které nezbytně potřebuje (Šulc, 2018).

1.1.4 Rozdíl mezi kybernetickou bezpečnostní událostí a incidentem a postup při jejich řešení

Kybernetická bezpečnostní událost označuje situaci, která by mohla vést k ohrožení bezpečnosti informací v informačních systémech nebo k narušení bezpečnosti služeb a sítí elektronických komunikací. Pokud však taková událost skutečně způsobí narušení těchto prvků, jedná se o kybernetický incident. Jinými slovy, kybernetický incident je specifickým

případem kybernetické události, která reálně ohrozila nebo poškodila bezpečnost informačních systémů či elektronických komunikací. (Rohel, 2022)

Hlášení kybernetického bezpečnostní incidentu se týká státních institucí a firem spravujících kritické systémy, které mají za povinnost hlásit incidenty ihned po jejich zjištění. Dále se pak týká poskytovatelů digitálních služeb (např. cloudové platformy), které musí hlásit incidenty, pokud významně naruší jejich provoz. Hlášení se podává buď národnímu týmu CERT nebo Národnímu úřadu pro kybernetickou bezpečnost (dále v textu jen „NÚKIB“). Pokud incident významně ohrozí základní službu, její provozovatel musí okamžitě informovat o dané skutečnosti právě tento úřad (Česko, 2014).

Evidence incidentů a ochrana informací

NÚKIB vede databázi všech hlášených incidentů. Databáze obsahuje identifikaci postiženého systému, zdroje útoku a postup řešení. Data mohou být sdílena s CERT týmy a zahraničními bezpečnostními institucemi, ale přístup k nim je omezený. Zaměstnanci NÚKIB mají přísnou povinnost mlčenlivosti o těchto údajích – a to i po odchodu ze zaměstnání (Česko, 2014).

Opatření k ochraně před kybernetickými útoky

Zákon rozlišuje tři hlavní opatření pro ochranu systémů: varování, reaktivní opatření a ochranné opatření. Reaktivní opatření se provádí za stavu kybernetického nebezpečí nebo nouzového stavu (Česko, 2014).

Stav kybernetického nebezpečí

Stav nebezpečí nastává, když je ve velkém měřítku ohrožena bezpečnost informačních systémů, elektronických komunikačních služeb nebo integrity a ochrana komunikačních sítí. Tento stav může vést k narušení nebo ohrožení zájmů České republiky (dále v textu jen „ČR“) v souladu se zákonem o ochraně utajovaných informací (Česko, 2014).

1.1.5 Sít'ové zabezpečení

Sít'ová bezpečnost zahrnuje soubor opatření zaměřených na ochranu dat při jejich přenosu mezi zařízeními. Efektivní strategie sít'ového zabezpečení zahrnuje kombinaci fyzických, technických a administrativních kontrol, které chrání síť před neoprávněným přístupem a útoky. Nejčastěji zahrnuje: Firewall ochranu, segmentační síť a monitorování provozu. Firewall ochrana je klíčovým prvkem, který blokuje neoprávněný sít'ový provoz a zabraňuje tak přístupu k citlivým systémům. Dále je důležité zavést segmentaci sítí, která spočívá

v oddělení důležitých systémů od méně citlivých částí infrastruktury, čímž se zvyšuje bezpečnost a minimalizuje riziko přenosu útoků mezi různými částmi sítě. K tomu se přidává monitorování síťového provozu, které pomocí systému SIEM (Security Information and Event Management) umožňuje včasnou detekci anomálií a potenciálních hrozeb. Tato kombinace opatření vytváří komplexní ochranu, která je schopná reagovat na různorodé bezpečnostní incidenty (Yarali et al., 2022).

SIEM je zásadním nástrojem pro monitorování bezpečnostních událostí v reálném čase. Analyzuje bezpečnostní incidenty a identifikuje anomálie. Shromažďuje a archivuje logy z různých systémů.

Cloudová bezpečnost a vzdálený přístup

Rostoucí popularita cloudových služeb přináší nové výzvy v síťové bezpečnosti. Hlavní bezpečnostní principy zahrnují:

- Šifrování dat při přenosu i v klidu – ochrana citlivých informací uložených v cloudu.
- Monitorování cloudových aktivit například pomocí CASB (Cloud Access Security Broker) pomáhá sledovat a řídit přístup ke cloudovým službám (Yarali et al., 2022).

1.1.6 Počítačové zabezpečení

Ochrana počítačových systémů se soustředí na zabezpečení hardwaru, softwaru a dat proti interním i externím hrozbám, aby bylo zajištěno jejich stabilní fungování. Naopak zabezpečení počítačových sítí se zaměřuje na ochranu dat během přenosu, bezpečnost úložišť v síťovém prostředí a obranu proti únikům dat informací (Zhang, 2024).

Hardwarová zabezpečení

Na základní úrovni musí být počítačové zařízení uloženo na zabezpečených místech, ke kterým mají přístup pouze oprávněné osoby. Proto ve většině kanceláří v organizacích bývají počítače zabezpečeny například biometrickými prostředky. Uvnitř počítačů může být speciální procesor založený na trusted platform module (TPM), který řídí šifrované spojení mezi zařízeními. Díky tomu může zbytek systémů fungovat i když je jeden napaden. Jedním z nejpokročilejších bezpečnostních hardwarových prvků je systém detekce průniku (IDS – Intrusion Detection systém). IDS monitoruje datový tok a dokáže identifikovat pokus o hackerský útok na síť (CRELIN, 2024).

Softwarová zabezpečení

Jedním z nejdůležitějších softwarových zabezpečení jsou firewally, které chrání citlivá data v počítačích nebo přenášených po síti. Jsou využívány k ochraně osobních identifikačních údajů, například rodných čísel stejně jako důvěrných obchodních či vládních informací (CRELIN, 2024).

Dalším typem zabezpečení jsou antivirové softwary, které detekují, blokují a odstraňují malware, jako jsou viry, trojský koně nebo spywary. Je snadno dostupný, široce používaný a jeho instalace je jednoduchá. Automatické skenování a pravidelné aktualizace zajišťují ochranu před novými hrozbami. Minimalizuje kybernetická rizika a chrání zařízení i data před neoprávněným přístupem (A. Anderson Sr., 2024).

Příbuzným softwarem antiviru je EDR, který poskytuje monitoraci a reakční schopnosti pro koncové zařízení, jako jsou počítače, chytré telefony a servery. Tyto technologie překračují možnosti tradičního antiviru díky strojovému učení (A. Anderson Sr., 2024).

1.2 Fyzická bezpečnost

Fyzickou bezpečnost lze chápat jako soubor opatření, který má za cíl neoprávněné osobě zabránit nebo ztížit přístup k utajovaným informacím. K tomu slouží zabezpečené objekty a jednacích oblasti. Těmito objekty se rozumí zabezpečené budovy, ve kterých dochází ke zpracování, uchování a ochraně utajovaných informací. Pravidla pro jejich zabezpečení stanovuje zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti (Národní bezpečnostní úřad, © 2024).

Fyzická bezpečnost zahrnuje tradiční ochranná opatření proti různým hrozbám, a to jak úmyslným, tak neúmyslným, které mohou ohrozit fyzické prostředí a infrastrukturu organizace. Úroveň fyzické bezpečnosti odpovídá hodnotě chráněného majetku. Vládní instituce a firmy provádějí špičkový výzkum a využívají pokročilé bezpečnostní systémy, včetně biometrických kontrol. Nicméně i organizace s nižší úrovní citlivých dat musí chránit osobní a zaměstnanecké informace, aby předešly právním problémům (Merkow a Breithaupt, 2014).

1.2.1 Prostředky fyzické bezpečnosti

Do těchto prostředků spadají mechanické zábranné prvky, které definují fyzické hranice zařízení, činností nebo oblastí. Mají za úkol zmírnit nebo zpomalit přístup a obvykle tvoří trvalou překážku kolem chráněného objektu.

Tyto bariéry jsou:

- přírodní bariéry: například hory, pouště, útesy, příkopy,
- strukturální bariéry: lidsky vytvořené prvky, jako jsou ploty, zdi, podlahy.

U těchto bariér jsou důležité jejich vlastnosti jako je velikost, náklady, velikost chráněné oblasti nebo ochrana proti vozidlům. Například v případě prevence výbuchu bomb je důležitá dostatečná vzdálenost od chráněného objektu. U bariér je nezbytná také jejich údržba a kontrola, aby nedošlo k narušení její odolnosti. Důležitou součástí bariér jsou vstupy a výstupy, které musí mít obecně vzato stejnou nebo vyšší úroveň zabezpečení než samotný plot (Fennelly, 2013).

Systém kontroly vstupu do zabezpečené oblasti zahrnuje poplachové a elektronické bezpečnostní systémy, které se zaměřují na detekci podmínek pro vstup. Mezi tyto podmínky patří identifikační prvky, jako je heslo, PIN, biometrie nebo jiné prvky, které slouží k ověření oprávnění osob pro vstup do chráněných prostor. K zabezpečení oblasti se používají také poplachové zabezpečovací a tísňové systémy. Tyto systémy zahrnují ústředny elektrické zabezpečovací signalizace, detektory, ořesové detektory a perimetrické detekční systémy, které monitorují okolí, a tísňové signály pro rychlou reakci v případě ohrožení (Kolouch a Bašta, 2019).

Dále jsou součástí ochrany CCTV (uzavřený televizní okruh), přičemž kamerové systémy slouží k monitorování chráněné oblasti. Pro prevenci požáru jsou využívána zařízení elektrické požární signalizace (EPS) a také prostředky, které omezují působení požáru a živelních událostí, jako jsou poplachové systémy, detektory kouře, stejně jako samočinné hasicí systémy, které automaticky reagují na vznikající požár (Kolouch a Bašta, 2019).

Aby byla zajištěna kontinuita provozu i v případě výpadku elektrického napájení, používají se zařízení pro zajištění ochrany před selháním dodávek elektrické energie. Patří sem například záložní zdroje (UPS) nebo diesel agregáty, které zajistí napájení klíčových systémů v krizových situacích (Kolouch a Bašta, 2019).

1.2.2 Integrace fyzické a kybernetické bezpečnosti

V moderním bezpečnostním prostředí dochází ke stále větší integraci fyzické a kybernetické bezpečnosti. Mnoho bezpečnostních systémů, jako jsou kamery, dveřní zámky nebo alarmy, je dnes propojeno s IT infrastrukturou, což vytváří nové výzvy v oblasti ochrany.

V souvislosti s tím je nutné zajistit ochranu síťových prvků, a to především zabezpečením přístupových bodů, serveroven a dalších síťových zařízení proti fyzickému poškození nebo neoprávněnému přístupu (Yarali et al., 2022).

Dalším důležitým prvkem je zabezpečení cloudových a datových center, kde přístup k serverům a citlivým datům musí být chráněn nejen z hlediska kybernetické bezpečnosti, ale i fyzicky. To zahrnuje fyzickou ochranu prostor, v nichž jsou servery umístěny, a kontrolu přístupů, aby bylo zajištěno, že neoprávněné osoby nemohou manipulovat s těmito klíčovými zařízeními (Yarali et al., 2022).

Prevence proti útokům na přístupové systémy se zaměřuje na ochranu před kybernetickými útoky, které cílí na zařízení jako přístupové karty, čtečky biometrie nebo bezpečnostní kamery. Útoky na tyto systémy mohou vést k závažným bezpečnostním incidentům, a proto je nezbytné implementovat účinné ochranné mechanismy na obou stranách – jak na fyzické, tak i na kybernetické (Yarali et al., 2022).

2 PRÁVNÍ NORMY

Informační bezpečnost a ochrana obyvatelstva jsou regulovány mnoha předpisy na národní, mezinárodní i evropské úrovni. Tato kapitola se zaměří na právní normy, které stanovují povinnosti a opatření v této oblasti.

Základní právní rámce v České republice:

Zákon č. 181/2014., o kybernetické bezpečnosti a souvisejících předpisy

Stanovuje pravidla ochrany informačních systémů, zejména kritické infrastruktury. Zákon je opakovaně novelizován především zákonem č. 205/2017 Sb., které zavádí evropskou Směrnicí NIS.

Klíčové vyhlášky:

- Vyhláška č. 317/2014 Sb. – definuje významné informační systémy a kritéria pro jejich určení.
- Vyhláška č. 437/2017 Sb. – stanovuje kritéria pro určení provozovatelů základních služeb, vychází ze Směrnice NIS.
- Vyhláška č.82/2018 Sb. – nahrazuje starší vyhlášky, stanovuje požadavky na bezpečnostní opatření informačních systémů kritické infrastruktury a základních služeb. (Smejkal et al., 2019)

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

Tento zákon stanovuje pravidla pro určování utajovaných informací, podmínky jejich zpřístupnění a opatření k jejich ochraně. Zároveň upravuje zásady pro vymezení citlivých činností, podmínky jejich provádění a související výkon státní správy. V zákoně se nachází zmínky o informační bezpečnosti například v paragrafu 19, kde se přímo zabývá požadavky na ochranu utajovaných informací při jejich zpracování, přenosu a uchovávání informačních a komunikačních systémů (Česko, 2005).

Zákon č. 110/2019 Sb., o zpracování osobní údajů

Upravuje ochranu osobních údajů v České republice a doplňuje obecné nařízení Evropské unie známé jako GDPR. Zaměřuje se na stanovení fyzických osob při zpracování jejich údajů a povinností subjektů, které tyto údaje zpracovávají. Věnuje se mimo jiné pravidlům pro nakládání s osobními údaji, podmínkám pro jejich zpracování, povinnostem správce a zpracovatele, i otázkám zabezpečení a dohledu. Součástí právní úpravy je rovněž vymezení

role dozorového orgánu a nástroje k zajištění souladu s legislativou, včetně možné odpovědnosti za porušení pravidel ochrany údajů (Česko, 2019).

Národní strategie kybernetické bezpečnosti a Akční plán kybernetické bezpečnosti

Národní strategie kybernetické bezpečnosti České republiky na období 2021 až 2025 je dokument, který vysvětluje hlavní principy a strategické směry v oblasti kybernetické bezpečnosti. Je strukturován do tří hlavních vizí: sebevědomě v kyberprostoru, silná a spolehlivá spojení, odolná společnost 4.0 (Smejkal et al., 2019).

Pro implementaci této strategie byl vypracován akční plán k národní strategii kybernetické bezpečnosti České republiky na období 2021 až 2025. Tento plán obsahuje konkrétní úkoly a opatření, které mají zajistit dosažení stanovených cílů strategie (Smejkal et al., 2019).

2.1 Evropská legislativa a mezinárodní normy

Směrnice NIS

Směrnice Evropského parlamentu a Rady (EU) 2016/1148, známá jako směrnice NIS, byla přijata 6. července 2016 a vstoupila v platnost 8. srpna 2016. Jejím hlavním cílem je sjednotit právní předpisy členských států v oblasti ochrany informačních systémů a sítí a zajistit jednotnou úroveň kybernetické bezpečnosti v rámci celé Evropské unie (dále v textu jen „EU“) (Smejkal, 2022).

Směrnice NIS2

EU nyní přichází s novou směrnicí NIS2, která bude reagovat na nové kybernetické hrozby a rozšiřuje pravidla pro více organizací a institucí. Dále rozšiřuje působnost do více sektorů (např. výzkumná centra, potravinářství, veřejné správy). Zpřísňuje bezpečnostní požadavky pro firmy a instituce. Přidává povinnost hlášení kybernetických incidentů, a to například v situaci kybernetického útoku, kdy je organizace povinna hlásit tuto skutečnost například CERT týmu. Také stanovuje přísnější sankce za nedodržení pravidel. NIS2 byla oficiálně schválena 27. prosince 2022 a platnost nabyla dne 16. ledna 2023. Česká republika musí své nová pravidla dle směrnice NIS2 zpracovat, a proto se rozhodla ne o novelizování původního zákona o kybernetické bezpečnosti, ale o vytvoření zcela nového zákona, kde bude tato směrnice implementována. Očekává se, že tento zákon vstoupí v platnost v červenci roku 2025 (Národní úřad pro kybernetickou a informační bezpečnost, 2024).

ISO/IEC 27000

Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí jsou důležitými aspekty pro organizaci a subjekt ochrany obyvatelstva, zejména v souvislosti s prevencí narušení informační bezpečnosti. Soubor norem ISO/IEC 27000 poskytuje strukturovaný rámec pro zajištění ochrany citlivých dat a minimalizaci kybernetických rizik. ISO/IEC je celosvětově uznávaným standardem pro systémy řízení bezpečnosti informací (ISMS), který stanovuje požadavky na jejich zavedení a správu. Kromě něj existuje řada dalších norem v rámci souhrnu ISO/IEC 27000, které organizacím pomáhají posilovat bezpečnostní opatření, chránit důvěrná data a zajišťovat kybernetickou odolnost. Tyto normy umožňují efektivní řízení ochrany informačních aktiv, včetně osobních údajů, finančních informací, citlivých dat zaměstnanců či důvěrných informací svěřených třetími stranami, a to je zásadní pro bezpečnostní subjekty i veřejnou správu (International organization for standardization, 2018).

Nařízení Evropského parlamentu o ochraně osobních údajů (GDPR)

Toto nařízení stanovuje zásady pro zpracování osobních údajů, mezi které patří zákonnost, korektnost, transparentnost, účelové omezení, minimalizace údajů, přesnost, omezení uložení, integrita a důvěrnost. Tyto zásady jsou důležité pro správné nakládání s osobními údaji. GDPR posiluje práva jednotlivců, jejichž údaje jsou zpracovávány. Mezi tato práva patří přístup k údajům, právo na opravu, výmaz (právo být zapomenut), omezení zpracování, přenositelnost údajů a právo vznést námitku proti zpracování (Evropská Unie, 2016).

V české legislativě nahradilo zákon č. 101/2000 Sb., o ochraně osobních údajů, který byl zrušen, zákonem č. 110/2019 Sb. V české republice dohlíží na implementaci GDPR Úřad pro ochranu osobních údajů, který má pravomoc kontrolovat dodržování nařízení a udělovat sankce za jeho porušení (Smejkal, 2022).

2.2 Národní instituce a bezpečnostní týmy

Národní úřad pro kybernetickou bezpečnost (NÚKIB)

Zajišťuje kybernetickou bezpečnost, ochranu utajovaných informací v oblasti informační a komunikačních systémů, kryptografickou ochranu a také se věnuje bezpečnostním aspektům veřejně regulované služby navigačního systému GALILEO (PRS). Spolupracuje s ostatními CERT a CSIRT bezpečnostními týmy v ČR i po celém světě. Přípravuje národní bezpečnostní standardy v oblasti kyberbezpečnosti, stanovuje ochranu utajovaných informací v oblasti informačních a komunikačních systémů a věnuje se výzkumu v oblasti

kybernetiky, především v oblasti šifrování (Národní úřad pro kybernetickou a informační bezpečnost, © 2025a).

Úřad pro ochranu osobních údajů (ÚOOÚ)

Úřad pro ochranu osobních údajů (dále v textu jen „ÚOOÚ“) byl zřízen 1. června 2000 jako nezávislý správní orgán dohlížející na dodržování právních předpisů v oblasti ochrany osobních údajů. Úřad se zapojil do evropských iniciativ, podílel se na ochraně osobních údajů v nových evropských demokraciích. Získal evropská ocenění za svou činnost a byl pořadatelem významných mezinárodních konferencí. Od 25. května 2018 dohlíží ÚOOÚ na implementaci GDPR, včetně odborných konzultací, seminářů a školení pro veřejnost a organizace. Poskytuje poradenství a sleduje vývoj v oblasti ochrany osobních údajů na národní i mezinárodní úrovni. Úřad se aktivně podílí na vzdělání, organizuje semináře pro veřejnou správu, ministerstva a školy (Úřad pro ochranu osobních údajů, © 2025).

