Detekce anomálií v síti subjektu ochrany obyvatelstva

Bc. Jiří Čamek

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. Jiří Čamek**
Osobní číslo:	**L23666**
Studijní program:	**N1032A020002 Bezpečnost společnosti**
Specializace:	**Ochrana obyvatelstva**
Forma studia:	**Prezenční**
Téma práce:	**Detekce anomálií v síti subjektu ochrany obyvatelstva**

Zásady pro vypracování

1. Proveďte teoretický vstup do řešené problematiky.
2. Seznamte se se současnými trendy v oblasti monitoringu sítí.
3. Pojednejte o možných anomáliích v síti subjektu ochrany obyvatelstva.
4. Zpracujte scénáře vybraných útoků na subjekt ochrany obyvatelstva.

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

Seznam doporučené literatury:

1. BROOKS, Charles J.; GROW, Christopher; CRAIG, Philip a SHORT, Donald. *Cybersecurity Essentials.* Indianapolis, Indiana: Sybex, John Wiley, 2018. ISBN 978-1-119-36239-5.
2. DOUCEK, Petr, KONEČNÝ Martin, NOVÁK Luděk a SHORT Donald. *Řízení kybernetické bezpečnosti a bezpečnosti informací: problematika bezpečnosti v kyberprostoru.* Vydání: první. Praha: Professional Publishing, 2019. ISBN 978-80--88260-39-4.
3. EVANS, Lester. *Cybersecurity: What you Need to Know About Computer and Cybersecurity, Social Engineering, The Internet of Things + An Esential Guide to Ethical Hacking for Beginners.* USA: Lester Evans, 2019. ISBN 9781794647237.
4. KOLOUCH, Jan a BAŠTA, Pavel. *CyberSecurity*. CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2019. ISBN 978-80-88168-31-7.
5. SEDLÁK, Petr; KONEČNÝ Martin; CRAIG Philip a SHORT Donald. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru.* Vydání: první. Brno: CERM, akademické nakladatelství, 2021. ISBN 978-80-7623-068-2.

Další odborná literatura dle doporučení vedoucího diplomové práce.

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

Datum zadání diplomové práce: **2. června 2025**
Termín odevzdání diplomové práce: **4. srpna 2025**

L.S.

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

prof. Ing. Dušan Vičar, CSc.
ředitel ústavu

V Uherském Hradišti dne 2. června 2025

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 0.4.08.2025 .....

podpis autora

ABSTRAKT

Diplomová práce se věnuje problematice kybernetické bezpečnosti v počítačových sítích a tvorbě scénářů kybernetických útoků, které v současnosti mohou ohrozit subjekty ochrany obyvatelstva. V teoretické části jsou uvedeny a popsány základní pojmy týkající se problematiky kybernetické bezpečnosti, počítačových sítí, kybernetických útoků na tyto sítě a monitoring sítí.

Praktická část práce se zabývá analýzou monitorovacích nástrojů, charakteristikou vyskytujících se anomálií v počítačové síti, popisem vybraného subjektu ochrany obyvatelstva, analýzou současného stavu ohledně bezpečnosti IT v subjektu a následnou tvorbou scénářů kybernetických útoků. V závěru scénářů jsou zpracovány návrhy na zlepšení bezpečnosti počítačových sítí v subjektu.

Klíčová slova: anomálie, DDoS, hrozby, kybernetická bezpečnost, monitoring, počítačová síť, monitoring

ABSTRACT

The thesis deals with the issue of cyber security in computer networks and the creation of cyber attack scenarios that can currently threaten the subjects of public protection. In the theoretical part, the basic concepts related to cyber security, computer networks, cyber attacks on these networks and network monitoring are presented and described.

The practical part of the thesis deals with the analysis of monitoring tools, characterization of occurring anomalies in the computer network, description of the selected subject of population protection and subsequent creation of cyber attack scenarios. At the end of the scenarios, proposals for improving the security of computer networks in the subject are elaborated.

Keywords: anomalies, cyber security, computer network, DDoS, Monitoring, Threats

Za odborné vedení, cenné rady a poznámky v průběhu psaní diplomové práce bych chtěl poděkovat panu Ing. Petru Svobodovi Ph.D. Dále bych rád poděkoval paní Mgr. Yvettě Jahnové za kontrolu českého jazyka a pracovníkům Městské policie za poskytnuté informace. Velké poděkovaní náleží mé rodině a kamarádům za podporu v průběhu celého studia.

OBSAH

ÚVOD

Neustálý vývoj informační infrastruktury otevírá stále nové možnosti k řešení běžných situací skrze technologie. Tablety, počítače a komunikační zařízení pomáhají nejen běžným uživatelům ale i firmám a jejich zaměstnancům s každodenní prací a každodenním fungováním na internetu. Tyto technologie se ale časem staly až moc potřebné pro běžný život a dlouhodobým využíváním sbírají o svých uživatelích hodně citlivých informací. Ukládání těchto informací jako jsou jména, telefonní čísla, emaily, hesla, bankovní údaje, dokumenty, myšlenky a data o osobních zájmech vytvořilo novu oblast o kterou se občané musejí strachovat. Každý pohyb a zápis dat na internetu může být klíčový a spousta občanů si ani neuvědomuje že jejich akce mohou ohrozit je samotné, a i další v jejich blízkosti. O tato data a jejich zneužití mají zájem i hackeři kteří mohou chtít data využít pro finanční prospěch nebo je jen záměrně zničit. V uplynulých třech letech se výskyt kybernetických útoků na počítačové servery ve světě několikanásobně zvýšil. Tyto útoky mají většinou za cíl ochromit IT infrastrukturu a tím omezit provoz dané firmy nebo subjektu ochrany obyvatelstva. Za některými tyto útoky se ale skrývá pravá podstata, kterou je krádež a využití citlivých informací proti samotným občanům nebo danému státu. Ochromení některých systémů a krádež dat může vést ke kompletnímu narušení kybernetické bezpečnosti státu.

Oblast kybernetické bezpečnosti se za daných okolností stále vyvíjí a kvalifikovaní pracovníci IT jsou schopni na vzniklé hrozby včas reagovat. Hlavním problémem při těchto hrozbách je ale samotný vznik prostoru v síti pro kybernetický útok. Tento prostor vytváří sami uživatelé nebo správci sítě špatnou konfigurací zabezpečovacích systémů nebo nepřívětivým chováním při připojení k interní síti. Klíčovou roli v ochraně kybernetické bezpečnosti hraje informovanost a pochopení, že každá akce na síti může vyvolat negativní reakci která poté může ohrozit bezpečnost dat. Různé vývojářské firmy nabízí několik druhů softwarů, které pomáhají tyto takzvané anomálie v sítích včas identifikovat a pomoc správcům sítě v čas reagovat a ochránit jak jejich systémy, tak i data.

Z těchto důvodů, a hlavně z důvodu předešlých zkušeností s kybernetickou bezpečností, díky bakalářské práci, jejichž poznatky z teoretické části jsem využil a obohatil o nové myšlenky při zpracování teoretické části diplomové práce byl jednoznačný výběr tohoto tématu, aby se prohloubila informovanost o problematice bezpečností sítí jak u běžných uživatelů, tak i v menších subjektech ochrany obyvatelstva.

CÍLE PRÁCE A POUŽÍTÉ METODY

Hlavním cílem diplomové práce je v souvislosti s detekcí anomálií vytvořit možné scénáře kybernetických útoků na počítačovou síť v subjektu ochrany obyvatelstva. Pro splnění hlavního cíle bylo nutné splnit následující dílčí cíle:

- Zpracovat teoretický vstup z oblasti kybernetické bezpečnosti.
- Seznámit se s problematikou monitoringu sítí a pojednat o možný anomáliích v síti.
- Vyhodnotit síťové zabezpečení subjektu.
- Navrhnout možná opatření ke zmírnění rizik spojených se scénáři kybernetických útoků.

Pro účely vypracování této diplomové práce byly využity následující metody:

- Syntéza – Informace převzaté z bakalářské práce byly doplněny o nová zjištění z dalších odborných zdrojů a společně tvoří ucelený teoretický rámec.
- Dedukce – Scénáře kybernetických útoků reflektují obecné trendy v oblasti kybernetických hrozeb, které byly deduktivně aplikovány na specifické prostředí Městské policie v Rýmařově.
- Indukce – V rámci praktické části byly na základě konkrétních zjištění z analýzy dokumentace, výstupů z rozhovorů a výsledků modelových scénářů odvozeny obecné závěry o úrovni připravenosti a odolnosti Městské policie Rýmařov vůči kybernetickým hrozbám.
- Analýza – V praktické části je provedena analýza softwarových nástrojů z hlediska využití při detekci anomálií.
- SWOT analýza – V praktické části je vytvořena pro identifikaci nedostatků v krizových plánech obce.
- Rozhovor – Pro vyhodnocení současného stavu zabezpečení sítí u MP byl vyhodnocen rozhovor s pracovníkem MP, který poskytl informace o síťové bezpečnosti.

- Modelování – Scénáře byly vytvořeny na základě získaných informací pro otestování informační bezpečnosti v subjektu a následně navrhnuty opatření na zlepšení bezpečnosti.
- Metoda what-if – Tato metoda byla využita v praktické části při vyhodnocování síťových anomálií. Pomocí hypotetických otázek bylo zkoumáno, jaké důsledky by nastaly, pokud by se konkrétní anomálie skutečně vyskytla v síti Městské policie Rýmařov.

Omezení práce

Při zpracování 8. kapitoly, která se zaměřuje na anomálie v síti Městské policie Rýmařov, nebylo možné provést přímou analýzu síťové infrastruktury na pracovišti z důvodu omezeného přístupu. Velitel stanice odmítl umožnit přístup k síti s ohledem na důvěrnost a možné riziko úniku citlivých informací. Z tohoto důvodu jsou uvedené typy anomálií formulovány na obecné úrovni a vycházejí z obecně známých typů. Možné dopady anomálií na MP byly však částečně konzultovány se zaměstnanci IT oddělení, kteří působí v obci.

I. TEORETICKÁ ČÁST

1 KYBERNETICKÁ BEZPEČNOST

Kybernetická bezpečnost se pod vlivem moderní doby a uskutečněnými událostmi v kyberprostoru za několik uplynulých let posunula a získala velkou pozornost a stala se jednou z hlavních priorit mnoha národních politik. Je to z velké části způsobeno celosvětovým rozvojem informačních a komunikačních technologií (dále jen ICT). Ani Česká republika nezaostává a v letošním roce se snaží implementovat nové změny v zákoně o kybernetické bezpečnosti. Narůstající závislost na technologiích s sebou však nese potenciální hrozby a rizika. Mezi hlavní otázky patří ochrana citlivých státních informací a kritické infrastruktury. Pokud by se to nepodařilo, mohlo by to mít vážné důsledky pro národní bezpečnost, ekonomiku, administrativu i bezpečnost obyvatelstva. Kyberprostor není omezován hranicemi ani kontinenty, což umožňuje téměř neomezený přístup a relativní anonymitu. Zvážení těchto vlastností vytváří příznivé prostředí pro kyberkriminalitu. (Kybernetická bezpečnost, © 2009–2025)

Vzhledem k dnešní době, pro mnoho lidí kybernetická bezpečnost představuje obor, kterým se zabývají oddělení s informačními a komunikačními technologiemi. Jenže tato dedukce je chybná. Jelikož kybernetická bezpečnost se týká všech uživatelů, kteří využívají jakýkoliv prvek jejího ICT v každodenním životě. (Kolouch, Bašta, 2019)

„*Kybernetickou bezpečnost nelze v současné době ani podceňovat ani bagatelizovat. Je to oblast, která je pro řadu organizací, ale i jedinců samotných klíčová, a proto by měla být řešena dlouhodobě a systematicky*.“ (Kolouch, Bašta, 2019, s. 40)

Kybernetická bezpečnost se primárně definuje jako soubor technologií, procesů a postupů speciálně navržených tak aby byly schopny efektivně ochránit internetové systémy, počítačové sítě, softwary a data před kybernetickými útoky které mohou tato aktiva poškodit, odcizit nebo jakkoliv s nimi neoprávněně manipulovat. Kybernetické útoky jsou primárně cílené na citlivé informace, díky kterým pak útočníci mohou zajistit jejich změnu, smazání anebo vymáhání peněz od uživatelů za jejich obnovení. (Doucek et al., 2019)

Při zajišťování kybernetické bezpečnosti je nejdůležitější pochopit, aby všichni uživatelé, kteří vlastní jakoukoliv informační nebo komunikační technologii představili že veškerý pohyb a jakékoliv chování v kyberprostoru ovlivňuje úspěšnost útočníků při kybernetických útocích. Kybernetickou bezpečnost a veškerou její aktivitu lze aplikovat i mimo kyberprostor a nesmí se podceňovat. (Kolouch, Bašta, 2019)

Kybernetická bezpečnost zahrnuje široké spektrum preventivních opatření, mezi která patří například:

- Školení zaměstnanců v oblasti kybernetické bezpečnosti.
- Ochrana softwaru pro sítě, cloudová úložiště, aplikace, data a informace.
- Zabezpečení databází a IT infrastruktury.
- Ochrana mobilních zařízení, jako jsou telefony a tablety.
- Fyzická ochrana citlivých informací.
- Opatření pro bezpečný provoz.
- Pravidelné zálohování dat.
- Obnova dat po kybernetickém útoku. (Doucek et al., 2019)

Při aplikaci kybernetické bezpečnosti jsou implementovány 3 hlavní principy, známé také jako triády kybernetické bezpečnosti. Mezi tyto triády se řadí CIA, prvky kybernetické bezpečnosti a životní cyklus kybernetické bezpečnosti. (Kolouch, 2016)

1.1 Kyberprostor

Kyberprostor je virtuální prostředí počítačů, který tvoří globální síť složenou z menších sítí, které využívají TCP/IP protokol. Interakce subjektů v kyberprostoru je totožná s interakcí v reálném světě, ale bez potřeby fyzické přítomnosti. Informace jsou sdíleny v reálném čase nebo s určitým zpožděním a lidé mohou nakupovat, sdílet zkušenosti, prozkoumávat obsah, provádět výzkum, pracovat nebo se bavit. (Kolouch, 2016)

Kyberprostor lze rozdělit na tři části

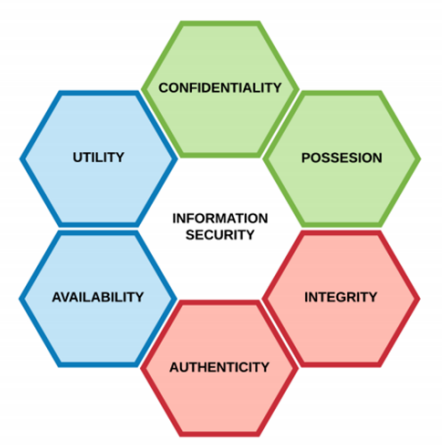
- Surface Web – Běžná část internetu, která je dostupná velké části společnosti a lze se v ní pohybovat pomocí webových prohlížečů. Surface Web zahrnuje jenom 4 % celého internetu.
- Deep Web – Je součást World Wide Webu, která není dostupná prohlížeči jako jsou Google nebo bing. Deep Web obsahuje 96 % veškerých informací v kyberprostoru.

- Dark Web – Je součástí Deep Webu se zaměřením na nelegální činnosti. Dostat se do této části kyberprostoru vyžaduje speciální prohlížeč. (Co je deep web? A jak se liší od dark webu? © 1994–2025)

1.2 Triáda CIA

Triáda CIA, je model vyvinutý jako vodítko pro politiku informační bezpečnosti v rámci organizací. Složená z těchto tří prvků důvěrnost, integrita a dostupnost Tyto prvky jsou nejzákladnější a nejdůležitější principy kybernetické bezpečnosti. V této souvislosti je důvěrnost souborem pravidel, která omezují přístup k informacím, integrita je ujištění, že informace jsou důvěryhodné a přesné, a dostupnost je zárukou spolehlivého přístupu oprávněných osob k informacím. (Kolouch, Bašta, 2019)

Odborníci tento model ale nepovažují za dostačující, a tak v roce 1998 Donn B. Parker potvrdil že Triáda CIA potřebuje rozšířit a doplnil ji o nové 3 principy. Tento soubor principů Parker nazval Parkerian hexad (viz. Obrázek 1).



Obrázek 1 - Parkerian hexad

(Marks, © 2023)

Do nového souboru principů zařadil držení a kontrolu, autentičnost a užitečnost:

- Držení a kontrola – Představuje stav, kdy osoba bez oprávnění získá kontrolu nad něčím, co nevlastní, ale nedojde k jejímu zneužití.
- Autentičnost – Představuje stav, kdy je zdroj informací správně označen certifikátem pravosti.

- Užitečnost – Představuje stav, kdy data musejí splňovat dostupnost ale také užitečnost. (Pender-bey, 2012)

1.3 Prvky kybernetické bezpečnosti

Vhodná úroveň kybernetické bezpečnosti je dosažena díky vzájemné interakci mezi lidmi, technologiemi a procesy. Ačkoli technologie mohou být zásadním prvkem pro kybernetickou bezpečnost, důležitějšími stavebními kameny jsou správně nastavené procesy a zejména lidé, kteří jsou schopni tyto procesy aplikovat a dodržovat dohodnutá pravidla. (Kybernetická bezpečnost, © 2025)

Lidé

Lidé patří mezi klíčový prvek v oblasti kybernetické bezpečnosti. Jsou tvůrci bezpečnostních pravidel a zároveň jejich uživateli. Ale také jsou nejslabším článkem v celém systému a často se stávají cílem útočníků. Je nutné je pravidelně informovat o základních pravidlech a posilovat jejich vzdělání v oblasti kybernetické bezpečnosti, protože jsou největší hrozbou pro tuto oblast.

Lidé, kteří používají ICT by měli znát a dodržovat tyto principy a pravidla kyberprostoru:

- Základní principy a pravidla kybernetické bezpečnosti.
- Znát základní funkce počítačových systémů které používají.
- Zanalyzovat si aplikace které využívají.
- Vzdělávat se v oblasti kybernetické bezpečnosti. (Kolouch, Bašta, 2019)

Technologie

Technologie patří mezi obvyklé prostředky uživatelů, jenž jim umožnují připojení k internetu, různým aplikacím a sociálním sítím. Tyto nástroje slouží k vytváření dokumentů, zasílání e-mailů a sledování videí. Běžný uživatel interaguje se svými koncovými technologiemi (PC, tablet, mobilní telefon), ale zpravidla se nezajímá o další technologie, které jsou nezbytné pro danou činnost v kyberprostoru.

Technologie jsou pro organizace nezbytné, a to včetně zařízení, která jsou určena pro uživatele (mobilní zařízení), kompletní infrastruktury sítě (LAN, Wi-Fi), služeb (servery, aplikace) a prvky zajišťující bezpečnost, ať už v perimetru (firewall, IDS/IPS) nebo v rámci infrastruktury (prvky pro autentizaci a autorizaci, monitoring a analýzu). (Smejkal et al., 2019)

Technologie jsou obvykle nevyhnutelnou součástí kybernetické bezpečnosti, a to ohledu na to, zda jsou používány jednotlivci nebo organizací. Pro zajištění kybernetické bezpečnosti je tedy nutné udržovat technologie v takovém stavu, aby byly schopny reagovat na změny, které souvisejí s vývojem ICT. Hlavním způsobem, jak toho dosáhnout, je pravidelné aktualizování a zabezpečení technologií včetně hardwaru a softwaru. (Kybernetická bezpečnost, © 2025)

Procesy

Procesy představují činnosti, které je nutné provést, aby lidé měli možnost využívat implementované technologie a příslušné služby. Mezi základní procesy se řadí:

- Definování aktiv a analýza rizik.
- Implementace ICT a aplikací.
- Zpráva uživatelů a rolí.
- Autorizace a autentizace.
- Údržba systémů a služeb.
- Testování zabezpečení jednotlivých systémů.
- Analýza a realizace opatření.
- Školení a cvičení atd.

Tyto procesy se týkají celého životního cyklu ICT, informací a dat a zahrnují i uživatele. Implementace, údržba a modifikace těchto procesů představují nejnáročnější část budování kybernetické bezpečnosti a vyžadují vysokou úroveň odbornosti ze strany správců systémů. Pokud organizace implementuje pravidla kybernetické bezpečnosti, je důležité udržovat software a hardware aktuální a dodržovat přístupová pravidla pro jednotlivé systémy. (Kolouch, 2016)

1.4 Životní cyklus kybernetické bezpečnosti

Při budování kybernetické bezpečnosti je nutné brát v úvahu časový průběh a uplatňovat nebo modifikovat triádu CIA a další prvky v průběhu celého cyklu. Prevence, detekce a reakce na útok jsou klíčovými prvky. Diagramy jsou často používány k zobrazování životního cyklu kybernetické bezpečnosti pro lepší přehlednost. (Hub, 2013)

Obrázek 2 - Životní cyklus Kybernetické bezpečnosti

(Základní pojmy, © 2021)

Kybernetickou bezpečnost lze přirovnat k neustálému hodnocení rizik, ale kromě běžné analýzy je nutné provádět i další podpůrné procesy, které mohou přispět ke zlepšení kybernetické bezpečnosti organizace. (Kolouch, Bašta, 2019)

1.5 Právní rámec

Hlavní právní základ pro oblast kybernetické bezpečnosti v českém právním systému tvoří především:

Zákon č.181/2014 Sb. – Zákon o kybernetické bezpečnosti řeší práva a povinnosti osob, ale také pravomoci a činnosti orgánů veřejně moci, zejména Národního bezpečnostního úřadu a Národního úřadu pro kybernetickou a informační bezpečnost ve věcech týkajících se oblasti kybernetické bezpečnosti. Tento zákon vymezuje:

- Klíčové pojmy související s kybernetickou bezpečností.
- Pravidla pro bezpečnostní opatření.
- Rozdíl mezi kybernetickou událostí a incidentem.
- Povinnost evidovat hrozby, reaktivní a ochranná opatření.
- Fungování a pravomoci státní správy.
- Kontrolní mechanismy, nápravná opatření a sankce za přestupky. (Česko, 2014)

Zákon č. 110/2019 Sb., o zpracování osobních údajů: Tento zákon doplňuje obecné nařízení o ochraně osobních údajů (GDPR) a stanovuje pravidla pro zpracování osobních údajů v České republice. (Česko, 2019)

Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti: Tento zákon upravuje ochranu utajovaných informací a stanovuje požadavky na bezpečnostní způsobilost osob, které s těmito informacemi pracují. (Česko, 2005)

Vyhláška č. 82/2018 Sb. – Tato vyhláška pojednává o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat.

Vyhláška o kybernetické bezpečnosti definuje klíčové pojmy, stanovuje bezpečnostní, technická a organizační opatření, ukládá povinnosti týkající se bezpečnostní politiky a dokumentace a zároveň se zabývá řešením kybernetických bezpečnostních incidentů a reaktivních opatření. (Česko, 2018)

Vyhláška č. 205/2016 Sb. – Novelizuje vyhlášku č.317/2014 Sb. O významných informačních systémech a jejich určujících kritériích. Hlavním předmětem úprav této vyhlášky je stanovování významných informačních systémů a jejich určujících kritérií.

