VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ

FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY

INSTITUTE OF INFORMATICS

NÁVRH ŘÍZENÍ INFORMAČNÍ BEZPEČNOSTI V PROSTŘEDÍ OUTSOURCINGU ÚČETNICTVÍ

DESIGN OF INFORMATION SECURITY MANAGEMENT IN ACCOUNTING OUTSOURCING ENVIRONMENT

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

AUTOR PRÁCE — Bc. Matěj Hlaváček

AUTHOR

VEDOUCÍ PRÁCE — Ing. Petr Sedlák

SUPERVISOR

BRNO 2023

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Student:	**Bc. Matěj Hlaváček**
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:

Návrh řízení informační bezpečnosti v prostředí outsourcingu účetnictví

Charakteristika problematiky úkolu:

Úvod
Teoretická východiska práce
Analýza současného stavu
Vlastní návrhy řešení
Závěr

Cíle, kterých má být dosaženo:

Pro vybranou organizaci na základě analýz vypracovat návrh opatření bezpečnosti za pomoci best practices.

Základní literární prameny:

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

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

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

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

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

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

V Brně dne 5.2.2023

L. S.

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

Abstrakt

Tato práce analyzuje a navrhuje zlepšení řízení bezpečnosti informací ve společnosti XYZ. K tomuto účelu využívá různé nástroje, rámce a analýzy, které slouží k posouzení současného stavu řízení bezpečnosti. Mezi tyto nástroje patří notace BPMN pro procesy, software Esko pro správu aktiv a rizik, analýza PESTLE, Porterova analýza, rámec 7S a matice IFE a EFE. Práce se zabývá posouzením, popisem a zhodnocením stávajícího stavu řízení bezpečnosti a následně navrhuje procesy a postupy pro správu informací, řízení dodavatelů, řízení lidských zdrojů, řízení změn, řízení kontinuity podnikání, bezpečnostní audity, fyzickou bezpečnost, řízení přístupu, správu mobilních zařízení a další aspekty. V závěru práce jsou prezentovány přínosy a náklady spojené se zaváděním efektivního řízení bezpečnosti v malé společnosti.

Klíčová slova

Kyberprostor, řízení informační bezpečnosti, minimální bezpečnostní standard, česká vyhláška kybernetické bezpečnosti.

Abstract

This paper analyses and proposes improvements to information security management at company XYZ. To this end, it uses various tools, frameworks, and analyses to assess the current state of security management. These tools include BPMN notation for processes, Esko software for asset and risk management, PESTLE analysis, Porter's analysis, 7S framework, and IFE and EFE matrices. The paper examines, describes, and evaluates the current state of security management and then proposes processes and procedures for information management, vendor management, human resource management, change management, business continuity, security audits, physical security, access control, mobile device management and other aspects. The paper concludes by presenting the valuable benefits and costs associated with implementing effective security management in a small company.

Key words

Cyberspace, information security management, minimum security standard, Czech cybersecurity decree.

Bibliografická citace

HLAVÁČEK, Matěj. *Návrh řízení informační bezpečnosti v prostředí outsourcingu účetnictví* [online]. Brno, 2023 [cit. 2023-05-14]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/150889. 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 14. 5. 2023

Bc. Matěj Hlaváček

autor

Poděkování

Chtěl bych touto cestou vyjádřit upřímné poděkování panu Ing. Petru Sedlákovi za jeho neocenitelnou pomoc, cenné rady a snahu. Jeho přednášky, cvičení a sdílené zkušenosti byly pro mě nezaplaceným zdrojem poznání a inspirace. Dále bych také rád poděkoval vedení společnosti za dlouholetou spolupráci, jejich podporu a ochotu poskytnout veškeré nezbytné informace a podklady.

Obsah

Úvod

V dnešní digitální éře výrazně vzrostl význam informační bezpečnosti a kybernetické hrozby představují pro organizace všech velikostí značné nebezpečí. Tato práce popisuje současný stav řízení bezpečnosti informací ve společnosti XYZ, která se zaobírá outsourcingem účetnictví a s ním spojenými službami. Tato práce si také klade otázky, jak a jakou formou se dá současné řešení řízení bezpečnosti ve společnosti zlepšit.

V úvodní kapitole jsou nastíněny různé nástroje, rámce a analytické metody použité k posouzení současného stavu řízení bezpečnosti informací ve společnosti XYZ. V první kapitole jsou popsány také předpisy a normy, včetně zákona kybernetické bezpečnosti a role Národního úřadu kybernetické a informační bezpečnosti (dále jen NÚKIB) v této oblasti. Následující druhá kapitola přináší popis současného stavu a porovnává bezpečnostní postupy společnosti XYZ s minimální bezpečnostním standardem stanoveným NÚKIBem. S využitím doporučení tohoto standardu je ve třetí kapitole navržena řada doporučení zaměřených na zlepšení řízení bezpečnosti informací ve společnosti XYZ. Tyto návrhy se dotýkají mnoha aspektů, jako je řízení bezpečnosti informací, řízení dodavatelů, řízení lidských zdrojů, řízení změn, kontinuita provozu, audity bezpečnosti, fyzická bezpečnost, řízení přístupu, šifrování, zálohovací systémy a zabezpečení webových stránek. Ve čtvrté kapitole jsou sestaveny potenciální náklady a přínosy realizace těchto doporučení.

Závěrem lze říci, že záměrem této práce je vybavit společnost XYZ rozsáhlým souborem návrhů na posílení postupů řízení bezpečnosti informací, a tím snížit pravděpodobnost kybernetických událostí a ochránit její digitální aktiva a procesy.

1 Teoretická východiska

Tato kapitola popíše řadu analýz a nástrojů, které budou použity k zavedení minimálního bezpečnostního standardu ve společnosti XYZ. Kapitola začíná popisem Business Process Model and Notation, což je grafická notace používaná k reprezentaci podnikových procesů, která bude použita k popisu řady procesů v podniku.

V druhé podkapitole bude představen cloudový software Esko, který slouží jako nástroj evidence aktiv a jejich garantů. Zároveň slouží pro evidenci rizik aktiv spojených s aktivy a pro evidenci opatření.

Dále se kapitola zabývá analýzou PESTLE, která pomáhá zkoumat vnější faktory, jež mohou mít vliv na jejich činnost, rozhodování a celkovou strategii.

Dále bude nastíněna situace na trhu a vztahy společnosti XYZ s ostatními účastníky trhu pomocí analýzy Porterových pěti tlaků.

K posouzení efektivnosti společnosti XYZ bude použit rámec 7S, diagnostický nástroj pro analýzu a výkonnosti společnosti.

K vyhodnocení současného stavu kybernetické bezpečnosti společnosti budou použity matice hodnotící interní faktory a hodnotící externí faktory, které budou zahrnovat poznatky z předchozích analýz.

V následující podkapitole bude obecně popsán Zákon o kybernetické bezpečnosti č. 181/2014. V navazující podkapitole bude popsána také mezinárodně uznávaná norma ISO/IEC 27001 pro systémy řízení bezpečnosti informací.

Další část kapitoly se zaměří na úlohu Národního úřadu pro kybernetickou a informační bezpečnost. Popíše také Minimální bezpečnostní standard, soubor pravidel a osvědčených postupů, který slouží jako základ této práce.

V neposlední řadě se první kapitola zabývá směrnicí o sítích a informačních systémech (NIS) a její aktualizovanou verzí NIS2, jejichž cílem je zlepšit kybernetickou bezpečnost napříč životně důležitou infrastrukturou v Evropské unii.

1.1 Business Process Model and Notation

Business Process Model and Notation (dále jen BPMN) je grafická notace používaná k modelování procesů. Nabízí standardizovaný slovník pro popis, vyhodnocování a vývoj podnikových procesů a pracovních postupů. BPMN se hojně využívá při řízení podnikových

procesů a při automatizaci pracovních postupů, protože má být srozumitelný jak technickým, tak netechnickým zájemcům.

Diagramy BPMN se skládají z grafických komponentů a spojení, které představují různé části obchodního procesu, jako jsou aktivity, události, brány a toky. BPMN specifikuje standardizovanou sbírku komponentů a principů pro tvorbu procesních modelů, což usnadňuje pochopení a diskusi o složitých podnikových procesech.

Obrázek č. 1: Použité elementy BPMN
(zdroj: vlastní zpracování)

Tyto elementy jsou v BPMN propojeny za pomoci šipek, které prezentují následnosti jednotlivých úkolu a události. V případě, že je v diagramu přerušovaná šipka, tak ta reprezentuje následnost mezi liniemi.

V rámci této práce bude tento nástroj použit k interpretaci několika procesů. Primárně takových, které potřebují spolupráci několika oddělení.

1.2 Esko

Software Esko je cloudově řešený software, který slouží jako nástroj evidence aktiv, jejich garantů, riziky spojených s aktivy a evidenci opatření. Tento software umožňuje získat přehled o aktivech používaných společností.

Aktiva jsou v rámci Esko evidována do tří pod sebou zařazených úrovní. Pro správné fungování softwaru je potřeba zajistit a ověřit následující údaje:

- **Primárním aktivum:** popis primárního aktiva, jeho lokalitu (vybírá se z uživatelem definovaného číselníku), garant (vybírá se z uživatelem definovaného číselníku), úroveň GDPR, kategorie aktiva (VIS, ZS, KII), úroveň důvěryhodnosti (od nízké po kritickou), úroveň integrity (od nízké po kritickou), úroveň dostupnosti (od nízké po kritickou), způsob zabezpečení a způsob manipulace.
- **Podpůrné aktivum:** popis, kategorie (HW, SW. Služby, Data, Facility), jeho lokalita (vybírá se z uživatelem definovaného číselníku), garant (vybírá se z uživatelem definovaného číselníku), úroveň důvěryhodnosti (od nízké po kritickou), úroveň integrity (od nízké po kritickou), úroveň dostupnosti (od nízké po kritickou).
- **Upřesněné aktivum:** popis, kategorie (HW, SW. Služby, Data, Facility), jeho lokalita (vybírá se z uživatelem definovaného číselníku), funkce, správce (vybírá se z uživatelem definovaného číselníku), provozovatel, úroveň důvěryhodnosti (od nízké po kritickou), úroveň integrity (od nízké po kritickou), úroveň dostupnosti (od nízké po kritickou).

Software Esko umožňuje vypracování analýzy rizik. V této funkcionalitě se eviduje zranitelnost (předem definovaný seznam zranitelností), hodnota zranitelnosti (od nízké po kritickou), definice hrozby (předem definovaný seznam hrozeb) a hodnota hrozby. Esko následně ze zadaných hodnot určí hodnotu míry rizika. Esko zároveň umožňuje svým uživatelům evidovat opatření spojená s těmito riziky a hrozbami. V evidenci opatření jde z předem definovaného seznamu vybrat opatření a úroveň, jak je aplikované.

Všechny tyto evidence se dají následně exportovat v PDF formě.

V rámci této práce bude Esko použit k evidenci aktiv společnosti. Reporty v něm sestavené budou přílohou této práce.

1.3 Analýza PESTLE

Společnosti obvykle využívají analýzu PESTLE ke zkoumání vnějších prvků, které by mohly ovlivnit činnost společnosti, rozhodování a celkovou strategii. Každý z faktorů PESTLE je stručně popsán níže:

- **Politický:** Jako tento faktor se označuje vliv zákonů, mezinárodní legislativy a politické stability na organizaci nebo podnik.

- **Ekonomický:** Tento faktor zohledňuje vliv ekonomických podmínek, jako je inflace, úrokové sazby a hospodářský růst, na organizaci.
- **Sociokulturní:** Tento faktor se týká vlivu sociálních a kulturních aspektů na společnost.
- **Technologický:** Tento faktor poukazuje na vliv technologií, inovací a digitální transformace na organizaci.
- **Právní:** Takto označovaný faktor popisuje vliv právních a regulačních pravidel a nařízení na organizaci.
- **Životní prostředí:** Tento prvek se týká vlivu environmentálních proměnných na organizaci.

V rámci této práce bude analýza PESTLE použita k popisu vnějších faktorů kyberbezpečnosti společnosti XYZ. Obecně se zaměřením na odvětví společnosti.

1.4 Analýza Porterových pět sil

Porterových pět sil je strategický rámec vyvinutý k analýze konkurenčních sil v odvětví. Tento model vychází z myšlenky, že existuje pět základních sil, které určují úroveň konkurence a ziskovosti v odvětví. Každá z pěti základních sil je stručně popsána níže:

- **Hrozba nových účastníků na trhu:** tato síla zohledňuje snadnost vstupu nových konkurentů do odvětví.
- **Vyjednávací síla dodavatelů:** tato síla zohledňuje sílu dodavatelů ovlivňovat ceny a podmínky dodávek v odvětví.
- **Vyjednávací síla kupujících:** tato síla zohledňuje sílu kupujících ovlivňovat ceny a podmínky prodeje v odvětví.
- **Hrozba substitutů:** tato síla zohledňuje hrozbu, kterou představují substituční výrobky nebo služby, jež mohou uspokojit stejnou potřebu jako nabídka odvětví.
- **Stávající konkurenti:** tato síla zohledňuje intenzitu konkurence mezi stávajícími konkurenty v odvětví.

V rámci této práce bude Porterova analýza použita k nastínění situace na trhu. Zároveň bude sloužit k základnímu popisu vztahů společnosti XYZ s jednotlivými účastníky trhu.

1.5 Analýza 7S

Rámec 7S se používá jako diagnostický nástroj pro analýzu a zlepšování výkonnosti společnosti. Každý z prvků 7S je stručně popsán níže:

- **Strategie:** plán, který organizace používá k dosažení svých cílů s ohledem na vnitřní i vnější faktory.
- **Struktura:** hierarchické uspořádání rolí, odpovědností a komunikačních kanálů v organizaci.
- **Systémy:** procesy a postupy, které řídí každodenní činnosti a usnadňují realizaci strategie organizace.
- **Sdílené hodnoty:** základní popis kultury organizace a zásad, které řídí chování jejích členů.
- **Schopnosti:** dovednosti a odborné znalosti členů organizace, a to jak individuální, tak kolektivní.
- **Spolupracovníci:** personální aspekt organizace, včetně školení a rozvoje pracovníků.
- **Styl:** přístup k vedení a styl řízení organizace, který ovlivňuje celkové organizační klima.

Rámec 7S je v této práci použit k zhodnocení samotné společnosti XYZ a její bezpečnosti.

1.6 IFE a EFE matice

Internal Factor Evaluation (dále jen IFE) matice je nástroj strategického řízení, který se používá k hodnocení vnitřních silných a slabých stránek společnosti.

Organizace nejprve určí své vnitřní proměnné, jako jsou například její zdroje, dovednosti, kultura, a teprve poté vypracuje matici IFE. Kde se každému prvku přiřadí váha, která vyjadřuje jeho důležitost pro celkový úspěch podniku.

Organizace pak hodnotí svou úspěšnost v každém aspektu na stupnici od jedné do čtyř, přičemž jedna znamená špatnou a čtyři vynikající.

Nakonec se skóre interního faktoru vynásobí váhou každého faktoru a určí se celkové vážené skóre organizace. Výsledné skóre IFE ukazuje, jak dobře organizace využívá svých vnitřních aktiv a jak řeší své vnitřní slabé stránky.

Matice EFE je akronym, který popisuje matici pro External Factor Evaluation. Jedná se o nástroj strategického řízení, který pomáhá organizacím při hodnocení jejich vnějšího prostředí.

Organizace nejprve určí hlavní vnější faktory, které se vztahují k jejímu odvětví, tak aby mohla sestavit matici EFE. Příkladem takových faktorů jsou trendy, předpisy, konkurence, technický pokrok a další proměnné, které mohou ovlivnit úspěch organizace.

V této práci budou tyto matice použity k celkovému zhodnocení současného stavu kyberbezpečnosti společnosti XYZ. Vstupními faktory zde budou výsledky a poznatky předchozích analýz.

1.7 Zákon o kybernetické bezpečnosti

Zákon o kybernetické bezpečnosti (dále jen ZKB) č. 181/2014, je zákonem České republiky, který upravuje ochranu informačních systémů a prevenci kybernetických útoků. Cílem tohoto zákona je zvýšení kybernetické bezpečnosti a vytvoření rámce pro ochranu klíčové informační infrastruktury.

Hlavními cíli ZKB jsou:

- Vytvořit právní rámec pro kybernetickou bezpečnost v České republice.
- Definovat role a povinnosti různých subjektů, jako jsou státní orgány, podniky a provozovatelé kritické infrastruktury.
- Zřídit Národní úřad pro kybernetickou a informační bezpečnost (dále jen NÚKIB) odpovědný za monitorování, vyhodnocování a reakci na kybernetické bezpečnostní incidenty a hrozby.
- Vymezit nezbytná bezpečnostní opatření a povinnosti hlášení incidentů pro provozovatele kritické informační infrastruktury a poskytovatele základních služeb.
- Usnadnit spolupráci a sdílení informací mezi veřejným a soukromým sektorem v oblasti kybernetické bezpečnosti.
- Implementovat směrnici EU o síťových a informačních systémech (NIS).

Zákon se také zabývá různými aspekty kybernetické bezpečnosti, jako je řízení rizik, hlášení incidentů a spolupráce mezi státním a soukromým sektorem. Ukládá provozovatelům kritické informační infrastruktury a poskytovatelům základních služeb povinnost zavést odpovídající bezpečnostní opatření na ochranu svých informačních systémů před kybernetickými hrozbami a hlásit významné incidenty NÚKIB. Zákon rovněž stanoví sankce v případě nedodržení předpisů.

1.8 ISO/IEC 27001

ISO/IEC 27001 je mezinárodně uznávaná norma pro systémy řízení bezpečnosti informací (dále jen ISMS). Norma, kterou společně vyvinuly Mezinárodní organizace pro normalizaci (dále jen ISO) a Mezinárodní elektrotechnická komise (dále jen IEC), poskytuje systematický přístup ke správě citlivých podnikových informací tak, aby zůstaly v bezpečí. Norma poskytuje

zainteresovaným stranám ujištění, že organizace přijímá nezbytná opatření k ochraně svých informací.

Mezi klíčové aspekty normy ISO/IEC 27001 patří:

- řízení rizik,
- ISMS,
- bezpečnostní kontroly provozu,
- neustálé zlepšování,
- certifikace.

Podle normy ISO/IEC 27001 jsou definovány bezpečnostní události a incidenty.

„Definice dle ISOIEC 27001:

- **Bezpečnostní událost:** Bezpečnostní událost je jakákoli pozorovatelná událost v informačním systému nebo síti, která naznačuje možné narušení bezpečnosti nebo ohrožení bezpečnostní politiky nebo bezpečnosti zpracovávaných, ukládaných nebo přenášených informací.
- **Bezpečnostní incident:** Bezpečnostní incident: Bezpečnostní incident je jedna nebo řada nežádoucích nebo neočekávaných událostí, které mohou s velkou pravděpodobností ohrozit obchodní operace a bezpečnost informací. Bezpečnostní incidenty mohou být úmyslné nebo náhodné a mohou vést ke ztrátě, vyzrazení, změně nebo zničení informací. [5, s. 90]“

1.9 NIS a NIS2

Směrnice o sítích a informačních systémech (dále jen NIS) je soubor předpisů, které Evropská unie zavedla v roce 2018 s cílem zlepšit kybernetickou bezpečnost životně důležité infrastruktury v celém regionu. Směrnice vyžaduje, aby podniky v určitých odvětvích, jako je energetika, doprava a zdravotnictví, přijaly opatření kybernetické bezpečnosti na ochranu svých sítí a systémů před kybernetickými útoky.

Směrnice NIS2 je zlepšením a rozšířením původní směrnice. U nás vejde v platnost s novým zákonem o kybernetické bezpečnosti. Podle plánu NÚKIBu by se tak mělo stát v druhé polovině roku 2024. Navrhované doplnění NIS2 zahrnují vývoj standardizovaného certifikačního rámce pro kybernetickou bezpečnost pro zboží a služby.

„Dosavadní regulace kybernetické bezpečnosti byla v České republice koncipována pro poměrně úzkou skupinu několika stovek nejdůležitějších a nejvýznamnějších organizací s velkým dopadem na celou společnost. Směrnice NIS2 přináší nový pohled a pro Českou republiku nutnost přizpůsobit se těmto změnám.

Provázanost fungování společnosti jako celku a organizací v ní je již tak velká, že prakticky neexistuje odvětví, kde by informační systémy nehrály významnou roli. Z tohoto důvodu již ani směrnice NIS2 nehledá systémy důležité pro společnost, ale požaduje zabezpečit vše, co souvisí s poskytováním služeb potřebných pro její fungování. [6]“

Důležité je zmínit, že NIS2 je primárně zaměřená na střední a velké podniky. Tedy společnosti s více jak 50 zaměstnanci anebo bilanční sumou rozvahy alespoň 10 milionů EUR.

1.10 NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost (dále jen NÚKIB) je správní organizací, která má na starosti ochranu životně důležité infrastruktury a vládních sítí před kybernetickými hrozbami. NÚKIB radí a pomáhá společnostem a dalším organizacím při zlepšování jejich vlastních opatření v oblasti kybernetické bezpečnosti.

NÚKIB má na starosti administraci směrnice o sítích a informačních systémech pro Českou republiku, která vyžaduje, aby společnosti v určitých odvětvích dodržovali určité postupy v oblasti kybernetické bezpečnosti a informovaly úřad o všech významných kybernetických událostech.

Kromě kybernetické bezpečnosti má NÚKIB na starosti garantování ochrany utajovaných materiálů v České republice. NÚKIB má na starosti také organizaci reakce země na hrozby národní bezpečnosti.

1.11 Minimální bezpečnostní standard

Minimální bezpečnostní standard (dále jen MBS) je souborem pravidel a osvědčených postupů pro zajištění bezpečnosti informací a dat. MBS je zamýšlen jako základní nástroj pro ochranu citlivých informací a zachování důvěrnosti, integrity a dostupnosti dat.
MBS vypracoval Národní úřad pro kybernetickou a informační bezpečnost. Tento standard vychází z mezinárodně uznávaných norem a rámců, jako je ISO/IEC 27001 a Rámec kybernetické bezpečnosti Národního institutu pro standardy a technologie.

MBS zahrnuje širokou škálu bezpečnostních postupů. Příkladem jsou technologické, organizační a fyzické opatření. Dalšími postupy, které MBS zahrnuje jsou kontroly přístupu, šifrování, zabezpečení sítě, reakce na incidenty a plánování kontinuity provozu.
Minimální bezpečností standard slouží této práci jako základ, podle kterého je vypracována. V další části této práce bude podle něj sestavena analýza současného stavu a bude vypracována návrhová část této práce.

2 Analýza současného stavu

V této části práce se zabýváme analýzou současného stavu společnosti XYZ. V úvodní části dojde k seznámení se společností XYZ, jejími službami a oborem.

Druhá část této kapitoly zahrnuje komplexní hodnocení prostředí, ve kterém firma působí, prostřednictvím analýz PESTLE, PORTER a 7S. Výsledky těchto analýz jsou poté interpretovány s pomocí IFE a EFE matic, které pomáhají lépe pochopit vnitřní a vnější faktory ovlivňující společnost.

Třetí část kapitoly se zaměřuje na současný stav společnosti XYZ podle informací poskytnutých v dokumentu od Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB). Tato část se skládá ze dvou podkapitol, které se věnují manažerské a technické perspektivě bezpečnosti firmy. Součástí této sekce je také detailní popis topologie sítě společnosti, který nám umožní lépe pochopit její infrastrukturu a potenciální slabiny. Na závěr této kapitoly je představen přehled používaných zařízení ve společnosti XYZ, což nám poskytuje ucelený obraz o technologiích a nástrojích, které firma využívá pro svůj provoz.

Tato analýza současného stavu pomůže identifikovat oblasti, kde je možné zlepšit efektivitu a bezpečnost společnosti, a stanovit tak strategie pro její další růst a rozvoj.

2.1 Představení společnosti

Hlavní činností společnosti XYZ je vedení účetnictví, mzdové agendy, daňová optimalizace, účetnictví e-shopu, zpracování Intrastatu a služby One Stop Shop.

Společnost XYZ je na trhu od roku 1994. V průběhu let společnost pomohla více než tisícovce mikro a malých podniků s jejich účetními potřebami. XYZ postupně rozšířila svou nabídku o daňové poradenství, daňovou optimalizaci a další služby, jako je zpracování Intrastatu, ekonomické poradenství a správa elektronického obchodu.

V současné době má XYZ celkem tři pobočky.

Historicky měla společnost větší počet poboček, včetně poboček mimo Českou republiku. Vzhledem ke změnám v chování klientů a pokroku v oblasti informačních technologií však společnost dospěla k závěru, že udržování fyzických poboček v blízkosti klientů již není v dnešním podnikatelském prostředí nezbytné.

Společnost má v současnosti okolo 30 zaměstnanců, kteří se věnují následujícím činnostem:

- **Vedení účetnictví:** komplexní vedení účetnictví od příjmu prvotních dokladů až po zpracování účetní závěrky a vyúčtování na konci roku.
- **Daně a daňové poradenství:** XYZ je registrována společnost u Komory daňových poradců. Díky více než 29 letům zkušeností na trhu minimalizuje daňová rizika a pomáhá klientům dosáhnout daňových úspor.
- **Účetnictví pro E-commerce, Ebay a Amazon:** komplexní účetní a daňové poradenství související s elektronickým obchodováním, včetně souvisejících služeb, jako je registrace k DPH v zahraničí nebo překladatelské služby.
- **Zpracování Intrastatu:** Intrastat je statistický systém EU, který monitoruje pohyb zboží mezi členskými státy EU. Společnosti, které překročí prahovou hodnotu Intrastatu, musí vykazovat obchod uvnitř EU. XYZ pro své klienty zpracovává vše od registrace až po pravidelné zasílání údajů.
- **One Stop Shop** (dále jen OSS)**:** OSS usnadňuje výběr DPH v České republice u přeshraničních transakcí B2C v rámci EU, kdy je dodavatel povinen odvést DPH v členském státě spotřebitele. Společnost zajišťuje vše od registrace OSS až po běžné operace pro klienty.

Kromě komplexních účetních služeb nabízí XYZ i vedení mezd, což je jeden z nejcitlivějších aspektů pro všechny organizace. Její služby v oblasti mezd zahrnují:

- měsíční zpracování mezd zaměstnanců,
- zpracování evidenčních listů důchodového pojištění a ročního zúčtování daní,
- měsíční výkazy společnosti,
- základní pracovněprávní poradenství.

Společnost má v současnosti IT oddělení, marketingové oddělení a má k dispozici firemního právníka.

