Životní cyklus informací v prostředí ochrany obyvatelstva

Bc. Zuzana Balloková

Diplomová práce
2024

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

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

Akademický rok: 2023/2024

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Zuzana Balloková**
Osobní číslo:	**L22424**
Studijní program:	**N1032A020002 Bezpečnost společnosti**
Specializace:	**Ochrana obyvatelstva**
Forma studia:	**Prezenční**
Téma práce:	**Životní cyklus informací v prostředí ochrany obyvatelstva**

Zásady pro vypracování

1. Na základě provedené rešerše zpracujte teoretický vstup do dané problematiky.
2. Analyzujte životní cyklus informací ve vybraném subjektu ochrany obyvatelstva.
3. Identifikujte nedostatky v analyzovaném životním cyklu informací.
4. Navrhněte opatření pro zlepšení současného stavu.

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

Seznam doporučené literatury:

1. EVANS, Lester. *Cybersecurity: What You Need to Know About Computer and Cyber Security, Social Engineering, The Internet of Things + An Esential Guide to Ethical Hacking for Beginners.* USA: Lester Evans, 2019. ISBN 978-1794647237.
2. KOLOUCH, Jan a BAŠTA, Pavel. *CyberSecurity.* Edice CZ.NIC, 2019. ISBN 978-80-88168-31-7. Dostupné také z: https://knihy.nic.cz/files/edice/cybersecurity.pdf.
3. SMEJKAL, Vladimír; SOKOL, Tomáš a KODL, Jindřich. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. ISBN 978-80-7380-765-8.

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 2023**
Termín odevzdání diplomové práce: **26. dubna 2024**

L.S.

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

prof. Ing. Dušan Vičar, CSc.
ředitel ústavu

V Uherském Hradišti dne 4. prosince 2023

PROHLÁŠENÍ AUTORA 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: 23.4.2024

Jméno a příjmení studenta: Bc. Zuzana Balloková

.....
podpis studenta

ABSTRAKT

Diplomová práce se zabývá tématem kybernetické bezpečnosti se zaměřením na životní cyklus informací ve vybraném subjektu, který se angažuje v oblasti ochrany obyvatelstva. Teoretická část rozebírá jak současný stav ochrany obyvatelstva, tak kybernetické bezpečnosti. Následují klíčové prvky, které jsou relevantní pro řešené téma, za nimiž následují kybernetické hrozby současnosti. Praktická část je zaměřena na vybraný subjekt, u kterého je analyzován současný stav životního cyklu informací, na což navazuje návrhová část, díky které může být dosaženo vyšší úrovně zajištění kybernetické bezpečnosti.

Klíčová slova: analýza současného stavu, kybernetická bezpečnost, ochrana obyvatelstva, životní cyklus informací

ABSTRACT

The thesis deals with the topic of cyber security with a focus on the information lifecycle in a selected entity involved in the field of public protection. The theoretical part discusses both the current state of population protection and cybersecurity. The following are the key elements that are relevant to the topic at hand, followed by contemporary cyber threats. The practical part focuses on a selected entity, for which the current state of the information lifecycle is analysed, followed by a design part through which a higher level of cyber security assurance can be achieved.

Keywords: analysis of the current situation, cyber security, information lifecycle, population protection

Poděkování

Poděkování patří rodině a příteli za podporu, které se mi během celého studia a psaní diplomové práce dostávalo.

Taktéž bych chtěla poděkovat mému vedoucímu Ing. Petru Svobodovi, Ph.D. za ochotu a vstřícnost při vedení diplomové práce a za cenné rady a připomínky během zpracování.

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

OBSAH

ÚVOD **9**
CÍLE PRÁCE A POUŽITÉ METODY **11**
I TEORETICKÁ ČÁST **13**
1 SOUČASNÝ STAV OBLASTI OCHRANY OBYVATELSTVA **14**
2 SOUČASNÝ STAV KYBERNETICKÉ BEZPEČNOSTI V ČESKÉ REPUBLICE **18**
2.1 PRÁVNÍ PROSTŘEDÍ V OBLASTI KYBERNETICKÉ BEZPEČNOSTI 18
2.1.1 Závazné předpisy 18
2.1.2 Doporučující předpisy 21
2.1.3 Koncepční dokumenty 23
2.2 INSTITUCE KYBERNETICKÉ BEZPEČNOSTI 24
2.3 ZÁKLADNÍ TERMÍNY V OBORU KYBERNETICKÉ BEZPEČNOSTI 26
3 KLÍČOVÉ PRVKY KYBERNETICKÉ BEZPEČNOSTI **29**
3.1 TRIÁDA CIA 29
3.2 ŽIVOTNÍ CYKLUS INFORMACÍ 33
3.2.1 Data at Rest 34
3.2.2 Data in Motion 35
3.2.3 Data in Use 36
3.2.4 Likvidace dat 37
4 KYBERNETICKÉ HROZBY SOUČASNOSTI **39**
4.1 SOCIÁLNÍ INŽENÝRSTVÍ 39
4.2 MALWARE 41
4.3 NOVÉ PERSPEKTIVY A NEBEZPEČÍ 42
5 DÍLČÍ ZÁVĚR **44**
II PRAKTICKÁ ČÁST **45**
6 POPIS SOUČASNÉHO STAVU VYBRANÉHO SUBJEKTU **46**
6.1 CHARAKTERISTIKA VYBRANÉHO SUBJEKTU 46
6.2 BEZPEČNOSTNÍ OPATŘENÍ 48
6.3 ŽIVOTNÍ CYKLUS INFORMACÍ 78
7 NÁVRHY OPATŘENÍ **82**
7.1 ZAJIŠŤOVÁNÍ KYBERNETICKÉ BEZPEČNOSTI 83
7.2 POVINNOSTI VRCHOLOVÉHO VEDENÍ 84
7.3 ŘÍZENÍ AKTIV 84
7.4 ŘÍZENÍ RIZIK 85
7.5 BEZPEČNOST LIDSKÝCH ZDROJŮ 88

7.6 Řízení přístupu 89
7.7 Řešení kybernetických bezpečnostních incidentů 92
ZÁVĚR 93
SEZNAM POUŽITÉ LITERATURY 95
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK 103
SEZNAM OBRÁZKŮ 106
SEZNAM TABULEK 107
SEZNAM PŘÍLOH 108

ÚVOD

Kybernetická bezpečnost je aktuálním tématem z důvodu možných kybernetických útoků, které ohrožují státy, státní organizace, právní subjekty i jednotlivce. Lidé, technologie a procesy jsou stěžejními elementy kybernetické bezpečnosti, přičemž právě lidé jsou nejslabším článkem, protože jejich interakce s kyberprostorem může způsobit zranitelnost systému. Existují profesionální skupiny útočníků, které disponují financemi a technickou zdatností. Tyto skupiny mohou být významným bezpečnostním rizikem pro státy, organizace i jednotlivce. Praktická část diplomové práce se zaměřuje na vybranou organizaci, která pracuje s informacemi, které by mohly být důvodem pro kybernetický útok, například z důvodu následného vydírání a požadavku finančního obnosu. Informace jsou v moderní společnosti stále důležitější, a proto je nutné zajistit jejich ochranu.

Kybernetická bezpečnost je klíčová pro ochranu kritické infrastruktury, jako jsou energetické systémy, dopravní sítě, zdravotnická zařízení a komunikační sítě. Útoky na prvky kritické infrastruktury mohou mít závažný dopad pro obyvatelstvo, a proto je nutné soustavně zajišťovat jejich bezpečnost, aby bylo dosaženo ochrany obyvatelstva v co největší možné míře. Bezpečnostní strategie České republiky 2023 uvádí, že zajištění kybernetické bezpečnosti je významnou oblastí, která si zaslouží strategickou a dlouhodobou pozornost.

V současné chvíli je zásadním tématem evropská strategie kybernetické bezpečnosti NIS2, která přináší významné změny v oblasti kybernetické bezpečnosti. Státy Evropské Unie mají povinnost tuto implementovat do národních právních předpisů. Národní úřad pro kybernetickou bezpečnost rozhodl, že implementace do českého právního prostředí bude uskutečněna vznikem nového zákona o kybernetické bezpečnosti, nejen jeho novelizací. Společně s novým zákonem budou vznikat nové vyhlášky tohoto se týkající.

Téma diplomové práce je vybráno z důvodu zájmu autorky textu o rozšíření znalostí v oblasti kybernetické bezpečnosti, kterou zaujal vyučovaný předmět s totožným názvem. Téma je zaměřeno na životní cyklus informací vybraného subjektu, který působí v oblasti ochrany obyvatelstva. Po celou dobu zpracování je brán zřetel na zmíněný nově vznikající zákon o kybernetické bezpečnosti, aby bylo dosaženo co největší aktuálnosti v rámci návrhové části, která je důležitá pro zlepšení stávající úrovně zajištění kybernetické bezpečnosti vybraného subjektu se zřetelem na životní cyklus informací.

Subjekt, který se mimo jiné zabývá ochranou obyvatelstva a krizovým řízením pracuje s citlivými informacemi a daty, které se týkají veřejné bezpečnosti, infrastruktury a dalších důležitých oblastí. Kybernetická bezpečnost je proto nezbytná pro ochranu těchto dat a informací před kybernetickými hrozbami, jako jsou úniky dat, krádeže identity nebo ransomware útoky. Taktéž musí být schopen identifikovat a řešit kybernetické hrozby, které mohou ohrozit veřejnou bezpečnost a bezpečnost infrastruktury.

CÍLE PRÁCE A POUŽITÉ METODY

Kapitola uvádí hlavní cíl práce včetně dílčích, které slouží pro lepší uchopení cíle hlavního. Dále jsou jmenovány a krátce popsány metody, které jsou v diplomové práci používány a slouží k dosažení stanovených cílů.

Cíle práce

Hlavním cílem práce je navrhnout opatření ke zlepšení současné úrovně kybernetické bezpečnosti v souvislosti s vybraným životním cyklem informací subjektu ochrany obyvatelstva. Pro dosažení hlavního cíle jsou stanoveny následující dílčí cíle:

- Pojednat o souvisejících teoretických východiscích práce.
- S pomocí modelování analyzovat životní cyklus informací vybraného subjektu.
- Provést komparaci zamýšleného stavu kybernetické bezpečnosti se stavem aktuálním.

Výzkumné otázky

- Jak jsou naplněny požadavky zabezpečení životního cyklu informací vybraného subjektu z hlediska kybernetické bezpečnosti?
- Které prvky v životním cyklu informací ve vybraném subjektu nesplňují požadovanou úroveň kybernetické bezpečnosti?

Použité metody

- **Sběr dat a informací –** Metoda je využita během zpracování teoretické části a následně v praktické části pro popis současného stavu subjektu.
- **Pozorování –** Metoda je využita během zpracování současného stavu vybraného subjektu, především při modelování areálu a popisu fyzického přístupu.
- **Indukce** – Na základě sběru dat a informací byla zpracována teoretická východiska diplomové práce a byla provedena analýza současného stavu kybernetické bezpečnosti a v návaznosti na to navržena opatření ke zlepšení současné úrovně.
- **Dedukce** – Za pomoci logického vyvozování je zpracována diplomová práce, kdy je postupováno od obecnému ke konkrétnímu. Metody je využito především při vytváření návrhů opatření, které vycházejí z analýzy současného stavu kybernetické bezpečnosti.

- **Řízený rozhovor** – Na základě řízených rozhovorů s pracovníky vybraného subjektu jsou prohloubeny znalosti o zavedených bezpečnostních opatřeních uvnitř organizace.
- **Dotazování** – Je využito metody dotazování pro doplnění chybějících informací, které je potřeba získat pro ucelení praktické části.
- **Deskripce** – Je využito metody deskripce po řízených rozhovorech, které jsou následně utříděny tak aby respektovaly strukturu nově vznikajícího zákona o kybernetické bezpečnosti.
- **Modelování** – Metody modelování je využito v praktické části pro vyobrazení areálu subjektu, jeho pokrytí kamerami, ale také při vytváření diagramů procesů pro lepší představu probíhajících procesů uvnitř subjektu. Metoda je využita při tvorbě swimlane diagramu pro zobrazení životního cyklu informací a v návrhové části pro jejich možnou implementaci.
- **Analýza** – V práci je aplikována metoda analýzy formou checklistů, které jsou v případě potřeby rozšířeny o návrhy opatření.
- **Syntéza** – Metoda syntézy je použita pro propojení jednotlivých částí do konečného celku. Je použita především při syntéze tabulek jednotlivých checklistů v kapitole s návrhy opatření, aby bylo dosaženo lepšího přehledu o následujících návrzích a důvodech jejich navržení.

V diplomové práci není zmíněn název subjektu ani jeho lokace pro zachování kompletní anonymity z bezpečnostních důvodů, protože se v práci nachází informace, které by mohly být zneužity.

I. TEORETICKÁ ČÁST

1 SOUČASNÝ STAV OBLASTI OCHRANY OBYVATELSTVA

Počátkem ochrany obyvatelstva, jak ji známe dnes, je vznik civilní protiletecké ochrany přijetím zákona č. 82/1935 Sb., o ochraně a obraně proti leteckým útokům. V roce 1951 došlo ke změně prostřednictvím Vládního usnesení o civilní obraně a tím se civilní obrana dostala do působnosti ministerstva vnitra a byla rozdělena na vojenskou a nevojenskou část. V působnosti ministerstva vnitra ale nezůstala a od roku 1976 již spadala pod ministerstvo obrany (Chronologická geneze civilní ochrany (obrany), © 2023).

V roce 1990 vyvstala potřeba změnit uspořádání této problematiky a vybudovat spolehlivý systém ochrany obyvatelstva (Chronologická geneze civilní ochrany (obrany), © 2023). Vláda v březnu roku 1993 přijala Usnesení č. 126, které obsahovalo Opatření civilní ochrany České republiky. Zásadní změnou v problematice ochrany obyvatelstva bylo přijetí usnesení vlády ČR ze dne 12. listopadu 1997 č. 710 ke koncepci zabezpečení úkolů civilní ochrany definovaných Dodatkovým protokolem I k Ženevským úmluvám o ochraně obětí mezinárodních ozbrojených konfliktů z 12. srpna 1949. Tímto usnesením se předpokládá odpovědnost ministerstva vnitra za plnění úkolů civilní ochrany v míru, za mimořádných událostí nebo krizových situací a válečného stavu a výkon státní správy ve věcech civilní ochrany na republikové úrovni (Linhart, © 2023).

V polovině roku 2000 byl přijat takzvaný „balíček krizových zákonů“, jehož součástí byl zákon č. 239/2000 Sb., o integrovaném záchranném systému (dále jen „IZS“), který definuje a tím i zavádí pojem ochrana obyvatelstva tak jak ho známe dnes.

> *„Ochranou obyvatelstva se rozumí plnění úkolů civilní ochrany, zejména varování, evakuace, ukrytí a nouzové přežití obyvatelstva a další opatření k zabezpečení ochrany jeho života, zdraví a majetku.“* (Zákon č. 239/2000 Sb., o IZS)

Mimo balíček krizových zákonů, který bude rozebírán v této kapitole později, je stěžejním ústavní zákon č. 1/1993 Sb., **Ústava České republiky** a s ním zákon č. 2/1993 Sb., Usnesení předsednictva České národní rady o vyhlášení **Listiny základních práv a svobod** jako součást ústavního pořádku ČR.

V rámci budování nového systému ochrany obyvatelstva byla potřeba ukotvení otázek bezpečnosti státu, a to ústavním zákonem č. 110/1998 Sb., **o bezpečnosti ČR**. Zákon se zabývá zajištěním svrchovanosti a územní celistvosti státu, ochranou jeho demokratických základů a ochranou životů, zdraví a majetkových hodnost. Bezpečnost ČR zajišťují ozbrojené síly, ozbrojené bezpečnostní sbory, ale také záchranné sbory a havarijní služby.

Podstatné je také zmínit zákon české národní rady č. 2/1969 Sb., o **zřízení ministerstev a jiných ústředních orgánů státní správy**, kterým jsou definovány okruhy jejich působnosti a zásady činností.

Již zmíněný balíček krizových zákonů byl vydán roku 2000, a obsahuje čtyři klíčové zákony pro uchopení v té době vznikajícího integrovaného záchranného systému. Prvním je zákon č. 238/2000 Sb., **o hasičském záchranném sboru**, tento byl ale nahrazen zákonem č. 320/2015 Sb. Druhým vydaným zákonem je č. 239/2000 Sb., o **integrovaném záchranném systému** (dále jen IZS). Další zákon z krizového balíčku je č. 240/2000 Sb., o **krizovém řízení** a posledním je zákon č. 241/2000 Sb., o **hospodářských opatřeních pro krizové stavy**.

Vyhláška ministerstva vnitra č. 380/2002 Sb., k **přípravě a provádění úkolů ochrany obyvatelstva** navazuje na zákon o IZS a je významným právním předpisem, který určuje konkrétní postupy, způsoby a požadavky k jednotlivým úkolům ochrany obyvatelstva (Vyhláška MV č. 380/2002 Sb., k přípravě a provádění úkolů OO).

Významným dokumentem v oblasti ochrany obyvatelstva je **Koncepce ochrany obyvatelstva do roku 2025 s výhledem do roku 2030**. Navazuje na předchozí koncepce, které pružně reagují na aktuální, ale i předpokládané vývojové trendy v této oblasti. Koncepce se zakládá na klíčovém motivu „Připravený občan. Připravený systém.“. Aby bylo možné zajistit bezpečnost občanů a tím dosáhnout kvalitní úrovně života dle Ústavy České republiky, je potřeba mít kvalitní systém, který je schopen reagovat na hrozby různého charakteru. Pro správné zvládnutí úkolů jednotlivých složek, musí probíhat ustavičné zlepšování jejich schopností.

Jak vyplývá z motivu celé koncepce, je důležité, vedle dostatečně připravených jednotlivých složek, mít připravené občany, jak z pohledu jejich informovanosti, tak z pohledu vzájemné pomoci. Pro splnění těchto závazků byly definovány tři strategické cíle, které jsou dále rozvětveny. Celkem bylo stanoveno dvanáct úkolových oblastí, díky kterým bude zajištěna připravenost obyvatelstva a posílení jednotlivých složek tohoto systému (KONCEPCE OCHRANY OBYVATELSTVA do roku 2025 s výhledem do roku 2030, © 2024).

V Koncepci ochrany obyvatelstva do roku 2020 s výhledem do roku 2030 bylo Ministerstvo vnitra pověřeno úkolem zpracovat analýzu hrozeb a její výsledky implementovat do dalších metodických a strategických materiálů v oblasti bezpečnosti státu. V roce 2015 tak vyšla

Analýza hrozeb pro Českou republiku. Na zpracování se nepodílelo jen Ministerstvo vnitra, ale také další ministerstva a odborníci v dané oblasti. Postup řešení tohoto úkolu byl zvolen na základě ČSN EN 31 010 Management rizik – techniky a posuzování rizik. V prvním kroku bylo identifikováno celkem 72 typů nebezpečí, z nichž byl sestaven registr. Identifikovaná nebezpečí byla následně podrobena další analýze, některá z nich byla vyhodnocena jako nebezpečí s nízkým rizikem, proto se další analýze již nepodrobila.

Dva typy nebezpečí (narušení bezpečnosti informací kritické informační infrastruktury, narušení finančního a devizového hospodářství státu velkého rozsahu) byly předběžně vyhodnoceny jako nebezpečí s vysokým rizikem a označeny jako rizika nepřijatelná. Detailnější analýze bylo podrobeno 49 typů nebezpečí. Celkově bylo pro Českou republiku identifikováno 22 typů nebezpečí, u kterých je vysoká pravděpodobnost vyhlášení krizového stavu a jsou tak označena jako nebezpečí s nepřijatelným rizikem (Analýza hrozeb pro Českou republiku, © 2024).

Bezpečnostní strategie České republiky 2023 je základním bezpečnostním dokumentem bezpečnostní politiky. Je vládním dokumentem, na který budou navazovat další strategické a koncepční dokumenty. Byla zpracována ve spolupráci s Kanceláří prezidenta republiky a Parlamentem ČR, jež mají za cíl hledat nadstranické přístupy k zajišťování bezpečnosti. Ke zpracování byla přizvána také bezpečnostní komunita ze státní i nestátní sféry. Více než kdy předtím, je strategie zaměřena na oblast kybernetické bezpečnosti.

Již v úvodu je zmíněná důležitost odolnosti vůči nepřátelskému působení v kybernetické oblasti. Mezi bezpečnostními strategickými zájmy ČR je uvedeno zabezpečení komunikační, informační a kybernetické bezpečnosti a obrany ČR s důrazem na otevřený, stabilní a bezpečný kybernetický prostor. Další významné bezpečnostní zájmy poukazují na snižování kybernetické kriminality a kladou důraz na kybernetickou a informační gramotnost, která by měla být zajištěna změnou ve vzdělávacím systému (Bezpečnostní strategie České republiky 2023, © 2024).

Bezpečnostními hrozbami a zdroji nestability jsou hrozby v kybernetické prostoru, které využívají zranitelnosti informačních a komunikačních systémů. Strategie uvádí, že kybernetický útok velkého rozsahu by mohl mít za následek aktivaci kolektivní ochrany NATO. Jedním z cílů strategie prosazování bezpečnostních zájmů ČR může být zajišťování bezpečnosti a odolnosti v kybernetickém prostoru.

V rámci strategie prevence a potlačování hrozeb ekonomické bezpečnosti a s vědomím, že většina činností v oblasti ekonomiky již je, nebo bude postupně digitalizována, je kladen důraz na zajištění kybernetické bezpečnosti.

V nově zařazené kapitole „oblasti strategické pozornosti“, ve které se mimo jiné strategie věnuje obraně ČR a úkolům ozbrojených sil, je poukázáno na zapojení do mezinárodních organizací, a na to, že i když jsme účastni v systému kolektivní obrany, neznamená to, že bychom se neměli věnovat rozvoji schopností zajišťujících obranu našeho území, ale právě naopak. Mimo jiné oblasti, které je potřeba zajistit, jako například zajištění ochrany infrastruktury, je zde opět poukázáno na nutnost obrany před nepřátelskými hybridními operacemi včetně kybernetických hrozeb, informačně-manipulativních a vlivových akcí a pokusů o ovlivnění či ochromení rozhodovacích procesů. Stát již v současnosti zvyšuje obranyschopnost v různých operačních prostorech – země, vzduch, kybernetický prostor, vesmír (Bezpečnostní strategie České republiky 2023, © 2024).

Oblasti kybernetické bezpečnosti obsahují samostatnou podkapitolu věnující se kybernetické bezpečnosti. Pojednává o rozsáhlé škále aktérů, na kterých stojí systém zajišťování kybernetické bezpečnosti. Tito aktéři, ať už ze státního či nestátního sektoru, se musí ustavičně přizpůsobovat měnícímu se prostředí. Aby bylo dosahováno zvyšování odolnosti informační infrastruktury, je nutné vytvořit ucelený systém předcházení, odhalování a reakce na kybernetické hrozby.

Pozornost je věnována nutnosti vytváření právních norem a politik, které budou prezentovat aspekty globálního, otevřeného, stabilního, spolehlivého a bezpečného kybernetického prostoru. K zajištění takovéhoto kybernetického prostoru je zásadní mít nejen právní základ, odolnou infrastrukturu, ale také průběžné a systematické vzdělávání všech vrstev společnosti. Česká republika má výrazný nedostatek odborníků v oblasti kybernetické bezpečnosti. Strategie v návaznosti na tuto skutečnost vyžaduje, aby se stát a další aktéři podíleli na rozšiřování kvalifikované personální základny v této oblasti (Bezpečnostní strategie České republiky 2023, © 2024).

2 SOUČASNÝ STAV KYBERNETICKÉ BEZPEČNOSTI V ČESKÉ REPUBLICE

Současný stav kybernetické bezpečnosti v České republice je spravován pomocí právních norem, směrnic, národních i mezinárodních dokumentů, především na úrovni Evropské unie. Kontrolní činnost a dohled mají ve své kompetenci orgány působící v oblasti KB, které jsou taktéž popsány níže. Pro správné uchopení tématu jsou definovány vybrané základní pojmy, které se týkají dané problematiky.

2.1 Právní prostředí v oblasti kybernetické bezpečnosti

Kapitola je rozdělena na tři části. První část se věnuje závazným předpisům, které jsou z hlediska kybernetické bezpečnosti nezbytné pro zajištění její minimální úrovně. Další částí jsou doporučující předpisy, které mohou úroveň kybernetické bezpečnosti značně zvýšit. Poslední částí jsou koncepční dokumenty, které reflektují současný stav kybernetické bezpečnosti na území České republiky.

2.1.1 Závazné předpisy

Stěžejním právním předpisem je **zákon č. 181/2014 Sb., o kybernetické bezpečnosti** a o změně souvisejících zákonů. Zabývá se právy a povinnostmi osob, působnostmi a pravomocemi orgánů veřejné moci v této oblasti. Vychází ze Směrnice Evropského Parlamentu a Rady (EU) 2016/1148 o opatřeních k zajištění vysoké společenské úrovně bezpečnosti sítí a informačních systémů v Unii (směrnice NIS). Vymezuje pojmy, které se týkají této problematiky. Specifikuje systém zajištění kybernetické bezpečnosti, kde jsou rozdělena opatření na bezpečnostní, organizační a technická (Zákon č. 181/2014 Sb., o kybernetické bezpečnosti).

Stanovuje činnost dohledových pracovišť. Ukládá povinnost hlášení kybernetického bezpečnostního incidentu, jeho evidenci, opatření a varování. Cílem tohoto zákona je zlepšení detekce kybernetických bezpečnostních incidentů a jejich hlášení. Snaží se vymezit základní úroveň bezpečnostních opatření a zároveň zavést systém opatření k reakci na kybernetické bezpečnostní incidenty. Zákon o kybernetické bezpečnosti v průběhu let prošel několika novelizacemi, aktuálně poslední je zákonem č. 226/2022 Sb., znění zákona je účinné od srpna 2022 (Legislativa KB, © 2023).

Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti

a likvidaci dat, zkráceně **vyhláška o kybernetické bezpečnosti**, zapracovává směrnici NIS. Stanovuje pro informační a komunikační systémy náležitosti bezpečnostní dokumentace a bezpečnostních opatření, typy, kategorie a hodnocení významnosti kybernetických bezpečnostních incidentů včetně jejich hlášení a oznámení o provedení reaktivních opatření včetně vzoru oznámení kontaktních údajů a v neposlední řadě upravuje způsob likvidace dat, provozních údajů, informací a jejich kopií (Vyhláška č. 82/2018 Sb., o KB).

Vyhláškou č. 317/2014 Sb., o významných informačních systémech (dále jen „IS“) a jejich určujících kritériích jsou stanoveny právě významné IS, jejichž správcem je orgán veřejné moci, který je organizační složkou státu, krajem nebo hlavním městem Praha, využívaný při výkonu působnosti orgánu veřejné moci k zajištění například elektronické pošty, je-li určena k použití v rámci výkonu veřejné moci; výkonu veřejné moci při přípravě na krizové situace a jejich řešení; výkonu spisové služby; mezinárodní spolupráce; nebo zadávání veřejných zakázek. Významným informačním systémem může být také takový IS, který splňuje určující kritéria dle tohoto zákona. Může jím být skutečnost, že narušení bezpečnosti informací v IS by mohlo způsobit omezení či narušení poskytování služeb nebo informací orgánem veřejné moci veřejnosti nebo například ohrožení či narušení veřejného zájmu a toto omezení, narušení, zásah či ohrožení nebude možné odvrátit bez vynaložení nepřiměřených nákladů (Vyhláška č. 317/2014 Sb., o významných IS).

Podstatné je také zmínit **nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury**, které bylo změněno č. 315/2014 Sb., kde byla k odvětvovému kritériu VI. Komunikační a informační systémy přidána oblast kybernetické bezpečnosti (NV č. 432/2010 Sb., o kritériích pro určení prvku KI).

Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti upravuje zásady a způsoby ochrany informací, jejichž vyzrazení či zneužití by mohlo způsobit újmu některým ze zájmů ČR (svrchovanost, územní celistvost, vnitřní pořádek a bezpečnost aj.). Rozděluje informace na vyhrazené, důvěrné, tajné a přísně tajné. Stanovuje zásady pro posuzování bezpečnostní způsobilosti osob a subjektů, které se s těmito informacemi setkávají. Základními požadavky jsou plnoletost, svéprávnost a bezúhonnost (Zákon č. 412/2005 Sb., o ochraně utajovaných informací).

V České republice není GDPR v tomto znění právně ukotveno, oblast tohoto se týkající upravuje **zákon č. 110/2019 Sb., o zpracování osobních údajů.** Je v souladu právě s GDPR, ale také napomáhá orgánům při pátrání nebo odhalování trestné činnosti. Upravuje postavení

a pravomoc Úřadu pro ochranu osobních údajů a způsob zabezpečení systémů a ochrany osobních údajů (Zákon č. 110/2019 Sb., o ochraně osobních údajů).

Do této chvíle byly rozebrány závazné předpisy z českého právního prostředí. Nyní následují závazné právní předpisy z prostředí Evropské Unie.

Směrnice Evropského Parlamentu a Rady (EU) 2016/1148 o opatřeních k zajištění vysoké společenské úrovně bezpečnosti sítí a informačních systémů v Unii neboli **směrnice NIS** se zaměřuje na sítě a informační systémy, jež jsou nezbytné pro poskytování základních a digitálních služeb v oblasti energetiky, dopravy, zdravotnictví, finančních trhů či veřejné správy (SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/1148 …, © 2023). Hlavním cílem bylo sjednocení členských států EU v rámci zajištění vysoké úrovně bezpečnosti právě na úrovni sítí a informačních systémů. Nízký počet zemí měl ucelený právní rámec pro tuto oblast a měly k dispozici bezpečnostní týmy CSIRT/CERT. Směrnice tak vytvořila bezpečnostní požadavky, které měly do roku 2018 členské státy splnit a promítnout do potřebných právních předpisů. V České republice se tak stalo právě novelizací zákona o kybernetické bezpečnosti a vyhláškou o kybernetické bezpečnosti. V zákoně o kybernetické bezpečnosti však již byly některé povinnosti, které směrnice NIS ukládá, řešeny (Duračinská, © 2023).

V současné době je již zpracována také nová **směrnice NIS2**, která prohlubuje a rozšiřuje původní směrnici NIS. V platnost vešla 16. ledna 2023, členské státy měly splnit stanovené požadavky do 16. října 2024, což znamená zavést požadavky do národní legislativy v níž bude stanovena lhůta pro organizace, které do této doby nepodléhaly regulaci kybernetické bezpečnosti. Již v průběhu zpracovávání práce je velmi pravděpodobné, že implementace do českého právního prostředí bude provedena až během roku 2025. Nejdůležitější změny se budou týkat nejen subjektů na strategické úrovni jako je NÚKIB a Evropská agentura pro bezpečnost sítí a informací (ENISA), ale také povinných osob, kterými rozumíme konkrétní subjekty, společnosti a státní organizace. V ČR se již pracuje na implementaci nové směrnice NIS2 prostřednictvím nového zákona o kybernetické bezpečnosti, který v současnosti prochází legislativním procesem (Obecné informace o směrnici NIS2 …, © 2023).

The Digital Operational Resilience Act (DORA) je nařízení Evropské unie, které vstoupilo v platnost v lednu 2024, jehož cílem je posílit bezpečnost IT finančních subjektů, jako jsou banky, pojišťovny a investiční podniky. Snaží se o zajištění finančního sektoru v Evropě tak,

aby byl schopen zůstat odolný v případě vážného narušení provozu. DORA, do češtiny překládané jako Nařízení EU o digitální provozní odolnosti, přináší harmonizaci pravidel týkajících se provozní odolnosti pro finanční sektor, které se vztahují na dvacet různých typů finančních subjektů a poskytovatelů ICT služeb třetích stran. Účinnost má nabýt 17. ledna 2025 (Digital Operational Resilience Act (DORA), © 2024).

Směrnice o odolnosti kritických subjektů, z anglického **Critical Entities Resilience** (CER) má za cíl snížit zranitelnost a zvýšit odolnost kritických subjektů vůči různým hrozbám. Nahrazuje starou směrnici o evropské kritické infrastruktuře z roku 2008, které se týkala jen vybraných odvětví a daných částí odolnosti. Cílem nové směrnice z prosince 2022 je posílit odolnost zmíněných kritických subjektů vůči široké škále hrozeb, kterými mohou být přírodní katastrofy, terorismus, hybridní či vnitřní hrozby a sabotáže v různých oborech (Směrnice o odolnosti kritických subjektů CER…, © 2024).

2.1.2 Doporučující předpisy

Důležitou mezinárodní normou v oblasti kybernetické bezpečnosti je **ČSN ISO 27 000** s názvem **Information Security Management Systems** (ISMS), v českém jazyce Systém řízení bezpečnosti informací. Představuje souhrnný název pro spektrum norem, které jsou zaměřeny na konkrétní aspekty informační bezpečnosti v organizacích. Nejedná se o právně závaznou normu, ale pokud se organizace rozhodne získat toto ověření, prokáže tak, že je kybernetická/informační bezpečnost na dostatečné úrovni a firma se tak stane důvěryhodnou. Ověření spočívá především v analýze rizik a kontrole fyzické bezpečnosti (perimetr, autentizace a autorizace apod.). Systém řízení bezpečnosti informací zahrnuje větší spektrum bezpečnostních požadavků než zákon o kybernetické bezpečnosti (Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník, © 2024).

Za zmínku stojí **Národní institut pro standardy a technologie** neboli NIST, který byl založen v roce 1901 a nyní je součástí amerického ministerstva obchodu. Zabývá se mnoha odvětvími a jedním z nich je právě kybernetická bezpečnost v rámci, které vyvíjí normy, pokyny, osvědčené postupy a další zdroje týkající se kybernetické bezpečnosti, které odpovídají potřebám průmyslu, úřadů a širší veřejnosti. NIST prohlubuje porozumění rizikům v oblasti ochrany soukromí, z nichž některá přímo souvisejí s kybernetickou bezpečností a zlepšuje tak jejich řízení. Mezi prioritní oblasti patří kryptografie, vzdělání a pracovní síly, nové technologie, řízení rizik, správa identit a přístupu, soukromí, důvěryhodné sítě a důvěryhodné platformy (Cybersecurity, © 2024).

Další metodikou je COBIT neboli **Control Objectives for Information and Related Technology**. V českém jazyce chápeme jako „Kontrolní cíle pro informační a související technologie“, čímž rozumíme rámec vyvinutý organizací ISACA, sloužící k zajištění efektivního řízení firemních informací a informačních technologií. Snaží se o propojení cíle IT a hlavní obchodní aktivity organizace. Information System Audit and Control Association (ISACA) je nezávislou neziskovou mezinárodní profesní asociací, která se věnuje oblasti auditu, řízení, kontroly a bezpečnosti informačních systémů.

