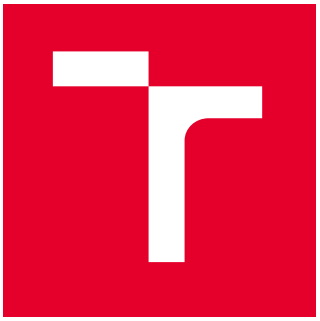


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ

FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY

INSTITUTE OF INFORMATICS

DOPADY RANSOMWAROVÉHO ÚTOKU: HODNOCENÍ RIZIK A ZAVEDENÍ MINIMÁLNÍHO BEZPEČNOSTNÍHO STANDARDU

THE IMPACTS OF A RANSOMWARE ATTACK: RISK MANAGEMENT AND IMPLEMENTATION OF THE MINIMAL SECURITY STANDARD

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Bc. Lucie Syrovátková**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. Petr Sedlák**
SUPERVISOR

BRNO 2023

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Studentka:	**Bc. Lucie Syrovátková**
Vedoucí práce:	**Ing. Petr Sedlák**
Akademický rok:	2022/23
Studijní program:	Informační management

Garant studijního programu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává diplomovou práci s názvem:

Dopady ransomwarového útoku: hodnocení rizik a zavedení minimálního bezpečnostního standardu

Charakteristika problematiky úkolu:

Úvod
Teoretická východiska práce
Analýza současného stavu
Vlastní návrhy řešení
Závěr

Cíle, kterých má být dosaženo:

Cílem práce je analýza dopadů ransomwarového útoku a zavedení vyšší úrovně informační a kybernetické bezpečnosti dle minimálního bezpečnostního standardu.

Základní literární prameny:

ČSN ISO/IEC 27001, Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky. Praha: Český normalizační institut, 2014.

ČSN ISO/IEC 27002, Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Soubor postupů. Praha: Český normalizační institut, 2014.

DOUCEK Petr, Martin KONEČNÝ a Luděk NOVÁK. Řízení kybernetické bezpečnosti a bezpečnosti informací. Praha: Professional Publishing, 2020. ISBN 978-80-88260-39-4.

ONDRÁK Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: CERM, Akademické nakladatelství, 2013. ISBN 978-80-7204-872-4.

SEDLÁK Petr, Martin KONEČNÝ a kolektiv. Kybernetická (ne)bezpečnost. Brno: CERM, Akademické nakladatelství, 2021. ISBN 978-80-7623-068-2.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2022/23

V Brně dne 5.2.2023

L. S.

doc. Ing. Miloš Koch, CSc. garant	doc. Ing. Vojtěch Bartoš, Ph.D. děkan

Abstrakt

Cílem diplomové práce je zavedení kybernetické bezpečnosti v malé společnosti v důsledku ransomwarového útoku, a to na základě požadavků Minimálního bezpečnostního standardu, který slouží jako podpůrný materiál pro subjekty, které nespadají pod regulaci Zákona o kybernetické bezpečnosti. Stanoveného cíle je dosaženo pomocí tří hlavních částí této práce. Úvodní část slouží jako teoretická podpora pro zbývající část práce a obsahuje hlavní pojmy a oblasti, které jsou v práci dále rozvinuty či využity. Analytická část je zaměřena na popis možného vektoru ransomwarového útoku a jeho následky a dále na zhodnocení současného stavu, které spočívá v porovnání stávající situace s požadavky Minimálního bezpečnostního standardu a v identifikaci neshod. Třetí část obsahuje navržení nápravných opatření, vytvoření bezpečnostních politik přizpůsobených možnostem společnosti a ekonomické zhodnocení.

Klíčová slova

Bezpečnostní politiky, Informační bezpečnost, Kybernetická bezpečnost, Minimální bezpečnostní standard, Národní úřad pro kybernetickou a informační bezpečnost, Systém řízení bezpečnosti informací, Ransomware

Abstract

The aim of the thesis is to implement cyber security in a small company as a result of a suffered ransomware attack based on the requirements of the Minimal Security Standard, which is a support material for entities that are not regulated by the Cyber Security Act in the Czech Republic. The main goal is achieved through the three main parts into which the thesis is divided. The introductory part is a theoretical support for the remainder of the thesis and contains the main concepts and areas that are used in the thesis. The analytical part focuses on the description of a possible vector of a ransomware attack and its consequences. In the second part of the analytical chapter, the current situation of the company is assessed in comparison to the requirements of the Minimal Security Standard. The last part proposes specific security measures, creation of security policies adapted to the company's capabilities and an economic evaluation.

Keywords

Cybersecurity policies, Information Security, Cybersecurity, Minimal Security Standard, National Cyber and Information Security Agency, Information Security Management System, Ransomware

Bibliografická citace

SYROVÁTKOVÁ, Lucie. *Dopady ransomwarového útoku: hodnocení rizik a zavedení Minimálního bezpečnostního standardu* [online]. Brno, 2023 [cit. 2023–05–12]. Dostupné z: https://www.vutbr.cz/studenti/zav–prace/detail/150896. Diplomová práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Ing. Petr Sedlák.

Čestné prohlášení

Prohlašuji, že předložená diplomová práce je původní a zpracovala jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušila autorská práva (ve smyslu zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 12. 5. 2023

Bc. Lucie Syrovátková

autor

Poděkování

Na tomto místě bych ráda poděkovala Ing. Petru Sedlákovi za jeho přístup v průběhu celého mého studia a jeho zkušenosti a odborné připomínky, které výrazně přispěly k vypracování diplomové práce. Dále bych ráda poděkovala Ing. Mateji Zápotočnému, Ph.D. za odbornou konzultaci a Společnosti X za možnost podílet se na procesu zvýšení kybernetické a informační bezpečnosti v jejich společnosti, za bezproblémovou spolupráci a sdílnost.

OBSAH

ÚVOD

Díky novým možnostem, výkonnějším technologiím, a také celkové rychlosti komplexního vývoje společnosti, se nyní téměř vše přesouvá do kybernetického prostoru. Mimo nespočet výhod, které virtuální svět nabízí, je nutno neopomínat také nástrahy, které v kybernetickém prostoru čekají. Zvýšení četnosti kybernetických incidentů je jedna strana mince, druhou stranou je však fakt, že díky větší dostupnosti informací a technickým posunům se v kyberprostoru nepohybují pouze lidé konající dobro, ale také útočníci, jejichž útoky se stávají sofistikovanějšími a pro oběti také závažnějšími. Všichni si podvědomě uvědomujeme, že toto nebezpečí někde v kyberprostoru čeká, málokdo z nás je však ochoten si připustit, jak blízko ve skutečnosti je. Problematika kybernetických útoků se dotýká nejen světových, či státních institucí a korporátů, ale také menších společností, a dokonce i jednotlivců. Právě zmíněný dopad na menší firmy a případně jednotlivce bych pomocí této diplomové práce chtěla na reálném příkladu v podobě kybernetického útoku a jeho následků demonstrovat.

Prostřednictvím této práce, konkrétně popisem uskutečněného útoku, popisem útočné plochy a návrhem bezpečnostních opatření pro zabezpečení vyššího stupně úrovně bezpečnosti firmy, bych ráda docílila osvěty v oblasti kybernetické a informační bezpečnosti. Věřím ale, že kromě vyřešení konkrétního problému Společnosti X a návrhu nápravných opatření může tato práce sloužit jako poučení, či vodítko při řešení problému obdobného rázu ve společnosti malé či střední velikosti.

VYMEZENÍ PROBLÉMU A CÍLE PRÁCE

Hlavním cílem této diplomové práce je, jak již bylo nastíněno v úvodu práce, analýza současného stavu společnosti a pochopení její současné situace v oblasti kybernetické bezpečnosti, popis kybernetického útoku, v tomto případě se konkrétně jedná o ransomwarový útok, identifikace nejslabších míst pomocí matice neshod, která vyplývá z analytické části, a nakonec také navržení nápravných opatření. Na základě vyhotovené matice neshod dojde k navržení nápravných opatření vedoucích ke zvýšení bezpečnostního stupně společnosti a také k mírnějším následkům při dalším pokusu o kybernetický útok. Sekundárním cílem této práce je také rozšíření povědomí o ransomwarových útocích a o mnohdy jednoduchému předejití nepříjemných a zbytečných následků.

Diplomová práce je členěna do tří hlavních částí, kterými jsou Teoretická východiska práce, Analýza původního stavu a Návrh vlastního řešení.

V Teoretické části jsou vysvětleny stěžejní pojmy, které budou využity v následujících částech diplomové práce. Druhá část, která se zabývá popisem uskutečněného útoku a také analýzou původního stavu, je zaměřena na analýzu stavu společnosti před a během kybernetického útoku, a to pomocí porovnání s doporučeními Minimálního bezpečnostního standardu (dále jen „MBS“), který byl vydán Národním úřadem pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“) a ze kterého celá práce vychází.

V závěrečné části práce je z nedostatků odhalených v Analytické části vytvořena matice neshod na základě které jsou poté navržena nápravná opatření, která společnosti pomohou předejít podobně drastickému průběhu při případném dalším kybernetickému útoku. Nakonec je provedeno také ekonomické vyhodnocení, ve kterém došlo k vyčíslení finančních dopadů samotného útoku a poté vyčíslení navržených nápravných opatření. Součástí závěrečné kapitoly je také závěrečné shrnutí, které popisuje plnění vytyčených cílů a dosažených přínosů.

1. TEORETICKÁ VÝCHODISKA PRÁCE

První část práce slouží k představení základních pojmů, díky kterým bude čtenář obeznámen s použitou terminologií v následujících kapitolách tak, aby došlo k zamezení nesprávného výkladu a práce tak komplexně pokrývala celou problematiku. Nejprve jsou v práci definovány obecné pojmy, poté jsou představeny dva kybernetické útoky, které jsou pro práci stěžejní. Mimo jiné je v práci představen také PDCA cyklus, se kterým je řízení kybernetické bezpečnosti velice úzce spjato. V poslední části této kapitoly došlo k představení, pro tuto práci základních, technických pojmů.

1.1. Obecné pojmy

V následující kapitole budou popsány obecné pojmy, se kterými se v diplomové práce pracuje a které je nutné znát pro správné pochopení problematiky, kterou se práce zabývá.

1.1.1. Kybernetická bezpečnost

Kybernetická bezpečnost označuje interdisciplinární obor jež pokrývá aspekty práva, politiky, lidského faktoru, etiky a řízení rizik, které napomáhají a směřují k zajištění ochrany kybernetického prostoru (1, s. 2, 3).

1.1.2. Kybernetický prostor

Kybernetickým prostorem je označováno digitální prostředí, které umožňuje vznik, zpracování či výměnu informací. Kybernetický prostor je tvořen informačními systémy, službami a sítěmi elektronických komunikací (2, § 2 odst. 1 písm. a).

1.1.3. Informační bezpečnost

Informační bezpečnost, nebo také CIA triáda, je zaměřena na organizaci z pohledu fyzické, personální, organizační a komunikační bezpečnosti a označuje zajištění důvěrnosti, integrity a dostupnosti informací (2, § 2 odst. 1 písm. a).

1.1.4. Dostupnost (C)

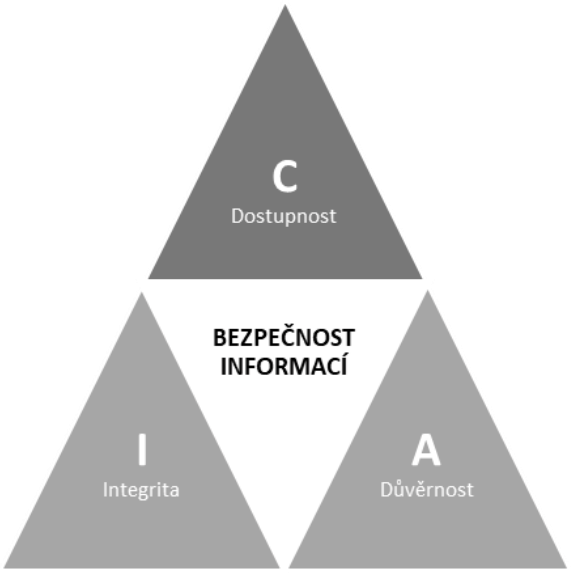
Pojem dostupnost značí zajištění dostupnosti informací pro oprávněné osoby v okamžiku potřeby (3).

1.1.5. Integrita (I)

Pojmem integrita je označováno zajištění správnosti a úplnosti informací (3).

1.1.6. Důvěrnost (A)

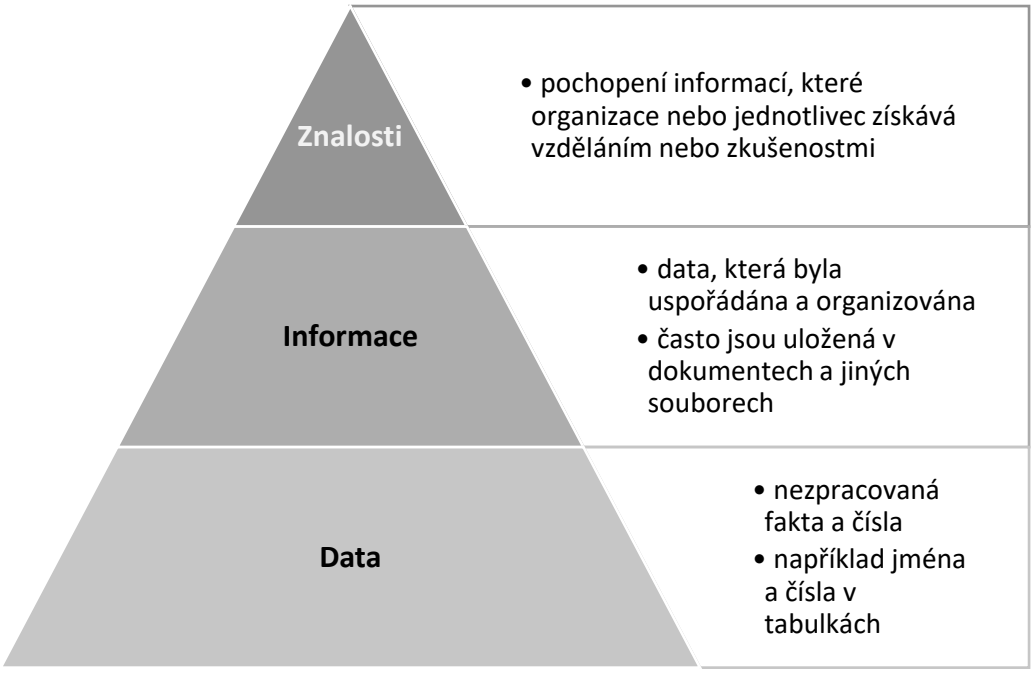
Pojmem důvěrnost je označováno zajištění přístupu k informacím a jejich poskytnutí pouze oprávněným osobám (3).



Obrázek č. 1: Triáda bezpečnosti informací
(Zdroj: Vlastní zpracování)

1.1.7. Znalostní trojúhelník

Informační bezpečnost pracuje s pojmy data, informace a znalosti. K správnému postupu při zajištění bezpečnosti informací je důležité správně přistupovat k jednotlivým částem následující pyramidy, která představuje **data** jako základnu, z níž vychází **informace** neboli strukturovaná data, a které jsou po jejich pochopení transformovány ve **znalosti** (6).



Obrázek č. 2: Znalostní trojúhelník
(Zdroj: Vlastní zpracování dle: 6)

1.2. Systém řízení bezpečnosti informací

Systém řízení bezpečnosti informací (dále jen „SŘBI“) označuje část systému řízení, která je založena na přístupu k rizikům informačního systému (dále jen „IS“) a na kterém je stanoven způsob ustanovení, zavádění, provozování, monitorování, přezkoumání, udržování a zlepšování bezpečnosti informací a dat (3, § 2 písm. j).

1.2.1. Bezpečnostní politiky

Pojem bezpečnostní politiky označuje souhrn bezpečnostních pravidel, které popisují a definují způsob zajišťování bezpečnosti v dané organizaci a v dané oblasti (1).

1.2.2. Bezpečnostní opatření

„*Bezpečnostním opatřením se rozumí souhrn úkonů, jejichž cílem je zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru*“ (2, § 4 odst. 1).

1.2.3. Bezpečnostní hrozba

Bezpečnostní hrozbou je označována možná příčina kybernetické bezpečnostní události nebo kybernetického bezpečnostního incidentu (dále jen „KBI“), která může způsobit škodu (4, § 2 písm. e).

1.2.4. Vektor útoku

Vektor útoku označuje způsob, jakým dochází ke zneužití zranitelnosti a kompromitaci cílového systému. Vektor útoku tedy popisuje, jakým způsobem útok probíhá a jaká aktiva zasahuje (5).

1.2.5. Útočná plocha

Útočnou plochou je označována plocha, na kterou je útočeno a také vstupní body, které by k útoku mohly být využity (5).

1.2.6. Aktivum

Pojem aktivum se používá pro označení čehokoliv, co má pro organizaci hodnotu. Pro potřeby kybernetické a informační bezpečnosti jsou poté aktiva dělena na primární a podpůrná.

Podpůrné aktivum

„Podpůrným aktivem je technické aktivum, zaměstnanci a dodavatelé podílející se na provozu, rozvoji, správě nebo bezpečnosti informačního a komunikačního systému“ (3, § 2 písm. f).

Primární aktivum

„Primárním aktivem informace nebo služba, kterou zpracovává nebo poskytuje IS a komunikační systém“ (3, § 2 písm. g).

1.2.7. Garant aktiva

„Garant aktiva je bezpečnostní role odpovědná za zajištění rozvoje, použití a bezpečnost aktiva“ (3, § 7 odst. 3).

1.2.8. Manažer kybernetické bezpečnosti

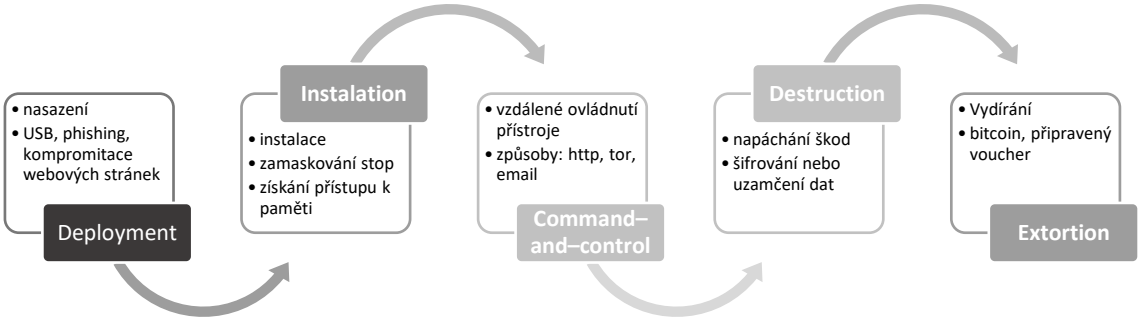
Manažer kybernetické bezpečnosti (dále jen „MKB“) je bezpečnostní role, která je odpovědná za SŘBI. Je povinen splňovat podmínky odborné praxe, kterou lze nahradit absolvovaným studiem na vysoké škole. MKB zajišťuje informování vrcholového vedení o stavu SŘBI a jeho role je neslučitelná s prováděním rolí odpovědných za provoz IS (3, § 7 odst. 1).

1.2.9. Řízení kontinuity činností

Řízení kontinuity činností spočívá v identifikaci potenciálních dopadů incidentů a přispívá k zajištění kontinuity a obnovy klíčových procesů organizace. Jedná se tedy o proces zajištění provozuschopnosti během katastrofy a po ní (7, s. 4).

1.3. Ransomwarový útok

Ransomwarový útok je jedním ze skupiny útoků, které jsou založeny na principu škodlivého kódu. Útočníkovým cílem je zašifrování dat s vidinou následného vydírání poškozeného výměnou za odšifrování dat (8).



Obrázek č. 3: Anatomie ransomwarového útoku
(Zdroj: Vlastní zpracování dle: 8)

1.4. Phishing

Phishingový útok je založen na zneužití lidského faktoru. Tento útok probíhá pomocí e-mailu, textových zpráv nebo webových stránek, a snaží se uživatele oklamat vydáváním se za důvěryhodnou osobu nebo organizaci. S využitím cizí identity útočník typicky žádá o kliknutí na odkaz nebo o stažení souboru a v případě, že uživatel následuje pokyny na podvodné stránce, ohrozí své soukromí a může vlastní vinou zapříčinit únik přihlašovacích údajů a hesel, únik citlivých dat, zneužití platebních údajů či instalaci škodlivého souboru, prostřednictvím kterého může útočníkovi zpřístupnit počítač a případně i celou síť. Útočníci využívající tento způsob útoku většinou zneužívají krizové či citlivé situace a v lidech vyvolávají pocit strachu nebo nátlaku. Typické znaky phishingového útoku, dle kterých je možno tento typ útoku rozeznat jsou znázorněny na obrázku níže (9).

Obrázek č. 4: Znaky phishingového útoku
(Zdroj: Vlastní zpracování dle: 9)

1.5. Legislativa, normy a standardy

Legislativa, normy a standardy jsou důležité pro jednotné řízení kybernetické a informační bezpečnosti, a lze na základě nich celý proces monitorovat a přezkoumávat. Pro stanovený cíl diplomové práce je stěžejní Minimální bezpečnostní standard, který přiměřeně reflektuje relevantní legislativu a normy v oblasti kybernetické a informační bezpečnosti.

1.5.1. Směrnice NIS2

„Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016, o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii“ (10).

V roce 2016 Evropská unie (dále jen „EU“) přijala směrnici bezpečnosti sítí a informací, označovanou jako směrnici NIS, která vedla k zvýšení bezpečnosti sítí a IS, které zajišťují důležité služby napříč členskými státy EU. Dne 27. prosince 2022 došlo k rozšíření rámce původní směrnice NIS a vznikla nová směrnice o kybernetické bezpečnosti, označována jako NIS2. Nová směrnice NIS2 je v současné době transponována do českého práva skrze připravovanou novelu Zákona o kybernetické bezpečnosti.

Mimo jiné s dopadem směrnice NIS2 na českou legislativu dojde k rozšíření souboru povinných osob, ke zvýšení důrazu na podporu vrcholového vedení v oblasti kybernetické bezpečnosti a také k zavedení povinného vzdělávání pro vrcholový management, a to primárně z důvodu nárůstu odpovědnosti vrcholového vedení za zajišťování kybernetické bezpečnosti v organizaci. Zásadní změnou je možno označit také významné navýšení pokut za nedodržení uložených povinností, které budou srovnatelné se sankcemi Obecného nařízení o ochraně osobních údajů, známého jako GDPR (10).

1.5.2. Zákon o kybernetické bezpečnosti č. 181/2014 Sb.

„*Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) ve znění pozdějších předpisů“* (11).

Zákon o kybernetické bezpečnosti (dále jen „ZKB“) reflektuje směrnici NIS, čímž zpracovává příslušné předpisy EU do českého práva. Konkrétně ZKB konkrétně upravuje práva a povinnosti osob a pravomoc a působnost orgánů veřejné moci v oblasti kybernetické a informační bezpečnosti. Jeho cílem je stanovit základní úroveň bezpečnostních opatření, zlepšit detekci a zavést hlášení a systém opatření k reakci na KBI. Mimo jiné ZKB upravuje také činnosti dohledových pracovišť (11).

V současnosti probíhá úprava ZKB dle nové směrnice NIS 2.

1.5.3. Vyhláška o kybernetické bezpečnosti

"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)" (4).

Vyhláška o kybernetické bezpečnosti (dále jen „VKB“) taktéž zpracovává příslušný předpis Evropské unie a reaguje tedy na směrnici NIS. VKB je také prováděcím předpisem k ZKB a konkrétně se zabývá úpravou následujících oblastí:

- obsah a strukturu bezpečnostní dokumentace,
- obsah a rozsah bezpečnostních opatření,
- typy, kategorie a hodnocení významnosti kybernetických bezpečnostních incidentů,
- náležitosti a způsob hlášení kybernetického bezpečnostního incidentu,
- náležitosti oznámení o provedení reaktivního opatření a jeho výsledku,
- vzor oznámení kontaktních údajů a jeho formu a
- způsob likvidace dat, provozních údajů, informací a jejich kopií.

Tyto oblasti jsou primárně určeny pro IS kritické informační infrastruktury, komunikační systémy kritické informační infrastruktury, významné IS, IS základní služby či IS nebo síť elektronických komunikací, které využívá poskytovatel digitálních služeb (4, § 1).

V současnosti probíhá úprava VKB dle nové směrnice NIS 2.

1.5.4. Normy ISO/IEC řady 27000

Normy řady 27000 byly vypracovány ve spolupráci organizace ISO, jenž je mezinárodní organizací pro normalizaci a organizace IEC – Mezinárodní elektronickou komisí. Tvůrcem normy je obvykle technická komise ISO a záležitosti normalizace v elektrotechnice je zaštiťovány organizací IEC. Zmíněné organizace společně tvoří technickou komisi označenou jako ISO/IEC JTC 1 Informační technologie subkomise SC 27 IT Bezpečnostní techniky (12, s. 7).