Kritéria pro určení významného informačního systému se dělí na dopadová a oblastní kritéria. Za významný informační systém se nepovažuje systém spravovaný obcí nebo hlavním městem Praha v rámci výkonu jejich působnosti. Pokud informační systém není uveden v příloze této vyhlášky, posouzení jeho významnosti provádí jeho správce. (Česko, 2016)

Vyhláška č. 573/2020 Sb. – Novelizuje vyhlášku č. 437/2017 Sb. o kritériích pro určení provozovatele základní služby která slouží k provedení zákona o kybernetické bezpečnosti. Tento zákon pověřuje Národní úřad pro kybernetickou a informační bezpečnost odpovědností za určování provozovatelů základních služeb a informačních systémů těchto služeb, podobně jako u správců kritické informační infrastruktury. Novela upravuje a rozšiřuje podmínky pro stanovení provozovatelů základních služeb v oblasti zdravotnictví. (Česko, 2020)

Směrnice NIS2 (EU 2022/2555) – Tato směrnice přináší zásadní změnu v přístupu k zabezpečení informačních technologií a kybernetické infrastruktury v rámci Evropské unie. NIS2 by měla být převedena do českého právního systému pomocí nového zákona o kybernetické bezpečnosti a související vyhlášky Národního úřadu pro kybernetickou bezpečnost, které nahradí stávající zákon č. 187/2014 Sb., o kybernetické bezpečnosti.

Tento nový zákon sjednotí pravidla o kybernetické bezpečnosti pro cca 6 000 subjektů a přinese tyto klíčové změny:

- Zavedení povinného školení vedoucích pracovníků managementu v oblasti kybernetické bezpečnosti.
- Zpřísnění sankcí za porušení bezpečnostních opatření
- Zavedení centralizovaného systému pro oznamování bezpečnostních incidentů skrze Portál NÚKIB.
- Stanovení jednotnějších pravidel pro spoluprací mezi členskými státy EU. (Obecné informace o směrnici NIS2, © 2025)

Cílem této regulace je posílit odolnost organizací proti kybernetickým hrozbám a zajistit bezpečnost strategickým službám.

Nový zákon o kybernetické bezpečnosti přináší spoustu změn v zajištění bezpečnosti v kyberprostoru. V § 15 nového zákona jsou vypsána veškerá bezpečnostní opatření která jsou povinni zavést poskytovatelé regulované služby v režimu vyšších povinností.

Tato technická opatření mají teoretickou návaznost na problematiku monitorování sítí a zajištění IT bezpečnosti pomocí různých nástrojů:

- Zajistit fyzickou bezpečnost prostředí a technologií.
- Zajištění bezpečnosti komunikačních sítí.
- Efektivní správa uživatelských identit a jejich ověřování.
- Kontrola a řízení přístupových práv podle rolí a oprávnění.
- Schopnost včasné detekce kybernetických bezpečnostních incidentů.
- Systémové zaznamenávání bezpečnostních událostí.
- Vyhodnocování zaznamenaných incidentů.
- Bezpečnost softwarových aplikací.
- Používání kryptografických metod.
- Zajištění nepřerušené dostupnosti služeb podléhajících regulaci.
- Ochrana průmyslových systémů, řídicích technologií a dalších specifických zařízení. (Vládní návrh Zákon o kybernetické bezpečnosti, 2024)

2 POČÍTAČOVÁ SÍŤ

Počítačová síť je skupina propojených počítačů, které umožňují sdílení dat mezi jednotlivými uzly dané sítě. Tyto uzly mohou být počítače, servery, tiskárny nebo další zařízení, která jsou připojena k síti a umožňují komunikaci s ostatními uzly pomocí různých technologií, jako jsou Ethernet, Wi-Fi nebo Bluetooth. Komunikace mezi těmito uzly probíhá podle předem stanovených pravidel a vysoké spolehlivosti komunikace. (Horák a Keršláger, 2011)

Počítačové sítě jsou dnes běžně používány v různých oblastech, jako jsou kancelářské prostředí, školy, nemocnice, průmysl, banky a ostatní domácí sítě. Využívají se pro sdílení internetového připojení a dalších zdrojů. Síťové technologie také umožňují vzdálený přístup k počítačům a datům, což umožňuje práci na dálku a zvyšuje efektivitu práce v mnoha oborech. Tyto počítačové sítě lze rozdělit do několika skupin. (Kolouch, 2016)

2.1 Klasifikace sítí

Počítačové sítě lze rozdělit do několika kategorií. Sítě dělíme podle typu přepojování, postavení uzlů, druhu přenášených signálů, rozlehlosti a podle vlastnictví.

Dělení podle typu přepojování

- Komutační síť (Přepojování okruhů) – Hlavním úkolem tohoto typu přepojování je zajistit, aby mezi zdrojovým a cílovým uzlem vzniklo nepřetržité spojení které vydrží po celou dobu komunikace, dokud není spojení ukončeno. Komutační sít je využitelná i pro přenos různých dat.
- Paketová sít (Přepojování paketů) – Základem tohoto typu přepojování je, aby cesta, kterou paket urazí byla neznámá od zdroje až po cílový uzel. Každý jedinečný paket se tak přenáší po vlastní trase, kterou zařizuje struktura dané sítě. Routery tudíž musí efektivně určovat optimální trasu pro přenos paketů a zároveň se přizpůsobovat změnám v síťové infrastruktuře. (Typy sítí, © 2022)

Dělení podle postavení síťových uzlů

- Peer-to-peer (rovný s rovným) – Tato počítačová síť, umožnuje komunikaci mezi jednotlivými počítačovými systémy. Veškeré uzly v této síti jsou si rovny. Používá se pro sdílení souborů a systémových prostředků.

- Klient-server – Je typ sítě, kde je jeden nebo více počítačových systému nadřazen jinému počítačovému systému nebo více počítačovým systémům. Na tomto modelu klient-server jsou založeny služby typu web a e-mail. (Kolouch, 2016)

Dělení podle rozlehlosti sítí

- Osobní síť (PAN) – Tato malá privátní síť slouží pro potřeby jednotlivce nebo celé domácnosti. K propojení jednotlivých systémů tato síť využívá Bluetooth nebo Wi-Fi. Tyto sítě neposkytují nejvyšší rychlost přenosu, ale dbají na odolnost proti rušení, snadnou nastavitelnost a malou spotřebu.
- Lokální síť (LAN) – Jedná se o velkou lokální síť v rámci, které dochází k propojení jedné nebo více budov. K propojení dochází za pomocí routeru nebo switch zařízení. Přenosová rychlost tohoto typu sítě je řádově v Gb/s. Mezi nejpoužívanější technologie v současných LAN sítích patří Ethernet, bezdrátová síť Wi-Fi nebo WLAN.
- Metropolitní síť (MAN) – Jedná se o síť, která propojuje veškeré lokální sítě, které se vyskytují v dosahu desítek kilometrů. MAN síť poskytuje rozšíření lokálním sítím v podobě prodloužení dosahu, navýšením počtu připojených a rychlosti. K propojení této sítě se využívá Wi-Fi nebo optické vlákno.
- Vzdálená síť (WAN) – Jedná se o síť, která propojuje jednotlivé LAN a MAN sítě na geografické úrovni v rozsahu kontinentu ale i celosvětově. Přenosová rychlost WAN sítě se odvíjí od typu sítě mezi Kb/s až Gb/s. (Kolouch, 2016)

Dělení podle druhů přenášených signálů

- Analogová síť – Tento elektronický systém zprostředkovává propojení počítačů prostřednictvím sítě, která využívá analogový signál ke komunikaci. K této síti je nutno připojit modem, aby byla schopna převést digitální data na analogový signál. Analogové signály lze rozdělit podle média které je přenáší na akustický, elektrický a optický signál.
- Digitální síť – Tato síť slouží k přenosu a propojení signálů, které mají obvykle dvé úrovně. Například v analogové síti lze mít na jednom kanále jen jeden program, ale v digitální síti lze mít na jednom kanále více programů například televizní a rozhlasové. (Digitální a analogové signály a průběhy, © 2025)

Dělení podle vlastnictví sítí

- Privátní síť – Tato síť využívá privátní IP adresy a jsou používány hlavně v rámci sítě LAN. Tyto sítě se využívají z důvodu nedostatečného množství veřejných IP adres ve verzi IPv4.
- Veřejná síť – Tento typ sítě je využíván ke komunikaci a přenosu dat mezi širokou veřejností. Tyto sítě provozují spojové organizace, které splňují veškeré potřebné požadavky.
- Virtuální privátní síť (VPN) – VPN je mechanismus který propojuje počítačové systémy za pomocí nedůvěryhodné sítě tak, že komunikace mezi těmito systémy vypadá jako by byly propojeny důvěryhodnou sítí. (Kolouch, 2016)

2.2 TCP/IP

V počítačových sítích se používá několik druhů síťových protokolů pro komunikaci. Transmission Control Protocol/Internet Protocol je nejdůležitější skupina protokolů používaná na internetu. V této skupině se nachází protokoly sloužící k přenosu dat, vytvoření spojení v síti a připojení počítače k internetu. Název tohoto protokolu je odvozen od dvou nejvýznamnějších světových komunikačních protokolů. Internet protocol (dále jen IP) umožňuje vzájemnou komunikaci libovolných uzlů v propojených sítích. (Podkapitola 2.3).

Transmission Control Protocol (dále jen TCP) je transportní protokol, který umožňuje spolehlivý a obousměrný přenos dat mezi aplikacemi běžícími na dvou propojených uzlech. TCP je doplňující protokol pro Internet protocol a přináší spolehlivost a správnost v doručování datagramů. Také zajišťuje identifikaci a distribuci dat mezi více aplikacemi, jako je například webový server a e-mailový server, které jsou provozovány na jednom počítači. TCP byl vyvinut americkým ministerstvem obrany, a proto je považován za nejbezpečnější protokol pro přenos dat. (Brooks et al., 2018)

2.3 Internetový Protokol a IP adresa

Internet Protocol zajišťuje přenos datagramů na základě síťových IP adres, které jsou uvedeny v jejich hlavičce. Datagram je samostatná datová jednotka, která obsahuje všechny potřebné informace o adresátovi a odesílateli, včetně pořadového čísla datagramu ve zprávě. Datagramy jedné zprávy jsou přenášeny nezávisle na sobě a mohou putovat sítí v různém pořadí, přičemž doručení nemusí odpovídat pořadí ve zprávě. (Kolouch, 2016)

Podstatnou informací je, že pro komunikaci v síti potřebuje každý počítačový systém unikátní IP adresu. IP adresy mohou být přidělovány staticky (kdy je adresa manuálně přidělena počítačovému systému) nebo dynamicky (kdy je nová IP adresa přidělena automaticky na základě MAC adresy při připojení k síti). IP adresa slouží jako jeden z identifikátorů počítačového systému při komunikaci s ostatními počítačovými systémy a standardně není anonymní. (Dostálek, 2003)

V současnosti existují dvě verze IP

- IPv4 – Jedná se o první rozšířenou a stále nejpoužívanější verzi internet protokolu která využívá 32bitové adresy. Tyto adresy jsou psány dekadicky po jednotlivé osmici bitů.
- IPv6 – Tento nový internetový protokol byl vytvořen z důvodu nedostatku veřejných IPv4 adres a má délku 128 bitů, které jsou psány hexadecimálně. V této verzi protokolu byla odstraněna potřeba funkce překladu síťových adres. (Co je ti IP adresa? © 1994–2025)

2.4 MAC Adresa

MAC adresa je speciální identifikátor, který se skládá ze 48 bitů. Mac adresa se používá pro síťová zařízení a je využívána různými protokoly druhé vrstvy. MAC adresa se přiděluje při výrobě síťové karty a je proto také označována jako fyzická adresa. Každá přidělená MAC adresa je unikátní na celém světě, ale prakticky je možné ji zfalšovat za pomocí operačního systému Linux. Adresa je rozdělena na dvě poloviny kde první polovina identifikuje výrobce síťové karty a druhá polovina je jedinečným identifikátorem karty, který byl přidělen výrobcem. (Brooks et al., 2018)

3 KYBERNETICKÉ ÚTOKY

Kybernetické útoky jsou početnější více než v předchozích letech, a nejen díky většímu využívání počítačových serverů a samotných počítačů ve všech možných oborech na kterých se jejich uživatelé stali více závislí, ale také kvůli probíhající válce na Ukrajině. Každá firma už využívá počítačové servery pro své účely jako je například zálohování dat, provozování e-shopu a internetové bankovnictví. Většina z těchto útoků jsou zaměřené na servery s cílem získat data nebo je vyřadit z provozu. Jako další se využívají programy, které zablokují server nebo celý firemní systém a za jeho obnovu útočnici požadují peníze. Útoky cílí nejen na energetické společnosti, banky a vládní agentury, ale také na univerzity, zdravotnická zařízení a další subjekty ochrany obyvatelstva. (Kolouch a Bašta, 2019)

Útok na IT infrastrukturu je úmyslný čin útočníka nebo skupiny útočníků. K útokům na cizí servery a počítače používají svou IT technologii, a to k získání kritických informací nebo k poškození či deaktivaci počítačových systémů. Všechny tyto aktivity se konají v kyberprostoru. Aktivity ve formě kybernetických útoků přitom mohou být jednáním sociálního inženýrství s jediným cílem získat informace, nebo naopak s cílem omezit pomocí DoS nebo DDoS útoku funkčnost jednoho nebo více serverů. (Jirovský, 2007)

Kybernetický útok lze také definovat jako nezákonné jednání v kyberprostoru s cílem ublížit jiné osobě nebo skupině osob. „*Tato jednání nemusí mít vždy podobu trestného činu, podstatné je, že narušují běžný způsob života poškozeného. Kybernetický trestný čin musí být zároveň kybernetickým útokem, avšak ne každý kybernetický útok musí být trestným činem. Řadu kybernetických útoků je, i díky absenci trestněprávní normy, možné subsumovat pod jednání, které bude mít povahu správněprávního, či občanskoprávního deliktu, případně se nemusí jednat o jednání, které je postižitelné jakoukoli právní normou.“* (Kolouch, 2016)

3.1 DoS a DDoS útoky

Denial of service (dále jen DoS) je typ kybernetického útoku za účelem omezit uživatelům používání některých síťových služeb nebo znepřístupnit počítač a tím zamezit normální fungování daného zařízení. Pro tento typ útoku stačí vlastnit jeden počítač, a proto je velice oblíbený mezi útočníky. Útoky DoS se zaměřují na internetové služby, které mohou zahrnovat e-mail, webové stránky, internetové bankovnictví nebo jiné služby které závisí na dotčeném počítači nebo síti. Stavu odepření služby dochází ze dvou důvodů. V první možnosti se útočník snaží přetížit síť nebo aplikaci uživatele velkým objemem provozu což způsobí zpomalení nebo zhroucení systému. V druhé možnosti se útočník pokouší dosáhnout

zpomalení nebo zhroucení systému za pomocí posílání velkého množství paketů v nefunkčním formátu. (*Understanding Denial-of-Service Attacks*, © 2010–2025)

Distributed Denial of Service (dále jen DDoS) je efektivnější typ kybernetického DoS útoku. Hlavní rozdíl mezi těmito útoky je ten, že DDoS využívá celou síť napadených zařízení. Počítače v této síti jsou napadány bot malwarem a stávají se z nich zombie zařízení. Pomocí řídících serverů posílají přes zombie zařízení nežádoucí požadavky. Tato zařízení pak útočí na síťové prvky systému, které se potřebují připojit k internetu, webovým stránkám, serverům nebo databázím, dokud nedojde k přetížení systému. (*DDoS útok*, © 1992–2025)

Distributed Reflected Denial of Service (dále jen DRDoS), je typ distribuovaného DoS útoku, který využívá mechanismus odražení. Tento útok funguje tak, že útočník rozesílá podvržené požadavky na spojení na mnoho počítačových systémů, které na ně odpovídají. Tyto podvržené požadavky mají jako zdrojovou adresu uvedenou adresu oběti, což má za následek zahlcení oběti odpověďmi na tyto požadavky. Tím se mnoho počítačových systémů stává nevědomými účastníky útoku. (Kolouch, 2016)

Jako další typy DoS útoků existují:

Ping flood – Za pomocí Internet Control Message Protokol a nástroje Ping útočník zjistí, zda je zařízení připojené v síti. Po zjištění útočník posílá co nejrychleji velké množství zpráv, na které dané zařízení nezvládá odpovídat, a proto přestává správně fungovat.

SYN-flood – Útočník se pokouší zahlcovat svou oběť množstvím požadavků na navázání spojení. Cílový systém se snaží na požadavky odpovědět, ale útočník neodpovídá. Cílový počítačový systém čeká na finální potvrzení a drží pro toto spojení omezené zdroje. To může vést k vyčerpání systémových zdrojů a jeho selhání.

DNS flood – Útočník provádí útok, při kterém zasílá falešné DNS dotazy na DNS server z mnoha podvržených IP adres. Počet falešných dotazů je tak velký, že DNS server není schopen odpovídat včas a dochází k jeho zpomalení nebo dokonce k jeho zhroucení.

Falšování zdrojové adresy – Metoda nazývaná IP spoofing spočívá v úpravě zdrojové adresy odesílaných datových paketů. Tento postup umožňuje útočníkovi zesílit DoS útoky. Útočník používá tuto techniku tehdy, když nepotřebuje odpověď od cíle na svou žádost o navázání spojení, ale pouze chce cílový systém přetížit a zahlcovat ho tak, aby způsobil jeho výpadek. (Kolouch, 2016)

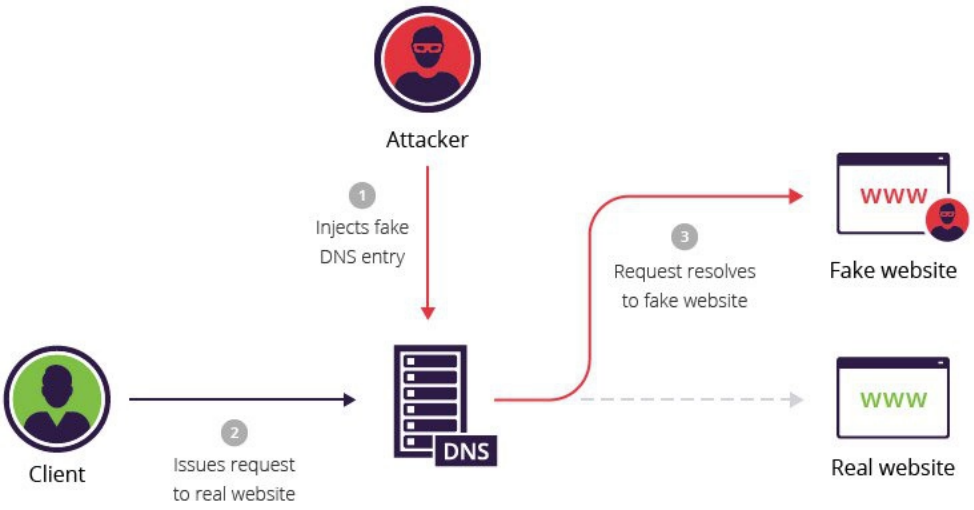
3.2 Spoofing útoky

DNS Spoofing – Domain Name Server (dále jen DNS) je typ kybernetického útoku který se zaměřuje na počítačovou bezpečnost při kterém útočník do vyrovnávací paměti DNS vloží poškozená data zaměněná za systémová data doménových jmen. Mezi primární strategii za použití tohoto typu kybernetického útoku patří tvorba falešných webových stránek, které působí na první pohled jako pravé nebo přímo napadení serveru dané společnosti a zfalšování přístupových cest do serveru.

DNS Server Compromise je první metoda založená na principu kompromitace serveru DNS tím získají nad serverovým procesem kontrolu a přesměrovávají uživatele na škodlivé webové stránky. Tato metoda je velmi nebezpečná z důvodu složité identifikace zaměněné webové stránky. Uživatelé jsou totiž natolik oklamáni pravostí dané domény až do té míry, že se na stránce přihlásí na svůj uživatelský účet čímž umožní útočníkovi zjistit jejich cenné informace jakožto přihlašovací údaje a další. Tuto metodu lze posílit o počítačové viry které se skrytě nainstalují uživateli do počítače a trvale dodávají útočníkovi přístup k zařízení a důležitým datům uživatele. (DNS Spoofing, © 2025)

Man in the Middle je druhá metoda založená na principu odposlouchávání komunikace mezi oběma komunikačními stranami. Útočník tajně čte danou komunikaci a získává citlivé informace, aniž by to žádná z odposlouchávaných stran nějak zjistila. Tato metoda využívá metody jako ARP spoofing a DNS spoofing aby útočník co nejefektivněji zachytil a oklamal komunikaci mezi uživatelem a severem. (Man-in-the-Middle (MITM), © 1992–2025)

Exploitong Time-To-Live Tato technika spoléhá na úpravu hodnoty TTL (Time-To-Live) v mezipaměti serveru DNS. Útočníci záměrně manipulují s těmito hodnotami, aby zajistili dlouhodobé uchování nesprávných DNS záznamů. Tím prodlužují dobu trvání útoku a rozšiřují počet potenciálních obětí. Dokonce i uživatelé, kteří nebyli původním cílem, mohou být přesměrováni na škodlivé webové stránky, pokud se falešné odpovědi DNS uchovají v mezipaměti. (DNS Spoofing, © 2025)



Obrázek 3 - Útok na DNS sever

Zdroj: (DNS Spoofing, © 2025)

Každá z těchto výše uvedených metod představuje vážné riziko pro integritu a bezpečnost DNS, což podtrhuje potřebu zavedení silné ochrany proti útokům typu DNS spoofing.

ARP Spoofing – Address Resolution Protocol (dále jen ARP) je protokol, který umožňuje síťové komunikaci dosáhnout konkrétního zařízení v síti. Protokol překládá adresy IP na adresy MAC a naopak. ARP uchovává tabulku, která propojuje IP adresy s odpovídajícími MAC adresami, a využívá se k navazování spojení se zařízeními v síti. Pokud hostitel nezná danou MAC adresu přiřazenou k určité IP adrese, vyšle ARP dotaz, kterým požádá ostatní zařízení v síti o poskytnutí správné MAC adresy. Když ARP obdrží dotaz tak neověřuje, zda pochází od správného odesílatele a tím otevírá možnosti pro spoofing útoky.

ARP spoofing je kybernetický útok který zachytává komunikaci mezi síťovými zařízeními a spadá pod metodu Man in the Middle. Tento útok funguje následovně:

Útočník se získaným přístupem do sítě prohledá síť a zjistí IP adresy alespoň dvou zařízení. Dále použije podvržený nástroj a odešle podvržené odpovědi ARP. Tyto podvržené odpovědi inzerují, že je správná MAC adresa pro obě adresy IP, patřící směrovači a pracovní stanici, je MAC adresa útočníka. Tím se směrovač i pracovní stanice oklamou a připojí se k útočníkovu počítači místo k sobě navzájem. Obě zařízení aktualizují své záznamy v mezipaměti ARP a od tohoto okamžiku komunikují s útočníkem místo přímo mezi sebou. Útočník je nyní skrytě uprostřed veškeré komunikace. (ARP Spoofing, © 2025)

3.3 Škodlivý software – Malware

Malware neboli škodlivý software, je termín, který označuje jakýkoli škodlivý program nebo kód, jenž infikuje a poškozuje zařízení. Tento software se může do zařízení dostat prostřednictvím sociálních sítí nebo e-mailových zpráv. Škodlivý malware má za cíl narušit a poškodit počítače, systémy, sítě, tablety a mobilní zařízení, často tím, že částečně přebírá kontrolu nad jejich fungováním a ovlivňuje jejich normální provoz. (Kolouch a Bašta, 2019)

Tento škodlivý software je vytvořen s cílem generovat zisk, narušit uživatelskou pracovní činnost, vyjádřit politické názory nebo se jednoduše chlubit odcizenými osobními informacemi. I když malware nemůže přímo poškodit fyzický hardware daného zařízení nebo síťové prvky, může ukrást data, šifrovat je, mazat, upravovat nebo napadat základní funkce počítače a špehovat uživatelskou aktivitu bez jakéhokoliv vědomí. (Malware, © 2025)

Dělení podle šíření

- Virus – Tento škodlivý program se s pomocí člověka dostane do počítače, kde kopíruje sám sebe do ostatních souborů a provádí škodlivou činnost.
- Počítačový červ – Tento škodlivý program má stejné chování jako virus jen pro své šíření hledá chyby v softwaru.
- Trojský kůň – Tento škodlivý program se schovává v uživateli již ověřeném programu. Při infikování systému okamžitě působí škody a uděluje útočníkovi vzdálený přístup.

