VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ

FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY

INSTITUTE OF INFORMATICS

IMPLEMENTACE MINIMÁLNÍHO BEZPEČNOSTNÍHO STANDARDU VE SPOLEČNOSTI

IMPLEMENTATION OF THE MINIMUM SECURITY STANDARD IN COMPANY

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

AUTOR PRÁCE — Bc. Adam Křiva

AUTHOR

VEDOUCÍ PRÁCE — Ing. Petr Sedlák

SUPERVISOR

BRNO 2023

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Student:	**Bc. Adam Křiva**
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:

Implementace minimálního bezpečnostního standardu ve společnosti

Charakteristika problematiky úkolu:

Úvod
Teoretická východiska práce
Analýza současného stavu
Vlastní návrhy řešení
Závěr

Cíle, kterých má být dosaženo:

Hlavním cílem diplomové práce je zavedení kybernetické bezpečnosti podle minimálního bezpečnostního standardu pro danou společnost.
Společnost by ráda zvýšila úroveň své kybernetické bezpečnosti podle minimálního bezpečnostního standardu vytvořeného NÚKIB. Dále by ráda vzdělávala své zaměstnance a tím minimalizovala hrozby.

Základní literární prameny:

Národní úřad pro kybernetickou a informační bezpečnost. Minimální bezpečnostní standard [online]. [cit. 2023-1-31]. Dostupné z: https://www.nukib.cz/download/publikace/podpurne_materialy/2020-07-17_Minimalni-bezpecnostni-standard_v1.0.pdf

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

Předmětem diplomové práce je implementace minimálního bezpečnostního standardu v rámci společnosti. Práce se v první části zaměřuje na teoretická východiska. Následně je provedena analýza současného stavu ve společnosti. Vlastní návrh řešení určuje rozsah minimálního bezpečnostního standardu, identifikuje a hodnotí aktiva, popisuje vytvořené bezpečnostní politiky po manažerské i technické stránce. Vytvořené bezpečnostní politiky jsou následně ekonomicky zhodnoceny.

Klíčová slova

Kybernetická bezpečnost, Informační bezpečnost, Minimální bezpečnostní standard, Bezpečnostní politiky, Aktiva

Abstract

The subject of the diploma thesis is the implementation of a minimal security standard within a company. The thesis focuses on theoretical foundations in the first part. Subsequently is conducted an analysis of the current state within the company. The actual solution proposal determines the scope of the minimal security standard, identifies and evaluates assets, describes the created security policies from the managerial and technical aspects. The developed security policies are then economically assessed.

Keywords

Cybersecurity, cyber security, Information Security, Minimal Security Standard, Cybersecurity policies, Assets

Bibliografická citace

KŘIVA, Adam. *Implementace minimálního bezpečnostního standardu ve společnosti* [online]. Brno, 2023 [cit. 2023-05-15]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/152020. 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 zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 15. května 2023 .....

Bc. Adam Křiva

autor

Poděkování

Tímto bych chtěl poděkovat vedoucímu mé diplomové práce panu Ing. Petru Sedlákovi za skvělý přístup, cenné rady a připomínky, které mi poskytl při vypracování mé diplomové práce. Dále bych rád poděkoval Ing. Mateji Zápotočnému, Ph.D. za odbornou konzultaci. Také bych chtěl poděkovat společnosti za poskytnuté informace potřebné pro vypracování práce a své rodině za velkou podporu při studiu.

Obsah

Úvod

Efektivní fungování organizací je primárním cílem každého vrcholového vedení. Tohoto cíle je dosahováno přesouváním procesů do kybernetického prostoru a využitím výkonných výpočetních technologií umožňující vznik, zpracování a výměnu dat i informací. S tím však rostou i rizika ohrožující procesy organizace v podobě kybernetické kriminality.

Pro fungování organizací jsou v současné době zásadní technologie, data a informace. Aby nedošlo k omezení činnosti z důvodu vzniku nestandardní situace, která by poškodila tato aktiva, musí být adekvátně chráněna z pohledu informační a kybernetické bezpečnosti.

Tato bezpečnost bývá velmi často zanedbávaná, a proto jsou určené organizace nuceny investovat do kybernetické bezpečnosti na základě Zákona o kybernetické bezpečnosti. Tyto vybrané organizace musí splňovat přísná bezpečnostní pravidla pro ochranu, které jsou úřadem kontrolovány.

Pro menší organizace, které se však zákonem o kybernetické bezpečnosti řídit nemusí, by bylo dodržování těchto pravidel vysoce nákladné a neefektivní. Z toho důvodu vytvořil Národní úřad pro informační a kybernetickou bezpečnost návod s doporučením v podobě Minimálního bezpečnostního standardu, který nabízí zjednodušené postupy a doporučení v oblasti kybernetické bezpečnosti. Tyto doporučené minimální bezpečnostní požadavky by měla ideálně splňovat každá společnost, pro kterou jsou její data a informace důležité.

Cíle práce, metody a postupy zpracování

Hlavním cílem diplomové práce je zavedení kybernetické bezpečnosti podle minimálního bezpečnostního standardu pro danou společnost. Společnost by ráda zvýšila úroveň své kybernetické bezpečnosti podle minimálního bezpečnostního standardu vytvořeného Národním úřadem pro kybernetickou a informační bezpečnost (NÚKIB). Dále by ráda vzdělávala své zaměstnance a tím minimalizovala kybernetické hrozby.

Bezpečnostní politiky budou vycházet z Minimálního bezpečnostního standardu vydaného NÚKIB.

Diplomová práce je rozdělena do tří základních částí. Teoretická východiska práce, analýza současného stavu a návrh vlastního řešení.

Teoretická východiska práce vysvětlují základní pojmy z oblasti kybernetické bezpečnosti, které jsou podstatné k pochopení problematiky informační a komunikační bezpečnosti.

Druhá část je zaměřena na analýzu současného stavu ve společnosti, kde je společnost stručně představena, je analyzována infrastruktura společnosti, a to konkrétně hardware, software, síť, datové rozvaděče a zálohování. Následně je provedena analýza současného stavu podle Minimálního bezpečnostního standardu (MBS) a její zhodnocení.

Závěrečná část se zabývá návrhem vlastního řešení, kde je vytvořena identifikace a hodnocení aktiv. Následně jsou vytvořeny bezpečnostní politiky z manažerské a technické části dle MBS. Na závěr je provedeno ekonomické zhodnocení vlastního návrhu bezpečnostních politik a stanovení přínosů diplomové práce.

1 Teoretická východiska práce

V této části jsou popsána základní teoretická východiska, která jsou zásadní pro správné pochopení problematiky této diplomové práce. Jsou zde uvedeny termíny a definice jednotlivých pojmů, vysvětlení Demingova cyklu PDCA, přiměřené bezpečnosti, znalostního trojúhelníku, bezpečnosti informací, bezpečnostní role v organizaci, význam bezpečnostního povědomí, řízení kontinuity činnosti, normalizační instituce a právního prostředí.

1.1 Termíny a definice

Informační systém IS

Je funkční celek zajišťující účelné a systematické shromažďování, zpracování, uchovávání a zpřístupňování dat i informací. Skládá se z datových a informačních zdrojů, nosičů, programových vybavení, technologií, procesů a lidských zdrojů podílejících se na zacházení s daty a informacemi. [3, 4]

Informační a komunikační technologie ICT

Jsou veškeré technické komponenty, které umožňují zpracování a přenos dat a informací. Primárně se jedná o výpočetní a komunikační techniku a její programové vybavení. [4]

Síťová infrastruktura

Jsou všechny síťové prvky a zařízení využívané k provozu ICT prostředí. Síťovou infrastrukturou můžeme označit také všechna aktiva z oblasti informačních a komunikačních technologií využívaných k tvorbě a podpoře IS. [5]

Počítačová síť

Jedná se o část síťové infrastruktury, která vytváří komunikační prostředí mezi uživateli sítě. [5]

Kybernetický prostor

Je globálně propojené digitální prostředí, které se skládá z internetu a dalších počítačových sítí, systémů, služeb a procesů na nich poskytovaných. Umožňuje propojení

osobních i podnikatelských aktivit spolu se vznikem, vytvářením, zpracováním a výměnou informací. [4, 6]

Kybernetická bezpečnost

Je soubor právních, organizačních, technických a vzdělávacích prostředků chránící lidi a organizace před kybernetickými hrozbami. [4, 6]

Aktivum

Pojmem aktivum můžeme definovat vše, co má pro organizaci určitou hodnotu v podobě hmotného i nehmotného majetku. Aktiva dělíme do dvou skupin, a to na primární a podpůrná aktiva. [3, 6]

- **Primární aktiva**

  Primární aktiva jsou služby, informace a procesy, které v případě ztráty nebo jejich narušení mají významný dopad na funkčnost a bezpečnost organizace z hlediska důvěrnosti, integrity a dostupnosti. [3, 7]

- **Podpůrná aktiva**

  Všechna aktiva, která souvisejí a podporují primární aktiva. Mezi podpůrná aktiva patří lidské zdroje, hardware, software a síťová infrastruktura organizace. [3, 7]

Zranitelnost

Zranitelnost je slabé místo aktiva nebo opatření, které může být využito hrozbami k narušení bezpečnosti informací. [3]

Kybernetické riziko

Soubor možností, při kterých může hrozba využít zranitelnost aktiva nebo skupiny aktiv k narušení bezpečnosti informací a způsobení škody organizaci. [6]

Kybernetická hrozba

Je potenciální příčina nechtěného incidentu, která se nachází v kybernetickém prostoru, jehož výsledkem může dojít k poškození systému, informací nebo organizace. [6, 8]

Kybernetická událost KBÚ

Je událost, která může narušit bezpečnost informací, služeb nebo zapříčinit výpadek činnosti organizace či informačního systému. [6]

Kybernetický incident KBI

Je kybernetická událost, která již způsobila narušení bezpečnosti informací, služeb nebo zapříčinila výpadek činnosti organizace či informačního systému. [4, 6]

Kybernetický útok

Úspěšný nebo neúspěšný neoprávněný pokus o zničení, vystavení hrozbě, změnu, zablokování, vyřazení z činnosti nebo získání neoprávněného přístupu k aktivu nebo zcizení či neoprávněné použití aktiva. [3, 8]

Kybernetická obrana

Souhrn prvků umožňující se účinně bránit proti kybernetickému útoku a zmírňovat nebo eliminovat jeho následky. [6]

Dopad

Vyjadřuje rozsah škody způsobené rizikem při narušení bezpečnosti informací. [4]

Opatření

Opatření můžeme definovat jako kroky, které upravují nebo zachovávají riziko. Například bezpečnostní politika riziko pouze zachovává, zatímco dodržování bezpečnostní politiky může riziko snižovat. [3]

Bezpečnostní politika

Je formální směřování organizace, které je dokumentované a odsouhlasené vrcholovým vedením organizace. [8]

Bezpečnostní politika je základním stavebním prvkem zabezpečení organizace. Musí být přiměřená záměrům organizace. Zahrnuje cíle, závazek ke splnění a dodržování aplikovaných požadavků týkajících se bezpečnosti. Tato pravidla v organizaci určují systém, kterým jsou chráněna všechna aktiva organizace. [2, 5]

Rozsah

Stanovuje a dokumentuje části organizace a části určené k implementaci týkající se bezpečnosti informací. Definuje rozsah a hranice na základě specifických potřeb organizace dle jejího uspořádání, organizační struktury, lokality, topologie, technologií a aktiv. [5]

Řízení přístupu

Zajištění omezeného fyzického i logického autorizovaného přístupu k aktivům oprávněným osobám na základě bezpečnostních požadavků vyplývajících z činnosti organizace a požadavků na bezpečnost informací. [3, 8]

Autentizace

„Zaručuje, že prohlašovaná charakteristika entity je správná.“ [8]

Autenticita

Vlastnost vyjadřující, že entita je tím, za co se vydává. [6]

Autorizace

Uděluje práva k přístupům jednotlivých aktiv organizace na základě stanovení práv osobám nebo procesů. [4]

Proces

Soubor aktivit se vzájemným vztahem nebo vzájemně na sebe působících, který přeměňuje vstupy na výstupy. [8]

Neustálé zlepšování

Proces, kterým organizace zajišťuje neustálé zlepšování vhodnosti, přiměřenost a efektivnost systému řízení bezpečnosti informací. [2]

Koncová zařízení

„Hardwarové zařízení informačních a komunikačních technologií připojené k síti.“ [3]

UPS *„Nepřerušitelný zdroj napájení.“* [3]

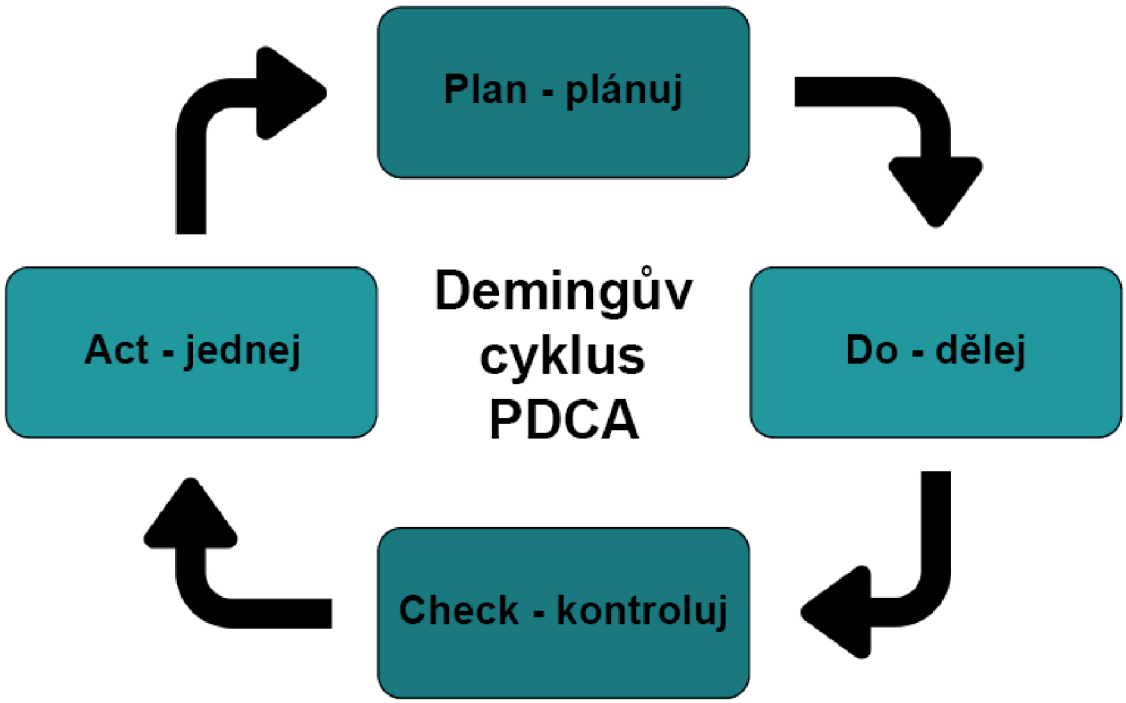
VPN *„Virtuální privátní síť.“* [3]

1.2 Demingův cyklus PDCA

Demingův cyklus nebo také PDCA model je jedním ze základních a osvědčených manažerských principů systému řízení a neustálého zlepšování procesů. Tento osvědčený model se skládá ze čtyř hlavních činností Plan, Do, Check a Act. [4]

- **Plan** (plánuj) – V této fázi dochází k definování cílů, kterých má být dosaženo a nutných procesů k jejich splnění. Jak mají být tyto cíle a procesy měřeny, vyhodnocovány a kdo za tyto cíle a procesy odpovídá. [4]
- **Do** (dělej) – Druhá fáze se zabývá realizací navržených cílů a procesů stanovených v první fázi a nastavení jejich sledování. [4]
- **Check** (kontroluj) – Zde dochází k vyhodnocování realizovaných cílů a procesů.
- **Act** (jednej) – V poslední fázi jsou na základě výsledků z předchozí fáze realizována nápravná opatření procesů, aby byly co nejefektivnější. [4]

Všechny fáze musí být řádně dokumentovány. Součástí dokumentace musí být identifikované procesy, jejich popis a dokumentace na základě nichž dochází k řízení a optimalizaci těchto procesů. [4]

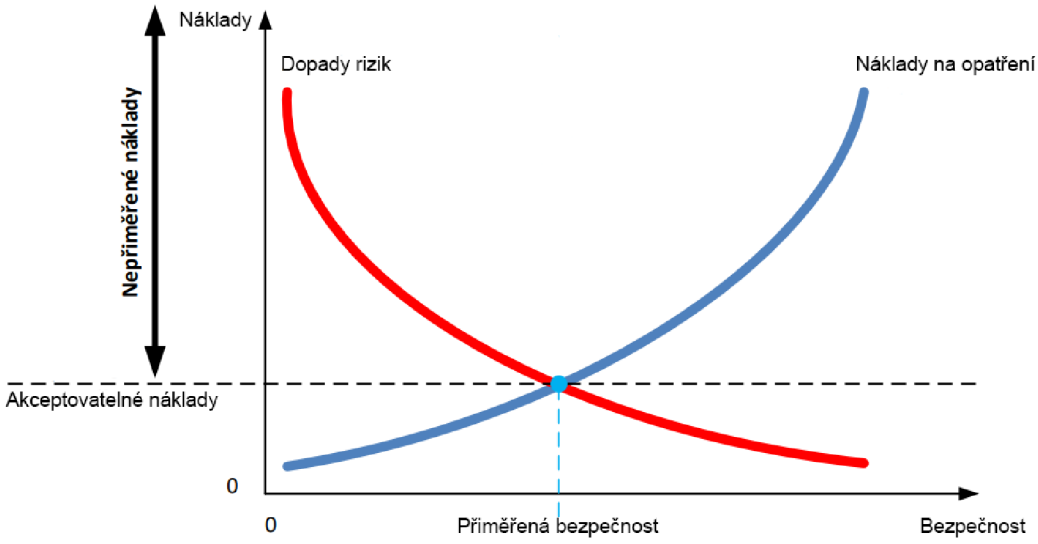


Obrázek 1 - Demingův cyklus PDCA [Vlastní zpracování dle zdroje 4]

1.3 Přiměřená bezpečnost

Úsilí vynaložené na zajištění bezpečnosti musí být přiměřené k hodnotě aktiv, které chrání a míře rizik, která mohou využít zranitelností těchto aktiv. Přiměřená bezpečnost se stanovuje na základě bezpečnostních politik zavedených ve společnosti. [5]

Je důležité zaměřit rozsah bezpečnosti tak, aby chránil nejen primární aktiva, ale i podpůrná aktiva jejichž ochrana je neméně důležitá pro zajištění bezpečnosti určeného systému. [9]



Obrázek 2 - Přiměřená bezpečnost [Vlastní zpracování dle zdroje 5 a 9]

1.4 Znalostní trojúhelník

Znalostní trojúhelník představuje obecný model, jak jsou definována data, informace a znalosti v kontextu bezpečnosti informací. Data si můžeme představit jako základ pro informace, ze kterých jsou následně získávány znalosti na základě vzdělání nebo zkušeností lidských zdrojů a organizace. [6]

Data

Data můžeme rozumět jako nezpracovaná čísla a fakta, která následně plní informace. Jsou vhodná ke zpracování, komunikaci a vyhodnocování. Můžou to být jména a čísla v tabulkách. [5,6]

Informace

Informace popisují stavy, reálné prostředí a procesy, které jsou zpracovány ve formě údajů. Jsou to data, která jsou strukturovaná, organizovaná a jsou uložena v dokumentech nebo jiných souborech. [5,6]

Informace také představují aktivum, které je pro organizaci zásadní a musí být chráněno. Jsou uchovány v mnoha formách, a to v digitálních, materiálních, nebo jako nevyjádřené znalosti lidských zdrojů a organizace. [8]

Z hlediska ochrany je můžeme dělit do skupin.