Dalšími relevantními normami řady 27000 jsou:

- ČSN EN ISO/IEC 27001 (36 9797) Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky
- ČSN EN ISO/IEC 27002 (36 9798) Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací
- ČSN ISO/IEC 27003 (36 9790) Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Pokyny
- ČSN ISO/IEC 27004 (36 9790) Informační technologie – Bezpečnostní techniky – Řízení bezpečnosti informací – Monitorování, měření, analýza a hodnocení
- ČSN ISO/IEC 27005 (36 9790) Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací (12)

1.5.5. Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB)

„NÚKIB je ústředním správním orgánem pro kybernetickou bezpečnost včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany“ (13).

Mimo jiné se NÚKIB zabývá přípravou zákonů, podzákonných norem v oblasti kybernetické bezpečnosti a metodickou přípravou podpůrných materiálů. Dále například NÚKIB podporuje a provádí osvětu a vzdělávání v oblasti kybernetické bezpečnosti (13).

1.5.6. Minimální bezpečnostní standard

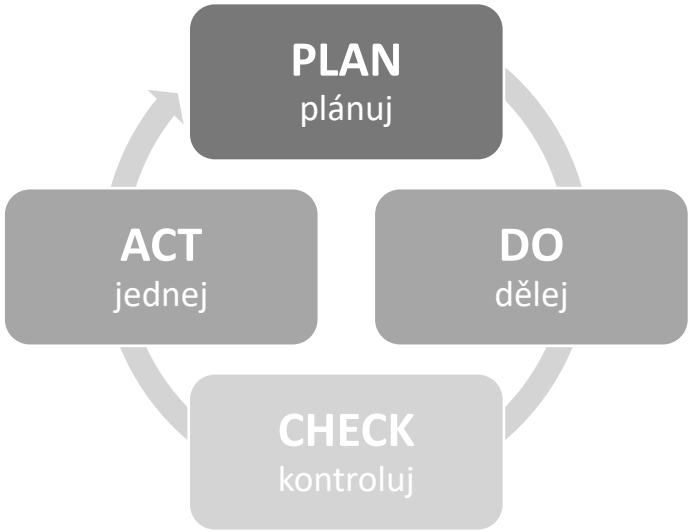
MBS „*nabízí zjednodušené principy, postupy a doporučení v oblasti kybernetické bezpečnosti pro organizace, které nespadají pod regulaci ZKB*“ (14, s. 4).

MBS byl vytvořen NÚKIB jako podpůrný materiál pro zavedení SŘBI ve společnostech, které nejsou v oblasti kybernetické bezpečnosti regulovány. Tento dokument je rozdělen na dvě stěžejní části. První, manažerská, část je zaměřena na organizační opatření a věnuje se procesní stránce SŘBI. Jedná se tedy o popisy postupů, které je třeba mít v rámci organizace zavedeny a dle kterých je třeba se řídit. Druhá, technická, část je zaměřena na konkrétní návody a doporučení, jak docílit minimální úrovně zabezpečení a je určena primárně pro IT techniky (14, s. 4).

1.6. PDCA cyklus v SŘBI

PDCA cyklus, neboli Demingův cyklus, je založen na kontinuálním opakováním čtyř činností PLAN–DO–CHECK–ACT. Obecně se jedná o následující činnosti:

- PLAN (plánuj) – identifikace procesů
- DO (dělej) – popis a dokumentace procesů
- CHECK (kontroluj) – řízení procesů na základě dokumentace
- ACT (jednej) – následná optimalizace procesů



Obrázek č. 5: PDCA cyklus
(Zdroj: Vlastní zpracování dle:15, s. 24, 25)

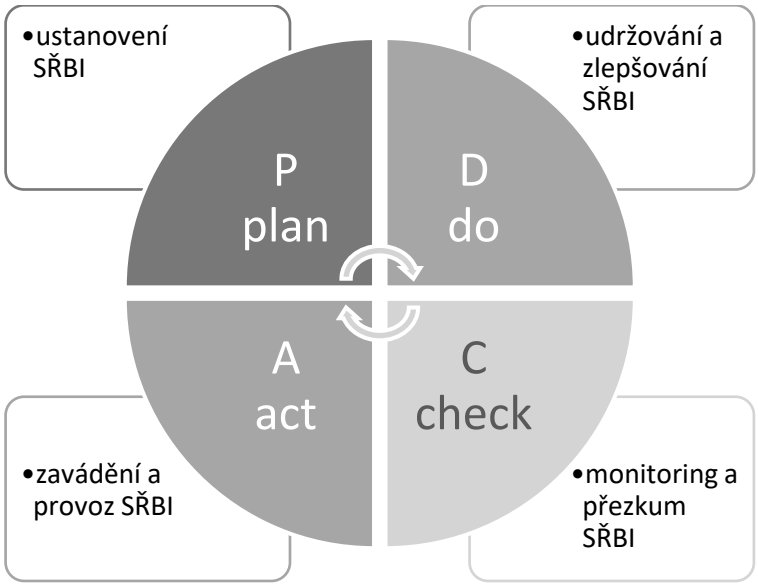
PDCA cyklus je aplikován také na SŘBI. Pomocí PDCA cyklu je v řízení bezpečnosti informací docíleno neustálého a kontinuálního zlepšování.

Ve fázi PLAN, která je obecně popisována jako ustanovení SŘBI, dochází k určení rozsahu a upřesnění hranic řízení bezpečnosti a stanovení odpovědností. Fáze PLAN tedy znamená upřesnění rozsahu samotného SŘBI a jeho hranic, vytvoření jasného manažerského zadání a provedení hodnocení rizik, na základě kterého jsou následně zvolena nezbytná bezpečnostní opatření.

Fáze DO, tedy udržování a zlepšování SŘBI, představuje prosazení zvolených bezpečnostních opatření, jejím cíle je účelně a systematicky nasazovat daná bezpečnostní opatření a začlenit je do chodu organizace.

Třetí fáze CHECK, je zaměřena na monitoring a přezkum SŘBI. Jejím cílem je tedy získávání zpětné vazby, vyhodnocování provedených kroků a sledovaných parametrů. Podstatnou součástí tohoto kroku jsou například nastavené klíčové ukazatele výkonnosti (KPI – key performance indicator), případně plnění stanovených strategických či dílčích cílů SŘBI. Tato fáze k vyhodnocení často využívá formu pravidelného auditního přezkumu.

Poslední fáze ACT, neboli zavádění a provozování SŘBI, značí realizaci navržených bezpečnostních opatření a zaměření se na redukci identifikovaných slabých míst (15, s. 24, 25).



Obrázek č. 6: PDCA cyklus v souvislosti se SŘBI
(Zdroj: Vlastní zpracování dle: 15, s. 24, 25)

1.7. Lewinův model změny

Lewinův model změny je v této části popsán z důvodu spousty změn, které tato diplomová práce v ideálním případě vyvolá. Správná implementace a přístup k daným změnám je stěžejní pro docílení navrhovaného stavu a zlepšení bezpečnostní situace ve Společnosti X. Lewinův model je také navržen v bezpečnostních politikách pro budoucí řízení změn.

1.7.1. Fáze rozmrazení

V první fázi, označované také fází rozmrazení, je nutné seznámit všechny zainteresované strany s plánovanou změnou, vysvětlit jim v čem bude daná změna přínosná a jaké kroky budou podniknuty k jejímu provedení. Je nutné, aby společnost danou změnu dostatečně zpropagovala na straně zainteresovaných stran.

Součástí fáze rozmrazení je analýza silového pole (určení hybných a brzdných sil), díky které lze zjistit, zda je změnu možné provést. Pokud změna vyjde jako proveditelná, je dále třeba identifikovat klíčové nositele změny, konkrétně se jedná o role agenta, sponzora a advokáta změny. Posledním krokem je stanovení a popis intervenčních oblastí, mezi které patří oblast technologie, oblast toků a procesů, oblast organizační struktury a oblast lidských zdrojů (16).

1.7.2. Fáze přechodu a aplikace změny

Druhá fáze Lewinova modelu, tedy fáze změny a přechodu, popisuje sled činností, které vedou k naplnění cíle navrhované změny (16).

1.7.3. Fáze zamrazení

Fáze rozmrazení je třetí a poslední fází Lewinova modelu změny, která slouží ke stabilizaci a adaptaci po provedené změně. Jedná se o fázi, ve které dochází k přijetí změny a zavedení tohoto stavu novým standardem. K vyhodnocení úspěšnosti změny je nutno zavést také ukazatele, které budou v průběhu a po změně monitorovány (16).

1.8. Ekonomický a informační systém POHODA

Ekonomický a informační systém POHODA (dále jen „POHODA“) zajišťuje funkci komplexního účetního a ekonomického softwaru pro malé, střední, ale i větší firmy. Systém disponuje velkým množství funkcí a agend, usnadňující administrativu v oblasti účetnictví, či daňové evidence (17).

1.9. Technické pojmy

V této podkapitole jsou popsány použité technické pojmy, aby bylo pro čtenáře snazší orientovat se v technických oblastech diplomové práce.

1.9.1. Zálohovací pravidlo 3–2–1

Zálohovací pravidlo 3–2–1 slouží ke zvýšení možnosti pro obnovu ztracených či poškozených dat. Konkrétně popisuje následující postup vyjádřen číselným stupňováním:

- **Pravidlo tří kopií** – Uchovávat alespoň tři kopie (zálohy), jednu primární a dvě záložní,
- **Pravidlo dvou médií** – Udržovat soubory alespoň na dvou různých médiích a
- **Pravidlo jedné kopie mimo pracoviště** – Uložit alespoň jednu kopii (zálohu) mimo pracoviště (18, s. 2).

1.9.2. LDAP

LDAP, neboli Lightweight Directory Access Protocol, je softwarový protokol, který umožňuje lokalizaci dat o organizacích a jednotlivcích nebo jiných typech zdrojů v podobě souborů a zařízení připojených v síti. LDAP je centrálním nástrojem pro autentizaci, lze ho ale také využít pro ukládání a přístup k datům na adresářovém serveru, který umožňuje uchovávat různé typy dat nevyžadující častou aktualizaci (19).

1.9.3. VPN

VPN, Virtual Private Network, představuje vytvoření chránění síťového připojení při použití veřejných sítí. Pomocí VPN je v reálném čase šifrován internetový provoz a je maskována online identita uživatele. Připojení přes VPN vytváří zabezpečené spojení mezi uživatelem a internetem. Přes VPN je datový provoz směrován přes šifrovaný virtuální tunel, díky čemuž dochází k maskování IP adresy a její poloha je tím neviditelná (20).

1.9.4. Log management

Log management popisuje proces transformace logů do uchopitelné podoby, kterou lze dále analyzovat, vizualizovat, ukládat, sledovat, archivovat a likvidovat. Log management je nezbytný, jelikož samotné logy jsou pro tvorbu manažerských výstupů nečitelnou záležitostí (21).

SIEM

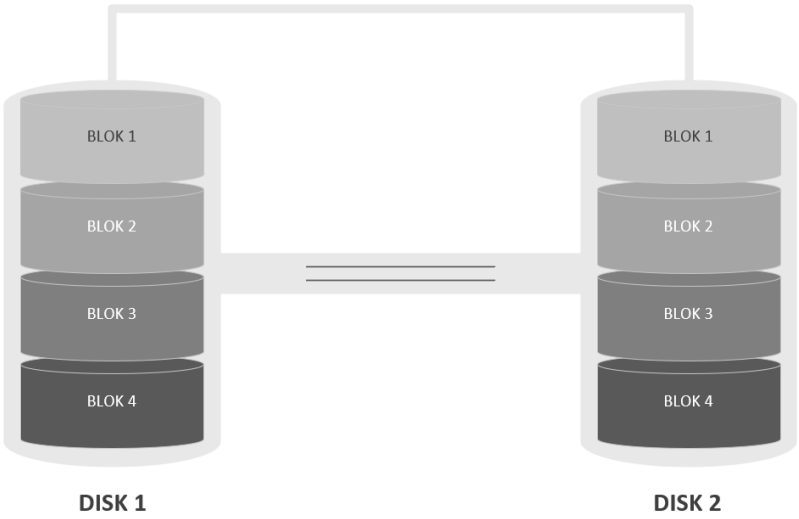
SIEM, Security Information and Event Management, je nástroj pro centralizovanou správu sbíraných bezpečnostních logů a dle nastavených pravidel vizualizuje výstupy z analyzovaných logů. Jedná se o nástroj využívaný pro log management a monitoring sítě. SIEM analyzuje velké množství dat a identifikuje a třídí je do kategorií a umí detekovat známky škodlivé činnosti a generovat bezpečnostní výstrahy (22).

1.9.5. NTP

NTP, Network Time Protocol, je internetový protokol, který slouží k synchronizaci vnitřních hodin počítačů, díky čemuž dochází k synchronizace času u všech počítačů v síti (23).

1.9.6. Zrcadlení disku – RAID 1

Zrcadlení disku, neboli RAID 1, značí replikaci dat na dva nebo více disků. Jedná se o metodu seskupování fyzických jednotek do jednoho většího disku, tedy sady RAID. RAID 1 vyžaduje minimálně dva fyzické disky, na které dochází k současnému zápisu dat. Tímto mechanismem dochází k vytvořením zrcadlené kopie a v případě selhání jednoho z disků může dojít k okamžitému zastoupením druhým diskem. Tato metoda je výhodná pro rychlé čtení, časově náročnější operací je však zápis, jelikož je nutné zapisovat na oba disky. Tato metoda je vhodná pro menší množství dat, protože pro větší množství režijní kapacity by se řešení RAID 1 stalo příliš nákladné (24).



Obrázek č. 7: Zrcadlení disku - RAID 1
(Zdroj: Vlastní zpracování dle: 24)

1.9.7. LAN

LAN, neboli Local Area Network je soubor zařízení spojených na jednom fyzickém perimetru (kancelář, budova, atp.). Síť LAN je složena z kabelů, koncových zařízení, routerů a switchů, které umožňují zařízením připojit se k interním serverů, webovým serverům a dalším LAN sítím (25).

1.9.8. Protokol SMB

Protokol Server Message Block, neboli SMB protokol, je síťový komunikační protokol, který pracuje na aplikační vrstvě na principu klient–server. Tento protokol je využíván ke sdílení přístupu k souborům, tiskárnám, sériovým portům a dalším zdrojům připojených v síti. Protokol SMB umožňuje aplikacím a jejich uživatelům přistupovat k souborům na vzdálených serverech. SMB poskytuje klientským aplikacím bezpečnou a řízenou formu pro otevírání, čtení, přesouvání, vytváření a aktualizaci souborů na vzdálených serverech. (26).

1.9.9. RDP

Remote Desktop Protocol, neboli RDP, je zabezpečený síťový komunikační protokol společnosti Microsoft, který slouží ke zprostředkování vzdáleného přístupu (27).

1.9.10. EDR

EDR (Endpoint Detection and Response) je označení pro systém pro sběr a analýzu informací, které souvisejí s bezpečnostními hrozbami z koncových bodů jejichž cílem je narušení zabezpečení. EDR také dokáže na nalezené hrozby reagovat. EDR může mít také schopnosti antiviru, ale nejedná se o antivirový SW (28).

2. ANALÝZA PROBLÉMU A SOUČASNÉHO STAVU

2.1. Základní informace o společnosti

Z důvodu zpracování citlivých dat, které jsou pro tuto práci stěžejní, došlo po domluvě s vedením společnosti k anonymizaci některých údajů, včetně názvu společnosti (dále jen „Společnost X“). Společnost X je v obchodním rejstříku vedena jako společnost s ručením omezeným a byla založena v roce 2015. V současné době má společnost patnáct zaměstnanců s ročním obratem zhruba 45 mil. Kč. Společnost X je inženýrsko-dodavatelská společnost se zaměřením na průmyslovou vzduchotechniku, která nabízí svým zákazníkům souhrn optimálních úsporných a ekologických opatření formou rekuperace odpadního tepla z výrobních procesů, jež vedou ke snížení spotřeb energií.

Provozovna společnosti je umístěna v pronajatých kancelářských prostorech, což je limitující z pohledu stavebních a rozsáhlejších úprav.

2.2. Organizační struktura

Společnost X se velikostně řadí mezi malé podniky. Je složena z pěti oddělení, konkrétně se jedná o oddělení realizace, oddělení projekce, obchodní oddělení, ekonomické oddělení a IT oddělení. Vzhledem k předmětu práce a samotnému cíli útoku je podstatné definovat, jaká oddělení mají přístup do POHODY.

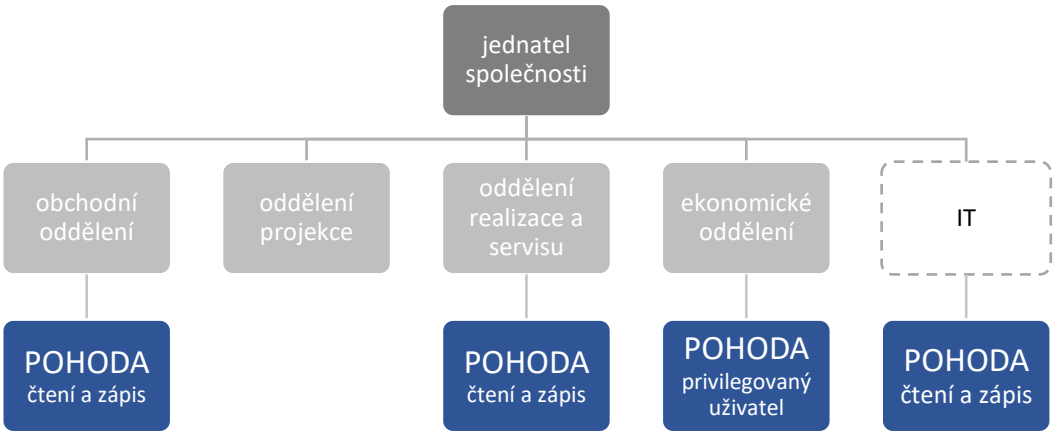
Obchodní oddělení se zabývá kontaktem se zákazníky a dodavateli, dále zajišťuje získávání nových zakázek a objednávek materiálu pro jednotlivé realizace. Zaměstnanci tohoto oddělení mají přístup do POHODY v podobě čtení a zápisu.

Oddělení projekce se zabývá tvorbou projektové dokumentace, přístup do POHODY zaměstnanci tohoto oddělení nemají, jelikož je pro jejich práci nerelevantní.

Oddělení realizace a servisu se stará o plynulý chod zakázek přímo na místě její realizace, zajišťuje komunikaci se zákazníkem a dodavateli (kontrolní dny) a zajišťuje služby servisu. Z podstaty náplně práce oddělení mají práva pro přístup do POHODY stejná jako obchodní oddělení, tedy práva pro čtení a zápis.

Ekonomické oddělení zajišťuje služby externě, tedy i připojování do POHODY probíhá vzdáleně. Jako jediní mají zaměstnanci ekonomického oddělení přístup do POHODY jako privilegovaní uživatelé.

IT služby jsou zajišťovány interně jedním ze zaměstnanců projekce, co se týče přístupů do POHODY, vlastní navíc oproti ostatním zaměstnancům projekce práva pro čtení a zápis.



Obrázek č. 8: Organizační struktura Společnosti X společně se zobrazením přístupů k systému POHODA
(Zdroj: Vlastní zpracování)

2.3. Identifikace aktiv

Společnost nemá formálně určena primární ani podpůrná aktiva. Z důvodu dalšího využití a celkového zmapování situace je nutno určit primární i podpůrná aktiva určit.

Primárním aktivem byla identifikována služba projektové činnosti ve výstavbě. Tato informace byla převzata z obchodního rejstříku jako předmět podnikání společnosti. Podpůrným aktivem bylo určeno softwarového a hardwarové vybavení, které je dále členěno do skupin aktiv s podobnými vlastnostmi (dále jen „typové aktivum“). Dále je nutno mít přehled o dodavatelích a zaměstnancích. Zaměstnanci byli identifikováni v kapitole 2.2 v podobě organizační struktury a je postačující na ně nahlížet v obecné podobě v rámci členění na jednotlivá oddělení.

Společnost ke své činnosti využívá následující softwarové vybavení:

- Operační systémy Windows 11
- Kancelářský balík Office 365
- Autodesk produkty:
    - AutoCAD
    - Revit
    - Robot Structural Analysis Professional
- Ekonomický a informační systém POHODA

Základní hardwarové vybavení společnosti:

- Router
    - Synology RT2600ac
- File server – NAS
    - Synology DS920+
- UPS
    - CPS BR700ELCD
- Switch (8x)
    - TP Link TL–SG108E
- Koncová zařízení
    - Notebooky
    - Tiskárny
    - Mobilní telefony

Dodavatelé, se kterými společnost spolupracuje, jsou z důvodu anonymizace identifikováni dle oblastí, které dodávají:

- Dodavatel montážních činností
- Dodavatelé technologií
- Dodavatel stavebních prací

Tabulka č. 1: Identifikace aktiv
(Zdroj: Vlastní zpracování)

Typ aktiva	Název aktiva	Označení aktiva	Typové aktivum
primární	Projektová činnost ve výstavbě	P–1	
podpůrné	Operační systémy Windows 11	SW–1	
podpůrné	Kancelářský balík Office 365	SW–2	
podpůrné	AutoCAD	SW–3	Produkty Autodesk
podpůrné	Revit	SW–4	Produkty Autodesk
podpůrné	Robot Structural Analysis Professional	SW–5	Produkty Autodesk
podpůrné	Ekonomický a informační systém POHODA	SW–6	
podpůrné	Synology RT2600ac	HW–1	Router
podpůrné	Synology DS920+	HW–2	File server
podpůrné	CPS BR700ELCD	HW–3	UPS
podpůrné	TP Link TL–SG108E	HW–4	Switch
podpůrné	Lenovo E 560	HW–5	Notebook
podpůrné	Brother + Canon plotter	HW–6	Tiskárna
podpůrné	Sony Xperia	HW–7	Mobilní telefony
podpůrné	Zaměstnanci	Z–1	Zaměstnanci
podpůrné	Dodavatelé	D–1	Dodavatelé

2.4. Popis útočné plochy – situace před útokem

Situace před útokem a tedy prostředí, do kterého útočník útočil, bude popsána pomocí výčtu z MBS, který byl vydán pod záštitou NÚKIB jako podpůrný materiál pro subjekty, které nespadají pod zákon o kybernetické bezpečnosti. Výčet bude obsahovat všechna doporučení, které MBS uvádí, a bude v něm popsáno, zda bylo dané doporučení zavedeno a pokud ano, bude také popsáno, jakým způsobem.

Vzhledem k faktu, že společnost nepodstupuje žádné auditní přezkumy, dosud nedokumentovala žádné činnosti v ohledu vedení bezpečnosti, a ani neprochází školeními s bezpečnostní tematikou, je proto bezpředmětné se organizační částí MBS zabývat.

Činnosti v oblasti technické bezpečnosti už však částečně zavedeny jsou, a tak je nutno vyhodnotit jejich dostatečnost pomocí technické části MBS. Technická část je rozpadnuta do dvanácti celků, které budou v následujících podkapitolách popsány a vyhodnoceny dle reálného stavu, ve kterém se společnost v době útoku nacházela. Konkrétně se jedná o následující oblasti:

- Fyzická bezpečnost
- Řízení přístupů
- Požadavky v oblasti ochrany před škodlivým kódem
- Kybernetické bezpečnostní události a incidenty
- Požadavky v oblasti aplikační bezpečnosti
- Kryptografické prostředky
- Požadavky v oblasti zajišťování úrovně dostupnosti informací
- Požadavky v oblasti cloudových služeb
- Výjimky běhu, chyby a hlášení
- Ochrana webových aplikací proti známým zranitelnostem
- Rozvoj informačních a komunikačních systémů
- Komunikace

Každá z oblastí výše bude podrobně popsána v samostatné podkapitole a její stav nasazení bude vyhodnocen i tabulkově. Pokud bude daný požadavek naplněn, bude v posledním sloupci ANO, pokud se stav nebude shodovat s danými požadavky, bude v posledním sloupci NE. Skladba tabulky, která je pro vyhodnocení stavu použita, je k dispozici níže.