CERT a CSIRT týmy

Vládní CERT a specializované CSIRT týmy hrají klíčovou roli v ochraně kritické informační infrastruktury a významných informačních systémů v souladu se zákonem o kybernetické bezpečnosti a jeho prováděcími předpisy. Každý stát, jehož kritické systémy jsou připojeny k internetu, musí být schopen efektivně reagovat na bezpečnostní hrozby, koordinovat řešení incidentů a přijímat opatření k jejich prevenci. Tyto týmy zároveň fungují jako první kontaktní bod pro státní instituce, organizace i pro veřejnost, poskytují bezpečnostní informace a pomáhají s řešením kybernetických útoků. Kromě toho hrají důležitou roli také v oblasti veřejnosti. Poskytují větší povědomí o kybernetické bezpečnosti a vzdělávají uživatele v oblasti bezpečnosti internetu. Subjekty spadající pod zákon o kybernetické bezpečnosti mají povinnost spolupracovat s vládním CERT týmem, zatímco organizace definované v paragrafu 3 písm. a) a b) se primárně řídí povinnostmi vůči národnímu CERT týmu. (Národní úřad pro kybernetickou a informační bezpečnost, © 2025b)

3 HROZBY A ÚTOKY NA INFORMAČNÍ BEZPEČNOST

Informační systémy jsou často vystaveny různým typům hrozeb, které mohou způsobit různé typy škod, které mohou vést ke značným finančním ztrátám. Škody na bezpečnosti informací mohou sahát od malých ztrát až po úplné zničení informačních systémů. Účinky různých hrozeb se značně liší. Některé ovlivňují důvěryhodnost nebo integritu dat, zatímco jiné ovlivňují dostupnost systémů (Jouini et al., 2014).

V současné době se organizace snaží pochopit, jaké jsou hrozby pro jejich informační aktiva a jak získat nezbytné prostředky k boji proti nim, což stále představuje výzvu. (Jouini et al., 2014)

3.1 Kybernetické útoky

Kybernetický útok může být provedený interně nebo externě. Záleží na organizaci, která je cílem útoku. Na základě tohoto rozlišení lze kybernetické útoky rozdělit do dvou kategorií, a to na vnitřní a vnější útok.

Vnitřní útok představuje narušení sítě nebo počítačového systému osobou, která má autorizovaný přístup k systému organizace. Tento typ útoku bývá často prováděn nespokojenými zaměstnanci nebo dodavateli, kteří mají přístup k citlivým informacím. Motivací pro takové útoky bývá nejčastěji pomsta nebo chamtivost. (Pande, 2017)

Safa et. al. (2015) zjistili, že hlavním důvodem selhání bezpečnosti informačních systémů je skutečnost, že právě tito odborníci představují nejzranitelnější článek bezpečnostním řetězci. Přesto že jsou jejich služby nepostradatelné, mohou zároveň představovat významnou hrozbu pro organizaci. V roce 2016 specialista na informační bezpečnost pracující pro společnost Zhaopin, známou internetovou firmu v Číně, prodal více než 155 000 osobních údajů z interních databází. (Ma, 2022)

Vnější útok je proveden útočníkem, který není součástí organizace a může být buď nezávislým útočníkem nebo osobou najatou někým zevnitř organizace. Organizace čelící vnějšímu kybernetickému útoku se obvykle potýká nejen s finančními ztrátami, ale také se ztrátou reputace. Externí útočníci často před útokem provádějí průzkum a shromažďují informace o zranitelnostech cílového systému (Pande, 2017).

Stále více společností je postiženo narušením kybernetické bezpečnosti, což vede k narušení osobních údajů a porušení soukromí jednotlivců. Přestože si stále více lidí uvědomuje hrozby kybernetické bezpečnosti, zůstávají často nejslabším článkem při

kybernetických útocích. Podle výroční zprávy společnosti Cisco jsou hlavním cílem kybernetických útoků nedostatečné znalosti kybernetické bezpečnosti u jednotlivců, kteří se dopouštějí chování ohrožujícího bezpečnost, například klikání na škodlivé odkazy v e-mailu nebo na webových stránkách (Ng et al., 2021).

3.1.1 Hacking

Označuje aktivity, které se snaží kompromitovat digitální zařízení, jako jsou počítače, smartphony, tablety, a dokonce i celé sítě. Hacking nebývá vždy označován za škodlivý, dnešní době je obvykle spojován s nelegálními aktivitami kyberzločinu. Hackeři jsou často motivováni finančním ziskem, protestem, špionáží nebo jenom zábavou a výzvou. Je obvykle technického charakteru, ale hackeři často využívají také psychologické metody, aby oběť přiměli ke kliknutí na škodlivou přílohu nebo k poskytnutí osobních údajů. Tyto metody se nazývají sociální inženýrství.

Ve skutečnosti lze hacking považovat za zastrašující pojem, který zahrnuje většinu ne-li všechny typy malwaru a škodlivých kybernetických útoků zaměřené na jednotlivce, firmy a vlády. Kromě sociálního inženýrství mezi běžné hackingové útoky patří malware a samotné útoky například DDOS útoky (Dushaj, © 2020).

3.1.2 Sociální inženýrství

Jedná se o způsob, jak donutit lidi, aby udělali něco, co by normálně neudělali, nebo aby prozradili citlivé informace, a to ne pomocí hackování nebo prolomení zabezpečení, ale přes manipulaci a klamání. Útočníci často používají různé triky k získání přístupu k informacím, podvodům nebo proniknutí do počítačových systémů. Jednou z technik je vydávání se za někoho jiného a přemlouvání uživatele, aby došlo k získání potřebných dat. Tento způsob se někdy nazývá blagging. Tento pojem se nevyužívá jen v kyberzločinech, ale využívá se například u vymahačů dluhů, soukromých detektivů, lovců odměn nebo bulvárních novinářů, kteří chtějí získat tajné informace (Crelin, © 2024).

Příklady metod:

Phishing a jeho varianty – Nejběžnější metoda, útočníci se vydávají za zástupce například bank nebo společností vydávající kreditní karty nebo jiné významné instituce. Tito útočníci kontaktují oběti prostřednictvím e-mailu nebo telefonu, aby z nich vylákali osobní údaje. Útočníci obvykle uvádějí falešné důvody, proč je nutné, aby oběť poskytla své citlivé informace (Crelin, © 2024).

a) Podle cíle

Spear phishing, při kterém útočníci provádějí důkladný průzkum svých obětí a vytvářejí osobní a relevantní zprávy. Kvůli této personalizaci je spear phishing těžké rozpoznat, a ještě těžší se proti němu bránit (Dushaj, © 2020).

b) Podle způsobu doručení:

- Smishing (SMS + phishing) – Útoky probíhají pomocí podvodných SMS zpráv, které se snaží oběť přimět k poskytnutí osobních údajů nebo kliknutí na škodlivý odkaz.
- Vishing (voice+ phishing) – Útočník využívá telefonní hovory, kde se vydává za důvěryhodnou osobu a zmanipuluje oběť k odhalení citlivých informací (Dr. Gururaj et al., 2024)
- Quishing (QR + phishing) – Termín quishing vznikl spojením slov QR a phishing a popisuje útok, při kterém kyberzločinci využívají QR kód k přesměrování uživatele na falešnou webovou stránku. Jakmile uživatel na tento web přistoupí, útočníci mohou pomocí sociálního inženýrství získat osobní nebo finanční údaje nebo ho dokonce přimět k instalaci malwaru (Dyer, 2023).

Honey trap – V této metodě útočník předstírá romantický nebo sexuální zájem o oběť a láká ji do online vztahu. Poté se snaží oběť přesvědčit, aby mu poskytla důvěrné informace nebo dokonce zaplatila peníze výměnou za to, že útočník nezveřejní sexuální obsah.

Baiting – Je jedním z nejběžnějších a nejjednodušších příkladů sociálního inženýrství. Sdílí rysy s phishingem, ale místo e-mailu využívá tzv. návnadu, kterou láká oběť k provedení určité akce. Příkladem: USB disk nalezený na veřejném místě při připojení se zpustí malware nebo falešné stahování zdarma (příklad – pirátské filmy, hudba a software, které obsahují škodlivý vir).

Další metody mohou být například pretexting (falešný scénář), sniffing (metoda odposlechu) a mnoho dalších. (Dr. Gururaj et al., 2024)

3.1.3 Malware

Jedná se o škodlivý software, známý také jako malware, který vytvořil hacker za účelem škodlivé činnosti. Vývojáři malwaru se snaží narušit důvěrnost, integritu nebo dostupnost dat nebo systémů, které tato data zpracovávají, přenášejí a ukládají. Většina dnešních druhů malwaru jsou v kombinovaných formách. Tím se myslí, že před mnoha lety byly hrozby

oddělené – malware byl buď červ nebo trojský kůň, ale ne obojí. Dnes většina malwaru vykazuje vlastnosti více kategorií škodlivého softwaru. Například určitý malware může mít vlastnosti červa, trojského koně nebo ransomware. Malware se do IT prostředí nedostává náhodou, ale skrze konkrétní slabiny například: neoprávněné zranitelnosti, chybné bezpečnostní konfigurace (nesprávné nastavení systému a služeb), slabé, uniklé nebo odcizené přihlašovací údaje, sociální inženýrství, hrozby zevnitř organizace a další (Rains, 2023).

Hlavní funkce malwaru

- Zachytávání stisků kláves (keylogging) – odcizení hesel a přihlašovacích údajů.
- Mazání nebo poškození souborů.
- Přístup k citlivým datům.
- Mazání systémových záznamů (logů).
- Vytváření zadních vrátek (backdoor) – umožňuje vzdálené ovládání infikovaného systému (Cornish, 2023).

Příklady malwaru

Ransomware – jedná se o vyděračský software, který zašifruje data na disku, zablokuje koncové zařízení a heslo uživateli sdělí až potom co zaplatí výkupné. (Šulc, 2018).

Adware – Adware je softwarová aplikace používaná společnostmi k marketingovým účelům: při běhu jakéhokoli programu se zobrazují reklamní odkazy. Adware může být automaticky stažen do systému při procházení jakékoli webové stránky a může se zobrazovat prostřednictvím vyskakovacích oken nebo prostřednictvím lišty, která se automaticky objeví na obrazovce (Dushaj, © 2020).

Spyware – je typ programu, který je nainstalován za účelem shromažďování informací o uživateli, jejich počítačích nebo zvyklostech při procházení internetu. Sleduje vše, co uživatel dělá bez jeho vědomí a odesílá data vzdálenému uživateli. Může také stahovat a instalovat další škodlivé programy z internetu (Dushaj, © 2020).

Příklady Šíření malwaru

Virus – Šíří se tak, že se připojí k jiným souborům a spustí se spolu s nimi. Může se dostat do počítače například přes nakažené programy nebo přenosná média. Aby se aktivoval, musí ho uživatel nevědomky spustit.

Trojský kůň – Vydává se za neškodný program, například aktualizaci nebo hru, ale na pozadí provádí škodlivé operace. Může umožnit útočníkům vzdálený přístup, krást citlivá data nebo instalovat další škodlivý software. Uživatel si ho často stáhne sám, aniž by tušil, že jde o hrozbu.

Červi – Šíří se automaticky mezi zařízeními, například přes e-mail, internet nebo síť a využívá slabiny zabezpečení k tomu, aby se bez zásahu uživatele dostal do dalších programů (Šulc, 2018).

3.1.4 Další příklady kybernetických útoků

V posledních letech se stále častěji setkáváme s útoky, které mají za cíl zablokovat určité části informační a komunikačních struktur, především servery připojené k síti internetu. Tyto útoky zahrnují například internetové bankovníctví a označují se jako **DoS** (Denial of service) nebo **DDoS** (distributed Denial of Service). Závisí to na tom, zda útok pochází z jednoho nebo více počítačů současně a jakými způsoby je prováděn. Tyto útoky se obecně definují jako pokus o dočasné nebo trvalé zamezení přístupu oprávněným uživatelům k nějaké službě (Smejkal, 2022).

SQL injection – se stal běžným problémem webových stránek využívajících databáze. K tomu dochází, když útočník provede škodlivý SQL příkaz do vstupního pole (například místo přihlašovacího jména nebo hesla), čímž obchází běžné ověřovací mechanismy. Úspěšný útok umožňuje útočníkovi: číst citlivá data z databáze, měnit její obsah (vkládat, upravovat nebo mazat data), provádět administrativní operace, například vypnutí databázového severu, získat obsah souborů uložených na serveru a v některých případech dokonce spustit příkazy přímo v operačním systému (Dushaj, © 2020).

Pharming je pokročilejší a nebezpečnější forma phishingu, která cílí na DNS servery. Při útoku dochází k přesměrování uživatele na podvrženou IP adresu místo skutečného webu. Falešné stránky věrně napodobují originál, takže uživatel nic nepozná a zadá své přihlašovací údaje, které následně získá útočník. Tento typ útoku se často zaměřuje na internetové bankovníctví (Kolouch, 2016).

3.2 Fyzické hrozby informační bezpečnosti

Fyzická bezpečnost hraje zásadní roli v ochraně kritické infrastruktury, informačních systémů a citlivých dat. Pro zajištění efektivní ochrany je nezbytné předem identifikovat možné fyzické hrozby, které mohou ohrozit bezpečnost organizace. Tyto hrozby mohou být způsobené přírodními faktory, technickým selháním nebo cílenými útoky ze strany jednotlivců či skupin.

Hlavní typy fyzických hrozeb:

Přírodní katastrofy představují významné hrozby pro bezpečnost a stabilitu infrastruktury. Mezi tyto katastrofy patří požáry, povodně, hurikány, tornáda, zemětřesení a extrémní klimatické podmínky, jako jsou silné mrazy, vedra a vysoká vlhkost. Tyto hrozby mohou mít vážný dopad na fyzickou i kybernetickou bezpečnost. Vedle přírodních hrozeb mohou nastat technická selhání, například výpadky elektrické energie, poruchy chlazení, elektromagnetické rušení nebo selhání stavebních konstrukcí, které mohou být způsobeny nadměrným zatížením nebo vnějšími vlivy (Merkow a Breithaupt, 2014).

V oblasti fyzické bezpečnosti informačních technologií se opíráme o zákon č. 40/2009., trestní zákoník, který stanovuje právní rámec pro ochranu IT infrastruktury před neoprávněným přístupem, poškozením či zničením. Tento zákon postihuje široké spektrum hrozeb, od krádeže a vandalismu až po sabotáž kritických systémů, čímž vytváří právní základ pro prevenci a postih kybernetické kriminality spojené s fyzickými útoky na informační aktiva.

- Krádeže – odcizení počítače, serveru nebo jiných IT zařízení.
- Poškození cizí věci: Úmyslné rozbití serveru, vymazání dat, zničení pevného disku.
- Neoprávněný přístup k počítačovému systému a nosiči informací – hacknutí serveru, získání citlivých informací bez povolení.
- Porušení domovní svobody – Vniknutí do serveroven za účelem sabotáže nebo odcizení zařízení.
- Neúmyslné poškození hardwaru.
- Vandalismus – zničení nebo narušení kabeláže, políh hardwaru atd.

- Sabotáž – Útok na kritickou IT infrastrukturu (např. datová centra, servery státní správy) (Česko, 2009).

Hlavním cílem prevence fyzických hrozeb je minimalizace rizika narušení provozu, ochrana majetku a snížení pravděpodobnosti krádeže či sabotáže. Přesto je fyzická ochrana brána jako druhotná ve srovnání s kybernetickou bezpečností. Její podcenění může mít závažné následky v podobě poškození infrastruktury, ztráty dat nebo dokonce ohrožení lidských životů (Merkow a Breithaupt, 2014).

4 OCHRANA OBYVATELSTVA

Ochrana obyvatelstva není omezena pouze na civilní ochranu, jako je varování, evakuace nebo nouzové přežití, ale zahrnuje širší spektrum opatření. Na její realizaci se podílejí nejen statní instituce, ale i právnické a fyzické osoby, včetně samotných občanů. Hlavním cílem je ochrana životů, zdraví, majetku a životního prostředí, a to v souladu s platnými zákony. Každý zodpovědný subjekt má jasně dané povinnosti vyplývající z právních předpisů, které nelze přenést na jinou instituci nebo osobu (Česko, 2020).

Strategické cíle a vize OO

V koncepci ochrany obyvatelstva jsou vymezeny tři hlavní strategické cíle, jejichž účelem je zajistit komplexní rozvoj systému ochrany obyvatelstva. Tyto cíle jsou dále rozpracovány do dvanácti specifických (dílčích) cílů, přičemž každý strategický cíl je podpořen čtyřmi konkrétními kroky. Mezi hlavní strategické cíle patří: zajištění rozvoje podmínek pro účinnou ochranu obyvatelstva. Mezi hlavní strategické cíle patří: zajištění rozvoje podmínek pro účinnou ochranu obyvatelstva, podpora realizace jednotlivých úkolů a opatření, a v neposlední řadě zefektivnění organizace a koordinace činností. V rámci těchto opatření je kladen důraz mimo jiné na zvýšení úrovně připravenosti veřejnosti na krizové situace ohrožujících životy, zdraví, majetek a životní prostředí, stejně jako na posílení schopností jednotlivých složek systému ochrany obyvatelstva (Česko, 2020).

4.1 Hlavní subjekty ochrany obyvatelstva

Mezi hlavní aktéry systému ochrany obyvatelstva patří složky integrovaného záchranného systému (IZS), který tvoří především Hasičský záchranný sbor České republiky (HZS ČR), Policie České republiky (PČR), Zdravotnická záchranná služba (ZZS) a jednotky požární ochrany zaražené do systému plošného pokrytí území kraje (MAGISTRÁT HMP, 2025).

Hasičský záchranný sbor České republiky (HZS ČR)

HZS ČR představuje základní koordinační složku integrovaného záchranného systému, která zpravidla přebírá velení na místě mimořádné události. Je odpovědný za koordinaci spolupráce mezi jednotlivými složkami IZS při provádění záchranných a likvidačních činností. Nasazení potřebných sil a prostředků probíhá prostřednictvím operačních a informačních středisek HZS ČR. Na strategické úrovni je činnost IZS řízena krizovými orgány krajských úřadů (MAGISTRÁT HMP, 2025).

HZS ČR využívá široké spektrum komunikačních a informačních technologií, zahrnujících systémy operačního řízení, radiokomunikační a telekomunikační platformy, geografické a analytické nástroje, a také jednotný systém varování a vyrozumění obyvatelstva. Tyto nástroje slouží nejen ke koordinaci zásahů, ale také k efektivnímu přenosu informací mezi složkami systému a veřejností (HZS ČR, © 2025a).

Policie ČR

PČR je jednotná ozbrojená složka, která zajišťuje bezpečnost a pořádek na celém území státu. Jejím hlavním posláním je ochrana života, zdraví a majetku občanů, udržování veřejného pořádku a prevence kriminality (Česko, 2008).

PČR využívá informační systémy ke splnění úkolů v rámci různých služeb, jako je pořádková, dopravní či kriminální policie, a také k provozování systémů, jejichž zřízení jí ukládá zákon. Každý informační systém má předem stanovený účel, od kterého se odvíjí doba uchování zaznamenaných údajů. Neexistuje tedy jednotná lhůta pro uchování dat ve všech systémech, ale každý z nich má svou vlastní. Po uplynutí stanovené doby jsou údaje automaticky vymazány (Schimmer, 2024).

V těchto informačních systémech se zpracovávají osobní údaje odpovídající jejich konkrétnímu účelu. Není proto možné obecně stanovit přesný seznam osobních údajů, které se v nich evidují, protože každý systém pracuje s jiným typem dat. PČR uchovává údaje o osobách ve svých informačních systémech podle stanovených skartačních lhůt, které jsou primárně určeny promlčecí dobou související s konkrétní událostí nebo protiprávním jednáním. Tyto lhůty se mohou pohybovat například v rozmezí jednoho, tří, pěti nebo deseti let, v závislosti na závažnosti případu (Schimmer, 2024).