Společnost XYZ neustále rozšiřuje nabízené služby a nabídku pro své klienty. V rámci nich vznikl požadavek na analýzu kyberbezpečnosti společnosti.

2.2 Analýza PESTLE společnosti XYZ

2.2.1 Politické faktory

Společnost může být povinna dodržovat zákony a normy mezinárodních organizací, jako je Mezinárodní organizace pro normalizaci nebo Mezinárodní elektrotechnická komise.

Aby firma zůstala v souladu a předešla právním problémům, bude muset držet krok se změnami v legislativě a předpisech o kybernetické bezpečnosti.

Pokud společnost poskytuje účetní služby vládním agenturám nebo subjektům, může být požadováno, aby dodržoval konkrétní předpisy nebo požadavky. Podobné požadavky mohou vzniknout například i v případě poskytování služeb pro organizaci podnikající ve zdravotnictví, dopravě, mezinárodního obchodu atd.

Vláda může poskytnout finanční prostředky nebo pobídky podnikům, které se zabývají opatřeními v oblasti kybernetické bezpečnosti, což by mohlo pomoci kompenzovat náklady na zavedení těchto opatření.

Případné geopolitické konflikty nebo napětí, které by mohly vést ke zvýšeným rizikům kybernetické bezpečnosti nebo útokům, mohou vyžadovat monitorování ze strany společnosti.

2.2.2 Ekonomické faktory

S tím, jak se česká ekonomika rozvíjí a digitálně transformuje, přibývá příležitostí k možným kybernetickým útokům.

Pokud nastane kybernetický útok a dojde ke ztrátě citlivých finančních dat, může společnost utrpět finanční ztráty. Klient může požadovat náhradu nebo přerušit spolupráci.

Aby se společnost mohla bránit potenciálním útokům, bude muset investovat do opatření kybernetické bezpečnosti. Firma bude muset zvážit nákladovou efektivitu různých řešení kybernetické bezpečnosti a také to, zda si může dovolit zapojit se do špičkových řešení.

2.2.3 Sociokulturní faktory

Široká veřejnost si stále více uvědomuje význam kybernetické bezpečnosti, to má za následek, že klientela společnosti má vyšší standardy bezpečnosti svých citlivých informací.

Mezi klienty společnosti existují různé úrovně digitální gramotnosti, což by mohlo ovlivnit účinnost různých opatření v oblasti kybernetické bezpečnosti.

Opatřením společnosti proti kybernetické bezpečnosti může být nutnost přizpůsobit se kulturním normám a hodnotám jejich klientů.

Společnost by měla u svých zaměstnanců zvyšovat povědomí o kybernetické bezpečnosti. Tyto zkušenosti společnosti a IT oddělení mohou pomoci identifikovat možné hrozby a vyhýbat se jim.

2.2.4 Technologické faktory

Aby si společnost udržela konkurenceschopnost musí se držet krok s vývojem technologie a kybernetické bezpečnosti. Příkladem takových technologií jsou umělá inteligence nebo strojové učení. Vzhledem k tomu, že se technologie v účetnictví používají stále častěji, existuje více možných slabin, kterých by mohli útočníci využít.

Pro identifikaci a eliminaci následků kybernetických útoků, musí společnost nejen přijmout špičkové technologické řešení, ale i best practices z oboru kyberbezpečnosti.

2.2.5 Legislativní faktory

V České republice jsou kromě zákona č. 181/2014 Sb., o kybernetické bezpečnosti a Vyhlášky o bezpečnostních opatřeních, přijaty i zákony EU. Příkladem je zákon o zpracování osobních údajů (GDPR). Společnost musí dodržovat všechny ostatní platné mezinárodní zákony o kybernetické bezpečnosti, včetně směrnice EU o sítích a informačních systémech (NIS). S příchodem NIS2 je možnost, že se společnost stane významným dodavatelem.

2.2.6 Environmentální faktory

Výpadky proudu, způsobené přírodní katastrofou by mohly zastavit procesy společnosti a otevřít systém společnosti útokům. Aby se snížily negativní účinky tohoto faktoru musí podnik zavést záložní systémy a plány nouzové obnovy.

2.2.7 Výsledek analýzy PESTLE

Společnost musí dodržovat zákony a normy kybernetické bezpečnosti stanovené mezinárodními organizacemi a v případě poskytování služeb v určitých odvětvích může být nutné přizpůsobit svá opatření konkrétním předpisům. Vládní financování a pobídky mohou pomoci kompenzovat náklady na opatření kybernetické bezpečnosti. Společnost musí držet krok s vývojem technologií a osvědčených postupů v oblasti kybernetické bezpečnosti, aby si udržela konkurenceschopnost. Dopad potenciálních kybernetických útoků může mít za následek finanční ztráty, odškodnění klientů nebo ohrožení činnosti. Společnost musí dodržovat všechny platné mezinárodní zákony a předpisy týkající se kybernetické bezpečnosti, včetně GDPR a NIS. Přírodní katastrofy, jako je výpadek proudu, mohou zastavit obchodní procesy, což vyžaduje záložní systémy a plány nouzového obnovení.

2.3 Porterova analýza společnosti XYZ

2.3.1 Substituty

Nejvýznamnějším substitutem služeb firmy je "In house accounting", kde si klient řeší své účetnictví sám, bez pomoci zvenčí. Toto řešení je, ale mnohem dražší a může být i nebezpečné z perspektivy kyberbezpečnosti. Výhodou služeb společnosti oproti takovému substitutu je povědomí o zákonech, normách a best practices v oblasti, jak nacházet s daty klientů.

2.3.2 Konkurence

Bezpečnost dat je klíčovým faktorem pro poskytování účetnictví. Na trhu je velké množství jednotlivců (OSVČ) a firem (středních a velkých), které poskytují služby vedení účetnictví. OSVČ až na výjimky kyberbezpečnost neřeší a ohrožují tím data svých klientů. Větší podniky poskytující účetnictví mají možnost do bezpečnosti vkládat větší kapitál, na druhou stranu mohou být jejich bezpečností procesy příliš strohé a nemusí vyhovovat klientovi. Společnost XYZ se snaží získat konkurenční výhodu na základě kvality poskytovaných služeb, místo toho, aby se spoléhala na cenu jako argument pro získání klientů.

2.3.3 Dodavatelé

Primárním dodavatelem softwaru je firma STORMWARE, se kterou má společnost XYZ velmi dobrý, dlouholetý vztah. V současné době je třeba, aby došlo k revizi tohoto vztahu z pohledu bezpečnosti. Je třeba stanovit jasně nadefinované Service-level agreement (SLA).

Další smlouvy s dodavateli softwaru, je třeba podrobně prověřit, zdali splňují požadavky bezpečnosti.

Dodavatelem hardwaru, je samo IT oddělení analyzované firmy.

2.3.4 Odběratelé

Největší podíl zákazníků tvoří jednotlivci, přesněji OSVČ. Z perspektivy generování zisku jde především o mikro a malé společnosti. Společnost XYZ se v posledních letech více snaží zaměřit na poskytování svých služeb pro malé a středně velké firmy. Obecně je tedy vliv jednotlivých klientů menší. Firma kyberbezpečnost řeší individuálně a primárně na přání klienta.

2.3.5 Nové vstupy

Odvětví účetnictví je již rozsáhlý trh s mnoha velkými hráči. To znamená, že nováček na trhu musí bojovat s konkurencí o zákazníky a mít konkurenceschopnou cenu a kvalitu služeb.

Outsourcing účetnictví je citlivá a regulovaná oblast, kdy organizace musí plnit všechny zákony, předpisy a požadavky týkající se ochrany osobních údajů a finančního vykazování.

2.3.6 Výsledky Porterovy analýzy

Náhradou služeb společnosti je interní účetnictví, které je však obvykle dražší a může být méně bezpečné. Konkurenční výhodou firmy oproti substitutům je její povědomí o zákonech, standardech a osvědčených postupech pro nakládání s daty klientů. Konkurenci na trhu představují osoby samostatně výdělečně činné, které kybernetickou bezpečnost neupřednostňují, a větší firmy, které mohou mít příliš přísné bezpečnostní procesy. Analyzovaná společnost se snaží odlišit spíše kvalitou služeb než cenou. Dodavatelé, například poskytovatelé softwaru, musí být prověřeni z hlediska dodržování bezpečnostních předpisů. Největší podíl zákazníků tvoří fyzické osoby. Společnost se nově snaží zaměřit i na malé a středně velké podniky. Pro zákazníky na trhu je zásadní dodržování předpisů o ochraně osobních údajů a finančních zprávách.

2.4 Analýza 7S společnosti XYZ

2.4.1 Strategie

Společnost se snaží zvýšit povědomí o svých službách, a to především svými novými službami, které zahrnují například zpracování účetnictví pro obchodní platformu Amazon. S ohledem na zvyšující se hrozby kybernetických útoků, posiluje společnost svou pozici v oblasti kyberbezpečnosti, aby zajistil bezpečné zpracování a ochranu citlivých finančních informací svých klientů.

Obecně dochází k expanzi a růstu společnosti. Vzhledem k rostoucímu počtu klientů, kteří vyžadují vysokou úroveň kyberbezpečnosti, investuje společnost do moderních technologií a školení svých zaměstnanců v oblasti kybernetické bezpečnosti.

2.4.2 Struktura

Struktura společnosti je zorganizována za pomocí Linově-štábního řešení. Povinnosti ve společnosti jsou tedy rozděleny podle následující struktury: Nejvyšší odpovědnost mají jednatelé, kteří mají na starosti řízení XYZ. Pod svou zodpovědností mají také senior účetní a mzdové účetní, kteří pracují s citlivými finančními informacemi.

IT oddělení, které má klíčovou roli v zabezpečení kybernetické bezpečnosti, je pod kontrolou jednatelů. Jednatelé chtějí zajistit, aby byli zaměstnanci IT oddělení školeni v oblasti kyberbezpečnosti, a aby byly implementovány moderní technologie zabezpečení.

2.4.3 Systémy

Enterprise Resource Planning (dále jen ERP) systémy, se kterými společnost pracuje primárně, jsou od firmy STORMWARE. Konkrétně se jedná o Pohodu, Pohodu SK, Pamicu a Tax. Dalšími využívaný ERP systémy jsou Vema a Helios.

Pro ukládání dat společnosti slouží lokální server, který je pod správou IT oddělení. Dostupnost dat je pro XYZ prioritou, a proto jsou data pravidelně zálohována a archivována. IT oddělení má také na starosti pravidelné aktualizace a zabezpečení serveru proti možným útokům.

Jednotlivé části systému společnosti jsou pod správou IT oddělení, které prosazuje, že zabezpečení a ochrana dat je zohledněna již při návrhu a implementaci nových procesů a systémů v rámci firmy.

Komunikace mezi jednotlivými lokalitami probíhá na základě pravidelných setkáních jednatelů a IT oddělení, kde se mimo jiné řeší i otázky bezpečnosti. Pro komunikaci mimo schůzky se používají firemní e-maily na platformě Microsoft 365 a případně se komunikace řeší telefonicky. Emailová komunikace je šifrovaná a chráněná před neoprávněným přístupem.

2.4.4 Styl

Styl vedení XYZ je Laissez-faire. Vzhledem k předmětu podnikání, kdy je část zaměstnanců OSVČ případně mají své společnosti s ručením omezeným, existuje ve společnosti předpoklad určité samostatnosti. Zodpovědné osoby posléze kontrolují výstupy zaměstnanců a případně přerozdělují práci.

Styl vedení společnosti může být spojen s určitými riziky kybernetických hrozeb. Vzhledem k relativní samostatnosti zaměstnanců a OSVČ může být obtížné kontrolovat jejich aktivity a zabezpečit data XYZ. Z tohoto důvodu se snaží IT oddělení zvýšit povědomí zaměstnanců o kybernetických hrozbách a zabezpečit vhodné nástroje a postupy pro ochranu dat.

2.4.5 Spolupracovníci

Společnost XYZ má tři pobočky. Vzhledem k rostoucím kybernetickým hrozbám, které mohou ohrozit bezpečnost dat klientů, bylo nutné zaměřit se na zabezpečení systémů a procesů. Očekává se také specializace zaměstnanců v této oblasti a jejich pravidelné vzdělávání v oblasti kyberbezpečnosti. Zaměstnanci jsou pravidelně validování a odměňování, nejen finančně, ale také například firemními akcemi zaměřenými na zlepšení firemní kultury a vztahů mezi zaměstnanci. V současnosti tato validace neřeší jejich bezpečností povědomí a schopnosti.

S rozšířením portfolia se však objevila potřeba posílení nejen IT oddělení, ale i vznik oddělení bezpečnosti.

2.4.6 Schopnosti

Vzhledem k citlivosti a důvěrnosti dat, se kterými společnost pracuje, je kyberbezpečnost klíčovým faktorem. Zaměstnanci jsou pouze základně seznámeni s hrozbami jako jsou phishingové útoky, malware a ransomware. Praxí ve společnosti je, že podezřelá komunikace je přeposlána na IT oddělení k analýze.

Kromě toho XYZ implementuje bezpečnostní opatření, jako je silné heslování, pravidelné aktualizace softwaru a zálohování dat.

2.4.7 Sdílené hodnoty

Kultura společnosti XYZ je rodinná a zaměřená na poskytování vysoké úrovně služeb pro klienty. Kyberbezpečnost je pro společnost a její zaměstnance poměrně novým, ale velmi důležitým tématem. Vedení chce zvýšením povědomí o kyberbezpečnosti a zamezit útokům, snížit finanční rizika a zlepšit obraz organizace. Pro zaměstnance by takto získané zkušenosti mohli přinést výhody i v osobním životě.

2.4.8 Výsledek analýzy 7S

Společnost se zaměřuje na rozšiřování svých služeb. Investuje do moderních technologií a školení zaměstnanců, aby uspokojila rostoucí poptávku svých klientů po kybernetické bezpečnosti na vysoké úrovni. Společnost je organizována pomocí linkového řešení s rozdělením odpovědností mezi jednotlivá oddělení. Klíčovou roli v kybernetické bezpečnosti hraje oddělení IT, na které dohlíží jednatelé. Společnost používá především systémy ERP od společnosti STORMWARE. Jejich data jsou uložena na místním serveru spravovaném oddělením IT. Komunikaci mezi pobočkami usnadňují šifrované firemní e-maily na platformě Microsoft 365. Styl vedení společnosti je Laissez-faire, což může představovat problém při kontrole činností zaměstnanců a zabezpečení firemních dat. Výsledkem analýzy 7S je, že i přes určité překážky má společnost XYZ potenciál na zlepšení své bezpečnosti.

2.5 IFE a EFE matice společnosti XYZ

IFE Matice			
Silné stánky			
Popis	***Váha***	***Vliv(1-4)***	***výpočet***
Vysoké odhodlání vedení k inovacím.	0,11	4	0,44
Vysoká míra kvalifikace a motivace IT oddělení.	0,09	3	0,27
Doba působení na trhu.	0,07	2	0,14
Vysoká míra kvalifikace a motivace zaměstnanců.	0,07	2	0,14
Klienti se zkušenostmi v kyberbezpečnosti.	0,05	2	0,1
Výsledek celkem za silné stánky	0,39		1,09
Slabé stránky			
Popis	***Váha***	***Vliv(1-4)***	***výpočet***
Existuje SPoF.	0,11	4	0,44
V součastnosti nejsou popsané bezpečností postupy.	0,09	4	0,36
Není sestaven DRP.	0,09	3	0,27
Organizace je závislá na omezeném počtu klíčových zaměstnanců a týmů.	0,07	3	0,21
Organizace má omezené finanční prostředky na investice do nových technologií.	0,07	3	0,21
Zastaralé technologie a infrastruktura.	0,09	2	0,18
Není sestaven BCP.	0,09	2	0,18
Výsledek celkem za slabé stránky	0,61		1,85
Výsledky IFE Matice			2,94

Obrázek č. 2: IFE matice
(zdroj: vlastní zpracování)

S výsledkem 2,94 u IFE matice má společnost XYZ středně silnou vnitřní pozici k dosažení svých strategických. cílů.

EFE Matice			
Příležitosti			
Popis	*Váha*	*Vliv(1-4)*	*výpočet*
Zkušenosti IT oddělení s kyberbezpečností.	0,11	5	0,55
Nabízení služeb zabezpečení kyberberprostoru klientům.	0,07	4	0,28
Velká poptávka po kyberbezpečnosti.	0,11	3	0,33
Výsledek celkem za příležitosti	0,29		1,16
Hrozby			
Popis	*Váha*	*Vliv(1-4)*	*výpočet*
Závislost na velkém dodavateli SW.	0,11	1	0,11
Nové přísnější normy a zákony.	0,14	3	0,42
Společnost bude označena, jako významný dodavatel v rámci NIS2.	0,14	4	0,56
Zvýšená konkurence na trhu.	0,06	1	0,06
Zvýšení počtu bezpečnostních hrozeb a kybernetických útoků.	0,06	3	0,18
Ztráta citlivých údajů dodavateli.	0,06	2	0,12
Nové technologické trendy.	0,14	1	0,14
Výsledek celkem za hrozby	0,71		1,59
Výsledky EFE Matice			2,75

Obrázek č. 3: EFE matice
(zdroj: vlastní zpracování)

Výsledkem EFE matice je 2,75. Citlivost záměru vyšší kyberbezpečnosti z perspektivy vnějšího prostředí se tak pohybuje okolo středu.

Výsledky matic jsou tak nevyhovující. Naznačují, že by mělo v podniku dojít k řešení a případné eliminaci rizik spojených s jeho bezpečností.

2.6 Výsledky vstupních analýz

Souhrnně řečeno, aby si společnost udržela konkurenceschopnost, musí dodržovat zákony a předpisy o kybernetické bezpečnosti, přizpůsobovat svá opatření konkrétním předpisům. Společnost může být označena jako významný dodavatel společnosti podléhající nové normě NIS2. V takovém případě bude muset zdůraznit svoje snahy v kyberbezpečnosti.

Jedním z kroků ke zlepšení bude i popsání současných procesů, bezpečnosti, práv, zacházení s daty atd. Dalším krokem ke zlepšení bude i eliminace detekovaných zranitelných bodů.

Důležitým krokem bude i sestavení bezpečnostních plánů jako je Disaster recovery plan a Business continuity plan. Pokud tak společnost neučiní, může to mít za následek finanční ztráty, odškodnění klientů nebo i ukončení činnosti.

Dobrým uchopením problematiky kyberbezpečnosti může být získána konkurenční výhoda pro společnost XYZ. Tato konkurenční výhoda se může stát zdrojem, který může alespoň částečně eliminovat náklady spojené s eliminací hrozeb.

2.7 Manažerská část

2.7.1 Klasifikace a ochrana informací

Společnost v současnosti rozeznává 11 základních typů informací.

Typ	Jedna strana	Druhá strana	Způsob předání	Integrita	Nedostupnost
.xls, .csv, .gpc	Klient	Zaměstnanec	Email	Narušení integrity ohrožuje oprávněné zájmy klienta	Maximálně několik hodin
.xls, .csv, .gpc	Klient	Zaměstnanec	Cloud	Narušení integrity ohrožuje oprávněné zájmy klienta	Maximálně několik hodin
Pokyny, reporty, smlouvy	Klient	Vedení firmy	Email	Narušení integrity ohrožuje oprávněné zájmy klienta	Maximálně několik hodin
Pokyny, reporty	Zaměstnanec	Úřady	Email, DS	Narušení integrity ohrožuje oprávněné zájmy klienta	Maximálně několik hodin
Pokyny, reporty	Zaměstnanec	Úřady	Web	Narušení integrity ohrožuje oprávněné zájmy klienta	Maximálně několik hodin
Pokyny	Vedení firmy	Zaměstnanec	Email	Narušení integrity neohrožuje oprávněné zájmy organizace	Maximálně několik hodin
Pokyny, reporty, smlouvy	Vedení firmy	Vedení firmy	Email	Narušení integrity vede k poškození oprávněných zájmů organizace	Maximálně několik hodin
Pokyny, výpadky	Vedení firmy	IT oddělení	Email	Narušení integrity vede k poškození oprávněných zájmů organizace	Není přípustné
Pokyny, výpadky, požadavky	Zaměstnanec	IT oddělení	Email	Narušení integrity vede k poškození oprávněných zájmů organizace	Maximálně několik hodin
Požadavky, nedostatky	IT oddělení	Dodavatelé	Email	Narušení integrity vede k poškození oprávněných zájmů organizace	Maximálně několik hodin
.xls, .csv, .gpc	IT oddělení	Dodavatelé	Email	Narušení integrity vede k poškození oprávněných zájmů organizace	Maximálně několik hodin
.xls, .csv, .gpc	IT oddělení	Dodavatelé	Cloud	Narušení integrity vede k poškození oprávněných zájmů organizace	Maximálně několik hodin
Pokyny, výpadky	IT oddělení	IT oddělení	Email	Narušení integrity ohrožuje oprávněné zájmy organizace	Maximálně několik hodin

Obrázek č. 4: Tabulka typů informací
(zdroj: vlastní zpracování)

Za pomoci vedení společnosti se podařilo typy informací seřadit. K jednotlivým typům byly přiřazeny následující informace:

- Typ nosiče informací, případně přípona datového souboru.
- Jednotlivé strany, mezi kterými informace prochází.
- Způsob předání informace.
- Integrita informace.
- Požadovaná dostupnost k informaci.

V současnosti nemá společnost vypracovanou metodiku, se kterou by mohla hodnotit tyto informace.

2.7.2 Řízení dodavatelů

Společnost v současnosti nerozděluje své dodavatele. Hardware je do společnosti dodáván buď IT oddělením anebo za pomoci velkých českých e-shopů jako je například Alza.

Důležitým dodavatelem je pro společnost firma ABC, která je internetovým providerem pro lokalitu 1. Zároveň je smluvně zavázaná poskytnout prostor pro zapojení a provoz HW společnosti v případě vyřazení serverovny XYZ. V současnosti nejsou považovány provideři internetu lokalit 2 a 3 za kriticky důležité a jejich smlouvy mají klasické B2B znění.

Velkým softwarovým providerem je nyní pro společnost Microsoft. Servery společnosti v současnosti běží na jeho operačních systémech. Společnost začátkem roku 2023 přešla k řešení Microsoft 365. S jeho pomocí řeší primárně nově emailovou komunikaci, cloudové uložiště a firemní kalendáře.

Developer	Wolters Kluwer	STOMWARE				Seyfor
Název	Preator	Pohoda	Pamica	TAX	Pohoda SK	VEMA
Typ	Bi, CRM	ERP	ERP	ERP	ERP	ERP

Obrázek č. 5: Tabulka Softwaru používaného společností
(zdroj: vlastní zpracování)

Primárním ERP systém společnosti pro vedení účetnictví klientů a mzdovou agendu jsou serverová řešení softwarů od společnosti STORMWARE, od které má společnost i stejným způsobem provozované řešení pro daně.

Společnost se snaží rozšířit svoji nabídku i o jiné ERP systémy, například softwarem pro mzdovou agendu VEMA od společnosti Seyfor. Dalším příkladem ERP systému používaného společností je Helios.

Společnost přes rok používá aplikaci Praetor II, která jí slouží jako systém BI, fakturační systém a nově i jako CRM systém.

Providerem antivirového řešení pro společnost je firma DEF. Společnost její řešení používá na svých pracovních stanicích.

Všechen software a hardware je nově v rámci vypracovaní této práce evidován v softwaru Esko. Výstupy z něj jsou přiloženy v příloze této práce.

2.7.3 Řízení lidských zdrojů

Řízení lidských zdrojů nebylo do okamžiku vypracovaní této práce systémově řešeno. Zaměstnanci v případě, že se obávají, že jsou cílem útoku, byli poučení, aby kontaktovali IT oddělení. Příkladem takové situace je například strach z phisingu u emailové komunikace.

2.7.4 Řízení změn

Řízení změn nebylo doposud ve společnosti řešeno komplexně. Vedení v současnosti k získání informací o změnách používá smlouvy a faktury.

Společnost řeší změny přístupových práv u jednotlivých klientů. IT oddělení začalo s jednoduchou evidencí, kdy, kým a o jakou změnu práv bylo žádáno.

2.7.5 Řízení kontinuity činností

Ve společnosti nejsou sestaveny komplexní plány Disaster Recovery Plan a ani Business Continuity Plan. Z perspektivy vedení nebyly tyto plány potřeba doposud řešit.

Prioritou pro vedení je obnovení funkce serveru a možnosti se k němu dálkově připojit. Zaměstnanci by tak mohli alespoň pracovat na dálku. Další priority nebyly zatím společností sestaveny.

2.7.6 Audit kybernetické bezpečnosti

Ve firmě doposud nebyl sestaven žádný audit hodnotící kybernetickou bezpečnost. Tato práce má sloužit jako první interní audit.

2.8 Technická část

2.8.1 Fyzická bezpečnost

Společnost definovala 5 základních lokalit, které v současnosti pro svou činnost využívá. Jedná se o:

- kancelář Lokalita 1,
- serverovna Lokalita 1,
- kancelář Lokalita 2,
- kancelář Lokalita 3,
- serverovna Lokalita 3.

Všechny tyto lokality jsou zabezpečené pomocí kamer a alarmu na kód. V případě lokalit 2 a 3 je vstup do budov omezen za pomoci recepce, kde se musí nehlášené návštěvy evidovat při vstupu.

Z dalších lokalit je možnost spojení pomocí vzdáleného přístupu – tzv. práce na dálku. Tyto lokality jsou především domovy zaměstnanců. Společnost je nemonitoruje a neeviduje jejich fyzickou bezpečnost.

Podrobnější informace o fyzické bezpečnosti je v rámci vypracovaní této práce evidován v softwaru Esko. Výstupy z něj jsou přiloženy v příloze této práce.

2.8.2 Řízení přístupů

Společnost v současnosti nemá jasně stanovená pravidla, co se týče donesených mobilních zařízení a datových nosičů.

Přístupy jsou rozdělené do čtyř kategorií:

- **Klient**: Někteří klienti mají přístup ke svým datům. Jejich přístupy jsou evidovány a omezeny pouze na jejich data. Důvody připojení jsou následující:
  - kontrola účetnictví v ERP systému Pohoda,
  - vystavení faktur v ERP systému Pohoda,
  - kontrola a úprava faktur v ERP systému Pohoda.
- **Zaměstnanec:** Velice omezený přistup, vidí pouze data klientů, kteří jsou mu zpřístupněni. Případně pracuje přímo v síti klienta.
- **Vedení společnosti**: Má přístup ke všem datům. Nemůže ale ovlivnit informační systémy.
- **IT oddělení:** Má veškerá práva. Povinnosti jsou rozděleny.

Přístupy jsou podrobněji popsány v následujících podkapitolách.