V současné chvíli je nejaktuálnější verzí zmíněného rámce COBIT 2019, který zachovává pozici COBIT jako rámce zastřešujícího. Je aktualizován tak aby byl v souladu s příslušnými normami, rámci a předpisy, ale opírá se také o koncepty vycházející z jiných zdrojů, jimiž jsou další IT standardy a rámce. Model COBIT zahrnuje celkem 40 cílů. Cíle řízení jsou sdruženy do čtyř domén:

- Zarovnat, plánovat a organizovat (Align, Plan and Organize = APO) – doména se soustředí na celkovou organizaci, strategii a podpůrné činnosti v oblasti informační systémů a informačních technologií.
- Vytvořit, osvojit si a implementovat (Build, Acquire and Implement = BAI) – nakládá s definicí, osvojením a implementací řešením informačních systémů a informačních technologií a jejich sjednocení do podnikových činností.
- Doručování, servis a podpora (Deliver, Service and Support = DSS) – zabývá se provozní dodávkou a podporou informačních systémů a informačně technologických služeb, včetně bezpečnostní podpory.
- Monitorovat, vyhodnocovat a hodnotit (Monitor, Evaluate and Access = MEA) – soustředí se na sledování výkonu a soulad informačních systémů a informačních technologií s vnitřními výkonnostními cíli, cíli interní kontroly a externími požadavky (Smejkal et al., 2019).

Za zmínku stojí certifikace CISA, „**Certified Information Systems Auditor**“, kterou taktéž vyvinula společnost ISACA. Jedná se o celosvětově uznávaný standard pro všechny, kteří provádějí audit, kontrolu, monitorování a hodnocení informačních a obchodních systémů organizace. Pokud má organizace certifikát CISA, prezentuje tak své znalosti a schopnosti uplatňování přístupu založeném na rizicích při plánování, provádění a podávání zpráv o auditních zakázkách (What is the CISA difference?, © 2024).

V neposlední řadě existuje **Information Technology Infrastructure Library** (ITIL). Soubor konceptů a postupů ITIL byl vytvořen vládou Velké Británie v 80. letech minulého století. Od svého vzniku prošel řadou změn až k nynější aktuální verzi ITIL 4, která navazuje na ITIL 3 z roku 2011. Hlavní složkou ITIL 4 je takzvaný systém hodnoty služeb, z anglického Service Value System (dále jen SVS), jež umožňuje využívání nových principů řízení služeb. SVS umožňuje znázornit, jak mezi sebou spolupracují složky a činnosti organizace při tvoření hodnot, umožňuje podporu realizace očekávaných přínosů, pomocí správy a podpory IT produktů a služeb.

Soubor ITIL 4 je postaven na uceleném přístupu k řízení procesu služeb, který zahrnuje čtyři dimenze, jež jsou zásadní pro každou organizaci. Dimenzemi jsou organizace a lidé, informace a technologie, partneři a dodavatelé a procesy (Smejkal et al., 2019).

2.1.3 Koncepční dokumenty

Zpráva o stavu kybernetické bezpečnosti ČR za rok 2022 byla vydána v červenci 2023 Národním úřadem pro kybernetickou a informační bezpečnost a schválena byla vládou ČR. Dokument obsahuje aktuální výzvy a nové hrozby v oblasti KB. Uvádí, že během roku 2022 došlo k menšímu počtu kybernetických incidentů než v roce předchozím, které NÚKIB zaznamenal, Policie ČR naopak zaznamenala téměř dvakrát vyšší počet kybernetických aktivit. Významnou událostí roku 2022 byl konflikt na Ukrajině, který měl dopad na bezpečnostní prostředí v Evropě a na projevy kybernetické kriminality. S ruskou invazí na Ukrajině jsou spojovány útoky dvou ruskojazyčných skupin, přičemž obě skupiny konaly v souvislosti s českou podporou Ukrajiny.

Kromě vymezení nejčastějších typů útoků, kterými jsou phishing, scanning a podvodné e-maily, dokument řeší také novou směrnici NIS2 a zpracování nového zákona o kybernetické bezpečnosti. Přináší téma nedostatečného ohodnocení zaměstnanců v oblasti kybernetické bezpečnosti a s tím související nedostatek odborníků v této oblasti, což znamená významný problém nejen v tomto roce, ale také v budoucnosti, pokud bude nedostatek dále přetrvávat. Sděluje, že se dají očekávat útoky na subjekty v oblasti energetiky a dopravního sektoru. Informuje, že i když jsou ransomwarové incidenty páchány především kyberkriminálními skupinami, nelze vyloučit využití sankciovanými státy pro účel finančního zisku, kamufláže destruktivních či kyberšpionážních cílů (Zpráva o stavu kybernetické bezpečnosti české republiky za rok 2022, © 2023).

Kybernetická bezpečnost ČR stojí na principech, které popisuje **Národní strategie kybernetické bezpečnosti ČR 2021-2025**. Je vrcholných dokumentem této oblasti. Schválen byl na konci listopadu roku 2020 a vychází ze zákona o kybernetické bezpečnosti. Priority, úkoly, cíle a klíčové oblasti, na které je třeba se zaměřit jsou zapracovány do **Akčního plánu k Národní strategii kybernetické bezpečnosti pro období let 2021 až 2025**. Akční plán se zaměřuje na tři klíčové oblasti, kterými jsou „Sebevědomě v kyberprostoru", „Silná a spolehlivá spojenectví" a „Odolná společnost 4.0". Oblasti jsou dále rozděleny dle konkrétních odvětví, která jsou dále rozvětvena do konkrétních úkolů. Každému úkolu je přidělen odpovědný subjekt včetně stanoveného časového rámce do kdy mají být úkoly splněny (Národní strategie KB ČR 2021-2025, © 2023) (Akční plán k Národní strategii KB ČR na období let 2021 až 2025, © 2023).

2.2 Instituce kybernetické bezpečnosti

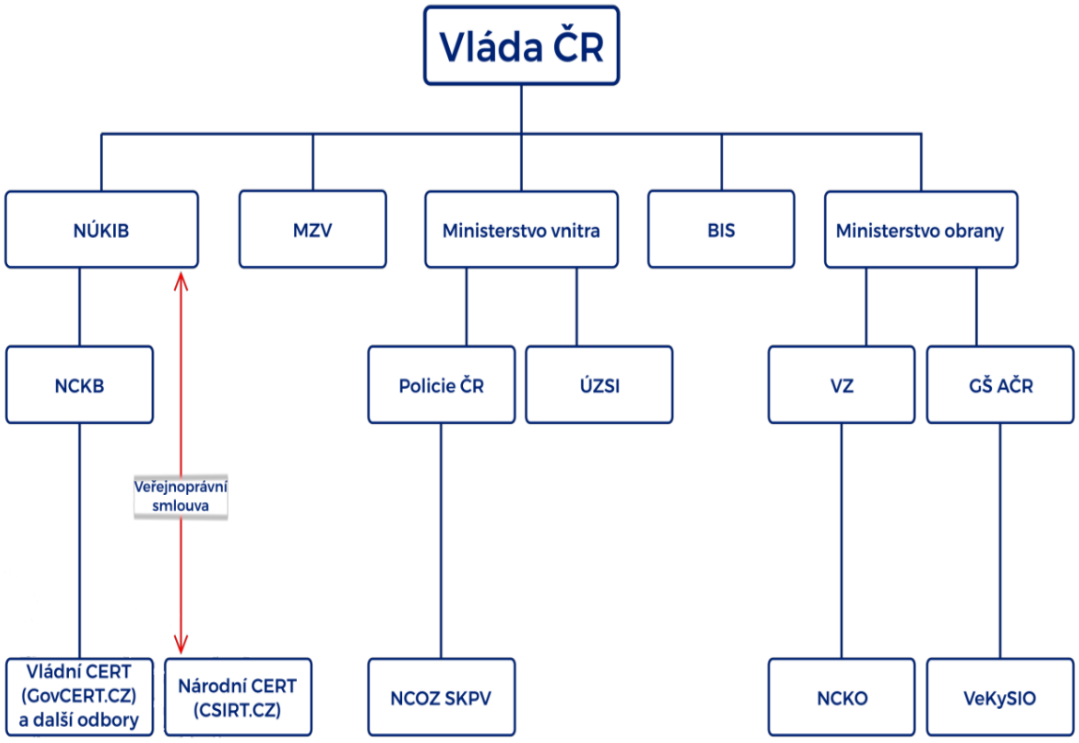
Zastřešujícím orgánem je **Národní úřad pro kybernetickou a informační bezpečnost**, který se zaobírá také ochranou utajovaných informací ve sféře informačních a komunikačních systémů a kryptografické ochrany. Vznikl na základě zákona o kybernetické bezpečnosti v srpnu 2017. V čele stojí ředitel Ing. Lukáš Kintr, který se pravidelně účastní zasedání Bezpečnostní rady státu a je členem Výboru pro kybernetickou bezpečnost, který je stálým pracovním orgánem BRS (NÚKIB, © 2023). Pod NÚKIB patří **Národní centrum kybernetické bezpečnosti**, které je jeho výkonnou sekcí. To, mimo jiné, zajišťuje činnost Vládního bezpečnostního týmu, takzvaný Vládní CERT ČR. Jedná se také o týmy typu CSIRT, které mají hlavní úlohu při ochraně kritické informační infrastruktury a významných informačních systémů. Jejich hlavním posláním je prvotní zdroj bezpečnostních informací pro státní subjekty. CERT či CSIRT týmy můžeme zjednodušeně chápat jako výjezdový tým, který je vyslán na místo, kde došlo k bezpečnostnímu incidentu (Vládní CERT, © 2023).

Nařízení Evropské Unie 2019/881 o **agentuře ENISA** a o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií neboli **akt o kybernetické bezpečnosti** usiluje o zvýšení úrovně kybernetické bezpečnosti, kybernetické odolnosti a důvěry v Evropskou unii. Stanovuje rámec pro dobrovolné evropské systémy certifikace KB pro produkty, služby a procesy informačních a komunikačních technologií (dále jen ICT). Usiluje o dosažení cílů prostřednictvím stanovených úkolů a organizačních hledisek pro Agenturu EU pro KB (ENISA). Agentuře byl definován mandát, ale také správní a řídící struktura,

které napomáhají k dosažení stanovených cílů. Výsledkem by mělo být zvýšení důvěry v produkty, služby a procesy v oblasti ICT. Právě produkty, služby či procesy, které projdou touto evropskou certifikací získají osvědčení o dosažení bezpečnostních cílů stanovených aktem o KB v oblastech dostupnosti, autentičnosti, důvěrnosti a integrity (Cybersecurity Act, © 2023).

Kybernetickou bezpečností se zabývá také **Bezpečnostní informační služba**, jejíž působení je podstatné pro ochranu bezpečnostních a ekonomických zájmů ČR. Vyšetřuje elektronické útoky, shromažďuje a analyzuje informace o hrozbách a rizicích pro strategické ICT. Udržuje spolupráci s mezinárodními partnery a monitoruje aktuální dění ve vývoji ICT (Kybernetická bezpečnost, © 2023). V rámci Národní strategie kybernetické bezpečnosti 2021-2025 zpracovává a analyzuje informace, které jsou relevantní pro kybernetickou nebo národní bezpečnost ČR. Stejný úkol v oblasti KB má také **Vojenské zpravodajství** a **Úřad pro zahraniční styky a informace**. Vojenské zpravodajství nese odpovědnost za budování systému kybernetické obrany v ČR. Mimo jiné je VZ v součinnosti s Armádou ČR, konkrétně **Velitelstvím kybernetických sil a informačních operací**. Činí nezávisle, společně nebo v součinnosti s pozemními, vzdušnými a speciálními silami v případě nutné ochrany kybernetického prostoru a vedení vojenských kybernetických operací (Národní strategie KB ČR 2021-2025, © 2023).

Policie České republiky má také svou úlohu v tomto oboru, a to prostřednictvím **Národní centrály proti organizovanému zločinu Služby kriminální policie a vyšetřování**. Plní funkci kontaktního bodu pro kybernetickou kriminalitu a pro hlášení závadného obsahu a závadových aktivit v síti Internet. Kybernetická kriminalita je především v gesci orgánů trestního řízení (Národní strategie KB ČR 2021-2025, © 2023).



Obrázek 1 Struktura zajišťování kybernetické bezpečnosti v ČR (Národní strategie KB ČR 2021-2025, © 2023)

2.3 Základní termíny v oboru kybernetické bezpečnosti

Hardware jsou fyzické součásti počítače, jako je základní deska, procesor, paměť, úložné jednotky a další zařízení. Právě hardware hostí a podporuje software nebo programy, které poskytují instrukce pro počítač k provádění jeho úkolů. Hardwarem může být také externí vstupní a výstupní zařízení, jako je klávesnice, myš, monitor, tiskárna a reproduktory (What is Hardware, © 2022). **Software** chápeme jako soubor pravidel nebo programů, které dávají počítači pokyny k provádění konkrétních úkolů. Software je obecným termínem používaným pro popis počítačových programů jako jsou skripty, aplikace, programy, webové stránky apod. Jedná se o cokoli, co je na počítači spustitelné (What is Software, © 2022).

Firewall je zařízení, které představuje bránu pro zabezpečení sítě. Monitoruje příchozí a odchozí síťový provoz a na základě definované sady bezpečnostních pravidel rozhoduje o povolení nebo zablokování určitého provozu. Vytváří bariéru mezi zabezpečenými a kontrolovanými vnitřními sítěmi, které mohou být důvěryhodné, a nedůvěryhodnými vnějšími sítěmi, jako je například internet. Firewall může být ve formě hardwaru, softwaru, softwaru jako služby, veřejného cloudu či soukromého (virtuálního) cloudu (What Is a Firewall?, © 2024).

Basic Input Output System (BIOS) v překladu znamená vstupně-výstupní systém, což je velmi krátký kód obsažený v čipu na základní desce. Po spuštění počítače je BIOS prvním softwarem, který se spustí. Po spuštění identifikuje hardware počítače, konfiguruje jej, testuje a připojuje k operačnímu systému pro další úkony. Jedná se o takzvaný zaváděcí proces (What Is BIOS?, © 2024).

DNS (Domain Name System) je systém kdy uživatelé přistupují k informacím online prostřednictvím doménových jmen, například google.com. Webové prohlížeče komunikují prostřednictvím IP adres. Systém DNS převádí názvy domén na IP adresy, aby prohlížeče mohli načítat internetové zdroje. Proces překladu DNS zahrnuje převod hostitelského jména (google.com) na počítačovou IP adresu (8.8.8.8.). Převod probíhá „za oponou" a kromě počátečního požadavku nevyžaduje žádnou interakci ze strany uživatelova počítače (What is DNS?, © 2024). **IP adresa** chápeme jako jedinečnou adresu, která identifikuje zařízení na internetu nebo v místní síti. IP je zkratkou pro „Internet Protocol", což je soubor pravidel, jimiž se řídí formát dat odesílaných prostřednictvím internetu nebo místní sítě. Jsou identifikátorem, který umožňuje posílání informací mezi zařízeními v síti, které obsahují informace o poloze a zpřístupňují zařízení pro komunikaci. Jedná se o způsob, jak jsou na internetu rozlišovány různé počítače, směrovače a webové stránky. Adresy IP slouží právě k tomuto a tvoří základní součást fungování internetu (IP address definition, © 2024).

MAC adresa je unikátní identifikátor obsahující čísla a znaky každého síťového zařízení, přidělený výrobcem (Jirásek et al., 2022). **DHCP server** je síťový server, protokol, který automaticky poskytuje a přiděluje koncovým zařízením IP adresy, výchozí brány a další síťové parametry. Obvykle DHCP server přiděluje každému uživateli jedinečnou dynamickou IP adresu, která se průběžně mění (What is a DHCP Server?, © 2024).

Malware chápeme jako zkratku pro škodlivý software (malicious software). Je souhrnným označením pro pět nejčastějších typů malwaru, kterými jsou červi, trojské koně, spyware, adware a ransomware (What is Anti-Malware…, © 2024). **Antimalware** je **s**oftware sloužící k ochraně sítí a důležitých dat před malwarovými útoky. Používá tři základní techniky ochrany proti malwaru – monitorování chování, sandboxing (izolace a zkoumání potenciálně škodlivých souborů) a odstraňování škodlivého softwaru (What is Anti-Malware…, © 2024). **Antivirem** rozumíme reaktivní základní obranný mechanismus, který chrání zařízení před viry a škodlivými soubory, které nejsou výslovně identifikovány jako malware. Slouží spíše proti „zavedeným" virům, které jsou v oběhu již nějakou dobu a lze je snáze identifikovat (What is Anti-Malware…, © 2024).

Pásky jsou záložní systém, který není elektronickým archivem, ale naopak je systémem pro ochranu dat. Jsou využívány převážně jako mechanismus pro obnovu dat po havárii a zajištění kontinuity provozu (Jirásek et al., 2022). **Log** je záznam obsahující informace o činnostech v počítačovém systému. Jedná se o informace o tom, kdo k systému přistupoval, kdy k němu přistupoval, jaké soubory byly otevřeny a jaké změny byly provedeny. Slouží ke sledován výkonu, diagnostice chyb či identifikaci podezřelého chování. Správci systémů pomocí logů odhalují abnormální chování prostředí, díky čemuž jsou schopni pohotově řešit potenciální problémy a narušení (What is a Log in Computing?, © 2024).

Local Areal Network (LAN) je soubor zařízení propojených v jednom fyzickém místě, například v budově nebo kanceláři. Lokální síť může obsahovat od jednoho až k tisícům uživatelů. Propojuje zařízení, která se nacházejí v jedné omezené oblasti (What Is a LAN?, © 2024). **ICT** znamená informační a komunikační technologie zahrnující všechny technické prostředky používané ke zpracování informací a podpoře komunikace. Pojem zahrnuje jako počítačový a síťový hardware, tak i software (Glossary: Information and communication technology (ICT), © 2023).

SQL je zkratkou pro Structured query language neboli standardizovaný dotazovací jazyk, který je používán pro práci s daty v relační databázi (Jirásek et al., 2022). **SQL injection** je technika využívající bezpečnostní zranitelnost, které se nachází v databázové vrstvě aplikace (Jirásek et al., 2022).

Pojem **Systém generálního klíče** zahrnuje celkem čtyři druhy klíčů, cylindrické vložky, visací zámky i průmyslové zámky. Pro potřeby diplomové práce jsou definovány jen druhy klíčů. Prvním je **generální klíč**, čímž rozumíme takový klíč, který odemyká všechny dveře v takzvaném uzamykacím systému. **Hlavní skupinový klíč** pak odemyká dveře v rámci definované skupiny či podskupiny. **Skupinový klíč** pak odemyká dveře v rámci určené skupiny. **Vlastním klíčem** je umožněn přístup do konkrétních dveří (Princip systému, © 2024).

Kybernetickou bezpečnostní událostí chápeme takovou událost, která by mohla způsobit narušení bezpečnosti informací v informačních systémech, narušení bezpečnosti služeb nebo bezpečnosti a integrity sítí elektronických komunikací (Zákon č. 181/2014 Sb., o KB). **Kybernetický bezpečnostní incident** je naopak nastalá událost, která již způsobila narušení bezpečnosti informací v informačních systémech, narušení bezpečnosti služeb nebo bezpečnosti a integrity sítí elektronických komunikací (Zákon č. 181/2014 Sb., o KB).

3 KLÍČOVÉ PRVKY KYBERNETICKÉ BEZPEČNOSTI

Kapitola obsahuje vybrané aspekty kybernetické bezpečnosti, které jsou relevantní pro téma diplomové práce. Zabývá se triádou CIA, kde je nejprve definován rozdíl mezi daty a informacemi, následně jsou rozebrány jednotlivé prvky CIA, společně se zmínkou triády DAD. Následuje životní cyklus informací, kde jsou probrány jednotlivé podoby, kterých mohou data nabývat včetně jejich likvidace.

3.1 Triáda CIA

V rámci řízení kybernetické bezpečnosti často dochází k uplatnění takzvaných „triád kybernetické bezpečnosti“. Může se jednat například o „Prvky kybernetické bezpečnosti – lidé, technologie a procesy“, „Životní cyklus kybernetické bezpečnosti – prevence, detekce a reakce“ anebo o „CIA – Confidentiality, Integrity a Availability“. Právě triádě CIA se bude tato kapitola věnovat.

Jedná se o nejznámější a nejpoužívanější triádu kybernetické bezpečnosti. Pro komplexní kybernetickou bezpečnost sama o sobě není dostatečná bez využití dalších principů KB. Často se mluví o „Parkerian hexad“, což je v podstatě triáda CIA doplněná o další tři prvky: Possession/Control (držení/kontrola), Authenticity (autentičnost) a Utility (užitečnost).

Triáda CIA je zkratka pro tři původně anglická slova, jež jsou uvedená v úvodu této podkapitoly. V překladu *důvěrnost, celistvost* a *dostupnost*. Jejich konkrétní definice budou vysvětleny později, nejdříve je nutné si ujasnit **rozdíl mezi daty a informacemi**. V současnosti se v odborné literatuře objevuje, že definice informační bezpečnosti není dostačující a měla by být nahrazena pojem kybernetická bezpečnost. Informační bezpečnost se totiž zaměřuje na informace jako takové, tímto ale dochází k přehlédnutí důležitých prvků, které jsou podstatné pro správné uchopení bezpečnosti v kyberprostoru (Kolouch et al., 2019).

Pochopitelně je k dispozici nespočet definic dat a informací, pro potřeby této práce jsou vybrány definice, které jsou více nakloněné k problematice kybernetické bezpečnosti. **Daty** rozumíme prvky s informační hodnotou, se kterými pracuje počítačový systém, a které jsou následně zpracovány tak, aby vytvořili informaci.

Informace jsou potom chápány jako něco způsobilejšího, kompetentnějšího než data. Data se stávají informacemi, pokud jsou následně složena v tzv. „významnou“ informaci, lépe pochopitelnou pro lidi (Kolouch et al., 2019). Laicky řečeno by se dalo říct, že **data** jsou „jedničky a nuly“ a **informace** jsou poté „jedničky a nuly převedené do lidské řeči“.

Informace mohou mít několik podob, můžeme je dělit dle řady různých kritérií, například dle způsobu záznamu dat – písemné, obrazové, zvukové, audiovizuální nebo strojem čitelné, pod čímž si můžeme představit informace elektronické a digitální. Dalším dělením je dle odvozenosti obsahu – primární, sekundární a terciální, či podle kontinuity – periodické a neperiodické (Typologie dokumentů, © 2024).

Pokud bychom se v rámci informační bezpečnosti zaměřovali jen na informace, jednoduše by mohlo dojít k narušení bezpečnosti jako celku. V návaznosti na to je podstatné aplikovat **triádu CIA** na veškeré prvky kybernetické bezpečnosti, čímž můžeme chápat právě data, ale také počítačové systémy či fyzickou bezpečnost v kontextu ochrany prvků informačních a komunikačních technologií (Kolouch et al., 2019).

Důvěrnost, z anglického **Confidentiality**, vyjadřuje fakt, že k informacím či datům mají přístup jen ti, kteří přístup mít mají neboli ti, kteří jsou k tomu oprávnění. K dosažení důvěrnosti je zapotřebí uplatnit některou z klasifikací informací. Tyto certifikace lze uplatňovat i na další prvky KB a přístup k nim.

Klasifikací existuje spousta. Jednou z nich může být klasifikace dle zákona 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. Utajovaná informace se klasifikuje stupněm utajení:

- Přísně tajné – takto jsou klasifikovány informace, jestliže jejich vyzrazení neoprávněné osobě nebo zneužití může způsobit mimořádně vážnou újmu zájmům státu.
- Tajné – klasifikace tohoto stupně uvádí, že její vyzrazení neoprávněné osobě nebo zneužití může způsobit vážnou újmu zájmům státu.
- Důvěrné – tímto stupněm jsou označeny informace, jestliže vyzrazení neoprávněné osobě nebo zneužití může způsobit prostou újmu zájmům státu.
- Vyhrazené – stupněm tohoto charakteru jsou označeny informace, jestliže jejich vyzrazení neoprávněné osobě nebo zneužití může být nevýhodné pro zájmy státu (Zákon č. 412/2005 Sb., o ochraně utajovaných informací).

Další klasifikací informací je velmi rozšířený Protokol TLP neboli **Traffic Light Protocol**, který byl vytvořen s cílem usnadnit šíření informací. Je souborem označení, který slouží k zajištění sdílení citlivých informací s příslušným publikem. Používá čtyři barvy (pátá

je bez barvy) k označení očekávaných hranic sdílení, které má příjemce použít. TLP poskytuje jednoduché a intuitivní schéma pro označení, kdy a jak mohou být citlivé informace sdíleny, což usnadňuje častější a efektivnější spolupráci.

- Red – není určeno ke zveřejnění, vyhrazeno pouze pro účastníky.
- Amber + Strict – omezené zveřejnění, vyhrazeno organizaci účastníků.
- Amber – omezené zveřejnění, omezené na organizaci účastníků a její klienty.
- Green – omezené zveřejňování, vyhrazeno pro komunitu.
- Clear – zveřejnění není omezeno (Traffic Light Protocol (TLP) Definitions and Usage, © 2023).

Vyhláška o kybernetické bezpečnosti č. 82/2018 Sb. definuje v příloze stupnici důvěrnosti, které v podstatě přejímá pravidla TLP protokolu a sama na něj odkazuje.

- Nízká – veřejné přístupné nebo určena ke zveřejnění. Narušení důvěrnosti neohrožuje zájmy.
- Střední – veřejné nepřístupné. Ochrana není vyžadována žádným právní předpisem či smluvním ujednáním.
- Vysoká – veřejně nepřístupná, ochrana je vyžadována právními předpisy, jinými předpisy nebo smluvními ujednáními.
- Kritická – veřejně nepřístupná, vyžadují nadstandardní míru ochrany na rámec předchozí kategorie (Vyhláška č. 82/2018 Sb., o KB).

Celistvost, z anglického **Integrity**, je ve výkladovém slovníku kybernetické bezpečnosti definována následovně:

> *„Vlastnost přesnosti a úplnosti.“* (Jirásek et al., 2022)

Integrita dat je poté definována takto:

> *„Jistota, že data nebyla změněna. Přeneseně označuje i platnost, konzistenci a přesnost dat, např. databází nebo systémů souborů. Bývá zajišťována kontrolními součty, hašovacími funkcemi, samoopravnými kódy, redundancí, žurnálováním atd. V kryptografii a v zabezpečení informací všeobecně integrita znamená platnost dat.“* (Jirásek et al., 2022)

Integrita systému je definována:

> *„Kvalita systému zpracování dat plnicího svůj provozní účel a zabraňující přitom neautorizovaným uživatelům provádět změny zdrojů nebo používat zdroje a zabraňující autorizovaným uživatelům provádění nesprávných změn zdrojů nebo je nesprávně používat. Vlastnost, že systém vykonává svou zamýšlenou funkci nenarušeným způsobem, bez záměrné nebo náhodné neautomatizované manipulace se systémem.“* (Jirásek et al., 2022)

V konečném slova smyslu integrita znamená zabránění zásahu do informací, dat a dalších prvků ICT jinou než oprávněnou osobou. Integrita zaručuje, že systém nebude narušen neoprávněným zásahem. Je potřeba chápat skutečnost, že pokud by k narušení dat skutečně došlo, nemusí to být na první pohled znát a může trvat značnou dobu, než je narušení integrity odhaleno (Kolouch et al., 2019). Vyhláška o kybernetické bezpečnosti představuje vedle stupnice pro hodnocení důvěrnosti také stupnici pro hodnocení integrity:

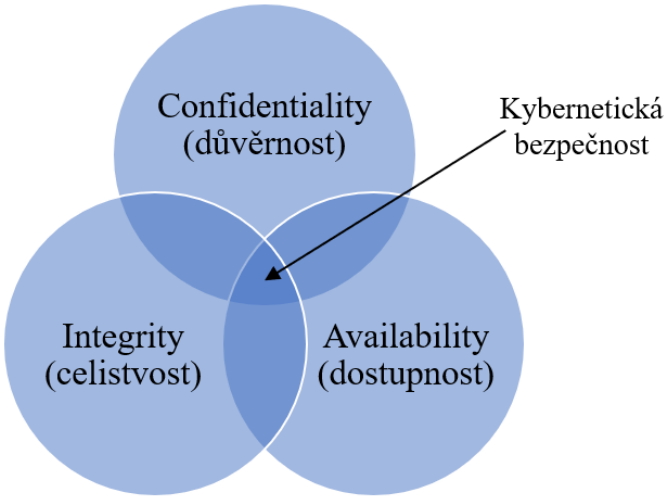
- Nízká – není vyžadována ochrana z hlediska integrity, narušení neohrožuje oprávněné zájmy.
- Střední – může vyžadovat ochranu z hlediska integrity, narušení může vést k poškození oprávněných zájmů a může se projevit méně závažnými dopady na primární aktiva.
- Vysoká – je vyžadována ochrana z hlediska integrity, narušení vede k poškození oprávněných zájmů s podstatnými dopady na primární aktiva.
- Kritická – je vyžadována ochrana z hlediska integrity, narušení vede k velmi vážnému poškození oprávněných zájmů s přísnými a velmi vážnými dopady na primární aktiva (Vyhláška č. 82/2018 Sb., o KB).

Dostupnost, z anglického **Availability**, znamená možnost přístupu v době, ve kterém je potřeba. Pokud by nebyl zajištěn přístup k datům, informacím či k samotnému systému ve chvíli kdy je to nutné, postrádalo by smysl mít zajištěnou celistvost a důvěrnost (Kolouch et al, 2019). Vyhláška definuje také stupnici pro hodnocení dostupnosti:

- Nízká – narušení dostupnosti není důležité a v případě výpadků je tolerováno delší časové období pro nápravu.
- Střední – narušení dostupnosti by nemělo překročit dobu pracovního dne, dlouhodobější výpadek vede k možnému ohrožení oprávněných zájmů.

- Vysoká – narušení dostupnosti by nemělo překročit dobu několika hodin, jakýkoli výpadek je nutné řešit neprodleně, protože vede k přímému ohrožení oprávněných zájmů.
- Kritická – narušení aktiva není přípustné, a i krátkodobá nedostupnost, v řádu několika minut, vede k vážnému ohrožení oprávněných zájmů (Vyhláška č. 82/2018 Sb., o KB).

Prostor kybernetické bezpečnosti v kontextu uplatnění triády CIA, si můžeme představit jako tři kružnice, kdy každá zastupuje jeden prvek triády CIA a jejich průnik je právě prostorem kybernetické bezpečnosti (Kolouch et al, 2019).



Obrázek 2 Triáda CIA a kybernetická bezpečnost

Kybernetická bezpečnost se v maximální míře snaží o funkčnost triády CIA. Útočníci se právě naopak snaží o triádu DAD, které vyjadřuje **Disclosure** neboli odhalení¸ **Alteration** neboli modifikace a v poslední řadě **Destruction** neboli zničení (Kybernetická bezpečnost, © 2024).

3.2 Životní cyklus informací

Informace by měly být patřičně zabezpečeny po celou dobu jejich životního cyklu (Information Lifecycle). Proto je potřeba pochopit tři základní stavy, kterými informace prochází během celé jejich existence. Těmito stavy jsou data v úložišti/v klidu (data at rest), data v pohybu/během přenosu (data in motion), data během používání (data in use). Během těchto procesů může docházet k narušení jejich důvěrnosti, integrity a dostupnosti (Informační bez-

pečnost: životní cyklus informace, © 2008–2023). Likvidace dat je nedílnou součástí životního cyklu informací. Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti stanovuje způsob likvidace dat, provozních údajů, informací a jejich kopií a likvidaci technických nosičů dat s ohledem na úroveň aktiv (Vyhláška č. 82/2018 Sb., o KB).

3.2.1 Data at Rest

Prvním stavem jsou *Data at Rest*, která v tuto chvíli bereme jako data neaktivní, což znamená, že se data nepohybují mezi zařízeními či sítěmi. Z důvodu uložení či archivování těchto dat jsou méně zranitelná než data v pohybu. Znamená to, že informace, které si společnosti uchovávají ve své blízkosti jsou hackery považovány za cennější a stávají se tak přitažlivějšími cíli pro vnější útoky. Data at rest jsou data fyzicky umístěna na počítačových datových úložištích v jakékoli digitální podobě, tím můžeme chápat cloudová úložiště, služby hostingu souborů, databáze, datové sklady, tabulky, archivy, pásky, zálohy mimo pracoviště nebo cloud, mobilní zařízení apod. Ochránit je můžeme bezpečnostním softwarem, firewally nebo použitím šifrování (Argintaru, © 2003–2023).

Data v klidovém stavu můžeme ochránit také souborem nástrojů a postupů, který se nazývá „Prevence ztráty dat“, z anglického „Data Loss Prevention“. Jedná se o součást celkové bezpečnostní strategie společnosti a zaměřuje se na odhalování a prevenci ztráty, úniku nebo zneužití dat v důsledku narušení, úniku přenosů a neoprávněného použití. Využití tohoto souboru nástrojů a postupů se stává stále více relevantnější, protože společnosti často využívají cloudovou infrastrukturu, tím pádem je ochrana citlivých dat stále náročnější (Boehm, © 2024).

Existují tři typy DLP. Prvním typem je síťové DLP, které sleduje a analyzuje síťovou aktivitu a provoz organizace v běžné síti a cloudu. Tím rozumíme monitorování e-mailů, zpráv a přenosů souborů, aby se zjistilo, kdy jsou kritická data odesílána v rozporu se zásadami zabezpečení informací organizace. Vytváří databázi, která zaznamenává, kdy je k citlivým nebo důvěrným datům přistupováno, kdo k nim přistupuje a případně, kde se data v síti pohybují. Poskytuje týmu, který se zabývá zabezpečením informací, kompletní přehled o všech datech v síti, včetně dat, která jsou používaná, v pohybu nebo v klidu.

Druhým typem je takzvaná DPL pro koncové body. Monitoruje všechny koncové body sítě, včetně serverů, cloudových úložišť, počítačů, notebooků, mobilních telefonů a dalších zařízení, na kterých jsou data používána, přesouvána či ukládána, aby se zabránilo úniku, ztrátě

nebo zneužití dat. Pomáhá při klasifikaci regulačních, důvěrných, vlastnických nebo kritických dat s cílem zefektivnit vykazování a požadavky na dodržování předpisů. Sleduje data uložená na koncových bodech v síti i mimo ni.

Třetím typem je Cloud DLP, což je určeno k ochraně organizací, které využívají cloudová úložiště pro ukládání dat. Prověřuje a kontroluje data v cloudu a automaticky detekuje a šifruje citlivé informace před jejich přijetím a uložením na cloudovém úložišti. Zároveň udržuje seznam autorizovaných cloudových aplikací a uživatelů, kteří mohou přistupovat k citlivým datům. Může upozorňovat tým zabezpečující informace na porušení zásad nebo anomální aktivity. Udržuje protokol o tom, kdy byl získán přístup k důvěrným datům v cloudu, a o identifikaci uživatele. Vytváří tak komplexní přehled o všech datech na cloudovém úložišti (Boehm, © 2024).

