Stalkerware v podmínkách subjektu ochrany obyvatelstva

Bc. Radim Pešák

Diplomová práce
2022

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: 2021/2022

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Radim Pešák**
Osobní číslo:	**L20201**
Studijní program:	**N1032A020002 Bezpečnost společnosti**
Specializace:	**Ochrana obyvatelstva**
Forma studia:	**Kombinovaná**
Téma práce:	**Stalkerware v podmínkách subjektu ochrany obyvatelstva**

Zásady pro vypracování

1. Zpracujte literární rešerši současného stavu předmětné oblasti.
2. Zvolte vhodný subjekt ochrany obyvatelstva v kontextu následného řešení problematiky hrozby stalkerware.
3. Analyzujte současný stav vybraného subjektu ochrany obyvatelstva v kontextu hrozby stalkerware.
4. Navrhněte opatření pro zlepšení současného stavu vybraného subjektu ochrany obyvatelstva v kontextu hrozby stalkerware.

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

Seznam doporučené literatury:

1. BARKER, Dylan. *Malware Analysis Techniques: Tricks for the triage of adversarial software.* Packt Publishing, 2021. ISBN 978-1839212277.
2. JOHNSON, Thomas A. *Cybersecurity: protecting critical infrastructures from cyber attack and cyber warfare.* Boca Raton: CRC Press/Taylor and Francis Group, 2015. ISBN 9781482239225.
3. SMEJKAL, Vladimír, Tomáš SOKOL a Jindřich KODL. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. ISBN 978-80-7380-765-8.

Další odborná literatura dle doporučení vedoucího diplomové práce.

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

Datum zadání diplomové práce: **1. prosince 2021**
Termín odevzdání diplomové práce: **6. května 2022**

L.S.

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

prof. Ing. Dušan Vičar, CSc.
ředitel ústavu

V Uherském Hradišti dne 1. prosince 2021

PROHLÁŠENÍ AUTORA
DIPLOMOVÉ PRÁCE

Beru na vědomí, že:

- diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- 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 autorského zákona 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 samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

V Uherském Hradišti, dne: 5. 8. 2022

Jméno a příjmení studenta: Bc. Radim Pešák

.....
podpis studenta

ABSTRAKT

Diplomová práce se zabývá problematikou stalkerwaru v podmínkách subjektu ochrany obyvatelstva. V teoretické části práce mapuje zdroje a shrnuje danou problematiku za účelem jejího dostatečného pochopení. Praktická část je zaměřena na analýzu interní dokumentace kybernetické bezpečnosti Městského úřadu ve Vyškově, a to ve všech aspektech bezpečnosti, které může potenciální útočník prolomit ke stalkování své oběti. Na základě zjištěných informací byl vytvořen prototyp desktopové aplikace s názvem Secura, která má za cíl zvýšit povědomí zaměstnanců v oblasti hrozby stalkerware, lépe je zabezpečit, vzdělávat je a následně jejich vědomosti otestovat.

Klíčová slova: informační systém, kybernetická bezpečnost, malware, stalkerware, subjekty ochrany obyvatelstva, školicí aplikace

ABSTRACT

The diploma thesis deals with the issue of stalkerware in the Population Protection. The theoretical part of the thesis maps the sources of information and summarizes the whole issue in order to understand it sufficiently. The practical part is focused on the analysis of internal cyber security documentation of the Municipal Office in Vyškov, in all aspects of security that a potential attacker can break to stalk his victim. Based on the information obtained, a prototype of a desktop application called Secura was created, which aims to increase the awareness of employees in the area of the stalkerware threat, better secure them, educate them and then test their knowledge.

Keywords: information system, cyber security, malware, stalkerware, population protection, training application

Chtěl bych poděkovat v prvé řadě svému vedoucímu diplomové práce Ing. Petru Svobodovi, Ph.D., který mi poskytl odbornou pomoc a cenné rady a také mě vždy podporoval ve všech mých návrzích. Dále bych chtěl poděkovat celé své rodině, která mě po celou dobu studia nesmírně podporovala.

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

OBSAH

ÚVOD

Světové ekonomické fórum považuje hrozby pro kybernetickou bezpečnost za jedno z pěti největších globálních rizik, kterým dnes čelí národy světa. Kybernetické hrozby se stále více zaměřují na klíčové funkce ekonomik v jednotlivých zemích světa, stejně jako na jejich vlády na místní, regionální a národní úrovni. Potenciál kybernetických útoků narušit kritické služby soukromých podniků a nevládních agentur roste alarmujícím tempem.

Obrana proti možným útokům motivovaných skupin nebo jednotlivců, které mohou narušit kritické služby, napadnout kritickou infrastrukturu a způsobit řadu poškození, od velkého narušení ekonomiky, až po masivní fyzické zničení, je stále obtížnější. Rostoucí je i hrozba kybernetických útoků na ministerstvo obrany a jeho vojenské prostředky, jelikož kybernetické útoky by mohly vážně narušit nebo deaktivovat armádní systémy velení a řízení, stejně jako komunikaci, zpravodajství a systémy společného velení, což by mělo za následek ohrožení národní bezpečnosti.

V současné době procházíme velkým souborem celoodvětvových transformačních změn, které prohlubují problémy v oblasti kybernetické bezpečnosti. Tyto transformační výzvy se objevují v důsledku virtualizace, sociálních médií, internetu věcí, cloud computingu, strukturovaných a nestrukturovaných dat, velkých dat, datové analytiky apod. Potenciální dopady, které tyto transformační změny budou mít na oblast kybernetické bezpečnosti, budou obrovské a budou vyžadovat další školení a vzdělávací kurzy.

Téměř každý kybernetický útok využívá hrozby malware a počet takových útoků se každým dnem zvyšuje a útočníci jsou čím dál odvážnější. Miliony malwaru se vyskytují na zařízeních každý den, ale není dostatek analytiků, kteří by se s tím vším vypořádali. Objem unikátních druhů malwaru, podobně jako objem dat přenášených internetem každým rokem rychle roste. Dříve se jednalo o stovky až tisíce vzorků denně, které cílily spíše na průmyslové sektory jako bankovnictví, finanční sektor a vládu. V dnešní době jde o miliony vzorků malwaru, které cílí i na běžné uživatele. Dříve vznikal malware za účelem zisku, ale data jsou nyní největší měnou v každém aspektu našeho života a také se stala primárním cílem malwaru.

Jeden typ počítačové kriminality, který má potenciál způsobit utrpení a napáchat škody, se nazývá kyberstalking. Kybernetické pronásledování je definováno jako používání internetu nebo jiných elektronických prostředků k obtěžování, zastrašování, vyhrožování, sledování obětí. Může zahrnovat přímé obtěžování prostřednictvím e-mailů, chatovacích místností

a sociálních sítí, nebo se využívá tajného shromažďování důvěrných informací pomocí softwaru či hardwaru, nainstalovaných na zařízení oběti.

Kyberstalkeři často obtěžují své oběti zcela anonymně pomocí stalkerwaru. Stalkerware disponuje širokou škálou funkcí, včetně všudypřítomného sledování textových zpráv a online konverzací, nahráváním telefonních hovorů, sledováním příspěvků na sociálních sítích, sledováním návštěv webových stránek, aktivací systému GPS, zaznamenáváním stisknutích kláves, a dokonce i aktivací mikrofonů či web kamery, stejně jako blokováním příchozích telefonních hovorů. Těmito funkcemi stalkerware disponuje velkou mocí a kontrolou nad každodenním životem jedince.

Diplomová práce se zabývá analýzou stávající bezpečnostní politiky Městského úřadu ve Vyškově a tvorbou desktopové aplikace, která si klade za cíl zvýšit povědomí zaměstnanců v oblasti hrozby stalkerware a tím snížit budoucí riziko nákazy.

CÍLE A METODY

Hlavní cíl

Návrh uživatelského rozhraní a funkcionalit aplikace zaměřené na osvětu a ochranu před hrozbou stalkerware a vybraných hrozeb kybernetické bezpečnosti.

Dílčí cíle

Dílčí cíle slouží k naplnění hlavního cíle a jsou následující:

- Rešerše předmětné problematiky.
- Výběr subjektu ochrany obyvatelstva pro snížení míry rizika hrozby stalkerware a dalších vybraných kybernetických hrozeb.
- Analýza interních dokumentů kybernetické bezpečnosti vybraného subjektu vzhledem k určení úrovně kybernetické bezpečnosti a ochraně před stalkerware.
- Návrh funkcionalit aplikace sloužící ke zvýšení úrovně kybernetické bezpečnosti a ochraně před stalkerware vybraného subjektu ochrany obyvatelstva.
- Návrh uživatelského rozhraní aplikace sloužící ke zvýšení úrovně kybernetické bezpečnosti a ochraně před stalkerware vybraného subjektu ochrany obyvatelstva.

V diplomové práci je využito mnoho vědeckých metod. Jednou z nich je literární rešerše, jejímž cílem bylo sesbírat co nejvíce dostupných informací a seznámit se s veškerými odbornými pojmy z oblasti kybernetické bezpečnosti, subjektů ochrany obyvatelstva a malwaru. Dále byly využiti následující vědecké metody:

- Analýza – při zpracování teoretické a praktické části byla použita dostupná literatura, platné právní předpisy, časopisy, články a dostupné internetové zdroje.
- Syntéza – metoda je použita v rámci celé diplomové práce.
- Dedukce – závěrečná část praktické části vychází z metody dedukce, kdy se na základě logické posloupnosti jednotlivých kroků formulovalo uživatelské prostředí aplikace.
- Deskripce – tato metoda byla použita v praktické části při popisu uživatelského prostředí aplikace sloužící ke zvýšení úrovně kybernetické bezpečnosti a ochraně před stalkerwarem.

- Vedený rozhovor – poznatky z rozhovoru byly využity v praktické části při analýze bezpečnostní politiky Městského úřadu ve Vyškově.

I. TEORETICKÁ ČÁST

1 ÚVOD DO PROBLEMATIKY

Rizika, která se pojí se zabezpečením vlastních dat a systémů, se dotýkají každého uživatele, který používá informační technologie. Rozsah systémů připojených k internetu se značně zvýšil a tyto systémy jsou více než kdy jindy vystaveny kybernetickým útokům. Složitost a dynamika kybernetických útoků vyžaduje, aby ochranné mechanismy byly citlivé, adaptivní a škálovatelné. (Nguyen, Reddi, 2021)

1.1 Právní předpisy

Četnost využívání informačních technologií a celková závislost společnosti na jejich fungování přispělo k nutnosti přijmout závazné právní úpravy, které budou regulovat oblast kybernetické bezpečnosti. Oblast kybernetické bezpečnosti je jednou z klíčových oblastí bezpečnostního prostředí České republiky. (Hromada et al., 2015)

Primárním dokumentem, který popisuje hlavní principy, na kterých stojí kybernetická bezpečnost v České republice (ČR), je Národní strategie kybernetické bezpečnosti ČR 2021–2025. Tento dokument rovněž definuje strategické směřování v oblasti kybernetické bezpečnosti a její vize. Vize zní, aby ČR měla odolnou společnost a infrastrukturu a v kyberprostoru bude schopna aktivně čelit kybernetickým hrozbám za pomoci spolehlivých spojenectví. Dalším neméně důležitým dokumentem je Koncepce rozvoje Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB) z roku 2020. Koncepce si klade za cíl stabilizovat, dobudovat a stále rozvíjet kapacity NÚKIB. (NÚKIB, 2020)

Kybernetická bezpečnost je dále upravena zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů. Zákon nabyl účinnosti od 1. ledna 2015 a upravuje práva a povinnosti osob a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti. Klade si za cíl předcházet vzniku kybernetických incidentů a pokud k nějakému dojde, tak zabránit ohrožení celkového fungování informačních a komunikačních systémů. Je založen na třech pilířích:

- Bezpečnostní opatření.
- Hlášení kybernetických incidentů.
- Opatření úřadu. (Smejkal, Sokol a Kodl, 2015)

Dále je založen na zásadách:

- Snaha minimalizovat zásahy do práv soukromých objektů.
- Individuální odpovědnost každého subjektu za bezpečnost vlastní sítě.
- Technologická neutralita. (Hromada et al., 2015)

Mezi prováděcí předpisy vztahující se k zákonu o kybernetické bezpečnosti patří:

- Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti („Vyhláška o kybernetické bezpečnosti“). Tato vyhláška nabyla účinnosti dne 28. května 2015. (Česko, 2018)
- Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích („Vyhláška o VIS“). Vyhláška nabyla účinnosti dne 1. ledna 2015.
- Novelizované nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury („Nařízení o kritériích pro určení prvku KI“). Novelizované znění nařízení nabylo účinnosti dne 1. ledna 2015. (Hromada et al., 2015)

1.1.1 Evropské regulace

Na půdě Evropské unie (EU) začalo v roce 2013 fungovat Evropské centrum pro boj proti kybernetické kriminalitě. Ve vytvoření tohoto střediska hrála klíčovou roli Evropská komise a funguje v rámci Evropského policejního úřadu (Europol). Svou činnost směřuje na ochranu fyzických a právnických osob před nezákonnými činnostmi na internetu prováděnými organizovanými zločineckými skupinami. (Hromada et al., 2015)

V roce 2013 byla přijata Strategie pro kybernetickou bezpečnost EU. Jsou v ní definovány základní principy, jejichž plnění by mělo dopomoci k udržení kybernetické bezpečnosti. Ve strategii je stanoveno pět základních pilířů, kterých chce dosáhnout:

- Dosažení kybernetické způsobilosti.
- Redukce kybernetické kriminality.
- Příprava politik k obraně proti kybernetickým útokům.
- Vyvinutí průmyslových a technologických zdrojů pro kybernetickou bezpečnost.
- Zavedení mezinárodní politiky pro kybernetickou bezpečnost, odrážející evropské hodnoty. (Hromada et al., 2015)

Závěrem roku 2020 byla představena nová Strategie pro kybernetickou bezpečnosti EU. Cílem nové strategie je zajistit globální a otevřený internet se silnými zárukami tam, kde existují rizika pro bezpečnost a základní práva lidí v Evropě. V návaznosti na pokrok dosažený v rámci předchozích strategií obsahuje konkrétní návrhy na nasazení tří hlavních nástrojů. Mezi tyto nástroje patří regulace, investice a politická iniciativa. (European Commission, 2021)

1.1.2 Základní normy řady 27000

Mezinárodní organizace pro normalizaci (ISO) je celosvětová federace národních normalizačních orgánů (členů ISO). Mezinárodní normy jsou zpracovány technickými komisemi ISO. Každý člen, který se zajímá o předmět, pro který byla vytvořena technická komise, má právo být v této komisi zastoupen. Na zpracování norem se podílely rovněž vládní i nevládní mezinárodní organizace a také došlo k úzké spolupráci s Mezinárodní elektrotechnickou komisí (IEC) ve všech záležitostech normalizace v oblasti elektrotechniky. (ISO/IEC 27000, 2018)

ISO/IEC 27000

Norma Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník popisuje základy systémů řízení bezpečnosti informací, které tvoří předmět rodiny norem systémů řízení bezpečnosti informací (ISMS) a definuje související pojmy pro další normy z této série. Skupina norem má pomoci se zavedením a provozováním systému ISMS ve všech typech organizací. (ISO/IEC 27000, 2018)

ISO/IEC 27001

Norma Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky. Tento dokument specifikuje požadavky na zřízení, implementaci, provoz, monitorování, kontrolu, údržbu a zlepšování formalizovaných ISMS v kontextu celkových obchodních rizik organizace. Specifikuje požadavky na implementaci kontrol informační bezpečnosti přizpůsobených potřebám jednotlivých organizací nebo jejich částí. Tento dokument mohou používat všechny organizace bez ohledu na typ, velikost a povahu.

Norma rovněž uplatňuje zavedení procesu k řešení ISMS, tzv. model PDCA (plan-do-check-act), který lze využít pro všechny procesy ISMS tak, jak povoluje norma. Norma je

propojena s normou pro systémy řízení jakosti ISO 90001 a ISO 14001 pro systém řízení ochrany životního prostředí. (Hrůza, 2012; ISO/IEC 27000, 2018)

ISO/IEC 27002

Norma Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací. Tento dokument poskytuje seznam běžně přijímaných kontrolních cílů a kontrol osvědčených postupů, které se mají použít jako vodítko pro implementaci při výběru a zavádění kontrol pro dosažení bezpečnosti informací. Obsahuje více než 5000 přímých a odvozených bezpečnostních opatření, která vedou k dosažení podnikatelských cílů. (ISO/IEC 27000, 2018)

ISO/IEC 27032

Norma řeší otázky bezpečnosti kyberprostoru a kybernetické bezpečnosti, dále také poskytuje pokyny a vysvětlení, jak mohou společnosti splnit nezbytná kritéria k zajištění bezpečnějšího zpracování dat. Existují bezpečnostní hrozby, které nejsou plně pokryty současnou informační bezpečností a zabezpečením sítí, protože mezi těmito doménami jsou mezery v důsledku nedostatku komunikace mezi organizacemi. Z hlediska kybernetické bezpečnosti se jedná zejména o:

- Informační bezpečnost.
- Zabezpečení sítě.
- Zabezpečení internetu.
- Ochranu kritické informační infrastruktury.

Z hlediska základních bezpečnostních postupů pro zúčastněné strany v kyberprostoru poskytuje:

- Přehled kybernetické bezpečnosti.
- Vysvětlení vztahu mezi kybernetickou bezpečností a jinými typy zabezpečení.
- Definici zúčastněných stran a popis jejich rolí v kybernetické bezpečnosti.
- Pokyny pro řešení běžných problémů kybernetické bezpečnosti.
- Rámec, který umožní zúčastněným stranám spolupracovat na řešení problémů kybernetické bezpečnosti. (Zeneli, 2016)

Další publikované normy:

- ISO/IEC 27003 – návod k implementaci.
- ISO/IEC 27004 – monitorování, měření, analýza a vyhodnocování.
- ISO/IEC 27005 – řízení rizik.
- ISO/IEC 27007 – návod k provádění auditů.
- ISO/IEC 27008 – pokyny pro auditory.
- ISO/IEC 27010 – mezisektorová a meziorganizační komunikace.
- ISO/IEC 27011 – řízení informační bezpečnosti v telekomunikačních organizacích.
- ISO/IEC 27013 – implementace ISO/IEC 27001 a ISO/IEC 20000-1.
- ISO/IEC 27014 – řízení informační bezpečnosti.
- ISO/IEC 27799 – řízení informační bezpečnosti ve zdravotnictví.
- A jiné. (Smejkal, Sokol a Kodl, 2015)

1.1.3 Systém řízení bezpečnosti informací

Systém řízení bezpečnosti informací je založen na modelu PDCA. Tento model zavádí kontinuální systém řízení bezpečnosti informací v organizaci, což znamená, že zavedení systému nebude jen jednorázovou aktivitou.

Plánuj (ustavení ISMS) – stanovení cílů, procesů a postupů tak, aby vedly k výsledkům v souladu s politikou a cíli organizace.

Dělej (zavádění a provozování ISMS) – zavedení opatření, procesů a postupů.

Kontroluj (monitorování a přezkoumání ISMS) – vyhodnocení změn, které byly zavedeny v předchozím kroku. Pokud změny nejsou vyhodnoceny kladně, je potřeba vymyslet jiná opatření.

Jednej (udržování a zlepšování ISMS) – přijetí opatření k nápravě a preventivních opatření do praxe. Přezkoumání systému řízení ze strany vedení organizace tak, aby bylo dosaženo kontinuálního zlepšování ISMS. (Hrůza, 2012; ISO/IEC 27000, 2018)

1.1.4 Cybersecurity Framework

Směrnice 2016/11481 o bezpečnosti sítí a informačních systémů (směrnice NIS) je první právní předpis přijatý na úrovni EU pro ochranu sítí a informačních systémů v celé Unii.

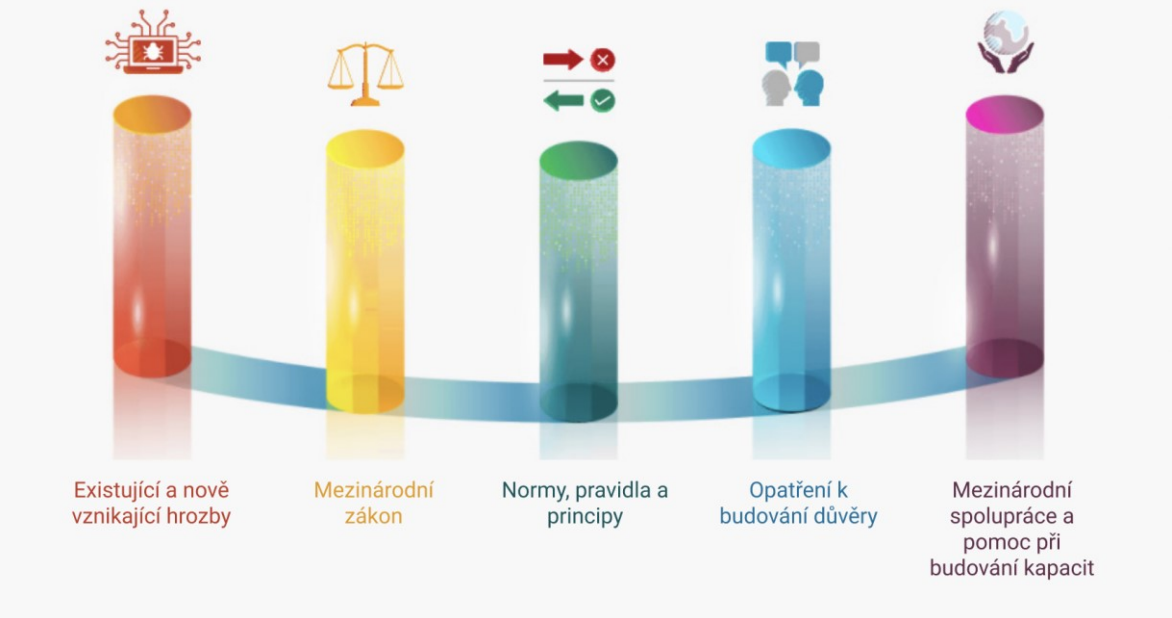
V současné době je všeobecně známo, že úmyslné incidenty způsobující narušení IT služeb a kritických infrastruktur představují vážnou hrozbu pro jejich provoz a následně pro fungování vnitřního trhu a Unie. Stávající protiopatření, pokud jde o bezpečnostní nástroje a postupy, nejsou v EU dostatečně rozvinutá a nejsou společná ve všech členských státech.

Směrnice NIS se snaží tuto potřebu řešit pomocí „opatření s cílem dosáhnout vysoké společné úrovně bezpečnosti sítí a informačních systémů v rámci Unie a rovněž zlepšit fungování vnitřního trhu“. (ScienceDirect, 2019)

Směrnice NIS se skládá z 27 článků. Články 1–6 uvádí její rozsah a hlavní definice, včetně identifikace provozovatelů základních služeb. Články 7–10 popisují vnitrostátní rámce, které musí přijmout každý členský stát pro bezpečnost sítí a informačních systémů. Tyto rámce zahrnují mimo jiné povinnost členských států zavést vnitrostátní strategii a jmenovat příslušné vnitrostátní orgány (tým pro reakci na bezpečnostní incidenty počítačů CSIRT), jakož i vytvoření skupiny pro spolupráci. Mechanismus spolupráce je uveden v článcích 11–13. Následující články 14–18 definují bezpečnostní požadavky a oznamování incidentů pro operátory základních služeb a poskytovatele digitálních služeb. Procesem dobrovolného oznamování se zabývají články 19 a 20. Konečně články 21–27 obsahují závěrečná ustanovení směrnice. (ScienceDirect, 2019)

1.1.5 Kybernetická diplomacie

Samotná definice kybernetické diplomacie je velmi složitá, jelikož se stále jedná o neprobádanou oblast. Obvykle je definována jako využití diplomatických schopností v kybernetickém prostoru. Cílem je dosáhnout zájmů jednotlivých států stejně jako u běžné diplomacie. Kybernetickou diplomacii lze vnímat ve dvou úrovních, a to na bilaterální a multilaterální. Na obrázku č. 1 lze vidět, na jakých pilířích stojí kybernetická diplomacie. (Šmejkalová, 2020)



Obrázek 1 – Pět pilířů kybernetické diplomacie (Šmejkalová, 2020)

1.2 Kybernetická bezpečnost

Kybernetickou bezpečnost lze popsat jako celkovou ochranu sítí před kybernetickými útoky a hrozbami, aby byla zachována bezpečnost informací. Pojem kybernetická bezpečnost se často zaměňuje s pojmem informační bezpečnost. Ačkoliv se kybernetická bezpečnost a informační bezpečnost značně překrývají, tyto dva koncepty nejsou zcela analogické. Kybernetická bezpečnost překračuje hranice tradiční informační bezpečnosti a zahrnuje nejen ochranu informačních zdrojů, ale i dalších aktiv včetně samotných osob. V informační bezpečnosti se odkaz na lidský faktor obvykle vztahuje k roli lidí v bezpečnostním procesu. V kybernetické bezpečnosti má tento faktor další rozměr, a to člověka jako potenciální cíl kybernetických útoků nebo jako účastníka, který se nevědomě účastní kybernetického útoku.

Na obrázku č. 2 je vyobrazen životní cyklus kybernetické bezpečnosti, kde první trojice slouží k prevenci a předcházení kybernetických hrozeb, které by mohly narušit funkčnost systému. Důležitější, než prevence je pak detekce a reakce. (Solms a Niekerk, 2013)

Obrázek 2 – Životní cyklus kybernetické bezpečnosti (KYBEZ, ©2021)

Je rozdělována na:

- Zabezpečení kritické infrastruktury – postupy pro ochranu počítačových systémů, sítí a dalších aktiv pro zachování národní bezpečnosti, ekonomického zdraví a veřejné bezpečnosti.
- Zabezpečení sítě – bezpečnostní opatření pro ochranu počítačové sítě před narušiteli, včetně kabelového i bezdrátového (Wi-Fi) připojení.
- Zabezpečení aplikací – procesy, které pomáhají chránit aplikace provozované lokálně na zařízeních a v cloudu. Cloud označuje servery, ke kterým se přistupuje přes internet, a také software a databáze, které na těchto serverech fungují. Díky cloudu nemusí uživatelé a společnosti sami spravovat fyzické servery.
- Cloudové zabezpečení – šifrování cloudových dat v klidném stavu (v úložišti), v pohybu (při cestování dat z cloudu a v rámci cloudu) a při používání (během zpracování).