2.8.3 Řízení přístupů mobilních zařízení

Zaměstnanci v současnosti nepoužívají mobilní telefonní zařízení k připojení k síti XYZ. Společnost nabízí, jak svým zaměstnancům, tak klientům možnost připojit se na Wi-Fi. Tato síť je oddělená od firemní a dá se použít pouze jako přístup k internetu.

Několik zaměstnanců používá notebooky pro připojení k síti společnosti. Tyto zařízení byly pořízeny a nastaveny IT oddělením.

2.8.4 Řízení přístupů k zálohám

Přímý přístup má k zálohám pouze IT oddělení. Zaměstnanec o ně může požádat. Způsob a pravidelnost záloh je předem nastavena a popsána v další částí této práce.

2.8.5 Řízení přístupů u obnovy dat

Na základě požadavku od zaměstnance nebo vedení obnoví nebo přepošle člen IT oddělení požadovaná data obnovy.

2.8.6 Řízení přístupů u distribuce aktualizací operačního systému a aplikací

O aktualizace serverových aplikací a systémů se ve společnosti stará IT oddělení. Ostatní uživatelé mají omezená práva a mohou pouze IT oddělení požádat o aktualizaci.

Aktualizaci antivirového systému má na starosti opět IT oddělení.

Společnost má sestaveny plány garantů zařízení. Tito garanti ručí za jejich pravidelné aktualizace. Daný seznam byl v rámci práce převeden do softwaru Esko. Výstupy z něj jsou přiloženy v příloze práce.

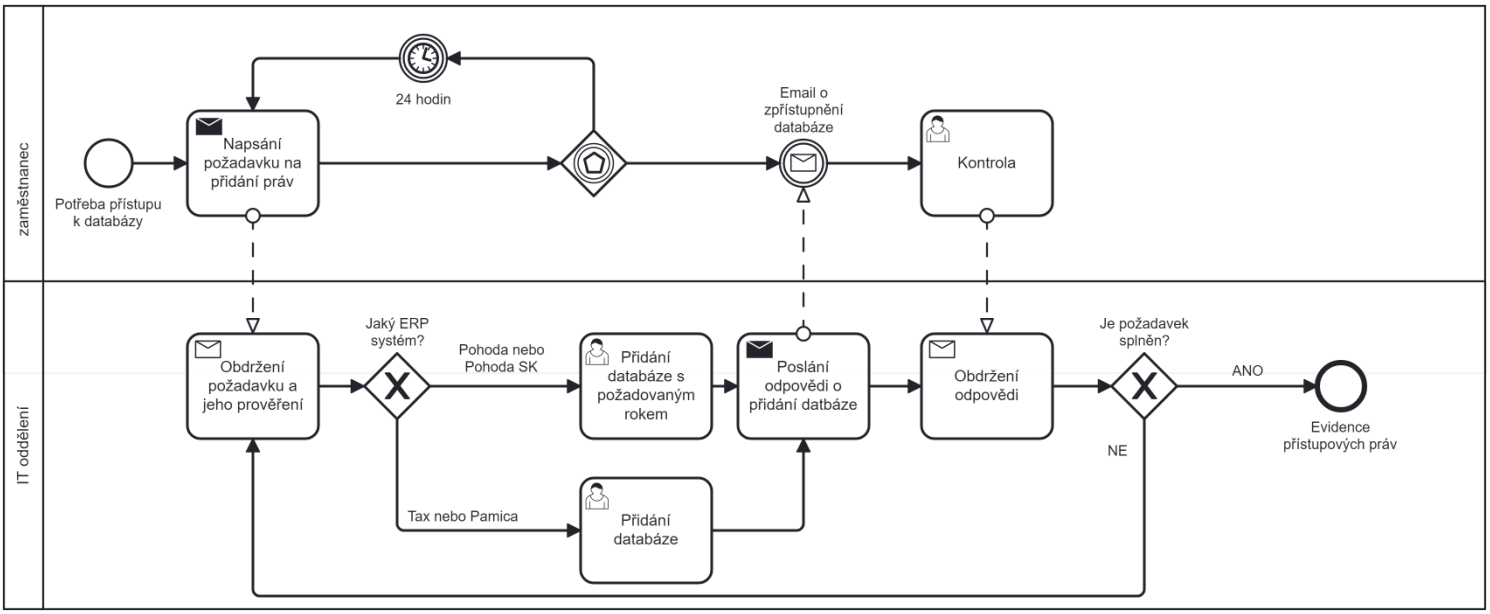
2.8.7 Řízení přístupů k monitoring zařízení

Přístup k síťovým monitorovacím zařízením má pouze IT oddělení. Na požádání vedení jim poskytne člen IT oddělení informace o zařízení.

2.8.8 Řízení přístupů k ERP systémy a datům klientů

Specifickým problémem pro společnost představují její ERP systémy od STORMWARU. Existuje v nich potřeba nastavení přístupových práv pro jednotlivé klienty. Uživatel s administrátorskými právy může nejen ostatním uživatelům ERP systému přidělovat jednotky, ale i nastavit specifické agendy. Může je i omezit v tom jaké činnosti s nimi může provádět.

Administrátor musí při spolupráci více zaměstnanců přidávat každého uživatele k dané databázi jednotlivě.



Obrázek č. 6: Diagram přidání přístupových práv do ERP systémů
(zdroj vlastní zpracování)

Je zde i rozdíl mezi jednotlivými ERP systémy. Pamica a Tax berou jednoho klienta jako jednotlivé databáze. Pohoda a Pohoda SK mají databáze rozdělené nejen na klienty, ale i po letech.

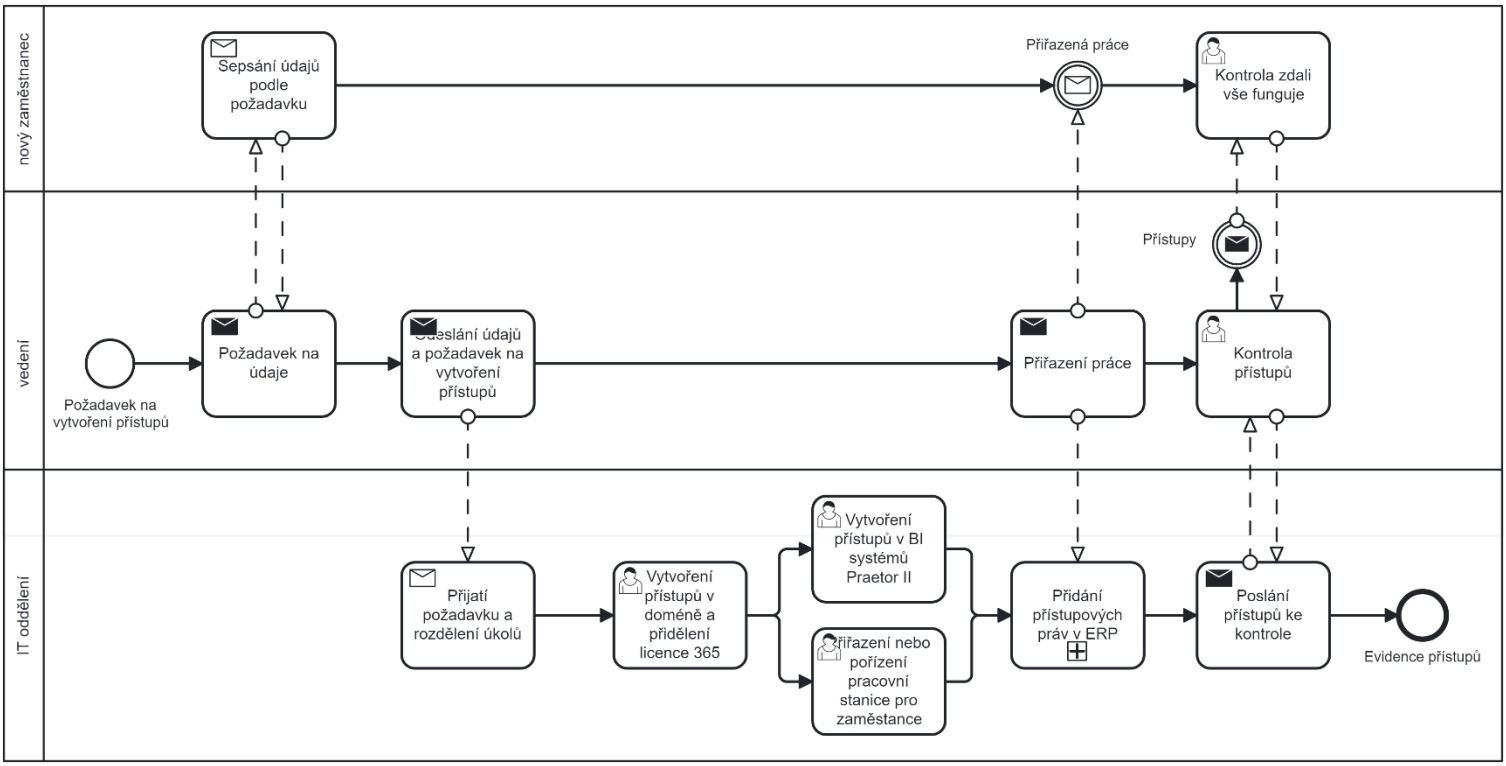
V současnosti je za tuto činnost zodpovědný jeden z členů IT oddělení. Zaměstnanci byli poučeni, koho mají informovat. Byla nastavena lhůta 24h, do které musí být požadavek splněn.

V současnosti se drží společnost pravidla, že aktivně jsou dostupné poslední tři roky. Ostatní databáze jsou archivovány a odebrány z primárního serveru.

Společnost nemá vypracovány pravidelné postupy pro odebírání těchto pravomocí. Praxí ve společnosti je, že jednou za rok kontaktuje IT oddělení všechny zaměstnance a požádá je o seznam nepotřebných databází. Následně jim jsou databáze odebrány.

Někteří klienti mají přístupy ke svých datům v Pohodě. XYZ má pro ně nachystané specifické uživatele, kteří jsou co do pravomocí ještě více omezení než normální uživatel.

2.8.9 Registrace, autentizace a identifikace uživatelů



Obrázek č. 7: Diagram vytvoření nových přístupů
(zdroj vlastní zpracování)

Registraci nového uživatele má na starosti IT oddělení, a to na základě podkladů od vedení společnosti. Nový uživatel je prvně přihlášen do domény, je vytvořena jeho emailová schránka. Následně je mu přiděleno, potažmo pořízeno zařízení. Uživateli jsou pak přiděleny přístupy do systému, se kterými bude pracovat. Speciálně je vytvořen uživatel v BI systému společnosti. Tyto přístupy jsou pak novému uživateli sděleny.

Uživatel potřebuje tyto přístupy, aby se připojil ke svému počítači, firemní síti a k procesům, které bude potřebovat ke své práci.

2.8.10 Politika hesel pro privilegované účty

Pro privilegované účty nemá společnost sestavena globální pravidla. Na základě dotazu má IT oddělení komplexní hesla, která splňují všechny požadavky, které jsou uvedené v dokumentu od NÚKIBu, který slouží jako základ této práce.

2.8.11 Politika hesel pro uživatelské účty

Společnost má sestaven postup pro sestavení uživatelských hesel. První přístupy jsou vytvořené na základě pravidla, které je ve firmě obecně známo. U všech těchto uživatelů je, ale vynucena změna hesla po prvním přihlášení. Hesla jsou následně v zodpovědnosti jednotlivých zaměstnanců.

Systém XYZ je aktuálně nastaven, tak aby každý rok vyžádal změnu hesla po uživateli.

V současnosti neexistuje žádné poučení či doporučení pro zaměstnance, jak sestavovat silná hesla.

2.8.12 Požadavky v oblasti ochrany před škodlivým kódem

Společnost XYZ nemá v současnosti vypracovaný systém pro komplexní ochranu své sítě před škodlivým kódem.

Síť není v současnosti plně segmentována. Pro hosty byly vytvořeny segmentované bezdrátové sítě, které mají pouze přístup na internet. Zaměstnanci byli poučeni, aby klientům poskytovali pouze připojení na tyto sítě.

Systémy pro správu domény byly odděleny a jsou pouze k dispozici na druhém serveru, ke kterému je omezený přístup.

Společnost v současnosti nepoužívá software pro detekci a odstranění škodlivých programů nebo kódů.

2.8.13 Kybernetické bezpečnostní události a incidenty

Kybernetické bezpečnostní události a incidenty jsou situace, kdy jsou informační technologie společnosti cíleně napadnuty, zneužity nebo porušeny, což může mít dopad na bezpečnost a integritu sítě, systémů a dat společnosti. Zaměstnanci jsou poučeni, že v případě podezřelé situace nebo komunikace mají kontaktovat IT oddělení. V současnosti však nebyly poskytnuty žádné konkrétní příklady takových incidentů a zaměstnanci nebyli kompletně poučeni o preventivních opatřeních.

Ve společnosti XYZ nejsou tyto události evidovány. Na poradách vedení a IT jsou pouze jednou za čtrnáct dní projednávány a navrženy řešení, aby se neopakovaly.

V současnosti není ve společnosti systém pro uchování a analýzu logů.

2.8.14 Požadavky v oblasti aplikační bezpečnosti

Ve společnosti se primárně pracuje s ERP systémy od společnosti STORMWARE. Data klientů jsou zabezpečeny za pomoci nástrojů, které jsou součástí licenčního řešení společnosti. Databáze tak nemůžou být otevřeny v ERP systému s jinou licencí.

V případě testovaní nových procesů, například importu dat přímo ERP systému jsou použity testovací databáze. V případě chybného importu tak nejsou narušeny provozní data.

Společnost v současnosti používá tři aplikace vytvořené na míru. Ve všech případech se jedná pouze o nástroje pro transformaci dat podle šablony. Tyto nástroje nemají přímý přístup do ERP systémů. Podobně jako zbytek jsou tyto aktiva popsána v příloze nástroje Esko.

2.8.15 Kryptografické prostředky

Data XYZ nejsou v současnosti šifrována. Jedním z důvodů přechodu na Microsoft 365 byl pro společnost možnost šifrovat komunikaci, jak interní, tak externí. Vedení společnosti používá pro obchodně a strategicky důležité hovory mobilní aplikaci Signal.

2.8.16 Ukládání hesel

Společnost využívá Active Directory pro ukládání hesel svých uživatelů. Active Directory umožňuje spravovat a nastavit bezpečnostní politiky pro hesla, jako například minimální délku a složitost hesla a interval platnosti. Dále může nastavit počet neúspěšných pokusů o přihlášení, při kterých bude účet uživatele uzamčen.

2.8.17 Řešení vysoké dostupnosti

Společnost má licencované ERP systémy na svém serveru, ale nemá implementováno řešení vysoké dostupnosti (dále jen HA). HA není pro XYZ prioritou. Společnost má záložní server, ale postup jeho zapojení a převedení provozu na něj není popsán a otestován.

2.8.18 Single Point of Failure

Společnost XYZ má Single Point of Failure na svém serveru, což znamená, že tento server je kritický pro provoz a jeho výpadek by mohl mít negativní dopad na výkon a dostupnost kritických systémů a aplikací společnosti. Společnost má záložní server, ale postup jeho zapojení a převedení provozu na něj není popsán a otestován.

2.8.19 Zálohování

Proces zálohování v systému Pohoda se skládá ze tří hlavních částí. První částí je denní zálohování, které se provádí každý den v čase 23:30. Během této části se zálohují data SQL databáze na disky D a Z. Druhou částí je zálohování, které se provádí jednou týdně. Během této části se data zálohují do cloudového úložiště Google Cloud. Poslední částí procesu zálohování je archivní zálohování, které se provádí čtyřikrát ročně. Během této části se vytváří archivní zálohy dat, které se uchovávají po dobu alespoň 30 dní. Archivní zálohy se provádějí ručně a mají za úkol zajistit, že data jsou uchována pro případné budoucí použití. Celkově se proces zálohování v systému Pohoda skládá ze tří hlavních částí: denního zálohování, týdenního zálohování a archivního zálohování. Tyto části jsou navzájem propojeny tak, aby zajistily pravidelné a spolehlivé zálohování dat v systému.

Proces zálohování v systémech Pohoda-SK, Pamica a Tax se skládá ze tří hlavních částí. První částí je denní zálohování, které se provádí každý den v čase 22:30. Během této části se zálohuje veškerý obsah složky "data" včetně všech MDB databází na disky D a Z. Druhou částí je zálohování, které se provádí jednou týdně. Během této části se data zálohují do cloudového úložiště Google. Poslední částí procesu zálohování je archivní zálohování, které se provádí čtyřikrát ročně. Během této části se vytvářejí archivní zálohy dat, které se uchovávají po dobu alespoň 30 dní. Archivní zálohy se provádějí ručně a mají za úkol zajistit, že data jsou uchována pro případné budoucí použití. Celkově se proces zálohování v systémech Pohoda-SK, Pamica a Tax skládá ze tří hlavních částí – denního zálohování, týdenního zálohování a archivního zálohování. Tyto části jsou navzájem propojeny tak, aby zajistily pravidelné a spolehlivé zálohování dat v systémech.

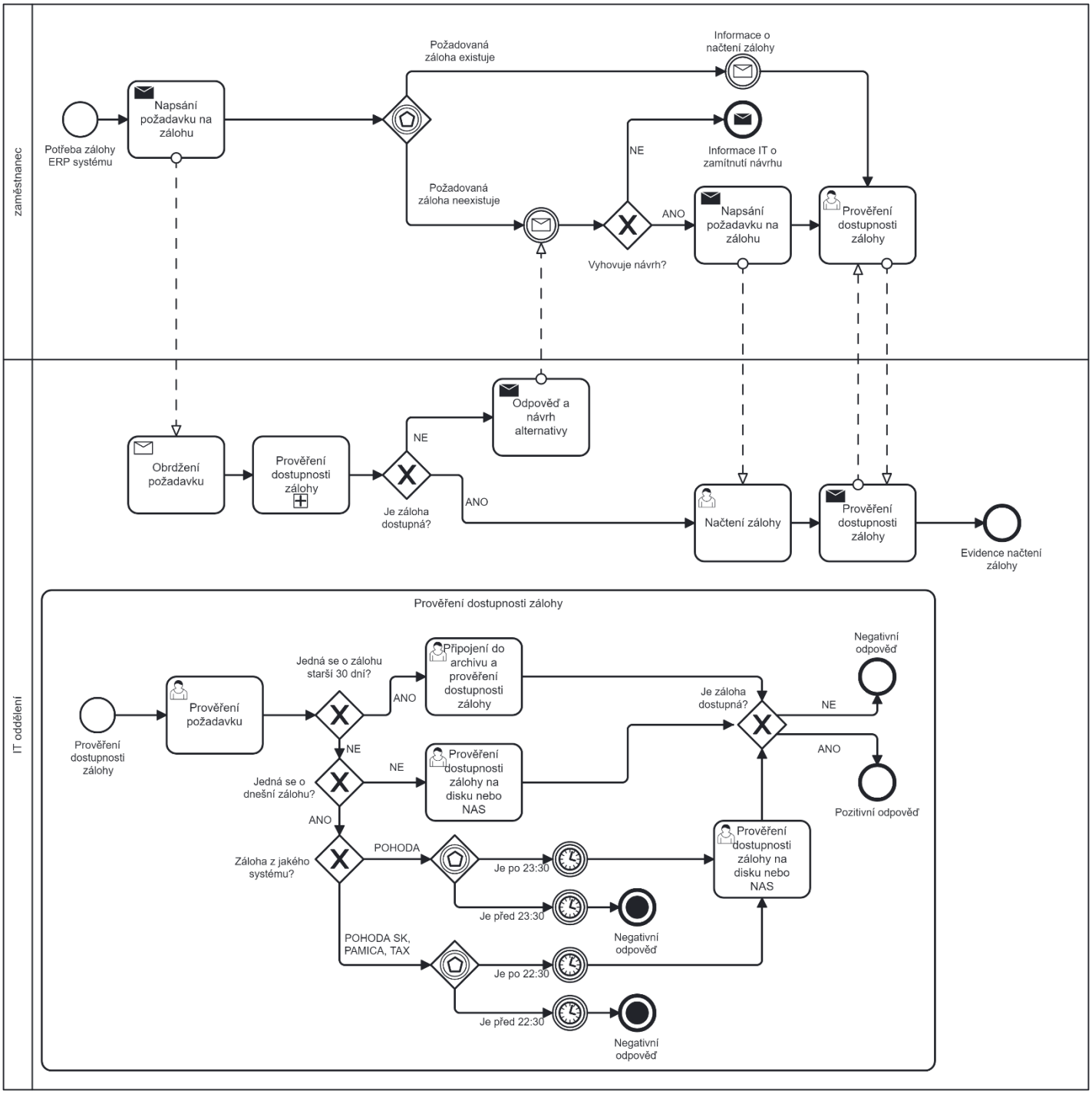
Proces zálohování na disku R se skládá z několika kroků. Každý den ve 21:30 se provádí zálohování všech souborů, které jsou umístěny ve firemní složce, a to jak na disk D, tak na NAS – disk D v podobě zrcadlového zálohování. Jednou týdně se data z této složky zálohují do cloudového úložiště Google, aby byla zajištěna další úroveň ochrany proti ztrátě dat.

Celkově se zálohování na disku skládá z pravidelného denního zálohování, které zahrnuje všechny soubory z firemní složky a zrcadlového zálohování na disky D a Z, a týdenního zálohování do cloudového úložiště. Tyto kroky zajišťují, že data jsou chráněna a kdykoliv k dispozici, i v případě výpadku nebo havárie.

V současnosti nejsou vypracované postupy pro zálohy ERP systému VEMA a BI systému společnosti.

2.8.20 Načtení zálohy ERP systému

Zaměstnanec pošle požadavek na IT oddělení, ve kterém specifikuje, jakou zálohu chce načíst. IT oddělení ověří, zda požadavek splňuje stanovená kritéria. Pokud je požadavek platný, IT oddělení zahájí načtení zálohy. Po dokončení procesu načtení zálohy IT oddělení potvrdí úspěšné načtení zálohy a odešle zprávu zaměstnanci. Zaměstnanec ověří, zda byla záloha úspěšně načtena a potvrdí IT oddělení, že obnovení bylo úspěšné. IT oddělení následně požadavek a výsledek zaeviduje.



Obrázek č. 8: Načtení zálohy ERP systému
(zdroj vlastní zpracování)

2.8.21 Požadavky v oblasti cloudových služeb

Společnost XYZ v současnosti používá troje cloudové služby. Jsou jimi work flow, Microsoft 365 a cloudového úložiště Google.

Work flow je cloudová služba, která umožňuje firmám a organizacím spravovat a automatizovat své obchodní procesy. V současnosti je tato služba ve společnosti testována. Jedním z klíčových

prvků wflow je integrace s nástrojem Rossum, který využívá umělou inteligenci a algoritmy strojového učení k extrakci dat z nestrukturovaných dokumentů jako jsou faktury, účtenky a smlouvy. Ve společnosti se používá k importu jejich faktur přijatých. Vizí společnosti je nabízet tyto služby klientům.

Jak již bylo uvedeno v této kapitole společnost využívá Microsoft 365. V prostředí společnosti je tato služba novinkou. IT oddělení a vedení se snaží nají využití pro všechny služby, které Microsoft 365 obsahuje.

- Začalo se s využíváním OneDrive, který by měl do budoucna nahradit sdílený disk.
- Zaměstnanci byli seznámeni s funkcemi kalendářů, které se pravidelně nahrávají do BI systému společnosti.
- IT a marketingové oddělení začínají používat služby Planner. Pro obě oddělení slouží k upomínání a kontrole úkolů.

Cloudové úložiště Google slouží ve společnosti k uchování záloh. Proces zálohování probíhá jednou za čtrnáct dní a zodpovědný za něj je jeden senior IT pracovník.

2.8.22 Výjimky běhu, chyby a hlášení

V současnosti není navržen proces pro evidenci, řízení a zabránění selhání informačního nebo komunikačního systému.

2.8.23 Ochrana informačního nebo komunikačního systému typu webové aplikace

Web společnosti XYZ slouží pouze jako informační kanál a pro získání nových klientů. Jeho řešení je v současnosti outsourcované. V průběhu tohoto roku by měla webová aplikace projít změnou. Bezpečnost webu je z perspektivy vedení XYZ zodpovědností dodavatelů.

2.8.24 Rozvoj informačních a komunikačních systémů

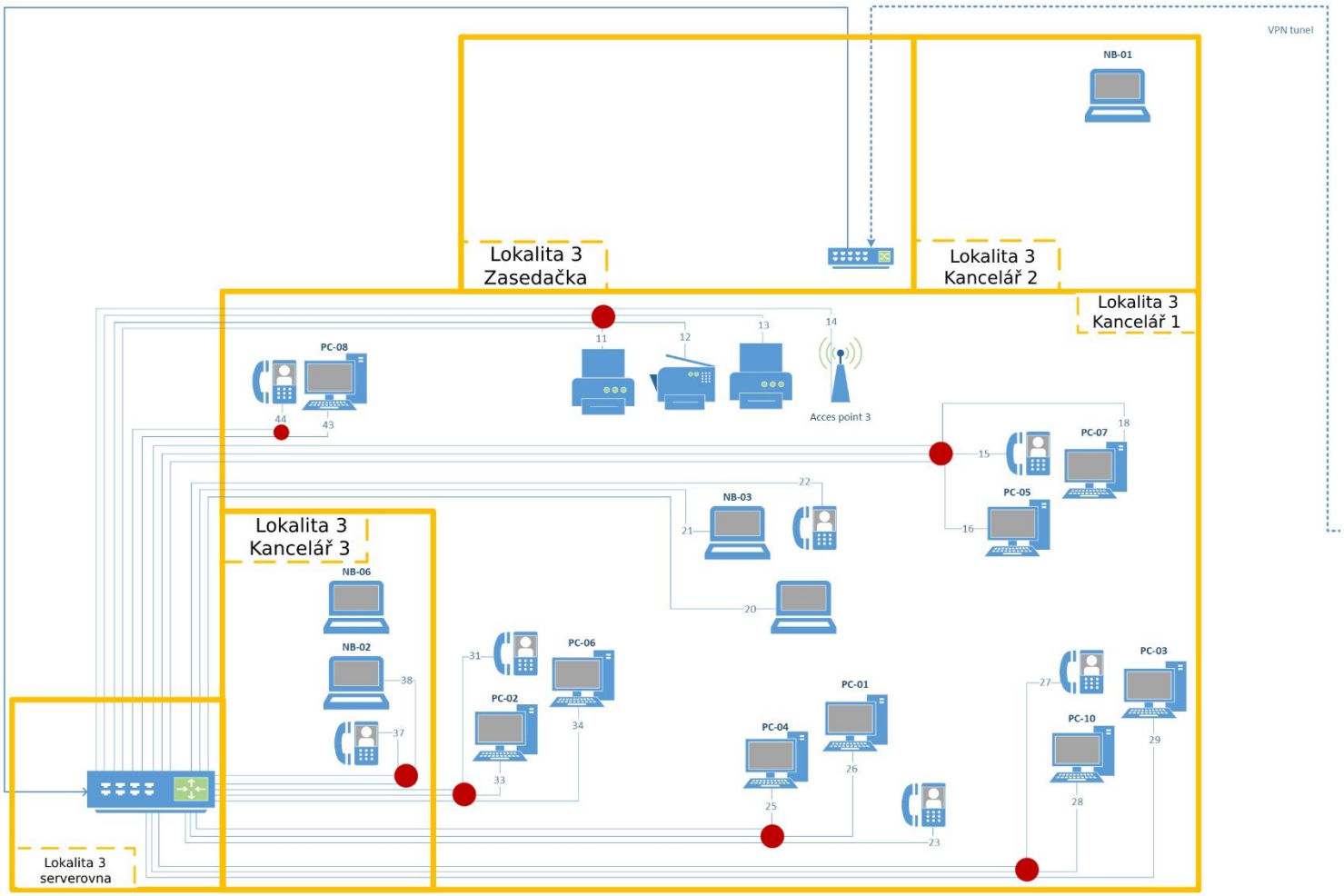
Tato práce je zamýšlena jako základ a odůvodnění důslednějšího zvyšování kyberbezpečnosti společnosti XYZ. Doposud byla bezpečnost řešena nadstandardně pouze u klientů, kteří o to žádali při navázání spolupráce.