3.2.2 Data in Motion

Dalším stavem, který mohou data nabývat, jsou data v pohybu neboli *Data in Motion*, v některých zdrojích nazývané také *Data in Transit*. Těmito informacemi rozumíme takové informace, které putují z jednoho bodu do druhého. Příkladem může být e-mailová korespondence, nástroje pro spolupráci, služby pro okamžité zasílání zpráv a téměř všechny veřejné komunikační kanály. Vzhledem k dostupnosti prostřednictvím internetu nebo soukromé podnikové sítě při cestování z jednoho místa na druhé jsou tato data často méně bezpečná než neaktivní data. Z tohoto důvodu jsou přenášená data potenciálním cílem hackerů (Dinic, © 2024).

Ochrana dat v pohybu je jednodušší než ochrana dat v klidu, z důvodu, že zabezpečení dat pro internetová připojení je již po dlouhou dobu velkým problémem. Existují kompetentní protokoly, které blokují pokusy hackerů o útoky na data při přenosu. Zachycení dat při přenosu prostřednictvím internetu vyžaduje odborné technické dovednosti, kterými mnoha hackerů nedisponuje. Novější útoky, v tomto případě spíše podvody, spočívají ve vyzvědění přihlašovacích údajů od uživatelů, pomocí takzvaného sociálního inženýrství, kterému se mimo jiné věnuje následující kapitola.

Při ochraně dat v pohybu je pozornost věnována webovým transakcím, přenosům souborů a týmové spolupráci. Vzhledem ke skutečnosti, že komunikace je spojovacím článkem mezi aplikacemi, jsou problémy spojené se zabezpečením dat při přenosu úzce spjaty se správou dat v klidu. Úkol sledovat aktivitu pomocí protokolů a přísně definovat přístupová práva se rozprostírá napříč všemi prostředky v systému. Důležité je mít dostatečně zabezpečena

data v klidu, pokud se tak stane, většina úkolů potřebných k zabezpečení dat v pohybu je splněna (Cooper, © 2024).

Ochranu webových transakcí lze zabezpečit aktivací a spravování protokolu HTTPS pro všechna webová připojení. Po zavedení této bezpečnostní služby je zabezpečení webových transakcí v podstatě zajištěno. Pro zvýšení úrovně zabezpečení je nutné pravidelné skenování zranitelnosti webových aplikací, což zajistí, že hackeři nebudou mít možnost proniknout do klíčových systémů prostřednictvím veřejné webové sítě. Firewally webových aplikací mohou také zajistit stálou ochranu webových prostředků.

Pro zajištění ochrany při přenosu souborů není vhodné používání zastaralého protokolu FTP (File Transfer Protocol), který je sice osvědčený, ale nezajišťuje dostatečnou úroveň bezpečnosti. Pro přesun dat je vhodnější použít SFTP (Secure File Transfer Protocol) či FTPS (File Transfer Protocol – Secure). K lepší úrovni zabezpečení je vhodné také systémová dokumentace a skenování zranitelností, což poskytne informace o tom, kde není činnost přenosu souborů dostatečně chráněna.

Systémy týmové spolupráce vyžadují sílení informací. To vede k tomu, že stejná data jsou v klidu a zároveň v pohybu. Příkladem může být skupina lidí, která sdílí přístup ke stejnému dokumentu na Google Disku a přistupuje k němu prostřednictvím Dokumentů Google. Tento dokument je v klidu na serveru Google, jeho obsah se zároveň přenáší tam a zpět mezi serverem Google na prohlížeči lidí, kteří s ním pracují a aktualizují jej.

Tyto přenosy jsou zpravidla zabezpečeny HTTPS protokolem a zabezpečení dat v klidu je pokryto šifrováním účtu. Tato opatření ale neblokují neoprávněné zpřístupnění dat oprávněným uživatelům. Řešení DLP bude muset mít schopnost monitorovat cloudové prostředky i koncové body sítě (Cooper, © 2024).

3.2.3 Data in Use

Poslední stav dat se nazývá *Data in Use* neboli používaná data. Tím rozumíme data, ke kterým uživatelé aktivně přistupují a zpracovávají je. Jedná se o nejvíce zranitelnou fázi vůči datům, ať už jsou čtena, zpracovávána nebo aktualizována, protože jsou okamžitě k dispozici. Mohou tak být vystavena útoku nebo lidské chybě, což může mít v obou případech závažné důsledky. Pro ochranu tohoto typu dat má zásadní význam šifrování. Spousta společností doplňuje toto opatření o další, kterým může být ověřování či omezení přístupu k datům.

Vhodné je zavést ochranná opatření pro používaná data ještě předtím, než k nim kdokoli získá přístup. Neexistuje způsob, jak limitovat hackery v jejich činnosti po nabourání se k citlivým dokumentům. Důležité je také zvýšení úsilí o správu identity. Krádeže identity jsou stále častější záležitostí v kyberprostoru, zejména proto, že lidé sdílejí více osobních údajů než kdykoli předtím. Systémy správy identit pomáhají organizacím zajistit, že uživatelé jsou těmi, za které se vydávají, ještě předtím, než jim poskytnou přístup k jakýmkoli dokumentům a citlivým údajům (Dinic, © 2024).

3.2.4 Likvidace dat

Správce informačního a komunikačního systému je povinen stanovit taková pravidla mazání dat a způsobů likvidace technických nosičů informace, provozních údajů, informací a jejich kopií, která odpovídají požadavkům vyhlášky o kybernetické bezpečnosti. Pravidla musí být stanovena tak aby odpovídala hodnotě aktiv, především z hlediska důvěrnosti, typu a velikosti nosiče a jeho kapacitu. Ohled musí být brán také na to, kdo bude likvidaci provádět, zda bude zaměstnancem nebo dodavatelem. Mimo další zohledněné náležitosti, je nutné disponovat vyškoleným personálem a nástroji pro likvidaci.

Nosičem informace mohou být nejen tištěné dokumenty, psané poznámky a podobně, ale také mobilní zařízení, síťová zařízení (např. router), kancelářská vybavení jako tiskárny a scannery, magnetická média, kterými mohou být magnetické pásky, disky či HDD, optická média, jimiž rozumíme CD či DVD, elektronická média jako flash paměti a také outsourcing a cloude, jako například Google Disk. Každá kategorie nosičů informací je ve vyhlášce vyobrazena tabulkově společně s přípustnými způsoby likvidací dle úrovně důležitosti aktiva (Vyhláška č. 82/2018 Sb., o KB).

Existují tři způsoby likvidace dat, jimiž jsou odstranění, přepsání a fyzická likvidace nosiče informace. **Odstranění** se zakládá na likvidaci dat takovým způsobem, aby se stala pro systém nepřístupná. Jedná o například o vhození tištěného dokumentu do odpadkového koše či smazání datového souboru. Tato metoda je nejméně bezpečná. Pokud by bylo vynaloženo dostatečné úsilí lze data obnovit. Odstranění dat nelze využít v případě nosiče digitálních dat neumožňující opětovný zápis. Lze jej aplikovat jen v případě aktiv, která jsou v kontextu důvěrnosti identifikována jako ta s nízkým rizikem (viz kapitola 3.1 Triáda CIA).

Přepsání chráněné informace nahodilými hodnotami je středně bezpečným způsobem, jak data likvidovat. Běžně dostupná zařízení nejsou schopna obnovení přepsaných infor-

mací. Je vhodné tuto metodu kombinovat, popřípadě nahradit bezpečnou likvidací kryptografických klíčů k zašifrované informaci. Nelze použít pro poškozená média, média neumožňující opětovný zápis a pro média s vysokou kapacitou. Metodu lze uplatnit u aktiv identifikovaných s nízkou až kritickou úrovní důvěrnosti.

Nejbezpečnější metodou likvidace dat je **fyzická likvidace nosiče informace**, která je založena na destrukci, případně na rozebrání zařízení a následné destrukci nosiče informace. Může se jednat o mechanické, chemické nebo tepelné působení. Nosič není možné znova použít pro jeho prvotní účel a informace není možné za žádných okolností obnovit. Metodu fyzické likvidace lze využít u aktiv se střední až kritickou úrovní důvěrnosti (Vyhláška č. 82/2018 Sb., o KB).

4 KYBERNETICKÉ HROZBY SOUČASNOSTI

Kapitola se zabývá vybranými kybernetickými hrozbami současnosti, které jsou relevantní k tématu diplomové práce, potažmo k subjektu, na který je zaměřena praktická část práce.

4.1 Sociální inženýrství

Sociální inženýrství a útoky s nimi spojené nutí, bez nátlaku na oběť, sdílet s útočníkem informace, které by sdílet neměl, stahovat software, který je škodlivý, navštěvovat webové stránky, které by navštěvovat neměl, posílat útočníkovi peníze a další chyby, které mohou ohrozit oběť jako jednotlivce či celou organizaci. Sociální inženýrství používá spíše psychologickou manipulaci a využívá lidské chyby nebo slabé stránky, než technické či digitální zranitelnosti systému (What is social engineering?, © 2023).

Modelovou situací provedení útoku tohoto typu může být manažerka účtů v bance, která klientům refinancuje hypotéky, otevírá účty a řeší s nimi dluhy. Jednoho dne je manažerka zahlcena prací, když jí někdo zavolá. Jedná se o váženého klienta banky (později zjistíme, že se jedná o útočníka), který žádá o informace jedné ze svých transakcí. Říká, že je na dovolené na Arubě o čemž se zmínil, když spolu mluvili naposledy. Chce vědět, zda proběhla transakce, kterou dnes provedl. Manažerka si skutečně vzpomene, že se o tom klient zmiňoval, a tak se podívá na snímač telefonních hovorů a vidí, že číslo skutečně odpovídá číslu klienta a opravdu na jeho účtu proběhla transakce. Manažerka tedy odpovídá, že transakce proběhla v 9:31 ráno. Klient zdvořile poděkuje a telefon pokládá.

Situace by se mohla zdát naprosto v pořádku, bohužel manažerce volá ředitel banky a ptá se na neoprávněnou transakci na účtu klienta, se kterým hovořila. Došlo k tomu, že se někdo pokusil vybrat všechny peníze z účtu, naštěstí si neoprávněných transakcí skutečný klient všiml a zrušil je. Nebýt tohoto pohotového jednání skutečného klienta, mohlo vše dopadnout jinak. Manažerka banky se stala obětí útoku sociálního inženýrství, kdy má falešný klient důmyslnou počítačovou sestavu s několika nastavenými monitory a sleduje všechny své cíle v reálném čase a v podstatě si z nich utahuje, ale přitom je obírá o peníze. Jde o to, že si falešný klient vytvořil falešný účet pohledné ženy na Facebooku a delší dobu si psal se skutečným klientem banky, aby od něj získal potřebné informace, i když z počátku velmi nenápadné. Pak už jen stačilo použít tzv. „spoofing“, tedy skrývání informací o původci hovoru. Existuje stránka, na které si tuto službu lze zaplatit za pouhých 10 centů za minutu, a dokonce dokáže změnit i hlas volajícího (Lester Evans, 2019).

Než se falešný klient dovolal dotyčné manažerce, musel volat několika zaměstnancům banky, než konečně dostal přístup ke klientově účtu. A zde záleží právě na tom, aby byl útočník zdvořilý a trpělivý. Lidé pak v podstatě udělali všechno za něj. I kdyby si manažerka uvědomila, že mluví s hackerem, moc toho nezmůže, protože ve skutečnosti k žádné újmě nedošlo a útočník by mohl policii tvrdit, že šlo jen o žert.

Namísto dobrovolného poskytnutí informací mohla ale manažerka provést nenápadnou kontrolu identity. Nabídnout nesprávné informace a sledovat, zda ji volající opraví. Hovor například mohl proběhnout tak, že se manažerka zeptá: „Byla to ta transakce v 8:31 nebo 8:52?“ I když to nebyla ani jedna z nich. Útočník v tu chvíli vymýšlí nejlepší postup a uvědomuje si, že mlčení může vypadat podezřele, a tak rychle odpovídá „To druhé.“ a pozorně naslouchá, jestli se objeví nějaká reakce. Manažerka si již uvědomuje, že má pravděpodobně co do činění s hackerem a dál se ptá na tyto nenápadné otázky.

Pokud by byl personál vyškolen k těmto kontrolám totožnosti, může daného útočníka zaměstnat, dokud to nevzdá, což je ideální řešení – aniž by zaměstnanci zapojili policii, vyvolali poplach nebo zvýšit hlas, útočníkovi pomalu dochází, že zločin se nevyplácí a rozhodne se s útoky skončit (Lester Evans, 2019).

Jak již bylo řečeno, dle Zprávy o stavu kybernetické bezpečnosti ČR za rok 2022 je nejčastějším kybernetickým útokem phishing. **Phishing** je kybernetický trestný čin, při kterém jsou cíle kontaktovány e-mailem, telefonicky nebo textovou zprávou někým, kdo se vydává za legitimní instituci s cílem vylákat citlivé údaje. Může se jednat o osobní identifikační údaje, bankovní údaje, údaje o kreditní kartě a hesla. Tyto informace jsou pak zpravidla použity k přístupům k účtům a mohou vést ke krádeži identity a finanční ztrátě (What is Phishing?, © 2024).

Existuje mnoho druhů phishingu, ať už se jedná o klasický e-mailový phishing, který je rozesílán velkému množství uživatelů hromadně, spear phishing, kdy útočník předem sbírá potřebné informace o jeho cíli, přes whaling, jehož cílem jsou vrcholoví manažeři a majitelé firem. Opakem whalingu je CEO fraud, což jsou zprávy, které vypadají jako by je posílali právě vysoce postavení manažeři zaměstnancům organizace.

Možným phishingovým útokem je také vishing, což je podvodný telefonát. Útočníci k provedení toho útoku využívají předem namluvené a následně automaticky přehrávané zprávy. Jedná se o princip, který je popsán v této kapitole v části o sociálním inženýrství. Další mož-

nou variantou je smishing, známý také jako SMS phishing. Jak název napovídá, útok je proveden pomocí SMS zprávy, která se snaží majitele telefonu přimět ke kliknutí na závadný odkaz, či ke kontaktování organizace, za kterou se útočník vydává.

Page hijacking funguje tak, že útočníci vytvoří téměř totožnou webovou stránku, která se začne v internetové vyhledávači zobrazovat před původní, legitimní webovou stránkou a nenásilně tak donutí uživatele navštívit jejich závadné stránky. Další formou je catfishing, kdy si útočník vytvoří neexistující identitu, zpravidla na sociálních sítích. Jeho cílem může být zostuzení oběti, kyberšikana či navázání vztahu za účelem finančního zisku (Phishing, © 1992–2024). Novým typem phishingu je takzvaný quishing, který k útoku využívá QR kód, kdy se uživatel po načtení může ocitnout na stránce, která po něm bude vyžadovat přihlašovací údaje a tím je útočníci získají (Quishing – vylepšená forma phishingu, © 2024).

4.2 Malware

Zpráva o stavu kybernetické bezpečnosti ČR zmiňuje narůstající trend ransomware útoků, konkrétně **ransomware jako službu** (ransomware-as-a-service – RaaS). Jedná se o obchodní model mezi provozovateli ransomwaru a přidruženými společnostmi. Společnosti platí za zprostředkování ransomwarových útoků vyvinutých provozovateli. Společnosti, které si tuto službu platí nemají potřebné dovednosti či čas na vlastní vývoj ransomwaru, proto tuto službu využívají pro svůj prospěch tím, že takto poškodí konkurenci. Takovouto službu mohou zakoupit na dark webu, kde jsou inzerovány podobným způsobem, jakým je inzerováno zboží na legálním internetu (What is Ransomware as a Service…, © 2024).

Mobile malware je typ škodlivého softwaru, který je speciálně určen pro mobilní zařízení. Bývá používán k různým poškozujícím činnostem, jako je krádež osobních údajů zásah do nastavení zařízení nebo zasílání podvodných zpráv. K napadení mobilním malwarem může dojít například tehdy, když si uživatelé stáhnou aplikace z nedůvěryhodných zdrojů, navštíví na zařízení škodlivé webové stránky nebo kliknou na textovou zprávu, která je škodlivým phishingem.

Útočníci mohou mobilní malware využít ke sledování aktivit uživatelů a údajů o jejich poloze, zobrazování nežádoucích reklam a krádeži důvěrných informací, které jsou v zařízení uloženy. V zájmu ochrany soukromí osobních a firemních informací by měli uživatele při stahování aplikací, návštěvě webových stránek a připojování k veřejným Wi-Fi dbát zvýšené opatrnosti. Bezpečnostním opatřením může být pravidelná aktualizace operačního sys-

tému a vyhýbání se stahování pochybného obsahu, čímž mohou značně snížit riziko úspěšného útoku. Ve firemním prostředí je vhodné nechat koncové uživatele mobilních zařízení absolvovat školení o kybernetické bezpečnosti, aby věděli, jak rozpoznat případnou podezřelou aktivitu na svých zařízeních a v návaznosti na to ji nahlásit bezpečnostnímu týmu, popřípadě oddělení informačních technologií.

Bezpečnostní rizika, které mobilní malware představuje mohou být pro informační bezpečnost firmy zásadní. Aby bylo dosaženo snížení rizika vystavení se tomuto typu hrozby a ochránili mobilní zařízení svých zaměstnanců, je vhodné zavést komplexní správu mobilních zařízení neboli Mobile Device Management a školení o bezpečnostním povědomí.

Mobile Device Management umožňuje podnikům spravovat a zabezpečovat jejich mobilní zařízení a správci IT tak mohou prosazovat zásady, monitorovat používání a bezpečně nasazovat aplikace na všech koncových zařízeních (How to protect mobile devices …, © 2003 – 2024).

4.3 Nové perspektivy a nebezpečí

Internet věcí, z anglického Internet of Things, je v současné době stále více se rozvíjející trend. Jedná se o fyzickou síť objektů (věcí), které jsou vybaveny senzory, softwarem a dalšími technologiemi za účelem propojení a výměny dat s jinými zařízeními a systémy prostřednictvím internetu (What is IoT?, © 2023), a to je ten hlavní problém – přístup k internetu – to znamená, že hackeři z jakéhokoli místa na světě mohou přistupovat k těmto „věcem“ stejně snadno jako majitel a dělat s nimi co se jim zlíbí.

Zařízení s připojením k internetu jako jsou kamery a teploměry, mohou být také předmětem kryptografického útoku. Skupina „White hat“, což jsou etičtí hackeři, úspěšně provedla kryptojacking nejprodávanější bezdrátové kamery na Amazonu. Po otevření kamery a připojení vlastního hardwaru k ní se ukázal účet správce chráněný heslem. Heslo bylo prolomeno hrubou silou za 15 vteřin, obsahovalo osm nul.

Nejjednodušším a velmi účinným opatřením je změna výchozího uživatelského jména a hesla, kterou většina uživatelů nikdy nezmění. Podobně je tomu tak i u Wi-Fi routeru (Lester Evans, 2019).

V současnosti je stálé omílaným tématem **umělá inteligence**, která je pomocníkem v mnoha oblastech, od velkoobjemových počítačových úloh, které jsme kdysi dělali manuálně, přes získávání dat a informací až k využití v oblasti medicíny, kde lze díky technice umělé

inteligence založené na hlubokém učení a rozpoznávání objektů použít k přesnějšímu určení rakoviny na lékařských snímcích (Artificial Intelligence, © 2024). Mimo významné příležitosti, které nám jako společnosti umělá inteligence přináší, bychom měli mít stále na paměti mnohá potenciální rizika a problémy, které s ní přicházejí. Příkladem může být předpojatost a diskriminace, kdy mohu systémy umělé inteligence neúmyslně udržovat nebo posilovat společenské předsudky v důsledku neobjektivních tréninkových dat nebo návrhu algoritmu. Abychom tomuto předešli, bylo by vhodné investovat do vývoje nezaujatých algoritmů a rozmanitých souborů tréninkových dat (Marr, © 2024).

Obavy plynou také z ochrany soukromí, neboť technologie umělé inteligence často shromažďují a analyzují velké množství osobních údajů. V této oblasti se diskutuje o zasazení přísných předpisů na ochranu údajů a bezpečné postupy při nakládání s daty. Technologie umělé inteligence se stávají stále sofistikovanějšími, čímž rostou bezpečnostní rizika spojená s jejich používáním. Hackeři mohou využít sílu těchto technologií k vývoji pokročilejších kybernetických útoků, obcházení bezpečnostních opatření a zneužívání zranitelností systémů. Může dojít k vzestupu autonomních zbraní poháněných umělou inteligencí, což vyvolává obavy z možnosti, že tuto technologii mohou použít státní i nestátní aktéři, zejména ve chvíli, kdy vezmeme v potaz potenciální ztrátu lidské kontroly nad kritickými rozhodovacími procesy. Abychom se tomuto vyhnuli, je nutné, aby vlády a organizace vypracovali osvědčené postupy pro bezpečný vývoj a nasazení umělé inteligence a podpořili mezinárodní spolupráci s cílem zavést globální normy a předpisy, které chrání před bezpečnostními hrozbami umělé inteligence.

V neposlední řadě je velkým problémem umělé inteligence šíření dezinformací a manipulací. Je nesmírně jednoduché vygenerovat obsah za pomocí umělé inteligence, který má charakter deepfake, což přispívá k šíření nepravdivých informací a manipulací s veřejným míněním. Některé zdroje uvádí, že systémy umělé inteligence, jež jsou využívány pro šíření dezinformací na internetu, mají potenciál stát se hrozbou pro demokracii a nástroj extremistické ideologie. Tyto taktiky mohou podkopat společenskou důvěru a manipulovat lidmi za účelem ekonomického zisku či politického prospěchu (Marr, © 2024).

5 DÍLČÍ ZÁVĚR

V teoretické části práce byla stručně shrnuta témata, která jsou podstatná pro správné uchopení záměru diplomové práce. Nejprve byla přiblížena oblast ochrany obyvatelstva od vývoje pojmu, přes stručné vymezení právního prostředí k bezpečnostním dokumentům týkající se této oblasti. Pomocí Bezpečnostní strategie České republiky z roku 2023 došlo k propojení tématu ochrany obyvatelstva a kybernetické bezpečnosti, kdy je zřejmé, že téma KB je skloňováno více než kdy předtím.

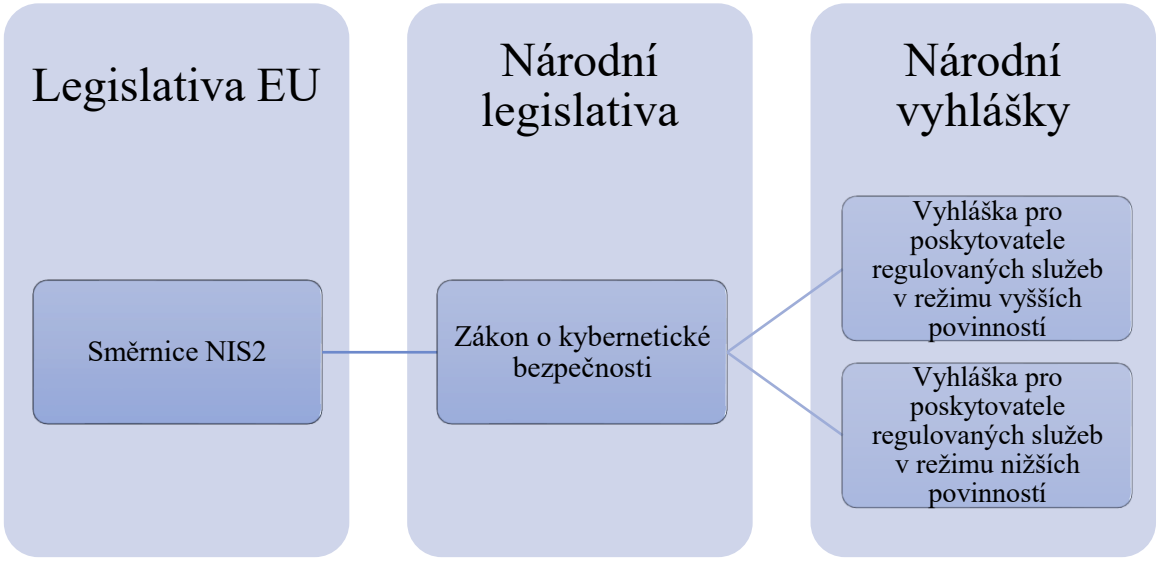
Část o kybernetické bezpečnosti je zaměřena na právní prostředí, důležité koncepční dokumenty a instituce, které jsou v problematice KB zainteresovány. V propojení v kybernetickou bezpečnostní je popsána triáda CIA a následně životní cyklus informací. Poslední částí jsou kybernetické hrozby současnosti, které mohou mít závažný dopad na organizace či celou společnost, pokud by byly použity ve větším měřítku.

Protože je téma kybernetické bezpečnosti velmi obsáhlou problematikou, obsahuje teoretická část jen vybrané základní informace z dané oblasti pro potřeby diplomové práce.

II. PRAKTICKÁ ČÁST

6 POPIS SOUČASNÉHO STAVU VYBRANÉHO SUBJEKTU

Kapitola je vytvořena na základě sběru dat a informací, analýzy a řízených rozhovorů s vybranými pracovníky, kteří v subjektu působí na různých pracovních pozicích (viz Příloha I). Subjekt si přeje zachovat anonymitu především z bezpečnostních důvodů. V úvodu kapitoly je krátce popsán subjekt, tak aby byla anonymita co nejvíce zachována. V další části se nachází samotná analýza současného stavu, která je strukturovaná podle nového zákona o kybernetické bezpečnosti, který v současnosti podléhá legislativnímu procesu, nicméně již nyní je k nahlédnutí pravděpodobné znění. Na základě tohoto je kapitola strukturována dle části „Stanovení rozsahu řízení kybernetické bezpečnosti“. Zákon dělí poskytovatele regulovaných služeb na poskytovatele s vyšší povinností a poskytovatele s nižší povinností. Subjekt spadá právě pod poskytovatele s nižší povinností, tudíž nejsou bezpečnostní opatření rozdělena na organizační a technická, jako je tomu u poskytovatelů s vyšší povinností, ale jsou sloučena. Kapitola je zpracována také na základě vznikající Vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností, která je taktéž k nahlédnutí a přímo souvisí s částí „Stanovení rozsahu řízení kybernetické bezpečnosti“.



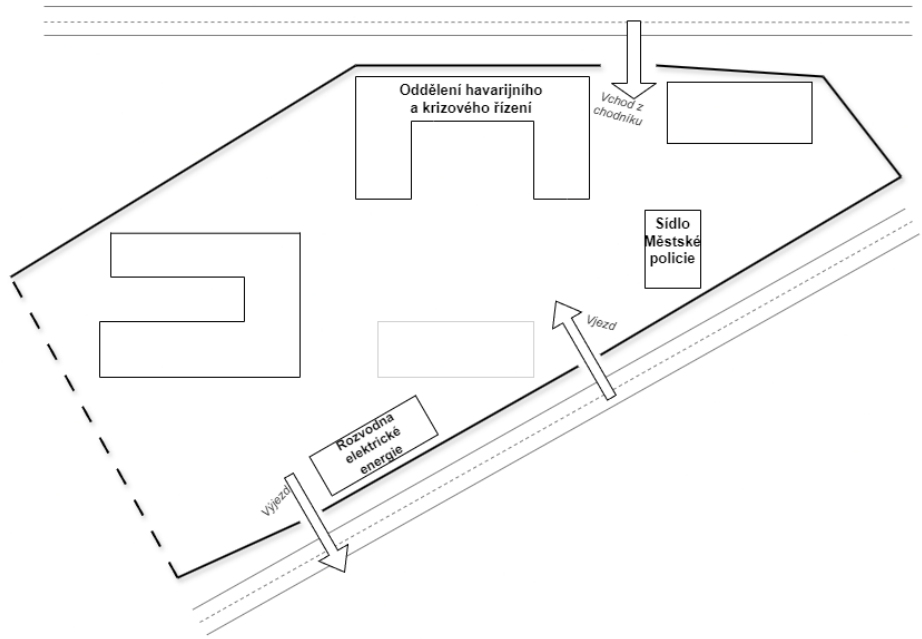
Obrázek 3 Struktura zákona a vyhlášek dle posledního návrhu NÚKIB (vlastní dle Evropská směrnice NIS2…, © 2024)

6.1 Charakteristika vybraného subjektu

Subjekt, který byl vybrán pro analýzu životního cyklu informací v prostředí ochrany obyvatelstva, je takový subjekt, který nakládá s osobními údaji a citlivými informacemi, nejen v oblasti OO, ale nachází se zde také oddělení havarijního a krizového řízení, kde je činnost

zaměřena na plnění úkolů ochrany obyvatelstva, jimiž rozumíme varování, evakuaci, ukrytí a nouzové přežití. Mimo jiné poskytují podklady HZS při zpracování havarijního plánu kraje. Protože se jedná o město s více než 50 tisíci obyvateli, má pod sebou tento subjekt osm městských části, ve kterých zajišťuje ochranu obyvatelstva.

V areálu subjektu i mimo něj se nachází celkem osm budov, kdy má každá z nich své zaměření. V jedné z budov sídlí i Městská policie (viz Obrázek 4). Mimo hlavní areál se ve vzdálenosti přibližně jednoho kilometru nachází čtyři místa, ve kterých úřad sídlí, které jsou také součástí subjektu. Protože se oddělení havarijního a krizového řízení nachází v hlavním areálu, kde jsou dislokovány čtyři budovy, analýza se týká především tohoto areálu. V areálu, na který je analýza zaměřena, se mimo čtyř budov, ve kterých subjekt sídlí, nachází také rozvodna elektrické energie (viz Obrázek 4).



Obrázek 4 Přibližný nákres hlavního areálu subjektu (vlastní)

Po levé straně od vjezdu se nachází budova, která není součástí subjektu (viz Obrázek 4). Budova je vyznačena z důvodu dalšího využití obrázku v následujících částech práce.

Směrnice NIS2, která v současné chvíli prochází implementací do nového zákona o kybernetické bezpečnosti bude zahrnovat i vybraný subjekt. V současné chvíli se na její zavedení již připravují, nicméně v současnosti pod zákon o kybernetické bezpečnosti nespadají. Ve většině oblastí se ale chovají tak, jako by pod něj spadali (Respondent č. 1, 23. 1. 2024).

6.2 Bezpečnostní opatření

Jak již bylo uvedeno, subjekt bude zařazen mezi poskytovatele regulovaných služeb s nižší povinností. V následující části je respektována struktura nového zákona o kybernetické bezpečnosti, společně s vyhláškou o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností. Struktura je sice respektována, nicméně dochází k prolínání jednotlivých oblastí, tudíž nelze přesně strukturu dodržet. Oba předpisy v současné chvíli prochází legislativním procesem. Za každou z následujících kategorií se nachází checklist, který shrnuje jednotlivé části společně s návrhem, jak dané položky vylepšit. Návrhy jsou dále rozpracovány v kapitole „Návrhy opatření".

Zajišťování kybernetické bezpečnosti

Prevence úniku dat je zabezpečena pomocí firewallů, nástrojem Application Delivery Controller (dále jen ADC), antiviry, antispamy a web filteringem. Monitoring toků v síti probíhá za pomoci Flowmon (Respondent č. 2, 31. 1. 2024). ADC je účelovým zařízením, které se využívá ke zlepšení výkonu, zabezpečení a odolnosti aplikací doručovaných přes web. Je schopen vyvažovat zatížení připojení a optimalizovat jej. Uplatňuje zásady zabezpečení a blokuje napadení (What is an application delivery controller?, © 2024). Pro ochranu koncových zařízení uživatele dodržují zaměstnanci desatero základních bezpečnostních pravidel, které je určeno všem zaměstnancům úřadu i Městské policii (Respondent č. 1, 23. 1. 2024).

Pokud v subjektu dochází k přerozdělování zařízení, například při výměně notebooků na vyšších úrovních a následném předání starších modelů zaměstnanců na nižších pozicích, je tato činnost na odpovědném pracovníkovi, který má na starosti koncové stanice. Ten kompletně vyčistí zařízení pomocí Eraseru a teprve poté se mohou zařízení přesunou na jiné pozice. Stává se, že jsou zařízení přidělována Hasičskému záchrannému sboru nebo jsou používána ve školských zařízení (Respondent č. 2, 31. 1. 2024).

V pracovních smlouvách je jen obecně zahrnuta odpovědnost za informační bezpečnost. Zaměstnanci očekávají, že mohou nastat kontroly z pozice zaměstnavatele. Nejsou uzavřeny samostatné dohody o mlčenlivosti, nicméně v pracovních smlouvách je tento požadavek řešen. Závazek týkající se mlčenlivosti není nijak přezkoumávám, požadavky jsou uvedeny tak obecně, že jsou používány dlouhodobě.

Pokud jsou uzavírány smlouvy s jinými zainteresovanými stranami, než jsou samotní zaměstnanci, požadavek na důvěrnost a mlčenlivost je ve smlouvě uveden. Pokud by smluvní

strana jakýmkoli nepřípustným způsobem nakládala s informacemi, byla by sankciována a okamžitě by došlo k vypovězení smlouvy (Respondent č. 1, 23. 1. 2024).

Aktualizace jak na počítačích, tak na mobilních telefonech jsou vynucené. Slouží pro to několik nástrojů. Pravidelné aktualizace jsou zavedeny jen u kritických serverů. Zodpovědný pracovník provádí aktualizace pomocí Windows Server Update Services. Microsoft vydává každé druhé a čtvrté úterý v měsíci záplaty pro své operační systémy. Nekritické servery, čímž rozumíme například měřič vlhkosti či teploty, se neaktualizují pravidelně. U mobilních telefonů se aktualizuje ihned, jakmile Mobile Iron aktualizaci vydá. Vynucené aktualizace probíhají především podle potřeby, pravidelná aktualizace je zavedena na koncových zařízeních každé úterý, kdy je zaměstnanci nechávají přes noc v provozu. Proběhne kompletní sken antivirem a následně jsou zařízení aktualizována. BIOS je zaheslován na každém koncovém zařízení. Bootování z externích zařízení je na koncových stanicích zakázáno.

Koncová zařízení uživatele jsou mimo silných hesel chráněna pomocí Microsoft System Center Configuration Manager. Péči o koncová zařízení zajišťuje Bitdefender. Komunikace citlivých věcí po síti probíhá jen na privátní Wi-Fi. Pro návštěvy úřadu je k dispozici Wi-Fi pro návštěvy. Zabezpečení Wi-Fi je řešeno centrálně pomocí CISCO, které centrálně ovládá přibližně třicet Access Pointů (dále jen „AP“) Wi-Fi pomocí CISCO kontrolérů, pomocí kterých ovládají právě AP Wi-Fi. Jsou schopni zjistit kolik je připojených uživatelů, z jakých zařízení a podobně. Konkrétní Wi-Fi jsou poté zabezpečeny pomocí WPA 2 (Respondent č. 2, 31. 1. 2024).