- **Důvěrná informace**

  Důvěrná informace je taková, která není určena k zpřístupnění nebo vyzrazení neoprávněným osobám. [3]

- **Citlivá informace**

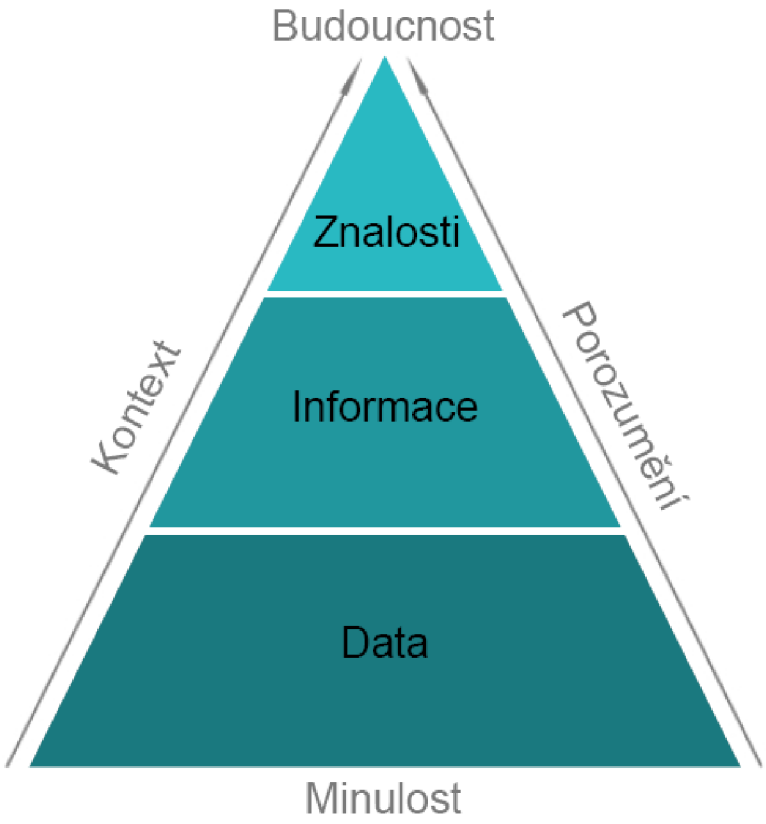
  Tyto informace by v případě nedostupností, neoprávněného přístupu, změny nebo zveřejnění měly nepříznivý dopad na jednotlivce nebo organizaci. [3]

- **Osobně identifikovatelné informace**

  Jsou informace, které mohou vytvářet spojení ať už přímo nebo nepřímo mezi informací a fyzickou osobou, které se tato informace týká. [3]

Znalosti

Znalosti jsou získané informace na základě pochopení, vzdělání nebo zkušeností jednotlivce či organizace. [6]



Obrázek 3 - Znalostní trojúhelník [Vlastní zpracování dle zdroje 6]

1.5 Bezpečnost informací

Bezpečnost informací je definována dle normy ČSN ISO/IEC 27001 jako *„zachování důvěrnosti, integrity a dostupnosti.“* K zajištění těchto tří aspektů a s tím souvisejícím zajištěním činností organizace s kontinuitou těchto činností a minimalizování vzniku incidentů a jejich dopadů je vyžadováno řízení bezpečnosti informací s řízením vhodných bezpečnostních opatření, zohledňujících rozsah hrozeb. [8]

Systém řízení bezpečnosti informací

Organizace stanoví, implementuje, udržuje a neustále zlepšuje systém řízení bezpečnosti informací v souladu s požadavky organizace a bezpečnostních politik. [2]

Správa a řízení bezpečnosti informací

„Systém, který řídí a kontroluje činnosti týkající se bezpečnosti informací organizace.“ [8]

1.5.1 CIA triáda

CIA triáda je jiný název pro bezpečnost informací a zaměřuje se na zajištění důvěrnosti, integrity a dostupnosti informací v organizaci z pohledu dostupnosti pro fyzickou, personální, procesní a komunikační bezpečnost. [5]

Integrita

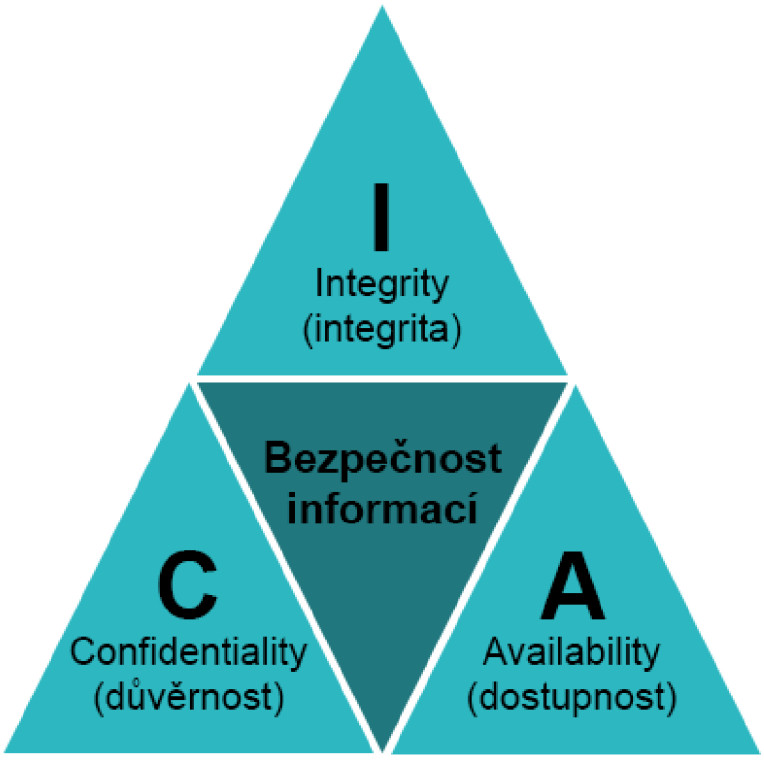
Stanovuje zajištění přesnosti, správnosti a úplnosti informace. [5, 8]

Dostupnost

Vyjadřuje přístup a použitelnost na žádost oprávněného uživatele v okamžiku potřeby dané informace. [8]

Důvěrnost

Důvěrnost je vlastnost informace, která zajišťuje, že není dostupná nebo není zpřístupněna neoprávněným jednotlivcům nebo procesům. [8]



Obrázek 4 - CIA triáda [Vlastní zpracování dle zdroje 17]

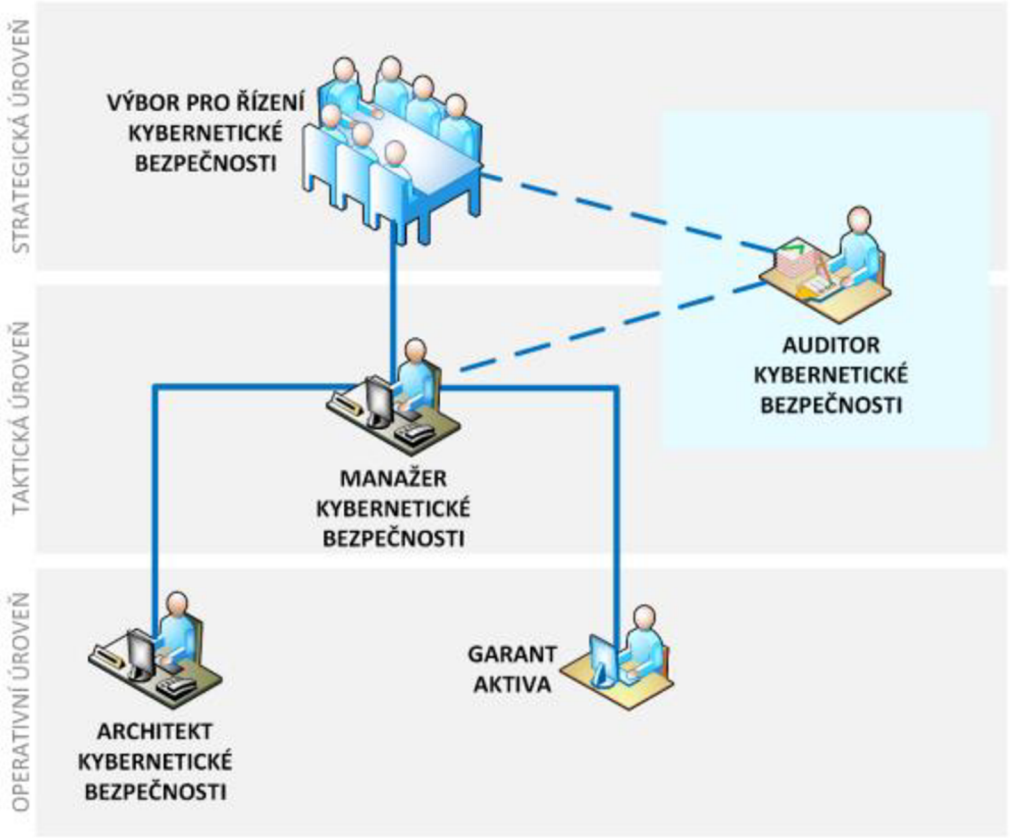
1.6 Bezpečnostní role

Kybernetická bezpečnost je součástí všech úrovní organizace a bezpečnostní role jsou zásadní pro zajišťování kybernetické bezpečnosti. Útvar kybernetické bezpečnosti by měl být přímo řízen vrcholovým vedením organizace a tento útvar musí být oddělen od útvaru zajišťujícího provoz ICT. [4, 18]

Výbor pro řízení kybernetické bezpečnosti

Výbor je organizovaná skupina skládající se z osob pověřených řízením a rozvojem systému řízení bezpečnosti informací a osob významně se podílejících na řízení a koordinaci činností spojených s kybernetickou bezpečností. Součástí výboru musí být podle vyhlášky o kybernetické bezpečnosti člen vrcholového vedení nebo jím pověřená osoba a manažer kybernetické bezpečnosti. [18]

Výbor je odpovědný za celkové řízení a rozvoj kybernetické bezpečnosti, tvorbu rámce KB, definování rolí, odpovědnosti, kontrolu aktuálního stavu a naplňování plánovaných cílů. [4]



Obrázek 5 - Výbor pro řízení kybernetické bezpečnosti [18]

Manažer kybernetické bezpečnosti

Bezpečnostní role definovaná zákonem o kybernetické bezpečnosti. Tato role je odpovědná za řízení a rozvoj systému řízení bezpečnosti informací. Musí být pro tuto činnost vyškolena a odborně způsobilá prokazatelnou praxí v řízení bezpečnosti minimálně po dobu tří let nebo jednoho roku v případě absolvování studia na vysoké škole. Role manažera kybernetické bezpečnosti musí být oddělena od rolí odpovědných za řízení ICT. [6, 18]

MKB je odpovědný za řízení systému řízení bezpečnosti informací, pravidelné informování a komunikování s vrcholovým vedením, vyhodnocování účinnosti a vhodnosti bezpečnostních opatření spolu s hodnocením aktiv a rizik. [4]

Architekt kybernetické bezpečnosti

Bezpečnostní role definovaná zákonem o kybernetické bezpečnosti zajišťující návrh a implementaci bezpečnostních opatření. Musí být pro tuto činnost vyškolena a musí prokázat odbornou způsobilost praxí s navrhováním bezpečnostní architektury nejméně po dobu tří let nebo jednoho roku, pokud absolvoval studium na vysoké škole. [18]

Je odpovědný za návrh implementace bezpečnostních opatření a zajišťování architektury bezpečnosti se zaměřením na bezpečnostní cíle. [4]

Auditor kybernetické bezpečnosti

Je osoba provádějící audit kybernetické bezpečnosti. Musí být pro tuto činnost vyškolena a musí prokázat odbornou způsobilost praxí s prováděním auditů kybernetické bezpečnosti nejméně po dobu tří let nebo jednoho roku, pokud absolvoval studium na vysoké škole. Auditor musí být nestranný a výkon této role musí být oddělen od ostatních bezpečnostních rolí. [18]

- **Audit**

  Je systematická, nezávislá a dokumentovaná činnost, která získává důkazy o činnostech kybernetické bezpečnosti, na niž je audit zaměřen a jejich objektivní vyhodnocení a určení rozsahu, v jakém jsou kritéria auditu splněna. [8]

- **Interní audit**

  Interní audit musí být prováděn v plánovaných intervalech a slouží k získání informací o tom, zda systém řízení bezpečnosti informací vyhovuje požadavkům organizace a je efektivně implementován a udržován. [2]

Garant aktiva

Garant aktiva je definovaná bezpečnostní role v souladu se zákonem o kybernetické bezpečnosti, představující fyzickou osobu pověřenou organizací zajišťující rozvoj, použití a bezpečnosti aktiva z pohledu zajištění důvěrnosti, dostupnosti a integrity ve spolupráci s osobami zastávající ostatní bezpečnostní role. [4, 6, 18]

1.7 Bezpečnostní povědomí

Povědomí

„Osoby pracující pro organizaci si musí být vědomy politiky bezpečnosti informací a důsledků nepřizpůsobení se požadavkům systému řízení bezpečnosti informací.“ [2]

Bezpečnostní povědomí je zásadním prvkem bezpečnosti. Je nutné prohlubovat informovanost o bezpečnostních hrozbách mezi zaměstnanci, stanovených bezpečnostních politikách a pravidlech v organizaci, kterými je nutné se řídit, aby byla zajištěna bezpečnost informací. [4]

Budování bezpečnostního povědomí SAE

Security-Awareness-Education je principem budování bezpečnostního povědomí. Tato metodika je podrobně rozebrána v normě NIST SP 800-16 a NIST SP 800-50. Metodika vychází ze čtyř hlavních vzdělávacích částí, a to povědomí, výcvik, vzdělávání a profesní rozvoj. Tyto hlavní části následně rozděluje uživatele podle obtížnosti do tří kategorií. Začátečník, středně pokročilí a pokročilí. [6]

Bezpečnostního povědomí je dosaženo systematickým plánováním s přesně specifikovanými oblastmi školení pro skupiny a jednotlivé uživatele. Matice SAE nám stanovuje a eviduje individuální plán školení pro jednotlivé uživatele. Za budování bezpečnostního povědomí musí být stanovena odpovědná osoba, a to buď manažer kybernetické bezpečnosti (MKB) nebo chief information security officer (CISO). [6]

1.8 Řízení kontinuity činností organizace

Řízení kontinuity činností je dokumentovaný proces, kterým organizace zajišťuje kontinuitu svých klíčových činností v případě neočekávaných situací. Tato neočekávaná situace může mít podobu kybernetické události, incidentu, technologických poruch nebo přírodních katastrof. Cílem řízení kontinuity činnosti je vytvoření postupů a prostředí pro minimalizaci dopadů těchto neočekávaných událostí a co možná nejrychlejší zajištění minimální úrovně služeb. [5, 6]

K efektivnímu řízení kontinuity činností je nutné identifikovat mimořádné události, které mohou způsobit výpadek činnosti organizace. Sestavit k nim plán obnovy po havárii (DRP) a stanovit postupné kroky tohoto plánu včetně odpovědných osob podílejících se na obnově, které musí vědět, jak mají postupovat, kdy tak mají postupovat, kde jsou dostupné zdroje potřebné k obnově a jak znovu dosáhnout kontinuity činnosti. [6]

Minimální úroveň služeb

Je stav, který znamená zajištění minimální úrovně služeb potřebných k dosažení kontinuity klíčových činností organizace. [6]

Plán obnovy po havárii

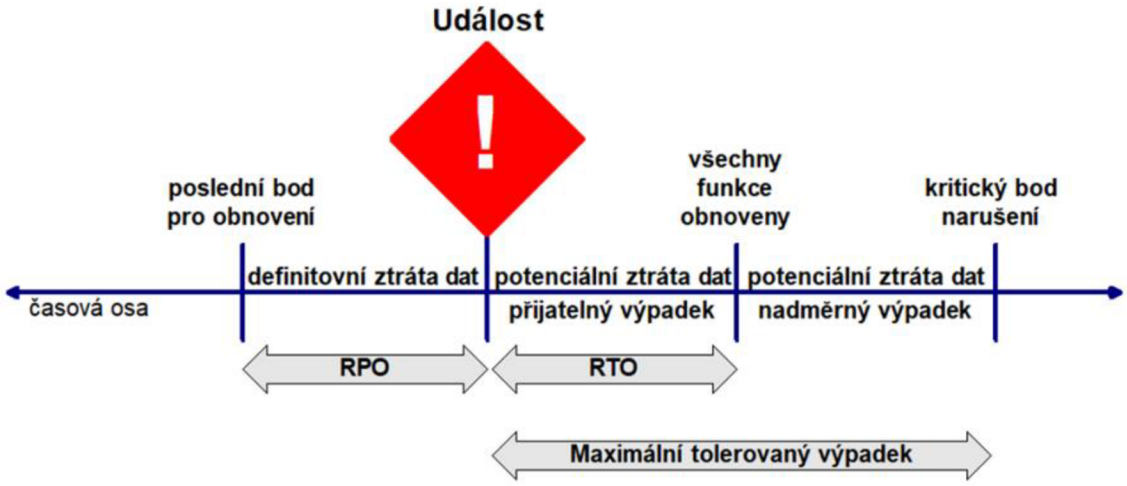
Plán obnovy po havárií je dokumentovaný postup, který je součástí plánu kontinuity činností. Předem stanovuje jasný scénář, který se využívá k obnovení klíčových činností s co nejrychlejší a nejvěrnější obnovou včetně správnosti celé obnovy po havárii provozu organizace, IS, infrastruktury a dat. [5, 6]

Cílový bod obnovy RPO

Je bod, který vyjadřuje stav obnovy dat a času, ke kterému je možné zpět data obnovit od výskytu mimořádné události. [3, 6]

Cílová doba obnovy RTO

Je definovaný úsek časového období po incidentu, který je potřebný k obnovení dat, IS a s tím související minimální úrovně služeb od výskytu mimořádné události. [3, 4, 6]



Obrázek 6 - RPO a RTO ve vztahu k události [6]

1.9 Normalizační instituce

1.9.1 NIST

National Institute for Srandards and Technology je vládní standardizační agentura Spojených států amerických, která vyvíjí a poskytuje standardy v oblastech měřících technik a technologií s cílem zvýšení efektivnosti, produktivity, usnadnění obchodu a zlepšení života. [5]

1.9.2 ISO

International Organization for Standardization je nezávislá mezinárodní organizace jejímž posláním je podporování rozvoje mezinárodní standardizačních norem v různých oblastech, které usnadňují mezinárodní směnu zboží a služeb. Díky publikování norem, které sjednocují postupy, tak umožňují mezinárodní spolupráci ve sféře intelektuálních, vědeckých, technologických a ekonomických aktivit. Standardy ISO zajišťují zlepšování kvality, efektivnosti a vzájemné spolupráce různých systémů. [4]

1.9.3 ENISA

European Union Network and Information Security Agency je agentura Evropské unie, která se zaměřuje na kybernetickou bezpečnost. ENISA úzce spolupracuje s členskými státy a se soukromým sektorem a poskytuje doporučení, podporuje při tvorbě

a implementaci národních politik a koordinuje vzdělávání, školení a sdílení informací o hrozbách a zranitelnostech. [6]

Pro Evropskou unii zajišťuje expertní znalosti a sekretariát komunity CSIRT týmů členských států, podporuje tvorbu národních bezpečnostních strategií, hlásí a koordinuje reakce na kybernetické bezpečnostní incidenty, určuje poskytovatele základních služeb, zajišťuje standardizaci a certifikaci v oblasti kybernetické bezpečnosti. [6]

1.9.4 NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost je gestor pověřený za vykonávání a řízení kybernetické bezpečnosti v České republice. Tento úřad zastává klíčové činnosti vyplývající ze zákona o kybernetické bezpečnosti. [4, 6]

Mezi jeho činnosti patří provoz Vládního CERT týmu České republiky, spolupráce s ostatními týmy CERT a CSIRT, příprava bezpečnostních standardů pro systémy regulované kybernetickým zákonem, podpora vzdělávání, osvěta, výzkum a vývoj v oblasti kybernetické bezpečnosti, ochrana utajovaných informací informačních a komunikačních systémů a kryptografická ochrana. [4, 6]

Bezpečnostní týmy

Náplní těchto bezpečnostních týmů je odpovědnost související s řešením bezpečnostních incidentů v rámci státu, odvětví, organizace nebo sítě. Zajišťují efektivní reakce na kybernetické bezpečnostní incidenty, prevenci a zvyšování povědomí, detekci, sledování a řešení bezpečnostních incidentů s jejich následným vyhodnocováním. [6]

- **CERT**

  Computer Emergency response team je tým profesionálů odpovědných za řešení kybernetických hrozeb a zranitelností. Navíc zveřejňuje svá zjištění a zkušenosti s veřejností, aby posílili bezpečnost infrastruktury. [6]

- **CSIRT**

  Computer Security Incident Response Team je skupina, která řeší bezpečnostní události a incidenty v počítačových sítích provozovaných na celém území ČR. [6]

1.10 Právní prostředí

Standard

Je dokument obsahující technické specifikace a přesně stanovená kritéria využívaná jako pravidla a směrnice zabezpečující, že služby, procesy, materiál a výrobky splňují takové parametry, jaké byly zamýšleny. [5]