- Informační bezpečnost – opatření na ochranu údajů, jako je obecné nařízení o ochraně osobních údajů nebo GDPR, které chrání nejcitlivější osobní údaje před neoprávněným přístupem, vystavením nebo krádeží.
- Vzdělávání koncových uživatelů – budování povědomí o bezpečnosti v celé organizaci za účelem posílení zabezpečení koncových bodů. Uživatelé mohou být například vyškoleni, aby odstraňovali podezřelé přílohy e-mailů, vyhýbali se používání neznámých zařízení USB atd. (Kaspersky, 2020)

1.2.1 Kyberprostor

Je velice náročné jednoznačně definovat kybernetický prostor. V minulosti bylo na tento pojem nahlíženo z mnoha rovin. Poprvé tento pojem použil a vymyslel v roce 1982 spisovatel William Gibson ve své povídce „Burning Chrome“. Od této doby tento pojem začalo využívat čím dál více autorů pro interpretaci svých myšlenek. John Perry Barlow poprvé použil tento pojem pro existující počítačové sítě, který definoval jako symbolický prostor komunikace, kde komplexnost tohoto prostoru závisí na vyspělosti technologie. V návaznosti na Johna Perryho Barlowa antropolog David Hakken charakterizoval kybernetický prostor jako sociální arénu, do které vstupují sociální aktéři, kteří používají k vzájemné interakci pokročilé technologie. Definuje jej jako distinktivní typ kultury.

V roce 2001 Computer Science and Communications Dictionary definovalo kyberprostor jako nehmotný svět informací, který vzniká na základě propojení informačních a komunikačních systémů. Mezi komunikační systémy byl zařazen internet. V roce 2003 Leo Troy připsal kyberprostoru nové možnosti komunikace jako např. emaily, webové stránky, počítačové sítě apod. Sofia Tzimopoulou v roce 2006 popsala kyberprostor jako imaginární místo, na které neplatí zákonitosti ze světa fyzického. Uživatel v tomto prostředí podle ní opouští své fyzické tělo a pobývá zde bez něj.

Kyberprostor lze chápat jako metaforu virtuálního světa vytvořeného propojením počítačových systémů v síti. Dochází zde mezi uživateli k interakcím, stejně jako v reálném (fyzickém) světě, akorát bez nutnosti fyzické aktivity. (Hrůza, 2012)

1.2.2 Základní terminologie kybernetické bezpečnosti

Oblast kybernetické bezpečnosti obsahuje nepřeberné množství pojmosloví, která se k tomuto tématu vážou. Všechny tyto pojmy lze nalézt ve Výkladovém slovníku

kybernetické bezpečnosti, který obsahuje i pojmy z oblasti obecné bezpečnosti, informatiky, managementu apod.

Kybernetický terorismus – *"Nezákonný útok proti počítačům, počítačovým sítím a v nich uloženým informacím, při kterém je záměrem útočníka získat informace, negativně je ovlivnit nebo převzít kontrolu nad prvky infrastruktury systému."*

Kritická informační infrastruktura státu – *"Komplex informačních a komunikačních systémů a jejich služeb, sloužící k informačnímu zajištění řádné funkčnosti kritické infrastruktury. Sestává z částí, jakými jsou telekomunikace, počítačové systémy a jejich programové vybavení, internet, přenosové sítě, poskytované služby atd."*

Aktivní hrozba – *"Jakákoliv událost, která může mít za následek narušení důvěrnosti, integrity a dostupnosti dat."*

Antivirový program – *"Program pro vyhledávání počítačových virů, léčení napadených souborů, zálohování a obnovu systémových oblastí na disku, ukládání kontrolních informací o souborech na disku."*

Kybernetický bezpečnostní incident – "*Kybernetická bezpečnostní událost, která představuje narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb a sítí elektronických komunikací.*"

Stav kybernetického nebezpečí – "*Stav, ve kterém je ve velkém rozsahu ohrožena bezpečnost informací v informačních systémech nebo bezpečnost služeb nebo sítí elektronických komunikací, a tím dojde nebo by mohlo dojít k porušení nebo ohrožení zájmu České republiky.*" (Hrůza, 2012; Jirásek et al., 2012)

1.2.3 Kybernetické útoky v současné době

Kybernetické útoky se odlišují podle různých kritérií, jako je např. motivace útočníka. Do této kategorie spadá:

- Kyberkriminalita – útočníci páchají trestnou činnost k vlastnímu obohacení.
- Hacktivismus – útočníci upozorňují na určitý problém formou apelu.
- Kybernetická válka – útoky směřující k poškození infrastruktury jiným státem či nestátním aktérem.

- Kybernetická špionáž – slouží k získávání informací v obchodním či mezinárodním styku. (Hromada et al., 2015)

Kybernetická kriminalita začala být postihována v ČR od roku 2002 podle zákona č. 140/1961 Sb., trestního zákona, ve znění pozdějších předpisů. Postihování kybernetické kriminality bylo značně rozšířeno oproti původní právní úpravě, čímž byl splněn závazek České republiky vyplývající z Úmluvy Rady Evropy o počítačové kriminalitě ze dne 23. listopadu 2001. (Hromada et al., 2015)

Kyberšikana

Lze hovořit o šikaně, která probíhá v kyberprostoru bez fyzické přítomnosti útočníka a oběti. Tento termín se začal objevovat s rozmachem v oblasti elektronických zařízení. Může se jednat o bezhlasé telefonáty či opakované zasílání krátkých SMS zpráv. V současné době se jedná spíše o šikanující e-mailové zprávy nebo o zprávy zasílané na sociálních sítích. Samotná kyberšikana není trestný čin, musí dojít k naplnění skutkové podstaty trestného činu § 175 Vydírání, § 191 Šíření pornografie, § 191 Účast na sebevraždě apod. (Šmahaj, 2014)

Kyberstalking

Je velmi úzce spojen s termínem kyberšikana. Jedná se o dlouhodobé a obvykle i stupňující vyhledávání oběti ze strany pachatele. Kyberstalking je jednou z forem stalkingu, kde pachatel využívá ke svému pronásledování informační a komunikační technologie. Kyberstalking je v trestním zákoníku přiřazován k § 175 Nebezpečnému pronásledování a k § 353 Nebezpečnému vyhrožování. Ke kyberstalkingu se váže i termín stalkerware. (Kolouch a Volevecký, 2013)

Sexting

Tato problematika je založená na elektronickém rozesílání fotografií nebo videonahrávek se sexuálním obsahem. Jedná se o aktivitu, která vzniká již na straně budoucí oběti, která si to zpočátku neuvědomuje. Obvykle ze zamilovanosti zašle intimní fotografie či videonahrávky, jelikož je o to partnerem či kamarádem požádána. Zpočátku se nemusí nic dít, problém nastává až po rozchodu, nebo po ukončení kamarádství, kdy druhá strana může tento materiál zneužít. Podle trestního zákoníku je sexting spojován se zločinem § 175 Vydírání a s § 191 Šíření pornografie. (Šulc, 2018)

Kybergrooming

Tento kybernetický útok probíhá obvykle přes internetové komunikační prostředky (seznamky, sociální sítě apod.). Obětmi v této problematice jsou nejčastěji děti (častěji slečny, než chlapci), kdy útočník si získá jejich důvěru a chce si s nimi dohodnout osobní setkání. Útočníci mohou být různého sociálního postavení a různého stupně intelektu. Kybergrooming může vyeskalovat až do sexuálního zneužití dítěte, zneužití pro výrobu dětské pornografie apod. V trestním zákoníku lze kybergrooming přiřazovat např. ke zločinu § 191 Výroba a jiné nakládání s dětskou pornografií, § 187 Pohlavní zneužívání, § 168 Obchodování s lidmi, § 201 Ohrožování výchovy dítěte atd. (Kopecký, 2010)

1.2.4 Organizace zabývající se kybernetickou bezpečností v ČR

NÚKIB je ústředním správním orgánem pro kybernetickou bezpečnost. Současně je ústředním správním orgánem v oblasti ochrany utajovaných informací v mezích informačních a komunikačních systémů a kryptografické ochrany.

Dále spravuje veřejně regulované služby, co se týče družicového systému Galileo. Vznikl 1. srpna 2017 na základě zákona č. 205/2017 Sb., kterým se změnil zákon č. 181/2014 Sb., o kybernetické bezpečnosti.

Ředitel NÚKIB se rovněž pravidelně účastní jednání Bezpečnostní rady státu a je členem Výboru pro kybernetickou bezpečnost. Tento výbor je stálým pracovním orgánem Bezpečnostní rady státu pro koordinaci plánování opatření k zajišťování kybernetické bezpečnosti ČR. (NÚKIB, ©2022)

Dohled nad dodržováním povinností plynoucích ze zákona o kybernetické bezpečnosti zajišťují:

- Pracoviště vládního CERTu (Computer Emergency Response Team) – provozovaný jako součást Národního centra kybernetické bezpečnosti. Dle zákona disponuje nařizovacími a sankčními pravomocemi. Hlavním cílem vládního CERTu je uplatňování státní moci v oblasti kybernetické bezpečnosti.
- Pracoviště národního CERTu – provozováno právnickými osobami podle soukromého práva a ke své činnosti jsou oprávněni na základě výběrového řízení a veřejnoprávní smlouvy uzavřené s NÚKIB. Dle zákona nedisponuje nařizovacími a sankčními pravomocemi. Funguje jako metodická podpora subjektů, které projeví zájem o kolektivní ochranu před kybernetickými bezpečnostními incidenty. Díky

> tomu, že se jedná o soukromý subjekt, může Národní CERT v nepředvídatelných situacích reagovat operativně, tzn., že je způsobilý konat vše, co mu není zákonem zakázáno, a vytvořit nová řešení či technické postupy. (Hrůza, 2012)

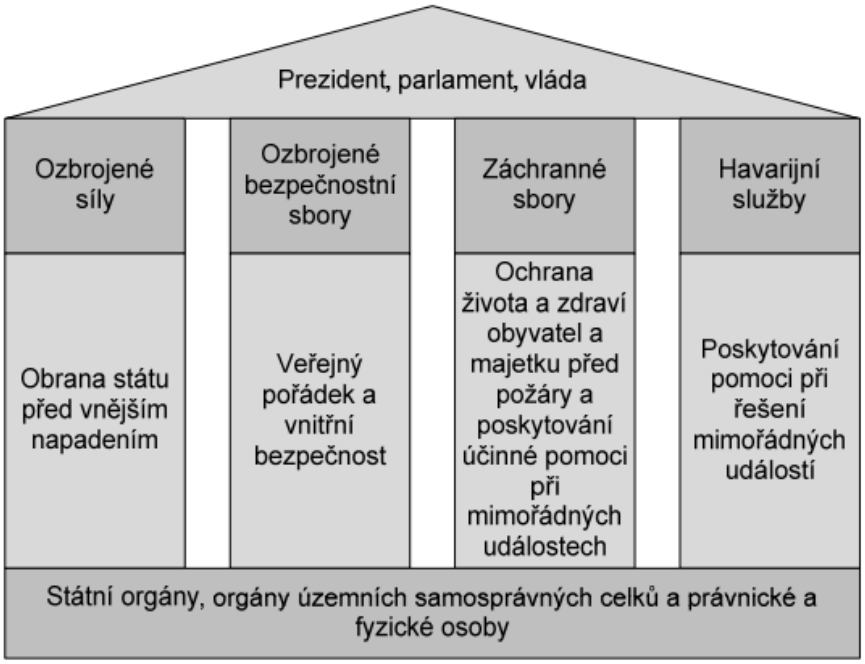
Na úrovni jednotlivých organizací vznikají CSIRT týmy. Do těchto typů organizací spadají organizace, které zprostředkovávají chod internetu, i organizace, které samotný internet využívají ke své pracovní činnosti. Hlavní činností CSIRT týmů je řešení problémů v rámci jejich působnosti např. ve vlastní síťové infrastruktuře. Rozdíl oproti normálním bezpečnostním týmům tkví v tom, že týmy CSIRT jsou zapojeny do světové bezpečnostní infrastruktury. Musí veřejně deklarovat své kontaktní informace a pravidla činnosti (členové týmu, jakým způsobem tým zastihnout, pravomoci a odpovědnost za služby atd.)

CSIRT týmy se dělí na:

- Národní CSIRT – věnuje se vzdělávání a spolupráci. Jeho postavení je bráno jako "*last resort*" – tedy poslední instance, u které lze zažádat o pomoc. Národní CSIRT nevládne nad fyzickou infrastrukturou, tudíž oproti interním týmům nejsou způsobilí k přímému zásahu. Slouží spíše jako zprostředkující a koordinační složka.
- Vládní CSIRT – zaměřuje se na oblast státní správy a samosprávy. Rovněž se zabývá řešením bezpečnostních incidentů, které mohou ohrozit bezpečnost státu a služeb. Oproti Národnímu CSIRT může mít podobu interního týmu způsobilého k přímému zásahu. (Kolouch et al., 2019)

2 SUBJEKTY OCHRANY OBYVATELSTVA

Problematika ochrany obyvatelstva v České republice je obsažena jak v rámci právních předpisů (zákony, vyhlášky apod.), tak i v koncepcích, což jsou dokumenty nelegislativního charakteru. Právní předpisy striktně stanovují obecný a závazný právní rámec výkonu ochrany obyvatelstva, vykonávaný jednotlivými orgány veřejné správy, právnickými a fyzickými osobami. Koncepce zastává pozici podrobného popisu a vyobrazení struktury systému ochrany obyvatelstva společně s podrobným popisem úkolů a termínů pro jejich splnění. Na obrázku č. 3 lze vidět celá struktura bezpečnostního systému ČR. (GŘ HZS ČR, 2015)



Obrázek 3 – Bezpečnostní systém České republiky (GŘ HZS ČR, 2015)

2.1 Koncepce ochrany obyvatelstva

Koncepce ochrany obyvatelstva představuje základní strategický plánovací dokument. Existuje více výchozích podkladů k jejímu zpracování, např. Bezpečnostní strategie ČR. Koncepce slouží k rozpracování a uchopení vizí, které jsou nastavené ve strategických dokumentech, a k jejich implementaci do praxe. Zpracování koncepce upravuje zákon č. 239/2000 Sb., o integrovaném záchranném systému (IZS) a je v gesci ministerstva vnitra – generálního ředitelství hasičského záchranného sboru ČR (MV-GŘ HZS ČR). Problematikou se kromě MV mimo jiné zabývají i další orgány veřejné správy. Výstupem

je poté dokument, který řeší problematiku ochrany obyvatelstva v celé její šíři. (GŘ HZS ČR, 2015)

Koncepce je projednávána a schválena vládou ČR (cestou Výboru pro civilní nouzové plánování a Bezpečnostní rady státu). Významné oblasti ochrany obyvatelstva: výchova a vzdělávání, síly, věcné zdroje, úkoly ochrany obyvatelstva krizového řízení, věda a výzkum. Jsou v ní obsaženy i základní úkoly pro realizaci stanovených priorit ochrany obyvatelstva na celé období její platnosti, včetně jejího výhledu. Součástí je i hodnocení dosavadního stavu plnění úkolů. Pro úspěšné splnění vrcholových strategických cílů a vizí v oblasti ochrany obyvatelstva je nutné se zaměřit na:

- Širší zapojení občanů (fyzických osob) do systému ochrany obyvatelstva cestou zvýšení jejich schopnosti sebeochrany za využití informací a znalostí získaných v rámci plošného a cíleného systému výchovy a přípravy.
- Širší zapojení právnických a podnikajících fyzických osob do přípravy na mimořádné události (MU) a krizové stavy (KS) a jejich řešení cestou užší spolupráce s odpovědnými orgány veřejné správy a zvýšeným podílem na realizaci konkrétních úkolů u subjektů představujících zvýšené riziko pro své okolí.
- Zvýšení odolnosti a ochrany prvků kritické infrastruktury proti možným rizikům a zajištění širšího zapojení subjektů kritické infrastruktury do procesu přípravy na MU a KS a jejich řešení.
- Cílená podpora vědy a výzkumu, vývoje, inovací s důrazem na využívání dosažených výsledků v aplikační sféře v rámci systému vzdělávání a přípravy odborníků.
- Vyvážené a komplexně využitelné úkoly a nástroje ochrany obyvatelstva umožňující efektivní prevenci a přípravu na MU a KS a jejich řešení založené na přesně definovaném a zakotveném systému ochrany obyvatelstva. (GŘ HZS ČR, 2015)

Kontrole plnění jednotlivých priorit a informování vlády ČR o stavu ochrany obyvatelstva se věnuje Zpráva o stavu ochrany obyvatelstva v ČR, která se zpracovává v tříletých cyklech a je v gesci MV-GŘ HZS ČR. Hodnocení se týká oblastí: školství, zdravotnictví, místního rozvoje, dopravy, obrany, vnitra, zahraničních věcí, zemědělství, životního prostředí,

státních hmotných rezerv a jaderné bezpečnosti. Výsledný dokument je výsledkem práce odborníků ze všech dotčených resortů. (GŘ HZS ČR, 2015)

2.2 Prvky určené k ochraně obyvatelstva

Ministerstva a ústřední správní úřady při přípravě na mimořádné události, při provádění záchranných a likvidačních prací a při ochraně obyvatelstva ve své působnosti vykonávají tyto činnosti:

- Vedou celkový přehled možných zdrojů rizik, provádějí analýzy ohrožení a v rámci preventivních opatření, podle právních předpisů, také sjednávají nápravu skutečností a stavů, které by mohly vyústit až do vzniku mimořádné události.
- Mají rozhodovací roli v oblasti provádění záchranných a likvidačních opatření a zmírnění jejich následků.
- Organizují okamžité opravy veřejných zařízení, která slouží pro ochranu obyvatelstva. (Lukáš, 2015)

2.2.1 Ministerstvo vnitra

Tento orgán je v gesci generálního ředitelství Hasičského záchranného sboru ČR. V oblasti přípravy na mimořádné události, IZS a ochrany obyvatelstva plní následující úkoly:

- Sjednocuje postupy ostatních ministerstev, krajských a obecních úřadů, právnických a fyzických osob.
- Má kontrolu nad IZS.
- Zpracovává ústřední poplachový plán IZS a provádí kontrolu nad poplachovými plány IZS krajů.
- Vede výstavbu komunikačních sítí, které slouží pro komunikaci služeb IZS a zajišťuje jejich provoz.
- Zpracovává koncepci ochrany obyvatelstva.
- Zajišťuje provoz jednotného systému varování a vyrozumění (JSVV).
- Zajišťuje pravidelné školení v oblasti ochrany obyvatelstva.
- Stanovuje technické požadavky na stavby, které jsou určené k ochraně obyvatelstva.

- Rozhoduje o zapojování ČR do mezinárodních záchranných a humanitárních operací.
- Stanovuje postupy při zařizování civilní ochrany. (Lukáš, 2015)

2.2.2 Krajský úřad

Má na starosti organizování a sjednocování postupů při součinnosti mezi jednotlivými obecními úřady obcí s rozšířenou působností a dalšími správními úřady a obcemi v kraji v oblasti ochrany obyvatelstva. Zpracovává poplachový plán IZS, usměrňuje jednotlivé složky IZS na úrovni kraje a zajišťuje havarijní připravenost, která je ověřována cvičením. Úkoly orgánů kraje plní HZS daného kraje a v oblasti ochrany obyvatelstva plní následující úkoly:

- Varování a vyrozumění.
- Zajišťuje a označuje nebezpečné oblasti, provádí dekontaminaci a další ochranná opatření.
- Plní úkoly ochrany obyvatelstva: evakuace, nouzové ubytování, nouzové zásobování pitnou vodou, potravinami a dalšími nezbytnými prostředky k zajištění přežití obyvatelstva.
- Organizuje humanitární pomoc a hospodaření s materiálem civilní ochrany.
- Usměrňuje postupy při zřizování zařízení civilní ochrany a následně provádí kontrolu staveb civilní ochrany a dohlíží na odbornou připravenost personálu v kraji.
- Zabezpečuje preventivně výchovnou, propagační a ediční činnost. (Lukáš, 2015)

2.2.3 Obecní úřad obce s rozšířenou působností

Kromě obecných úkolů při výkonu státní správy, které jsou spojené s činnostmi obecních úřadů, zajišťuje připravenost svého správního obvodu na mimořádné události, provádění záchranných a likvidačních prací a ochranu obyvatelstva. Úkoly obecního úřadu obce s rozšířenou působností plní HZS kraje a jsou prakticky totožné s úkoly, které plní krajský úřad. O výjimku se jedná v případě:

- Organizování součinnosti s ostatními obcemi.

- Seznamování ostatních obcí, právnických a fyzických osob ve svém správním obvodu s charakterem možného ohrožení obyvatel, s připravenými záchrannými a likvidačními pracemi a celkově s ochranou obyvatelstva. (Lukáš, 2015)

2.2.4 Obecní úřad

K plnění úkolů ochrany obyvatelstva je obec oprávněna zřizovat zařízení civilní ochrany. Organizuje celkovou přípravu obce na mimořádné události, společně s IZS se podílí na záchranných a likvidačních pracích a ochraně obyvatelstva. Obecní úřad dále připravuje a poskytuje podklady pro HZS kraje ke zpracování havarijních plánů, seznamuje právnické a fyzické osoby s možným ohrožením obyvatelstva a podílí se na zajištění nouzového přežití obce. (Lukáš, 2015)

Starosta obce má na starosti:

- Zajišťování varování osob, které se nacházejí na území obce, před hrozícím nebezpečím.
- Organizaci evakuace osob z ohroženého území ve spolupráci s velitelem zásahu nebo se starostou obce s rozšířenou působností.
- Organizaci činností obce v podmínkách nouzového přežití. (Lukáš, 2015)

2.2.5 Právnická osoba a podnikající osoba

Pokud je tato osoba zahrnuta do havarijního plánu kraje, nebo do vnějšího havarijního plánu, je nucena bezplatně poskytnout a aktualizovat požadované podklady a zajistit svým zaměstnancům:

- Informování ohledně hrozících mimořádných událostí a plánovaných opatřeních.
- Varování, evakuaci, a pokud je to nutné, tak i ukrytí.
- Organizování záchranných prací a přípravy k sebeochraně a vzájemné pomoci.
- K plnění úkolů ochrany obyvatelstva má oprávnění zřizovat zařízení civilní ochrany. (Lukáš, 2015)

Právnické a podnikající osoby jsou povinny strpět na svých nemovitostech zařízení systému varování a vyrozumění a umožnit oprávněným osobám přístup k těmto zařízením za účelem používání, kontroly, údržby apod. Pokud osoba vlastní stavby civilní ochrany, musí dbát na to, aby nedošlo ke změně charakteru stavby a musí opět kdykoliv zajistit přístup oprávněným

osobám. Při provozování školských, zdravotnických a obdobných zařízení musí vytvořit takové podmínky, aby v nich mohlo docházet k výdeji prostředků individuální ochrany. (Lukáš, 2015)

2.2.6 Fyzická osoba

Každá osoba, která pobývá na území ČR, tak má právo na veškeré informace, které se týkají opatření k zabezpečení ochrany obyvatelstva a na poskytnutí instruktáží a školení ke své činnosti při vzniku mimořádné události. Obdobně jako u právnické a podnikající fyzické osoby, mají fyzické osoby povinnost strpět stejné okolnosti, které byly u těchto osob uvedeny. (Lukáš, 2015)

2.2.7 Integrovaný záchranný systém

„*Představuje koordinovaný postup jeho složek při přípravě na MU a při provádění záchranných a likvidačních prací. Potřeba vzniku IZS vyplynula z každodenní činnosti záchranářů při odstraňování následků MU nebo KS a zejména z nutnosti organizování společné činnosti všech subjektů, které disponují potřebnými silami a prostředky a jsou vybaveny nezbytnými kompetencemi*“. (GŘ HZS ČR, 2015)

IZS se používá v případě potřeby provádění záchranných a likvidačních prací dvěma nebo více složkami IZS a při přípravě na vznik mimořádné události. Při zásahu jsou složky IZS povinny se řídit příkazy velitele zásahu, popřípadě pokyny starosty obce s rozšířenou působností, hejtmana kraje nebo ministerstva vnitra. Při vyhlášení jednoho z krizových stavů (nouzový stav, stav ohrožení státu, válečný stav) se složky IZS řídí pokyny ministerstva vnitra. (GŘ HZS ČR, 2015)

V zákoně č. 239/2000 Sb., o integrovaném záchranném systému jsou popsány jeho základní a ostatní složky. Mezi základní složky IZS jsou zařazeny:

- HZS ČR a jednotky požární ochrany zařazené do plošného pokrytí kraje jednotkami požární ochrany.
- Poskytovatelé zdravotnické záchranné služby.
- Policie ČR.

Ostatní složky IZS jsou:

- Vyčleněné síly a prostředky ozbrojených sil.