Tabulka 1 Checklist pro kategorii „zajišťování kybernetické bezpečnosti“ (vlastní)

Checklist – zajišťování kybernetické bezpečnosti			
Pořadové číslo	**Otázka**	**Odpověď**	**Navrhovaná opatření**
1.	Je zabezpečena prevence úniku dat?	✓	×
2.	Probíhá monitoring toků v síti?	✓	×
3.	Ochrana koncových zařízení z hlediska uživatele je řešena desaterem základních bezpečnostních opatření?	✓	×
4.	Dodržují uživatelé při změně hesel předepsaná pravidla?	✓	×
5.	Jsou stanoveny přesné postupy pro případ přerozdělování zařízení v rámci subjektu?	✓	×

Checklist – zajišťování kybernetické bezpečnosti			
Pořadové číslo	**Otázka**	**Odpověď**	**Navrhovaná opatření**
6.	Je ve smlouvách řešena povinnost mlčenlivosti?	✓	×
7.	Je pravidelně přezkoumávám závazek o mlčenlivosti?	✘	Zavést pravidelné přezkoumávání dohod o mlčenlivosti.
8.	V případě uzavření smlouvy s jinými zainteresovanými stranami, je uveden požadavek na důvěrnost a mlčenlivost?	✓	×
9.	V případě nedodržení požadavků ze strany smluvních dodavatelů, bylo by toto sankciováno a následně by došlo k vypovězení smlouvy?	✓	×
10.	Probíhají pravidelné aktualizace kritických serverů?	✓	×
11.	Probíhají pravidelné aktualizace nekritických serverů (měřič vlhkosti, teploty)?	✘	Zavést pravidelné aktualizace nekritických serverů.
12.	Jsou aktualizace koncových zařízení vynucené?	✓	×
13.	Probíhají pravidelné aktualizace koncových zařízení?	✓	×
14.	Probíhá před aktualizací kompletní sken pomocí antivirového programu?	✓	×
15.	Je BIOS zaheslován na každém koncovém zařízení?	✓	×
16.	Je zakázáno bootování z externích zařízení?	✓	×
17.	Jsou koncová zařízení uživatele chráněna i jiným způsobem, než jsou silná hesla?	✓	×
18.	Je zajištěna péče o koncová zařízení pomocí Bitdefender?	✓	×
19.	Je centrálně řešeno zabezpečení Wi-Fi?	✓	×
20.	Jsou jednotlivé AP Wi-Fi zabezpečena šifrováním pomocí WPA 2?	✓	×

V rámci kategorie zajišťování kybernetické bezpečnosti byly zjištěny celkem dva nedostatky, kterým je potřeba věnovat pozornost v kapitole s návrhy opatření.

Povinnosti vrcholového vedení

Vrcholové vedení subjektu tvoří vedení města, a to z důvodu, že se jedná o subjekt úřední povahy. Vrcholovým vedením je primátor, první náměstek primátora, náměstek primátora, uvolněný radní a tajemník úřadu. Vedení podstupuje školení v oblasti kybernetické bezpečnosti, na což jsou pravidelně vynakládány finanční prostředky. Povinnosti vrcholového vedení nejsou právně stanoveny. Na kybernetické bezpečnosti se podílí především odbor informatiky společně s bezpečnostním manažerem a dalšími stanovenými osobami (Respondent č. 1, 23. 1. 2024).

Tabulka 2 Checklist pro kategorii „povinnosti vrcholového vedení“ (vlastní)

Checklist – povinnosti vrcholového vedení			
Pořadové číslo	**Otázka**	**Odpověď**	**Navrhovaná opatření**
1.	Je stanoveno vrcholové vedení?	✓	×
2.	Postupuje vedení školení v oblasti kybernetické bezpečnosti?	✓	×
3.	Jsou právně stanoveny povinnosti vrcholového vedení?	✘	Právně stanovit povinnosti vrcholového vedení.

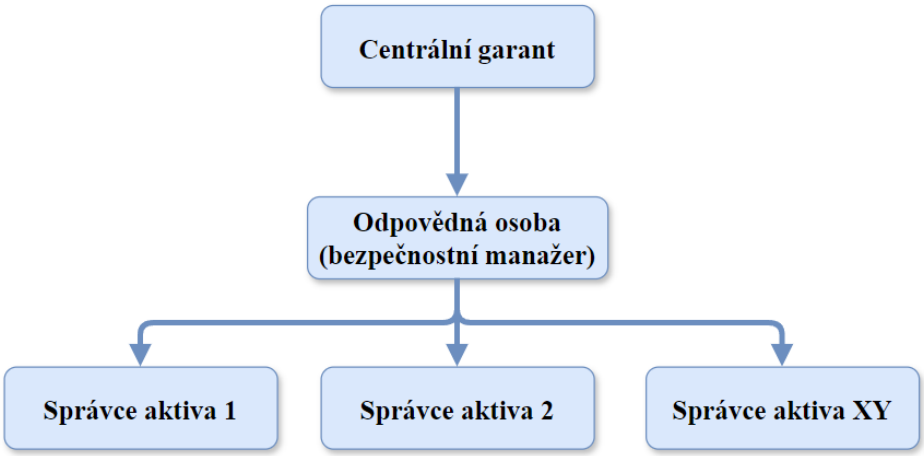
Na základě provedené analýzy bylo zjištěno, že nejsou právně stanoveny povinnosti vrcholového vedení, což může zapříčinit, že vrcholové vedení nebude schopno adekvátně reagovat na vzniklé kybernetické bezpečnostní incidenty.

Řízení aktiv

Seznam aktiv byl subjektem zpracován před mnoha lety. V návaznosti na novou směrnici NIS2 a její implementace do českého právního prostředí bude seznam aktiv aktualizován. Každé aktivum má svého vlastníka, který by se měl o aktivum náležitě starat. Některá aktiva budou propojena. Zde už se nejedná o činnost na základě nového zákona o KB, nýbrž aby bylo dosaženo větší logiky. Aktiva budou vytvářena pro celý proces. Spisová služba bude zahrnovat veškerá aktiva od serveru přes systémy a každé dílčí aktivum bude mít svého vlastníka, zastřešovat je bude centrální garant.

V rámci administrace chráněných aktiv je určena odpovědná osoba, bezpečnostní manažer, který zastřešuje tyto úkony, ale nelze zajistit jeho přítomnost u každého dílčího úkonu. Proto je vždy určen správce konkrétního aktiva, podle funkce a typu aktiv. Tento člověk je náležitě

vzdělán ke svým úkonům. Hierarchii administrace chráněných aktiv si můžeme představit následovně:



Obrázek 5 Hierarchie administrace chráněných aktiv (vlastní)

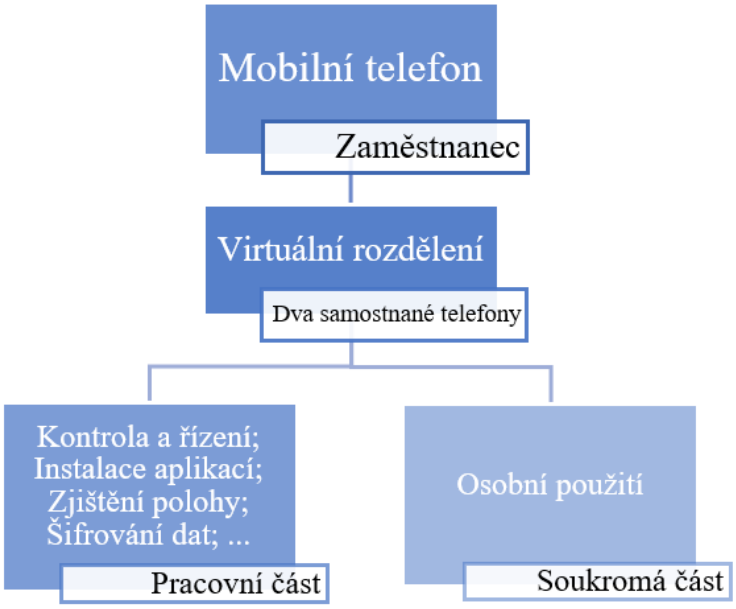
Některá aktiva jsou považována za primární. Tato má subjekt v plánu ošetřovat ve smlouvách i dodatcích, pravděpodobně také s poskytovateli některých aktiv. Důraz je kladen na mailovou službu, webové stránky, komunikaci s ministerstvy. Některé činnosti musí být řešeny prioritně. Výpadek webové služby na pár hodin je zanedbatelný, pokud by se jednalo o výpadek na několik dní, už by to problém představovalo. Servisní organizace, se kterými jsou uzavřeny smlouvy, musí reagovat do určitého času, v některých případech se jedná o vteřiny, jindy o minuty a hodiny (Respondent č. 1, 23. 1. 2024).

Při spravování dokumentů, čímž rozumíme příjem, označování, třídění, evidence, předávání, vyřizování dokumentů a spisů, podepisování a parafování dokumentů a také archivace dokumentů a spisů, vyřazování a následná **likvidace** dokumentů či spisů se subjekt řídí zákonem č. 499/2004 Sb., o archivnictví a spisové službě a vyhláškou č. 259/2012 Sb., o podrobnostech výkonu spisové služby. Tyto právní předpisy řeší především fyzické dokumenty a v menší míře elektronickou podobu dokumentů, nikoli však jiné nosiče informací, kterými mohou být optická média, síťová média či elektronická média jako jsou flash paměti.

Skartační řízení probíhá ve spolupráci se Státním okresním archivem a Národním digitálním archivem prostřednictvím portálu Národního digitálního archivu s krátkou osobní konzultací archivářů Státního okresního archivu přímo ve spisovně subjektu. Po obdržení souhlasu těchto dvou institucí proběhne fyzické i elektronické předání vybraných archiválií a se souhlasem následně také likvidace již nepotřebného materiálu, kdy proběhne tzv. mobilní skartace certifikovanou společností přímo ve spisovně úřadu. Likvidace datových nosičů,

jako je CD, DVD, USB flash disk je realizována ve Spalovně nebezpečných odpadů (Respondent č. 4, 22. 3. 2024).

Někteří zaměstnanci pracují z domova za pomoci mobilního telefonu. Tato aktiva jsou chráněna pomocí softwarového nástroje Mobile Iron, což zapříčiní virtuální rozdělení telefonu na dva samostatné. Na prvním je možné provádět kontrolu, instalovat potřebné aplikace na dálku, zjistit polohu telefonu a je zabezpečen šifrováním. Druhý virtuální telefon slouží jako soukromá část, se kterou lze nakládat jako s osobním telefonem, k tomuto nemají nadřízení přístup. Nástroj Mobile Iron není využíván oddělením havarijního a krizového řízení i přes to, že mají pracovní mobilní telefony, na které mimo jiné pořizují záznamy z míst zásahu a komunikují s nimi s dalšími zainteresovanými osobami. V minulosti vlastnili pracovně nazývané „protiatomové“ mobilní telefony. Tento název je užíván z důvodu vysoké fyzické odolnosti vůči vnějším vlivům, nebyly však chráněny z pohledu informační bezpečnosti. Tyto mobilní telefony byly nahrazeny klasickými chytrými telefony, které nejsou žádným způsobem zabezpečeny.



Obrázek 6 Virtuální rozdělení mobilního telefonu (vlastní)

Zajištění všech prvků triády CIA z hlediska správné údržby je dáno předepsanými parametry. Jedním z úkonů ke splnění parametrů bylo zazdění okna v serverovně. Téměř nikdo do serverovny nechodí, tudíž se zde prach prakticky nevyskytuje. Nicméně, pokud je potřeba, pracovníci úklidu sem vstupují pod dohledem oprávněné osoby.

Fyzická kontrola serverovny probíhá jednou až dvakrát týdně. Na dveřích se nachází magnetické kontakty, které zaznamenávají, že došlo k otevření dveří. Data se ukládají do databáze s historií několika let. Vstup do serverovny je na čip, který má k dispozici jen odbor informatiky (Respondent č. 2, 31. 1. 2024).

Tabulka 3 Checklist pro kategorii „řízení aktiv“ (vlastní)

Checklist – řízení aktiv			
Pořadové číslo	**Otázka**	**Odpověď**	**Navrhovaná opatření**
1.	Zpracován aktuální seznam aktiv?	✘	Aktualizovat seznam aktiv v návaznosti na NIS2.
2.	Má každé aktivum svého vlastníka?	✓	×
3.	Je ustanovena odpovědná osoba v rámci administrace chráněných aktiv?	✓	×
4.	Určuje odpovědná osoba odpovědná za administraci aktiv další správce konkrétních aktiv?	✓	×
5.	Jsou správci konkrétních aktiv náležitě proškoleni k provádění daných úkonů?	✓	×
6.	Je zabezpečena obnova provozu se servisními organizacemi v případě výpadku služeb?	✓	×
7.	Je likvidace dat řešena podle vyhlášky o kybernetické bezpečnosti?	✘	Zvážit zavedení postupů likvidace dat dle vyhlášky o kybernetické bezpečnosti.
8.	Jsou mobilní telefony běžných zaměstnanců chráněny v kontextu Mobile Device Management?	✓	×
9.	Jsou pracovní mobilní telefony využívané pracovníky krizového řízení chráněny v kontextu Mobile Device Management?	✘	Zajistit ochranu mobilních telefonů pracovníků KŘ.
10.	Jsou zabezpečeny všechny prvky triády CIA z hlediska správné údržby?	✓	×
11.	Vstupují do serverovny pracovníci úklidu pod dozorem jiné osoby?	✓	×
12.	Jsou dveře serverovny opatřeny magnetickými kontakty?	✓	×
13.	Ukládají se data z magnetických kontaktů do databáze s několikaletou historií?	✓	×

Checklist – řízení aktiv			
Pořadové číslo	**Otázka**	**Odpověď**	**Navrhovaná opatření**
14.	Je vstup do serverovny umožněn jen pomocí čipu, který má omezené množství lidí?	✓	×

Zásadním zjištěním je neaktuálnost seznamu aktiv, což je z hlediska kybernetické bezpečnosti stěžejním prvkem z důvodu častých změn. Další podstatnou skutečností je neexistující Mobile Device Management u mobilních telefonů, které jsou využívány na oddělení havarijního a krizového řízení.

Řízení rizik

Subjekt ve velké míře využívá služeb různých dodavatelů, kteří nejsou ve větší míře ověřováni z hlediska věrohodnosti, ověřují se odborem informatiky na základě referencí. Jejich náležitosti jsou uvedeny ve smlouvě standardní právní formulací.

Ochrana před fyzickými hrozbami je brána v potaz poměrně zodpovědně. Subjekt má zpracovány scénáře potenciálních situací. Největší hrozbou je lidský sektor. Pracovníci úklidu mají povolen přístup jen do některých kanceláří. Jsou i místnosti, do kterých přístup umožněn není. Jedná se o takové místnosti, které jsou nepřístupné všem, například druhá kancelář bezpečnostního manažera. V místnostech tohoto typu probíhá úklid jen za jeho přítomnosti, z důvodu možnosti výskytu některých citlivých informací.

Přítomnost pracovníků úklidu v kancelářích, kde by mohly být zneužitelné informace je dle bezpečnostního manažera nežádoucí. Pracovníci úklidu jsou vnímáni jako bezpečnostní hrozba, ale přesto mají k dispozici náhradní klíče k některým kancelářím. Jiné problémové osoby se v objektu nachází běžně, protože zde probíhají úkony, které mohou být velmi emotivní. Příkladem může být odebrání řidičského oprávnění a tím ztráta zaměstnání. V případě ohrožení mohou pracovníci subjektu využít tlačítko vyvedené k Městské policii, popřípadě použít klávesovou zkratku. Městská policie může být na místě téměř okamžitě, v případě potřeby se volá Policie České republiky (Respondent č. 1, 23. 1. 2024).

Tabulka 4 Checklist pro kategorii „řízení rizik“ (vlastní)

Checklist – řízení rizik			
Pořadové číslo	**Otázka**	**Odpověď**	**Navrhovaná opatření**
1.	Jsou dodavatelé služeb dostatečně ověřování?	✘	Zajistit ověřování dodavatelů v dostatečné míře.
2.	Mají dodavatelé ve smlouvách dostatečně uvedeny jejich náležitosti?	✘	Uvádět ve smlouvách konkrétní náležitosti.
3.	Má subjekt zpracovány scénáře potenciálních situací?	✓	×
4.	Jsou pracovníci úklidu považováni za bezpečnostní hrozbu?	✓	×
5.	Mají náhradní klíče jen osoby, které nejsou považovány za hrozbu?	✘	Odebrat náhradní klíče pracovníkům úklidu.
6.	Mohou zaměstnanci v případě ohrožení použít nouzové tlačítko?	✓	×

V kategorii řízení rizik byly zjištěny tři nedostatky, z čehož dvě se týkají dodavatelů, kteří jsou důležitým prvkem kybernetické bezpečnosti. Jejich ověřování a smluvním povinnostem by měla být věnovaná pozornost, protože mohou být významnou bezpečnostní hrozbou.

Bezpečnost lidských zdrojů

Zaměstnanci jsou seznámeni s vnitřními předpisy, které zahrnují bezpečnostní politiku. Je zpracováno desatero základních bezpečnostních pravidel. Nově probíhá každoroční školení na různá témata bezpečnosti. Poslední školení se týkalo obecných nebezpečí vyskytujících se na internetu, nebezpečí sociálních sítí, jak se tyto informace dají zneužít, poučení o trestné činnosti, které se může týkat krádeže identity. Zaměstnanci jsou vzděláváni pomocí příspěvků, které jsou zveřejňovány bezpečnostním manažerem na intranetu. Kromě kybernetické bezpečnosti jsou zaměstnanci prostřednictvím intranetu poučování i o bezpečnostních rizicích, jako je např. aktivní střelec.

Získané informace o bezpečném chování nejsou žádným způsobem přezkušovány. Je zastáván názor, že některé formální testy jsou postaveny tak, že se člověk musí soustředit spíše na slovíčka, než aby pochopil principy, o které se jedná (Respondent č. 1, 23. 1. 2024).

Při přijímacím řízení nových uchazečů nedochází k ověřování minulosti uchazečů, většinou je důvěřováno informacím uvedených v životopisech. Jedinou prověřovanou skutečností je bezúhonnost, kterou při přijímacím pohovoru uchazeč dokládá (Respondent č. 3, 14. 3. 2024).

Jak již bylo řečeno, subjekt má zpracováno desatero základních bezpečnostních pravidel, které je potřeba mít neustále na paměti. Desatero obsahuje pravidla jako zásada prázdné obrazovky, zásada prázdného pracovního stolu. Mimo jiné obsahuje pravidla poučující o skartaci, nebezpečí elektronické pošty či bezpečném pohybu po pracovišti. Zaměstnanci jsou poučeni o nutnosti uschování veškerých citlivých věcí při každém opuštění své kanceláře. Každý ze zaměstnanců má možnost cokoli uzavřít do skříňky k tomu určené.

Kontrola dodržování stanovených předpisů probíhá nahodile, kdy si manažer bezpečnosti společně s tajemníkem nechávají vedoucím oddělení/odboru otevírat jednotlivé kanceláře a dohlíží na plnění bezpečnostních požadavků. Zaměřují se především na zásadu prázdného stolu a prázdné obrazovky. Na stole se nesmí nacházet žádné osobní údaje ani citlivé informace. Citlivé informace mají svůj vlastní režim, jak s nimi nakládat. Před opuštěním počítače je nutné počítač zamknout, ať už pomocí klávesové zkratky Win+L či jakýmkoli jiným způsobem.

Při zjištění, že některá opatření nejsou dodržována, dojde k poučujícímu rozhovoru se zaměstnancem. Pokud by nebyl tento krok dostatečný, provede rozhovor personalista a dojde k návrhu na snížení jeho platu. Přístup je ale spíše veden formou výchovy, kdy je kladen důraz na nutnost zamknuté pracovní stanice a zamknutého stolu při odchodu (Respondent č. 1, 23. 1. 2024).

Tabulka 5 Checklist pro kategorii „bezpečnost lidských zdrojů“ (vlastní)

Checklist – bezpečnost lidských zdrojů			
Pořadové číslo	**Otázka**	**Odpověď**	**Navrhovaná opatření**
1.	Jsou zaměstnanci seznámeni s vnitřními předpisy?	✓	×
2.	Je zpracováno desatero bezpečnostních pravidel?	✓	×
3.	Je desatero bezpečnostních pravidel dostatečné?	✓	×
4.	Probíhají pravidelná školení?	✓	×
5.	Jsou zaměstnanci vzděláváni i jiným způsobem, než je školení?	✓	×

Checklist – bezpečnost lidských zdrojů			
Pořadové číslo	**Otázka**	**Odpověď**	**Navrhovaná opatření**
6.	Jsou znalosti zaměstnanců přezkušovány?	✘	Zavést pravidelné přezkušování zaměstnanců.
7.	Dochází k ověřování minulosti uchazečů?	✘	Prověřovat minulost uchazečů.
8.	Jsou zaměstnanci poučeni o nutnosti uschování citlivých informací po dobu jejich nepřítomnosti?	✓	×
9.	Probíhá kontrola dodržování stanovených předpisů?	✓	×
10.	Nastávají kroky při zjištění porušování předpisů?	✓	×

Bezpečnost lidských zdrojů je klíčovým prvkem informační bezpečnosti, neboť právě lidský sektor je v kontextu kybernetické bezpečnosti vnímán jako nejslabší článek. Byly zjištěny dva zásadní nedostatky, které jsou rozpracovány v návrzích opatření.

Řízení kontinuity činností

Řízení kontinuity provozu, čímž rozumíme zálohování a obnovu po havárii, je zabezpečeno předem vytvořenými havarijními plány, kdy probíhá každého půl roku testování 25 kritických serverů. Je zavedeno plné a přírůstkové zálohování. Plné zálohování znamená, že jsou zálohována všechna data, která jsou k dispozici, přírůstkové znamená, že se zálohují data, které naposledy zálohována nebyla. Taktéž je používáno dvoustupňové zálohování. První stupněm je záloha na k tomu určené reduplikační a komprimační backup úložiště a druhým stupněm je kopie těchto záloh na pásková zařízení. Pásky jsou uloženy v trezoru v jiné budově, aby byly chráněny v případě požáru. Je využívám koncept záloh 3, 2, 1, čímž rozumíme zálohy na třech místech, ve dvou lokalitách a jednou offline.

Kontrola záloh společně s replikacemi neprobíhá tak často z důvodu stálého obnovování, nicméně je prováděna alespoň kvartálně. Obnova záloh je považována v mnoha případech za rychlejší způsob než zjišťování chyby (Respondent č. 2, 31. 1. 2024).

Systém nouzové komunikace je zabezpečen pomocí poplachu, který je schopen vydávat jen zvukovou signalizaci. V současnosti je vylepšován systém pro nouzovou komunikaci se zaměstnanci pomocí hromadných SMS a e-mailů. K zasílání těchto zpráv budou oprávnění vybraní zaměstnanci v případě kybernetických útoků, aktivního střelce apod. Mohou tak komunikovat v reálném čase. Někteří zaměstnanci mají přidělen služební telefon,

na který by jim byla zaslána SMS. Někteří ale služební telefony nepoužívají, jejich osobní telefonní čísla jsou evidována, prostřednictvím těchto by v případě ohrožení mohli být kontaktováni.

Pokud by se odehrávala nějaká mimořádná událost na budově, která není v hlavním areálu, byly by zaměstnanci neprodleně kontaktování, aby se k této budově nepřibližovali. Subjekt má více než 350 zaměstnanců, tudíž by všichni byly upozorněni v reálném čase. Někteří zaměstnanci mohou tento systém spravovat z domova (Respondent č. 1, 23. 1. 2024). Ve dvou městských částech jsou instalována dvě čidla, která jsou napájena solární energií a pokud se zvedne hladina řeky přijde SMS pracovníkům krizového řízení a dalším zainteresovaným osobám. Na stránkách povodí běžně sledují hodnoty a aktuální situaci, ale tato čidla umožňují rozeslat upozornění v reálném čase.

Další dvě čidla jsou umístěna v jiné městské části na veřejném osvětlení, kde je riziko úniku amoniaku z mrazíren. Další čidlo je umístěno u zimního stadionu, kde také hrozí únik amoniaku. Pokud čidlo únik zachytí okamžitě vysílá informaci HZS ČR, které neprodleně přijede na místo. Na tento systém jsou napojeny okolní budovy, ve kterých se může nacházet větší množství obyvatel. Jedná se například o školská zařízení. Vedení přilehlých budov je poučeno, že pokud je spuštěn poplach, musí se přemístit do vyšších pater, uzavřít okna a přijmout další bezpečnostní opatření, aby byla zajištěna ochrana obyvatelstva v okolí zimního stadionu (Respondent č. 3, 14. 3. 2024).

V případě výpadku dodávky elektrické energie subjekt disponuje UPS (nepřerušitelný zdroj energie), který je schopen zásobovat hlavní datové centrum elektrickou energií tři a půl hodiny. V objektu se nachází také diesel agregát, který je schopen obnovy elektrické energie do půl minuty (Respondent č. 2, 31. 1. 2024) (Respondent č. 3, 14. 3. 2024).

Tabulka 6 Checklist pro kategorii „řízení kontinuity činností“ (vlastní)

Checklist – řízení kontinuity činností		
Pořadové číslo	**Otázka**	**Odpověď**
1.	Jsou vytvořeny havarijní plány?	✓
2.	Probíhá pravidelné testování?	✓
3.	Je zavedeno plné a přírůstkové zálohování?	✓
4.	Je zavedeno dvoustupňové zálohování?	✓
5.	Jsou pásky uloženy v trezoru v jiné budově?	✓
6.	Je využíván koncept zálohování 3, 2, 1?	✓

Checklist – řízení kontinuity činností		
Pořadové číslo	**Otázka**	**Odpověď**
7.	Probíhá pravidelná kontrola záloh?	✓
8.	Je zabezpečen systém nouzové komunikace?	✓
9.	Je zabezpečen systém nouzové komunikace pro potřeby činnosti krizového řízení?	✓
10.	Je zabezpečena obnova provozu v případě výpadku elektrické energie prostřednictvím UPS?	✓
11.	Je zabezpečena obnova provozu v případě výpadku elektrické energie prostřednictvím agregátu?	✓

V kategorii řízení kontinuity činností nebyly zjištěny žádné nedostatky. Subjekt má tuto oblast náležitě řešenou prostřednictvím komplexních bezpečnostních opatření, což zajišťuje adekvátní ochranu a bezpečnost v této oblasti.

Řízení přístupu

Protože se jedná o úřední zaměření subjektu, mimo pracovní dobu není občanům umožněno do budov volně vstoupit. Jedna z budov se nachází mimo hlavní areál. Její hlavní brána se otevírá v šest hodin ráno a uzavírá v 18 hodin. Za bránou se nachází dvoje skleněné vstupní dveře, které se otevírají na čip ve formě karty a zaměstnanci tak vstupují do objektu pomocí něj. Před vstupem musí projít kolem recepce. Pokud chce běžný občan do budovy vstoupit, musí se na recepci nahlásit a buď se do subjektu dostane, protože je úřední den, a tak je vstup volný, anebo mají domluvenou schůzku s některým ze zaměstnanců. V tom případě se zaměstnanec s občanem setká přímo u recepce a do své kanceláře jej dovede a při odchodu jej vyprovodí. Ostatní budovy jsou zabezpečeny obdobným způsobem s výjimkou vstupní brány a skleněných dveří. Vstup na čip a zpřístupnění probíhá obdobným způsobem (Respondent č. 1, 23. 1. 2024).

Při přiložení čipu se údaje, jako jméno, příjmení, čas a místo zapisují do databáze společnosti Microsoft. Celkově pracují s pěti velkými databázemi, dalších 15 databází zprostředkovává společnost Microsoft. Vše je zapisováno v reálném čase a synchronizace hodin je zabezpečena (Respondent č. 2, 31. 1. 2024).

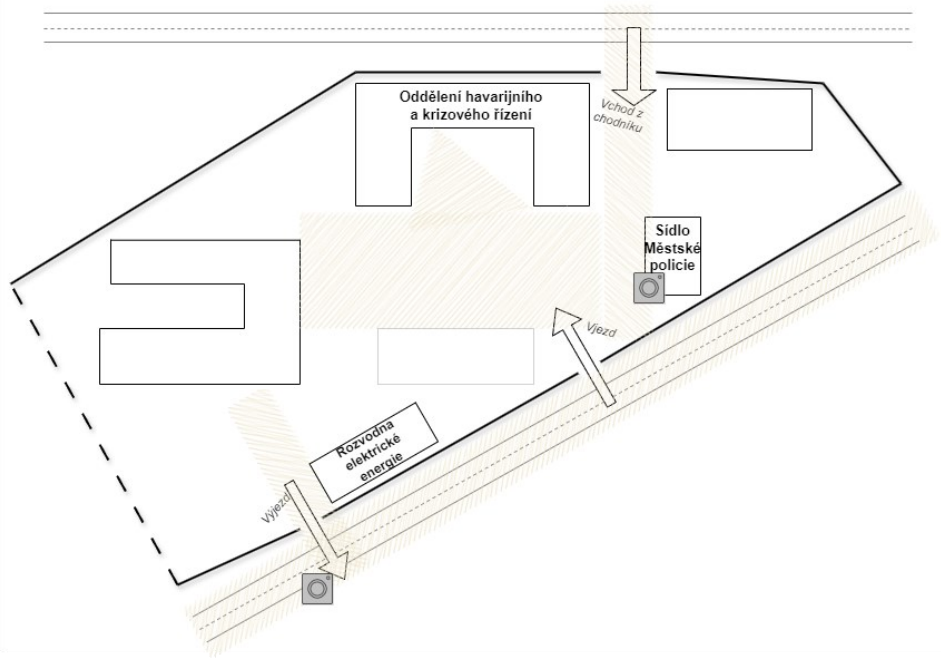
Obrázek 7 Čtecí zařízení pro vstup do budovy (vlastní)

Pokud by někdo ze zaměstnanců chtěl vstoupit do budovy mimo dobu, kdy jsou hlavní vstupy otevřeny, což znamená před šestou hodinou ranní, musel by jít na Městskou policii, kde by se musel vyplnit záznam o vstupu. Dotyčného zaměstnance by tak příslušník Městské policie doprovodil k budově, kde by mu odemknul hlavní vstup a pak ho zase pustil ven. Do záznamu se zadává, kdo vstoupil, z jakého důvodu a co přesně v budově dělal. V tu chvíli by primátorovi a tajemníkovi města přišla SMS zpráva s těmito informacemi. Následně by byla sepsána formální zpráva (Respondent č. 1, 23. 1. 2024).

Areál je z větší části ohraničen vysokým betonovým plotem se třemi možnými vstupy. První slouží pro vjezd motorových vozidel do areálu, druhý pro výjezd. Do areálu se dá vstoupit i z jiné ulice, než na které se nachází vjezd a výjezd. Vstup je alokován na chodníku, tudíž se vjezd vozidel nepředpokládá. Z bezpečnostních důvodů je zde ale umístěn zátaras ve formě zahrazovacího betonového sloupku. Výjezd je možné zavřít posuvnou bránou o výšce přibližně 1,6 m. Vjezd byl v minulosti opatřen zvedací závorou, ta se tam v současnosti už nenachází. Nicméně se dá do areálu vstoupit i přes území jiných pozemků, které se nacházejí z levé strany, jak je naznačeno na nákresu hlavního areálu.

Oblast je zabezpečena kamerovým systémem pomocí městského kamerového systému, který ale není schopen dohlédnout na všechna místa, nicméně na většinu prostoru ano (viz Obrázek 8). Vnitřní prostory objektu nejsou pokryty kamerovým systémem vůbec. Městská policie, která sídlí v areálu, má operační středisko, díky čemuž je okolí neustále pod kontrolou.

Kamerový systém od roku 2021 disponuje inteligentními funkcemi, které umožňují rozpoznat objekty nebo uživatelem definované situace, které je pak snadné vyhledat ve videozáznamu (Respondent č. 1, 23. 1. 2024).



Obrázek 8 Pokrytí kamer v areálu subjektu (vlastní)

Hlavní vstup do budov probíhá pomocí karty, jak již bylo řečeno. Stejná karta je používána i pro procházení průchody, které jsou čtecím zařízením opatřeny. Vstup do některých kanceláří je možný pomocí karty s čipem a následně klíčem. Každý ze zaměstnanců má svou kartu a vlastní klíče k prostorům, které využívá.

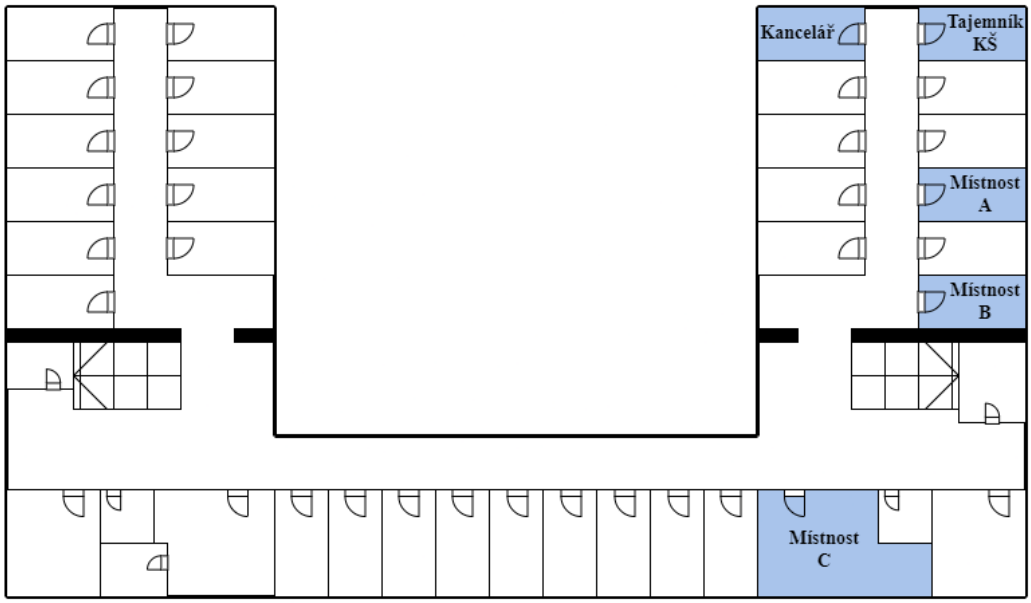
Obrázek 9 Čtecí zařízení jednotlivých průchodů (vlastní)

Není zaveden systém generálního klíče. Náhradní klíče jsou uloženy u správce budov, což je jednou z náplní jeho práce. Některé duplikáty klíčů má u sebe také Městská policie, která sídlí pár metrů od budovy, kde se nachází oddělení havarijního a krizového řízení. Duplikáty klíčů jsou uzamčeny v zapečetěné skříňce, pokud by nastala potřeba jejich použití, musel by se sepsat protokol, kde by byl uveden důvod použití.