2.8.25 Komunikace

Společnost v současnosti rozpoznává tři externí typy organizací se kterými komunikuje. Jedná se klientelu, úřady a dodavatele. Společnost XYZ nemá vypracovanou metodiku pro jejich dělení.

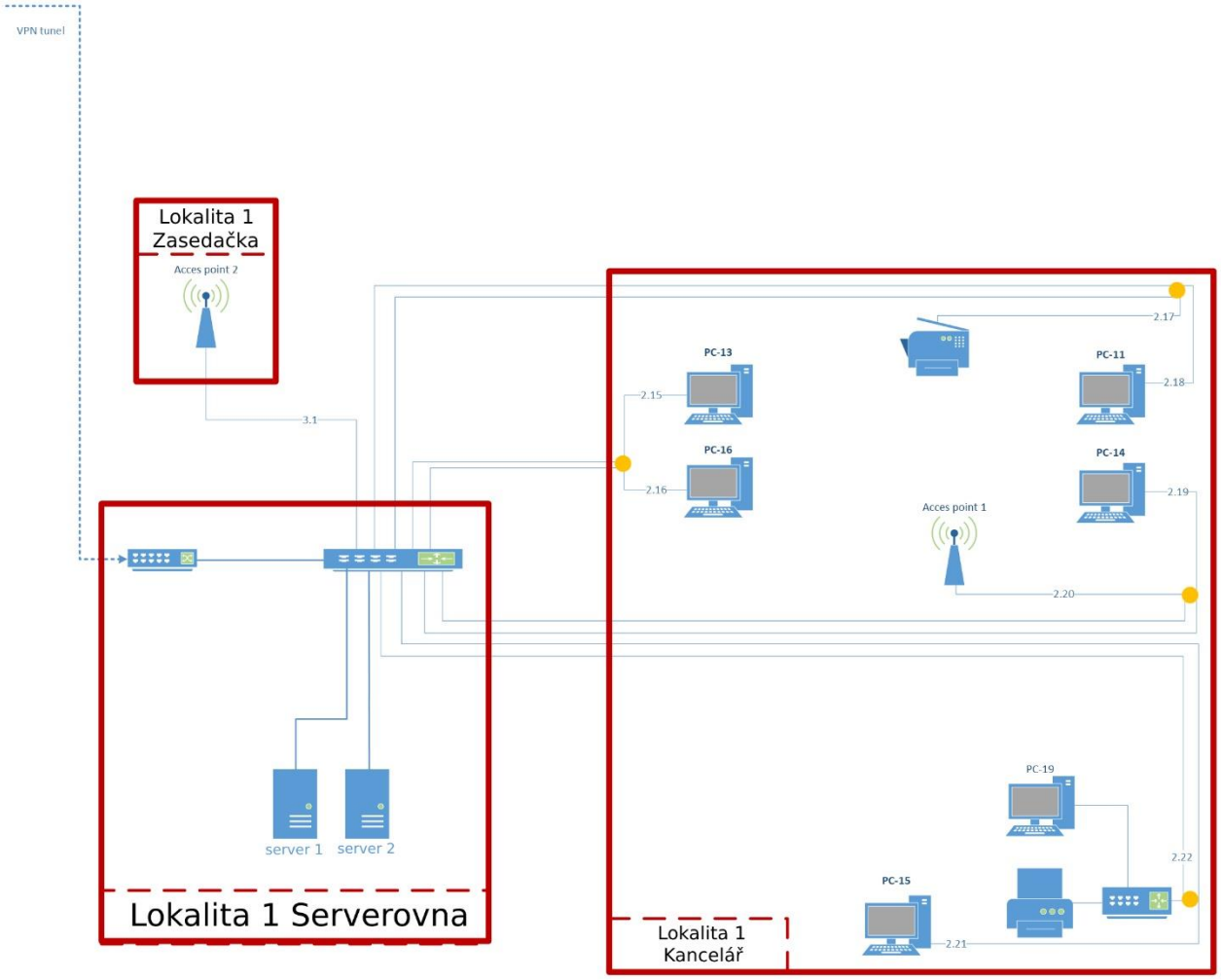
2.9 Topologie

Na základě fyzického prošetření byla v prostředí MS Visio sestavena topologie firemní sítě.



Obrázek č. 9: Topologie pobočky Lokalita 3
(zdroj vlastní zpracování)

V topologii pobočky Lokalita 3 je krom pracovních stanic označeno i umístnění IP telefonie. Červeně jsou zde označeny podlahové datové zásuvky.



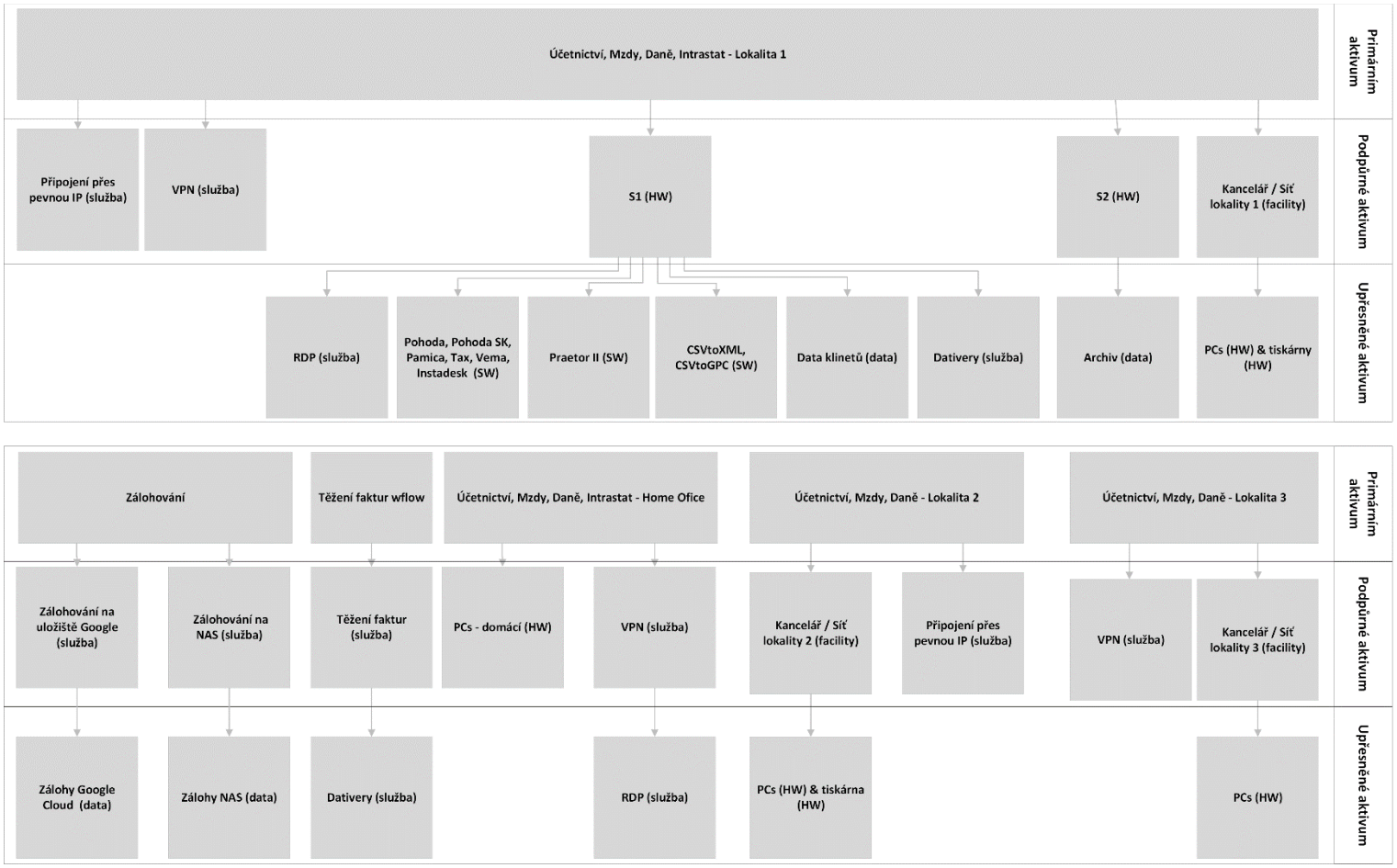
Obrázek č. 10: Topologie pobočky Lokalita 1
(zdroj vlastní zpracování)

Trasy v Lokalitě 1 jsou vyvedeny do klasických datových zásuvek. Žluté body představují, kde se přibližně tyto zásuvku nachází. Kancelář Lokality 1 nemá oproti Lokalitě 3 IP telefonii.

Topologie pro Lokalitu 2 pobočku nebyla vypracována. V současné době se zde nachází pouze jedna datová zásuvka a jedna tiskárna.

2.10 Přehled používaných zařízení

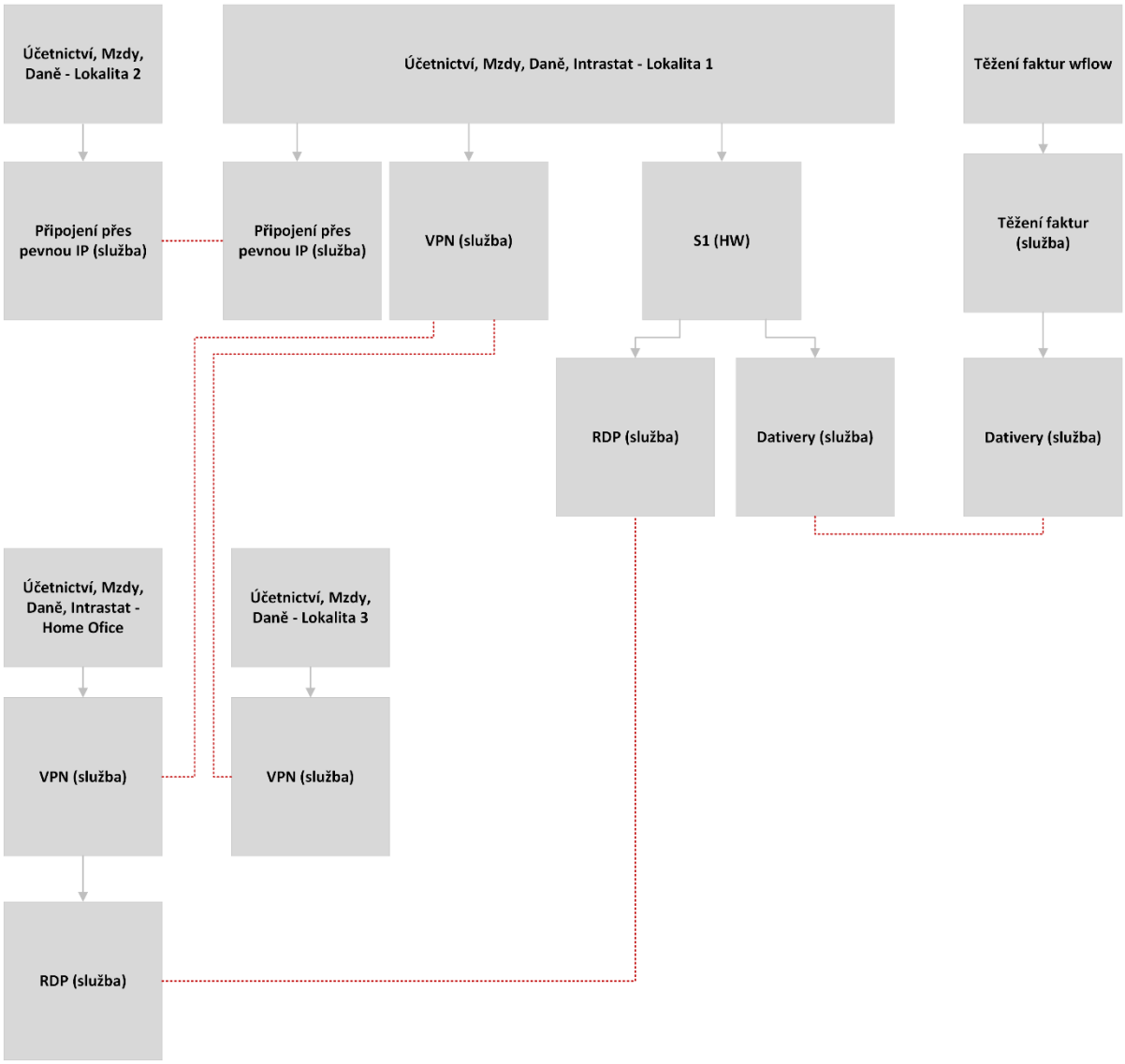
Informační aktiva společnosti XYZ jsou evidována v softwaru Esko, který byl podrobněji popsán v předchozí kapitole.



Obrázek č. 11: Struktura aktiv v Esku
(zdroj vlastní zpracování)

Pro lepší přehled byl vypracován v MS Visio přehled sktruktury, jak jsou jednotlivá aktiva zapsána do Esko.

V příloze této práce je podrobnější seznam aktiv. Například jsou zde rozepsané jednotlivé seznamy všech počítačů a notebooků. V tomto seznamu jsou i garanti aktiv, kteří za ně odpovídají a je v něm i seznam lokací, kde se aktiva nachází.



Obrázek č. 12: Propojení primárních aktiv
(zdroj vlastní zpracování)

Za pomoci MS Visio byl vypracován i nákres propojení jednotlivých primárních aktiv. Služby, které jsou navzájem spojené červenou přerušovanou čarou, představují jednotlivé spoje. Jde tak získat komplexní přehled všech informačních aktiv společnosti XYZ.

3 Návrhová část

Pro potřeby zvýšení bezpečnosti v malých organizacích sestavil Národní Úřad Kybernetické a Informační Bezpečnosti (dále jen NÚKIB) dokument s názvem Minimální bezpečnostní standard (dále jen MBS). Tento dokument poskytuje rámec doporučených postupů a požadavků pro zajištění bezpečnosti informací a ochrany osobních údajů v organizacích působících v České republice. Má pomoci organizacím identifikovat a řídit rizika pro bezpečnost informací a ochranu osobních údajů a zajistit soulad s platnými zákony a předpisy.

Tato práce by měla sloužit jako plán zavádění bezpečnostních opatření doporučených v tomto dokumentu. Pro lepší přehled byla sestavena tabulka, která spojuje podkapitoly této části práce a dokumentu MBS.

Část	Název	Vyhovuje současný stav?	Název podkapitoly
Manažerská	Klasifikace a ochrana informací	NE	Návrh řešení pro klasifikaci a ochranu informací
	Řízení dodavatelů	NE	Návrh řešení pro řízení dodavatelů
	Řízení lidských zdrojů	NE	Návrh řešení pro řízení lidských zdrojů
	Řízení změn	NE	Návrh řešení pro řízení změn
	Řízení kontinuity činností	NE	Návrh řešení pro řízení kontinuity činností
	Audit kybernetické bezpečnosti	NE	Interní a externí audit kyberbezpečnosti
Technická	Fyzická bezpečnost	NE	Postup pro zlepšení fyzické bezpečnosti
	Řízení přístupů	NE	Návrh řešení pro řízení přístupů
	Řízení přístupů mobilních zařízení	NE	Audit a evidence mobilních zařízení
	Řízení přístupů k zálohám	ANO	-
	Řízení přístupů u obnovy dat	ANO	-
	Řízení přístupů u distribuce aktualizací operačního systému a aplikací	NE	Audit a evidence mobilních zařízení
	Řízení přístupů k monitoring zařízení	ANO	-
	Řízení přístupů k ERP systémy a datům klientů	NE	Metodika pro odebrání přístupových práv
	Registrace, autentizace a identifikace uživatelů	NE	Metodika pro deaktivaci identit
	Politika hesel pro privilegované účty	ANO	-
	Politika hesel pro uživatelské účty	NE	Návrh řešení pro řízení lidských zdrojů
	Požadavky v oblasti ochrany před škodlivým kódem	NE	Návrh na segmentaci sítě
	Kybernetické bezpečnostní události a incidenty	NE	Sestavení metodiky při vzniku nestandartní situace
	Požadavky v oblasti aplikační bezpečnosti	NE	Metodika testování ERP
	Kryptografické prostředky	NE	Používání kryptografických prostředků
	Ukládání hesel	ANO	-
	Řešení vysoké dostupnosti	NE	Návrh řešení pro řízení dodavatelů
	Single Point of Failure	NE	Test záložního systému
	Zálohování	NE	Zálohování pro ERP systém VEMA a BI/CRM systém
	Požadavky v oblasti cloudových služeb	NE	Návrh řešení pro řízení dodavatelů
	Výjimky běhu, chyby a hlášení	NE	Návrh řešení pro řízení kontinuity činností
	Ochrana informačního nebo komunikačního systému typu webové aplikace	ANO	Nový web společnosti XYZ
	Rozvoj informačních a komunikačních systémů	NE	Doplnění procesu získání nového klienta
	Komunikace	NE	Audit externích systémů a jejich hodnocení

Obrázek č. 13: Tabulka návrhů řešení
(zdroj vlastní zpracování)

3.1. Návrh řešení pro klasifikaci a ochranu informací

Na základě doporučení MBS došlo k sestavení čtyř úrovní, které slouží k přerozdělení a hodnocení informací. Nejvyšší úroveň citlivosti je označena číslem tři.

Úroveň		Označení	Manipulace	Likvidace	Nachází se v BI?
0	*úřady*	-	požadavky úřadu	požadavky úřadu	ANO
1	*minimum*	-	-	bez omezení	ANO
2	*standard*	informace má označení INTERNÍ	omezený přístup, šifrovaní komunikace	bez omezení	ANO
3	*nadstandard*	informace má označení CITLIVÉ	omezený přístup, šifrovaní komunikace	přepis nosiče informací, anebo jeho fyzická likvidace	NE

Obrázek č. 14: Klasifikační úrovně informací
(zdroj vlastní zpracování)

Specifickým problémem je pro společnost, zdali se informace nachází v jejím BI systému. Pokud ano, předpokládá se, že se jedná o informaci, která má být sdílená. Může se například jednat o odpověď úřadu. Současný BI systém společnosti obsahuje funkci pro evidenci změny dokumentu, zajistí tak, že s bude zřejmá případná manipulace s informacemi.

Dalším specifickým problémem jsou informace sdílené s úřady. Kvůli této problematice byla sestavena specifická úroveň. Úřady, se kterými společnost spolupracuje, mají svoje vlastní postupy a někdy se tyto postupy liší.

Typ	Jedna strana	Druhá strana	Způsob předání	Integrita	Nedostupnost	Navrhovaná úroveň
.xls, .csv, .gpc	Klient	Zaměstnanec	Email	Narušení integrity ohrožuje oprávněné zájmy klienta	Maximálně několik hodin	**2**
.xls, .csv, .gpc	Klient	Zaměstnanec	Cloud	Narušení integrity ohrožuje oprávněné zájmy klienta	Maximálně několik hodin	**2**
Pokyny, reporty, smlouvy	Klient	Vedení firmy	Email	Narušení integrity ohrožuje oprávněné zájmy klienta	Maximálně několik hodin	**2**
Pokyny, reporty	Zaměstnanec	Úřady	Email, DS	Narušení integrity ohrožuje oprávněné zájmy klienta	Maximálně několik hodin	**0**
Pokyny, reporty	Zaměstnanec	Úřady	Web	Narušení integrity ohrožuje oprávněné zájmy klienta	Maximálně několik hodin	**0**
Pokyny	Vedení firmy	Zaměstnanec	Email	Narušení integrity neohrožuje oprávněné zájmy organizace	Maximálně několik hodin	**1**
Pokyny, reporty, smlouvy	Vedení firmy	Vedení firmy	Email	Narušení integrity vede k poškození oprávněných zájmů organizace	Maximálně několik hodin	**3**
Pokyny, výpadky	Vedení firmy	IT oddělení	Email	Narušení integrity vede k poškození oprávněných zájmů organizace	Není přípustné	**3**
Pokyny, výpadky, požadavky	Zaměstnanec	IT oddělení	Email	Narušení integrity vede k poškození oprávněných zájmů organizace	Maximálně několik hodin	**1**
Požadavky, nedostatky	IT oddělení	Dodavatelé	Email	Narušení integrity vede k poškození oprávněných zájmů organizace	Maximálně několik hodin	**2**
.xls, .csv, .gpc	IT oddělení	Dodavatelé	Email	Narušení integrity vede k poškození oprávněných zájmů organizace	Maximálně několik hodin	**2**
.xls, .csv, .gpc	IT oddělení	Dodavatelé	Cloud	Narušení integrity vede k poškození oprávněných zájmů organizace	Maximálně několik hodin	**2**
Pokyny, výpadky	IT oddělení	IT oddělení	Email	Narušení integrity ohrožuje oprávněné zájmy organizace	Maximálně několik hodin	**2**

Obrázek č. 15: Tabulka typů informací včetně klasifikace
(zdroj: vlastní zpracování)

V analýze současného stavu bylo určeno 11 základních typů informací, které XYZ v současnosti rozpoznává. Tento seznam byl doplněn o úrovně, které byli popsány v předchozí podkapitole. Přesněji došlo k doplnění úrovní pro jednotlivé typy informací. Tento seznam by měl být minimálně jednou do roka prověřen, zdali obsahuje všechny typy digitálních informací, se kterými společnost pracuje a mělo by dojít k přehodnocení všech klasifikací jednotlivých typů.

V rámci společnosti by mělo dojít k určení zodpovědných osob, které se stanou garantem informace. S tím je i spojené určení osoby zodpovědné za jednotlivé způsoby předání. V současném řešení jsou tyto typy:

- Email
- Cloud
- Datové schránky
- Web

XYZ by měla pro citlivé a interní dokumenty využívat šifrovanou komunikaci. V rámci IT oddělení musí být sestaven postup pro prověření současného stavu a zaučení vedení a zaměstnanců.

3.2 Návrh řešení pro řízení dodavatelů

Na základě výsledku analýzy současného stavu vznikl požadavek na interní audit dodavatelů společnosti XYZ. Návrh postupu pro audit je následující:

1) Sestavení tabulky všech dodavatelů společnosti.
2) Sestavení profilu každého dodavatele.
   a) Typ informací, k jakým má dodavatel přístup.
   b) Způsob, jak dodavatel přistupuje k informacím.
   c) Certifikace dodavatele.
   d) Zkušenosti s dodavateli.
3) Porovnání současné smlouvy s kritérii vyhlášky č. 82/2018 Sb.

„Požadavky na smluvní ustanovení, které vyhláška o kybernetické bezpečnosti ve své příloze č. 7 vyjmenovává, představují povinnou součást smluv povinných subjektů podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) s významnými dodavateli. Pro obsah smluv s ostatními dodavateli má tato příloha doporučující povahu. I v případě, že je stanovena povinnost zařadit taková ustanovení do smlouvy s významným dodavatelem, lze některé požadavky označit za nerelevantní pro danou smlouvu prostřednictvím prohlášení o aplikovatelnosti.

a) ustanovení o bezpečnosti informací (z pohledu důvěrnosti, dostupnosti a integrity),
b) ustanovení o oprávnění užívat data,
c) ustanovení o autorství programového kódu a programových licencích,
d) ustanovení o kontrole a auditu dodavatele (pravidla zákaznického auditu),
e) ustanovení upravující řetězení dodavatelů,
f) ustanovení o povinnosti dodavatele dodržovat bezpečnostní politiky povinné osoby,
g) ustanovení o řízení změn,

h) ustanovení o souladu smluv s obecně závaznými právními předpisy,
i) ustanovení o povinnosti dodavatele informovat povinnou osobu o kybernetických bezpečnostních incidentech a řízení rizik,
j) specifikace podmínek z pohledu bezpečnosti při ukončení smlouvy,
k) specifikace podmínek pro řízení kontinuity činností v souvislosti s dodavateli,
l) specifikace podmínek pro formát předání dat a informací,
m) pravidla pro likvidaci dat,
n) ustanovení o právu odstoupit od smlouvy v případě významné změny kontroly nad dodavatelem nebo změny kontroly nad zásadními aktivy využívanými dodavatelem,
o) ustanovení o sankcích za porušení povinností. [2]“

4) Zhodnocení, zdali je současný stav vyhovující a další kroky.

Vedení by mělo být seznámeno s výsledky interního auditu a společně s IT oddělením rozhodnout, jaké budou další kroky.

3.3 Návrh řešení pro řízení lidských zdrojů

3.3.1 Sestavení manuálu pro bezpečnost

Postup pro vypracování manuálu bezpečnosti pro zaměstnance by mohl mít tuto podobu:

1) Určení zodpovědné osoby.
2) Definice cíle a rozsahu manuálu.
3) Sestavení seznamu potencionálních hrozeb a zranitelnosti.
4) Sestavení a popis bezpečnostních politik:
   a) pro přístupy,
   b) pro hesla,
   c) pro zálohy,
   d) pro řešení incidentů,
   e) pro garanty aktiv.
5) Sestavení postupu pro pravidelnou kontrolu.
6) Workshopy pro seznámení s manuálem.

Tento manuál by měl být volně dostupný pro zaměstnance a měl by být pravidelně aktualizován.