Norma

Norma je definovaná jako doporučení pro daný standard nebo řešení. Může se jednat o doporučení použitelných standardů k realizaci požadovaného řešení. [5]

1.10.1 Zákon o kybernetické bezpečnosti

Zákon č.181/2017 Sb. o kybernetické bezpečnosti s účinností od 1. 1. 2015 podpořily závazky a požadavky plynoucí z mezinárodních společenství České republiky s NATO a Evropskou unií. [6]

Cílem kybernetického zákona bylo zajištění státní instituce odpovědné za zajišťování kybernetické bezpečnosti státu. Tato instituce je oprávněna k regulaci klíčových subjektů. Protože státní moc lze uplatňovat pouze v mezích zákona a ukládání povinnosti soukromoprávním subjektům je možné jen zákonem, musel takový zákon projít legislativním procesem, aby mohl regulovat a stanovovat povinnosti subjektů, kterými se musí řídit. [6]

Zákon také prošel několika legislativními úpravami, které zapříčinily vznik NÚKIB a zajištěním zvýšení kybernetické bezpečnosti, což rozšířilo dopad nejen na správce důležitých systémů, ale i na jejich provozovatele. [6]

1.10.2 Vyhláška o kybernetické bezpečnosti

Vyhláška o kybernetické bezpečnosti v celém znění Vyhláška č. 82/2018 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat. Obsahuje požadavky na organizační a technická opatření, jež musí být implementovány vybranými typy povinných subjektů. [6]

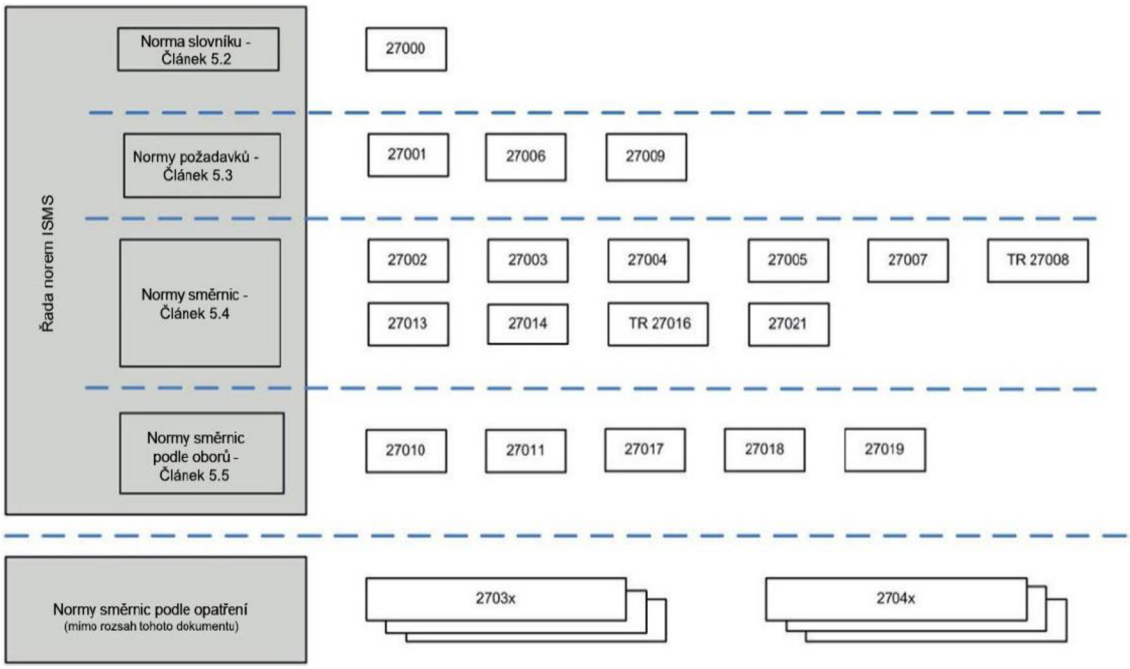
Tyto požadavky jsou založeny na základech mezinárodní normy ISO/IEC 21001 a definují požadavky v oblasti:

- Organizačních a technických opatření.
- Bezpečnostní politiky a bezpečnostní dokumentace.
- Hlášení kontaktních údajů.
- Hlášení kybernetických bezpečnostních incidentů.

[6]

1.10.3 Řada norem ISO/IEC 27000

Normy ISO a IEC řady 27000 tvoří souhrn podpůrných materiálů v oblasti systémů řízení bezpečnosti informací. Jsou složeny ze vzájemně souvisejících norem a obsahují celou řadu významných strukturálních popisů požadavků pro různou problematiku v této oblasti. [5, 8]



Obrázek 7 - Vztahy mezi normami ISMS [7]

ISO/IEC 27000

Tato norma poskytuje organizacím a jednotlivcům přehled řady norem 27000. Dále poskytuje úvod k systémům řízení bezpečnosti informací spolu se slovníkem obsahujícím použité termíny a jejich definic v této řadě norem. [8]

ISO/IEC 27001

Norma specifikuje požadavky na ustavení, implementování, provozování, monitorování, přezkoumávání, udržování a zlepšování formalizovaných systémů řízení bezpečnosti informací v souvislosti s celkovými riziky činnosti organizace. Specifikuje požadavky na implementaci opatření bezpečnosti informací přizpůsobených na základě potřeb organizace. [8]

ISO/IEC 27002

Norma poskytuje soubor obecně akceptovaných cílů opatření. Dále popisuje doporučené postupy, které slouží jako návod k implementaci opatření specifikovaných v normě ISO/IEC 27001. [5, 8]

ISO/IEC 27003

Tato norma poskytuje směrnici pro implementaci normy ISO/IEC 27001:2013. [6, 8]

ISO/IEC 27004

Dokument poskytuje směrnice, na základě nichž má být hodnocena výkonnost bezpečnosti informací a efektivnosti systémů řízení bezpečnosti informací podle požadavků normy ISO/IEC 27001. [8]

1.10.4 Minimální bezpečnostní standard

Minimální bezpečnostní standard je podpůrný materiál vytvořený NÚKIB pro subjekty, které nespadají pod zákon o kybernetické bezpečnosti. [1]

Obsahuje zjednodušené principy, postupy a doporučení v oblasti kybernetické bezpečnosti pro organizace, které nespadají pod regulaci zákona č. 181/2014 Sb., o kybernetické bezpečnosti. [1]

Zavedení kybernetické bezpečnosti podle MBS je doporučeno především tam, kde se s kybernetickou bezpečností teprve začíná, protože je zde ke kybernetické bezpečnosti přistupováno s návodným doporučením. MBS je členěn na dvě části, a to manažerskou část, která se zaměřuje na procesní oblast a jsou zde zahrnuty popisy postupů, které je nutné v rámci organizace zavést a dodržovat. Druhá část je zaměřena technicky a je určena primárně pro IT specialisty, kterým popisuje konkrétní návody, jak zajistit minimální úroveň zabezpečení. [1]

2 Analýza současného stavu

Z důvodu práce s interními informacemi společnosti je v této práci společnost anonymizována, aby nedošlo ke zneužití informací a zvýšení rizika hrozeb pro společnost. Kapitola obsahuje stručné představení společnosti. Její hlavní předmět podnikání a organizační strukturu. V následující části je představen hardware, software a síť. Následně je popsán současný stav dle minimálního bezpečnostního standardu a zhodnocení tohoto stavu.

2.1 Představení společnosti

Dlouholetá a prosperující společnost, na níž je vypracována tato diplomová práce, vznikla v roce 2001 pod prvotním názvem a s více společníky. V roce 2008 došlo k prodeji podílu společnosti a vlastníkem se stal jediný majitel. Následně došlo k přejmenování společnosti na současný název. Dále v roce 2017 došlo ke koupi a sdružení s další společností pod nově vzniklý holding. Společnost úspěšně zavedla a pravidelně obhajuje certifikát systému managementu kvality ČSN EN ISO 9001:2016 a certifikát systému environmentálního managementu ČSN EN ISO 14001:2016.

Hlavním předmětem podnikání společnosti je podle obchodního rejstříku výroba, obchod a služby neuvedené v přílohách 1 až 3 živnostenského zákona. Konkrétně společnost prodává příslušenství pro výpočetní techniku a nabízí pro ni i spotřební materiál do tiskáren a kopírek.

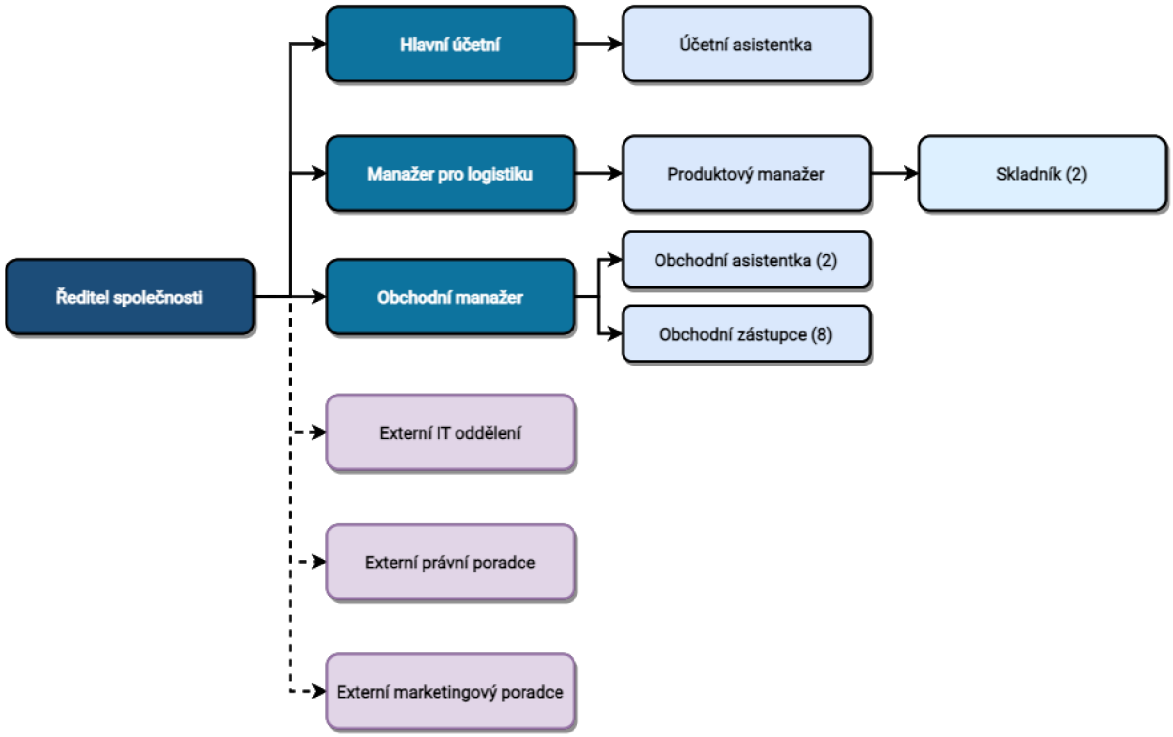
Produktové portfolio

- Výpočetní technika – servery, notebooky, počítače, tablety, mobilní telefony a datová uložiště.
- Komponenty pro výpočetní techniku – pevné disky, grafické karty, procesory, operační paměti, napájecí zdroje a flash disky.
- Příslušenství – tiskárny, skenery, velkoformátové tiskárny, kopírky, multifunkční tiskárny, monitory a periferní zařízení.
- Video a foto – televize, fotoaparáty, objektivy a kamery.
- Spotřební materiál pro tiskárny – papíry, inkousty a tonery v originálním, renovovaném a kompatibilním provedení.

2.1.1 Organizační struktura společnosti

Organizační hierarchie společnosti má jednoduchou liniovou strukturu. Liniová struktura udává, jaké jsou zde vztahy podřízenosti a nadřízenosti. V současné době pracuje ve společnosti osmnáct zaměstnanců. Společnost řídí ředitel, který má nejvyšší rozhodovací pravomoc. Obchodní oddělení řídí obchodní manažer a na oddělení pracují dvě obchodní asistentky spolu s osmi obchodními zástupci, kteří svými službami pokrývají všechny kraje České republiky. Hlavní náplní pracovní činnosti je získávání nových zákazníků a péče o stávající zákazníky. Manažer pro logistiku se stará o nákup zboží a řídí produktového manažera. Produktový manažer má zodpovědnost za správnost zboží v objednávce, předání balíků dopravci, reklamace zboží a řídí dva skladníky. Hlavní účetní s asistentkou se starají o účetnictví společnosti.

Společnost také využívá externích služeb, a to z oblasti správy IT, marketingu a právních služeb.



Obrázek 8 - Struktura společnosti [Vlastní zpracování]

2.2 Analýza ICT

V této části je představen hardware, software a síť společnosti, který je využíván pro pracovní činnosti zaměstnanců.

2.2.1 Hardware

Zaměstnanci společnosti využívají ke své práci převážně notebooky, aby jim v případě potřeby byla umožněna práce mimo kancelář, a to jak na pracovních cestách, tak i z domova. Pracovní stanice mají pouze pracovníci ve skladu a asistentka obchodního oddělení. Kanceláře jsou rozděleny podle oddělení a každý zaměstnanec má vlastní místo určené k pracovní činnosti. Na svém místě mají potřebné periferie k efektivní práci.

Většina níže uvedeného hardwaru je však starší než pět let.

Notebooky

Společnost využívá převážně produkty společnosti HP Inc. z důvodu dlouhodobé spolupráce s výrobcem a spokojeností s kvalitou jejich produktů. Modely, které jsou ve společnosti využívány zaměstnanci jsou HP ProBook 450 G6, HP EliteBook 840 G2, HP EliteBook 850 G3, HP EliteBook 855 G8, HP EliteBook 850 G5, HP EliteBook Folio 1040 G1, HP ProBook 640 G1, HP EliteBook 840 G5, HP ProBook 430 G6 a HP ZBook Firefly G8.

Obrázek 9 - Notebook HP ZBook Firefly G8 [10]

Dokovací stanice

Pro zjednodušení a snadné připojení notebooků k externím monitorům, periferiím a síťovému připojení jsou využívány dokovací stanice typu HP Thunderbolt Dock G2, HP UltraSlim Docking Station, HP USB-C Dock G5 a HP Docking Station HSTNN-I11X.

Obrázek 10 - Dokovací stanice HP Thunderbolt G4 [11]

Desktopy

Desktopy jsou využívány ve skladu a také obchodní asistentkou. K práci využívají modely jako HP Z230 Workstation a HP ProDesk 405 G4 Desktop Mini.

Obrázek 11 - Desktop HP ProDesk 405 G4 [12]

Telefony

Ke komunikaci využívá společnost digitální IP telefonní ústřednu Panasonic KX-NS500. K této telefonní ústředně je připojeno dvanáct telefonů, také od společnosti Panasonic, které jsou kompatibilní s ústřednou.

Tiskárny

Tiskárny jsou ve společnosti využívány pro tisk faktur, účetních dokladů, smluv, dodacích listů, svozových listů a dalších dokumentů, bez kterých se společnost neobejde. V budově se nachází celkem pět tiskáren, a to OKI MC853, HP Color LaserJetPro MFP M477fdw, HP Page Wide Pro MFP 477dw, HP LaserJet Pro 400 MFP a HP LaserJet P4014 s přídavným 5-ti přihrádkovým výstupním zásobníkem pro přehledné třídění dokumentů.

Obrázek 12 - Tiskárna HP Color LaserJet Pro M477fdw [13]

2.2.2 Software

Pro každodenní a efektivní naplnění pracovních povinností zaměstnanců je využívání softwaru, který jim usnadňuje jejich pracovní činnost. K využívání softwaru dochází napříč celou společností a zkvalitňuje komunikaci mezi zaměstnanci i přímo se zákazníky.

Windows 10 Pro

Na noteboocích i desktopech je nainstalován operační systém Windows 10 Pro. Verzi Pro společnost aplikovala z důvodu rozšířených funkcí, které základní verze operačního systému Windows neumožňuje využívat. Mezi hlavní funkci, které zaměstnanci potřebují pro svou práci patří Active Directory. Na základě této funkce se mohou zaměstnanci připojit k doméně společnosti a tím získají přístup k síti, tiskárnám a sdíleným souborům na datovém uložišti.

Pro správce sítě je důležitá funkce nastavení zásad skupin. Tím může rozdělit zaměstnance, spravovat jejich uživatelské účty a definovat přístupy v rámci sítě. Tato funkce napomáhá bezpečnosti a určuje přístupová práva uživatelů.

Microsoft Office

Balík aplikací od společnosti Microsoft přináší nepostradatelné aplikace, díky nimž zaměstnanci mohou efektivněji pracovat. Pro komunikaci ve společnosti i mimo ni je využíván MS Outlook. Pro vytváření a úpravu smluv je využíván MS Word a ke kalkulaci komplexních nabídek pro soutěžení veřejných zakázek slouží MS Excel.

Money S3

Tento účetní software je využíván pouze ředitelem společnosti, který zde zpracovává mzdovou agendu. Je to z toho důvodu, že hlavní informační systém, jež je ve společnosti využíván, tuto funkci nepodporuje.

Informační systém I6

Hlavní informační systém, který je ve společnosti používán k informačnímu zpracování procesů, poskytuje výrobce CYBERSOFT, s.r.o. formou služby. Tento IS společnost využívá již téměř dvacet let. Velký důraz společnosti je kladen na co největší automatizaci při importu a aktualizaci dat od svých dodavatelů. Pro efektivní nabízení

produktů potřebují obchodní zástupci aktuální data o dostupnosti a ceně produktů, které nabízejí. Tyto důležité funkce informační systém I6 zcela podporuje.

I6 je vyvíjen od roku 2000 a je vybudován na moderní technologii s využitím prostředků od Microsoftu. Jeho databáze využívá databázový Microsoft SQL Server k transakčnímu zpracování dat. Informační systém se řadí do kategorie Enterprise Resource Planning. [14]

Tento IS je společnosti poskytován formou pronájmu licencí. V současnosti je placeno za sedmnáct licencí pro připojení. Tyto licence jsou variabilní a umožňují přihlášení až sedmnácti uživatelů v jeden okamžik. To znamená, že IS může využívat více uživatelů, v jeden čas jich může být maximálně sedmnáct. K pronájmu jsou přidány měsíčně čtyři hodiny podpory typu HelpDesk a Hot line. V případě potřeby nadstandartních časových kapacit výrobce jsou služby účtovány zvlášť.

Kaspersky Endpoint Security

Společnost se snaží chránit své koncové zařízení a klade důraz na bezpečnost dat na zařízeních svých zaměstnanců. Z tohoto důvodu pořídila licence této bezpečnostní aplikace a přispěla tím ke snížení rizik, které na koncová zařízení mohou působit.

Kaspersky Endpoint Security pro Windows je vhodná ochrana pro všechny koncové stanice a data na těchto zařízeních. Ochrana je určena pro notebooky, stolní počítače i servery. Kaspersky je světově nejtestovanější a nejoceňovanější bezpečnostní aplikace k ochraně všech koncových zařízení s operačním systémem MS Windows. [16]

2.2.3 Síťová infrastruktura

Společnost před šesti lety změnila sídlo podnikání a před stěhováním bylo nutné přizpůsobit prostory tak, aby splňovaly všechny potřeby a požadavky společnosti. Díky tomu je infrastruktura vyhovující a má dostatečné rezervy pro případné rozšiřování.

O infrastrukturu, hardware, veškerou správu a zálohy se stará externí IT oddělení, které společnost využívá formou služby. Velkou výhodou je, že společnost pronajala poskytovali této služby místnosti přímo v budově, což umožňuje v případě potřeby okamžitou fyzickou komunikaci a spolupráci.