Dělení podle efektu

- Spyware – Tento škodlivý program bez vědomí krade a ukládá si důvěrné informace o uživateli a následně je zasílá útočníkovi.
- Adware – Tento škodlivý program posílá nežádoucí reklamy, ze kterých generuje zisky, které posílá tvůrci programu.
- Keylogger – Tento typ škodlivého program zaznamenává konkrétní stisky kláves na napadeném počítači. Využívá se ke zjištění přihlašovacích údajů.
- Cryptojacking – Pomocí škodlivého programu útočník těží na infikovaném zařízení kryptoměny.

- Wiper – Tento typ škodlivého programu je navržený tak aby kompletně zničil nebo poškodil data v cíleném systému. (Kolouch, 2016)

3.4 Vyděračský software – Ransomware

Ransomware spadá do kategorie malware podle jeho efektu. Vzhledem k jeho závažnosti je důležité se mu věnovat podrobněji. Jedná se o typ škodlivého softwaru, který blokuje přístup uživatelům k jejich zařízením, osobním souborům, počítačům, tabletům a telefonům. Útočníci za obnovení přístupu požadují výkupné, obvykle ve formě platby kreditními kartami nebo převodem kryptoměny. Tento druh malwaru patří mezi nejrozšířenější a nejvážnější kybernetické hrozby současnosti, které útočníci cíleně využívají. Jsou zaměřeni na jednotlivce, firmy i různé organizace. (Ransomware, © 2025)

- Diskcoder – Zabraňuje uživateli používat operační systém tím, že blokuje záznamy z pevného disku.
- Screen locker – Zablokuje uživateli přístup k hlavní obrazovce.
- PIN locker – Zablokuje uživateli přístup tím, že vytváří falešný PIN kód.
- Kryptografický ransomware – Blokuje uživateli přístup k datům pomocí šifrování. (Ransomware, © 1992–2025)

3.5 Doplňující typy útoků na sítě

Zero Day útok – Tato metoda kybernetického útoku využívá chyby v systému, které pro vývojáře ještě neexistují, a tudíž neexistuje žádná obrana vůči těmto útokům. Útočnici využívají chyb v programátorském kódu a snaží se infikovat systém. K tomu může útočník využít spyware, ransomware, malware, keylogger nebo trojského koně. Tyto škodlivé programy mohou vést k úniku dat, jejich poškození nebo dokonce k úplnému převzetí a ovládnutí cílového zařízení či systému. (Zero day útok, © 1992–2025)

Sniffing – Metoda sniffing je velice specifická technika, jenž umožnuje odposlouchávání počítačů v lokální síti. Tato metoda umožnuje čtení a ukládání TCP paketů. Využívá se zejména při diagnostice sítě, zjištění používaných služeb a protokolů a odposlechu datové komunikace.

Firemní zaměstnanec ale i jiný útočník který má přístup do vybraného podniku může na výhodné místo umístit odposlouchávací zařízení čímž se mu do rukou dostanou používaná hesla pro přístup k celé síti. Útočník potom může nabourat firemní komunikaci

a zjistit hodnotné informace které mohou být následně užitečné při nasazení botnetu, síťového červa nebo DDoS.

Pro síťový odposlech je primárně využíváno softwarové vybavení s názvem sniffer. Tato technologie je upravovaná a vylepšovaná samotnými útočníky pro zlepšení rychlosti a efektivity. (Co je sniffing, © 2022)

Phishing je typ kybernetického útoku, který využívá techniky sociálního inženýrství, pomocí kterých se útočník snaží získat důvěrné informace ze zařízení nebo na něm spustit škodlivý kód. Nejzákladnější formou těchto útoků jsou podvodné e-maily požadující informace o platební kartě nebo záznamy internetového bankovnictví. Útočníci se nejčastěji vydávají za již známe firmy, ke kterým mají oběti důvěryhodný vztah. V e-mailu pak už jen stačí otevřít falešný odkaz a vyplnit přístupové údaje. Výjimkou ale nejsou ani chatovací aplikace a sociální sítě. (Phishing, © 1992–2025)

Insider threat patří mezi závažnější typy kybernetických útoků. Škodlivou aktivitu z pravidla provádí osoba s oprávněným přístupem k počítačovým systémům, nejčastěji se jedná o zaměstnance, dodavatele nebo bývalého pracovníka, jehož přístupové údaje pořád fungují. Tento typ hrozby je obzvlášť nebezpečný právě proto, že zasvěcená osoba dobře zná interní prostředí organizace a případné slabiny systému.

Útoky tohoto druhu nemají vždy jednotný průběh, ale často je spojuje podobná motivace chamtivost, zlomyslnost, osobní nespokojenost, nebo i prostá neopatrnost. Útočník může při své činnosti využít škodlivý software, různé metody sociálního inženýrství nebo techniky pro získání a zneužití citlivých dat, které má daná organizace k dispozici. (Fujak, 2022)

4 MONITORING SÍTĚ

S rostoucím využíváním síťových technologií v malých, středních a velkých podnicích je monitoring sítě důležitou součástí pro zachování firemní bezpečnosti. Počítačová síť zaujímá v moderním světě standard pro veškeré firmy a podniky. Stabilní a funkční síť je nepostradatelnou součástí pro plynulé fungování daného podniku a její narušení může znamenat velkou ztrátu integrity a důvěry mezi osobami, které s podnikem přichází do styku.

Monitoring sítě je využíván k neustálému sledování dostupnosti a aktuálního stavu sítě a možných aktivních komponentů, které jsou součástí sítě. Pro důkladnou zprávu sítě je tato metoda velmi důležitá a také pomáhá IT specialistům tím, že je včas informuje o problémech a možných výpadcích ještě předtím, než je zaznamenají samotní uživatelé. Mezi další přínosy patří snížení provozních nákladů a prevence finančních ztrát způsobených výpadky systému. (Co je monitoring sítě a proč ho používat, © 2021)

Mezi účinné metody, jak předcházet těmto problémům v počítačové síti patří kvalitně provedená diagnostika sítě za pomocí techniky čtení a ukládání TCP paketů nebo zpracování záložního scénáře známého jako Disaster Recovery Plan který je klíčovou součásti řízení kontinuity podnikání. Tyto metody spolu s dostatečně zabezpečenou počítačovou sítí dokážou pomoci subjektům odolat kybernetickým útokům a nepřijít o citlivá data. (Co je to monitoring sítě, © 2022)

Mezi nejčastější důvody pro používání softwarů na monitorování sítě patří:

- Rychlá identifikace problému a následná analýza.
- Včasná identifikace nedostatků k jejich odstranění.
- Identifikace oblastí pro aktualizaci.
- Přehledný seznam zpráv o průběžném stavu.
- Zabezpečení nepřetržitého provozu. (Co je monitoring sítě a proč ho používat, © 2021)

Správci sítě pro monitoring využívají různé systémy pro monitorování. Tyto systémy zahrnují různé hardwarové a softwarové nástroje které pomáhají sledovat provoz sítě a její aspekty. Mezi hlavní aspekty patří provoz, využití šířky pásma a doba daného provozu. Monitorovací systémy mohou dále detekovat možná zařízení a prvky, které pomáhají tvořit síť nebo se různými způsoby sítě dotýkají, poskytují také aktuální informace o stavu.

Správci využívají monitorovací systémy k rychlému odhalení poruch zařízení, připojení nebo problémů, jako jsou přetížené úseky omezující tok dat. Možnost identifikace potíží nyní zahrnuje i části sítě, které dříve ležely mimo jejich přímou správu. Tyto systémy mohou administrátory informovat o problémech prostřednictvím e-mailu či textových zpráv a poskytovat detailní analýzu sítě. (Co je monitorování sítě? © 2025)

4.1 Síťové monitorovací protokoly

Protokoly pro správu sítě tvoří soubor standardů, které definují zásady a postupy usnadňující údržbu a sledování zařízení v síti. Tyto protokoly propojují monitorovací software s jednotlivými síťovými zařízeními a umožňují efektivní sledování sítě v reálném čase.

Díky síťovým protokolům lze získat podrobné informace o aktivitách v síti, jako je dostupnost zařízení, ztráta paketů, latence nebo síťové zpoždění. Mezi klíčové úlohy těchto protokolů patří detekce, monitorování, mapování, upozorňování a generování zpráv. Mezi nejčastěji používané protokoly patří SNMP a Internet Control Message Protocol (ICMP), z nichž vycházejí i další protokoly.

Simple Network Management Protocol (SNMP) tento síťový protokol se nachází na aplikační vrstvě a pomáhá při přenosu dat mezi zařízeními, čímž kontroluje odezvu mnoha typů zařízení přítomných v síti. Tento protokol lze také použít ke konfiguraci a sledování stavu systému.

Internet Control Message Protocol (ICMP) V informatice patří mezi klíčové protokoly používané v počítačových sítích, které jsou postaveny na sadě protokolů TCP/IP. Tento protokol využívají síťové komponenty, například směrovače a servery k předávání informací o provozu v síti IP a k vytváření chybových hlášení při poruše zařízení.

Cisco Discovery Protocol (CDP) slouží k výměně informací o dalších přímo připojených zařízeních Cisco, například o verzi jejich operačního systému nebo IP adrese. Tento protokol lze také využít pro směrování na vyžádání, což znamená, že směrovací údaje jsou zahrnuty v oznámeních CDP. Díky tomu není v jednodušších sítích nutné nasazovat dynamické směrovací protokoly. (Co je monitorování sítě? © 2025)

4.2 Zabezpečení sítě

Síťové zabezpečení zahrnuje soubor pravidel a opatření, která mají za cíl chránit síť před neoprávněným přístupem, zneužitím nebo změnami v datech. Správce sítě je odpovědný za kontrolu přístupu a zajištění bezpečnosti informací v síti. Přístup k síti je řízen prostřednictvím unikátních identifikačních údajů, jako je uživatelské jméno nebo heslo. Tímto způsobem správce určuje, kdo má oprávnění přistupovat k určitým informacím a aplikacím. Pravidla pro přístup mohou být přizpůsobena různým požadavkům a úrovním bezpečnosti. (Sedlák a Konečný, 2021)

Zabezpečení sítě se vztahuje jak na soukromé sítě (například v domácnostech či firmách), tak na veřejné sítě (například Wi-Fi v restauracích nebo kavárnách). Tyto sítě vyžadují odlišné úrovně ochrany, přičemž veřejné sítě bývají vystaveny větším rizikům. Nejdůležitější a nejběžnější metodou ochrany sítě je její uzamčení pomocí hesla.

Tímto způsobem mají přístup pouze ti uživatelé, kteří znají správné přihlašovací údaje, což pomáhá minimalizovat možnost neoprávněného přístupu a ochranu sítě před zneužitím. Tyto zabezpečovací metody nemusí být vždy dostačující, a proto je pro lepší zabezpečení jak soukromé, tak i veřejné sítě důležité využívat různé služby a softwary které zlepší ochranu sítě a zamezí útočníkům odcizit citlivé informace. (C. van Oorschot, 2021)

4.3 Metody zabezpečení sítě

Zabezpečení sítě vyžaduje dodržovaní řady postupů a metod, aby se zabránilo cizímu zneužití citlivých dat, které obsahují firemní nebo soukromé servery. Mezi nejzávažnější ohrožení těchto dat patří lidská nepozornost při údržbě a manipulaci s operačním systémem nebo s různými softwary. Existuje několik efektivních metod pro zabezpečení počítačové sítě, které pomáhají chránit data, zařízení a síťové prostředí před útoky a neoprávněným přístupem. Většina z těchto metod slouží k zabezpečení sítě před kybernetickými útoky, ale také existují metody, které pomáhají eliminovat lidský faktor a díky tomu je možné odolávat známým útokům nebo i přírodním haváriím.

Firewall – je klíčovým prvkem bezpečnostní infrastruktury, který se využívá již dlouhou dobu. Tato technologie umožňuje nastavit filtry, které regulují síťový provoz tím, že určují, jaká komunikace je povolena a která naopak blokována. Firewall může chránit síť jak před vnějšími hrozbami z internetu, tak i řídit přenos dat uvnitř samotné sítě. (Síťová ochrana (VPN, FW, GW, SD-WAN), © 2025)

Intrusion Detection Systém (IDS) – je systém navržený, aby detekoval neautorizované připojení k síti a možný nežádoucí provoz. Používá se k monitorování sítě a na základě předem stanovených vzorců detekuje známé i neznámé kybernetické útoky. Tento systém se primárně používá k detekci DoS útoků, skenování sítě a různých typů proniknutí do sítě.

Intrusion Prevention Systém (IPS) – je vylepšená verze IDS systému. IPS se nejen používá k detekci útoků, ale také může aktivně reagovat na vzniklé hrozby. Pomocí nastavených opatření může automaticky podnikat kroky k zastavení nebo omezení nežádoucího provozu. K minimalizaci rizik úspěšného útoku blokuje nežádoucí provoz, nežádoucí snahy o připojení k síti a také může upravovat pravidla sítě. (IDS/IPS: Ochrana sítě před hrozbami a útoky, © 2004–2025)

Šifrování – je proces při kterém se využívají různé metody kryptografie, tyto metody dokážou zabezpečit citlivá data pomocí šifrovacího klíče který data přepíše pomocí šifrovacích algoritmů. Tato data jsou díky tomu dostatečně chráněná před čtením od cizího uživatele, který k nim nemá mít přístup. Zašifrovaná data dokáže přečíst jen majitel dešifrovacího klíče který je přímo určen k dešifraci daného objemu dat. (Burda, 2019)

Antivirový program – tyto softwarové nástroje slouží k rozpoznání, odstranění a likvidaci počítačových virů a dalšího škodlivého softwaru, který se může do systému dostat záměrně nebo neúmyslně při používání internetu. Programy prověřují soubory uložené na disku i operační paměť a sledují podezřelé aktivity různých aplikací, které uživatel využívá. Pokud objeví infikované soubory, pokusí se je opravit odstraněním počítačového viru nebo odstraní kompletní soubor.

Endpoint detection and response (EDR) – tato bezpečnostní technologie monitoruje koncová zařízení jako jsou notebooky, stolní počítače a telefony. Pomocí aktivního sledování hrozeb v reálném čase odhaluje nežádoucí aktivity a anomálie lépe než běžný antivirový program. Díky funkcím jako vyhledávání hrozeb, vyšetřování incidentů a detailních analýz pomáhá IT pracovníkům okamžitě reagovat na hrozby. SentinelOne Singularity Endpoint je nástroj, který poskytne lepší zabezpečení s pomocí této technologie.

Networ detection and response (NDR) - je technologie určená k monitorování sítě a odhalování hrozeb v síťové infrastruktuře. Díky analýze dat a síťového provozu identifikuje nežádoucí vzorce v síti. NDR také dokáže detekovat nežádoucí pohyb útočníka po síti, když útočník k získaní přístupu k účtům využije jiné účty. Za pomocí sledování komunikace mezi zařízeními, servery a aplikacemi dokáže odhalit potenciální hrozby.

Extended detection and response (XDR) – sjednocuje více bezpečnostních nástrojů do jedné platformy. Pomocí integrace dat z dalších bezpečnostních vrstev jako jsou koncová zařízení, sítě, cloud, e-maily a aplikace dokáže zajistit kompletní přehled a automatickou reakci na hrozby v celé infrastruktuře organizace. Díky komplexnímu pohledu na bezpečnostní pokrytí XDR překonává možnosti EDR a NDR a je ideálním řešením pro zajištění IT bezpečnosti. (EDR vs NDR vs XDR, © 2025)

Autentizace a kontrola přístupu – autentizační metody využívají různé postupy nebo softwary, které zajišťují, že do určité sítě mají přístup jenom autorizovaní uživatelé s povoleným přístupem od správce sítě. Tyto metody mohou zahrnovat přihlašovací údaje, biometrické údaje nebo identifikační karty. (Síťová ochrana (VPN, FW, GW, SD-WAN), © 2025)

Virtuální privátní síť – využívání virtuální privátní sítě (VPN) pomáhá zabezpečit komunikaci mezi zařízením a serverem pomocí šifrování internetového provozu. Tato metoda zajišťuje bezpečnou komunikaci, zejména při využívaní veřejných nebo nechráněných Wi-Fi sítí a umožnuje bezpečné přistupovat k firemním serverům. (Co to je VPN a proč si ji pořídit? © 1992–2025)

Zálohování dat – Pravidelné provádění zálohy důležitých dat je klíčové při ochraně firmy nebo vlastního soukromí před možnou ztrátou dat v důsledku kybernetického útoku. Při kvalitní záloze není možné, aby se nadobro ztratila nebo byla zneužita jakákoliv citlivá data, která jsou pro firmu nebo běžného uživatele příliš cenná. Pro zálohu dat lze využít externí úložiště jako hard disk nebo flash disk. Obě tato zařízení je možné dále chránit pomocí hesla. (Hendl, 2021)

5 DÍLČÍ ZÁVĚR

Teoretická část této diplomové práce byla věnována popisu základních oblastí kybernetické bezpečnosti a problematiky informačních technologií. Byly vymezeny nejčastější typy kybernetických útoků, které se využívají při konfrontaci počítačových systémů a specializují se na krádež citlivých dat uživatelů. Součástí teoretické části je mimo jiné popis právního rámce, který vymezuje nejdůležitější zákony a prováděcí vyhlášky z oblasti kybernetické bezpečnosti a monitoringu sítí. Hlavní součástí teoretické části je problematika monitoringu počítačových síti, kde byly uvedeny síťové protokoly a proč je monitorování důležité pro zajištění bezpečnosti sítě v subjektu. Také byly popsány nejvyužívanější metody, které pomáhají správcům sítě se zajištěním bezpečnosti. Spousta běžných uživatelů informačních technologií ani nevyužívá základní zabezpečovací systémy anebo je neumějí správně nakonfigurovat, a proto je potřeba informovat každého kdo přijde do styku s těmito technologiemi o možnostech lepšího zabezpečení.

II. PRAKTICKÁ ČÁST

6 SOFTWARY PRO MONITORING POČÍTAČOVÝCH SÍTÍ

Software pro sledování sítě slouží jako nástroj pro kontrolu a řízení výkonu, dostupnosti a provozu počítačové sítě. Díky nepřetržitému monitorování síťového provozu a stavu jednotlivých zařízení umožňuje získat přehled o fungování sítě a pomáhá správcům zajistit její efektivní a spolehlivý provoz. Tento software se obvykle instaluje na sdílený server v rámci zákaznické sítě, avšak stále větší oblibě se těší také cloudová monitorovací řešení.

Síťové monitorovací nástroje se dělí do těchto 4 kategorií.

Sledování výkonnosti – Monitoring výkonu sítě je proces zaměřený na kontrolu kvality a efektivity jejího provozu. Nástroje určené k monitorování výkonu nabízejí správcům sítě komplexní přehled, díky kterému mohou včas rozpoznat počínající problémy a přijmout opatření k jejich odstranění dříve, než ovlivní fungování sítě.

Tento typ monitorování sítě zahrnuje analýzu aktuálních i historických metrik, mezi něž patří využití šířky pásma, ztráta paketů, latence a doba odezvy. Cílem je zajistit, aby síť fungovala na optimální úrovni a byla schopna efektivně reagovat na požadavky uživatelů.

Nástroje pro sledování výkonu síťových zařízení obvykle využívají metody jako Simple Network Management Protokol (dále jen SNMP), protokoly událostí, syslog spouštěče, monitorování toku dat, analýzu zachycených paketů a streamování telemetrických dat.

Sledování dostupnosti – Cílem monitorování dostupnosti, známého také jako monitorování chyb, je pomoci zajistit nepřetržitou dostupnost síťových zdrojů a infrastruktury. Nástroje pro tento typ monitorování umožňují v reálném čase detekovat různé problémy – od hardwarových selhání, například nefunkčního routeru, až po softwarové chyby, jako jsou výpadky kritických webových aplikací nebo potíže s připojením.

Typickým příkladem je neustálé odesílání ICMP pingů na klíčová síťová zařízení a servery k ověření jejich dostupnosti. Další metodou je využití SNMP trapů, které upozorňují na změny stavu síťových zařízení, například zda je rozhraní aktivní nebo nefunkční.

Nástroje pro monitorování dostupnosti obvykle zahrnují výstražné mechanismy, které informují administrátory o problémech prostřednictvím e-mailů, SMS, vizuálních upozornění na řídicím panelu nebo jinými způsoby.

Sledování provozu – Software pro monitoring síťového provozu analyzuje datové toky v síti, aby správcům poskytl přehled o tom, kdo síť využívá a k jakému účelu. Zajišťuje také monitorování šířky pásma, tedy měření objemu a rychlosti přenášených dat, což pomáhá optimalizovat výkon sítě a předcházet jejímu přetížení.

Nástroje pro trasování sítě usnadňují diagnostiku problémů analýzou přenášených paketů, čímž pomáhají identifikovat zdroje síťových potíží nebo zpomalení provozu.

Bezpečnostní monitorování – Monitorování bezpečnosti sítě je klíčové pro ochranu integrity, dostupnosti a důvěrnosti dat i dalších IT zdrojů, a zároveň pomáhá minimalizovat náklady spojené s bezpečnostními incidenty. (Nástroje pro monitorování sítě, © 2004–2025)

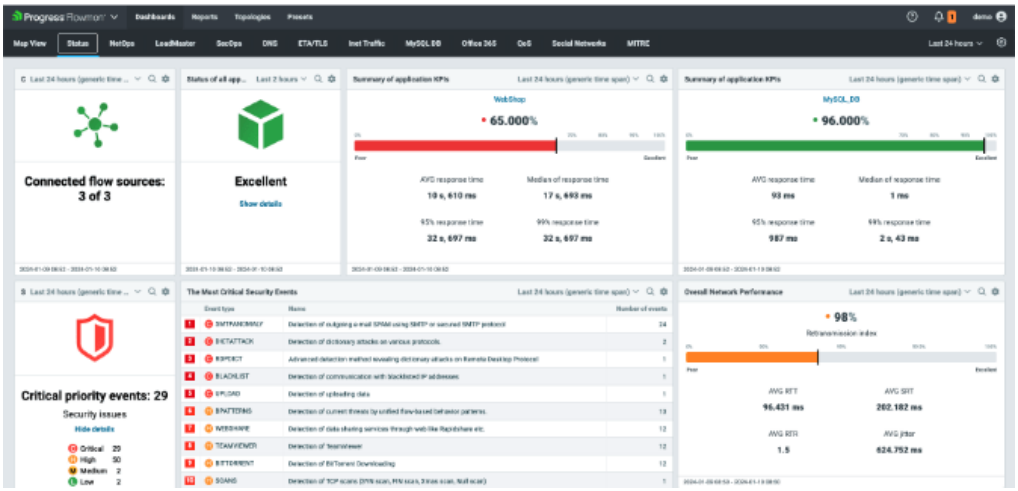
Na trhu existuje široká škála bezpečnostních nástrojů, mezi které patří:

- Nástroje síťového protokolování – shromažďují, ukládají a analyzují protokolová data z různých síťových zařízení, čímž poskytují podrobný přehled o veškerých síťových aktivitách.
- Software pro detekci sítě – sleduje síťový provoz v reálném čase a identifikuje možné hrozby či škodlivé aktivity, umožňující okamžitou reakci.
- Software pro řízení sítě – pomáhá organizacím spravovat a kontrolovat síťové operace, zajišťuje povolení pouze autorizovaných akcí a kontroluje, zda jsou opravené potenciální zranitelnosti.
- Software pro sledování sítě – důkladně monitoruje síťové aktivity, aby zajistil soulad s bezpečnostními zásadami a včas detekoval podezřelé či neoprávněné činnosti.
- Monitorování síťových zařízení – sleduje nežádoucí změny v konfiguraci zařízení, například v ACL nebo pravidlech firewallu, které mohou negativně ovlivnit funkčnost sítě nebo ji dokonce zcela vyřadit z provozu.

