
# VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

## FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

## ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS


# NÁVRH ZABEZPEČENÍ FIRMY A VZDÁLENÉHO PŘIPOJENÍ
COMPANY SECURITY OUTLINE AND LONG DISTANCE CONNECTION SCHEME

**BAKÁLÁŘSKÁ PRÁCE**
BACHELOR'S THESIS


**AUTOR PRÁCE** — Dominika Hanáková
AUTHOR

**VEDOUCÍ PRÁCE** — Ing. Viktor Ondrák, Ph.D.
SUPERVISOR



**BRNO 2021**

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

# Zadání bakalářské práce

| | |
|---|---|
| Ústav: | Ústav informatiky |
| Student: | **Dominika Hanáková** |
| Studijní program: | Systémové inženýrství a informatika |
| Studijní obor: | Manažerská informatika |
| Vedoucí práce: | **Ing. Viktor Ondrák, Ph.D.** |
| Akademický rok: | 2020/21 |

Ředitel ústavu 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 bakalářskou práci s názvem:

## Návrh zabezpečení firmy a vzdáleného připojení

**Charakteristika problematiky úkolu:**
Úvod
Cíle práce, metody a postupy zpracování
Teoretická východiska práce
Analýza současného stavu
Vlastní návrh řešení
Závěr
Seznam použité literatury
Přílohy

**Cíle, kterých má být dosaženo:**

Navrhnout management bezpečnosti

**Základní literární prameny:**

ČSN ISO/IEC 27001:2006 Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací – Požadavky. Český normalizační institut, 2006.

ČSN ISO/IEC 27002:2005 Informační technologie – Bezpečnostní techniky – Soubor postupů pro řízení bezpečnosti informací. Český normalizační institut, 2005.

DOUCEK P., L. NOVÁK a V. SVATÁ. Řízení bezpečnosti informací. Praha: Professional Publishing, 2008. ISBN 80-86898-38-5.

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

POŽÁR, J. Informační bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. ISBN 80-86898-38-5.

POŽÁR, J. Základy teorie informační bezpečnosti. Praha: Vydavatelství PA ČR, 2007. ISBN 978-8--7251-250-8.

Termín odevzdání bakalářské práce je stanoven časovým plánem akademického roku 2020/21

V Brně dne 28.2.2021

L. S.

| | |
|---|---|
| Mgr. Veronika Novotná, Ph.D. | doc. Ing. Vojtěch Bartoš, Ph.D. |
| Ředitel | Děkan |

## Abstrakt

Tato bakalářská práce se zabývá analýzou bezpečnostních opatření a vzdáleného připojení společnosti. Na základě této analýzy byly vymezeny jejich hranice, identifikována jednotlivá aktiva firmy, bezpečnostní hrozby, rizika, a zhodnocena dosavadní bezpečnostní opatření. V praktické části práce předložím návrhy na zlepšení daných opatření. Tato opatření by měla společnosti pomoci chránit její aktiva a co nejvíce snížit rizika poškození.



## Klíčová slova

Informační bezpečnost, vzdálené připojení, ochrana dat, virtuální privátní síť, VPN, SSTP



## Abstract

This bachelor's thesis deals with the analysis of the security measures and remote access of the company. On the basis of this analysis it's boundaries have been defined, the individual assets, security threats and risks have been identified and current security measures evaluated. In the practical part of the thesis, I'm going to propose suggestions for improvement of the measurements. These measures should help the company with the protection of the assets and lower the risks of damage.



## Keywords

Information security, remote access, data protection, virtual private network, VPN, SSTP

## Bibliografická citace

HANÁKOVÁ, Dominika. *Návrh zabezpečení firmy a vzdáleného připojení* [online]. Brno, 2021 [cit. 2021-05-15]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/131980. Bakalářská práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Viktor Ondrák.

# Čestné prohlášení

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

V Brně dne 16. května 2021 ----------

podpis studenta

## Poděkování

Ráda bych poděkovala svému vedoucímu práce Ing. Viktoru Ondrákovi, Ph.D., za jeho rady a čas, který mi věnoval při tvorbě práce. Zároveň chtěla poděkovat své rodině a přátelům za podporu, kterou mi poskytli při tvorbě práce.

# Obsah

# ÚVOD

V bakalářské práci jsem se zabývala zhodnocením bezpečnosti ICT dané společnosti a návrhem na zlepšení stávajících opatření, konkrétně jsem se zaměřila na dostupnost dat a vzdálený přístup. Vzdálený přístup jsem se rozhodla řešit konfigurací VPN (Virtual Private Network) typu SSTP. Jedná se o větší společnost na obrábění a výrobu autodílů. Bylo mi dovoleno využít jejich data, ale firma si nepřála být jmenována. Jednotlivé analýzy jsem provedla po konzultacích s vedoucími jednotlivých oddělení firmy XYZ s.r.o. a externím IT specialistou. IT služby poskytuje firma Antea.

V první části se zabývám vyměřením základních pojmů informační bezpečnosti, síťového připojení a vzdáleného přístupu. V druhé kapitole jsem vymezila hranice firmy, popisuji její prostředí, organizační strukturu, identifikuji aktiva, hrozby a rizika, která by jim mohla škodit. Analýza stavu a dosavadních bezpečnostních opatření společnosti XYZ s.r.o. byla provedena po konzultaci s vedoucími zaměstnanci společnosti a IT specialistou. Ve třetí kapitole navrhuji opatření, která by měla společnosti pomoci lépe a efektivně chránit její aktiva. Také zde popisuje proces konfigurace VPN pomocí Mikrotik Router OS. V závěru jsem zhodnotila, jaký dopad by mělo nasazení navrhovaných opatření pro společnost a jak by se změnila úroveň rizik.

# CÍL PRÁCE, METODY A POSTUPY ZPRACOVÁNÍ

Cílem práce bakalářské práce je navrhnout změny, které by měly pomoci zlepšit dosavadní bezpečnostní opatření společnosti na obrábění autodílů. Jedním z návrhů bude konfigurace virtuální privátní sítě. Nová VPN by také umožnila oprávněným pracovníkům bezpečnou práci z domu. Analýza byla provedena ve spolupráci s firmou Antea, která provozuje externě správu IT pro danou společnost, která si nepřeje být jmenována. Bude k ní nadále odkazováno jako k firmě XYZ s.r.o.

V analytické části práce se zabývám vymezením hranic, popisem prostředí a základními charakteristikami firmy, definicí incidentů, hrozeb a možných rizik na základě dopadu a pravděpodobnosti výskytu. Tyto analýzy byly provedeny po konzultaci s IT specialistou a managementem společnosti. Na základě konzultace jsem volila jednotlivé hodnoty analýz. Také zde popisuji dosavadní opatření, která firma aplikuje, aby zabezpečila ochranu svých aktiv.

V praktické části představím vlastní návrhy na zlepšení dosavadních opatření. Podrobněji se budu zabývat konfigurací VPN typu SSTP. V závěru vyhodnotím, jaký přínos by pro společnost měla nová opatření a jak by se změnila úroveň rizik.

# 1. TEORETICKÁ VÝCHODISKA PRÁCE

Na úvod práce je nutné vymezit si pojem informační bezpečnost a termíny s ní spojené. Nejprve budou objasněny základní pojmy týkající se informačního systému a bezpečnosti, dále možné hrozby a rizika a na závěr se zaměřím na objasnění vzdáleného přístupu a základní terminologie týkající se síťového připojení.

## 1.1. Informační systém

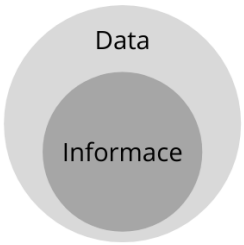
Informační systém je systém vzájemně propojených informací a procesů, které s danými informacemi pracují. Rozumí se jím soubor technických, lidských a organizačních prostředků a metod, které oprávněným uživatelům poskytují dané informační služby v určité kvalitě. Kvalitu, bezpečnost a parametry informačního systému určují jeho složky (součásti, prostředky). Jedná se o hardware, software, data, organizaci a lidskou složku (1, s. 129 - 130).

**Informace**

Pod pojmem informace se rozumí to, co vyplývá z pečlivých analýz, zpracování a prezentace v takové formě, která bude vhodná pro rozhodovací proces. Jde o poznatek, který se týká jakýchkoliv objektů, např. procesů, událostí nebo myšlenek (1, s. 34).

**Data (Údaje)**

Data představují vhodně vyjádřené zprávy, aby byly srozumitelné pro příjemce. Tím může být jak člověk, tak technický prostředek. Hodnota dat je dána cenou informačního obsahu a vynaloženými náklady na jejich pořízení. Data se rozdělují na strukturovaná a nestrukturovaná. Každá informace je údajem, datem, ale ne všechna data se dají považovat za informaci. Pokud data přinesou příjemci užitek, můžeme je nazývat informacemi (2, s. 13).




**Obrázek 1: Vztah dat a informací**
(Zdroj: Vlastní zpracování dle (2, s. 13))

### Znalosti

Dokážeme-li získaná data a informace využít k řešení problému, jsou pro nás srozumitelná a jsme schopni je použít v různých situacích, můžeme je nazývat znalostmi (3, s. 6).

### Hardware

Jedná se o veškeré fyzické prostředky, které jsou součástí informačního systému. Kvalita hardwaru podstatně ovlivňuje kvalitu IS.

### Software

Software je sada veškerých programů v IS, které provádějí nějakou činnost. Lze jej rozdělit na systémový software a aplikační software. Systémový software zajišťuje chod IS, běžný uživatel s ním přímo nepracuje. Nejobvyklejším příkladem je BIOS. Aplikační software se zaměřuje přímo na uživatele, umožňuje mu provozovat určitou činnost, řešit nějaký konkrétní problém. Pro interakci s uživatelem využívá textového nebo grafického rozhraní.

### Lidský faktor

Lidský faktor v IS představuje lidi zabezpečující obsluhu, údržbu, užívání a zabezpečení informačního systému.

### Organizační struktura

Organizační struktura je definována jako směrnice, předpisy a pravidla určující pravomoci, zodpovědnost, činnost a chování lidí při užívání IS. (4, s. 2)

## 1.2. Informační bezpečnost

Informační bezpečnost lze definovat jako vzájemně provázaná opatření pro zajištění dostupnosti, integrity a důvěryhodnosti informací. Jde o systém ochrany informací ve všech jejich formách a po celý jejich životní cyklus – během jejich vzniku, zpracování, ukládání, přenosu a likvidace (2, s. 16).

### 1.2.1. Atributy bezpečnosti IS

Základními atributy bezpečnosti IS jsou důvěrnost, dostupnost a integrita. Za další důležité faktory můžeme považovat také odpovědnost a spolehlivost. Hlavní je to, aby relevantní informace byly dostupné pouze autorizovaným osobám jen v potřebnou dobu (4, s. 5).

**Důvěrnost**

Stav, při kterém jsou důvěrné informace poskytovány pouze autorizovaným osobám (4, s. 5).

**Dostupnost**

Stav, při kterém jsou informační služby k dispozici v moment požadavku (4, s. 6).

**Integrita**

Stav, při kterém jsou informace správné a úplné. Obvykle se zabezpečuje elektronickými podpisy (4, s. 5).

**Odpovědnost**

Stav, při kterém je upřednostňována individuální odpovědnost (2, s. 17)

**Spolehlivost**

Stav, při kterém jsou výsledky a chování systému konzistentní (2, s. 17).

### 1.2.2. Aktiva a jejich klasifikace

Aktiva počítačové bezpečnosti jsou jakékoliv hmotné i nehmotné součásti informačního systému, které pro svého vlastníka mají nějakou hodnotu. Každé aktivum má svou

specifickou funkci, která zaručuje správnou činnost IS. Rozsáhlé informační systémy obsahují mnoho aktiv různých typů. Nejobvyklejší jsou informační, softwarová a fyzická aktiva. Do rozdělení aktiv můžeme také zahrnout služby, kvalifikaci lidí a nehmotná aktiva (5, s. 81).

**Informační aktiva**

- datové soubory, archivovaná data, záznamy z auditů, školící materiály, jakékoliv údaje a informace, které jsou evidovány v elektronické nebo papírové podobě (4, s. 10)

**Softwarová aktiva**

- programy, softwary, licence, komunikační prostředky IS, operační systémy, vlastní aplikace, softwarové nástroje a utility používané při práci, objekty, ve kterých jsou systémy umístěny (4, s. 10)

**Fyzická aktiva**

- jsou to taková aktiva, na kterých je možné evidovat, uchovávat nebo prezentovat dané informace a údaje o firmě, hardware, kamery, servery, stroje (4, s. 10)

**Služby**

- technické, počítačové, komunikační služby (4, s. 10)

**Lidé**

- jejich kvalifikace, zkušenosti, dovednosti (4, s. 10)

**Nehmotná aktiva**

- image společnosti a její pověst (4, s. 10)

**Zranitelnost aktiv**

Zranitelnost můžeme definovat jako slabinu určitého aktiva, skupiny aktiv nebo samotného systému. Výskyt zranitelnosti nezpůsobí škodu jako takovou, musí existovat hrozba, která ho využije. Pokud zranitelnost nemá odpovídající hrozbu, nemusí být nutné přijetí bezpečnostních opatření. Určitě by měla být identifikována a zaevidována pro případ, že by se objevila odpovídající hrozba, která je bude schopná využít (4, s. 16).