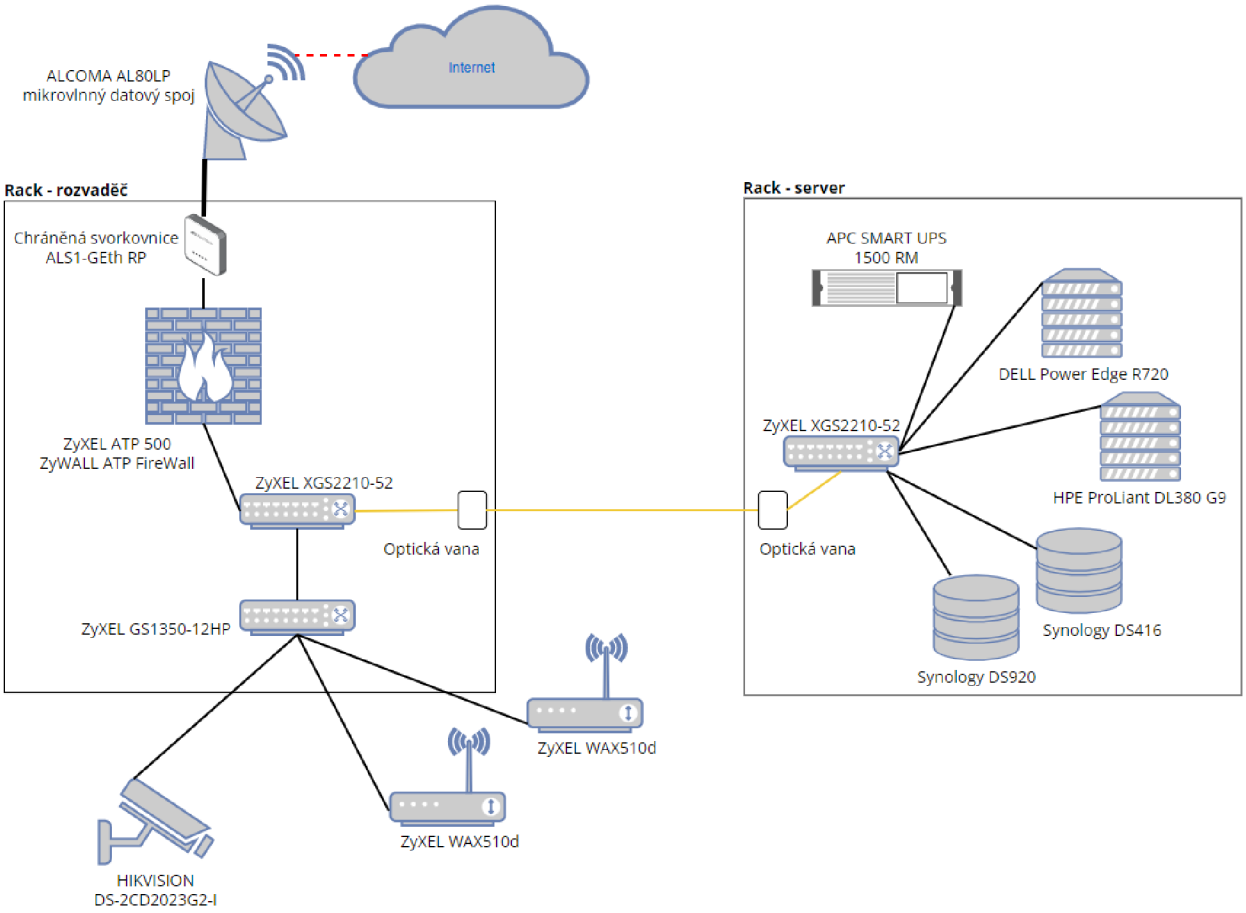
STARNET s.r.o. je poskytovatelem internetového připojení. Rychlost stahování a odesílání dat je až 500Mb/s. Toto připojení je do budovy přivedeno pomocí mikrovlnného datového spoje. Na střeše budovy je připevněna anténa ALCOMA AL80LP z níž vede signál po ethernetovém kabelu do chráněné svorkovnice ALS1-Geth RP a z ní přímo do firewallu.

ZyXEL ATP 500 ZyWALL ATP Firewall je součástí rodiny produktů ZyWALL, která získala certifikaci Common Criteria (CC) podle mezinárodního standardu pro certifikaci počítačové bezpečnosti a pro certifikaci kybernetické bezpečnosti. [15]

Dále jsou v infrastruktuře použity pro hlavní komunikaci switche ZyXEL XGS2210-52, které jsou propojeny pomocí SFP modulu s kabelem s optickým vláknem. Ten propojuje dva oddělené datové rozvaděče a vzniká tak páteřní sekce infrastruktury společnosti. Datové rozvaděče jsou odděleny z důvodu využití pasivního chlazení v chladnější části budovy společnosti, kde i při vyšších letních teplotách zůstává konstantně nižší teplota a není tak nutné pro datový rozvaděč se servery využívat klimatizovanou místnost.

ZyXEL GS1350-12HP slouží pro oddělení kamer HIKVISION DS-2CD2023G2-I, které monitorují okolí budovy a dvou přístupových bodů ZyXEL WAX510d, které umožňují bezdrátové připojení po celých vnitřních prostorech společnosti.

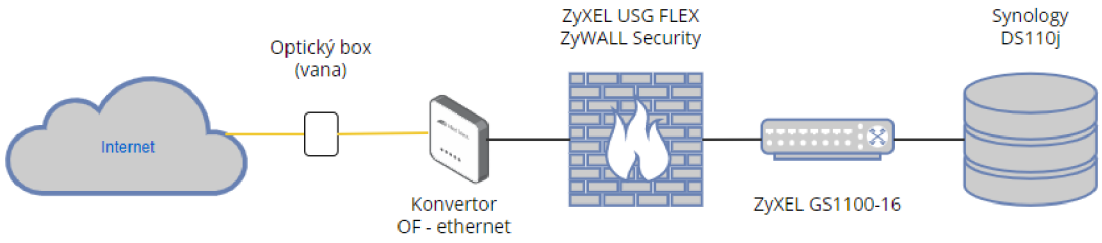
Datový rozvaděč se servery obsahuje dvě datové uložiště, a to Synology DS416, na které jsou ukládány soubory jako dokumenty a fotky společnosti. Druhé datové uložiště Synology DS920 slouží pro ukládání záloh. V tomto rozvaděči jsou také umístěny dva servery, a to DELL Power Edge R720, který je hlavním serverem a běží na něm informační systém, veškeré virtualizace a terminál server. Server HPE ProLiant DL380 G9 funguje jako replikační kopie serveru DELL. Je zde také záložní zdroj APC SMART UPS 1500 RM, který slouží jako ochrana napájení.



Obrázek 13 - Síťová infrastruktura společnosti [Vlastní zpracování]

Společnost má také vytvořenou druhou infrastrukturu mimo hlavní sídlo, která slouží jako druhé místo mimo budovu pro ukládání záloh.

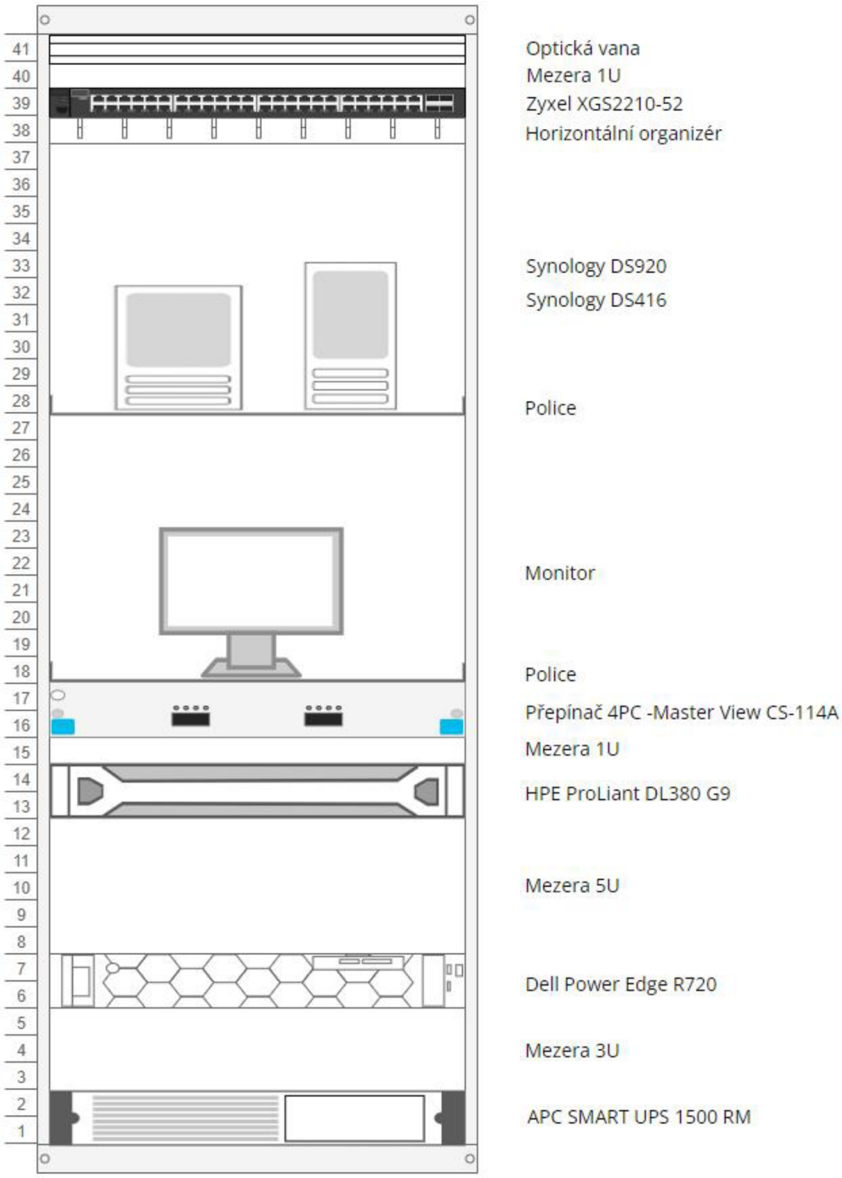
Můžeme vidět jednoduché zapojení, kde datové uložiště Synology DS110j je za firewallem ZyXEL USG FLEX ZyWALL Security a switchem ZyXEL GS1100-16.



Obrázek 14 - Síťová infrastruktura zálohy [Vlastní zpracování]

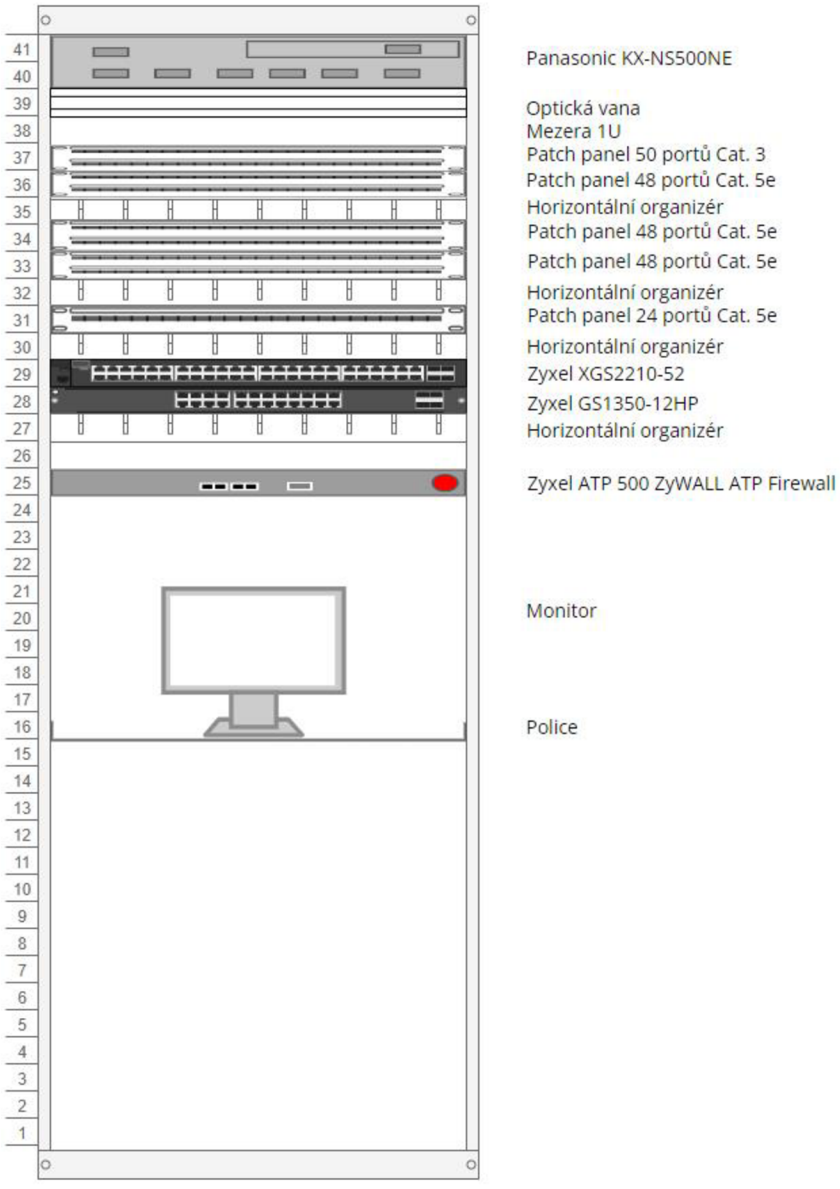
2.2.4 Serverovna a rozvaděče

Jak už bylo výše zmíněno, datové rozvaděče byly rozděleny na dva z důvodu využití pasivního chlazení v jiné části budovy. Na obrázku č. 15 je vykresleno sestavení datového rozvaděče se servery. Shora dolů můžeme vidět optickou vanu, ZyXEL XGS2210-52, horizontální organizér, datová uložiště Sylonogy DS920 a DS416 uložené na polici. Pod nimi je na druhé polici uložen monitor. Pod monitorem je přepínač Master View CS-114A, který umožňuje ovládat až 4 servery pomocí jediného monitoru, klávesnice a myši. Dále je zde hlavní server DELL Power Edge R720 a replikační kopie HPE ProLiant DL380 G9. Na spodu rozvaděče je záložní zdroj APC SMART UPS 1500 RM.



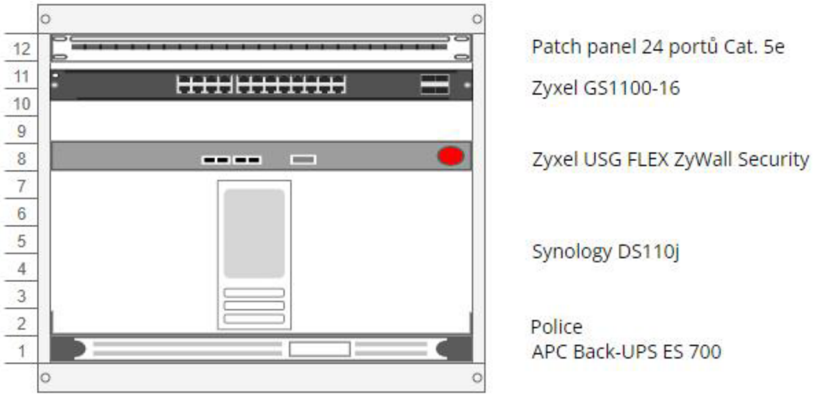
Obrázek 15 - Rack 1 serverový [Vlastní zpracování]

V druhém datovém rozvaděči můžeme vidět dle obrázku č. 16 jeho složení. Shora dolů je zde IP telefonní ústředna Panasonic KX-NS500, optická vana, dva patch panely. První patch panel je kategorie 3 a má 50 portů. Druhý patch panel je kategorie 5e a má 48 portů. Horizontální organizér, další dva patch panely, oba kategorie 5e se 48 porty. Horizontální organizér, patch panel kategorie 5e s 24 porty a znovu horizontální organizér. Pod nimi jsou dva switche a to ZyXEL XGS2210-50 a ZyXEL GS1350-12HP, poslední horizontální organizér a firewall ZyXEL ATP 500 ZyWALL ATP Firewall. Posledním vybavením rozvaděče je police s monitorem.



Obrázek 16 - Rack 2 rozváděcí [Vlastní zpracování]

Poslední datový rozvaděč je uložen mimo budovu sídla společnosti. Tento rozvaděč je malý a obsahuje pouze nejnutnější prvky. Na obrázku č. 17 můžeme vidět složení shora dolů, a to patch panel kategorie 5e s 24 porty, switch ZyXEL GS1100-16, firewall ZyXEL USG FLEX ZyWALL Security, polici s datovým uložištěm Synology DS 110j a záložní zdroj APC Back-UPS ES 700.



Obrázek 17 - Rack 3 zálohový [Vlastní zpracování]

2.2.5 Zálohování

Zálohování koncových zařízení zaměstnanců nejsou v tomto případě prováděna. Aby si zaměstnanci mohli nechat zálohovat své soubory, musí je nahrát na datové uložiště, na kterých mají vytvořené své vlastní adresáře, nebo tyto soubory nahrát do společných adresářů. Zálohování těchto adresářů na společném datovém uložišti je prováděno pravidelně jednou za týden a jsou vytvořeny dvě online kopie. Jedna uložená v sídle budovy a druhá mimo ni.

Dále dochází k záloze informačního systému, a to způsobem kompletní zálohy jednou týdně ve stejné formě dvou online kopií. Současně dochází k replikaci serveru na druhý server. Replikační kopie hlavního serveru DELL na replikační HPE. Toto je prováděno dvakrát denně. Obnova kompletní zálohy trvá zhruba čtyři hodiny a pokud je nutná rychlá obnova, nebo spíše přepnutí provozu na replikační server, může dojít k obnovení do patnácti minut. Tato obnova může být však ztrátová a je nutné počítat se ztrátou dat vytvořených v rozmezí posledních minut až čtyř hodin podle doby od uplynutí poslední replikace.

2.3 Manažerská část dle minimálního bezpečnostního standardu

První část minimálního bezpečnostního standardu (MBS) se zabývá manažerským pojetím kybernetické bezpečnosti. Zaměřuje se na procesy a postupy, které je nutné ve společnosti zavést, řídit se jimi a respektovat je.

2.3.1 Základní předpoklady

Cílem této části je vytvořit uspořádanou strategii, která bude směřovat ke zvýšení kybernetické bezpečnosti ve společnosti. K tomu je nutné získat plnou podporu vedení včetně potřebných zdrojů. Součástí této strategie je určení odpovědné osoby za tuto oblast a vytvoření bezpečnostních politik. [1]

Ředitel společnosti si je vědom závažnosti možných hrozeb, které na společnost mohou z vnějšího prostředí působit a ohrozit nebo omezit tak vnitřní procesy společnosti, čímž by mohlo dojít k finančním ztrátám, zhoršení jména společnosti nebo ztrátě zákazníka. Proto plně podporuje zavedení MBS ve společnosti.

Společnost nespadá mezi subjekty, kterých se týká zákon o kybernetické bezpečnosti, a proto v tomto směru nemá vybudované politiky, dokumentace a ani nedochází k pravidelnému auditu externím auditorem v oblasti bezpečnosti.

2.3.2 Klasifikace a ochrana informací

V této kapitole je stěžejní zjistit a rozdělit informace společnosti, které vlastní a vytváří. Následně všechny tyto informace budou přiděleny do skupin dle obsahu a jejich důležitosti a budou hodnoceny na základě důvěrnosti, integrity a dostupnosti. [1]

Ve společnosti v současné situaci není provedena identifikace s hodnocením informací a nejsou ani určeny pravidla, jak k těmto informacím přistupovat a chránit je před osobami, které by k nim neměli mít přístup.

2.3.3 Řízení dodavatelů

Cílem je eliminace možných problémů, které mohou vznikat při dodávání externích služeb. Dále upozorňuje na důležité části, které by měli být podchyceny ve smluvních podmínkách s hlavními dodavateli. [1]

Pro společnost je nejdůležitější dodavatel informačního systému, se kterým má sepsanou licenční smlouvu o užívání softwarového produktu. Ve smlouvě jsou uvedeny počty programových licencí, povinnosti společnosti pro přípravu infrastruktury, povinnosti autora o době pro odstranění závad a případných sankcí plynoucích z nedodržení smluvních podmínek.

Následujícím důležitým dodavatelem je externí IT oddělení, které má pronajato prostory přímo v sídle společnosti. S tímto dodavatelem nemá společnost sjednanou žádnou smlouvu o poskytování služeb a vše je řešeno formou ústní dohody. Tento formát funguje na základě téměř dvacetileté spolupráce s dodavatelem.

2.3.4 Řízení lidských zdrojů

Řízení lidských zdrojů souvisí se vzděláváním v oblasti kybernetické bezpečnosti a rozšíření povědomí mezi zaměstnanci. Součástí jsou pravidelná školení a seznámení s bezpečnostními politikami, a to nejen zaměstnanců, ale i dodavatelů externích služeb. [1]

Po přijetí nového zaměstnance a před nástupem na určenou pracovní pozici dochází k sepsání pracovní smlouvy, která obsahuje informace o pracovní pozici, náplň hlavní pracovní činnosti, určené místo pro výkon práce. Po sepsání smlouvy je zaměstnanci přiděleno pracoviště spolu s přidělením připravené výpočetní techniky nutné pro výkon činnosti a přidělení přístupů do sítě a informačního systému.

V případě, že dojde k ukončení pracovního poměru je tato výpočetní technika a veškeré přístupy odebrány.