Zdravotnická záchranná služba

ZZS je základní složkou IZS a poskytuje zdravotní péči. Děje se tak na základě tísňového volání, pokud zákon nestanoví jinak. Jejím hlavním úkolem je zajištění přednemocniční neodkladné péče pro osoby s vážným poškozením zdraví (Česko, 2011).

ZZS disponuje například Národním informačním systémem IZS (NIS IZS): jedná se o jednotný systém pro všechny složky IZS, který byl předmětem kontroly Nejvyššího kontrolního úřadu. Slouží k efektivnějšímu zpracování tísňových volání, optimalizaci nasazení záchranných jednotek a zlepšení vzájemné komunikace mezi složkami IZS. Díky tomu se zvyšuje úroveň veřejných služeb poskytovaných občanům (Nováková, 2024).

4.2 Ostatní důležité subjekty

Mezi ostatní složky IZS patří obecní policie, vyčleněné síly a prostředky ozbrojených sil, další bezpečnostní sbory, jiné záchranné sbory, orgány ochrany veřejného zdraví, havarijní, pohotovostní, odborné a další služby, nařízení civilní ochrany, neziskové organizace a sdružení občanů, které mohou být využity pro záchranné a likvidační práce.

Tyto složky poskytují pomoc při záchranných a likvidačních pracích na základě požadavků. V krizových situacích se také k ostatním složkám IZS připojují poskytovatelé lůžkové péče, kteří mají zřízený urgentní příjem (s výjimkou poliklinik). V Praze k těmto složkám patří městská policie, Český červený kříž, Záchranná brigáda kynologů, Vodní záchranná služba a další subjekty splňující stanovená kritéria podle zákona (Magistrát HMP, © 2025).

Informační systémy zřizuje například Agentura komunikačních a informačních systémů, která zajišťuje propojení resortních systémů s aliančními a veřejnými informačními systémy (Honek, 2025).

Subjekty krizového řízení

Krizové řízení v České republice zahrnuje soubor opatření a postupů zaměřených na přípravu, reakci a obnovu při krizových situacích, jako jsou přírodní katastrofy, technologické havárie či jiné mimořádné události. Klíčovou roli v tomto systému hrají různé subjekty na úrovni státu, krajů i obcí (Odbor bezpečnostní politiky, 2023). Hlavní subjekty krizového řízení jsou: vláda, ministerstva a jiné ústřední správní úřady, hejtmani krajů, starostové obcí s rozšířenou působností, starostové obcí, právnické osoby a podnikající fyzické osoby.

Tento systém zajišťuje koordinovanou reakci na krizové situace napříč různými úrovněmi veřejné správy a zahrnuje spolupráci s dalšími subjekty, jako jsou neziskové organizace, odborné služby či subjekty kritické infrastruktury (Malinovský a Zrucký, 2023).

Příklady informačních systémů krizového řízení:

- SYPOS: Tento systém poskytuje informační podporu krizového řízení a zajišťuje krizovou připravenost na všech úrovních organizace (TLP Solutions, spol. s r.o., © 2024).

- KISKAN: Krizový informační systém, který ukládá všechny relevantní informace do jedné databáze. Je určen například pro zpracování krizových plánů nebo plánů krizové připravenosti (ANAKAN s.r.o, © 2025).
- IS KRIZKOM: Nástroj pro koordinaci a podporu procesů při řešení požadavků na věcné zdroje během krizových stavů (SSHR Czech Republic, © 2025).
- ARGIS: Systém pomáhá orgánům krizového řízení obcí, krajů a ústředních úřadů plnit povinnosti podle příslušných zákonů a vyhlášek. Je spravován správou státních hmotných rezerv a slouží jako nástroj pro podporu hospodářských opatření při krizových stavech, zejména pro zajištění věcných zdrojů (SSHR, © 2025).

Subjekty kritické infrastruktury

Kritická infrastruktura zahrnuje důležité prvky a systémy, jejichž narušení by mělo závažný dopad na bezpečnost státu, základní životní potřeby obyvatelstva, zdraví osob nebo ekonomiku. V České republice je evidováno přibližně 1300 prvků kritické infrastruktury (HZS ČR, © 2025b).

Subjektem kritické infrastruktury se rozumí majitel nebo provozovatel prvků kritické infrastruktury, určené nařízením vlády o kritériích pro určení prvků kritické infrastruktury v platném znění. Mezi obecné oblasti, které zahrnují prvky kritické infrastruktury patří:

- energetika: elektřina, zemní plyn, ropa a ropné produkty, centrální zásobování teplem,
- vodní hospodářství,
- potravinářství a zemědělství: rostlinná a živočišná výroba, potravinářská výroba,
- zdravotnictví,
- doprava: silniční, železniční, letecká a vnitrozemská vodní doprava,
- komunikační a informační systémy: pevné a mobilní sítě elektronických komunikací, sítě pro rozhlasové a televizní vysílání, satelitní komunikace, poštovní služby, informační systémy, oblast kybernetické bezpečnosti,
- finanční trh a měna,
- nouzové služby,

- veřejná správa (Smejkal et al., 2019).

Provozovatelé těchto prvků, označení jako subjekty kritické infrastruktury, jsou odpovědní za jejich ochranu a musí splňovat specifické povinnosti stanovené zákonem, včetně vypracování plánu krizové připravenosti a určení odpovědného bezpečnostního zaměstnance (Ministerstvo vnitra ČR, © 2025).

DÍLČÍ ZÁVĚR

Teoretická část práce poskytla základní rámec pro pochopení problematiky informační bezpečnosti, a to zejména ve vztahu k institucím veřejné správy. Byly vymezeny hlavní principy a cíle informační bezpečnosti a kybernetické bezpečnosti, včetně důležitosti ochrany důvěrnosti, integrity a dostupnosti dat. Zvláštní pozornost byla věnována subjektům ochrany obyvatelstva, které čelí specifickým nárokům na spolehlivost a dostupnost svých informačních systémů.

Text se dále zaměřil na různé vrstvy ochrany – od síťového a systémového zabezpečení až po řízení přístupu a prevenci incidentů. Popsány byly rozdíly mezi běžnou bezpečnostní událostí a incidentem, včetně základních kroků, které by měli následovat po jejich řešení. Zdůrazněna byla i nezbytnost propojení fyzické a kybernetické bezpečnosti, která je důležitá pro ochranu kritické infrastruktury.

Samostatnou část tvořil přehled právního rámce, včetně evropských směrnic a národních bezpečnostních struktur, které se podílejí na ochraně informačních systémů. Právní prostředí vymezuje nejen povinnosti organizací, ale také nástroje, kterými lze incidentům předcházet nebo na ně reagovat.

Dále byla věnována pozornost konkrétním typům hrozeb, mezi které patří například phishing, malware nebo fyzické narušení technického prostředí. Tyto hrozby ukazují, že bezpečnostní rizika nejsou pouze technologického charakteru, ale často souvisejí i s lidským faktorem a organizačními nastaveními.

Získané poznatky slouží jako výchozí bod pro praktickou část práce, kde jsou modelovány konkrétní scénáře narušení informační bezpečnosti. Teoretická část tak napomohla vytvořit ucelený přehled, na jehož základě lze identifikovat slabá místa a navrhnout vhodná opatření pro zvýšení bezpečnosti organizace.

II. PRAKTICKÁ ČÁST

5 INFORMAČNÍ BEZPEČNOST SUBJEKTU OCHRANY OBYVATELSTVA

Vybraným subjektem ochrany obyvatelstva byl zvolen hasičský záchranný sbor územního odboru Olomouckého kraje, pro který je informační bezpečnost zásadním pilířem, protože ovlivňuje schopnost plnit různé úkoly. HZS ČR provozuje důležité informační systémy pro tísňovou komunikaci a koordinaci zásahů. Cílem je zajistit důvěrnost, integritu a dostupnost těchto informací – tedy chránit je před neoprávněným přístupem, zabránit jejich neoprávněné změně a zajistit, aby byly vždy k dispozici, když jsou potřeba. Následující body budou představovat principy informační bezpečnosti v HZS, které zahrnují ochranu citlivých informací, bezpečnost IT systémů, řízení přístupů a reakce na kybernetické hrozby.

HZS přichází s citlivými informacemi denně do styku. Mohou to být například osobní údaje občanů volajících na tísňovou linku, krizové a havarijní plány, informace o nebezpečných objektech či technologiích a další důvěrné materiály. Je nesmírně důležité, aby všechny tyto informace byly pečlivě chráněny před zneužitím nebo únikem. Pro tuto ochranu by HZS mělo využívat principy důvěrnosti informací: přístup k citlivým údajům mají pouze oprávnění pracovníci a vždy jen v rozsahu nezbytném pro výkon jejich práce. Důležité dokumenty a záznamy by měli být zabezpečeny jak technicky (šifrováním v elektronické podobě), tak i organizačně (ukládání archivech nebo zabezpečených databázích). Všichni příslušníci a zaměstnanci by měli být vedeni a seznámeni se zodpovědným sdílením informací.

5.1 Analýza současného stavu vybraného územního odboru v Olomouckém kraji

Na základě konzultace s příslušníkem HZS, který pracuje v daném územním odboru Olomouckého kraje, byly zjištěny následující skutečnosti.

Zaměstnanci mohou využívat počítače, které jsou již přihlášeny. Přihlašování uživatele se nevyžaduje při každém použití zařízení, což může být z hlediska fyzického přístupu rizikové, pokud pracovník od počítače odejde a relaci neuzamkne. Stahování souborů do počítačů je zakázáno, dá se to tedy považovat za prevenci proti zavlečení škodlivého softwaru. Nebylo však potvrzeno, zda je toto omezení technicky omezeno přímo v systému nebo pouze stanoveno organizačním opatřením.

Přístup k internetu je zaměstnancům povolen. Bylo uvedeno, že mohou navštěvovat například webové stránky sociálních sítí. Nebylo však potvrzeno, zda existují technická omezení nebo filtrování obsahu. Systém dvoufaktorové autentizace pro přístup do vnitřních systémů zaveden podle informací není. Také bylo uvedeno, že logování činnosti na pracovních počítačích probíhá, nicméně nelze vždy s jistotou určit, který konkrétní uživatel se v danou chvíli nachází u daného zařízení.

Pro zadávání údajů o výjezdech a další provozní činnosti se používá interní informační systém. Ten slouží primárně k evidenci zásahů, dokumentaci činností a zajištění přehledu o provozu. Prostřednictvím systému jsou zaměstnanci také informováni o důležitých interních změnách nebo bezpečnostních upozorněních, jako je například výzva ke změně hesla. Změna hesla probíhá pravidelně, konkrétní interval však není z bezpečnostních důvodů specifikován. Přístup do systému je realizován prostřednictvím osobního uživatelského účtu.

Rozsah oprávnění v informačním systému se liší podle pracovní pozice zaměstnance. Například velitel směny nebo vedoucí pracovníci mají přístup k širší škále funkcí než běžní výjezdoví hasiči. Mezi rozšířené možnosti může patřit zadávání a úprava údajů o výjezdech, přístup k organizační dokumentaci, evidence školení nebo administrativní operace v rámci systému.

Každý zaměstnanec HZS disponuje osobním identifikačním čipem, který je zároveň propojen se služebním průkazem. Tento čip určuje přístupová oprávnění zaměstnance na základě jeho zařazení a pracovní funkce. V případě změny zaměstnání nebo přearažení do jiného územního odboru dochází k úpravě přístupových práv – zaměstnanec automaticky ztrácí oprávnění na předchozím stanovišti.

V rámci územního odboru se nachází zabezpečená technická místnost, která slouží jako úložiště pro elektronické a komunikační zařízení. Bylo uvedeno, že úroveň zabezpečení se může mezi jednotlivými územními odbory lišit. Tento konkrétní územní odbor má přiděleného pracovníka, který zajišťuje technickou podporu a správu IT prostředků.

Při zásazích mají příslušníci HZS přístup k základním údajům osob, které nahlásily událost – typicky se jedná o jméno, adresu a telefonní číslo. Tyto údaje slouží výhradně pro potřeby zásahu a nejsou dlouhodobě uchovávány.

Během rozhovoru vyplynulo, že školení zaměstnanců, alespoň tedy v případě výjezdových hasičů, v oblasti kybernetické bezpečnosti probíhá, avšak spíše v obecné rovině. Zaměstnanci jsou seznámeni se základními pravidly, ale rozsah a pravidelnost školení nebyla podrobněji specifikována.

Jelikož se získané informace zakládají na rozhovoru s příslušníkem HZS a nejedná se o oficiální technickou dokumentaci nebo stanovisko organizace, je nutné na popsany stav nahlížet jako na orientační přehled praxe konkrétního územního odboru. Tyto poznatky slouží především jako výchozí materiál pro navržení možných scénářů.

5.2 Bezpečnostní rámec informačních systémů ve veřejné správě

Na základě provedené analýzy aktuálního stavu informační bezpečnosti na úrovni jednoho z územních odborů HZS bylo možné identifikovat určité reálné podmínky a způsob fungování IT systémů, ale také potenciální slabá místa. Pro objektivní posouzení těchto aspektů a následný návrh realistických scénářů narušení informační bezpečnosti je vhodné srovnat tato zjištění s obecně uznávanými zásadami, které by měly být v prostředí veřejné správy a krizového řízení standardem.

Jedním ze základních principů informační bezpečnosti je řízení přístupů. Každý uživatel by měl mít přístup pouze k těm systémům a datům, které potřebuje ke své práci. Tato oprávnění by měla být nastavována podle pracovního zařazení a pravidelně kontrolována. K zajištění identity uživatelů slouží autentizační mechanismy. Pokud je potřeba zvýšit úroveň zabezpečení, doporučuje se kromě hesla používat i další formu ověření, například čipovou kartu nebo jiný fyzický prvek.

Technická opatření zahrnují využití bezpečnostních prvků, jako jsou firewally, antivirové programy, systémy detekce a prevence průniku, segmentace sítí nebo šifrování. Tyto nástroje chrání infrastrukturu před neoprávněným přístupem, škodlivým kódem nebo pokusy o zneužití systémových zranitelností. Důležitou součástí obrany je rovněž zajištění bezpečné komunikace a ochrana dat, a to jak při přenosu, tak při ukládání. Šifrování datových přenosů a citlivého obsahu v úložištích minimalizuje riziko jejich zneužití v případě úniku nebo odcizení.

Další důležitou oblastí je zálohování a obnova provozu. Organizace veřejné správy by měly pravidelně vytvářet zálohy svých dat a konfigurací, a to ideálně do fyzicky či logicky oddělených úložišť. Součástí bezpečnostního rámce je také existence a testování plánů

obnovy provozu, které zajistí rychlé zotavení v případě kybernetického útoku. S tím úzce souvisí i schopnost včasného odhalení a reakce na bezpečnostní incidenty. Pro tyto účely se využívají monitorovací nástroje, logování přístupů, systém včasného varování a předem definované postupy reakce. Klíčové je nejen rychlé odhalení hrozby, ale i její izolace, odstranění a následná analýza s cílem zabránit opakování podobné situace.

Neméně důležitou součástí bezpečnostního rámce je vzdělávání zaměstnanců a budování bezpečnostního povědomí. Lidský faktor je často nejslabším článkem v oblasti kybernetické bezpečnosti, a proto je třeba věnovat pozornost pravidelnému školení, prevenci sociálního inženýrství a výuce správných návyků při práci s IT systémy. Zaměstnanci by měli být pravidelně informováni o aktuálních hrozbách a postupech, jak s nimi bezpečně nakládat.

5.3 Návrhy scénářů narušení informační bezpečnosti

Narušení informační bezpečnosti HZS představuje reálnou hrozbu, protože pracuje s citlivými osobními údaji, interními dokumenty, havarijními a krizovými plány a tím pádem také se strategickými informacemi. Jakékoli nedodržení bezpečnostních opatření může vést k neoprávněnému přístupu, úniku dat nebo narušení operačního řízení. Kybernetické útoky často zneužívají lidský faktor a patří mezi nejčastější hrozby, které mohou vést k vážným incidentům. Důležitou roli zde hraje také fyzická bezpečnost, která chrání datová centra a IT infrastrukturu před neoprávněným vniknutím.

Scénáře budou navrženy tak, aby ilustrovali reálné situace, které mohou v prostředí HZS nastat a zároveň aby daly vhodný podklad pro analýzu rizik a návrhu preventivních opatření a mohli upozornit na slabá místa v oblasti informací a IT systémů.

Každý scénář bude zahrnovat:

- identifikaci útočníka nebo původce incidentu,
- popis průběhu útoku nebo selhání,
- upřesnění zasaženého aktiva (informační systém, data),
- přímé a nepřímé dopady na činnost HZS,
- možnou reakci organizace a návrh protiopatření.

Scénáře také poukážou na možnou slabinu v systému, kterým může být například lidská chyba nebo slabé IT zabezpečení a ukážou, jak mohou jednotlivé reakce ovlivnit průběh incidentu. Volba scénářů je znázorněna v tabulce 1.

Tabulka 1 Volba scénářů.

Název scénáře	Typ útoku	Odkaz na realitu HZS
Spear-phishing s malwarem	Sociální inženýrství + malware	Absence 2FA, přihlášené stanice
Fyzický útok na serverovnu a ransomware	Fyzická + technická hrozba	Omezené fyzické zabezpečení
DDoS útok na tísňovou linku	Útok na dostupnost služby	Možné přetížení dispečinku

(zdroj: vlastní)

5.4 Důvody výběru jednotlivých scénářů

Výběr jednotlivých scénářů narušení informační bezpečnosti vychází z kombinace informací získaných během rozhovoru s pracovníkem HZS na úrovni územního odboru a teoretických východisek uvedených v předešlé podkapitole. Cílem bylo zvolit takové typové situace, které by realisticky mohly nastat v provozu HZS, a zároveň pokrývaly různorodé oblasti kybernetických hrozeb.

Mezi hlavní aspekty, které ovlivnily výběr konkrétních scénářů, patří zejména:

- Absence vícefaktorového ověřování, které zvyšuje riziko zneužití přihlašovacích údajů,
- nedostatečné zabezpečení fyzického přístupu k serverovně,
- přístup zaměstnanců k internetu bez jasně stanovených technických filtrů,
- nepotvrzené využívání VPN při vzdáleném připojení,
- obecně nízká úroveň školení v oblasti kybernetické bezpečnosti.

Vybrané scénáře proto reflektují nejen různé typy hrozeb, ale zároveň jsou úzce propojeny s konkrétními slabými místy, která byla během rozhovoru identifikována. Scénáře

nebyly zvoleny nahodile, ale s ohledem na reálnou proveditelnost útoků a jejich potenciální dopad na chod HZS.

Spear-phishing s malwarem

Scénář byl zařazen na základě dlouhodobého sledování trendů phishingových útoků, které patří mezi nejčastější vektory útoku v prostředí veřejné správy. Zprávy NÚKIB opakovaně konstatují, že phishing je stále velmi efektivní metodou, jak kompromitovat systémy organizací a dostat do jejich infrastruktury škodlivý kód. Přitom rozpoznat nebezpečný e-mail může být obtížné a v mnoha případech chybí technická i organizační opatření, která by těmto útokům zabránila (NÚKIB, 2023).

Spear-phishing navíc cílí konkrétně na vybrané osoby a využívá dostupné informace z veřejných zdrojů, což výrazně zvyšuje jeho úspěšnost. Vzhledem k tomu, že zaměstnanci HZS pravidelně komunikují s externími subjekty a přijímají velké množství dokumentů, je tento typ útoku pro organizaci vysoce relevantní (NÚKIB, 2023).

Fyzické napadení serverovny novým zaměstnancem s nasazením ransomwaru

Rizika spojená s tzv. vnitřním aktérem (Insider threat) představují důležitou, přesto často podceňovanou oblast informační bezpečnosti. NÚKIB ve svých výstupech opakovaně upozorňuje na nutnost věnovat dostatečnou pozornost správě přístupových práv, zejména při odchodu zaměstnanců z organizace. Nedostatečná kontrola fyzických přístupů nebo opomenutí deaktivace uživatelských účtů může vést k tomu, že osoba, která již nemá být oprávněna manipulovat s daty, získá přístup k důležitým systémům nebo serverům (NÚKIB, 2022).