Zranitelnost může být určena:

- způsobem použití aktiva v IS
- vadou aktiva
- špatným užitím aktiva
- vlastností aktiva

**Zranitelné místo**

Zranitelné místo je slabina IS, která je využitelná ke způsobení škod nebo ztrát útokem na IS. Jeho existence je důsledek chyb v návrhu nebo implementaci IS (2, s. 19).

**Vlastnictví aktiv**

Každé aktivum musí mít svého vlastníka, který má odpovědnost za jeho stav, funkčnost, údržbu, bezpečnost, opravy a činnost. Může se jednat o konkrétní osobu nebo o jednoznačně určenou pracovní pozici, vlastník musí být zaměstnancem dané organizace. Není významné, zda se za účelem oprav či údržby najímá třetí osoba (4, s. 12).

### 1.2.3. Hrozby v informačních systémech

**Bezpečnostní hrozba**

Hodnota každého aktiva je ohrožena různými vlivy. Působí-li tyto vlivy na zranitelná místa aktiv, nazýváme je hrozbami (4, s. 10).

Hrozbou nazýváme skutečnost, která může způsobit nežádoucí změnu ve vlastnostech a struktuře aktiva. Pokud tato změna ohrozí bezpečnosti IS nazýváme ji bezpečnostní hrozbou (5, s. 81). Jde o jakoukoliv okolnost, která působí na zranitelná místa aktiv, může být. Hrozby můžeme dělit na objektivní (přírodní a technické) a subjektivní, hrozby plynoucí z lidského faktoru (neúmyslné a úmyslné (2, s. 23).

**Přírodní**

- za přírodní hrozby považujeme přírodní katastrofy, povodně, požáry. K jejich prevenci je potřeba, aby společnost měla havarijní plán (2, s. 23)

**Technické**

- technickou hrozbou je myšlen výpadek internetu, elektřiny nebo porucha hardwaru (2, s. 23)

**Neúmyslné**

- neúmyslné hrozby často způsobuje nedostatečné proškolení zaměstnanců. Jejich nedostatečná znalost může způsobit mylné smazání dat, jejich chybné uložení a následné poškození záloh (2, s. 24)

**Úmyslné**

- úmyslnou hrozbou rozumíme hackerské útoky, vynášení citlivých informací ze společnosti a jejich poskytnutí konkurenci (2, s. 24)

### 1.2.4. Bezpečnostní událost

Pokud se bezpečnostní hrozba realizuje a způsobí změnu stavu, struktury, vazeb, nebo funkce aktiva, mluvíme o bezpečnostní události (4, s. 10).

Bezpečnostní událost je aktivní působení na aktivum v čase. Během ní mohlo dojít k narušení informačního systému a ohrožení bezpečnosti informací (6, s. 23). Jde o realizovanou bezpečnostní hrozbu, která způsobila změna stavu, vazeb, struktury nebo funkci aktiva. Bezpečnostní událost má určitou dobu trvání a dané příznaky, podle kterých je možné hrozbu identifikovat (4, s. 8).

### 1.2.5. Bezpečnostní incident

Jedná se o stav aktiva, kdy je narušen některý z jeho bezpečnostních atributů.

Bezpečnostní incident lze definovat jako případ selhání bezpečnosti, pro daný IS musí být stanoveno, co je považováno za bezpečnostní incident a jaké jsou formální procedury jeho řešení (7, s. 346).

U každého bezpečnostního incidentu je nutné posoudit, jaký dopad může mít tento incident na organizaci. Incident může mít dopad i na více aktiv a jeho účinek je buď okamžitý nebo budoucí. Nemusí být vždy materiální, jedná se také o ztrátu dobrého jména společnosti (4, s. 24).

### 1.2.6. Bezpečnostní riziko

Rizikem můžeme nazývat pravděpodobnost vzniku incidentu. Jde o možnost, že daná hrozba využije zranitelnosti aktiva, aby byla způsobena jeho ztráta či poškození. (5, s. 81)

Úroveň rizika je součin pravděpodobnosti vzniku bezpečnostního incidentu a následku tohoto incidentu. Tato hodnota pomáhá objektivně stanovit priority nasazování bezpečnostních opatření.

Ošetření rizik má za hlavní úkol navrhnout opatření ke snížení rizik. Rizika mohou být ošetřena čtyřmi způsoby:

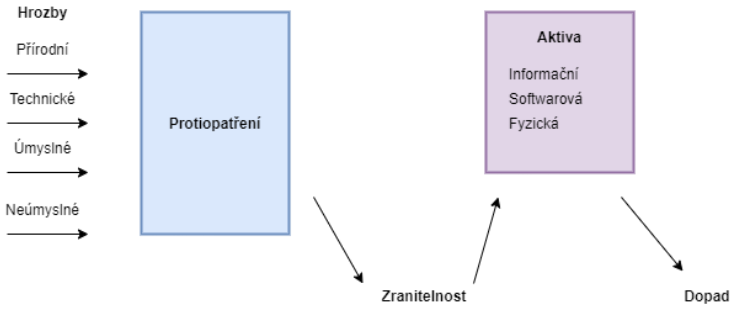
- modifikace rizik
- podstoupení rizik
- vyhnutí se riziku
- sdílením rizika

Tyto způsoby ošetření rizik se navzájem nevylučují a je možné je kombinovat (4, s. 39 - 40).

### 1.2.7. Bezpečnostní opatření

Jedná se o proces, proceduru nebo technický prostředek, který je speciálně navržený, aby zmírnil působení hrozby, snížení zranitelnosti, nebo dopadu hrozby (7, s. 347).

Proti bezpečnostním hrozbám se dá bránit navržením různých opatření. Opatřením se rozumí cokoliv, co je navrženo pro zajištění větší bezpečnosti a snížení hrozeb, navrhují se na základě analýzy rizik (4, s. 16).




**Obrázek 2: Zranitelnost aktiv**
(Zdroj: vlastní zpracování dle (2, s. 25))

## 1.3. Normy informační bezpečnosti

**ISO 9001** – standard požadavků na zavedení systému managementu kvality ve firmě který vydává Mezinárodní organizace pro standardizaci, účelem normy je udržení vysoké úrovně výrobního procesu a kvalitu poskytovaných služeb a výrobků pro koncové spotřebitele (8)

**ISO 14001** - normy ISO 14001 tvoří systém environmentálního managementu, řídí dopad firmy na životní prostředí, je určena výrobcům, dodavatelům a poskytovatelům služeb ve všech oborech podnikání (9)

**ISO 27001** - mezinárodně platný standard, který definuje požadavky na systém managementu bezpečnosti informací, především pak řízení bezpečnosti důvěry informací pro zaměstnance, procesy, IT systémy a strategii firmy (10)

**IATF 16949** – certifikace kladoucí důraz na rozvoj systému managementu kvality, systém je procesně orientovaný a založený na neustálém zlepšování, na prevenci vad, na snižování odchylek a plýtvání v dodavatelském řetězci (11).

## 1.4. Základní pojmy síťového připojení

**Počítačová síť**

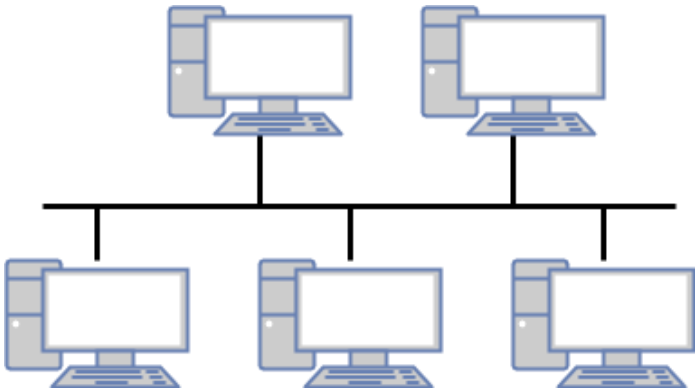
Počítačová síť je spojení dvou či více koncových uzlů vzájemně propojených tak, aby mohli mezi sebou komunikovat a využívat vzájemně svých prostředků podle předem stanovených pravidel a při vysoké spolehlivosti komunikace. Jde o otevřený deterministický systém, který zajišťující komunikaci mezi koncovými uzly.

- **Síťová infrastruktura**
  - Pasivní vrstva – kabeláž, rozvaděče – má na starosti vedení dat
  - Aktivní vrstva – router, switch, firewall – řídí tok dat
- **Koncové uzly** – jednotlivá zařízení, počítač, tiskárna, skener, … - mohou mít roli klienta nebo serveru

### Síťové topologie

Topologie sítí se zabývá zapojením různých prvků do počítačových sítí a zachycením jejich skutečné a logické podoby. Tři nejznámější topologie jsou sběrnice, kruh a hvězda. V praxi se využívá kombinace těchto topologií, například polynom. (12, s. 64)

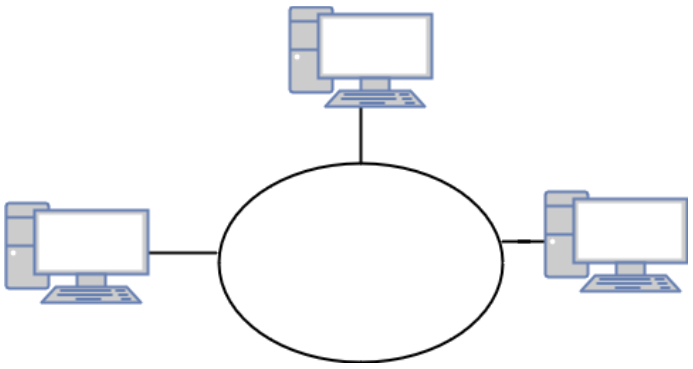
- **Sběrnice (Bus)**
  Sběrnicoví anebo lineární topologie je založená na propojení všech koncových uzlů jedním hlavním (páteřním) kabelem (13, s. 17).



**Obrázek 3: Topologie sběrnice**

(Zdroj: Vlastní zpracování dle (13, s. 17))

- **Kruh**
  Jedná se o topologii, kde jsou koncové uzly propojeny jeden s druhým tak, aby tvořili kruh, jde o uzavřenou lineární topologii (13, s. 17).

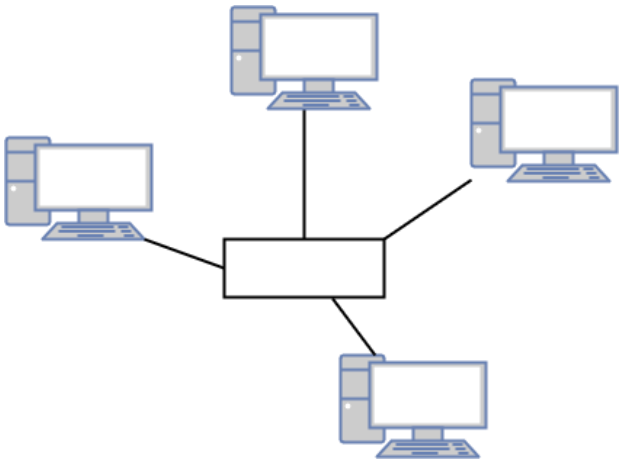


**Obrázek 4: Topologie kruh**

(Zdroj: Vlastní zpracování dle (13, s. 17))

- **Hvězda**

  Hvězda je nejvyužívanější topologií, jde o propojení koncových uzlů do útvaru připomínajícího hvězdu. Každý počítač je připojen k centrálnímu prvku, kterým je hub nebo switch (13, s. 18).



**Obrázek 5: Topologie Hvězda**

(Zdroj: Vlastní zpracování dle (13, s. 18))

## Protokol

Protokol je množina určitých pravidel, podle kterých probíhá komunikace a přenos dat mezi dvěma koncovými body (7, s. 350). Většinou také zahrnuje i navázání spojení, způsob přenosu dat, adresaci, zpracování chyb a další. Protokol definuje pravidla řídící syntaxi, sémantiku a synchronizaci vzájemné komunikace. Určuje formát protokolové datové jednotky (PDU) a jak reagovat na nestandartní situace. Každá vrstva může ke komunikaci využívat několik různých protokolů.

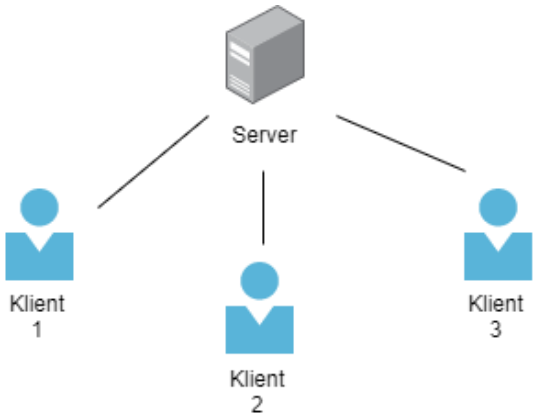
## Druhy připojení

- **Klient-klient (Peer to peer, P2P)**

  Jedná se o vzájemnou komunikaci klientů připojených k síti, všechny informace si vyměňují přímo mezi sebou. Uživatelé mezi sebou nemají žádnou hierarchii, jsou si všichni rovni. Každý slouží jako klient i server (12, s. 45).

- **Klient-server**

  Klienti vždy komunikují s hlavním serverem (servery) a prostřednictvím daného serveru mohou navázat i komunikaci s jinými klienty. Server není využíván jako klient nebo pracovní stanice (12, s. 46).