Skříně a zásuvky v kancelářích jsou zabezpečeny klíčem. Každý ze zaměstnanců má svůj, žádný generální neexistuje. Náhradní klíče by měly být zapečetěny a uloženy u vedoucího oddělení. V případě, že by se na pracovišti vyskytovalo něco, co by mohlo být zneužitelné, je nutné tyto věci uložit ve skříňce vedle stolu a uzamknout (Respondent č. 1, 23. 1. 2024).

Jedním z oddělení je právě havarijní a krizové řízení, tudíž má náhradní klíče právě vedoucí oddělení, se kterým byl veden jeden z řízených rozhovorů. Místnosti týkající se tohoto oddělení jsou právě kancelář vedoucího oddělení, který je zároveň tajemníkem krizového štábu, kancelář druhého pracovníka krizového řízení a následně tři místnosti, kde zasedá krizový štáb. První místnost je označena jako A, kde se schází krizový štáb v případě potřeby, další dvě místnosti (B a C) se využívají v případech, kdy nastane dlouhotrvající mimořádná událost a je nutné krizový štáb rozdělit na tři skupiny, taktéž označeny písmeny A, B, C shodně s místnostmi.

V případě déle trvající MU by se z kanceláře druhého pracovníka krizového řízení stal sekretariát a byly by zde přijímány telefonní hovory na zřízenou krizovou linku a další činnosti pro potřeby KŠ. Pracovník by tuto kancelář nevyužíval, protože by se stal vedoucím skupiny C. Pokud by došlo ke svolání celého krizového štábu, sešel by se v místnosti A, kde jsou již mapy, podklady, kreslící potřeby, počítače atd. Všechny tyto prostředky jsou předem přichystány a je možné si je rozebrat jednotlivými skupinami KŠ (Respondent č. 3, 14. 3. 2024). Tyto místnosti jsou vyobrazeny na obrázku níže tak aby byla zachována anonymita subjektu. Proto jsou vyznačeny jen místnosti, které se týkají činností krizového řízení. V případě potřeby je na Územním odboru HZS ČR vyhrazena jedna zasedací místnost pro činnost krizového štábu.



Obrázek 10 Půdorys patra s vyznačenými místnostmi týkající se KŘ (vlastní)

Kancelář vedoucího oddělení havarijního a krizového řízení je zabezpečena pouze klíčem. Další klíč ke kanceláři, vyjma náhradních, mají pracovníci úklidu, i když uklízí jen v době přítomnosti pracovníka. V kanceláři se nachází také malá skříňka, ve které jsou uloženy nejen náhradní klíče, ale i klíče k dalším místnostem pro výkon práce (Respondent č. 3, 14. 3. 2024). Skříňka je zabezpečena jen klíčem, nikoli pečetí (viz Obrázek 11).

Obrázek 11 Skříňka s náhradními a dalšími klíči u vedoucího oddělení havarijního a krizového řízení (vlastní)

Pro sdílení informací slouží přímo určený server, kde jsou definována práva pro 300 různých přístupů. Pomocí tohoto serveru komunikuje také zastupitelstvo (Respondent č. 2,

31. 1. 2024). Pokud pracovník krizového řízení posílá e-mail jiným zainteresovaným stranám, použije USB token, který umožňuje použití elektronického podpisu. Tato podpora pro elektronický podpis je umožněna pomocí Bit4 Universal Middleware, který slouží jako softwarová vrstva, jež umožňuje komunikaci mezi elektronickými zařízeními a aplikacemi (Respondent č. 3, 14. 3. 2024).

Pokud běžný zaměstnanec ukončuje pracovní poměr, uzavřené smlouvy či dohody, nejsou zavedena žádná opatření v rámci kybernetické bezpečnosti, kdy by byl zamezen přístup k některým systémům či zařízením před vypršením výpovědi. Zatím nedošlo k takovémuto chování (Respondent č. 1, 23. 1. 2024). Na pracovišti krizového řízení je odebrán přístup k systémům, se kterými pracují. Odebírá se přístup například ke krizovému plánu, kde musí vedoucí pracovník informovat HZS kraje o ukončení pracovního poměru a tím dojde k odebrání přístupu. Výpovědní lhůta trvá po dobu dvou měsíců, během které jsou odebrány přístupy k systémům souvisejících s činností krizového řízení (Respondent č. 3, 14. 3. 2024).

Zaměstnanci mají limitován přístup na některé webové stránky, nicméně se mohou připojit na návštěvní Wi-Fi a odtud už se mohou dostat na jakékoli internetové stránky například pomocí svého mobilního telefonu či tabletu. Na stránky YouTube mají povolený přístup jen někteří zaměstnanci pro výkon své práce, pokud se jedná o prezentaci města apod. Koncová zařízení uživatelů jsou kontrolována, tudíž je zajištěn přehled o prováděných činnostech.

Pro filtrování přístupů na webové stránky jsou používány nástroje, které prohledávají webové stránky a hledají závadná, předem definovaná slova. Pokud se tato slova objeví na webové stránce opakovaně, je stránka zablokována. Pro některé účely pracovní činnosti může být přístup povolen. Filtrování přístupů neprobíhá ani na úrovni DNS či firewallu, je zabezpečeno přímo softwarem pomocí webové brány.

Skupiny informačních služeb, uživatelů a informačních systémů jsou od sebe odděleny. Někteří zaměstnanci mají přístup k počítačům pomocí karty s certifikáty (Respondent č. 2, 31. 1. 2024), nikoli však pracovníci krizového řízení. K počítačům přistupují pouze pomocí uživatelského jména a hesla. Ke všem systémům v rámci krizového řízení byly obdrženy přihlašovací údaje přímo od HZS kraje.

Dle nového zákona o kybernetické bezpečnosti bude zavedeno dvou-faktorové ověřování. Běžní uživatelé koncových zařízení se přihlašují pomocí dvanáctimístného hesla, administrátoři mají hesla o délce šestnácti znaků, v blízké době se bude přecházet na sedmnáct znaků pro administrátory.

Při změně hesel zaměstnanci musí dodržovat pravidla pro změnu hesel. Hesla jsou měněna jednou ročně, protože v nedávné době došlo ke změně z devítimístných hesel na dvanáctimístné. Pravidla pro změnu hesel obsahují požadavek na komplexitu znaků, kterými jsou malá a velká písmena, číslice a speciální znaky. Poučují také o nepřípustnosti výměny číslic na konci hesla při jejich změně. Pravidla obsahují i špatné a dobré příklady různých možností změn. Systém je schopen kontrolovat změnu hesel a hlídá právě zmíněnou výměnu čísel na konci. Pokud takovouto podobnost detekuje, nedovolí uživateli heslo změnit. Koncová zařízení uživatele jsou zabezpečena mimo jiné pomocí automatického zamknutí počítače po 15 minutách nečinnosti (Respondent č. 1, 23. 1. 2024) (Respondent č. 2, 31. 1. 2024).

Obrázek 12 Diagram procesu změny hesla (vlastní)

Subjekt využívá sdílená zařízení, jako je tiskárna a skener. Oboje zařízení je na čip. Po přiložení čipu se vytisknou jen dokumenty, které si konkrétní člověk zaslal k tisku. Zařízení jsou zabezpečena pomocí SafeQ (Respondent č. 1, 23. 1. 2024). SafeQ Print Management Suite zajišťuje správu tisku a ochranu dokumentů za pomoci jednoduchého definování zásad a pravidel. Umožňuje tisk na více lokalitách (YSoft SafeQ, © 2024) což je pro subjekt užitečné z toho důvodu, že sídlí v několika budovách.

Obrázek 13 Čip ke sdíleným zařízením
(Klíčenka ID TAG…, © 2024)

Veškeré záznamy jsou chráněny pomocí Active Directory, aby bylo zamezeno ztrátě, zničení, falšování, neoprávněnému přístupu a neoprávněnému uvolnění (Respondent č. 2, 31. 1. 2024). Active Directory je databáze a soubor služeb, které propojují uživatele se síťovými prostředky potřebnými k práci. Databáze (nebo adresář) obsahuje důležité informace o prostředí, včetně informací o tom, jací uživatelé a počítače existují a kdo má k čemu oprávnění (What is Active Directory?, © 2024). Správa je rozdělena na uživatelskou a administrativní. Defaultní přístupové údaje jsou vždy měněny, ať už se jedná a jakékoli zařízení. Tuto problematiku řeší oddělení kritické infrastruktury a hesla znají jen čtyři lidé (Respondent č. 2, 31. 1. 2024).

Tabulka 7 Checklist pro kategorii „řízení přístupu“ (vlastní)

Checklist – řízení přístupu			
Pořadové číslo	**Otázka**	**Odpověď**	**Navrhovaná opatření**
1.	Hlavní vstup je zabezpečen čtecím zařízením na čip?	✓	×
2.	Vyzvedává si pracovník své klienty u recepce mimo úřední dobu?	✓	×

Checklist – řízení přístupu			
Pořadové číslo	**Otázka**	**Odpověď**	**Navrhovaná opatření**
3.	Jsou údaje o vstupu zapisovány do databáze v reálném čase?	✓	×
4.	Je zabezpečena synchronizace hodin?	✓	×
5.	Jsou vyplňovány záznamy o vstupu mimo běžnou dobu otevření?	✓	×
6.	Je sepsána formální zpráva o vstupu mimo dobu, kdy je běžně otevřeno?	✓	×
7.	Je celá oblast areálu zabezpečena kamerovým systémem?	✗	Přidat další kamery, aby byl získán přehled o celém areálu.
8.	Jsou vnitřní prostory zabezpečeny kamerovým systémem?	✗	Zvážit umístění kamer do vnitřních prostor.
9.	Jsou čtecími zařízeními pro vstup vybaveny i jednotlivé průchody v budovách?	✗	Umístit průchozí dveře se čtecím zařízením v blízkosti kanceláří krizového řízení.
10.	Místnosti týkající se havarijního a krizového řízení jsou zabezpečeny čipem a klíčem?	✗	Kanceláře dvou pracovníků krizového řízení opatřit čtecím zařízením.
11.	Je zaveden systém generálního klíče?	✗	Zvážit zavedení systému generálního klíče.
12.	Jsou náhradní klíče uzamčeny a zapečetěny u každé pověřené osoby?	✗	Zajistit, aby byly náhradní klíče vždy zapečetěny.
13.	Mají zaměstnanci k dispozici uzamykatelnou skříň, kde mohou uschovat citlivé dokumenty?	✓	×
14.	Má krizový štáb v případě dlouhotrvající MU odpovídající místnosti ke své činnosti?	✓	×
15.	Jsou v místnostech pro krizový štáb veškeré potřebné prostředky pro jeho činnost?	✓	×
16.	Je v případě potřeby ustanovena místnost pro činnost krizového štábu na místě mimo areál subjektu?	✓	×
17.	Je zabezpečeno bezpečné sdílení informací?	✓	×
18.	Je odebírán přístup běžným pracovníkům v případě ukončení pracovního poměru po dobu výpovědní lhůty?	✗	Odebírat přístup k systémům, které obsahují citlivé informace.
19.	Je odebrán přístup v případě ukončení pracovního poměru k systémům KŘ?	✓	×

Checklist – řízení přístupu			
Pořadové číslo	**Otázka**	**Odpověď**	**Navrhovaná opatření**
20.	Je v pracovních smlouvách uvedena odpovědnost za informační bezpečnost?	✓	×
21.	Mají zaměstnanci limitován přístup na některé webové stránky?	✓	×
22.	Probíhá filtrování přístupů pomocí webové brány?	✓	×
23.	Jsou od sebe odděleny skupiny informačních služeb, uživatelů a informačních systémů?	✓	×
24.	Jsou hesla pravidelně měněna?	✓	×
25.	Jsou uživatelská hesla dvanáctimístná?	✓	×
26.	Jsou pravidla pro změnu hesel dostatečná?	✓	×
27.	Je zaveden systém, který je schopen kontrolovat náležitosti pro změnu hesel?	✓	×
28.	Systém pro kontrolu změny hesel nepovolí změnu v případě nedodržení stanovených pravidel?	✓	×
29.	Uzamkne se počítač uživatele automaticky v případě delší nečinnosti?	✓	×
30.	Využívá subjekt sdílená zařízení?	✓	×
31.	Používají uživatele čip k obsluze sdílených zařízení?	✓	×
32.	Jsou sdílená zařízení zabezpečena z hlediska správy tisku a ochrany dokumentů?	✓	×
33.	Jsou veškeré záznamy chráněny před ztrátou, zničením, falšováním, neoprávněným přístupem a neoprávněným uvolněním?	✓	×
34.	Je správa informačních služeb rozdělena na uživatelskou a administrativní?	✓	×
35.	Jsou měněny defaultní přístupové údaje u všech zařízení?	✓	×

Analýza řízení přístupu ukázala, že některé prvky jsou nedostatečně řešeny. Zásadním zjištěním je nesoulad s vnitřními politikami týkající se náhradních klíčů. Možné řešení je rozebráno v návrzích opatření.

Řízení identit a jejich oprávnění

Přidělování a používání privilegovaných práv probíhá podle funkce, činnostní role a podle zaměření konkrétního pracovníka. Oprávnění je vymezováno vedoucím odboru a vedoucím oddělení, aby se dosáhlo přehledu o tom, kdo do agendy může a nemůže vstupovat. Pokud zaměstnanec mění pracovní pozici, proběhne přezkoumání přístupových práv a změní se vzhledem k charakteru nové funkce (Respondent č. 1, 23. 1. 2024).

Tabulka 8 Checklist pro kategorii „řízení identit a jejich oprávnění“ (vlastní)

Checklist – řízení identit a jejich oprávnění		
Pořadové číslo	**Otázka**	**Odpověď**
1.	Probíhá přidělování a používání privilegovaných práv podle funkce, činnostní role a podle zaměření konkrétního pracovníka?	✓
2.	Je zajištěn dostatečný přehled o oprávněních jednotlivých uživatelů?	✓
3.	Proběhne přezkoumání přístupových práv a následná změna v případě změny pracovní pozice?	✓

Řízení identit a jejich oprávnění je subjektem řešeno v dostatečné míře prostřednictvím navržených procesů, které zabezpečují správné přidělování oprávnění a správu uživatelských identit, což přispívá k minimalizaci rizik spojených s neoprávněným přístupem a zajišťuje bezpečnost informačních systémů.

Detekce a zaznamenávání kybernetických bezpečnostních událostí

Největší hrozbou jsou zaměstnanci za klávesnicí, kteří se mohou vědomě či nevědomě zachovat nesprávně. Když selže zaměstnanec, jsou přijata opatření, která odhalí úmyslnou i neúmyslnou nebezpečnou činnost. Zatím nenastala zkušenost s některým ze zaměstnanců, který by měl postranní úmysly. Pokud nastane aktuální bezpečnostní hrozba, jsou zaměstnanci informováni prostřednictvím e-mailu, což zabezpečí, že o hrozbě vědí co nejdříve je to možné (Respondent č. 1, 23. 1. 2024).

Informace o technických zranitelnostech používaných informačních systémů a následné vyhodnocení vystavení organizace těmto zranitelnostem zpracovává určený technický konzultant, který všechna zjištění posílá organizaci na vědomí. Pokud se jedná o dílčí úkony, subjekt je schopen si tyto informace a následné vyhodnocení zajistit sám. Na co sám nestačí,

zajišťuje dodavatel. Spolupráce funguje s více než třiceti dodavateli, pokud nastane nečekaná událost, neprodleně kontaktují daného dodavatele nebo nastávají i situace, kdy dodavatel sám kontaktuje subjekt.

S logy pracuje dohledové Security Operation Center (bezpečnostní dohledové centrum kybernetické bezpečnosti). Ať už se jedná o jejich vytváření, uchovávání, ochranu či analýzu, výjimky, poruchy a další relevantní události, se všemi pracuje právě Security Operation Center. V případě potřeby jsou informace zasílány organizaci. Monitoring sítě z hlediska abnormálního chování zajišťuje nástroj Flowmon a IBM TIVOLI software.

Pravidelná údržba LAN a prvků ICT probíhá pomocí různých softwarových nástrojů (IBM TIVOLI software, CISCO) a vše je monitorováno pomocí Flowmon, který by abnormální chování neprodleně oznámil. Auditní testy týkající se informatiky probíhají přibližně každé tři roky. Ověřovací činnosti zahrnující posouzení provozních systémů probíhají prostřednictvím penetračních testů, kdy jsou najatí etičtí hackeři, kteří vyhledávají slabiny v systému. Penetrační testování využívají například k minimalizaci rizika SQL injection (Respondent č. 2, 31. 1. 2024).

Tabulka 9 Checklist pro kategorii „detekce a zaznamenávání kybernetických bezpečnostních událostí“ (vlastní)

Detekce a zaznamenávání kybernetických bezpečnostních událostí		
Pořadové číslo	**Otázka**	**Odpověď**
1.	Jsou uživatelé neprodleně informováni o možné bezpečnostní hrozbě?	✓
2.	Informuje příslušné osoby určený technický konzultant o možných technických zranitelnostech?	✓
3.	Vyhodnocuje technický konzultant vystavení organizace možným zranitelnostem?	✓
4.	Využívá organizace služeb dodatelů, pokud sama nestačí na dílčí úkony týkající se vyhodnocení vystavení organizace zranitelnostem?	✓
5.	Je komunikace s dodavateli v kontextu nečekaných bezpečnostních událostí oboustranná?	✓
6.	Pracuje s logy Bezpečnostní dohledové centrum kybernetické bezpečnosti?	✓
7.	Jsou v případě potřeby zasílány záznamy/informace organizaci?	✓
8.	Je zajištěn monitoring sítě z hlediska abnormálního chování?	✓

Detekce a zaznamenávání kybernetických bezpečnostních událostí		
Pořadové číslo	**Otázka**	**Odpověď**
9.	Probíhá pravidelná údržba LAN a prvků ICT?	✓
10.	Probíhají pravidelně auditní testy týkající se informatiky?	✓
11.	Ověřovací činnosti zahrnující posouzení provozních systémů probíhá prostřednictvím penetračních testu?	✓
12.	Je využívání penetrační testování k minimalizaci rizika SQL injection?	✓

Oblast detekce a zaznamenávání kybernetických bezpečnostních incidentů je subjektem zajištěna na dostatečné úrovni, což umožňuje včasnou a adekvátní reakci.

Řešení kybernetických bezpečnostních incidentů

Ve vnitřních politikách jsou uvedeny postupy pro řešení kybernetických bezpečnostních incidentů. S týmy CSIRT a Národním úřadem pro kybernetickou a informační bezpečnost proběhla spolupráce jen jednou. Nastal pokus o napadení systému pomocí zaslaného e-mailu, kdy zaměstnanec otevřel odkaz, který neměl. Úřad byl na krátkou chvíli uzavřen, proběhlo obnovení systému a zjištění příčiny. Bylo zjištěno ochromení šesti pracovních stanic (Respondent č. 1, 23. 1. 2024).

V případě napadení ransomware se odbor informatiky řídí takzvaným *Response Plan*, který obsahuje nespočet variant, jak na útok reagovat. Existuje zde i možnost zaplacení, kdy plán obsahuje konkrétní postup od vytvoření bitcoinové peněženky až po komunikaci s hackery. Nicméně se dává přednost obnovení než zaplacení útočníkům. *Response Plan* uvádí také možnost využití firmy, která se na problematiku ransomware specializuje. Nicméně bylo uznáno, že reakce na ransomware útoky není kompletní a je potřeba postup vylepšit.

V obálkách, která jsou umístěny v trezoru jsou k dispozici účty s nejvyššími oprávněními, takzvané administrátorské účty technických aktiv, které by se použili v případě kybernetického incidentu a v nezbytně nutných případech, kdy by došlo v rozsáhlejší poruše (Respondent č. 2, 31. 1. 2024).

Zaměstnanci, administrátoři, osoby odpovědné za kybernetickou bezpečnosti a dodavatelé jsou povinni oznamovat oboru informatiky neobvyklé chování technických aktiv a podezření na zranitelnosti, což je také v jejich zájmu (Respondent č. 1, 23. 1. 2024).

Tabulka 10 Checklist pro kategorii „řešení kybernetických bezpečnostních incidentů“ (vlastní)

Checklist – řešení kybernetických bezpečnostních incidentů			
Pořadové číslo	**Otázka**	**Odpověď**	**Navrhovaná opatření**
1.	Jsou ve vnitřních politikách uvedeny postupy pro řešení kybernetických bezpečnostních incidentů?	✓	×
2.	Probíhá spolupráce s týmy CSIRT v případě potřeby?	✓	×
3.	Probíhá spolupráce s NÚKIB v případě potřeby?	✓	×
4.	Proběhla v minulosti spolupráce s týmy CSIRT a NÚKIB?	✓	×
5.	Je dostatečně zpracován postup pro řešení ransomware útoků?	✘	Dopracovat postup pro řešení ransomware útoků.
6.	Je dávána přednost obnově před zaplacením útočníkům?	✓	×
7.	Jsou k dispozici administrátorské účty technických aktiv v případě potřeby?	✓	×
8.	Jsou zaměstnanci, administrátoři, osoby odpovědné za KB a dodavatelé povinni oznamovat oboru informatiky neobvyklé chování technických aktiv a podezření na zranitelnosti?	✓	×

Kategorie řešení kybernetických bezpečnostních incidentů má jeden zásadní nedostatek, a to nedostatečně dopracován postup pro řešení ransomware útoků, což může mít zásadní vliv na kybernetickou a informační bezpečnost subjektu. Možné řešení je uvedeno v návrhové části.

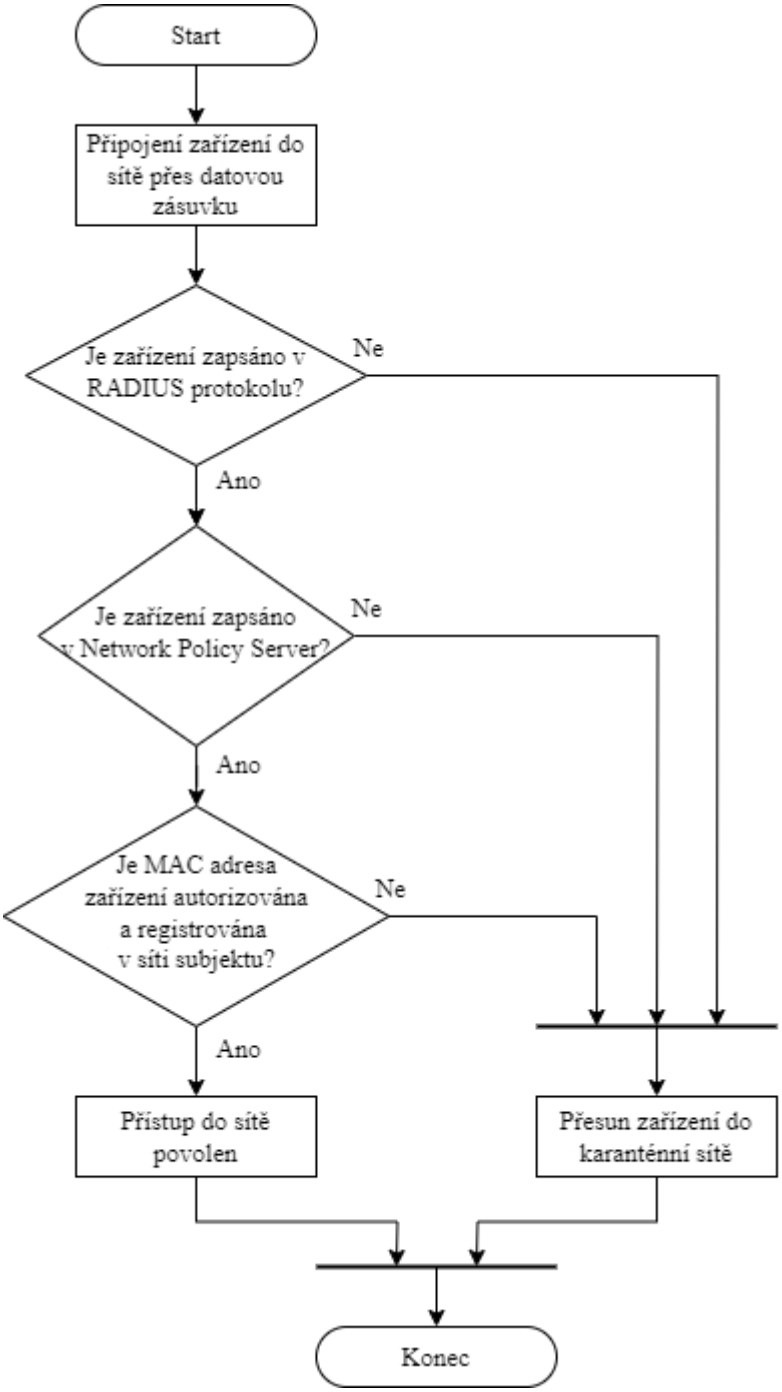
Bezpečnost komunikačních sítí

Hlasové, obrazové a textové komunikace jsou zabezpečeny antispamovými a antivirovými softwarovými nástroji, konkrétně jsou používány web filtering, Firepower Cluster a ADC (Respondent č. 2, 31. 1. 2024). Web filtering je bezpečnostní technologie, která monitoruje webovou aktivitu a zabraňuje uživatelům v přístupu na webové stránky se škodlivým obsahem či stránky, které jsou považovány za nevhodné z hlediska činnosti subjektu (What

is Web Filtering?, © 2003 - 2024). Firepower Cluster od společnosti CISCO umožňuje seskupení více jednotek ochrany proti hrozbám do jednoho logického zařízení (Firepower Management Center…, © 2024).

Ochrana kabelů přenášející napájení, data či podpůrné služby je zajištěna pomocí řízeného přístupu osob. K těmto kabelům má přístup jen velmi omezený počet lidí. Jsou zavedeny systémy, které by neprodleně odhalily podezřelou činnost. Je používán jak metalický, tak i optický kabel. Je využíváno VPN neboli virtuální privátní síť, která zajišťuje anonymitu na síti. Firewall je taktéž implementován.

Přístup k síti je filtrován pomocí MAC adres jen částečně. Všechna zařízení jsou poznačena a v rámci protokolu RADIUS a Network Policy Server jsou kontrolována zařízení, která se snaží připojit do sítě skrz datovou zásuvku. Dojde ke kontrole, jestli se jedná o povolené zařízení a když ověření neprojde, dojde k přesunu do karanténní sítě, kde je k dispozici pouze internet. Pro povolení přístupu k síti je zapotřebí projít třemi komponenty, kterými je právě MAC adresa, RADIUS server a Network Policy Server, mimo to probíhá spolupráce s doménou, kterými musí zařízení projít, aby bylo do sítě puštěno. Připojení do sítě je graficky znázorněno na diagramu procesu (viz Obrázek 14).



Obrázek 14 Diagram procesu připojení zařízení do sítě (vlastní)

DHCP server je využíván ve spolupráci s RADIUS serverem a Network Policy Server, což umožňuje efektivní autentizaci a autorizaci uživatelů v síti. IP adresy jsou přidělovány konkrétním zařízením pomocí rezervačního listu (Respondent č. 2, 31. 1. 2024).

Tabulka 11 Checklist pro kategorii „bezpečnost komunikačních sítí“ (vlastní)

Checklist – bezpečnost komunikačních sítí		
Pořadové číslo	**Otázka**	**Odpověď**
1.	Jsou dostatečně zabezpečeny hlasové, obrazové a textové komunikace?	✓
2.	Je ochrana kabelů přenášející napájení, data a podpůrné služby zajištěna pomocí řízeného přístupu osob?	✓
3.	Jsou zavedeny systémy, které by odhalily podezřelou činnost v rámci kabelů?	✓
4.	Je používán metalický i optický kabel?	✓
5.	Je využíváno VPN?	✓
6.	Je implementován firewall?	✓
7.	Je dostatečným způsobem filtrován přístup k síti?	✓
8.	V případě připojení nepovoleného zařízení do sítě, je toto přesunuto do karanténní sítě?	✓
9.	Je zajištěna autentizace a autorizace uživatelů v síti?	✓
10.	Je využíván rezervační list IP adres?	✓

Subjekt se k bezpečnosti komunikačních sítí staví zodpovědně a systematicky implementací moderních bezpečnostních protokolů a monitorováním provozu, což zajišťuje ochranu citlivých dat a minimalizaci rizik spojených s možnými kybernetickými hrozbami.

Aplikační bezpečnost

Ochrana před škodlivým softwarem je zajištěna pomocí Bitdefender a pomocí inteligentní nástavby EDR (Endpoint Detection and Response) (Respondent č. 2, 31. 1. 2024). Jedná se o kombinaci jedné z nejúčinnější ochranné platformy na světě pro ochranu koncových bodů společně s funkcemi detekce a reakce na koncových bodech (EDR). Za pomoci analýzy rizik koncových zařízení a hrozeb z pozice uživatele a propojení inovací v oblasti bezpečnosti je Bitdefender spolu s nástavbou EDR schopen zmenšit pomyslný útočný povrch koncového zařízení a pro útočníky je tak mnohem složitější proniknout do systému (GravityZone Business Security Enterprise, © 2024).

Tabulka 12 Checklist pro kategorii „aplikační bezpečnost“ (vlastní)

Checklist – aplikační bezpečnost		
Pořadové číslo	**Otázka**	**Odpověď**
1.	Je zajištěna ochrana před škodlivým softwarem?	✓
2.	Je využíváno ochrany koncových bodů společně s funkcemi detekce a reakce na koncových bodech?	✓

Aplikační bezpečnost je zajištěna za pomocí odpovídajících softwarových nástrojů a inteligentní nástavby, díky čemuž je dosaženo požadované úrovně kybernetické bezpečnosti.

Kryptografické algoritmy

Maskování informací probíhá za pomocí BitLocker. Kryptografie je zabezpečena na pracovních mobilních telefonech a následně na vybraných externích discích, které jsou používány pro výkon práce. Šifrování dat na discích notebooků ve výchozím stavu probíhá pomocí BitLocker.

Jak již bylo řečeno, hesla jsou buďto dvanácti či šestnáctimístná (v budoucnu sedmnáctimístná). Hashování přihlašovacích údajů probíhá automaticky pomocí určeného systému (Respondent č. 2, 31. 1. 2024).

Tabulka 13 Checklist pro kategorii „kryptografické algoritmy“ (vlastní)

Checklist – kryptografické algoritmy		
Pořadové číslo	**Otázka**	**Odpověď**
1.	Probíhá maskování informací?	✓
2.	Je zabezpečena kryptografie na pracovních mobilních telefonech?	✓
3.	Je zabezpečena kryptografie na externích discích, které slouží k výkonu práce?	✓
4.	Je zabezpečeno šifrování na discích notebooků ve výchozím stavu?	✓
5.	Probíhá automatické hashování přihlašovacích údajů?	✓

U kategorie kryptografické algoritmy nebyl zjištěn žádný nedostatek. Subjekt je implementovány adekvátní postupy, které zajišťují ochranu citlivých dat.

6.3 Životní cyklus informací

Na následujícím diagramu je vyobrazen životní cyklus informací v prostředí ochrany obyvatelstva, konkrétně krizového štábu za mimořádné události, která může přerůst v krizovou situaci. Swimlane diagram je omezen na činnost jednoho krizového štábu ORP společně se stálou pracovní skupinou. Nejsou zde vyobrazeny činnosti krizového štábu kraje ani ústředního krizového štábu a složek IZS, které s krizovým štábem spolupracují. Činnosti krizového štábu, stejně jako části swimlane diagramu, jsou rozděleny následovně:

- Předseda krizového štábu.
- Tajemník krizového štábu.
- Stálá pracovní skupina (dále jen „SPS“), včetně vedoucího stálé pracovní skupiny.
- Odborná skupina pro součinnost a komunikaci, včetně vedoucího odborné skupiny, která zahrnuje:
    - Komunikační středisko.
    - Sekretariát.
- Odborná skupina analýzy situace a nasazení sil a prostředků (dále jen „SaP“), včetně vedoucího odborné skupiny.
- Odborná skupina týlového zabezpečení a ochrany obyvatelstva, včetně vedoucího odborné skupiny.

Iniciační událostí je svolání krizového štábu tajemníkem KŠ na pokyn předsedy KŠ v důsledku nastalé mimořádné události. Na popud vedoucího SPS vyjíždí členové KŠ na místo MU. Po činnosti členů KŠ na místě MU soustřeďuje odborná skupina analýzy situace a nasazení SaP potřebné informace a dokumentaci činností a postupů při zásahu ve spolupráci s velitelem zásahu.

Zjištěné informace předává odborná skupina analýzy situace a nasazení SaP vedoucímu SPS. Vedoucí SPS následně předává informace tajemníkovi KŠ. Tajemník KŠ na základě zjištěných informací rozhoduje, zda lze nebo nelze MU řešit běžně dostupnými prostředky. V případě, že nelze MU řešit běžně dostupnými prostředky, navrhuje předsedovi KŠ aby byl vyhlášen krizový stav na zasaženém území. Předseda KŠ na základě doporučení žádá hejtmana kraje o vyhlášení krizového stavu, který po projednání v krizovém štábu kraje krizový stav vyhlásí.