Tento scénář navíc reaguje na stále častější případy útoků pomocí ransomwaru. Ten se řadí mezi nejškodlivější typy útoků posledních let a je typický zejména svou schopností ochromit celé systémy a požadovat výkupné za obnovu přístupu k datům. I přesto, že se většina ransomwarových útoků realizuje vzdáleně, není vyloučeno jeho nasazení formou fyzického připojení ke kritickému zařízení, to se může stát v případě slabých fyzických a organizačních opatření (NÚKIB, 2022).

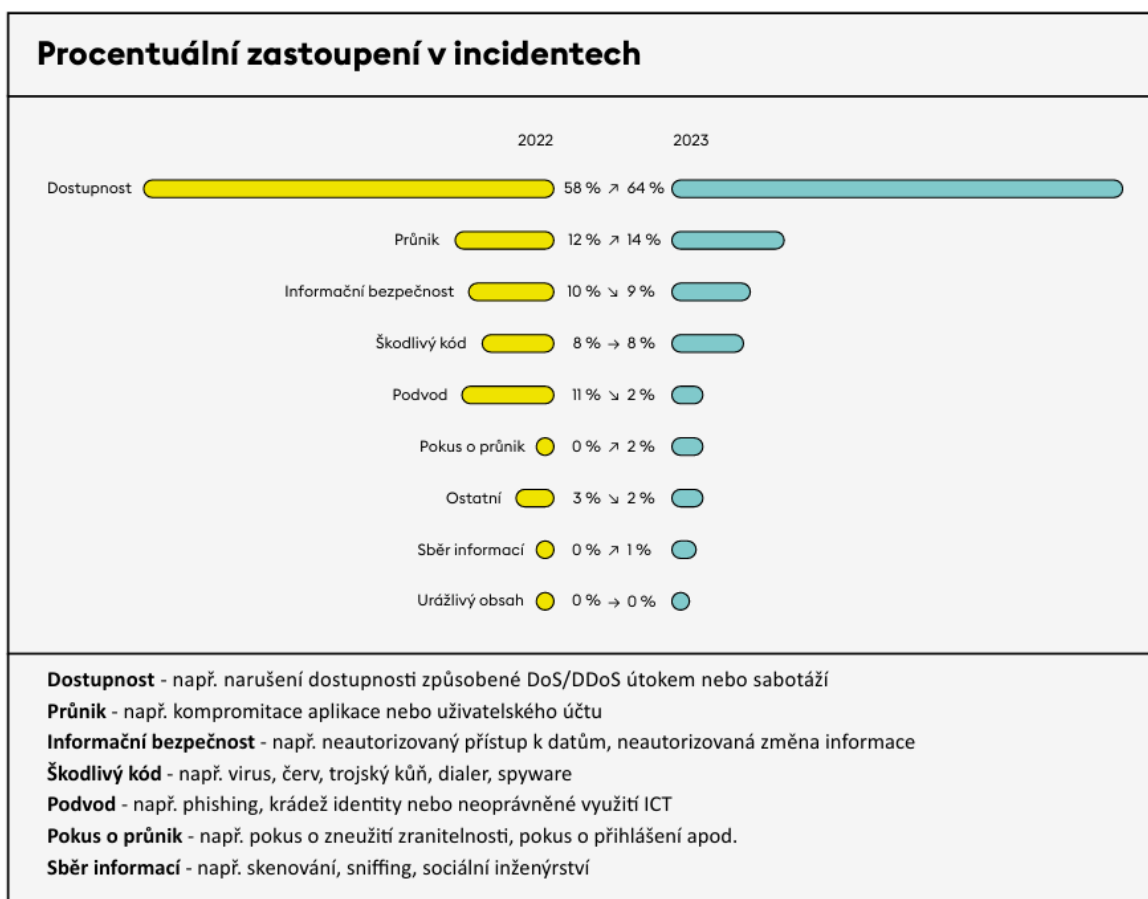
DDoS útok na tísňovou linku HZS

Narušení dostupnosti služeb je jedním z nejčastějších a nejvíce sledovaných typů incidentů. Útoky typu DDoS jsou v posledních letech hojně využívány nejen kriminálními skupinami, ale i jako nástroj hybridního působení. NÚKIB zaznamenal v roce 2022 a 2023 výrazný

nárůst tohoto typu útoku. Cílem se často stávaly právě veřejné instituce, jejich webové portály a další digitální rozhraní určené občanům.

V případě HZS může být útok na tísňovou linku závažný zejména v krizových situacích, kdy slouží jako hlavní komunikační kanál směrem k obyvatelstvu. Nedostupnost těchto linek může ohrozit včasné šíření pokynů, krizových oznámení a dalších informací důležitých pro veřejnost. Výběr tohoto scénáře je logickým krokem vzhledem k jeho frekvenci ve statistikách a důležitosti dostupnosti v HZS (NÚKIB, 2023). Tento scénář bude pouze hypotetický vzhledem k nízkému počtu informací od zaměstnance Územního odboru.

Následující obrázek znázorňuje porovnání jednotlivých kybernetických útoků za roky 2022 a 2023. Tyto incidenty jsou zastoupeny v procentech. Největší zastoupení má dostupnost, a to poměrně ve vysokém rozsahu.



Obrázek 5 Klasifikace kybernetických incidentů nahlášených NÚKIB – porovnání roku 2022 a 2023

(zdroj: NÚKIB, 2024)

6 POPIS SCÉNÁŘU NARUŠENÍ INFORMAČNÍ BEZPEČNOSTI

Tato kapitola se věnuje detailnímu rozpracování jednotlivých modelových scénářů narušení informační bezpečnosti, které byly navrženy v předchozí části. Každý scénář představuje specifický typ hrozby, který může v podmínkách HZS ČR teoreticky nastat, a to buď v podobě kybernetického útoku, neúmyslného pochybení zaměstnance nebo fyzického narušení bezpečnostní infrastruktury.

Každý scénář je členěn do několika částí, zahrnující identifikaci aktérů, popis průběhu incidentu, určení zasažených aktiv, analýzu dopadu a návrh správné reakce. Scénáře nejsou zamýšleny jako technická rekonstrukce skutečných incidentů, ale jako modelové situace odrážející známé bezpečnostní hrozby a slabiny, které se běžně vyskytují ve veřejném a soukromém sektoru.

Součástí analýzy jednotlivých scénářů narušení informační bezpečnosti byla také metoda what-if, která dokáže identifikovat potenciální rizika formou hypotetických otázek. Pro každý z modelovaných scénářů byla vytvořena stručná tabulka v textu, která zachycuje fáze útoku, možné situace typu, otázku, co kdyby, jejich potenciální dopady, pravděpodobnost výskytu a návrh vhodných opatření. Tato metoda přináší praktický pohled o slabých místech v jednotlivých fázích útoku a slouží jako základ pro návrh preventivních nebo reaktivních bezpečnostních opatření. Výsledky jsou uvedeny v rámci příslušných scénářů níže formou přehledných tabulek.

Dále byly u každého scénáře aplikovány specifické reakční plány podle charakteru útoku. Konkrétně se jedná o plán reakce na incident (IRP), plán kontinuity činností (BCM) nebo plán obnovy po havárii (DRP). Tyto plány byly strukturovány podle metodiky NIST SP 800-61r2 a slouží k systematickému zvládnutí incidentů od jejich identifikace až po obnovu běžného provozu a poučení se z dané události. Reakční plány navazují na výsledky what-if analýzy a představují návrh opatření pro každý modelový scénář.

Využití frameworku MITRE ATTACK v analýze scénářů

Pro popis jednotlivých scénářů bylo částečně přihlédnuto k rámci MITRE ATTACK. Tento framework poskytuje přehledné členění postupů, které útočníci využívají při realizaci kybernetických útoků. Útoky jsou zde rozděleny do tzv. taktik (jednotlivé fáze útoku) a technik (konkrétní způsoby provedení útoku). Díky tomu jde lépe porozumět průběhu incidentu, identifikovat slabá místa a zvažovat vhodná obranná opatření. (MITRE Corporation., © 2015–2025)

6.1 Modelový scénář Spear – phishing s malwarem

Sběr informací: Útočník začíná sběrem informací o vybraném zaměstnanci HZS. Útočník využívá veřejně dostupné zdroje, jako jsou oficiální webové stránky HZS, sociální sítě, profesní profily a další. Z těchto míst může útočník zjistit spoustu informací o zaměstnanci. Může se jednat například o příjmení nadřízeného, pracovní pozici, aktuální projekty nebo pracovní zařazení daného zaměstnance. Přes sociální sítě může útočník dohledat osobní e-mailové adresy, kdy osoba pracuje a jaké vykonává během pracovní doby činnosti. Také může zjistit další údaje o aktivitách, zájmech a profesním zaměření oběti. Analýza pracovního harmonogramu pomáhá útočníkovi určit vhodnou dobu pro doručení spear-phishingového e-mailu.

Phishingový útok: Na základě získaných informací útočník vytvoří falešnou e-mailovou adresu, která je velmi podobná oficiálnímu e-mailu velitele jednotky nebo pracovníka IT oddělení HZS. Obsah zprávy je navržen tak, aby vyvolal dojem naléhavosti a přiměl tak oběť jednat v panice nebo bez váhání.

Příklad e-mailové adresy:

Dobrý den pane (Jméno)

Potřebuji urgentně vyplnit dokument o dostupnosti jednotek v naší oblasti pro krizové plánování. V příloze naleznete formulář, který je nutné vyplnit a odeslat zpět do dnešního odpoledne.

Děkuji

S pozdravem (jméno nadřízeného)

Příloha: Kontrola_jednotek_HZS.xlsx

Infikování malwarem: Pokud oběť otevře přílohu, může se v dokumentu automaticky spustit škodlivý kód, který využívá přednastavené funkce programu. Tento kód následně stáhne a nainstaluje do systému škodlivý software. V tomto případě se jedná o tzv. keylogger, což je škodlivý software navržený k zaznamenávání všech stisknutých kláves na napadeném zařízení. Program se po instalaci skryje a běží tiše na pozadí operačního systému bez vědomí uživatele. Zaznamenává přihlašovací údaje, odeslané e-maily, texty, které uživatel píše, a případně dokáže také pořizovat snímky obrazovky.

Keylogger pravidelně odesílá získaná data útočníkovi prostřednictvím internetu, např. na vzdálený server pomocí šifrovaného přenosu. Útočník tak získává přístup k interním účtům včetně systémů, jako je např. e-mail, informační systémy HZS nebo aplikace pro krizové řízení. Po získání přístupů může manipulovat s krizovými plány, šířit malware dál nebo eskalovat útok do vnitřní sítě organizace.

Mezi možné dopady na HZS patří: neoprávněný přístup k operačním plánům a citlivým údajům HZS, riziko manipulace s krizovými opatřeními, to může ovlivnit efektivitu zásahu, narušení důvěry veřejnosti a složek IZS v bezpečnostní opatření HZS, právní následky v případě úniku citlivých informací, omezení koordinace a komunikace při mimořádných událostech.

Bezpečnostní reakce na incident: V případě podezření na kybernetický incident HZS implementuje následující kroky. Okamžitě nahlásí incident IT oddělení HZS. Izoluje infikované zařízení, aby se zabránilo dalšímu šíření malwaru. Resetují se přihlašovací údaje a zavede se více faktorové autentizace. Proběhne analýza malwaru a odstranění škodlivého softwaru bezpečnostním týmem. Bezpečnostní tým zkontroluje přístup k datům, aby zajistil, zda nedošlo k neoprávněné manipulaci. Nastolí se dlouhodobé preventivní opatření, včetně pravidelného bezpečnostního školení zaměstnanců, posílení ochrany e-mailové komunikace a monitorování síťové aktivity. Pokud je identifikován únik citlivých dat, incident je nutné ohlásit příslušným úřadům, a to včetně Úřadu pro ochranu osobních údajů.

6.1.1 What-if analýza – spear-phishing

Jako první je zpracována aplikace metody What-if na scénář spear-phishingového útoku (viz tabulka 3). Tento přístup umožňuje systematicky identifikovat slabá místa v jednotlivých fázích útoku prostřednictvím hypotetických otázek. Pro každou fázi byly stanoveny události, jejich možné dopady, pravděpodobnost výskytu a návrhy odpovídajících opatření.

Tabulka 2 What-if Scénář spear-phishing s malwarem.

Fáze útoku	Otázka "Co když..."	Dopady	Pravděp.	Opatření
Příprava útoku	Útočník získá informace o zaměstnanci HZS a jeho e-mailové adrese?	Cílený spear-phishingový útok, vyšší šance na úspěch.	Střední	Omezit veřejné údaje, školení o ochraně identity

Fáze útoku	Otázka "Co když..."	Dopady	Pravděp.	Opatření
Vniknutí (e-mail)	Zaměstnanec otevře škodlivou přílohu z podvrženého e-mailu?	Neoprávněný vstup do systému, instalace malwaru, krádež dat.	Střední	Školení proti phishingu, technické filtry, e-mailová bezpečnost
Infikování keyloggerem	Byl nainstalován keylogger a sbírání dat?	Zneužití citlivých informací.	Střední/nízká	Zálohování dat, segmentace sítí, omezení práv
Dopady incidentu	Dojde k neoprávněnému přístupu k citlivým datům HZS?	Finanční ztráty, ohrožení zásahů, právní následky.	Střední	Řízení přístupových práv, šifrování dat, logování
Reakce na incident	Detekce incidentu proběhne pozdě a útočník získá rozsáhlý informace z prostředí?	Rozšíření infekce, prodloužení doby obnovy provozu, poškození reputace.	Střední	Hlášení incidentů, monitoring logů, reakční scénáře
Vyšetřování incidentu	Analýza útoku a identifikace pachatele je neúplná nebo zdlouhavá?	Ztráta důkazů, obtížnější zavedení účinných preventivních opatření do budoucna.	Střední	Incidentní tým, forenzní nástroje, spolupráce s experty
Preventivní opatření	Zavedená preventivní opatření nejsou dostatečně účinná proti sofistikovaným útokům?	Opakování podobných incidentů, trvalé ohrožení informační bezpečnosti.	Střední	Bezpečnostní audity a penetrační testy, aktualizace politik, vzdělávání

(zdroj: vlastní)

6.1.2 Reakční plán – IRP

1. Příprava: Cílem přípravné fáze je vytvořit podmínky, které umožní efektivní detekci a zvládnutí incidentu. V prostředí HZS by měla být zavedena školení uživatelů zaměřená na rozpoznávání phishingových e-mailů, podezřelých příloh a hypertextových odkazů. Dále je vhodné mít technické nástroje pro analýzu příloh, antivirovou ochranu a bezpečnostní politiky zakazující spouštění neznámých souborů. Organizace by měla také zavést systém hlášení incidentů, jasně definovat odpovědné osoby (např. IT správce) a mít vytvořený plán pro izolaci zařízení.

Součástí prevence je i důsledné řízení přístupových práv a ideálně zavedení vícefaktorové autentizace pro přístup k e-mailovým účtům. Vzhledem k tomu, že počítače jsou již přihlášeny, je vhodné aplikovat časový limit pro automatické odhlášení nebo zámek obrazovky.

2. Detekce a analýza: Incident typu spear-phishing s nasazením keyloggeru může být odhalen několika způsoby – např. antivirovým programem, bezpečnostním nástrojem pro správu koncových bodů nebo samotným uživatelem. Typické projevy zahrnují zpomalení zařízení, neautorizované odesílání e-mailů nebo přístup z neznámé IP adresy.

Po detekci musí zaměstnanec incident nahlásit pověřené osobě. Tato osoba provede základní identifikaci incidentu: zjištění typu útoku, napadeného zařízení a jeho uživatele, časového průběhu incidentu a rozsahu napadení. Pokud došlo k možnému úniku osobních údajů, je nutné zvažovat i ohlášení incidentu Úřadu pro ochranu osobních údajů.

3. Zvládání incidentu:

Zabránění šíření: Prvním krokem je odpojení infikovaného zařízení od sítě a zablokování přístupového účtu, aby nedošlo k dalšímu přenosu dat či rozesílání phishingových zpráv.

Odstranění hrozby: následuje forenzní analýza zařízení – identifikace škodlivého souboru, odstranění keyloggeru, kontrola systémových procesů a registry. Provádí se aktualizace systému a bezpečnostních nástrojů.

Obnova: Zařízení je znovu připojeno k síti pouze po provedení testů a ověření, že je zbaveno hrozby. Změní se přihlašovací údaje a ověří se integrita e-mailového účtu. V případě větší kompromitace se může využít zálohovaný stav operačního systému nebo zařízení kompletně reinstalovat.

4. Závěrečná fáze: Po vyřešení incidentu je vhodné provést revizi organizačních a technických opatření. Vyhodnocuje se, jak došlo k průniku – zda byl selháním uživatele, nedostatečnou ochranou systému nebo chybějícím školením. Doporučuje se zpřísnění e-mailové politiky (např. filtrování příloh), zavedení sandboxů pro otevírání neznámých souborů a audit dalších uživatelských zařízení. Na závěr je incident zdokumentován a případně využit při budoucím školení zaměstnanců. Pokud šlo o závažný incident, může být vytvořen interní report vedení s doporučením změn v infrastruktuře.

6.2 Modelový Scénář DDOS útoku na tísňovou linku HZS

Tento scénář popisuje modelovou situaci, při které dochází k narušení informační bezpečnosti HZS v důsledku rozsáhlého kybernetického útoku typu DDoS. Jedná se o cílený útok, který má za cíl záměrně přetížit komunikační infrastrukturu – v tomto případě tísňovou linku HZS. Tím, že ji přetíží, naruší její fungování a znemožní tak komunikovat a reagovat HZS na vzniklé mimořádné události. Oproti ostatním útokům se DDoS útok nesnaží získat data nebo neoprávněný přístup do systému.

Příprava útoku: Útok začíná fází přípravy, během které účastník hrozby sbírá veřejně dostupné informace o fungování tísňových linek. Věnuje se především technickým aspektům infrastruktury, jako je zpracování hlasových hovorů, používané technologie, struktura přístupových bodů a úroveň zajištění proti přetížení. Cílem útočníka je najít slabá místa, která je možné zneužít pro přetížení systému. Na základě zjištěných informací si účastník hrozby připraví útokovou infrastrukturu, nejčastěji v podobě botnetu. Jedná se o síť kompromitovaných zařízení, které lze vzdáleně ovládat a koordinovaně využít k útoku.

Zahájení útoku a jeho průběh: Útok je zahájen v momentě, kdy lze očekávat největší dopad. Jedná se o situace během krizové situace, v nočních hodinách nebo při výskytu jiné události. Botnet začne generovat velké množství falešných požadavků na spojení, které jsou směřovány na komunikační rozhraní tísňové linky. Dispečeri nejsou schopni identifikovat reálné volání, protože jsou pohlceni několika neexistujícími požadavky. Dochází tak k odříznutí obyvatelstva od možnosti přivolání pomoci. Útok může být zaměřen nejen na jednu lokalitu, ale i koordinovaně po celém kraji. V důsledku toho se veřejnost snaží kontaktovat ostatní složky IZS, a tím dochází k přetížení celého záchranného systému.

Dopady incidentu: Nedostupnost tísňové linky má za následek zpoždění nebo dokonce znemožní reakce na mimořádné události. Útok způsobuje narušení koordinace mezi složkami IZS, a to má dopad na rychlost zásahů a na efektivitu rozhodovacích procesů. Dlouhodobá nedostupnost může způsobit ztrátu důvěry veřejnosti v instituce krizového řízení. Z hlediska právního rámce pak vzniká povinnost nahlásit incident NÚKIBu, pokud se jedná o subjekt spadající pod zákon o kybernetické bezpečnosti.