**Obrázek 6: Struktura Klient – server**
(Zdroj: Vlastní tvorba)

**Rozdělení sítí podle rozsahu**

- **PAN (Personal area network)**

  Jedná se o malou domácí síť, například propojení mobilního telefonu s notebookem a tiskárnou
- **LAN (Local area network)**

  Jde o rozsáhlejší počítačovou síť, obvykle je její dosah desítky až stovky metrů
- **MAN (Metropolitan area network)**

  MAN je propojení lokálních sítí na území měst, propojuje vzdálenosti až desítek kilometrů, je optimalizována pro stovky až tisíce přijímačů
- **WAN (Wide area network)**

  Jedná se o sítě propojují velké vzdálenosti, v praxi jde primárně o veřejné sítě

**Rozdělení sítí podle vlastnictví**

- Veřejná
- Privátní
- Poloprivátní/poloveřejná

**Síťový model**

- definice síťové struktury, specifikace počtu vrstev a účelu každé vrstvy

### Síťová architektura

- rozšíření síťového modelu o specifikaci protokolů

### Referenční model ISO/OSI

Referenční model ISO/OSI vypracovala organizace ISO (Organization for Standardization) jako hlavní část snahy o standardizaci počítačových sítí nazvané OSI (Open Systems Interconnection, propojení otevřených systémů) a v roce 1984 ho přijala jako mezinárodní normu ISO 7498. Tento model byl shora vnucen uživatelům a má značné nedostatky, tudíž se prakticky skoro nepoužívá. Stál však plní roli referenčního modelu a reálné modely vychází z jeho logiky a architektury. Model se skládá ze sedmi vrstev (13, s. 13)

**Tabulka 1: Referenční ISO/OSI model**

(Zdroj: vlastní zpracování dle (13, s. 13))

| | |
|---|---|
| Aplikační vrstva | Vrstvy orientované na podporu aplikací |
| Prezenční vrstva | |
| Relační vrstva | |
| Transportní vrstva | Přizpůsobovací vrstva |
| Síťová vrstva | Vrstvy orientované na přenos dat |
| Linková vrstva | |
| Fyzická vrstva | |

### Architektura TCP/IP

Transmission Control Protocol/ Internet Protocol označuje síťovou architekturu, kterou tvoří na rozdíl od modelu ISO/OSI jen čtyři vrstvy. Neoznačuje pouze dva protokoly, ale celý jejich soubor. Tato sada komunikačních protokolů je využívána sítí Internet. (14, s. 83 - 84)

**Tabulka 2: Porovnání ISO/OSI modelu s architekturou TCP/IP**

(Zdroj: Vlastní tvorba)

| ISO/OSI | TCP/IP |
|---|---|
| Aplikační vrstva | Aplikační vrstva |
| Prezenční vrstva | |
| Relační vrstva | |
| Transportní vrstva | Transportní vrstva |
| Síťová vrstva | Síťová vrstva |
| Linková vrstva | Vrstva síťového rozhraní |
| Fyzická vrstva | |

**MAC adresa** – jednoznačný identifikátor síťového zařízení přiřazen výrobcem, jde o adresaci na vrstvě síťového rozhraní

**IP adresa** – unikátní číslo, které je přiděleno počítači komunikujícímu prostřednictvím internetového protokolu, tvořena adresou sítě a adresou uzlu, jde o adresaci na síťové vrstvě

**Firewall**

Firewall je síťové zařízení, které blokuje nebo povoluje navazování komunikace na základě definovaných pravidel. Slouží k zabezpečení síťového provozu mezi sítěmi s různou úrovní zabezpečení a chrání síťové zdroje před neoprávněným přístupem (7, s. 348).

## 1.5. Vzdálené připojení

### 1.5.1. Virtuální privátní síť (VPN)

Virtuální privátní síť je síťová technologie vytvářející šifrované připojení mezi uživatelem a sítí, popřípadě dvěma sítěmi. Jde o neveřejnou síť využívající veřejnou komunikační infrastrukturu, například internet. Jako celek se chová jako privátní síť, ale pro propojení součástí využívá veřejné sítě. K datům mohou z pravidla přistupovat pouze ověření uživatelé.

VPN je obvykle definována jako konektivita klienta prostřednictvím veřejné datové infrastruktury, ale se stejnou připojovací a provozní politikou jako privátní datová síť. (15, s. 224).

### 1.5.2. RDP

Remote desktop protocol (RDP) je síťový protokol, které uživateli umožňuje připojení a ovládání vzdálené plochy pomocí počítačové sítě. Připojení je typu klient – server. Protokol vyvinula společnost Microsoft, ale je dostupný na všech informačních systémech. Funguje na portu 3389, který je velice často napadán a blokován, tudíž je využití tohoto protokolu považováno za rizikové (16).

### 1.5.3. PPTP

Point-to-Point Tunneling Protocol (PPTP) je jeden z nejstarších VPN protokolů, byl vyvinut společností Microsoft. Jeho instalace je poměrně snadná a každé zařízení je standartně vybaveno PPTP. Podporuje všechny operační systémy, ale kvůli nízké úrovni zabezpečení se nedoporučuje. V dnešní době je považován za zastaralý. Nicméně nastavení VPN tohoto typu se považuje za jednoduché. Tento protokol pracuje na datové vrstvě OSI modelu a je rozšířením protokolu PPP, Point-to-point protocol (17, s. 8 - 10).

### 1.5.4. SSTP

Secure Socket Tunneling Protocol (SSTP) je protokol integrován v rámci systému Windows, který je snadno použitelný. Byl představen společností Microsoft v roce 2007 a dokumentace ohledně nej je zdarma dostupná na internetových stránkách společnosti. Jeho nastavení na jiných platformách, než těch od Microsoftu je však nesmírně obtížné. Jediným požadavkem pro vytvoření této VPN je, aby na všech zařízeních byl otevřený port TCP 443 (18, s. 20 - 22).

### 1.5.5. Open VPN

Open VPN je volně dostupný software, který dokáže vytvořit šifrovanou VPN. Byla vyvinuta Jamesem Yonanem v roce 2002. Využívá architektury klient-server a je to podporován na platformách Microsoft, MacOS i Linux. Umožňuje ověřit spojení pomocí digitálního SSL certifikátu, sdíleného klíče nebo uživatelského jména a hesla. Pro výměnu klíčů využívá SSL/TLC. K šifrování využívá knihoven OpenSSL. VPN lze

nakonfigurovat, aby běžela na jakémkoliv portu UDP nebo TCP. Pro nastavení vyžaduje instalaci softwaru (19).

### 1.5.6. L2TP

Layer 2 tunneling protocol je protokol (public-private partnership), jehož funkcí je tunelování protokolu PPP po sítích různého typu, například Internet. Pracuje se dvěma typy zpráv, datové a řídící. Je garantováno doručení řídících zpráv, ale datových ne. Při případné ztrátě se L2TP nestará o jejich opětovaný přenos. L2TP je k dispozici na všech zařízeních a operačních systémech, která jsou kompatibilní s technologií VPN. Nevýhodou toho protokolu je omezení ze stran některých firewallu a pomalá rychlost (20, s. 2 - 4).

### 1.5.7. IPSEC

IP security protocol je rozšíření IP protokolu o autentifikaci a šifrování. Může být využito na připojení typu klient – klient, ale také umožňuje bezpečnou komunikaci mezi klientem a VPN serverem. Skládá se ze dvou částí: Security Protocols a Internet Key Exchange. Security Protocols jsou protokoly definující, které informace mohou být přidány do IP paketu. IKE slouží převážně k autentizace zařízení, která si vyměňují klíč sloužící k šiforvání a dešifrování dat. Vyžaduje instalaci klientského softwaru na systému koncového uživatele (21).

### 1.5.8. SSL-VPN

Secure Sockets Layer Virtual Private Network využívá knihoven SSL pro zašifrovanou komunikaci pomocí socketů. Umožňuje bezpečné připojení uživatele se serverem přes veřejnou IP síť. Hodí se pro připojení mobilních uživatelů. Nabízí dva mechanismy, přesměrování portů a rozšíření sítě. Rozšíření sítě prostřednictvím tunelů povoluje širší přístup k síti a přesměrování portů poskytuje ochranu pro aplikace na známých serverech (22).

# 2. ANALÝZA SOUČASNÉHO STAVU

Analýza společnosti byla provede po konzultaci s IT specialistou a vedoucími jednotlivých oddělení. Identifikovala jsem jednotlivá aktiva společnosti, vymezila hrozby, které by je mohli poškodit a posoudila jednotlivá rizika. Na závěr této kapitoly jsem zhodnotila, jak firma chrání svá aktiva a která bezpečnostní opatření nasazují.

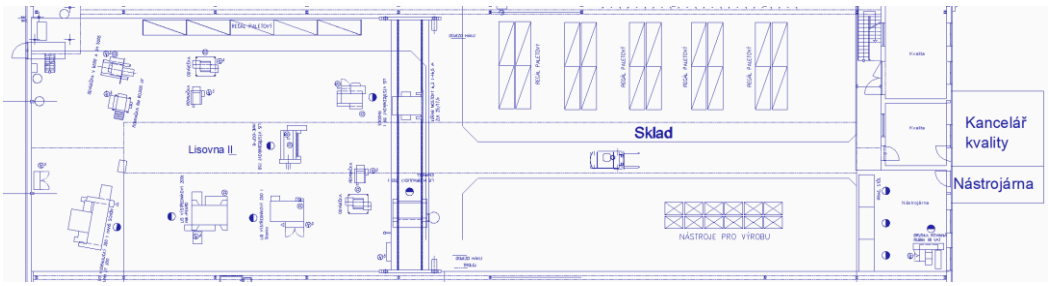
## 2.1. Společnost

Analýzu současného stavu společnosti jsem provedla při práci s firmou Antea, která dané společnosti provádí správu IT. Společnost si nepřála být jmenována, dále k ní bude odkazováno jako k firmě XYZ s.r.o. Firma se zabývá obráběním a výrobou autodílů. Sídlí u Olomouce ve vlastních prostorách, které jsou neustále monitorovány kamerovým systémem. Ve společnosti pracuje přibližně 180 zaměstnanců, ale prací s počítači se věnují převážně vedoucí pracovníci.

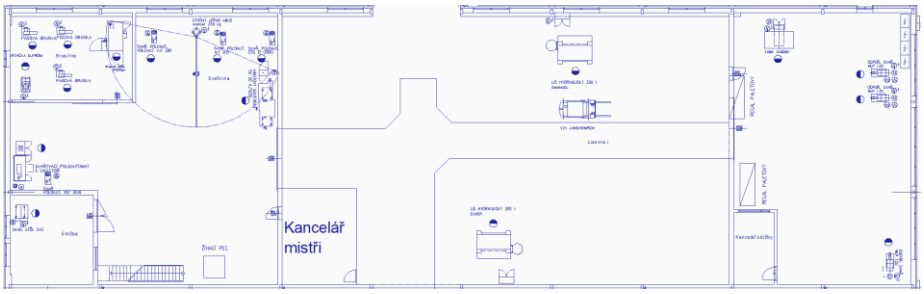
## 2.2. Vymezení hranic

### 2.2.1. Prostředí a budova

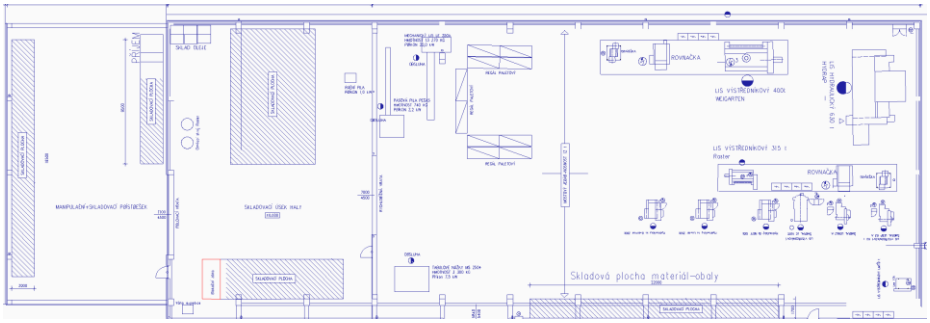
Společnost se skládá ze tří hlavních výrobních hal, administrátorské budovy a vedlejších kanceláří.




**Obrázek 7: Půdorys haly 1**
(Zdroj: Poskytla společnost)




**Obrázek 8: Půdorys haly 2**
(Zdroj: Poskytla společnost)

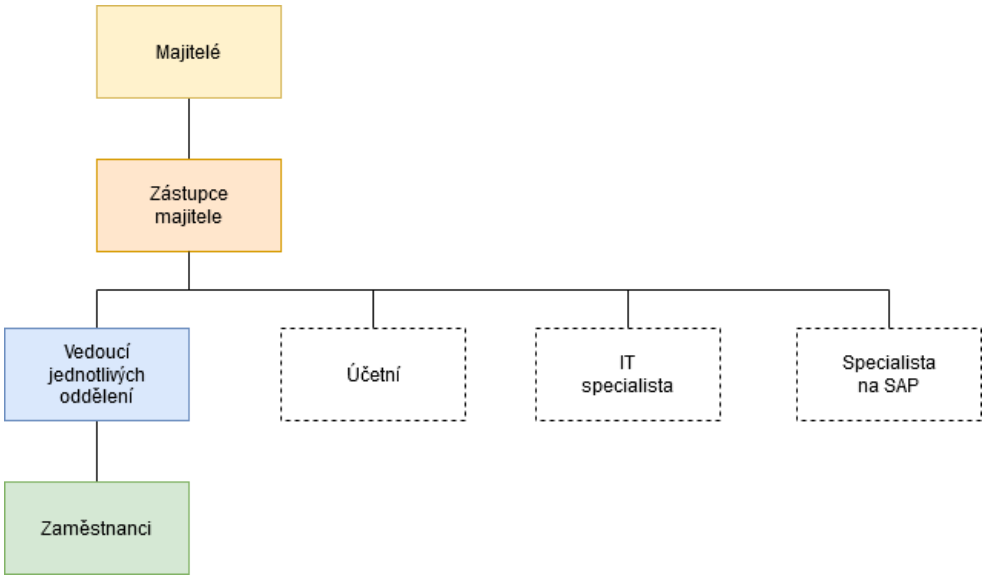



**Obrázek 9: Půdorys haly 3**
(Zdroj: poskytla společnost)

Firma má dále pronajatou halu v Prostějově, kterou bude potřebovat připojit zabezpečeným způsobem ke své síti. Halu bude využívat jako externí sklad.