- Ostatní ozbrojené bezpečnostní sbory (např. Vězeňská služba ČR, obecní policie).
- Ostatní záchranné sbory (např. Báňská záchranná služba).
- Orgány ochrany veřejného zdraví (hygienická služba).
- Havarijní, pohotovostní, odborné a jiné služby (energetika, komunikační a informační systémy apod.).
- Zařízení civilní ochrany.
- Neziskové organizace a sdružení občanů, která lze využít k záchranným a likvidačním pracím (horská služba, vodní záchranná služba, kynologové, Český červený kříž, ADRA, Hand for Help apod.). (GŘ HZS ČR, 2015)

Způsob řízení IZS se rozděluje do třech úrovní:

- Taktická – koordinace je prováděna velitelem zásahu v místě nasazení složek IZS a odpovídá za záchranné a likvidační práce. Velitelem zásahu je většinou velitel jednotky požární ochrany, pokud právní předpisy nestanovují jinak. Při větších mimořádných událostech se může zřídit štáb velitele zásahu. (Vilášek, Fiala a Vondrášek, 2014)
- Operační – řízení je prováděno v operačních a informačních střediscích (OPIS) HZS. Pokud si lidé volají pomoc pomocí tísňového volání, dovolají se právě do OPISu. Na krajské úrovni jsou zřízena krajská operační a informační střediska (KOPIS). Plní koordinační roli (na žádost mohou povolávat ostatní složky IZS), ovládá systémy varování a vyrozumění a funguje jako spojka mezi místem zásahu a nadřazenou úrovní řízení. (Vilášek, Fiala a Vondrášek, 2014)
- Strategická – řízení prováděno starostou obce s rozšířenou působností, hejtmanem kraje, nebo MV a ostatními správními úřady v případech stanovených zákonem o IZS. K činnosti je využíván krizový štáb a vychází se ze zpracovaných krizových plánů. Pokud se jedná o mimořádnou událost, u které se vyhlašuje nejvyšší stupeň poplachu, zapojuje se hejtman a MV. (Vilášek, Fiala a Vondrášek, 2014)

2.3 Typy informací v subjektech ochrany obyvatelstva

Utajované informace se rozdělují podle stupňů utajení na přísně tajné, tajné, důvěrné a vyhrazené. Tuto problematiku upravuje zákon č. 412/2005 Sb., o ochraně utajovaných

informací a o bezpečnostní způsobilosti. Dále se k tomu vztahuje řada prováděcích předpisů, konkrétně: nařízení vlády č. 522/2005 Sb., vyhláška č. 523/2005 Sb., vyhláška č. 524/2005 Sb., apod. Ochrana utajovaných informací je zajišťována následovně:

- Personální bezpečnost – jedná se o výběr kompetentních osob, které mají přístup k utajovaným informacím, jejich ochrana a výchova. Důležité je také pravidelné ověřování podmínek pro jejich přístup k utajovaným informacím.
- Průmyslová bezpečnost – systém zajištění a kontroly podmínek k udělení přístupů podnikateli k utajovaným informacím.
- Administrativní bezpečnost – systém opatření, jakým způsobem musí pracovníci nakládat s utajovanými informacemi při jejich příjmu, tvorbě, evidenci, zpracování, odesílání, přepravě, přenášení, ukládání, skartačním řízení, archivaci apod.
- Fyzická bezpečnost – opatření, která mají za cíl znesnadnit či zabránit přístupu nepovolené osobě k utajovaným informacím.
- Bezpečností informační či komunikační systémy – cílem je dosažení důvěrnosti, integrity a dostupnosti utajovaných informací, se kterými tyto informační systémy (IS) pracují. Patří sem i odpovědnost za správu těchto systémů a odpovědnost uživatele pracovat s těmito systémy takovým způsobem, jak je nařízeno.
- Kryptografická ochrana – využití kryptografických metod na ochranu utajovaných informací při jejich zpracování, přenosu nebo ukládání. (HZS ČR, 2014; Česko, 2005)

Informace ve všech svých podobách patří k velmi cennému aktivu a musí k nim být přistupováno s prioritou a patřičně je chránit. Příkladem informačního aktiva může být např. databáze, datové soubory apod. a s tím i spojená aktiva programová (software, operační systém) a fyzická (počítačové zařízení, servery). Informace nabývají mnoha podob, mohou být v elektronické podobě, v tištěné, písemné, nahrané nebo vyřčené. Při budování efektivní informační kultury je nutné brát ohled na zásadu použití informací pouze tam, kde jsou potřeba.

Přístup k chráněným informacím můžou mít pouze ty osoby, které tuto konkrétní informaci potřebují znát a budou s ní nakládat ve prospěch a zájmu daného subjektu. Za chráněné informace můžeme označit informace v jakékoliv formě a na jakémkoliv nosiči.

Za ochranu informací nelze brát pouze ochranu informačních systémů, ale musí se brát zřetel na ochranu všech informací na všech druzích nosičů. (Požár, 2005; Smejkal a Rais, 2013)

Nejčastěji se jedná o informace z oblasti:

- Finančního řízení – výkazy, účetní doklady.
- Informačních a komunikačních technologií – databáze, aplikace, systémy, zdrojové kódy, síťová infrastruktura.
- Managementu – taktické plány, strategické plány, projektová dokumentace, pracovní postupy, operativní plány, směrnice a standardy, bezpečnostní politika.
- Marketingu – informace o dodavatelích a klientech, analýzy, průzkum trhu, informace o produktech a službách, připravované marketingové kampaně, detaily o stávajících, proběhlých a budoucích obchodech.
- Zařízení – umístění čidel, kamer, spínačů, ostraha a její úkoly, plány budov.
- Řízení lidských zdrojů – pracovní pozice, jejich obsazenost a popis, osobní údaje zaměstnanců (kontaktní informace, osobní číslo, výsledky hodnocení, pracovní zařazení, výše mzdy), motivační systém (zaměstnanecké výhody, bonusy, systém hodnocení). (Singer a Freidman, 2013)

V rámci krizového řízení se využívá k ochraně informací zejména povinnost zachovat mlčenlivost, dále administrativně-technická opatření, režim utajení a zvláštních skutečností. Do režimu zvláštních skutečností spadá administrativní bezpečnost, personální bezpečnost, fyzická bezpečnost a bezpečnost informačních a komunikačních systémů. Pokud se jedná o zvláštní skutečnost, tak se dokumenty, média, krizové plány, důležité listiny apod. označují slovy zvláštní skutečnost či zkratkou ZS. Zvláštní skutečnosti se evidují v samostatném jednacím protokolu a je pro ně vyhrazené zvláštní místo pro jejich uložení, které je odděleno od ostatních dokumentů. Pracoviště, kde se tento druh dokumentů ukládá, má pouze jeden vstup, který je zajištěný proti volnému pohybu osob. Nejedná se tedy o žádnou kategorii ze stupňů utajení, které jsou uvedeny v zákonu č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. Aby pracovník měl přístup ke zvláštním skutečnostem, musí být zapsán v seznamu, který musí být předem schválen vedoucím zaměstnancem orgánu krizového řízení a tato osoba může rovněž daného pracovníka ze seznamu vyřadit. Pracovník, který se nachází na seznamu, musí opět zachovávat mlčenlivost a nesdělovat informace komukoliv, kdo nemá oprávnění. Zneužití těchto informací

neoprávněnou osobou může mít za následek znemožnění činnosti orgánu krizového řízení a ohrozit život a zdraví osob, majetku a životního prostředí. (Česko, 2000; Adamec, Řehák a Černá, 2012)

2.3.1 Příklady informačních systémů subjektů ochrany obyvatelstva

Příklady informačních systémů subjektů ochrany obyvatelstva:

- Informační systém veřejné správy (ISVS) - zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů, stanovuje práva a povinnosti, které souvisejí s vytvářením, užíváním, provozem a rozvojem informačních systémů veřejné správy. (Česko, 2000)
- Městské informační systémy (MIS) – tyto systémy slouží pro podporu administrativy v městských a obecních úřadech. Zabezpečuje centrální správu dat a umožňuje zálohovat data, která uživatelům umožňují rychlou a účinnou orientaci v evidovaných datech, provedení veškerých výpočetních operací a přípravu tiskových výstupů. (Profi Press, ©2022)
- Národní informační systém integrovaného záchranného systému (NIS IZS) – pro představu, s jakým množstvím informací pracují operátoři tísňové linky, lze vyjádřit v číslech:
    - Cca každých deset sekund odbaví operátor tísňové linky hovor, tzn. ročně je to přes tři miliony hovorů.
    - Jedna mimořádná událost obnáší zadání cca 450 datových vět do systému (informace sloužící ostatním složkám IZS, které vyjíždějí na pomoc). V prvé řadě se jedná o informace, které popisují vzniklou událost, tzn., jakým způsobem vznikla a kde, kolik osob je raněných apod. V případě doplňujících informací se jedná o detailní popis zasahujících vozidel a informace o jejich poloze. (HZS ČR, 2016)
- Informační systém JITKA – je součástí NIS IZS. Tento informační systém funguje odděleně od veřejné sítě internetu. Funguje jako podpora operačního řízení při vzniku mimořádné události, jejího oznámení, také při nasazování sil a prostředků a jejich kontrole. (Kodad, 2016)
- Geografické informační systémy (GIS) – jedná se o IS, který pracuje s prostorovými daty a propojuje databázové informace s grafickými. GIS není pouze

software, ale skládá se i z ostatních komponent, jako jsou data, hardware, personál a způsob použití. Nejčastěji využívaný software v oblasti GIS je:

- ArcGis – jedná se o GIS, který je určen pro práci s prostorovými daty. Mezi jeho funkce patří vytváření dat, jejich správa a analýza, hledání nových vztahů mezi nimi a jejich přehledná vizualizace. Výsledky lze sdílet nejen jako tradiční mapy, ale i jako interaktivní aplikace či přehledné reporty.
- GIS HZS ČR – webová verze GIS, která byla spuštěna generálním ředitelstvím HZS ČR v roce 2009. Tento IS slouží jako centralizovaná správa dat. Umožňuje sdílet data s dalšími složkami IZS, veřejné správy a státní samosprávy a vizualizovat dynamická data o mimořádných událostech apod.
- ArGis – IS plánování civilních zdrojů, který využívá správa státních hmotných rezerv. Je to hlavní nástroj informační podpory hospodářských opatření pro krizové stavy v oblasti zajišťování věcných zdrojů.
- QGIS – IS s otevřeným zdrojovým kódem, což znamená, že jej lze zdarma stáhnout a nainstalovat na počítačové zařízení. Existuje také mnoho zásuvných modulů, které rozšiřují funkčnost QGIS. (Aghajani, Farnia a Velayati, 2017; Zaoralová, 2015; SSHR ČR, ©2022; GISMentors, ©2022)

2.3.2 Narušení bezpečnosti informací kritické informační infrastruktury

Jedná se o typový plán, který se využívá v případě vzniku krizové situace způsobené narušením bezpečnosti informací kritické informační infrastruktury. V současné době je závislost společnosti na informačních a komunikačních systémech stále na vzestupu, tudíž možnosti výskytu krizové situace jsou reálné. Charakteristika krizové situace:

- Mezi prvky kritické infrastruktury, které se vážou k této krizové situaci, patří – oblast energetiky, veřejné správy, elektronických komunikací a finančního trhu a měny.
- Dopad na funkčnost subjektu kritické infrastruktury – dopad na jeho fungování a služby.
- Řeší ji převážně zasažený subjekt, NÚKIB a další instituce na centrální úrovni státu.

- Vyskytují se zde dva typy rizik:
    - Riziko neúmyslného selhání technologií či lidského faktoru – může vést k selhání služby poskytované informačními nebo komunikačními systémy.
    - Riziko úmyslného napadení informačních nebo komunikačních systémů – různé motivace a dopady. (Narušení bezpečnosti informací kritické informační infrastruktury, 2019)
- Způsoby řešení:
    - Následky ve fyzické rovině (zapojení složek IZS – dle zákona č. 240/2000 Sb., krizový zákon).
    - Následky v kyberneticko-bezpečnostní rovině (řešení incidentů dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti).
- Příčina vzniku:
    - Dle povahy narušení – neúmyslná (selhání technologií, selhání osob, živelní pohroma, blackout) a úmyslná (kybernetický útok).
    - Dle typu útoku – kinetický zásah, DoS/DDoS, škodlivý malware, sociální inženýrství, kombinace.
    - Dle motivace – hacktivismus, materiální obohacení, špionáž, terorismus apod. (Narušení bezpečnosti informací kritické informační infrastruktury, 2019)

3 MALWARE

Počet kybernetických útoků v dnešní době nepochybně roste, zaměřují se na vládu, armádu, veřejný a soukromý sektor. Jednotlivé kybernetické útoky cílí na jednotlivce, resp. organizace, se snahou získat cenné informace. Někdy jsou tyto útoky spojeny s kyberkriminalitou nebo státem podporovanými skupinami, ale mohou být také prováděny i zločineckými skupinami k dosažení svých cílů. Většina těchto kybernetických útoků využívá škodlivý software (také nazývaný malware) k infikování jejich cílů. Požadované znalosti, dovednosti a nástroje analyzovat škodlivý software jsou nezbytné pro detekci, vyšetřování a obranu proti útokům.

3.1 Popis malwaru a jeho typů

Malware je zkratka pro škodlivý software, který se používá k narušení počítačových operací, shromažďování citlivých informací, získávání přístupu k soukromým počítačovým systémům nebo k zobrazování nežádoucí reklamy. Může mít podobu spustitelného souboru, skriptu, kódu nebo jakéhokoliv jiného softwaru. Obvykle se dostane do vašeho systému bez vašeho souhlasu a může být stažen do systému prostřednictvím různých komunikačních kanálů, jako je např. e-mail, web nebo USB disky. (Monnappa K A, 2018)

Malware může způsobovat následující události:

- Narušení provozu počítače.
- Krádež citlivých informací, včetně osobních, obchodních a finančních údajů.
- Neoprávněný přístup do systému oběti.
- Špehování oběti.
- Odesílání spamových e-mailů.
- Zapojení do distribuovaných útoků typu denial-of-service (DDoS).
- Zamykání souborů v počítači a jejich držení za účelem výkupného. (Monnappa K A, 2018)

Nejznámější typy malwaru, viry, červi a trojské koně, jsou známé spíše způsobem, jakým se šíří než, že by se vyznačovaly nějakým konkrétním typem chování:

- Počítačový virus – tento termín popisuje program, který je vložen do jiného softwaru (včetně operačního systému) bez souhlasu uživatele. Po spuštění programu se virus dále šíří do ostatních souborů.
- Červ – jedná se o samostatný malwarový program, který se sám přenáší po síti, aby infikoval další počítače. Rozdíl mezi virusem a červem je v tom, že virus vyžaduje, aby uživatel spustil infikovaný program nebo operační systém, aby se virus rozšířil, zatímco červ se šíří sám.
- Trojské koně – vydávají se za běžný program, který má přimět uživatele tento program nainstalovat na svoje zařízení. Po instalaci může trojský kůň provádět akce, jako je např. krádež citlivých dat, nahrávání souborů na server útočníka nebo monitorování webkamery. Na rozdíl od počítačových virů a červů se trojské koně obecně nepokoušejí vložit do jiných souborů nebo se jinak šířit. (Gregersen, 2013; Clark, 2020; Monnappa K A, 2018; UITS, 2021)

Klasifikovat malware lze i na základě motivu útočníka. Pokud je malware použit ke krádeži osobních, obchodních nebo vlastnických informací za účelem zisku, pak malware lze klasifikovat jako zločinecký nebo komoditní malware. Pokud se malware zaměřuje na konkrétní organizaci nebo odvětví, za účelem špionáže informací, pak může být klasifikován jako cílený nebo špionážní malware. (Monnappa K A, 2018)

Při provádění analýzy malwaru lze přijít na různé typy škodlivých programů. Některé z nich jsou kategorizovány na základě jejich funkčnosti a vektoru útoku, jak je uvedeno zde:

- Backdoor / Remote Access Trojan (RAT) – jedná se o typ trojského koně, který umožňuje útočníkovi získat přístup k napadenému systému a provést v něm příkazy. Jedná se o metodu, která obchází běžné ověřovací postupy, obvykle přes připojení k internetu. Jakmile dojde ke kompromitaci systému, může být nainstalováno jedno nebo více zadních vrátek, aby byl v budoucnu umožněn útočníkovi přístup, který je pro uživatele neviditelný. V minulosti se spekulovalo o tom, že výrobci počítačů předinstalují na své systémy zadní vrátka, aby zákazníkům poskytli okamžitou technickou podporu. Toto tvrzení ale nebylo nikdy spolehlivě ověřeno. V roce 2014 americké vládní agentury přesměrovávaly počítače zakoupené osobami, které byly v jejich „hledáčku“, do tajných dílen, kde byl nainstalován software nebo hardware, který umožňoval vzdálený přístup agentury. Tyto akce jsou považovány za jedny z nejproduktivnějších na celém světě

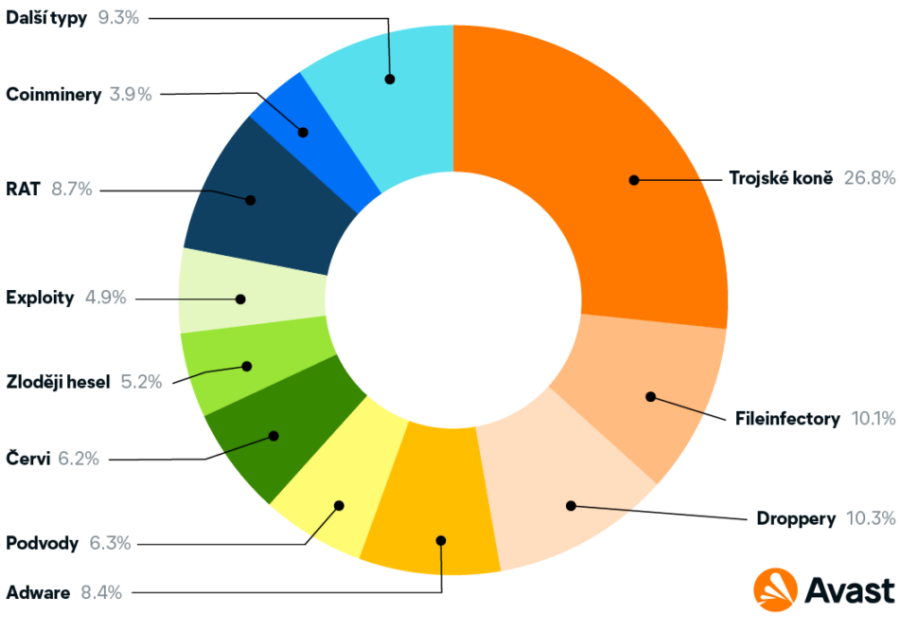
v oblasti získání přístupu k sítím útočníků. Zadní vrátka mohou být instalována trojskými koňmi, červy a jinými metodami. (Spiegel, 2014; Monnappa K A)

- Adware – malware, který uživateli zobrazuje nežádoucí reklamy, nejčastěji prostřednictvím bezplatných aplikací (freeware) a nutí uživatele k instalaci dalšího softwaru na jejich zařízení. Adware tímto způsobem často znepříjemňuje práci. (Monnappa K A, 2018)
- Botnet – jedná se o skupinu počítačů, které jsou infikované stejným typem malwaru (tzv. boti), kteří čekají na přijetí pokynů z příkazového a řídicího serveru ovládaného útočníkem. Útočník pak může těmto botům vydat příkaz, aby prováděly škodlivé aktivity, jako jsou např. DDOS útoky nebo rozesílání spamu na e-mailové adresy. (Monnappa K A, 2018)
- Information stealer – malware určený ke krádeži citlivých dat, jako jsou např. přihlašovací údaje od bankovnictví nebo také zaznamenává stisknutí kláves na klávesnici. Do této kategorie malwaru patří např. keyloggery, spyware, sniffery, stalkerware a lapače formulářů. (Monnappa K A, 2018)
- Ransomware – malware, který zablokuje uživateli používání systému nebo zašifruje jeho soubory a data za účelem výkupného. (Monnappa K A, 2018)
- Rootkit – malware, který poskytuje útočníkovi přístup k infikovanému systému a zatajuje v něm svou přítomnost. Toto ukrytí je dosaženo úpravou operačního systému hostitele tak, aby jeho procesy byly zcela neviditelné. (Monnappa K A, 2018)
- Evasion – od roku 2015 značná část malwaru využívá kombinaci mnoha technik navržených tak, aby se vyhnuly detekci a analýze. Nejběžnější technika je, když se malware při spuštění vyhýbá analýze a detekci pomocí „fingerprint“ techniky prostředí, ve kterém se nachází. Druhou nejběžnější technikou jsou matoucí metody detekce. To umožňuje malwaru vyhnout se detekci antivirového softwaru pomocí změny serveru používaného malwarem. Třetí nejčastější technika je únik na základě načasování. To znamená, že se malware spouští pouze v určitých časech nebo po určitých akcích provedených uživatelem, zatímco zbytek času zůstává nečinný. Čtvrtá nejběžnější technika se provádí zatemněním interních dat uživatele, tudíž antivirový program není schopen odhalit malware. Jedním

z nejsofistikovanějších způsobů ukrytí malwaru v systému je Stegomalware, který používá techniky ke skrývání informací. (HNS, 2015).

Nejčastěji detekované kategorie malwaru v roce 2022 jsou vyobrazeny na obrázku č. 4.

3.2 Zranitelnost vůči Malwaru



Obrázek 4 - Kategorie Malwaru (InSmart, 2022)

Nejčastější způsob šíření malwaru je skrze internet a e-mailovou schránku. Do zařízení, která nejsou chráněna antimalwarovým či antivirovým softwarem, se dostává prostřednictvím napadených webových stránek, demo-verzí her, různých programů, bezplatných služeb či jakýchkoli stažených dat. (Avast, ©2022)

Kyberzločinci často využívají jakékoli zranitelnosti operačního systému nebo aplikačního softwaru, který běží na počítači oběti. Příkladem zranitelnosti webového prohlížeče je, pokud jsou infikované soubory a skriptovací program umístěny na webové stránce. V momentě, kdy uživatel navštíví tuto stránku, skriptovací program stáhne infikovaný soubor do počítače uživatele a poté soubor spustí. Aby tvůrce malwaru infikoval co nejvíce zařízení, využívá k tomu řadu metod, jak budoucí oběti na svou webovou stránku nalákat:

- Odesílání spamových zpráv, které obsahují adresu infikované stránky.
- Odesílání zpráv prostřednictvím systémů IM.

- Prostřednictvím vyhledávačů – text umístěný na infikované stránce je zpracován vyhledávači a odkaz na stránku je poté zahrnut do seznamů výsledků vyhledávání. Jedná se o SEO metodu, kterou využívají i běžné weby. (Kaspersky, ©2022)

Zranitelnost vzniká i v případě, pokud uživatel používá starší verze webových prohlížečů, jako je Microsoft Internet Explorer, nebo starší verze zásuvných modulů (pluginů) pro prohlížeče (Adobe Flash Player, Adobe Acrobat a Java SE). V mnoha případech nepomůže ani aktualizace softwaru, jelikož starší verze stále zůstávají uloženy v zařízení. (Kaspersky, ©2022)

Zranitelnost je ve skutečnosti chyba v kódu nebo logice provozu v rámci operačního systému nebo aplikačního softwaru. Jelikož dnešní operační systémy a aplikace jsou velmi složité a obsahují mnoho funkcí, je pro vývojový tým obtížné vytvořit takový software, který by neobsahoval žádné chyby. Bohužel existuje velké množství tvůrců virů a kyberzločinců, kteří věnují značné úsilí prozkoumání toho, jak mohou profitovat ze zneužití jakékoli zranitelnosti, než dojde k její opravě samotným výrobcem softwaru. (Kaspersky, ©2022)

Příklady zranitelnosti softwaru a operačního systému:

- Chyby zabezpečení aplikace – Poštovní červi Nimda a Aliz zneužívali zranitelnosti aplikace Microsoft Outlook. Když oběť otevřela infikovanou zprávu, nebo dokonce umístila kurzor na zprávu v okně náhledu – spustil se soubor s červem.
- Chyby zabezpečení operačního systému (OS) – CodeRed, Sasser, Slammer a Lovesan (Blaster) jsou příklady červů, které zneužívají zranitelnosti operačního systému Windows. Příkladem červů, kteří využívají zranitelnosti operačního systému Linux a jeho aplikací, jsou např. červi Ramen a Slapper. (Kaspersky, ©2022)

3.3 Ochrana proti malwaru

Každý plán zabezpečení v oblasti informačních technologií se musí vypořádat se všemi druhy malwaru. Malware lze přirovnat k bakterii, která se dostane do vašeho těla a způsobí nemoc. Neexistuje žádné řešení, které by se dokázalo bránit proti veškerému malwaru, stejně jako neexistuje žádný lék, který by dokázal ochránit lidi před všemi nemocemi. Každý problém vyžaduje jiné řešení. 85 % útoků malwaru na zařízení lze zmírnit preventivními postupy. Prevence je nejlepší obranou proti malwaru, ransomwaru a dalším kybernetickým

hrozbám. Vzhledem k tomu, že se tyto hrozby stále množí a stávají se složitějšími, musí být správně pochopeny a riziko, které s sebou přináší, musí být řízeno s nejvyšší prioritou. (Mindanao, 2020)

3.3.1 Antivirus a Antimalware

Cílem tohoto softwaru je zastavit jakékoliv nežádoucí operace, o které se malware může pokusit, dříve, než k nim dojde. Součástí antivirového a antimalwarového softwaru je tzv. on-access nebo real-time scanner, který je umístěn uvnitř operačního systému. Jeho funkčnost je postavena na podobné bázi jako malware, s tím rozdílem, že funguje ve prospěch uživatele a slouží jako ochrana systému. Kdykoli operační systém přistupuje k souboru, on-access skener zkontroluje, zda je soubor „legitimní“, nebo ne. Pokud skener identifikuje soubor jako malware, zamezí jeho otevření a soubor umístí zpravidla do karantény, kde už není hrozba pro systém. Používání antivirového a antimalwarového softwaru může mít značný vliv na výkon zařízení, z velké části závisí na tom, jak byl software naprogramován a kolik funkcí nabízí. (Comodo Cybersecurity, 2015)

Antimalwarové programy chrání systém proti malwaru dvěma způsoby:

- Poskytují ochranu v reálném čase proti instalaci malwarového softwaru do počítače. Tento typ ochrany proti malwaru funguje stejně jako antivirová ochrana v tom, že antimalwarový software neustále prohledává a kontroluje všechna příchozí síťová data na přítomnost malwaru a blokuje jakékoliv hrozby, na které narazí.
- Druhým způsobem je použití detekce a odstranění již nainstalovaného malwaru v systému. Dojde k prohledání obsahu registrů, souborů a nainstalovaných programů v systému. Na konci detekce je poskytnutý seznam všech nalezených hrozeb, což uživateli umožňuje si vybrat, které soubory chce smazat a které ponechat.