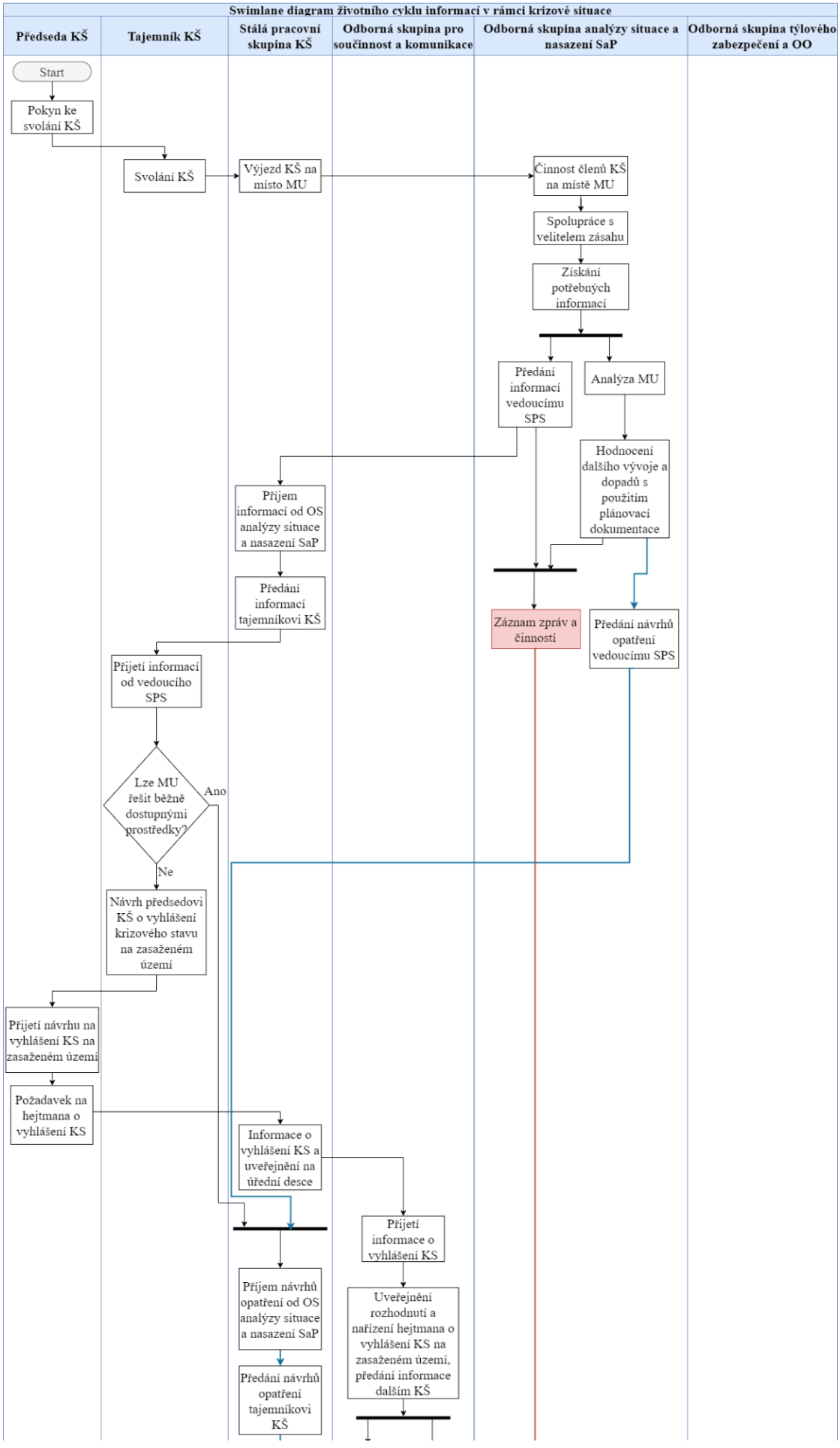
Vedoucí SPS nechá uveřejnit rozhodnutí o vyhlášení krizového stavu na úřední desce a předává informaci o vyhlášení krizového stavu odborné skupině pro součinnost a komunikaci, která uveřejňuje rozhodnutí a nařízení hejtmana kraje o vyhlášení krizového stavu a předává tuto informaci dalším krizovým štábům. Následně odborná skupina pro součinnost a komunikaci zřizuje telefonní linku tísňového volání pro obyvatelstvo včetně zajištění provozu komunikačního střediska KŠ. Veškeré postupy zapisuje do záznamu zpráv a činností. V návaznosti na zřízení tísňové linky připravuje komunikační středisko informaci pro veřejnost o zřízení tísňové linky a nastalé mimořádné události. Informace pro veřejnost je prostřednictvím odborné skupiny týlového zabezpečení a OO poskytnuta veřejnosti pomocí internetových stránek města a médií, tímto je zabezpečeno varování a informování obyvatelstva. Odborná skupina týlového zabezpečení a OO po uveřejnění informací pro veřejnost provádí zápis do záznamu zpráv a činností.

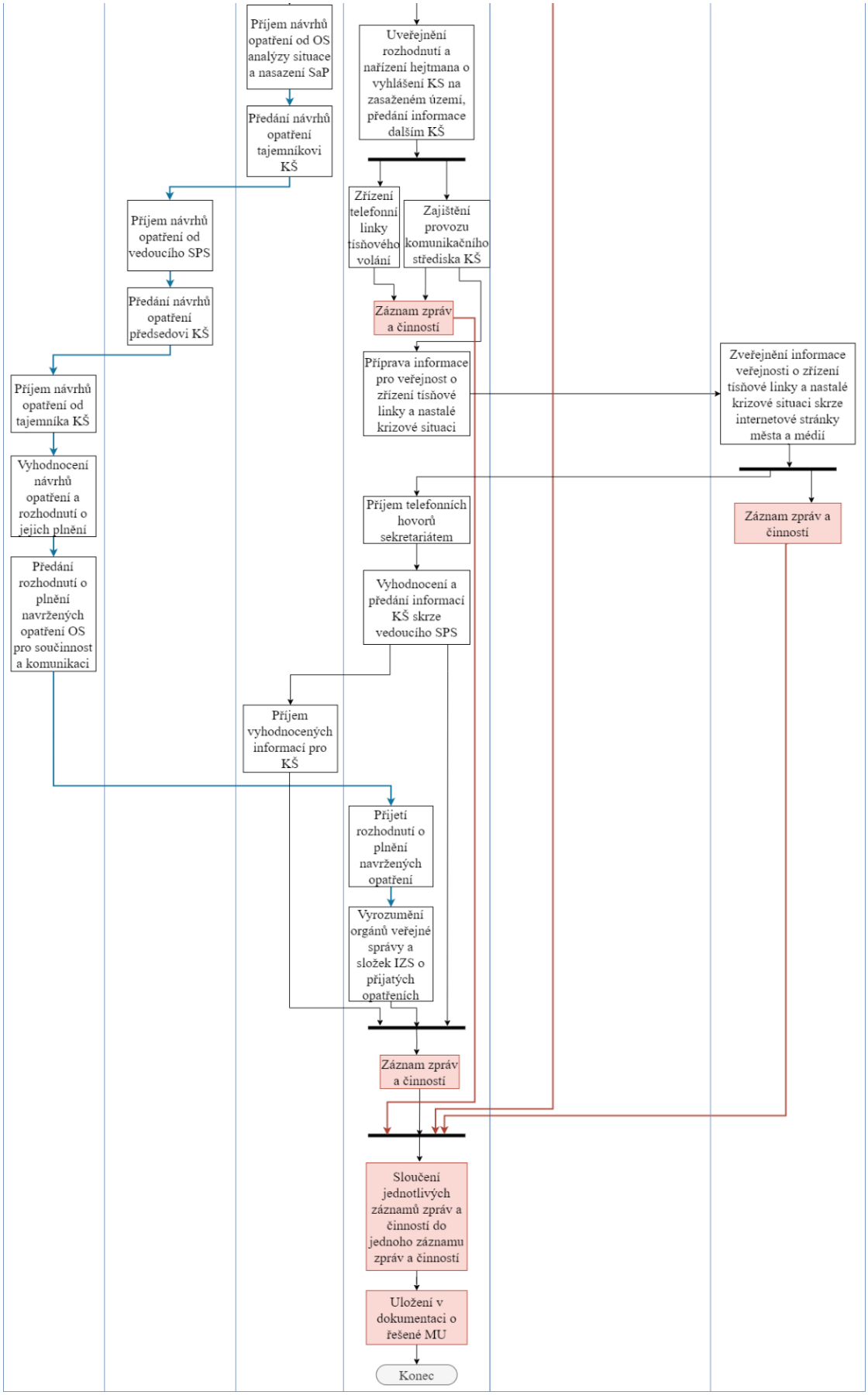
V návaznosti na uveřejnění informace o zřízení krizové linky, přijímá sekretariát telefonní hovory adresované krizovému štábu. Tyto informace následně vyhodnocuje a předává krizovému štábu ve spolupráci s vedoucím SPS. O veškerých hovorech sekretariát vede záznam zpráv a činností.

V průběhu zřizování tísňové linky pro veřejnost probíhají další činnosti. Odborná skupina analýzy situace a nasazení SaP analyzuje krizovou situaci v návaznosti na zjištění informací od velitele zásahu a hodnotí další vývoj včetně možných dopadů, což propisuje do záznamu zpráv a činností. Po analýze s pomocí plánovací dokumentace navrhuje opatření, které předává vedoucímu SPS, který je následně předává tajemníkovi KŠ. Tajemník KŠ navrhovaná opatření předává předsedovi KŠ, který je vyhodnotí a rozhodne o jejich plnění. Odborná skupina pro součinnost a komunikaci vyrozumívá orgány veřejné správy a složky IZS o přijatých opatřeních. Tato činnost je opět zapsána do záznamu zpráv a činností.

Finálním dějem swimlane diagramu je sjednocení veškerých záznamů o činnostech, které průběžně zapisovaly jednotlivé odborné skupiny patřící pod stálou pracovní skupinu krizového štábu. Veškeré záznamy jsou sjednoceny do jediného dokumentu s totožným názvem. Tento dokument je následně fyzicky uložen v dokumentaci o řešené mimořádné události.

Z důvodu lepší čitelnosti je swimlane diagram rozdělen na dvě části a rozložen na dvě stránky. Z důvodu lepší přehlednosti o navazujících dějích, se některé buňky v předělu opakují. V diagramu jsou používány zkratky, jako je OS, čímž je myšlena odborná skupina a zkratka KS, která znázorňuje krizový stav. Další používané zkratky jsou upřesněny v textu výše.


Swimlane diagram životního cyklu informací v rámci krizové situace
Předseda KŠ
Tajemník KŠ
Stálá pracovní skupina KŠ
Odborná skupina pro součinnost a komunikace
Odborná skupina analýzy situace a nasazení SaP
Odborná skupina týlového zabezpečení a OO
Start
Pokyn ke svolání KŠ
Svolání KŠ
Výjezd KŠ na místo MU
Činnost členů KŠ na místě MU
Spolupráce s velitelem zásahu
Získání potřebných informací
Předání informací vedoucímu SPS
Analýza MU
Hodnocení dalšího vývoje a dopadů s použitím plánovací dokumentace
Příjem informací od OS analýzy situace a nasazení SaP
Předání informací tajemníkovi KŠ
Záznam zpráv a činností
Předání návrhů opatření vedoucímu SPS
Přijetí informací od vedoucího SPS
Lze MU řešit běžně dostupnými prostředky?
Ano
Ne
Návrh předsedovi KŠ o vyhlášení krizového stavu na zasaženém území
Přijetí návrhu na vyhlášení KS na zasaženém území
Požadavek na hejtmana o vyhlášení KS
Informace o vyhlášení KS a uveřejnění na úřední desce
Přijetí informace o vyhlášení KS
Příjem návrhů opatření od OS analýzy situace a nasazení SaP
Uveřejnění rozhodnutí a nařízení hejtmana o vyhlášení KS na zasaženém území, předání informace dalším KŠ
Předání návrhů opatření tajemníkovi KŠ



Obrázek 15 Swimlane diagram životního cyklu informací v rámci KS (vlastní)

7 NÁVRHY OPATŘENÍ

Kapitola vychází z kontrolních checklistů, které jsou rozšířeny o návrhy opatření. Veškeré návrhy mají doporučující charakter, ale většina vychází ze Směrnice NIS2, která je v současnosti implementována do českého právního prostředí. Subjekt bude spadat pod poskytovatele regulované služby v režimu nižších povinností, na což je v kapitole brán zřetel a návrhy jsou ve většině případů s ní v souladu.

Níže se nachází syntéza tabulek, která obsahuje řádky předchozích checklistů, které mají zápornou odpověď a obsahují návrhová opatření. U pořadového označení jsou použity římské číslice, a nikoliv původní čísla, aby nedošlo ke zmatení.

Tabulka 14 Syntéza checklistů, zaměřena na záporné odpovědi

Checklist – zajišťování kybernetické bezpečnosti			
Pořadové číslo	**Otázka**	**Odpověď**	**Navrhovaná opatření**
I.	Je pravidelně přezkoumávám závazek o mlčenlivosti?	✘	Zavést pravidelné přezkoumávání dohod o mlčenlivosti.
II.	Probíhají pravidelné aktualizace nekritických serverů?	✘	Zavést pravidelné aktualizace nekritických serverů.
Checklist – povinnosti vrcholového vedení			
III.	Jsou právně stanoveny povinnosti vrcholového vedení?	✘	Právně stanovit povinnosti vrcholového vedení.
Checklist – řízení aktiv			
IV.	Zpracován aktuální seznam aktiv?	✘	Aktualizovat seznam aktiv v návaznosti na NIS2.
V.	Je likvidace dat řešena podle vyhlášky o kybernetické bezpečnosti?	✘	Zvážit zavedení postupů likvidace dat dle vyhlášky o kybernetické bezpečnosti.
VI.	Jsou pracovní mobilní telefony využívané pracovníky krizového řízení chráněny v kontextu Mobile Device Management?	✘	Zajistit ochranu mobilních telefonů pracovníků KŘ.
Checklist – řízení rizik			
VII.	Jsou dodavatelé služeb dostatečně ověřování?	✘	Zajistit ověřování dodavatelů v dostatečné míře.
VIII.	Mají dodavatelé ve smlouvách dostatečně uvedeny jejich náležitosti?	✘	Uvádět ve smlouvách konkrétní náležitosti.

Pořadové číslo	Otázka	Odpověď	Navrhovaná opatření
IX.	Mají náhradní klíče jen osoby, které nejsou považovány za hrozbu?	✖	Odebrat náhradní klíče pracovníkům úklidu.
Checklist – bezpečnost lidských zdrojů			
X.	Jsou znalosti zaměstnanců přezkušovány?	✖	Zavést pravidelné přezkušování zaměstnanců.
XI.	Dochází k ověřování minulosti uchazečů?	✖	Prověřovat minulost uchazečů.
Checklist – řízení přístupu			
XII.	Je celá oblast areálu zabezpečena kamerovým systémem?	✖	Přidat další kamery, aby byl získán přehled o celém areálu.
XIII.	Jsou vnitřní prostory zabezpečeny kamerovým systémem?	✖	Zvážit umístění kamer do vnitřních prostor.
XIV.	Jsou čtecími zařízeními pro vstup vybaveny i jednotlivé průchody v budovách?	✖	Umístit průchozí dveře se čtecím zařízením v blízkosti kanceláří krizového řízení.
XV.	Místnosti týkající se havarijního a krizového řízení jsou zabezpečeny čipem a klíčem?	✖	Kanceláře dvou pracovníků krizového řízení opatřit čtecím zařízením.
XVI.	Je zaveden systém generálního klíče?	✖	Zvážit zavedení systému generálního klíče.
XVII.	Jsou náhradní klíče uzamčeny a zapečetěny u každé pověřené osoby?	✖	Zajistit, aby byly náhradní klíče vždy zapečetěny.
XVIII.	Je odebírán přístup běžným pracovníkům v případě ukončení pracovního poměru po dobu výpovědní lhůty?	✖	Odebírat přístup k systémům, které obsahují citlivé informace.
Checklist – řešení kybernetických bezpečnostních incidentů			
XIX.	Je dostatečně zpracován postup pro řešení ransomware útoků?	✖	Dopracovat postup pro řešení ransomware útoků.

Další podkapitoly detailně rozpracovávají navrhovaná opatření. Jedná se o možné návrhy, které může subjekt zavést pro zajištění vyšší úrovně kybernetické bezpečnosti.

7.1 Zajišťování kybernetické bezpečnosti

Zavedení pravidelného přezkoumávání dohod o mlčenlivosti – Subjekt neuzavírá samostatné dohody o mlčenlivosti. Tyto jsou součástí pracovních smluv a smluv s dodavateli služeb. Závazek o mlčenlivosti je zásadní z hlediska úniku informací, což by mohlo subjekt

významně poškodit. Povinnost mlčenlivosti musí smluvní strana dodržovat i po vypovězení smlouvy. Smlouvy o mlčenlivosti by měly obsahovat prvky, které jsou zaměřené přímo na protistranu s ohledem na její přístup k informacím. Přezkoumávání dohod o mlčenlivosti dokáže posoudit a aktualizovat opatření v souladu s vyvíjecími se hrozbami v kyberprostoru. Díky pravidelnému přezkoumávání je možné upravit dohody tak, aby zahrnovaly nové technologické výzvy a zabezpečily ochranu informací nejen před kybernetickými útoky a jejich zneužitím.

Návrhem je vypracovat dohody o mlčenlivosti samostatně a nikoli je mít jako součást běžných pracovních smluv. Popřípadě v přílohách smluv, ale tak aby byly odděleny od hlavní části smlouvy, což by v případě změn v dohodách o mlčenlivosti zjednodušilo implementaci nového znění. Dalším návrhem je pravidelné přezkoumávání těchto dohod, a to alespoň jedenkrát ročně vždy s ohledem na nové trendy v oblasti kybernetické bezpečnosti.

Zavedení pravidelných aktualizací nekritických serverů – I když aktualizace nekritických serverů probíhají dle potřeby, je nutné stanovit ve vnitřních politikách pravidelnou aktualizaci, a to alespoň jednou za půl roku a zároveň následovat požadavky Windows Servere Update Services.

7.2 Povinnosti vrcholového vedení

Smluvní stanovení povinností vrcholového vedení – Protože subjekt je úřední povahy, jsou jeho vrcholovým vedením orgány města, které ale nemají smluvně stanoveny povinnosti. Návrhem je smluvně stanovit povinnosti a rozsah odpovědností vrcholového vedení a prokazatelně jej o nich poučit. Finanční zdroje jsou pravidelně uvolňovány pro potřebu školení vrcholového vedení, tudíž by mohly být použity i pro zajišťování kybernetické bezpečnosti v souladu s přehledem bezpečnostních opatření. Subjekt by měl mít zpracován seznam bezpečnostních opatření, který obsahuje přehled veškerých bezpečnostních opatření, která jsou zavedena včetně opatření, která zavedena teprve budou, a to i s popisem zavedení. Musí obsahovat také přehled bezpečnostních opatření, která zavedena nebyla spolu s důvodem nezavedení. Vrcholové vedení by mělo být s tímto náležitě seznámeno.

7.3 Řízení aktiv

Pravidelná kontrola seznamu aktiv – I když má subjekt v plánu seznam aktiv přepracovávat, bylo uvedeno, že byl zpracován před mnoha lety. Seznam aktiv by měl být pravidelně přezkoumáván a aktualizován s ohledem na současný stav, protože se v čase dynamicky

mění. Doporučující interval pro kontrolu aktuálnosti seznamu aktiv je alespoň jednou ročně, při zjištění jakýchkoli změn je pak do seznamu aktiv zahrnout.

Likvidace dat – Jelikož nově vznikající vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností, pod kterou subjekt spadá, neobsahuje stanovené postupy likvidace dat, je tento návrh pouze doporučující, z hlediska zajištění vysoké úrovně kybernetické bezpečnosti. Návrhem je při likvidaci dat postupovat podle vyhlášky o kybernetické bezpečnosti, která je v současnosti stále v platnosti, nicméně s vydáním nového zákona o kybernetické bezpečnosti bude zrušena, proto bude vhodnější postupovat podle nově vznikající Vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, která obsahově zahrnuje tytéž náležitosti jako vyhláška o kybernetické bezpečnosti.

Mobile Device Management u mobilních telefonů krizového řízení – Mobilní telefony používané pracovníky krizového řízení nejsou nijak chráněny vůči únikům informací. Subjekt ale využívá softwarový nástroj Mobile Iron, který je schopen zajistit informační bezpečnost koncových zařízení. Pro využití Mobile Iron je nutné mít mobilní telefon, který je schopen datového připojení, musí mít podporu operačního systému a být kompatibilní s bezpečnostními politikami, které Mobile Iron vyžaduje.

Veškeré požadavky, které Mobile Iron ukládá, mobilní telefony, které jsou pracovníky krizového řízení používány, splňují. Bylo by vhodné použít softwarový nástroj Mobile Iron pro zabezpečení mobilních telefonů krizového řízení, což by neměl být problém, protože subjekt tento nástroj již využívá u jiných pracovníků.

7.4 Řízení rizik

Ověřování dodavatelů – Ověřování dodavatelů jen na základě recenzí na internetu je jen jedním z prvků hodnocení dodavatele. Důležité je ověřovat dodavatele v oblastech historie a pověsti dodavatele, jeho certifikace v oblasti bezpečnosti informací či řízení jakosti, reference ze spolehlivých zdrojů, transparentnosti vlastnické struktury, kvality a dostupnosti informací z veřejných zdrojů a jejich přechozích zkušeností. Do zkušeností můžeme zahrnout spolupráci, technickou podporu, dodržení termínů, včasné informace o změnách a jejich odůvodnění apod. Tyto informace je nejjednodušší propsat do tabulky, kterou veřejnosti nabízí NÚKIB (viz Tabulka 15).

Tabulka 15 Hodnocení dodavatele dle NÚKIB (Metodika řízení dodavatelů, © 2024)

HODNOCENÍ DODAVATELE		
Hodnotil:		
Datum hodnocení:		
Základní informace o dodavateli		
Název subjektu (firma):		
IČ:		
Adresa (sídlo):		
Statutární zástupce:		
Právní forma:		
Základní kapitál:		
Oblast hodnocení	**Počet bodů**	**Komentář**
Historie/pověst dodavatele:		
Certifikace:		
Reference ze spolehlivých zdrojů:		
Transparentnost vlastnické struktury:		
Kvalita a dostupnost informací z veřejných zdrojů:		
Předchozí zkušenosti:		
kvalita spolupráce		
kvalita technické podpory		
dodržení termínů dodávky		
včasné informace o změnách a jejich zdůvodnění		
reklamace a případné problémy s jejich uplatněním		
výsledky zákaznických auditů u dodavatele		
Výsledek hodnocení		
Celkový počet bodů:	**0**	
Zařazen do kategorie:	**B**	

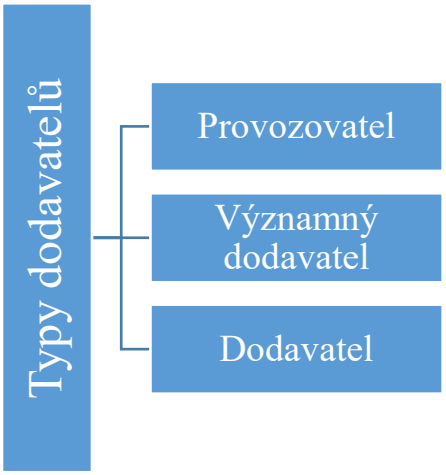
Důležité je tyto informace získávat z legálních a ověřených zdrojů. Pro vyplnění zjištěných informací do tabulky je možné využít bodovací systém, který taktéž uvádí NÚKIB, který má hodnoty 2 až -2. Je zde uveden popis jednotlivého bodování a vodítko, které uvádí možné situace, které vyplývají z bodového ohodnocení. Bodová hodnocení se přiřazují každé z oblastí a po následném sečtení a získání celkového počtu bodů je dodavatel zařazen do kategorie A až D. Dle tohoto je pak snazší se rozhodnout, zda dodavatele přijmout či nikoli.

Smluvní náležitosti dodavatelů – Jejich náležitosti jsou ve smlouvách stanoveny standardní právní formulací, měly by však obsahovat konkrétní náležitosti a povinnosti. Dle nově vznikající Vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností jsou to tyto požadavky:

- Ustanovení o auditu dodavatele.
- Ustanovení o řetězení dodavatelů.

- Ustanovení upravující tzv. exit strategií, podmínky ukončení smluvního vztahu u pohledu bezpečnosti.
- Ustanovení o sankcích za porušení smluvních povinností.
- Ustanovené o oprávnění užívat data.
- Ustanovení o autorství programového kódu, případě o programových licencích.
- Ustanovení o důvěrnosti smluvního vztahu.
- Ustanovení upravující povinnost dodržovat pravidla pro dodavatele, se kterými byli relevantní pracovníci dodavatele prokazatelně seznámeni.
- Ustanovení o řízení změn.
- Ustanovení o kybernetických bezpečnostních incidentech souvisejících s plněním smlouvy.
- Ustanovení upravující zajištění řízení kontinuity činností.
- Náležitosti smlouvy o úrovní služeb a způsobu a úrovni realizace bezpečnostních opatření.

Vhodné je zahrnout také specifické požadavky, které jsou v souladu s poskytovanými službami (Návrh zákona o kybernetické bezpečnosti, © 2024). Vhodným krokem jsou pravidelné kontroly smluv, které se týkají zavedených bezpečnostních opatření. Dodavatelé musí být rozděleni na provozovatele (rozumíme provozovatele nebo správce informačních nebo komunikačních systémů), významné dodavatele a dodavatele. U významného dodavatele je kontrola doporučena každého půl roku a u dodavatele každý rok.



Obrázek 16 Základní typy dodavatelů dle Vyhlášky o KB (vlastní)

Za kontrolu smluvních náležitostí je odpovědný zaměstnanec, který je nazýván jako „zaměstnanec odpovědný za smluvní vztah“, který je předem určen. Kontrolovanými náležitostmi může být například zajištění důvěrnosti, dostupnosti a integrity informací, postupy předávání informací třetím stranám, výsledky kybernetických bezpečnostních incidentů či aktualizace hodnocení rizik souvisejících s dodavatelem v souhrnném hodnocení rizik (Metodika řízení dodavatelů, © 2024).

Odebrání klíčů pracovníkům úklidu – Pracovníci úklidu jsou z hlediska kybernetické bezpečnosti považování za vysokou bezpečnostní hrozbu. Jedná se o nejméně placenou skupinu, která by mohla být lehce ovlivnitelná a podplacena, aby zajistila důležité informace, které by mohly být pro iniciátora zásadní například pro následné vydírání subjektu. I přesto, že pracovníci úklidu uklízí kanceláře krizového řízení pod dohledem osoby, které kancelář patří, mají k dispozici vlastní klíče k těmto prostorům. Z tohoto hlediska by neměl být problém klíče pracovníkům úklidu odebrat, protože dle vnitřní bezpečnostní politiky mohou do kanceláří vstupovat jen pod dohledem, vlastnit náhradní klíče ztrácí smysl a zvyšuje bezpečnostní riziko úniku informací.

7.5 Bezpečnost lidských zdrojů

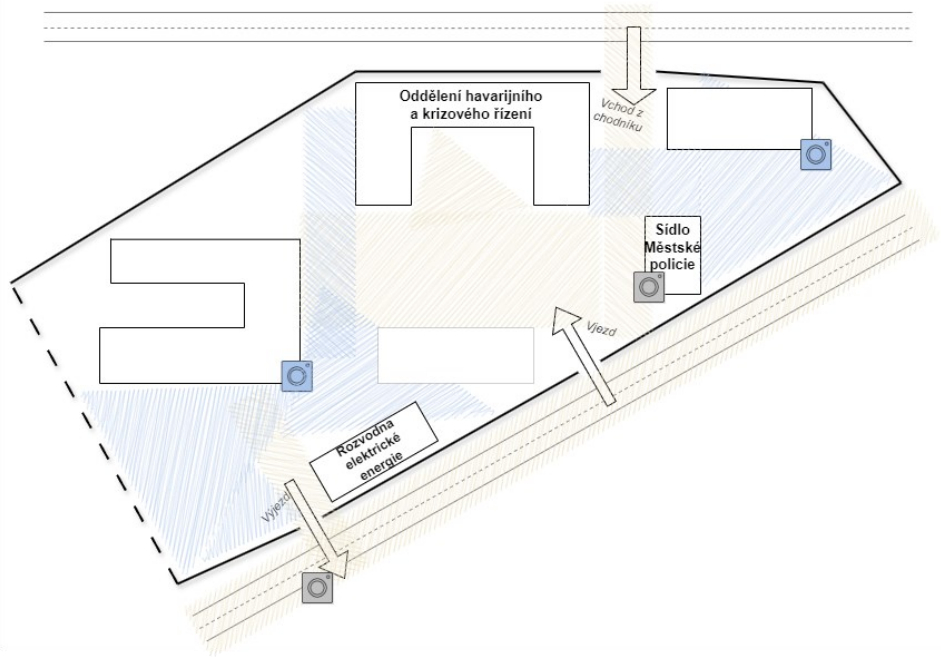
Zavedení pravidelného přezkušování zaměstnanců – Subjekt uvádí, že nepřezkušuje zaměstnance z důvodu důrazu na „slovíčkaření“ ve formálních testech. Není nutné využívat formální testy. Každoročně probíhá školení zaměstnanců z hlediska kybernetické bezpečnosti a pokaždé je zaměřeno na jinou oblast. Vhodným řešením je před každým školením vytvořit krátký test, který je zaměřen na dané téma o délce 5-10 otázek, což záleží na zvoleném tématu. Dalších nanejvýš 5 otázek se může týkat obecného přehledu, který by mohl obsahovat například otázky uvedené níže, popřípadě otázky podobného charakteru:

- Co si představujete pod termínem „zásada prázdného pracovního stolu“?
- Co si představujete pod termínem „zásada prázdné obrazovky“?
- Co je potřeba udělat, pokud si posíláte k tisku dokumenty, které obsahují osobní údaje?
- Jak zareagujete ve chvíli, kdy zjistíte, že jste ztratili přístupovou kartu?
- Jak byste zacházeli s e-mailem, který přišel od cizího odesílatele a obsahuje hypertextový odkaz na možnou výhru?

Ověřování minulosti uchazečů – Spoléhat pouze na údaje uvedené v životopise je nedostatečné. Ověřování bezúhonnosti uchazečů je na místě, k tomuto by se měla ověřovat také bezdlužnost, například protože se lidé v exekuci mohou zachovat nepoctivě. Mimo to je vhodné ověřit platnost dokladů uchazeče včetně pracovního víza či povolení k pobytu, jedná-li se o cizince. V případě uvádění vzdělání či certifikace, je vhodné platnost těchto dokumentů ověřit. Tyto a některé další náležitosti je schopna platforma Backround Check Scaunt zkontrolovat a ověřit. Platforma nabízí různé stupně nabídek, dle potřeby subjektu. Cena se pohybuje od 250 Kč až k 4 150 Kč za prověřovanou osobu, je zde také možnost sestavit si vlastní „balíček" ověřovaných skutečností. Minulost uchazečů, především z hlediska činnosti na sociálních sítích je možné prověřit pomocí OSINT, které může poskytnout podstatné informace o uchazeči. Pomocí OSINT lze provést sběr a analýzu informací z otevřených veřejně dostupných zdrojů, díky čemuž lze zjistit, zda je uchazeč vhodný pro pracovní pozici.

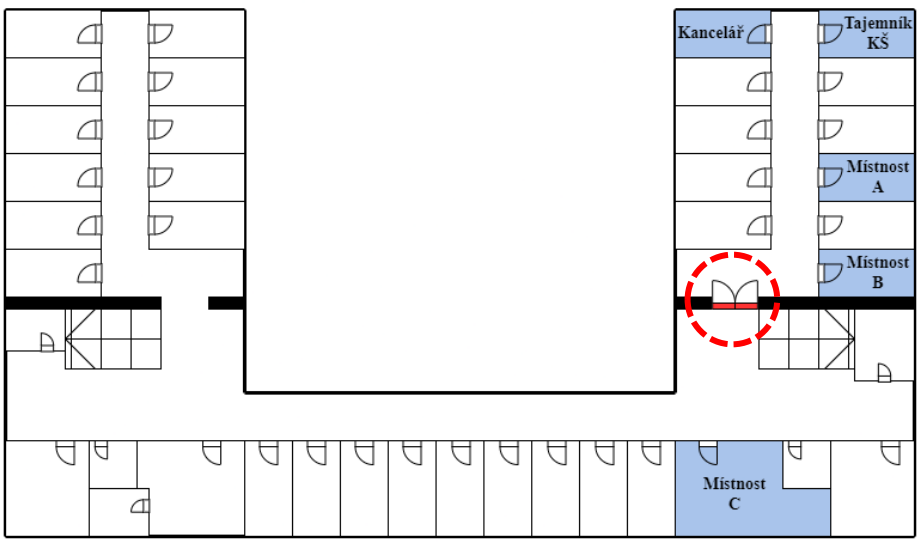
7.6 Řízení přístupu

Zabezpečení kamerovým systémem – Areál je z části pokrytý kamerami, nedohlédne však na všechna místa areálu (viz Obrázek 8). Návrhem je přidat další dvě kamery (vyobrazeny modrou barvou), což by zajistilo pokrytí kamerami téměř celého prostoru (viz Obrázek 17). Vzhledem k tomu, že v nočních hodinách neprobíhají žádné obchůzky ze strany Městské policie, ale hlídají prostor jen skrze kamerový systém, zajistilo by další rozmístění kamer téměř 100% přehled o oblasti areálu. Pokud by byly instalovány další dvě kamery, nebyla by potřeba zajišťovat také vnitřní prostory kamerovým systémem.



Obrázek 17 Návrh rozmístění dalších kamer v areálu subjektu (vlastní)

Umístění průchozích dveří v patře oddělení havarijního a krizového řízení – Nejen hlavní vchod do budovy, ale i veškeré průchody jsou během úředních hodin odemčeny a do prostor mohou občané volně vstupovat. Oddělení havarijního a krizového řízení se nachází v jednom z vyšších podlaží a lze se zde jednoduše dostat po schodištích, která se nacházejí v obou křídlech budovy (viz Obrázek 10). Návrhem je umístění průchozích dveří, které budou zamčeny i během úředních hodin a vstup bude umožněn za pomocí čipové karty, kterou každý zaměstnanec subjektu vlastní. Umístění průchozích dveří na čipovou kartu je vyobrazeno na obrázku níže.

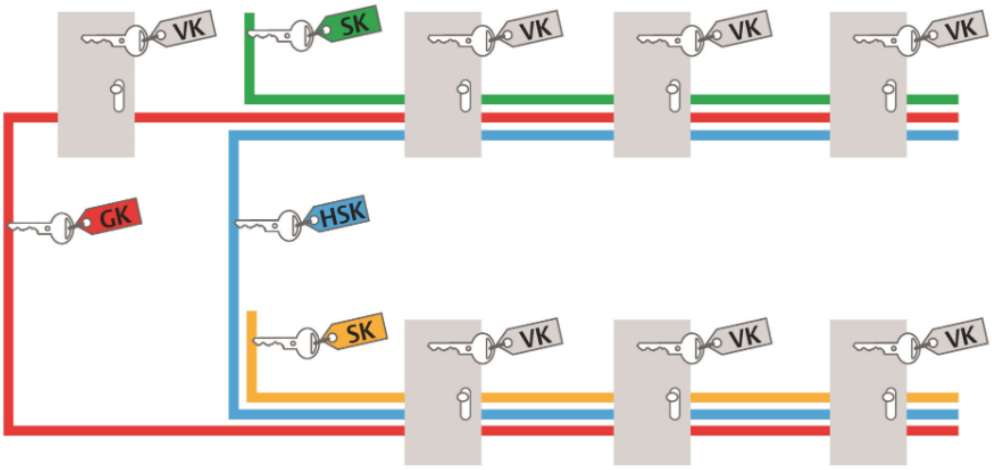


Obrázek 18 Návrh umístění průchozích dveří na čipovou kartu (vlastní)

Umístění je zvoleno na místě před vstupem do kanceláří pracovníků krizového řízení a dvěma místnostmi určenými pro zasedání krizového štábu. Místnost C by se nenacházela v „uzamčeném prostoru“, protože by se před tuto místnost dveře těžko umisťovaly nejen z důvodu dvou různých schodišť. V místnosti C se za běžné situaci, kdy není vyhlášen jeden z krizových stavů nenachází žádné citlivé informace.