### 2.2.2. Organizační struktura

Nejvyšší pozici ve firmě zastává majitel a jeho zástupce. Zástupce majitele se zároveň stará o personalistiku. Zodpovídá se jim 7 vedoucích oddělení. Jde o oddělení údržby, kvality, projektů, nákupů, svařovny, expedice a skladu. Firma dále zaměstnává účetní, externího IT specialistu a autorizovaného externího specialistu na SAP.




**Obrázek 10: Organizační struktura společnosti XYZ s.r.o.**
(Zdroj: Vlastní tvorba)

### 2.2.3. ICT vybavení

Do lokální počítačové sítě firmy XYZ s.r.o. je připojeno celkem 50 stolních počítačů či notebooků. Většina je umístěna v hlavní budově (výrobní hala s napojenými administrativními budovami a buňkami), pouze 6 z nich je umístěno v sousední budově, která slouží jako sklad a expedice. Někteří zaměstnanci využívají notebooky. Firma dále vlastní 3 servery, 2 databázové a jeden souborový. Servery jsou umístěny v samostatné a klimatizované místnosti. Jde o zamykatelnou místnost, kam mají přístup pouze majitel a IT specialista. Firma používá firewall routeru Mikrotik.

### 2.2.4. Informační systém

Pro svou činnost společnost využívá informační systém SAP Business One 9 a mzdový systém AZ Pro. Pro účely neustálého zvyšování kvality výroby také využívají systém Palstat.

Firma od zavedeného informačního systému požaduje splnění legislativních povinností, evidence zákazníků, dodavatelů a produktů, monitoring práce zaměstnanců a zabezpečení citlivých informací.

## 2.3. Identifikace aktiv

Na základě poskytnutých podkladů a informací o firmě jsem identifikovala následující aktiva a kdo za ně zodpovídá.

**Tabulka 3: Identifikace aktiv**

(Zdroj: Vlastní tvorba)

| Druh aktiva | Název | Odpovědnost |
|---|---|---|
| Informační aktiva | Data ohledně odběratelů | Vedoucí |
| | Data o zaměstnancích | Majitel |
| | Data o dodavatelích | Vedoucí |
| | Zálohy dat | IT specialista |
| | Účetnictví | Účetní |
| | Firemní politika a metodiky | Zástupce majitele |
| | Záznamy o výrobcích a produktech | Vedoucí |
| | Výrobní dokumentace | Vedoucí |
| Softwarová aktiva | SAP Business One 9 | SAP specialista |
| | mzdový systém AZ Pro | IT specialista/ (Podpora AZ Pro) |
| | Palstat | IT specialista/ (Podpora Palstat) |
| | Databáze | SAP specialista |
| Fyzická aktiva | Hardware (PC, notebooky,…) | IT specialista |
| | 2 Databázové servery | SAP specialista |
| | Souborový server | IT specialista |
| | Kamerový systém | IT specialista |
| | Aktivní síťové prvky | IT specialista |
| | Pasivní síťové prvky | IT specialista |

## 2.4. Klasifikace aktiv

Jednotlivá aktiva jsem dále ohodnotila, hodnotu určuje velikost rizika při poškození aktiva. Pro klasifikaci aktiv byla použita následující tabulka klasifikačních stupňů podle možných stupňů dopadu na společnost.

**Tabulka 4: Klasifikační stupně aktiv**

(Zdroj: Vlastní tvorba)

| Klasifikační stupeň | Klasifikační kritérium | Riziko pro organizaci |
|---|---|---|
| 1 | Žádný dopad na společnost | Bezvýznamné |
| 2 | Zanedbatelný dopad na společnost | Akceptovatelné |
| 3 | Potíže či finanční ztráty | Nízké |
| 4 | Vážné potíže či velké finanční ztráty | Nežádoucí |
| 5 | Existenční potíže | Nepřijatelné |

Výsledná hodnota klasifikačního stupně je vypočítán jako aritmetický průměr součtu hodnot důvěrnosti, dostupnosti a integrity.

$$\text{Výsledný klasifikační stupeň} = \frac{důvěrnost + dostupnost + integrita}{3}$$

**Tabulka 5: Klasifikace aktiv**

(Zdroj: Vlastní tvorba)

| Aktivum | Bezpečnostní atributy | | | Hodnota |
|---|---|---|---|---|
| | Dostupnost | Důvěrnost | Integrita | |
| Data ohledně odběratelů | 5 | 4 | 5 | 4,7 |
| Data o zaměstnancích | 2 | 3 | 5 | 3,3 |
| Data o dodavatelích | 3 | 4 | 4 | 3,7 |
| Zálohy dat | 4 | 4 | 4 | 4 |
| Účetnictví | 5 | 4 | 5 | 4,7 |
| Firemní politika a metodiky | 3 | 3 | 4 | 3,3 |
| Záznamy o výrobcích a produktech | 2 | 3 | 3 | 2,7 |
| Výrobní dokumentace | 3 | 4 | 4 | 3,7 |
| SAP Business One 9 | 2 | 3 | 3 | 2,7 |
| mzdový systém AZ Pro | 4 | 5 | 3 | 4 |
| Palstat | 2 | 1 | 2 | 1,7 |
| Databáze | 5 | 4 | 5 | 4,7 |
| Hardware (PC, notebooky,…) | 1 | 2 | 1 | 1,3 |
| 2 Databázové servery | 4 | 3 | 4 | 3,7 |
| Souborový server | 4 | 4 | 3 | 3,7 |
| Kamerový systém | 3 | 4 | 5 | 4 |
| Aktivní síťové prvky | 3 | 2 | 3 | 2,7 |
| Pasivní síťové prvky | 3 | 2 | 3 | 2,7 |

## 2.5. Oprávnění uživatelů

V následující tabulce je znázorněno, kteří zaměstnanci mají přístup k daným aktivům.

**Tabulka 6: Oprávnění uživatelů**

(Zdroj: Vlastní tvorba)

| | Majitel | Zástupce majitele | Vedoucí oddělení | IT specialista | Zaměstnanci | Účetní | Specialista na SAP |
|---|---|---|---|---|---|---|---|
| Data o klientech | X | X | X | | | | |
| Data o zaměstnancích | X | X | X | | | X | |
| Data o dodavatelích | X | X | X | | | X | |
| Zálohy dat | X | X | | X | | | X |
| Účetnictví | X | X | | | | X | |
| Firemní politika a metodiky | X | X | X | | | | |
| Záznamy o výrobcích a produktech | X | X | X | | X | | X |
| Výrobní dokumentace | X | X | X | X | X | | X |
| SAP Business One 9 | X | X | X | X | X | X | X |
| mzdový systém AZ Pro | X | X | X | X | | X | |
| Palstat | X | X | X | X | X | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Databáze | | | | X | | | X |
| Hardware (PC, notebooky, …) | X | X | X | X | X | X | X |
| 2 Databázové servery | | | | X | | | X |
| Souborový server | | | | X | | | |
| Kamerový systém | X | | | X | | | |
| Aktivní síťové prvky | | | | X | | | |
| Pasivní síťové prvky | | | | X | | | |

## 2.6. Identifikace hrozeb a zranitelnosti

Jednotlivé hrozby a příklady zranitelnosti jsem určila na základě konzultace s IT specialistou a vedoucími zaměstnanci firmy. Pro identifikaci hrozeb byla využita následující tabulka.

**Tabulka 7: Klasifikační stupně hrozeb**

(Zdroj: Vlastní tvorba)

| Klasifikační stupeň | Pravděpodobnost |
|---|---|
| 1 | Nízká |
| 2 | Střední |
| 3 | Vysoká |
| 4 | Velmi vysoká |

Možné hrozby a jejich klasifikační stupně jsem zaznamenala v následující tabulce.

**Tabulka 8: Klasifikace hrozeb**

(Zdroj: Vlastní tvorba)

| Druh hrozby | Hrozba | Stupeň zranitelnosti | Příklad zranitelnosti |
|---|---|---|---|
| Přírodní | Požár | 2 | Porušení detektorů kouře |
| | Vlhkost | 2 | Poloha v zátopové oblasti |
| | Zemětřesení | 1 | Poloha v rizikové oblasti |
| Technická | Výpadek proudu | 3 | Chyba na straně dodavatele |
| | Chyba v softwaru | 1 | Použití zastaralých verzí softwaru |
| | Výpadek internetového připojení | 2 | Chyba na straně dodavatele |
| | Poškození hardwaru | 2 | Výrobní vada |
| Úmyslná | Hackerský útok | 4 | Nedostačující zabezpečení sítě |
| | Napadení malwarem | 4 | Nedostatečné zabezpečení sítě |
| | Krádež | 1 | Nedostatečná zabezpečení budov |
| Neúmyslná | Neúmyslné smazání dat | 2 | Nedostatečné proškolení zaměstnanců |
| | Chybné uložení dat | 2 | Nedostatečné proškolení zaměstnanců |
| | Neúmyslné poškození dat | 3 | Nedostatečné proškolení zaměstnanců |

## 2.7. Možné bezpečnostní incidenty

V následující tabulce jsem uvedla příklady incidentů k daným hrozbám.

**Tabulka 9: Bezpečnostní incidenty**

(Zdroj: Vlastní tvorba)

| Druh hrozby | Hrozba | Incident |
|---|---|---|
| Přírodní | Požár | Poškození HW a ztráta dat, finanční újma |
| | Vlhkost | Poškození HW a ztráta dat, finanční újma |
| | Zemětřesení | Poškození HW a ztráta dat, finanční újma |
| Technická | Výpadek proudu | Pád serveru a následné narušení zálohování a ukládání dat |
| | Chyba v softwaru | Zaměstnanci nemohou plnohodnotně vykonávat svou činnost |
| | Výpadek internetového připojení | Zaměstnanci nemohou plnohodnotně vykonávat svou činnost |
| | Poškození hardwaru | Ztráta či únik dat, zaměstnanci nemohou plnohodnotně vykonávat svou činnost |
| Úmyslná | Hackerský útok | Ztráta cenných informací, finanční újma, zneužití dat |
| | Napadení malwarem | Ztráta cenných informací, finanční újma, know-how se může dostat ke konkurenci, zneužití dat |
| | Krádež | Odcizení hardwaru nebo dat a jejich následný prodej, poskytnutí konkurenci |
| Neúmyslná | Neúmyslné smazání dat | Zaměstnanec se z důvodu nedostatečného proškolení dopustil ztráty dat |
| | Chybné uložení dat | Zaměstnanec se z důvodu nedostatečného proškolení dopustil narušení záloh dat |
| | Neúmyslné poškození dat | Zaměstnanec se z důvodu nedostatečného proškolení dopustil poškození dat |

## 2.8. Matice zranitelnosti a úrovní rizik

Matice zranitelnosti a matice úrovní rizik byla vytvořena po konzultaci s IT specialistou a vedoucími jednotlivých oddělení. K vytvoření matic byl použit MS Excel.

### 2.8.1. Matice zranitelnosti

Matice zranitelnosti identifikovaných aktiv byla vyhodnocena na základě následující tabulky. Tato matice představuje pravděpodobnost vzniklé škody v důsledku hrozby u daných aktiv.