Tabulka č. 2: Popis struktury tabulky využité k posouzení stavu a shody s MBS
(Zdroj: Vlastní zpracování)

ID	Požadavek	Poznámky	Stav zavedení
Identifikátor požadavku	Popis požadavku, který vyplynul z doporučení MBS.	Popis stavu ve Společnosti X, specifikace podrobností a implementovaného řešení.	ANO (splňuje požadavek) x NE (nesplňuje požadavek)

2.4.1. Fyzická bezpečnost

Oblast fyzické bezpečnosti, konkrétně fyzický perimetr, je vymezen pracovním prostorem firmy, který má společnost v pronájmu. Fyzický perimetr je tedy omezen předmětem nájemní smlouvy a stavební či radikálnější zásahy tak nejsou možné. Fyzický perimetr je zabezpečen pomocí elektronického zabezpečovacího systému Jablotron, který je přímo navázán na policejní složky. Při nepovoleném vniknutí do objektu je informována policie, která následně provede fyzickou kontrolu objektu, tato služba je zpoplatněna cenou za daný výjezd. Objekt je také pravidelně zamykán a vchodové dveře

jsou vybaveny bezpečnostním zámkem. Kromě zabezpečení systémem Jablotron je objekt střežen také kamerovým systémem. Kamery jsou kromě recepce a chodeb umístěny také na parkoviště, které je celou noc osvětleno nočními světly. Kritickým místem, v tomto případě spíše objektem společnosti je pouze stojanový rozvaděč, který je umístěn ve společných kancelářských prostorech, tedy ve stanoveném fyzickém perimetru. V rozvaděči je také umístěno záložní napájení UPS a aktivní chlazení v rozvaděči je řešeno pomocí ventilátoru. Z bezpečnostního hlediska je rozvaděč uzamčen. Z hlediska infrastruktury není společnost vybavena strukturovanou kabeláží. Pravidla pro návštěvy nejsou nijak definována, dodržuje se však takový režim, že za návštěvu je vždy zodpovědná osoba, která návštěvu přivedla.

Tabulka č. 3: Vyhodnocení stavu v oblasti fyzické bezpečnosti
(Zdroj: Vlastní zpracování dle: 14, s. 18)

ID	Požadavek	Popis stavu	Stav zavedení
1	Definovat nový, či rozšířit stávající soubor opatření předcházející poškození, krádeži či zneužití informací či majetku nebo přerušení služeb IS nebo komunikačního systému (dále jen „KS“), vymezit fyzický perimetr.	Fyzický perimetr je dán pracovním prostorem firmy, respektive je omezen pracovním prostorem firmy a předmětem nájemní smlouvy.	NE
2	Fyzický perimetr je chráněn a zabezpečen před neoprávněným vstupem a poškozením, krádeží či zneužitím.	Chráněn fyzicky pomocí zamykání prostor a pomocí EZS Jablotron (elektronický zabezpečovací systém).	ANO
3	Zajištěna ochrana kritických míst v rámci objektů (serverovny, kanceláře zaměstnanců, technologické místnosti).	Z dispozičních důvodů je stojanový rozvaděč (rack tower) obsahující hlavní síťové prvky umístěn ve společných prostorách a je uzamčen.	ANO
4	Jasně definována pravidla pro návštěvy.	Pravidla nejsou nijak definována. Neformálně platí postup, že zaměstnanec, který návštěvu pozve, je za její pohyb na pracovišti zodpovědný a věnuje se jí.	NE
5	Zajištěno záložní napájení (UPS).	UPS zařízení je využíváno a definováno v HW prostředcích.	ANO
6	Zajištěna klimatizace serverovny.	Aktivní chlazení zajištěno ventilátory.	ANO
7	Zajištěna bezpečnost kabelových rozvodů.	Prostory společnosti nejsou vybaveny strukturovanou kabeláží.	NE

2.4.2. Řízení přístupů

V oblasti řízení přístupů nebyla vytvořena žádná politika, ale pravidla v této oblasti jsou nepřímo nastavena a využívána, avšak nejsou formalizována. Řízení přístupů je zajištěno pomocí LDAP serveru, kde jsou přidělovány jedinečné identifikátory uživatelům a privilegovaným uživatelům, dále je pomocí něj prováděno řízení přístupu na základě skupin a rolí, zaměstnancům s privilegovanými účty jsou přidělovány i samostatné přihlašovací údaje k běžným účtům, aby pro běžnou činnost nepoužívali privilegované účty. Běžné účty jsou tedy používány jak vedením společnosti a zaměstnanci s privilegovanými účty, tak i běžnými zaměstnanci.

Politika pro přidělování a odebírání rolí není formalizována, avšak je aktivně používána a při ukončení pracovního poměru jsou uživateli veškeré přístupy a role odebrány. LDAP server je také využíván k centrální registraci všech uživatelů a k nastavování politiky hesel, která je ovšem v tuto chvíli nastavena nedostatečně, jak je upřesněno v tabulce níže.

Přístupová práva a oprávnění aplikací a technických účtů jsou upravována při instalaci nové aplikace, či při tvorbě technických účtů. Postupy a pravidla pro nastavení omezení a kontrolu používaného SW a HW, který by mohl narušit systémovou a aplikační bezpečnost, nejsou stanovena. Princip need–to–know není vzhledem k velikosti a předmětu podnikání společnosti v praxi realizovatelný. Pravidla pro procesy jsou nastavena a v praxi jsou využívána, k jejich dokumentaci ale nedochází, vždy totiž došlo k individuálnímu proškolení nově příchozího zaměstnance. Lokální účty nejsou využívány, vyjma koncových zařízení, avšak i tyto účty jsou řízeny nastavenou politikou hesel.

Tabulka č. 4: Vyhodnocení stavu v oblasti řízení přístupů
(Zdroj: Vlastní zpracování dle: 14, s. 19, 20)

ID	Požadavek	Popis stavu	Stav zavedení
8	Vytvořena politika řízení přístupu.	Pravidla pro řízení přístupu jsou nastavena a využívají se, avšak samotná politika není sepsána.	NE
9	Přiděleny jedinečné identifikátory jednotlivým uživatelům a administrátorům přistupujících k IS nebo KS.	Pomocí LDAP serveru.	ANO
10	Řízeny a evidovány identifikátory, přístupová práva a oprávnění aplikací a technických účtů.	Upravováno při instalaci nové aplikace a při tvorbě technických účtů.	ANO

11	Prováděno řízení přístupu na základě skupin a rolí.	Pomocí LDAP serveru.	ANO
12	Jsou definovány postupy a pravidla potřebné pro omezení a kontrolu používaného SW a HW, který by mohl narušit systémovou a aplikační bezpečnost.		NE
13	Privilegované účty mají přiděleny samostatné přihlašovací údaje.	Pomocí LDAP serveru.	ANO
14	Jednotliví administrátoři mají vedle privilegovaného účtu i účet běžného uživatele pro činnost, které nevyžadují privilegovaná oprávnění.	Zaměstnanec, který má nadstandardní práva, má mimo tento privilegovaný účet vytvořen i běžný účet, který využívá pro náplň jeho běžné pracovní činnosti.	ANO
15	Uplatňován princip need–to–know.	Vzhledem k velikosti a předmětu podnikání společnosti není realizovatelné dodržování need to know principu. Není v možnostech.	NE
16	Vedení organizace využívá běžné uživatelské účty.		ANO
17	Politika pro přidělování, odebírání rolí.	Politika se využívá, avšak není formalizována.	NE
18	IS nebo KS zajišťuje registraci všech uživatelů centrálně.	Pomocí LDAP serveru.	ANO
19	Jsou stanoveny pravidla pro procesy:	Pravidla jsou nastavena a využívají se, avšak nebylo třeba je sepisovat, vždy došlo k individuálnímu proškolení příchozího zaměstnance.	ANO
19.1	• registrace	Pouze neformálně	ANO
19.2	• schvalování		
19.3	• generování identit		
19.4	• přidělování a odebírání přístupů		
19.5	• deaktivace identit		
19.6	• monitorování činnosti uživatelů		
20	IS nebo KS musí umožňovat využívat stávající IS nebo KS pro Identity management.	Není používáno	
21	Jestliže existují v rámci IS nebo KS lokální účty, je nezbytné, aby se řídily následující politikou hesel pro privilegované účty, nebo je nutné umožnit integraci s IS nebo KS pro správu privilegovaných účtů.	Lokální účty nejsou využívány vyjma koncových zařízení.	
22	Existuje politika hesel pro privilegované účty v minimální míře:	Upraveno v nastavení LDAP.	ANO
22.1	• minimální délka hesla je 17 znaků	8 znaků	NE
22.2	• musí obsahovat: velká písmena, malá písmena, číslice a speciální znak		ANO
22.3	• maximální doba platnosti hesla je 18 měsíců	Není maximální doba platnosti.	NE

22.4	• zákaz používaní stejného hesla (posledních 12 hesel)		NE
22.5	• minimální platnost hesla 1 den		NE
22.6	• zamčení účtu po 5 neplatných pokusech zadání hesla v řadě		ANO
22.7	• jednorázové prvotní heslo, které musí být změněno po prvním přihlášení nebo zneplatněno po 24 hodinách		ANO
23	Existuje politika hesel pro uživatelské účty v minimální míře:	Upraveno v nastavení LDAP.	
23.1	• minimální délka hesla je 10 znaků	8 znaků	NE
23.2	• zákaz používaní stejného hesla (posledních 12 hesel)		NE
23.3	• maximální doba platnosti hesla je 18 měsíců		NE
23.4	• zamčení účtu po 10 neplatných pokusech zadání hesla v řadě		ANO
23.5	• jednorázové prvotní heslo, které musí být změněno po prvním přihlášení nebo zneplatněno po 24 hodinách		ANO

2.4.3. Požadavky v oblasti ochrany před škodlivým kódem

Ochrana před škodlivým kódem je řešena pomocí antivirového programu, kdy je nastaven režim pravidelné antivirové kontroly, konkrétně v 00:40 hodin každý den. Způsob ochrany před škodlivým kódem v oblasti směru, výstupu a vstupu dat, jejich uložení a zpracování v informačním systému není nijak nastaven ani navrhnut.

Segmentace síťového prostředí není zavedena a vzhledem k velikosti sítě nemá ani smysl toto řešení do budoucna zvažovat. Software pro detekci a odstranění škodlivých programů je jak na serverech, tak na koncových zařízením nainstalován. K aktualizaci tohoto softwaru však v doporučeném rozsahu, nejméně jednou denně, nedochází.

Tabulka č. 5: Vyhodnocení stavu v oblasti ochrany před škodlivým kódem
(Zdroj: Vlastní zpracování dle: 14, s. 22)

ID	Požadavek	Popis stavu	Stav zavedení
24	V rámci IS nebo KS je navržen a implementován způsob řešení ochrany před škodlivým kódem	Antivirová kontrola probíhá pro data na serveru každý den v 00:40 pomocí antiviru a EDR.	ANO
25	Správce IS nebo KS musí zhodnotit všechny směry, vstupy/výstupy dat a jejich uložení či další zpracování v IS nebo KS a navrhnout způsob ochrany před škodlivým kódem.		NE

26	V rámci IS nebo KS jsou zavedeny minimálně následující opatření:		
26.1	• segmentace síťového prostředí (oddělení sítí pro provoz a pro správu), kde je to opodstatněné	Není zavedeno, vzhledem k velikosti sítě nemá segmentace smysl.	NE
26.2	• instalace SW pro detekci a odstranění škodlivých programů a na IS nebo KS, kde je to technicky realizovatelné	Instalováno jak na serverech, tak na koncových zařízeních.	ANO
26.3	• pravidelná aktualizace SW pro detekci a odstranění škodlivých kódů včetně databáze vzorků nejméně jednou denně		NE
27	V prostředí IS nebo KS je zakázáno vzdálené spouštění kódu ze zdroje mimo jejich prostředí.	Upraveno, například Powershell nesmí být spouštěn vzdáleně.	ANO

2.4.4. Kybernetické bezpečnostní události a incidenty

Pravidla pro vyhodnocování kybernetických bezpečnostních událostí (dále jen „KBU“) a zvládání KBI nejsou stanovena, stejně tak ani auditní požadavky. Analýza a evidence KBU a KBI je prováděna pomocí log managementu, a to za účelem eliminace jejich dalšího výskytu. Řízení a hlášení nestandardního chování je prováděno pomocí push notifikací v mobilní aplikaci DS finder a zprávou v elektronické poště pouze správci systému. Pokud jde o hlášení uživateli, není tento postup nijak formalizován.

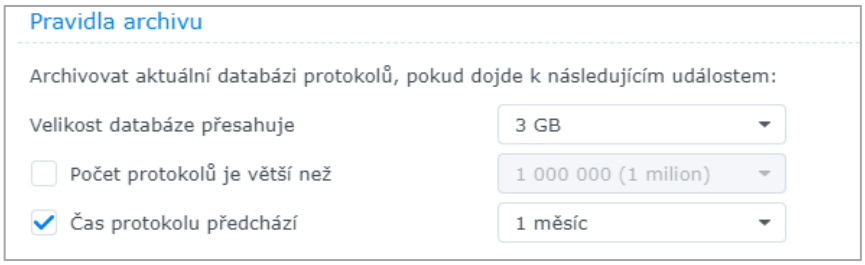
Dále, s ohledem na velikost společnosti, není nijak specifikován seznam kontaktních osob, kterým KBI a KBU hlásit. Dalším nalezeným nedostatek je, že zaměstnanci nebyli poučeni ani proškoleni o možném nebezpečí. Eskalační proces se seznamem osob, které budou o nestandardní situaci informovány a bude na ně případně přenesena odpovědnost za její řešení, není nastaven, jelikož je vzhledem k velikosti společnosti nerelevantní. Auditovatelnost dat a procesů je řízena pomocí log managementu, který také řeší uchovávání provozních záznamů z doby KBI a poskytuje všechny relevantní záznamy pro ex–post analýzu. Tyto záznamy jsou poté využitelné i pro řízení přístupu. Jedná se o kompletní výčet, který je doporučen dle MBS:

- přihlášení a odhlášení uživatelů a administrátorů, a to včetně neúspěšných pokusů
- činnosti provedené administrátory,
- použití privilegovaných účtů, např. účtu supervisora, či administrátora
- spuštění a ukončení IS nebo KS

- změny konfigurací
- úspěšné i neúspěšné činnosti vedoucí ke změně přístupových oprávnění
- zahájení a ukončení činností zařízení a aplikací
- automatická varovná nebo chybová hlášení zařízení a aplikací
- přístupy k záznamům o činnostech, pokusy o manipulaci se záznamy o činnostech a změny nastavení nástroje pro zaznamenávání činností
- použití mechanismů identifikace a autentizace včetně změny údajů, které slouží k přihlášení

Jednotlivé položky logu poté obsahují datum a čas události (uvedený s jednoznačnou identifikací časové zóny, např. UTC nebo lokální čas s uvedením offsetu), síťové identifikátory komunikujících bodů (tj. např. IP adresy a porty – v případě použití proxy nebo NATu musí být síťový identifikátor předán jinou formou nebo musí být možné tyto logy vyhodnocovat), identifikátor uživatele, pod kterým byla činnost provedena, typ události a úspěšnost, či neúspěšnost činnosti. V rámci logů nejsou přenášeny citlivé informace (hesla atp.).

Provozní a bezpečnostní logy jsou uchovávány dle nastavených pravidel archivace, které lze vidět na obrázku níže.



Obrázek č. 9: Pravidla archivace provozních a bezpečnostních logů
(Zdroj: Vlastní zpracování)

Centrálně jsou pak logy řízeny pomocí Central Management System, který uchovává logy všech zařízení, které jsou v síti přenášeny ve formátu IETF. Integrace do SIEM je vzhledem k velikost společnosti nerelevantní, vše je uchováváno v log managementu v nástroji Synology, který je umístěn na file serveru (NAS).

Je zavedena ochrana proti deaktivaci, selhání, či změnám v pořizování auditních záznamů, a také ochrana proti změnám a zničení samotných auditních záznamů. Přístup k auditním záznamům je chráněn pomocí omezením přístupu. Pomocí protokolu NTP je možno kontrolovat korelaci logu z více zařízení a systémový čas je synchronizován jednou za 24 hodin.

Tabulka č. 6: Vyhodnocení stavu v oblasti KBI a KBU
(Zdroj: Vlastní zpracování dle: 14, s. 23–27)

ID	Požadavek	Popis stavu	Stav zavedení
28	Stanovena pravidla pro vyhodnocování KBU a KBI.		NE
29	Evidování a analýza KBU a KBI za účelem eliminace dalšího výskytu.	Pomocí log managementu.	ANO
30	Stanoveny auditní požadavky.		NE
31	Stanoven proces pro řízení hlášení nestandardního chování IS nebo KS.	Hlášení je zasíláno správci sítě e-mailem a pomocí notifikace v aplikaci v mobilu. Proces hlášení nestandardního chování uživateli však není formalizován.	ANO
32	Zaměstnanci jsou seznámeni s tím, co mají hlásit a mají k dispozici konkrétní kontakty, na koho se v rámci organizace obracet.	Ne vzhledem k velikosti společnosti, ale jsou seznámeni s možným nebezpečím, avšak neexistuje žádná metodika, dle které se postupuje.	NE
33	Funguje eskalační proces, v rámci kterého jsou přesně definovány v rámci organizace osoby, které budou o situaci informovány a případně na ně bude přenesena odpovědnost za její řešení.	Ne vzhledem k velikosti společnosti, není relevantní.	NE
34	IS nebo KS zajišťuje auditovatelnost dat i procesů, včetně procesu řízení identit uživatelů.	Sledován provoz sítě pomocí log managementu.	ANO
35	Organizace disponuje provozními záznamy z doby KBI pro ex–post analýzu, tyto záznamy poskytují například: • bezpečnostní nástroje (antivirus, IDS/IPS, proxy, router, switch, firewall, …) • operační systémy (autentizace, privilegované spuštění, systémové události, …) • aplikace (komunikace mezi klientem a serverem, uživatelské události, přístupy, …)	Řešeno pomocí log managementu.	ANO
36	IS nebo KS uchovává provozní i bezpečnostní logy:	Probíhá dle nastavených pravidel archivace.	ANO

37	Logy IS nebo KS musí být integrovatelné do centrálního řešení pro vyhodnocování provozních a bezpečnostních logů, pokud takový IS nebo KS není zaveden, doporučuje se při výběru nové technologie vyžadovat minimálně jednu z následujících metod pro zajištění kompatibility v případě zavedení centrálního log managementu: • Syslog (RFC 5424) • SNMPv3 TRAP • JDBC • Microsoft Event Log	Central management system – uchovává logy všech zařízení, kterou jsou v síti přenášeny ve formátu IETF.	ANO
38	IS nebo KS, včetně infrastruktury (je jeho podpůrnou součástí a jeho další komponenty musí být připraveny na integraci do SIEM obdobným způsobem tak, aby naplňovaly požadavky na bezpečnostní monitoring.	Není relevantní – log management v nástroji Synology.	NE
39	Musí být pořizovány a uchovávány auditní záznamy tak, aby byly využitelné pro monitorování řízení přístupu a případné budoucí vyšetřování KBI. Jedná se minimálně o tyto typy událostí:	Auditní záznamy, které MBS doporučuje uchovávat, jsou uchovávány v rozsahu odpovídajícímu MBS.	ANO
40	Jednotlivé položky logu IS nebo KS nebo jeho jednotlivé řádky záznamu musí obsahovat minimálně tyto pole	Položky logu či jednotlivé řádky záznamu obsahují pole, které požaduje MBS.	ANO
41	V případě, že záznamy zapisované do logu IS nebo KS obsahují citlivé informace (heslo, soukromý klíč či jeho prekurzor, session ID apod.) musí být před zapsáním přepsány pseudonáhodnou sekvencí. V žádném případě nesmí dojít k zapsání citlivých informací v čistém textu.		ANO
42	V IS nebo KS musí být zavedena ochrana proti deaktivaci, selhání či změnám v pořizování auditních záznamů a ochrana proti změnám nebo zničení auditních záznamů.		ANO
43	Přístup k auditním záznamům musí být chráněn, aby bylo zabráněno jeho zneužití nebo ohrožení.	Ošetření přístupu.	ANO
44	IS nebo KS musí umožnit nastavení přístupových práv k auditním záznamům tak, aby mohly být auditovány samostatnou rolí (auditor, security officer apod.).		ANO
45	Aby bylo možné korelovat logy z více zařízení IS nebo KS, musí být systémový čas synchronizován v rámci IS nebo KS alespoň jednou za 24 hodin (např. pomocí protokolu NTP).	Řešeno pomocí NTP protokolu.	ANO

2.4.5. Požadavky v oblasti aplikační bezpečnosti

Požadavky, které MBS stanovuje v oblasti aplikační bezpečnosti, spočívají primárně ve stanovení základních principů pro oblast aplikační bezpečnosti a jejího testování. Konkrétně se pak jedná o provádění testování v odděleném prostředí a o stanovení pravidel pro testovací data (14, s. 27).

Jelikož Společnost X žádné aplikační testy neprovádí a je pro ni tato oblast bezpředmětná a to hlavně z důvodu, že sama nevyvíjí žádné aplikace. Společnost X využívá pouze aplikace třetích stran, které byly schváleny pro provoz v těchto typech společností a proběhla jejich nezávislá kontrola renomovanou instituci. Možnost testování těchto aplikací tedy není prakticky realizovatelná ani žádoucí.

2.4.6. Kryptografické prostředky

Šifrování přenosu dat je definováno klientem. Autorizovaný přístup k datům a informacím je chráněn pomocí nastavení oprávnění uživatelů. K šifrování disků nedochází. Ukládaná hesla jsou odolná proti offline útokům pomocí použití hashovacího algoritmu defaultně.

Tabulka č. 7: Vyhodnocení stavu v oblasti kryptografických prostředků
(Zdroj: Vlastní zpracování dle: 14, s. 28)

ID	Požadavek	Popis stavu	Stav zavedení
52	Zajistit šifrování přenosu dat. Šifrování uložených dat je pouze doporučeno, a to v návaznosti na typ a charakter dat a v návaznosti na možné technologické řešení.	Definováno klientem.	NE
53	Data a informace zpracovávaná v rámci IS nebo KS musí být chráněna proti zneužití vhodnými kryptografickými metodami, které zajistí pouze autorizovaný přístup k těmto datům a informacím.	Autorizovaný přístup řešen pomocí rolí.	ANO
54	Dle aktuálního doporučení NÚKIB je pro šifrování disků možné použít následující symetrické blokové šifrovací algoritmy: • Advanced Encryption Standard (AES) s využitím délky klíčů 128, 192 a 256 bitů • Twofish s využitím délky klíčů 128 až 256 bitů • Serpent s využitím délky klíčů 128, 192, 256 bitů	Nešifruje se.	NE

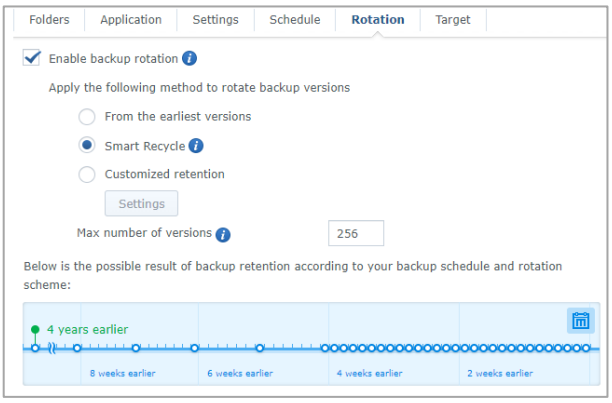
	• Camellia s využitím délky klíčů 128, 192 a 256 bitů • Přitom mezi preferované patří AES, Camellia a Serpent (v uvedeném pořadí) a velikost klíče 256 bitů		
55	Pro šifrování disků doporučení schvaluje použití následujících módů: • XTS • EME		NE
56	Pokud IS nebo KS ukládá hesla, musí být takto uložená hesla odolná proti offline útokům (tedy takovým způsobem, u kterého je výpočetně náročné z uloženého hesla získat původní heslo) nejlépe použitím k tomu určenému hašovacímu algoritmu spolu s náhodně vygenerovanou „solí“.	Defaultně pomocí hashovacího algoritmu.	ANO
57	Pokud IS nebo KS umožňuje volbu algoritmu nebo se jedná o nově vznikající IS nebo KS, doporučujeme použít jeden z následujících algoritmů (v pořadí od nejvhodnějšího): • Argon2 (nejlépe ve verzi „id“), • Scrypt, • Bcrypt, • Pbkdf2 (s použitím schváleného hašovacího algoritmu).	Nerelevantní.	x
58	„Sůl“ by měla mít velikosti minimálně 64 bitů (doporučujeme 128 bitů). Pokud je možné zvolit výpočetní náročnost algoritmu, výpočet by měl trvat výpočet minimálně 100 ms (doporučeno 500 ms) a využít minimálně 1 MB paměti.	Velikost soli nebyla zjištěna.	NE

2.4.7. Požadavky v oblasti zajišťování úrovně dostupnosti informací

Nejsou zpracovány plány kontinuity činností a dostupnost není nijak stanovena a definována, jelikož to z pohledu společnosti není relevantní. Zajištění dostupnosti je vyřešeno redundancí pomocí RAID1 a clusterování není využíváno, jelikož síť není natolik vytížená. Pravidlo eliminace Single Point of Failure (SPOF) je řešeno částečně na úrovni RAID 1. Zálohování je využíváno pouze pro file systém pro soubory, které jsou využívány k práci. Data aplikací zálohována nejsou.

Pro zálohování je využita metoda 3–2–1, tedy jedná se o alespoň tři různé verze dat v různých časových obdobích uložených na dvou různých médiích, aby při selhání jednoho disku mohlo dojít k obnově z druhého disku. Jedna záloha je dále umístěna mimo pracoviště.