Příklady antivirového a antimalwarového softwaru: Avast, McAfee, Bitdefender, Norton, AVG apod. (Comodo Cybersecurity, 2015)

3.3.2 Prevence

Nejlepším způsobem, jak se vyhnout infekci malwarem, je vyhnout se otevírání podezřelých dokumentů a v prvé řadě instalaci malwaru. Lidé s lepšími počítačovými

a technickými znalostmi mají o něco lepší instinkt na to, co by mohl být malware a co ne, ale dobře cílené útoky umí být velmi přesvědčivé. (SSD, 2018)

Příkladem prevence může být otevírání souborů na cloudu předtím, než jsou staženy do zařízení. Používáním méně známých počítačových platforem, jako je Ubuntu nebo ChromeOS, taktéž výrazně zlepší šance proti nakažení malwarem. Důležitá je také aktualizace používaného softwaru, jelikož v aplikacích dochází k neustálé opravě chyb a zranitelných míst. (SSD, 2018)

Bezpečností praktiky:

- Používání více než jednoho obranného systému – webové bezpečnostní brány, firewall, antivirus, antimalware.
- Věnování pozornosti ohledně nejnovějších kyberútoků od známých hackerských skupin. Opravení všech zranitelností co nejdříve.
- Vytvoření a prosazování firemní bezpečnostní politiky. Jakákoliv citlivá data by měla být šifrována jak v klidném stavu, tak při přenosu.
- Používání silných hesel – alespoň 8 až 10 znaků a měla by obsahovat kombinaci písmen a číslic. Zákaz sdílení hesel mezi další osoby a používání stejného hesla na více webových stránkách. Důležité je také pravidelně měnit své heslo a co nejvíce používat dvoufázové ověření.
- Odstranění starých a nepoužívaných účtů, profilů a přihlašovacích údajů.
- Vzdělávání uživatelů ohledně problematiky malware a phishingových útoků. Klást důraz na otevírání příloh od podezřelých profilů a mazání všech nevhodných e-mailů, zejména těch, které pro zobrazení vyžadují použití makra.
- Používání aktualizovaného softwaru a operačního systému.
- Zabezpečení hardwaru proti krádeži. Ukradené pevné disky nebo dokonce flash disky mohou představovat riziko budoucího útoku.
- Zálohování svých souborů v pravidelných intervalech. Zálohovací médium je dobré zapojovat do zařízení pouze tehdy, když chce uživatel provést novou zálohu, nebo obnovit zařízení z předchozí zálohy, aby se minimalizovalo riziko nakažení média. Pokud dojde k nakažení zálohovacího média, může se pak malware roznášet mezi ostatní zařízení, pokud dojde k jeho připojení. (Imaginovation, 2018)

- Vytvoření plánu na reakci v případě kybernetického útoku. Tento plán by měl obsahovat pokyny pro uživatele, co dělat během útoku a jakým způsobem pokračovat v používání zařízení. (Imaginovation, 2018)

3.3.3 Co dělat při nákaze malwarem

Pokud dojde k infikování zařízení malwarem, lze tímto způsobem alespoň omezit jeho dopad:

- Okamžité odpojení infikovaných počítačů, notebooků nebo tabletů od všech síťových připojení – kabelových, bezdrátových nebo mobilních.
- Při velmi vážné nákaze je nutno zvážit, kromě vypnutí Wi-Fi, také deaktivování všech připojení k základní síti (včetně přepínačů) a odpojení se od internetu.
- Obnovení přihlašovacích údajů včetně hesel (zejména pro administrátorské a další systémové účty) – je nutné ověření, že se uživatel nezamyká před systémy, které jsou potřebné pro obnovu.
- Bezpečné vymazání infikovaných zařízení a opětovná instalace operačního systému.
- Před obnovením ze zálohy ověřit, že neobsahuje žádný malware. Obnova ze zálohy by měla být prováděna pouze tehdy, pokud záloha a zařízení, ke kterému je připojována, jsou čisté.
- Připojení zařízení k neinfikované síti, aby mohlo dojít ke stáhnutí, nainstalování a aktualizaci operačního systému a dalšího softwaru.
- Instalace, aktualizace a spuštění antivirového či antimalwarového softwaru.
- Neustálé monitorování síťového provozu a spuštění antivirové nebo antimalwarové kontroly, aby bylo zjištěno, zda přetrvávají nějaké infekce. (NCSC, 2020)

K odhalení časové osy útoku a ke zodpovězení otázek, co se stalo a kdy, mohou pomoci počítačové forenzní vědy následujícím způsobem:

- Kdy infekční vektor dosáhl cíle.
- Kdy byl malware nainstalován.
- Kdy se malware poprvé dostal k útočníkovi.

- Kdy se malware poprvé pokusil rozšířit.
- Kdy malware poprvé provedl svou direktivu.
- Kdy se malware zničil sám, pokud se jednalo o tento typ malwaru k tomu navržený. (Johnson, 2015)

3.4 Analýza malwaru

Analýza malwaru studuje, jakým způsobem se malware chová. Cílem analýzy malwaru je pochopit fungování malwaru a jak jej detekovat a eliminovat. Funguje to na bázi analýzy podezřelého binárního souboru v bezpečném prostředí, kde se identifikuje z hlediska jeho charakteristik a funkcí, aby bylo možné vytvořit lepší obranu pro sítě uživatelů a organizací. (Monnappa K A, 2018)

3.4.1 Důvody provádění analýzy

Primárním cílem provádění analýzy malwaru je extrahovat informace z jeho vzorku, který může pomoci při řešení kybernetického incidentu. Pomáhá také v určení podobných vzorců chování malwaru, které lze použít k ošetření zařízení a prevenci budoucích infekcí. Hlavními důvody provádění analýzy malwaru jsou:

- Určení povahy a účelu malwaru. Například může pomoci určit, zda je malware information stealer, HTTP bot, spamový bot, rootkit, keylogger nebo RAT atd.
- Porozumění tomu, jak byl systém kompromitován a jeho dopadu.
- Identifikace síťových indikátorů spojených s malwarem, které pak lze použít k detekci podobných infekcí pomocí monitorování sítě. Např. během analýzy, pokud je zjištěno, že malware kontaktuje konkrétní doménu/IP adresu, pak lze tuto doménu/IP adresu použít k vytvoření podpisu a monitorování síťového provozu, aby došlo k odhalení všech hostitelů, kteří ji kontaktují.
- Extrahování indikátorů založených na hostiteli, např. názvy souborů a klíče registrů, které je možné použít k určení podobné infekce pomocí monitorování založeného na hostiteli. Pokud je zjištěno, že malware vytvořil klíč registru, lze tento klíč použít jako indikátor pro vytvoření podpisu nebo skenování sítě pro identifikaci hostitelů, kteří mají stejný klíč registru.

- Určení úmyslu a motivu útočníka. Např. pokud během analýzy je zjištěno, že malware krade bankovní přihlašovací údaje, pak je možné odvodit, že motivem útočníka je peněžní zisk. (Barker, 2021; Monnappa K A, 2018)

3.4.2 Typy analýzy malwaru

K pochopení, jakým způsobem malware funguje a jaké má vlastnosti, se využívají různé analytické metody:

- Statická analýza – pokrývá vše, co lze ze vzorku získat, aniž by byl malware skutečně spuštěn a načten do operační paměti. Principiálně to funguje na bázi, jako když člověk zatřese dárkovou krabičkou, aby zjistil, co může očekávat, když ji otevře. Statická analýza umožňuje získat mnoho informací, jež poskytují kontext pro chování malwaru, který se zkoumá při dynamické analýze. Výstupy z této analýzy lze použít jako ochrana proti případnému útoku malwaru. (Barker, 2021)
- Dynamická analýza – proces spuštění zkoumaného vzorku v izolovaném prostředí, monitorování jeho chování a zkoumání technik, které protivník používá k dosažení svých cílů. Poznání a porozumění malwaru umožňuje budovat lepší obranné mechanismy a zabránit dalším incidentům, což činí tuto techniku neuvěřitelně důležitou. (Barker, 2021; Monnappa K A, 2018)
- Analýza kódu – pokročilá technika, která se zaměřuje na analýzu kódu k pochopení vnitřního fungování zkoumaného vzorku. Tato technika odhaluje informace, které nelze získat ze statické a dynamické analýzy. Analýza kódu se dále dělí na statickou analýzu kódu a dynamickou analýzu kódu. Statická analýza kódu zahrnuje rozebírání podezřelého vzorku a nahlížení do jeho kódu k porozumění jeho chování, zatímco dynamická analýza kódu zahrnuje ladění podezřelého vzorku kontrolovaným způsobem, aby bylo možné porozumět jeho funkčnosti. Technika analýzy kódu vyžaduje znalost programovacích jazyků a konceptu fungování operačního systému. (Monnappa K A, 2018)
- Analýza paměti – technika analýzy operační paměti počítače pro forenzní artefakty. Jedná se o typicky forenzní techniku, ale její integrace do analýzy malwaru pomáhá získat poznatky k porozumění chování malwaru po nakažení. Analýza paměti je obzvláště užitečná pro určení tajných a únikových schopností malwaru. (Monnappa K A, 2018)

3.5 Stalkerware

Spyware a další formy malwaru, které umožňují intimní dohled nad partnerem, se označují jako stalkerware. Nejčastěji se stalkerware objevuje v intimních vztazích ke skrytému a vynucenému sledování mobilního zařízení jednoho z partnerů bez jejich vědomí. Zpravidla se tak děje po rozchodu. Po nainstalování stalkerwarové aplikace má útočník přístup k řadě důvěrných osobních údajů o cíli, který sleduje. Aplikace umožňují ze vzdáleného přístupu v reálném čase sledovat textové zprávy, e-maily, fotografie, videa, příchozí a odchozí telefonní hovory, polohu GPS, hesla k bankovním nebo jiným účtům, sociální sítě, mediální účty a další. Aplikace stalkerware se nejčastěji používají skrytě, ale mohou sloužit i k zastrašování, obtěžování nebo vydírání oběti.

Na trhu aplikací jsou volně k dispozici stovky spywarových aplikací, které se tváří jako aplikace pro rodičovskou kontrolu svých dětí. Výzkum provedený v Kanadě a na mezinárodní úrovni naznačuje, že významný podíl žen, které zažívají intimní partnerské násilí, zneužívání a obtěžování také uvádí zkušenosti s řadou zneužívání skrze stalkerware, který jim byl nainstalován na jejich mobilní zařízení. I přes tyto následky se u kanadských soudů objevilo pouze pár nahlášených případů zahrnujících intimní dohled nad partnerem pomocí stalkerwaru. Společnosti zabývající se stalkerwarem v dnešní době profitují z prodeje jejich aplikací na kanadském trhu, aniž by jim v tom bránily trestní nebo regulační zákony. (Khoo, Robertson a Deibert, 2019)

3.5.1 Definice stalkerwaru

Označení stalkerware spíše popisuje, jakým stylem se aplikace používá, než jakým způsobem jsou navrženy její funkce. Komerční spywarové aplikace monitorují a umožňují přístup k:

- Textovým zprávám SMS a zprávám v aplikaci iMessage (včetně historie zpráv a zpráv, které byly ze zařízení odstraněny po instalaci aplikace).
- Aktuálním a historickým datům polohy mobilního telefonu, k záznamům z GPS.
- Záznamům hovorů, včetně historie hovorů.
- Seznamu kontaktů.
- Kalendáři a zapsaným událostem v něm.
- Seznamu všech nainstalovaných aplikací v zařízení.

- Seznamu Wifi sítí, do kterých je jednotlivec přihlášen.
- Fotografiím a videím.
- E-mailovým účtům.
- Historii procházení webu (např. navštívené stránky, počet návštěv a záložky).
- Účtům na sociálních sítích a k jejich soukromému obsahu, včetně aplikací, jako je např Twitter (včetně seznamů a přímých zpráv), Tinder (včetně profilů, shody, seznamy Líbí se/Super/Vynechané) a Instagram (včetně zpráv).
- Datům aplikací pro zasílání zpráv třetím stranám spojená s WhatsApp (včetně smazaných vláken), Kik, Snapchat, Facebook Messenger, WeChat, LINE, Google Hangouts a Telegram.
- Informacím o zařízení, jako je model telefonu, verze Androidu, ID zařízení (UDID číslo) a vnitřní paměť. (Khoo, Robertson a Deibert, 2019)

Všechny tyto funkce, které aplikace nabízí, mohou být potenciální hrozbou, kterou stalkerware představuje, jelikož jsou záměrně navrženy tak, aby monitorovaly a sledovaly cílenou osobu bez jejího vědomí a souhlasu. Nicméně, tyto komerční aplikace představují pouze jeden konec spektra všech aplikací, které lze zneužít ke stalkingu. Na druhém konci spektra jsou neškodné aplikace, jako je např. Find My iPhone, které jsou skutečně navrženy tak, aby uživatelům pomohli najít jejich ztracené telefony. Nicméně, zneužívající mohou využívat funkce takových aplikací ke sledování svých cílů. (Khoo, Robertson a Deibert, 2019)

Některé aplikace obsahují další invazivní funkce, jako je např. schopnost zaznamenávat všechny úhozy zadané na zařízení nebo omezit funkčnost samotného zařízení (vzdálené blokování příchozích hovorů nebo přístupu na určité webové stránky). V některých případech aplikace umožňují operátorovi přijímat upozornění na základě geografické polohy cíle umístění („geofencing“) nebo zadáním konkrétních klíčových slov na klávesnici. Mezi další funkcionalitu stalkerwaru lze zahrnout odposlouchávání telefonních hovorů prostřednictvím „tichého volání“, vzdálenou aktivaci mikrofonu nebo kamery cílového zařízení a SMS spoof, která umožňuje operátorovi stalkerwaru posílat SMS zprávy přes cílové zařízení a tyto zprávy nezobrazovat v historii odeslaných zpráv. (Khoo, Robertson a Deibert, 2019)

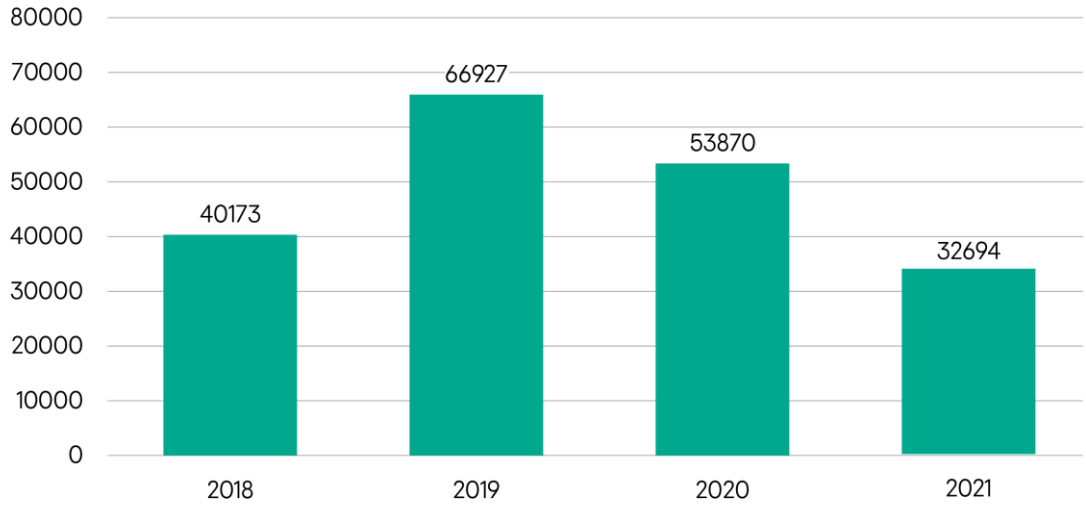
Stalkerware se dělí na tři hlavní kategorie:

- Spywarové aplikace v intimních vztazích – zahrnují aplikace, které jsou záměrně navrženy tak, aby usnadnily skryté sledování mobilního zařízení svého partnera.
- Spywarové aplikace, které jsou využívány jiným způsobem, než byly navrženy – do této kategorie patří aplikace, které jsou záměrně a primárně navrženy za účelem skrytého sledování aktivit jiného jednotlivce na jejich zařízení, ale nejsou výslovně uváděny na trh pro skryté sledování obětí. Mezi tyto aplikace se řadí ty, které se na trhu prodávají jako programy určené ke sledování zaměstnanců nebo dětí.
- Kategorie dalších technologií, které lze využít ke stalkingu – sledovací a monitorovací software, který není ve své podstatě určen k tomu, aby fungoval skrytým způsobem nebo pro účely sledování. Aplikace v této kategorii zahrnují aplikace navržené s funkcemi sledování, jako je Find My Friends nebo Find My iPhone. (Khoo, Robertson a Deibert, 2019)

3.5.2 Nebezpečnost stalkerwaru v dnešní době

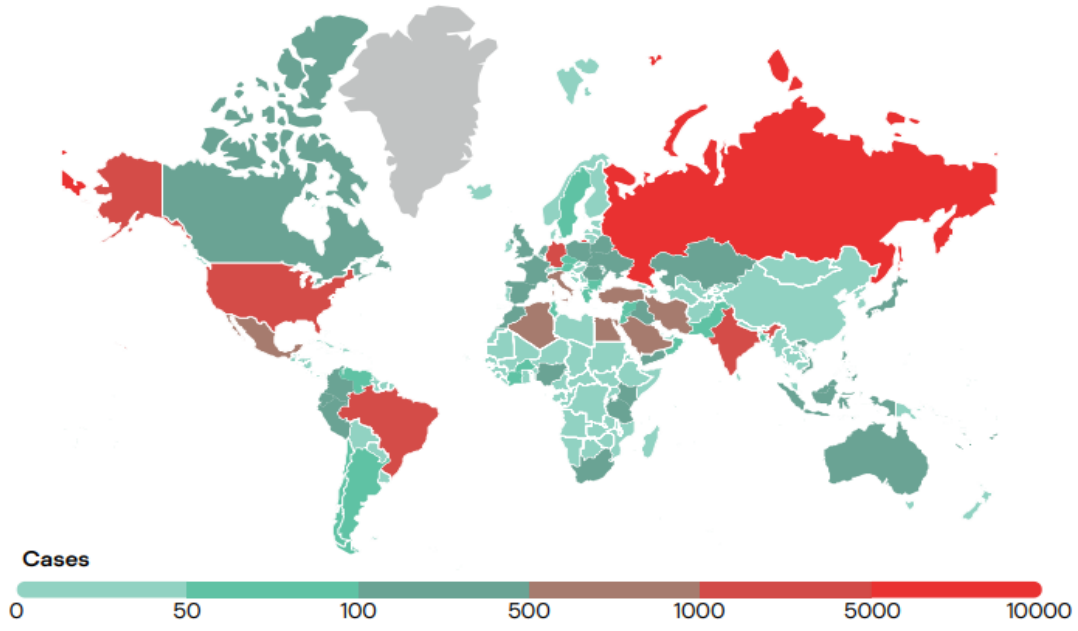
Je důležité zmínit, že metody stalkingu se stále vyvíjejí. Mezi účastníky průzkumu Kaspersky Security Network (KSN) v roce 2021, kteří uvedli, že je jejich intimní partneři špehovali pomocí technologie (samozřejmě nejsou bráni v úvahu ti, kteří o takovém špehování nevěděli), bylo rozdělení stalking nástrojů následující:

- Mobilní aplikace – 50 %.
- Sledovací zařízení (například AirTags, což jsou klíčenky využívané pro snadno ztratitelné předměty) – 29 %.
- Aplikace pro notebooky – 27 %.
- Webové kamery – 22 %.
- Systémy chytré domácnosti – 18 %.
- Fitness trackery – 14 %. (Kaspersky, 2022)



Obrázek 5 – Počet unikátních uživatelů ovlivněných stalkerwarem v letech 2018–2021 (Kaspersky, 2022)

Graf na obrázku č. 5 vychází z dat, která poskytli uživatelé zapojení do průzkumu KSN. Na grafu lze vidět, že počet unikátních uživatelů, kteří se setkali se stalkerwarem na svém mobilním zařízení, má klesající tendenci. Neznamená to ovšem, že by se tato hrozba ze společnosti postupně vytrácela, ale velký vliv na to má celosvětová pandemie. Kvůli lockdownu útočníci nepotřebovali v posledních dvou letech žádné další nástroje pro špehování a kontrolu svých obětí, jelikož ve většině případů spolu pobývali v jedné domácnosti. Je nutné dodat, že tyto statistiky zahrnují pouze údaje od uživatelů, kteří souhlasí s jejich poskytnutím KSN. Coalition Against Stalkerware – organizace sdružující zástupce IT průmyslu a neziskových společností uvedla, že celkový počet uživatelů zasažených touto hrozbou může být až 30krát vyšší. Jinými slovy, podle těchto předpokladů lze tvrdit, že se každý rok stane obětí stalkerwaru asi milion lidí na celém světě. (Kaspersky, 2022)



Obrázek 7 - Stalkerware ve světě v roce 2022 (Kaspersky, 2022)

Na obrázku č. 6 lze vidět, že Rusko, Brazílie, Spojené státy a Indie se drží na prvních příčkách s nejvíce identifikovanými případy stalkerwaru u jednotlivých uživatelů na světě. Oproti roku 2020 klesly případy napadení stalkerwarem v Mexiku, Itálii, Spojeném království a Saudské Arábii. Naopak více případů se začalo objevovat v Alžírsku, Turecku a Egyptě. Obrázek č. 7 přibližuje situaci stalkerwaru v Evropě v roce 2021, kdy byl celkový počet jednotlivých postižených uživatelů celkem 4 236. Německo, Itálie a Spojené království se umístily na prvních příčkách a do seznamu se přidala Česká republika a vystřídala na své pozici Rakousko. (Kaspersky, 2022)

	Country	Affected users
1	Germany	1012
2	Italy	611
3	United Kingdom of Great Britain and Northern Ireland	430
4	France	410
5	Poland	321
6	Spain	321
7	Netherlands	165
8	Romania	125
9	Belgium	94
10	Czechia	82

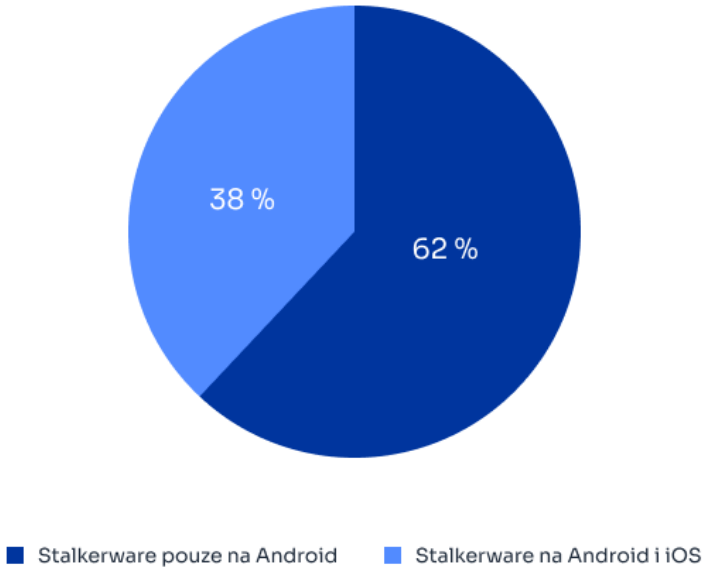
Obrázek 6 - Země s nejvíce identifikovanými případy stalkerwaru v Evropě v roce 2021 (Kaspersky, 2022)

I když se jedná za poslední rok o výrazné snížení počtu postižených uživatelů stalkerwarem, stále veřejnost vnímá používání stalkerwaru za velmi znepokojivé. Většina respondentů (70 %) nevěří, že je přijatelné monitorovat svého partnera bez souhlasu. Významná část lidí (30 %) v tom nevidí žádný problém a za určitých okolností to považuje za přijatelné. Z těch, kteří si myslí, že je stalkování ospravedlnitelné, tak by téměř dvě třetiny využily stalkerware, kdyby měli podezření, že je jejich partner nevěrný (64 %), závisela by na tom jejich bezpečnost (63 %) a kdyby se domnívali, že je jejich partner zapojený do trestné činnosti (50 %). 15 % respondentů na celém světě uvádí, že jejich partner vyžaduje instalaci monitorovací aplikace a 34 % z nich také zažilo fyzické a/nebo verbální zneužívání ze strany tohoto intimního partnera. (Kaspersky, 2022)

Vysokorychlostní internet ve spojení s rychlým šířením informací a komunikačními technologiemi podpořily kybernetické násilí vytvořením dalšího nástroje pro násilníky šířit násilí a nebezpečné materiály. Zatímco tyto technologie daly lidem schopnost udržovat sociální a emocionální vztahy na dálku, nicméně také umožnily vznik kybernetického násilí, které má vliv i na offline svět s negativními dopady na skutečné oběti. (Kaspersky, 2022)

3.5.3 Mobilní zařízení a nejčastější typy stalkerware

Jak lze vidět na obrázku č. 8, nejčastěji se stalkerware objevuje na zařízeních s operačním systémem android (podíl na trhu 72 % všech uživatelů), méně na zařízeních s iOS (jedná se o uzavřený systém). Útočníci však dokážou toto omezení obejít na tzv. jailbreaknutých iPhonech (jailbreak slouží k odstranění vestavěných omezení systému), ale stále potřebují mít přímý fyzický přístup k telefonu, aby tento jailbreak provedli. Alternativním způsobem může být, že útočník prodá oběti předem nakažený iPhone stalkerwarem, nebo zjistí přihlašovací údaje do služby iCloud. Mezi nejčastěji používané stalkerware aplikace patří: Cerberus, Reptilicus, Track My Phones, AndroidLost, MobileTracker Free, Hoverwatch, wSpy. Celkem tyto aplikace postihly více než 17 000 lidí. Nejvíce aplikací funguje na principu freemium a trialu. (Kaspersky, 2022)



Obrázek 8 – Dostupnost stalkerwaru dle mobilního operačního systému (vlastní; Štefanko, 2021)

3.5.4 Počítačová zařízení a nejčastější typy stalkerwaru

Stalkerware se neobjevuje tak často na stolních počítačích a noteboocích, jak je tomu u mobilních zařízení. Tento výskyt je velice vzácný, ale v každém případě existuje. Stejně jako u mobilních zařízení je často stalkerware představován pod záštitou softwaru pro rodičovskou kontrolu nebo monitorování zaměstnanců. V praxi se více setkáváme s keyloggery jako s formou stalkerwaru na počítačích. Keylogger je nástroj, který dokáže zaznamenávat a hlásit aktivitu uživatele při interakci s počítačem. Nejčastěji zaznamenávají úhozy klávesnice. Existují ovšem i jiné druhy keyloggerů:

- Keyloggery na úrovni API (application programming interfaces) – tyto programy nemají správcovské oprávnění, ale přesto dokážou zachytit informace přenášené v rámci API, které umožňuje různým aplikacím přijímat vstup z klávesnice. V systému Microsoft Windows takové keyloggery sledují funkce GetAsyncKeyState nebo GetKeyState API a používají knihovnu DLL k záznamu zachycených dat.
- Keyloggery na úrovni jádra – složitější na vývoj a instalaci do zařízení, ale jakmile se dostanou do systému, je velmi obtížné je detekovat a odstranit.