Kombinací těchto nástrojů lze vytvořit bezpečnostní rámec, který pomáhá udržovat síťové prostředí bezpečné a efektivní.

6.1 Progress Flowmon

Program flowmon je bezpečnostní nástroj sloužící k monitorování počítačové sítě, který se zaměřuje na analýzu síťového provozu pomocí technologie flow-based monitoring. Je vyvíjen společností Flowmon Networks která vznikla v roce 2007. Další produkty jakožto i tento software slouží k monitorování síťového provozu, analýzy sítě, řízení výkonosti a ochranu sítě před DDoS útokem. Primárně jsou tyto softwary určeny pro správce sítí, kteří patří mezi podnikové specialisty v oboru bezpečnosti. (Řešení Flowmon, ©2025)



Obrázek 4 - Platforma Progress Flowmon

(Zdroj: Řešení Flowmon, ©2025)

Přímo software Flowmon je pokročilá platforma pro monitorování a zabezpečení sítě, která využívá umělou inteligenci k detekci hrozeb a anomálií. Poskytuje rychlý přehled o výkonu vaší sítě a aplikací. Platforma nabízí 30denní zkušební lhůtu nebo také testovací demo, aby si každý zákazník mohl sám vyzkoušet, jak funguje a co nabízí.

Monitorování a analýza síťového provozu

- Poskytuje detailní přehled o síťové komunikaci tím, že shromažďuje a vyhodnocuje síťové toky.
- Pomáhá identifikovat provozní problémy a optimalizovat výkon infrastruktury.

Detekce hrozeb pomocí AI

- Flowmon využívá strojové učení k rozpoznávání bezpečnostních incidentů.
- Upozorňuje na DDoS útoky, malware, podezřelé chování v síti nebo laterální pohyb útočníků.

Přehled o výkonu aplikací

- Sleduje klíčové metriky, například latenci a ztrátovost paketů.
- Rychlá odezva o problémech.

Podpora různých IT prostředí

- Umožňuje monitorování nejen lokálních sítí, ale také cloudových platforem.
- Zajišťuje kontrolu na více sítích a mobilních zařízeních.

Automatizace a integrace

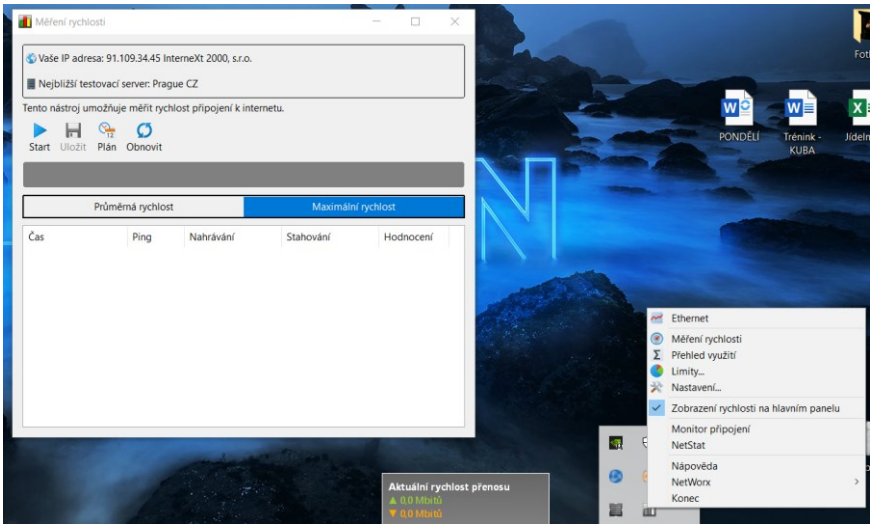
- Snadno se propojuje s platformami SIEM a dalšími bezpečnostními nástroji.
- Nabízí automatické generování reportů a upozornění na neobvyklé aktivity. (Řešení Flowmon, ©2025)

Díky těmto vlastnostem je Progress Flowmon spolehlivým řešením pro firmy, poskytovatele služeb i státní organizace, které chtějí zajistit výkonnou a bezpečnou síťovou infrastrukturu.

6.2 NetWorx

Program NetWorx je univerzální nástroj určený k monitorování internetového připojení. Umožňuje sledovat využití dat, kontrolovat kvalitu připojení a měřit jeho rychlost. Pomáhá také s odhalováním síťových problémů, hlídáním datových limitů poskytovatele a identifikací podezřelé aktivity v síti.

Díky NetWorx lze monitorovat síťový adaptér na osobním zařízení, routeru nebo sledovat, které aplikace na počítači se připojují k internetu. Uložené statistiky o využití připojení jsou přehledně tříděny do denních, týdenních a měsíčních reportů. Aktuální síťová aktivita je vizualizována v přizpůsobitelném grafu doplněném o seznam aktivních aplikací. (NetWorx, © 2000–2025)



Obrázek 5 - Program NetWorx (Měření rychlosti)

(Zdroj: Vlastní)

Integrovaný test rychlosti internetu lze spustit manuálně nebo naplánovat na určitý čas, což pomůže ověřit, zda vlastník internetu skutečně dosahuje poskytované rychlosti. Kromě toho monitor připojení sleduje výpadky a měří dobu odezvy v průběhu dne.

Funkce programu

- Historické přehledy využití připojení podle dne, týdne a měsíce.
- Podrobné sledování odesílaných a přijímaných dat v reálném čase.
- Monitorování aplikací připojených k internetu.
- Podpora místních síťových adaptérů a vzdálených zařízení přes SNMP a UPnP.
- Možnost nastavení akcí při překročení určité úrovně síťové aktivity.
- Test rychlosti internetu pro měření výkonu připojení.
- Monitor připojení pro pravidelnou kontrolu stavu připojení. (NetWorx, © 2000–2025)

Program NetWorz je velmi užitečný pro běžné, ale i pokročilé uživatele internetového připojení. Díky stabilnímu a nepřetržitému monitoringu dokáže včas identifikovat různé problémy tykající se internetu v domácnosti nebo na pracovišti.

6.3 LogicMonitor

LogicMonitor je platforma sloužící k monitorování síťové infrastruktury založená na konceptu software jako služba. Tato platforma poskytuje vlastníkovi sledovat počítačovou síť, servery, cloudové služby a aplikace. Tyto komponenty lze kontrolovat a analyzovat v reálném čase, což poskytuje uživateli kompletní přehled o výkonu a stavu celého technologického prostředí. (What is LogicMonitor, © 2025)

Obrázek 6 – Platforma LogicMonitor

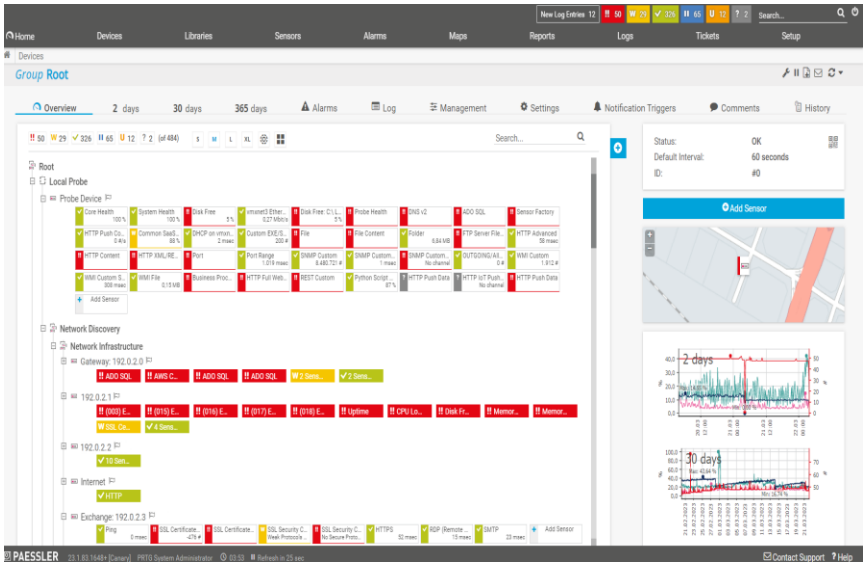
(Zdroj: All MS Windows Devices, © 2025)

Tato monitorovací platforma vyniká automatickou detekcí s možností monitorovat zařízení během několika minut po připojení. Platforma generuje dynamické topologické mapy, které zobrazují vzájemné propojení klíčových zdrojů. Pomocí umělé inteligence a vývojové metody strojového učení nabízí pokročilé funkce, jako je detekce anomálií, prediktivní analýzy a včasné upozornění. S přizpůsobitelnými řídicími panely, přednastavenými výstrahami a možnostmi integrace usnadňuje správu IT, snižuje provozní náklady a sjednocuje nástroje. (What is LogicMonitor, © 2025)

Díky výkonnému a rychlému nasazení je LogicMonitor podobně jako Progress Flowmon spolehlivým nástrojem pro IT specialisty ve firmách, kteří chtějí výkonnou pomůcku při zabezpečení firemní počítačové sítě.

6.4 PRTG Network Monitor

Tento nástroj vyvinutý společnostní Paessler GmbH pomáhá, aby počítačové systémy fungovaly správně bez zbytečných chyb a výpadků v síti. Díky nepřetržitému monitoringu sítě dokáže tento software včas identifikovat možné anomálie a upozornit včas vlastníka na nacházející se problém. Upozornění o hrozbě lze dostat emailem nebo SMS zprávou kdekoliv a kdykoliv. Software PRTG také sbírá data od dalších připojených zařízeních na síti jako jsou různé počítače, tablety, telefony a směrovače. K těmto zařízením umí zobrazit grafické statistiky a protokoly o objemu přenesených dat. Freeware verze navíc obsahuje přes 100 typů senzorů, které umožňují monitorovat TCP/IP připojení, databáze, HTTP obsah, běžné internetové protokoly ale i vlastní senzory. (Co je PRTG a k čemu se používá? © 2020)



Obrázek 7 – Platforma PRTG Network Monitor

(Zdroj: Device Tree View Layout, © 2025)

Základní funkce softwaru

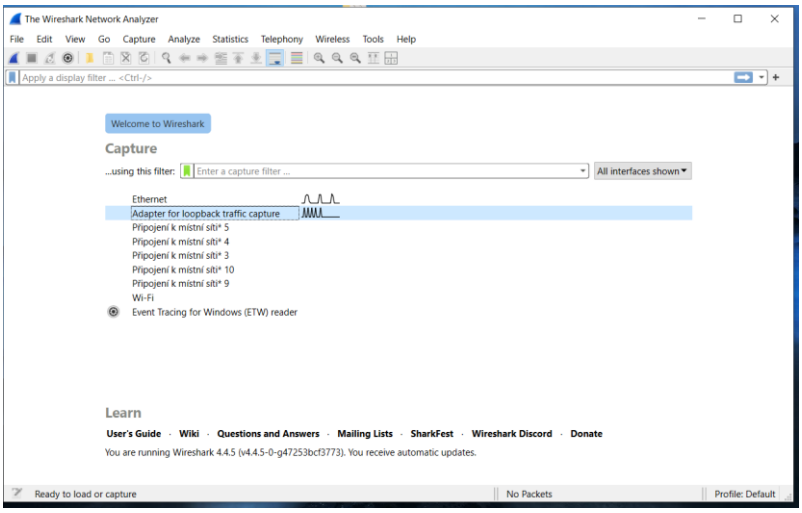
- Monitorování aktivity v síti a doby provozu.
- Podporuje sledování více sítí či umístění v rámci jedné licence.
- Možnost automatické konfigurace senzorů a sítě.
- Kompatibilita s různými typy operačních systémů.
- Obsahuje senzory pro monitorování virtuálních prostředí.

- Obsahuje předpřipravené šablony pro zařízení s OS, routery, switche, SQL servery, síťové tiskárny, NAS a další. (Co je PRTG a k čemu se používá? © 2020)

PRTG Network Monitor díky nepřetržitému dohledu nad sítí pomáhá předcházet výpadkům a zajišťuje plynulý provoz. Pomocí senzorů a kompatibilitě s různými systémy je vhodný jak pro menší podniky, tak pro rozsáhlé korporátní sítě. Automatická konfigurace a uživatelsky přívětivé rozhraní umožňují snadné nastavení i méně zkušeným uživatelům, čímž usnadňují efektivní správu a dohled nad celou sítí.

6.5 Wireshark

Počítačový program Wireshark se používá pro analýzu a odstraňování chyb v počítačových sítích. Dále program slouží ke studiu síťové komunikace a vývoji protokolů určených ke komunikaci po síti. Projekt byl zahájen v roce 1998 a dodnes patří mezi nejrozšířenější nástroje pro monitorování sítí. Je napsán v programovacích jazycích (C, C++). Tento multiplatformní software s intuitivním uživatelským rozhraním podporuje přibližně stovku analyzátorů síťových protokolů a formátů. Wireshark je volně ke stažení a lze jej využívat v základním balíčku na různých operačních systémech jako Linux, Mac, Solaris a Microsoft Windows. (About Wireshark, ©2025)



Obrázek 8 - Program Wireshark

(Zdroj: Vlastní)

Funkce programu

- Monitorování síťové komunikace v reálném čase a generování souhrnné statistiky.
- Analyzování online i offline provozu.
- Zachytávání paketů z různých síťových rozhraní (Wi-Fi, Ethernet, VPN, Bluetooth).
- Možnost použití filtrů pro snazší identifikaci paketů podle (IP adres, portů), barevné zvýrazňování paktů, vyhledávání v zachycených datech (IP a MAC adres).
- Bohatá analýza VoIP
- Zachycované komprimované soubory lze dekomprimovat za běhu.
- Živá data lze číst z Ethernetu, Bluetooth, USB a dalších.
- Podpora dešifrování pro mnoho protokolů, WPA/WPA2.
- Na seznam paketů lze použít pravidla barvení pro rychlou a intuitivní analýzu.
- Výstup lze exportovat do různých formátů (CSV, XML)
- Podpora automatizace a vytváření skriptů. (About Wireshark, ©2025)

Wireshark je výborný nástroj pro zkoumání síťového provozu, ale není bez omezení. Nehodí se pro nepřetržité sledování sítě, obtížně analyzuje šifrovanou komunikaci a práce s velkým množstvím dat může být složitá. I přes tyto nevýhody patří mezi nejúčinnější nástroje využívané síťovými specialisty, etickými hackery a správci IT.

Vyhodnocení použitelnosti programů v subjektu ochrany obyvatelstva

Na základě výše uvedených programů pro monitorování sítě byla vytvořena komparační tabulka, která poskytne užitečné informace pro jakýkoliv subjekt ochrany obyvatelstva při výběru softwaru pro monitoring sítě.

Tabulka 1 – Výhody a nevýhody zkoumaných softwarů

Nástroj	Výhody	Nevýhody
Wireshark	- Detailní analýza síťového provozu s možností ukládání - Podpora stovky protokolů - Filtrování, barvení paketů, export - Open-source	- Nevhodný pro nepřetržitý monitoring - Slabší práce se šifrovanou komunikací - Může být náročný na orientaci ve velkém množství dat
PRTG Network Monitor	- Intuitivní rozhraní - Monitoring v reálném čase - Podpora SNMP, ping - Grafy, mapy, e-mail/SMS notifikace	- Omezený počet senzorů v bezplatné verzi - Vyšší cena u lepších balíčků s více senzory - Závislost na Windows serveru
Progress Flowmon	- Detailní přehled sítové komunikace a analýza toků - Detekce síťových anomálií a hrozeb za pomocí AI - Integrace s SIEM platformami	- Vysoká cena - Vyžaduje nasazení sond do sítě - Komplexnější správa (vhodné spíše pro větší organizace)
NetWorx	- Jednoduchý a přehledný nástroj pro sledování využití sítě - Statistiky, grafy, export do souborů - Nízká náročnost	- Není určen pro monitoring celé podnikové sítě - Omezené pokročilé funkce (cloudové monitorování, monitorování virtuálních strojů)
LogicMonitor	- Umožnuje sledovat síť, servery, cloudové služby a aplikace - Využívá AI k detekci anomálií - Poskytuje prediktivní analýzy a včasné upozornění	- Závislost na připojení k internetu - Vyšší cena (podle počtu monitorovaných zařízení) - Neposkytuje pravidelné reporty a stavu

(Zdroj: Vlastní)

Tabulka 2 – Komparační tabulka funkcí softwarů

Funkce	Wireshark	PRTG	Flowmon	NetWorx	LogicMonitor
Monitoring provozu	✓	✓	✓	✓	✓
Podpora SNMP	x	✓	✓	✓	✓
AI detekce	x	x	✓	x	✓
Monitorování aplikací	x	✓	x	✓	✓
Historie/Statistiky	✓	✓	✓	✓	✓
Notifikace (e – mail, SMS)	x	✓	✓	✓	✓
Grafické zobrazení dat	✓	✓	✓	✓	✓
Podpora cloud	x	✓	✓	x	✓
Integrace s jinými nástroji	✓	✓	✓	x	✓

(Zdroj: Vlastní)

Každý z výše analyzovaných nástrojů má své výhody i omezení při monitorování síťového provozu. Jejich využití závisí na konkrétních potřebách daného subjektu a preferencích správce sítě. Kterýkoliv z těchto nástrojů může dobře posloužit při zlepšování zabezpečení informační infrastruktury v subjektu. V praxi je vhodné zvolit nástroj nejen podle funkcí, ale také s ohledem na rozsah sítové infrastruktury a typu organizace. Také se doporučuje, aby subjekt využíval kombinaci více nástrojů pro efektivnější zabezpečení.

Na základě výše uvedených tabulek s přehledem funkcí a srovnáním výhod a nevýhod jednotlivých softwarů bych pro potřeby subjektu ochrany obyvatelstva doporučil kombinaci těchto tří nástrojů, které disponují svou spolehlivostí, rychlou detekcí problémů, bezpečností a dostupností (PRTG Network Monitor, Progress Flowmon a Wireshark) každý z těchto nástrojů lze využít pro jiný účel, ale vzájemně se dobře doplňují.

Klíčové funkce těchto programů velmi dobře korespondují s potřebami subjektů ochrany obyvatelstva při dostatečné zprávě počítačové sítě. PRTG Network Monitor pomáhá při monitorování dostupnosti a výkonu, Progress Flowmon poskytuje data o detekci bezpečnostních hrozeb, Wireshark se specializuje na analýzu incidentů a síťových událostí. Program Wireshark je také skvělá možnost, jak odhalovat různé anomálie v síti jak při provozu v reálném čase, tak i zpětně při kontrolách.

7 MĚSTSKÁ POLICIE RÝMAŘOV

Pro tuto diplomovou práci byl jako subjekt ochrany obyvatelstva zvolena stanice Městské policie (dále jen MP) ve městě Rýmařov, která primárně slouží jako podpůrný subjekt v oblasti krizového řízení a ochrany obyvatelstva. Prostřednictvím této stanice MP obec zajišťuje klid a pořádek ve svém katastrálním území. Město má také uzavřeno celkem 8 veřejnoprávních smluv s dalšími obcemi ve správním obvodu obce s rozšířenou působností, jedná se o obce Horní Město, Tvrdkov, Jiříkov, Dolní Moravice, Břidličná, Malá Morávka, Stará Ves a Malá Štáhle, které se týkají zajišťování výkonu působnosti dle zákona o obecní policii. Na základě požadavku od představitelů těchto obcí může MP Rýmařov vyjíždět do katastrálního území těchto obcí. Ve směnném provozu zajišťují činnost na stanici 4 strážníci městské policie. (Městská policie)

Obec má zpracované různé plány a postupy řešení krizových a havarijních situací, které se nejen týkají obecného řešení krizové připravenosti, ale také i řešení zabezpečení kritické informační infrastruktury a ochrany IT technologií. Tyto plány mi byly poskytnuty Městským úřadem Rýmařov v tištěné podobě a bylo mi dovoleno, je částečně popsat pro účely diplomové práce.

7.1 Typový plán

Tento dokument zpracovává obecní úřad v souladu s nařízením vlády č. 431/2010 Sb. Pro řešení konkrétní krizové situace, která by dle analýzy rizik mohla v daném ORP nastat. Plán obsahuje základní typové postupy, zásady a opatření. Tento typový plán obsahuje tři části (základní, operativní, pomocnou) a je zpracován na krizovou situaci Narušení bezpečnosti informací kritické informační infrastruktury.

Základní část

Krizové situace (dále jen „KS“), které vznikající v důsledku narušení bezpečnosti informací kritické informační infrastruktury (dále jen „KII“) se liší svou povahou, a to vzhledem k rozdílným charakteristikám informačních a komunikačních systémů určených jako KII i k různorodosti služeb, které tyto systémy zajišťují.

Struktura těchto KS je přímo určená způsobem narušení bezpečnosti informací KII, kdy různé typy těchto narušení můžou způsobit jiné efekty. Vzhledem k rozdílnosti ohrožení je nutné ke každé KS přistupovat individuálně.

Mezi možná rizika patří

- Neúmyslné selhání technologií či lidí.
- Úmyslné napadení systémů.

Následky těchto KS je nutné vést ve dvou rovinách. Řešení následků ve fyzickém světě za pomocí složek IZS bude zcela odlišné od řešení následků v kyberprostoru. Kdy předpokládaný časový rozsah působení KS je odvíjen od průběhu situace. Tudíž nelze určit, zda bude řešení KS trvat hodiny nebo dny.

Narušení dle povahy

- *„Selhání technologie (Přímé poškození, chyby v systémech)“*
- *„Špatný výkon zaměstnanců“*
- *„Zásah živelní pohromou“*
- *„Výpadek elektrické energie“* (Typový plán)

Narušení dle typu útoku

- *„Kinetický zásah“*
- *„DoS/DDoS útok“*
- *„Škodlivý malware“*
- *„Sociální inženýrství“*
- *„Různé kombinace uvedených útoků“* (Typový plán)

Narušení dle typu motivace

- *„Hacktivismus nebo terorismus“*
- *„Peněžní zisk“*
- *„Napadení konkurencí“*
- *„Cílený útok zaměstnance nebo špionáž“*
- *„Prosazování politických názorů“* (Typový plán)

Zvládání KS tohoto typu je nutné rozdělit na dvě roviny. První se věnuje zvládání důsledků, které narušení způsobuje a druhá rovina se zaměřuje na řešení příčiny a nápravu fungování systémů KII.

Následky KS lze také rozdělit do dvou rovin. V rovině dopadů způsobených omezením nebo zastavením služeb, které narušeni KII způsobilo, je nutné odkázat na typové plány pro jednotlivé oblasti, které jsou určenou KII ovlivňovány či ovládány. Obecný a jednotný popis platný pro veškeré KII není možný.