**Tabulka 10: Klasifikační stupně pro matici zranitelnosti**

(Zdroj: Vlastní tvorba)

| Klasifikační stupeň | Pravděpodobnost |
|---|---|
| 1 | Velmi nízká |
| 2 | Nízká |
| 3 | Střední |
| 4 | Vysoká |
| 5 | Kritická |

**Tabulka 11: Matice zranitelnosti**

(Zdroj: Vlastní tvorba)

| Aktiva | Požár | Vlhkost | Zemětřesení | Výpadek proudu | Chyba v softwaru | Výpadek internetového připojení | Poškození hardwaru | Hackerský útok | Napadení malwarem | Krádež | Neúmyslné smazání dat | Chybné uložení dat | Neúmyslné poškození dat |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Data ohledně odběratelů | 1 | 1 | 1 | 2 | 2 | 1 | | 5 | 5 | 2 | 4 | 3 | 4 |
| Data o zaměstnancích | 2 | 1 | 1 | 2 | 2 | 2 | | 5 | 5 | 1 | 4 | 2 | 3 |
| Data o dodavatelích | 1 | 1 | 2 | 2 | 2 | 1 | | 5 | 5 | 1 | 4 | 3 | 3 |
| Zálohy dat | 2 | 2 | 3 | 4 | 3 | 3 | 1 | 4 | 3 | 2 | 3 | 4 | 2 |
| Účetnictví | 3 | 2 | 2 | 3 | 4 | 2 | 1 | 3 | 4 | 1 | 3 | 3 | 2 |
| Firemní politika a metodiky | 2 | 1 | 1 | 2 | 2 | 1 | 1 | 2 | 2 | 1 | 2 | 3 | 3 |
| Záznamy o výrobcích a produktech | 3 | 2 | 2 | 1 | 3 | 1 | 1 | 2 | 1 | 2 | 3 | 2 | 2 |
| Výrobní dokumentace | 3 | 2 | 2 | 2 | 2 | 1 | 1 | 2 | 1 | 3 | 2 | 2 | 3 |
| SAP Business One 9 | | | | 5 | 5 | 3 | | 3 | 2 | | 3 | 2 | 1 |
| mzdový systém AZ Pro | | | | 4 | 4 | 3 | | 3 | 4 | | 2 | 1 | 1 |
| Palstat | | | | 4 | 4 | 3 | | 2 | 2 | | 3 | 2 | 3 |
| Databáze | 2 | 1 | 2 | 4 | 4 | 2 | | 3 | 3 | 2 | 4 | 2 | 2 |
| Hardware (PC, notebooky,…) | 4 | 3 | 3 | 1 | | 1 | 5 | 1 | | 5 | | | |
| 2 Databázové servery | 3 | 3 | 4 | 5 | 3 | 2 | 4 | 3 | 3 | 3 | 2 | 2 | 2 |
| Souborový server | 3 | 3 | 4 | 5 | 3 | 2 | 4 | 2 | 3 | 3 | 1 | 2 | 1 |
| Kamerový systém | 4 | 2 | 3 | 3 | 2 | 1 | 3 | 2 | | 2 | 1 | | |
| Aktivní síťové prvky | 3 | 3 | 4 | 3 | 2 | 2 | 4 | 2 | 1 | 3 | 2 | 1 | 1 |
| Pasivní síťové prvky | 3 | 3 | 2 | 3 | 1 | 2 | 4 | 2 | 1 | 3 | 1 | 2 | 1 |

## 2.8.2. Matice úrovní rizik

Matice úrovní rizik byla vyhodnocena na základě následující tabulky. Úroveň rizika jsem vypočítala jako součin rizika a dopadu.

**Tabulka 12: Klasifikační stupně pro matici úrovně rizik**

(Zdroj: Vlastní tvorba)

| Klasifikační stupeň | Pravděpodobnost |
|---|---|
| 0 - 20 | Velmi nízká |
| 21 - 40 | Nízká |
| 41 - 60 | Střední |
| 61 - 90 | Vysoká |
| 91 - 125 | Kritická |

**Tabulka 13: Matice úrovně rizik**

(Zdroj: Vlastní tvorba)

| Úroveň rizika | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Aktiva | A | Hrozby | T | Pozár | 2 | Vlhkost | 2 | Zemětřesení | 1 | Výpadek proudu | 3 | Chyba v softwaru | 1 | Výpadek internetového připojení | 2 | Poškození hardwaru | 2 | Hackerský útok | 4 | Napadení malwarem | 4 | Krádež | 1 | Neúmyslné smazání dat | 2 | Chybné uložení dat | 2 | Neúmyslné poškození dat | 3 |
| Data ohledně odběratelů | 4,7 | | 9,40 | | 9,40 | | 4,70 | | 28,20 | | 9,40 | | 9,40 | | | | 94,00 | | 94,00 | | 9,40 | | 37,60 | | 28,20 | | 56,40 |
| Data o zaměstnancích | 3,3 | | 13,20 | | 6,60 | | 3,30 | | 19,80 | | 6,60 | | 13,20 | | | | 66,00 | | 66,00 | | 3,30 | | 26,40 | | 13,20 | | 29,70 |
| Data o dodavatelích | 3,7 | | 7,40 | | 7,40 | | 7,40 | | 22,20 | | 7,40 | | 7,40 | | | | 74,00 | | 74,00 | | 3,70 | | 29,60 | | 22,20 | | 33,30 |
| Zálohy dat | 4,0 | | 16,00 | | 16,00 | | 12,00 | | 48,00 | | 12,00 | | 24,00 | | 8,00 | | 64,00 | | 48,00 | | 8,00 | | 24,00 | | 32,00 | | 24,00 |
| Účetnictví | 4,7 | | 28,20 | | 18,80 | | 9,40 | | 42,30 | | 18,80 | | 18,80 | | 9,40 | | 56,40 | | 75,20 | | 4,70 | | 28,20 | | 28,20 | | 28,20 |
| Firemní politika a metodiky | 3,3 | | 13,20 | | 6,60 | | 3,30 | | 19,80 | | 6,60 | | 6,60 | | 6,60 | | 26,40 | | 26,40 | | 3,30 | | 13,20 | | 19,80 | | 29,70 |
| Záznamy o výrobcích a produktech | 2,7 | | 16,20 | | 10,80 | | 5,40 | | 8,10 | | 8,10 | | 5,40 | | 5,40 | | 21,60 | | 10,80 | | 5,40 | | 16,20 | | 10,80 | | 16,20 |
| Výrobní dokumentace | 3,7 | | 22,20 | | 14,80 | | 7,40 | | 22,20 | | 7,40 | | 7,40 | | 7,40 | | 29,60 | | 14,80 | | 11,10 | | 14,80 | | 14,80 | | 33,30 |
| SAP Business One 9 | 2,7 | | | | | | | | 32,40 | | 13,50 | | 16,20 | | | | 32,40 | | 21,60 | | | | 16,20 | | 10,80 | | 8,10 |
| mzdový systém AZ Pro | 4,0 | | | | | | | | 48,00 | | 16,00 | | 24,00 | | | | 48,00 | | 64,00 | | | | 16,00 | | 8,00 | | 12,00 |
| Palstat | 1,7 | | | | | | | | 20,40 | | 6,80 | | 10,20 | | | | 13,60 | | 13,60 | | | | 10,20 | | 6,80 | | 15,30 |
| Databáze | 4,7 | | 18,80 | | 9,40 | | 9,40 | | 56,40 | | 18,80 | | 18,80 | | | | 56,40 | | 56,40 | | 9,40 | | 37,60 | | 18,80 | | 28,20 |
| Hardware (PC, notebooky,...) | 1,3 | | 9,20 | | 6,90 | | 3,90 | | 3,90 | | | | 2,30 | | 11,50 | | 5,20 | | | | 6,50 | | | | | | |
| 2 Databázové servery | 3,7 | | 22,20 | | 22,20 | | 14,80 | | 55,50 | | 11,10 | | 14,80 | | 29,60 | | 44,40 | | 44,40 | | 11,10 | | 14,80 | | 14,80 | | 22,20 |
| Souborový server | 3,7 | | 22,20 | | 22,20 | | 14,80 | | 55,50 | | 11,10 | | 14,80 | | 29,60 | | 29,60 | | 44,40 | | 11,10 | | 7,40 | | 14,80 | | 11,10 |
| Kamerový systém | 4,0 | | 32,00 | | 16,00 | | 12,00 | | 36,00 | | 8,00 | | 8,00 | | 24,00 | | 16,00 | | | | 8,00 | | 8,00 | | | | |
| Aktivní síťové prvky | 2,7 | | 16,20 | | 16,20 | | 10,80 | | 24,30 | | 5,40 | | 10,80 | | 21,60 | | 21,60 | | 10,80 | | 8,10 | | 10,80 | | 5,40 | | 8,10 |
| Pasivní síťové prvky | 2,7 | | 16,20 | | 16,20 | | 5,40 | | 24,30 | | 2,70 | | 10,80 | | 21,60 | | 21,60 | | 10,80 | | 8,10 | | 5,40 | | 10,80 | | 8,10 |

Z analýz vyplývá, že by se společnost měla primárně zaměřit na ochranu svých dat, protože jejich narušení, případná ztráta, by pro ně byla kritická. Největší hrozby jsou hackerský útok a napadení malwarem.

Mnoho aktiv společnosti podléhá střední úrovni rizika. Snížení těchto rizik nemusí být pro společnost prioritou, ale určitě by je neměla zanedbat a nasadit určitá opatření. Společnost může akceptovat hrozby s nízkou úrovní rizik.

**Tabulka 14: Kritické a vysoké úrovně rizika**

(Zdroj: Vlastní zpracování)

| Hrozba | Aktivum | Úroveň rizika |
|---|---|---|
| Hackerský útok | Data ohledně odběratelů | 94 |
| | Data o zaměstnancích | 66 |
| | Data o dodavatelích | 74 |
| | Zálohy dat | 64 |
| Napadení malwarem | Data ohledně odběratelů | 94 |
| | Data o zaměstnancích | 66 |
| | Data o dodavatelích | 74 |
| | Účetnictví | 75,2 |
| | Mzdový systém AZ Pro | 64 |

## 2.9. Vzdálené připojení

Společnost využívá pro vzdálené připojení protokolu RDP a program TightVNC, který využívá protokolu RFB. Protokol RDP je primárně využíván na připojení k serveru, protokol RFB (TightVNC) na sdílení a ovládání vzdálené obrazovky pracovních stanic v případě řešení problémů.

Vybraní zaměstnanci se potřebují připojovat na vzdálenou plochu serveru, kde běží SAP Business One 9. Protokol RDP využívá porty 3389, tento port je z vnější sítě velmi často napadán a blokován. Z důvodu zvýšení bezpečnosti jsou ve vstupním routeru nastaveny pravidla pro přeložení z vyšších portů pro jednotlivé servery 8600 až 8603. Jsou používána dlouhá bezpečná hesla k přihlašování k serveru. Ve firewallu je nastaveno

pravidlo, které umožňuje vzdálené připojení pouze z povolených IP adres. Na serveru Windows je nastavený počet pokusů zadání hesla s následnou blokací účtu.

V případě problému na pracovních stanicích se využívá program TightVNC, jenž komunikuje na portech 5900. Ve vstupním firewallu jsou rovněž pravidla pro přeložení komunikace pro jednotlivé stanice na porty 8800 až 8850. TightVNC používá při ověřování uživatele DES šifrování. Tato šifra je v současné době považována za nespolehlivou, protože využívá klíč o délce 64 bitů. Dá se prolomit za méně než 24 hodin.

## 2.10. Současná opatření

Jelikož společnost dbá na svá data, vyžaduje určitou úroveň bezpečnosti informačních aktiv, softwarových aktiv a hardwarových aktiv. Společnost má zavedená certifikát systému řízení ISO 9001, ISO 14001 a IATF 16949. Vyžaduje dodržování vhodných bezpečnostních opatření, která mají pomoci zabezpečit společnost. Jejími současnými opatřeními jsou:

- Vstup a provoz je monitorován kamerovým systémem
- Součástí přijímacího řízení nového zaměstnance je proškolení a podepsání interní směrnice o bezpečném chování
- Společnost má zavedenou směrnici o bezpečném chování uživatelů
- Společnost nemá ISO27001
- Společnost nezaměstnává žádného specialistu na informační bezpečnost, jediný, kdo se o ni určitým způsobem stará je externí IT specialista
- Jako vstupní firewall je použit firewall routeru Mikrotik, který je možno konfigurovat pro účely VPN, umí pouze paketové a stavové filtry
- Každý uživatel má na svém počítači/notebooku nainstalovaný antivirový program
- Každý uživatel má přidělena přístupová práva na úrovni operačního systému
- Je používán systém silných hesel
- Účetnictví je přístupné pouze autorizovaným osobám
- Zálohy dat probíhají každý den na jiný fyzický disk, zálohují se soubory, všechny databáze a s ní související přílohy
- Vzdálený přístup je umožněn pomocí RDP protokolu

- Doménový server sloužící k ověřování uživatelů zatím není součástí sítě – firma nemá zavedenou doménu
- Ověřování uživatelů je pouze na úrovni serveru Windows, uživatelská jména a hesla jsou dále ověřována na úrovni serveru SAP
- Routery Mikrotik umožňují vytvoření VPN typu PPTP, SSTP a L2TP
- Routery Mikrotik dále umožňují vytvoření Radius serveru, který společnost dosud nezavedla
- Jednotlivý uživatelé nemají administrátorské oprávnění
- Na počítačích je nastaven lokální firewall

## 2.11. Požadavky vedení společnosti

Společnost vyžaduje zvýšení zabezpečení především informačních a softwarových aktiv, jelikož ta jsou pro ni nejcennější. Z fyzických aktiv je pro ni důležité, aby server byl na bezpečném uzamčeném místě a byla zajištěna jeho pravidelná údržba.

Společnost si je vědoma, že její zaměstnanci nejsou řádně proškoleni o bezpečnosti ICT. Dále požadují zvýšené zabezpečení pro vzdálené připojení uživatelů do podnikové sítě a zároveň zabezpečené propojení pobočky skladu přes internet a možnost komunikace z pobočky s centrálním serverem SAPu. Pro přihlašování uživatelů do sítě firma požaduje zavést doménový server a virtuální logické sítě (VLAN), aby došlo k oddělení administrace důležitých síťových prvků a serverů, vedení, managementu a zaměstnanců. O tento požadavek se stará jiná externí dodavatelská firma.

## 2.12. Zhodnocení současného stavu

Společnost používá připojení s nízkým zabezpečením přes RDP a TightVNC. Ověřování uživatelů je pouze na úrovni serveru, což umožňuje odposlech provozu na síti. Do sítě se může připojit jakýkoliv uživatel s jakýmkoliv počítačem, který může být zavirovaný nebo obsahovat závadný software. V případě spuštění škodlivého kódu může dojít ke smazání, poškození nebo zašifrování sdílených dat. Dále vzniká nebezpečí cíleného útoku uvnitř sítě, kdy uživatel může odposlouchávat provoz na síti (například pomocí programu Wireshark). Je žádoucí zabezpečit připojení z externích sítí za pomocí šifrované VPN.