Manuál by měl být součástí souboru dokumentů, který obdrží nový zaměstnanec po nástupu do společnosti XYZ.

3.3.2 Školení zaměstnanců

Doporučení NÚKIBu zní následovně:

„Pro všechny zaměstnance by měla být stanovena pravidelná školení týkající se základů kybernetické bezpečnosti a to minimálně 1× ročně.

Všichni zaměstnanci musí být seznámeni s bezpečnostními politikami a je potřeba kontrolovat jejich dodržování. Pro řešení případů porušení stanovených bezpečnostních pravidel je vhodné mít nastavena přesná pravidla a postupy.

Zaměstnanci by měli být také proškoleni, jak se chovat v případě neobvyklého či podezřelého chování informačního nebo komunikačního systému, doručení nevyžádaného e-mailu, problémů s dostupností informací či služby nebo při jiné nestandardní situaci. Současně by měli být seznámeni se způsobem, jak tyto neobvyklé situace hlásit. [3, s. 12]“

Postup Společnosti XYZ by mohl být následující:

1) Zpracování plánu pravidelných školení zaměstnanců.
2) Určení frekvence opakování a rozdělení školení. Společnost se může rozhodnout rozdělit školení například na oblasti ERP, emailových služeb a používání BI systému.
3) Určení odborného lektora. V případě, že by byli členové IT oddělení vytíženi nebo by neměli dostatečné zkušenosti, NÚKIB nabízí služby školení. Společnost se může případně obrátit na externistu.
4) Zajistit a naplánovat lokalitu školení. V případě společnosti XYZ bude lepším řešením vypracování dvou školení, a to pro Čechy a Moravu zvlášť.

Ideálním řešením pro společnost XYZ by bylo školení ve formě workshopu. Zaměstnanci by se tak seznámili nejen s pravidly společnosti a best practices na trhu, ale mohli by se podělit o své poznatky a zkušenosti.

3.3.3 Certifikace klíčových osob

Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti a ani její přílohy neuvádí konkrétní certifikáty, které by byly vyžadovány. Nicméně existují certifikace a certifikační standardy v oblasti kybernetické bezpečnosti, které mohou být užitečné pro společnost XYZ.

Obrázek č. 16: Certifikát základů kybernetické bezpečnosti
(zdroj: vlastní certifikace)

Prvním certifikát je vystaven absolventu kurzu základů kybernetické bezpečnosti. Tento certifikát vydává sám NÚKIB, po úspěšném splnění elektronického testu. Před závěrečným testem musí žadatel projít osmi okruhy:

- hesla a přihlašování,
- odemykání zařízení,
- sociální inženýrství,
- důvěryhodná komunikace,
- škodlivé soubory,
- ochrana zařízení,
- stahování aplikací,
- připojení a soukromí.

Tímto kurzem by v ideálním stavu měli projít všichni zaměstnanci společnosti XYZ. Certifikát platí na dva roky a poté je ho třeba obnovit.

Obrázek č. 17: Certifikát kurzu pro manažery kybernetické bezpečnosti
(zdroj: vlastní certifikace)

Druhým certifikátem, vhodným pro XYZ, je certifikát NÚKIBu, který je vystaven po absolvování kurzu pro manažery kybernetické bezpečnosti.

„Kurz, do kterého vstupujete, je určen profesionálům z oblasti kybernetické bezpečnosti a podrobně rozebírá obsah Vyhlášky o kybernetické bezpečnosti (VKB). Záměrem kurzu je poskytnout oporu při zavádění požadavků VKB do praxe. Obsah kurzu je otevřený, abyste se k němu mohli kdykoliv vracet pro nápovědu, inspiraci nebo ujištění jako do učebnice.

Klíčové paragrafy VKB (3 až 16) jsou přiblíženy jednoduše, srozumitelně a jsou doplněny o doporučení, komentáře a praktické příklady. Můžete si také vyzkoušet teoretický výklad aplikovat do praxe v interaktivním workshopu, který je založený na profilu fiktivního úřadu. [4]“

Tímto certifikátem by měli projít klíčové osoby IT oddělení společnosti XYZ.

3.4 Návrh řešení pro řízení změn

Jedním z klíčových prvků kybernetické bezpečnosti je řízení změn, což znamená systematické a koordinované řešení změn v informačním nebo komunikačním systému s cílem minimalizovat rizika narušení jeho funkčnosti a bezpečnosti dat. Proces řízení změn zahrnuje identifikaci změn, jejich dokumentaci, koordinaci, implementaci a testování.

3.4.1 Evidenční systém pro řízení změn

V současné době se jako nejvhodnější řešení pro XYZ nabízí vytvoření tabulky na evidenci změn. Postup by mohl být následující:

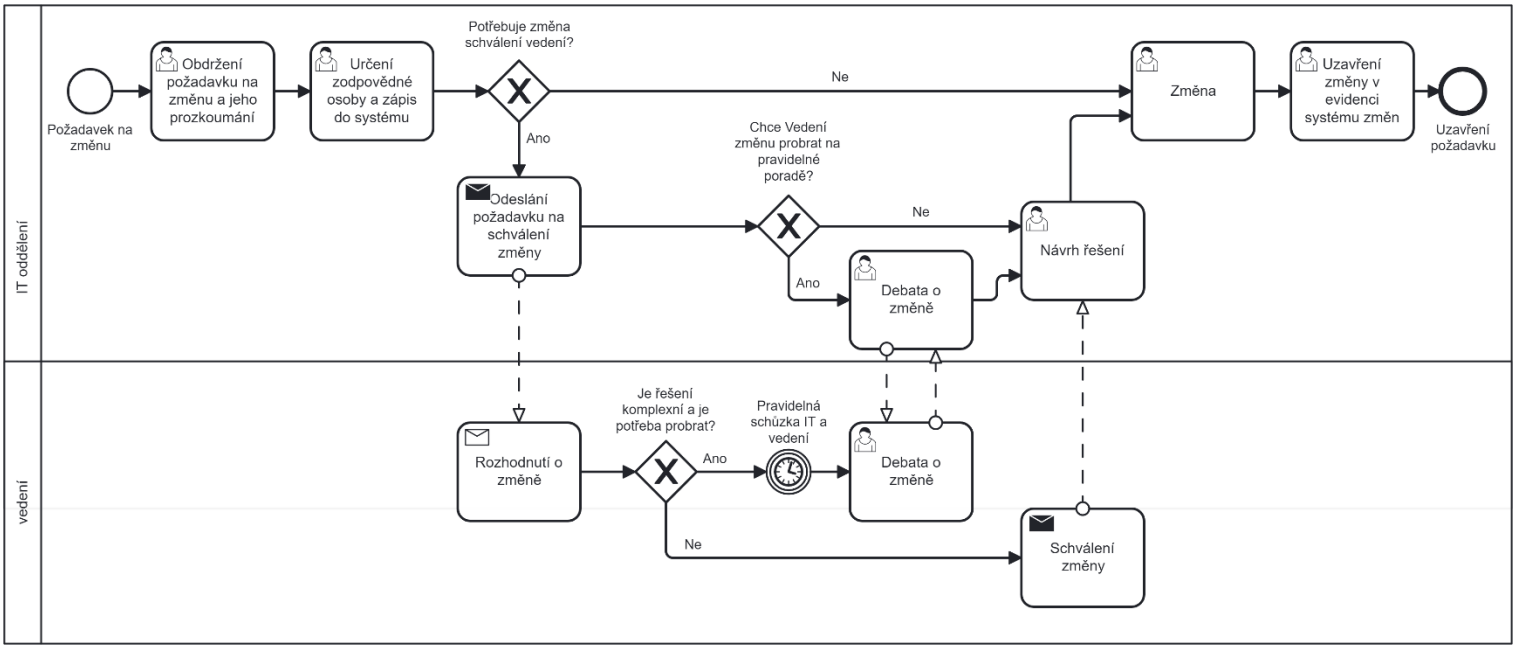
1. Určení zodpovědné osoby.
2. Vytvoření tabulky Excel na OneDrive. Tabulka by měla obsahovat sloupce:
    a. platforma (Pohoda, Pohoda SK, Pamica, Tax, Vema, Praetor, doména)
    b. zodpovědná osoba (zkratka),
    c. popis změny,
    d. datum změny,
    e. důvod změny,
    f. stav změny,
    g. poznámky.
3. Nasdílení tabulky v rámci IT oddělení.
4. Sestavení šablony emailu žádosti o změnu.
5. Seznámení zaměstnanců s novým postupem.

Platforma	Zkratka	Popis	Datum změny	Důvod změny	Stav změny	Poznámky
Doména	MH	Dokoupení licence 365	1.1.20xx	nedostatek licencí	HOTOVO	
Pohoda	MH	Aktualizace Pohody	1.1.20xx	potřebná	HOTOVO	

Obrázek č. 18: Tabulka evidenčního systému pro změny
(zdroj: vlastní zpracování)

Alternativou je použití MS Planneru. Výhodou je zde větší bezpečí, možnost posílání upomínek, vkládání mezikroků a jasná dělba úkolů. Na druhou stranu není tak přehledný jako navrhovaná tabulka v Excelu.

3.4.2 Metodika procesu změny



Obrázek č. 19: Diagramu metodiky procesu změny
(zdroj: vlastní zpracování)

V diagramu je jasně znázorněn postup pro řízení změn ve společnosti. Nejprve je nutné požadavek prozkoumat a zaznamenat do systému evidence, popsaný v předchozí podkapitole. Poté následuje rozhodnutí, zda je nutné spolupracovat s vedením společnosti. Jako příklad změny lze uvést nedostatek licencí MS office 365, kdy je nutné schválit navýšení kvůli vyšší faktuře od dodavatele. Vedení může také rozhodnout, že je nutné projednat změnu s IT oddělením a dohodnout se s ním na dalším postupu. O takové změně se rozhodne na pravidelné schůzce. Po úspěšném dokončení změny je nutné uzavřít změnu v systému pro evidenci.

3.5 Návrh řešení pro řízení kontinuity činností

Tato podkapitola se zaměřuje na doporučení pro zavedení a implementaci účinných postupů řízení kontinuity provozu (dále jen BCM). Mezi klíčové prvky BCM patří:

- Definování práv a povinností správců a bezpečnostních pracovníků.
- Vyhodnocení a zdokumentování potenciálních kybernetických bezpečnostních rizik.
- Stanovení cílů řízení kontinuity činností.
- Vypracování politiky řízení kontinuity činností.
- Vytvoření a aktualizace plánů kontinuity provozu a pohotovostních plánů.
- Zavedení opatření pro zvýšení odolnosti.

BCM používá dva typy plánu, a to Disaster Recovery Plan (dále jen DRP) a Business Continuity Plan (dále jen BCP). DRP se zaměřuje na obnovu kritických IT systémů a infrastruktury po závažném narušení nebo katastrofě, jako je přírodní katastrofa, kybernetický útok nebo selhání zařízení. Hlavním cílem DRP je minimalizovat prostoje, obnovit ztracená data a co nejrychleji obnovit služby IT. Plán BCP je širší a komplexnější plán, jehož cílem je zajistit nepřerušené fungování kritických podnikových procesů a operací organizace, během narušení a po něm. Nezabývá se pouze IT systémy, ale zohledňuje i další aspekty organizace, jako jsou personál, zařízení, dodavatelský řetězec a komunikace.

Postup pro vypracování DRP a BCP, by pro společnost XYZ mohl vypadat následovně:

1. Vytvoření interního týmu. Sestavení skupiny osob s různými odbornými znalostmi:
    a. zkušenost s IT,
    b. vedení účetnictví,
    c. mzdové agendy,
    d. daňového poradenství,
    e. obchodních operací společnosti XYZ,
    f. managementu společnosti XYZ.
2. Provedení analýzy rizik za pomoci nástroje Esko.
3. Provedení analýzy dopadů na podnikání, kde je třeba určit:
    a. potenciální důsledky každého identifikovaného rizika na primární aktiva,
    b. maximální tolerovatelnou dobu výpadku každé funkce,
    c. minimální úroveň služeb potřebnou k zachování provozu.
4. Určení cíle obnovy po havárii. Na základě posouzení rizik a analýzy dopadů na podnikání. Například cíle doby obnovy (dále jen RTO) a cíle bodu obnovy (dále jen RPO) pro kritické systémy a data.
5. Vypracování strategií obnovy. Určení a zdokumentování metody a zdrojů potřebných k obnově kritických systémů a jejich dat v rámci stanovených RTO a RPO.
6. Vytvoření plánu obnovy po havárii, který bude obsahovat podrobnosti o rolích a odpovědnostech jednotlivých členů týmu, strategiích obnovy a co bude obsahovat postupy krok za krokem pro obnovu po různých scénářích havárie.
7. Ověření, zdali DRP je v souladu s českým zákonem o kybernetické bezpečnosti.
8. Vytvoření BCP. Vypracování komplexních písemných plánů zachování kontinuity, které budou obsahovat podrobnosti o rolích a odpovědnosti členů týmu, komunikačních

protokolech, strategiích obnovy a postupech, krok za krokem pro zachování nebo obnovení kritických funkcí během různých scénářů narušení.

9. Ověření, zdali je BCP v souladu s českým zákonem o kybernetické bezpečnosti.
10. Integrace DRP a BCP.
11. Seznámení zaměstnanců s DRP a BCP.

DRP a BCP je třeba oba typy pravidelně kontrolovat a je třeba je i pravidelně aktualizovat.

3.5.1 Disaster Recovery Plan

Hlavním cílem DRP je minimalizovat dopady výpadků, obnovit ztracená data a co nejrychleji obnovit služby IT. Mezi klíčové prvky DRP patří identifikace kritických systémů a aplikací, stanovení cílů doby obnovy, cílů bodu obnovy a vypracování podrobných postupů obnovy.

PLÁN OBNOVY PRO ZTRÁTU DAT KLIENTA Z POHODY

I. Přehled

Účelem tohoto plánu obnovy po havárii (DRP) je popsat kroky, které organizace potřebuje k obnově ztracených dat klientů z ERP systému POHODA do 48 hodin od incidentu. Plán se zaměřuje na obnovení systému do normálního funkčního stavu a zajištění kontinuity účetních služeb pro klienty.

II. Tým pro obnovu po havárii

IT oddělení	Kybernetické bezpečnosti	Zástupce managementu	Zástupce účetnictví
Zkratka jména [IT]	Zkratka jména [KB]	Zkratka jména [MN]	Zkratka jména [UČ]

III. Postup

Krok	Akce	Zodpovědnost	Termín
A	*Ztráta dat*		
1)	Identifikace incidentu	UČ	co nejdříve
2)	Uvědomte tým DR	KB	co nejdříve
3)	Informovat dotčeného klienta	MN, UČ	co nejdříve
4)	Určení příčiny ztráty dat	IT, KB	do 24 hodin
5)	Posouzení rozsahu ztráty dat	IT, KB, UČ	do 24 hodin
6)	Obnova ze záloh	IT, KB	do 24 hodin
7)	Snaha o obnovu dat	IT, KB	co nejdříve
8)	Ověření integrity dat	IT, KB, UČ	co nejdříve
B	*Ztráta přetrvává => Chyba systému*		
1)	Kontaktovat dodavatele ERP systému POHODA	IT, KB	do 24 hodin
2)	Použít nezbytné opravy	IT, KB	co nejdříve
3)	Obnovení dat	IT, KB	co nejdříve
4)	Testování funkčnosti systému	IT, KB, UČ	do 24 hodin
Po incidentu	*Činnosti po incidentu*		
1)	Uvědomit klienta	MN, UČ	co nejdříve
2)	Provést postmortální analýzu	IT, KB, MN, UČ	do 48 hodin
3)	Aktualizace DRP	IT, KB, MN, UČ	do 48 hodin

Obrázek č. 20: Vzor plánu obnovy po ztrátě dat
(zdroj: vlastní zpracování)

Pro potřeby této práce byl vypracován vzor, jak by DRP plán mohl vypadat pro společnost XYZ. Tento DRP plán obsahuje na úvodu popis incidentu, v druhé části obsahuje výpis jednotlivých členů DRP, kteří jsou zapsaní ve zkratkách. Třetí část obsahuje rozepsané jednotlivé činnosti, jejich následnosti, zodpovědnosti jednotlivých členů a termíny ukončení.

3.5.2 Business Continuity Plan

Hlavním cílem BCP je minimalizovat dopad narušení činnosti organizaci a její zainteresované strany. Mezi klíčové prvky BCP patří provedení analýzy dopadů na podnikání (BIA), identifikace kritických procesů, stanovení strategie kontinuity a vypracování komunikačního plánu.

„BCP je vytvářen s ohledem na hrozící dopady do činností a nákladů na potřebná opatření. Jedním ze základních parametrů dostupnosti je tzv. RTO, jenž vyjadřuje množství času potřebné pro obnovení data celého provozu nedostupného informačního nebo komunikačního systému. Dalším ukazatelem dostupnosti je tzv. RPO, který definuje, do jakého stavu (bodu) v minulosti lze obnovit data v informačním nebo komunikačním systému. Jinými slovy množství dat, o která lze přijít. [3, s. 14]“

PLÁN KONTINUITY ČINNOSTÍ (BCP)

Hrozba	Vnik neoprávněné osoby do serverovny
Nebezpečí	Zničení serverů, ztráta dat
Pravděpodobnost vzniku	Střední

OPATŘENÍ

Prevence

a) Instalace nového alarmu a IP kamer.
b) Vytvoření záloh.
c) Smlouvání náhradního místa. Pokud dojde k nečekané události, přesunutí provozu informačního nebo komunikačního systému na alternativní (záložní) místo.

Činnosti v případě aktivace zdroje hrozby

Scénář se zaměřuje na případ, kdy se neoprávněná osoba dostane do serverovny umístěné v budově společnosti a zničí serverovnu a server. Během testování a nasazení plánu na protiopatření je důležité zaznamenávat veškeré kroky obnovy, aby bylo možné postupy aktualizovat nebo upřesnit v případě potřeby. Tuto dokumentaci má na starosti určený člen týmu.	**Doba trvání**
I. Svolání krizového štábu společnosti	1h
1) Svolání krizového týmu IT	
2) Rozhodnutí o aktivaci záložní lokality.	
II. Zahájení přípravy spuštění záložní lokality	4h
1) Sbalení vytvořených záloh na základě DRP.	
2) Přesun odpovědných osob do záložní lokality – pracovníci oddělní IT a další členové týmu potřební pro zachování chodu nezbytných činností společnosti.	
3) Aplikace opatření pro minimalizaci škod.	
4) Instalace a konfigurace serverů, aplikací, síťových prvků na základě DRP.	
III. Zahájení ostrého provozu v záložní lokalitě	1h
Informování vedení společnosti o obnovení dostupnosti aplikací v záložní lokalitě.	
Konec (Celková doba trvání)	**6h**

Doporučení pro méně závažný vývoj situace

Pokud krizový štáb rozhodne o nepoužití záložního místa, dojde k utlumení činnosti organizace, ale budou přijata opatření k minimalizaci škod.

Další postup

Mimořádná událost bude nadále monitorována. Po opadnutí povodně začnou likvidační práce a obnovení činností organizace v plném rozsahu.

Obrázek č. 21: Vzor plánu kontinuity činnosti
(zdroj: vlastní zpracování)

Na základě příkladu přiloženého k dokumentu MBS byl pro společnost vypracován vzorový BCP, pro situaci, kdy dojde k vniknutí neoprávněné osoby do serverovny společnosti a dojde k poškození jejího vybavení.

3.6 Interní a externí audit kyberbezpečnosti

Tato práce slouží pro společnost XYZ jako podklad pro první interní audit kybernetické společnosti. Na základě tohoto interního auditu dojde k sestavení a posouzení společnosti XYZ.

„Posuzuje soulad s:

1. bezpečnostní dokumentací a bezpečnostními politikami organizace,
2. právními předpisy,
3. jinými předpisy a smluvní závazky, které se vztahují k informačnímu nebo komunikačnímu systému a
4. nejlepší praxí. [3, s. 16]“

Tento interní audit by se měl pravidelně opakovat. Společnost by jím měla projít i v případě velké změny.

Důležitým krokem bude pro společnost XYZ i projít nezávislým externím auditem. V rámci druhé části této podkapitoly dojde k sepsání doporučených postupů a kroků při výběru externího partnera pro audit:

- Při výběru externího partnera pro kybernetický audit je důležité hledat společnost s rozsáhlými zkušenostmi a odbornými znalostmi v této oblasti. Příkladem jsou organizace, které mají za sebou řadu úspěšných auditů. Je třeba projít reference od současných klientů potencionálního partnera.
- Důležité by mělo být i ověření, zda mají potencionální partneři příslušné certifikace, například Certified Information Systems Auditor (dále jen CISA) nebo Certified Information Security Manager (dále jen CISM).
- Dalším důležitým krokem bude nalezení partnera, který má zkušenosti z oboru společnosti XYZ. Takový partner bude dobře rozumět specifickým bezpečnostním rizikům a požadavkům na shodu s předpisy.
- Dalším krokem ke zvážení je i velikost partnera. Větší firmy mohou mít více zdrojů a širší spektrum odborných znalostí, nicméně menší firmy mohou nabídnout individuální přístup a flexibilitu.
- Posledním krokem pro výběr bude i cena. Externí kybernetické audity mohou být nákladné. **Cena by neměla být rozhodujícím faktorem.**

3.7 Postup pro zlepšení fyzické bezpečnosti

Výsledky analýzy v softwaru Esko objevily několik nedostatků fyzické bezpečnosti. Na základě těchto nedostatků je třeba definovat cíle bezpečnosti. Příkladem takových cílů je:

- ochrana majetku společnosti,
- zabránění neoprávněnému přístupu,
- zajištění bezpečnosti zaměstnanců.

Po definování těchto cílů je třeba sestavit komplexní plán fyzické bezpečnosti. Ten může zahrnovat instalaci bezpečnostních IP kamer, použití opatření pro kontrolu přístupu a zavedení opatření, které odradí potencionálního narušitele.

V dalším kroku je třeba implementovat tento plán a zaučit zaměstnance společnosti. Po implantaci by mělo docházet k jeho pravidelnému testování, ověřování a aktualizaci.

Konkrétní návrhy na vylepšení současného stavu se nachází v příloze této práce.

3.8 Návrh řešení pro řízení přístupů

Řízení přístupů společnosti XYZ by mělo projít následujícími kroky, tak aby splňovalo doporučení MBS:

Určení a přidělení jedinečných identifikátorů. Společnost v současnosti používá systém zkratek, který ale není zaveden do všech systémů společnosti. Současný systém přidělení zkratek má navíc mezery. Tento systém by měl být aktualizován a zaveden na celou společnost.

Definování politiky pro Bring Your Own Device (dále jen BYOD). Ve společnosti je třeba definovat a zavést politiku pro kontrolu a monitorování používání osobních zařízení, která si zaměstnanci přinášejí na pracoviště. Prvním krokem je evidence mobilních zařízení, podrobněji pospaná v příští podkapitole.

Nadefinování a zavedení pravidel a postupů používání hardwaru a softwaru, které by mohly potenciálně ohrozit bezpečnost systému.

Jasné rozdělení privilegovaných účtů. Každý správce musí mít kromě privilegovaného účtu i účet pro ostatní činnosti. Servisní nebo technické účty používané informačním nebo komunikačním systémem musí být zdokumentovány a musí být určen jejich účel a postupy pro resetování hesel nebo certifikátů. Ve společnosti se v současnosti používá jeden administrátorský účet v rámci ERP systému.

Zavedení zásady need-to-know. „Pro všechny typy účtů musí být uplatněn princip need-to-know. To znamená, že každý účet má nastavena pouze taková oprávnění, která jsou nezbytná pro provádění činností odpovídajících pracovní pozici a náplni práce uživatele. Vedení organizace by nemělo být výjimkou a mělo by využívat běžné uživatelské účty. [3, s. 19]“

Společnost XYZ nemá v současnosti tento princip zaveden u svého BI systému. Všichni uživatelé vidí všechny subjekty. Tento stav musí být, co nejdříve napraven.

Za udělování a rušení přístupových práv musí být odpovědná pověřená osoba a tato činnost musí být koordinována s bezpečnostní politikou. Oprávnění k přístupu a jeho zrušení musí být zdokumentováno a zahrnuto do provozní a bezpečnostní dokumentace informačního nebo komunikačního systému. Společnost XYZ má v současnosti stanovenou osobu, která přidává a odebírá práva v systému. Společnost má nastavenou i zastupitelnost této osoby.

3.9 Návrh řešení pro evidenci mobilních zařízení

Současný stav používání a evidence mobilních zařízení byl ve společnosti určen jako nedostatečný. Návrh pro zlepšení je následující:

1) Zapsání mobilních zařízení do evidence společnosti a do softwaru Esko.
2) Evidence hrozeb u jednotlivých zařízení. Příkladem hrozby může být, že zaměstnanec není jediným uživatelem zařízení. Může tak dojít k vniknutí neoprávněné osoby do systému společnosti.
3) Na základě výsledků auditu můžou být podstoupeny následovné kroky:
    a. podstoupení hrozby u konkrétního zařízení,
    b. podstoupení zařízení do správy IT oddělení,
    c. pořízení malých pracovních stanic určených pro home office.

Nové mobilní zařízení by měly být automaticky přidávány do evidence společnosti XYZ.