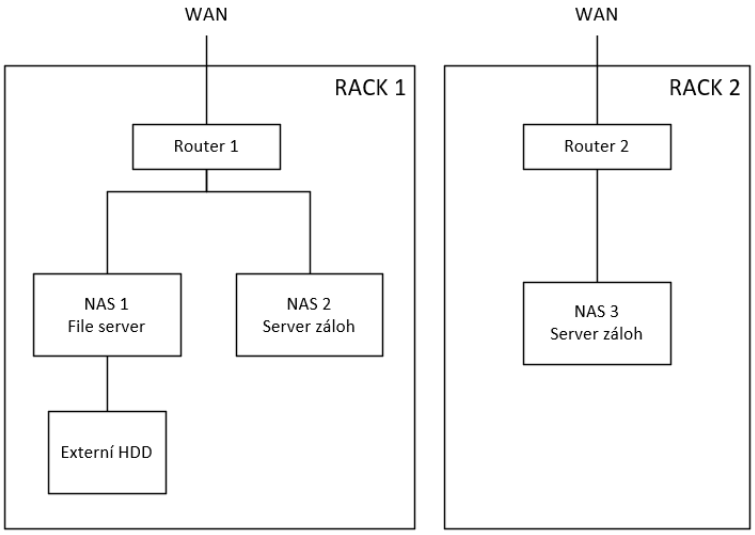
Prvním z médií je file server, ke kterému je připojen externí hard disk a na nějž se zálohy provádí, je umístěn v kancelářských prostorech v rozvaděči (RACK 1). Zálohy na file serveru se provádějí každých deset minut a ukládají se pouze jako změny. Je evidováno posledních 256 verzí a toto zálohování funguje na principu smart recycle. Princip smart recycle je založen na velikosti časové prodlevy, tedy čím je provedená záloha dál v čase, tím je delší časová prodleva mezi jednotlivými verzemi.



Obrázek č. 10: Smart recycle nastavení záloh
(Zdroj: Vlastní zpracování)

Server záloh, který je také umístěn v kancelářských prostorech v rozvaděči, je připojen po síti LAN. Zálohy jsou na něj prováděny jednou denně v 04:00 hodin a funguje také na principu smart recycle.

Zálohový server v sídle společnosti (RACK 2) je připojen přes internet. Zálohy jsou na něj prováděny jednou denně v 02:00 hodin, a také funguje na principu smart recycle.



Obrázek č. 11: Schéma zálohování Společnosti X
(Zdroj: Vlastní zpracování)

Tabulka č. 8: Vyhodnocení stavu v oblasti zajišťování úrovně dostupnosti informací
(Zdroj: Vlastní zpracování dle: 14, s. 30, 31)

ID	Požadavek	Poznámky	Stav zavedení
59	Dostupnost IS nebo KS musí být stanovena a definována správcem na požadovanou úroveň na základě plánu kontinuity činností – BCP	Není řešeno.	NE
60	Je řešeno zajištění dostupnosti implementací redundantních a clusterovaných schémat v režimu vysoké dostupnosti (HA), stanovením úrovně podpory, postupy obnovy po havárii a zálohováním.	Redundance zajištěna pomocí RAID1, clusterování není používáno, protože síť není natolik vytížená.	ANO
61	V maximální možné míře zohlednit dodržování pravidla eliminace „SPOF“ (Single Point of Failure) – to znamená, že porucha jedné komponenty nezpůsobí výpadek celého IS nebo KS. Při zohlednění pravidla SPOF je nutné brát do úvahy efektivitu (tedy náklady) a požadavky na dostupnost	Řešeno částečně na úrovni RAID1.	ANO
62	Vytvořen detailní návrh zálohování celého IS nebo KS v následující struktuře: Z hlediska potřebných zálohovacích médií je vhodné uvažovat o uplatnění pravidla 3–2–1. Toto pravidlo znamená, že jsou k dispozici tři kopie dat na dvou různých typech médií, přičemž jedno z nich by se mělo nacházet mimo lokalitu umístění IS nebo KS („offsite“).	Ano, zálohování využíváno pro file systém a pro soubory používány k práci metodou 3–2–1. Data aplikací nejsou zálohována.	NE

2.4.8. Požadavky v oblasti cloudových služeb

Doporučení MBS týkající se oblasti cloudových služeb spočívají v zajištění kybernetické bezpečnosti při využívání cloudových služeb. Pokud jsou cloudové služby využívány pro provoz IS nebo KS, je třeba zajistit na této úrovni kybernetickou bezpečnost. Na poskytovatele cloudových služeb je vhodné vztáhnout stejná pravidla jako pro ostatní dodavatele a stejně k nim přistupovat. MBS stanovuje následující podmínky pro využívání cloudových služeb:

- deklarace místa uložení zákaznických dat v rámci jurisdikce EU,
- deklarace úrovně bezpečnosti poskytovaných cloudových služeb – (doporučeno doložení certifikátu ČSN ISO/IEC 27001 nebo Auditní zpráva SOC 2 Type II (AT101), případně zajištění auditu na místě),
- šifrovaná komunikace (TLS/VPN) přes internet s využitím kryptografických algoritmů publikovaných v doporučení NÚKIB,
- smlouva s provozovatelem cloudových služeb obsahující vymezení provozních podmínek (SLA) a tzv. exit strategii (exit plán) včetně předání dat,
- smluvní podmínky s provozovatelem cloudových služeb, které jsou v souladu s požadavky na zpracovatele dle čl. 28 Obecného nařízení GDPR (v případě zpracování osobních údajů v IS nebo KS),
- smlouva s provozovatelem cloudových služeb obsahující povinnost informovat o KBI týkajících se daného zákazníka, a spolupracovat při jejich zvládání (14, s. 33).

V případě Společnosti X jsou externí přístupy k datům zajišťovány interně pomocí vlastních serverů – používána VPN s šifrováním a přenosem souborů pomocí protokolů SMB.

2.4.9. Výjimky běhu, chyby a hlášení

MBS v oblasti výjimek běhu, chyb a hlášení požaduje řídit výjimky a také je evidovat. Výjimkou je v tomto případě myšlena libovolná chyba nebo neočekávané chování IS nebo KS, která se vyskytne během vykonávání programu. Pro řízení výjimek je nutno, aby IS nebo KS řízení výjimek podporoval, výjimky byly zaznamenávány v logu a tyto logy byly pravidelně vyhodnocovány a zjištěné nedostatky byly řešeny.

Proces pro řízení výjimek a ani proces jejich evidence není stanoven, jelikož výjimky nejsou používány. Výjimky je možné udělovat, s ohledem na nastavení a dostatečnou definici uživatelských skupin, však není tato možnost využívána. V případě, že by k udělení výjimky došlo, bude toto udělení zaznamenáno v příslušném logu. Logy jsou pravidelně vyhodnocovány.

Tabulka č. 9: Vyhodnocení stavu v oblasti výjimek běhu, chyb a hlášení
(Zdroj: Vlastní zpracování dle: 14, s. 34)

ID	Požadavek	Popis stavu	Stav zavedení
65	Je stanoven proces řízení výjimek a jejich evidence.	Nejsou používány výjimky, uživatelské skupiny jsou nastaveny dostatečně a není třeba využívat výjimky.	ANO
66	IS nebo KS podporuje řízení výjimek	Řízení výjimek je podporováno.	ANO
67	Výjimky jsou zaznamenány v logu.	Ano, v případě, že by došlo k udělení výjimky, bude toto udělení zaznamenáno v logu.	ANO
68	Log je pravidelně vyhodnocován, přičemž zjištěné nedostatky nebo závady v IS nebo KS jsou v maximální možné míře ošetřeny.	Dochází k pravidelnému vyhodnocování logů a při zjištění nestandardní události dochází k prozkoumání stavu a její případné nápravě.	ANO

2.4.10. Ochrana IS nebo KS typu webové aplikace

V oblasti ochrany IS nebo KS webové aplikace je dle MBS vhodné řídit se doporučením komunity zabývající se bezpečností webových aplikací, OWASP, a věnovat se jimi zveřejněnými zranitelnostmi. Z webových aplikací má Společnost X dostupný balíček služeb Microsoft 365, který ale není žádným ze zaměstnanců využíván, a k práci je používána pouze desktopová verze aplikace. Z tohoto důvodu tedy není zavedena ochrana webových aplikací a Společnost X doporučení OWASP nezohledňuje (14, s. 34).

2.4.11. Rozvoj informačních a komunikačních systémů

V oblasti rozvoje IS a KS je MBS doporučeno posoudit bezpečnostní aspekty vyvíjeného IS nebo KS a na základě posouzení poté definovat obecné bezpečnostní požadavky pro IS nebo KS v oblasti triády CIA, tedy důvěrnosti, dostupnosti a integrity informací. Součást těchto požadavků jsou dle MBS následující body:

- identifikace dat vytvářených, zpracovávaných a ukládaných v IS nebo KS,
- definice klíčových bezpečnostních rolí včetně školení uživatelů, správců a vývojářů,
- identifikace zdrojů požadavků na IS nebo KS z hlediska bezpečnosti a regulatorních požadavků.

V případě, že se jedná o IS nebo KS vyvíjen dodavatelem na míru dané společnosti, je nutno definovat a dokumentovat alespoň následující požadavky:

- požadavky na licenční ujednání, vlastnictví kódu a práv duševního vlastnictví,
- požadavky na osvědčení kvality a správnosti provedených prací,
- požadavky na uložení zdrojového kódu,
- požadavky na právo přístupu k vývoji pro audit bezpečnosti a správnosti provedené práce,
- požadavky na smluvní podmínky na bezpečnost a zabezpečení kódu,
- smluvně ošetřit uložení zdrojových kódů u důvěryhodné třetí strany (code escrow) v případě, že dodavatel nepředává zdrojový kód jako součást dodávky vyvíjeného programového vybavení
- požadavky na provedení testů zranitelností před instalací v produkčním prostředí

Tyto požadavky musí být v souladu s existujícími směrnicemi jejichž součástí je i komunikační matice při vývoji aplikace, a na tuto skutečnost dohlíží správce IS nebo KS. Ten dále definuje a dokumentuje akceptační kritéria pro přechod do nového IS nebo KS při přechodu z testovacího do produkčního prostředí. V případě vývoje nového IS nebo KS je nutno oddělit testovací prostředí od provozního prostředí včetně správy uživatelských oprávnění. V případě vývoje aplikace, která bude součástí IS nebo KS je nutno zhotovit metodiku pro její vývoj, programování, kódování a testování. Zhotovitel metodiky je povinen doložit typ metodiky, který použil pro vývoj aplikace

prostřednictvím čestného prohlášení a dodání popisu nebo dokumentace této metodiky. Tato metodika z bezpečnostního hlediska obsahuje minimálně:

- požadavky na kybernetickou bezpečnost a
- principy organizační bezpečnosti pro vývoj a testování (14, s. 35).

Jelikož jsou využívány pouze IS a KS třetích stran, které byly schváleny pro provoz v těchto typech společností a proběhla jejich nezávislá kontrola renomovanou instituci a k samotnému vývoji nedochází, je irelevantní se touto problematikou zabývat.

2.4.12. Komunikace

Ke komunikaci je využíván Microsoft Exchange Server, který umožňuje následující rozdělení komunikace s externími IS nebo KS dle stupně zabezpečení vyhovujícímu požadavkům MBS:

- zabezpečený kanál přenosu (šifrování dat) s povinnou úrovní zabezpečení koncových bodů IS nebo KS na úrovni infrastruktury
- šifrování dat pro přenos a autorizací uživatele v rámci IS nebo KS
- zajištění šifrování nebo náhradu citlivých dat na úrovni poskytovatelských a konzumentských informačních nebo komunikačních systémů pomocí end to end metody při přenosu dat

Tabulka č. 10: Vyhodnocení stavu v oblasti komunikace
(Zdroj: Vlastní zpracování dle: 14, s. 36)

ID	Požadavek	Popis stavu	Stav zavedení
80	Komunikace s externími IS nebo KS by měla být rozdělena podle stupně zabezpečení na:	Zajišťováno pomocí Microsoft Exchange Server, který níže doporučované zabezpečení umožňuje a společností je tato možnost využívána.	
80.1	• zabezpečený kanál přenosu (šifrování dat) s povinnou úrovní zabezpečení koncových bodů IS nebo KS na úrovni infrastruktury,		ANO
80.2	• šifrování dat pro přenos a autorizací uživatele v rámci IS nebo KS,		ANO
80.3	• zajištění šifrování nebo náhradu citlivých dat na úrovni poskytovatelských a konzumentských IS nebo KS pomocí end to end metody při přenosu dat.		ANO

2.5. Vektor útoku

Útok, který společnost postihl a který je také impulsem pro tuto diplomovou práci, byl detekován jako ransomwarový útok. Byly identifikovány dva nejpravděpodobnější vektory útoku, které budou více popsány dále. Hlavním motivem útoku bylo napadení dat, která byla zašifrována. Po detailnějším průzkumu napadeného systému byl nalezen i vzkaz s žádostí o vyplacení výkupného pro odšifrování dat. Jak je ale známo z nejlepší praxe, neexistuje jistota, že po zaplacení výkupného k dešifrování dat opravdu dojde. Společnost X se tedy možnost zaplacení výkupného rozhodla nevyužít a se situací se vypořádala jiným způsobem.

Ransomwarový útok společnost postihl v pátek večer a problémy zaznamenal zaměstnanec až v pondělí ráno. Společnost na situaci zareagovala ihned po jejím zjištění a po zhodnocení a finančním vyčíslení snahy o obnovu dat jiným způsobem (například pokusem o dešifrování dat vlastními silami) se rozhodla pro úplné smazání dat za dané účetní období a o naplnění databáze POHODY ručním nahráváním. Jelikož ekonomické výsledky předchozích let byly vždy po ukončení účetního roku vyexportovány a zaslány účetní, byla možnost smazání dat efektivní. Došlo tedy ke ztrátě dat pouze za dané účetní období.

Prvním možným vektorem útoku byl ransomware nasazený do systému pomocí **phishingového emailu**. V tomto případě by se jednalo o zásadní pochybení lidského faktoru, kterému se dalo snadno předejít pravidelným školením zaměstnanců.

Druhou možností je pak ransomware nasazený do systému při připojení pomocí vzdáleného přístupu. V tomto případě by se jednalo o **zneužití RDP protokolu** (Remote Desktop Protocol) jehož popularita v době koronavirové krize výrazně vzrostla z důvodu častějšího využívání home office (práce z domova). V případě, že by zaměstnanec vzdáleně přistupoval bez využití VPN nebo bez použití vícefázového ověření, mohlo snadno dojít k napadení společnosti právě touto formou.

2.6. Následky útoku – situace po útoku

Ransomwarový útok, ať už proběhl jedním nebo druhým způsobem, zapříčinil kompletní zašifrování dat POHODY, která obsahovala faktury za účetní rok 2021/2022. Jelikož se útok stal na konci února roku 2022 a účetní období Společnosti X začalo v říjnu roku 2021, jednalo se o ztrátu dat za pět měsíců.

Společnost neměla pro POHODU aktivní zálohu, a proto se nepodařilo zašifrovaná data obnovit. Z tohoto důvodu bylo nutné všechna ztracená data doplnit do systému ručně, což stálo mnoho lidské práce a času, a tedy i finančních prostředků.

Jelikož se část zaměstnanců musela věnovat ručnímu zadávání údajů z tohoto účetního období bylo nutno zadat nejprve historické údaje a až poté doplňovat do účetního systému nově vzniklé účetní případy. Celkem tento proces trval tři týdny, než bylo možné opět nastolit běžný provoz POHODY.

3. VLASTNÍ NÁVRH ŘEŠENÍ

Vzhledem k nulové úrovni plnění organizační části MBS se vlastní návrh řešení primárně zaměří na organizační část. Konkrétně se bude jednat o nastavení politik a metodik, které jsou dále stěžejní pro nasazení relevantních technických bezpečnostních opatření. Dále budou navržena relevantní technická bezpečnostní opatření, jež budou řešit stěžejní nedostatky z Analytické části, které budou v souladu s navrženými bezpečnostními politikami
a budou podporovat jejich účel. Pro Společnost X je bezpředmětné disponovat všemi technikáliemi, které MBS doporučuje, pokud nezajistí kvalitnější úroveň kybernetické bezpečnosti a pokud nebude společnost schopna tyto prostředky korektně spravovat prostřednictvím kvalifikované osoby.

3.1. Matice stávajících neshod a návrh nápravných opatření

V následující matici jsou znázorněny vztahy mezi nalezenými neshodami, jednotlivé neshody jsou poté ohodnoceny z hlediska finanční a časové náročnosti a z těchto dvou veličin je poté součtem vyjádřena náročnost implementace. Dále byla určena kritičnost těchto neshod, aby bylo možné v rámci zavádění nápravných opatření prioritizovat. Mnoho z nalezených neshod lze vyřešit zavedením a dodržováním bezpečnostní politiky, některé z nich však není možné realizovat s ohledem na omezení, které plynou například z nájemní smlouvy, což omezuje možné zásahy do komunikační infrastruktury a provádění rozsáhlých úprav. Neshody, které je nutno akceptovat, jsou také technického rázu a není možno je řešit, jelikož by řešení bylo příliš nákladné nebo vzhledem k velikosti společnosti nadbytečné. Dále byly nalezeny neshody v technické oblasti, které lze napravit pouhou změnou nastavení, v některých případech se jedná o časově, či finančně náročnější řešení. Takové neshody mohou být zavedeny až do dvou let od jejich identifikace.

Tabulka č. 11: Hodnotící stupnice pro časovou a finanční náročnost a pro kritičnost dané položky
(Zdroj: Vlastní zpracování)

	Finanční náročnost	**Časová náročnost**	**Kritičnost**
Nízké	3	3	1
Střední	2	2	2
Vysoké	1	1	3

Zjištění náročnosti implementace bylo vypočteno součtovou metodou dle následujícího vzorce, kdy NI vyjadřuje náročnost implementace, FN vyjadřuje finanční náročnost a ČN vyjadřuje časovou náročnost.

$$NI = ČN \cdot FN$$

Vzorec č. 1: Vzorec náročnosti implementace
(Zdroj: Vlastní zpracování)

Tabulka č. 12: Hodnotící stupnice pro náročnost implementace
(Zdroj: Vlastní zpracování)

Náročnost implementace – hodnoticí stupnice		
snadná implementace		6–9
středně náročná implementace		3–4
náročná implementace		1–2

Rozhodnutí o zavedení daného opatření je nutno vypočíst, a z důvodu budoucí potřeby a je učiněno na základě kritičnosti a náročnosti implementace. Tento výpočet je proveden metodou součinu obou činitelů dle následujícího vzorce, kdy písmeno R označuje rozhodnutí o zavedení, NI označuje náročnost implementace a K kritičnost nalezené neshody.

$$R = NI \cdot K$$

Vzorec č. 2: Vzorec pro rozhodnutí o zavedení
(Zdroj: Vlastní zpracování)

Tabulka č. 13: Hodnotící stupnice pro rozhodnutí o zavedení
(Zdroj: Vlastní zpracování)

Rozhodnutí o zavedení – hodnotící stupnice		
Zavést do 2 let od nalezení neshody		1–4
Zavést do 1 roku od nalezení neshody		6–9
Zavést okamžitě		12–27

U každé nalezené neshody byl identifikován i typ, tedy zda nalezená neshoda spadá do oblasti organizační (ORG) nebo technické (TECH).

Tabulka č. 14: Hodnotící matice neshod dle MBS a analytické části v technické oblasti
(Zdroj: Vlastní zpracování dle: 14, s. 17–36)

ID	Požadavek	Stav zavedení	Nápravné opatření	FN	ČN	NI	K	R	Typ
Fyzická bezpečnost									
1	Definovat nový, či rozšířit stávající soubor opatření předcházející poškození, krádeži či zneužití informací či majetku nebo přerušení služeb IS nebo KS, vymezit fyzický perimetr.	NE	Není možné, vychází z pravidel nájemní smlouvy.	x	x	x	x	x	ORG
4	Jasně definována pravidla pro návštěvy.	NE	Upravit v politice.	3	1	3	2	6	ORG
7	Zajištěna bezpečnost kabelových rozvodů.	NE	Není možné, vychází z pravidel nájemní smlouvy.	x	x	x	x	x	TECH
Řízení přístupů									
8	Vytvořena politika řízení přístupu.	NE	Vytvořit politiku řízení přístupů.	3	2	6	3	18	ORG
12	Jsou definovány postupy a pravidla potřebné pro omezení a kontrolu používaného SW a HW, který by mohl narušit systémovou a aplikační bezpečnost.	NE	Upravit v politice řízení přístupů.	3	2	6	3	18	ORG
15	Uplatňován princip need–to–know.	NE	Není v možnostech, vychází z velikosti firmy a předmětu podnikání.	x	x	x	x	x	ORG
22	Existuje politika hesel pro privilegované účty v minimální míře:		Upravit v politice řízení přístupů a změnit současné nastavení.	3	2	6	3	18	ORG, TECH
22.1	• minimální délka hesla je 17 znaků	NE							
22.3	• maximální doba platnosti hesla je 18 měsíců	NE							
22.4	• zákaz používaní stejného hesla (posledních 12 hesel)	NE							
22.5	• minimální platnost hesla 1 den	NE							
23	Existuje politika hesel pro uživatelské účty v minimální míře:		Upravit v politice řízení přístupů a změnit současné nastavení.	3	2	6	3	18	ORG, TECH
23.1	• minimální délka hesla je 10 znaků	NE							
23.2	• zákaz používaní stejného hesla (posledních 12 hesel)	NE							
23.3	• maximální doba platnosti hesla je 18 měsíců	NE							

ID	Požadavek	Stav zavedení	Nápravné opatření	FN	ČN	NI	K	R	Typ
Požadavky v oblasti ochrany před škodlivým kódem									
25	Správce IS nebo KS musí zhodnotit všechny směry, vstupy/výstupy dat a jejich uložení či další zpracování v IS nebo KS a navrhnout způsob ochrany před škodlivým kódem.	NE	Vytvořit politiku ochrany před škodlivým kódem.	3	2	6	3	18	ORG
26	V rámci IS nebo KS jsou zavedeny minimálně následující opatření:			x	x	x	x	x	TECH
26.1	• segmentace síťového prostředí (oddělení sítí pro provoz a pro správu), kde je to opodstatněné	NE	Segmentace z hlediska velikosti společnosti nemá smysl.	x	x	x	x	x	
26.3	• pravidelná aktualizace SW pro detekci a odstranění škodlivých kódů včetně databáze vzorků nejméně jednou denně	NE	Upravit v politice ochrany před škodlivým kódem a změnit současné nastavení.	3	2	6	3	18	
Kybernetické bezpečnostní události a incidenty									
28	Stanovena pravidla pro vyhodnocování KBU a KBI.	NE	Vytvořit politiku kybernetických událostí a incidentů.	3	2	6	3	18	ORG
30	Stanoveny auditní požadavky.	NE	Upravit v politice kybernetických událostí a incidentů.	2	2	4	2	8	ORG
32	Zaměstnanci jsou seznámeni s tím, co mají hlásit a mají k dispozici konkrétní kontakty, na koho se v rámci organizace obracet.	NE	Upravit v politice kybernetických událostí a incidentů.	3	2	6	2	12	ORG
33	Funguje eskalační proces, v rámci kterého jsou přesně definovány v rámci organizace osoby, které budou o situaci informovány a případně na ně bude přenesena odpovědnost za její řešení.	NE	Upravit v politice kybernetických událostí a incidentů.	3	2	6	2	12	ORG
38	IS nebo KS, včetně infrastruktury (je jeho podpůrnou součástí a jeho další komponenty musí být připraveny na integraci do SIEM obdobným způsobem tak, aby naplňovaly požadavky na bezpečnostní monitoring.	NE	Bezpečnostní monitoring je nahrazen sledováním a aktivním prováděním log managementu. Zakoupení a následná implementace SIEM je pro společnost v poměru přínos x cena nevýhodnou investicí, která je příliš nákladná.	x	x	x	x	x	TECH

ID	Požadavek	Stav zavedení	Nápravné opatření	FN	ČN	NI	K	R	Typ
Kryptografické prostředky									
52	Zajistit šifrování přenosu dat. Šifrování uložených dat je pouze doporučeno, a to v návaznosti na typ a charakter dat a v návaznosti na možné technologické řešení.	NE	Vynutit šifrování přenosu.	2	3	6	2	12	TECH
Požadavky v oblasti zajišťování úrovně dostupnosti informací									
59	Dostupnost IS nebo KS musí být stanovena a definována správcem na požadovanou úroveň na základě plánu kontinuity činností – BCP	NE	Bude definováno pomocí RTO a RTP.	2	2	4	2	8	ORG
62	Vytvořen detailní návrh zálohování celého IS nebo KS v následující struktuře:	NE		x	x	x	x	x	ORG, TECH
	• Z hlediska potřebných zálohovacích médií je vhodné uvažovat o uplatnění pravidla 3–2–1. Toto pravidlo znamená, že jsou k dispozici tři kopie dat na dvou různých typech médií, přičemž jedno z nich by se mělo nacházet mimo lokalitu umístění IS nebo KS („offsite“).		Zálohovat data aplikací, speciálně se jedná o POHODU.	2	3	6	3	18	TECH
Ochrana IS nebo KS typu webové aplikace									
69	Řídit se doporučeními OWASP a věnovat pozornost zranitelnostem.	NE	Jelikož webovou aplikaci nikdo ze zaměstnanců nepoužívá, bude možnost webové aplikace zakázána a zaměstnanci budou i nadále využívat pouze desktopovou verzi.	3	3	9	2	18	ORG, TECH

3.2. Organizační část MBS

V rámci této kapitoly došlo k navržení bezpečnostních politik, jež reflektují požadavky MBS které byly upraveny dle možností Společnosti X. Tato kapitola slouží mimo jiné i jako metodická podpora pro navržená řešení technického rázu, jelikož některá technická řešení je nutno nejen fyzicky přenastavit, ale také jejich postup formalizovat příslušnou politikou. Je proto žádoucí, aby se obsahově organizační a technická část prolínaly.