Reakce na incident: Po zjištění přítomné anomálie v provozu je aktivován reakční postup. Probíhá vyhodnocení útoku, přesměrování provozu na alternativní linky a zapojení jiných krajských dispečerů. Současně se zajišťuje informovanost obyvatelstva

prostřednictvím jiných komunikačních kanálů, například webové stránky, sociální sítě, SMS. Do řešení se zapojuje poskytovatel služeb, popřípadě NÚKIB.

Opatření a prevence: Po odeznění útoku je provedena forenzní analýza, která slouží k identifikaci slabin a určení preventivních opatření. Následně je aktualizována bezpečnostní dokumentace a procesy krizové komunikace. Mezi doporučená opatření patří implementace anti-DDoS technologií, segmentace sítí, monitoring provozu a pravidelná cvičení připravenosti. Důležité je také vzdělávání personálu a posilování alternativních forem komunikace pro případ výpadku primárních služeb.

6.2.1 What-if analýza – DDoS útok

Scénář DDoS útoku byl analyzován také metodou What-if (viz tabulka 4), která umožňuje podrobně posoudit jednotlivé fáze útoku a identifikovat možná rizika spojená s narušením dostupnosti důležitých služeb. V rámci analýzy byly formulovány hypotetické situace, jejich pravděpodobnosti, dopady a vhodná technická či organizační opatření ke snížení zranitelnosti systému.

Tabulka 3 What-if Scénář DDoS na tísňovou linku HZS.

Fáze útoku	Otázka "Co když..."	Dopady	Pravděp.	Opatření
Příprava útoku	Útočník získá detailní informace o specifické infrastruktuře hlasové komunikace?	Efektivnější útok, rychlejší zahlcení	Střední	Ochrana detailů, zabezpečená dokumentace, školení
Zahájení a průběh útoku	Koordinovaný útok zahltní primární komunikační infrastrukturu rychleji, než se očekávalo?	Nedostupnost tísňové linky, panika	Střední	Záložní systémy, sítě s vyšší kapacitou a spolehlivá technická zařízení
Reakce na nedostupnost	Alternativní komunikační kanály (např. volání na jiné složky IZS) budou také přetíženy v důsledku paniky veřejnosti?	Omezený přístup k poskytnutí pomoci, frustrace	Nízká	Posílení náhradních kanálů, komunikace s veřejností
Dopady incidentu	Ztráta komunikační linky způsobí zpoždění při řešení kritických událostí?	Zpoždění zásahu, ohrožení života osob	Vysoká	Krizové plány, nácvik, záloha komunikace

Fáze útoku	Otázka "Co když..."	Dopady	Pravděp.	Opatření
Reakce na incident	Přesměrování provozu na záložní systémy selže z technických důvodů nebo nedostatečné kapacity?	Prodloužení výpadku, výpadek komunikace	Nízká	Záložní systémy umístěné na více místech, automatické přepínání při výpadku, testování kapacit
Informování veřejnosti	Informování o výpadku a alternativních způsobech kontaktu bude zpožděné nebo neúčinné?	Zmatek, panika, dezinformace	Střední	Komunikační plán, automatizace, spolupráce s médii
Opatření a prevence	Testování odolnosti infrastruktury proti zahlcení neodhalí všechny zranitelnosti nebo nově vzniklé hrozby?	Opakování útoků, nízká připravenost	Střední	Penetrační testy, monitorování, aktualizace systémů

(zdroj: vlastní)

6.2.2 Reakční plán – IRP

1. Příprava: Před samotným incidentem je nezbytné zajistit základní ochranu proti distribuovaným útokům typu DDoS. Mezi klíčová opatření patří spolupráce s poskytovatelem internetového připojení na nasazení filtračních mechanismů. Využít lze také aplikační firewally a dostupné možnosti filtrování provozu prostřednictvím infrastruktury poskytovatele. Dále je doporučeno nastavit limity příchozích požadavků a zavést pravidelní zátěžové testy infrastruktury. V rámci příprav musí být vypracován aktualizován krizový komunikační plán a všichni pracovníci musí být seznámeni s nouzovým režimem fungování tísňové linky.

2. Detekce a analýza: Incident je detekován prostřednictvím síťového monitoringu, který indikuje abnormálně vysoký počet požadavků směřující na síťovou infrastrukturu využívanou HZS. Může se jednat např. o interní systémy podporující provoz dispečerských a operačních činností. Zaznamenává se výrazné zpomalení systému, případně úplná nedostupnost služby. Následuje analýza logů, identifikace typů provozu a zjištění, o jaký typ DDoS útoku se jedná. Zároveň se vyhodnocuje, zda se nejedná o součást většího koordinovaného útoku.

3. Reakce:

Zabránění dopadu: Ve spolupráci s poskytovatelem konektivity se aplikuje přesměrování provozu nebo filtrování škodlivého provozu pomocí upstream filtrů.

Odstranění hrozby: Identifikované rozsahy IP adres útočníka jsou blokovány, služba je přesměrována na alternativní infrastrukturu.

Obnova: Po odeznění útoku je provedená obnova plné funkcionality služeb a detailní ověření provozuschopnosti tísňové linky.

4. Aktivita po incidentu: V závěrečné fázi je zpracována zpráva o incidentu a vyhodnocena účinnost použitých opatření. Identifikují se slabá místa v infrastruktuře a navrhuje se další kroky ke zvýšení odolnosti. Součástí je i revize krizové komunikace a aktualizace bezpečnostní dokumentace. Incident je zařazen do evidence a slouží jako případová studie pro školení zaměstnanců.

6.3 Modelový scénář: Fyzické napadení serverovny novým zaměstnancem s implementací ransomware na USB disku

Příprava útoku: Nově přijatý zaměstnanec HZS, který šel do této bezpečnostní složky s cílem narušit chod fungování HZS, dostal díky své funkci oprávnění vstupovat do zabezpečených místností, do kterých má přístup menší množství zaměstnanců. Tento zaměstnanec se již po půl roce vyzná v prostředí organizace a také ví, že servery HZS obsahují citlivé údaje o krizovém řízení, evakuačních plánech, komunikaci s IZS a dalších důležitých informací. Tyto informace získal z pozorování a vyptávání se svých kolegů. Do serverovny se tak dostal za pomoci svého identifikačního čipu. V době přípravy probíhá příprava infikovaného USB disku ransomwarem, který je navržený tak, aby zašifroval soubory v síti HZS a tím znemožnil jejich využití bez poskytnutí dešifrovacího klíče. Ransomware je často navržen tak, aby se po připojení do sítě rychle šířil do dalších systémů, a tím postihl co největší část infrastruktury.

Vniknutí do serverovny: Zaměstnanec využívá mezery v bezpečnostních opatřeních a vstupuje do serverovny bez povšimnutí. Tam připojí svůj USB disk k serveru nebo jinému síťově propojenému zařízení a spustí škodlivý ransomware, který se začne šířit do propojených IT systémů.

Infikování ransomwarem: Jakmile se ransomware aktivuje, začne šifrovat soubory v napadených systémech, a to včetně systémů operačního řízení HZS, komunikace

se složkami IZS a záznamů o zásazích. Do několika minut může být zasažena celá síť, včetně záloh, pokud nejsou odděleny. Po dokončení šifrování se na napadených systémech objeví zpráva s požadavkem o výkupném za dešifrování dat. Pokud HZS nemá aktuální zálohy, může se tak ocitnout v nepříjemné situaci, kdy data bude obtížné nebo nemožné obnovit.

Dopady incidentu: Mezi hlavní dopady patří: ztráta přístupu k IT systémům, nenávratná ztráta dat, finanční a provozní škody, porušení ochrany osobních údajů a také poškození reputace. Šifrování databází paralyzuje krizové řízení, a to může vést k nefunkčnosti komunikačních a operačních systémů. Pokud nejsou dostupné aktuální zálohy, mohou být důležité informace neobnovitelné, a tím dojde k ohrožení zásahů HZS. Náklady na obnovu systémů, forenzní analýzu a posílení bezpečnosti mohou být velké. Pokud ransomware postihne databáze obsahující osobní údaje občanů nebo zaměstnanců, může dojít k porušení nařízení GDPR.

Reakce na incident: Zde by došlo k izolování infikovaných serverů to by znamenalo okamžité odpojení serveru od sítě, aby se ransomware dále nešířil. Začalo by probíhat vyšetřování ze strany Policie ČR. Také by probíhala analýza ransomwaru kontaktováním IT bezpečnostním týmem, který by analyzovat kód ransomwaru a následně hledal možnosti dešifrování dat. Proběhla by kontrola záloh, pokud nějaké jsou, tak by proběhla jejich obnova a také analýza integrity dat. Pokud nejsou zálohy z nějakého důvodu dostupné, vedení HZS bude muset rozhodnout o dalším postupu, a to včetně možného vyjednávání s útočníkem. Platit výkupné se nedoporučuje.

6.3.1 What-if analýza – serverovna

Metoda What-if byla dále aplikována na scénář fyzického narušení serverovny (tabulka 5). Analýza zohledňuje jak lidský faktor, tak technické prvky fyzického zabezpečení a přístupu. Identifikace potenciálních situací a jejich možných důsledků slouží jako základ pro návrh bezpečnostních opatření zaměřených na minimalizaci následků případného fyzického útoku.

Tabulka 4 What-if Scénář serverovny.

Fáze útoku	Otázka "Co když..."	Dopady	Pravděp.	Opatření
Přístup do serverovny	Zaměstnanec má přístup o mimo pracovní dobu?	Vstup bez dozoru, vyšší riziko útoku	Střední	Zvýšený monitoring u nových zaměstnanců

Fáze útoku	Otázka "Co když..."	Dopady	Pravděp.	Opatření
Přístup do serverovny	Nikdo pravidelně nekontroluje čipové záznamy?	Neodhalený nestandardní pohyb	Střední	Dodržování vnitřních směrnic zaměstnanci, školení
Infikování ransomwarem	USB porty nejsou blokovány, zařízení lze připojit?	Šíření ransomwaru, šifrování dat, narušení provozu	Vysoká	Zakázání automatického spouštění USB disků, školení, detekce anomálií
Dopady incidentu	Zálohy dat jsou poškozené nebo nedostupné v době, kdy jsou potřeba po útoku?	Ztráta dat, narušení provozu, delší obnova, ohrožení zásahů.	Střední	Testování záloh, geograficky oddělené zálohy, šifrování
Reakce na incident	Reakce HZS na zjištěný fyzický průnik byla pomalá?	Rozšíření útoku, zničení dat, prodloužení doby obnovy provozu.	Vysoká	Okamžité hlášení, přesné postupy pro reakci
Vyšetřování incidentu	Kamery/logy nebyly dostupné?	Ztížení identifikace pachatele, pozdní reakce	Nízká	Pravidelná kontrola funkčnosti kamerového systému a přístupových logů, zabezpečení dat
Preventivní opatření	Jsou fyzická bezpečnostní opatření nedostatečná?	Neoprávněný vstup, možnost opakování útoků.	Střední	Posílení zámků, přístupových prvků, ochrana

(zdroj: vlastní)

6.3.2 Reakční plán – IRP

1. Příprava: V rámci přípravy by mělo být zajištěno fyzické zabezpečení serverovny např. přístup na základě čipových karet, kamerový dohled monitorování vstupů. Dále je nezbytné pravidelně vytvářet zálohy důležitých systémů a dat a uchovávat je odděleně. Musí být definované odpovědnosti jednotlivých externích úložištích. Musí být definované odpovědnosti jednotlivých zaměstnanců při reakce na incident a existovat dokument plán obnovy (DRP).

2. Detekce a analýza: Incident může být detekován fyzicky přítomným zaměstnancem nebo monitoringem bezpečnostních systémů (např. log vstupu, pohybové čidlo). Po napadení serveru ransomwarem se zpravidla objeví výzva k zaplacení výkupného. Prvním krokem je zajištění, jakým způsobem došlo k neoprávněnému přístupu, které systémy byly zasaženy a zda došlo k šíření malwaru do ostatních částí sítě.

3. Zvládání incidentu:

Zabránění šíření: Zasažené servery se okamžitě odpojí od vnitřní sítě přístup do serverovny je omezen pouze na incident response tým.

Odstranění hrozby: Je identifikován typ ransomwaru a vyhodnocena možnost jeho odstranění bez dešifrovacího klíče. Pokud je šíření potvrzeno, nasadí se specializovaný antivirový software a vyčistí se zasažené systémy.

Obnova: Pro obnovu dat a služeb se využijí poslední bezpečné zálohy. Po obnovení systémů je třeba provést důkladné testování a ověření integrity dat. V případě, že nebylo možné obnovit kompletní stav, zajišťuje se alespoň minimální funkčnost.

4. Závěrečná fáze: V závěrečné fázi je zpracována zpráva o incidentu a vyhodnocena účinnost použitých opatření. Identifikují se slabá místa v infrastruktuře a navrhuje se další kroky ke zvýšení odolnosti. Součástí je i revize krizové komunikace a aktualizace bezpečnostní dokumentace. Incident je zařazen do evidence a slouží jako případová studie pro školení zaměstnanců.

7 MODELOVÁNÍ JEDNOTLIVÝCH SCÉNÁŘŮ

Cílem této kapitoly je vizuálně znázornit průběh jednotlivých scénářů narušení informační bezpečnosti, které byly popsány v předchozí části práce. Modelování slouží k určitému zjednodušení a lepšímu pochopení jednotlivých kroků, rozhodovacích bodů a důsledků, které mohou nastat v závislosti na konkrétním chování aktérů.

Každý s uvedených scénářů v předchozí kapitole bude převeden do vývojového schématu, kde jsou vyznačeny důležité události a možné větvení v závislosti na tom, jestli dojde k následné akci (otevření e-mail, instalace softwaru, reakce na incident) Diagramy zároveň odhalují možná riziková místa v jednotlivých událostí a ukazují na to, jak důležité role hraje lidský faktor při vzniku i zvládnutí bezpečnostních incidentů. Proto tedy modelování nepřináší jen přehledný popis scénářů, ale také hlouběji podporuje analýzu dopadů a usnadňuje návrh preventivních nebo nápravných opatření

Softwarový nástroj

Visio je součástí produktové řady Microsoft office a díky tomu nabízí známé uživatelské rozhraní a integraci s dalšími aplikacemi (např. PowerPoint). Dále pak podporuje širokou škálu symbolů, šablon, tvarů pro různé účely – od IT infrastruktury, přes podnikové procesy až po technické výkresy.

Tabulka 5 Seznam použitých symbolů.

Symbol	Název	Význam
Ovál (terminator)	Začátek/ Konec procesu	Označuje vstupní nebo výstupní bod procesu (např. start, konec)
Obdélník (proces)	Proces/ činnost	Reprezentuje akci, činnost, krok nebo operaci
Kosočtverec	Rozhodnutí	Logický bod, kde se rozhoduje mezi více cestami (např. ANO/NE)
Úzký černý dlouhý obdélník	Forknode/joinnode	Rozdělení nebo sloučení více toků činností
Šipka	Směr toku	Udává směr postupu mezi jednotlivými prvky v diagramu

(zdroj: vlastní)

V oblasti kybernetické a informační bezpečnosti je Visio vhodné pro tvorbu vývojových diagramů bezpečnostních scénářů, procení mapy reakce na incidenty, vizualizaci toků informací a rolí jednotlivých aktérů. Díky intuitivnímu ovládání a možnosti přizpůsobit schémata konkrétnímu účelu je MS – Visio vhodným nástrojem pro modelování scénářů narušení informační bezpečnosti. Pro pochopení vývojového diagramu jsou v tabulce 7 popsány použité symboly, které byly při tvorbě vývojových diagramů použity.

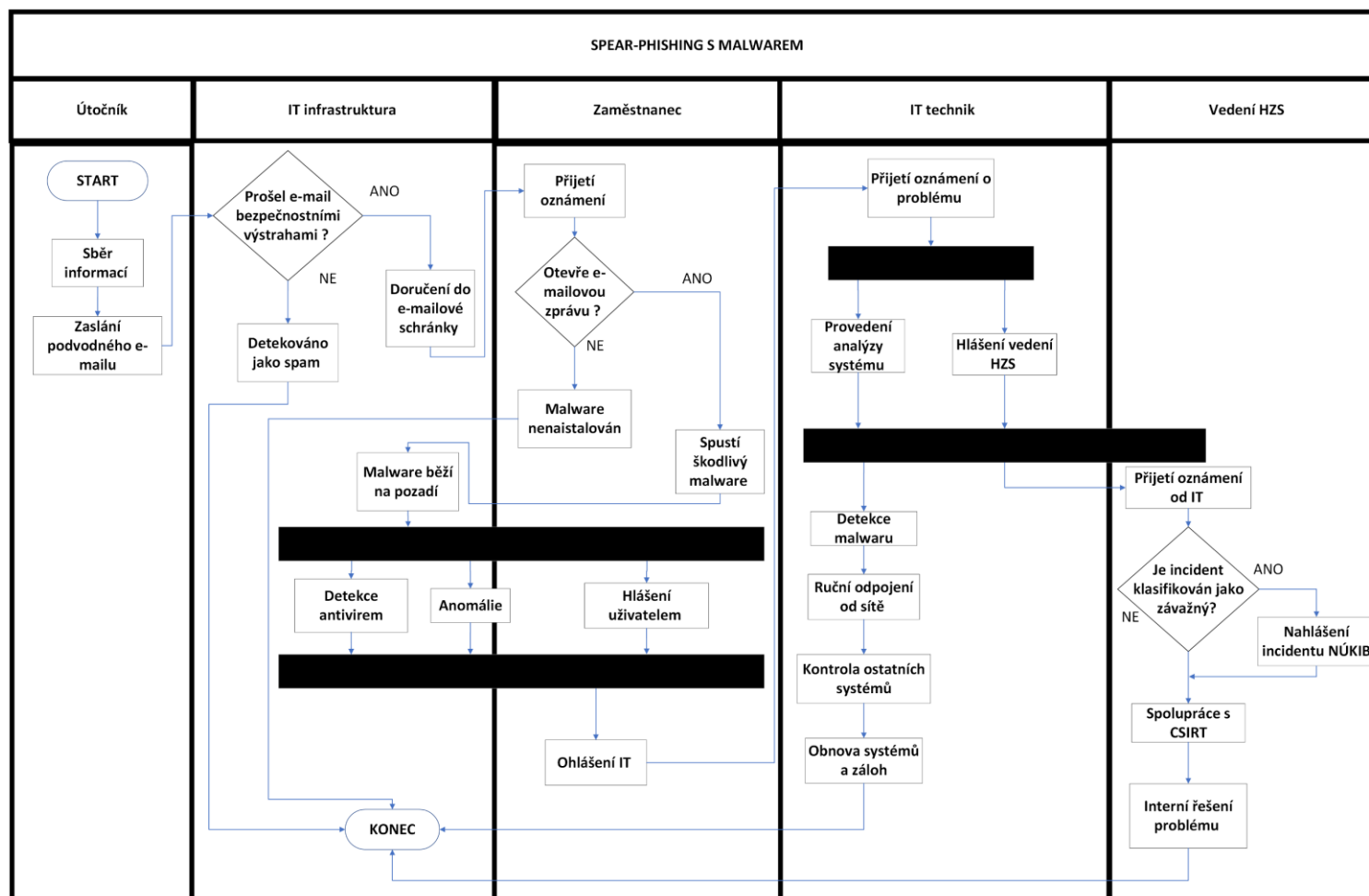
7.1 Model spear-phishingového útoku s malwarem

Model spear-phishingového útoku (viz obrázek 5) slouží nejen jako vizualizace incidentu, ale především jako nástroj pro identifikaci rizik a nedostatků v bezpečnostním prostředí jako nástroj pro identifikaci rizik a nedostatků v bezpečnostním prostředí organizace. Jeho důležitým přínosem je možnost zpětného pohledu na celý průběh útoku z různých úhlů – technického, organizačního i lidského. Z modelu je patrné, že rozhodovací rolu v celém scénáři sehrává zaměstnanec, který na základě nedostatečného školení nebo momentální nepozornosti spouští škodlivý kód. Zároveň ukazuje, jak rychle se po tomto bodě přenáší odpovědnost na technický personál, to naznačuje o silnou závislost na připravenosti IT týmu.