Společná sdílená data, ERP systém a informační systém jsou instalovány a centralizovány na serverech a je nutné soustředit se na zvýšení zabezpečení přístupu k nim.

V případě poškození nebo nepředvídaného výpadku některého ze serverů může dojít k významnému výpadku výroby celé firmy do té doby, než bude opraven nebo přeinstalován.

Firma má vyšší počet zaměstnanců a bylo by žádoucí zaměstnat odborníka na informační bezpečnost a správce sítě. Měl by být kladen větší důraz na pravidelné proškolení zaměstnanců v oblasti informační bezpečnosti, aby chyby z nepozornosti a neznalosti nevznikaly tak často. Měli by klást větší důraz na ochranu citlivých dat.

Administrace celé sítě začíná být neúměrně složitá, protože v případě hromadné instalace programů na více stanic je nutné obcházet všechny tyto stanice a instalovat odděleně – není využito výhod domény.

# 3. VLASTNÍ NÁVRHY ŘEŠENÍ

V této kapitole se zabývám vlastním návrhem konkrétních opatření, která by firma měla podstoupit pro zlepšení zabezpečení jejích aktiv. Opatření byla navržena na základě analýzy aktiv a požadavků společnosti.

## 3.1. Záložní server

Jeden z návrhů na zlepšení bezpečnosti ICT by byla instalace dalšího záložního serveru pro případ havárie. Záložní server by obsahoval virtualizované funkční servery, jejichž data jsou pravidelně zálohovaná na denní bázi. Zálohování by probíhalo metodou zrcadlení a převodem do virtuálních disků jednou denně, přičemž data musí být zašifrovaná. Data jsou uchovávána deset dní zpětně, než dochází k přepsání záloh novými daty. Každá jedna měsíční záloha je archivovaná po dobu dvou let. V případě ztráty dat je nutné stanovit postup, jak bude obnova záloh probíhat. Stav záloh by měl být kontrolován minimálně jednou měsíčně. Záložní server nesmí být volně přístupný a musí se nacházet na bezpečném místě, kam mají přístup pouze oprávněné osoby. Ideálně by měl být zamčený v samostatné místnosti. Měly by být zavedeny kontroly funkčnosti technických zařízení minimálně jednou měsíčně. Pro servis některých zařízení bude nutné využít služby externích dodavatelů. Veškeré kontroly musí být evidovány.

Zavedení záložního serveru sníží úroveň rizika výpadku nebo přerušení výrobního procesu firmy z důvodu neočekáváné poruchy hlavních serverů. Rovněž se zkrátí doba přechodu na záložní server. Zůstane zachována výhoda centralizace dat firmy.

## 3.2. Zavedení doménové struktury

Pro snížení úrovně rizika v oblasti správy uživatelů doporučuji zavedení domény, která by zvýšila bezpečnost na vnitřní síti a zjednodušila centrální správu všech uživatelů. Doménový server by řešila dodavatelská firma. Doména poběží na doménovém serveru a bude obsahovat všechny informace o objektech v síti (uživatelé, skupiny, počítače, tiskárny, …). Aby se uživatelé mohli přihlásit, musí být ověřeni na doménovém serveru, kde jim budou rovněž nastavena přístupová práva v závislosti na jejich pracovní činnosti.

Správa a nastavení všech uživatelů a přístupů se tak sjednocuje, centralizuje a usnadňuje.

Windows server obsahuje rovněž Network Policy Server, který umožňuje propojení hlavního routeru Mikrotik s Windows serverem a využít autentizaci pomocí Radius serveru.

Zavedením domény je možné využít globálních skupinových politik pro nastavení všech objektů domény (počítače, tiskárny, …). Tímto způsobem bude vynucováno dodržování následujících pravidel:

- Dodržování pravidel silného hesla
- Pravidelná změna hesla
- Zamezení přístupu uživatelů ke konfiguračním nastavením
- Zákaz přístupu k příkazovému řádku
- Zákaz přístupu vybraných zaměstnanců k externím paměťovým médiím
- Zákaz instalace nepovoleného softwaru
- Zákaz přihlášení k účtu hosta

Pomocí skupinových politik budou mapovány přístupy uživatelů a skupin k jednotlivým tiskárnám a sdíleným složkám. Tiskárny využívají printserver, který je součástí doménového serveru.

Zavedením skupin se zjednoduší správa tím způsobem, že administrátor může nastavovat oprávnění hromadně, nikoliv po jednotlivcích. Společnost využije dva typy skupin, distribuční skupinu a skupinu zabezpečení. Distribuční skupinu použije k doručování elektronické pošty. Skupinu zabezpečení využije k nastavení zabezpečení veškerých objektů domény.

Názvy uživatelských skupin budou určeny dle potřeb firmy. Jednotlivým skupinám nastavuje oprávnění administrátor. Administrátorem bude IT specialista a nastaví jednotlivá oprávnění po dohodě s majitelem a vedením společnosti. Počáteční nastavení rozdělení na skupiny se nachází v příloze III.

Dalším přínosem zařazení počítačů do domény je možnost automatické instalace softwaru pro klientské počítače pomocí připravených spouštěcích skriptů. Tyto spustitelné skripty spolu s instalačními balíčky budou nasdíleny ve společném adresáři. Ke spouštění skriptů se využije konzolová aplikace Windows PowerShell.

**Zabezpečení přístupu do sítě pomocí standardu IEEE 802.1x**

Z důvodu možnosti připojení do sítě cizích počítačů, které mohou být zavirovány anebo odposlouchávat důležitá data, navrhuji zavést zabezpečení přístupu do sítě pomocí standardu IEEE 802.1x. Standard IEEE 802.1x využívá kontrolu řízení přístupu založenou na portu. Zavedení tohoto způsobu zabezpečení vyžaduje nasazení síťových switchů s managementem podporujících 802.1x. Firma používá síťové prvky výrobce Mikrotik, který tento standard podporuje. Když se klientský počítač připojí do sítě, je síťový port ve stavu „neautorizován" takže veškerá komunikace kromě provozu standardu 802.1x je blokována. Roli autentifikačního serveru může plnit Radius server. V případě úspěšného zadání autentifikačních údajů je povolena další síťová komunikace (port je přepnut do stavu autorizován). Pokud se klientský počítač odpojí, je port přepnut opět do stavu „neautorizován". Stejný princip je aplikován na bezdrátové připojení.

**Přidělení VLAN Radius serverem**

Úroveň rizik by mohla být snížena zavedením VLAN sítí. V hlavním routeru firmy budou nadefinovány sítě VLAN, které budou přiřazeny uživatelům dle výsledků autentifikace serverem Radius. Ve firewallu jsou následně nadefinovány pravidla komunikace pro sítě VLAN. Navrhuji samostatnou VLAN síť pro každé oddělení.

## 3.3. Autentizační pravidla

Každý zaměstnanec dostane přidělené heslo do operačního a informačního systému, které si musí ihned po přihlášení změnit. Politiku hesel má na starosti určený administrátor IT. Doporučuji častou obnovu hesel a přístupových údajů. Hesla musí být bezpečná a měla by obsahovat minimálně 15 znaků, velká a malá písmena, speciální nealfanumerický znak a nesmí mít slovníkový význam. Mohou být také nastavena dvoufázová hesla. Rovněž by bylo vhodné nastavit interval vynucení změny hesla jedenkrát za čtvrt roku. Nově zvolené heslo nesmí být shodné s dříve používaným heslem. Pokud zaměstnanec zadá pětkrát po sobě špatné heslo, účet se uzamkne na dobu jedné hodiny. Dodržování těchto pravidel výrazně sníží riziko odposlechu hesla počítačovými roboty. Pokud zaměstnanec opouští své pracoviště, je nutné, aby se odhlásil. Zároveň musí zabezpečit, aby jakékoliv dokumenty obsahující citlivé údaje nebyly volně dostupné a ideálně byly uloženy v uzamykatelné zásuvce nebo kartotéce.

## 3.4. Chování uživatelů

Chování uživatelů je vymezeno ve firemní směrnici o bezpečnosti IT. Firma by měla omezit zaměstnancům přístup na určité webové stránky, které mohou být nebezpečné. Navrhovala bych povolit pouze stránky nutné k práci. Také by měl být pravidelně aktualizován antivirový program. Navrhuji zavedení centrální aktualizace antivirového programu na všech stanicích. Aktualizace by probíhala co nejdříve mimo pracovní dobu zaměstnanců. Dále bez povolení vedení nebude možná instalace jiných programů než těch, potřebných k práci, které pochází z ověřených zdrojů.

Zaměstnanec bude mít dovoleno přistupovat pouze k těm datům, která potřebuje k výkonu své pracovní činnosti.

V případě výskytu incidentu by je zaměstnanci měli okamžitě ohlásit telefonicky nebo prostřednictvím e-mailu vedení nebo externímu IT specialistovi. Bude stanoven přesný postup, jak má zaměstnanec v tomto případě postupovat. Bude zaevidován čas a datum výskytu incidentu, jméno zaměstnance, jenž incident nahlásil, místo výskytu a popis incidentu.

**Školení uživatelů**

Dalším navrženým opatřením je pravidelné a důkladné proškolení zaměstnanců i vedení v oblasti kybernetické bezpečnosti. Veškeré náležitosti týkající se vzdělávacího plánu budou stanoveny ve směrnici. Za školení by byl zodpovědný externí odborník na informační bezpečnost z firmy Antea, ze které je IT specialista firmy. Školení budou povinná a měla by probíhat minimálně jednou ročně. V rámci školení by měl být kladen důraz na znalost směrnic, škodlivých softwarů, škodlivou elektronickou poštu, otevírání podezřelých e-mailů a stahování jejich příloh, které mohou obsahovat viry. Měl by být probrán aktuální stav bezpečnostní politiky organizace a zdůrazněny změny oproti minulému školení. Každé školení by mělo být zakončené kontrolním testem pro ověření znalosti zaměstnanců. Cílem tohoto opatření je předejití možný chyb způsobených neznalostí zaměstnanců.

Zaměstnanci by byli rozděleni do školících skupin na základě jejich pracovních pozic. Vedoucí oddělení by absolvovali také školení pro management. Popřípadě by bylo možné zajistit také školení ohledně GDPR o zpracování citlivých údajů pro externí účetní a

zástupce majitele, který se zabývá personalistikou organizace. Byl by najat odborný školitel z externí firmy, která se touto problematikou specializuje.

Školení managementu by se účastnili vedoucí oddělení. Zaměstnanci by jejich školení absolvovali vždy po jednotlivých odděleních, přítomen by byl také příslušný vedoucí.

Nově nastupující zaměstnanci musí podstoupit povinná školení, například BOZP, tento proces by mohl být usnadněn využitím například platformy www.instructor.cz. Některá míň komplexní školení by mohli probíhat formou e-learningu. Na závěr by každý e-learning obsahoval test a po úspěšném splnění testu by měl v systému označené školení jako splněno.

**Postihy**

Porušení určených pravidel informační bezpečnosti bude považováno za porušení pracovní smlouvy. Pracovní smlouva může zahrnovat finanční postih v případě porušení směrnic. Při úniku osobních dat může navíc firmě hrozit pokuta za porušení GDPR a tento incident může způsobit výrazné zhoršení pověsti společnosti.

**Next-Generation firewall**

Společnost by v případě expanze bezpečnost síťového provozu a ochranu dat mohla dále zlepšit implementací Next-Generation Firewallu. Nasazení této technologie by zařizoval externí dodavatel, například FortiGate. V případě, že bude použitý NGFW, bude VPN realizována pomocí tohoto firewallu, protože nabízí výkonnější šifrování a nižší latenci.

Mezi výhody NGFW patří kontrola SSL komunikace před škodlivým obsahem. Optimalizuje funkčnost sítě a její zabezpečení na základě monitorování kapacity šířky pásma. Používá bezpečnostní technologie IPS (Intrusion Prevention Systém) s velmi nízkou latencí. Obsahuje optimalizované připojení ke cloudovým službám. Tvorba pravidel pro práci na internetu a její monitoring je jednodušší. Dokáže zabezpečit a ochránit pobočky firmy. Má vestavěné bezpečnostní funkce jako jsou IPS, VPN, firewall, filtrování webu, antivirus a antimalware. Umožňuje monitoring všech připojených uživatelů a zařízení.

## 3.5. Ochrana proti malwaru

Všechna zařízení, která zaměstnanci využívají k práci musí být řádně zabezpečena antivirovým programem, který se spouští při startu zařízení v pozadí a je pravidelně aktualizován. V případě, že antivirus nalezne cokoliv podezřelého, zaměstnanec má povinnost kontaktovat IT specialistu.

## 3.6. Ochrana citlivých informací

K citlivým osobním údajům o zaměstnancích, například jejich zdravotní stav, mzda, adresa bydliště a další, by měla mít přístup pouze mzdová účetní a personalistka. Tyto údaje jsou na serveru rovněž šifrovány a zabezpečeny heslem. Při nástupu do zaměstnání bude založena zabezpečená karta zaměstnance v IT systému a zaměstnanec musí podepsat souhlas se zpracováním osobních údajů pro nezbytně nutné účely organizace. Po dobu trvání pracovního poměru jsou veškeré osobní údaje zaměstnanců uchovávány v osobním spisu v rozsahu nezbytném pro vykonávání práce (životopis, pracovní posudek, pracovní smlouva, …). Při ukončení pracovního poměru zaměstnance jsou tyto údaje ze všech informačních systémů odstraněny dle zákona 101/2000 Sb. o ochraně osobních údajů s ohledem na nařízení GDPR.