Ve společnosti doposud nebyly stanoveny bezpečnostní politiky, a proto není možné je vyžadovat po zaměstnancích. Jednorázová ani pravidelná školení z oblasti bezpečnosti ve společnosti doposud neproběhla a zaměstnanci se o možných hrozbách dozvídají pouze formou informativních e-mailů, které zasílá ředitel společnosti nebo externí IT oddělením.

2.3.5 Řízení změn

Tato část MBS se zabývá změnami ve spojení informačního nebo komunikačního systému a kybernetickou bezpečností. Tyto změny by měly být systematicky řízeny, aby nedošlo k negativnímu ovlivnění funkčnosti. Veškeré změny by měly být dokumentovány, vyhodnocovány a schvalovány oprávněnou osobou. Mělo by být zajištěno také testování těchto změn a možnost návratu k původnímu stavu před změnou. [1]

Společnost se nachází v současnosti ve stabilním prostředí, jehož největší změnou v posledních letech bylo stěhování do nových prostor a s tím související přípravy pro nové funkční prostředí. Před stěhováním došlo k testování nových komponentů, funkčnosti sítě pomocí nahrání kompletní zálohy na novou infrastrukturu.

2.3.6 Řízení kontinuity činností

Jedná se o plány pro obnovu kontinuity činnosti společnosti po případném negativním vlivu. Mezi tyto vlivy patří živelné pohromy a kybernetické útoky. Součástí by měl být Business Continuity Plan (BCP), Disaster Recovery Plan (DRP) a havarijní plán. [1]

Ve společnosti tyto plány v souvislosti s informačním a komunikačním systémem a kybernetickou bezpečností nebyly vytvořeny a k haváriím je přistupováno intuitivně.

Poslední havárie, která ve společnosti nastala v listopadu 2022 byla způsobena lidským faktorem při pravidelné měsíční údržbě, kdy IT oddělení omylem smazalo síťový disk a došlo k výpadku informačního systému na čtyři hodiny. Jedenkrát nastalo selhání pevného disku, tato havárie však neovlivnila poskytování služby, protože jsou disky zrcadleny, čímž správné nastavení zabránilo výpadku. V minulosti také došlo k půl dennímu výpadku informačního systému z důvodu chybného upgradu I6. Tento výpadek nastal ze strany výrobce poskytovaného softwaru, který měl v nové verzi chybu.

2.3.7 Audit kybernetické bezpečnosti

Cílem auditu je nezávislá kontrola osoby mimo interní prostředí společnosti. Tento proces by měl být pravidelně prováděn, aby vyhodnocoval stav kybernetické bezpečnosti. [1]

Jelikož společnost nespadá pod subjekty, po kterých je tento audit vyžadován ze zákona, nebyly doposud tyto audity ve společnosti prováděny s využitím služeb třetích stran. O audit bezpečnosti se zde stará externí IT oddělení, které pravidelně kontroluje logy, zda nedošlo k nestandardním zápisům. Tímto způsobem však není zaručena nezávislost provedeného auditu.

2.4 Technická část dle minimálního bezpečnostního standardu

Druhá část MBS se zabývá technickým řešením a návody potřebnými pro splnění minimální kybernetické bezpečnosti.

2.4.1 Fyzická bezpečnost

Budovu můžeme rozdělit na tři části. V první části se nachází kancelářské prostory. V druhé části jsou skladové a manipulační prostory a poslední část je sklep, který je využíván jako úložný prostor společnosti.

Okolní pozemek i s budovou je majetkem holdingu, do kterého společnost spadá. Perimetr je oplocen a budova celý pozemek rozděluje na dvě části. Zadní část je přístupná z budovy, nebo přes elektrickou bránu, která je primárně zavřená a otevřít ji můžou jen zaměstnanci, kteří mají přístup k ovladači od brány. Přední část se vstupem na pozemek není volně přístupná mimo pracovní dobu a je chráněna elektrickou bránou vedle níž je i zamčená jednokřídlá branka. Za branou se nachází parkovací plocha pro osobní vozidla zaměstnanců, zákazníků a manipulační plocha pro přijímání a expedici zboží.

Vstup do budovy pro osoby mimo zaměstnance není volně možný, protože jsou všechny vchody opatřeny bezpečnostní pevnou koulí místo klik, a proto se nikdo bez klíče, nebo otevření dveří zevnitř, do budovy nedostane. V případě tailgatingu, kdy se neoprávněná osoba snaží proniknout do budovy zneužitím pomoci vzniklé z dobré víry zaměstnance, je spoléháno, že danou osobu zaměstnanec nenechá bez dozoru.

Okolí budovy společnosti je také monitorováno kamerovým systémem.

Fyzické zabezpečení infrastruktury je realizováno pro kabelové rozvody v podobě uložení do uzavřených kabelových žlabů. Datový rozvaděč bez serverů je otevřený a stojí v místnosti, která nemá okna, avšak přístup k němu není nijak omezen a prostor není klimatizován, to však není nutné, protože nedochází k přehřívání HW. Přístup k druhému

datovému rozvaděči se servery je omezen a do místnosti, ve které se nachází je nutné projít přes zamčené dveře a zároveň je rozvaděč uzavřený a zamčený. V tomto rozvaděči se také nachází záložní zdroj napájení UPS a místnost také není klimatizována, protože jsou servery chlazeny pasivně nižší a stabilní teplotou v místnosti.

2.4.2 Řízení přístupů

Ve společnosti není zaveden žádný evidenční docházkový systém či elektronická kontrola vstupu do budovy pro zaměstnance.

Zaměstnanci mají na svých noteboocích a počítačích vytvořené uživatelské účty, které nemají administrátorská oprávnění. Pro instalaci nových programů potřebují asistenci externího IT oddělení, které zhodnotí potřebu tohoto programu pro daného uživatele. Aby se zaměstnanci dostali k sdílenému datovému uložišti, musí být jejich zařízení a účet přidán do firemní domény, která současně určuje přístupová práva pro tyto uživatele. Tyto skupiny a jejich oprávnění nejsou nijak dokumentovány, jsou však správcem sítě nastaveny pomocí Active Directory na serveru.

Následně se musí zaměstnanci pro připojení do informačního systému prokázat jiným uživatelským jménem a heslem, než slouží k přístupu k zařízení a do domény společnosti. Probíhá zde tedy dvojí ověřování identity uživatele.

Administrátoři z externího IT oddělení mají přiděleny jak uživatelské, tak i administrátorské účty pro správu.

Na všech koncových zařízeních jsou také nainstalovány antiviry Kaspersky Endpoint Security for Windows, k nimž jsou zakoupeny licence, a které jsou pravidelně obnovovány, aby nepřišly o pokročilou úroveň ochrany.

Ve společnosti je zaveden v informačním systému princip need-to-know, který určuje jednotlivým zaměstnancům přístup ke konkrétním modulům v informačním systému. Výjimkou je pouze ředitel společnosti, který má přístup ke všem modulům. Ve společnosti nedochází k fluktuaci zaměstnanců či výměně pracovních pozic, a proto není nutné pravidelné přezkoumávání přístupových oprávnění.

Politiky hesel pro privilegované a uživatelské účty zde nejsou zavedeny a řídí se pouze pravidly danými registrací do aplikací. Změny hesel jsou pro uživatele možné, registrace do informačního systému však není otevřená a je nutné o tento přístup požádat správce.

Mobilní telefony, které zaměstnanci vlastní, jsou chráněny aplikací CyberWall poskytované mobilním operátorem Vodafone v rámci firemních tarifů.

2.4.3 Požadavky v oblasti ochrany před škodlivým kódem

Síť společnosti je rozdělena na více VLAN z důvodu bezpečnosti. Je vytvořena VLAN pro zařízení zaměstnanců, které jsou využívány ke každodenní pracovní činnosti a komunikaci koncových stanic s informačním systémem. Dále je vytvořena oddělená VLAN pro kamerový systém, WiFi a mobilní zařízení. Jako poslední je také vytvořena demilitarizovaná zóna (DMZ).

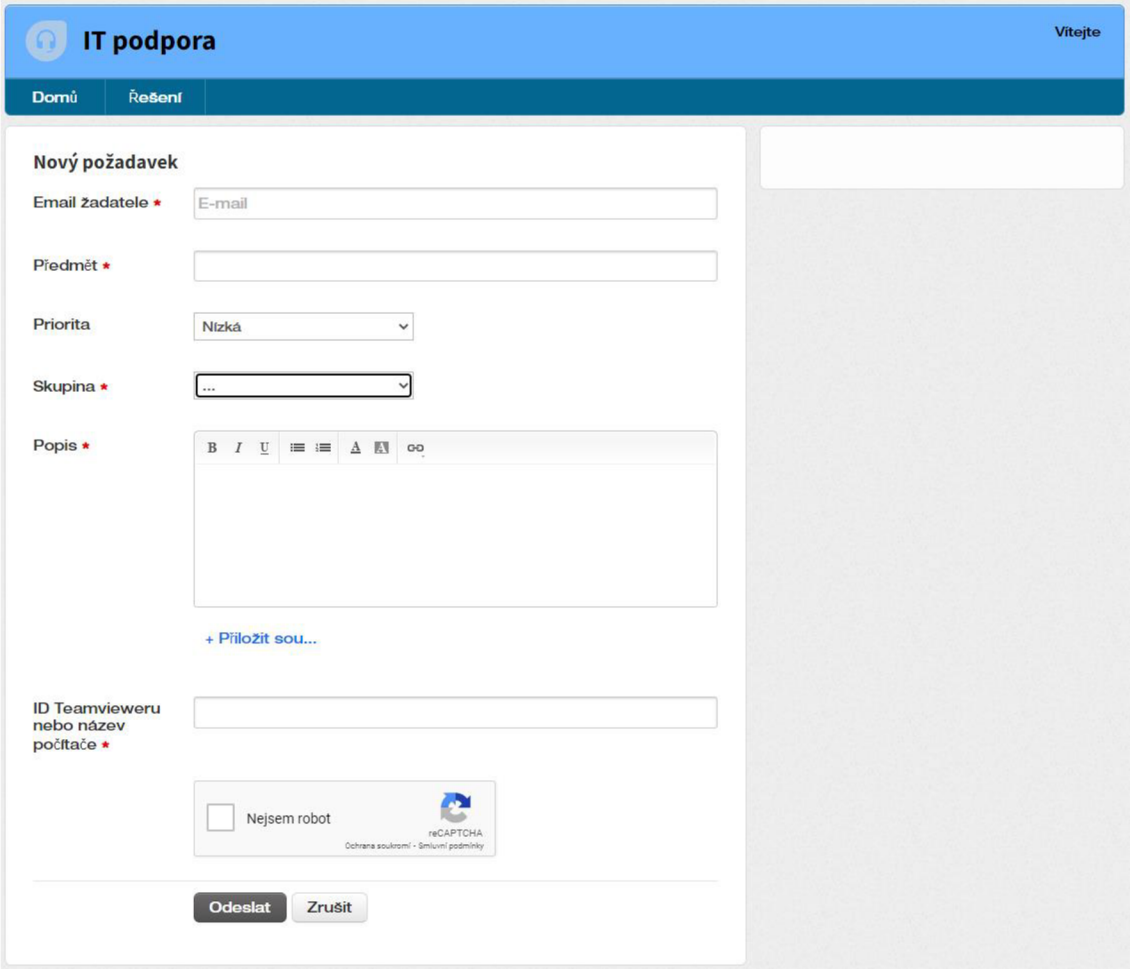
Software pro detekci škodlivého kódu je využíván na všech koncových stanicích, a to již zmíněný Kaspersky Endpoint Security for Windows. Pro mobilní zařízení je využívána aplikace CyberWall. K další ochraně internetové komunikace jsou využívány funkce firewallu a k ochraně před škodlivým kódem v emailu slouží Untangle Network Defender.

Veškerý software pro ochranu před škodlivým kódem je pravidelně aktualizován s vydáním nové verze.

V síti společnosti je také zakázán přístup na stránky, které nepodporují šifrovanou komunikaci protokolu HTTPS a jsou také blokovány stránky se zvýšeným výskytem rizika.

2.4.4 Kybernetické bezpečnostní události a incidenty

Postupy při vzniku nestandardní situace nejsou nijak stanoveny. Pokud k takové situaci dojde, zaměstnanci jdou přímo osobně kontaktovat správce sítě, aby se šel na vzniklý problém podívat. Pokud se správce sítě nevyskytuje v budově, zaměstnanci vše evidují na HelpDesk a až je správce přítomný, tak se problémem zabývá. Pro HelpDesk je vytvořen tiketový portál od Freshdesk Support Desk, ke kterému mají zaměstnanci vytvořené účty a můžou přidávat a prověřovat stav tiketů. U tiketu je možné vybrat konkrétní osobu, která se má požadavkem zabývat a nastavovat prioritu ve čtyřech úrovních a to nízká, střední, vysoká a naléhavá.



Obrázek 18 - HelpDesk tiket [Vlastní zpracování]

K vyřizování tiketů není sepsána smlouva o poskytování služby (SLA) a IT oddělení se snaží tikety vyřizovat co nejdříve dle svých časových možností a priority tiketu.

Provozní logy jsou uchovávány po dobu 6 týdnů a ke kontrole logů dochází pravidelně minimálně jednou za měsíc, zda se neobjevily žádné nestandardní situace.

2.4.5 Požadavky v oblasti aplikační bezpečnosti

Společnost nevyvíjí a netestuje žádné aplikace a touto oblastí se nijak nezabývá. Veškeré používané aplikace, které společnost využívá jsou aplikace zakoupeny od třetích stran. Je tedy předpokládáno, že tyto aplikace byly testovány a jsou způsobilé pro provoz.

2.4.6 Kryptografické prostředky

Ve společnosti je využíváno šifrování všech záloh algoritmem Advanced Encryption Standard (AES) s využitím délky klíčů 256 bitů. Přístup k těmto zálohám je chráněn

nastavenými oprávněními, které má pouze správce sítě a pro ostatní uživatele jsou tyto soubory skryty. Informační systém I6 využívá šifrovanou komunikaci přenosu dat. Zbylé datové přenosy v síti nejsou šifrovány.

Informační systém ukládá hesla, které jsou hashované. Jakým algoritmem však není možné dohledat.

2.4.7 Požadavky v oblasti zajišťování úrovně dostupnosti informací

Společnost nemá vypracován plán kontinuity činnosti a nejsou ani stanoveny požadavky na dostupnost. Ve společnosti nedochází k častým výpadkům informačního a komunikačního systému. Pokud k takové situaci dojde, jsou tyto problémy vyřešeny v řádu hodin. Incidenty, které v minulosti nastaly jsou zmíněny v kapitole 2.3.6 řízení přístupů. Společnost nevyrábí žádné produkty a takový výpadek je schopná dohnat nejpozději následující den po obnovení všech systémů a nevznikají jí tak žádné ztráty. Z tohoto důvodu není vysoká dostupnost systému pro společnost zásadní.

Dostupnost je však řešena pomocí RAID1, který zrcadlí data na více disků. V případě vypadnutí jednoho z disků nedojde k úplnému výpadku. Navíc je vytvořena na serveru HPE replikační kopie, která se nachází ve stejném datovém rozvaděči jako hlavní server DELL, a na který je možné přepnout provoz v řádu minut s částečnou ztrátou dat při vyšší poruše serveru DELL.

Single Point of Failure (SPOF) je tedy částečně řešeno pomocí replikačního serveru a RAID1.

Zálohy jsou ukládány ve formě dvou online kopií. Jedna kopie je uložena v sídle společnosti a druhá mimo sídlo. Offline zálohy společnost nevyužívá.

2.4.8 Požadavky v oblasti cloudových služeb

Společnost nevyužívá žádné cloudové služby z důvodů vysokých provozních nákladů a obavy ze ztráty obchodních informací.

Přístup mimo sídlo společnosti do informačního systému je zajištěn pomocí VPN s šifrovaným přenosem dat, které zajišťuje vlastní server společnosti.

2.4.9 Další požadavky

Výjimky běhu, chyby a hlášení

Výjimky nejsou udělovány a uživatelé mají přiděleny právo podle vytvořených skupin v Active Directory.

Ochrana informačního nebo komunikačního systému typu webové aplikace

Webové aplikace nejsou ve společnosti využívány. Všechny aplikace jsou nainstalovány přímo na koncových zařízeních zaměstnanců.

Rozvoj informačních a komunikačních systémů

Společnost využívá pouze aplikace třetích stran. Do informačního systému jsou nutné někdy přidat požadavky, které IS defaultně neumožňuje. Tyto požadavky jsou však konzultovány, vytvořeny a implementovány výrobcem IS, který funkčnost naprogramované funkce testuje před přidáním do IS společnosti. Tyto funkce jsou následně dokumentovány v HelpDesku výrobce.

Komunikace

Ke komunikaci ve společnosti i mimo ni je využíván Microsoft Outlook. Jeho komunikace však není nijak šifrovaná. Dále může být také využíván Skype ke komunikaci se zákazníkem a pro konferenční hovory Google Meet.

2.5 Zhodnocení současného stavu

Analýza současného stavu nám představila přehled oblasti informační a kybernetické bezpečnosti, která je ve společnosti aktuálně nastavena.

Bylo zjištěno, že ve společnosti nejsou vytvořeny žádné strategie, politiky ani dokumentace, které by zajišťovaly zlepšování bezpečnosti ve vybrané společnosti. Důležité však je, že ředitel společnosti si uvědomuje důležitost kybernetické bezpečnosti a zavedení bezpečnostních politik podporuje.

Není provedena identifikace a hodnocení informací a nejsou určena pravidla, jak k informacím ve společnosti přistupovat a chránit je.

Řízení dodavatelů informačního systému a externího IT oddělení, které se stará o infrastrukturu společnosti, není taktéž dokumentováno a jsou vytvořeny jen základní smluvní podmínky pro poskytování softwaru.

Nedochází k informování při příchodu nového zaměstnance ani k pravidelným školením zaměstnanců v oblasti informační a kybernetické bezpečnosti.

Nejsou vytvořeny plány pro kontinuitu činnosti a plán obnovy po havárii.

Fyzická bezpečnost ve společnosti je na dobré úrovni. K tomu přispívá, že společnost má ve svém vlastnictví sídlo a pozemek, který je chráněn proti neoprávněnému přístupu a je monitorován kamerovým systémem. Rozvaděče jsou vybaveny záložním zdrojem napájení UPS.

Řízení přístupu je centrálně nastaveno pomocí Active Directory. Koncová zařízení s informačním systémem jsou chráněna ověřováním identity a uživatelské účty musí být přiřazeny do domény. Přístupy ke koncovým zařízením a IS jsou odlišné a pro IS je zaveden princip need-to-know pro přístupy k různým modulům. Koncová zařízení jsou chráněna antivirem Kaspersky Endpoint Security for Windows. Není vytvořena politika pro minimální délku hesla u administrátorských a uživatelských účtů.

Segmentace sítě zvyšuje ochranu před škodlivým kódem a je implementováno více antivirových aplikací pro různé části infrastruktury s pravidelnou aktualizací. Kaspersky Endpoint Security for Windows, CyberWall, Bitdefender a Untangle Network Defender.

Nejsou písemně specifikovány postupy při vzniku nestandartních situací. Provozní logy jsou pravidelně kontrolovány a jsou uchovány po dobu šesti týdnů.

Zálohy jsou šifrovány algoritmem AES256 a přístup k zálohám je přidělen jen správci sítě. Informační systém využívá šifrovanou komunikaci přenosu dat a hesla jsou v něm ukládána hashované.

Dostupnost informačního systému je zajištěna replikační kopií serveru. K zabezpečení dat proti selhání pevného disku je využito zrcadlení RAID1. Je také částečně eliminován Single Point of Failure (SPOF). Zálohy jsou vytvářeny v podobě dvou online kopií na dvou různých místech. Chybí pouze offline kopie pro splnění principu 3-2-1.

Není vytvořena identifikace a hodnocení aktiva na primární a podpůrná.

Tabulka 1 - Zhodnocení současného stavu

Části	Stav
Základní předpoklady - strategie, politiky a dokumentace zvyšující bezpečnost	Nezavedeno
Klasifikace a ochrana informací	Nezavedeno
Řízení dodavatelů	Nezavedeno
Řízení lidských zdrojů - bezpečnostní školení	Nezavedeno
Řízení změn	Nezavedeno
Řízení kontinuity činností	Nezavedeno
Audit kybernetické bezpečnosti	Nezavedeno
Fyzická bezpečnost	Částečně zavedeno
Řízení přístupů	Částečně zavedeno
Ochrana před škodlivým kódem	Částečně zavedeno
Kybernetické bezpečnostní události a incidenty	Částečně zavedeno
Kryptografické prostředky	Částečně zavedeno
Zajišťování úrovně dostupnosti informací	Částečně zavedeno
Požadavky v oblasti cloudových služeb	Nezavedeno

3 Vlastní návrh řešení

V této části diplomové práce jsou navrhnuty konkrétní politiky, kterými se společnost musí řídit pro zajištění kybernetické bezpečnosti dle minimálního bezpečnostního standardu. Protože je každá organizace svými potřebami jedinečná, jsou tato doporučení uvedené v MBS upravována a nastavována na míru společnosti. Nejprve je uveden rozsah MBS, jsou identifikovány a hodnoceny aktiva společnosti, následně jsou sestaveny politiky z manažerské a technické části MBS a jejich ekonomické zhodnocení.