Druhou rovinu následků lze identifikovat jako specifickou kybernetickou bezpečnostní. Touto rovinou se rozumí zejména dopad na ostatní subjekty využívající kyberprostor či subjekty s operujícími systémy, které by mohly být KS dotčeny.

Dopady se rozdělují na

- *„Životy a poškození zdraví osob“*
- *„Zničení nebo poškození majetku“*
- *„Poškození životního prostředí“*
- *„Mezinárodní dopady“*
- *„Ekonomické ztráty“*
- *„Sociální dopady“*
- *„Dopady na kritickou infrastrukturu“* (Typový plán)

Operativní část typového plánu obsahuje popis zásad pro řešení krizové situace a výpis principů zajišťování kybernetické bezpečnosti v ČR. Jako hlavní zásady dokument uvádí (Prevenci, Komunikaci, Koordinaci). Mezi principy zajišťování KB nalezneme (Individuální odpovědnost za bezpečnost, Důvěru a spolupráci).

Při dodržování těch zásad a principů je taky důležitá komunikace s orgány řešící oblast kybernetické bezpečnosti. Mezi tyto orgány patří:

- *„NÚKIB a CERT“*
- *„Policie ČR“*
- *„Soukromé a akademické sektory“*
- *„Regionální složky“* (Typový plán)

Proces řešení dopadů KS v problematice kybernetické bezpečnosti je řešen v souladu se zákonem č. 240/2000 Sb., o krizovém řízení, a zásadami řešení KS v oblastech, kde dopad nastal.

Tento proces zahrnuje

- *„Hlášení kontaktních údajů“*
- *„Hlášení kybernetického bezpečnostního incidentu“*
- *„Komunikace krizové situace“*
- *„Metodickou podporu“*
- *„Expertní asistenci“*
- *„Vydání varování od NÚKIB“*
- *„Vydání reaktivního opatření“*
- *„Vydaní ochranného opatření“*
- *„Možnost vyhlášení stavu kybernetického nebezpečí“* (Typový plán)

O vážnosti KS je nutné informovat vládu a prostřednictvím medií je také informována veřejnost.

Pomocná část dokumentu obsahuje

- *„Právní předpisy tykající se dané oblasti“*
- *„Podklady a formuláře k nahlášení incidentu“*
- *„Údaje o zainteresovaných organizacích“*
- *„Identifikační údaje o zpracovateli plánu“* (Typový plán)

Analýza SWOT – typového plánu

Typový plán zaměřený na řešení krizové situace v podobě narušení bezpečnosti kritické informační infrastruktury (KII) v ORP Rýmařov, představuje důležitý nástroj pro zajištění bezpečnosti v kyberprostoru. Následující SWOT analýza hodnotí silné a slabé stránky tohoto plánu a identifikuje příležitosti a hrozby, které mohou ovlivnit jeho funkčnost a efektivitu v reálném provozu. Následně je zpracována tabulka s hodnotami a váhami které byli přiděleny na základě brainstormingu se zaměstnanci oddělení vnitřních věcí v obci. Dále na základě výsledků vznikne doporučená strategie pro tento plán.

Tabulka 3 – Matice SWOT č.1 analýza typového plánu

S – (Silné stránky)	W – (Slabé stránky)
S1 Rozdělení krizových situací podle povahy, typu a motivace. S2 Zohlednění dopadů ve fyzickém světě i v kyberprostoru. S3 Zapojení klíčových institucí. S4 Důraz na zásady prevence, komunikace a koordinace.	W1 Absence technických aspektů detekce a reakce (např. logování, automatizace detekce hrozeb). W2 Chybí zlepšování nebo testování plánu, zpětná vazba, školení, simulace. W3 Nízká úroveň detailů u nápravných kroků. W4 Neřeší možnosti při kombinovaných krizích (např. kyberútok + blackout).
O – (Příležitosti)	**T – (Hrozby)**
O1 Doplnění plánu o prvky dle, ISO/IEC 27001, NIS2. O2 Vytvoření dynamického plánu s pravidelnou aktualizací. O3 Zavedení školení, testování a cvičení pro zaměstnance. O4 Možnost získání financí z grantů EU	T1 Rychlý vývoj kybernetických hrozeb – plán může zastarat. T2 Závislost na lidském faktoru – bez automatizace hrozí zpoždění. T3 Nízká připravenost na pokročilé útoky. T4 Nedostatek IT odborníků v menších obcích.

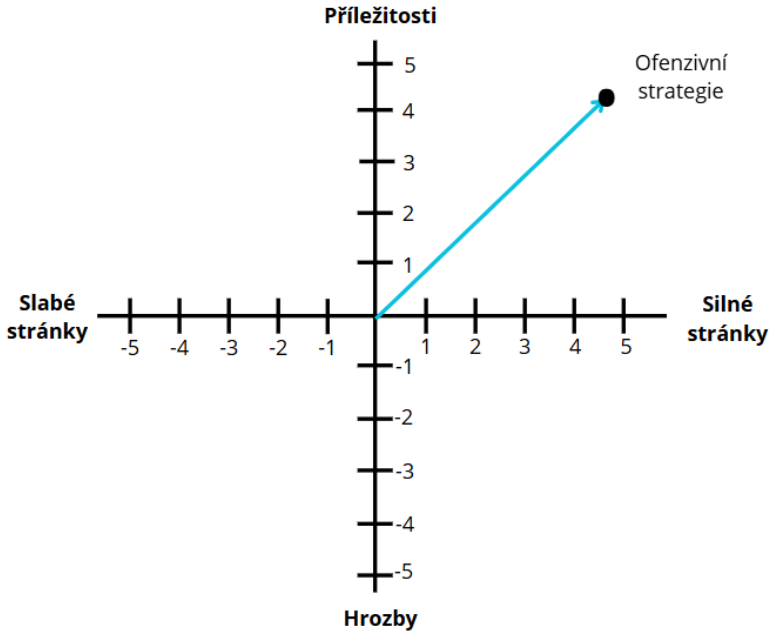
(Zdroj: Vlastní)

Tabulka 4 – Výpočet matice SWOT č.1

	Parametr	Body	Váhy	Výsledek
Silné stránky	Rozdělení krizí dle typu	5	0.30	1.50
	Zohlednění dopadu fyzicky i v kyberprostoru	4	0.15	0.60
	Zapojení klíčových institucí	4	0.30	1.20
	Prevence, komunikace, koordinace	5	0.25	1.25
	Celkem (S)	**<1; 5>**	**∑1.00**	**∑4.55**
Slabé stránky	Absence technické detekce	-2	0.30	-0,60
	Chybí testování nebo zlepšování	-2	0.25	-0,50
	Nízká úroveň detailů nápravných kroků	-2	0.15	-0,30
	Neřeší kombinované hrozby	-1	0.30	-0,30
	Celkem (W)	**<-1; -5>**	**∑1.00**	**∑-1,70**
Příležitosti	Doplnění o ISO/NIS2	4	0.25	1.00
	Vytvoření dynamického plánu	5	0.30	1.50
	Školení a cvičení zaměstnanců	4	0.25	1.00
	Financování z EU	3	0.20	0.60
	Celkem (O)	**<1; 5>**	**∑1.00**	**∑4.10**
Hrozby	Rychlý vývoj hrozeb	-2	0.30	-0.60
	Závislost na lidském faktoru	-1	0.25	-0.25
	Nízká připravenost na pokročilé útoky	-1	0.25	-0.25
	Nedostatek IT odborníků	-1	0.20	-0.20
	Celkem (T)	**<-1; -5>**	**∑1.00**	**∑-1.30**

(Zdroj: Vlastní)

Celkový výsledek SWOT analýzy poukazuje na velmi příznivou situaci, kdy silné stánky a příležitosti převyšují nad slabinami a hrozbami. Na základě těchto hodnot je doporučenou strategií pro MÚ společně s MP ofenzivní strategie, která pomůže s aktualizací typového plánu. Pro aktualizaci lze využít silných stánek plánu a čerpat z příležitostí, které se nabízejí k jeho zlepšení.



Obrázek 9 – Výsledná doporučená strategie č.1

(Zdroj: Vlastní)

Slabiny a hrozby, které byly v plánu detekovány, nemají tak výraznou váhu pro narušení IT bezpečnosti a lze je zvládnout při zavedení vhodných opatření. V současnosti se ale kybernetické hrozby vyvíjejí neustálým tempem a je důležité, aby subjekty ochrany obyvatelstva na tyto změny byly připraveny a rozvíjely tyto plány. Pro kvalitnější reakci na neustále vyvíjející se hrozby je potřeba zvážit a začlenit tyto body:

- Využívání technických prostředků pro detekci hrozeb.
- Využívat softwary pro monitorování sítě.
- Posílení technického vybavení v subjektech.
- Začlenění mezinárodních standardů.
- Začlenit do hrozeb i kombinované krize.

- Zlepšit detailnost při obnově po kybernetických hrozbách.
- Zavedení pravidelného školení zaměstnanců a kontroly připravenosti v oblasti kybernetické bezpečnosti.

Bez důkladné připravenosti na vyvíjející se situaci v kybernetické bezpečnosti by typový plán mohl při složitější formě kybernetického útoku selhat nebo mít omezenou činnost při reakci na vzniklou situaci.

7.2 Postupy řešení krizové, havarijní situace

Tento dokument je zaměřený na ochranu IT technologií v objektech, které souvisejí s krizovým řízením v daném ORP. V dokumentu se nacházejí možné druhy ohrožení, při jejichž naplnění by došlo k omezení nebo úplnému zastavení činnosti daného objektu. (Postupy řešení krizové, havarijní situace, 2022)

Tabulka 5 – Ochrana IT technologií

Přehled havárií	Plní	Spolupracuje	Dokumentace
Selhání systému elektronických komunikací	Externí pracovník informatiky	Externí dodavatel	Zprovoznění systému, prevence: spuštění záložního připojení k internetu
Selhání dodávky el. energie	Dodavatel energie	Odbor vnitřních věcí	Prevence: napájení TC pomocí motorgenerátoru
Selhání softwaru	Pracovník informatik	Odbor vnitřních věcí	Zprovoznění SW v co nejkratším čase, prevence: aktualizace SW
Selhání hardwaru	Pracovník informatik	Odbor vnitřních věcí	Zprovoznění HW v co nejkratším čase, prevence: systémové aktualizace, obnova starého HW
Zavedení škodlivého softwaru	Pracovník informatik	Odbor vnitřních věcí	Odstranění škodlivého SW v co nejkratším čase, prevence: bezpečnostní aktualizace spec. HW SW a testování detekce
Přetížení provozu	Pracovník informatik	Odbor vnitřních věcí	Snížení zatížení provozu, např. řízením uživatelů, aplikací systémových konfiguračních změn, prevence: monitoring provozu kritických systémových komponentů

(Zdroj: Postupy řešení krizové, havarijní situace, 2022)

Analýza SWOT – plánu s postupy řešení krizové, havarijní situace

Tento dokument formou tabulky identifikuje základní typy incidentů, které mohou ohrozit subjekty v ORP Rýmařov. Cílem tohoto plánu je zajistit provoz klíčových IT systémů a minimalizovat dopady identifikovaných havárií. Stejně jako u předchozí SWOT analýzy je následně zpracována tabulka s příslušnými hodnotami a váhami, které byly taktéž konzultovány se zaměstnanci krizového řízení v obci. Na základě výsledku byla také identifikována výsledná strategie pro tento dokument.

Tabulka 6 – Matice SWOT č.2 analýza postupů řešení krizové a havarijní situace

S – (Silné stránky)	**W – (Slabé stránky)**
S1 Přehledně definované hrozby. S2 Dostatečně zajištěna zodpovědnost. S3 Přehledně popsané preventivní opatření. S4 Zaměření na běžné incidenty.	W1 Absence časového plánu pro obnovu. W2 Nedostatečná operativní hloubka. W3 Absence postupů ověřování funkčnosti opatření. W4 Závislost na externích pracovnících.
O – (Příležitosti)	**T – (Hrozby)**
O1 Zavedení centrálních dokumentací incidentů a analýz. O2 Zavedení monitorování v reálném čase. O3 Zavedení školení, testování a cvičení. O4 Vytvoření víceúčelových plánu.	T1 Technologická závislost na externích dodavatelích – možné zpoždění reakce T2 Zastaralá preventivní opatření. T3 Nízká připravenost na pokročilé útoky. T4 Nedostatek IT odborníků v menších obcích.

(Zdroj: Vlastní)

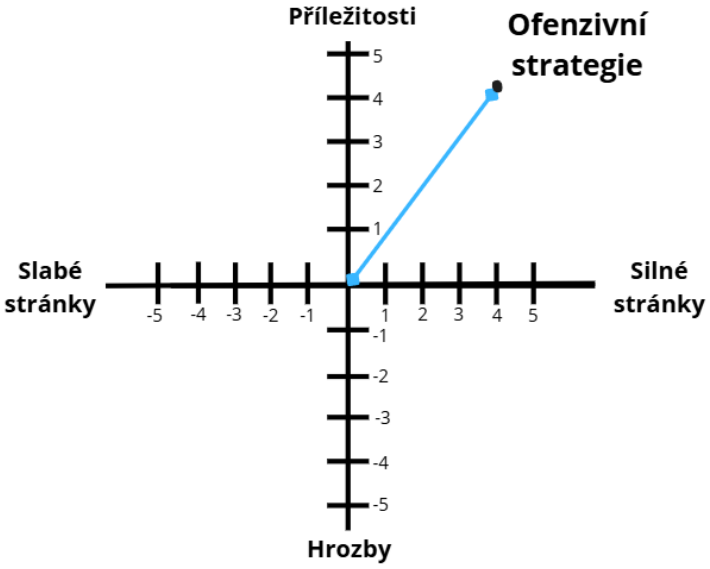
Tabulka 7 – Výpočet matice SWOT č.2

	Parametr	Body	Váhy	Výsledek
Silné stránky	Přehledně definované hrozby	5	0.30	1.50
	Dostatečně zajištěna zodpovědnost	4	0.20	0.80
	Přehledně popsaná preventivní opatření	4	0.30	1.20
	Zaměření na běžné incidenty	3	0.20	0.60
	Celkem (S)	**<1; 5>**	**∑1.00**	**∑4.10**
Slabé stránky	Absence časového plánu pro obnovu	-3	0.25	0.75
	Nedostatečná operativní hloubka	-2	0.25	0.50
	Absence ověřování funkčnosti opatření	-2	0.25	0.50
	Závislost na externích pracovnících	-2	0.25	0.50
	Celkem (W)	**<-1; -5>**	**∑1.00**	**∑-2.25**
Příležitosti	Centrální dokumentace incidentů	4	0.25	1.00
	Monitorování v reálném čase	5	0.25	1.25
	Školení, textování, cvičení	4	0.25	1.00
	Víceúčelové plány	3	0.25	0.75
	Celkem (O)	**<1; 5>**	**∑1.00**	**∑4.00**
Hrozby	Závislost na externích dodavatelích	-2	0.25	0.50
	Zastaralá preventivní opatření	-3	0.25	0.75
	Nízká připravenost na pokročilé útoky	-3	0.25	0.75
	Nedostatek IT odporníků v obcích	-2	0.25	0.50
	Celkem (T)	**<-1; -5>**	**∑1.00**	**∑-2.50**

(Zdroj: Vlastní)

Celkový výsledek SWOT analýzy poukazuje, že tento plán má dobré základy, ale vyskytují se také potencionální rizika. Doporučenou strategii pro aktualizaci plánu je ofenzivní

strategie Za pomocí této strategie subjekt může využít silných stánek plánu a čerpat z příležitostí, které se nabízejí k jeho zlepšení.



Obrázek 10 - Výsledná doporučená strategie č.2

(Zdroj: Vlastní)

Dokument poskytuje klíčové informace pro řešení běžných IT incidentů. Mezi výhody dokumentu patří přehlednost, jasně určená odpovědnost a důraz na prevenci. Jako nevýhodu vnímám absenci hlouběji rozepsaných operativních detailů, způsoby ověřování funkčnosti opatření a absenci nových technologií pro řešení kybernetických incidentů. Pro lepší efektivitu by bylo vhodně dokument doplnit o scénáře řešení incidentů a zapojit moderní technologie v závislosti s kontrolou a odstraňováním vzniklých havárií.

Mezi další návrhy, jak zlepši tento plán za pomocí příležitostí, by bylo dobré začlenit tyto body:

- Zpracovat podrobný časový plán obnovy.
- Posílit technické vybavení subjektů ochrany obyvatelstva v obci.
- Zavést využívaní monitorovacích nástrojů.
- Provádět pravidelné simulace kybernetických incidentů.
- Pravidelně provádět školení zaměstnanců v oblasti kybernetické bezpečnosti.

Modernizace subjektů ochrany obyvatelstva a aktualizace tohoto plánu výrazně pomůže posílit vnitřní bezpečnost a eliminovat slabiny.

7.3 Vyhodnocení současného stavu zabezpečení sítí v subjektu

Na základě rozhovoru (viz Příloha č.1) se strážníkem Městské policie v Rýmařově, který na služebně pracuje již přes 20 let, bylo možné orientačně provést kvalitativní zhodnocení stavu zabezpečení IT infrastruktury. Jelikož se nejedná o oficiální technickou dokumentaci je toto zhodnocení čistě orientační pro získání přehledu, jak má subjekt zajištěnou ochranu IT.

Zaměstnanci MP při své každodenní činnosti využívají služební počítače a komunikační zařízení která jsou propojena s centrální sítí Městského úřadu v obci. Tento systém je provozně stabilní a během jeho provozu nebyly zaznamenány výpadky ani jiné technické problémy, které by se týkaly kybernetických útoků. Přístup na stanici je zabezpečen kamerovým systémem a elektronickým zámkem na vchodových dveřích. V hlavní části stanice se vždy nachází jeden ze strážníků, který je zodpovědný za dozor u vstupních dveří. Tudíž běžný občan se na stanici dostane jen při použití zvonku a následným otevřením dveří které jsou odemknuty strážníkem.

Do služebních počítačů mají strážníci přístup pomocí vlastních přihlašovacích údajů a jejich aktivita by se měla primárně týkat pracovních povinností. Přístup k webovým stránkám není nijak omezen. Kladen je ale důraz na stahování soborů v rámci různých webů je zakázáno cokoliv stahovat a v rámci emailové komunikace je důležité si ověřit, zda komunikace probíhá mezi zaměstnanci a nadřízenými a nejedná se o možný phishingový útok.

Správa infrastruktury je zajišťována externí IT podporou v obci a mezi používané technologie, které pomáhají zajistit IT bezpečnost se na stanici nacházejí v podobě firewallu, antivirových programů a zálohování dat, které má nestarosti externí IT pracovník. Pokročilé technologie, jako je šifrování, VPN nebo dvoufaktorová autentizace, nejsou aktuálně využívány. Odpovědnost za případné incidenty je nastavena jednoznačně, jejich řešení přebírá IT pracovník, a v případě pochybení zaměstnance je vyžadováno, aby podstoupil školení v rámci zamezení dalšího incidentu.

Z rozhovoru vyplynulo že strážnici MP jsou na pravidelné bázi informování o aktuálních hrozbách formou měsíčních porad, kde jsou také probírány aktuální případy z praxe v rámci ČR. Dodatečné školení v oblasti kybernetické bezpečnosti probíhá jako reakce na konkrétní situace, ale také mají strážnici možnost se dobrovolně přihlásit a podstoupit školení navíc.

8 ANOMÁLIE V SÍTI MĚSTSKÉ POLICIE

V síťovém provozu se mohou vyskytovat anomálie, což jsou odchylky od normálního, standardního provozu dané počítačové sítě. Provoz sítě může být pod určitým vlivem vlastníkem sítě nebo dalšími uživateli používaných technologií ohrožen nebo zahlcen množstvím požadavků. Funkčnost sítě by měla být pod neustálým dohledem jejího správce, aby bylo možné včas a efektivně reagovat na možné anomálie, které se v síti mohou objevit. Tyto anomálie mohu pomoci odhalit, zda se jedná o bezpečnostní hrozbu nebo technický problém podle základních rysů dané anomálie.

Pro identifikování možných anomálií, které se mohou vyskytovat v síti subjektu, nebyla provedena žádná analýza sítě za pomocí softwaru fyzicky na stanici z důvodu zákazu nadřízeného pracovníka stanice. Zjištěné údaje, které by bylo nutno uvést v práci, by mohli přímo odhalit citlivé informace. Proto následující anomálie vycházejí z obecně známých typů. K anomáliím byly popsány možné příčiny vzniku dané anomálie a jejich důsledky. Na základě identifikovaných anomálií je zpracována What-if analýza, která vyhodnotí nejzávažnější anomálie pro následnou tvorbu scénářů kybernetických útoků na subjekt.

8.1 Výkonnostní anomálie

Neobvyklá latence – Latence označuje časový interval, který uplyne mezi odesláním paketu z výchozího bodu do cílového bodu. Za běžných podmínek by měla zůstat nízká a stabilní. Neočekávané zvýšení latence může negativně ovlivnit síťový provoz, zejména u časově citlivých aplikací, jako jsou komunikační a cloudové služby. Může se však projevit i zpomalením načítání webových stránek nebo prodloužením doby stahování souborů.

Možné příčiny

- Přetížení sítě vysokým provozem.
- Síťové přepínače nebo směrovače pracují pod vysokým vytížením.
- Nevhodně nastavené QoS (Quality of Service).
- Kybernetické útoky, jako DoS/DDoS.
- Problémy s fyzickou vrstvou (vadné kabely, rušení).

Důsledky

- Zpoždění v komunikaci.

- Špatná kvalita hlasových a video hovorů.
- Ztráta odezvy v reálném čase u online aplikací.

Zvýšená chybovost paketů – Při přenosu dat přes internet jsou informace rozděleny na menší části zvané pakety. K jejich ztrátě dochází, pokud některé pakety nedorazí do cílového bodu nebo se během přenosu poškodí. V takovém případě je nutné je znovu odeslat. Nízká úroveň ztráty paketů (například pod 1 %) je běžná a obvykle neovlivňuje výkon sítě, ale vyšší ztráty mohou signalizovat technické potíže.

Možné příčiny

- Přetížená síť, která nestíhá zpracovávat pakety.
- Vadný hardware (např. síťové adaptéry, switche, směrovače).
- Rušení u bezdrátových sítí (Wi-Fi).
- Nestabilní internetové připojení (problémy u poskytovatele).
- Chyby v síťových protokolech nebo nesprávná konfigurace.

Důsledky

- Výpadky spojení v aplikacích.
- Problémy se synchronizací dat.
- Přerušování VoIP hovorů nebo zhoršená kvalita videa.

Kolísání šířky pásma – Šířka pásma udává maximální možnou přenosovou rychlost v síti. Pokud dochází k jejím náhlým výkyvům, může to vést k nestabilitě síťového připojení.

Možné příčiny

- Velký nárůst síťového provozu (např. zálohování dat, streaming, cloudové aplikace).
- Nesprávně nastavené síťové priority (např. chybně nakonfigurované QoS).
- Špatná optimalizace směrování datových toků.
- Kybernetické útoky, například DDoS nebo síťové skenování.

Důsledky

- Zpomalení internetu a aplikací.

- Zhoršená kvalita videokonferencí.
- Výpadky nebo nestabilita připojení.

Neobvyklé špičky v síťovém provozu – Síťový provoz by měl mít určité předvídatelné chování. Pokud dochází k nečekaným špičkám v zatížení, může to být znakem problému.

Možné příčiny

- Náhlé zvýšení požadavků uživatelů (např. začátek pracovní doby).
- Automatické aktualizace softwaru na velkém množství zařízení.
- Napadení škodlivým programem
- Útoky DoS nebo síťové skenování útočníkem.