Obrázek č. 22: Intel NUC
(zdroj: vlastní fotografie)

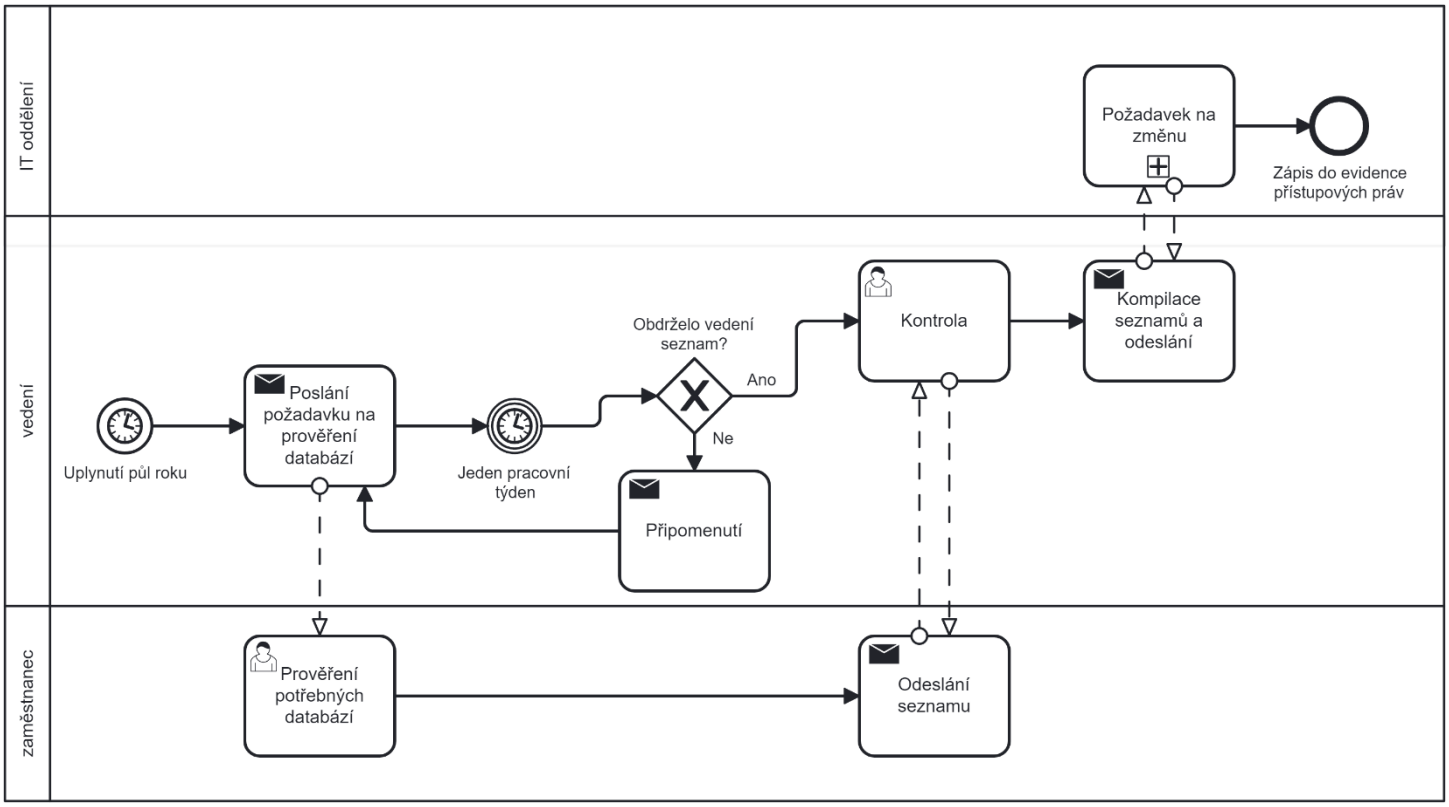
Společnost XYZ v současnosti používá Intel NUC, jako svoje pracovní stanice. IT oddělením byli navrženy i jako řešení pro mobilní zařízení kvůlí své velikosti. Alternativou je použití notebooku. Společnost v současnosti nemá preferovanou značku ani model.

3.10 Metodika pro odebrání přístupových práv

Z analýzy současného stavu vyplývá, že ve společnosti XYZ v současnosti chybí jasně definovaná metodika pro odebírání přístupových práv. ERP systémy od STORMWARU v současnosti nenabízí možnost vyjetí seznamu přidělených firem. IT oddělení nemůže navíc určit, kdy a kdo na jaké databázi pracuje. Vedení tedy po svých zaměstnancích jednou za nespecifikovanou dobu chce odeslat seznam databází, ke kterým potřebují přístup. Návrh upravené metodiky vypadá následovně:

1) Jednou za půl roku informuje vedení zaměstnance, aby prověřili svoje přístupy v ERP systému.
2) Zaměstnanci sestaví seznam databází, které potřebují pro svou práci. Ideálně v prostředí MS Excel. Tento seznam pošlou vedení.
3) Vedení zkontroluje seznamy a odsouhlasí.
4) Vedení odešle seznamy IT oddělení v rámci požadavku na změnu.
5) IT oddělení provede potřebné změny.

6) IT oddělení informuje vedení a zanese změny do evidence přístupových práv.



Obrázek č. 23: Diagram metodiky pro odebrání přístupových práv
(zdroj: vlastní fotografie)

Metodika odebrání přístupových práv by měla být pravidelně kontrolována a aktualizována.

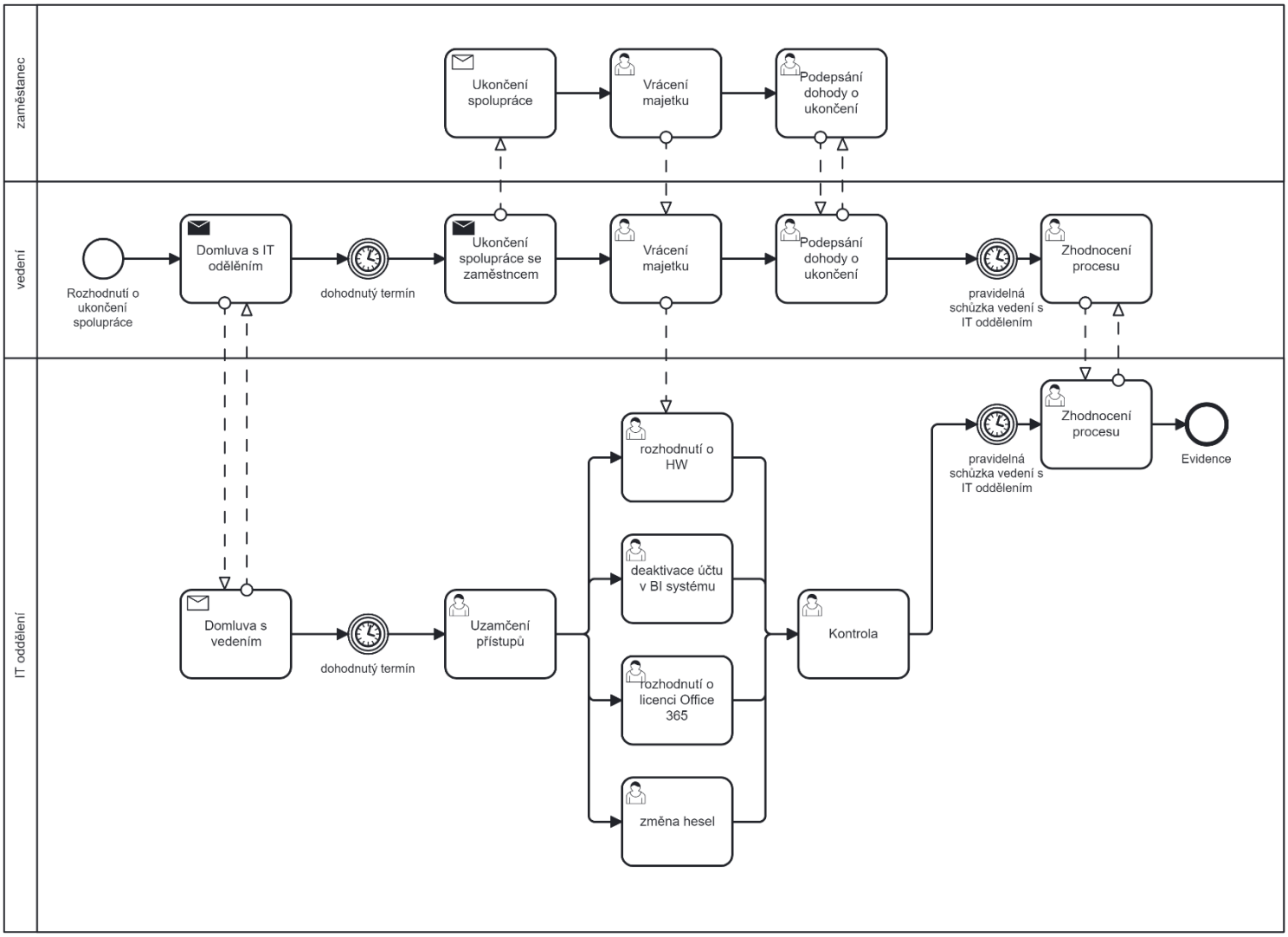
3.11 Metodika pro deaktivaci identit

V této podkapitole bude navržena metodika pro deaktivaci identit ve společnosti XYZ. Deaktivací indenty se rozumí zrušení uživatelských účtů a přístupových práv zaměstnanců, kteří opouštějí společnost. Tento proces je třeba rozdělit na dvě možnosti: zaměstnanec je propuštěn na základě svého nedostatečného výkonu nebo zaměstnanec opouští společnost na základě vlastního rozhodnutí.

Navrhovaný postup pro propuštění:

1) Vedení společnosti se rozhodne o propuštění zaměstnance.
2) Vedení informuje IT oddělení.
3) IT oddělení společně s vedením projde, k jakým aktivům má zaměstnanec přístup a určí termín pro deaktivaci.
4) V termínu deaktivace dojde k uzamčení přístupů a vedení informuje zaměstnance o propuštění.

5) Vedení se domluví na ukončení spolupráce se zaměstnancem. Domluví se na vrácení majetku společnosti.
6) IT oddělení projde následovnými kroky:
    a. deaktivuje účet v BI systému,
    b. rozhodne o licenci MS office 365,
    c. rozhodne o hardwaru,
    d. změna hesel u služeb, ke kterým měl zaměstnanec přístup,
    e. úprava bezpečnostních politik.
7) Zhodnocení ukončení spolupráce na příští poradě IT a vedení



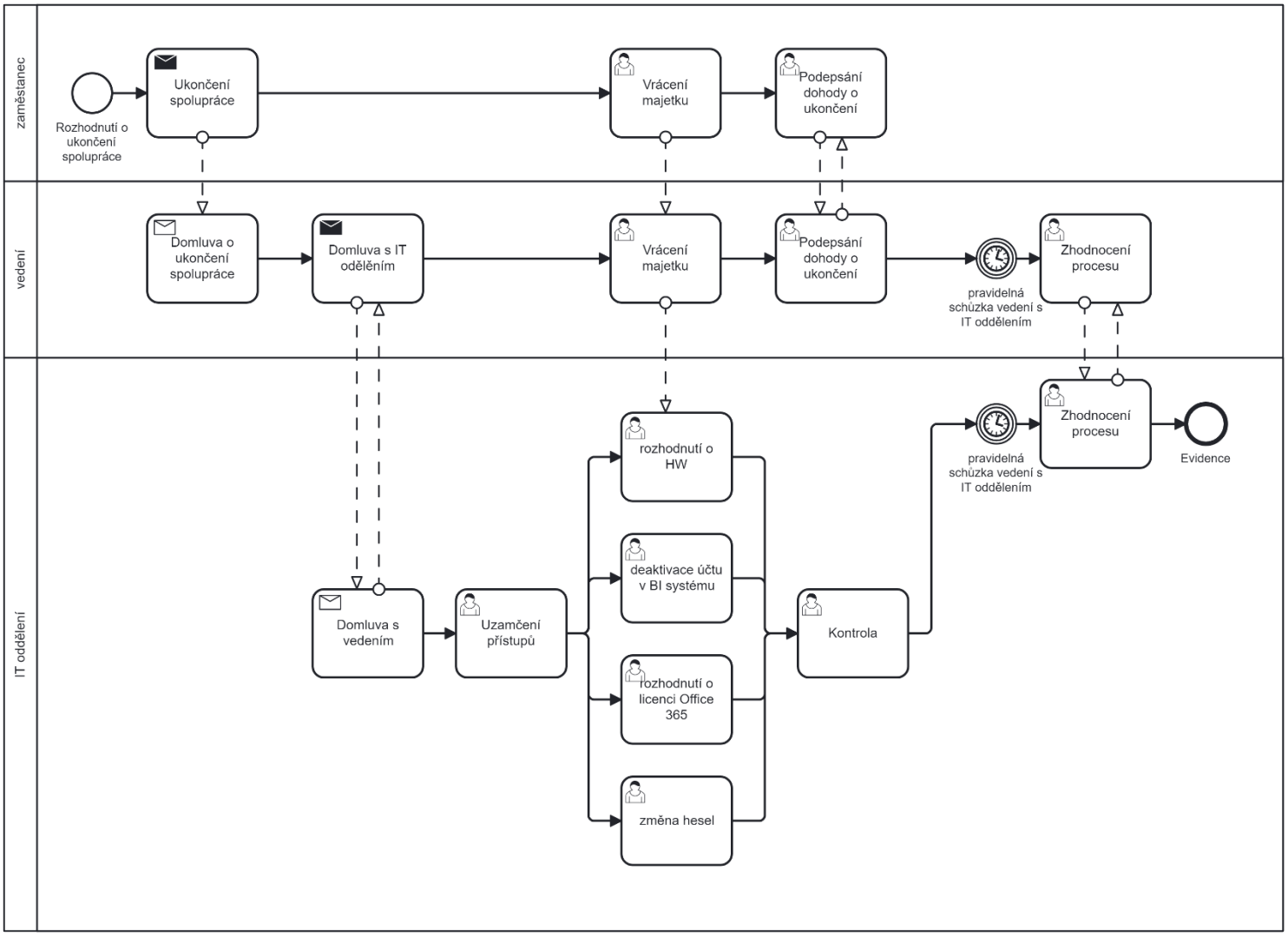
Obrázek č. 24: Diagram první metodiky pro deaktivaci identit
(zdroj: vlastní fotografie)

U první varianty je důležité, aby IT oddělení vědělo o propuštění předem. Bude tak připraveno na případnou aktivitu nespokojeného bývalého zaměstnance. Dojde k výraznému omezení potencionální útočné plochy. Pokud se jedná o zaměstnance, který

má přístup k citlivým informacím, jako například nedostatky bezpečnosti, musí dojít k co nejrychlejšímu řešení a eliminaci hrozby. Časové sladění pro tuto variantu je kriticky důležité.

Pro propuštění je navrhován následovný postup:

1) Zaměstnanec se rozhodne ukončit činnost ve společnosti a informuje vedení.
2) Vedení, co nejdříve informuje IT oddělení. Dojde k určení, k jakým aktivům má zaměstnanec přístup.
3) IT oddělení projde následovnými kroky:
    a. deaktivuje účet v BI systému,
    b. rozhodne o licenci office 365,
    c. rozhodne o hardwaru,
    d. změna hesel u služeb, ke kterým měl zaměstnanec přístup,
    e. úprava bezpečnostních politik.
4) Zhodnocení ukončení spolupráce na příští poradě IT a vedení.



Obrázek č. 25: Diagram druhé metodiky pro deaktivaci identit
(zdroj: vlastní fotografie)

Oproti první variantě nemá IT oddělení prostor se připravit na odchod zaměstnance. IT oddělení musí být vedením informováno co nejdříve.

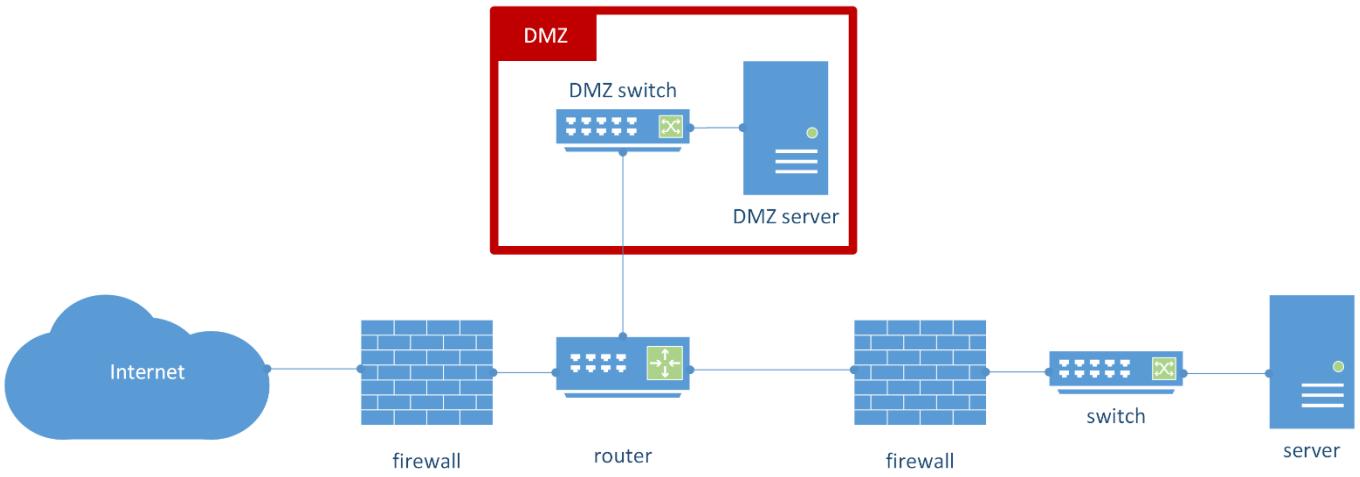
Oba procesy by měly být pravidelně kontrolovány a aktualizovány.

3.12 Návrh na segmentaci sítě

Doporučením pro zvýšení ochrany společnosti XYZ je vytvoření demilitarizované zóny (dále jen DMZ). DMZ slouží jako bezpečný bod připojení. V této zóně se uživatel dostane jen k omezeným zdrojům. Tato zóna by byla pro XYZ primárně určená pro klienty. Postup pro sestavení DMZ by mohl vypadat následovně:

1. Určení databází ERP systému Pohoda, které jsou kandidáty na přesunutí do DMZ.
2. Nakonfigurování firewallů nebo jiného síťové zařízení pro vytvoření DMZ.
3. Testování DMZ.
4. Sestavení zásad a postupů pro práci v DMZ.

5. Poučení a obeznámení zaměstnanců a klientů, kteří byli posunuti do DMZ.



Obrázek č. 26: Návrh segmentace sítě
(zdroj: vlastní fotografie)

Segmentaci je třeba řádně popsat a ideálně zakreslit. IT oddělení proto může použít prostředí MS Visia.

DMZ je třeba pravidelně monitorovat a aktualizovat, aby fungovala tak jak je zamýšlená.

3.13 Metodika při vzniku bezpečnostní události a incidentů

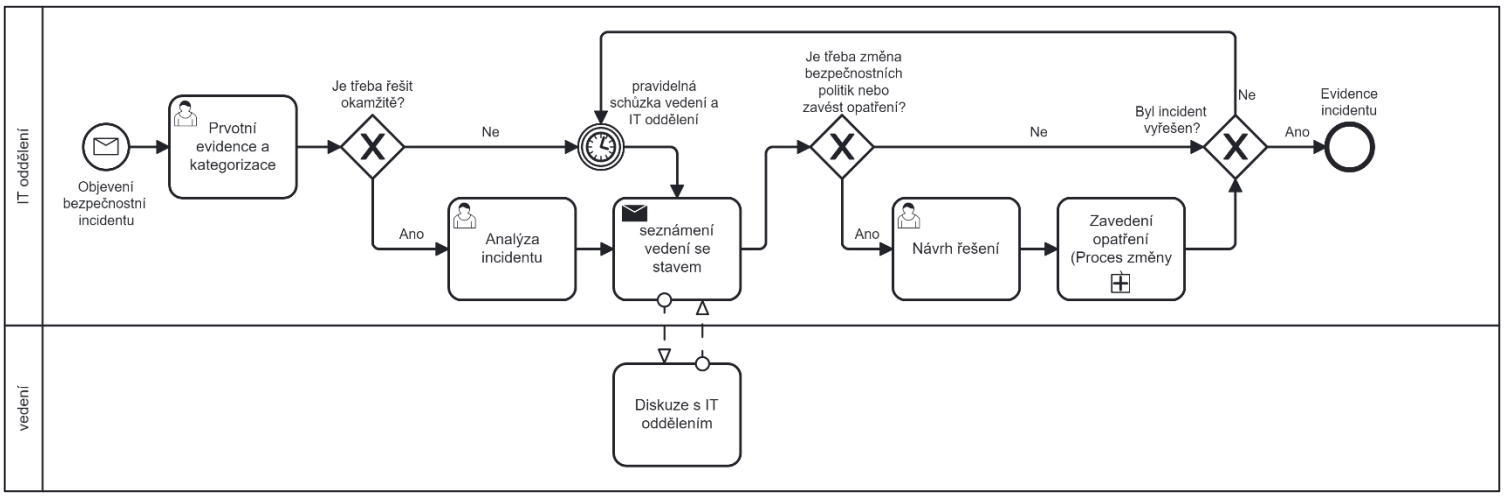
Z výsledku analýzy současného stavu je jasné, že současný stav řešení bezpečnostních událostí a incidentů je nedostačující. Navrhovaný postup pro zlepšení situaci je následující:

1. Určení zodpovědných osob.
2. Sestavení parametrů pro kategorizaci.

   „Pro potřeby hlášení a zvládání je třeba kategorizovat kybernetické bezpečnostní incidenty podle významnosti:

   - dopadů obsažených v dopadových určujících kritériích, podle kterých byly povinné osoby určeny,
   - počtu dotčených uživatelů,
   - způsobené nebo předpokládané škody,
   - důležitosti dotčených aktiv informačního a komunikačního systému,
   - dopadů na poskytované služby informačního a komunikačního systému,
   - dopadů na služby poskytované jinými informačními a komunikačními systémy,
   - délky trvání incidentu,
   - zeměpisného rozsahu dotčené oblasti a dalších dopadů. [5, s. 93]“
3. Sestavení systému pro evidenci incidentů.

4. Sestavení metodiky při vzniku nestandardní situace. Návrh této metodiky:
   4.1. IT oddělení obdrží informace o bezpečnostním incidentu.
   4.2. Kategorizace incidentu.
   4.3. Rozhodnutí, kdy bude zapojeno vedení.
   4.4. Diskuse s vedením.
   4.5. Rozhodnutí, zdali budou změněny bezpečnostní politiky společnosti nebo zdali budou zavedena nová opatření.
   4.6. Evidence, popis a uzavření bezpečnostního incidentu.
5. Seznámení zaměstnanců se systémem hlášení.



Obrázek č. 27: Diagram metodiky při vzniku bezpečnostní události a incidentů
(zdroj: vlastní fotografie)

Současný návrh počítá s tím, že bude vedení zapojeno do managementu incidentů.

Společnost XYZ musí být připravena v rámci této problematiky ještě na řešení dvou dalších témat.

Prvním je možnost, že se XYZ může stát dle české legislativy takzvanou povinou osobou. Povinné osoby mají povinnost hlášení bezpečnostních událostí a incidentů. Společnost by se měla na tuto možnost připravovat. Bude muset být určená zodpovědná osoba a bude muset být jasně nadefinovaný postup pro hlášení událostí a incidentů.

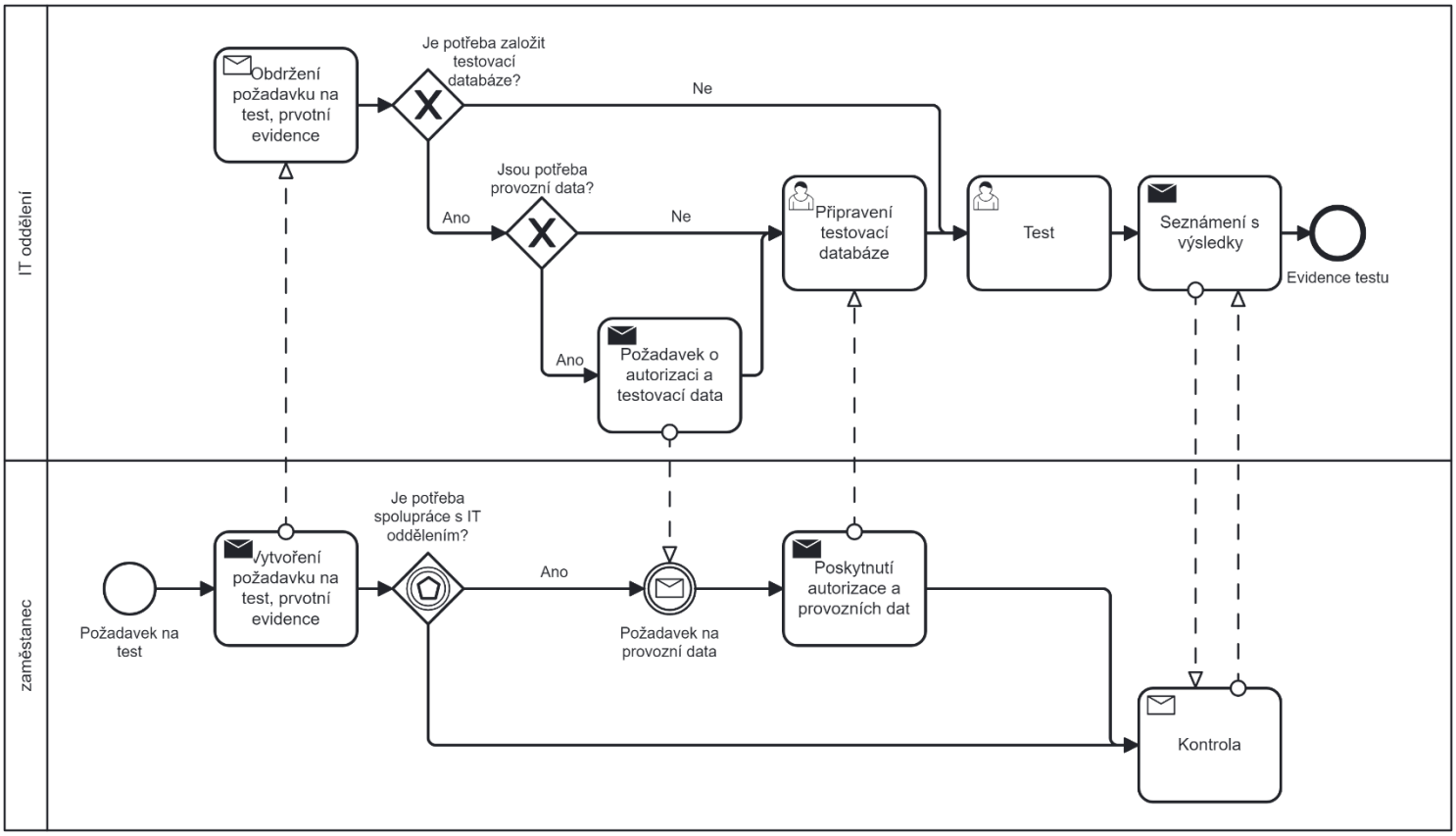
Druhým tématem je využití Security Information and Event Management. Jedná se o nástroj, který slouží ke zpracování, evidenci a analýze logů systémů organizace. Společnost zvažovala zavedení toho systému, ale nepodařilo se nalézt vhodný systém pro společnost.

3.14 Metodika testování ERP

V případě společnosti XYZ je většina jejích operací prováděna v rámci ERP systémů. To znamená, že když přijde nový klient, je třeba do jednotlivých systémů nahrát jeho data, aby bylo možné efektivně pokračovat v práci předchozího účetního. Kromě toho je třeba na těchto datech otestovat různé funkce, jako je import banky, automatická likvidace banky, import přijatých faktur.