Zabezpečení kanceláří krizového řízení – Pokud by nebyly umístěny průchozí dveře, viz předchozí návrh, bylo by vhodné zabezpečit kanceláře krizového řízení mimo klíče také čtecím zařízením na čipovou kartu. Čipovou kartu by vlastnili pouze dva pracovníci na oddělení havarijního a krizového řízení. Zavedení tohoto opatření by nemělo být finančně nákladné z důvodu, že některé kanceláře subjektu jsou tímto již opatřeny.

Zavedení systému generálního klíče – Vzhledem k velkému počtu místností a počtu zaměstnanců by zavedení systému generálního klíče mohlo mít pozitivní přínos pro řízení přístupu. Generální klíč by vlastnil bezpečnostní manažer společně s tajemníkem úřadu. Měli by tak přístup do veškerých prostor subjektu. Vedoucí oddělení by měli hlavní skupinový klíč, který by odemykal pouze dveře týkající se daného oddělení, popřípadě dalších místností, které využívají pro svou práci. Jednotliví zaměstnanci by pak vlastnili skupinový klíč, který umožňuje přístup pouze do jejich kanceláře a dalších potřebných místností. Zaměstnanci, kteří používají k výkonu práce pouze jednu kancelář by vlastnili takzvaný vlastní klíč. Pro lepší pochopení rozdělení jednotlivých klíčů (viz Obrázek 19). V kombinaci s čipovými kartami by tak mohl subjekt dosáhnout nejen vyšší bezpečnosti, ale také lepšího přehledu o počtu klíčů a jejich vlastnictví. Systém generálního klíče by mohl nahradit velký počet klíčů, který mají například vedoucí oddělení (viz Obrázek 11), což by vedlo ke snížení nákladů.



Obrázek 19 Systém generálního klíče (Princip systému, © 2024)

Jednotná bezpečnost náhradních klíčů – I když pravidla vnitřní politiky, uvádí že náhradní klíče mají být zapečetěny, ve skutečnosti tomu tak není. Vedoucí oddělení havarijního a krizového řízení má uloženy náhradní klíče spolu s dalšími potřebnými klíči pro výkon práce ve stejné uzamykatelné skříňce (viz Obrázek 11). Návrhem je oddělit tyto dvě skupiny klíčů a náhradní umístit do uzamykatelné a zároveň pečetí opatřené skříňky. Další klíče, které slouží k výkonu práce je možné zanechat tak jak jsou v současnosti umístěny, popřípadě zvážit zavedení hlavního klíče. Tím by se docílilo snížení počtu klíčů v jeden jediný, který může mít vedoucí oddělení neustále u sebe a na stávající skříňku přidat pečeť, což by bylo z hlediska vynaložení zdrojů nejpřívětivější.

Odebírání přístupu k systémům – V rámci zajištění vysoké úrovně kybernetické bezpečnosti subjektu je vhodné zavést vnitřní pravidlo o odebírání přístupu k systémům dva měsíce před uplynutím výpovědní lhůty. Odebírání přístupu by se mělo týkat především systémů, které zpracovávají citlivé údaje a obsahují informace, které by mohly poškodit nejen pověst subjektu, ale také narušit informační bezpečnost, z důvodu, že subjekt pracuje s velmi citlivými osobními údaji.

7.7 Řešení kybernetických bezpečnostních incidentů

Adekvátní reakce na ransomware útoky – Ačkoli je subjektu k dispozici *Response Plan*, bylo uznáno, že obsahuje tolik možností, že nejsou schopni adekvátně reagovat. Návrhem je zpracovat vlastní plán reakce na ransomware útoky a *Response Plan* použít jako inspiraci ke zpracování. Prvním krokem by mělo být cvičení, kdy bude simulováno několik útoků ransomware. Následně by oddělení IT mělo postupně projít veškeré činnosti, které *Response Plan* obsahuje a na základě rychlosti, správnosti a uchráněných aktiv postupně zjistit, které kroky z *Response Plan* propsat do vlastního dokumentu reakce na ransomware útoky.

Tato činnost sice může zabrat mnoho času, v řádu týdnů, ale v případě napadení tímto typem útoku, bude subjekt náležitě připraven a bude schopen reagovat okamžitě a může zabezpečit minimální ztrátu citlivých informací.

ZÁVĚR

Diplomová práce se zabývala kybernetickou bezpečností se zaměření na životní cyklus informací ve vybraném subjektu, který je činný v oblasti ochrany obyvatelstva. V teoretické části byla přiblížena témata, která se dané problematiky týkají. V úvodu práce byl popsán současný stav ochrany obyvatelstva v České republice se zřetelem na právní předpisy a významné dokumenty týkající se řešené problematiky. Následovalo přiblížení současného stavu kybernetické bezpečnosti, nejen v České republice, ale také v zahraničí. Taktéž bylo přiblíženo právní prostředí řešené problematiky spolu s významnými institucemi, které se oblastí kybernetické bezpečnosti zabývají. Pro správné uchopení tématu byly definovány některé termíny, které jsou stěžejní pro pochopení náležitostí praktické části.

Vybrané statě kybernetické bezpečnosti obsahují témata, která jsou taktéž důležitá pro vybrané téma diplomové práce. Poměrně důkladně byla rozebrána triáda CIA a následně životní cyklus informací, kde byly zahrnuty stavy, kterých mohou informace nabývat. Poslední téma, kterému se teoretická část věnovala byly kybernetické hrozby současnosti, kde byla zahrnuta častá rizika kyberprostoru. Větší část kapitoly byla věnována sociálnímu inženýrství a hrozbám umělé inteligence, která je v poslední době stále skloňovaným tématem.

Praktická část diplomové práce byla zaměřena na vybraný subjekt, u něhož byla provedena analýza současného stavu životního cyklu informací. Pomocí metod sběru dat a informací, indukce, dedukce, řízených rozhovorů a dotazování byla napsána kapitola týkající se současného stavu vybraného subjektu. Kapitola byla doplněna o checklisty ve formě tabulek, pro získání lepší přehlednosti zavedených opatřeních. Obsahovala fotky z místa subjektu, které přibližují skutečnost bezpečnostních opatření a taktéž byly za pomocí softwarového nástroje vytvořeny nákresy areálu objektu pro získání lepší představy o subjektu.

V závěrečné části diplomové práce byla navržena opatření, která mohou subjektu pomoci zajistit vyšší úroveň kybernetické bezpečnosti z důvodu respektování nově vznikajícího zákona o kybernetické bezpečnosti společně s vyhláškou pro poskytovatele regulovaných služeb v režimu nižších povinností. Jedním ze zásadních zjištění byl nesoulad v rámci politiky náhradních klíčů. Jejich zabezpečení je stanoveno vedením subjektu, nicméně u vedoucího oddělení havarijního a krizové řízení dochází k porušování těchto předpisů. Řešení tohoto problému je součástí návrhové části.

Dalšími podstatnými zjištěními, která byla rozpracována v kapitole o současném stavu a následně řešena v návrzích opatření, jsou nedostatečné ověřování dodavatelů, Mobile Device Management u pracovníků krizového řízení, přezkušování zaměstnanců v oblasti kybernetické bezpečnosti a zpracování postupu pro řešení ransomware útoků.

První výzkumnou otázkou bylo, jak jsou naplněny požadavky zabezpečení životního cyklu informací vybraného subjektu z hlediska kybernetické bezpečnosti. Dalo by se říci, že celková kybernetická bezpečnost subjektu je na velmi dobré úrovni. Nicméně, pokud bychom se měli řídit novým zákonem, který teprve bude vcházet v platnost, není úroveň kybernetické bezpečnosti dostatečná. Nicméně, v návrzích opatření byla uvedena možná řešení, jak tuto úroveň kybernetické bezpečnosti zvýšit.

Další výzkumnou otázkou bylo, které prvky v životním cyklu informací ve vybraném subjektu nesplňují požadovanou úroveň kybernetické bezpečnosti. Životní cyklus informací obsahuje tří základní stavy, kterých mohou data nabývat – data v klidu, data v pohybu a data, která jsou zrovna používaná. Navíc sem patří i likvidace dat. Vzhledem ke zjištěným nedostatkům (viz Tabulka 14) můžeme říci, že ani jeden z prvků životního cyklu informací zcela nenabývá požadované úrovně kybernetické bezpečnosti.

Hlavním cílem práce bylo navrhnout opatření ke zlepšení současné úrovně kybernetické bezpečnosti v souvislosti s vybraným životním cyklem informací subjektu ochrany obyvatelstva. Za pomoci dílčích cílů, které byly stanoveny na začátku diplomové práce bylo dosaženo cíle hlavního.

Vedoucí oddělení infrastruktury a aplikací, správce operačních systémů poskytl vyjádření k navrhovaným opatřením, která jsou dle jeho názoru zcela na místě. Na základě nově vznikajícího zákona je velmi pravděpodobné, že bude vytvořeno nové pracovní místo z hlediska zajišťování kybernetické bezpečnosti, kde bude odpovědná osoba pověřena implementací bezpečnostních opatření v souladu s novým zákonem a vyhláškami. Diplomová práce bude tomuto člověku k dispozici jako podpůrný materiál pro implementaci navrhovaných opatření.

SEZNAM POUŽITÉ LITERATURY

Akční plán k Národní strategii kybernetické bezpečnosti ČR na období let 2021 až 2025, © 2023. Online. In: Národní úřad pro kybernetickou a informační bezpečnost. Dostupné z: https://nukib.cz/download/publikace/strategie_akcni_plany/akcni_plan_2021-2025.pdf. [cit. 2023-10-30].

Analýza hrozeb pro Českou republiku: Závěrečná zpráva, © 2024. Online. In: Úvodní strana - Hasičský záchranný sbor České republiky. Dostupné z: https://www.hzscr.cz/soubor/analyza-hrozeb-zprava-pdf.aspx. [cit. 2024-01-25].

ARGINTARU, Daniel, © 2003–2023. *Data Encryption - Data at Rest vs In Transit vs In Use*. Online. Cloud Cybersecurity Services for Email, Data and Web | Mimecast. Dostupné z: https://www.mimecast.com/blog/data-in-transit-vs-motion-vs-rest/. [cit. 2023-10-30].

Artificial Intelligence, © 2024. Online. SAS: Analytics, Artificial Intelligence and Data. Dostupné z: https://www.sas.com/en_us/insights/analytics/what-is-artificial-intelligence.html. [cit. 2024-04-13].

Bezpečnostní strategie České republliky 2023, © 2024. Online. In: Ministerstvo obrany a Armáda České republiky. Dostupné z: https://mocr.army.cz/images/id_40001_50000/46088/Bezpecnostni_strategie_Ceske_republiky_2023.pdf. [cit. 2024-01-25].

BOEHM, Amber, © 2024. *What Is Data Loss Prevention (DLP)?* Online. CrowdStrike: Stop breaches. Drive business. Dostupné z: https://www.crowdstrike.com/cybersecurity-101/data-loss-prevention-dlp/. [cit. 2024-01-29].

COOPER, Stephen, © 2024. *Data at Rest vs. Data in Motion*. Online. Comparitech - Tech researched, compared and rated. Dostupné z: https://www.comparitech.com/net-admin/data-at-rest-vs-data-in-motion/. [cit. 2024-01-29].

Cybersecurity, © 2024. Online. National Insitute od Standards and Technology. Dostupné z: https://www.nist.gov/cybersecurity. [cit. 2024-04-08].

Digital Operational Resilience Act (DORA), © 2024. Online. Homepage - European Union. Dostupné z: https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en. [cit. 2024-04-08].

DINIC, Marko, © 2024. *A Complete Guide to Encryption — Data at Rest, Data in Motion and Data in Use*. Online. Best Data Archiving Solutions for All Indrustries | Jatheon. Dostupné z: https://jatheon.com/blog/data-at-rest-data-in-motion-data-in-use/. [cit. 2024-01-29].

DURAČINSKÁ, Zuzana, © 2023. *NIS: Co přináší nová směrnice EU o síťové a informační bezpečnosti?* Online. CZ.NIC. Dostupné z: https://www.nic.cz/files/nic/doc/ITSystems_NIS_102016.pdf. [cit. 2023-10-30].

EVANS, Lester, 2019. *Cybersecurity: what you need to know about computer and cyber security, social engineering, the internet of things + an esential guide to ethical hacking for beginners*. USA: Lester Evans. ISBN 9781794647237.

Evropská směrnice NIS2 a český zákon o kybernetické bezpečnosti, © 2024. Online. DReport – Zprávy o daních, účetnictví, právu a technologiích. Dostupné z: https://www.dreport.cz/blog/evropska-smernice-nis2-a-cesky-zakon-o-kybernetickebezpecnosti/. [cit. 2024-04-13].

Firepower Management Center Configuration Guide, Version 6.4, © 2024. Online. Networking, Cloud, and Cybersecurity Solutions – Cisco. Dostupné z: https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/clustering_for_the_firepower_threat_defense.html. [cit. 2024-02-21].

Glossary: Information and communication technology (ICT), © 2023. Online. Statistics Explained. Dostupné z: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Glossary:Information_and_communication_technology_(ICT). [cit. 2024-02-27].

GravityZone Business Security Enterprise, © 2024. Online. Globální leader v kybernetické bezpečnosti | Bitdefender.cz. Dostupné z: https://www.bitdefender.cz/gravityzone-business-security-enterprise. [cit. 2024-02-22].

Heading. Online. Draw.io. Dostupné z: https://app.diagrams.net/. [cit. 2024-03-17].

How to protect mobile devices from malware in the enterprise, © 2003 - 2024. Online. Enterprise Mobile Computing news and information. Dostupné z: https://www.techtarget.com/searchmobilecomputing/tip/How-to-protect-mobile-devices-from-malware-in-the-enterprise. [cit. 2024-04-15].

Chronologická geneze civilní ochrany (obrany), © 2023. Online. In: HZS Moravskoslezského kraje – Hasičský záchranný sbor České republiky. Dostupné z: http://www.hzsmsk.cz/sklad/kraoo/vyvoj_co.htm. [cit. 2023-10-18].

Informační bezpečnost: životní cyklus informace, © 2008–2023. Online. CleverAndSmart Management Consulting. Dostupné z: https://www.cleverandsmart.cz/informacni-bezpecnost-zivotni-cyklus-informace/. [cit. 2023-10-30].

Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník, © 2024. Online. In: Česká agentura pro standardizaci. Dostupné z: https://csnonlinefirmy.agentura-cas.cz/html_nahledy/36/510056/510056_nahled.htm. [cit. 2024-04-08].

IP address definition, © 2024. Online. Kaspersky Cyber Security Solutions for Home and Bussines. Dostupné z: https://www.kaspersky.com/resource-center/definitions/what-is-an-ip-address. [cit. 2024-02-21].

JIRÁSEK, Petr; NOVÁK a POŽÁR, Josef, 2022. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Online. Páté doplněné a upravené vydání. Praha: Česká pobočka AFCEA. ISBN 978-80-908388-4-0. [cit. 2023-11-27].

Klíčenka ID TAG Unique 125kHz EM4100 pro ZAMKA 50ks, © 2024. Online. In: Allegro - Super ceny - Hlavní stránka. Dostupné z: https://allegro.cz/nabidka/klicenka-cernobila-unique-125khz-em4100-50-kusu-14489482141?utm_feed=712e6653-4749-4512-b084-b6e297fc9e0b&ev_campaign_id=20035822444&gad_source=1. [cit. 2024-03-17].

KOLOUCH, Jan a BAŠTA, Pavel, 2019. *CyberSecurity*. Online. CZ.NIC. Praha: CZ.NIC, z.s.p.o. ISBN 978-80-88168-34-8. Dostupné z: https://knihy.nic.cz/files/edice/cybersecurity.pdf. [cit. 2023-10-20].

KONCEPCE OCHRANY OBYVATELSTVA do roku 2025 s výhledem do roku 2030, © 2024. Online. In: Úvodní strana - Hasičský záchranný sbor České republiky. Dostupné z: https://www.hzscr.cz/soubor/koncepce-oob-2025-2030-pdf.aspx. [cit. 2024-01-24].

Kybernetická bezpečnost, © 2023. Online. Bezpečnostní informační služba České republiky | BIS. Dostupné z: https://www.bis.cz/kyberneticka-bezpecnost/. [cit. 2023-10-30].

Kybernetická bezpečnost, © 2024. Online. Kybernetická bezpečnost - Cyber Security - dohledové centrum. Dostupné z: https://acsoffice.cz/kyberneticka-bezpecnost/. [cit. 2024-04-08].

Legislativa KB, © 2023. Online. Národní úřad pro kybernetickou a informační bezpečnost. Dostupné z: https://nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/. [cit. 2023-10-30].

LINHART, Petr, © 2023. *Pojmy 1. část*. Online. Úvodní strana - Hasičský záchranný sbor České republiky. Dostupné z: https://www.hzscr.cz/clanek/pojmy-1-cast.aspx?q=Y2hudW09NQ%3D%3D. [cit. 2023-10-18].

MARR, Bernard, © 2024. *The 15 Biggest Risks Of Artificial Intelligence*. Online. Forbes. Dostupné z: https://www.forbes.com/sites/bernardmarr/2023/06/02/the-15-biggest-risks-of-artificial-intelligence/. [cit. 2024-04-13].

Metodika řízení dodavatelů, © 2024. Online. In: Národní úřad pro kybernetickou a informační bezpečnost. Dostupné z: https://nukib.gov.cz/download/publikace/podpurne_materialy/Metodika-rizeni-dodavatelu.pdf. [cit. 2024-03-30].

Národní strategie kybernetické bezpečnosti ČR 2021-2025, © 2023. Online. In: Národní úřad pro kybernetickou a informační bezpečnos. Dostupné z: https://nukib.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2020-2025_%20cr.pdf. [cit. 2023-10-30].

Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury – znění od 22. 3. 2022, © 2010-2023. Online. Zákony pro lidi. Dostupné z: https://www.zakonyprolidi.cz/cs/2010-432#f5452926. [cit. 2023-10-30].

Návrh zákona o kybernetické bezpečnosti, © 2024. Online. In: ODol Portál. Dostupné z: https://odok.cz/portal/services/download/attachment/KORNCZQBPJJT/. [cit. 2024-03-30].

NÚKIB, © 2023. Online. Národní úřad pro kybernetickou a informační bezpečnost. Dostupné z: https://www.nukib.cz/cs/o-nukib/. [cit. 2023-10-30].

Obecné informace o směrnici NIS2 a budoucí národní úpravě, © 2023. Online. NUKIB (GUEST). Dostupné z: https://osveta.nukib.cz/mod/page/view.php?id=2582. [cit. 2023-10-30].

Phishing, © 1992-2024. Online. Antivirus a pokročilá internetová ochrana | ESET. Dostupné z: https://www.eset.com/cz/phishing/. [cit. 2024-02-05].

Princip systému, © 2024. Online. Vítejte - NOHAL Svět zámků - služby. Dostupné z: https://svetzamku-sluzby.cz/sluzby/system-generalniho-klice-a-hlavniho-klice/. [cit. 2024-04-13].

Quishing – vylepšená forma phishingu, © 2024. Online. Hlavní stránka | Komerční banka. Dostupné z: https://www.kb.cz/cs/o-bance/novinky/bezpecnost/quishing-vylepsena-forma-phishingu. [cit. 2024-04-08].

REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repe-aling Regulation (EU) No 526/2013 (Cybersecurity Act), © 2023. Online. In: EU law - EUR-Lex. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881. [cit. 2023-10-30].

RESPONDENT č. 1, 23. 1. 2024. *Bezpečnostní manažer.* Osobní rozhovor. Kancelář bezpečnostního manažera. Řízený rozhovor.

RESPONDENT č. 2, 31. 1. 2024. *Vedoucí oddělení infrastruktury a aplikací, správce operačních systémů*. Osobní rozhovor. Kancelář vedoucího oddělení infrastruktury a aplikací, správce operačních systémů. Řízený rozhovor.

RESPONDENT č. 3, 14. 3. 2024. *Vedoucí oddělení havarijního a krizového řízení*. Osobní rozhovor. Kancelář vedoucího oddělení havarijního a krizového řízení. Řízený rozhovor.

RESPONDENT č. 4, 22. 3. 2024. *Referent spisové služby*. Osobní komunikace. Elektronická pošta. Dotazování.

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

SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/1148 ze dne 6. červen-ce 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii, © 2023. Online. In: Národní úřad pro kybernetickou a informační bezpečnost. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32016L1148&from=EN. [cit. 2023-10-30].

Směrnice o odolnosti kritických subjektů CER – co přináší a jak se na ni připravit?, © 2024. Online. Deloitte Česká republika. Dostupné z: https://www2.deloitte.com/cz/cs/pages/risk/solutions/smercice-o-odolnosti-kritickych-subjektu-cer.html. [cit. 2024-04-08].

Traffic Light Protocol (TLP) Definitions and Usage, © 2023. Online. Home Page | CISA. Dostupné z: https://www.cisa.gov/news-events/news/traffic-light-protocol-tlp-definitions-and-usage. [cit. 2023-11-19].

Typologie dokumentů, © 2024. Online. In: Https://dl1.cuni.cz/mod/resource/view.php?id=196356. Dostupné z: https://dl1.cuni.cz/mod/resource/view.php?id=196356. [cit. 2024-04-12].

Vládní CERT, © 2023. Online. Národní úřad pro kybernetickou a informační bezpečnost. Dostupné z: https://www.nukib.cz/cs/kyberneticka-bezpecnost/vladni-cert/. [cit. 2023-10-30].

Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích – znění od 1. 1. 2023, © 2010-2023. Online. Zákony pro lidi. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-317#p3-1. [cit. 2023-10-30].

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) - znění od 28. 5. 2018, © 2010-2023. Online. Zákony pro lidi. Dostupné z: https://www.zakonyprolidi.cz/cs/2018-82#p1-1. [cit. 2023-10-30].

Vyhláška Ministerstva vnitra č. 380/2002 Sb., k přípravě a provádění úkolů ochrany obyvatelstva. Online. Zákony pro lidi. Dostupné z: https://www.zakonyprolidi.cz/cs/2002-380. [cit. 2024-01-24].

What is a DHCP Server?, © 2024. Online. Ifoblox | Simplify & Unite Networking and Security. Dostupné z: https://www.infoblox.com/glossary/dhcp-server/. [cit. 2024-02-22].

What Is a Firewall?, © 2024. Online. Networking, Cloud, and Cybersecurity Solutions - Cisco. Dostupné z: https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html#~related-topics. [cit. 2024-02-21].

What Is a LAN?, © 2024. Online. Networking, Cloud, and Cybersecurity Solutions - Cisco. Dostupné z: what-is-a-lan-local-area-network.html. [cit. 2024-02-27].

What is a Log in Computing?, © 2024. Online. Your One-Stop Shop for Laptops, PCs, Tablets & More | Lenovo US. Dostupné z: https://www.lenovo.com/us/en/glossary/log/. [cit. 2024-02-27].

What is Active Directory?, © 2024. Online. Quest | IT Management | Mitigate Risk | Accelerate Results. Dostupné z: https://www.quest.com/solutions/active-directory/what-is-active-directory.aspx. [cit. 2024-02-13].

What is an application delivery controller?, © 2024. Online. NetScaler: Application Delivery at Scale. Dostupné z: https://www.netscaler.com/articles/what-is-an-application-delivery-controller. [cit. 2024-02-28].

What is Anti-Malware & How Does It Work?, © 2024. Online. MSP Technology - IT Management Software. Dostupné z: https://www.connectwise.com/cybersecurity-center/glossary/anti-malware. [cit. 2024-02-27].

What Is BIOS?, © 2024. Online. Oficiální web Lenovo Česká republika | Notebooky, tablety, ... Dostupné z: https://support.lenovo.com/cz/cs/videos/vid100790-what-is-bios. [cit. 2024-02-29].

What is DNS?, © 2024. Online. Connect, Protect and Build Everywhere | Cloudflare. Dostupné z: https://www.cloudflare.com/learning/dns/what-is-dns/. [cit. 2024-02-21].

What is Hardware, © 2022. Online. Digital strategy agency in Spain | Digital Marketing | Marketplace. Dostupné z: https://www.arimetrics.com/en/digital-glossary/hardware. [cit. 2024-02-21].

What is IoT?. © 2023. Online. Oracle Česká republika. Dostupné z: https://www.oracle.com/cz/internet-of-things/what-is-iot/. [cit. 2023-11-18].

What is Phishing?, © 2024. Online. Phishing | General Phishing Information and Prevention Tips. Dostupné z: https://www.phishing.org/what-is-phishing. [cit. 2024-02-05].

What is Ransomware as a Service (RaaS)?, © 2024. Online. CrowdStrike: Stop breaches. Drive business. Dostupné z: https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/. [cit. 2024-02-05].

What is social engineering?, © 2023. Online. IBM – United States. Dostupné z: https://www.ibm.com/topics/social-engineering. [cit. 2023-11-17].

What is Software, © 2022. Online. Digital strategy agency in Spain | Digital Marketing | Marketplace. Dostupné z: https://www.arimetrics.com/en/digital-glossary/software. [cit. 2024-02-21].

What is the CISA difference?, © 2024. Online. In Pursuit of Digital Trust | ISACA. Dostupné z: https://www.isaca.org/credentialing/cisa. [cit. 2024-02-29].

What is Web Filtering?, © 2003 - 2024. Online. Email & Collaboration Security | Mimecast. Dostupné z: https://www.mimecast.com/content/web-filtering/. [cit. 2024-02-21].

YSoft SafeQ, © 2024. Online. Konica Minolta Business Solutions Czech spol. s r. o. | KONICA. Dostupné z: https://www.konicaminolta.cz/cs-cz/software/output-management/ysoft-safeq-(1). [cit. 2024-02-22].

Zákon č. 110/2019 Sb., o zpracování osobních údajů – znění od 24. 4. 2019, © 2010-2023. Online. Zákony pro lidi. Dostupné z: https://www.zakonyprolidi.cz/cs/2019-110#p2-1-a. [cit. 2023-10-30].

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) - znění od 6. 8. 2022., © 2010-2023. Online. Zákony pro lidi. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181#f5278856. [cit. 2023-10-30].

Zákon č. 239/2000 Sb. Zákon o integrovaném záchranném systému a o změně některých zákonů. In: Zákony pro lidi.cz. Online. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-239#p2-1-e. [cit. 2320-10-18].

Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti – znění od 1. 2. 2022, © 2010-2023. Online. Zákony pro lidi. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-412#p1-1. [cit. 2023-10-30].

Zpráva o stavu kybernetické bezpečnosti české republiky za rok 2022, © 2023. Online. In: Národní úřad pro kybernetickou a informační bezpečnost. Dostupné z: https://www.nukib.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_kyberneticke_bezpecnosti_CR_za_rok_2022.pdf. [cit. 2023-10-30].

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ADC	Application Delivery Controller
AP	Access Point
BIOS	Basic Input Output System
BIS	Bezpečnostní informační služba
BRS	Bezpečnostní rada státu
CEO	Chief executive officer
CERT	Computer Emergency Response Team
CIA	Confidentiality, Integrity and Availability
CISA	Certified Information Systems Auditor
COBIT	Control Objectives for Information and Related Technology
CSIRT	Computer Security Incident Response Team
ČSN	Česká soustava norem
DHCP	Dynamic Host Configuration Protocol
DLP	Data Loss Prevention
DNS	Domain Name System
EDR	Endpoint Detection and Response
EN	Evropské normy
ENISA	Evropská agentura pro bezpečnost sítí a informací
FTP	File Transfer Protocol
FTPS	File Transfer Protocol – Secure
GDPR	General Data Protection Regulation
GŠ AČR	Generální štáb Armády České republiky
HDD	Hard Disk Drive
HTTPS	Hypertext Transfer Protocol Secure
HZS	Hasičský záchranný sbor

ICT	Information and Communication Technologies (informační a komunikační technologie)
IP	Internet Protocol
IS	Informační systém
ISACA	Information Systems Audit and Control Association
ISMS	Information Security Management System (Systém řízení bezpečnosti informací)
ISO	International Organization for Standardization (Mezinárodní organizace pro normaliaci)
IT	Informační technologie
ITIL	Information Technology Infrastructure Library
IZS	Integrovaný záchranný systém
KB	Kybernetická bezpečnost
KI	Kritická infrastruktury
KS	Krizový stav
KŠ	Krizový štáb
LAN	Local Area Network
MAC	Media Access Control
MV	Ministerstvo vnitra
MZV	Ministerstvo zahraničních věcí
NATO	North Atlantic Treaty Organization (Severoatlantická aliance)
NCKB	Národní centrum kybernetické bezpečnosti
NCKO	Národní centrum kybernetických operací
NCOZ SKPV	Národní centrála proti organizovanému zločinu Útvar Služby kriminální policie a vyšetřování
NIS	Network a Information Security
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost

OO	Ochrana obyvatelstva
OPIS	Operační a informační středisko
OS	Odborná skupina
OSINT	Open Source Intelligence
RaaS	Ransomware-as-a-service
SaP	Síly a prostředky
SFTS	Secure File Transfer Protocol
SQL	Structured query language
SVS	Service Value System
TPL	Traffic Light Protocol
USB	Universal Serial Bus
ÚZSI	Úřad pro zahraniční styky a informace
VeKySIO	Velitelství informačních a kybernetických sil
VPN	Virtuální privátní síť
VZ	Vojenské zpravodajství
Wi-Fi	Wireless Fidelity
WPA	Wi-Fi Protected Access

SEZNAM OBRÁZKŮ

Obrázek 1 Struktura zajišťování kybernetické bezpečnosti v ČR (Národní strategie KB ČR 2021-2025, © 2023) 26

Obrázek 2 Triáda CIA a kybernetická bezpečnost 33

Obrázek 3 Struktura zákona a vyhlášek dle posledního návrhu NÚKIB (vlastní dle Evropská směrnice NIS2…, © 2024) 46

Obrázek 4 Přibližný nákres hlavního areálu subjektu (vlastní) 47

Obrázek 5 Hierarchie administrace chráněných aktiv (vlastní) 52

Obrázek 6 Virtuální rozdělení mobilního telefonu (vlastní) 53

Obrázek 7 Čtecí zařízení pro vstup do budovy (vlastní) 61

Obrázek 8 Pokrytí kamer v areálu subjektu (vlastní) 62

Obrázek 9 Čtecí zařízení jednotlivých průchodů (vlastní) 62

Obrázek 10 Půdorys patra s vyznačenými místnostmi týkající se KŘ (vlastní) 64

Obrázek 11 Skříňka s náhradními a dalšími klíči u vedoucího oddělení havarijního a krizového řízení (vlastní) 64

Obrázek 12 Diagram procesu změny hesla (vlastní) 66

Obrázek 13 Čip ke sdíleným zařízením (Klíčenka ID TAG…, © 2024) 67

Obrázek 14 Diagram procesu připojení zařízení do sítě (vlastní) 75

Obrázek 15 Swimlane diagram životního cyklu informací v rámci KS (vlastní) 81

Obrázek 16 Základní typy dodavatelů dle Vyhlášky o KB (vlastní) 87

Obrázek 17 Návrh rozmístění dalších kamer v areálu subjektu (vlastní) 90

Obrázek 18 Návrh umístění průchozích dveří na čipovou kartu (vlastní) 90

Obrázek 19 Systém generálního klíče (Princip systému, © 2024) 91

SEZNAM TABULEK

Tabulka 1 Checklist pro kategorii „zajišťování kybernetické bezpečnosti“ (vlastní) 49
Tabulka 2 Checklist pro kategorii „povinnosti vrcholového vedení“ (vlastní) 51
Tabulka 3 Checklist pro kategorii „řízení aktiv“ (vlastní) 54
Tabulka 4 Checklist pro kategorii „řízení rizik“ (vlastní) 56
Tabulka 5 Checklist pro kategorii „bezpečnost lidských zdrojů“ (vlastní) 57
Tabulka 6 Checklist pro kategorii „řízení kontinuity činností“ (vlastní) 59
Tabulka 7 Checklist pro kategorii „řízení přístupu“ (vlastní) 67
Tabulka 8 Checklist pro kategorii „řízení identit a jejich oprávnění“ (vlastní) 70
Tabulka 9 Checklist pro kategorii „detekce a zaznamenávání kybernetických bezpečnostních událostí“ (vlastní) 71
Tabulka 10 Checklist pro kategorii „řešení kybernetických bezpečnostních incidentů“ (vlastní) 73
Tabulka 11 Checklist pro kategorii „bezpečnost komunikačních sítí“ (vlastní) 76
Tabulka 12 Checklist pro kategorii „aplikační bezpečnost“ (vlastní) 77
Tabulka 13 Checklist pro kategorii „kryptografické algoritmy“ (vlastní) 77
Tabulka 14 Syntéza checklistů, zaměřena na záporné odpovědi 82
Tabulka 15 Hodnocení dodavatele dle NÚKIB (Metodika řízení dodavatelů, © 2024) 86

SEZNAM PŘÍLOH

Příloha P I: Přepis řízených rozhovorů

PŘÍLOHA P I: PŘEPIS ŘÍZENÝCH ROZHOVORŮ

ŘÍZENÝ ROZHOVOR S BEZPEČNOSTNÍM MANAŽEREM – RESPONDENT Č. 1

Otázka č. 1: Bude se na vás vztahovat směrnice NIS2? Pokud ano, připravujete se na její zavedení?

Ano, budeme pod ni spadat. Nepatříme pod zákon o kybernetické bezpečnosti. Chováme se tak, jako by zákon platil, ale přiměřeně, ne úplně ve všem, ale nebude to pro nás novinka, jen v některých oblastech.

Otázka č. 2: Máte definovány bezpečnostní parametry, které slouží k ochraně oblasti? Máte vypracován mapový podklad?

Ano, mapový podklad vypracován máme. Úřad sedí v osmi budovách. Do budovy, která sídlí mimo hlavní areál, se mimo pracovní dobu nikdo nedostane. Úředníci mohou do budov vstupovat od šesti hodin ráno, kdy se otevírá vstupní brána. Za ni následují dvoje skleněné dveře, které se otevírají na čip a zaměstnanci vstupují do objektu na čip. Přede dveřmi je recepce, pokud chce občan vstoupit, zahlásí se na recepci a buď je to v úředních dnech otevřené, nebo mají domluvenou schůzku a úředník si pro něj přijde a zase s ním odejde.

Všechny budovy fungují na čip. Omezen je přístup veřejnosti v neúřední dny. Údaje o tom, že zaměstnanci vstupují do budovy, se zapíše do systému, že tato osoba vstoupila, v kolik hodin apod.