3.1 Rozsah MBS

Jelikož společnost, na níž je tato diplomová práce zpracována, se řadí do kategorie malého podniku podle počtu zaměstnanců a nespadá pod subjekty jež musí splňovat zákon o kybernetické bezpečnosti, bude rozsah stanoven na celou organizaci a v rámci ní budou řešeny pouze na vybrané části MBS dle stanovení požadavků ředitele společnosti.

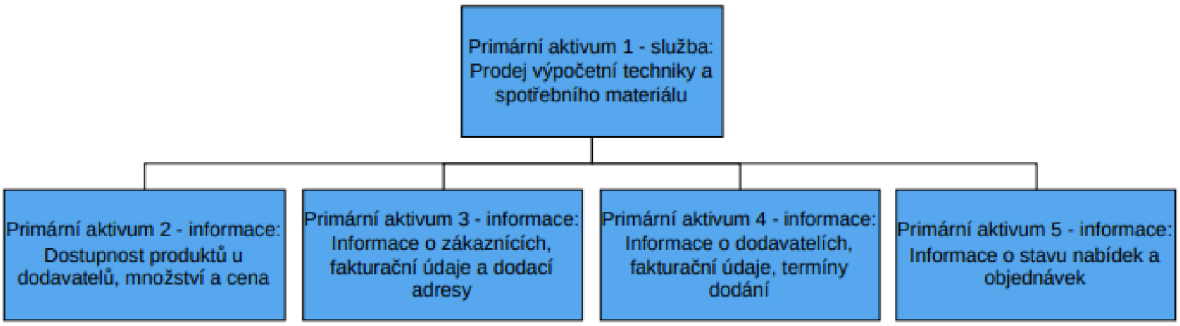
3.2 Identifikace a hodnocení aktiv

Pokud společnost nemá identifikována svá primární a podpůrná aktiva, není možné řídit jejich bezpečnost. Bez identifikace není možné rozhodnout, která aktiva jsou pro ni důležitá, jaké hrozby na ně mohou působit a jak tato aktiva chránit. Z toho důvodu budou v této části aktiva identifikována a bude k nim přidělen garant aktiva.

3.2.1 Identifikace aktiv

Primární aktiva

Primárním aktivem společnosti je služba prodej výpočetní techniky a spotřebního materiálu zákazníkům. K tomu jsou potřeba zásadní informace o prodávaných produktech, dodavatelích, zákaznících, nabídkách a objednávkách. Jelikož jsou tyto informace součástí primárního aktiva, jsou tedy také řazeny do kategorie primárních aktiv.



Obrázek 19 - Primární aktiva [Vlastní zpracování]

Níže je vytvořen katalog primárních aktiv. Každé primární aktivum má přiděleno ID, typ, kategorii a garanta aktiva.

Tabulka 2 - Katalog primárních aktiv [Vlastní zpracování]

ID	Typové primární aktivum	Kategorie	Garant aktiva
S1	Prodej výpočetní techniky a spotřebního materiálu	Služba	Ředitel společnosti
P1	Dostupnost produktů u dodavatelů, množství a cena	Informace	Manažer pro logistiku
P2	Informace o zákaznících, fakturační údaje a dodací adresy	Informace	Obchodní manažer
P3	Informace o dodavatelích, fakturační údaje, termíny dodání	Informace	Manažer pro logistiku
P4	Informace o stavu nabídek a objednávek	Informace	Manažer pro logistiku

Podpůrná aktiva

Podpůrná aktiva jsou aktiva, která zajišťují podporu primárním aktivům v podobě správné funkčnosti a bezpečnosti. Podpůrná aktiva nejsou pro společnost zásadní a jsou nahraditelná. Tato aktiva jsou rozdělena do kategorií technické vybavení (HW), komunikační prostředky, programové vybavení (SW), objekty, lidské zdroje, dodavatelé a externí systémy a služby. Kategorie se dále dělí na skupiny a typy podpůrných aktiv.

Tabulka 3 - Katalog podpůrných aktiv [Vlastní zpracování dle zdroje 7]

Kategorie podpůrného aktiva	Skupina podpůrného aktiva	Typové podpůrné aktivum
Technické vybavení (HW)	Pracovní stanice	Stolní počítače
	Mobilní zařízení	Notebooky
		Mobilní telefony
	Datová uložiště	Interní HDD
		Interní SSD
		Diskové pole (RAID1)
		NAS
	Periferie	Myš
		Monitor
		Klávesnice
		Multifunkční tiskárna
		Dokovací stanice
	Servery	Hlavní server
		Replikační server
Komunikační prostředky	Komunikační sítě	Pevné internetové připojení
		Bezdrátové internetové připojení
	Síťová zařízení	Switche
		HW firewall
	Strukturovaná kabeláž	Síťové a telefonní kabely
		Konektory
		Patch panel
		Zásuvka
		Propojovací kabely
Programové vybavení (SW)	Systémový SW	Operační systém
		Virtuální server
		Virtuální aplikační server
		Virtuální databázový server
		Virtuální proxy server
		Podpora funkcionalit IS
	Bezpečnostní SW	Antivir
		SW firewall
		Zálohovací SW
	Standardní SW	Kancelářské balíky
		Elektronická pošta
		Internetový prohlížeč
Objekty	Areály	Areál
	Budovy	Budova
	Místnosti	Místnost
	Vybavení	Vybavení
	Inženýrské sítě	Inženýrské sítě
Lidské zdroje	Management	Ředitel
	Uživatelé	Uživatel
	Administrátoři	Administrátor
Dodavatelé	Externí provozovatel	Externí provozovatel
	Výrobce	Výrobce HW
		Výrobce SW
		Výrobce komunikačních prostředků
Externí systémy a služby	Externí služba	Síťová konektivita
		Certifikační služby
		Digitalizace

3.2.2 Hodnocení primárních aktiv

Stupnice hodnocení

K hodnocení primárních aktiv musí být nejprve stanovena metodika, která popisuje jednotlivé úrovně ochrany dle tří kritérií CIA triády. Aktiva jsou hodnocena z pohledu důvěrnosti, integrity a dostupnosti.

Metodika rozděluje aktiva z hlediska významu do čtyř úrovní, a to na nízkou, střední, vysokou a kritickou. Pro každé kritérium a jejich všechny čtyři úrovně jsou stanoveny jednotlivé popisy hodnocení.

Tabulka 4 - Hodnocení aktiv [Vlastní zpracování dle zdroje 7]

Úroveň		Důvěrnost	Integrita	Dostupnost
1	Nízká	Aktiva jsou veřejně přístupná nebo byla určena ke zveřejnění. Narušení důvěrnosti aktiv neohrožuje oprávněné zájmy povinné osoby.	Aktivum nevyžaduje ochranu z hlediska integrity. Narušení integrity aktiva neohrožuje oprávněné zájmy povinné osoby.	Narušení dostupnosti aktiva není důležité a v případě výpadku je běžně tolerováno delší časové období pro nápravu (cca do 1 týdne).
2	Střední	Aktiva nejsou veřejně přístupná a tvoří know-how povinné osoby, ochrana aktiv není vyžadována žádným právním předpisem nebo smluvním ujednáním.	Aktivum může vyžadovat ochranu z hlediska integrity. Narušení integrity aktiva může vést k poškození oprávněných zájmů povinné osoby a může se projevit méně závažnými dopady na primární aktiva.	Narušení dostupnosti aktiva by nemělo překročit dobu pracovního dne, dlouhodobější výpadek vede k možnému ohrožení oprávněných zájmů povinné osoby.
3	Vysoká	Aktiva nejsou veřejně přístupná a jejich ochrana je vyžadována právními předpisy, jinými předpisy nebo smluvními ujednáními (například obchodní tajemství, osobní údaje).	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity aktiva vede k poškození oprávněných zájmů povinné osoby s podstatnými dopady na primární aktiva.	Narušení dostupnosti aktiva by nemělo překročit dobu několika hodin. Jakýkoli výpadek je nutné řešit neprodleně, protože vede k přímému ohrožení oprávněných zájmů povinné osoby. Aktiva jsou považována za velmi důležitá.
4	Kritická	Aktiva nejsou veřejně přístupná a vyžadují nadstandardní míru ochrany nad rámec předchozí kategorie (například strategické obchodní tajemství, zvláštní kategorie osobních údajů).	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity vede k velmi vážnému poškození oprávněných zájmů povinné osoby s přímými a velmi vážnými dopady na primární aktiva.	Narušení dostupnosti aktiva není přípustné, a i krátkodobá nedostupnost (v řádu několika minut) vede k vážnému ohrožení oprávněných zájmů povinné osoby. Aktiva jsou považována za kritická.

Primární aktiva

Hodnocení primárních aktiv z hlediska osobních údajů, zda jsou součástí určeného informačního systému a hodnocení dostupnosti, důvěrnosti a integrity.

Tabulka 5 - Hodnocení primárních aktiv [Vlastní zpracování]

ID	Typové primární aktivum	Kategorie	Garant aktiva	Osobní údaje	Určený IS	Dostupnost	Důvěrnost	Integrita
S1	Prodej výpočetní techniky a spotřebního materiálu	Služba	Ředitel společnosti	ANO	ANO	3	3	3
P1	Dostupnost produktů u dodavatelů, množství a cena	Informace	Manažer pro logistiku	NE	ANO	2	2	2
P2	Informace o zákaznících, fakturační údaje a dodací adresy	Informace	Obchodní manažer	ANO	ANO	3	3	3
P3	Informace o dodavatelích, fakturační údaje, termíny dodání	Informace	Manažer pro logistiku	ANO	ANO	3	3	3
P4	Informace o stavu nabídek a objednávek	Informace	Manažer pro logistiku	NE	ANO	3	2	3

3.3 Politiky manažerské části MBS

Politiky manažerské části dokumentují procesy a jejich postupy, které je nutné ve společnosti zavést a dodržovat pro zvýšení kybernetické bezpečnosti.

3.3.1 Definování významu klíčových slov

Před ponořením se do bezpečnostních politik je nutné si vyjasnit význam klíčových slov, která jsou použita v politikách, a jak silný důraz kladou tato slova na dodržování stanovených pravidel.

- MUSÍ – Přímé nařízení, které je nutné dodržovat bez jakýchkoliv výjimek.
- NESMÍ – Naprostý zákaz, který není možné z žádných důvodů porušit.
- MĚLY BY – Doporučené nařízení, které je možné za určitých situací obejít. V tomto případě však MUSÍ být nutně zvážena rizika, která mohou obejitím daného pravidla nastat.
- NEMĚLO BY – Doporučený zákaz, který je možné za určitých situací povolit. V tomto případě však MUSÍ být nutně zvážena rizika, která mohou povolením nastat.
- MŮŽE – Plně volitelné doporučení, které není sledováno ani vyžadováno v rámci společnosti.

3.3.2 Politika organizační bezpečnosti

Politika dokumentuje systematickou strategii vedení společnosti ke zvyšování kybernetické bezpečnosti. Součástí politiky organizační bezpečnosti je zavázání společnosti k vyčlenění potřebných zdrojů, a to jak finančních a technických, tak i lidských.

Vedení společnosti také stanoví bezpečnostní role, současně k nim přidělí jejich odpovědnosti, povinnosti a pravomoci a stanoví zastupitelnost těchto rolí. Tyto osoby budou mít k pracovní smlouvě přidánu smlouvu o zachování mlčenlivosti.

Dále se společnost zavazuje, že vytvoří přiměřené bezpečnostní politiky, jejich dokumentaci a bude dožadovat jejich dodržování a pravidelnou kontrolu. Tato dokumentace bude aktualizována v pravidelně stanovených intervalech, aby zaznamenávala aktuální stav ve společnosti.

Určení bezpečnostních rolí

Organizace MUSÍ určit výbor pro řízení kybernetické bezpečnosti. Tento výbor se MUSÍ skládat z člena vrcholového vedení a manažera kybernetické bezpečnosti.

V tomto případě se bude jednat přímo o ředitele společnosti. Vytvořením pozice manažera kybernetické bezpečnosti na plný pracovní poměr z hlediska velikosti organizace by došlo ke vzniku příliš vysokých nákladů a náplň této pracovní pozice by nebyla dostatečně využita z hlediska poměru mezi cenou a výkonem, proto bude tato pozice obsazena formou externí služby, kterou si společnost najme. Zastupitelnost role by měla být řešena v rámci poskytování služby, pokud tak nebude možné, stanoví ředitel společnosti zastupitelnost v rámci organizace.

MĚLY BY také být obsazeny role architekta a auditora kybernetické bezpečnosti. Na těchto rolích nebudeme však z hlediska velikosti organizace a omezených zdrojů v rámci politiky trvat.

Posledním členem výboru MŮŽE být zástupce externího IT oddělení, se kterým se budou konzultovat požadavky vzniklé ze strany manažera kybernetické bezpečnosti.

Všechny role zmíněné výše MUSÍ být striktně odděleny a NESMÍ být vykonávány jednou osobou.

Určení práv a povinností rolí

V tabulce č. 6 můžeme vidět rozdělení práv a povinností dle rolí. Každá role má přidělenu jednu nebo více povinností dle RACI matice, kde R je Responsible a role má fyzickou odpovědnost za daný proces. A znamená Accountable a role je odpovědná za vykonání procesu, tak jak byl nastaven. C je Consulted a s touto rolí je daný proces konzultován nebo se na procesu podílí, není však odpovědná za proces. I znamená Informed a role je o výstupu procesu informována.

Tabulka 6 - Práva a povinnosti rolí [Vlastní zpracování dle zdroje 1]

Procesy	Výbor KB	Bezpečnostní role		IT oddělení
		Manažer KB	Garant aktiva	
Celkové řízení a rozvoj KB	R,A	C,I	C,I	C,I
Systém řízení bezpečnosti informací	A,C,I	R	C,I	C,I
Návrh bezpečnostních opatření	C,I	A,C,I	C,I	R
Implementace bezpečnostních opatření	C,I	A,C,I	C,I	R
Zajištění rozvoje, použití a bezpečnosti aktiva	C,I	A,C,I	R	C,I

3.3.3 Politika řízení informací

Cílem politiky řízení informací je identifikace, hodnocení, evidence informací a aplikování přiměřené ochrany a přístupu k těmto informacím.

Identifikace informací a odpovědnosti

Pro co nejefektivnější využívání zdrojů určených k ochraně informací je důležité identifikovat informace společnosti a následně je rozdělit do skupin s podobnými potřebami na ochranu. Tím, že rozdělíme informace do skupin se stejnými požadavky na ochranu, můžeme snížit náklady vynaložené k ochraně, protože každá skupina podle její potřeby bude mít odlišný přístup a zabezpečení. K těmto skupinám je také nutné přiřadit garanta, který za danou skupinu informací odpovídá.

Tabulka 7 - Identifikace informací [Vlastní zpracování]

ID	Název	Popis	Garant
I1	Komunikace	Vybrané produkty, dotazy na produkty, poptávky ze strany zákazníků, emailová komunikace.	Obchodní zástupce
I2	Nabídky	Cenové nabídky produktů pro zákazníky ze segmentu B2B/B2G.	Obchodní zástupce
I3	Nabídky před zveřejněním	Nabídka do soutěžené zakázky před ukončením termínu výběrového řízení B2G případně B2B.	Ředitel společnosti
I4	Nabídky po zveřejnění	Nabídky po ukončení výběrového řízení, nabídky z vyhraného výběrové řízení B2G jež je nutné ze zákona zvěřejňovat.	Ředitel společnosti
I5	Objednávky	Finální objednávky potvrzené zákazníkem.	Obchodní zástupce
I6	Smlouvy	Můžou zde být smlouvy s výrobci, dodavateli a zákazníky.	Ředitel společnosti
I7	Dodací listy	Soupis dodávaného zboží v zásilce.	Manažer logistiky
I8	Účetní doklady	Faktury, mzdy, bankovní výpisy.	Hlavní účetní
I9	Interní dokumenty	Interní směrnice, smlouvy se zaměstnanci, strategie.	Ředitel společnosti

Hodnocení informací

K hodnocení informací musí být nejprve stanovena metodika, dle níž jsou informace hodnoceny na základě tří kritérií CIA triády. CIA triáda hodnotí informace dle důvěrnosti, integrity a dostupnosti. Z těchto tří hodnotících kritérií je vypočítána výsledná hodnota ochrany informací. Důvěrnost nám určuje, komu jsou tyto informace přístupné, zda jsou pro veřejnost, k potřebám uvnitř společnosti nebo jen vybraným osobám či nejvyššímu vedení. Integrita se vyznačuje kompletností a správností informací, kdy nedošlo k pozměnění informace ať už neoprávněnou osobou, přenosem nebo jinými vlivy. Dostupnost je stav, jež určuje, zda jsou informace dostupné v okamžiku, kdy je oprávněná osoba potřebuje využívat.

Metodika rozděluje informace z hlediska významu do tří úrovní, a to na nízkou, střední a vysokou. U každé úrovně je popsán význam všech tří kritérií, který přesně

stanovuje, jak by z hlediska významnosti mělo být k těmto informacím přistupováno. Metodika je popsána v tabulce č. 8.

Tabulka 8 - Metodika hodnocení informací [Vlastní zpracování dle zdroje 1]

Úroveň	Důvěrnost	Integrita	Dostupnost
1 - nízká	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 - střední	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 - vysoká	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.

Identifikované skupiny jsou ohodnoceny na základě vzniklé metodiky a významnost kritérií byla konzultována s garanty aktiv. Výsledná hodnota byla vytvořena na základě průměrné hodnoty hodnocených kritérií.

Tabulka 9 - Hodnocení informací [Vlastní zpracování]

ID	Název	Důvěrnost	Integrita	Dostupnost	Výsledná hodnota
I1	Komunikace	1	1	1	1 - nízká
I2	Nabídky	2	2	1	2 - střední
I3	Nabídky před zveřejněním	3	3	2	3 - vysoká
I4	Nabídky po zveřejnění	1	1	1	1 - nízká
I5	Objednávky	2	3	2	2 - střední
I6	Smlouvy	3	3	2	3 - vysoká
I7	Dodací listy	2	2	2	2 - střední
I8	Účetní doklady	3	3	2	3 - vysoká
I9	Interní dokumenty	2	2	2	2 - střední

K takto ohodnocené skupiny informací musí být chráněny a musí k nim být přistupováno podle výsledné hodnoty. Postup, jak tyto informace chránit a přistupovat k nim je popsán v tabulce č. 10.

Je popsáno, jak tyto dokumenty označovat v záhlaví a zápatí, kdo s těmito dokumenty může manipulovat a zda by měly být šifrovány. Pravidla jak budou tyto dokumenty likvidovány, zda bude vytvořena evidence změn a přiděleny práva na změnu a jak budou zálohovány.

Tabulka 10 - Ochrana informací dle výsledné hodnoty [Vlastní zpracování dle zdroje 1]

Úroveň	Důvěrnost	Manipulace	Likvidace	Změny	Zálohování
1 - nízká	Dokument MŮŽE mít na všech stranách v záhlaví označení VEŘEJNÉ.	Bez omezení.	Bez omezení.	MŮŽE být vytvořena evidence verzí.	MŮŽE být nastaveno zálohování podle individuální potřeby.
2 - střední	Dokument MUSÍ mít na všech stranách v záhlaví označení INTERNÍ.	Pro interní potřebu BY MĚL být omezen přístup k informacím osobám, které je nepotřebují k výkonu práce, MŮŽE být využito šifrování.	MUSÍ být zajištěno přepsání nosiče informací nebo jeho fyzická likvidace.	MUSÍ být zajištěna evidence verzí, MĚLO BY být nastaveno omezení práv na změnu.	MĚLO BY být nastaveno pravidelné zálohování podle individuální potřeby a pravidelná kontrola záloh.
3 - vysoká	Dokument MUSÍ mít na všech stranách v záhlaví i zápatí označení CITLIVÉ.	Dodržování principu need-to-know, MĚLO BY být přístupné pouze pro vybrané skupiny uživatelů, MUSÍ být využito šifrování, šíření BY MĚLO být schváleno garantem informace.	MUSÍ být zajištěno trvalé znehodnocení informace bez možnosti obnovy dle typu nosiče, nebo fyzická likvidace nosiče.	MUSÍ být zajištěna evidence verzí a auditní záznamy o změnách, MUSÍ být nastaveno omezení práv na změnu.	MUSÍ být nastaveno pravidelné zálohování podle individuální potřeby a pravidelná kontrola záloh.