- Screen scrapers – nezaznamenávají stisknuté klávesy, ale pořizují snímky obrazovky počítače k zaznamenávání textu na obrazovce.
- Keyloggery na úrovni prohlížeče – dokážou detekovat pouze text zadaný do vyhledávače v prohlížeči (vzhledem k tomu, jak velká část našeho online života se odehrává na webovém prohlížeči, jedná se stále o dost nebezpečnou variantu keyloggeru).
- Hardware keyloggery – jedná se o záznamová zařízení, která lze skrýt přímo do samotné kabeláže klávesnice, nebo může být zařízení vytvořeno tak, aby vypadalo jako běžný USB disk, který se následně zapojí do počítače nebo notebooku. Existují i zařízení, která dokážou zaznamenat bluetooth komunikaci mezi bezdrátovou klávesnicí a počítačem. (Gupta, 2022; Fruhlinger, 2022)

3.6 Indikátory nákazy a jakým způsobem se bránit

Pokud se baterie mobilního zařízení a mobilní data vyčerpají příliš rychle, může to být známka toho, že je v zařízení nainstalovaný stalkerware. Stalkerware aktivně využívá zdroje mobilního zařízení, protože potřebuje neustále udržovat spojení se servery, které ho ovládají. Pokud mobilní zařízení samo zapíná Wi-Fi, mobilní internet nebo geolokaci, přestože byla vypnutá, je nutné zkontrolovat, které aplikace spotřebovávají data a přistupují k poloze. Dalším indikátorem stalkerwaru může být neustálé přehřívání zařízení, i když na něm v dané chvíli nic neprobíhá. Majitelé androidů by měli věnovat pozornost aplikacím, které mají nebezpečná oprávnění. Pokud jsou na seznamu aplikací neznámá jména, je to vážný důvod se obávat, kdo nainstaloval tyto neznámé aplikace, kdy a proč.

Je důležité mít na paměti, že na mobilním zařízení může být již předinstalován stalkerware, pokud jej dostanete jako dárek. V dnešní době existují společnosti, které poskytují službu instalace stalkerwaru na nové telefony a jejich dodání v původním balení. Může také dojít ke změně nastavení bez vašeho souhlasu např., pokud je náhle nastavená nová domovská stránka prohlížeče nebo dochází k zobrazování podivných zpráv, např. náhlá záplava vyskakovacích oken nebo chybových zpráv z programů, které předtím vždy fungovaly dobře. (Kaspersky, 2022; Gracej, 2020; Lapienytė, 202)

Stalkerware na počítači funguje na podobném principu jako na Androidu a iOS. Buď má útočník přístup k vašemu počítači nebo vás oklame, abyste si stalkerware nainstalovali sami vlastní chybou. Jako příklad lze uvést IT manažera, který zaměstnancům dodává pracovní

notebooky, nebo někoho z vaší domácnosti, kdo má přístup k vašemu počítači. Detekce stalkerwaru v počítači může být velmi obtížná. Ve většině případů nebude mít počítač s nainstalovaným spywarem znatelné změny ve způsobu jeho fungování (počítač se nemusí nutně zpomalit nebo zamrznout). Pokud bylo nainstalováno hardwarové zařízení, může se nacházet mezi počítačem a kabelem klávesnice, nebo může dojít ke změně celé klávesnice či myši. Na notebooku nemusí být hardwarové zařízení tak patrné, jelikož může být nainstalované přímo uvnitř notebooku přes přístupový panel. (Nield, 2020)

Vlastní průzkum počítače může probíhat pomocí správce úloh ve Windowsu, kde se nachází veškeré procesy, které jsou v danou chvíli na počítači aktivní. Je nutné mít na paměti, že spyware se obvykle neuvádí pod svým skutečným jménem a může se pokusit vydávat za systémovou aplikaci nebo použít krátký název, který lze snadno přehlédnout. Pokud se v seznamu nachází nějaký proces, který je pro uživatele neznámý, nebo cokoli, co se neshoduje s programy, o kterých uživatel ví, že v minulosti nainstalovali, nebo co se zdá podezřelé svým chováním (nadměrné využití disku), pak je nutné rychle vyhledat název aplikace/procesu např. na internetu a odhalit, o co se jedná. Doporučené je zkontrolovat i aplikace a procesy, které se spouštějí ve stejnou dobu jako operační systém, protože většina stalkerwaru se tímto způsobem bude muset aktivovat. K dohledání stalkerwaru může také přispět kontrola aplikací a jejich oprávnění k vašemu zařízení, např. sledování polohy, přístup k webkameře apod. (Nield, 2020)

Společnosti Microsoft a Apple si jsou dobře vědomy problému stalkerwaru, a proto operační systémy Windows a macOS odhalí a zablokují některé skryté nástroje bez jakékoliv další pomoci. Stejně jako u jakéhokoli jiného druhu malwaru lze stalkerware obvykle detekovat pomocí antiviru nebo antimalwaru. Pokud si ovšem uživatel chce být naprosto jistý jeho smazáním, pomůže úplný reset systému do továrního nastavení, což by mělo odstranit i stalkerware, který je zachycený přímo v jádru systému. Důležité je myslet na předchozí zálohování systému, než se provede úplný jeho reset. Vždy je nutné zabezpečit notebook nebo stolní počítač pomocí silného hesla a věnovat pozornost také jejich fyzickému zabezpečení, např. kdo a kdy k němu má přístup. (Nield, 2020)

Jak již bylo uvedeno, stalking často souvisí s obtěžováním a jinými formami násilí. Oběti mohou být psychicky donuceny, zastrašovány nebo fyzicky nuceny deaktivovat svůj přístupový kód, nebo ho útočníkovi odhalit. Zvláště pokud žijí ve společné domácnosti s kyberstalkerem. Oběti musí pečlivě zvážit odstranění jakéhokoli stalkerwaru nebo softwaru s tímto typem funkcí, jelikož stalker to dříve nebo později zjistí, což může často

vést k dalším problémům. V extrémních případech, kdy je kyberstalking pouze jednou z částí velmi nezdravého a zneužívajícího vztahu, oběti se mohou rozhodnout oslovit orgány činné v trestním řízení. To však vyžaduje náležitou přípravu, jelikož budou potřebovat bezpečné zařízení (mobilní telefon s novým telefonním číslem, novou e-mailovou adresou, novými hesly a povolenou vícefaktorovou autentizací), nebo oslovit důvěryhodnou osobu, prostřednictvím které může kontaktovat organizace nabízející pomoc. (Štefanko, 2021)

Existují nástroje, které byly přímo vyvinuté, aby pomáhaly obětem stalkerwaru. Jedná se o nástroj TinyCheck, který umožňuje diskrétně zkontrolovat, zda mobilní zařízení neobsahuje nějaký druh spywaru. TinyCheck se neinstaluje přímo do telefonu, ale funguje na principu externího zařízení (mikropočítač Raspberry Pi). Toto zařízení funguje jako prostředník mezi Wi-Fi routerem a zkoumaným mobilním zařízením. Po instalaci TinyCheck zanalyzuje internetový provoz mobilního zařízení v reálném čase. Na základě toho lze zjistit, zda se v mobilním zařízení nachází stalkerware (pokud aplikace odesílá velké množství dat na známé spywarové servery, nástroj TinyCheck to odhalí). (Kaspersky, 2022)

3.7 Dílčí závěr

Kapitola shrnuje problematiku malware a jeho dělení, které slouží pro hlubší pochopení, jakým způsobem malware funguje a jak se proti němu bránit. V poslední části byla detailně rozebrána problematika stalkerware, bez které by nebylo možné vytvořit prototyp školicí aplikace v praktické části práce. Primárním úkolem je shrnutí oblastí, které stalkerware dokáže sledovat a monitorovat a také jakým způsobem se může zařízení infikovat.

Stalkerware a spyware se stali mnohem sofistikovanějšími a jsou schopni infiltrovat zařízení bez pomoci nic netušících uživatelů. Jakmile se dostanou do zařízení, použijí techniky zatemnění, aby se skryli, a přitom útočníkům poskytnou neomezený přístup ke každé aktivitě na zařízení. V některých případech jsou příznaky nakažení zřejmé, jako jsou četná vyskakovací okna, časté systémové chyby nebo pomalý výkon počítače. Ve většině případů to však není tak snadné, jelikož tento typ malwaru je navržen tak, aby bylo obtížné jej odstranit. Jedna infekce může otevřít dveře mnoha dalším. Díky tomu jsou pokusy o odstranění svépomocí ve většině případů neúspěšné.

K detekci a odstranění hrozby lze využít antivirový nebo antimalwarový software. Je však vhodné připomenout, že při detekci prohledávají známé cílové oblasti spywaru a porovnávají počítačové soubory s databází spywaru, což znamená, že software bude detekovat pouze známé hrozby.

II. PRAKTICKÁ ČÁST

4 POPIS OBJEKTU

Městský úřad se nachází ve Vyškově, v okresním městě v severní části Jihomoravského kraje na řece Haná, 30 km severovýchodně od Brna. Leží téměř uprostřed Moravy na rozhraní Drahanské vrchoviny, Litenčických vrchů a nížiny Hornomoravského úvalu v nadmořské výšce okolo 250 m n. m. Je jedním z hraničních měst regionu Haná. Žije zde přibližně 21 tisíc obyvatel.

Jak lze vidět na obrázku č. 9, úřad se nachází v samotném centru města Vyškova na Masarykově náměstí. Dříve byl umístěn na ulici Brněnská. Nachází se zde tyto odbory: Kancelář starosty a tajemníka, Odbor dopravy, Odbor finanční, Odbor investiční, Odbor majetkoprávní, Odbor místního hospodářství, Odbor sociálních věcí a zdravotnictví, Odbor správní a vnitřních věcí, Odbor školství, kultury a sportu, Odbor územního plánování a rozvoje, Odbor životního prostředí, Obecní živnostenský úřad, Stavební úřad. (Město Vyškov, 2020)

Obrázek 9 – Mapa města Vyškova (Mapy.cz)

4.1 Bezpečnostní politika informačního systému Městského úřadu Vyškov

Informační bezpečnost je jedním ze stěžejních pilířů při budování informačního systému úřadu. Městský úřad ve Vyškově (MěÚ) získává a pracuje s celou řadou informací, které je nutné chránit. Bezpečnostní politika se vztahuje na město Vyškov a jeho zaměstnance, kteří pro svou práci využívají data uložená v informačním systému města Vyškov. Nevztahuje se na organizace, které využívají data, nacházející se v informačním systému prostřednictvím dálkového přístupu se stupněm oprávnění pro veřejnost. Tato politika je dennodenně prověřována, kontinuálně kontrolována a aktualizována. (Vyškov, 2018)

4.1.1 Cíle bezpečnostní politiky

Cílem bezpečnostní politiky městského úřadu ve Vyškově je zajištění takové ochrany informačního systému a informací v něm uložených, aby k nim měly přístup pouze oprávněné osoby a nedošlo k jejich nekontrolovatelnému úniku. Musí být zajištěna dostupnost těchto informací, integrita, prokazatelnost a odpovědnost za danou informaci. Aktiva mají pro subjekt hodnotu, která je v absolutní většině případů z hlediska jejího fungování kritická. (Karel Břoušek, 2021; Vyškov, 2018)

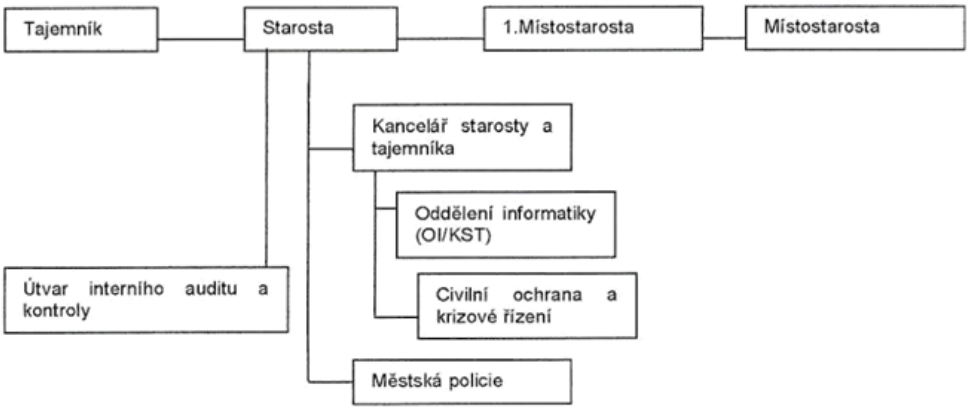
Subjekt se pomocí stanovených cílů, strategií a politik dělí na oblasti řešení bezpečnosti:

- Fyzické – ochrana fyzických aktiv, budov, počítačů, médií, prevence krádeží apod.
- Personální – pokrytí hrozeb představovaných zaměstnanci, dodavateli, nezkušenými uživateli, hackery a ochrana vlastních zaměstnanců.
- Komunikační – ochrana datové a hlasové komunikace.
- Provozní – postupy při uplatňování preventivních bezpečnostních opatření, postupy při detekci útoku, havarijní plány a vývoj metod prevence a detekce. (Vyškov, 2018)

4.1.2 Organizace bezpečnostní politiky

Postavení jednotlivých organizačních prvků při organizaci bezpečnostní politiky vychází z organizační struktury úřadu stanovené organizačním řádem, který lze vidět na obrázku č. 10.

Vedení organizace (starosta, místostarostové, tajemník) schvaluje doporučení pro tvorbu bezpečnostní politiky na základě zvážení rizik a charakteru přijímaných opatření pro jejich minimalizaci. Oddělení informatiky zpracovává a realizuje bezpečnostní politiku informačního systému. Vedoucí Útvaru interního auditu a kontroly spolupracuje s oddělením informatiky při vytváření bezpečnostní politiky informačního systému tak, aby byla v souladu s celkovou bezpečnostní politikou organizace. (Vyškov, 2018)



Obrázek 10 – Organizace bezpečnostní politiky (Vyškov, 2018)

4.2 Fyzické zabezpečení

Fyzická bezpečnost na Městském úřadě ve Vyškově je velice spolehlivá. Prostory jsou rozděleny pro veřejnost a zvlášť pro zaměstnance. (Karel Břoušek, 2021)

4.2.1 Fyzická bezpečnost perimetru

Objekt je neustále pod dohledem bezpečnostních kamer, které jsou 24 hodin denně sledovány Městskou policií Vyškov, která se nachází ve vedlejší budově úřadu. Před vstupem do prostoru úřadu se nachází velká železná brána a z druhé strany úřadu dřevěná vrata, která se po ukončení pracovní doby zavírají a zamykají. Samotný úřad má zamykatelné automatické dveře, které se rovněž zamykají a v průběhu dne jsou kontrolovány recepční. Okna ve spodních patrech jsou zabezpečena mřížemi. (Karel Břoušek, 2021)

4.2.2 Fyzická kontrola vstupu do veřejného prostoru

Při vstupu do veřejné části, kde se nachází vstupní hala, toalety, společně s informacemi, kde se každý odbor nachází, není vyžadována žádná fyzická kontrola vstupu. Při vchodu se nachází recepční, která má pomoci lidem při jejich dotazech. V této veřejné části se nachází video-dohledový systém, elektronická požární signalizace a poplachové zabezpečovací

tísňové systémy. V případě požárů by mělo ve veřejné části také dojít ke spuštění sprinklerů. (Karel Broušek, 2021)

4.2.3 Fyzická kontrola vstupu do prostoru pro zaměstnance

Každý zaměstnanec po svém příchodu přikládá zaměstnaneckou kartu k zařízení, které monitoruje jejich přítomnost na úřadě. Každé patro a jednotlivé kanceláře jsou zabezpečeny alarmem, který zaměstnanec při svém příchodu odblokuje pomocí kódu. Každá kancelář je zabezpečena dveřmi se zámkem, který lze odemknout patřičným klíčem. Pracoviště systémového administrátora, vedoucího OI/KST a bezpečnostního tajemníka jsou opatřeny uzamykatelnými dveřmi bez kliky a ostatní pracovníci zde mohou vstupovat pouze s předchozím svolením příslušných osob. Při opuštění pracoviště je povinen zaměstnanec zajistit pracoviště takovým způsobem, aby nedošlo k vniknutí nepovolené osoby, tzn. uzamčení kanceláře, všechny důvěrné údaje uzamknout v trezorech a uzamykatelných skříňkách a vypnout či uzamknout počítač. Nesmí poskytnout klíče ostatním zaměstnancům, kteří v kanceláři nepracují, a nesmí je tam zanechat bez dozoru. (Karel Broušek, 2021; Vyškov, 2018)

4.2.4 Fyzické zabezpečení technických místností a vybavení

Servery, rozvodné skříně a komunikační zařízení jsou opatřeny uzamykatelnými protipožárními dveřmi a pokud se nacházejí na spodních patrech, tak rovněž i okenními mřížemi. Jsou vybaveny automatickými protipožárními prostředky vhodnými pro daný typ zařízení. Přístup je povolen pouze správci sítě a vedoucímu (OI/KST). Jiným např. servisním pracovníkům pak pouze za přítomnosti některého z výše jmenovaných pracovníků. Místnosti jsou trvale uzamčeny a klíče má k dispozici pouze vedoucí OI/KST, náhradní klíče se nacházejí v prostorách městské policie, kde jsou nepřetržitě chráněny. (Karel Broušek, 2021; Vyškov, 2018)

Komunikační zařízení (aktivní prvky LAN, modemy, rozvaděče, routery, ústředny apod.) jsou umístěny v uzamykatelných skříních (rack). Servery mají uzamykatelné kryty, které jsou zajištěny proti náhodnému vypnutí či resetu ovládacími tlačítky. Při výpadku elektrické energie jsou zajištěny záložním zdrojem (UPS) a dieselagregátem. Klíče od těchto skříní jsou opět uloženy u vedoucího OI/KST a v trezoru na oddělení informatiky. (Karel Broušek, 2021; Vyškov, 2018)

4.3 Bezpečnost provozu informačního systému

Provozní postupy jsou pro každý informační systém specifikovány v uživatelských příručkách, které jsou průběžně aktualizovány dle verze jednotlivého informačního systému. Uživatelské příručky jsou umístěny na intranetu MěÚ. (Karel Břoušek, 2021; Vyškov, 2018)

4.3.1 Organizace bezpečnosti

Pro zajištění provozu všech aplikací je správa těchto aplikací rozdělena mezi pracovníky oddělení informatiky, jsou tedy zároveň v roli správců informačního systému. Správce aplikace zajišťuje chod aplikace v souladu se systémovou příručkou a provozní bezpečnostní dokumentací. V rámci aplikace je oprávněn řídit přístup oprávněných uživatelů. Při řešení problémů spolupracuje s dodavatelem aplikace a instaluje opravy nebo nové verze. Je odpovědný za ochranu dat před poškozením nebo ztrátou (zálohování). (Karel Břoušek; Vyškov, 2018)

Pro zajištění provozu lokální počítačové sítě je ustanoven správce sítě, který je zodpovědný za zajištění bezporuchového provozu serverů a počítačové sítě a zajištění přístupu všem oprávněným uživatelům k uživatelským programům serverů, zajištění ochrany dat uložených na síťových serverech před zneužitím, poškozením, ztrátou a zničením. (Karel Břoušek; Vyškov, 2018)

Vedoucí OI/KST je zodpovědný za uplatňování bezpečnostní politiky. V součinnosti s vedoucími pracovníky odborů, prostřednictvím správce sítě a správci aplikací povoluje přístup oprávněných uživatelů k jednotlivým aplikacím a vede evidenci jejich přístupových práv. Pravidelně provádí kontroly dodržování pravidel stanovených bezpečnostní politikou a informuje o výsledcích vedení organizace. (Vyškov, 2018)

Uživatelem aplikace je každý uživatel, který má povolen přístup k určitému programovému vybavení, nebo k určitým službám sítě a je povinen:

- Projít základním zaškolením a seznámit se s uživatelskou příručkou informačního systému, se kterým pracuje a má k němu pověření, a dodržovat zásady uvedené v provozní bezpečnostní dokumentaci informačního systému.
- Užívat informační a komunikační technologie (ICT) pouze k plnění svých pracovních povinností a v souladu s účelem, ke kterému byly ICT určeny a vytvořeny a řídit se pokyny pracovníků oddělení informatiky.

- Zabezpečit fyzicky hardware (počítač či terminál) proti poškození či odcizení (Směrnice č. 4/2018).
- Používat pouze software, na jehož užívání má město Vyškov platnou licenci a který je nainstalován. Používání jakéhokoliv jiného software, včetně volně šířených programů (freeware), případně dalších zkušebních verzí a demoverzí, není povoleno bez souhlasu správce informačního systému.
- Hlásit veškeré závady jak na výpočetní technice, tak na programovém vybavení zaměstnancům OI/KST.
- Nesmí používat ani poskytnout jiným uživatelům jakékoliv neoprávněně získané klíče – dekodéry či jiné technické prostředky sloužící k zajištění informační bezpečnosti a ochraně počítačových programů, např. různá sériová čísla softwaru nalezená na internetu apod.
- Odpovídá za případné škody způsobené jím rozšířenými počítačovými viry, např. při manipulaci s přenosnými datovými médii, s elektronickou poštou, mobilními prostředky. (Vyškov, 2018)

4.3.2 Bezpečnost přístupu třetích stran

Třetí stranu představují z hlediska přístupu k informačnímu systému servisní pracovníci dodavatelů informačních systémů či pracovníci organizací spolupracující na výstavbě a údržbě dat GIS.

Přístup těchto pracovníků může být realizován pouze se souhlasem vedoucího OI/KST a na základě zřízení samostatného účtu pouze s nezbytnými přístupovými právy. Při servisním zásahu dodavatelem informačního systému je navíc nezbytný souhlas správce aplikace nebo správce sítě a každá taková událost se zaznamenává v evidenci mimořádných událostí (formou deníku či elektronickou formou). Vzdálený přístup dodavatelů k informačnímu systému MěÚ musí být vždy smluvně ošetřen. (Vyškov, 2018)

4.3.3 Personální bezpečnost

Nově nastupující pracovník je povinen se seznámit se základními dokumenty úřadu (organizační a provozní řády, směrnice, pravidla pro nakládání s osobními údaji apod.), včetně zásad bezpečnostní politiky a základními uživatelskými znalostmi v rámci úvodního školení. Na základě jeho pracovního zařazení a pracovní náplně po schválení vedoucím

pracovníkem jsou mu vedoucím OI/KST stanovena jeho přístupová práva a zapsána do evidence záznamů o přístupových právech. Správcem sítě jsou pracovníkovi vytvořeny účty s odpovídajícím přístupovými právy na základě „pověření“. To stejné probíhá i při změně pracovního poměru (přechodu na jinou funkci).

Při ukončení pracovního poměru jsou zrušeny nebo zablokovány všechny přístupové účty využívané pracovníkem. Dokumenty vytvořené pracovníkem jsou systémovým administrátorem zálohovány a dle situace předány pracovníkovi přebírajícímu funkční náplň. Následně jsou odstraněny. (Vyškov, 2018)

4.3.4 Monitoring

Monitorování bezpečnosti provozu je realizováno standardními administrátorskými prostředky jednotlivých operačních a aplikačních systémů. Oddělení informatiky využívá testovací sondy, které monitorují základní funkčnost hardwaru (komunikaci, volné místo) a zasílá zprávy při překročení nastavených hodnot. V roce 2018 došlo k nákupu nového softwaru, který monitoruje celou infrastrukturu MěÚ, včetně aplikací a komunikace jak zevnitř, tak zvenčí.

V současné době se také monitorují event logy operačních systémů na serverech i stanicích včetně firewallu, logy aplikačních programů, výsledky antivirových testů, aktivní síťové prvky i dostupnost serverů.

U informačních systémů je sledována míra jejich využívání, aby bylo včas možné zajistit upgrade provozního prostředí IS z důvodu zajištění jeho správné funkcionality i při nárůstu objemu zpracovávaných dat nebo počtu uživatelů. Při úpravách IS je nezbytné stanovit akceptační kritéria a provést odpovídající testy. Při akceptaci systému je třeba zvážit požadavky systému na výpočetní a paměťový výkon, schopnost jeho zotavování z chyb, přípravu a test rutinních provozních postupů a vliv na ostatní systémy. (Karel Břoušek, 2021; Vyškov, 2018)

4.3.5 Ochrana proti škodlivým programům

Ochrana proti škodlivým programům se dělí na prevenci (stanovení pravidel, vhodné nastavení prostředí operačního systému, update aplikací a vzdělávání uživatelů) a detekci (antivirové, antispamové a antispywarové programy).

Potenciálním zdrojem nákazy mohou být výměnná datová média, notebooky, ostatní přenosná zařízení, elektronická pošta a internet.

Mezi škodlivé programy patří programy typu virus, červ, trojský kůň, neschválený software, e-mailový spam a spyware. Jsou to obecně programy narušující bezpečnost IS úřadu (provádějící neautorizované operace na datech), které nesouvisejí s výkonem agendy úřadu, zatěžují a blokují zdroje a komunikační cesty. (Vyškov, 2018)

Povinnosti každého uživatele:

- Uživatel nesmí nijak měnit nastavení antivirového systému.
- Uživatel nesmí instalovat na počítač jakýkoli software.
- Je povinen při užívání prověřit přenosná média antivirovým programem.
- Je povinen provádět na stanici pravidelnou antivirovou kontrolu (alespoň jedenkrát týdně, v současné době je to nastaveno automaticky).
- Je povinen oznámit podezření na výskyt škodlivého programu správci sítě.
- Neotevírat nedůvěryhodné soubory.
- Neotevírat přílohy v doručených e-mailech, pokud si není jist, že pochází z důvěryhodného zdroje.
- V rámci přístupu na internet, nesmí stahovat, spouštět nebo instalovat jakýkoliv software získaný ze zdrojů na internetu a vyhledávat informace nesouvisející s pracovní náplní zaměstnance (na nedůvěryhodných serverech). (Karel Břoušek, 2021; Vyškov, 2018)

K detekci virů a malwaru slouží antivirový systém. Působí jako ochrana souborového systému pracovních stanic a serverů, a ve spojení s e-mailovým klientem i jako kontrola emailových zpráv. Je schopen detekovat a odstranit většinu známých virů, červů a trojských koní. Jeho aktualizace je prováděna automaticky dle nastavení intervalu pro kontrolu přítomnosti nové aktualizace na serveru. Aktualizační soubory dodává správce sítě a odpovídá za stav antivirového systému na serverech i jednotlivých stanicích. Při detekci viru na serveru nebo pracovní stanici rozhoduje o dalším postupu. (Karel Břoušek, 2021; Vyškov, 2018)

4.3.6 Bezpečnost komunikačních technologií

IS je vystaven riziku napadení prostřednictvím počítačové sítě zvenčí i zevnitř. Ke snížení rizika odposlechu provozu na vnitřní síti je využita segmentace sítě s využitím přepínačů,

pro překlenutí vzdáleností mimo budovu optického spoje a zabezpečené mikrovlnné spoje. (Karel Břoušek, 2021)

Sít' LAN MěÚ je připojena na internet kombinací firewallu a proxy serveru. Firewall rovněž řídí dálkový přístup třetích stran k IS MěÚ. Kromě sítě LAN MěÚ je pro výkon správních a dopravně-správních činností provozována sít' připojená WAN spojem k síti Ministerstva vnitra. Tato sít' je fyzicky oddělená od sítě LAN MěÚ. Komunikační rozhraní této sítě je ve správě Ministerstva vnitra a je přístupné jen pro správce této sítě. K síti není povoleno připojovat žádná jiná zařízení, než která jsou k tomu určena. (Vyškov, 2018)

Komunikace ve vnitřní síti LAN se servery nebo ostatními stanicemi a terminály je umožněna pouze uživatelům autentizovaným prostřednictvím síťového operačního systému. Je zakázáno připojovat uživatelům do sítě LAN další zařízení.