**Zásada prázdného stolu a prázdné obrazovky**

Zaměstnanci společnosti by měli dodržovat zásadu prázdného stolu a prázdné obrazovky počítače. Pracovní stůl zaměstnance musí být v době, kdy se na něm nepracuje, uklizený, v ideálním případě prázdný. Všechno dokumenty týkající se klientů nebo obsahující citlivá data, musí být uchovaný v uzamykatelných skříňkách. Dokumenty nesmí zůstat volně ležet na místech, kde k nim mají přístup třetí osoby. Pokud zaměstnanec opouští počítač na krátkou chvíli, například na obědovou pauzu, a ponechá počítač zapnutý, musí uzamknout obrazovku. Dodržováním těchto pravidel se zamezí případnému zneužití uživatelského účtu a informací.

**Likvidace aktiv**

Při výměně nebo likvidaci aktiva musí být data na něm důkladně smazána. K likvidaci dat je možno použít speciální software. Pokud bylo zlikvidováno aktivum s citlivými údaji, měly by se o tom vést záznamy. Bude-li nutné cestovat se zařízením na služební

cestu nebo za klientem, je taktéž potřeba vše zaznamenat a dbát na bezpečnost aktiva. Data musí být řádně zašifrována v případě krádeže. K cestování je možná využít pouze zařízení, která mají aktuální zálohu.

**BitLocker**

Dále by bylo možné zašifrovat disky v počítačích nástrojem BitLocker, který je součástí operačního systému Windows. Po zašifrování je k datům přístupu nutný dešifrovací klíč, který se načte ze serveru ve firemní síti. Při zapnutí počítače je možné vyžadovat po uživateli PIN, identifikační kód. Po opakovaném chybném zadání tohoto kódu se počítač uzamkne.

Proti úmyslnému útoku ze strany zaměstnance se lze chránit pouze důkladným výběrovým řízením.

## 3.7. Zrušení přímého připojování přes RDP

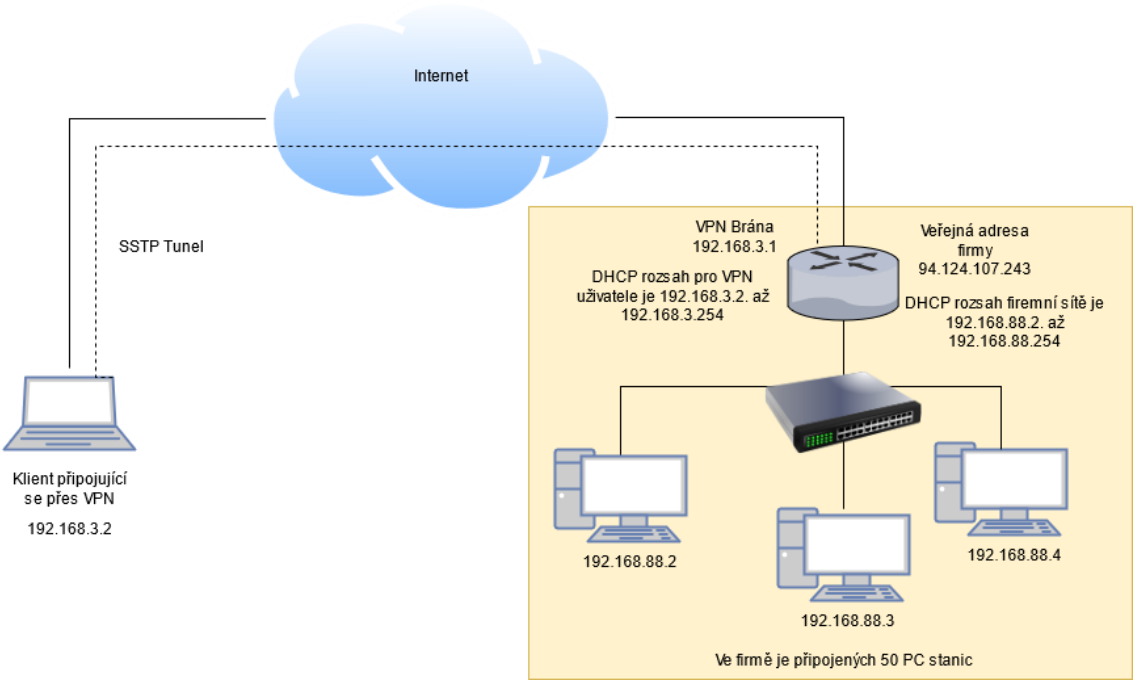
Společnost pro vzdálené připojení využívá protokol RDP a program TightVNC. Tento způsob připojování do sítě je velice rizikový a navrhovala bych, aby veškeré připojení z venku bylo realizováno přes nově zavedenou šifrovanou VPN s případnou autentizací na Radius serveru. Veškerá komunikace bude takto lépe zabezpečená.

## 3.8. Zavedení virtuální privátní sítě

Dále doporučuji zavést VPN pomocí protokolu SSTP (prostřednictvím šifrování SSL/TLS). SSL/TLS komunikuje na portu 443. Typ SSTP byl zvolen z důvodu vysoké průchodnosti, schopnosti obejít většinu firewallů, podpory společnosti Microsoft a vysoké úrovni šifrování.

V případě, že bude ve firmě zavedena doména, lze využít k ověření uživatele VPN Radius Server, který může spolupracovat s routerem výrobce Mikrotik.

Následující blokové schéma znázorňuje připojení vzdáleného klienta do firemní sítě. Testovací konfigurace byla programována na počítači s OS Windows 10. Jako testovací router byl použit Mikrotik 750GR3 s operačním systémem RouterOS. Ke konfiguraci hlavního routeru byl použit program WinBox, který je zdarma ke stažení u výrobce Mikrotik.




**Obrázek 11: Blokové schéma zapojení sítě**
(Zdroj: Vlastní zpracování)

Instalace a nastavení VPN umožní bezpečným způsobem propojit firmu s externím skladem. VPN se rovněž využije pro zvýšení bezpečnosti přístupu na vzdálenou plochu. Vzdálený přístup je v současné době velmi často vyžadován. Práce z domu bude umožněna pouze zaměstnancům na vyšší pozici a podmínky budou specifikovány ve směrnici. Při práci z domova musí zaměstnanec dodržovat stejně pravidla o bezpečnosti práce jako na pracovišti.

Zaměstnanci, kteří budou mít možnost pracovat přes VPN budou muset být náležitě proškoleni. Každý uživatel dostane přidělený firemní notebook s nastaveným přístupem přes VPN. Dále mu bude přiděleno uživatelské jméno a heslo. Pravidla pro používání VPN budou zanesena ve směrnici.

## 3.9. Analýza rizik po nasazení navrhovaných opatření

Následující matice ukazuje, jak by nasazením navrhovaných opatření bylo možné výrazně snížit úrovně rizika ve firmě.

Důkladné a pravidelné školení by mohlo zabránit neúmyslným chybám při práci s daty nebo jejich smazání. Zaměstnanci by měli lepší povědomí o stavu zabezpečení firmy a díky testům by byli kontrolovány jejich znalosti. Také by zlepšilo povědomí zaměstnanců o škodlivých emailech obsahujících viry a dalo by se tak zabránit hackerským útokům či napadení malwarem. Této hrozbě by předcházelo i používání a pravidelná aktualizace antivirového programu. Dále by ztrátě dat zamezilo pravidelné zálohování a zrcadlení disků. Ochraně citlivých dat výrazně pomohou nasazení BitLockeru a dodržování zásady prázdného stolu a prázdné obrazovky. Omezení rizika zavirování z cizích počítačů lze také snížit zavedením standardu IEEE 802.1x. Zrušením přímého připojování do firmy pomocí protokolu RDP a nasazením nové VPN by bylo vylepšeno zabezpečení sítě a umožněno bezpečné připojení externího skladu.

**Tabulka 15: Matice úrovní rizik po nasazení navržených opatření**

(Zdroj: Vlastní tvorba)

| Úroveň rizika | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Aktiva | A | Hrozby | T | Požár | 2 | Vlhkost | 2 | Zemětřesení | 1 | Výpadek proudu | 3 | Chyba v softwaru | 1 | Výpadek internetového připojení | 3 | Poškození hardwaru | 2 | Hackerský útok | 3 | Napadení malwarem | 3 | Krádež | 1 | Neúmyslné smazání dat | 2 | Chybné uložení dat | 2 | Neúmyslné poškození dat | 3 |
| Data ohledně odběratelů | 4,7 | | | 9,40 | | 9,40 | | 4,70 | | 28,20 | | 9,40 | | 14,10 | | | | 56,40 | | 56,40 | | 9,40 | | 28,20 | | 28,20 | | 56,40 |
| Data o zaměstnancích | 3,3 | | | 13,20 | | 6,60 | | 3,30 | | 19,80 | | 6,60 | | 19,80 | | | | 39,60 | | 39,60 | | 3,30 | | 19,80 | | 13,20 | | 29,70 |
| Data o dodavatelích | 3,7 | | | 7,40 | | 7,40 | | 7,40 | | 22,20 | | 7,40 | | 11,10 | | | | 44,40 | | 44,40 | | 3,70 | | 22,20 | | 22,20 | | 33,30 |
| Zálohy dat | 4,0 | | | 8,00 | | 16,00 | | 12,00 | | 48,00 | | 12,00 | | 36,00 | | 8,00 | | 36,00 | | 36,00 | | 8,00 | | 16,00 | | 24,00 | | 24,00 |
| Účetnictví | 4,7 | | | 18,80 | | 18,80 | | 9,40 | | 42,30 | | 18,80 | | 28,20 | | 9,40 | | 42,30 | | 42,30 | | 4,70 | | 18,80 | | 18,80 | | 28,20 |
| Firemní politika a metodiky | 3,3 | | | 6,60 | | 6,60 | | 3,30 | | 19,80 | | 6,60 | | 9,90 | | 6,60 | | 19,80 | | 19,80 | | 3,30 | | 6,60 | | 13,20 | | 29,70 |
| Záznamy o výrobcích a produktech | 2,7 | | | 10,80 | | 10,80 | | 5,40 | | 8,10 | | 8,10 | | 8,10 | | 5,40 | | 16,20 | | 8,10 | | 5,40 | | 10,80 | | 5,40 | | 16,20 |
| Výrobní dokumentace | 3,7 | | | 22,20 | | 14,80 | | 7,40 | | 22,20 | | 7,40 | | 11,10 | | 7,40 | | 22,20 | | 11,10 | | 11,10 | | 7,40 | | 7,40 | | 33,30 |
| SAP Business One 9 | 2,7 | | | | | | | | | 32,40 | | 13,50 | | 24,30 | | | | 24,30 | | 16,20 | | | | 10,80 | | 5,40 | | 8,10 |
| mzdový systém AZ Pro | 4,0 | | | | | | | | | 48,00 | | 16,00 | | 36,00 | | | | 36,00 | | 48,00 | | | | 8,00 | | 8,00 | | 12,00 |
| Palstat | 1,7 | | | | | | | | | 20,40 | | 6,80 | | 15,30 | | | | 10,20 | | 10,20 | | | | 6,80 | | 6,80 | | 15,30 |
| Databáze | 4,7 | | | 18,80 | | 9,40 | | 9,40 | | 56,40 | | 18,80 | | 28,20 | | | | 42,30 | | 42,30 | | 9,40 | | 28,20 | | 18,80 | | 28,20 |
| Hardware (PC, notebooky,…) | 1,3 | | | 10,40 | | 7,80 | | 3,90 | | 3,90 | | | | 3,90 | | 13,00 | | 3,90 | | | | 6,50 | | | | | | |
| 2 Databázové servery | 3,7 | | | 22,20 | | 22,20 | | 14,80 | | 33,30 | | 11,10 | | 22,20 | | 29,60 | | 33,30 | | 33,30 | | 11,10 | | 14,80 | | 14,80 | | 22,20 |
| Souborový server | 3,7 | | | 22,20 | | 22,20 | | 14,80 | | 33,30 | | 11,10 | | 22,20 | | 29,60 | | 22,20 | | 33,30 | | 11,10 | | 7,40 | | 14,80 | | 11,10 |
| Kamerový systém | 4,0 | | | 32,00 | | 16,00 | | 12,00 | | 36,00 | | 8,00 | | 12,00 | | 24,00 | | 24,00 | | | | 8,00 | | 8,00 | | | | |
| Aktivní síťové prvky | 2,7 | | | 16,20 | | 16,20 | | 10,80 | | 24,30 | | 5,40 | | 16,20 | | 21,60 | | 16,20 | | 8,10 | | 8,10 | | 10,80 | | 5,40 | | 8,10 |

**Tabulka 16: Nová úroveň rizik u nejohroženějších aktiv**

(Zdroj: Vlastní zpracování)

| Hrozba | Aktivum | Úroveň rizika |
|---|---|---|
| Hackerský útok | Data ohledně odběratelů | 56,4 |
| | Data o zaměstnancích | 39,6 |
| | Data o dodavatelích | 44,4 |
| | Zálohy dat | 36 |
| Napadení malwarem | Data ohledně odběratelů | 56,4 |
| | Data o zaměstnancích | 39,6 |
| | Data o dodavatelích | 44,4 |
| | Účetnictví | 42,3 |
| | Mzdový systém AZ Pro | 48 |

## 3.10. Přínosy nových opatření

Doporučená bezpečnostní opatření mají za hlavní cíl zvýšit zabezpečení aktiv společnosti a snížit riziko výskytu incidentů. Požadavky, které firma určila budou splněny. Pokud by organizace do budoucna zvažovala získání ISO 27001, tato opatření jí by pomohla ke splnění auditu.