Nabídky před zveřejněním, smlouvy a účetní doklady MUSÍ být označeny v záhlaví a zápatí jako CITLIVÉ, protože jsou v kategorii s nejvyšší ochranou. Nabídky, objednávky, dodací listy a interní dokumenty MUSÍ být označeny jako INTERNÍ a komunikace s nabídkami po zveřejnění, které mají nejnižší úroveň ochrany MŮŽOU být označeny jako VEŘEJNÉ, ale toto značení nebude přísně vyžadováno.

3.3.4 Politika řízení dodavatelů

Společnost využívá informační systém I6 od výrobce CYBERSOFT, s.r.o., který tento IS poskytuje téměř od vzniku společnosti. Je sepsána smlouva, která stanovuje autorství programového kódu a programové licence a zavazuje výrobce rozšiřovat software o funkce vyžadované zákony. Autorská práva pro funkce nad rámec základní části IS jsou majetkem společnosti a nemůžou být zahrnuta v základní části IS pro ostatní zákazníky výrobce. Výrobce se nepodílí na provozu IS a výhradně poskytuje pouze SW a poradenství při instalaci na vlastní hardware. Jelikož se výrobce přímo nepodílí na funkčnosti a nemá přístup k informačnímu systému, tak společnost nepokládá za důležité vytvořit politiku řízení dodavatelů.

Z těchto důvodů nebude ve společnosti tato politika řešena ani vytvořena. V případě změny nebo nutnosti potřeby bude tato politika vytvořena dodatečně.

3.3.5 Politika bezpečnosti lidských zdrojů

Politika popisuje požadavky na zvyšování bezpečnostního povědomí u zaměstnanců společnosti. Zajištění pravidelných i jednorázových školení a seznámení se zavedenými bezpečnostními politikami.

Pravidla rozvoje bezpečnostního povědomí

Společnost se zavazuje, že MUSÍ v pravidelných intervalech (minimálně jednou ročně) zajistit školení pro všechny zaměstnance a MUSÍ být kontrolováno jejich úspěšné dokončení. K tomu BY MĚL být minimálně využit veřejně přístupný kurz „DÁVEJ KYBER!“ dostupný na stránkách NÚKIB, nebo MUSÍ být zajištěno školení na dostatečně stejné úrovni v oblasti základů kybernetické bezpečnosti. Každý zaměstnanec MUSÍ prokázat úspěšné splnění školení vygenerovaným certifikátem, který je předložen manažerovi kybernetické bezpečnosti. Ten MUSÍ záznam o splnění školení zaevidovat a evidenci školení předá řediteli společnosti.

Společnost se dále zavazuje, že MUSÍ své zaměstnance proškolit na nově vydané bezpečnostní politiky. Seznámení s těmito politikami MŮŽE BÝT provedeno z hlediska velikosti společnosti na hromadném interním školení nebo pomocí zaslání nové bezpečnostní politiky na email každého zaměstnance. Následně MUSÍ být evidované seznámení každého zaměstnance s bezpečnostní politikou, které MUSÍ být potvrzeno podpisem zaměstnance o seznámení s politikou a možných důsledcích při porušení bezpečnostní politiky.

Součástí školení MUSÍ být i proškolení pro případ, kdyby došlo k nestandardnímu chování informačního nebo komunikačního systému.

Po vybraných pozicích ve společnosti MŮŽE BÝT vyžadováno nad rámec základního kurzu také pokročilý kurz pro manažery kybernetické bezpečnosti „ŠÉFUJ KYBER!“ veřejně dostupný na stránkách NÚKIB. Jeho splnění MUSÍ být také kontrolováno vygenerovaným certifikátem.

Při neúspěšném dokončení školení MUSÍ být opakováno, dokud zaměstnanec školení nesplní a MŮŽE dojít k odvození důsledků viz Pravidla řešení případů porušení bezpečnostní politiky.

Bezpečnostní školení nových zaměstnanců

Nový zaměstnanec projde všemi školeními jako stávající zaměstnanci. Na základě pracovní pozice MUSÍ projít školením všech současných bezpečnostních politik. Také MUSÍ projít online kurzem „DÁVEJ KYBER!“ a pokud to pozice vyžaduje MĚL BY být vyžadován i certifikát z „ŠÉFUJ KYBER!“ pro hlubší vědomosti z oblasti kybernetické bezpečnosti.

Stejně jako u stálých zaměstnanců MUSÍ být evidováno jejich úspěšné dokončení a u bezpečnostních politik MUSÍ být podepsáno, že byl nový zaměstnanec s těmito politikami seznámen.

Pravidla řešení případů porušení bezpečnostních politik

Pokud dojde k porušení vytvořených a schválených bezpečnostních politik, nebo zaměstnanec úspěšně nesplní bezpečnostní školení, MUSÍ být ústně nebo písemně napomenut.

Závažnost porušeného bezpečnostního pravidla MUSÍ zhodnotit manažer kybernetické bezpečnosti, který MUSÍ bezprostředně informovat o závažnosti ředitele společnosti. Ten po konzultaci s manažerem kybernetické bezpečnosti zhodnotí situaci a vyvodí patřičné důsledky.

Ředitel dle závažnosti MUSÍ udělit ústní nebo písemné napomenutí zaměstnanci a vyzvat ho přestudování dané bezpečnostní politiky, kterou zaměstnanec porušil.

Při opakovaném porušování bezpečnostních politik se ředitel MUSÍ řídit systémem třikrát a dost. Ředitel BY MĚL udělit maximálně dvě napomenutí a při třetím porušení bezpečnostních politik BY MĚL snížit měsíční bonusové ohodnocení. Tento systém může být dle závažnosti porušení bezpečnostní politiky upraven a MŮŽE dojít přímo po prvním porušení ke snížení měsíčního bonusového ohodnocení zaměstnance.

Pravidla pro ukončení pracovního vztahu nebo změnu pracovní pozice

Při rozvázání pracovního poměru MUSÍ být okamžitě zrušeny veškeré přístupy této osoby. MUSÍ dojít k oznámení v rámci společnosti, že konkrétní osoba již není zaměstnancem, a proto nemá žádný přístup ani pravomoci. MŮŽE být přesměrován email této osoby na jiného zaměstnance, aby nedošlo ke ztrátě komunikace ohledně záležitostí, které měla daná osoba na starosti.

Ve společnosti nedochází k zásadním změnám v rámci pracovních pozic. Pokud však k takové změně dojde, MUSÍ být zajištěna přístupová práva, která souvisejí s novou funkcí zaměstnance. MĚLO BY být také vyžadováno případné splnění školení související s nově vykonávanou funkcí zaměstnance.

Pravidla pro hlášení nestandardních situací

Zaměstnanec, který zjistí nestandardní chování informačního nebo komunikačního systému MUSÍ toto zjištění okamžitě nahlásit nejprve manažerovi kybernetické bezpečnosti, následně řediteli společnosti a IT oddělení, a to buď osobně nebo emailem.

Manažer kybernetické bezpečnosti MUSÍ zjištění nestandardní situace prošetřit ve spolupráci s IT oddělením MUSÍ udělat účinná opatření, aby bylo této situaci zabráněno.

O vzniklé nestandardní situaci MUSÍ být následně provedeno školení, ve kterém bude vysvětleno, jak této situaci v budoucnu předcházet, aby se neopakovala.

3.3.6 Politika řízení změn

Politika řízení změn zavádí systematický způsob, jakým budou řízeny změny v oblasti informačních a komunikačních systémech. Pro úspěšné řízení změn je nutné znát aktuální stav, ve kterém se společnost právě nachází, aby nedošlo k mylnému vnímání potřeby ke změně.

Veškeré změny MUSÍ být řádně dokumentovány, aby byl zaručen v každém okamžiku přesný stav, v jakém se aktuálně společnost nachází a jaký vliv by mohly mít další změny na bezpečnost. Současně s dokumentováním změny MUSÍ být zajištěno aktualizování souvisejících bezpečnostních politik.

MUSÍ být přijata přiměřená opatření zaručující snížení negativního vlivu, který by mohl vzniknout ve spojení s danou změnou.

Také BY MĚLO být zajištěno testování veškerých změn a v případě potřeby MŮŽE být provedeno penetrační testování.

MUSÍ být zajištěna možnost navrácení do původního stavu, který byl stabilní před zahájením procesu změny.

Pro úspěšné řízení změn MUSÍ být využit systematický model řízení. K tomuto MŮŽE být využit například Lewinův model řízené změny, nebo Kottlerův model osmi kroků.

3.3.7 Politika řízení kontinuity činností

Na základě vzniku mimořádné situace může dojít k omezení nebo úplnému zamezení využívání nejen informačních a komunikačních systémů, ale také lidských zdrojů a zázemí poskytovaného sídlem společnosti.

Tyto situace, které mohou různě působit na správný chod společnosti, je třeba efektivně řídit tak, aby došlo co možná nejrychleji k obnově do stavu, kdy je společnost schopna nadále provozovat své každodenní procesy související s hlavní pracovní náplní.

Z toho důvodu je nutné, aby osoby, již se vyskytnutá mimořádná situace týká, věděly, jak mají efektivně postupovat a jaké další osoby mají být do tohoto procesu obnovy zahrnuty.

K tomu MUSÍ být zaveden plán kontinuity činnosti, který obsahuje konkrétní plány obnovy po havárií.

Osoby podílející se na obnově

Při vzniku mimořádné situace MUSÍ dojít neprodleně k informování zaměstnancem, který mimořádnou situaci identifikoval. Tento zaměstnanec MUSÍ informovat manažera kybernetické bezpečnosti, IT oddělení a ředitele společnosti. K okamžité komunikaci MUSÍ dojít osobně nebo telefonicky a následně MUSÍ být mimořádná situace zaznamenaná tiketem v HelpDesku.

MKB MUSÍ vzniklou situaci vyhodnotit a MUSÍ postupovat podle vytvořeného plánu obnovy pro vzniklou havárii. Všechny osoby, které se podílejí na plánu obnovy MUSÍ mít přesně stanoveny práva a povinnosti, proto co mají při mimořádné situaci dělat.

Po vyřešení mimořádné situace MUSÍ IT oddělení zaznamenat k tiketu řešení, aby se v budoucnu v případě výskytu stejné nebo podobné situace mohlo využít postupu řešení.

Identifikované scénáře

- **Nedostupnost energií**

  V případě výpadku elektrické energie je poskytovaná služba nedostupná, dokud dodavatel znovu neobnoví své dodávky. Záložní zdroj UPS slouží pouze k bezpečnému vypnutí hardwaru a minimalizaci datových ztrát. Využití elektrocentrály je pro společnost ekonomicky nevýhodné.

  V případě výpadku dodávek plynu může společnost v zimních měsících vytápět kancelářské prostory nainstalovanou klimatizací.

- **Nedostupnost budovy**

  Jelikož je budova ve vlastnictví holdingu, který současně vlastní i společnost, je tento scénář vysoce nepravděpodobný a muselo by například dojít k silnému požáru, který by poničil budovu způsobem, na základě něhož by statik zakázal vstup do budovy. S tím by pravděpodobně došlo i ke zničení veškerého HW vybavení a společnost by tak nebyla schopna v krátké době obnovit svou činnost.

  Při nedostupnosti budovy a splnění podmínky zachování funkčnosti informačního a komunikačního systému, je možné převážnou většinu pracovních pozic vykonávat na dálku za pomoci vzdáleného a bezpečného připojení přes VPN.

- **Nedostupnost internetového připojení**

  V případě výpadku internetového připojení je služba částečně omezena. Zákazníci nemohou komunikovat s obchodními zástupci skrze email. Pro vnitřní funkčnost společnosti však internetový výpadek nemá zásadní vliv a informační systém je stále dostupný všem zaměstnancům v sídle společnosti. Pro zaměstnance připojené pomocí vzdáleného přístupu je připojení nedostupné.

- **Nedostupnost serveru**

  V případě výpadku hlavního serveru a vyhodnocení situace, že v nejbližších hodinách nedojde k obnovení provozu hlavního serveru, a tento výpadek nastal v pracovní době, MUSÍ BÝT provoz přesunut na replikační server.

- **Nedostupnost lidských zdrojů**

  Při příchodu nové pandemie, jako byla v posledních letech COVID-19, MUSÍ být znovu zavedena zvýšená hygienická opatření a MUSÍ být minimalizován počet nutných osob pro provoz v sídle společnosti.

Pokud bude zaměstnanec, který pro výkon práce musí být v budově a je nepostradatelný při poskytování služby a jeho práci je nutné zastávat pro poskytování služby, MUSÍ být tato pracovní pozice zastoupena jiným zaměstnancem, kterého určí ředitel společnosti po dobu jeho pracovní neschopnosti, ať už z důvodu krátkodobé nebo dlouhodobé nemoci, tak případné karantény.

Stanovení cíle řízení kontinuity činnosti

Pro efektivní řízení kontinuity činnosti je důležité stanovit hlavní části, které jsou pro společnost zásadní k poskytování služby.

- **Minimální nutná úroveň pro zachování poskytované služby**

  Pro zachování minimální úrovně poskytované služby MUSÍ společnost zajistit dostupnost informačního a komunikačního systému, jehož součástí je server a infrastruktura.

- **Doba obnovení chodu**

  Pokud dojde k chybě HW na serveru, je provoz možné obnovit do půl hodiny od selhání díky replikačnímu serveru. V tomto případě při rychlém obnovení chodu však může dojít k částečné ztrátě dat, které vznikly od poslední replikace. Při nutné výměně části HW, který je součástí infrastruktury a nelze jinak nahradit, je doba obnovy do 24 hodin, protože společnost nedrží náhradní HW skladem a je nutné jej objednat u dodavatelů. Doba obnovy do 24 hodin je reálná pouze v pracovní dny. V případě víkendu se doba obnovy úměrně prodlužuje.

- **Bod obnovení dat**

  Obnovení dat ze zálohy bylo v tomto roce testováno a kompletní obnova dat ze zálohy, která je přístupná v sídle společnosti, trvá čtyři hodiny. Pokud dojde i ke ztrátě zálohy v sídle společnosti, je čas pro obnovu dat prodloužen o hodinu, a tedy celkový čas obnovy se prodlouží na pět hodin. Tato hodina je přidána z důvodu obstarání zálohy mimo společnost, což spočívá ve fyzickém přivezení uložiště do sídla společnosti. Šifrování záloh je na úrovni klienta s využitím šifrovacího klíče. Z důvodu bezpečnosti jsou po celou dobu zálohy šifrovány. Po přemístění druhé zálohy do sídla společnosti, tak nehrozí nečitelnost dat z důvodu

změny HW konfigurace. Tento způsob je zvolen, protože obnova tak velkého množství dat by byla časově náročná a neefektivní při obnově zálohy přes internet.

Udržení minimální úrovně pro zachování poskytované služby

Pro zvýšení minimální úrovně nutné pro zachování poskytované služby BY MĚLA společnost pravidelně obnovovat hardware, a to ideálně vždy před skončením záruky výrobce. Tato doba se může u různých produktů lišit, a to od tří až do pěti let podle toho, zda byla zakoupena při pořízení HW také prodloužená záruka.

3.3.8 Politika řízení dokumentace

Jelikož bezpečnost není jednorázová záležitost, a pro co nejvyšší účinnost a postupné zvyšování je zásadní pravidelná kontrola, aktualizace a evidence současného stavu, je nutné veškeré bezpečnostní politiky udržovat aktuální.

Vzhledem k velikosti a stabilitě společnosti MUSÍ být provedena pravidelná kontrola minimálně jednou za dva roky anebo při každé provedené změně.

Tyto dokumenty MUSÍ být označeny v záhlaví a zápatí každé stránky jako CITLIVÉ a MUSÍ být uloženy v elektronické podobě s právy pro zápis určenými pouze pro manažera kybernetické bezpečnosti. Tyto dokumenty MUSÍ být přístupné také v tištěné formě u ředitele společnosti.

3.4 Politiky technické části dle MBS

Politiky technické části dokumentují konkrétní doporučené instrukce zajišťující minimální úroveň bezpečnosti.

3.4.1 Politika fyzické bezpečnosti

Fyzická bezpečnost snižuje možnost vzniku poškození, zneužití či krádeže všech aktiv společnosti, čímž by mohlo dojít k omezení nebo úplnému přerušení poskytované služby. Fyzickým bezpečnostním perimetrem je pozemek a budova sídla společnosti.

Pravidla pro ochranu objektu

Ochrana vnějšího perimetru je zajištěna vnější zadní elektronickou bránou, která MUSÍ být vždy zavřená. Pokud je její využití nutné, zaměstnanec si ji sám otevře a odpovídá i za její zavření po jejím využití. Přední brána je otevřená pouze v době pracovní

doby a poslední zaměstnanec, který opouští pozemek MUSÍ přední elektronickou bránu zavřít a před odchodem MUSÍ zkontrolovat, jestli je branka vedle brány zamknutá. Zda je zaměstnanec poslední, MUSÍ zjistit fyzickou kontrolou objektu.

Vnitřní perimetr je chráněn dveřmi s bezpečnostní koulí a každý zaměstnanec, který prochází MUSÍ za sebou dveře zabouchnout, aby nezůstaly otevřené, a to i v pracovní době. Poslední zaměstnanec, který opouští budovu MUSÍ vstupní dveře i zamknout.

Pro vizuální kontrolu nad vstupy a pohybu osob po pozemku společnosti MUSÍ být neustále zapnutý kamerový systém a záznam MŮŽE být pravidelně kontrolován.

Pravidla pro kontrolu vstupu osob

Volný vstup pro osoby mimo zaměstnance není možný, proto zaměstnanec, který otevře dveře a pustí osobu do budovy za ni MUSÍ nést zodpovědnost a NESMÍ ji nechat samotnou bez dozoru. Pokud jde osoba za jiným zaměstnancem, MUSÍ ji k tomuto zaměstnanci doprovodit a zodpovědnost za osobu v budově přebírá druhý zaměstnanec. Osoba se NESMÍ sama pohybovat po sídle společnosti a při opuštění budovy MUSÍ být doprovázena zaměstnancem, který je za ni zodpovědný, dokud se za ní nezavřou dveře. Vzhledem k velikosti společnosti a ojedinělým případům návštěv není zavedena žádná evidence.

Vstup zaměstnanců není nijak kontrolován ani evidován a každý zaměstnanec má vlastní klíč od budovy.

Pravidla pro ochranu zařízení

Hlavní datový rozvaděč se servery MUSÍ mít záložní napájení UPS, aby při náhlém přerušení dodávek elektrické energie nedošlo k poškození serveru.

Teplota v místnostech s datovými rozvaděči je aktuálně stabilně nízká a nedochází k přehřívání hardwaru. Pokud by se tato situace změnila, MUSÍ být zajištěno dostatečné chlazení. Aktivní chlazení MŮŽE být řešeno ventilací nebo klimatizací prostor.

MUSÍ být zajištěna bezpečnost datových rozvodů, aby nedošlo k neúmyslnému poškození. Tato ochrana MUSÍ být zajištěna uložením datových rozvodů do uzavřených kabelových žlabů.

Detekce narušení fyzické bezpečnosti

Pro případ vniknutí neoprávněné osoby do prostor společnosti MUSÍ být nainstalován zabezpečovací systém k ochraně majetku.

Aktiva je také třeba chránit před vznikem požáru. Z toho důvodu MUSÍ být v každé místnosti nainstalován detektor kouře.

3.4.2 Politika řízení přístupů

Na základě řízení přístupů jsou stanovena přístupová oprávnění všem uživatelům s jedinečným identifikátorem a rozdělení do skupin se stejnými přístupovými právy. Dále jsou určeny minimální požadavky na sílu hesel pro přístup do informačního systému a jak často se hesla mají měnit.

Nejprve MUSÍ být stanovena nutná pravidla pro přístupy a omezení práv k využívanému hardwaru a softwaru. Tato pravidla MUSÍ být evidována, dokumentována a upravována při nutnosti změny řízení přístupů.

Všichni uživatelé MUSÍ mít přiřazen jedinečný identifikátor, MUSÍ být stanovena práva dle principu need-to-know a MUSÍ být zařazeni do skupiny uživatelů s určenými přístupovými právy nutnými pro výkon jejich hlavní pracovní činnosti.