Rovněž je zakázáno připojovat se do jiných sítí např. pomocí modemu, mobilních zařízení apod. Nevyužívané vstupní body sítě (v prázdných místnostech, nevyužívané síťové přípojky na pracovištích) musí být správcem sítě zneaktivněny. (Karel Břoušek, 2021; Vyškov, 2018)

4.3.7 Bezpečnost při zacházení s médii

Z hlediska uloženého obsahu se média dělí na instalační, transportní a zálohovací.

Veškerá instalační média (flashdisky, CD, DVD) jsou uložena na OI/KST na určeném místě. Dle důležitosti je možno k instalačnímu médiu pořídit jednu záložní kopii. Za manipulaci s instalačními médii a soubory včetně kopií odpovídá vedoucí OI/KST. Vyřazená média obsahující licencovaný software, data interního nebo osobního charakteru musí být protokolárně zlikvidována po vyřazení softwaru z majetku MěÚ. Zálohovací média musí být uložena odděleně (v jiné místnosti) od místa uložení zálohovaných dat (serveru, stanice). Transportní média slouží k přenosu dat mezi jednotlivými subjekty. Média obsahující data interního nebo osobního charakteru se předávají pouze na základě předávacího protokolu. (Karel Břoušek, 2021; Vyškov, 2018)

4.4 Řízení přístupu

Řízení přístupu musí být uplatňováno ve všech případech přístupu uživatelů k neveřejným datům. Základním prostředkem řízení přístupu je autentizace uživatele prostřednictvím uživatelského jména a hesla. Na základě autentizace je uživatel jednoznačně identifikován a jsou mu zpřístupněna odpovídající data IS. (Vyškov, 2018)

4.4.1 Správa přístupu uživatelů

Standardní uživatelský účet pracovníka MěÚ a pracovníka městské policie ho opravňuje používat pracovní stanice MěÚ a další systémové zdroje (tiskárny apod.), přistupovat ke všeobecně dostupným datům na serverech (systém právních informací-ASPI, docházkový systém), přistupovat ke svému privátnímu a společnému adresáři na serveru a využívat služeb elektronické komunikace (e-mail).

Přidělení, změnu nebo odebrání dalších přístupových práv provádí vedoucí OI/KST podle funkční náplně činnosti pracovníka ve spolupráci příslušného vedoucího pracovníka a tajemníka. (Karel Břoušek, 2021)

4.4.2 Uživatelská hesla

Uživatelská hesla musí splňovat tato základní kritéria:

- Minimální délka hesla je 5 znaků, u privilegovaných a administrátorských účtů minimálně 8 znaků.
- Heslo musí obsahovat bezvýznamovou kombinaci alfanumerických znaků.
- V případě zvýšených nároků na bezpečnost dat lze zvýšit nároky na minimální délku hesla nebo hesla časově omezit, tzn. uživateli bude nařízeno provádění pravidelné změny hesla a stanovení maximálního počtu neúspěšných přihlášení, po němž dojde k zablokování účtu.
- Počáteční nastavené heslo nebo implicitní heslo musí být uživatelem při prvním přihlášení změněno.
- V případě zapomenutí hesla oznámí uživatel tuto skutečnost bezpečnostnímu správci, který mu přidělí nové počáteční heslo.
- Platnost uživatelského hesla uživatele „Administrátor“ je stanovena na 6 měsíců a je nastavena na doménovém řadiči, který uživatele vyzve po uplynuté lhůtě ke změně hesla.

4.4.3 Odpovědnost uživatelů, administrátorů, servisu a bezpečnostního správce

Každý uživatel smí užívat přidělený uživatelský účet výlučně pro vlastní potřebu. Získané údaje nesmí sdělovat neoprávněným osobám. Přihlášení může být provedeno pouze pod vlastním uživatelským jménem a heslem. Heslo je povinen uživatel držet v tajnosti, tzn.,

nesmí jej zapisovat a nikomu sdělovat. Jakékoliv pochybnosti o možném prozrazení, zneužití nebo při zapomenutí hesla je uživatel povinen kontaktovat bezpečnostního správce. Po dobu přihlášení nesmí uživatel nechávat počítač bez dohledu a při opuštění pracoviště je povinen jej uzamknout nebo vypnout. (Karel Břoušek)

Administrátoři a servisní pracovníci mají povinnosti jako standardní uživatelé a používají standardní uživatelské účty. Privilegované uživatelské účty mohou využívat pouze v nezbytně nutných případech. (Karel Břoušek)

Bezpečnostní správce musí mít do každého systému nastavena taková přístupová práva, která odpovídají právům administrátora systému. Bezpečnostní správce je povinen po každé změně svého přístupového hesla nebo jakéhokoliv hesla na úrovni administrátora systému (pokud existuje více uživatelů s právem přístupu na úrovni administrátora) toto heslo zapsat, vložit do obálky a obálku zalepit. Tato obálka je potom opatřena razítkem MěÚ znemožňujícím její otevření bez zanechání stop a následně uložena na sekretariátu. V případě nutnosti (úmrtí bezpečnostního správce, dlouhodobá neočekávaná nepřítomnost, zapomenutí hesla bezpečnostním správcem) může být obálka otevřena za splnění následujících podmínek:

- Otevření obálky se zúčastní minimálně 2 osoby, z nichž alespoň jedna osoba je starosta, místostarosta nebo tajemník Městského úřadu.
- Po otevření obálky se provede zápis do dokumentu Evidence poruch a mimořádných událostí informačního systému.
- Odpovědná osoba okamžitě po otevření obálky změní heslo v informačním systému.

4.4.4 Řízení přístupu k vnitřní síti

K vnitřní LAN lze přistupovat z vnitřní pracovní stanice a případně i z vnější pracovní stanice dálkovým přístupem prostřednictvím internetu. Vnitřní přístup je řízen logicky (nastavením přístupových práv), vnější přístup logicky i fyzicky (omezení firewallem na konkrétní počítač prostřednictvím pevné IP adresy, konkrétní komunikační port). Přístup je blokován mimo pracovní dobu úřadu zavedením časových restrikcí na přihlašování uživatelů. Případné výjimky povoluje vedoucí OI/KST.

Dálkový přístup je umožněn každému smluvně vázanému dodavateli města Vyškov, který o to požádá. Důvodem může být buď vzdálená správa IS nebo urgentní oprava systému. Veškeré přístupy jsou ovšem monitorovány a předem oznámeny či vyžádány objednatelem. V případě zvýšeného nebezpečí (rozšíření nového viru apod.) je přístup blokován na dobu nezbytně nutnou. Provádí se o tom záznam do Evidence poruch a mimořádných událostí informačního systému a tato skutečnost je také oznamována všem, kdo tohoto typu přístupu využívají. (Karel Břoušek, 2021; Vyškov, 2018)

4.5 Vývoj a údržba informačního systému

Nevyužívají se aplikační systémy, které by byly vyvíjeny vlastními prostředky. Požadavky na dodavatelské aplikační systémy:

- Atest dle požadavku zákona č. 365/2000 Sb., o informačních systémech veřejné správy.
- Možnost autentizace a identifikace přístupu jednotlivých uživatelů.
- Možnost přidělování přístupových práv uživatelům k jednotlivým modulům a datům IS.
- Možnost monitorování přístupu jednotlivých uživatelů.
- Možnost sledování změn prováděných v IS (historie).
- Provozně-bezpečnostní dokumentace.
- Garance dalšího vývoje systému. (Vyškov, 2018)

4.5.1 Bezpečnost systémových souborů

Bezpečnost systémových souborů je řešena na úrovni operačních systémů a jejich bezpečnostních prvků, běžní uživatelé k nim nemají přístup. (Karel Břoušek, 2021)

4.5.2 Bezpečnost procesu vývoje a údržby

V procesu údržby dochází často k instalaci nových verzí či oprav. Pro tento proces platí následující pravidla:

- Pokud příslušný IS má podstatný vliv na chod úřadu, provádí se mimo úřední hodiny MěÚ nebo po dohodě s pracovníky využívajícími tento IS.
- Před jeho započetím musí být provedena taková záloha dat, aby bylo IS možno vrátit do původního stavu.

- Nedílnou součástí tohoto procesu je dokumentace od dodavatele aplikace s podrobným popisem instalace, změn v aplikaci a záznam v provozní evidenci daného IS. (Karel Broušek, 2021; Vyškov, 2018)

4.6 Informační bezpečnost a správa incidentů

Bezpečnostní incidenty všech úrovní má na starosti vedoucí OI/KST ve spolupráci s bezpečnostním ředitelem úřadu a pověřencem pro ochranu osobních údajů. Týká-li se bezpečnosti incident osobních údajů, je do toho zapojen i pověřenec pro ochranu osobních údajů, který má za povinnost incident hlásit Úřadu na ochranu osobních údajů (do 72 hodin). Na základě analýzy příčin a průběhu incidentu navrhuje vedení organizace nápravná opatření. (Karel Broušek, 2021; Vyškov, 2018)

V rámci správy přístupových oprávnění k registru živnostenského podnikání mohou vzniknout nestandardní situace, které musí řešit kontaktní osoba ve spolupráci s uživateli. Jedná se konkrétně o:

- Ztrátu karty.
- Zničení, poškození, trvalé zablokování karty.
- Zneužití přístupu k IS registru živnostenského podnikání (RŽP). (Vyškov, 2018)

U nestandardních situací, které uživatel mohl vyřešit nebo vyřešil sám (vyzrazení PIN ke kartě), kontaktní osoba pouze předává zpětně prostřednictvím Helpdesku informaci o nestandardní situaci poskytovateli služby. Ostatní nestandardní situace je nutno řešit podle pokynů poskytovatele služby. (Karel Broušek, 2021; Vyškov, 2018)

4.7 Řízení kontinuity podnikání

Při provozu IS muže nastat celá řada krizových situací ovlivňujících kontinuitu využívání IS, kdy po takové události by nemuselo dojít k obnovení IS do stavu před touto událostí. Mezi takové situace patří havárie datových zařízení (serveru, paměťových zařízení apod.), živelní pohroma (povodeň, požár apod.), ztráta dat např. v případě uživatelské chyby nebo chyby softwaru, krádež dat, delší nepřítomnost administrátorů.

Pro minimalizaci těchto rizik slouží následující opatření:

- Záloha dat IS je prováděna denně. Zálohy jsou uloženy na bezpečném místě (dle povahy uložených dat v trezoru nebo uzamykatelné skříni), v oddělené místnosti vzhledem k umístění datových zařízení.
- Datová zařízení jsou umístěna v takových místech, aby bylo minimalizováno riziko jejich poškození, např. při povodni nebo požáru a fyzicky zabezpečena proti přístupu neoprávněných osob.
- Instalační média jsou uložena centrálně na OI/KST včetně jejich seznamu.
- Administrátorská hesla a hesla privilegovaných účtů jsou uložena v trezoru MěÚ.
- Ke každému IS je vedena provozní evidence, obsahující historii updatů, změn a provedení nastavení daného IS. (Karel Břoušek, 2021; Vyškov, 2018)

4.7.1 Krizové plány a havárie

Krizové plány musí být vytvořeny tak, aby v případě přerušení nebo selhání procesů vhodným způsobem bylo možné procesy udržet nebo obnovit v odpovídajícím časovém horizontu. Pro případ nebezpečí živelních pohrom (požár, povodeň apod.) se zpracovávají požární a poplachové směrnice či evakuační plán. Další plány musí reagovat na situace, kdy dojde k selhání technických prostředku přerušení dodávky el. energie nebo selhání lidského faktoru (úmyslné nebo nedbalostní narušení IS). (Karel Břoušek, 2021; Vyškov, 2018)

V případě havárie týkající se aktiv IS zodpovídá za její řešení vedoucí OI/KST. Havárii řeší pracovníci OI/KST vlastními silami, v případě havárií hardwaru nebo informačních systémů, k nimž je poskytována smluvní podpora, tak ve spolupráci se smluvními dodavateli. (Vyškov, 2018)

4.7.2 Kryptografie

Kryptografické systémy a techniky jsou používány pro ochranu informací, které jsou považovány za rizikové a pro které ostatní opatření neposkytují odpovídající ochranu. V rámci těchto opatření lze rozlišit kryptování dat k ochraně důvěrnosti chráněných informací, nebo vytvoření bezpečného komunikačního kanálu a digitální podepisování k ochraně autentičnosti a integrity elektronických dokumentů, nebo ověření identity uživatele např. při komunikaci se serverem. (Karel Břoušek, 2021; Vyškov, 2018)

Kryptografie se v případě MěÚ využívá u:

- Aplikace Profibanka, ČS lnternetbanking, ČSOB Internetbanking pro autorizaci platebních příkazů a pro komunikaci s bankou prostřednictvím internetu za využití digitálního certifikátu vydávaného bankou konkrétní osobě.
- Kryptování dat odesílaných a přijímaných od České pošty e-mailem prostřednictvím poštou dodaného kryptovacího softwaru a kryptovacích klíčů.
- Komunikace, např. získávání dat prostřednictvím internetu za využití digitálního certifikátu vydávaného konkrétní osobě.
- Příchozí i odchozí elektronické pošty podepsané elektronickým podpisem.
- IS spravované státem, které se na MěÚ používají k výkonu státní správy. Jde o aplikace ISSDE (odbor dopravy, odbor správní a vnitřních věcí), systém datových schránek či základní registry. (Karel Břoušek, 2021; Vyškov, 2018)

5 NÁVRH PROTOTYPU APLIKACE

Tato část diplomové práce popisuje navržené opatření pro snížení míry rizika stalkerware a dalších hrozeb kybernetické bezpečnosti v podobě prototypu desktopové aplikace, která má za cíl zabezpečit a zároveň školit zaměstnance Městského úřadu ve Vyškově v oblasti této problematiky. Popisuje její strukturu, vzhled a nejdůležitější komponenty pohledem designéra a běžného uživatele. Prototyp aplikace byl vytvořen v programu Figma.

Secura

Obrázek č. 11 představuje vytvořený prototyp, který nese jméno „Secura“. Cílem aplikace je uživatele zabezpečit a chránit před nebezpečným malwarem, zejména před všemi formami stalkerwaru a zároveň uživatele školit a následně jejich znalosti otestovat. Uživateli je vždy představena obecná teorie dané problematiky, spojená s příklady z reálného života, které mohou kdykoliv nastat. Prototyp je navržen tak, aby fungoval jako uživatelské prostředí při přihlašování se do počítačového zařízení. Tudíž se nejedná o software, který by uživatel musel manuálně zapínat.Školení funguje na principu třicetidenních cyklů. Tudíž zaměstnanec musí jednou za 30 dní úspěšně projít školením. Pro pracovníky z oddělení informatiky je aplikace navržená tak, aby mohli otestovat zaměstnance pomocí „falešných“ e-mailů, které se tváří jako reálné e-maily obsahující malware. Po odeslání těchto e-mailů mohou sledovat úspěšnost zaměstnanců pomocí grafů. (vlastní)

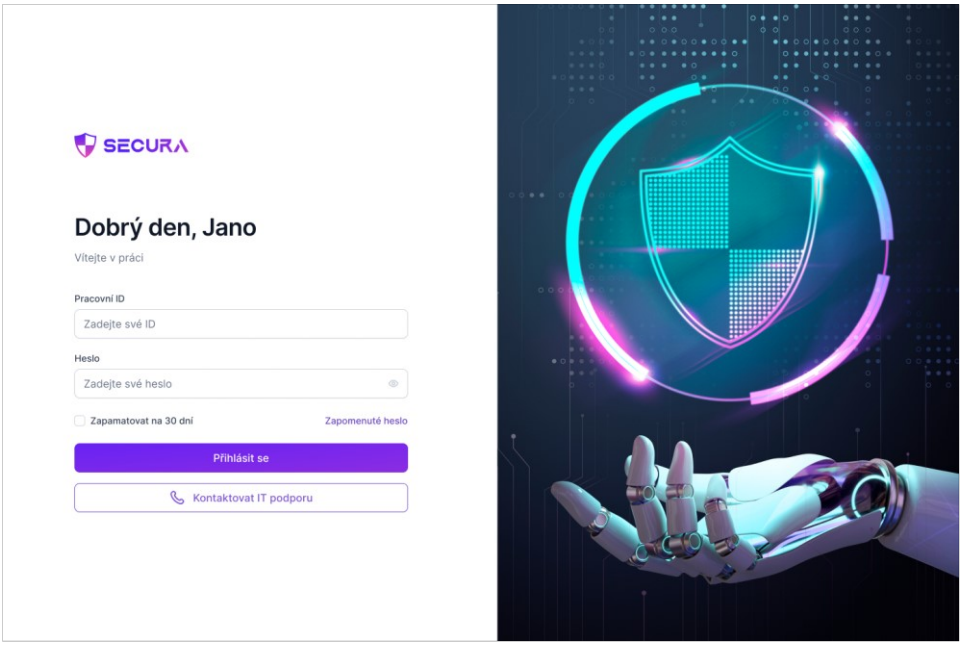
Obrázek 11 – Aplikace Secura (vlastní)

5.1 Uživatelské prostředí pro běžné zaměstnance úřadu

První část se věnuje uživatelskému prostředí, do kterého se budou přihlašovat všichni zaměstnanci úřadu, kromě správců z oddělení informatiky.

5.1.1 Přihlášení uživatele

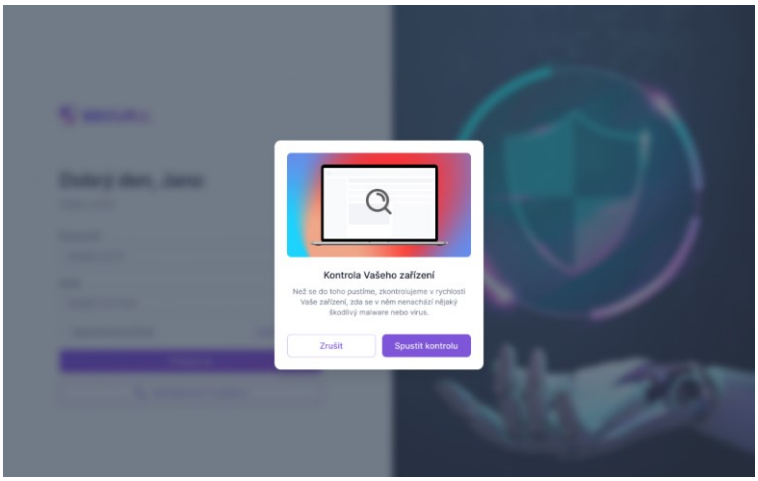
Po spuštění počítače se uživateli zobrazí přihlašovací obrazovka, kterou lze vidět na obrázku č. 12. Do příslušných kolonek zaměstnanec zadá své údaje a přihlásí se. Pokud by si zaměstnanec nevěděl rady, může ihned kontaktovat svého kolegu z oddělení informatiky. Možnost zapamatovat si údaje pouze na 30 dní je z toho důvodu, že zaměstnanec bude na konci tohoto období vyzván ke změně svého hesla.



Obrázek 12 – Přihlašovací obrazovka (vlastní)

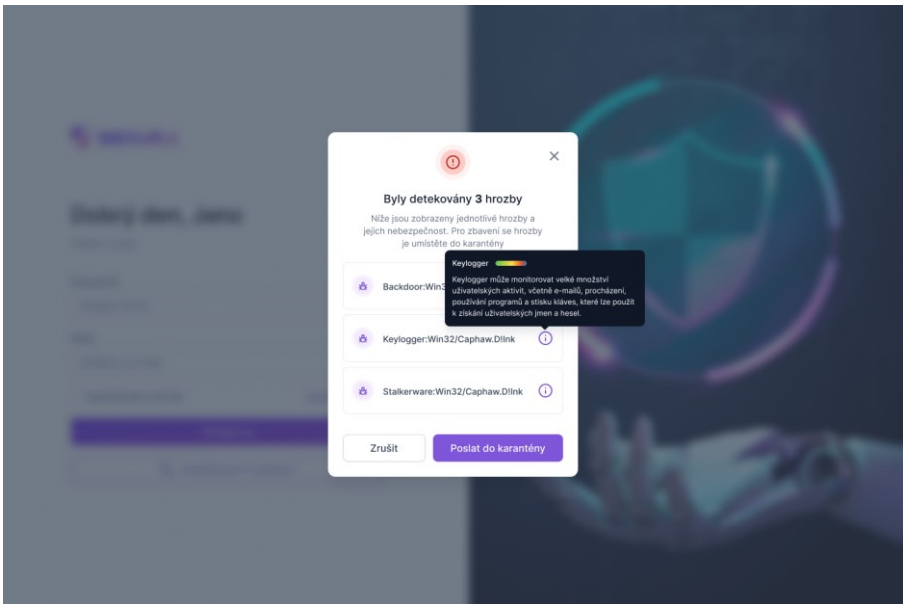
5.1.2 Kontrola počítače

Jak lze vidět na obrázku č. 13, ihned po přihlášení aplikace vyzve zaměstnance ke kontrole svého počítače, zda se v něm nenachází nějaké viry nebo malware.



Obrázek 13 – Kontrola počítače (vlastní)

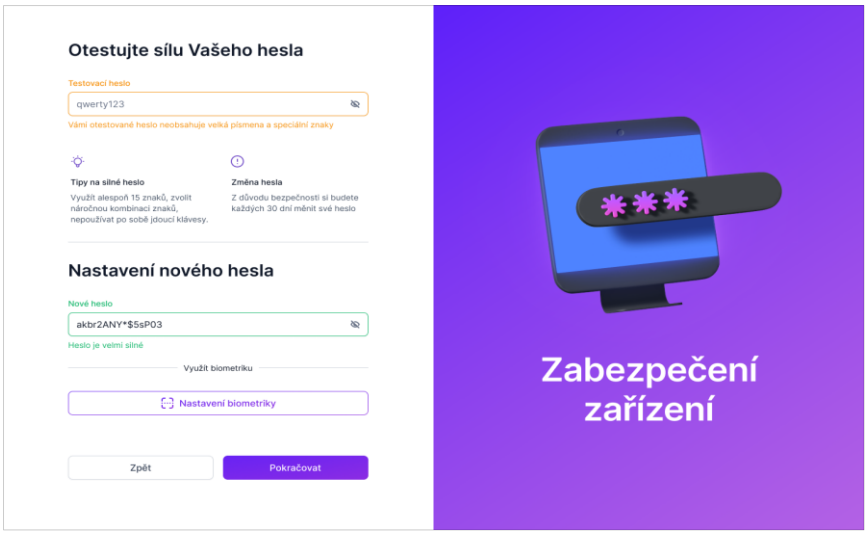
Po proběhlé kontrole aplikace zobrazí zaměstnanci nalezené hrozby. Na obrázku č. 14 lze vidět, že ke každé hrozbě lze zobrazit její detail, který obsahuje základní popis malwaru a je zde umístěn i indikátor nebezpečnosti, jež daná hrozba představuje. Po prozkoumání lze všechny hrozby umístit do karantény.



Obrázek 14 – Detail hrozby (vlastní)

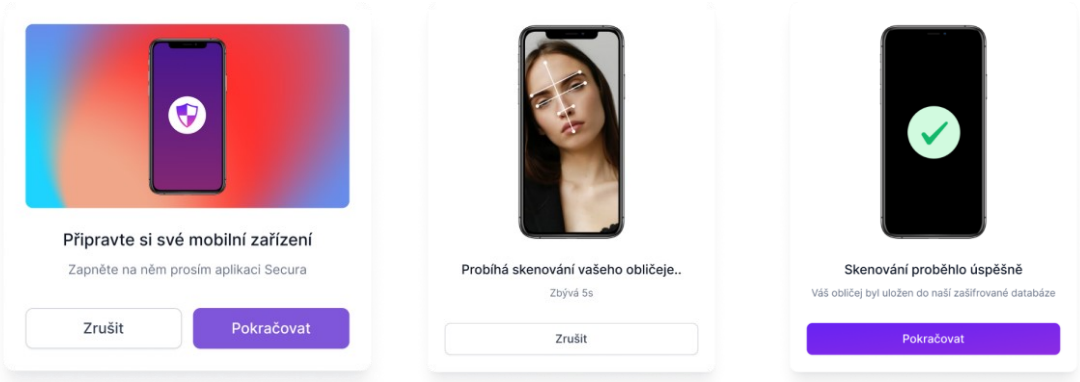
5.1.3 Zabezpečení zařízení

Obrázek č. 15 zobrazuje proces otestování a změny hesla. Zaměstnanec si může otestovat své heslo, zda je považováno za silné či slabé a rovněž si může prohlídnout tipy na vytvoření silného hesla. Poté si nastaví nové heslo, které bude využívat ke svému přihlašování. Je zde i možnost využití biometriky pro zvýšení bezpečnosti jejich počítače.