Zajímavým prvkem je také načasování jednotlivých kroků. Model poukazuje na to, že mezi aktivací malwaru a reakcí IT oddělení může dojít k určité prodlevě, která je pro útočníka klíčová. Právě tato část může organizaci sloužit jako výchozí bod pro zkrácení reakčního času – například pomocí automatizované detekce anomálií, lepšího logování nebo nastavení bezpečnostních pravidel přímo v e-mailovém systému.

Vizuálně je zřetelné, jak izolovaně některé kroky působí – zejména na straně zaměstnance a IT technika. To ukazuje na potřebu efektivnějších interních komunikačních kanálů a předem nastavených postupů, které by zaměstnanci pomohly správně vyhodnotit podezřelé situace dříve, než dojde k infekci.

Tento model lze také využít při revizi bezpečnostní politiky nebo při návrhu školení. Díky vizualizaci se s ním snadno pracuje i při simulacích incidentu a testování připravenosti jednotlivých týmů. Umožňuje vést diskusi nejen o tom, co se stalo, ale i o tom, co se mělo stát jinak – kde byla příležitost útok zastavit.



Obrázek 6 Modelování scénáře Spear-phishing.

(zdroj: vlastní)

7.2 Model DDoS útoku na tísňovou linku HZS

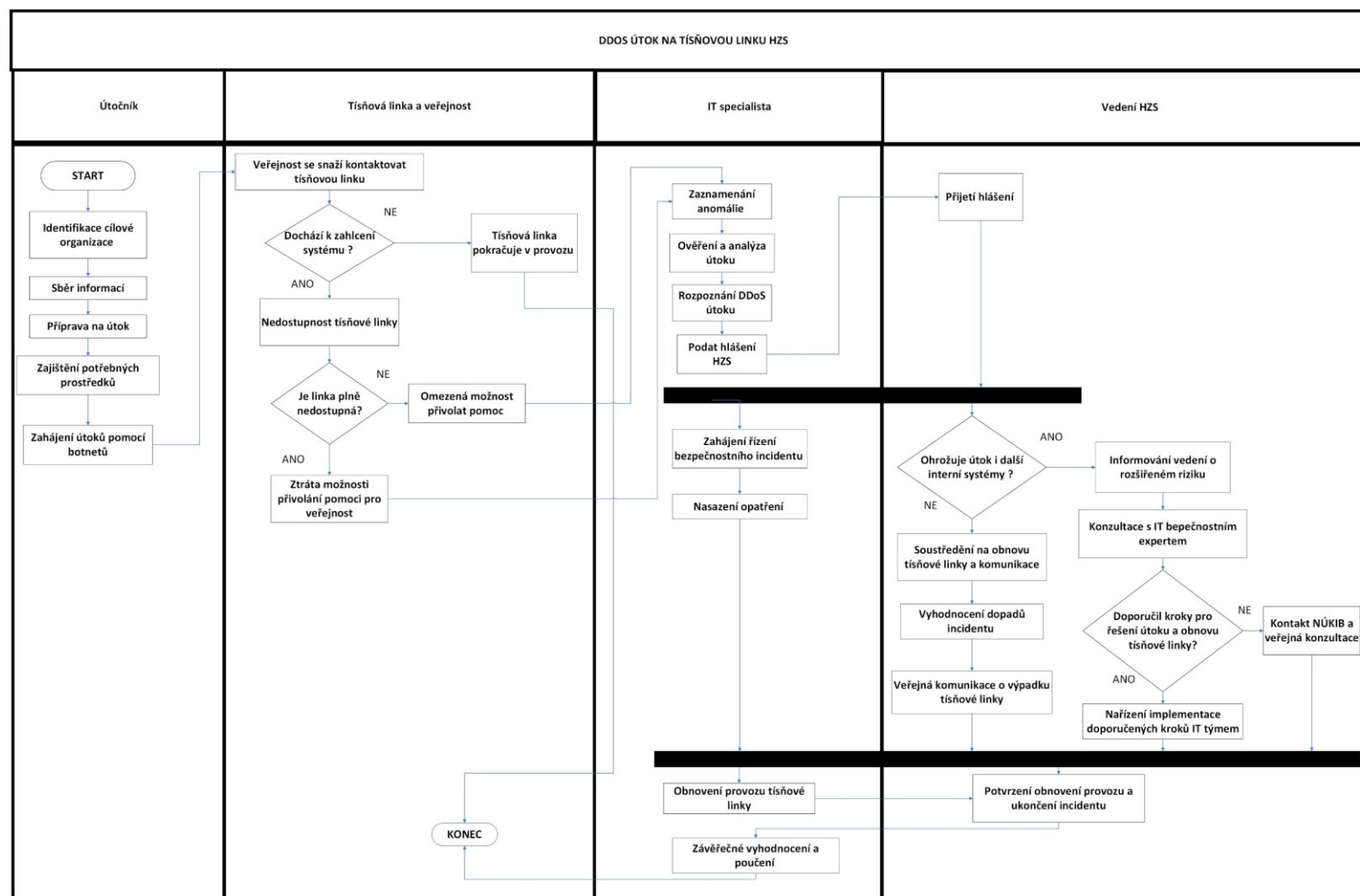
Diagram DDoS útoku na tísňovou linku HZS (viz obrázek 6) nabízí pohled na to jak, může být ohrožena jedna z nejdůležitějších služeb organizace – možnost veřejnosti přivolat pomoc. Na rozdíl od scénářů, které se zaměřují na zcizení nebo poškození dat, zde útočník nesleduje přímý zisk, ale záměrně narušuje dostupnost, čímž ochromuje schopnost organizace plnit svou základní funkci. To z něj činí mimořádně závažnou hrozbu, jejíž dopady mohou být okamžité a přímo ohrožující životy.

Z modelu je zřejmé, že útok zasahuje nejen technickou infrastrukturu, ale přímo i veřejnost. Swimlane schéma tak vhodně odděluje tři důležité roviny – reakci veřejnosti, technické řešení incidentu a rozhodování na úrovni vedení. Umožňuje sledovat, jak se informace o výpadku šíří napříč strukturou HZS a jak na ni jednotlivé úrovně reagují. Výrazným prvkem je včasné rozpoznání útoku IT specialistou a jeho schopnost spustit bezpečnostní postupy, a to je důležité pro minimalizaci škod.

Současně je vidět, že samotné obnovení provozu linky nestačí – Model upozorňuje i na potřebu vyhodnotit dopad incidentu a informovat veřejnost o jeho průběhu. To ukazuje, že zvládnutí útoku zahrnuje nejen technická opatření, ale i efektivní krizovou komunikaci. Vedení HZS zde hraje také zásadní roli, protože umožňuje posoudit rizika a zapojit externí aktéry, jako je NÚKIB nebo IT bezpečnostní experti.

Model tak může sloužit nejen jako popis scénáře, ale i jako podklad pro plánování opatření v rámci kontinuity provozu (BCM). Pomáhá identifikovat body, kde je možné zlepšit připravenost například v oblasti detekce přesměrování hovorů nebo informování veřejnosti. Zároveň vizualizuje, jak důležité je mít jasně stanovené kompetence a schopnost rozhodovat i pod tlakem.

V praxi by mohl být model využit jako součást interních cvičení nebo jako nástroj pro přehodnocení krizových plánů. Z modelu je patrné, že i dobře připravený systém může selhat, pokud není současně zajištěna funkční spolupráce mezi technickým týmem a vedením organizace. Právě schopnost reagovat a správně vyhodnotit situaci a rozhodnout o dalších krocích je tím, co určuje, zda bude dopad útoku pouze technický, nebo i společenský.



Obrázek 7 Modelování scénáře DDoS útoku na tísňovou linku HZS.

(zdroj: vlastní)

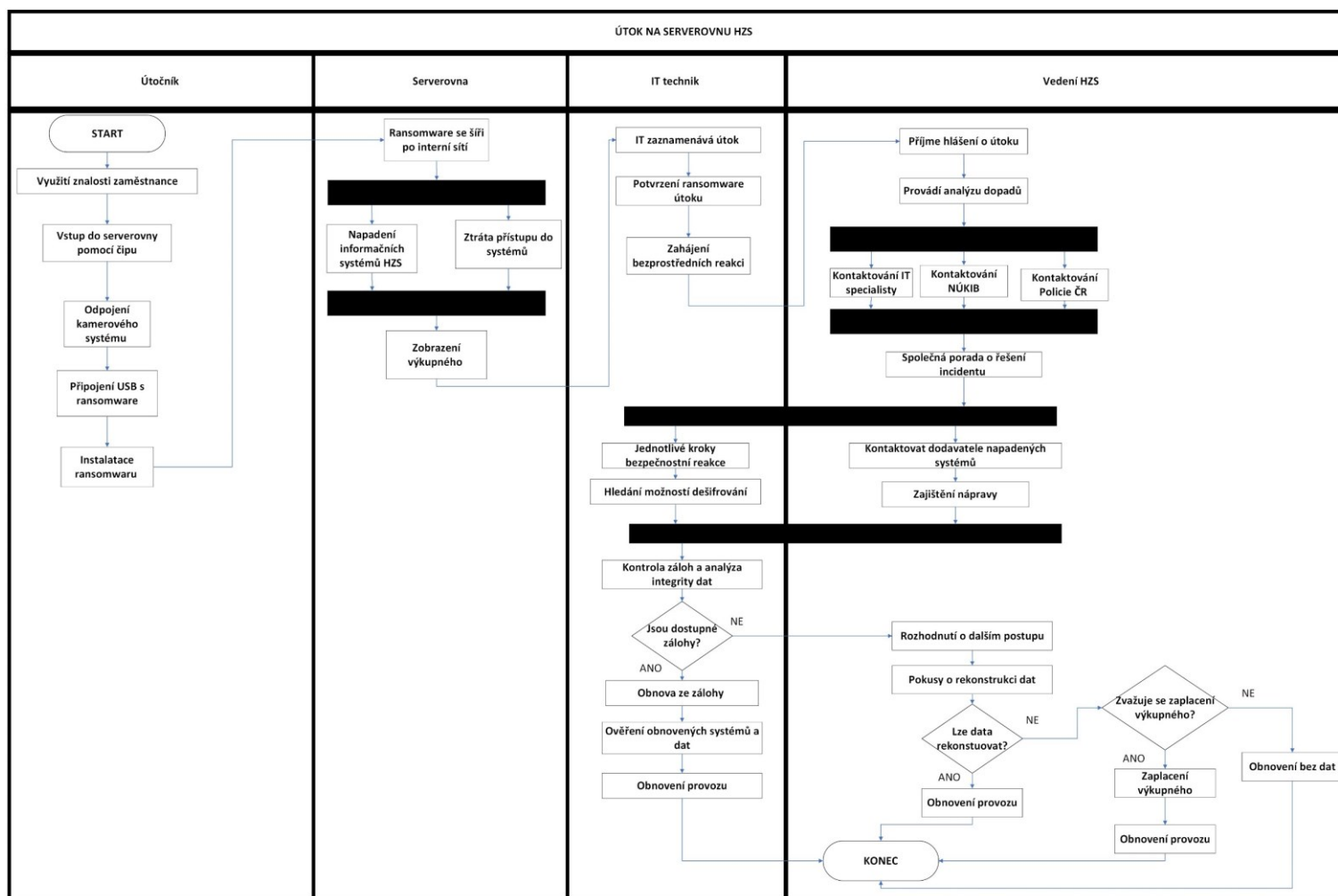
7.3 Model fyzického napadení serverovny novým zaměstnancem HZS s implementací ransomware na USB disku

Třetí scénář se zaměřuje na méně častý, ale o to závažnější incident – fyzický průnik do serverovny HZS spojený s instalací škodlivého softwaru typu ransomware. Swimlane diagram níže zobrazuje sled událostí od okamžiku, kdy útočník vstoupí do budovy se znalostí interních zabezpečení až po samotnou infiltraci serverového systému. Na rozdíl od předchozích scénářů, tento model zdůrazňuje kombinaci fyzické a digitální hrozby, čímž ukazuje, jak důležité je zabezpečení nejen kybernetické, ale také prostorové. V diagramu jsou opět využity plavecké dráhy, které reprezentují aktivity čtyř hlavních účastníků – útočník, serverovny jako prostředí útoku IT technika a vedení HZS. Postupně dochází k napadení systémů, ztrátě přístupu, analýze incidentu a volbě vhodné reakce – ať už ztrátě přístupu, analýze incidentu a volbě vhodné reakce typu obnovením ze záloh, nebo v krajním případě vyjednávání s útočníkem.

V modelu je v procesu „zahájení bezpečnostních reakcí“ shrnuto několik důležitých činností, které se při tomto procesu musí provést. Jedná se o odpojení zařízení na síťové úrovni, pokud to není možné, tak je nutné ji vypnout. Dále se musí odpojit komunikace do veřejné sítě, zjistit rozsah napadení a izolovat infikované systémy, dokumentovat zjištění, pořídit bitovou kopii zasažených systémů a zařízení, shromáždit relevantní logy, vzorky malwaru, indikátory kompromitace, zajistit uchování dočasných důkazů, požádat o logy z firewallu od poskytovatele internetu, analýza ransomwaru. To vše provádí IT technik.

V případě, že nelze provést obnovu dat ze záloh a ani rekonstrukce dat není možná, může být přistoupeno k obnovení provozu bez historických dat. Tento krok se realizuje především v situacích, kdy je důležitější zachovat funkčnost základních služeb než úplnost dat, a další data jsou získávána postupně v rámci běžného provozu. Podle doporučení NÚKIB se v žádném případě nedoporučuje platit výkupné.

Scénář je typický svou strukturou a důsledky, které mohou ovlivnit nejen běžný chod organizace, ale i schopnost zasahovat v krizových situacích. Vizuální znázornění odhaluje potenciální slabiny v kontrole fyzického přístupu, nedostatečným oddělením sítí a absencí pravidelného testování záloh. Je zde i zásadní součinnost mezi technickým personálem a vedením při zvládání podobných bezpečnostních incidentů.



Obrázek 8 Modelování scénáře útoku na serverovnu HZS.

(zdroj: vlastní)

8 VYHODNOCENÍ A ANALÝZA VÝSLEDKŮ MODELOVÁNÍ

Na základě vytvořených scénářů narušení informační bezpečnosti a jejich analýza pomocí metody What-if a modelování pomocí nástroje v prostředí Microsoft Visio byla provedena podrobná analýza výsledků. Tato analýza slouží k identifikaci nejslabších míst v informační infrastruktuře HZS ČR, posouzení opakujících se vzorců chování a formulaci návrhů ke zlepšení.

8.1 Identifikované slabiny napříč scénáři

Z modelování jednotlivých scénářů narušení informační bezpečnosti vyplynulo několik opakujících se slabin, které zvyšují celkovou zranitelnosti subjektu ochrany obyvatelstva:

- Lidský faktor: Většina útoků byla umožněna či usnadněna lidskou chybou, nedostatečnou informovaností nebo nízkou úrovní kybernetického vzdělávání zaměstnanců. Příkladem je spear-phishing, který spoléhá na důvěřivost oběti. Lidská nepozornost rovněž sehrála roli při neohlášení podezřelé aktivity ve fyzicky zabezpečené oblasti.
- Nedostatečná technická opatření: Modelování odhalilo slabiny v infrastruktuře, především v oblasti kontroly přístupových práv a absence bezpečnostních prvků (např. detekce opakovaných pokusů o přihlášení). V případě fyzického útoku se ukázalo, že nedostatečná kontrola přístupu umožňuje potenciálně škodlivé chování i ze strany interních osob.
- Chybějící pokročilé obranné mechanismy: DDoS scénář prokázal, že systémy HZS nemusí být plně připraveny na masivní zahlcení infrastruktury. Ačkoliv nejde o útok, který směřuje k odcizení dat, jeho dopady mohou být výrazně ohrožující pro běžný provoz i krizové situace, zejména v případě znepřístupnění tísňové linky.
- Reakce na incident a forenzní šetření: V několika scénářích bylo patrné, že reakce na incident může být zpomalena nebo může být neúplná, a to jak z hlediska detekce útoku, tak i jeho šíření či následného vyhodnocení. Zvláště v případech, kde chybí kontinuální monitoring a detailní logování, je komplikované zpětně vyhodnotit rozsah narušení a přijmout adekvátní opatření.

8.2 Shrnutí výsledků v matici rizik

Každý ze scénářů byl analyzován z hlediska jeho pravděpodobnosti výskytu a závažnosti dopadu na činnost organizace. K tomuto účelu byla využita tzv. matice rizik, která umožňuje graficky a přehledně vyjádřit úroveň jednotlivých rizik na základě jejich rizikového skóre, které vzniklo kombinací hodnot pravděpodobnosti a dopadu. Matice rizik zároveň slouží jako rozhodovací nástroj pro stanovení priorit v oblasti bezpečnostních opatření. Incidenty, které se nacházejí v červené nebo oranžové oblasti matice, představují hrozby s vysokým nebo středním rizikem a měly by být řešeny přednostně. Naproti tomu scénáře nacházející se v zelené barvě představují nižší rizika, u nichž lze zvažovat jiný režim řízení.

Tabulka 6 Vyhodnocení scénářů.

Scénář	Pravděpodobnost	Dopad	Riziko	Hodnocení
Spear-phishing	Střední (3)	Kritický (5)	15	Vysoké riziko
DDoS útok na tísňovou linku	Vysoká (4)	Střední (3)	12	Střední až vysoké riziko
Fyzický útok na serverovnu	Nízká (2)	Kritický (5)	10	Nízké riziko, ale kritický dopad

(zdroj: vlastní)

Tabulka 8 poskytuje vstupní informace pro vytvoření hodnocení matice rizik. U každého z vybraných scénářů narušení informační bezpečnosti byla stanovena pravděpodobnost výskytu a závažnost dopadu na činnost organizace. Tyto dvě veličiny byly následně vynásobeny a výsledkem je ohodnocení rizika. Pravděpodobnost a dopad byly přiřazeny na základě kombinace několika faktorů – zejména aktuálních bezpečnostních trendů, statistik reálných incidentů (např. hlášení NÚKIB) a modelovaných scénářů. Hodnocení také zohledňuje typ útoku, obtížnost jeho provedení a potenciální následky pro fungování HZS ČR.

V případě spear-phishingového útoku byla pravděpodobnost označená jako střední. Jedná se o častou techniku útočníků, jejíž úspěšnost závisí na míře školení zaměstnanců, použití bezpečnostních filtrů a celkové odolnosti organizace vůči sociálnímu inženýrství. Dopad byl vyhodnocen jako kritický, protože úspěšné proniknutí do systému může vést k úniku dat, instalaci škodlivého kódu a dalšímu šíření malwaru. Výsledné riziko 15 odpovídá podle kategorie vysokému riziku.

Pravděpodobnost výskytu útoku typu DDoS byla určena jako vysoká, protože útoky na dostupnost služeb jsou poměrně časté a mohou být realizovány i bez větších technických znalostí. Útočníci mohou využít botnety či pronajaté služby. Dopad byl stanoven jako střední. Přestože nedochází k úniku dat, znepřístupnění tísňové linky může mít závažné následky. Výsledné riziko vyšlo 12, a proto to odpovídá střednímu až vysokému riziku.

Pravděpodobnost fyzického útoku na serverovnu byla označena jako nízká. Přístup do serverovny je obvykle omezen, a fyzické zabezpečení bývá na vyšší úrovni. Na druhou stranu dopad byl vyhodnocen jako kritický. Fyzické poškození serveru nebo nasazení malwaru může způsobit rozsáhlé škody a vyřadit důležité systémy. Výsledné riziko je sice nízké, ale je důležité dodat, že i když se jedná o nízké riziko, tak má kritický dopad.