Organizační část MBS nebyla, co se týče formalizace daných pravidel a politik, řízena vůbec. Bylo proto bezpředmětné se jí věnovat v analytické části, jelikož zde byla úroveň nasazení nulová. Předmětem této kapitoly je vytvoření bezpečnostních politik v jednotlivých oblastech, které jsou MBS doporučeny obsáhnout a formalizovat. Je ale nutné zdůraznit, že navrženou bezpečnostní dokumentaci je třeba udržovat aktuální, aby dostatečně reflektovala stav bezpečnosti v organizaci. Konkrétně se jedná o oblasti:

- Základní předpoklady, které jsou obsaženy v Politice systému řízení bezpečnosti informací
- Identifikace aktiv, popsáno v Politice řízení aktiv
- Klasifikace a ochrana informací, popsáno v Metodice pro identifikaci a hodnocení informací
- Řízení dodavatelů, popsáno v Politice řízení dodavatelů
- Řízení lidských zdrojů, popsáno v Politice bezpečnosti lidských zdrojů
- Řízení změn, popsáno v Politice řízení změn
- Řízení kontinuity činností, popsáno v Politice řízení kontinuity činností
- Audit kybernetické bezpečnosti, popsáno v Politice auditu kybernetické bezpečnosti

3.2.1. Obsazení pozice manažera kybernetické bezpečnosti

Nejvýznamnějším nedostatkem, který však nebyl přímo identifikován v matici neshod, avšak s ní úzce souvisí, je absence MKB. Jedná se o pozici, jejíž náplní práce je právě zajišťování systému řízení bezpečnosti informací (dále jen „SŘBI“). MKB má za úkol zajištovat aktualizaci bezpečnostních politik, kontrolovat jejich dodržování, zajišťovat organizační i technické aspekty SŘBI a provádět interní audit.

Po zhodnocení nákladnosti zaměstnání MKB a jeho začlenění do organizační struktury společnosti a také zhodnocení jeho předpokládaného pracovního vytížení je doporučeno obsadit pozici MKB formou služby a jeho služeb bude fyzicky třeba jednou měsíčně.

3.2.2. Politika systému řízení bezpečnosti informací

Účelem této politiky je popis obecných procesů, které jsou klíčové pro stanovení správného SŘBI. V následující politice budou popsány stěžejní oblasti této problematiky.

Závazek vedení

Vedení Společnosti X se zavazuje ke vzniku, řízení, kontrole a podpoře uceleného a funkčního SŘBI. Vedení společnosti se dále zavazuje k podpoře řízení SŘBI zajištěním lidských, finančních a technických zdrojů. Řízení SŘBI je proces, který je dokumentovaný, opakovatelný a přezkoumatelný.

Cíle, principy a potřeby SŘBI

- Zajištění potřebných zdrojů pro rozvoj oblasti SŘBI
- Implementace bezpečnostních opatření a jejich průběžná aktualizace
- Formalizace procesů a postupů
- Stanovení bezpečnostní role
- Stanovení zodpovědností
- Průběžná aktualizace relevantních bezpečnostních politik
- Zvýšení úrovně bezpečnostního povědomí zaměstnanců (30)

Měřitelné cíle

- Zajistit soulad s MBS alespoň z 70 %.
- Zavést školení v oblasti kyberbezpečnosti a zvýšit bezpečnostní povědomí ve společnosti pomocí školení alespoň jednou ročně.

Rozsah a hranice SŘBI

Rozsah SŘBI je určen na celou organizaci, jelikož se jedná o malou společnost, je tedy pro zajištění celkové bezpečnosti organizace po kybernetické stránce žádoucí pojmout rozsah SŘBI na celou organizaci. Rozsah tedy konkrétně zahrnuje fyzické, organizační a personální a technologické aspekty. Jednotlivé složky rozsahu jsou konkretizovány níže.

- **Fyzické aspekty rozsahu**
  - Fyzickým perimetrem jsou všechny prostory, které společnost využívá a provozuje a jsou v jejím vlastnictví nebo v nájmu, konkrétně se pak jedná o:
    - Skladové prostory
    - Kancelářské prostory
    - Sídlo společnosti
- **Organizační a personální aspekty rozsahu**
  - Oblast organizačních a personálních aspektů obsahuje lidské zdroje, které mají vliv na rozsah ŠRBI. Jedná se tedy o všechny zaměstnance, ale i dodavatele a subdodavatele.
- **Technologické aspekty rozsahu**
  - Do technologických aspektů se řadí primární a podpůrná aktiva, které jsou spravovány či provozovány v rámci organizace, ale také dodavateli.

Pravidla a postupy pro přezkoumání SŘBI

Pravidelné přezkoumání SŘBI probíhá každý rok a obsahuje hodnocení současného stavu, příležitostí pro rozvoj a nutnost změn. Toto přezkoumání provádí odpovědná osoba, která má oblast kybernetické bezpečnosti na starost a kooperuje na této činnosti s dalšími zainteresovanými stranami. Po dokončení přezkoumání je vytvořena zpráva z přezkoumání, která je prezentována vedení společnosti.

Vstupy do přezkoumání SŘBI

- Matice neshod
- Přehled KBU a KBI za uplynulé období
- Vyhodnocení plánu vzdělávání v oblasti kybernetické bezpečnosti

Výstupy z přezkoumání SŘBI

- Zpráva z interního auditu SŘBI
- Identifikace možností pro neustálé zlepšování
- Doporučení potřebných rozhodnutí, stanovení nápravných opatření a osob zajišťujících výkon jednotlivých činností

Pravidla a postupy pro nápravná opatření a zlepšování systému řízení bezpečnosti informací

Nápravná opatření vychází ze zprávy z přezkumu SŘBI. Pro každé nápravné opatření je pak stanoven termín jeho zavedení a také odpovědná osoba, která je za celý proces implementace daného nápravného opatření zodpovědná. Zavedení bezpečnostních opatření bude kontrolováno při dalším přezkumu SŘBI.

3.2.3. Metodika pro hodnocení a ochranu informací

Pro zajištění adekvátní ochrany informací je třeba informace třídit dle jejich hodnoty a následně důležitosti. Jelikož všechny informace není nutno chránit na stejné úrovni, je možno s nimi manipulovat rozdílně. Díky tomuto ohodnocení může dojít k úspoře finančních prostředků, jelikož existují informace, které je třeba chránit méně.

Informace je třeba ohodnotit dle následující stupnice z hlediska triády CIA, tedy dle důvěrnosti, integrity a dostupnosti. **Důvěrností** je myšleno zajištění, že se k informaci dostane pouze člověk, kterému je určena, **integritou** je myšlen nezměněný stav dané informace či systému neautorizovanou osobou (informace se přenosem nezměnila) a **dostupností** je myšlen stav, kdy je informace, služba či systém dostupný v případě potřeby.

Tabulka č. 15: Hodnocení informací
(Zdroj: 14, s. 8)

Úroveň	Důvěrnost	Integrita	Dostupnost
1	Informace jsou veřejně přístupné nebo byly určené ke zveřejnění. Narušení důvěrnosti neohrožuje oprávněné zájmy organizace.	Narušení integrity neohrožuje oprávněné zájmy organizace.	Narušení dostupnosti není důležité a v případě výpadku je běžně tolerováno delší časové období pro nápravu.
2	Informace nejsou veřejně přístupné a tvoří know–how organizace	Narušení integrity informace může vést k poškození oprávněných zájmů organizace.	Narušení dostupnosti by nemělo překročit dobu několika hodin. Výpadek je nutné řešit bez zbytečného odkladu, protože vede k ohrožení oprávněných zájmů organizace.
3	Informace nejsou veřejně přístupné a vyžadují nadstandardní míru ochrany nad rámec předchozí kategorie.	Narušení integrity vede k poškození oprávněných zájmů organizace.	Narušení dostupnosti není přípustné, a i krátkodobá nedostupnost vede k vážnému ohrožení oprávněných zájmů organizace.

Po ohodnocení jednotlivých složek informace je třeba zvolit nejvyšší hodnotu a dle ní k informaci přistupovat. Toto ohodnocení by měl provést MKB společně s garantem dané informace. Pro zvolení správného postupu při ochraně informací je nutno řídit se následující tabulkou:

Tabulka č. 16: Úroveň ochrany informací
(Zdroj: 14, s. 9)

Úroveň		Důvěrnost	Manipulace	Likvidace	Změny	Zálohování
1	Nízká	Dokument má na všech stranách v záhlaví označení VEŘEJNÉ	Bez omezení	Bez omezení	Evidence verzí	Zálohování podle individuální potřeby
2	Střední	Dokument má na všech stranách v záhlaví a zápatí označení INTERNÍ	Pro interní potřebu, je omezen přístup k informacím osobám, které je nepotřebují k výkonu práce, pokud lze je nutno využívat šifrování	Přepis nosiče informací, anebo jeho fyzická likvidace	Evidence verzí, omezení práv na změnu	Pravidelné zálohování podle individuální potřeby, pravidelná kontrola záloh
3	Vysoká	Dokument má na všech stranách v záhlaví a zápatí označení CITLIVÉ	Přístupné pouze pro vyhrazené skupiny uživatelů, vyžadováno šifrování, šíření nutno nechat schválit garantem informace	Zajištění trvalého znehodnocení informace bez možnosti obnovy dle typu nosiče, případně fyzická likvidace nosiče	Evidence verzí, omezení práv na změnu, auditní záznamy o změnách	Pravidelné zálohování podle individuální potřeby, pravidelná kontrola záloh

3.2.4. Identifikace a ohodnocení informací

Následující kapitola popisuje proces hodnocení a identifikace informací dle Metodiky pro hodnocení a ochranu informací.

Společnost využívá různé typy informací a dokumentů k výkonu práce. Jednotlivé typy jsou rozděleny do skupin. Rozdělení do skupin je pro Společnost X optimální volbou, jelikož jsou skupiny nastaveny na dostatečný rozsah tak, aby byl název skupiny vypovídající a výstižný. Následně jsou jednotlivé skupiny ohodnoceny dle metodiky pro hodnocení informací a poté dle mechanismu nejvyšší hodnoty stanovena výsledná hodnota informace.

Identifikace informací

Nejprve byla provedena identifikace základních skupin informací, se kterými společnost pracuje. U jednotlivých skupin byl proveden stručný popis a poté byli určeni garanti informace, kteří nesou odpovědnost za zabezpečení správného nakládání.

Tabulka č. 17: Identifikace informací
(Zdroj: Vlastní zpracování)

ID	Název	Popis	Garant
1	Podklady od zákazníka pro zpracování nabídky	Podrobnosti o předpokládaném chování technologie, zadání projektu, finanční možnosti, předpoklady, cíle projektu, zadávací podmínky	Obchodní oddělení
2	Poptávky subdodavatelům	Zajištění dílčích řešení, technická podpora, montážní činnost	Obchodní oddělení
3	Nabídky subdodavatelů	Cenové nabídky a nabídky termínů	Obchodní oddělení
4	Kalkulace zakázky	Sestavení nákladů a stanovení marže	Oddělení realizace
5	Nabídka na realizaci projektu	Finální cenová nabídka pro zákazníka	Obchodní oddělení
6	Objednávka nebo smlouva se zákazníkem	SLA, smluvní pokuty, termíny, objednávka	Obchodní oddělení
7	Projektová dokumentace pro realizaci projektu	DWG výkresy, projekty v příslušných SW programech	Oddělení projekce
8	Objednávky subdodavatelům	Objednávky na materiál, pracovní sílu, …	Obchodní oddělení
9	Řízení zakázky	Stavební deníky, zápisy z kontrolních dnů, protokoly, ...	Oddělení realizace
10	Předávací dokumentace pro zákazníka	Projekty v online a tištěné formě	Oddělení projekce
11	Fakturace a účetnictví	Faktury, zálohové faktury, mzdy	Ekonomické oddělení
12	Interní dokumenty	Smlouvy se zaměstnanci, s dodavateli, směrnice	Jednatel společnosti
13	Bezpečnostní dokumentace	Nově vzniklé politiky	MKB

Ohodnocení informací

Ohodnocení informací bylo provedeno na identifikovaných skupinách společně s garanty daných skupin. Následně byla zvolena vždy nejvyšší hodnota z parametrů důvěrnosti, dostupnosti a integrity a byl vytvořen výsledek, který byl dle Tabulky č. 18 interpretován.

Tabulka č. 18: Ohodnocení informací
(Zdroj: Vlastní zpracování)

ID	Informace	Důvěrnost	Dostupnost	Integrita	Výsledek	Interpretace výsledku
1	Podklady od zákazníka pro zpracování nabídky	1	1	1	1	nízká
2	Poptávky subdodavatelům	2	1	2	2	střední
3	Nabídky subdodavatelů	2	1	2	2	střední
4	Kalkulace zakázky	3	2	2	3	vysoká
5	Nabídka na realizaci projektu	3	2	3	3	vysoká
6	Objednávka nebo smlouva se zákazníkem	2	1	2	2	střední
7	Projektová dokumentace pro realizaci projektu	2	1	2	2	střední
8	Objednávky subdodavatelům	2	1	2	2	střední
9	Řízení zakázky	2	1	2	2	střední
10	Předávací dokumentace pro zákazníka	2	1	2	2	střední
11	Fakturace	3	1	3	3	vysoká
12	Interní dokumenty	2	1	2	2	střední
13	Bezpečnostní dokumentace	3	1	2	3	vysoká

Z tabulky výše je patrné, že jako CITLIVÉ musí být nově v záhlaví a zápatí dokumentu označovány dokumenty týkající se následujících oblastí:

- Bezpečnostní dokumentace
- Fakturace
- Kalkulace zakázky
- Nabídka na realizaci projektu

Informace, které musí být označovány jako INTERNÍ, jsou informace týkající se celkového know-how společnosti, případně nastavení interních procesů. Tyto informace by mohly být zneužity a snížit tak Společnosti X možnost konkurenční výhody. Je tedy nutno do této skupiny zařadit:

- Interní dokumenty
- Projektovou dokumentaci pro realizaci projektu
- Objednávky subdodavatelům
- Řízení zakázky

- Předávací dokumentace pro zákazníka
- Objednávky nebo smlouvy se zákazníkem
- Poptávky subdodavatelům
- Nabídky subdodavatelů

Za veřejné lze obecně považovat dokumenty a informace získávané z veřejně přístupných zdrojů. V souvislosti s předmětem podnikání firmy se nejčastěji jedná o informace přímo od zákazníka, kterou jsou téměř vždy uveřejněny v zadávacím řízení a jedná se o podklady od zákazníka pro zpracování nabídky. Tyto informace je v rámci dokumentace a interních pravidel Společnosti X vhodné uchovávat s označením VEŘEJNÉ, případně lze tolerovat také možnost neoznačení informace, která je považována za veřejnou.

3.2.5. Politika řízení dodavatelů

Při uzavírání smlouvy s dodavatelem je s ohledem na jeho důležitost vhodné zvážit, které z následujících oblastí jsou relevantní, a ty následně zohlednit ve smlouvě:

a) ustanovení o bezpečnosti informací (z pohledu důvěrnosti, dostupnosti a integrity),

b) ustanovení o oprávnění užívat data,

c) ustanovení o autorství programového kódu, popřípadě o programových licencích,

d) ustanovení o kontrole a auditu dodavatele (pravidla zákaznického auditu),

e) ustanovení upravující řetězení dodavatelů, přičemž musí být zajištěno, že poddodavatelé se zaváží dodržovat v plném rozsahu ujednání mezi povinnou osobou a dodavatelem a nebudou v rozporu s požadavky povinné osoby na dodavatele,

f) ustanovení o povinnosti dodavatele dodržovat bezpečnostní politiky povinné osoby nebo ustanovení o odsouhlasení bezpečnostních politik dodavatele povinnou osobou,

g) ustanovení o řízení změn,

h) ustanovení o souladu smluv s obecně závaznými právními předpisy,

i) ustanovení o povinnosti dodavatele informovat povinnou osobu o:

- kybernetických bezpečnostních incidentech souvisejících s plněním smlouvy,
- způsobu řízení rizik na straně dodavatele a o zbytkových rizicích souvisejících s plněním smlouvy,

- významné změně ovládání tohoto dodavatele podle zákona o obchodních korporacích nebo změně vlastnictví zásadních aktiv, popřípadě změně oprávnění nakládat s těmito aktivy, využívaných tímto dodavatelem k plnění podle smlouvy se správcem,

j) specifikace podmínek z pohledu bezpečnosti při ukončení smlouvy (například přechodné období při ukončení spolupráce, kdy je třeba ještě udržovat službu před nasazením nového řešení, migrace dat a podobně),

k) specifikace podmínek pro řízení kontinuity činností v souvislosti s dodavateli (například zahrnutí dodavatelů do havarijních plánů, úkoly dodavatelů při aktivaci řízení kontinuity činností),

l) specifikace podmínek pro formát předání dat, provozních údajů a informací po vyžádání správcem,

m) pravidla pro likvidaci dat,

n) ustanovení o právu jednostranně odstoupit od smlouvy v případě významné změny kontroly nad dodavatelem nebo změny kontroly nad zásadními aktivy využívanými dodavatelem k plnění podle smlouvy,

o) ustanovení o sankcích za porušení povinností,

p) ustanovení o mlčenlivosti (např. v případě outsourcované pozici manažera kybernetické bezpečnosti či IT služeb)

V rámci řízení dodavatelských vztahů je nutno prokazatelně seznamovat konkrétní osoby dodavatele s bezpečnostními politikami a pravidly a následně kontrolovat jejich dodržování (14, s. 10,11).

3.2.6. Politika bezpečnosti lidských zdrojů

Politika bezpečnosti lidských zdrojů cílí na zvyšování povědomí v oblasti kybernetické bezpečnosti u všech zaměstnanců. Cílem rozšíření bezpečnostního povědomí u zaměstnanců je zavést pravidelné školení zaměřené na bezpečnostní minimum.

Školení zaměstnanců

Každý zaměstnanec je povinen jednou ročně splnit kurz „Dávej kyber“, který je dostupný na stránkách NÚKIB. Kurz „Dávej kyber“ poskytuje uživatelům základní informace týkající se kybernetické bezpečnosti a je plně dostačující.

V případě nově příchozího zaměstnance je nutno kromě provozních školení, která jsou mimo oblast kybernetické bezpečnosti úspěšně projít školením „Dávej kyber“.

Postup při nesplnění závěrečného testu školení

Po dokončení kurzu „Dávej kyber“ je při úspěšném dokončení vygenerován certifikát, který je zaměstnancem odeslán MKB, který dané certifikáty uchovává a v Excelu vede záznamy o jednotlivých zaměstnancích včetně data absolvování a úspěšnosti či neúspěšnosti.

V případě, že zaměstnanec daným kurzem neprojde, je nucen opakovat tento kurz. Opakování kurzu probíhá, dokud nedojde k jeho úspěšnému splnění a získání certifikátu.

Seznámení s bezpečnostními politikami

Další důležitou částí vzdělávání zaměstnanců je seznámení se s vydanými bezpečnostními politikami. Při vytvoření nové politiky je vzhledem k nízkému počtu zaměstnanců dostačující zaslat novou politiku e-mailem. Každý zaměstnanec povinen potvrdit, že se s danou politikou seznámil, a to pomocí odpovědi na tento e-mail. Vyhodnocení obeznámení všech zaměstnanců s novou politikou vyhodnocuje MKB a v případě nepotvrzení zašle danou politiku danému zaměstnanci znovu a urguje potvrzení o seznámení s politikou.

Porušení bezpečnostních politik

Při zjištění porušování stanovených bezpečnostních politik existují tři úrovně disciplinárních činností:

- **Ústní výtka nadřízeného v** případě porušení pravidel ustanovených bezpečnostními politikami, jejichž následkem byla nevýznamně snížena nebo ohrožena úroveň bezpečnosti informací.
- **Písemná výtka nadřízeného** v případě porušení pravidel ustanovených bezpečnostními politikami, jejichž následkem byla významně snížena nebo ohrožena úroveň bezpečnosti informací, nebo když se porušení pravidel opakuje.
- **Osobní projednání porušení povinností zaměstnance** v případě závažného porušení pravidel ustanovených bezpečnostními politikami, jejichž následkem byla velmi významně snížena nebo ohrožena úroveň bezpečnosti informací nebo soustavné méně závažné porušování pravidel bezpečnosti informací.

Všechny písemné výtky a výsledky osobního projednání porušení povinností zaměstnance musí být písemně či elektronicky zaznamenány a uloženy v osobním spisu zaměstnance.

Chování při podezření na nestandardní situaci

Každý zaměstnanec má povinnost hlásit podezření na nestandardní situace e-mailem osobě, která zastává pozici MKB. V případě, že dojde ke KBI, je po jeho prošetření MKB uspořádáno speciální školení, na kterém dojde k představení proběhlého útoku, jak se mu vyhnout, k jakému došlo nápravnému opatření. V závěru školení jsou zopakovány základní zásady kybernetické bezpečnosti.

3.2.7. Politika řízení změn

Řízení změn je podstatnou částí SŘBI, kterou je třeba projektově řídit a dokumentovat. V případě, že se společnost chystá provést změnu která bude mít dopad do kybernetické bezpečnosti, je třeba u takové změny zvážit dopady. Pokud bude objeven nepříznivý dopad změny, je třeba jej dokumentovat a nalézt možná rizika, která je třeba minimalizovat. Pokud rizika nelze minimalizovat, je třeba plánovanou změnu přehodnotit. Do diskuse o rozhodnutí je třeba vždy kromě vedení společnosti zapojit také MKB, v případě, že se jedná o změnu technického rázu, je vhodné zahrnout do rozhodování také IT technika.

Pro úspěšné řízení změn je vhodné projít třemi následujícími fázemi:

- **Fáze rozmrazení** – zde dochází k přesvědčení a nadchnutí zaměstnanců pro provedení dané změny, osvěta, propagace benefitů změny, management musí zajistit, že všichni zaměstnanci jsou se změnou seznámeni.
- **Fáze změny** – provedení samotné změny.
- **Fáze zamrazení** – aklimatizace, zvyknutí si na nové prostředí, začlenění změny do běžného pracovního života.

Po provedení změny, která má zásah do SŘBI, je třeba aktualizovat relevantní bezpečnostní politiky a dokumentaci.

V případě, že změna nebude provedena korektně, je třeba zajistit možnost vrácení do původního stavu bez ztráty dat.

Kromě řízení velkých změn je třeba popsat také proces řízení menších změn, které nemají vliv na práci zaměstnanců. V případě velkých i malých změn je třeba tento proces řádně dokumentovat a dokumentaci uchovat.

3.2.8. Politika řízení kontinuity činností

Pokud ve společnosti dojde ke KBU či KBI, je třeba zajistit, aby co nejméně ovlivnili celkový chod společnosti. Je třeba, aby všichni zaměstnanci věděli, co mají v takové situaci dělat a kdo se má účastnit nápravy krizové situace.

Zapojené osoby

Hlavní aktéry v řešení KBU nebo KBI jsou:

- MKB
- IT technik
- Vedení společnosti pouze v roli informované strany

Možné scénáře

- **Nedostupnost budovy**
    - Přesun na Home Office a práce pomocí vzdáleného připojení
    - Bez vlivu na dostupnost, integritu a důvěrnost
- **Nedostupnost file serveru**
    - Má zásadní vliv na dostupnost
    - Nelze poskytovat službu
- **Nedostupnost lidí** – epidemie, dlouhodobé onemocnění
    - Přesun do online prostředí pomocí vzdáleného připojení
    - V případě dlouhodobého onemocnění nábor nových zaměstnanců
- **Nedostupnost internetového připojení**
    - Využívání datových SIM karet a modemu do vyřešení problému

Minimální úroveň užívání, provozu a správy, která je akceptovatelná pro zachování poskytovaných služeb

Jelikož jsou veškerá data nutná k práci uložena na file serveru, nelze bez připojení k file serveru poskytovat službu. Bez připojení k internetu přes primární datovou linku je možno pracovat, jelikož společnost disponuje datovými SIM kartami a modemem. Lze tedy v tomto režimu po omezenou dobu pracovat. Tato situace však nedopadá na všechna oddělení společnosti stejně. Zatímco oddělení projekce může pokračovat v práci bez omezení, obchodní oddělení se s některými omezeními v souvislosti s konektivitou potýkat musí.