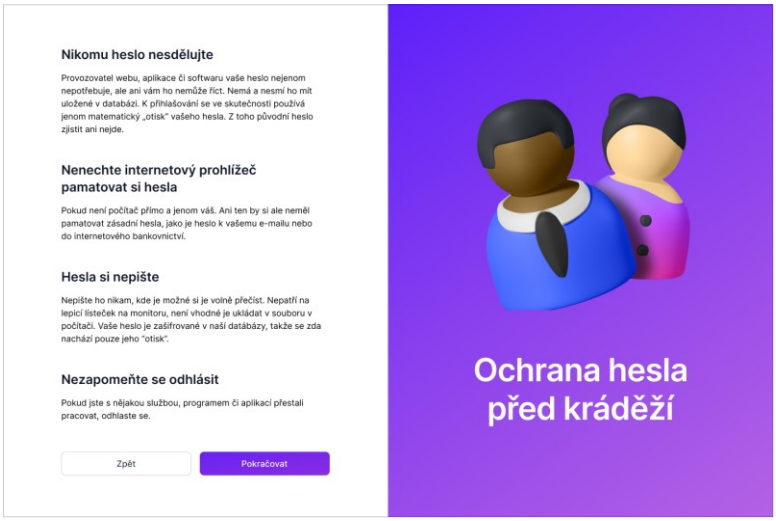
Obrázek 15 – Zabezpečení zařízení (vlastní)

Jak lze vidět na obrázku č. 16, k využití biometriky se využívá mobilní zařízení, kam si zaměstnanec nainstaluje aplikaci Secura. Po otevření se aplikace automaticky propojí s desktopovou aplikací a otevře se přední fotoaparát. Zaměstnanci se na mobilním zařízení zobrazí instrukce, co má udělat, aby došlo k úspěšnému zaměření obličeje. Po zaměření se zobrazí hláška, že se zaměření povedlo, nebo bude muset zopakovat předchozí postup.



Obrázek 16 – Proces nastavení biometriky (vlastní)

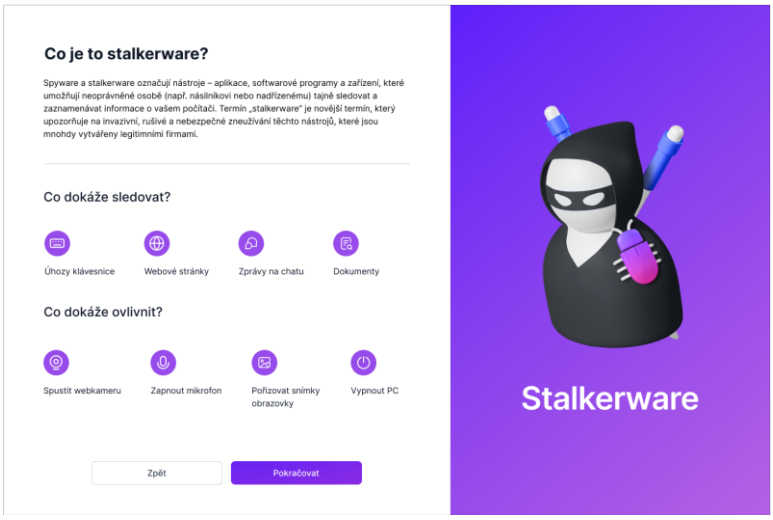
Na konci tohoto procesu jsou ještě připomenuty na obrázku č. 17 základní poučky o tom, jak své heslo chránit před krádeží.



Obrázek 17 – Ochrana hesla před krádeží (vlastní)

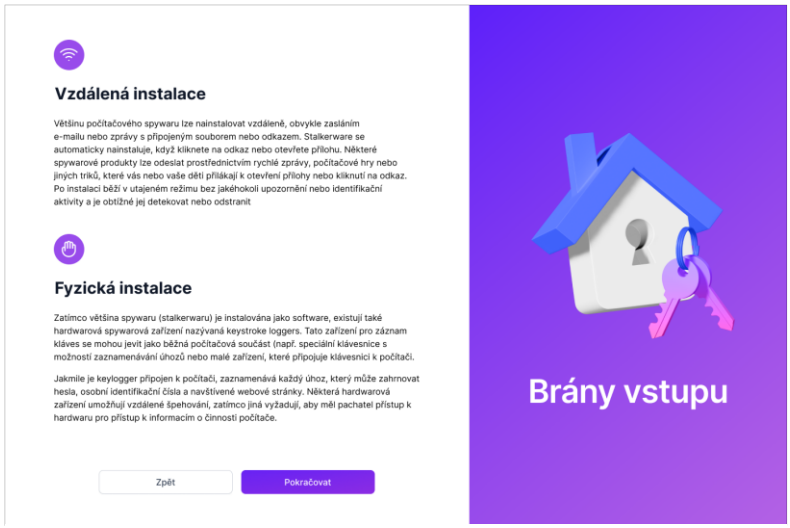
5.1.4 Stalkerware

Tato sekce se zaměřuje na seznámení zaměstnance s problematikou hrozby stalkerware. Hned na úvodní obrazovce, kterou představuje obrázek č. 18, je hrozba stručně popsána a jsou zde uvedeny i oblasti, které může stalkerware sledovat, a dokonce i ovlivňovat.



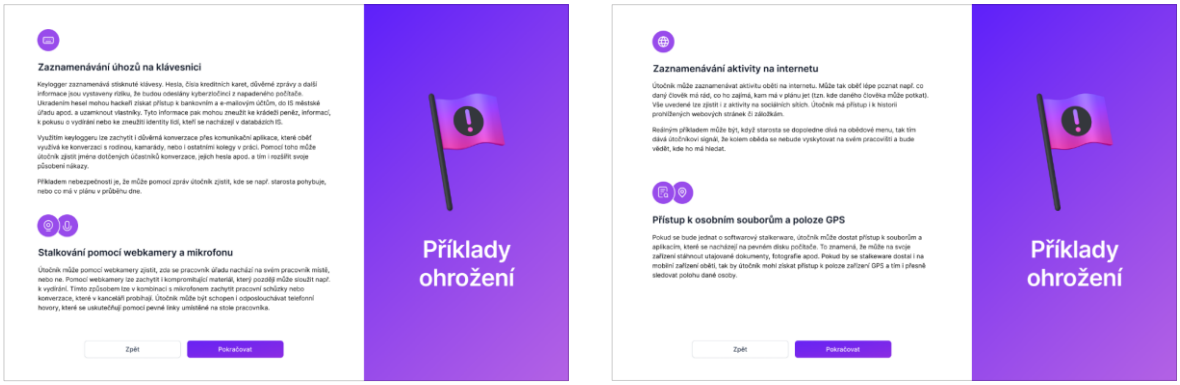
Obrázek 18 – Obecný popis hrozby stalkerware (vlastní)

Obrázek č. 19 blíže specifikuje brány vstupu stalkerwaru do počítačového zařízení. Zde je nutné zaměstnancům vysvětlit, že se nemusí jednat pouze o softwarový stalkerware, ale že ke stalkování oběti lze využít i různé typy hardwarových zařízení.



Obrázek 19 – Brány vstupu stalkerwaru (vlastní)

Závěrečná část této sekce na obrázku č. 20 přibližuje reálnou nebezpečnost stalkerwaru na konkrétních případech zaměstnance úřadu. Tato část je rozdělena podle oblastí, které stalkerware sleduje, tudíž se jedná o zaznamenávání úhozů na klávesnici, stalkování webkamery a mikrofonu, zaznamenávání aktivity na internetu a přístup k osobním souborům a poloze GPS.

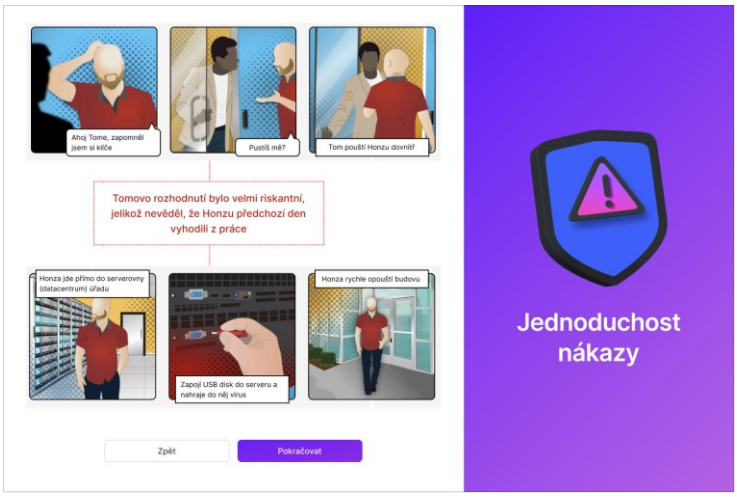


Obrázek 20 – Příklady ohrožení hrozbou stalkerware (vlastní)

5.1.5 Jednoduchost nákazy

Tato sekce je věnována ilustracím a poučkám, které mají upozornit zaměstnance úřadu na to, že si musí dávat pozor, když je cizí osoba požádá o přístup do budovy, nebo kamkoliv, kde je oprávněný přístup pouze určitým osobám. Je důležité školit zaměstnance i v této oblasti, jelikož stalkerware, jak již bylo uvedeno, lze nainstalovat i prostřednictvím hardwarových zařízení.

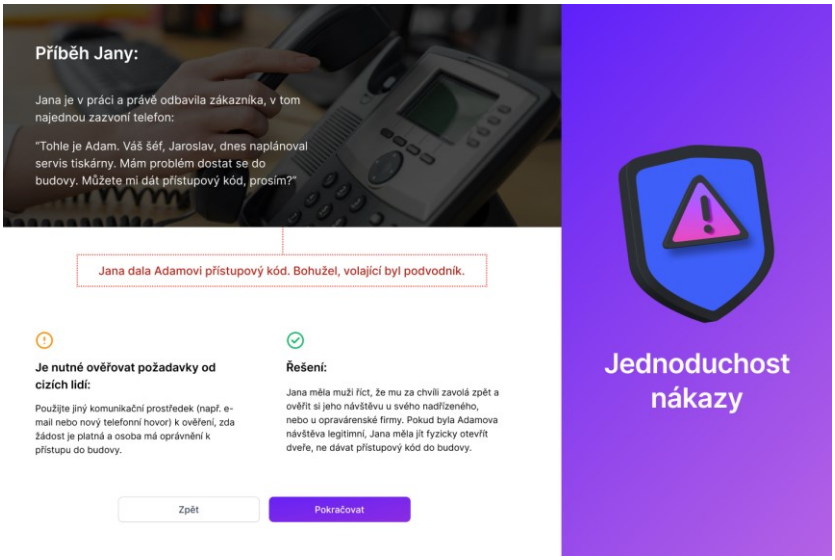
První příběh na obrázku č. 21 nastiňuje situaci, kdy se bývalý pracovník úřadu Jan (červené tričko) domáhá přístupu do budovy s výmluvou, že si uvnitř zapomněl klíče. Důvěřivý kolega Tomáš (béžový kabát) ho pustí a Jan se nekontrolovaně odebere do serverové místnosti, kde na server nahraje vir a poté opustí budovu. Jan byl den předtím vyhozen z práce, tudíž si měl Tomáš nejprve zjistit nebo povšimnout, proč se Jan tentýž den v práci nevyskytoval.



Obrázek 21 – Nákaza serveru (vlastní)

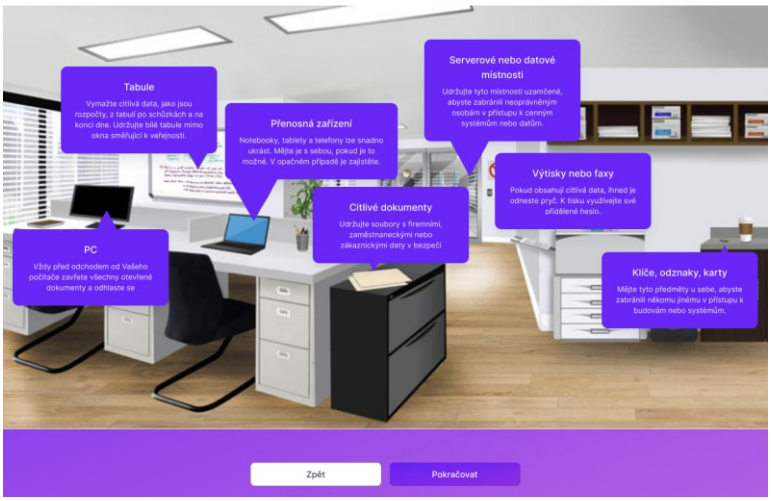
Druhý příběh na obrázku č. 22 nastiňuje situaci, kdy zaměstnankyni Janě zazvoní v kanceláři telefon, ve kterém ji osloví člověk s tím, že si jej objednal její nadřízený Jaroslav na servis tiskárny. Chce od Jany přístupový kód, aby měl možnost se dostat do budovy. Jana tento přístupový kód muži ze servisu řekne. Bohužel, volající byl podvodník, který volal jen za tím účelem, aby se dostal do budovy.

Dále se na této obrazovce nachází upozornění, které pracovníci musí brát v potaz a také nástin řešení, jak Jana měla v této situaci postupovat.



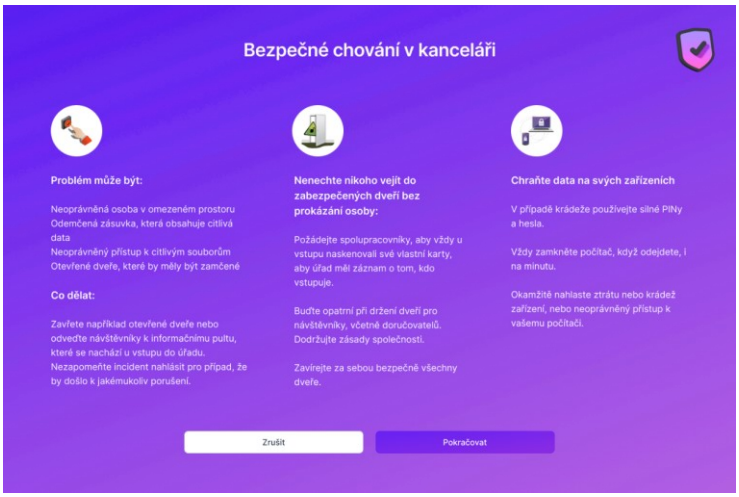
Obrázek 22 – Falešný volající (vlastní)

V další části této sekce lze na obrázku č. 23 vidět ilustrace serverové místnosti a kanceláře s běžnými zařízeními a pomůckami, jako je tabule, stolní počítač, notebook, klíče, přístupové karty apod. Ke každé položce, která je náchylná ke zneužití cizí osobou, je popis, jak s ní nakládat.



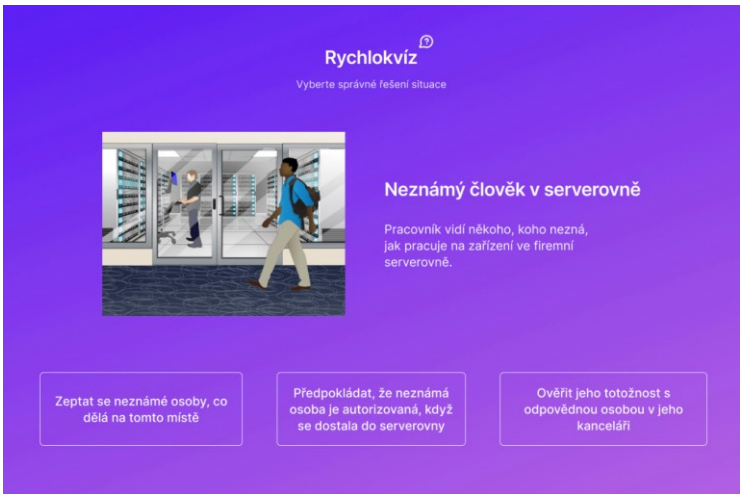
Obrázek 23 – Bezpečnost v zaměstnaneckých prostorech (vlastní)

Předposlední část sekce je věnována obecným poučkám, jak by se měl zaměstnanec chovat ve své kanceláři, aby vše zůstalo ochráněné proti zneužití či krádeži. Na obrázku č. 24 lze vidět, že se jedná např. o kontrolování přístupů cizích osob do zabezpečených prostorů nebo o ochranu dat na svých zařízeních.



Obrázek 24 – Bezpečnostní pokyny (vlastní)

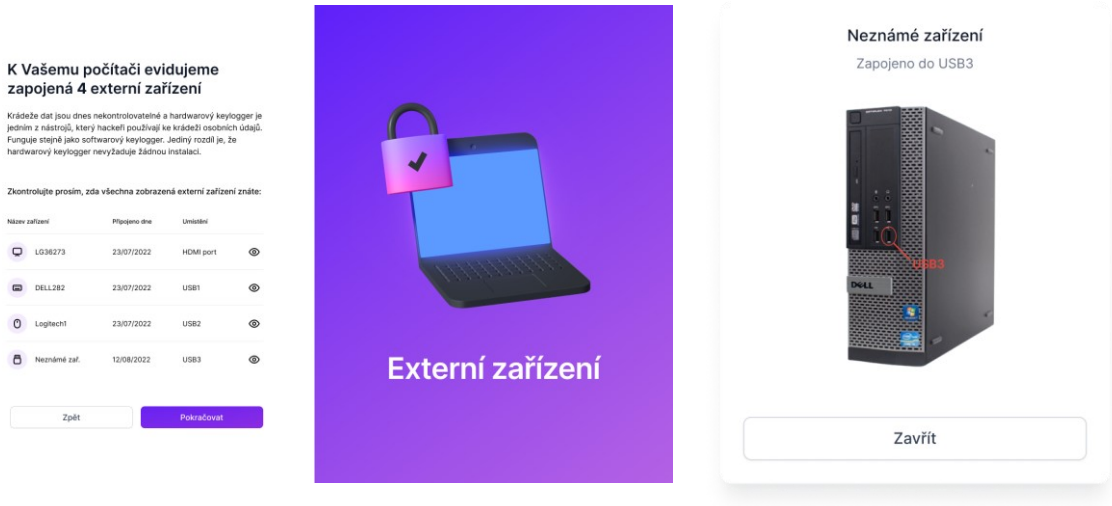
Na závěr čeká zaměstnance zodpovědět kontrolní otázky, které prověří jejich znalosti v oblasti dodržování fyzické bezpečnosti v budově úřadu, aby se eliminovalo riziko nákazy malwarem a zejména stalkerwarem. Na obrázku č. 25 lze vidět příklad „Rychlokvízu“, jehož obsah tvoří otázky z této oblasti. Zaměstnanec musí vždy vybrat jednu správnou odpověď ze tří nabízených. Rychlokvíz by se vždy skládal z pěti otázek.



Obrázek 25 – Rychlokvíz na fyzickou bezpečnost (vlastní)

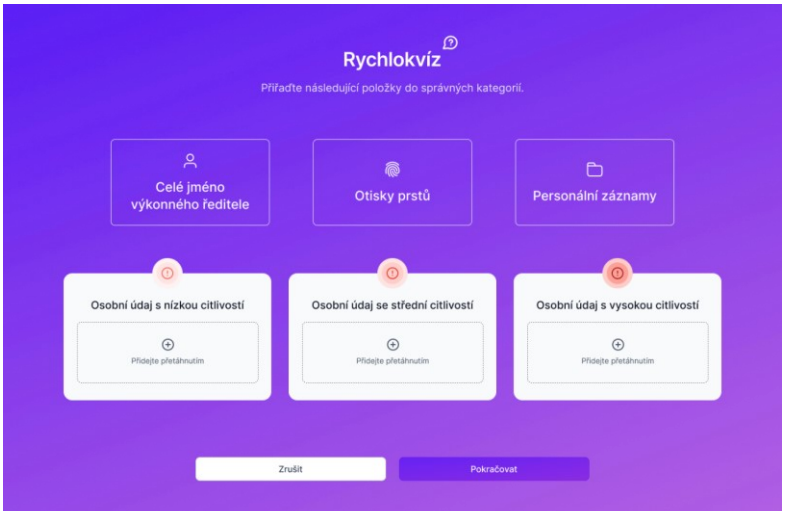
5.1.6 Kontrola externích zařízení

Tato sekce má za cíl naučit zaměstnance, aby před každým zapnutím počítače zkontrolovali všechna externí zařízení, která jsou do něho zapojena. Na obrázku č. 26 lze vidět, že u počítače jsou evidována 4 zapojená externí zařízení a jejich výpis v tabulce. Pak následuje krátké zopakování, co je to hardwarový keylogger a proč je nebezpečný. U konkrétního příkladu je do počítače zapojen monitor, klávesnice, myš a neznámé zařízení. U každého zařízení si lze kliknout na detail, který ukáže přesné místo, kde je zařízení zapojeno, aby zaměstnanec mohl provést jeho kontrolu.



Obrázek 26 – Externí zařízení

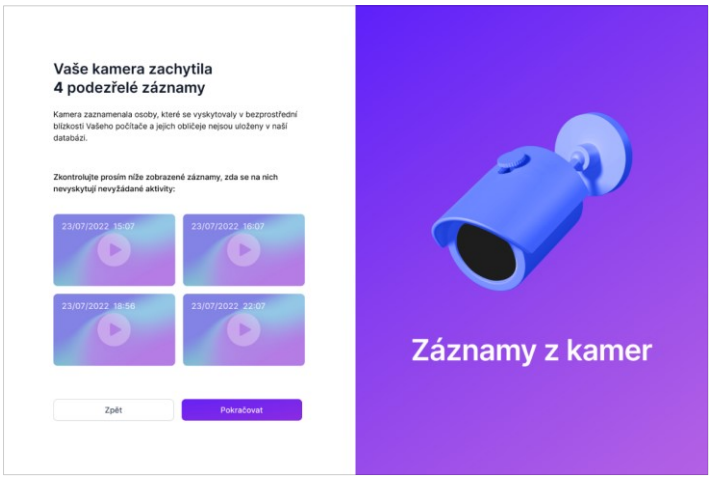
Po kontrole externích zařízení následuje Rychlokvíz, který má za cíl otestovat zaměstnance v oblasti dělení informací podle jejich důležitosti. Na obrázku č. 27 jsou zobrazeny tři druhy osobních údajů a zaměstnanec má za úkol je přiřadit do jedné ze tří kolonek.



Obrázek 27 – Rychlokvíz na osobní údaje (vlastní)

5.1.7 Záznamy z kamer

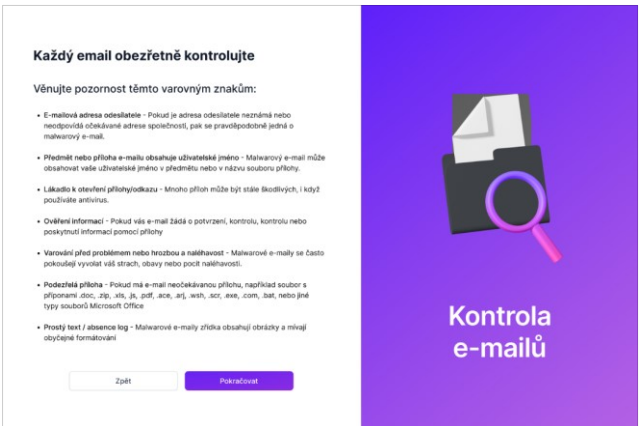
Další funkcionalitou aplikace Secura je neustálé zaznamenávání pohybu osob v kanceláři pracovníka. Pokud se bude v těchto prostorách nacházet neoprávněná osoba, záznam bude uložen a pracovník si ho bude moci zpětně pustit. Jednalo by se o vyspělé typy kamer, (které by disponovaly funkcionalitou na rozpoznávání obličejů, tudíž by se eliminovaly záznamy, na kterých by byl sám pracovník, který v kanceláři pracuje.



Obrázek 28 – Záznamy z kamer

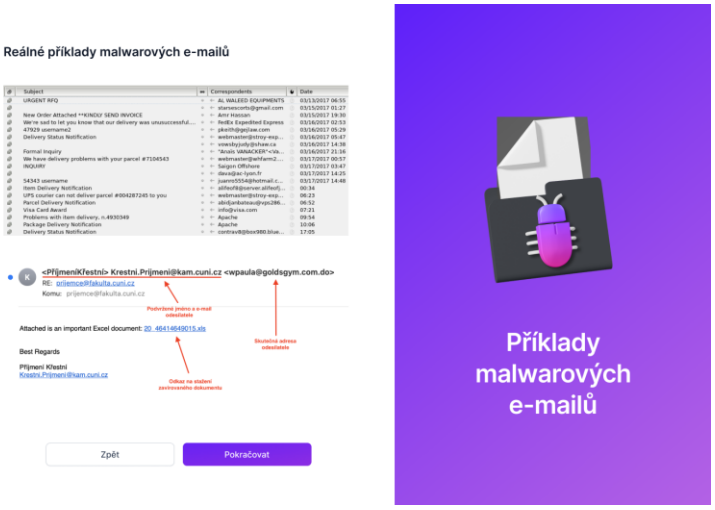
5.1.8 Kontrola e-mailů

Jeden z nejčastějších kanálů, kterými se viry a malware přenáší, je právě e-mailová komunikace. Proto je v této sekci věnována značná pozornost tomu, aby zaměstnanci dokázali úspěšně rozpoznat e-mail zaslaný legitimní firmou nebo člověkem od podvodného e-mailu obsahujícího škodlivý malware ve všech jeho formách. Úvod do sekce lze vidět na obrázku č. 29, který představuje soubor obecných pouček, jakým způsobem lze rozpoznat e-mail představující hrozbu.



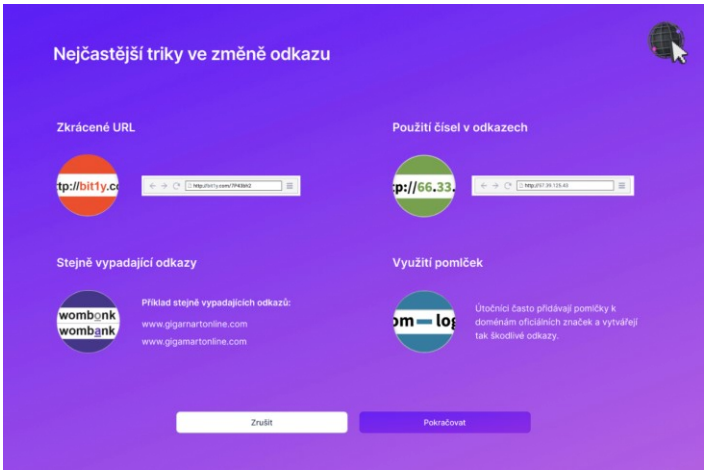
Obrázek 29 – Varovné znaky podvodných e-mailů (vlastní)

Na obrázku č. 30 jsou představeny reálné e-maily, které jsou odesílány za účelem poškození příjemce. V horní sekci je výčet e-mailů, které jsou považovány za škodlivé s obsahem malwaru a splňující parametry, které byly popsány na obrázku č. 29. Ve spodní sekci je rozbor samostatného e-mailu, kde jsou vyzdvihnuty nejdůležitější části, které vypovídají o tom, že se jedná o e-mail s obsahem malwaru.