Důsledky

- Přetížení serverů a zpomalení služeb.
- Nedostupnost určitých aplikací nebo výpadky síťových služeb.
- Možné zahlcení firemního firewallu nebo IDS/IPS systému.

Dlouhodobé přetížení síťových zařízení – Pokud síťová zařízení (např. směrovače, switche) dlouhodobě pracují na hranici své kapacity, může dojít k degradaci výkonu celé sítě.

Možné příčiny

- Nevhodná konfigurace síťových zařízení.
- Nedostatečný hardware vzhledem k aktuální síťové zátěži.
- Útoky zneužívající zranitelnosti síťových prvků.
- Přetížené cloudové nebo datové servery.

Důsledky

- Zvýšená latence a pomalejší odpovědi na požadavky.
- Výpadky nebo restartování síťových zařízení.
- Snížená spolehlivost síťového provozu.

8.2 Bezpečnostní anomálie

Neobvyklé přístupy k síťovým zdrojům – Přístup k síťovým funkcím by měl být umožněn pouze autorizovaným uživatelům a systémům. Neobvyklé pokusy o připojení z neznámých IP adres díky technologii VPN, například z nečekaných geografických oblastí nebo v neobvyklých časech, mohou signalizovat pokus o neoprávněný průnik do systému.

Možné příčiny

- Přístup z ukradených účtů (např. kvůli phishingu).
- Pokusy o útok hrubou silou na přihlašovací údaje.
- Neoprávněná aktivita zaměstnanců.
- Automatizované skenování sítě útočníky.

Důsledky

- Možná nelegální aktivita útočníka v interní síti.
- Získání citlivých dat.
- Zneužití interních dat k dalším útokům.

Zvýšený počet neúspěšných přihlášení – Neúspěšné pokusy o přihlášení jsou běžné z různých důvodů, například kvůli zapomenutému heslu, technickým problémům nebo drobným rozdílům při zadávání hesla, zejména pokud má uživatel více účtů. Pokud se však neúspěšné pokusy o přihlášení opakují ve velmi krátkých intervalech, například v řádu vteřin až minut, může to naznačovat pokus o útok hrubou silou nebo slovníkový útok.

Možné příčiny

- Automatizované útoky na hesla (brute-force, credential stuffing).
- Špatná konfigurace přihlašovacích systémů.
- Opakované pokusy uživatelů o přihlášení s chybným heslem.
- Technické problémy s hardwarem.

Důsledky

- Možnost prolomení slabých hesel.
- Zamknutí uživatelských účtů a narušení provozu.

- Indikace většího koordinovaného útoku na infrastrukturu.

Podezřelé datové přenosy – Domácí i firemní síťový provoz má obvykle stabilní a předvídatelnou strukturu, která se jen zřídka mění. Počet přihlášených uživatelů a objem přenášených dat se většinou drží v ustálených časových rámcích, odpovídajících pracovní době a plánovaným úkolům. Pokud však dojde k neočekávané změně tohoto vzorce, například k výraznému nárůstu přenosu dat nebo jejich odesílání na externí servery, může to signalizovat pokus o krádež citlivých dat.

Možné příčiny

- Napadení škodlivým programem.
- Kybernetické útoky APT (Advanced Persistent Threat).
- Narušení serveru zaměstnancem.

Důsledky

- Krádež firemních dat nebo osobních údajů.
- Kompromitace zákaznických nebo obchodních informací.
- Riziko vydírání nebo poškození reputace organizace.

Neobvyklé vzory síťového provozu – Standardní síťový provoz se vyznačuje pravidelnými vzory komunikace mezi zařízeními. Pokud začnou komunikovat systémy, které by za normálních okolností neměly, může jít o výskyt útočníka v síti.

Možné příčiny

- Nežádoucí aktivita útočníka v interní síti.
- Instalace a rozšiřování škodlivého kódu.
- Chybná konfigurace síťových pravidel.

Důsledky

- Šíření škodlivého kódu nebo kompromitace dalších zařízení.
- Získání přístupu k citlivým datům útočníkem.
- Potenciální příprava na další fázi útoku.

8.3 Anomálie související s útoky

Distributed Denial of Service (DDoS) – Útoky toho typu jsou charakterizovány výrazným nárůstem požadavků na server nebo síť, jehož cílem je ochromit službu. Tyto útoky jsou často realizovány prostřednictvím rozsáhlé sítě infikovaných počítačů, které jsou ovládány bot malwarem. Tato zařízení následně cílí na síťové prvky systému, které se potřebují připojit k internetu, což následně vede k přetížení systému.

Možné příčiny

- Koordinovaný útok z více zranitelných zařízení.
- Zneužívání zranitelností aplikací k vyvolání zvýšeného provozu.
- Špatná konfigurace v síťové infrastruktuře, která umožňuje snadné přetížení.
- Problémy v komunikaci s třetími stranami, které vedou k přetížení.

Důsledky

- Nedostupnost webových a síťových služeb pro uživatele.
- Ztráta důvěry zákazníků, zhoršení reputace organizace.
- Přetížení síťové infrastruktury a degradace výkonu.
- Zvýšená latence a ztráta paketů.
- Možné finanční ztráty kvůli výpadkům služeb.

DNS tunelování – Tunelovací metoda využívá DNS protokol ke skrytému přenosu dat přes firewall, obcházející standardní bezpečnostní opatření. Tento typ útoku často zůstává neodhalený, protože DNS je běžně považován za legitimní protokol.

Možné příčiny

- Použití škodlivých DNS požadavků k šíření malwaru.
- Nedostatečné monitorování DNS provozu.
- Kompromitované systémy využívající škodlivé DNS servery.
- Použití nástrojů pro tunelování dat.

Důsledky

- Únik citlivých informací.

- Obcházení bezpečnostních opatření a firewallů.
- Vytvoření skrytých komunikačních kanálů pro malware.
- Obcházení bezpečnostních opatření a možný přístup k interní síti.

MAC a ARP spoofing – Metoda spoofing zahrnuje falšování MAC nebo ARP adres za účelem získání neoprávněného přístupu k síťovým prostředkům nebo provádění útoků typu Man-in-the-Middle. Útočník může převzít IP adresu jiného zařízení a odchytávat nebo manipulovat s přenášenými daty.

Možné příčiny

- Útočník provádí útoky typu Man-in-the-Middle.
- Zneužívání ARP cache poisoning k přesměrování síťového provozu.

Důsledky

- Neoprávněný přístup k důležitým informacím a manipulace s nimi.
- Odposlech síťového provozu a krádež přihlašovacích údajů.
- Přesměrování provozu na škodlivé servery.
- Narušování spojení mezi různými zařízeními v síti.

8.4 Anomálie způsobené chybnou konfigurací

Chybné směrování paketů – Chybná konfigurace směrovacích tabulek může vést k nefunkčnosti síťových služeb nebo neefektivnímu směrování dat, což způsobí ztrátu paketů nebo přetížení některých částí sítě.

Možné příčiny

- Nesprávně nakonfigurované statické nebo dynamické směrování.
- Konflikty mezi směrovacími protokoly.
- Neaktuální nebo neplatné směrovací tabulky.

Důsledky

- Ztráta síťové konektivity mezi zařízeními.
- Zvýšená latence kvůli neoptimálním trasám.

- Zpomalení síťového provozu nebo ztráta paketů.

Nesprávná konfigurace firewallu – Pokud je firewall špatně nakonfigurován, může to vést k neúmyslnému otevření citlivých portů, což umožní útočníkům přístup k interním systémům, nebo naopak k blokování legitimního provozu.

Možné příčiny

- Chyby v pravidlech firewallu vedoucí k nadměrnému filtrování nebo naopak povolení nebezpečných spojení.
- Nesprávně nakonfigurované zóny důvěry.
- Konflikty mezi více vrstvami zabezpečení (např. IDS/IPS vs. firewall).

Důsledky

- Otevření zranitelných portů pro útočníky.
- Neoprávněné blokování služeb, což ovlivňuje uživatelskou zkušenost.
- Zvýšené riziko průniku a kompromitace dat.
- Možnost přístupu neautorizovaných uživatelů k citlivým systémům.

Chyby v přístupových právech – Nesprávné nastavení přístupových práv může vést k neautorizovanému přístupu k síťovým prostředkům. To znamená, že některý uživatel nebo aplikace má vyšší oprávnění, než je nutné.

Možné příčiny

- Chyby při správě uživatelských účtů a rolí.
- Špatně nastavení pravidel v přístupovém seznamu.
- Chybějící pravidelné audity přístupových práv.

Důsledky

- Neoprávněný přístup k důležitým datům.
- Zvýšené riziko úniku informací nebo vnitřních útoků.
- Možná manipulace s konfigurací a sítěmi útočníkem.

8.5 Analýza anomálií

Metoda What-if byla aplikována na anomálie, které se mohou vyskytovat v sítovém provozu Městské policie (viz Tabulka č.8). Tato analýza prostřednictvím otázek umožňuje identifikovat možné dopady při výskytu různých anomálií v síťovém provozu. Pro každou anomálii byla stanovena typická situace, ke které může dojít v sítovém provozu, očekávané dopady anomálie, pravděpodobnost výskytu a doporučená opatření.

Tabulka 8 – What-if analýza anomálií

Anomálie	Otázka	Dopady	Pravděp.	Opatření
Neobvyklá latence	Co když se latence v síti nečekaně zvýší?	Zpožděná komunikace mezi hlídkami, snížená efektivita při zásazích, zpožděné zpracování požadavků od občanů.	Vysoká	Monitorování síťového provozu, pravidelná údržba hardwaru ,detekce DoS/DDoS útoků.
Zvýšená chybovost paketů	Co když začnou být data při přenosu často poškozována nebo ztrácena?	Nespolehlivá komunikace přes dispečink, výpadky kamerových systémů, přerušení spojení s hlídkami.	Střední	Kontrola a výměna vadného hardwaru, stabilizace internetového připojení, revize konfigurace síťových protokolů.
Kolísání šířky pásma	Co když začne docházet k náhlým výkyvům v rychlosti připojení?	Výpadky připojení služebních zařízení v terénu, potíže při vzdáleném přístupu do systémů.	Vysoká	Optimalizace datových toků, detekce a blokování DDoS útoků, sledování a řízení zátěže.

Neobvyklý síťový provoz	Co když v síti dojde k náhlému nárůstu zatížení?	Zpomalování nebo výpadky informačního systému, zpoždění v evidenci přestupků.	Střední	Monitorování vzorců provozu, omezení automatických aktualizací, detekce botnetů a skenování
Dlouhodobé přetížení síťových zařízení	Co když síťová zařízení pracují dlouhodobě na hranici své kapacity?	Výpadky komunikace, problémy při přenosu záznamů z kamer, ztráta dostupnosti interních systémů.	Nízká	Upgrade hardwaru, kontrola konfigurací, detekce útoků.
Neobvyklé přístupy k síťovým zdrojům	Co když někdo přistupuje ze zahraniční IP nebo v netypickém čase?	Možnost úniku osobních údajů, zneužití přístupových práv zaměstnancem, narušení důvěry veřejnosti.	Vysoká	Monitorování přístupových logů, vícefaktorová autentizace, omezení přístupů podle práv.
Zvýšený počet neúspěšných přihlášení	Co když se opakovaně někdo pokouší přihlásit s chybným heslem?	Možnost pokusu o prolomení účtu strážníka, zablokování účtů a narušení provozu, riziko zneužití kompromitovaného účtu.	Střední	Nastavení limitu pokusů o přihlášení, blokace IP.
Podezřelé datové přenosy	Co když se najednou přenáší velké množství dat mimo firmu?	Riziko krádeže osobních údajů občanů, zveřejnění interních informací, reputační škody pro MP.	Střední	Monitorování datových toků, DLP systémy, šifrování, IDS/IPS.

Neobvyklé vzory síťového provozu	Co když komunikují zařízení, která spolu normálně nekomunikují?	Možný pohyb malwaru po síti, příprava cíleného útoku, obcházení segmentace.	Střední	Segmentace sítě, monitoring sítě, pravidelné skenování sítě.
Distributed Denial of Service (DDoS)	Co když dojde k zahlcení serveru nadměrným provozem?	Nedostupnost portálu pro občany, výpadky přístupových systémů, ztížená komunikace dispečinku s terénem.	Vysoká	Použití anti-DDoS služeb, filtrování provozu.
DNS tunelování	Co když je přes DNS přenášen škodlivý provoz?	Únik informací o vyšetřování nebo pohybu hlídek, nepozorovaná komunikace s útočníkem.	Nízká	Monitorování DNS provozu, detekce anomálií, blokování podezřelých domén.
MAC a ARP spoofing	Co když někdo falšuje síťovou identitu?	Možnost odposlechu komunikace, přesměrování citlivých dat, narušení důvěryhodnosti interní sítě.	Střední	Použití dynamické ARP inspekce, port security, šifrování provozu.
Chybné směrování paketů	Co když jsou data směrována neefektivně nebo špatně?	Ztráta spojení s mobilními jednotkami, snížení reakční schopnosti.	Střední	Pravidelný audit směrování, aktualizace směrovacích tabulek.

Nesprávná konfigurace firewallu	Co když firewall nechrání síť nebo blokuje legitimní provoz?	Otevřená síť pro neoprávněný přístup, výpadky komunikace, nedostupnost online systémů.	Nízká	Testování pravidel, pravidelné revize a konfigurace.
Chyby v přístupových právech	Co když mají uživatelé větší oprávnění, než potřebují?	Možnost zneužití systému zaměstnancem, únik nebo úprava důvěrných údajů občanů, manipulace s daty o přestupcích.	Vysoká	Kontrola minimálních oprávnění, pravidelné audity přístupů, řízení podle práv.

(Zdroj: Vlastní)

Cílem této analýzy bylo zjistit, které z obecných anomálií v sítovém provozu mají největší pravděpodobnost výskytu v síti Městské Police Rýmařov. Z analýzy vyplynulo, že anomálie typu (Neobvyklá latence, Kolísání šířky pásma, Neobvyklé přístupy k síťovým zdrojům, Distributed Denial of Service (DDoS) a Chyby v přístupových právech) mají největší pravděpodobnost výskytu v síti subjektu. Vysoká pravděpodobnost u těchto anomálií poskytuje možnosti při tvorbě scénářů, které mají za úkol prověřit efektivitu zabezpečení sítového provozu v subjektu.

9 NÁVRH SCÉNÁŘŮ

Městská policie Rýmařov se sídlem služebny na adrese 8. května 48 má na starosti zajišťování veřejného pořádku a plnění dalších úkolů, jako jsou různé typy kontrol a šetření situací při zabezpečování klidu a bezpečnosti v rámci svého katastrálního území. Každodenní provoz služebny je spjat s využíváním informačních systémů, které hrají klíčovou roli při chodu stanice.

Strážníci při své každodenní činnosti využívají standardní, ale i pokročilejší počítačové softwary. Mezi používané softwary patří standardní zapisovací programy pro evidenci dat o situacích, které občané u policie nahlašují, ale také využívají specializované aplikace přímo pro evidenci různých přestupků a trestné činnosti. Přístup k těmto softwarům je udělován prostřednictvím hlavního administrativního serveru celé obce. Díky tomuto serveru se k těmto a dalším softwarům mohou dostat jenom pracovníci dané organizace v rámci ORP.

Informační struktura MP je složena z několika stolních počítačů, mobilních telefonů a komunikačních prostředků, které se nacházejí v autech a na stanici. Bezpečný a nepřerušovaný přístup k těmto systémům je nezbytný pro efektivní výkon služby v reálném čase. Jakýkoliv výpadek nebo narušení může vést ke ztížení činnosti Městské policie a ohrozit ochranu osobních údajů.

Při výpadku sítě způsobené kybernetickým útokem není ohrožena jen efektivita práce daného pracoviště, ale také veškeré osobní informace strážníků a obyvatel, kteří jsou zapsáni v jednom z informačních systému MP. Z těchto důvodů by bylo dobré se více zaměřit na individuální kontroly sítí, popřípadě zavést nepřetržitý monitoring sítě i v takto malých pracovištích, jako jsou stanice MP.

Na základě What-if analýzy anomálií a vyhodnocení současného zabezpečení sítě u MP v Rýmařově byly zpracovány následující scénáře možných kybernetických útoků, které by při cvičení měly otestovat efektivitu a připravenost zaměstnanců při reakci na tyto útoky. Následně jsou i zpracována doporučení na zlepšení bezpečnosti, které se ztotožňují s výsledky analýz a rozhovoru.

9.1 Scénář DDoS útoku

Scénář kybernetického útoku se zaměřuje na simulaci útoku typu DDoS, jehož cílem je narušení dostupnosti interních systémů Městské policie. Tento typ útoku také může sloužit jako zástěrka pro další možné záměry útočníka. Útočník může dále proniknout k serveru subjektu, na který nahraje škodlivý software. Ten útočníkovi umožní získat přístup k citlivým informacím o pracovnicích a občanech, které může později využít ke špatným záměrům.

Z What-if analýzy vyplývá, že DDoS útok můžeme identifikovat podle těchto vyskytujících se anomálií v sítovém provozu (Neobvyklá latence, Kolísání šířky pásma, Distributed Denial of Service (DDoS)).

Cílem tohoto scénáře je popsat průběh, reakci a možné důsledky kybernetického útoku na subjekt, který pravidelně využívá IT systémy pro zajištění každodenního provozu. Pro lepší znázornění byl scénář modelován v programu MS Visio.

Fáze útoku

V první fázi se útočník co nejlépe připravuje na útok a snaží se shromáždit co nejvíce informací o cílové infrastruktuře a najít veškerá slabá místa, která by mohl při útoku využít. Jako první se pokouší přijít na veřejné IP adresy systémů, které mohou být primárně dostupné z internetu, a identifikovat tak konkrétní servery nebo služby, na které by mohl zaměřit svůj útok. Dále potřebuje zjistit topologii sítě, a jak jsou jednotlivé části systému vzájemné propojené a jakou mají zajištěnou ochranu a v které části by bylo možné síť přetížit.

Mezi další důležité informace k útoku patří:

- Jaké služby běží, na jakých portech.
- Kapacita připojení a výkon jednotlivých systémů.
- Používaný software a hardware MP.
- Typy ochranných systémů.
- Pracovní vytížení dané organizace.

Po získání dostatečného objemu informací si útočník připraví přesný postup, kterým se bude řídit při zahájení útoku s konkrétním načasováním vzhledem k menšímu dozoru nad

infrastrukturou. K útoku si také potřebuje připravit síť infikovaných zařízeních (botnet) nad kterými převezme kontrolu díky malwaru.

Ve druhé fázi útočník v předem zvolený čas zahájí koordinovaný DDoS útok. Pomocí sítě kompromitovaných zařízení (botnet) generuje na dálku velké množství nežádoucího síťového provozu. Primárně se při útoku zaměřuje na zranitelné síťové prvky a služby, dokud se mu je nepodaří přetížit množstvím požadavků až do bodu selhání.

V důsledku přetížení dochází k výpadkům komunikačních kanálů, omezení dostupnosti základních služeb a narušení kompletního provozu interní sítě. Tyto výpadky mají za úkol způsobit chaos mezi zaměstnanci, kteří nemohou využívat důležité informační technologie potřebné pro svou běžnou pracovní činnost.

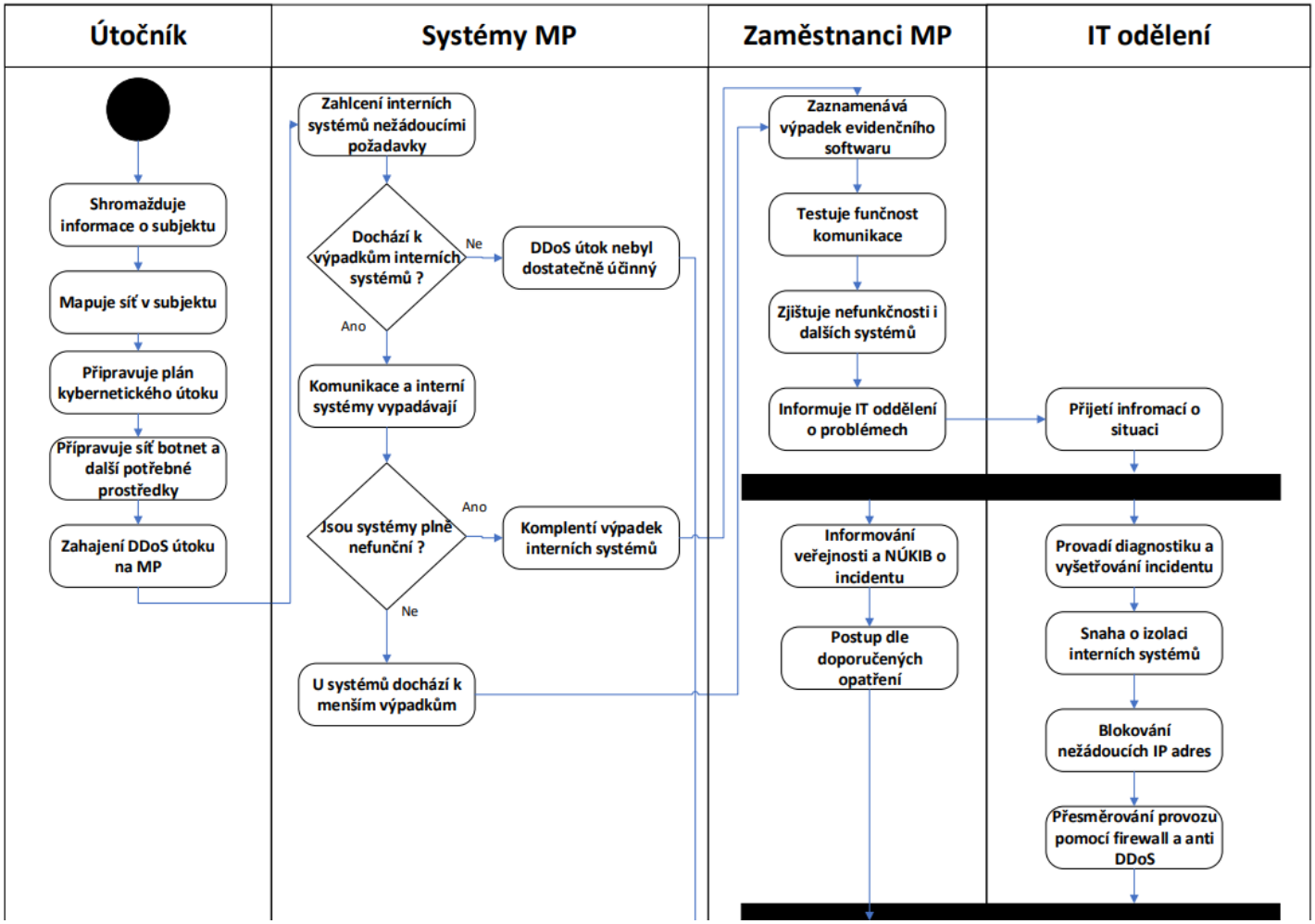
Možné dopady DDoS útoku

- Nedostupnost služeb (interní informační systémy, webové služby, komunikace, připojení k hlavnímu serveru)
- Omezení činnosti strážníků a vytížení IT specialistů.
- Zpoždění řešení dalších situací na stanici (přechod na papírový způsob zápisu a vyhledávání).
- Zvýšené finanční nálady na obnovu.
- Ztráta citlivých dat.
- Ztráta důvěry v organizaci a možné právní důsledky.