Doba obnovení chodu (RTO)

V případě výpadku file serveru nebo sítě LAN, který je zapříčiněn selháním HW vybavení (tedy file server Synology, router, switch) je třeba zakoupit nové zařízení. Není nutno tvořit v této oblasti podpůrných aktiv rezervy, jelikož jsou na trhu dostupné. Společnost X je tedy od počáteční chvíle selhání schopna do 24 hodin obnovit provoz.

Bod obnovení dat (RPO)

- **Obnova ze zálohy v kancelářských prostorech**

RPO pro obnovu ze zálohy disků, které jsou uloženy v kancelářských prostorech, je definován následující postup pro zjištění výsledné hodnoty. Záloha aktuálně obsahuje 3TB dat a rychlost přenosu vnitřní sítě je 650 Mb/s. Pro výpočet RPO byl použit následující postup:

$$vnitřní\ síť\ =\ 650\ Mb/s\ =\ 650/8\ =\ 81{,}25\ MB/s$$

Vzorec č. 3: Výpočet rychlosti přenosu po vnitřní síti
(Zdroj: Vlastní zpracování)

$$data\ =\ 3\ TB \rightarrow 3\ 000\ 000\ B\ /\ 81{,}25\ =\ 37\ 000\ s\ /\ 3600\ =\ 10{,}3\ hodin$$

Vzorec č. 4: Výpočet doby obnovy po vnitřní síti
(Zdroj: Vlastní zpracování)

Doba obnovy dat je tedy odhadována na 10,3 hodin. Mimo přenos dat je ale třeba provést analýzu situace, zjištění problému a přípravu na přenos dat. Celkem je tedy RPO určeno na 16 hodin.

- **Obnova ze zálohy v sídle společnosti**

RPO pro obnovu ze zálohy, která je umístěna v sídle společnosti, je postup pro její určení následující:

$$připojení\ k\ internetu\ =\ 20\ Mb/s\ =\ 20/8\ =\ 2{,}5\ MB/s$$

Vzorec č. 5: Výpočet rychlosti přenosu po internetu
(Zdroj: Vlastní zpracování)

$$data\ =\ 3\ TB \rightarrow 3\ 000\ 000\ B\ /\ 2{,}5\ =\ 1\ 200\ 000\ s\ /\ 3600\ =\ 333\ hodin$$

Vzorec č. 6: Výpočet doby obnovy po internetu
(Zdroj: Vlastní zpracování)

RPO pro obnovu dat ze zálohy umístěné v sídle společnosti je 333 hodin. Mimo přenos dat je ale třeba provést analýzu situace, zjištění problému a přípravu na přenos dat. Celkem je tedy RPO určeno na 340 hodin.

3.2.9. Politika provádění auditu kybernetické bezpečnosti

Pro zajištění neustálého zlepšování úrovně SŘBI je nutno provádět kontrolu stavu dosud zavedených opatření a případně také identifikovat nová rizika. Pro tyto účely musí pravidelně každý rok probíhat interní audit kybernetické bezpečnosti. Pro potřeby Společnosti X a z důvodu její velikosti je dostačující, aby audit kybernetické bezpečnosti probíhal v periodě dvou let a v rozsahu požadavků celého MBS, tedy musí obsáhnout jak manažerskou část, tak i technickou část. Pro potřeby interního auditu kybernetické bezpečnosti je doporučeno využívat checklist, který je přílohou této práce (Příloha A). Dále je nutno provádět audit při změnách, které mohou mít negativní dopad na kybernetickou bezpečnost, a při KBI se závažným dopadem na celou společnost.

Osoba, která je za provedení interního auditu odpovědná je osobou, která má na starost řízení kybernetické bezpečnosti ve Společnosti X, jedná se tedy o MKB.

Auditní zjištění a výsledky celého auditu jsou poté předkládány a prezentovány vedení MKB, který popíše nalezené neshody a představí výsledky provedeného auditu. Výsledky auditu jsou poté promítnuty do plánu zavádění bezpečnostních opatření a dle nich jsou aktualizovány bezpečnostní dokumentace.

3.2.10. Politika řízení přístupu

Cílem politiky řízení přístupu je stanovení přístupových práv jednotlivých uživatelů a jejich zařazení do uživatelských rolí.

Principy řízení přístupů

Pro řízení přístupů je využíván princip minimálních oprávnění, který je postaven na principu nulových počátečních práv. Všechna práva jsou přidělována postupně dle nutnosti přístupu k daným službám. Každý zaměstnanec má tedy ve výsledku pouze taková práva, která jsou nezbytně nutná pro náplň jeho práce. Vedení organizace využívá běžné uživatelské účty a nemá přístup k privilegovaným účtům. Přístupová práva je nutno pravidelně kontrolovat a to při příležitosti interního auditu. Osoba odpovědná za řízení přístupů je v tomto případě zaměstnanec zajišťující IT služby, který přiděluje, ruší a eviduje přístupová práva v dokumentované podobě z důvodu následného přezkumu. Každý uživatel musí mít v rámci přístupu přidělen jedinečný identifikátor.

Privilegované účty

Přístup k privilegovaným účtům má zaměstnanec spravující síťové prvky (IT pracovník). Ve formě privilegovaného účtu funguje také zaměstnanec ekonomického oddělení, který má nejvyšší práva v systému POHODA.

Heslová politika u privilegovaných účtů je následující:

- Minimální délka hesla je 17 znaků.
- Heslo musí obsahovat velká a malá písmena, číslice a také speciální znak.
- Maximální doba platnosti hesla je 18 měsíců.
- Je zakázáno používat stejné heslo v rozsahu posledních 12 hesel.
- Minimální platnost hesla pro opětovnou změnu je 1 den.
- Po 5 neplatných pokusech v zadání hesla v řadě dojde k uzamčení účtu.
- Jednorázové heslo pro prvotní přihlášení musí být ihned po přihlášení změněno a je do 24 hodin zneplatněno.

Uživatelské účty

Každý nový zaměstnanec je automaticky zařazen do skupiny běžných uživatelů, která jako výchozí stav nepřidělí danému uživateli žádná práva.

Uživatelské účty podléhají minimálně následujícím pravidlům:

- Minimální délka hesla je 10 znaků.
- Je zakázáno používat stejné heslo v rozsahu posledních 12 hesel.
- Maximální doba platnosti hesla je 18 měsíců.
- Po 10 neplatných pokusech v zadání hesla v řadě dojde k uzamčení účtu.
- Jednorázové heslo pro prvotní přihlášení musí být ihned po přihlášení změněno a je do 24 hodin zneplatněno.

Ukončení pracovního poměru

V případě ukončení pracovního poměru, jsou zaměstnanci ihned zrušena jeho přístupová práva a jsou mu odebrány firemní technologie. Tímto postupem dojde k zamezení jeho přístupu do firemní sítě z domova a také k předejití možné kompromitace Společnosti X.

Přístup k používanému SW a HW

Zaměstnanec je připojen svým počítačem k síti pomocí dokovací stanice v kanceláři přes síťový kabel. V případě, že zaměstnanec pracuje mimo kancelářské prostory, je nucen používat VPN.

Přidělování a odebírání rolí

Registrace všech uživatelů je zajišťována centrálně a jsou stanoveny pravidla pro procesy:

- Registrace nového zaměstnance – princip nulového oprávnění
- Přidělování a odebírání přístupů – při změně pozice a při odchodu ze zaměstnání je uživatelský účet a veškeré přístupy odebrány
- Deaktivace identit – v případě odchodu zaměstnance na mateřskou dovolenou případně v případě dlouhodobého onemocnění je žádoucí omezení přístupu v podobě dočasné deaktivace účtu
- Monitorování činnosti uživatelů – monitoring uživatelů je prováděn pomocí log managementu

Všechny výše zmíněné úkony má na starosti zaměstnanec zabezpečující IT.

3.2.11. Politika fyzické bezpečnosti

Pravidla pro návštěvy

Možnost návštěv je v prostorách společnosti povolena a v mnoha případech je žádoucí. I přes to, že společnost nepracuje s utajovanými informacemi a primárně se jedná o citlivé informace týkající se ceny poskytovaných služeb, je nutné mít přehled o osobách, které se v kancelářských prostorech pohybují. Konkurenční boj a vynesení těchto informací by mohlo znamenat znevýhodnění pozice na trhu.

Pro zajištění důvěrnosti informací, tedy nutno vést přehled návštěv. Vzhledem k velikosti společnosti je nutno návštěvy uvádět do sdíleného kalendáře, aby tuto informaci měl k dispozici každý zaměstnanec s předstihem.

Za návštěvu je vždy zodpovědný zaměstnanec, který ji do kancelářských prostor pozval. Tato osoba tedy návštěvu vyzvedne před budovou a po konci jejich jednání ji vyprovodí z budovy.

Pravidla pro zabezpečení prostor

Každý zaměstnanec má klíč od kancelářských prostor, klíč od objektu a také kód k elektronickému zabezpečovacímu systému Jablotron. Zaměstnanec je tedy povinen v případě, že jako poslední opouští kancelář, její prostory uzamknout. V případě, že zaměstnanec jako poslední opouští celý objekt, je třeba zakódovat a uzamknout kromě kancelářských prostor i celý objekt.

Mimo zabezpečení kanceláře a celého objektu je třeba zabezpečit také rozvaděč, kde jsou všechny síťové prvky. Rozvaděč musí vždy být uzamčen.

Rozvaděč

Je nutno, aby byl rozvaděč vybaven chlazením a nedošlo k ohrožení jeho funkčnosti z důvodu přehřátí. Dále musí být rozvaděč vybaven záložním napájením (UPS).

3.2.12. Ochrana před škodlivým kódem

V rámci ochrany před škodlivým kódem je implementován SW pro detekci a odstranění škodlivých programů. Tento SW zajišťuje pravidelnou kontrolu každý den v pevně stanovenou hodinu mimo nejvytíženější hodiny (doporučeno v nočních hodinách).

Nejméně jednou denně probíhá pravidelná aktualizace software pro detekci a odstranění škodlivých kódů včetně databáze vzorků.

Je zakázáno instalovat, kopírovat, užívat nebo testovat jakékoliv programové vybavení, které není schválenou součástí pracovní náplně. V tomto ohledu je dobré sledovat úřední desku NÚKIB, kde jsou zveřejňována opatření, varování a doporučení a tato skutečnosti v provozu zohlednit. Dále je zakázáno vzdálené spouštění kódu ze zdroje mimo prostředí společnosti.

3.2.13. Kybernetické události a incidenty

Postup pro zaměstnance

V případě podezření na nestandardní situaci jsou zaměstnanci povinni tuto skutečnost hlásit MKB e-mailem, aby byl o tomto hlášení evidován důkaz a dalo se s touto informací pracovat i zpětně v rámci forenzní analýzy.

Za nestandardní situaci jsou považovány následující podezření:

- Nedostupnost služby
- Nevyžádaný e-mail
- Neobvyklé chování služby

Reakce na kybernetický bezpečnostní incident nebo událost a eskalační proces

V případě, že MKB obdrží informaci s podezřením na nestandardní chování, je povinen tuto skutečnost prověřit za spolupráce s IT pracovníkem. V případě, že se dané podezření nepotvrdí, je nutno zaměstnance informovat o výsledku. Pokud se podezření potvrdí, je třeba informovat vedení společnosti a začít jednat o nápravě. Je také nutno informovat zaměstnance o této hrozbě a jejím možném opakování. V tuto chvíli na nápravě pracuje IT a MKB je k dispozici a účastní se dané nápravy. IT se tedy převážně zabývá technickou nápravou a MKB je zodpovědný za komunikaci se zaměstnanci a vedením.

Po vyřešení nestandardní události se sejde MKB s vedením (dále jen „Výbor kybernetické bezpečnosti“) a prezentuje vzniklé škody, které daná situace způsobila, popisuje způsob řešení a navrhuje bezpečnostní opatření pro zamezení opakování dané situace. MKB i vedení společnosti má možnost přizvat na setkání Výboru kybernetické bezpečnosti i další relevantní osoby.

Auditní požadavky

Z důvodu forenzní analýzy nestandardní situace je nutno zachovat informace o dané situaci, je tedy třeba uchovávat provozní záznamy z doby jejího výskytu (logy) nejméně po dobu 30 dní. Logy by měly obsahovat minimálně datum a čas události (uvedený s jednoznačnou identifikací časové zóny, např. UTC nebo lokální čas s uvedením offsetu), síťové identifikátory komunikujících bodů (tj. např. IP adresy a porty, v případě použití proxy nebo NATu musí být síťový identifikátor předán jinou formou nebo musí být možné tyto logy korelovat), identifikátor uživatele, pod kterým byla činnost provedena, typ události a úspěšnost nebo neúspěšnost činnosti.

Dále je třeba monitorovat a uchovávat následující typy událostí:

- přihlášení a odhlášení uživatelů a administrátorů, a to včetně neúspěšných pokusů,
- činnosti provedené administrátory, o použití privilegovaných účtů, např. účtu supervisora, administrátora,
- spuštění a ukončení informačního nebo komunikačního systému,
- změny konfigurací,
- úspěšné i neúspěšné činnosti vedoucí ke změně přístupových oprávnění,
- zahájení a ukončení činností zařízení a aplikací,
- automatická varovná nebo chybová hlášení zařízení a aplikací,
- přístupy k záznamům o činnostech, pokusy o manipulaci se záznamy o činnostech a změny nastavení nástroje pro zaznamenávání činností a
- použití mechanismů identifikace a autentizace včetně změny údajů, které slouží k přihlášení.

Je třeba, aby byl přístup k těmto záznamům chráněn pomocí omezení přístupu a došlo tak k zabránění zneužití, ohrožení či smazání těchto dat.

3.3. Technická část

V technické části práce budou představena řešení problémů, které byly vyjmenovány v kapitole 3.1. v matici neshod. Každá neshoda bude vztažena i ke konkrétnímu podpůrnému aktivu a bude navrženo optimální nápravné opatření. V následujících podkapitolách bude popsáno řešení identifikovaných neshod jednotlivých oblastí, kterými se technická část MBS zabývá, případně bude objasněno, proč řešení není doporučeno implementovat. V matici neshod byly identifikovány neshody, které není možno vyřešit ať už z důvodu irelevantnosti zavedení dané technologie anebo příliš vysoké finanční náročnosti daného řešení.

3.3.1. Fyzická bezpečnost

Neshodou identifikovanou v oblasti fyzické bezpečnosti byl požadavek zajištění bezpečnosti kabelových rozvodů. Tento požadavek není možné splnit, jelikož Společnost X není majitelem objektu a tento požadavek je v rozporu s nájemní smlouvou. Kabelové rozvody byly totiž instalovány při stavbě objektu. Tento nedostatek je tedy označen za přijatelný a v dalších auditech na něj nemusí být brán ohled.

Bezpečnost kabelových rozvodů není v gesci Společnosti X a nebylo možné provést detailní průzkum této oblasti. Na pohled však bylo zřejmé, že kabelové rozvody jsou řešeny korektně a v případě, že je kabeláž viditelná, je seskupena do svazků a mimo dosah návštěvníků a zaměstnanců.

Tabulka č. 19: Neshody a nápravná opatření v oblasti fyzické bezpečnosti
(Zdroj: Vlastní zpracování dle: 14, s. 18)

ID	Požadavek	Stav zavedení	Nápravné opatření	FN	ČN	NI	K	R	Typ
Fyzická bezpečnost									
7	Zajištěna bezpečnost kabelových rozvodů.	NE	Není možné zajistit, vychází z pravidel nájemní smlouvy.	x	x	x	x	x	TECH

3.3.2. Řízení přístupů

Ačkoliv má společnost vytvořená pravidla pro politiku hesel, nic jako formalizovaný dokument s přesnými pravidly pro tvorbu hesel neexistuje. Tento nedostatek je napraven metodicky vytvořením Politiky řízení přístupů v kapitole 3.2.10.

Náprava po technické stránce spočívá ve změně heslové politiky i ve správci hesel v nastavení LDAP. Pravidla pro tuto změnu budou vycházet z MBS, což je promítnuto i v nově vytvořené politice hesel a oba zdroje jsou ve vzájemném souladu. Je tedy třeba heslovou politiku pro privilegované a běžné účty nastavit v souladu s Politikou řízení přístupu.

Na základě náročnosti implementace nápravného opatření a kritičnosti dané neshody bylo dle matice neshod doporučeno **zavést** navržené nápravné opatření **okamžitě**.

Tabulka č. 20: Neshody a nápravná opatření v oblasti řízení přístupů
(Zdroj: Vlastní zpracování dle: 14, s. 19)

ID	Požadavek	Stav zavedení	Nápravné opatření	FN	ČN	NI	K	R	Typ
Řízení přístupů									
22	Existuje politika hesel pro privilegované účty v minimální míře:		Sepsat politiku a přenastavit současné nastavení LDAP.	3	2	6	3	18	ORG, TECH
22.1	• minimální délka hesla je 17 znaků	NE							
22.3	• maximální doba platnosti hesla je 18 měsíců	NE							
22.4	• zákaz používaní stejného hesla (posledních 12 hesel)	NE							
22.5	• minimální platnost hesla 1 den	NE							
23	Existuje politika hesel pro uživatelské účty v minimální míře:		Sepsat politiku a přenastavit současné nastavení LDAP.	3	2	6	3	18	ORG, TECH
23.1	• minimální délka hesla je 10 znaků	NE							
23.4	• zákaz používaní stejného hesla (posledních 12 hesel)	NE							
23.3	• maximální doba platnosti hesla je 18 měsíců	NE							

3.3.3. Požadavky v oblasti ochrany před škodlivým kódem

V oblasti ochrany před škodlivým kódem byly identifikovány dvě neshody s požadavky MBS. První neshodou je, že nedochází k segmentaci síťového prostředí. Vzhledem k tomu, že i MBS doporučuje oddělit sítě pro provoz a pro správu pouze v případech, kdy je tento krok opodstatněný, je akceptovatelné přijmout stávající řešení Společnosti X. Z podstaty velikosti společnosti je segmentace neopodstatněná a nepřinášela by kýžené výsledky. Druhým nedostatkem je zjištění, že neprobíhá pravidelná aktualizace SW pro detekci a odstranění škodlivých kódů včetně databáze vzorků nejméně jednou denně. Tento postup je třeba dodržovat a nastavit pravidelnou aktualizaci antivirového programu na file serveru Antivirus Essential od Synology a zde dále nastavit aktualizaci databáze vzorků alespoň jednou denně.

Na základě náročnosti implementace nápravného opatření a kritičnosti dané neshody bylo dle matice neshod doporučeno **zavést** navržené nápravné opatření **okamžitě**.

Tabulka č. 21: Neshody a nápravná opatření v oblasti požadavků na ochranu před škodlivým kódem
(Zdroj: Vlastní zpracování dle: 14, s. 22)

ID	Požadavek	Stav zavedení	Nápravné opatření	FN	ČN	NI	K	R	Typ
Požadavky v oblasti ochrany před škodlivým kódem									
26	V rámci IS nebo KS jsou zavedeny minimálně následující opatření:			x	x	x	x	x	
26.2	• segmentace síťového prostředí (oddělení sítí pro provoz a pro správu), kde je to opodstatněné	NE	Segmentace síťového prostředí Společnosti X nemá smysl, vychází z velikosti firmy.	x	x	x	x	x	TECH
26.3	• pravidelná aktualizace SW pro detekci a odstranění škodlivých kódů včetně databáze vzorků nejméně jednou denně	NE	Přenastavit na pravidelnou aktualizaci.	3	2	6	3	18	

3.3.4. Kybernetické bezpečnostní události a incidenty

Identifikovaná neshoda v oblasti KBU a KBI spočívá v přípravě na integraci do SIEM tak, aby byly splněny požadavky na bezpečnostní monitoring. Vzhledem k tomu, že bezpečnostní monitoring probíhá v rámci aplikace log managementu, bylo vyhodnoceno, že nákup samotného zařízení SIEM a jeho následná implementace nepřinese Společnosti X takový přínos, který by mohl pokrýt výši dané investice.

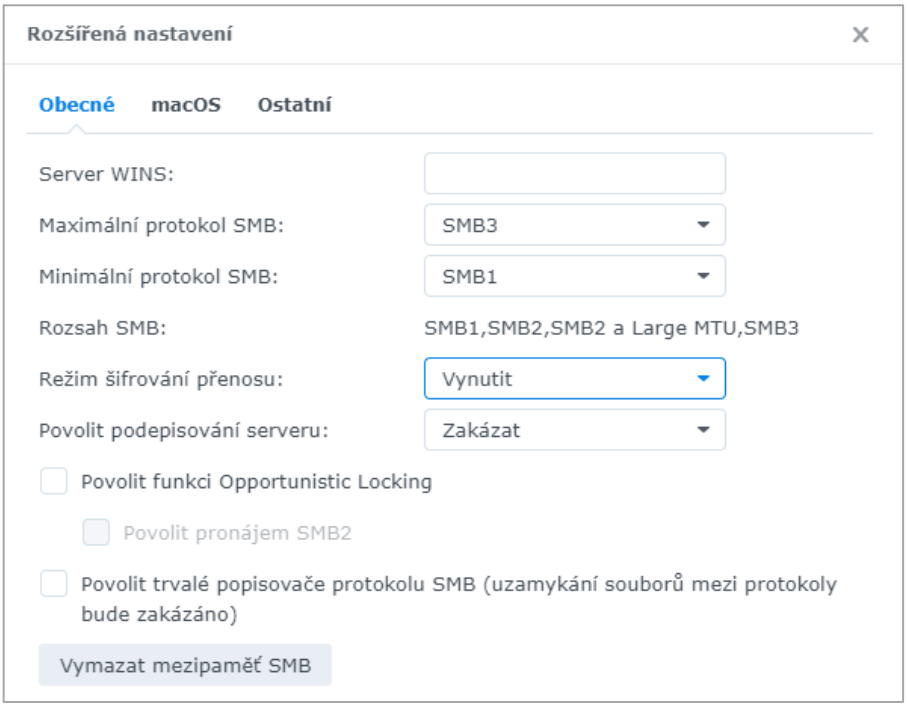
Tabulka č. 22: Neshody a nápravná opatření v oblasti kybernetických bezpečnostních událostí a incidentů
(Zdroj: Vlastní zpracování dle: 14, s. 23 – 27)

ID	Požadavek	Stav zavedení	Nápravné opatření	FN	ČN	NI	K	R	Typ
Kybernetické bezpečnostní události a incidenty									
38	IS nebo KS, včetně infrastruktury (je jeho podpůrnou součástí a jeho další komponenty musí být připraveny na integraci do SIEM obdobným způsobem tak, aby naplňovaly požadavky na bezpečnostní monitoring.	NE	Bezpečnostní monitoring je nahrazen sledováním a aktivním prováděním log managementu. Zakoupení a následná implementace SIEM je pro společnost v poměru přínos x cena nevýhodnou investicí, která je příliš nákladná.	x	x	x	x	x	TECH

3.3.5. Kryptografické prostředky

V tuto chvíli není vynuceno šifrování přenosu dat, tato neshoda s doporučením MBS jde snadno vyřešit úpravou v nastavení a šifrování přenosu lze vynutit v nastavení SMB na file serveru. Jedná o změnu, která může z bezpečnostního hlediska mít velký přínos a která není časově ani finančně náročná.

Na základě náročnosti implementace nápravného opatření a kritičnosti dané neshody bylo dle matice neshod tedy doporučeno **zavést** navržené nápravné opatření **okamžitě**.



Obrázek č. 12: Vynucené šifrování přenosu – změna nastavení
(Zdroj: Vlastní zpracování)

Tabulka č. 23: Neshody a nápravná opatření v oblasti kryptografických prostředků
(Zdroj: Vlastní zpracování dle: 14, s. 28–30)

ID	Požadavek	Stav zavedení	Nápravné opatření	FN	ČN	NI	K	R	Typ
Kryptografické prostředky									
52	Zajistit šifrování přenosu dat. Šifrování uložených dat je pouze doporučeno, a to v návaznosti na typ a charakter dat a v návaznosti na možné technologické řešení.	NE	Vynutit šifrování přenosu	2	3	6	2	12	TECH

3.3.6. Požadavky v oblasti zajišťování úrovně dostupnosti informací

Zálohy dat jsou aplikovány pouze pro file systém a pro soubory používány k práci. V současnosti nejsou zálohována data aplikací. Obecně je pro zálohovací média využíváno pravidlo 3–2–1. Stěžejním problémem, který pro společnost znamenal velké navýšení pracovního vytížení zaměstnanců, a tedy i nutnost upozadění běžné náplně jejich práce, byl ransomwarový útok na POHODU, ve které bude aplikována zásadní změna v oblasti zálohování.

Přímo na stránkách poskytovatele POHODY jsou zveřejněna doporučení pro zálohování. Je tedy vhodné tato doporučení následovat a zajistit zálohu celkové účetní jednotky programu, systémové databáze včetně nastavení HW a přístupových práv a globální databáze.