Obrázek 30 - Příklady malwarových e-mailů (vlastní)

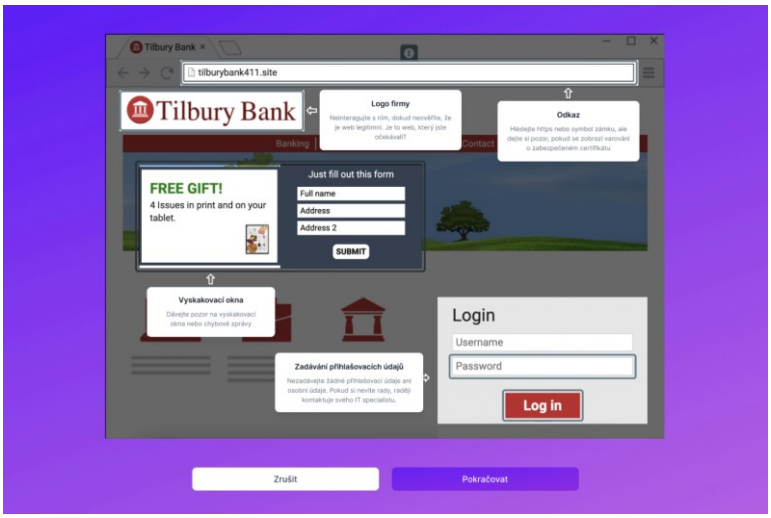
Další sekce je věnována odkazům, které bývají ve většině případů obsahem e-mailové zprávy. Útočníci často mění odkazy tak, aby působily věrohodně a příjemci na ně kliknuli. Na obrázku č. 31 jsou zobrazeny čtyři nejčastější metody ve změně odkazu.



Obrázek 31 - Změna odkazu (vlastní)

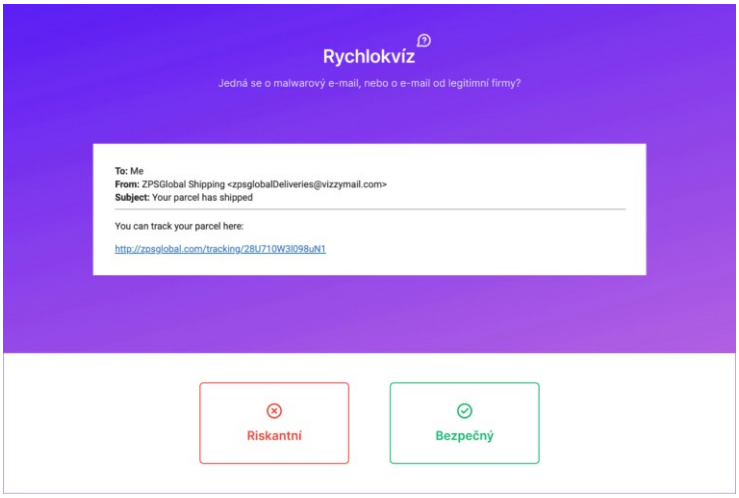
Předposlední část přibližuje konkrétní webovou stránku, která je rozebrána na jednotlivé komponenty s krátkým popisem, na co si dávat pozor, pokud s určitým prvkem

interagujeme. Na obrázku č. 32 je vyobrazena falešná webová stránka „Tilbury Bank“, která obsahuje celkem čtyři prvky, které mohou být potenciálně nebezpečné při jejich interakci ze strany zaměstnance.



Obrázek 32 - Rozbor webové stránky (vlastní)

Poslední částí je opět Rychlokvíz, který má za cíl otestovat zaměstnance na to, jestli jsou schopni rozpoznat malwarový e-mail od legitimního.

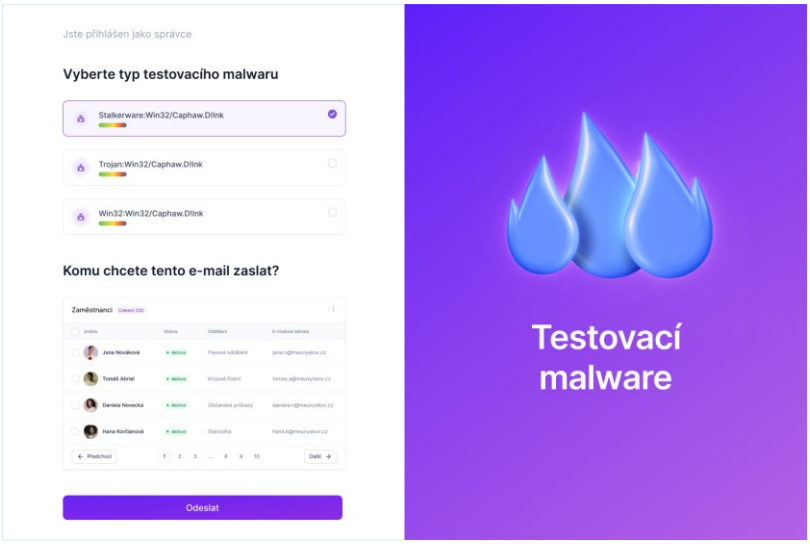


Obrázek 33 - Rychlokvíz na rozpoznávání e-mailů (vlastní)

5.2 Testovací platforma pro správce oddělení informatiky

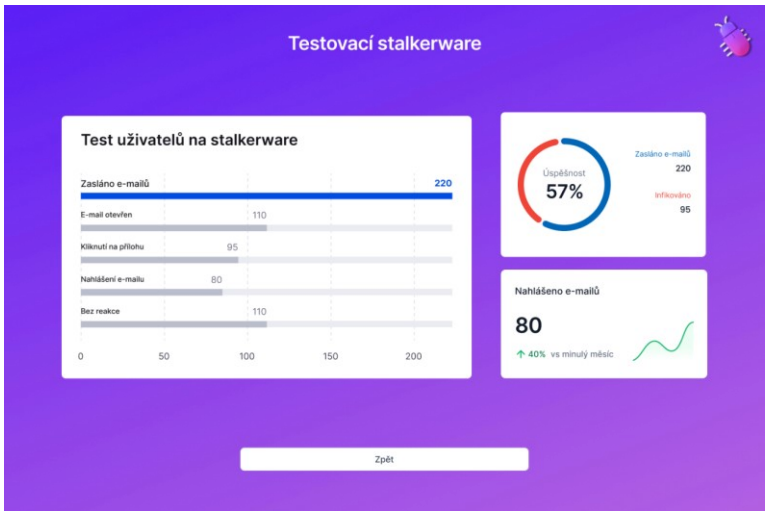
Pro správce z oddělení informatiky úřadu byla vytvořena platforma, která umožňuje rozesílat ostatním zaměstnancům testovací e-maily, které se tváří jako malwarové. Je zde možnost si vybrat, jaký typ malwaru si přeje správce odeslat a také tabulka se všemi

zaměstnanci úřadu, která obsahuje jejich jména, jestli jsou v dané chvíli online na svém zařízení a také na kterém oddělení pracují. Výběr testovacího malwaru a seznam všech zaměstnanců jsou vyobrazeny na obrázku č. 34.



Obrázek 34 - Konfigurace testovacího malwaru (vlastní)

Po odeslání testovacího e-mailu se správce dostane do uživatelského prostředí zvaného „dashboard“, kde může sledovat, kolik e-mailů bylo zasláno a jednotlivé interakce od dotčených osob. Na obrázku č. 35 si lze povšimnout, že správce má detailní pohled na to, kolik zaměstnanců e-mail otevřelo, kliknulo na přílohu, nahlásilo daný e-mail nebo s e-mailem nijak neinteragovali. V pravé části je vyzdvihnuto, jaká je úspěšnost zaměstnanců a kolik jich daný e-mail nahlásilo správci.



Obrázek 35 - Detailní statistika testovacího e-mailu (vlastní)

ZÁVĚR

Pokud jde o kybernetické útoky, neexistují v této oblasti žádné záruky. Jediná věc, kterou může jakýkoliv subjekt udělat, je zmírnit riziko a naplánovat obnovu. Jedna z oblastí, která je při vytváření strategie kybernetické bezpečnosti často přehlížena a opomíjena, je školení o kybernetické bezpečnosti zaměstnanců. Je prokázáno, že lidská chybovost je největší hrozbou pro kybernetickou bezpečnost, což má za následek až 95 % úniků dat. Není pochyb o tom, že vzdělávání zaměstnanců je velmi důležitou součástí silné strategie kybernetické bezpečnosti.

Odborně vytvořený školicí program může vštípit zaměstnancům znalosti a vybudovat v nich sebejistotu k tomu, aby byli schopni samostatně reagovat a rozpoznávat bezpečnostní hrozby. Pokud školení probíhá v pravidelných cyklech, posiluje to význam vzdělávání a rovněž buduje kulturu o povědomí v oblasti kybernetické bezpečnosti. Čím více toho budou zaměstnanci vědět, tím lépe mohou sloužit jako obranný mechanismus.

Teoretická část je rešeršního charakteru, kde v úvodu byly popsány nejdůležitější právní předpisy a normy z oblasti kybernetické bezpečnosti, dále také nástin kybernetické bezpečnosti a její terminologie, kyberprostoru a organizací věnující se kybernetické bezpečnosti v ČR. Další kapitola je věnována subjektům ochrany obyvatelstva v ČR, jejich dělení a funkcím, které zastávají. Poslední kapitola se věnuje malwaru, jeho dělení, zranitelnosti a obraně vůči němu, analýze a v neposlední řadě stalkerwaru, kde byla popsána jeho nebezpečnost, světové statistiky jeho výskytu a nakažlivosti a indikátorům nákazy společně s obrannými praktikami.

Praktická část byla zaměřena na analýzu interních dokumentů kybernetické bezpečnosti Městského úřadu ve Vyškově, která se dotýkala oblastí fyzické bezpečnosti, bezpečnosti provozu informačního systému, řízení přístupu, vývoji a údržbě informačního systému, informační bezpečnosti a správě incidentů, řízení kontinuity podnikání a kryptografii. Důležitou část tvořil návrh desktopové aplikace, která má za cíl posílit zabezpečení a vzdělanost všech zaměstnanců pracujících na Městském úřadě ve Vyškově v oblasti kyberbezpečnosti se zaměřením na hrozbu stalkerware. Školení na bázi třicetidenních cyklů pomáhá zajistit, aby všichni zaměstnanci disponovali znalostmi a dovednostmi, které potřebují, aby mohli efektivně a bezpečně vykonávat svou práci. Školení se skládá ze čtyř částí, kde v jednotlivých částech má zaměstnanec možnost posílit zabezpečení svého zařízení, dále je zde teoretická část, představení praktických příkladů dané problematiky a

na závěr každé sekce test. Pro správce oddělení informatiky bylo vytvořeno odlišné uživatelské prostředí, z něhož mají možnost rozeslat ostatním zaměstnancům testovací e-mail, který obsahuje malware. Tím dostanou možnost zjistit míru úspěšnosti u zaměstnanců, jakým způsobem si vedli během školení a zda dokážou zúročit svoje znalosti i v praxi.

Na základě výše uvedeného považuji cíle diplomové práce za splněné.

SEZNAM POUŽITÉ LITERATURY

ADAMEC, Vilém, David ŘEHÁK a Lenka ČERNÁ, 2012. *Základy organizace a řízení bezpečnosti v České republice. Sdružení požárního a bezpečnostního inženýrství*. ISBN 978-80-7385-123-1.

AGHAJANI, Jafar, Parissa FARNIA a Ali Akbar VELAYATI, 2017. *Impact of Geographical Information System on Public Health Sciences* [online]. [cit. 2022-07-19]. Dostupné z: https://bmbtrj.org/temp/BiomedBiotechnolResJ1294-3242861_090028.pdf

Avast, ©2022. *Malware*. Avast [online]. [cit. 2022-06-17]. Dostupné z: https://www.avast.com/cs-cz/c-malware

BARKER, Dylan, 2021. *Malware Analysis Techniques: Tricks for the triage of adversarial software*. Packt Publishing. ISBN 978-1-83921-227-7.

CLARK, Casey, 2020. *Trojan horse (computing)*. TechTarget [online]. [cit. 2022-06-16]. Dostupné z: https://www.techtarget.com/searchsecurity/definition/Trojan-horse

Comodo Cybersecurity, 2015. *How Antivirus Works?*. Comodo Cybersecurity [online]. [cit. 2022-06-17]. Dostupné z: https://antivirus.comodo.com/how-antivirus-software-works.php

CREUTZBURG, Reiner, 2016. *Handbook of Malware 2016* [online]. [cit. 2022-06-16]. Dostupné z: doi:10.13140/RG.2.1.5039.5122

ČESKO, 2000. *Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů. Krizový zákon*. In: Sbírka zákonů ČR.

ČESKO, 2000. *Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů*. In: Sbírka zákonů ČR.

ČESKO, 2005. *Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti: Zákon o ochraně utajovaných informací*. In: Sbírka zákonů ČR.

ČESKO, 2018. *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: Sbírka zákonů ČR.

European Commission, 2021. *The Cybersecurity Strategy* [online].[cit. 2022-02-10]. Dostupné z: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

FRUHLINGER, Josh, 2022. *Keyloggers explained: How attackers record computer inputs*. CSO [online]. [cit. 2022-07-01]. Dostupné z: https://www.csoonline.com/article/3326304/keyloggers-explained-how-attackers-record-computer-inputs.html

GISMentors, ©2022. *QGIS: Nejrozšířenější Open Source desktopový GIS*. GISMentors [online]. [cit. 2022-07-19]. Dostupné z: https://gismentors.cz/skoleni/qgis/

GREGERSEN, Erik, 2013. *Computer virus*. Britannica [online]. [cit. 2022-06-16]. Dostupné z: https://www.britannica.com/technology/computer-virus

GŘ HZS ČR, 2015. *Ochrana obyvatelstva a krizové řízení: skripta* [online]. [cit. 2022-06-23]. ISBN 978-80-86466-62-0.

GUPTA, Deepak, 2022. *What is stalkerware and how to remove it from your mobile or PC*. TechUnwrapped [online]. [cit. 2022-07-01]. Dostupné z: https://techunwrapped.com/what-is-stalkerware-and-how-to-remove-it-from-your-mobile-or-pc/

HNS, 2015. *Evasive malware goes mainstream*. Help Net Security [online]. [cit. 2022-06-17]. Dostupné z: https://www.helpnetsecurity.com/2015/04/22/evasive-malware-goes-mainstream/

HROMADA, Martin et al., 2015. *Kybernetická bezpečnost: teorie a praxe*. Praha: Powerprint. ISBN 978-80-87994-72-6.

HRŮZA, Petr, 2012. *Kybernetická bezpečnost*. Brno: Univerzita obrany. ISBN 978-80-7231-914-5.

HZS ČR, 2014. *Ochrana utajovaných informací*. Hasičský záchranný sbor České republiky [online]. [cit. 2022-06-27]. Dostupné z: http://www.hzscr.cz/soubor/ochrana-utajovanych-informaci-pdf.aspx

HZS ČR, 2016. *Přes nový informační a komunikační systém IZS již prošlo 100 000 000 datových vět*. Hasičský záchranný sbor České republiky [online]. [cit. 2022-06-27]. Dostupné z: https://www.hzscr.cz/clanek/informacni-servis-zpravodajstvi-2016-cervenec-pres-novy-informacni-a-komunikacni-system-izs-jiz-proslo-100-000-000-datovych-vet.aspx

HZS ČR, 2019. *Narušení bezpečnosti informací kritické informační infrastruktury*. Hasičský záchranný sbor České republiky [online]. [cit. 2022-06-27]. Dostupné z: https://www.hzscr.cz/soubor/635-priloha-c4-pdf

Imaginovation, 2018. *10 Tips for Defending Your Business Against Malware Attacks*. Medium [online]. [cit. 2022-06-17]. Dostupné z: https://medium.com/@Imaginovation/10-tips-for-defending-your-business-against-malware-attacks-db70ef22cc9c

InSmart, 2022. *Trojské koně útočí na česká PC: Jsou nejrozšířenějším typem malwaru v ČR*. InSmart [online]. [cit. 2022-07-14]. Dostupné z: https://insmart.cz/nejrozsirenejsim-typem-malwaru-v-cesku-jsou-trojske-kone-2022/

ISO/IEC 27000, 2018. *ISO27K information security* [online]. [cit. 2022-02-10]. Dostupné z: https://www.iso27001security.com/html/27000.html

JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR, 2012. *Výkladový slovník kybernetické bezpečnosti: první oficiální verze slovníku kybernetické bezpečnosti*. Praha: Policejní akademie České republiky, 2012. ISBN 978-80-7251-377-2.

JOHNSON, Thomas A., 2015. *Cybersecurity: protecting critical infrastructures from cyber attack and cyber warfare*. Boca Raton: CRC Press/Taylor & Francis Group. ISBN 9781482239225.

Kaspersky, ©2022. *Vulnerability Exploits & Malware Implementation Techniques*. Kaspersky [online]. [cit. 2022-06-17]. Dostupné z: https://www.kaspersky.com/resource-center/threats/malware-implementation-techniques

Kaspersky, 2020. *What is Cyber Security?*. Kaspersky [online]. [cit. 2022-05-18]. Dostupné z: https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

Kaspersky, 2022. *The State of Stalkerware in 2021*. Kaspersky [online]. [cit. 2022-07-01]. Dostupné z: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2022/04/12075509/EN_The-State-of-Stalkerware-2021.pdf

KHOO, Cynthia, Kate ROBERTSON a Ronald DEIBERT, 2019. *INSTALLING FEAR: A Canadian Legal and Policy Analysis of Using, Developing, and Selling Smartphone Spyware and Stalkerware Applications* [online]. [cit. 2022-06-27]. Dostupné z: https://www.citizenlab.ca/docs/stalkerware-legal.pdf

KODAD, Jaroslav, 2016. *Analýza IS pro operační řízení policie ČR a návrh na jeho zlepšení* [online]. [cit. 2022-06-27]. Dostupné z: https://dspace.vsb.cz/bitstream/handle/10084/115173/KOD0015_HGF_B2102_6209R013_2016.pdf?sequence=1&isAllowed=y

KOLOUCH, Jan a Petr VOLEVECKÝ, 2013. *Trestněprávní ochrana před kybernetickou kriminalitou: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Policejní akademie České republiky v Praze. ISBN 978-80-7251-402- 1.

KOLOUCH, Jan et al., 2019. *CyberSecurity* [online]. [cit. 2022-07-14]. ISBN 978-80-88168-34-8. Dostupné z: https://knihy.nic.cz/files/edice/cybersecurity.pdf

KOPECKÝ, Kamil, 2010. *Kybergrooming – nebezpečí kyberprostoru*. Olomouc: Net University Ltd. ISBN 978-80-254-7573-7.

KYBEZ, ©2021. *Základní pojmy*. KYBEZ [online]. [cit. 2022-05-18]. Dostupné z: https://www.kybez.cz/zakladni-pojmy/

LAPIENYTĖ, Jurgita, 2021. *Is someone tracking you? Signs that you may have been targeted by stalkerware*. Cybernews [online]. [cit. 2022-07-01]. Dostupné z: https://cybernews.com/editorial/is-someone-tracking-you-signs-that-you-may-have-been-targeted-by-stalkerware/

LUKÁŠ, Luděk, 2015. *Bezpečnostní technologie, systémy a management*. Zlín: Radim Bačuvčík - VeRBuM. ISBN 978-80-87500-57-6.

MACEJ, Grace, 2020. *How to spot the signs of stalkerware on your phone*. Avast [online]. [cit. 2022-07-01]. Dostupné z: https://blog.avast.com/mobile-stalkerware-signs-avast

Město Vyškov, 2020. *O Vyškově* [online]. [cit. 2022-07-03]. Dostupné z: https://www.vyskov-mesto.cz/o-vyskove/ms-135616/p1=135616

MINDANAO, Kharmela, 2020. *Best Defenses Against Malware*. Intelligent Technical Solutions [online]. [cit. 2022-06-17]. Dostupné z: https://www.itsasap.com/blog/defending-against-malware

Monnappa K A, 2018. *Learning Malware Analysis*. Birmingham: Packt Publishing. ISBN 978-1-78839-250-1.

NCSC, 2020. *Mitigating malware and ransomware attacks*. National Cyber Security Center [online]. [cit. 2022-06-17]. Dostupné z: https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks#actionstotake

NGUYEN, Thanh Thi a Vijay Janapa REDDI, 2021. *Deep Reinforcement Learning for Cyber Security* [online]. IEEE [cit. 2022-02-10]. Dostupné z: https://ieeexplore.ieee.org/document/9596578.

NIELD, David, 2020. *How to Check Your Devices for Stalkerware*. WIRED [online]. [cit. 2022-07-01]. Dostupné z: https://www.wired.com/story/how-to-check-for-stalkerware/

NÚKIB, ©2022. *O NÚKIB* [online]. Národní úřad pro kybernetickou a informační bezpečnost [cit. 2020-11-08]. Dostupné z: https://www.nukib.cz/cs/o-nukib/

NÚKIB, 2020. *Národní strategie kybernetické bezpečnosti České republiky na období let 2021–2025*. In: Strategie/Akční plán [online]. Národní úřad pro kybernetickou a informační bezpečnost [cit. 2022-02-10]. Dostupné z: https://www.nukib.cz/cs/kyberneticka-bezpecnost/strategie-akcni-plan/

POŽÁR, Josef, 2005. *Informační bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk. Vysokoškolské učebnice (Vydavatelství a nakladatelství Aleš Čeněk). ISBN 80-86898-38-5.

Profi Press, ©2022. *Jak zvolit vhodný informační systém*. [online]. [cit. 2022-06-27]. Dostupné z: https://moderniobec.cz/jak-zvolit-vhodny-informacni-system/

Rozhovor s Bc. Karlem Brouškem, Městský úřad ve Vyškově, odbor správní a vnitřních věcí, Vyškov 21.05.2021.

ScienceDirect, 2019. *The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation* [online]. [cit. 2022-02-10]. Dostupné z: doi:https://doi.org/10.1016/j.clsr.2019.06.007

SINGER, P. W. a Allan FRIEDMAN, 2013. *Cybersecurity: What everyone Needs to Know*. Oxford University Press, 2013. ISBN 0199918112

SMEJKAL, Vladimír a Karel RAIS, 2013. *Řízení rizik ve firmách a jiných organizacích*. Grada. ISBN 978-80-247-4644-9.

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

SOLMS, Rossouw a Johan NIEKERK. *From information security to cyber security*. Computers & Security [online]. [cit. 2022-05-16]. Dostupné z: doi:https://doi.org/10.1016/j.cose.2013.04.004

Spiegel, 2014. *Documents Reveal Top NSA Hacking Unit*. Spiegel international [online]. [cit. 2022-06-16]. Dostupné z: https://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html

SSD, 2018. *How Do I Protect Myself Against Malware?*. Surveillance Self-Defense [online]. [cit. 2022-06-17]. Dostupné z: https://ssd.eff.org/en/module/how-do-i-protect-myself-against-malware

SSHR ČR, ©2022. *Informační web IS Argis*. Argis [online]. [cit. 2022-07-19]. Dostupné z: https://www.argis.cz/

ŠMAHAJ, Jan, 2014. *Kyberšikana jako společenský problém: Cyberbullying as a social problem*. Olomouc: Univerzita Palackého v Olomouci. ISBN 978-80-244- 4227-3.

Šmejkalová, Marie, 2020. *Kybernetická bezpečnost*. AMO [online]. [cit. 2022-02-10]. Dostupné z: https://www.studentsummit.cz/wp-content/uploads/2020/11/Kybernetická-bezpečnost.pdf

ŠTEFANKO, Lukáš, 2021. *ANDROID STALKERWARE VULNERABILITIES*. Eset [online]. [cit. 2022-07-01]. Dostupné z: https://www.eset.com/fileadmin/ESET/CZ/Blog/2021/ESET_Android_stalkerware_vulnerabilities_white_paper.pdf

ŠULC, Vladimír, 2018. *Kybernetická bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7380–737-5.

UITS, 2021. *About viruses, worms, and Trojan horses*. University Information Technology Services [online]. [cit. 2022-06-16]. Dostupné z: https://kb.iu.edu/d/aehm

VILÁŠEK, Josef, Miloš FIALA a David VONDRÁŠEK, 2014. *Integrovaný záchranný systém ČR na počátku 21. století*. Praha: Karolinum. ISBN 978-80-246-2477-8.

VYŠKOV, 2018. *Směrnice č.3/2018: Řád bezpečnosti informačního systému MĚÚ Vyškov a městské policie*. In: Vyškov.

ZAORALOVÁ, Nicole, 2015. *Projekt Národní informační systém. HZS ČR* [online]. [cit. 2022-07-19]. Dostupné z: https://www.hzscr.cz/clanek/projekt-narodni-informacni-system.aspx

ZENELI, Gezim, 2016. *Guidelines to Cyber Security with ISO/IEC 27032* [online]. [cit. 2022-07-14]. Dostupné z: https://pecb.com/pdf/articles/82-guidelines-to-cyber-security-with-iso-27032.pdf

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

API	Application Programming Interfaces
ČR	Česká republika
EU	Evropská unie
GIS	Geografický informační systém
GŘ HZS	Generální ředitelství hasičského záchranného sboru
IEC	Mezinárodní elektrotechnická komise
IS	Informační systém
ISMS	Systém řízení bezpečnosti informací
ISO	Mezinárodní organizace pro normalizaci
IZS	Integrovaný záchranný systém
KOPIS	Krajské operační a informační středisko
KS	Krizové stavy
KSN	Kaspersky Security Network
MěÚ	Městský úřad ve Vyškově
MU	Mimořádné události
MV	Ministerstvo vnitra
NIS IZS	Národní informační systém integrovaného záchranného systému
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
OI/KST	Oddělení informatiky
OPIS	Operační a informační středisko

SEZNAM OBRÁZKŮ