9.1.1 Model DDoS útoku na Městskou policii

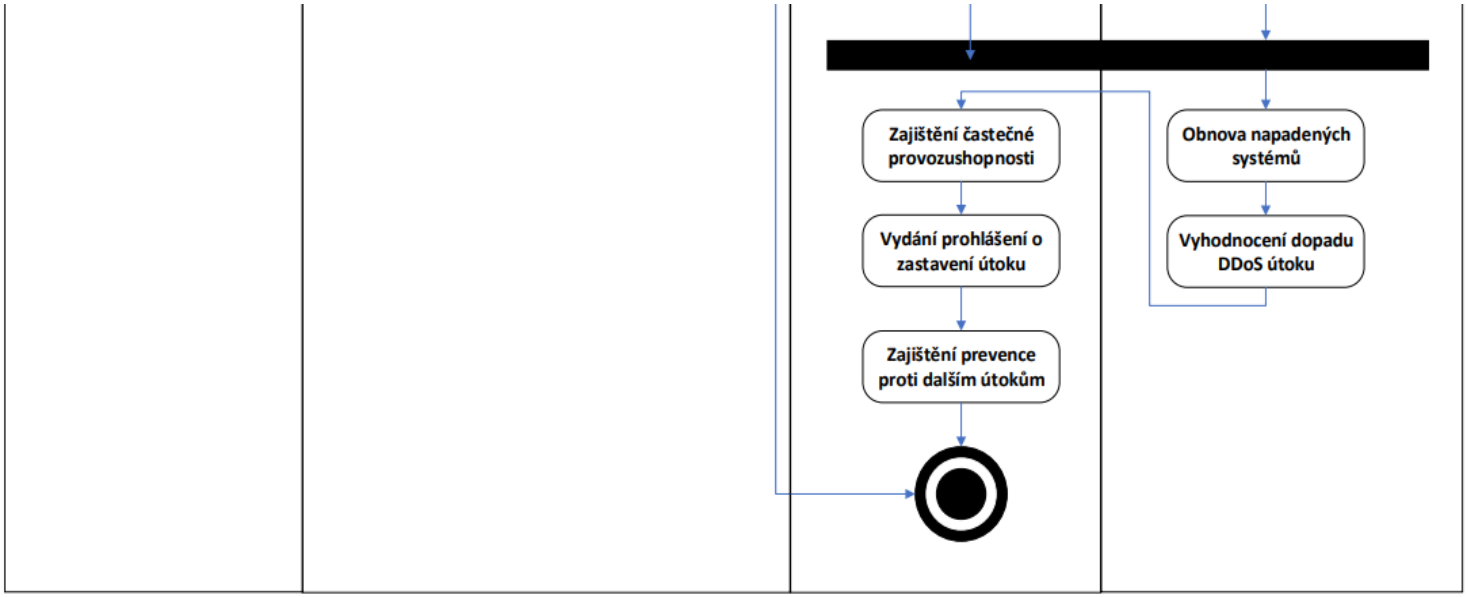
Swimlane diagram kybernetického útoku typu DDoS byl modelován v softwaru MS Visio. Tento model nabízí detailnější pohled na situaci, která by mohla vzniknout při DDoS útoku na interní systémy MP. Zaměstnanci MP využívají každý den hned několik technologií pro efektivnější provoz. V tomto scénáři se útočník snaží ochromit komunikaci a další služby MP které jsou důležité pro evidenci přestupků. S výpadky těchto systému mohou být spojené i ztráty na životech, jelikož ochromením komunikace může dojít ke zmatkům při řešení mimořádné události.

Při řešení těchto situací je zásadní, aby informační technologie byly na provozuschopné úrovni a aby zaměstnanci MP a IT oddělení dostatečně spolupracovaly na vyřešení vzniklého incidentu



Obrázek 11 - Swimlane diagram č.1 scénáře DDoS útoku

(Zdroj: Vlastní)



Obrázek 12 - Swimlane diagram č.2 scénáře DDoS útoku

(Zdroj: Vlastní

Reakce organizace

Strážníci, kteří mají zrovna službu, zaznamenají pokles funkčnosti nebo úplné odstavení možných napadených systémů, které běžně využívají. Tuto neobvyklou situací musí dle řádného postupu nahlásit IT pracovníkům, kteří neprodleně zahájí šetření dané situace. Dle typového plánu narušení bezpečnosti informací musejí IT specialisté řádně situaci nahlásit na Národní úřad pro kybernetickou bezpečnost a další teoreticky tímto kybernetickým útokem ohrožené subjekty. Dále musejí zahájit šetření incidentu za pomoci všech dostupných prostředků.

Možnosti reakce na DDoS útok

- Detekce a vyhodnocení incidentu.
- Zahájení izolace systémů.
- Informovat poskytovatele internetu a občanů o situaci.
- Ohlášení incidentu na NÚKIB.
- Blokovat podezřelé IP adresy nebo přesměrovat provoz pomocí firewall a antiddos služby.
- Dodržovat postupy při výpadku sítě pro zajištění částečného provozu.
- Zpětná analýza a prevence.

Po úspěšném zabránění kybernetického útoku DDoS je nutné, aby IT pracovníci zajistili rychlou analýzu útoku a obnovu systémů, v případě ztráty dat jejich obnovení. Pomocí analýzy logů a záznamů je možné zjistit způsob, jak se útočník dostal do systému a tyto chyby následně opravit.

Mezi nezbytné kroky organizace patří důkladná analýzy celé situace a následné posílení informační bezpečnosti, aby se daný incident nemohl snáze opakovat. Těmto incidentům nelze vždy stoprocentně zabránit, ale je možné svou informační infrastrukturu připravit na jejich výskyt.

Možné slabiny subjektu

- Nedostatečné zabezpečení síťových služeb a neefektivní správa šířky pásma.
- Absence systému pro detekci anomálií.
- Absence IT pracovníků přímo na stanici.

- Nedostatečné školení zaměstnanců na tyto incidenty.

9.1.2 Opatření proti DDoS útoku

Kybernetické útoky tohoto typu jsou velmi nebezpečné a když je ve velkém rozsahu ohrožena bezpečnost informací, informačních systémů a elektronických komunikací tak tím může dojít k ohrožení zájmů České republiky a k vyhlášení stavu kybernetického nebezpeční. Z těch důvodů je důležité klást na kybernetickou bezpečnost velký důraz a pravidelně zlepšovat připravenost na tento typ hrozby.

Návrhy na zlepšení ochrany proti DDoS útokům

- Síťová a technická opatření v subjektu.
- Monitoring sítě a včasná detekce.
- Organizační opatření.
- Spolupráce a komunikace.

Sítová a technická opatření – Jedním ze základních kroků je implementace specializované DDoS ochrany. Městská policie Rýmařov tak může využít služby od externích dodavatelů, jako jsou Cloudflare, Wedos, O2 nebo Radware, které zajišťují identifikaci a zmírnění útoků. Druhou možností je také využívaní DDoS ochrany, kterou mohou zpravovat IT odborníci přímo v obci, mezi tento typy ochrany patří Firewall, Intrusion Detection Systém, DDoS pračka, segmentace sítě nebo rate limiting.

Monitoring sítě a včasná detekce – Dalším krokem pro zlepšení zabezpečení sítě je zavedení systému pro detekci anomálií, protože tyto nástroje dokážou v reálném čase rozpoznat nežádoucí nebo podezřelý provoz a poskytnout automatickou reakci. Mezi spolehlivé nástroje pro monitoring sítě v oblasti ochrany obyvatelstva patří (PRTG Network Monitor, Progress Flowmon a Wireshark).

Spolu s monitoringem sítě je optimální zavést penetrační testování a simulace DDoS útoků, které ověří ochranná opatření a pomohou zajistit slabiny dříve, než je využije skutečný útočník.

Organizační opatření – Součástí technické ochrany proti DDoS útokům by měl být vypracovaný incident response plan. Tento plán určuje specifické akce, role a povinnosti pracovníků při identifikaci a řešení útoků. Spolu s tímto plánem je důležité mít zajištěnou záložní komunikaci.

Záložní komunikace musí být nezávislá na primární síti a zajištěná oddělenou infrastrukturou, například mobilními sítěmi nebo záložním připojením od jiného poskytovatele. Tato komunikace musí být dostatečně zabezpečena. Kontaktní informace a postupy k této záložní komunikaci by měly být přístupné i off-line při výpadku primární infrastruktury.

Spolupráce a komunikace – Mezi poslední ale velmi důležitý pod patří spolupráce s poskytovatelem internetového připojení, který může asistovat při filtrování nebezpečného provozu dříve, než se dostane do sítě MP.

Komunikace s veřejností a národními bezpečnostními organizacemi by měla také patřit mezi primární úkoly při ochraně před DDoS útoky, a to z důvodu včasného informování obyvatel a případné pomoci při incidentu od dalších organizací.

9.2 Scénář Insider threat

Tento typ kybernetického útoku se v subjektech ochrany obyvatelstva objevuje zřídka, ale není vyloučen jeho výskyt a je důležité, aby subjekty byly na tento typ útoku připraveny. Útočníkovou motivací pro tento typ kybernetického útoku je nejpravděpodobněji špatná finanční situace, kterou se touto cestou snaží zvládnout.

Z What-if analýzy vyplývá, že kybernetický útok typu Insider threat můžeme identifikovat podle těchto vyskytujících se anomálií v sítovém provozu (Neobvyklé přístupy k síťovým zdrojům a Chyby v přístupových právech).

Cílem tohoto scénáře je popsat průběh, možné reakce organizace a důsledky kybernetické situace, kdy strážník obchází své pravomoci při práci s IT systémy MP a snaží se získat různá citlivá data občanů a pomocí USB flashdisku s ransomware zašifrovat dokumenty důležité pro krizové řízení a díky následnému vydírání organizace si zajistit benefity v podobě peněžního zisku.

Fáze útoku

Strážník Městské policie, který pracuje u této bezpečnostní složky přes dva roky, se dostal do nepříjemné finanční situace. Při své práci u MP se díky znalostem z oboru IT dostal až k práci, kdy musí také kontrolovat servery a počítače na stanici. Díky tomuto má nepřetržitý přístup ke všem počítačům a serverům, které se nacházejí na stanici. Se svými znalostmi a důkladným pozorováním, jak to v daném prostředí organizace funguje, dostal nápad, jak jednoduše vyřešit své finanční problémy.

V první fázi útoku si strážník připraví důkladný postup, jak se dostat při své rutinní kontrole k hlavnímu serveru na několik minut nepozorován ostatními zaměstnanci. Aby se mu to povedlo, potřebuje dobře znát, kdo z dalších zaměstnanců bude v den útoku na stanici a jaké mají své povinnosti, díky dvouleté práci na stanici tyto informace dobře zná. Spolu s plánem si strážník vytvoří USB flashdisk infikovaný ransomwarem, který díky automatickému spuštění vyhledá a zašifruje data týkající se občanů a krizového řízení. Spolu s automatickým šifrováním dat si útočník na druhý USB flashdisk stáhne citlivá data občanů, jako jsou (Jména, adresy, e-maily, telefonní čísla).

V druhé fázi útoku strážník postupuje důkladně podle svého plánu a vchází na stanici i s připravenými USB flashdisky. Při své kontrole ví že v předem určený čas se může dostat k serveru, aby o něm nikdo nevěděl. Strážník tedy vejde do hlavní místnosti a vloží USB do počítače který má přístup k interní síti. Pokud systém nemá automatickou ochranu USB portů tak se malware automatický spustí a začne hledat cílová data.

V třetí fázi se ransomware šíří do všech možných zařízení nebo serverů a začne šifrovat cílená data o občanech a krizovém řízení. V průběhu šifrování strážník připojí druhý USB flashdisk a začne si kopírovat citlivá data občanů na disk. Až má strážník veškeré data, které potřebuje, nechá ransomware dělat svou práci a opouští místnost. Jelikož strážníkovy končí směna, vydává se domu a čeká, až se vedení MP ozve s výkupným za dešifrovací klíč.

Pokud MP policie nemá vytvořené zálohy veškerých dat na serveru, tak může dojít k úplné paralýze provozu stanice, včetně dispečinku, evidence přestupů i přístupových systému. Bez záloh může být totiž nemožné nebo složitě obnovit ukradená data.

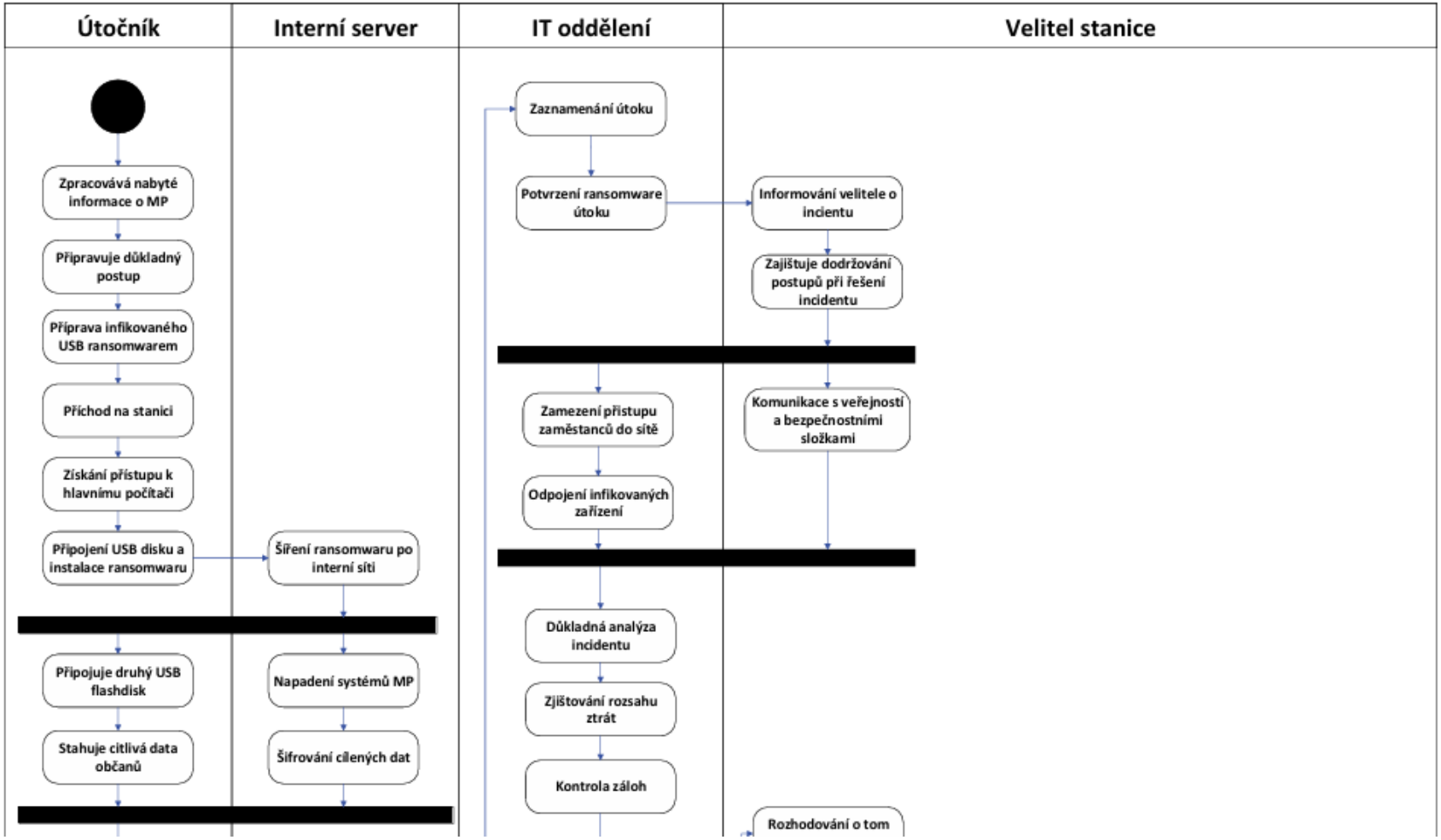
Možné dopady útoku

- Nedostupnost IT systémů a omezení provozní činnosti.
- Únik osobních údajů zaměstnanců a občanů.
- Ztráta důvěry ze strany veřejnosti.
- Ohrožení bezpečnosti zaměstnanců a občanů.
- Právní následky.
- Možné finanční ztráty při obnově dat.

9.2.1 Model scénáře Insider threat

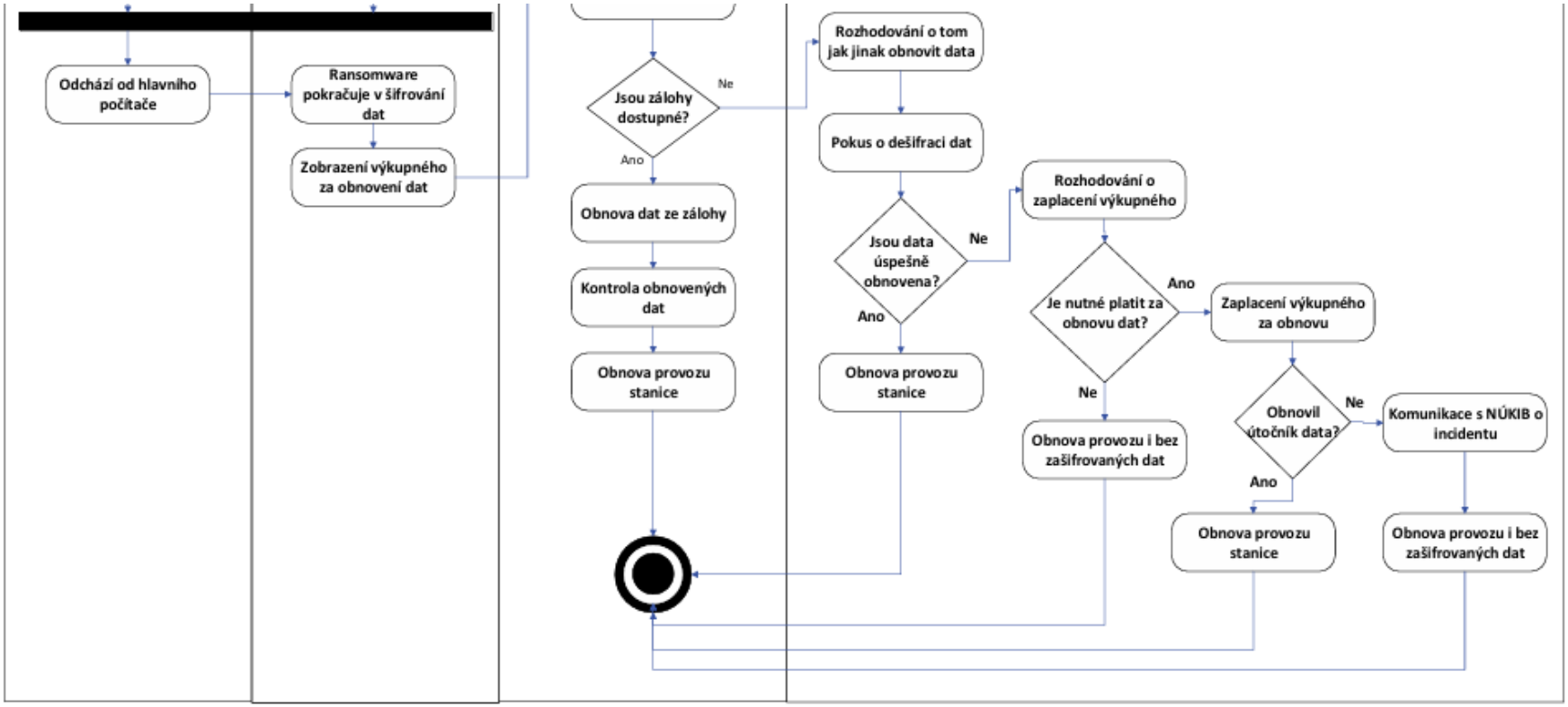
Swimlane diagram scénáře Insider threat nabízí pohled na kybernetický útok, který se nevyskytuje tak pravidelně v bezpečnostních složkách. Vzhledem k přijímacím testům, které se pro tyto pozice provádějí, není tak časté, že zaměstnanec má vlohy pro uskutečnění takové incidentu. V tomto scénáři se útočník ze strany zaměstnance MP snaží infikovat servery pomocí ransomwaru a zašifrovat tak citlivá data spolu s krádeží osobních údajů občanů. Tento útok bývá z principu prováděn za účelem peněžního zisku.

Aby tento incident nevyvolat nedůvěru a paniku mezi občany je důležité brát v potaz fyzické a technické zabezpečení dané stanice. Pokud je subjekt chráněn kamerovým systémem, zámky a možností identifikace přihlašování do systémů, tak mají ostatní zaměstnanci možnosti, jak včas identifikovat útočníka. Spolu s těmito zabezpečeními je důležité pravidelně provádět zálohování dat, aby se předešlo finančním ztrátám při nutné obnově způsobené kybernetickým útokem.



Obrázek 13 - Swimlane diagram č.1 scénáře Insider threat

(Zdroj: Vlastní)



Obrázek 14 - Swimlane diagram č.2 scénáře Insider threat

(Zdroj: Vlastní)

Reakce organizace

Správce sítě může narazit na informační zprávu ohledně zaplacení výkupného za obnovení dat při rutinní kontrole nebo je mu tento incident nahlášen zaměstnancem MP. Při vzniku této hrozby je důležité, aby správce vynaložil veškeré úsilí při obnově těchto dat a také při identifikaci útočníka.

Při snaze identifikovat útočníka by měl správce sítě zkontrolovat přístupy do systémů nebo záznamy z kamer. Díky těmto kontrolám je možné narazit na anomální chovaní daného strážníka, toto chování má obvykle specifické rysy (např: zdržování po pracovní době, velký počet exportovaných dat, časté přihlašování přes VPN, nepodnětné návštěvy stanice mimo pracovní dobu).

Správce při jakémkoliv podezření na bezpečnostní incident je povinen bezodkladně:

1. Zablokovat přístup daného zaměstnance do systému, aby zabránil dalšímu zneužití.
2. Informovat vedení MP a NÚKIB, pokud situace naplňuje znaky kybernetického bezpečnostního incidentu.
3. Zajistit důkazní materiály pro další analýzu a případně trestní řízení.
4. V návaznosti na charakter incidentu informovat ty, jejichž osobní data mohla být odcizena.

Možné reakce na útok

- Zamezení veškerého přístupu všem zaměstnancům do sítě.
- Odpojení napadených zařízení ze sítě.
- Ověření záloh, zda jsou dostupné, pokud nějaké existují.
- Provedení kontroly všech možných datových stop.
- Provedení revize práv a přístupů.
- Zajisti přístup k serveru přes VPN jen oprávněným zařízením.
- Nastavit časovou prodlevu pro přístup.
- Monitorovat veškerou aktivitu zaměstnanců při přístupu na server.
- Nahlášení incidentu na NÚKIB.

Vzhledem k probíhajícímu incidentu je nutné, aby IT pracovníci provedli kontrolu systému a zamezili dalšímu nežádoucímu manipulovaní s daty bez řádného oprávnění. Pokud zašifrovaná data nelze obnovit díky zálohám, je potřeba si pozvat experta, který pomůže obnovit tato data nebo další možností je, aby organizace zaplatila útočníkovi peníze za obnovení.

Slabiny subjektu

- Špatně nastavené přístupové oprávnění a jejich kontrola.
- Absence softwaru pro monitoring připojených USB zařízení.
- Nedostatečné školení personálu v oblasti zacházení s daty.
- Špatně nastavený VPN systém.
- Absence vícefaktorového ověření.

Vzhledem k přijímacím testům, které musí každý strážník podstoupit, není lehké identifikovat u těch, kteří těmito testy prošli další abnormální chování, jenž může být spojováno s možným provedením kybernetického útoku na pracoviště. I když je tato situace ojedinělá, je nutné mít správně nastavená přístupová oprávnění, aby se tyto situace nestávaly.