Otázka č. 3: Jak je řešena fyzická bezpečnost kanceláří?

Je řešeno hlavně klíči a kartami. Hlavní vstup je na klíč a čip. Od budov nemá klíč žádný zaměstnanec, jen ti, kteří to potřebují k práci, to znamená, že se většina dostane jen na čip. Je naprogramováno v kolik hodin se otevírá a zamyká. Někteří mohou, protože k tomu mají povolení. Pokud by se do budovy potřeboval dostat někdo mimo hodiny, kdy je otevřeno, musel by přijít na Městskou policii, tam by se musel udělat záznam, přišel by s ním městský policista a odemkl budovu, pustil ho dovnitř a pak zase ven. Udělal by se záznam, že tam byl, co tam dělal, proč tam byl. Přes SMS by přišlo oznámení primátorovi a tajemníkovi, o tom, že tam někdo ze zaměstnanců byl. Psala by se formální zpráva. Vstup pro veřejnost je v úřední dny kromě úterý. Otevírá se v úředních dnech od osmi hodin. Zaměstnanci mohou do budov vstupovat od šesti do osmnácti hodin.

Otázka č. 4: Jak je chráněn fyzický vstup? Nejen do kanceláří, ale také do budovy (karta zaměstnance, docházkový systém apod.).

Po přiložení karty na docházkový systém, se zapíší údaje jako jméno, čas, všechny průchody. Zálohuje se napořád, podle nějakého režimu. Některé jsou zálohované na páskách, nepoužívají se, ale pro potřeby Policie při vyšetřování jsou uloženy. Zálohy mají informatici uloženy na serverech.

Otázka č. 5: Jsou kanceláře pod neustálým dohledem (kamerový systém, security)? Sledují kamery nepřetržitě? Existují záznamy nebo nahrávají jen v reálném čase? Popřípadě jak dlouho se záznamy ukládají a jsou zálohovány?

Kamerový systém není ani vevnitř, ani z venku. Městský kamerový systém dohlédne jen na některá místa.

Otázka č. 6: Kde a jak jsou uloženy klíče? Jak je to s generálním klíčem? Je opatřen pečetí?

Generální klíč se nepoužívá. Zaměstnanci mají vše řešeno kartou. Dveře se pomocí ní zamykají, a navíc jsou k tomu používány i klíče. Každý u sebe má vlastní klíč k prostorům, které potřebuje. Náhradní klíče má na starost správce budov, které to má v pracovní náplni. Všechny duplikáty má také Městská Policie, která sídlí pár metrů od budovy. Duplikáty jsou zamčené a zapečetěné ve skříňce. Pokud jsou použity, musí se sepsat protokol s uvedením důvodu, proč se otevíralo a proč byl klíč použit.

Otázka č. 7: Jak je řešena ochrana před fyzickými hrozbami, ať už úmyslnými či neúmyslnými?

Máme zpracovány různé scénáře. Pracovníci úklidu mohou vstupovat jen do některých kanceláří. Existují i místnosti, do kterých nemají vstup umožněn. Jsou nepřístupny všem, úklid je prováděn za účasti jiné osoby. V jedné z těchto místností byly ukládány citlivé informace a je to děláno tak, že by zde mohly být v případě potřeby.

Pracovníci úklidu chápeme jako bezpečnostní hrozbu. Problémové osoby se v objektu nachází pravidelně. Pracovníci mají tlačítko vyvedené k Městské Policii, nebo mohou použít klávesovou zkratku. Pokud se něco stane, okamžitě se kromě Městské Policie volá také státní, pokud je potřeba.

Otázka č. 8: Víte, co je zásada prázdné obrazovky a zásada prázdného stolu?

Zaměstnanci jsou o této politice poučeni. Cokoli, co by se nemělo dostat do rukou nepovolaných osob tam nesmí být volně položeno, zejména pokud opouští kancelář. Do některých kanceláří mají uklízečky přístup a takovéto věci musí být uzamčené ve skříňce k tomu určené. Všichni mají zámky a není problém si tyto věci schovat. Bere se to tak, že když jde úředník mimo kancelář, tak by to mělo být pod kontrolou, zejména když jde domů.

Otázka č. 9: Jak je řešena fyzická bezpečnost místností, kde zasedá krizový štáb?

Místnost je zabezpečena pouze za pomocí klíče. Je omezený počet lidí, kteří jej vlastní. Funguje pouze jako zasedací místnost, žádné důležité věci se zde nenachází.

Otázka č. 10: Jak jsou zabezpečena sdílená zařízení, pokud je používáte?

Využíváme sdílená zařízení. Fungují na čip, vytiskne se jen to, co si na tisk poslal konkrétní člověk. Využíváme SaveQ, který umožňuje tisk na jakékoli budově.

Otázka č. 11: Jaké máte základní postupy pro vzdělávání a školení v oblasti kybernetické bezpečnosti?

Zaměstnanci se seznámí s vnitřními předpisy, bezpečnostní politikou, interním a externím desaterem. Nově máme zavedeno jednoroční školení na nějaké téma bezpečnosti. Naposledy se jednalo o obecných nebezpečích na internetu, nebezpečí sociálních sítí, jak se dají tyto informace zneužít, poučení o trestné činnosti, když identitu někdo převzal.

Některé vzdělávací akce probíhají na intranetu. Bylo zveřejněno i video vytvořené ministerstvem vnitra týkající se aktivního střelce. Chceme jít spíše formou, že největší hrozbou je zaměstnanec za klávesnicí, který dokáže v nestřežené chvíli cokoli. Vědí, že nemají klikat na hypertextové odkazy, kontrolovat emailové adresy, klasické škodlivé e-maily, které stále chodí. Nemáme žádnou zkušenost se zaměstnancem, který by chtěl něco zneužít. Permanentně posíláme řetězec e-mailu o situacích, které v současné chvíli hrozí.

Otázka č. 12: Jak často školení probíhají?

Jednou ročně.

Otázka č. 13: Přezkušujete nějakým způsobem účastníky školení a jak často?

Nepřezkušujeme. Některé testy nic neřeší, formální testy týkající se například BOZP nebo požární ochrany jsou postaveny na slovíčkaření, než že by ověřili znalosti.

Otázka č. 14: Jak jsou chráněna koncová zařízení uživatele? Máte zavedeno desatero zásad, které musí zaměstnanci dodržovat? Probíhá periodická změna hesel? Jak máte toto ošetřeno (síla hesel, výměna čísel na konci hesel atd.)?

Máme zavedeno desatero základních bezpečnostních pravidel, které musí mít zaměstnanci neustále na paměti. Máme také zpracovány pokyny pro vytváření hesel. Nově jsou dvanáctimístná, přecházeli jsme z 9 na 12 míst. Změna hesla probíhá jen jednou za rok, protože je 12místné. Každý si může změnit heslo, když chce, minimálně však jednou ročně.

Hesla do počítačů a systémů jsou většinou totožná. Ve většině případů mají stejné uživatelské jméno, hesla se mohou měnit na každý úkon. Dle systému a podle toho, jak to systém vyžaduje se mění formát přihlášení, buď je to jméno a příjmení společně se zkratkou nebo osobní číslo. Systém kontroluje změnu hesel, například jestli uživatel nezměnil jen číslo na konci hesla. Pokud se tak stane, systém nedovolí heslo změnit.

Otázka č. 15: Když zaměstnanci nebo jiné zainteresované strany ukončují pracovní poměr, smlouvy nebo dohody, jaká jsou opatření v rámci kybernetické bezpečnosti? Např. zamezujete přístup tři měsíce před vypršení výpovědi, odebíráte přístup apod.?

Nemáme takováto opatření. Pokud by se jednalo o podezřelou osobu, nějaké kroky by určitě nastaly.

Otázka č. 16: Prověřujete minulost uchazečů, kteří se chtějí stát pracovníky? Je prověřování prováděno před nástupem a průběžně (s ohledem na platné zákony, předpisy a etiku)?

Obvykle věříme tomu, co je v životopise. Je možné, že si personalisté dělají kontrolu mimo, např. na sociálních sítích, ale spíše ne.

Otázka č. 17: Jak je zajištěna bezpečnost z hlediska lidských zdrojů, kontroly přístupu a správa aktiv? (NDA – dohoda o mlčenlivosti, autorizace, autentizace.)

Autentizaci a autorizaci vyžadují jen některé systémy, které vyžadují např. bankovní identitu – dotační programy. V tom případě většinou vyžaduje certifikát, QR kód apod., takovéto činnosti dělá jen omezený počet zaměstnanců. Ve smlouvách je jasně uvedena mlčenlivost. Zaměstnanci toto ctí.

Otázka č. 18: Jsou v pracovních smlouvách jasně uvedeny odpovědnosti pracovníků za informační bezpečnost?

Je to obecně řešeno ve smlouvách. Počítá se s tím, že zaměstnavatel může provést kontrolu.

Otázka č. 19: Máte identifikovány, zdokumentovány, pravidelně přezkoumávány a podepsány pracovníky a dalšími příslušnými zainteresovanými stranami dohody o důvěrnosti nebo mlčenlivosti (NDA), které odrážejí potřeby organizace v oblasti ochrany informací?

Ve smlouvách je to řečeno tak obecně, že jsou dlouhodobě univerzální. Použitelnost tohoto je napořád. Zainteresované strany mají vše řešeno ve smlouvách. Pokud tyto strany jakýmkoli způsobem nakládají s informacemi, jsou přísně pod sankcemi a možností okamžité výpovědi.

Otázka č. 20: Máte formalizován a oznámen disciplinární postup pro přijímána opatření vůči pracovníkům a dalším zainteresovaným stranám, které se dopustily porušení politiky informační bezpečnosti? Používáte případně pozitivní motivaci pro ty, kteří všechna pravidla dodržují?

Nepoužíváme pozitivní motivaci, jen dobrý pocit z dobře odvedené práce. Postihy by teoreticky být mohly. Nepravidelně probíhá kontrola spolu s tajemníkem, kdy jsou nám otevřeny dveře vedoucím oddělení nebo vedoucím odboru a kontrolujeme, zda je kancelář v požadovaném režimu. Opravdu na stole nebudou žádné osobní údaje, citlivé už vůbec ne. Citlivé údaje jsou zvláštní kategorií a nakládá se s nimi jinak. Pokud by se něco stalo, okamžitě bychom si se zaměstnancem promluvili. Pokud by to nepomohlo, provede rozhovor personalista a provede se návrh na snížení jeho platu. Přístup je spíše takový, že si zaměstnance vychováváme a není v pořádku odejít od nezamknuté obrazovky nebo odejít a nezamknout stůl.

Otázka č. 21: Máte filtrovány přístupy na webové stránky?

Zaměstnanec se pravděpodobně může dostat kam bude chtít pomocí svého telefonu nebo tabletu. Na YouTube se dostanou jen někteří zaměstnanci, pro svůj výkon, pro prezentaci města. Máme detekovány všechny stanice, takže víme přesně kdo co vyhledává.

Otázka č. 22: Jakým způsobem probíhá přidělování a používání privilegovaných přístupových práv?

Podle funkce činnosti, dle činnostní role a podle zaměření. Záleží, kdo s čím může pracovat a podle toho dostane oprávnění. Toto oprávnění se vymezuje vedoucím odboru a vedoucím oddělení, aby věděli, kdo může do dané agendy vstupovat a že se nedostane někam kde nemůže. Když zaměstnanec přechází na jinou pozici, jeho práva jsou přezkoumána a změní se podle jeho funkce.

Otázka č. 23: V rámci administrace chráněných aktiv, máte odpovědnou osobu? Má tato osoba dostatečnou odbornost v oblasti?

Jako bezpečnostní manažer zastřešuji tyto úkony, nemůžu být ale u každého dílčího úkonu. Např. u kontroly serverovny. Určím tedy správce konkrétního aktiva, podle funkce, podle typu aktiv. Tento člověk je pak vzděláván ke svým úkonům.

Otázka č. 24: Jak máte zabezpečeny systémy nouzové komunikace v rámci objektu?

Máme poplach, který je schopen pouze tónů. Upgradujeme systém pro nouzovou komunikace se zaměstnanci pomocí hromadných SMS a e-mailů. Přístup k tomuto by mělo jen několik lidí v případě kybernetických útoků, aktivního střelce atd. aby byla zajištěna komunikace v reálném čase. Někteří zaměstnanci mají přidělený služební telefon, ale jsou i zaměstnanci, kteří služební telefon nemají. Jejich telefonní čísla vedeme a prostřednictvím těchto bychom je kontaktovali. Tím, že úřad sídli i mimo areál, přišla by SMS i kdyby se něco odehrávalo tam. Abychom varovali zaměstnanci před vstupem do této budovy. Přes 350 zaměstnanců bude ihned vědět, že se něco děje. Komunikovat se mohou jen krizové situace.

Otázka č. 25: Jaký je postup pro řešení kybernetických bezpečnostních incidentů? Jaký je rozsah spolupráce s týmy CSIRT, ČIMIB (Český institut manažerů informační bezpečnosti) a kontaktními místy?

Máme vedeno ve vnitřních politikách. Spolupracovali jsme při jednom kybernetickém útoku, který nastal. Spolupracovali jsme s CSIRT a úřadem pro kybernetickou bezpečnost. Nedošlo k žádné škodě, na krátkou dobu byl úřad uzavřen, kdy jsme vše obnovili a zjistili příčinu. Došlo k zavirování šesti počítačů, nic dalšího nakaženo nebylo. Zaměstnanci přišel e-mail, ve kterém kliknul na závadný odkaz.

Otázka č. 26: Máte zpracován seznam aktiv?

Seznam aktiv byl zpracován kdysi dávno, ale budeme jen aktualizovat dle nového zákona o kybernetické bezpečnosti.

Otázka č. 27: Máte vytvořen inventář informací a dalších souvisejících aktiv, včetně vlastníků?

Každé aktivum by mělo mít svého Mandáta, který by se o to měl starat. Některé věci budeme propojovat. Ty aktiva budeme vytvářet pro celý proces. Spisová služba bude mít všechny věci, od serveru přes systémy. Bude jeden centrální garant a poté budou částeční vlastníci po celém serveru. Není to dle zákona, budeme to dělat proto, aby to mělo lepší logiku. Máme

páteřní aktiva, která jsou pro nás nejdůležitější a pak budou nějakým způsobem opečovávána ve smlouvách i dodatcích, možná i s poskytovatelem. Např. mailová služba je velmi důležitá, stejně tak webové stránky a komunikace s ministerstvy. Některé věci musí být řešeny prioritně, některé počkají. Když nějaká webová služba nepůjde pár hodin tak to nevadí, pokud týden tak už to problém je. Servisní organizace má ve svých plánech, že musí reagovat do nějakých vteřin, minut nebo hodin, záleží od konkrétní služby.

Otázka č. 28: Které osoby, popřípadě pozice jsou vrcholovým vedením? Jsou prokazatelně poučeny o jejich povinnostech a rozsahu odpovědností? Je zajištěna dostupnost zdrojů potřebných pro zajišťování kybernetické bezpečnosti?

Vrcholové vedení tvoří vedení města což je primátor, 1. náměstek primátora, náměstek primátora, uvolněný radní + tajemník úřadu. Vedení města je proškolováno v oblasti kybernetické bezpečnosti. Finanční prostředky jsou pravidelně vynakládány.

Otázka č. 29: Jak jsou řešen povinnosti vrcholového vedení s ohledem na zajišťování kybernetické bezpečnosti?

Nemáme stanoveno právně, na kybernetické bezpečnosti se podílí odbor informatiky, bezpečnostní manažer atp.

Otázka č. 30: Jak dlouhá je výpovědní lhůta?

Dva měsíce.

Otázka č. 31: Jsou dodavatelé různých služeb ověřování z hlediska věrohodnosti? Pokud ano, jakým způsobem ověřování probíhá? Mají uzavřené smlouvy na dobu určitou či neurčitou, nebo se to liší u jednotlivých dodavatelů?

Dodavatelé jsou ověřování odborem informatiky individuálně na základě referencí atp.

Otázka č. 32: Jaké náležitosti mají dodavatelé ve smlouvě uvedeny?

Standardní právní formulace.

Otázka č. 33: Je prostor areálu v noci monitorován, např. Městskou policií? Provádí pravidelné obchůzky?

Městská policie má v areálu kamery a operační středisko. Vidí, co se v areálu děje.

Otázka č. 34: Na která místa dohlédne kamerový systém města?

Městský kamerový systém prokazatelně napomáhá vytvářet podmínky ke zvyšování bezpečnosti občanů, ochraně jejich majetku a zdraví. V blízkosti areálu se nachází dvě stacionární kamery. Od podzimu 2021 disponuje kamerový systém online a offline inteligentními funkcemi, díky kterým je možné rozpoznat objekty nebo uživatelem definované situace, a následně je pak velmi rychle vyhledat ve videozáznamu.

Otázka č. 35: Máte ustanoveny pozice Architekta KB, Auditora KB a Garanta aktiv?

Nemáme na úřadě zřízeny tyto pozice, nespadáme pod Zákon o kybernetické bezpečnosti, takže tyto pozice nemusíme zřizovat.

Otázka č. 36: Jsou zaměstnanci, administrátoři, osoby odpovědné za kybernetickou bezpečnosti a dodavatelé povinni oznamovat neobvyklé chovní technických aktiv a jiná podezření na jakékoliv zranitelnosti?

Oznamování neobvyklého chování technických aktiv musí všechny tyto osoby ihned hlásit odboru informatiky, je to i v jejich zájmu.

ŘÍZENÝ ROZHOVOR S VEDOUCÍM ODDĚLENÍ INFRASTRUKTURY A APLIKACÍ, SPRÁVCE OPERAČNÍCH SYSTÉMŮ – RESPONDENT Č. 2

Otázka č. 1: V kontextu přístupu zaměstnanců do budov – vstupují na čip. Do jakého systému se tyto údaje zapisují? Které údaje se zapisují a probíhá zápis v reálném čase? Probíhá záloha? Máte synchronizovány hodiny?

Údaje jsou zapisovány do Microsoft databáze. Máme 5 velkých databází a dalších 15 od společnosti Microsoft. Zálohu provádíme celkovou (full) a inkrementální. Zálohuje se každých 5 vteřin. V noci se zálohuje vše.

Otázka č. 2: Jak jsou chráněna koncová zařízení uživatele?

Stanice jsou chráněny pomocí Microsoft System Center Configuration Manager. Mimo Microsoft využíváme také Bitdefender, který zajišťuje péči.

Otázka č. 3: Jak máte řešena přístupová práva k počítačům?

Karty s certifikáty. Dle NIS2 budeme zavádět dvou-faktorové ověřování. Chtěli jsme zavádět už dřív, teď to bude povinné. Hesla pro uživatele jsou dvanáctimístná, administrátoři mají nyní šestnáctimístná, budou ale přecházet na sedmnáctimístná.

Otázka č. 4: Veškeré záznamy by měly být chráněny před ztrátou, zničením, falšování, neoprávněným přístupem a neoprávněným uvolněním. Jak máte řešenou tuto problematiku?

Pomocí Active Directory. Správa je buďto uživatelská nebo administrativní.

Otázka č. 5: Jsou nějakým způsobem chráněny kabely přenášející napájení, data nebo podpůrné informační služby? (Ochrana před odposlouchávánim, rušením, poškozením.) Používáte optický nebo metalický kabel?

Ochrana je chráněna klasickým způsobem. Nikdo nemá přístup kromě pár lidí. Máme systémy, které by okamžitě odhalili podezřelou činnost. Používáme oba kabely.

Otázka č. 6: Jak je zajištěna dostupnost, integrita a důvěrnost informací zařízení z hlediska správné údržby?

Máme parametry, které musíme splňovat. Například jsme museli zazdít okno v serverovně. Uklízečky mohou vstupovat jen s dohledem, ale úklid není potřeba, není tam prach, nikdo tam nechodí. Máme UPS hlavní datové centrum, které vydrží 3,5 hodiny. Máme také diesel agregát pro celý areál, který do půl minuty najede.

Otázka č. 7: Jaké máte postupy a nástroje pro bezpečné sdílení informací?

Máme přímo určený server, kde jsou nastavená práva. Je tam 300 přístupů. Přes tento server komunikuje i zastupitelstvo.

Otázka č. 8: Jak je řešeno řízení kontinuity provozu?

Máme zpracovány havarijní plány. Každého půl roku probíhá testování jen na kritické servery.

Otázka č. 9: S jakou periodou zkoušíte, zda fungují zálohy?

Stále se obnovují, nemusíme testovat, rychlejší je obnovení ze záloh než zjišťovat chybu.

Otázka č. 10: Jak máte zabezpečeny hlasové, obrazové a textové komunikace?

Antispam, Antivir. Web filtering, Firepower Cluster a ADC.

Otázka č. 11: Jakým způsobem jsou chráněna aktiva mimo prostory organizace (Mobile Device Management)? Kontrolujete, co na zařízeních uživatelé dělají?

Využíváme Mobile Iron. To znamená, že se mobil virtuálně rozdělí na dva. Na prvním je možné provádět kontrolu, instalovat na dálku, vidět umístění, šifrování… Druhá část je soukromá.

Otázka č. 12: Pracovníci krizového řízení také mají zabezpečeny telefony pomocí Mobile Iron?

Ne, jejich telefony jsou speciální, my jim z legrace říkáme protiatomové. Ty jsou odolné jen fyzicky. Zabezpečení úniku informací není nijak zabezpečeno, je to jen na tom člověku.

Otázka č. 13: Máte aktualizace vynucené?

Ano. Máme několik nástrojů. Serverovna má WSUS (Windows Server Update Services). U mobilních zařízení aktualizujeme vždy když Mobile Iron vydá aktualizace.

Otázka č. 14: Provádíte pravidelné aktualizace, jak u serverovny, tak u dalších zařízení?

Koncová zařízení aktualizujeme každé úterý, zaměstnanci musí nechat počítače zapnuté přes noc. Proběhne full scan antivirem a následně se zařízení aktualizují. Nekritické servery se neaktualizují tak často. Kritické servery jsou aktualizovány pravidelně, protože Microsoft vydává každé druhé a čtvrté úterý v měsíci záplaty pro své operační systémy.

Otázka č. 15: Máte filtrovány přístupy na webové stránky? Na úrovni DNS nebo na úrovni firewallu?

Jsou filtrovány. Máme i systémy, které prohledávají stránky pro některé slova, např. drogy, a pokud se toto slovo vyskytuje vícekrát je přístup na webovou stránku zablokován. V některých případech, pro některé účely, může být přístup povolen.

Ani na jedné z úrovní filtrování neprobíhá. Přímo software – webové brány za milion korun.

Otázka č. 16: Jak je řešena ochrana před škodlivým softwarem?

Pomocí Bitdefender. Poté máme EDR, což je inteligentní nástavba.

Otázka č. 17: Máte zpracovány informace o technických zranitelnostech používaných informačních systémů a následné vyhodnocení vystavení organizace těmto zranitelnostem?

K tomuto je určený technický konzultant. Co zvládneme sami, děláme samo. Co nezvládneme, dělá dodavatel. Pokud se něco děje, okamžitě se to řeší s dodavatelem. Dodavatelů máme 30–40. Nebo se dodavatel ozve sám.

Otázka č. 18: Jakým způsobem maskujete informace?

Za pomoci Bitdefender.

Otázka č. 19: Jak se řešena prevence úniku dat? (Systémy, sítě a jakákoli další zařízení, která zpracovávají, ukládají nebo přenášejí citlivé informace)

Application Delivery Controller, Flowmon – monitoring toků v síti. Antiviry, antispamy, web filtering.

Otázka č. 20: Jaké používáte zálohování? Plné, přírůstkové nebo rozdílové?

Plné a přírůstkové. Taktéž dvoustupňové zálohování na reduplikační a komprimační backup úložiště. Pásky jsou uloženy v trezoru v jiné budově kvůli požáru. Fungujeme na konceptu 3, 2, 1 – tři místa, dvě lokality, jedno offline.

Otázka č. 21: Jak pracujete s logy?

Vše s logy má na starost Dohledové SOC (Security Operation Center), které to dělá za nás. Posílá informace, když je potřeba.

Otázka č. 22: Monitorujete sítě, systémy a aplikace z hlediska abnormálního chování?

Flowmon a IBM TIVOLI.

Otázka č. 23: Máte odděleny skupiny informačních služeb, uživatelů a informačních systémů v sítích organizace?

Ano.

Otázka č. 24: Jaká je politika a jaké jsou postupy týkající se používání kryptografie?

Všechny na mobilech a na vybraných extérních discích.

Otázka č. 25: Šifrujete data na discích ve výchozím stavu? Jsou disky zaměstnanců šifrovány (např. BitLocker)? Používáte asymetrické šifrování? Jak silná máte hesla?

Ano, pomocí Bitlocker. Hesla jsou dvanácti až šestnáctimístná.

Otázka č. 26: Hashujete přihlašovací údaje?

Ano, systém to děla automaticky.

Otázka č. 27: Provádíte pravidelnou údržbu LAN a prvků ICT?

Údržba probíhá pomocí různých SW nástrojů (IBM TIVOLI monitoring, CISCO, network asistent atd.) a vše je monitorováno pomocí Flowmon. Flowmon okamžitě zahlásí.

Otázka č. 28: Probíhají u vás auditní testy a jiné ověřovací činnosti zahrnující posouzení provozních systému? Jak jsou naplánovány a následně odsouhlaseny?

Auditní testy na informatiku probíhají přibližně jednou za tři roky. Posouzení provozních systémů děláme pomocí penetračních testů, etických hackerů.

Otázka č. 29: Jaká máte bezpečnostní opatření k minimalizaci rizika SQL injection?

Právě penetrační testování.

Otázka č. 30: Využíváte VPN? Máte implementován firewall?

Ano využíváme VPN i firewall.

Otázka č. 31: Filtrujete přístup k síti dle MAC adres?

Ano, ale jen částečně. Máme poznačené všechna naše zařízení a v rámci protokolu RADIUS a NPS (Network Policy Server), tak když přijdete do naší sítě a napojíte se do datové zásuvky, tak ona zkontroluje, jestli jste naše zařízení nebo ne a když vás neověří tak vás hodí do takzvané karanténní sítě kde máte k dispozici jen internet. Skládá se to ze tří komponent a jedna z nich je MAC adresa, RADIUS server a NPP, navíc to spolupracuje s doménou, je tam více parametrů, kterými musí zařízení projít, aby bylo puštěno do naší sítě.

Otázka č. 32: Máte aktivní DHCP server? Využíváte rezervační list?

Je aktivní ve spolupráci s RADIUS a Network Policy Server. Ano, rezervační list používáme.

Otázka č. 33: Jak pracujete s BIOS? Máte jej zaheslovaný na každém koncovém zařízení?

Ano, na každém koncovém zařízení je zaheslován.

Otázka č. 34: Je povoleno bootování z externích zařízení?

Ne, není povoleno.

Otázka č. 35: Používáte defaultní přístupová údaje?

Ne. Toto řeší oddělení infrastruktury a hesla znají 4 lidi.

Otázka č. 36: Jak je řešeno zabezpečení Wi-Fi? Komunikujete po Wi-Fi jen nezbytné nebo i citlivé věci bez rozdílu?

Máme soukromou Wi-Fi, která je náležitě zabezpečena. Pro návštěvy máme jinou síť.

Otázka č. 37: Používáte šifrování WPA 2? Využíváte server RADIUS?

Používáme CISCO, nejlepší na trhu. CISCO centrálně ovládá cca 30 wifin, pomocí CISCO controlerů, pomocí kterých ovládáme koncové Wi-Fi Access Pointy, jsme schopni vidět kolik je připojených uživatelů, z jakých zařízení atd. Konkrétní Wi-Fi jsou pak zabezpečeny pomocí WPA 2. RADIUS využíváme.

Otázka č. 38: Jak často probíhá fyzická kontrola serverovny?

Jednou až dvakrát týdně. Jednou vždy, ale většinou dvakrát.

Otázka č. 39: Máte magnetické kontakty na dveřích, které zaznamenávají otevření dveří?

Ano, zaznamenává se do databáze s historií několika let. Jen odbor informatiky má čip, který si otevře elektronické dveře.

Otázka č. 40: Máte administrátorské účty technických aktiv? Měly by se využívat jen pro případ obnovy po kybernetickém incidentu a v nezbytně nutných případech.

Máme v trezoru v obálkách účty s nejvyššími oprávněními, které by se v případě kybernetického útoku nebo velké poruchy rozbalili a použili.

Otázka č. 41: Jak je řešeno přerozdělování zařízení v rámci subjektu? Formátujete je? Pokud ano, kolikrát? A jaký máte konkrétní postup?

Je určen konkrétní pracovník, který koncové zařízení vyčistí s využitím programu Eraser, kde si můžeme nastavit přepis 8x, 12x nebo 2x. Stává se, že se zařízení dostanou k HZS nebo do škol, kde zařízení nadále využívají.

Otázka č. 42: Testujete funkčnost záloh? Vyzkoušeli jste někdy cvičení? (Simulace různých kybernetických incidentů, jako jsou ransomware útoky, odstranění dat nebo selhání hardware. Poté se provede obnova záloh a ověří se, že je systém schopen vrátit se do provozu.)

Ano. Místo záloh máme i replikace, které testujeme 4x ročně v rámci testu havarijních plánů. Testujeme 25 kritických serverů. Stále obnovujeme. Děláme i cvičení. Postup v případě napadení ransomwarů je v Response Plan, kde je hodně variant. Je tam i možnost zaplacení, pokud se nepodaří obnovit. Je tam jak sehnat bitcoinovou peněženku, jak ji navít, jak jednat s hackery. Nemáme to úplně dotažené, je tam moc variant. Je zde i možnost využití firmy, která se na to specializuje.

ŘÍZENÝ ROZHOVOR S VEDOUCÍM ODDĚLENÍ HAVARIJNÍHO A KRIZOVÉHO ŘÍZENÍ – RESPONDENT Č. 3

Otázka č. 1: Jaký máte systém pro nouzovou komunikaci v rámci krizového řízení?

Máme dvě čidla pro zvedání hladiny řeky ve dvou městských částech, což je jako kdyby taková kamera, která je napájena solární energií a když se zvedne hladina tak přijde SMS. Běžně sledujeme stránky povodí, kde sledujeme aktuální situaci, tato zařízení nám ale právě umožňují dostat upozornění v reálném čase.

Další dvě čidla jsou umístěna v jiné městské části, kde hrozí únik amoniaku. Jsou umístěny na veřejném osvětlení. Další čidlo je u zimního stadionu, kde taktéž hrozí únik amoniaku. Dokáže odhalit únik čpavku a okamžitě vysílá informaci hasičům, kteří okamžitě vyjíždí. Na tento systém jsou napojeny budovy v okolí zimního stadionu, ve kterých se nachází větší množství lidí, například školy. Jsou poučeni, že jakmile dojde k úniku, měli by jít do vyšších pater, uzavřít a utěsnit okna a přijmout další bezpečností opatření.

Otázka č. 2: Máte uzavřeny smlouvy se servisními organizacemi. Do jaké doby musí tyto organizace reagovat a obnovit funkčnost systému?

Vše je ošetřeno smluvně. Doba obnovy je různá podle toho, co je ve smlouvě.

Otázka č. 3: Při výpadku elektrické energie máte záložní zdroj, kterým je agregát. Do jaké doby obnoví energii?

Do osmi vteřin se spustí. Celková obnova nastává do půl minuty.

Otázka č. 4: Při přijímání nových uchazečů, ověřujete jejich minulost?

Většinou ne. Ověřuje se jen bezúhonnost.

Otázka č. 5: Odebíráte přístupy při ukončování pracovního poměru k některým systémům týkající se krizového řízení?

Ano, odebíráme přístupy do systémů týkajících se krizového řízení, například do krizového plánu. Musím dát informaci HZS ČR, aby tento přístup odebrali. Dva nebo tři měsíce – po dobu výpovědní lhůty.

Otázka č. 6: Pracujete někdy z domova? Máte například pracovní mobilní telefon?

Z domu můžu jen odesílat e-maily. Pokud se něco stane, zaměstnanci krizového řízení musí být na pracovišti.

Otázka č. 7: S jakými typy dat/informací pracujete?

Na našem oddělení se řeší jen věcí týkající se krizového řízení.

Otázka č. 8: Jak je zajištěno bezpečné sdílení informací?

Pokud posílám e-mail, který chci mít zabezpečený, použiju flashdisk, který má na sobě nahrán podpis, pomocí kterého digitálně zprávu podepíši a nelze s ním potom jinak nakládat. Je to umožněno pomocí Bit4 Universal Middleware. Jakmile flashdisk vložím do počítače, musím zadat heslo a tím pádem to digitálně podepíšu a nedojde tak ke změně e-mailu a příjemce jej dál nepošle. Nebo používám GINIS, což je spisová služba, kterou používají například i hasiči.

Otázka č. 9: Pokud se přihlašujete do svého počítače a jiných systémů pro KŘ, používáte vícefaktrorové autentizační ověřování?

Zadávám jen uživatelské jméno a heslo. Heslo má nějaká pravidla. U všechny systémů, které používáme v rámci KŘ jsme od kraje dostali jak přihlašovací jména, tak hesla, které používáme. Žádné certifikáty nepoužívám, pokud si správně pamatuju.

Otázka č. 10: Jak jsou zabezpečeny místnosti týkající se krizového řízení? A které to jsou?

Jedná se mou kancelář a kancelář kolegy. Pak máme ještě zasedací místnosti pro krizový štáb je na tomto patře. V případě MU by z kanceláře kolegy byla udělána sekretariát, kde by se přijímaly telefonní hovory a podobně. Poté je jedna společná místnost, kde sedí KŠ. KŠ je dělen do tří skupin – A, B, C. Kolega by ve své kanceláři nebyl, protože by byl vedoucí skupiny C. Pokud by někdo svolal vedoucí skupin tak se scházíme v místnosti pro skupinu A, kde jsou mapy, podklady apod. Zde je skříň, kde jsou čtyři kufry, ve kterých je počítač, mapové podklady, kreslící potřeby apod., vše je připraveno a jednotlivé skupiny si to mohou rozebrat do místností. Pokud by se něco stalo tak máme záložní krizové pracoviště u HZS. Moje kancelář je zabezpečena pomocí klíče. Uklízečky mají klíče od našich kanceláří, ale uklízejí jen v době naší přítomnosti. Já jako vedoucí oddělení mám náhradní klíče v uzamykatelné skříňce, která je zabezpečena také klíčem. Další náhradní klíče jsou u městské policie.

Otázka č. 11: Náhradní klíče jsou tedy zabezpečeny jen klíčem a nikoli pečetí?

Ano, jen klíčem, pečeť tam není.

Otázka č. 12: Kde ukládáte citlivé informace, se kterými zrovna pracujete a odejdete z kanceláře?

Máme uzamykatelné skříně.