Tabulka 7 Matice rizik.

Důsledek	Pravděpodobnost				
	1	2	3	4	5
1	1	2	3	4	5
2	2	4	6	8	10
3	3	6	9	12	15
4	4	8	12	16	20
5	5	10	15	20	25

(zdroj: Jirsák, © 2017-2025)

V tabulce 9 je zobrazena matice rizik, která má dvě hodnotící škály. Pravděpodobnost se hodnotí od 1 do 5, slovně popsáno jako: vzácné, nepravděpodobné, možné, pravděpodobné, téměř jisté. Důsledky jsou také hodnoceny od bodové škály od 1 do 5, kdy to jde od nejnižší hodnoty v pořadí: zanedbatelný, menší, mírný, hlavní, katastrofální.

Riziko je hodnoceno:

- Nízké: hodnota 1 až 3
- Střední: hodnota 4 až 6
- Vysoké: hodnota 8 až 12
- Extrémní: hodnota 15 až 25 (Jirsák, © 2017–2025).

V následující tabulce je znázornění umístění jednotlivých scénářů narušení informační bezpečnosti v matici rizik na základě jejich vyhodnocení. Scénář 1 představuje spear-phishing s nasazením malwaru, scénář 2 odpovídá DDoS útoku na tísňovou linku a scénář 3 se zabývá fyzickým napadením serverovny spojeným s nasazením ransomwaru.

Tabulka 8 Zasazení vyhodnocení scénářů do matice rizik.

Důsledek	Pravděpodobnost				
	1	2	3	4	5
1	1	2	3	4	5
2	2	4	6	8	10
3	3	6	9	12 – scénář 2	15
4	4	8		16	20
5	5	10 – Scénář 3	15 – Scénář 1	20	25

(zdroj: vlastní)

Z grafické podoby matice vyplynulo, že největší hrozbou z hlediska kombinace dopadu a pravděpodobnosti je spear-phishing. Ačkoliv má spear-phishing nižší pravděpodobnost, je těžko detekovatelný a jeho dopad je extrémně vysoký, zejména při manipulaci s krizovými plány a daty. U neúmyslného úniku dat jsou lidské chyby časté a často se obtížně odhadují. Důsledky mohou zahrnovat ztrátu důvěry, porušení GDPR a narušení koordinace zásahů.

9 NÁVRHY OPATŘENÍ KE ZMÍRNĚNÍ IDENTIFIKOVANÝCH RIZIK

Na základě analýzy modelových scénářů narušení informační bezpečnosti u Hasičského záchranného sboru České republiky, jejich následného modelování a vyhodnocení pomocí matice rizik, byly identifikovány opakující se slabiny, které zvyšují zranitelnost organizace. Mezi tyto slabiny lze zařadit zejména lidský faktor, nedostatečně ošetřená správa přístupových práv, zranitelnost v oblasti technických a fyzických opatření a celková připravenost na kybernetické útoky. Navržená opatření vycházejí z odborných poznatků, doporučení NÚKIB i reálného rozhovoru s příslušníkem HZS, který přinesl důležitý vhled do vnitřního fungování a nastavení bezpečnostních opatření v praxi. Díky kombinaci teoretických poznatků a praktických informací byly navrženy opatření, které se zaměřují na konkrétní slabá místa a zároveň zohledňuje reálné provozní podmínky a omezení.

Cílem těchto opatření je komplexně posílit informační bezpečnosti subjektu. Návrhy se dotýkají technických, organizačních i personálních aspektů zabezpečení a slouží jako základ pro preventivní, detekční i nápravná opatření, která mohou pomoci zmírnit dopady případných bezpečnostních incidentů a zvýšit celkovou odolnost organizace vůči hrozbám.

9.1 Prevence spear-phishingového útoku

Spear-phishingové útoky jsou cílené útoky na konkrétní zaměstnance s cílem získat přihlašovací údaje nebo naistalovat malware do systémů. Tento útok závisí na důvěřivosti oběti, která je přitahována falešnými e-maily nebo jinými podvodnými komunikacemi.

Mezi opatření, které mohou pomoci zmírnit riziko tohoto typu útoku patří:

- pokročilá ochrana e-mailů,
- implementace vícefaktorové autentizace,
- pravidelná školení zaměstnanců,
- simulovaný phishingové scénáře,
- monitorování a záznamy přístupů,
- bezpečnostní testy.

Nasazení antispamových a antiphishingových filtrů pro detekci podezřelých e-mailů. Tyto filtry by měly kontrolovat nejen odesílatele, ale také obsah e-mailu, včetně příloh a odkazů. E-maily obsahující podezřelé odkazy nebo přílohy by měly být automaticky doručovány do karantény, kde mohou být ověřeny dříve, než budou doručeny do doručené pošty.

Pro všechny systémy by měla být povinná vícefaktorová autentizace. I když útočník získá přihlašovací údaje, nebude schopen se přihlásit bez druhého faktoru, jako je mobilní aplikace, SMS kód nebo biometrické ověření.

Zaměstnanci by měli být pravidelně školeni v oblasti identifikace phishingových e-mailů a bezpečných návyků při práci s e-mailem. Měli by být schopni rozpoznat podezřelé zprávy, včetně těch, které obsahují odkazy na neznámé webové stránky, nebo přílohy, které se tváří jako běžné dokumenty.

Provádění pravidelných simulovaných phishingových útoků, které pomohou zaměstnancům rozpoznat rizikové e-maily a správně na ně reagovat, aniž by se stali obětí skutečného útoku.

Všechna přihlášení do systémů by měla být monitorována. Anomálie, jako je časté přihlašování z neznámých IP adres nebo mimo pracovní dobu, by měly být automaticky detekovány a prošetřeny.

Pravidelně prováděné penetrační testy a bezpečnostní audity by měly ověřit, zda jsou systémy účinně chráněny proti phishingovým útokům a zda není možné obejít bezpečnostní opatření.

9.2 Opatření proti DDoS útoku na tísňovou linku

DDoS útoky jsou zaměřeny na zahlcení cílové infrastruktury, což může vést k dočasné nebo trvalé nedostupnosti služeb. V případě tísňové linky HZS by měl být tento typ útoku považován za závažný, protože může ohrozit schopnost reagovat na krizové situace.

Opatření, která pomáhají minimalizovat riziko a důsledky DDoS útoků, jsou:

- nasazení anti-DDoS ochrany,
- redundance a přesměrování provozu,
- technické testování záložních systémů,
- monitoring síťového provozu a komunikační plán.

Implementace technologií, které automaticky detekují a blokují nadměrný provoz směřující na tísňovou linku. Může to zahrnovat služby poskytované telekomunikačními operátory, které dokážou filtrovat podezřelý provoz ještě před jeho vstupem do vnitřní infrastruktury.

Zajištění redundance pro důležité systémy, včetně přesměrování provozu na záložní servery nebo jiné geograficky umístěné dispečinky, které mohou převzít komunikaci v případě, že hlavní systémy jsou zahlceny.

Pravidelně testovat záložní komunikační kanály (např. mobilní technologie, rádiové spojení) pro případ, že by došlo k výpadku primárních služeb. Tato řešení by měla být plně funkční v reálných krizových situacích.

Průběžné monitorování síťového provozu na detekci anomálií, které by mohly naznačovat probíhající DDoS útok. Jakmile jsou detekovány známky útoku, měly by být okamžitě aktivovány ochranné mechanismy a informování všichni důležití aktéři.

Vytvoření krizového plánu pro informování veřejnosti v případě, že dojde k výpadku tísňové linky. Veřejnost by měla být informována prostřednictvím jiných komunikačních kanálů, jako jsou sociální sítě, SMS zprávy nebo veřejné oznámení.

9.3 Opatření proti fyzickému napadení serverovny a vnitřnímu aktérovi

Scénář fyzického napadení IT infrastruktury novým zaměstnancem HZS upozorňuje na význam rizik spojených s tzv. vnitřním aktérem. V tomto případě se jedná o osobu, která se po nástupu do organizace v průběhu několika měsíců důkladně seznámila s interním prostředím, procesy i fyzickým uspořádáním pracoviště. Díky své pracovní pozici a přiděleným oprávněním získal přístup do prostor, kde se nachází citlivá infrastruktura, jako jsou servery nebo komunikační uzly. Po určité době pak využil této důvěry k útoku.

K prevenci podobných incidentů je vhodné zavést opatření, kterými jsou:

- zpřísnění kontroly fyzického přístupu do serveroven,
- zavedení vícefaktorové autentizace,
- monitoring a evidence fyzického vstupu,
- omezení možnosti připojení externích zařízení.

Vstup do těchto prostor by měl být umožněn pouze důvěryhodným osobám s dlouhodobou praxí a ověřenou bezpečnostní spolehlivostí. Vhodné je zavedení principu „čtyř očí“, tedy pravidla, že do prostoru nesmí vstupovat jeden člověk bez doprovodu druhého.

Přístup ke kritické infrastruktuře by neměl být umožněn pouze pomocí jednoho faktoru (např. čipu), ale měl by být kombinován s dalším ověřovacím prvkem, jak už bylo zmíněné v opatření předešlém.

Přístup do serveroven by měl být nepřetržitě monitorován kamerovým systémem a zaznamenáván do elektronické knihy vstupů, která umožní zpětné dohledání všech pohybů osob. Zároveň je nutné zakázat veškeré neschválené externí vstupy do systémů, zejména připojení USB zařízení. V operačním systému je možné nastavit politiky, které znemožní spouštění neautorizovaných přenosných médií. Je to možné doplnit ještě o tzv. softwarové hlídače, které zaznamenávají jakýkoliv pokus o narušení. Nezbytnou součástí ochrany před následky ransomwarového útoku je existence záloh, které jsou pravidelně vytvářeny, testovány a uchovávány na fyzicky odděleném úložišti. Kromě samotného zálohování je důležité také testovat obnovu dat. Tím je myšleno simulovat danou situaci, při kterém bude potřeba obnovit systém ze zálohy.

ZÁVĚR

Hlavním cílem této diplomové práce bylo vytvořit modelové scénáře narušení informační bezpečnosti v prostředí Hasičského záchranného sboru České republiky a na jejich základě navrhnout odpovídající bezpečnostní opatření. Vzhledem k tomu, že nebylo možné pracovat s reálnými interními údaji HZS, byly scénáře zpracovány jako hypotetické, vycházející z obecných bezpečnostních rámců, legislativy a známých kybernetických hrozeb.

Teoretická část se věnovala základnímu vymezení informační bezpečnosti, přehledu legislativy a specifikům, která se týkají subjektů ochrany obyvatelstva. V praktické části pak byly zpracovány konkrétní příklady incidentů, které by mohly v reálném světě nastat – od spear-phishingu, přes DDoS útok, až po fyzické ohrožení serverovny. Každý scénář byl znázorněn vývojovým diagramem, zhodnocen z hlediska rizikovosti a doplněn o návrh opatření, která by mohla snížit pravděpodobnost útoku nebo jeho dopady.

Jedná se o modelové situace, ukazuje se, že podobné hrozby nelze podcenit ani ve veřejném sektoru. Organizace, které zajišťují ochranu obyvatelstva, by měly počítat s tím, že informační systémy jsou dnes nedílnou součástí jejich činnosti a jejich například výpadek může mít vážné následky. Právě proto je důležité věnovat pozornost prevenci, vzdělání pracovníků a neustálému posuzování možných rizik.

Zpracování této práce ukázalo, že i bez přístupu k interním datům lze vytvořit užitečný rámec pro uvažování nad bezpečnostními hrozbami, kterým mohou čelit subjekty veřejné správy. Využití modelových scénářů se ukázalo jako vhodným způsob, jak strukturovaně popsat možné situace a přemýšlet nad tím, jaké dopady by mohly mít na provoz organizace. Zároveň tato práce upozorňuje na to, že informační bezpečnostní není jen záležitostí IT oddělení, ale celkové připravenosti organizace, a že i zdánlivě nepravděpodobné scénáře mohou mít v praxi velmi reálné následky.

Práce může přispět jako podklad pro další úvahy o tom, jak zvyšovat úroveň informační bezpečnosti veřejných institucí. Do budoucna by bylo vhodné navázat například hlubší analýzu skutečného stavu zabezpečení nebo spoluprací s konkrétní organizací, která by umožnila detailnější pohled do praxe. Doufám, že navržené postupy a analýzy mohou sloužit jako inspirace i pro další subjekty, které se snaží svou bezpečnost zlepšit nebo o ní alespoň začít seriózně uvažovat.

SEZNAM POUŽITÉ LITERATURY

A. ANDERSON SR., Anthonio, 2024. Understanding the Difference Between Antivirus and EDR Software Final - revised. Online. *Understanding the Difference Between Antivirus and EDR Software Final - revised*. Roč. 2024, č. 1, s. 4. Dostupné z: https://www.researchgate.net/publication/382681483_Understanding_the_Difference_Between_Antivirus_and_EDR_Software_Final_-_revised#fullTextFileContent. [cit. 2025-03-08].

ANAKAN S.R.O, © 2025. *Charakteristika KISKAN*. Online. ANAKAN s.r.o. Dostupné z: <https://anakan.cz/kiskan>. [cit. 2025-02-17].

COMMUNICATION TEAM, 2024. *Differences between computer security, information security and cybersecurity*. Online. Telefonica: leading telecommunications company. Dostupné z: <https://www.telefonica.com/en/communication-room/blog/differences-between-computer-security-information-security-cybersecurity/>. [cit. 2025-03-09].

CORNISH, Paul. *The Oxford Handbook of Cyber Security*. United Kingdom: Oxford University Press, 2021. ISBN 978-0-19-880068-2.

CRELIN, Joy, 2024. *Principles of Cybersecurity*. Salem Press. ISBN 978-1-63700-750-1.

ČESKO. MINISTERSTVO VNITRA – GRŮ HZS ČR, 2020. *Koncepce ochrany obyvatelstva do roku 2025 s výhledem do roku 2030*. Praha: Ministerstvo vnitra České republiky. Dostupné z: https://www.dataplan.info/img_upload/7bdb1584e3b8a53d337518d988763f8d/koncepce-oob-2025-2030.pdf. [cit. 2025-02-17].

ČESKO, 2014. Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: *Zákony pro lidi*. Dostupné také z: <http://www.zakonyprolidi.cz/cs/2014-181>. [cit. 2025-01-28].

ČESKO, 2008. Zákon č. 273/2008 Sb., o Policii České republiky. In: *Zákony pro lidi*. Dostupné také z: <https://www.zakonyprolidi.cz/cs/2008-273#cast1>. [cit. 2025-01-28].

ČESKO, 2011. Zákon č. 374/2011 Sb., o zdravotnické záchranné službě. In: *Zákony pro lidi*. Dostupné také z: <https://www.zakonyprolidi.cz/cs/2011-374>. [cit. 2025-01-28].

ČESKO, 2009. Zákon č. 40/2009 Sb., trestní zákoník. In: *Zákony pro lidi*. Dostupné také z: <https://www.zakonyprolidi.cz/cs/2009-40>. [cit. 2025-01-28].

ČESKO, 2005. Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. In: *Zákony pro lidi*. Dostupné také z: <https://www.zakonyprolidi.cz/cs/2005-412>. [cit. 2025-01-28].

ČESKO, 2019. Zákon č. 110/2019 Sb., o zpracování osobních údajů. In: *Zákony pro lidi*. Dostupné také z <https://www.zakonyprolidi.cz/cs/2019-110>. [cit. 2025-01-28].

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

DUSHAJ, Tom, © 2020. *THE COMPLETE GUIDE TO CYBER ATTACKS*. United States: Epic Media Publishing. ISBN 979-8565596854.

DYER, James, 2023. *What is a QR phishing ('quishing') attack?* Online. Egress Intelligent Email Security: Anti-phishing, data Loss Prevention and Encryption. Dostupné z: <https://www.egress.com/blog/phishing/what-is-a-quishing-attack#:~:text=These%20attacks%20use%20a%20QR%20code%20to%20lead,best%20practices%20for%20avoiding%20falling%20victim%20to%20them..> [cit. 2025-03-16].

Evropská Unie. *Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*, 2016. *Zákony pro lidi*. Dostupné z: <https://www.zakonyprolidi.cz/pravoou/dokument?celex=32016R0679>. [cit. 2025-01-28].

FENNELLY, Lawrence J., c2013. *Effective physical security*. 4th ed. Amsterdam: Elsevier Butterworth-Heinemann. ISBN 978-0-12-415892-4.

HONEK, Bohumil, 2025. *AGENTURA KOMUNIKAČNÍCH A INFORMAČNÍCH SYSTÉMŮ*. Online. Armáda ČR. Dostupné z: https://acr.mo.gov.cz/struktura/generalni/zn_ns/skis/fis/agentura-komunikacnich-a-informacnich-systemu-233431/. [cit. 2025-02-17].

HZS ČR, © 2025a. *Oddělení komunikačních a informačních systémů*. Online. HZS Jihomoravského kraje – HZS ČR. Dostupné z: <https://hzscr.gov.cz/clanek/oddeleni-komunikacnich-a-informacnich-systemu.aspx?q=Y2hudW09Mw%3d%3d>. [cit. 2025-02-18].

HZS ČR, © 2025b. *Subjekty kritické infrastruktury*. Online. HZS Olomouckého kraje. Dostupné z: <https://hzscr.gov.cz/clanek/subjekty-kriticke-infrastruktury.aspx>. [cit. 2025-02-18].

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2018. ISO/IEC 27000:2018, *Family – Information security management*. Geneva. Dostupné z: <https://www.iso.org/standard/iso-iec-27000-family>. [cit. 2025-02-17].

JIRSÁK, Milan, © 2017–2025. *Riziko*. Online. In: *Stručně – Zdravě*. Dostupné z: <https://www.strucne-zdrave.cz/riziko/>. [cit. 2025-04-04].

JOUINI, Mouna; RABAI, Latifa Ben Arfa a AISSA, Anis Ben, 2014. Classification of Security Threats in Information Systems. Online. *Procedia Computer Science*. Roč. 32, s. 489-496. ISSN 18770509. Dostupné z: <https://doi.org/10.1016/j.procs.2014.05.452>. [cit. 2025-02-18].

KOLOUCH, Jan a BAŠTA, Pavel. *CyberSecurity*. CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2019. ISBN 978-80-88168-31-7. Dostupné také z: <https://knihy.nic.cz/#cybersecurity>.

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

KYRIAZOGLU, John, 2024. *Information Security Incident and Data Breach Management*. APress Media, LLC, part of Springer Nature. ISBN 979-8-8688-0869-2.

MA, Xiaofen, 2022. IS professionals' information security behaviors in Chinese IT organizations for information security protection. Online. *Information Processing and Management*. Roč. 59, č. 1, s. 14. ISSN 03064573. Dostupné z: <https://doi.org/10.1016/j.ipm.2021.102744>. [cit. 2025-02-18].

MAGISTRÁT HMP, © 2025. *Integrovaný záchranný systém*. Online. Bezpečnostní portál Magistrátu hl. m. Prahy. Dostupné z: <https://bezpecnost.praha.eu/clanky/integrovaný-zachranny-system>. [cit. 2025-03-16].

MALINOVSKÝ, Karel a ZRUCKÝ, Matěj, 2023. *Krizové řízení v České republice*. Online. Příručka pro zastupitele. Dostupné z: <https://www.priuckazastupitele.cz/10-krizove-řízení-v-ceske-republice/>. [cit. 2025-02-17].

MARSHAL, 2023. *What is the difference between Data Security and Cyber Security?* Online. Marshal blog. Dostupné z: <https://marshalhub.com/blog/what-is-the-difference-between-data-security-and-cyber-security/>. [cit. 2025-03-09].

MERKOW, Mark S. a BREITHAUPT, Jim, 2014. *Information security: principles and practices*. Second edition. Indianapolis: Pearson. ISBN 978-0-7897-5325-0.