9.2.2 Opatření proti Insider threat útokům

Při kybernetických útocích hraje lidský faktor stejnou roly jako technická zařízení. Zaměstnanec nebo jiný hacker může díky svému odhodlání přijít na taktiky a metody, jak se dostat do různých systémů a provádět nežádoucí aktivity. Proto je důležité, aby organizace, které uchovávají citlivá data, tykající se organizace nebo občanů dbali důraz na zajištění bezpečnosti jak technické, tak i té personální.

Návrhy na zlepšení ochrany proti Insider threat útokům

- Technická opatření.
- Zálohování a obnova.
- Školení zaměstnanců.
- Incident Response plan a monitoring.

Technická opatření – Ochrana proti vnitřním kybernetickým útokům vyžaduje kombinaci technických a procesních opatření. Základním prvkem je správa přístupových práv – každý zaměstnanec by měl mít přístup pouze k těm oprávněním, která jsou nezbytná

pro výkon jeho práce. Tato práva je nutné pravidelně revidovat a odebírat těm, kteří již u MP nepracují. V případech vzdáleného přístupu pomocí VPN, je vhodné implementovat vícefaktorového ověřování. Důležitým aspektem je i zabezpečení externích médií – doporučuje se zakázat automatické spuštění, povolit pouze ověřené disky a sledovat jejich aktivitu. Tím lze předejít zavlečení malware nebo neoprávněnému přenosu citlivých dat. Technická ochrana by měla být také doplněna o segmentaci sítě, což znamená oddělení klíčových často infrastruktury, aby případný útok nemohl postihnout celou MP.

Zálohování a obnova – Kritické systémy by měly být často zálohovány, přičemž minimálně jedna kopie těchto záloh by měla být uchovávána mimo online prostředí nebo v izolované síti. Důležité je rovněž pravidelně ověřovat možnost obnovy dat, aby bylo možné v případě incidentu rychle obnovit provoz.

Školení zaměstnanců – Lidský faktor často představuje nejslabší článek bezpečnosti. Proto je klíčové vzdělávat zaměstnance v oblastech kybernetické bezpečnosti, správného nakládání s informacemi a schopnosti identifikovat rizikové chování. Doporučuje se také realizovat simulace těchto bezpečnostních incidentů, aby se zvýšila úroveň připravenosti. Rovněž lze do určité míry předejít snahám zaměstnanců o škodlivé jednání tím že informujeme zaměstnance o veškerém logování a monitoringu na stanici.

Incident Response plan a monitoring – Každá organizace by měla mít vypracovaný a pravidelně aktualizovaný plán reakcí na incidenty, který jasně určuje odpovědnosti a postupy. Je dobré zřídit centrální systém pro monitorování a analýzu bezpečnostních logů, jako je například SIEM, který poskytne možnost včas rozpoznat neobvyklé aktivity a spustit okamžitou reakci.

Tato technická a organizační opatření spolu s aktivní komunikací s národními bezpečnostními týmy, jako jsou CSIRT.CZ nebo NÚKIB mohou aktivně přispět ke zlepšení bezpečnosti informací, které jsou ukládány na serveru MP.

ZÁVĚR

Kybernetická bezpečnost a správa IT technologií patří mezi důležitá odvětví při zajištění bezpečnosti jak v běžné domácí síti, tak i v dalších subjektech spojených s kritickou infrastrukturou. Za posledních 5 let se tato oblast více vyvíjí společně s kybernetickými útoky které ohrožují bezpečnost občanů v důsledku ztráty citlivých dat. Je zapotřebí aby, společnost byla informována o vyvíjející se situaci v kyberprostoru a byla společně s bezpečnostními složkami schopna reagovat na kybernetické incidenty.

Hlavním cílem diplomové práce je v souvislosti s detekcí anomálií vytvořit možné scénáře kybernetických útoků na počítačovou síť v subjektu ochrany obyvatelstva. Tyto scénáře byly navrhnuty tak aby otestovaly již stávající opatření, které MP má, ale také aby pomohly odhalit slabiny v softwarovém zabezpečení.

V praktické části jsou analyzovány softwary, které jsou nejen vhodné pro běžné uživatele počítačových technologií ale i pro pokročilejší správce sítí ve větších firmách nebo subjektech ochrany obyvatelstva. Pomocí těchto softwarů byly identifikovány a popsány nejčastější anomálie které se mohou vyskytovat v sítích. Nedostatečné zajištění těchto anomálií a jejich kontrola může otevřít nežádoucí přístupy pro hackery kteří se snaží dostat k citlivým informacím. Na základě těchto poznatků byly analyzovány pomocí metody SWOT krizové plány v obci s rozšířenou působností, kde působí vybraný subjekt ochrany obyvatelstva, jímž je městská policie. Pro zjištění současné stavu byl vytvořen a zpracován rozhovor s vedoucím pracovníkem o problematice bezpečnosti sítě v subjektu. Informace získané ze What-if analýzy a rozhovoru byly klíčové k tvorbě scénářů kybernetických útoků na jejich základě by mohla být otestována opatření která městská policie využívá při zajištění bezpečnosti informací. Scénáře byla strukturovány tak aby cílili na oblasti a technologie které subjekt nevyužívá při zajištění bezpečnosti informací a byly navrženy opatření ke zlepšení a aktualizaci krizových plánů.

Hlavní cíl práce a dílčí cíle byly splněny. Přínosem práce je získání znalostí v oblasti monitorování sítě a možnost vyzkoušet v podpůrných subjektech ochrany obyvatelstva jejich zabezpečení proti důkladnějším kybernetickým útokům.

Závěrem lze konstatovat že neustálé informování a kontrola připravenosti v oblasti kybernetických útoků je velmi důležitá pro zajištění bezpečnosti subjektů a tím ovlivnit celý průběh těchto incidentů. Citlivá data občanů budou pořád nejčastějším důvodem k provádění těchto útoku, a proto je nutné zajistit dostatečnou bezpečnost, aby nebyly zneužity.

SEZNAM POUŽITÉ LITERATURY

About Wireshark, ©2025. Online. Wireshark. Dostupné z: https://www.wireshark.org/about.html. [cit. 2025-03-31].

All MS Windows Devices, © 2025. Online. In: LogicMonitor. Dostupné z: https://www.logicmonitor.com/integrations/windows. [cit. 2025-04-02].

ARP Spoofing, © 2025. Online. Impreva. Dostupné z: https://www.imperva.com/learn/application-security/arp-spoofing/. [cit. 2025-03-31].

BROOKS, Charles J.; GROW, Christopher; CRAIG, Philip a SHORT, Donald, 2018. *Cybersecurity essentials*. Indianapolis, Indiana: Sybex, John Wiley. ISBN 978-1-119-36239-5.

BURDA, Karel, 2019. Kryptografie okolo nás. CZ.NIC. Praha: CZ.NIC, z.s. p.o. ISBN 978-80-88168-49-2.

C. VAN OORSCHOT, Paul, 2021. Computer Security and the internet. Springer Nature Switzerland. ISBN 3030834107.

Co je deep web? A jak se liší od dark webu? © 1994–2025. Online. Alza.cz. 2019. Dostupné z: https://www.alza.cz/co-je-deep-web. [cit. 2025-03-31].

Co je monitoring sítě a proč ho používat, © 2021. Online. Awin IT. Praha: ESET, spol. s r.o, 2022. Dostupné z: https://www.awinit.cz/blog/co-je-monitoring-site-a-proc-ho-pouzivat/. [cit. 2025-03-31].

Co je monitorování sítě? © 2025. Online. Upit. Praha: ESET, spol. s r.o. Dostupné z: https://upit.cz/bezpecnost/co-je-monitorovani-site/. [cit. 2025-03-31].

Co je PRTG a k čemu se používá? © 2020. Online. Monitoruj. Dostupné z: https://www.monitoruj.cz/poradna/co-je-prtg-a-k-cemu-se-pouziva/. [cit. 2025-04-03].

Co je sniffing, © 2022. Online. Správa sítě. Praha: ESET, spol. s r.o. Dostupné z: https://www.sprava-site.eu/sniffing/. [cit. 2025-03-31].

Co je to IP adresa? © 1994–2025. Online. Alza.cz. 2021. Dostupné z: https://www.alza.cz/co-je-ip-adresa. [cit. 2025-02-15].

Co je to monitoring sítě, © 2022. Online. Správa sítě. Praha: ESET, spol. s r.o. Dostupné z: https://www.sprava-site.eu/monitoring-site/. [cit. 2025-03-31].

Co je to monitoring sítě, © 2022. Online. Správa sítě. Praha: Aira GROUP. Dostupné z: https://www.sprava-site.eu/monitoring-site/. [cit. 2025-03-05].

Co to je VPN a proč si ji pořídit? © 1992–2025. Online. Eset. Praha: ESET, spol. s r.o. Dostupné z: https://www.eset.com/cz/vpn/. [cit. 2025-03-31].

ČAMEK, Jiří. *Návrh praktické úlohy pro potřeby kybernetické laboratoře*. Bakalářská, vedoucí Svoboda, Petr. Zlín: Univerzita Tomáše Bati ve Zlíně. Fakulta logistiky a krizového řízení, Ústav ochrany obyvatelstva, 2023. Dostupné také z: http://digilib.k.utb.cz/handle/10563/54541.

ČESKO. Vyhláška č. 205/2016 Sb., vyhláška, kterou se mění vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích. In: Zákony pro lidi.cz [online]. © AION CS 2010–2025 [cit. 14. 4. 2025]. Dostupné z: https://www.zakonyprolidi.cz/cs/2016-205

ČESKO. Vyhláška č. 573/2020 Sb., vyhláška, kterou se mění vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby. In: Zákony pro lidi.cz [online]. © AION CS 2010–2025 [cit. 14. 4. 2025]. Dostupné z: https://www.zakonyprolidi.cz/cs/2020-573

ČESKO. Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti). In: Zákony pro lidi.cz [online]. © AION CS 2010–2025 [cit. 14. 4. 2025]. Dostupné z: https://www.zakonyprolidi.cz/cs/2018-82

ČESKO. Zákon č. 110/2019 Sb., o zpracování osobních údajů. In: Zákony pro lidi.cz [online]. © AION CS 2010–2025 [cit. 14. 4. 2025]. Dostupné z: https://www.zakonyprolidi.cz/cs/2019-110

ČESKO. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: Zákony pro lidi.cz [online]. © AION CS 2010–2025 [cit. 14. 4. 2025]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181

ČESKO. Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. In: Zákony pro lidi.cz [online]. © AION CS 2010–2025 [cit. 14. 4. 2025]. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-412

DDoS útok, © 1992–2025. Online. ESET. Praha: ESET, spol. s r.o. Dostupné z: https://www.eset.com/cz/ddos-utok/. [cit. 2025-01-22].

Device Tree View Layout, © 2025. Online. In: Paessler. Dostupné z: https://www.paessler.com/manuals/prtg/general_layout. [cit. 2025-04-14].

Digitální a analogové signály a průběhy, © 2025. Online. Electronic Components. 2024. Dostupné z: https://www.tme.eu/cz/news/library-articles/page/61486/digitalni-a-analogove-signaly-a-prubehy/. [cit. 2025-03-31].

DNS Spoofing, © 2025. Online. Imperva. Dostupné z: https://www.imperva.com/learn/application-security/dns-spoofing/. [cit. 2025-03-31].

DNS Spoofing: DNS Spoofing Attack Methods, © 2025. Online. In: Imperva. Dostupné z: https://www.imperva.com/learn/application-security/dns-spoofing/. [cit. 2025-03-31].

DOSTÁLEK, Libor, 2003. *Velký průvodce protokoly TCP/IP: Bezpečnost*. 3. aktualiz. vyd. Praha: Computer Press. ISBN 80-722-6849-X.

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

Download Wireshark, © 2025. Online. In: Wireshark. Dostupné z: https://www.wireshark.org/download.html. [cit. 2025-04-06].

EDR vs NDR vs XDR, © 2025. Online. SentinelOne. Dostupné z: https://www.sentinelone.com/cybersecurity-101/endpoint-security/edr-vs-ndr-vs-xdr/#what-is-edr. [cit. 2025-04-18].

EVANS, Lester, 2019. *Cybersecurity: what you need to know about computer and cyber security, social engineering, the internet of things an esential guide to ethical hacking for beginners*. USA: Lester Evans. ISBN 978-1-7946-4723-7.

FUJAK, Radek, 2022. *10 nejčastějších typů kybernetických útoků 10 nejčastějších typů kybernetických útoků*. Online. Datasys. Dostupné z: https://www.datasys.cz/10-nejcastejsich-typu-kybernetickych-utoku/. [cit. 2025-08-02].

HENDL, Jan, 2021. Big data. Průvodce. Praha: Grada Publishing. ISBN 978-80-271-3031-3.

HORÁK, Jaroslav a KERŠLÁGER, Milan, 2011. *Počítačové sítě pro začínající správce*. 5., aktualiz. vyd. Brno: Computer Press. ISBN 978-80-251-3176-3.

HUB, Miloslav, 2013. *Bezpečnost a ochrana informací v prostředí internetu*. Pardubice: Univerzita Pardubice. ISBN 978-80-7395-701-8.

IDS/IPS: Ochrana sítě před hrozbami a útoky, © 2004–2025. Online. My Dreams. Dostupné z: https://www.mydreams.cz/cz/wiki/290-ids-ips-ochrana-site-pred-hrozbami-a-utoky.html. [cit. 2025-04-18].

Jak detekovat a reagovat na anomálie v síťovém provozu? © 2004–2025. Online. My Dreams. Dostupné z: https://www.mydreams.cz/cz/wiki/4096-jak-detekovat-a-reagovat-na-anomalie-v-sitovem-provozu.html. [cit. 2025-03-31].

JIROVSKÝ, Václav, 2007. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada. ISBN 978-80-247-1561-2.

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

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

Kybernetická bezpečnost, © 2009–2025, 2021. Online. Vláda České republiky. Praha. Dostupné z: https://www.vlada.cz/cz/evropske-zalezitosti/umela-inteligence/kyberneticka_bezpecnost/kyberneticka-bezpecnost-192766/. [cit. 2025-03-10].

Kybernetická bezpečnost, © 2025. Online. Q-COM. Brno. Dostupné z: https://www.qcom.cz/systemy-rizeni/zokb/. [cit. 2025-03-10].

Malware, © 2025. Online. Malwarebytes. Dostupné z: https://www.malwarebytes.com/malware. [cit. 2025-03-15].

Man-in-the-Middle (MITM), © 1992–2025. Online. Eset. Praha: ESET, spol. s r.o. Dostupné z: https://www.eset.com/cz/slovnik/co-je-to-man-in-the-middle-mitm/. [cit. 2025-03-31].

Městská policie. Online. Rýmařov oficiální webové stránky města. Dostupné z: https://www.rymarov.cz/mestska-policie. [cit. 2025-04-14].

Nástroje pro monitorování sítě, © 2004–2025. Online. Solutia. Dostupné z: https://www.solutia.cz/2024/01/02/nastroje-pro-monitorovani-site/#toc_4_kategorie_nastroju_pro_monitorovani_site. [cit. 2025-03-31].

NetWorx, © 2000–2025. Online. SoftPerfect. Dostupné z: https://www.softperfect.com/products/networx/. [cit. 2025-03-31].

Obecné informace o směrnici NIS2, © 2025. Online. Porátl NÚKIB. Dostupné z: https://portal.nukib.gov.cz/informacni-servis/podpurne-materialy/67865ea9e8e3c7573907a500. [cit. 2025-04-14].

Phishing, © 1992–2025. Online. Praha: ESET, spol. s r.o. Dostupné z: https://www.eset.com/cz/phishing/. [cit. 2025-03-12].

Postupy řešení krizové, havarijní situace: Ochrana IT technologií, 2022. MÚ Rýmařov.

Ransomware, © 1992–2025. Online. Praha: ESET, spol. s r.o. Dostupné z: https://www.eset.com/cz/ransomware/. [cit. 2025-03-12].

Ransomware, © 2025. Online. Malwarebytes. Dostupné z: https://www.malwarebytes.com/malware. [cit. 2025-03-12].

Řešení Flowmon, ©2025. Online. Progress. Dostupné z: https://www.progress.com/cs/flowmon. [cit. 2025-03-31].

SEDLÁK, Petr a KONEČNÝ, Martin, 2021. Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru. Vydání: první. Brno: CERM, akademické nakladatelství. ISBN 978-80-7623-068-2.

Síťová ochrana (VPN, FW, GW, SD-WAN), © 2025. Online. Aricoma. Praha: ESET, spol. s r.o. Dostupné z: https://www.aricoma.com/cs/co-delame/kyberneticka-bezpecnost/bezpecnost-it-infrastruktury-a-cloudu/sitova-ochrana-vpn-fw-gw-sd-wan. [cit. 2025-03-31].

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.

The Parkerian Hexad, © 2012. Online. PENDER-BEY, Georgie. Dostupné z: https://cs.lewisu.edu/mathcs/msisprojects/papers/georgiependerbey.pdf. [cit. 2025-03-08].

The Parkerian Hexad, © 2025. Online. Staffhost Europe. Dostupné z: https://www.sciencedirect.com/topics/computer-science/parkerian-hexad. [cit. 2025-03-27].

Typový plán: Narušení bezpečnosti infromací kritické informační infrastruktury, MÚ Rýmařov.

Typy sítí, © 2022. Online. PC Síť. Dostupné z: https://pcsit.estranky.cz/clanky/typy-siti/. [cit. 2025-03-31].

Understanding Denial-of-Service Attacks, © 2010–2025, 2021. Online. Cisa.gov. Cybersecurity and Infrastructure Security Agency. Washington D.C. Dostupné z: https://www.cisa.gov/news-events/news/understanding-denial-service-attacks. [cit. 2025-03-12].

Vládní návrh Zákon o kybernetické bezpečnosti, 2024. In: Dostupné také z: https://www.zakonyprolidi.cz/media2/file/2401/File64629.pdf?attachment-filename=7704636-2023-07-19-text-navrhu-7824803.pdf.

What is LogicMonitor, © 2025. Online. LogicMonitor. Dostupné z: https://www.logicmonitor.com/support/about-logicmonitor/overview/what-is-logicmonitor. [cit. 2025-04-02].

Zero day útok, © 1992–2025. Online. Eset. Praha: ESET, spol. s r.o. Dostupné z: https://www.eset.com/cz/zero-day/. [cit. 2025-03-31].

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ARP Addresss Resolution Protocol

DDoS Distributed Denial of Service

DNS Domain Name Server

DoS Denial of Service

DRDoS Distributed Reflected Denial of Service

ICT Informační a komunikační technologie

IP Internet Protocol

IT Informační technologie

LAN Lokální síť

MAN Metropolitní síť

MP Městská policie

PAN Osobní síť

RSA Rivest-Shamir-Adleman

SNMP Simple Network Management Protokol

TCP Transmission Control Protocol

VPN Virtuální privátní síť

WAN Vzdálená

SEZNAM PŘÍLOH

PŘÍLOHA P I: ROZHOVOR

Tazatel: Bc. Jiří Čamek

Jméno respondenta: Michal

T: Jaké technické vybavení (počítače, rádia, mobily) denně při práci používáte?

R: Denně při práci jako policista používám firemní počítač a mobil. Při běžném provozu pro různé zápisy a komunikaci s ostatními zaměstnanci.

T: Fungují všechna zařízení přes jednu společnou síť, nebo máte různé systémy pro různé účely?

R: Naše pracoviště funguje na propojené síti Městského úřadu.

T: Setkáváte se někdy s problémy při připojení k síti nebo při práci se služebním systémem?

R: Při mém působení tady na pracovišti nikdy nedošlo k žádným problémům tohoto typu.

T: Jakou roli hraje IT infrastruktura v každodenním chodu MP Rýmařov?

R: Soužití s IT infrastrukturou je pro nás strážníky důležité. Bez technologií nejde efektivně fungovat. Naše pracovní schopnost je snížena tak na 40 %.

T: Kdo nese zodpovědnost za správu a bezpečnost počítačové sítě – řešíte to interně, nebo máte externí IT podporu?

R: Máme externí IT pracovníky v obci, kteří jsou schopni nám pomoci.

T: Máte zpracovanou oficiální strategii nebo plán pro zabezpečení sítě? Jak často se aktualizuje?

R: Veškeré tyto plány mají IT pracovníci a oni je korigují.

T: Jak je nastavena odpovědnost za případné bezpečnostní incidenty – kdo je řeší a jaký je váš postup?

R: Situaci řeší pracovník IT telefonicky nebo přijedou na služebnu. Já osobně kdybych způsobil tuto situaci a ohrozil bych IT infrastrukturu tak bych měl za povinnost absolvovat školení k tomu určené.

T: V jaké míře jsou vaši zaměstnanci školeni v oblasti kybernetické bezpečnosti?

R: Zaměstnanci mají obecné informace o kybernetické bezpečnosti. Průběžně probíhá hromadné informování 1 x měsíčně na poradě o nových hrozbách a o konkrétních situacích které se dějí na území ČR.

T: Máte vypracovaný plán reakce na mimořádné události typu kybernetického útoku nebo ztráty dat?

R: Ano existují typové plány pro tyto události.

T: Máte přehled o hlavních bezpečnostních opatřeních (např. firewall, antiviry, zálohování)?

R: Firewall a antiviry jsou na služebních počítačích, zálohování dat provádí pravděpodobně IT pracovník.

T: Využíváte některé pokročilé technologie pro ochranu dat (např. šifrování, VPN, dvoufázové ověření)?

R: Na služebně žádné tyto technologie nevyužíváme.

T: Jaké máte postupy pro řízení přístupů do systémů (např. správa uživatelských práv)?

R: Každý zaměstnanec má své vlastní přístupové údaje.

T: Zažil jste během svého působení na stanici nějaký významnější IT incident? Jak probíhalo jeho řešení?

R: Za 26 let co u police pracuji se žádná tato situace nestala.

T: Jak hodnotíte připravenost vašich systémů i lidí čelit bezpečnostním hrozbám?

R: Vzhledem k tomu že jsme tady za dlouhou dobu nemuseli žádnou tuto hrozbu řešit tak připravenost systémů funguje efektivně jak má.

T: Plánujete v blízké budoucnosti nějaké investice nebo změny v oblasti kybernetické bezpečnosti?

R: S novým zákonem o kybernetické bezpečnosti určitě přijdou nějaké nové změny.

T: Jak hodnotíte spolupráci s městem nebo jinými složkami při zajištění bezpečnosti?

R: Spolupráce s ostatními složkami a IT pracovníky je vzájemná a komunikace probíhá bez problému.

T: Jak vnímáte vaši roli v oblasti IT bezpečnosti? Připadá vám, že se dnes od zaměstnanců očekává i technologický přehled?

R: Osobně nemusím řešit tyto problémy jen předám informaci dál IT oddělení.

Já sám mám velmi dobrý technologický přehled a v této oblasti jsem přizpůsobivý novým věcem.

T: Kdybyste měl neomezené možnosti – co byste v oblasti bezpečnosti zlepšil jako první?

R: Určitě bych to chtělo zlepšit finanční podporu veškerých pracovišť, která se starají o ochranu obyvatelstva.

T: Máte pocit, že úroveň IT bezpečnosti odpovídá důležitosti vaší práce v rámci města?

R: Dle mého osobního názoru je úroveň IT bezpečnosti na dostatečné úrovni vzhledem k tomu že výskyt kybernetických hrozeb je nízký.

T: Tak to jsou za mě všechny otázky. Děkuji za váš čas.