MUSÍ být stanoveny a rozděleny uživatelské i administrátorské účty podle potřeby. Správci sítě MUSÍ mít přístup k oběma typům účtů a MUSÍ JE používat podle nutnosti potřeby výše práv ke správě.

Přezkoumání řízení přístupu MUSÍ být prováděno minimálně jednou za dva roky, nebo v případě požadavku, změny pozice zaměstnance či s nástupem nového zaměstnance.

Správa účtů

Všechny účty MUSÍ být spravovány centrálně, a to jak pro přístup do sítě společnosti za využití domény a Active Directory, tak i pro informační systém. Pro připojení k informačnímu systému MUSÍ být vytvořeny jiné přihlašovací údaje (jméno a heslo), než pro připojení do domény.

Rušení účtů, vytváření nových a veškerá správa jednotlivých účtů a skupin MUSÍ být v pravomoci pouze IT oddělení po přímém schválení ředitelem společnosti a manažerem

kybernetické bezpečnosti. Před ukončením pracovního poměru MUSÍ být zrušeny veškeré přístupové účty daného zaměstnance, aby nedošlo ke zneužití informací.

Řízení privilegovaných účtů

Privilegované účty mají nastavenu vyšší ochranu než běžné uživatelské účty, protože mají stanovena vyšší práva a přístupy. Privilegované účty jsou vytvořeny pro správu sítě a jejich vlastníkem je IT oddělení. K informačnímu systému je vytvořen privilegovaný účet a vlastní jej ředitel společnosti. Toto řešení není v souladu s bezpečnostním doporučením a ředitel společnosti MUSÍ mít pro běžné používání vytvořen uživatelský účet. Privilegovaný účet mu MŮŽE být ponechán, ale NESMÍ jej využívat k běžné pracovní činnosti, ke které je plně dostačující uživatelský účet.

Politika hesel privilegovaných účtů MUSÍ splňovat doporučené parametry dle MBS, které jsou uvedeny níže a to:

- Minimální počet znaků v hesle MUSÍ být sedmnáct.
- Znaky v hesle MUSÍ být použity minimálně jedenkrát ze skupiny velkých písmen, malých písmen, číslic a speciálních znaků.
- NESMÍ být použito heslo, které bylo použito v minulosti (posledních dvanáct).
- Platnost nově vygenerovaného jednorázového hesla pro změnu NESMÍ přesáhnout dvacet čtyři hodin.
- Po třetím neúspěšném zadání hesla MUSÍ být účet uzamčen a IT oddělení MUSÍ vygenerovat nové jednorázové heslo, které si následně uživatel změní.
- Heslo MUSÍ být změněno každé čtyři měsíce navzdory doporučení MBS.

Řízení uživatelských účtů

Uživatelské účty je nutné rozdělit do skupin podle nutnosti přístupu. Uživatelské skupiny jsou rozděleny na obchodní oddělení, účetní oddělení, ředitele společnosti, logistiku dohromady s produktovým manažerem a sklad. Každá skupina má jak jiná oprávnění pro přístup na datové uložiště, tak i přístupné moduly v rámci informačního systému.

Politika hesel pro uživatelské účty také MUSÍ splňovat doporučené parametry dle MBS, které nejsou tak přísné a jsou uvedeny níže:

- Minimální počet znaků v hesle MUSÍ být deset.

- Znaky v hesle MUSÍ být použity minimálně jedenkrát ze skupiny velkých písmen, malých písmen, číslic a speciálních znaků.
- NESMÍ být použito heslo, které bylo použito v minulosti (posledních dvanáct).
- Platnost nově vygenerovaného jednorázového hesla pro změnu NESMÍ přesáhnout dvacet čtyři hodin.
- Po pátém neúspěšném zadání hesla MUSÍ být účet uzamčen a IT oddělení MUSÍ vygenerovat nové jednorázové heslo, které si následně uživatel změní.
- Heslo MUSÍ být změněno každý rok.

Řízení přístupu k HW a SW

Nové koncové zařízení, které je zaměstnanci přiděleno, nebo o něj požádá, MUSÍ být nejprve nastaveno IT oddělením, aby byla dodržena všechna bezpečnostní pravidla a politiky.

Na všech koncových zařízeních BY NEMĚLO být povoleno žádné instalování softwaru. Pokud je nutné nainstalovat SW, který není standardně přístupný na koncovém zařízení, MUSÍ instalaci provést IT oddělení, a to pouze po souhlasu manažera kybernetické bezpečnosti. Výjimkou MŮŽE být automatická aktualizace operačního systému a antiviru.

V sídle společnosti MUSÍ být všichni zaměstnanci připojeni síťovým kabelem. V případně nutnosti využití interní bezdrátové sítě MŮŽE být použita virtuální soukromá síť (VPN).

Hesla uložená v informačním systému I6 MUSÍ být chráněna hashovacím algoritmem s náhodně vygenerovanou solí. Algoritmus MUSÍ být použit dle doporučení NÚKIB pro hashovací algoritmy a sůl MUSÍ mít minimálně 64 bitů.

3.4.3 Politika zajišťování úrovně dostupnosti informací

Pro zajištění dostupnosti informací MUSÍ být využito zrcadlení pomocí RAID1 a MUSÍ docházet k replikaci hlavního serveru dvakrát denně.

V rámci zálohování MUSÍ být uplatněno pravidlo 3-2-1. To znamená, že MUSÍ být k dispozici tři kopie zálohy na dvou typech médií a jedno z nich se MUSÍ nacházet mimo lokalitu umístění informačního systému.

Hlavní server MUSÍ být přírůstkově zálohován pravidelně každý den v čase 21:00. Tyto denní zálohy MUSÍ být uchovány po dobu jednoho měsíce. Navíc MUSÍ být kompletně zálohován pravidelně každý pátek v čase 22:00. Tyto týdenní zálohy MUSÍ být uchovány po dobu tří měsíců.

Všechny pevné disky, na kterých jsou uloženy zálohy MUSÍ být šifrovány algoritmem dle aktuálního doporučení NÚKIB pro šifrování disků. V současné době to MŮŽE být algoritmus Advanced Encryption Standard (AES) s délkou klíčů 256 bitů.

3.4.4 Politika řízení technických zranitelností

Pravidla pro omezení instalace programů byla stanovena v kapitole 3.4.2 řízení přístupů. Tato pravidla se týkají i opravných programových balíčků. Je také nutné zajistit testování a nasazení těchto opravných programových vybavení, aby nedošlo k výpadku, jako v případě chybného upgradu informačního systému I6.

Z tohoto důvodu MUSÍ být nejprve použita testovací kopie informačního systému, na kterém MUSÍ být veškeré upgrady testovány před nasazením na hlavní IS.

3.4.5 Politika bezpečného používání mobilních zařízení

Při připojování do sítě společnosti z veřejných sítí NESMÍ být použito podezřelé WiFi bez hesla. Pokud je WiFi připojení nezaheslované a není možné použít jiné, MUSÍ zaměstnanec využít vlastní hotspot z mobilního telefonu a využít mobilní data v rámci firemního tarifu.

Připojení do sítě společnosti zvenčí NESMÍ být umožněno jinak než za využití VPN.

3.4.6 Politika ochrany před škodlivým kódem

Komunikace mezi vnitřní a vnější sítí MUSÍ mít nastavena pravidla pro ochranu. Tato pravidla MUSÍ být nastavena na firewallu.

Servery MUSÍ mít nainstalovaný antivir a datová uložiště MUSÍ být chráněna udělením přístupů.

Koncová zařízení MUSÍ být chráněna antivirem, který umožňuje detekci a odstranění škodlivých programů. MUSÍ být zajištěna pravidelná aktualizace antiviru včetně databáze vzorků minimálně jedenkrát za den.

Síťové prostředí MŮŽE být segmentováno pomocí VLAN.

NESMÍ být v rámci společnosti povoleno používání makra v souborech Microsoftu a NESMÍ být stahovány, otevírány, instalovány ani testovány žádné programy, které nejsou potřebné k pracovní náplni.

3.5 Zhodnocení navrhovaného řešení

Byla vytvořena metodika pro hodnocení aktiv a následně byla provedena identifikace a hodnocení primárních aktiv.

Vytvořená politika organizační bezpečnosti dokumentuje strategii zajišťující zvyšování kybernetické bezpečnosti ve vybrané společnosti. Stanovuje role a povinnosti těchto rolí.

Byla vytvořena politika řízení informací, která stanovuje metodiku pro hodnocení. Dále byla provedena identifikace informací. Následně na základě vytvořené metodiky došlo k hodnocení informací, stanovení odpovědností a pravidel, jak k informacím přistupovat a chránit je.

Politika bezpečnosti lidských zdrojů stanovuje pravidla rozvoje bezpečnostního povědomí, pravidelná školení a následky porušení bezpečnostních politik.

Byla vytvořena politika řízení změn, dle níž společnost musí řídit změny informačních a komunikačních systémů.

Politika řízení kontinuity činností stanovuje povinnosti konkrétních osob a postupů v případě výskytu nestandardních situací dle plánu obnovy po havárii. Také určuje minimální úroveň pro zachování poskytované služby.

Byla vytvořena politika řízení dokumentace stanovující pravidelné kontroly bezpečnostních politik.

Fyzická bezpečnost stanovuje pravidla pro ochranu objektu, kontrolu vstupu osob, ochranu zařízení a detekci narušení fyzické bezpečnosti.

Vytvořená politika řízení přístupu zajišťuje nastavení práva uživatelů a skupin, správu účtů, řízení privilegovaných a uživatelských účtů včetně politiky hesel. Řídí také přístupy k hardware a softwaru.

Byla vytvořena politika zajišťování úrovně dostupnosti informací stanovující pravidla pro zrcadlení pevných disků, replikační server a zálohování.

Politika řízení technických zranitelností stanovuje pravidla pro testování upgradu informačního systému a zakazuje instalaci programů.

Vytvořená politika bezpečného používání mobilních zařízení stanovuje pravidla vzdáleného připojování.

Politika ochrany před škodlivým kódem stanovuje pravidla pro ochranu komunikace mezi vnitřní a vnější sítí, ochranu serverů, datových uložišť a koncových zařízení.

Tabulka 11 - Zhodnocení navrhovaného řešení [Vlastní zpracování]

Části	Stav před	Stav po
Politika organizační bezpečnosti	Nezavedeno	Zavedeno
Politika řízení informací	Nezavedeno	Zavedeno
Politika řízení dodavatelů	Nezavedeno	Nezavedeno
Politika bezpečnosti lidských zdrojů	Nezavedeno	Zavedeno
Politika řízení změn	Nezavedeno	Zavedeno
Politika řízení kontinuity činností	Nezavedeno	Zavedeno
Politika řízení dokumentace	Nezavedeno	Zavedeno
Politika fyzické bezpečnosti	Částečně zavedeno	Zavedeno
Politika řízení přístupů	Částečně zavedeno	Zavedeno
Politika řízení technických zranitelností	Nezavedeno	Zavedeno
Politika bezpečného používání mobilních zařízení	Nezavedeno	Zavedeno
Politika ochrany před škodlivým kódem	Částečně zavedeno	Zavedeno
Kybernetické bezpečnostní události a incidenty	Částečně zavedeno	Částečně zavedeno
Kryptografické prostředky	Částečně zavedeno	Částečně zavedeno
Politika zajišťování úrovně dostupnosti informací	Částečně zavedeno	Zavedeno
Požadavky v oblasti cloudových služeb	Nezavedeno	Nezavedeno

3.6 Implementace bezpečnostních politik

Níže je shrnuta implementace bezpečnostních politik. Obrázek obsahuje bezpečnostní politiku, popis jednotlivých částí, které je nutné splnit pro úspěšné implementování bezpečnostní politiky, odhadovanou dobu trvání a odpovědnou osobu. Celková doba odhadovaná k implementaci všech bezpečnostních politik je 43 týdnů.

Tabulka 12 - Plán implementace [Vlastní zpracování]

Plán implementace			
Bezpečnostní politika	**Popis částí**	**Odhadovaná doba**	**Odpovědná osoba**
Politika organizační bezpečnosti	Vypsání výběrového řízení na službu manažera kybernetické bezpečnosti	4 týdny	Ředitel společnosti
	Výběr manažera kybernetické bezpečnosti	4 týdny	Ředitel společnosti
	Seznámení ředitele, MKB a IT oddělení s politikou	2 týdny	Ředitel společnosti
Politika řízení informací	Seznámení všech s politikou	2 týdny	MKB
Politika bezpečnosti lidských zdrojů	Seznámení všech s politikou	2 týdny	MKB
	Splnění kurzu „DÁVEJ KYBER!“	2 týdny	MKB
	Bezpečnostní školení	1 den	MKB
Politika řízení změn	Seznámení všech s politikou	2 týdny	MKB
Politika řízení kontinuity činností	Seznámení všech s politikou	2 týdny	MKB
	Vypracování plánů obnovy po havárii	2 týdny	IT oddělení
Politika řízení dokumentace	Seznámení všech s politikou	2 týdny	MKB
Politika fyzické bezpečnosti	Seznámení všech s politikou	2 týdny	MKB
	Instalace zabezpečovacího systému	4 týdny	Ředitel společnosti
Politika řízení přístupů	Seznámení všech s politikou	2 týdny	MKB
	Přezkoumání práv všech účtů a vytvoření dokumentace	2 týdny	IT oddělení
	Nastavení politiky hesel	1 týden	IT oddělení
Politika řízení technických zranitelností	Seznámení IT oddělení s politikou	2 týdny	MKB
Politika bezpečného používání mobilních zařízení	Seznámení IT oddělení s politikou	2 týdny	MKB
Politika zajišťování úrovně dostupnosti informací	Seznámení všech s politikou	2 týdny	MKB
Politika ochrany před škodlivým kódem	Seznámení všech s politikou	2 týdny	MKB

3.7 Ekonomické zhodnocení

Pro úplné zavedení výše vytvořených bezpečnostních politik, je nutné splnit všechny uvedené části. Některé části bezpečnostních politik nejsou zavedeny a musí být pro jejich úspěšné zavedení vynaloženy finanční zdroje, které budou níže rozděleny na jednorázové počáteční náklady a každoročně se opakující náklady.

Pro splnění politiky organizační bezpečnosti je nutné obsadit formou služby pozici Manažer kybernetické bezpečnosti. Hodinová sazba manažera kybernetické bezpečnosti je stanovena na 800 Kč, měsíční fond pracovní doby je stanoven na 16 hodin.

Pro zvyšování bezpečnostního povědomí zaměstnanců je nutné zajistit každoročně bezpečnostní školení z oblasti kybernetické bezpečnosti.

Tabulka 13 - Roční náklady [Vlastní zpracování]

Položka	Roční náklady
Externí manažer kybernetické bezpečnosti	153 600 Kč
Bezpečnostní školení	25 000 Kč
Celkové roční náklady	**178 600 Kč**

K politice řízení kontinuity činností jen nutné vypracovat plány pro obnovu po havárii. Pro splnění politiky fyzické bezpečnosti musí být nainstalován zabezpečovací systém, který bude obsahovat alarm, detekci pohybu a kouře. K politice řízení přístupů je potřeba přezkoumání stávajících práv privilegovaných a uživatelských účtů včetně nastavení politiky hesel.

Tabulka 14 - Jednorázové náklady [Vlastní zpracování]

Položka	Jednorázové náklady
Vypracování plánů obnovy po havárii	20 000 Kč
Instalace zabezpečovacího systému (alarm,detektor pohybu a kouře)	145 000 Kč
Přezkoumání práv privilegovaných a uživatelských účtů s vytvořením dokumentace	6 400 Kč
Nastavení politiky hesel privilegovaných a uživatelských účtů	4 000 Kč
Celkové jednorázové náklady	**175 400 Kč**

Celkové roční náklady jsou ve výši 178 600 Kč a celkové jednorázové náklady jsou stanoveny ve výši 175 400 Kč.

Závěr

Hlavním cílem diplomové práce bylo zavedení kybernetické bezpečnosti ve společnosti podle minimálního bezpečnostního standardu. Zvýšení úrovně kybernetické bezpečnosti a zvýšení bezpečnostního povědomí mezi zaměstnanci. Tohoto cíle bylo úspěšně dosaženo po analýze současného stavu společnosti a na základě této analýzy vytvořených bezpečnostních politik. Bezpečnostní politiky primárně vycházející z MBS, byly částečně upraveny tak, aby co nejvíce vyhovovaly potřebám společnosti a docházelo k co nejefektivnějšímu využívání finančních, lidských a technických zdrojů při zajišťování kybernetické bezpečnosti.

Analýza současného stavu nastínila aktuální stav kybernetické bezpečnosti, využívanou ICT infrastrukturu, hardwarové a softwarové vybavení, zálohování, fyzickou bezpečnost, řízení přístupů, ochranu před škodlivým kódem, hlášení bezpečnostních událostí a incidentů, kryptografické prostředky a zajišťování úrovně dostupnosti.

Ve vlastním návrhu řešení byly vybrány a zpracovány bezpečnostní politiky související s potřebami společnosti. Mezi zpracovanými politikami jsou politiky: organizační bezpečnosti, řízení informací, bezpečnosti lidských zdrojů, řízení změn, řízení kontinuity činností, řízení dokumentace, fyzická bezpečnost, řízení přístupů, zálohování a obnovy, řízení technických zranitelností a bezpečné používání mobilních zařízení. Na závěr je zpracováno ekonomické zhodnocení bezpečnostních politik.

Seznam použitých zdrojů

[1] Národní úřad pro kybernetickou a informační bezpečnost. *Minimální bezpečnostní standard* [online]. [cit. 2023-1-31]. Dostupné z: https://www.nukib.cz/download/publikace/podpurne_materialy/2020-07-17_Minimalni-bezpecnostni-standard_v1.0.pdf

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

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

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

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

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

[7] Národní úřad pro kybernetickou a informační bezpečnost. *Průvodce řízením aktiv a rizik dle vyhlášky o kybernetické bezpečnosti* [online]. [cit. 2023-3-12]. Dostupné z: https://www.nukib.cz/download/publikace/podpurne_materialy/Prvodce%20zenm%20aktiv%20a%20rizik%20dle%20vyhlky%20o%20kybernetick%20bezpenosti.pdf

[8] ČSN ISO/IEC 27001, *Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník.* Praha: Český normalizační institut, 2014.

[9] Národní úřad pro kybernetickou a informační bezpečnost. *Nepřiměřené náklady* [online]. [cit. 2023-2-12]. Dostupné z: https://www.nukib.cz/download/publikace/podpurne_materialy/Neprimerene-naklady_v2.3.pdf

[10] HP: *HP ZBook Firefly 15 G8* [online]. [cit. 2023-04-26]. Dostupné z: https://www.hpmarket.cz/productOpt.asp?konfId=453A4ES

[11] HP*: Dokovací stanice HP Thunderbolt 120 W G4* [online]. [cit. 2023-04-26]. Dostupné z: https://www.hpmarket.cz/productOpt.asp?konfId=4J0A2AA

[12] HP: *HP ProDesk 405 G4 mini* [online]. [cit. 2023-04-26]. Dostupné z: https://www.hpmarket.cz/productOpt.asp?konfId=6QS11EA

[13] HP: *HP Color LaserJet Pro M477fdw* [online]. [cit. 2023-04-26]. Dostupné z: https://www.hpmarket.cz/productOpt.asp?konfId=CF379A

[14] I6: *Cybersoft, s.r.o.* [online]. Cybersoft: ©2023. [cit. 2023-04-26]. Dostupné z: https://www.cybersoft.cz/erpi6.html

[15] Zyxel: ZyWALL firewall series joins elite club with Common Criteria certification [online]. Zyxel: ©2018. [cit. 2023-04-26]. Dostupné z: https://www.zyxel.com/in/en-in/newsroom/press-releases/zywall-firewall-series-joins-elite-club-with-common-criteria-certification

[16] Kaspersky: Endpoint Security for Windows [online]. AO Kaspersky Lab ©2023. [cit. 2023-04-26]. Dostupné z: https://www.kaspersky.com/small-to-medium-business-security/endpoint-windows

[17] KOLOUCH, Jan, Pavel BAŠTA a Josef POŽÁR. CyberSecurity: Cyber security glossary. Třetí aktualizované vydání. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88168-34-8.

[18] Národní úřad pro kybernetickou a informační bezpečnost. *Bezpečnostní role a jejich začlenění v organizaci* [online]. [cit. 2023-4-28]. Dostupné z: https://www.nukib.cz/download/publikace/podpurne_materialy/bezpenostn-role_v3.1.pdf

Seznam použitých obrázků

Seznam použitých tabulek