MINISTERSTVO VNITRA ČR, © 2025. *Ochrana kritické infrastruktury*. Online. Ministerstvo vnitra ČR. Dostupné z: <https://mv.gov.cz/clanek/ochrana-kriticke-infrastruktury-ochrana-kriticke-infrastruktury.aspx>. [cit. 2025-02-18].

MITRE CORPORATION., © 2015–2025. *MITRE ATTACK*. Online. MITRE ATT&CK©. Dostupné z: <https://attack.mitre.org/>. [cit. 2025-04-03].

NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD, ©2024. *Informace k fyzické bezpečnosti*. Online. Národní bezpečnostní úřad. Dostupné z: <https://www.nbu.cz/cs/ochrana-utajovanych-informaci/fyzicka-bezpecnost-technicke-prostredky-a-dalsi-prvky-fyzicke-bezpecnosti-a-jejich-certifikace/1014-informace/#:~:text=Fyzickou%20bezpe%C4%8Dnost%2C%20tvo%C5%99%C3%AD%20syst%C3%A9m%20opat%C5%99en%C3%AD%20kter%C3%A1%20maj%C3%AD%20neopr%C3%A1vn%C4%9Bn%C3%A9,informac%C3%ADm%2C%20pop%C5%99%C3%ADpad%C4%9B%20p%C5%99%C3%ADstup%20nebo%20pokus%20o%20n%C4%9Bj%20zaznamenat..> [cit. 2025-02-17].

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST, © 2025a. *NÚKIB*. Online. Národní úřad pro kybernetickou a informační bezpečnost. Dostupné z: <https://nukib.gov.cz/cs/o-nukib/>. [cit. 2025-02-17].

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST, © 2025b. *Vládní CERT*. Online. Národní úřad pro kybernetickou a informační bezpečnost. Dostupné z: <https://nukib.gov.cz/cs/kyberneticka-bezpecnost/vladni-cert/>. [cit. 2025-02-17].

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST, 2024. *Obecné informace o směrnici NIS2*. Online. Portál NÚKIB. Dostupné z: <https://portal.nukib.gov.cz/informace/legislativa/zakon-o-kyberneticke-bezpecnosti/okruh-obecne-informace-o-smernici-nis2>. [cit. 2025-02-17].

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2023. Praha: NÚKIB, 2024. Dostupné z: https://nukib.gov.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_kyberneticke_bezpecnosti_CR_za_rok_2023.pdf. [cit. 2025-02-17].

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2022. Praha: NÚKIB, 2023.

Dostupné z: https://nukib.gov.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_kyberneticke_bezpecnosti_CR_za_rok_2022.pdf. [cit. 2025-02-17].

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. Zpráva o činnosti NÚKIB za rok 2021. Praha: NÚKIB, 2022. Dostupné z: https://nukib.gov.cz/download/publikace/zpravy_o_stavu/Zpr%C3%A1va%20o%20%C4%8Dinnosti%20N%C3%9AKIB%20-%202021.pdf. [cit. 2025-02-17].

NG, Ka Chung; ZHANG, Xiaojun; THONG, James Y. L. a TAM, Kar Yan, 2021. Protecting Against Threats to Information Security: An Attitudinal Ambivalence Perspective. Online. *Journal of Management Information Systems*. 2021-07-03, roč. 38, č. 3, s. 732-764. ISSN 0742-1222. Dostupné z: <https://doi.org/10.1080/07421222.2021.1962601>. [cit. 2025-02-18].

NOVÁKOVÁ, Lucie, © 2025. Díky Národnímu informačnímu systému IZS jsou záchranáři rychlejší a efektivnější. Online. Ministerstvo vnitra České republiky. Dostupné z: . [cit. 2025-02-17].

ODBOR BEZPEČNOSTNÍ POLITIKY, 2023. *Krizové řízení*. Online. Ministerstvo vnitra České republiky. Dostupné z: <https://mv.gov.cz/clanek/krizove-rizeni-72.aspx>. [cit. 2025-02-17].

PANDE, Jeetendra, 2017. *Introduction to Cyber Security*. Uttarakhand Open University. ISBN 978-93-84813-96-3.

RAINS, Tim, 2023. *Cybersecurity Threats, Malware Trends, and Strategies*. 2. vydání. Packt Publishing. ISBN 978-1804613672.

ROHEL, Vladimír, 2022. *Příprava řešení kybernetických incidentů*. Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB).

SCHIMMER, David, 2024. Informační systémy pro plnění úkolů policie. Online. Policie České republiky. Dostupné z: <https://policie.gov.cz/clanek/informacni-systemy-pro-plneni-ukolu-policie.aspx>. [cit. 2025-02-17].

SINGER, P. W. a FRIEDMAN, Allan, 2014. *Cybersecurity and cyberwar*. What everyone needs to know. New York: Oxford University Press. ISBN 978-0-19-991811-9.

SMEJKAL, Vladimír, 2022. *Kybernetická kriminalita*. 3. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk. ISBN 978-80-7380-849-5.

SMEJKAL, Vladimír; SOKOL, Tomáš a KODL, Jindřich, 2019. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk. ISBN 978-80-7380-765-8.

SSHR CZECH REPUBLIC, © 2025. *Informační web systému Krizkom*. Online. Informační web systému Krizkom-SSHR. Dostupné z: <https://krizkom.gov.cz/>. [cit. 2025-02-17].

SSHR, © 2025. *Informační web IS Argis*. Online. Informační web aplikace ARGIS. Dostupné z: <https://argis.gov.cz/>. [cit. 2025-03-16].

STALLINGS, William a BROWN, Lawrie, 2024. *Computer Security: Principles and Practice*. 5. vydání. Pearson Education. ISBN 978-1-292-43779-6.

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

TLP SOLUTIONS, SPOL. S R.O., © 2024. *Informační systém SYPOS*. Online. TLP solutions. Dostupné z: <https://www.tlp-solutions.cz/produkty/informacni-system-sypos/>. [cit. 2025-02-17].

ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ, © 2025. *Postavení Úřadu*. Online. Úřad pro ochranu osobních údajů. Dostupné z: <https://uoou.gov.cz/urad/postaveni-uradu>. [cit. 2025-02-17].

YARALI, Abdurrahman; JOYCE, Randal a SAHAWNEH, Faris, 2022. *Cybersecurity and Digital Forensics: Challenges and Future Paradigms*. Nova Science Publishers. ISBN 979-8-88697-012-8.

ZHANG, Guo-Liang, 2024. *Analysing Computer System Security and Computer Network Security*. Online. *Engineering Technology Trends*. Roč. 2, č. 4, s. 0-0. ISSN 2972-483X. Dostupné z: <https://doi.org/10.37155/2972-483X-0204-3>. [cit. 2025-03-08].

SEZNAM OBRÁZKŮ

Obrázek 1 Triáda CIA.....	15
Obrázek 2 Pilíře bezpečnosti.....	18
Obrázek 3 Triáda CIA doplněná o technologie, lidi a procesy.	19
Obrázek 4 Zjednodušené zobrazení životní cyklu kybernetické bezpečnosti.....	19
Obrázek 5 Klasifikace kybernetických incidentů nahlášených NÚKIB – porovnání roku 2022 a 2023.....	50
Obrázek 6 Modelování scénáře Spear-phishing.....	65
Obrázek 7 Modelování scénáře DDoS útoku na tísňovou linku HZS.	67
Obrázek 8 Modelování scénáře útoku na serverovnu HZS.....	69

SEZNAM TABULEK

Tabulka 1 Volba scénářů.	48
Tabulka 2 What-if Scénář spear-phishing s malwarem.	53
Tabulka 3 What-if Scénář DDoS na tísňovou linku HZS.	57
Tabulka 4 What-if Scénář serverovny.	60
Tabulka 5 Seznam použitých symbolů.	63
Tabulka 6 Vyhodnocení scénářů.	71
Tabulka 7 Matice rizik.	72
Tabulka 8 Zasazení vyhodnocení scénářů do matice rizik.	73

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

BCM	Plán kontinuity činností
CASB	Cloud Access Security Broker
CIA	Confidently, Integrity, Availability (Triáda bezpečnosti)
ČR	Česká republika
DDoS	Distributed Denial of Service
DRP	Plán obnovy po havárii
GDPR	General Data Protection Regulation
HZS	Hasičský záchranný sbor
ICT	Informační a komunikační technologie
IDS	Intrusion detection system
IEC	Mezinárodní elektrotechnická komise
IRP	Plán reakce na incident
IS	Informační systémy
ISO	Mezinárodní organizace pro standardizaci
IT	Informační technologie
MFA	Multi-Factor Authentication (vícefaktorové ověření)
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
OČTŘ	Orgány činné v trestním řízení
SIEM	Security Information and Event Management
TPM	Trusted platform module
UPS	Uninterruptible Power Supply
USB	Universal Serial Bus

SEZNAM PŘÍLOH

Příloha P I: Rozšířená tabulka what- if na spear-phishing

Příloha P 2: Rozšířená tabulka what-if na DDoS útok

Příloha P 3: Rozšířená tabulka what-if na napadení serverovny

PŘÍLOHA P I: ROZŠÍŘENÁ TABULKA WHAT – IF NA SPEAR-PHISHING

Fáze útoku	Otázka "co když"	Potenciální dopady	Pravděpodobnost	Opatření
Sběr informací	Útočník získá přístup k interním databázím HZS?	Zvýšená přesnost útoku, únik citlivých informací	Vysoká	Zabezpečení interních databází, omezení přístupu, šifrování dat
	Zaměstnanci HZS sdílejí příliš mnoho informací na soc. sítích?	Snadnější sběr informací pro útok, personalizované phishingové e-maily	Střední/ vysoká	Školení o bezpečnosti na soc. sítích, omezení sdílení informací
	Útočník využije slabých míst v zabezpečení webových stránek HZS?	Získání osobních údajů zaměstnanců, útoky na webové aplikace	Střední	Pravidelné bezpečnostní audity webových stránek, aktualizace softwaru
Phishingový útok	Útočník použije pokročilé techniky spoofingu?	Nerozeznatelný falešný e-mail, vysoká úspěšnost útoku	Střední	Technická opatření proti podvrženým e-mailům, školení o rozpoznání spoofingu
	E-mail obsahuje sociální inženýrství?	Manipulace s obětí, otevření přílohy z důvodu strachu nebo naléhavosti	Vysoká	Školení o sociálním inženýrství, ověřování naléhavých požadavků
	Příloha e-mailu obsahuje zero-day exploit?	Obcházení antivirového softwaru, instalace keyloggeru	Nízká/ střední	Pravidelné aktualizace antivirového softwaru, detekce anomálií v chování systému
Infikování malwarem	Keylogger zaznamená přihlašovací údaje k systémům s krizovými plány?	Únik krizových plánů, narušení zásahů, ohrožení bezpečnosti občanů	Střední	Dvoufaktorová autentizace, monitorování přístupu, šifrování dat
	Útočník použije keylogger k získání přístupu k šifrovaným datům?	Získání citlivých informací, i přes šifrování	Nízká	Silné šifrovací algoritmy, bezpečné ukládání šifrovacích klíčů
	Malware se šíří do dalších systémů v síti HZS?	Rozšíření útoku, narušení provozu, ztráta dat	Střední/ vysoká	segmentace sítě, izolace infikovaných systémů, detekce šíření malwaru

Fáze útoku	Otázka "co když"	Potenciální dopady	Pravděpodobnost	Opatření
Bezpečnostní reakce	HZS nemá zavedený plán reakce na kybernetické incidenty?	Zmatená reakce, šíření škod, ztráta důvěry	Vysoká	Vytvoření a pravidelné aktualizace plánu reakce na incidenty
	IT oddělení HZS nemá dostatečné zdroje?	Pomalá reakce, šíření malwaru, ztráta dat	Střední	Zvýšení kapacity IT oddělení, outsourcing bezpečnostních služeb
	Zálohy dat jsou poškozené nebo nedostupné?	Ztráta dat, narušení provozu, finanční ztráty	Nízká/střední	Pravidelné testování obnovy dat, geograficky oddělené zálohy

PŘÍLOHA P 2: ROZŠÍŘENÁ TABULKA WHAT-IF NA DDOS ÚTOK

Fáze útoku	Otázka "co když"	Potenciální dopady	Pravděpodobnost	Opatření
Příprava útoku	Útočník shromáždí detailní informace o infrastruktuře webu HZS?	Cílený útok na slabá místa, maximální narušení dostupnosti	Střední	Pravidelné bezpečnostní audity webových stránek, penetrační testy, omezení zveřejňování technických detailů
	Útočník získá kontrolu nad velkým botnetem?	Masivní útok, znemožnění obrany	Střední	Využití specializovaných služeb pro ochranu proti DDoS útokům, geograficky rozložená infrastruktura
	Útočník koordinuje útok v době krizové situace?	Zvýšené narušení krizové komunikace, ohrožení zásahů	Vysoká	Plán krizové komunikace s alternativními kanály, monitorování hrozeb v reálném čase
Průběh útoku	Botnet generuje obrovské množství požadavků na webový server?	Nedostupnost webových stránek, přetížení serveru	Vysoká	Filtrování síťového provozu, blokáce útočících IP adres, přesměrování komunikace na alternativní servery
	Útok trvá dlouhou dobu?	Dlouhodobá nedostupnost webových stránek, ztráta důvěry veřejnosti	Střední	Využití služeb pro ochranu proti DDoS útokům, škálovatelná infrastruktura
	Útok je kombinován s dalšími kybernetickými útoky?	Narušení integrity dat, únik citlivých informací	Nízká (ale s vysokými dopady)	Komplexní bezpečnostní opatření, monitorování síťového provozu
Důsledky výpadků webových stránek	Veřejnost ztrácí přístup k důležitým informacím?	Narušení krizové komunikace, dezinformace ohrožení zásahů	Vysoká	Nouzový komunikační plán, sociální sítě, telefonní linky, média
	Přetížení telefonních linek HZS?	Zpoždění zásahů, ohrožení bezpečnosti občanů	Vysoká	Posílení telefonních linek, alternativní způsoby komunikace (SMS, aplikace)

Fáze útoku	Otázka "co když"	Potenciální dopady	Pravděpodobnost	Opatření
	Dojde k výrazné ztrátě důvěry veřejnosti v HZS?	Poškození reputace, narušení spolupráce s jinými organizacemi	Vysoká	Transparentní komunikace s veřejností, posílení bezpečnostních opatření, krizová komunikace
	HZS zanedbává povinnost nahlásit incident NÚKIB?	Právní důsledky, pokuty, poškození reputace	Vysoká	Zavedení postupu pro hlášení incidentů, spolupráce s NÚKIB
Reakce na incident	IT oddělení HZS reaguje pomalu?	Dlouhodobá nedostupnost webu, zvýšené dopady	Vysoká	Vytvoření postupu pro reakci na DDoS útoky, školení IT pracovníků
	Nouzový komunikační plán je neúčinný?	Narušení informovanosti veřejnosti, dezinformace	Střední	Pravidelné testování nouzového komunikačního plánu, aktualizace informací
	Analýza incidentu odhalila závažné zranitelnosti?	Ohrožení dalších systémů, nutnost rozsáhlých bezpečnostních opatření	Střední	Aktualizace bezpečnostní dokumentace a procesů, posílení zabezpečení webu

PŘÍLOHA P 3: ROZŠÍŘENÁ TABULKA WHAT – IF NA NAPADENÍ SERVEROVNY

Fáze útoku	Otázka "co když"	Potenciální dopady	Pravděp.	Opatření
Příprava útoku	Nový zaměstnanec zná citlivé údaje o serverech HZS?	Cílený útok na kritické systémy, maximální škody	Střední	Omezení přístupu k citlivým informacím, segmentace sítě, šifrování dat
	Zaměstnanec připraví sofistikovaný ransomware?	Šifrování kritických dat, znemožnění obnovy dat	Střední	Detekce anomálií v chování systému, aktualizace antivirového softwaru, zálohování dat mimo síť
Vniknutí do serverovny	Zaměstnanec využije mezer v bezpečnostních opatřeních?	Neoprávněný vstup, instalace ransomware	Střední	Detektory pohybu, monitorování vstupu do serverovny, pravidelné audity fyzické bezpečnosti
	Serverovna nemá dostatečné fyzické zabezpečení?	Neoprávněný vstup, instalace ransomware, fyzické poškození serverů	Střední	Monitorování vstupu do serverovny, pravidelné audity fyzické bezpečnosti
	Zaměstnanec připojí infikovaný USB disk k serveru?	Šíření ransomware, šifrování dat	Vysoká	Zakázání automatického spouštění USB disků, detekce anomálií v chování systému
Infikování malwarem	Ransomware zašifruje kritické databáze?	Ztráta přístupu k IT systémům, narušení provozu	Vysoká	Zálohování dat mimo síť, plán obnovy provozu, šifrování dat
	HZS nemá aktuální zálohy dat?	Nenávratná ztráta dat, finanční ztráty, ohrožení zásahů	Vysoká	Pravidelné zálohování dat mimo síť, testování obnovy dat, plán obnovy provozu
	Útočník požaduje vysoké výkupné?	Finanční ztráty, rozhodování o platbě výkupného	Vysoká	Rozhodnutí o neplacení výkupného, kontaktování orgánů činných v trestním řízení, plán obnovy provozu

Fáze útoku	Otázka "co když"	Potenciální dopady	Pravděp.	Opatření
Dopady incidentu	Ztráta přístupu k IT systémům způsobí zpoždění zásahů HZS?	Narušení provozu, ohrožení zásahů, finanční ztráty	Vysoká	Plán obnovy provozu, záložní systémy, komunikace s veřejností
	Porušení GDPR povede k vysokým finančním sankcím a ztrátě důvěry veřejnosti?	Právní následky, finanční sankce, ztráta důvěry	Střední	Zavedení opatření pro ochranu osobních údajů, komunikace s úřadem pro ochranu osobních údajů
	Poškození reputace HZS naruší spolupráci s ostatními složkami IZS?	Ztráta důvěry veřejnosti a složek IZS, narušení spolupráce	Vysoká	Komunikace s veřejností, transparentní informování o incidentu, posílení bezpečnostních opatření
Reakce na incident	Izolování infikovaných serverů není dostatečně rychlé a ransomware se rozšíří do dalších systémů?	Rozšíření infekce, zvýšení finančních ztrát, prodloužení doby obnovy provozu, poškození reputace	Vysoká	Okamžité odpojení infikovaných systémů od sítě, izolace postižených segmentů sítě, nasazení nástrojů pro detekci a eliminaci malwaru, forenzní analýza pro identifikaci rozsahu infekce
	Vyšetřování Policie ČR nevede k identifikaci pachatele a získání důkazů?	Neschopnost pohnat pachatele k odpovědnosti, riziko opakování útoku, ztráta důvěry veřejnosti v schopnost orgánů činných v trestním řízení řešit kybernetické útoky	Vysoká	Spolupráce s mezinárodními OČTŘ, posílení vlastních bezpečnostních opatření, informování veřejnosti o průběhu vyšetřování
	Analýza ransomwaru neposkytne možnosti dešifrování dat?	Trvalá ztráta dat, prodloužení doby obnovy provozu, zvýšení finančních nákladů na obnovu systému	Vysoká	Alternativní metody obnovy dat, forenzní analýza pro identifikaci zranitelností, posílení bezpečnostních opatření pro prevenci budoucích útoků

Fáze útoku	Otázka "co když"	Potenciální dopady	Pravděp.	Opatření
	Obnova dat ze záloh je neúplná nebo poškozená?	Zpoždění obnovení provozu, ztráta důležitých dat, zvýšení finančních nákladů na obnovu	Vysoká (při nedostatečném zálohování)	Pravidelné testování obnovy dat, implementace redundance zálohování, geograficky oddělené zálohy
	Rozhodnutí o neplacení výkupného povede k trvalé ztrátě dat?	Finanční ztráty, etické dilemma	Vysoká	Rozhodnutí o neplacení výkupného, kontaktování orgánů činných v trestním řízení