Pro usnadnění práce, docílení automatizace procesu zálohování a zamezení chyb je doporučeno využít automatické zálohování. Možnost automatického zálohování je dostupná pro uživatele programů POHODA SQL nebo POHODA E1, kde je v rámci agendy Automatických úloh dostupná možnost plánování automatických záloh. Modul poskytuje výběr položek, které mají být zálohovány, dále je možnost výběru a plánování spouštění automatického zálohování, a nakonec je možné určit frekvenci spouštění zálohy. Je tedy doporučeno využít jednu ze zmíněných licencí. (29)

Na základě náročnosti implementace nápravného opatření a kritičnosti dané neshody bylo dle matice neshod doporučeno **zavést** navržené nápravné opatření **okamžitě**.

Tabulka č. 24: Neshody a nápravná opatření v oblasti zajišťování úrovně dostupnosti informací
(Zdroj: Vlastní zpracování dle: 14, s. 30, 31)

ID	Požadavek	Stav zavedení	Nápravné opatření	FN	ČN	NI	K	R	Typ
Požadavky v oblasti zajišťování úrovně dostupnosti informací									
62	Z hlediska potřebných zálohovacích médií je vhodné uvažovat o uplatnění pravidla 3–2–1. Toto pravidlo znamená, že jsou k dispozici tři kopie dat na dvou různých typech médií, přičemž jedno z nich by se mělo nacházet mimo lokalitu umístění IS nebo KS („offsite“).	NE	Zálohovat i data aplikací – využít nákup nové licence	2	3	6	3	18	TECH

3.3.7. Požadavky v ochrany IS nebo KS typu webové aplikace

Jak již bylo zmíněno v Analytické části, společnost má k dispozici webovou aplikaci ve formě balíčku služeb Microsoft 365. Žádný ze zaměstnanců však webovou aplikaci nevyužívá, a je tedy doporučeno tuto možnost zakázat a deaktivovat, a k práci umožnit pouze využívání desktopové verze aplikace.

Na základě náročnosti implementace nápravného opatření a kritičnosti dané neshody bylo dle matice neshod doporučeno **zavést** navržené nápravné opatření **okamžitě**.

Tabulka č. 25: Neshody a nápravná opatření v oblasti ochrany IS nebo KS typu webové aplikace (Zdroj: Vlastní zpracování dle: 14, s. 34)

ID	Požadavek	Stav zavedení	Nápravné opatření	FN	ČN	NI	K	R	Typ
Požadavky v oblasti zajišťování úrovně dostupnosti informací									
69	Řídit se doporučeními OWASP a věnovat pozornost zranitelnostem.	NE	Jelikož webovou aplikaci nikdo ze zaměstnanců nepoužívá, bude možnost webové aplikace zakázána a zaměstnanci budou i nadále využívat pouze desktopovou verzi.	3	3	9	2	18	ORG, TECH

EKONOMICKÉ A ZÁVĚREČNÉ ZHODNOCENÍ

V závěru této práce je provedeno finální ekonomické zhodnocení. Druhou částí závěru je také shrnutí přínosů práce a zhodnocení dosažení stanovených cílů.

Ekonomické zhodnocení

Pro relevantní a smysluplné ekonomické zhodnocení bylo třeba vyčíslit náklady, které přímo zapříčinil samotný ransomwarový útok. Jelikož se jednalo o neplánované a jednorázové náklady, měly pro Společnost X velký dopad. Dále byly vyčísleny náklady na navržená nápravná opatření, která nezahrnovala práci na tvorbě této diplomové práci, jelikož se jednalo o spolupráci, která byla pro obě strany přínosná.

Vyčíslení nákladů ransomwarového útoku

Náklady ransomwarového útoky spočívaly v zásahu odborného IT technika, který ve spolupráci s IT technikem Společnosti X řešil tento incident. Jeho práce byla vyčíslena na 800 Kč / hod a jeho služeb bylo třeba využívat dva pracovní dny. Náklady na vlastního IT technika nejsou do kalkulace započteny, jelikož se jedná o standardní náklady, které společnost každý měsíc musí uhradit.

Mimo nákladů na služby IT technika bylo nutno vyčíslit také počet hodin přesčasů dvou zaměstnanců, kteří byli odpovědni za obnovu dat a vedení účetnictví v offline režimu. Náklady na hodinu přesčasu pro daného zaměstnance jsou vyčísleny na 280 Kč a jak již bylo zmíněno dříve v této práci, bylo nutno využívat přesčasů po dobu tří týdnů a dvou hodin každý pracovní den.

Tabulka č. 26: Vyčíslení nákladů ransomwarového útoku
(Zdroj: Vlastní zpracování)

Název položky	Jednotková cena	Počet hodin	Celková cena
IT technik	800 Kč	2 * 8 = 16	12 800 Kč
Přesčasy zaměstnanců	280 Kč	2 * 2 * 5 * 3 = 60	16 800 Kč
Celkem			**29 600 Kč**

Celkem tedy náklady spojené s ransomwarovým útokem pro společnost znamenaly ztrátu 29 600 Kč. Tento údaj je však zavádějící, protože ransomwarový útok nezpůsobil pouze finanční škodu, ale také riziko úniku zašifrovaných dat a jejich zprostředkování konkurenci.

Vyčíslení nákladů na nápravná opatření

Náklady, které musí Společnost X vynaložit na zavedení nápravných opatření, jsou složeny hlavně z obsazení pozice MKB a z přechodu ze služby POHODA Jazz NET 3 na POHODA Jazz NET3 SQL. Navržená opatření v technické oblasti znamenaly pouze změny na stávajících technologiích, a tedy neznamenaly žádnou finanční investici.

Náklady na MKB jsou vyčísleny hodinovou sazbou a vzhledem k tomu, že zatím neproběhlo výběrové řízení na obsazení této pozice, je hodinová sazba odhadnuta na 650 Kč. MKB bude fyzicky přítomen ve Společnosti X odhadem jednou měsíčně a náklady na tuto pozici byly vyčísleny na rok.

Tabulka č. 27: Náklady na MKB
(Zdroj: Vlastní zpracování)

Název položky	Jednotková cena	Počet hodin	Celková cena
Obsazení pozice MKB	650 Kč	8 * 12 = 96	62 400 Kč

Dále bylo třeba identifikovat nové náklady na přechod na jinou službu od společnosti POHODA. Je nutno uhradit pořizovací cenu nové služby POHODA Jazz NET3 SQL. Tato služba je dostupná v síťové verzi pro dva až tři počítače. Náklad na pořízení je pouze jednorázový a poté bude nutno platit servisní poplatek ve výši 4 720 Kč. Oproti stávající verzi se jedná o navýšení servisního poplatku o 2 520 Kč.

Tabulka č. 28: Náklady na změnu POHODY
(Zdroj: Vlastní zpracování)

Název položky	Pořízení	Servis 1x ročně
Služba POHODA Jazz SQL NET3	14 980 Kč	4 720 Kč

Náklady na první rok provozu jsou vyčísleny na 77 380 Kč, jelikož služba POHODA při pořízení neúčtuje zákazníkovi servisní poplatek. Náklady na další rok provozu v tomto režimu jsou již sníženy o cenu pořízení a vyčísleny jsou na 67 120 Kč. Pro možnost vyhodnocení této investice pro jednatele společnosti byly vyčísleny náklady počáteční investice a poté náklady na další rok.

Tabulka č. 29: Náklady na nápravná opatření – počáteční investice a investice dalších let
(Zdroj: Vlastní zpracování)

Název položky	Počáteční investice	Další rok
Služba POHODA Jazz SQL NET3	14 980 Kč	4 720 Kč
Obsazení pozice MKB	62 400 Kč	62 400 Kč
Celkem	**77 380 Kč**	**67 120 Kč**

Je samozřejmé, že investice do zajištění vyššího stupně bezpečnosti je vyšší, než výše přímé finanční škody, kterou ransomwarový útok způsobil. Jednoduchým výpočtem však lze zjistit, že pokud by k došlo k dalšímu útoku ve stejném rozsahu a navržená bezpečnostní opatření by nebyla implementována, již při druhém útoku by Společnost X dosáhla minimální škody 59 200 Kč, což je částka téměř srovnatelná s ročními náklady na zajištění vyššího stupně bezpečnosti. Výrazným rozdílem těchto dvou situací však je to, že částka, kterou ransomwarový útok způsobil je pouze ztráta, kdežto částka vložená do opatření, které zvyšují úroveň bezpečnosti, je investicí.

Závěrečné shrnutí dosažených cílů a přínosů

Cílem diplomové práce bylo komplexně pokrýt proces analýzy současného stavu a nasazení bezpečnosti dle doporučení MBS. Stanovený cíl byl splněn a zavedení bezpečnosti dle doporučení MBS může být ve společnosti X provedeno. Nad rámec vytyčeného cíle byl také vytvořen auditní checklist, dle kterého může Společnost X postupovat při provádění pravidelných přezkumů SŘBI.

Hlavním přínosem této práce bylo tedy nasazení základní úrovně kybernetické bezpečnosti Společnosti X, tak aby splňovala doporučení MBS v maximální možné míře. Není však možné převzít doporučení MBS doslovně, aniž by byly zohledněny specifika společnosti, kdy některá z navrhovaných opatření není vhodné zavádět s ohledem na velikost společnosti a finanční náročnost takových řešení.

Díky Analytické části práce bylo možné identifikovat nedostatky, které společnost v technické oblasti má. Dále bylo nutno zhodnotit, které z problematických oblastí lze nasazením bezpečnostních opatření vyřešit. Tento výběr byl proveden na základě kritického posouzení daných oblastí, kde se přihlíželo na poměr zvýšení kybernetické bezpečnosti organizace a na finanční zátěž nasazených opatření.

Kromě kompletního zavedení organizačních opatření, které MBS požaduje, v podobě tvorby bezpečnostní dokumentace, metodiky a politik došlo také k navržení řešení vybraných bezpečnostních opatření technického rázu. Mezi stěžejní oblasti se řadí:

- Úprava heslové politiky
- Zálohování dat aplikace POHODA
- Vynucení šifrování dat

Navázáním spolupráce se společností X, která spočívala ve sdílení dat směrem ze společnosti ke mně, jako tvůrci práce, a v navržení postupu pro zavedení doporučení MBS, docílila společnost výrazné finanční úspory v oblasti zajištění bezpečnostního specialisty, jehož služeb by v opačném případě musela využít k nasazení dané úrovně bezpečnosti.

Dále věřím, že tato práce může sloužit jako vodítko pro malé a střední společnosti v případě implementace obdobné úrovně kybernetické bezpečnosti na základě doporučení MBS.

SEZNAM POUŽITÝCH ZDROJŮ

(1) SEDLÁK, Petr. Management kybernetické bezpečnosti – Kybernetická bezpečnost obecně: Materiály ze cvičení. Brno 2023.

(2) Zákon č.181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) – znění od 6. 8. 2022. In: Zákony pro lidi.cz [online]. © AION CS 2010–2023 [cit. 30. 4. 2023]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181

(3) SEDLÁK, Petr. Management informační bezpečnosti: Materiály ze cvičení. Brno 2023.

(4) 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. In: Zákony pro lidi.cz [online]. © AION CS 2010–2023 [cit. 30. 4. 2023]. Dostupné z: https://www.zakonyprolidi.cz/cs/2018-82

(5) SEDLÁK, Petr. Management oborových řešení: Materiály z přednášek. Brno 2023.

(6) What is Knowledge Management? TechTarget [online]. © 2021 [cit. 30.04.2023]. Dostupné z: https://www.techtarget.com/searchcontentmanagement/definition/knowledge-management-KM

(7) SEDLÁK, Petr. Management kybernetické bezpečnosti – Business Continuity Management: Materiály ze cvičení. Brno 2023.

(8) Ransomware | NIST. National Institute of Standards and Technology [online]. © 2023 [cit. 30.04.2023]. Dostupné z: https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/ransomware

(9) Phishing | NIST. National Institute of Standards and Technology [online]. © 2023 [cit. 30.04.2023]. Dostupné z: https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/phishing

(10) 1. Obecné informace o směrnici NIS2 a budoucí národní úpravě. Nová směrnice EU o bezpečnosti sítí a informací. Praha: Národní úřad pro kybernetickou a informační bezpečnost, 2023. © 2023 [cit. 30.04.2023]. Dostupné také z: https:// osveta.nukib.cz/course/view.php?id=145

(11) Národní úřad pro kybernetickou a informační bezpečnost – Legislativa. Národní úřad pro kybernetickou a informační bezpečnost – Úvodní stránka [online]. © 2023 [cit. 29.04.2023]. Dostupné z: https://nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/

(12) ČSN EN ISO/IEC 27000. Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník. Druhé vydání. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, červen 2020.

(13) Národní úřad pro kybernetickou a informační bezpečnost – O NÚKIB. Národní úřad pro kybernetickou a informační bezpečnost – Úvodní stránka [online]. © 2023 [cit. 29.04.2023]. Dostupné z: https://nukib.cz/cs/o-nukib/

(14) Národní úřad pro kybernetickou a informační bezpečnost, Národní agentura pro komunikační a informační technologie, Ministerstvo vnitra. Minimální bezpečnostní standard [online]. © 2023 [cit. 28.04.2023]. Dostupné z: https://nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/

(15) ONDRÁK Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: CERM, Akademické nakladatelství, 2013. ISBN 978–80–7204–872–4.

(16) JANKOVÁ, Zuzana. Risk management: Materiály ze cvičení. Brno 2023.

(17) POHODA – Účetní program. POHODA – ekonomický a informační systém [online]. © 2023 [cit. 29.04.2023]. Dostupné z: https://www.stormware.cz/pohoda/

(18) Protecting Data from Ransomware and Other Data Loss Events – Extended Version | NCCoE. Homepage | NCCoE [online]. © 1. 4. 2020 [cit. 29.04.2023]. Dostupné z: https://www.nccoe.nist.gov/publications/other/protecting-data-ransomware-and-other-data-loss-events-extended-version

(19) What is LDAP (Lightweight Directory Access Protocol). Definition from TechTarget. Purchase Intent Data for Enterprise Tech Sales and Marketing – TechTarget [online]. © 2022 [cit. 30.04.2023]. Dostupné z: https://www.techtarget.com/searchmobilecomputing/definition/LDAP

(20) What is VPN? How It Works, Types of VPN. Kaspersky Cyber Security Solutions for Home and Business | Kaspersky [online]. © 2022 [cit. 30.04.2023]. Dostupné z: https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn

(21) What is log management? | Definition from TechTarget. Purchase Intent Data for Enterprise Tech Sales and Marketing – TechTarget [online]. © 2022 [cit. 30.04.2023]. Dostupné z: https://www.techtarget.com/searchitoperations/definition/log-management

(22) What is SIEM? | A Definition from TechTarget.com. Purchase Intent Data for Enterprise Tech Sales and Marketing – TechTarget [online]. © 2022 [cit. 30.04.2023]. Dostupné z: https://www.techtarget.com/searchsecurity/definition/security-information-and-event-management-SIEM

(23) What is Network Time Protocol (NTP)? Purchase Intent Data for Enterprise Tech Sales and Marketing – TechTarget [online]. © 2022 [cit. 30.04.2023]. Dostupné z: https://www.techtarget.com/searchnetworking/definition/Network-Time-Protocol

(24) What is disk mirroring (RAID 1). Definition from TechTarget. Purchase Intent Data for Enterprise Tech Sales and Marketing – TechTarget [online]. © 2023 [cit. 30.04.2023]. Dostupné z: https://www.techtarget.com/searchstorage/definition/disk-mirroring

(25) What is a LAN? Local Area Network – Cisco. Networking, Cloud, and Cybersecurity Solutions – Cisco [online]. © 2023 [cit. 30.04.2023]. Dostupné z: https://www.cisco.com /c/en/us/products/switches/what-is-a-lan-local-area-network.html

(26) What is the Server Message Block (SMB) protocol? How does it work. Purchase Intent Data for Enterprise Tech Sales and Marketing – TechTarget [online]. © 2021 [cit. 30.04.2023]. Dostupné z: https://www.techtarget.com/searchnetworking/definition/ Server-Message-Block-Protocol

(27) What is RDP? Remote Desktop Protocol Explained. Purchase Intent Data for Enterprise Tech Sales and Marketing – TechTarget [online]. © 2022 [cit. 30.04.2023]. Dostupné z: https://www.techtarget.com/searchenterprisedesktop/definition/Remote-Desktop-Protocol-RDP

(28) What is endpoint detection and response (EDR)? Purchase Intent Data for Enterprise Tech Sales and Marketing – TechTarget [online]. © 2021 [cit. 30.04.2023]. Dostupné z: https://www.techtarget.com/searchsecurity/definition/endpoint-detection-and-response-EDR

(29) Doporučení pro zálohování. POHODA – ekonomický a informační systém [online]. © 2023 [cit. 28.04.2023]. Dostupné z: https://www.stormware.cz/podpora/faq/ doprouceni-pro-zalohovani.aspx

(30) Národní úřad pro kybernetickou a informační bezpečnost, Národní agentura pro komunikační a informační technologie, Ministerstvo vnitra, Státní pokladla Centrum sdílených služeb, Ministerstvo zemědělství, Ministerstvo školství a tělovýchovy, Fakultní nemocnice Plzeň, Ministerstvo průmyslu a obchodu. Průvodce řízením aktiv a rizik dle vyhlášky o kybernetické bezpečnosti – Příloha č. 1 – Vzorová politika systému řízení bezpečnosti informací [online]. © 2021 [cit. 05.05.2023]. Dostupné z: https://nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/

SEZNAM POUŽITÝCH ZKRATEK

CIA	Confidentiality, Integrity and Availability – Důvěrnost, integrita, dostupnost
EDR	Endpoint Detection and Response
EZS	Elektronická zabezpečovací signalizace
GDPR	General Data Protection Regulation – Obecné nařízení o ochraně osobních údajů
HA	High Availability – Vysoká dostupnost
HW	Hardware
ID	Identifikátor
IETF	Internet Engineering Task Force
IP	Internet Protocol
IS	Informační systém
IT	Information Technology
KBI	Kybernetický bezpečnostní incident
KBU	Kybernetická bezpečnostní událost
KPI	Key performance indicator
KS	Komunikační systém
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MBS	Minimální bezpečností standard
MKB	Manažer kybernetické bezpečnosti
NAT	Network Address Translation
NTP	Network Time Protocol
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
OWASP	The Open Worldwide Application Security Project
PDCA	Plan–Do–Check–Act
RAID	Redundant Array of Inexpensive Disks
RDP	Remote Desktop Protocol
RTO	Recovery Time Objective

RPO	Recovery Point Objective
SIEM	Security Information and Event Management
SIM	Subscriber Identity Module
SLA	Service–Level Agreement
SMB	Server Message Block
SOC	Security Operations Center
SPOF	Single Point of Failure
SŘBI	Systém řízení bezpečnosti informací
SW	Software
UPS	Uninterruptible Power Supply
UTC	Koordinovaný světový čas
VKB	Vyhláška č. 82/2018 Sb. o kybernetické bezpečnosti
VPN	Virtual Private Network
ZKB	Zákon č. 181/2014 Sb. o kybernetické bezpečnosti

SEZNAM POUŽITÝCH OBRÁZKŮ

SEZNAM POUŽITÝCH TABULEK

SEZNAM PŘÍLOH

Příloha A: Checklist pro kontrolu souladu s MBS

MANAŽERSKÁ ČÁST

1. Základní předpoklady

ID	Požadavek	Poznámky	Stav
1	Podpora ze strany vrcholového vedení		
2	Přidělení přiměřených zdrojů (finanční, lidské, technické)		
3	Podpis dohody o mlčenlivosti		
4	Stanovení bezpečnostních rolí • role je odpovědná za řízení a rozvoj kybernetické bezpečnosti, průběžnou kontrolu stavu kybernetické bezpečnosti, dohlížení na naplňování plánu zavádění bezpečnostních opatření a komunikaci v oblasti kybernetické bezpečnosti s vrcholovým vedením		
5	Tvorba PŘIMĚŘENÝCH bezpečnostních politik • + schválení, kontrola a dodržování		
6	Plán zavádění bezpečnostních opatření • plánování zavádění bezpečnostních opatření a tedy i k zajištění kontinuálního zlepšování • popis opatření, odpovědné osoby, potřebné zdroje a termíny • aktualizovat, zohledňovat kybernetické incidenty a dění v kybernetické bezpečnosti		

2. Klasifikace a ochrana informací

ID	Požadavek	Poznámky	Stav
8	Metodika pro identifikaci a hodnocení informací		
9	Provedení identifikace a hodnocení informací (C, I, A)		
10	Tvorba a aplikace zavedených pravidel pro ochranu informací		
11	Určení odpovědných osob		

3. Řízení dodavatelů

ID	Požadavek	Poznámky	Stav
12	Při uzavírání smluv s dodavateli zohlednit jejich důležitost a oblasti dle MBS zohlednit ve smlouvě.		

4. Řízení lidských zdrojů

ID	Požadavek	Poznámky	Stav
13	Poučit uživatele, administrátory a osoby zastávající bezpečnostní role o jejich povinnostech teoreticky i prakticky je školit, s platnými bezpečnostními politikami seznámit nejen tyto uživatele, ale i relevantní osoby dodavatele a kontrolovat jejich dodržování		
14	Pravidelná školení o základech kybernetické bezpečnosti, a to minimálně 1x ročně.		
15	Seznámení s bezpečnostními politikami a kontrola jejich dodržování.		
16	Postupy při porušení bezpečnostních pravidel.		

17	Zaměstnanci by měli být také proškoleni, jak se chovat v případě neobvyklého či podezřelého chování informačního nebo komunikačního systému, doručení nevyžádaného e-mailu, problémů s dostupností informací či služby nebo při jiné nestandardní situaci.		
18	Hlášení neobvyklých situací.		
19	Nadefinován soubor školení pro nové zaměstnance / pro konkrétní pracovní pozice.		
20	Při změně pozice je nutno absolvovat odpovídající školení.		
21	Specializovaná školení pro bezpečnostní role a IT zaměstnance.		
22	Školení při výskytu mimořádné / nestandardní události organizovat mimořádná školení, nebo zaměstnance vhodných způsobem informovat.		

5. Řízení změn

ID	Požadavek	Poznámky	Stav
23	Řešit problematiku řízení změn a konfigurací při provozu IS nebo KS.		
24	Evidence všech změn.		
25	Systematické vyhodnocování změn.		
26	Koordinování a implementace schválených změn a konfigurací.		
27	V případě provedení změny zvážení dopadů dané změny a pokud by mohla mít nepříznivý dopad, změnu dokumentovat.		
28	Změny v rámci IS nebo KS řídit prostřednictvím změnových požadavků, které jsou schvalovány osobou odpovědnou za kybernetickou bezpečnost.		
29	Změny je třeba řídit a dokumentovat.		
30	Přijmout opatření za účelem snížení všech nepříznivých dopadů spojených se změnami.		
31	Aktualizovat relevantní bezpečnostní politiky a dokumentaci.		
32	Zajistit testování změn.		
33	Zajistit možnost vrácení do původního stavu.		
34	V případě potřeby provést penetrační testování.		

6. Řízení kontinuity činnosti

ID	Požadavek	Poznámky	Stav
35	Vypracovat BCP, DRP a havarijní plány – vypracovány postupně s ohledem na důležitost IS nebo KS.		
36	Stanovit práva a povinnosti administrátorů a osob podílejících se na zajištění chodu organizace – kdo, kdy a co má v průběhu mimořádné situace dělat		
37	Vyhodnocení a posouzení možných rizik souvisejících s ohrožením kontinuity činností. Je nutné sestavit možné elementární scénáře toho, co se může stát (nedostupnost budov, IT systémů, lidí, vznik epidemie apod.) a jaký bude dopad na důvěrnost, dostupnost a integritu dat v informačním nebo komunikačním systému a co to bude znamenat pro poskytování služeb.		
38	Stanovení cíle řízení kontinuity činností formou určení:		
38.1	• minimální úrovně užívání, provozu a správy, která je akceptovatelná pro zachování poskytovaných služeb		

38.2	• doby obnovení chodu (RTO)		
38.3	• bodu obnovení dat (RPO)		
39	Vytvoření postupů, které obsahují naplnění cílů podle přechozího bodu – jak organizace dosáhne toho, aby jej splnila		
40	Vytvoření postupů, havarijních plánů, DRP pro obnovu chodu IS nebo KS		

7. Audit kybernetické bezpečnosti

ID	Požadavek	Poznámky	Stav
41	Provádění nezávislého auditu.		
42	Audit kybernetické bezpečnosti posuzuje soulad s: • bezpečnostní dokumentací a bezpečnostními politikami organizace • právními předpisy • jinými předpisy a smluvní závazky, které se vztahují k IS nebo KS • nejlepší praxí		
43	Prováděno pravidelně (jednou za 2/3 roky) a • při změnách, které mohou mít negativní dopad na kybernetickou bezpečnost • v pravidelných intervalech dle uvážení organizace • při kybernetickém incidentu se závažným dopadem provést mimořádný audit		
44	Osoba provádějící audit KB je vyškolena.		
45	Osoba provádějící audit KB je oddělena od provozních nebo bezpečnostních rolí a byla zajištěna její nezávislost.		
46	Je určen někdo, kdo bude dohlížet na průběh tohoto auditu.		
47	Výsledky auditu se předkládají vrcholovému vedení a promítnou se do plánu zavádění opatření a bezpečnostní dokumentace.		