Pro úspěšné testování systémů ERP je nezbytné dodržovat specifickou metodiku. Její návrh vypadá následovně:

1. IT oddělení obdrží požadavek na test funkcionality nebo test importu dat.
2. IT oddělení požadavek zaeviduje a rozhodne o parametrech:
    a. určení zodpovědné osoby,
    b. bude použita testovací databáze,
    c. budou použita provozní data,
    d. jaká bude příprava testovací databáze.
3. Zodpovědná osoba provede požadovaný test.
4. Dojde k vzájemné kontrole, zdali je výsledek vyhovující.
5. Uzavření požadavku a evidence testu.



Obrázek č. 28: Diagram metodiky testování ERP
(zdroj: vlastní fotografie)

Tuto metodika je potřeba pravidelně kontrolovat a případně aktualizovat.

3.15 Používání kryptografických prostředků

Na základě nové navrhované klasifikace informací vznikl pro společnost požadavek na použití kryptografických prostředků. Návrh postupu pro zavedení kryptografických prostředků je následující:

1. Určení zodpovědné osoby. Je třeba určit osobu, která bude ve společnosti odpovídat za implementaci a provoz kryptografických prostředků.
2. Analýza a posouzení kryptografických potřeb organizace. Na základě klasifikace informací je třeba provést komplexní analýzu.
3. Vypracování kryptografické politiky. Za pomocí best practices sestavit vhodnou politiku pro správné a efektivní využívání kryptografických prostředků.
4. Výběr vhodného šifrovacího algoritmu pro disky.

   „Dle aktuálního doporučení NÚKIB je pro šifrování disků možné použít následující symetrické blokové šifrovací algoritmy:

   1. Advanced Encryption Standard (AES) s využitím délky klíčů 128, 192 a 256 bitů
   2. Twofish s využitím délky klíčů 128 až 256 bitů

3. Serpent s využitím délky klíčů 128, 192, 256 bitů
4. Camellia s využitím délky klíčů 128, 192 a 256 bitů

Přitom mezi preferované patří AES, Camellia a Serpent (v uvedeném pořadí) a velikost klíče 256 bitů. [3, s. 28]“

5. Navrhnutí architektury pro kryptografické prostředky. Je třeba zajistit:
    a. bezpečnost architektury,
    b. škálovatelnost,
    c. soulad s českou legislativou.
6. Sestavení a implementace procesů pro správu klíčů. Pro fungování potřebují šifrovací algoritmy takzvané klíče. Ty slouží autorizovanému uživateli přístup k datům. Pro společnost XYZ bude třeba sestavit procesy pro jejich:
    a. generování,
    b. ukládání,
    c. distribuci,
    d. vyřazení.
7. Implementace vybraných kryptografických řešení.
8. Určení a školení vybraných zaměstnanců. IT oddělení společně s vedením společnosti určí, které osoby budou seznámeny a budou používat kryptografické prostředky.

Politiku a šifrovací algoritmy je třeba neustále kontrolovat a aktualizovat.

3.16 Test záložního systému

Z analýzy současného stavu vyplynulo, že XYZ má nachystaný záložní systém pro případ, kdy její současný systém vypadne. Přechod na záložní systém nebyl doposud otestován. Návrh přípravy na tento test vypadá následovně:

1. Ověření stavu záložního serveru. Ověření, zdali server funguje podle požadavků.
2. Ujištění, že starý server má nejnovější aktualizace všech ERP systému. Jednotlivé ERP systémy budou muset být zkontrolovány.
3. Ujistěte se, že starý server má nejnovější zálohu všech kritických dat, aplikací a konfigurací z primárního systému.
4. Určení nejvhodnějšího termínu pro XYZ. Na základě domluvy s vedením určit termín testu.
5. Informuje všechny zaměstnance a klienty o plánovaném testu a předpokládané době trvání přepnutí.

Pro samotný test je navržený následovný postup:

1. Provedení zálohy primárního serveru.
2. Vypnutí primárního serveru.
3. Kontrola procesu automatické detekce a aktivace záložního systému. Pokud nedojde k automatickému spuštění je třeba spustit přesun manuálně.
4. Ověření, zdali se na záložním serveru spustily všechny potřebné služby, aplikace a prostředky.
5. Ověření kritických funkcionalit:
    a. Přístupy a ověřování uživatelů.
    b. Integrity dat záložního systému oproti primárnímu.
    c. Výkonnost ERP systémů a ostatních služeb.
6. Identifikace všech problémů, které se během testu vyskytly.
7. Ukončení testu, spuštění a přechod na primární systém.
8. Ověření, zdali se primární systém obnovil správně a poskytuje všechny služby, aplikace a prostředky a zda k nim mají uživatelé bezproblémový přístup.
9. Dokumentace výsledků testu.

Po provedení testu by měly následovat tyto kroky:

1) Prozkoumání nedostatků, které se během testu ukázaly.
2) Vypracování návrhu úprav pro fungování záložního systému.
3) Aktualizace DRP a BCP na základě výsledků testu. Například dojde k získání jasných hodnot pro dobu obnovy, jak záložního, tak primárního systému.

Tento test by se měl pravidelně opakovat. Společnost XYZ, tak bude mít pravdivé a věrohodné hodnoty pro DRP a BCP.

Společnost by měla v podobné podobě otestovat druhý záložní systém v záložní lokalitě.

3.17 Zálohování pro ERP systém VEMA a BI/CRM systém

Na základě analýzy současného stavu vyplývá, že ve firemních pravidlech záloh chybí sekce týkající se ERP systému VEMA a BI/CRM systému Praetor. Tyto systémy jsou pro XYZ specifické a liší se od ERP systému od společnosti STORMWARE jak použitím, tak i rozsahem.

Systém VEMA i Pohoda, pracují na bázi databází, kam se ukládají data z podnikových procesů. Tyto databáze umožňují ukládat a spravovat různé typy dat, jako jsou účetní záznamy, faktury, objednávky, zákaznické kontakty, stav výroby, zásoby a další. V současnosti XYZ využívá

systém VEMA minimálně, a to pro vedení mzdové agendy. Návrh postupu pro zálohování ERP systému VEMA je tedy navržen podle současného stavu a zaměření společnosti. Návrh zálohování zní takto:

- Automatická každodenní záloha. Její přesný čas by byl určen po sérii testů. Drží se zálohy zpětně za 30 dní.
- Provedení manuální zálohy po uzavření měsíce. Na základě pokynu od zodpovědného zaměstnance dojde k vypracování zálohy databáze. Tyto zálohy se krom archivu a ostatních disků nakopírují i na cloud od Googlu. Drží se zálohy zpětně za 30 dní.
- Pravidelná čtvrtletní archivní záloha.

Na druhé straně má systém Praetor ve společnosti XYZ speciální místo. Krom funkcionalit controllingu slouží také jako CRM systém a v prostředí databáze Praetoru jsou uchována citlivá data hned několika oddělení společnosti XYZ. Proto je důležité, aby byly zálohy Praetoru vytvářeny s maximální opatrností a aby zahrnovaly jak databázi, tak i datovou složku v souborovém systému, kde jsou uchovávána data a dokumenty související s CRM funkcionalitou.

Pro zálohování Praetoru je navržen následovný postup:

- Každý den v 23:00 se zálohuje SQL databáze systému Praetor pomocí nástroje pro zálohování databáze, např. SQL Server Management Studio. Záloha se ukládá na oddělený disk D a na NAS na disk Z. Drží se zálohy zpětně za 30 dní.
- Jednou měsíčně se provádí zálohování do cloudového úložiště Google. Doporučuje se použít šifrování pro zabezpečení dat. Záloha by měla být spuštěna na základě pokynu, že byl uzavřen předešlý měsíc a sestaveny reporty v Praetoru. Doporučuje se držet zálohy zpětně za dva měsíce.
- Čtyřikrát do roka se provede ruční archivní záloha na externí disk nebo jiné oddělené zařízení. Konkrétně se doporučují měsíce únor, květen, srpen, listopad.

3.18 Nový web společnosti XYZ

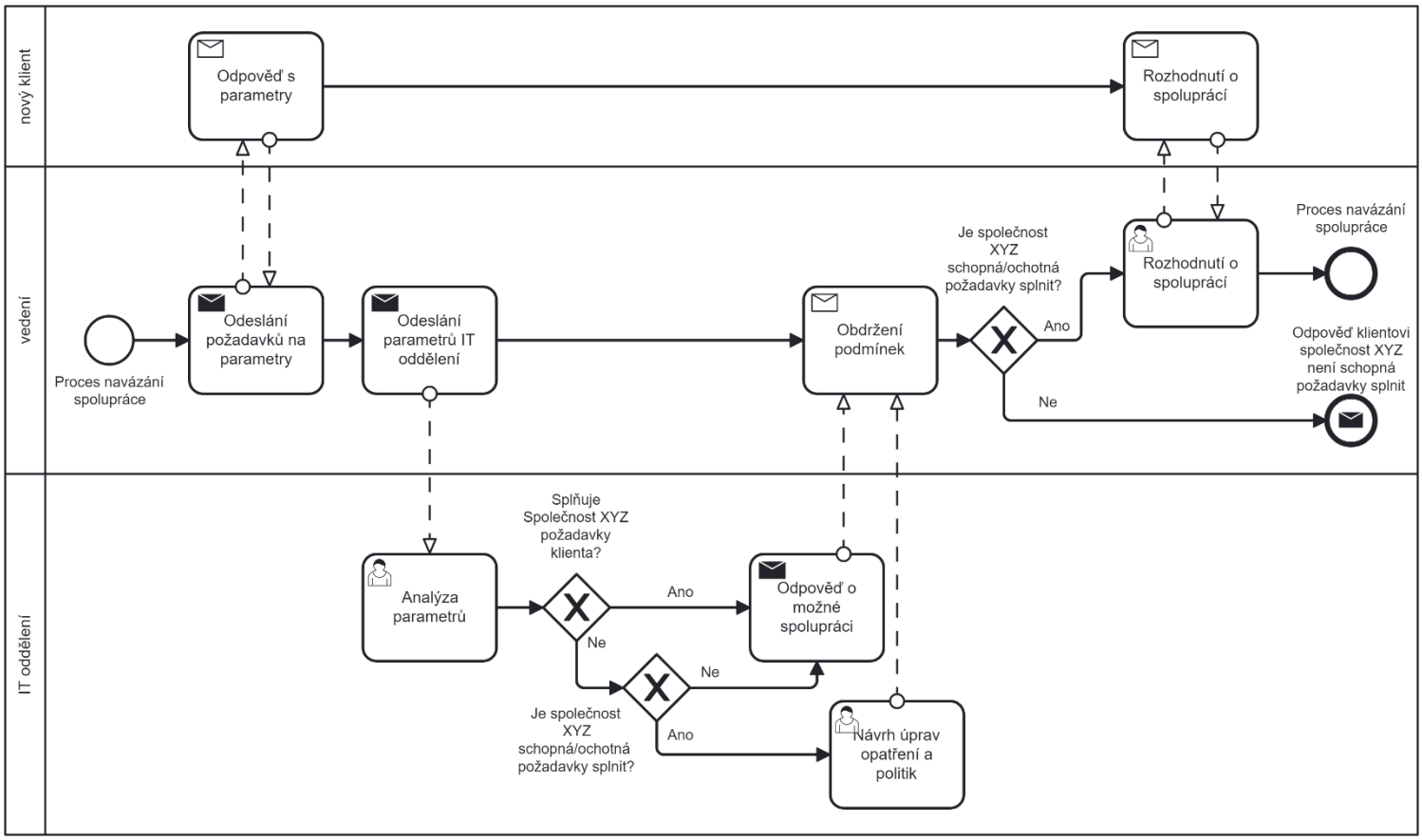
Společnost XYZ plánuje na rok 2023 spuštění nového webu. Konkrétní technické a bezpečnostní parametry nejsou doposud známé. Webová aplikace bude outsourcovaná i tak by mělo dojít k prověření best practices. „Podle tzv. best practices je nutné věnovat pozornost především následujícím známým zranitelnostem:

- Cross Site Scripting (XSS). XSS je metoda narušení webových stránek využitím bezpečnostních chyb ve skriptech (především neošetřené vstupy).
- Injection útoky. SQL injection je technika napadnutí databázové vrstvy programu vsunutím (injection) kódu přes neošetřený vstup a vykonání vlastního, pozměněného, SQL dotazu. Vedle SQL injection existují též další podobné scénáře s jiným cílem, např. shell command injection, LDAP injection atd.
- Vzdálené spuštění kódu. Buď vlivem zranitelnosti v samotném webovém serveru, použitém frameworku či logice ve webové aplikaci.
- Nezabezpečený přímý popis objektu. Zranitelnosti této kategorie umožňují útočníkovi získat informace o jednotlivých objektech cílové aplikace bez patřičné autentizace.
- Cross Site Request Forgery (CSRF). CSRF je technika, která umožňuje útočníkovi podvrhnout formulář na jiné stránce nebo pomocí některých HTTP metod přesměrovat prohlížeč oběti na skript zpracovávající legitimní formulář aplikace s daty, která můžou oběť poškodit.
- Únik informací nebo nedostatečné řízení chyb. Zranitelnosti tohoto typu útočníkovi zpřístupňují v případě chybového stavu aplikace informace, které lze později použít k lepšímu plánování útoku.
- Špatná autentizace a správa relace. Zranitelnosti tohoto typu umožňují útok na přihlašovací části aplikace či úplné obcházení přihlašovacího systému.
- Nezabezpečené kryptografické úložiště. Zranitelnosti tohoto typu můžou způsobit kompromitaci privátního šifrovacího klíče jedné či obou stran spojení.
- Nezabezpečená komunikace. Zranitelnosti tohoto typu umožňují útočníkům odchytávat komunikaci, která jim není určená, a provádět též aktivní útoky typu Man-in-the-Middle.
- Chybné zamezení URL přístupu. V případě, že aplikace umožňuje neautentizovaný přístup i ke stránkám, ke kterým by měl být přístup jen po příslušné autentizaci, je možnou zranitelností situace, kdy takto odkazovaná stránka zobrazí některé informace, které by měly být přístupné jen konkrétním autorizovaným uživatelům, či systémové informace citlivého charakteru. [3, s. 34]“

3.19 Doplnění procesu získání nového klienta

Z analýzy současného stavu vyplývá, že XYZ v současnosti neřeší bezpečnost při získání nového klienta. Do procesu byl tak zakomponován návrh na tento postup:

1) Ověření a doplnění následujících parametrů:
   a) Je klient povinnou osobou podle ZKB.
   b) Je klient významný dodavatel pro poskytovatele kritické infrastruktury.
   c) Forma komunikace.
   d) V jakých ERP systémech budou data klienta.
   e) Bude klient požadovat připojení do ERP systému.
   f) Specifické požadavky klienta na bezpečnost.
2) Návrh postupů podle jednotlivých parametrů.
3) Odpověď na otázku, zdali bude potřeba upravit opatření nebo politiku společnosti?
4) Seznámení klienta s bezpečnostními postupy společnosti XYZ.
5) Souhlas od klienta s bezpečnostními pravidly. Souhlas by měl být součástí návrhu smlouvy o spolupráci.



Obrázek č. 29: Diagram doplnění procesu získání nového klienta
(zdroj: vlastní fotografie)

Tuto metodiku je potřeba pravidelně kontrolovat a případně aktualizovat.

3.20 Audit externích systémů a jejich hodnocení

Na základě analýzy současného stavu byly rozpoznány tři základní typy externích systémů. Tyto systémy jsou:

- **Systémy úřadů:** Jako poskytovatel účetních a finančních služeb musí společnost XYZ spolupracovat s různými regulačními orgány, daňovými úřady a finančními institucemi. Společnost XYZ na systémy evropského celního úřadu odesílá například reporty Intrastatu.
- **Systémy klientů:** Zaměstnanci společnosti XYZ potřebují od některých klientů získat data přístupem do jejich systému. Příkladem může být třeba stažení podkladů pro agendu přijatých faktur.
- **Systémy dodavatelů:** Příkladem komunikace se systémem dodavatele je například řešení nové funkcionality. Dodavatel potřebuje zaslat vzorová data, aby mohl na funkcionalitě pracovat. Společnost STORMWARE používá například pro tuto komunikaci vlastní zabezpečené webové uložiště.

Prvotním krokem pro zvýšení zabezpečení komunikace bude pro společnost úplná klasifikace a identifikace informací. Po ukončení této analýzy bude potřeba jednotlivé informace projít a rozdělit za pomoci VKB.

„Komunikace s externími informačními nebo komunikačními systémy by měla být rozdělena podle stupně zabezpečení na:

- zabezpečený kanál přenosu (šifrování dat) s povinnou úrovní zabezpečení koncových bodů informačního nebo komunikačního systému na úrovni infrastruktury,
- šifrování dat pro přenos a autorizací uživatele v rámci informačního nebo komunikačního systému,
- zajištění šifrování nebo náhradu citlivých dat na úrovni poskytovatelských a konzumentských informačních nebo komunikačních systémů pomocí end to end metody při přenosu dat. [3, s. 36]“

4 Přínosy a náklady pro společnost XYZ

V následující kapitole budou sepsány možné přínosy a náklady spojené s procesem zavedení minimálního bezpečnostního standardu. Na závěr této kapitoly bude sestaven hrubý finanční plán celého procesu.

4.1 Přínosy pro společnost XYZ

Na základě předchozích kapitol byla sestavena tabulka názvů podkapitol a jednotlivých očekávaných přínosů. V této podkapitole budou následovně tyto přínosy podrobněji popsány. Budou k nim přidány i obecné příklady.

Název podkapitoly	Přínos
Návrh řešení pro klasifikaci a ochranu informací	Zlepšení zabezpečení informací, snížení nákladů, jasnější zodpovědnosti a odpovědnosti
Návrh řešení pro řízení dodavatelů	Získání přehledu o dodavatelích, lepší kontrola dodavatelů, možnost stanovení kompenzací
Návrh řešení pro řízení lidských zdrojů	Minimalizace rizik, zlepšení firemní kultury, menší vytížení IT oddělení, lepší rozhodování, lepší schopnost řešit problémy
Návrh řešení pro řízení změn	Minimalizace rizik, minimalizace výpadků a zajištění kontinuity provozu, jasný přehled o změnách
Návrh řešení pro řízení kontinuity činností	Zlepšení spolupráce jednotlivých oddělení, omezení dopadu katastrofy, minimalizace rizik, minimalizace výpadků, zajištění kontinuity provozu, lepší schopnost řešit problémy
Interní a externí audit kyberbezpečnosti	Ověření správnosti bezpečnostních politik, získání best practices, podklad pro certifikaci
Postup pro zlepšení fyzické bezpečnosti	Větší bezpečnost kritických prvků, zvýšení bezpečnosti zaměstnanců
Návrh řešení pro řízení přístupů	Omezení přístupu neoprávněné osoby k citlivým údajům, získání většího přehledu přístupových práv
Návrh řešení pro evidenci mobilních zařízení	Omezení útočného vektoru, získání přehledu o mobilních zařízeních, určení garantů
Metodika pro odebrání přístupových práv	Omezení přístupu neoprávněné osoby k citlivým údajům, jasně stanovený postup
Metodika pro deaktivaci identit	Omezení útočného vektoru bývalého zaměstnance, jasně stanovený postup pro deaktivaci, zlepšení spolupráce jednotlivých oddělení
Návrh na segmentaci sítě	Omezení útočného vektoru, lepší schopnost řešit problémy
Metodika při vzniku bezpečnostní události a incidentů	Jasně stanovený postup po bezpečnostním incidentu, zlepšení spolupráce jednotlivých oddělení, jasnější zodpovědnosti a odpovědnosti
Metodika testování ERP	Jasně stanovený postup pro testování, zrychlení procesu, jasnější zodpovědnosti a odpovědnosti
Používání kryptografických prostředků	Zvýšené zabezpečení a ochrana citlivých dat, jasnější zodpovědnosti a odpovědnosti
Test záložního systému	Získání přehledu o funkčnosti záložního systému, získání hodnot pro DRP a BCP
Zálohování pro ERP systém VEMA a BI/CRM systém	Lepší ochrana kritických obchodních dat, lepší dostupnost a přístupnost kritických podnikových dat, minimalizace výpadků, zajištění kontinuity provozu
Nový web společnosti XYZ	Získání důvěry k dodateli webu
Doplnění procesu získání nového klienta	Zlepšení spolupráce jednotlivých oddělení, lepší rozhodování
Audit externích systémů a jejich hodnocení	Zlepšení zabezpečení informací, jasnější zodpovědnosti a odpovědnosti, získání přehledu o dodavatelích

Obrázek č. 30: Tabulka přínosů
(zdroj: vlastní fotografie)

Splnění navržených postupů může pro společnost znamenat zlepšení v několika oblastech. Přínosy pro bezpečnost a kontinuita provozu v rámci společnosti XYZ jsou následující:

- **Minimalizace rizik:** Zavedením minimálního bezpečnostního standardu může ve společnosti dojít minimalizaci rizik. Díky lepšímu chápání stavu bezpečnosti společnosti můžou být lépe identifikována jednotlivá rizika. S takovými riziky se i díky navrhovaným nástrojům bude lépe pracovat.
- **Snížení nákladů:** Díky zavedení minimálního bezpečnostního standardu může XYZ omezit svoje náklady, a to například díky:
    - Vyhnutí se pokutám a sankcím spojeným s nedodržováním předpisů.
    - Snížením počtu bezpečnostních incidentů.
    - Nižším nákladům na nápravu bezpečnostních incidentů.
    - Vyšší efektivitě zaměstnanců a firemních procesů.
- **Lepší jméno společnosti:** Dobře pojatá a odprezentována bezpečnost může zlepšit pozici společnosti a pomůže jí získat konkurenční výhodu.
- **Minimalizace dopadu:** Dobře zavedené minimální bezpečnostní standardy může mít za následek minimalizaci dopadu bezpečnostního incidentu. Jasně stanovené postupy a odpovědnosti zaručí, že incidenty budou řešeny rychleji a efektivněji.
- **Lepší rozhodování:** Zavedení MBS ve společnosti XYZ může pomoci zaměstnancům, IT oddělení a vedení společnosti při rozhodování. Bezpečnostní postupy a politiky, které z něj vycházejí můžou sloužit k jednodušší identifikaci rizik, definování cílů a priorit, a následně i k vytvoření a implementaci účinných bezpečnostních opatření.
- **Jasný přehled o změnách:** Získání jasného přehledu o změnách pomůže v XYZ snižovat zmatky a zároveň pomůže zlepšit komunikaci. Členům IT oddělení, ale i vedení pomůže tento přehled při rozhodování. Například při koupi nového serveru se po nahlédnutí do evidence omezí výběr na značky, se kterými měla společnost v minulosti problémy. Lepší přehled o změnách také pomáhá při forenzním pátrání, protože může být snazší zjistit, proč došlo k výpadku. Například pokud člen IT oddělení aktualizuje ERP systém, ale zapomene aktualizovat záložní systém, to může vysvětlit, proč nedošlo k úspěšnému naběhnutí záložního systému.
- **Lepší schopnost řešit problémy:** Postupy pro řešení nestandardních situací, BCP a DRP umožňují společnosti a jejím zaměstnancům efektivněji řešit problémy. Zodpovědná osoba se může obrátit na již připravené postupy pro řešení problémů, což

může ušetřit čas a náklady. Tyto postupy také pomáhají minimalizovat dopady nečekaných událostí a urychlit obnovu činnosti v případě výpadku nebo krize.

- **Minimalizace výpadků a zajištění kontinuity provozu:** Dobře stanovené postupy pro řešení nestandardních situací, BCP a DRP bude mít za efekt snížení doby výpadku. Jsou jasně určené zodpovědné osoby a postupy. Například při selhání jednoho aktivního prvku víme přesně jaká osoba je zodpovědná, nemusí tak dojít k zapojení celého IT oddělení.

Pro oblast řízení lidských zdrojů jsou možné přínosy následující:

- **Zvýšení bezpečnosti zaměstnanců:** Jasně definovaná pravidla pro bezpečnost mohou mít pozitivní vliv na morálku a efektivitu zaměstnanců, kteří pracují s pocitem bezpečí. Zaměstnanci budou mít větší důvěru v XYZ. To může vést ke snížení stresu a lepší spokojenosti s prací.
- **Zlepšení firemní kultury:** Dobré vzdělávání ostatních zaměstnanců v oblasti bezpečnosti může vést k sestavení firemní kultury, ve které je kyberbezpečnost zahrnuta jako součást celkového přístupu. Takový stav by ve společnosti mohl znamenat, že zaměstnanci sami přichází s novými nápady a inovacemi. Aktivně by se tak podíleli na bezpečnostních opatřeních. Zaměstnanci tak mohou získat pocit, že jsou aktivními účastníky bezpečnostní kultury společnosti. Tento přístup může vést ke zlepšení efektivity, snížení nákladů a zvýšení celkové spokojenosti zaměstnanců s jejich prací.
- **Zlepšení spolupráce jednotlivých oddělení:** Díky jasně stanoveným postupům a odpovědnostem se dá očekávat lepší spolupráce jednotlivých oddělení.
- **Menší vytížení IT oddělení:** Dobré vzdělávání ostatních zaměstnanců v oblasti bezpečnosti může vést ke snížení pracovní zátěže oddělení IT. Zaměstnanci se například nebudou na IT oddělení obracet s jakýmkoliv podezřením na phishingový útok, posoudí hrozbu podle svých znalostí. Podobný efekt bude mít i dobře vypracovaný bezpečnostní manuál. IT oddělení se tak může plně soustředit na svoji prací a dojde k úspoře jejich zdrojů.
- **Jasně stanovený postup:** Pokud jsou kroky správně popsány, tak je možné jasně určit, jakým způsobem postup vykonat. To umožní každému oddělení stanovit, kdy a za jakých okolností se zapojit do tohoto procesu. Díky jasnému popisu postupu lze jednotlivé kroky vykonávat efektivněji, protože zaměstnanci nemusí trávit čas hledáním informací o tom, jak daný postup provést. Standardizované postupy také umožní společnosti snadněji měřit výkonnost.

- **Jasnější zodpovědnosti a odpovědnosti:** Správně nadefinované odpovědnosti a zodpovědnosti vedou k větší efektivitě na pracovišti. Pokud zaměstnanci jasně chápou své role a odpovědnosti, je pravděpodobnější, že převezmou odpovědnost za svou práci a budou zodpovědní za své činy. To může přispět ke snížení nedorozumění, omezení konfliktů a k méně chybám. Dojde také ke zlepšení komunikace a spolupráce mezi zaměstnanci, tak i mezi jednotlivými odděleními. Jasně definované povinnosti a odpovědnosti navíc mohou přispět ke zvýšení produktivity, protože zaměstnanci se mohou soustředit na svoji práci.