TECHNICKÁ ČÁST

1. Fyzická bezpečnost

ID	Požadavek	Poznámky	Stav
1	Definovat nový, či rozšířit stávající soubor opatření předcházející poškození, krádeži či zneužití informací či majetku nebo přerušení služeb IS nebo KS, vymezit fyzický perimetr.		
2	Fyzický perimetr je chráněn a zabezpečen před neoprávněným vstupem a poškozením, krádeží či zneužitím.		
3	Zajištěna ochrana kritických míst v rámci objektů (serverovny, kanceláře zaměstnanců, technologické místnosti)		
4	Jasně definována pravidla pro návštěvy		
5	Zajištěno záložní napájení (UPS)		
6	Zajištěna klimatizace serverovny.		
7	Zajištěna bezpečnost kabelových rozvodů.		

2. Řízení přístupů

ID	Požadavek	Poznámky	Stav
8	Vytvořena politika řízení přístupu.		
9	Přiděleny jedinečné identifikátory jednotlivým uživatelům a administrátorům přistupujících k informačnímu nebo komunikačnímu systému.		
10	Řízeny a evidovány identifikátory, přístupová práva a oprávnění aplikací a technických účtů.		
11	Prováděno řízení přístupu na základě skupin a rolí.		
12	Jsou definovány postupy a pravidla potřebné pro omezení a kontrolu používaného SW a HW, který by mohl narušit systémovou a aplikační bezpečnost.		
13	Privilegované účty mají přiděleny samostatné přihlašovací údaje.		
14	Jednotliví administrátoři mají vedle privilegovaného účtu i účet běžného uživatele pro činnost, které nevyžadují privilegovaná oprávnění.		
15	Uplatňován princip need-to-know.		
16	Vedení organizace využívá běžné uživatelské účty.		
17	Politika pro přidělování, odebírání rolí.		
18	IS nebo KS zajišťuje registraci všech uživatelů centrálně.		
19	Jsou stanoveny pravidla pro procesy:		
19.1	• registrace		
19.2	• schvalování		
19.3	• generování identit		
19.4	• přidělování a odebírání přístupů		
19.5	• deaktivace identit		
19.6	• monitorování činnosti uživatelů		
20	IS nebo KS musí umožňovat využívat stávající IS nebo KS pro Identity management.		

21	Jestliže existují v rámci informačního nebo komunikačního systému lokální účty, je nezbytné, aby se řídily následující politikou hesel pro privilegované účty, nebo je nutné umožnit integraci s informačním nebo komunikačním systémem pro správu privilegovaných účtů.		
22	Existuje politika hesel pro privilegované účty v minimální míře:		
22.1	• minimální délka hesla je 17 znaků		
22.2	• musí obsahovat: velká písmena, malá písmena, číslice a speciální znak		
22.3	• maximální doba platnosti hesla je 18 měsíců		
22.4	• zákaz používaní stejného hesla (posledních 12 hesel)		
22.5	• minimální platnost hesla 1 den		
22.6	• zamčení účtu po 5 neplatných pokusech zadání hesla v řadě		
22.7	• jednorázové prvotní heslo, které musí být změněno po prvním přihlášení nebo zneplatněno po 24 hodinách		
23	Existuje politika hesel pro uživatelské účty v minimální míře:		
23.1	• minimální délka hesla je 10 znaků		
23.2	• zákaz používaní stejného hesla (posledních 12 hesel)		
23.3	• maximální doba platnosti hesla je 18 měsíců		
23.4	• zamčení účtu po 10 neplatných pokusech zadání hesla v řadě		
23.5	• jednorázové prvotní heslo, které musí být změněno po prvním přihlášení nebo zneplatněno po 24 hodinách		

3. Požadavky v oblasti ochrany před škodlivým kódem

ID	Požadavek	Poznámky	Stav
24	V rámci IS nebo KS je navržen a implementován způsob řešení ochrany před škodlivým kódem		
25	Správce IS nebo KS musí zhodnotit všechny směry, vstupy/výstupy dat a jejich uložení či další zpracování v IS nebo KS a navrhnout způsob ochrany před škodlivým kódem.		
26	V rámci IS nebo KS jsou zavedeny minimálně následující opatření:		
26.1	• segmentace síťového prostředí (oddělení sítí pro provoz a pro správu), kde je to opodstatněné		
26.2	• instalace SW pro detekci a odstranění škodlivých programů a na IS nebo KS, kde je to technicky realizovatelné		
26.3	• pravidelná aktualizace SW pro detekci a odstranění škodlivých kódů včetně databáze vzorků nejméně jednou denně		
27	V prostředí IS nebo KS je zakázáno vzdálené spouštění kódu ze zdroje mimo jejich prostředí.		

4. Kybernetické bezpečnostní události a incidenty

ID	Požadavek	Poznámky	Stav
28	Stanovena pravidla pro vyhodnocování kybernetických bezpečnostních událostí a zvládání kybernetických bezpečnostních incidentů.		
29	Evidování a analýza kybernetických bezpečnostních událostí a incidentů za účelem eliminace dalšího výskytu.		
30	Stanoveny auditní požadavky.		
31	Stanoven proces pro řízení hlášení nestandardního chování IS nebo KS.		
32	Zaměstnanci jsou seznámeni s tím, co mají hlásit a mají k dispozici konkrétní kontakty, na koho se v rámci organizace obracet.		
33	Funguje eskalační proces, v rámci kterého jsou přesně definovány v rámci organizace osoby, které budou o situaci informovány a případně na ně bude přenesena odpovědnost za její řešení.		
34	IS nebo KS zajišťuje auditovatelnost dat i procesů, včetně procesu řízení identit uživatelů.		
35	Organizace disponuje provozními záznamy z doby kybernetického bezpečnostního incidentu pro ex-post analýzu, tyto záznamy poskytují například: • bezpečnostní nástroje (antivirus, IDS/IPS, proxy, router, switch, firewall, …) • operační systémy (autentizace, privilegované spuštění, systémové události, …) • aplikace (komunikace mezi klientem a serverem, uživatelské události, přístupy, …)		
36	IS nebo KS uchovává provozní i bezpečnostní logy následovně:		

Tabulka č. 3 Minimální počet dní uchování logů pro jednotlivé skupiny

SEC				
Počet dní	60			
OS	Systém	Audit		
Počet dní	30	30		
APP	C<>S	Využití účtů	Aktivita	Akce
Počet dní	7	7	1	30

Tabulka č. 4 Standard pro kategorie

Kategorie	Standard
Rotace logů	Každý týden nebo po dosažení max. 100 MB
Jak často zasílat do log managementu	Nejméně jednou za 24 hodin
Kontrola integrity (rotace)	Volitelná
Šifrování uložených záznamů	Volitelné
Šifrovaný přenos záznamů do log managementu v rámci vnitřní sítě	Volitelné
Šifrovaný přenos záznamů do log managementu skrz veřejnou síť	Povinné (např. v rámci VPN či TLS.)

ID	Požadavek	Poznámky	Stav
37	Logy IS nebo KS musí být integrovatelné do centrálního řešení pro vyhodnocování provozních a bezpečnostních logů, pokud takový IS nebo KS není zaveden, doporučuje se při výběru nové technologie vyžadovat minimálně jednou z následujících metod pro zajištění kompatibility v případě zavedení centrálního log managementu: • Syslog (RFC 5424) • SNMPv3 TRAP • JDBC • Microsoft Event Log		
38	IS nebo KS, včetně infrastruktury (je jeho podpůrnou součástí a jeho další komponenty musí být připraveny na integraci do SIEM obdobným způsobem tak, aby naplňovaly požadavky na bezpečnostní monitoring.		
39	Musí být pořizovány a uchovávány auditní záznamy tak, aby byly využitelné pro monitorování řízení přístupu a případné budoucí vyšetřování bezpečnostních incidentů. Jedná se minimálně o tyto typy událostí:		
39.1	• přihlášení a odhlášení uživatelů a administrátorů, a to včetně neúspěšných pokusů,		
39.2	• činnosti provedené administrátory, o použití privilegovaných účtů, např. účtu supervisora, administrátora		
39.3	• spuštění a ukončení informačního nebo komunikačního systému,		
39.4	• změny konfigurací,		
39.5	• úspěšné i neúspěšné činnosti vedoucí ke změně přístupových oprávnění,		
39.6	• zahájení a ukončení činností zařízení a aplikací,		
39.7	• automatická varovná nebo chybová hlášení zařízení a aplikací,		
39.8	• přístupy k záznamům o činnostech, pokusy o manipulaci se záznamy o činnostech a změny nastavení nástroje pro zaznamenávání činností,		
39.9	• použití mechanismů identifikace a autentizace včetně změny údajů, které slouží k přihlášení		
40	Jednotlivé položky logu informačního nebo komunikačního systému nebo jeho jednotlivé řádky záznamu musí obsahovat minimálně tyto pole		
40.1	• datum a čas události (uvedený s jednoznačnou identifikací časové zóny, např. UTC nebo lokální čas s uvedením offsetu),		
40.2	• síťové identifikátory komunikujících bodů (tj. např. IP adresy a porty, v případě použití proxy nebo NATu musí být síťový identifikátor předán jinou formou nebo musí být možné tyto logy korelovat),		

40.3	• identifikátor uživatele, pod kterým byla činnost provedena,		
40.4	• typ události,		
40.5	• úspěšnost nebo neúspěšnost činnosti.		
41	V případě, že záznamy zapisované do logu informačního nebo komunikačního systému obsahují citlivé informace (heslo, soukromý klíč či jeho prekurzor, session ID apod.) musí být před zapsáním přepsány pseudonáhodnou sekvencí. V žádném případě nesmí dojít k zapsání citlivých informací v čistém textu.		
42	V informačním nebo komunikačním systému musí být zavedena ochrana proti deaktivaci, selhání či změnám v pořizování auditních záznamů a ochrana proti změnám nebo zničení auditních záznamů.		
43	Přístup k auditním záznamům musí být chráněn, aby bylo zabráněno jeho zneužití nebo ohrožení.		
44	IS nebo KS musí umožnit nastavení přístupových práv k auditním záznamům tak, aby mohly být auditovány samostatnou rolí (auditor, security officer apod.).		
45	Aby bylo možné korelovat logy z více zařízení informačního nebo komunikačního systému, musí být systémový čas synchronizován v rámci informačního nebo komunikačního systému alespoň jednou za 24 hodin (např. pomocí protokolu NTP).		

5. Požadavky v oblasti aplikační bezpečnosti

ID	Požadavek	Poznámky	Stav
46	Musí probíhat integrační, systémové, zátěžové a akceptační testy ve vyhrazeném testovacím prostředí nebo módu, tak aby nemohla být narušena činnost produkčních systémů.		
47	Uvedené testy jsou prováděny		
47.1	• s ohledem na rozsah, složitost informačního nebo komunikačního systému, charakter zpracovávaných dat a informací a na okolní vazby informačního nebo komunikačního systému.		
48	Testovací údaje (data) musí být dostatečně chráněny a kontrolovány. Je-li to možné, musí být testování prováděno na neprovozních datech. Pokud je nezbytné využít k testování provozní data, upřednostní se použití již pozměněných dat.		
49	Při výběru provozních dat k testování z provozních databází je nutné použít maskování položek, které nejsou pro potřeby testování nezbytné.		
50	Pokud je nutné použít platná provozní data, musí být dodrženy následující zásady:		
50.1	• postupy kontroly přístupu platné pro provozní data musí být uplatněny i pro testovací data,		
50.2	• každé kopírování provozních dat do testovacího prostředí musí být autorizováno souhlasem odpovědné osoby (například ve schváleném zápisu),		

50.3	• neveřejné informace musí být okamžitě po ukončení testů odstraněny z testovaného prostředí bezpečným způsobem, aby nebyla možná jejich dodatečná obnova,		
50.4	• kopírování a užití provozních dat musí být zaznamenáváno do auditních záznamů.		
51	Pro zvýšení bezpečnosti je doporučeno u vyvíjených aplikací provést analýzu zdrojového kódu a otestovat zranitelnost. Součástí akceptace musí být prohlášení o provedení těchto testů a jejich výsledky. Dodavatel informačního nebo komunikačního systému poskytne prohlášení o provedení těchto testů, které bude obsahovat minimálně tyto položky:		
51.1	• datum provedení testu,		
51.2	• použitá testovací metodika a metodika scoringu,		
51.3	• název nástroje použitého pro testování,		
51.4	• konfigurace profilu pro testování,		
51.5	• výsledky testování, navržení opatření,		
51.6	• shrnutí výsledku testování a závěrečná zpráva,		
51.7	• osobní odpovědnost – jména odpovědných osob.		

6. Kryptografické prostředky

ID	Požadavek	Poznámky	Stav
52	Zajistit šifrování přenosu dat. Šifrování uložených dat je pouze doporučeno, a to v návaznosti na typ a charakter dat a v návaznosti na možné technologické řešení.		
53	Data a informace zpracovávaná v rámci informačního nebo komunikačního systému musí být chráněna proti zneužití vhodnými kryptografickými metodami, které zajistí pouze autorizovaný přístup k těmto datům a informacím.		
54	Dle aktuálního doporučení NÚKIB je pro šifrování disků možné použít následující symetrické blokové šifrovací algoritmy: • Advanced Encryption Standard (AES) s využitím délky klíčů 128, 192 a 256 bitů • Twofish s využitím délky klíčů 128 až 256 bitů • Serpent s využitím délky klíčů 128, 192, 256 bitů • Camellia s využitím délky klíčů 128, 192 a 256 bitů • Přitom mezi preferované patří AES, Camellia a Serpent (v uvedeném pořadí) a velikost klíče 256 bitů		
55	Pro šifrování disků doporučení schvaluje použití následujících módů: • XTS – délka jednotky dat (sektoru) nesmí přesáhnout 220 bloků šifry (v případě šifry se 128-bitovým blokem je to přibližně 16 MB) • EME		
56	Pokud IS nebo KS ukládá hesla, musí být takto uložená hesla odolná proti offline útokům (tedy takovým způsobem, u kterého je výpočetně náročné z uloženého hesla získat původní heslo) • nejlépe použitím k tomu určenému hašovacímu algoritmu spolu s náhodně vygenerovanou „solí“.		

57	Pokud IS nebo KS umožňuje volbu algoritmu nebo se jedná o nově vznikající IS nebo KS, doporučujeme použít jeden z následujících algoritmů (v pořadí od nejvhodnějšího): • Argon2 (nejlépe ve verzi „id“), • Scrypt, • Bcrypt, • Pbkdf2 (s použitím schváleného hašovacího algoritmu).		
58	„Sůl“ by měla mít velikosti minimálně 64 bitů (doporučujeme 128 bitů). Pokud je možné zvolit výpočetní náročnost algoritmu, výpočet by měl trvat výpočet minimálně 100 ms (doporučeno 500 ms) a využít minimálně 1 MB paměti.		

7. Požadavky v oblasti zajišťování úrovně dostupnosti informací

ID	Požadavek	Poznámky	Stav
59	Musí být stanovena a definována správcem na požadovanou úroveň na základě plánu kontinuity činností – BCP		
60	Je řešeno zajištění dostupnosti implementací redundantních a clusterovaných schémat v režimu vysoké dostupnosti (HA), stanovením úrovně podpory, postupy obnovy po havárii a zálohováním.		
61	V maximální možné míře zohlednit dodržování pravidla eliminace „SPOF“ (Single Point of Failure) – to znamená, že porucha jedné komponenty nezpůsobí výpadek celého informačního nebo komunikačního systému. Při zohlednění pravidla SPOF je nutné brát do úvahy efektivitu (tedy náklady) a požadavky na dostupnost		
62	Vytvořen detailní návrh zálohování celého IS nebo KS v následující struktuře: • Z hlediska potřebných zálohovacích médií je vhodné uvažovat o uplatnění pravidla 3-2-1. Toto pravidlo znamená, že jsou k dispozici tři kopie dat na dvou různých typech médií, přičemž jedno z nich by se mělo nacházet mimo lokalitu umístění informačního nebo komunikačního systému („offsite“).		

8. Požadavky v oblasti cloudových služeb

ID	Požadavek	Poznámky	Stav
63	Bezpečnostní opatření kybernetické bezpečnosti jsou aplikována na dodavatele cloudových služeb.		
64	Jsou stanoveny podmínky pro využívání cloudových služeb:		
64.1	• deklarace místa uložení zákaznických dat v rámci jurisdikce EU,		
64.2	• deklarace úrovně bezpečnosti poskytovaných cloudových služeb – (doporučujeme doložení certifikátu ČSN ISO/IEC 27001 nebo Auditní zprávu SOC 2 Type II (AT101), případně zajištění auditu na místě),		

64.3	• šifrovaná komunikace (TLS/VPN) přes internet s využitím kryptografických algoritmů publikovaných v doporučení NÚKIB,		
64.4	• smlouva s provozovatelem cloudových služeb obsahující vymezení provozních podmínek (SLA) a tzv. exit strategii (exit plán) včetně přádání dat,		
64.5	• smluvní podmínky s provozovatelem cloudových služeb, které jsou v souladu s požadavky na zpracovatele dle čl. 28 Obecného nařízení GDPR (v případě zpracování osobních údajů v informačním nebo komunikačním systému),		
64.6	• smlouva s provozovatelem cloudových obsahující povinnost informovat o bezpečnostních incidentech týkajících se daného zákazníka, a spolupracovat při jejich zvládání.		

9. Výjimky běhu, chyby a hlášení

ID	Požadavek	Poznámky	Stav
65	Je stanoven proces řízení výjimek a jejich evidence.		
66	IS nebo KS podporuje řízení výjimek • Výjimkou je myšlena libovolná chyba nebo neočekávané chování informačního nebo komunikačního systému, které se vyskytne během vykonávání programu a je následně zpracováno a zároveň nedojde k neřízenému selhání běhu informačního nebo komunikačního systému		
67	Výjimky jsou zaznamenány v logu.		
68	Log je pravidelně vyhodnocován, přičemž zjištěné nedostatky nebo závady v IS nebo KS jsou v maximální možné míře ošetřeny.		

10. Ochrana informačního nebo komunikačního systému typu webové aplikace

ID	Požadavek	Poznámky	Stav
69	Řídit se doporučeními OWASP a věnovat pozornost zranitelnostem.		
70	Je nutno věnovat pozornost především proti následujícím zranitelnostem:		
70.1	• Cross Site Scripting (XSS). XSS je metoda narušení webových stránek využitím bezpečnostních chyb ve skriptech (především neošetřené vstupy).		
70.2	• Injection útoky. SQL injection je technika napadnutí databázové vrstvy programu vsunutím (injection) kódu přes neošetřený vstup a vykonání vlastního, pozměněného, SQL dotazu. Vedle SQL injection existují též další podobné scénáře s jiným cílem, např. shell command injection, LDAP injection atd.		

70.3	• Vzdálené spuštění kódu. Buď vlivem zranitelnosti v samotném webovém serveru, použitém frameworku či logice ve webové aplikaci.		
70.4	• Nezabezpečený přímý popis objektu. Zranitelnosti této kategorie umožňují útočníkovi získat informace o jednotlivých objektech cílové aplikace bez patřičné autentizace.		
70.5	• Cross Site Request Forgery (CSRF). CSFR je technika, která umožňuje útočníkovi podvrhnout formulář na jiné stránce nebo pomocí některých HTTP metod přesměrovat prohlížeč oběti na skript zpracovávající legitimní formulář aplikace s daty, která můžou oběť poškodit.		
70.6	• Únik informací nebo nedostatečné řízení chyb. Zranitelnosti tohoto typu útočníkovi zpřístupňují v případě chybového stavu aplikace informace, které lze později použít k lepšímu plánování útoku.		
70.7	• Špatná autentizace a správa relace. Zranitelnosti tohoto typu umožňují útok na přihlašovací části aplikace či úplné obcházení přihlašovacího systému.		
70.8	• Nezabezpečené kryptografické úložiště. Zranitelnosti tohoto typu můžou způsobit kompromitaci privátního šifrovacího klíče jedné či obou stran spojení.		
70.9	• Nezabezpečená komunikace. Zranitelnosti tohoto typu umožňují útočníkům odchytávat komunikaci, která jim není určená, a provádět též aktivní útoky typu Man-in-the-Middle.		
70.10	• Chybné zamezení URL přístupu. V případě, že aplikace umožňuje neautentizovaný přístup i ke stránkám, ke kterým by měl být přístup jen po příslušné autentizaci, je možnou zranitelností situace, kdy takto odkazovaná stránka zobrazí některé informace, které by měly být přístupné jen konkrétním autorizovaným uživatelům, či systémové informace citlivého charakteru.		

11. Rozvoj informačních a komunikačních systémů

ID	Požadavek	Poznámky	Stav
71	Na základě výsledků posouzení bezpečnostních aspektů vyvíjeného informačního nebo komunikačního systému musí být definovány obecné požadavky na bezpečnost informačního nebo komunikačního systému pro zjištění důvěrnosti, dostupnosti a integrity informací v informačním nebo komunikačním systému. Součástí těchto obecných požadavků musí být:		
71.1	• identifikace dat vytvářených, zpracovávaných a ukládaných v informačním nebo komunikačním systému,		
71.2	• definice klíčových bezpečnostních rolí včetně školení uživatelů, správců a vývojářů,		

71.3	• identifikace zdrojů požadavků na IS nebo KS z hlediska bezpečnosti a regulatorních požadavků.		
72	V případě vyvíjeného informačního nebo komunikačního systému dodavatelem musí být definovány a dokumentovány následující požadavky:		
72.1	• požadavky na licenční ujednání, vlastnictví kódu a práv duševního vlastnictví,		
72.2	• požadavky na osvědčení kvality a správnosti provedených prací,		
72.3	• požadavky na uložení zdrojového kódu,		
72.4	• požadavky na právo přístupu k vývoji pro audit bezpečnosti a správnosti provedené práce,		
72.5	• požadavky na smluvní podmínky na bezpečnost a zabezpečení kódu,		
72.6	• požadavky na provedení testů zranitelností před instalací v produkčním prostředí		
73	V případě webových aplikací je dodavatel povinen zajistit vývoj dle principů definovaných ve standardu OWASP v aktuálním znění.		
74	Správce definuje konkrétní bezpečnostní požadavky na IS nebo KS na základě posouzení bezpečnostních aspektů IS nebo KS		
74.1	• Požadavky musí být v souladu s existujícími směrnicemi, zejména použité bezpečnostní komunikační protokoly, způsoby a možnosti šifrování. Součástí požadavků musí být i definování komunikační matice při vývoji aplikace		
75	Správce informačního nebo komunikačního systému definuje a dokumentuje akceptační kritéria bezpečnosti pro přechod informačního nebo komunikačního systému do produkčního provozu.		
76	Správce informačního nebo komunikačního systému zajistí v oprávněných případech návrh splnění bezpečnostních požadavků		
77	Vývojové prostředí používané pro vývoj komponent informačního nebo komunikačního systému musí být zcela odděleno od provozního prostředí, a to včetně správy uživatelských oprávnění		
78	Pro IS nebo KS vyvíjený externím dodavatelem musí být smluvně zajištěno právo auditu zdrojového kódu a dodržování požadavků na bezpečnost.		
78.1	• Smluvně též musí být zajištěno uložení zdrojových kódů u důvěryhodné třetí strany (code escrow) v případě, že dodavatel nepředává zdrojový kód jako součást dodávky vyvíjeného programového vybavení (informačního nebo komunikačního systému systému).		
79	V případě vývoje aplikace (součásti informačního nebo komunikačního systému) musí mít zhotovitel formalizovanou metodiku pro vývoj, programování a kódování aplikace a testování.		

79.1	• Tato metodika musí obsahovat mimo jiné požadavky na kybernetickou bezpečnost.		
79.2	• V metodice musí být uvedeny principy organizační bezpečnosti pro vývoj a testování aplikace.		
79.3	• Zhotovitel musí doložit typ metodiky, který použil pro vývoj aplikace prostřednictvím čestného prohlášení a dodání popisu nebo dokumentace této metodiky.		

12. Komunikace

ID	Požadavek	Poznámky	Stav
80	Komunikace s externími informačními nebo komunikačními systémy by měla být rozdělena podle stupně zabezpečení na:		
80.1	• zabezpečený kanál přenosu (šifrování dat) s povinnou úrovní zabezpečení koncových bodů informačního nebo komunikačního systému na úrovni infrastruktury,		
80.2	• šifrování dat pro přenos a autorizací uživatele v rámci informačního nebo komunikačního systému,		
80.3	• zajištění šifrování nebo náhradu citlivých dat na úrovni poskytovatelských a konzumentských informačních nebo komunikačních systémů pomocí end to end metody při přenosu dat.		