Přínosy oblasti řízení dodavatelů můžou být následovné:

- **Lepší kontrola dodavatelů:** Lepší kontrola dodavatelů může mít pro XYZ za následek snížení rizika podnikání, zlepšení kvality poskytovaných služeb a může vést i k optimalizaci nákladů. Na základě evidence může například společnost dojít k závěru, že pro stejnou službu používá dva rozdílné dodavatele. Na základě tohoto zjištění tak omezí svoje náklady a službu bude odebírat jen od jednoho. Za pomoci dobře vedené evidence dodavatelů může taky společnost získat přehled, jak jednotliví dodavatelé splňují podmínky stanovené ve svých smlouvách. To může pomoci předcházet problémům spojenými s nedostatky služeb, dodržováním termínu anebo problémy s legislativou. Díky lepší kontrole dodavatelů může XYZ budovat pevnější vztahy s dodavateli, což může vést k větší spolupráci, inovacím a vytváření lepších hodnot.
- **Možnost stanovení kompenzací:** Výsledkem dobrého řízení dodavatelů může být i evidence nedostatků dodavatelů. To může vést k sestavení robustnějšího SLA s dodavateli společnosti. Tyto smlouvy můžou obsahovat doložky o proplácení pokut společnosti XYZ při výpadku, čí jiném nedostatku.

Přínosy pro oblast dat mohou bát následující:

- **Lepší dostupnost a přístupnost kritických podnikových dat:** Při správném nastavení zálohovací politiky získá XYZ jasný přehled, kdy a kde jsou zálohována její citlivá a kritická data. Zodpovědná osoba, tak bude přesně vědět, jaká data jsou k dispozici a jaká již ne v případě bezpečnostního incidentu.
- **Lepší ochrana kritických obchodních dat:** Lepší ochrana kritických dat zajistí, že data společnosti neskončí u neoprávněné osoby, která by je mohla zneužít proti společnosti. Příkladem takového zneužití je například prodej dat klientů konkurenci, prodej dat na černém trhu anebo přímé vydírání společnosti XYZ.

- **Omezení útočného vektoru:** Příkladem omezení útočného vektoru je segmentací sítě, kdy dojde k omezení možných vstupních bodů do systémů společnosti. Útočník tak musí projít přes další vrstvu ochrany společnosti. Dalším příkladem je dobře nastavená politika ukončení spolupráce, která může IT oddělní sloužit jako nástroj pro efektivní omezení útočného vektoru bývalého zaměstnance. Při dodržení navrženého postupu jsou omezené jeho možnosti páchat škody v systémech XYZ.

Přínos doplnění evidence mobilních zařízení je následovný:

- **Získání přehledu o mobilních zařízeních:** Evidence mobilních zařízení nabízí přínos v podobě získání většího přehledu zařízení, na kterých zaměstnanci pracují. Umožní určit zařízení která jsou riziková a musejí se řešit. Součástí evidence je i určení garanta aktiva, určí se tak zodpovědná osoba za případný problém.

Na základě provedení testu záložního systému lze očekávat tyto přínosy:

- **Získání přehledu o funkčnosti záložního systému:** Provedení testu záložního systému prověří, zdali je systém funkční a splňuje požadavky společnosti XYZ.
- **Získání hodnot pro DRP a BCP:** Provedení testu záložního systému umožní IT oddělení získat reálné hodnoty doby obnovy (RTO) a cíle bodu obnovy (RPO), které jsou podstatné pro sestavení DRP a BCP.

Přínosy projitím externího auditu jsou následovné:

- **Ověření správnosti bezpečnostních politik:** Ověřením od externího specialisty dojde k ověření, že bezpečnostní politiky ve společnosti jsou dobře nastavené a jsou správně používané.
- **Získání best practices:** Externí specialista může poskytnout best practices z trhu, které můžou být podkladem pro další vylepšení bezpečnostních politik ve společnosti XYZ.
- **Podklad pro certifikaci:** Externí a interní audit může sloužit jako podklad pro certifikaci společnosti. Bezpečnostní certifikát posílí dobré jméno společnosti a může přilákat novou klientelu.

4.2 Náklady pro společnost XYZ

Na základě předchozích kapitol byla sestavena tabulka názvů podkapitol a jednotlivých odhadovaných nákladů. V této podkapitole budou následovně tyto přínosy podrobněji popsány.

Název podkapitoly	Náklady
Návrh řešení pro klasifikaci a ochranu informací	Práce IT oddělení, spolupráce vedení, tabulka office 365
Návrh řešení pro řízení dodavatelů	Práce IT oddělení, spolupráce vedení, tabulka office 365
Návrh řešení pro řízení lidských zdrojů	Práce IT oddělení, spolupráce vedení, spolupráce zaměstnanců, dokument office 365
Návrh řešení pro řízení změn	Práce IT oddělení, spolupráce vedení, tabulka office 365, editor diagramů BPMN
Návrh řešení pro řízení kontinuity činností	Práce IT oddělení, spolupráce vedení, spolupráce vybraných osob, tabulky office 365
Externí audit kyberbezpečnosti	Externí auditor, Spolupráce IT oddělení, spolupráce vedení,
Postup pro zlepšení fyzické bezpečnosti	Práce IT oddělení, spolupráce vedení, ESKO, náklady spojené s facility
Návrh řešení pro řízení přístupů	Práce IT oddělení, spolupráce vedení, dokument office 365
Návrh řešení pro evidenci mobilních zařízení	Práce IT oddělení, spolupráce vedení, ESKO, nový HW
Metodika pro odebrání přístupových práv	Práce IT oddělení, spolupráce vedení, dokument office 365, editor diagramů BPMN
Metodika pro deaktivaci identit	Práce IT oddělení, spolupráce vedení, tabulka office 365, editor diagramů BPMN
Návrh na segmentaci sítě	Práce IT oddělení, diagram office 365
Metodika při vzniku bezpečnostní události a incidentů	Práce IT oddělení, spolupráce vedení, tabulka office 365, editor diagramů BPMN
Metodika testování ERP	Práce IT oddělení, tabulka office 365, editor diagramů BPMN
Používání kryptografických prostředků	Práce IT oddělení, spolupráce vedení, tabulka office 365
Test záložního systému	Práce IT oddělení, dokument office 365, editor diagramů BPMN, jeden provozní den
Zálohování pro ERP systém VEMA a BI/CRM systém	Práce IT oddělení, dokument office 365
Nový web společnosti XYZ	Dodavatel webu, spolupráce IT oddělení
Doplnění procesu získání nového klienta	Práce IT oddělení, spolupráce vedení, dokument office 365, editor diagramů BPMN
Audit externích systémů a jejich hodnocení	Práce IT oddělení, spolupráce vedení, tabulka office 365

Obrázek č. 31: Tabulka nákladů
(zdroj: vlastní fotografie)

Splnění navržených postupů může pro společnost XYZ znamenat náklady v několika oblastech.

Náklady na interní lidské zdroje jsou následující:

- **Práce IT oddělení:** Hlavním řešitelem bezpečnosti ve společnosti XYZ bude IT oddělení. Členové IT oddělení tak nebudou moci vykonávat svoji normální činnost a společnosti XYZ vzniknou náklady. S prací na bezpečnosti budou spojené různé činnosti, za které bude IT oddělení odpovědné. Příklady takových činností může být:

    - zavedení metodiky,
    - zavedení evidence,
    - zavedení a popis postupu,
    - vypracování bezpečnostních politik,
    - testování,
    - zaškolení zaměstnanců.
- **Spolupráce IT oddělení:** IT oddělení bude u některých činností pouze spolupracovat a nebude za jejich průběh odpovědné. Příkladem je kontrola nového webu nebo externí audit.
- **Spolupráce vedení:** U některých činností bude potřeba spolupráce vedení. Vedení zde může sloužit například v poradenské roli nebo roli zprostředkovatele. Vzniknou tak náklady pro společnost, neboť se vedení nemůže věnovat své práci.
- **Spolupráce zaměstnanců:** Náklady vzniknou i ze strany zaměstnanců**.** Spolupráce zaměstnanců bude například potřebná při schválení podoby manuálu a školení.
- **Spolupráce vybraných osob:** Při sestavování bezpečnostních postupů jako jsou BCP a DRP bude potřeba spolupráce vybraných osob, která tak nebudou moci vykonávat svoji činnost.
- **Jeden provozní den:** V rámci testování záložního systému bude potřeba obětovat jeden provozní den celé společnosti. Společnost XYZ potřebuje ověřit, zdali její systém zálohy bude fungovat i při plném zatížení, pro termín testu tak musí určit jeden z pracovních dnů .

Pořízení majetku:

- **Náklady spojené s facility:** Na základě výsledků analýzy současného stavu a analýzy v softwaru Esko vyšlo na povrch několik nedostatků. S nápravou těchto nedostatků budou spojené náklady pro společnost XYZ.
- **Nový HW:** Výsledkem navrhované analýzy mobilních zařízení může být požadavek na pořízení nového hardwaru pro zaměstnance společnosti XYZ.

Náklady na SW nástroje:

- **MS Office 365:** Pro jednotlivé evidence, tabulky a diagramy se v současnosti navrhuje použít služeb office 365, ke kterým má společnost v současnosti licence a používá je. V současném prostředí nepředstavuje tento nástroj žádné náklady, ale v případě migrace na jiný systém budou diagramy, tabulky a dokumenty komplikovat přesun.

- **Esko:** Společnost v současnosti používá služeb nástroje Esko, který se ji osvědčil. Doporučením pro společnost XYZ je nástroj používat i nadále.
- **Editor diagramů BPMN:** Digramy v rámci této práce byly navrženy na platformě CAMUDA, pokud se společnost XYZ rozhodne používat BPMN stojí za zvážení placení licence, případně prohledat trh kvůli alternativě.

Náklady na externisty:

- **Dodavatel webu:** Požadavky společnosti XYZ na bezpečnost webu se může projevit do jejich nákladů. Dodavatel si splnění požadavků může fakturovat jako vícepráci.
- **Externí auditor:** Společnost XYZ by měla pro svůj externí bezpečnostní audit sestavit výběrové řízení. Externí audit není levná záležitost a může se společnosti XYZ prodražit.

4.3 Finanční ohodnocení řízení bezpečnosti pro společnost XYZ

Mimo rozsah doporučení MBS byl sestaven systém kategorizace a ohodnocení výpadků. Tento systém poslouží i pro výpočet výnosů této práce. Ve spolupráci s vedením společnosti XYZ byly vytvořeny čtyři kategorie výpadku, a to podle délky výpadku. Z praxe ve firmě byly vypočteny i náklady výpadku. Kategorie jsou následující:

- **Kategorie 0**: Systémy společnosti nebudou dostupné do čtyř hodin. Příkladem takového výpadku může být selhání serveru. Praxe ve společnosti ukázala, že zaměstnanci si s takovým výpadkem poradí bez problému. Použijí svůj čas například pro přípravu dokladů anebo řešení emailové komunikace. Společnosti vznikají minimální náklady.
- **Kategorie 1:** Systémy společnosti nejsou dostupné od čtyř hodin až po celý pracovní den. Při tak dlouhém výpadku již zaměstnanci nejsou schopní nalézt další práci, která nepotřebuje systémy společnosti. Náklady této kategorie byly určeny okolo 40 000 korun českých. Částka byla vypočtena průměrem a přepočtem mzdových nákladů společnosti. Je důležité podotknout, že výpadek v určitém termínu hraje velkou roli vzhledem k oboru společnosti. Například výpadek v den, kdy se podávají daňová přiznání k DPH, bude mít pro společnost mnohem vážnější následky než výpadek v následující den.
- **Kategorie 2:** Výpadek systémů společnosti trvá jeden až pět pracovních dní. Schopnost fungování společnosti je ohrožena, ale vedení věří, že dokáže splnit závazky v požadovaných termínech. Částka pro tuto kategorii bylo vypočítána z nákladů společnosti. Náklady této kategorie byli určeny okolo 60 000 korun českých za každý den výpadku. Je opět důležité podotknout, že výpadek v určitých termínech hraje velkou roli vzhledem k oboru společnosti.
- **Kategorie 3:** Výpadek trvá déle jak pět pracovních dní. Fungováni společnosti je vážně ohroženo. Náklady této kategorie se nepodařilo vyčíslit, neboť již zasahují i do výnosů společnosti XYZ.

Při splnění návrhů pro řízení informační bezpečnosti obsažených v rámci této práce se dá očekávat, že nedojde k výpadkům kategorie 2 a 3. Dojde také k minimalizaci výpadků kategorie 1. Společnost tak může mít zaručeno, že nedojde k ohrožující ztrátě.

Ztráty společnosti při nenaplnění návrhů této práce nejsou pouze v nákladech výpadků. Další ztráty můžou být:

- pokuty a sankce,
- ztráta důvěry zaměstnanců,
- ztráta důvěry klientů,
- náklady na kompenzaci,
- náklady na nápravu.

Jednotlivé přínosy a náklady pro jednotlivá doporučení byly podrobněji rozepsány v předchozích podkapitolách. Náklady jsou primárně spojeny s prací IT oddělní. Přínosy jednotlivých doporučení, ale převyšují tyto náklady. Přesná částka pro výnos řízení informační bezpečnosti se nedá jednoznačně pro společnost XYZ určit.

Závěr

Kapitola o teoretických východiscích poskytla popis různých nástrojů, rámců a analýz, které byly použity pro popis současného stavu řízení informační bezpečnosti ve společnosti XYZ. Začali jsme procesním modelem (BPMN), grafickou notací používanou k reprezentaci podnikových procesů, která byla použita k popisu různých procesů. Tato notace byla použita i v návrhové části pro několik procesů. Ve druhé podkapitole je představen cloudový software Esko, který slouží jako nástroj pro evidenci aktiv a jeho garantů. Software také slouží pro evidenci rizik a opatření. Dále jsme se zabývali analýzou PESTLE, která pomohla při zkoumání vnějších faktorů, jež mohou ovlivnit řízení informační bezpečnosti společnosti. Nastínili jsme také situaci na trhu a vztahy společnosti XYZ s ostatními hráči na trhu, a to za pomoci Porterovy analýzy pěti sil. K posouzení efektivnosti současného řízení bezpečnosti společnosti XYZ jsme použili rámec 7S. K celkovému vyhodnocení současného stavu kybernetické bezpečnosti jsme použili matice hodnocení interních faktorů (IFE) a hodnocení externích faktorů (EFE), které zahrnují zjištění z předchozích analýz. Dále jsme se zabývali úlohou Národní agentury pro kybernetickou a informační bezpečnost a jejím dokumentem Minimálním bezpečnostním standardem (dále jen MBS). MBS je souborem doporučení a osvědčených postupů, který slouží jako základ návrhové části této práce. Nakonec jsme se zabývali směrnicí o sítích a informačních systémech (NIS) a její aktualizovanou verzí NIS2, jejímž cílem je zlepšit kybernetickou bezpečnost napříč životně důležitou infrastrukturou v Evropské unii.

Druhá kapitola, analýza současné situace, zahrnovala nástroje, rámce a analýzy nadefinované v první kapitole. Konkrétně byla použita analýza PESTLE, Porterova analýza, analýza 7S a k zhodnocení analýz byly použity matice IFE a EFE. Tyto analýzy pomohly identifikovat silné a slabé stránky bezpečnosti společnosti. Kromě analýz obsahuje druhá kapitola i porovnání minimálního bezpečnostního standardu a současného stavu společnosti. Manažerské a technické části MBS pomohly poskytnout ucelený přehled o společnosti XYZ. Součástí této kapitoly je i současná topologie sítě společnosti.

Na základě analýzy současného stavu a za pomoci MBS byla sestavena třetí, návrhová, část této práce. Na úvod kapitoly byla sestavena tabulka, která obsahuje nedostatky a názvy podkapitol s návrhy jejich řešení. Návrhová část obsahuje následující podkapitoly:

- První podkapitola pojednává o řízení informací ve společnosti XYZ, včetně zavedení čtyř úrovní pro popis a klasifikaci informací. Podkapitola upozorňuje také na konkrétní

problémy související se systémem BI. V rámci této práce je kategorizováno 11 základních typů informací společnosti XYZ.

- Druhá podkapitola navrhuje řešení pro řízení dodavatelů ve společnosti. Navrhovaný postup zahrnuje sestavení evidence všech dodavatelů společnosti, vytvoření profilu každého dodavatele, porovnání stávajících smluv s kritérii vyhlášky 82/2018 a posouzení, zda je současná situace vyhovující.
- Třetí podkapitola obsahuje návrh pro řízení lidských zdrojů ve společnosti XYZ, který zahrnuje postup pro vypracování bezpečnostní příručky, školení zaměstnanců a certifikaci klíčových osob. Příručka by měla být volně přístupná zaměstnancům. Školení zaměstnanců by měla být plánována a prováděna pravidelně, přičemž četnost a rozdělení školení by měly být stanoveny na základě různých oblastí. Podkapitola také doporučuje certifikace klíčových osob v oddělení IT. Součástí jsou i návrhy dvou kurzů vydaných NÚKIBem.
- Čtvrtá podkapitola navrhuje řešení řízení změn pro XYZ. Návrh se snaží minimalizovat rizika narušení funkčnosti a bezpečnosti společnosti. Návrhem této podkapitoly je vytvoření evidence s jasně nadefinovanými parametry. Součástí je i metodika procesu změny.
- Pátá podkapitola obsahuje návrh řešení řízení kontinuity provozu (BCM) pro XYZ. Obsahem této části je postup pro sestavení plánu obnovy po havárii (DRP) a plánu kontinuity provozu (BCP). Součástí této podkapitoly jsou i příklady obou typů.
- Následující šestá podkapitola navrhuje postup pro interní a externí audit kybernetické bezpečnosti. Tato část práce obsahuje postup pro externí audit. Popisuje i požadavky a parametry, které by měl externí auditor splňovat.
- Sedmá podkapitola popisuje postup pro zlepšení fyzické bezpečnosti společnosti XYZ. Obsahem podkapitoly je příklad cílů pro fyzickou bezpečnost, popis postupu zlepšení fyzické bezpečnosti.
- Pro zlepšení řízení bezpečnosti ve společnosti XYZ navrhuje osmá podkapitola zavedení jedinečných identifikátorů a doporučuje aktualizaci systému přidělování zkratek v celé společnosti. Součástí podkapitoly jsou i další doporučení pro zlepšení bezpečnosti přístupů.
- Devátá podkapitola popisuje návrh pro zlepšení evidence mobilních zařízení. Doporučeným postupem podkapitoly je zápis všech mobilní zařízení do evidence a softwaru Esko. Na základě výsledků analýzy z Esko mohou být konkrétní zařízení

převedena pod správu oddělení IT nebo nahrazena malými pracovními stanicemi pro domácí použití.

- Desátá podkapitola popisuje metodiku odebrání přístupových práv ERP systémů.
- Podobnou formou je sestaven i návrh v jedenácté podkapitole, který popisuje metodiku pro deaktivaci identit.
- Dvanáctá podkapitola obsahuje popis a doporučení na segmentaci sítě společnosti XYZ. Navrhovaným řešením je vytvoření demilitarizované zóny pro klienty a externisty, kteří se připojují do sítě společnosti.
- Třináctá a následující čtrnáctá podkapitola popisují metodiky při vzniku bezpečnostní události a incidentů a metodiku testování ERP. Obje kapitoly popisují postup a doporučení pro oboje problematiky.
- Patnáctá podkapitola obsahuje popis postupu pro kryptografické prostředky. V podkapitole jsou navržené i příklady typů šifrovacích algoritmů, doporučených NÚKIBem.
- Šestnáctá podkapitola popisuje postup pro test záložního systému. Součástí podkapitoly je i popis před, v průběhu a po testu.
- Sedmnáctá podkapitola obsahuje návrh pro chybějící pravidla zálohování a jejich zapojení do současného řešení.
- Následující osmnáctá podkapitola poskytuje seznam parametrů, které musí společnost XYZ prověřit na svém novém webu.
- Předposlední podkapitola návrhové částí navrhuje rozšíření stávajícího procesu získání nového klienta o otázky bezpečnosti.
- Dvacátá podkapitola obsahuje parametry potřebné pro správnou klasifikaci a správné hodnocení externích systémů.

Čtvrtá podkapitola se zaobírá sestavením tabulek přínosu a nákladů, které společnosti XYZ vzniknou. Na závěr této kapitoly bylo sestaven i základní finanční ohodnocení pro zlepšení řízení bezpečnosti. Výsledkem této kapitoly je, že přínosy řízení bezpečnosti převyšují náklady.

V rámci této práce byly navrženy tyto procesy a postupy:

- Postup řízení dodavatelů.
- Postup pro sestavení manuálu pro bezpečnost.
- Postup pro školení zaměstnanců.
- Postup pro sestavení evidenčního systému pro řízení změn.

- Metodika procesu změny.
- Postup pro vypracování DRP (včetně příkladu).
- Postup pro vypracování BCP (včetně příkladu).
- Postup pro evidenci mobilních zařízení
- Metodika pro odebrání přístupových práv
- Metodiky pro deaktivaci identit.
- Postup pro segmentaci sítě.
- Metodika při vzniku bezpečnostní události a incidentů.
- Metodika testování ERP.
- Postup pro používání kryptografických prostředků.
- Postup testu záložního systému.
- Zálohování pro ERP systém VEMA.
- Zálohování pro BI/CRM systém Praetor.
- Doplnění procesu získání nového klienta.

Je důležité, aby společnost věnovala dostatečné prostředky a pozornost implementaci těchto návrhů a aby pravidelně monitorovala a hodnotila jejich účinnost.

Tato práce ukazuje na fakt, že řízení informační bezpečnosti by mělo být klíčovou součástí řízení společnosti XYZ. To znamená, že by měla být zapracována do všech kritických procesů a oblastí podnikání a měla by být chráněna pomocí jasně definovaných postupů. Důležitým závěrem této práce je také, že XYZ by mělo založit svou informační bezpečnost na dobře definovaném evidenčním systému, bezpečnostních pravidlech a na pravidelné analýze rizik. Cílem je, aby mohla identifikovat klíčové oblasti, které je třeba chránit, a přizpůsobit zabezpečení specifickým potřebám. Dále by mělo XYZ sestavit plány pro řešení incidentů a nestandardních situací. Je třeba zdůraznit i potřebu neustálého a systematického zlepšování informační bezpečnosti v rámci společnosti, aby byla schopna rychle reagovat na hrozby a minimalizovat jejich dopad.

Činnosti spojené s touto prací byly evidovány na základě úmluvy s vedením XYZ. V systému společnosti je v současnosti zaznamenáno okolo 88 hodin. S ohledem na sazbu 1 000 Kč za hodinu pro senior člena týmu IT tak se celkové náklady vyšplhají na částku 88 tisíc Kč.

Vypracování této práce mi poskytlo hlubší porozumění problematiky zavádění řízení bezpečnosti pro malé společnosti. Konkrétně jsem získal podrobný přehled o nutnosti plánování

celého procesu a o překážkách, které se mohou objevit. Měl jsem také možnost popsat některé interní procesy společnosti XYZ, což mi pomohlo získat cenné zkušenosti. Tyto nové poznatky mi mohou být prospěšné nejen při dalším zavádění řízení bezpečnosti, ale také v jiných oblastech, jako je například controlling. Díky této práci jsem také lépe porozuměl prostředí oboru účetnictví, české legislativy a bezpečnostních norem. Celkově jsem získal cenné zkušenosti, které mi otevřely nové perspektivy v mém dalším profesním rozvoji.

Seznam zkratek

- **B2B** – Business-to-business
- **BCP** – Business continuity plan
- **BI** – Business Intelligence
- **BYOD** – Bring Your Own Device
- **CRM** – Customer relationship management
- **DMZ** – Demilitarizovaná zóna
- **DRP** – Disaster recovery plan
- **EFE** – matice externích faktorů
- **ERP** – Enterprise Resource Planning
- **GDPR** – General Data Protection Regulation
- **HA** – High availability
- **HW** – hardware
- **IEC** – International Electrotechnical Commission
- **IFE** – matice interních faktorů
- **ISMS** – systém řízení bezpečnosti informací
- **ISO** – International Organization for Standardization
- **KII** – kritická informační infrastruktura
- **MBS** – Minimální bezpečnostní standard
- **MS** – Microsoft
- **NIS** – Network and Information Systems
- **NÚKIB** – Národní úřad pro kybernetickou a informační bezpečnost
- **RPO** – Recovery Point Objective
- **RTO** – Recovery Time Objective
- **SLA** – Service-level agreement
- **SPOF** – Single Point of Failure
- **SW** – software
- **VIS** – významný informační systém
- **VKB** – Vyhláška o kybernetické bezpečnosti
- **ZKB** – Zákon o kybernetické bezpečnosti
- **ZS** – základní informační systém

Seznam obrázků

Zdroje

[1] Vyhláška číslo 82/2018 Sb., novelizovaná vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti).

[2] Národní centrum kybernetické bezpečnosti. (n.d.). Výklad požadavků na smlouvy s dodavateli [PDF]. Získáno z https://www.govcert.cz/download/kii-vis/VKB/Vyklad_pozadavku_na_smlouvy_s_dodavateli_v1.1.pdf

[3] Národní památkový ústav. (2020). Minimální bezpečnostní standard [PDF]. Získáno z https://archi.gov.cz/_media/dokumenty:2020-07-17_minimalni-bezpecnostni-standard_v1.0.pdf

[4] Vzdělávací portál NÚKIB [online]. Dostupné z: https://osveta.nukib.cz/

[5] SEDLÁK, Petr a Martin KONEČNÝ. Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru. Brno: CERM, akademické nakladatelství, 2021. ISBN isbn978-80-7623-068-2.

[6] Nová směrnice EU o bezpečnosti sítí a informací. [online]. Dostupné z: https://osveta.nukib.cz/course/view.php?id=145#section-13

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

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

[9] ČSN EN ISO/IEC 27701 (36 9770) Bezpečnostní techniky – Rozšíření ISO/IEC 27001 a ISO/IEC 27002 pro řízení ochrany soukromí – Požadavky a směrnice. [Praha]: Česká agentura pro standardizaci, 2021.

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

[11] FFIEC IT Examination Handbook InfoBase – Business Continuity Management. FFIEC IT Examination Handbook InfoBase – Home [online]. Dostupné z: https://ithandbook.ffiec.gov/it-booklets/business-continuity-management.aspx

Přílohy

Hodnocení aktiv a Analýza rizik.pdf - PDF soubor, který obsahuje seznam aktiv a analýzu rizik v softwaru Esko.