Zřízením záložního serveru získá firma možnost pokračování v činnosti v případě havárie prvního serveru. Centrální systémy budou během krátké chvíle opět spuštěny na záložním serveru. V případě, že by nebyl k dispozici záložní server a došlo by k havárii, výroba by byla zastavená na dobu minimálně jednoho dne, než by byl znovu nainstalován a zprovozněn nový server externí firmou. Pravidelné zálohování a metoda zrcadlení disků předchází ztrátě dat společnosti.

Nasazení doménového serveru by umožnilo centrální správu všech uživatelů ve vnitřní síti, vynucení bezpečnostních pravidel a hromadnou instalaci softwaru.

Vynucením pravidla o silném heslu a jeho pravidelné změně bude zvýšeno zabezpečení pracovních počítačů, stejně jako zamezení přístupu zaměstnanců ke konfiguračním nastavení, příkazovému řádku a zákaz instalace jiných programů než těch, které jsou povoleny společností. Zabezpečení přístupu do sítě pomocí standardu IEEE 802.1x zamezí připojení cizích neautorizovaných počítačů do sítě a zmenší se riziko odposlechu provozu na síti nebo zavirování.

Spuštěním Radius serveru firma získá zabezpečené ověřování uživatelů. Využitím síťových komponent výrobce Mikrotik bude mít organizace možnost propojit komunikaci aktivních prvků s Radius serverem.

Dodržování zásady prázdného stolu a pracovní plochy bude mít za přínos zlepšení ochrany citlivých údajů. Ochraně citlivých dat také pomůže důkladná likvidace aktiv, která obsahovala tato data. Při ztrátě počítače s citlivými daty zabrání přístup neoprávněným osobám BitLocker, který při zadání chybného hesla uzamkne počítač a zašifruje disk.

Nastavením a instalací serverové části antivirového programu bude získána kontrola pravidelné aktualizace všech koncových stanic a serverů. Tím se výrazně sníží riziko zavirování nebo spuštění škodlivého kódu.

Přínosem důkladného a pravidelného proškolování zaměstnanců bude snížení úrovně rizika neúmyslných chyb při úpravě a ukládání dat a smazání dat z nepozornosti. Rovněž dojde ke snížení úrovně rizik v těchto oblastech a v oblasti hackerského útoku. Zaměstnanci budou mít větší znalost z oblasti informační gramotnosti a bezpečnosti.

Zavedením VPN a zrušením připojení přes protokol RDP se zvýší bezpečnost vzdáleně připojených uživatelů a firemní síť bude zpřístupněná pouze pro firemní uživatele. Zakázáním nevyžádané příchozí komunikace bude sníženo bezpečnostní riziko napadení sítě. Zvolením VPN typu SSTP budou získány výhody jako schopnost projít přes většinu firewallů poskytovatelů, integraci a kompatibilitu se systémem Windows, na kterém je provozována firma, a vysokou úroveň šifrování. Z hlediska budoucích aktualizací je také přínosem podpora firmy Microsoft. Hlavním přínosem tohoto opatření bude bezpečné propojení externího skladu s hlavní halou firmy a možnost práce z domova oprávněných zaměstnanců.

## 3.11. Náklady

Některá navržená opatření by realizoval IT specialista, který pro firmu již pracuje. Dále by firma investovala do:

- Záložního serveru – 180 000,- bez DPH
- Síťových prvků pro účely VPN – 3 routery Mikrotik (například CCR1036) + 2 switche – 80 000,- bez DPH
- Doménového serveru – 420 000,- bez DPH
- Antivirového programu – 3 roky/ 228 000,- bez DPH
- Školení zaměstnanců – 15 000,- až 20 000,- bez DPH za jedno školení
- Zaměstnání nových pracovníků, odborníka na informační bezpečnost (60 000,- měsíčně před zdaněním, pro společnost by bylo dostačující, aby pracoval pouze na poloviční pracovní úvazek za 30 000,- před zdaněním) a správce sítě (80 000 – 100 000,- měsíčně před zdaněním)

Celková cena za hardware a software bez DPH: 908 000,-

Celková cena za hardware a software s DPH: 1 098 680,-

# ZÁVĚR

V této bakalářské práci jsem se zabývala posouzením a analýzou současného stavu společnosti XYZ s.r.o. Na základě provedených analýz a požadavků společnosti jsem navrhla určitá opatření, která by měla společnosti pomoci lépe chránit její aktiva.

V úvodní teoretické části jsem vymezila základní pojmy týkající se dané problematiky. Pro pochopení tématu práce je nutné porozumět těmto teoretickým pojmům, jedná se o termíny z oblasti informační bezpečnosti a síťového připojení.

V následující analytické části jsem se zaměřila na popis společnosti XYZ s.r.o., jejích prostor a organizační struktury. Následné analýzy a hodnocení byly provedeny po konzultaci s IT specialistou a vedoucími jednotlivých oddělení společnosti. Nejprve jsem identifikovala jednotlivá aktiva firmy, která byla dále náležitě klasifikována. Zaznamenala jsem, kteří zaměstnanci mají k určitým aktivům přístup a uvedla hrozby a možné bezpečnostní incidenty. Sestavila jsem matici zranitelnosti a na základě zjištěných hodnot a dat vytvořila matici úrovní rizik. Podle této matice jsem zjistila, že společnost by se měla primárně zaměřit na ochranu svých dat a účetnictví. Úroveň rizika u těchto aktiv je vysoká nebo kritická. Jejich poškození či ztráta by pro firma byla kritická. U mnoha aktiv je střední úroveň rizika. Pro společnost není urgentní nasazovat opatření pro zvýšení ochrany těchto aktiv, ale určitě by je neměla zanedbat. Na závěr této části uvádím své subjektivní hodnocení současných opatření.

V poslední praktické části se věnuji návrhu vylepšení a změn bezpečnostních opatření. Tyto návrhy mají firmě primárně pomoci chránit její aktiva zabránit jejím poškození. Mezi návrhy patří například zavedení záložního serveru a doménové struktury, častější proškolování zaměstnanců, ochrana citlivých údajů a konfigurace VPN typu SSTP. Vytvořila jsem matici úrovní rizik, kde beru v potaz nově zavedená opatření. Po nasazení opatření by se kritická a vysoká úroveň rizika měla snížit na střední a nižší. Navržená opatření splňují požadavky společnosti. Na závěr práce vyhodnocuji přínosy nově navržených změn a opatření.

# SEZNAM POUŽITÝCH ZDROJŮ


(1) POŽÁR, Josef. *Manažerská informatika*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2010. ISBN 978-80-7380-276-9.

(2) POŽÁR, Josef. *Základy teorie informační bezpečnosti*. Praha: Vydavatelství PA ČR, 2007. ISBN 978-80-7251-250-8.

(3) KOCH, Miloš a Bernard NEUWIRTH. *Datové a funkční modelování*. Vyd. 4., rozš. Brno: Akademické nakladatelství CERM, 2010. ISBN 978-80-214-4125-5.

(4) ONDRÁK, Viktor. *Management informační bezpečnosti: Studijní opora pro předmět Management informační bezpečnosti* [online]. Vysoké učení technické v Brně, Fakulta podnikatelská, 2013 [cit. 2021-04-08]. Dostupné z: https://www.vutbr.cz/www_base/priloha_fs.php?dpid=106780&skupina=dokument_priloha

(5) KAJZAR, Dušan. *Tvorba informačních systémů III: management vývoje a provozu*. Vyd. 1. Opava: Slezská univerzita v Opavě, Filozoficko-přírodovědecká fakulta, Ústav informatiky, 2006. ISBN 80-7248-351-X.

(6) JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník Kybernetické bezpečnosti* [online]. Praha. Policejní akademie ČR v Praze, 2013 [cit. 2021-05-05]. Dostupné z: https://afcea.cz/wp-content/uploads/2015/03/Slovnik_Final_screen_v2_0.pdf

(7) ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice*. Vyd. 1. Brno: Akademické nakladatelství CERM, 2013. ISBN 978-80-7204-872-4.

(8) ISO 9000 family: Quality management. *ISO - International Organization for Standardization* [online]. [cit. 2021-04-12]. Dostupné z: https://www.iso.org/iso-9001-quality-management.html

(9) ISO 14000 family: Environmental management. *ISO - International Organization for Standardization* [online]. Ženeva [cit. 2021-04-12]. Dostupné z: https://www.iso.org/iso-14001-environmental-management.html

(10) ISO/IEC 27001: Information security management. *ISO - International Organization for Standardization* [online]. Ženeva [cit. 2021-04-12]. Dostupné z: https://www.iso.org/isoiec-27001-information-security.html

(11) IATF 16949:2016: About. *International Automotive Task Force* [online]. [cit. 2021-04-16]. Dostupné z: https://www.iatfglobaloversight.org/iatf-169492016/about/

(12) BIGELOW, Stephen J. *Mistrovství v počítačových sítích: správa, konfigurace, diagnostika a řešení problémů*. Vyd. 1. Brno: Computer Press, 2004. ISBN 80-251-0178-9.

(13) JORDÁN, Vilém a Viktor ONDRÁK. *Infrastruktura komunikačních systémů I: univerzální kabelážní systémy*. Druhé, rozšířené vydání. Brno: CERM, Akademické nakladatelství, 2015. ISBN 978-80-214-5115-5.

(14) PUŽMANOVÁ, Rita. *TCP/IP v kostce*. 1. vyd. České Budějovice: Kopp, 2004. ISBN 80-7232-236-2.

(15) JIROVSKÝ, Václav. *Vademecum správce sítě*. 1. vyd. Praha: Grada, 2001. ISBN 80-7169-745-1.

(16) Understanding the Remote Desktop Protocol (RDP). *Microsoft* [online]. 2021 [cit. 2021-05-12]. Dostupné z: https://docs.microsoft.com/en-us/troubleshoot/windows-server/remote/understanding-remote-desktop-protocol

(17) DEGEFA, Rodoya Takele. *VPN Scenarios, Configuration and Analysis*. Helsinki, 2015. Bachelor's Thesis. Helsinki Metropolia University of Applied Sciences. Vedoucí práce Erik Pätynen.

(18) ŠPAČEK, Stanislav. *Možnosti šifrované komunikace v prostředí MS Windows 7*. Brno, 2014. Bakalářská práce. Masarykova Univerzita. Vedoucí práce RNDr. Marku Kumpoštovi, PhD.

(19) Getting started with OpenVPN products. *OpenVPN* [online]. United States, 2021 [cit. 2021-05-12]. Dostupné z: https://openvpn.net/vpn-server-resources/getting-started/

(20) BIJEČEK, Richard a Lubomír MORIC. *Layer 2 Tunneling Protocol (L2TP): Teorie a praktické použití ve Windows a Linuxu*. Ostrava, 2007. VŠB TU Ostrava.

(21) IPsec VPN Overview. *Juniper Networks* [online]. United States: 1133 Innovation Way Sunnyvale, California 94089 USA, 2021 [cit. 2021-05-12]. Dostupné z: https://www.juniper.net/documentation/us/en/software/junos/vpn-ipsec/topics/topic-map/security-ipsec-vpn-overview.html#id-ipsec-vpn-overview

(22) What is SSL VPN?: F5 GLOSSARY. *F5* [online]. [cit. 2021-05-14]. Dostupné z: https://www.f5.com/services/resources/glossary/ssl-vpn

# SEZNAM POUŽITÝCH ZKRATEK A SYMBOLŮ

| | |
|---|---|
| BIOS | Basic Input-Output System |
| DES | Data Encryption Standard |
| ERP | Enterprise Resource Planning |
| GDPR | General Data Protection Regulation |
| IATF | International Automotive Task Force |
| ICT | Information and Communication Technologies |
| IEEE | Institute of Electrical and Electronics Engineers |
| IKE | Internet Key Exchange |
| IP | Internet Protocol |
| IPS | Intrusion Prevention Systems |
| IPSEC | Internet Protocol Security |
| IS | Informační systém |
| ISO | International Organization for Standardization |
| IT | Informační technologie |
| L2TP | Layer 2 Tunneling Protocol |
| LAN | Local Area Network |
| MAC | Media Access Control |
| MAN | Metropolitan Area Network |
| MS Excel | Microsoft Excel |
| NGFW | Next-Generation Firewall |
| OS | Operační systém |
| P2P | Peer-to-peer |

| | |
|---|---|
| PAN | Personal Area Network |
| PDU | Protokolová datová jednotka |
| PPP | Point-to-point Protocol |
| PPTP | Point-to-Point Tunneling Protocol |
| RDP | Remote Desktop Protocol |
| RFB | Remote Framebuffer |
| SSL | Secure Sockets Layer |
| TLS | Transport Layer Security |
| SSTP | Secure Socket Tunneling Protocol |
| TCP | Transmission Control Protocol |
| UDP | User Datagram Protocol |
| VLAN | Virtual Local Area Network |
| VPN | Virtuální privátní síť |
| WAN | Wide Area Network |

# SEZNAM POUŽITÝCH OBRÁZKŮ

# SEZNAM POUŽITÝCH TABULEK

# SEZNAM PŘÍLOH

**Příloha I**

# Směrnice firmy XYZ s.r.o.

# Pravidla bezpečného chování uživatelů

**Základní pravidla a povinnosti chování uživatelů**

Uživatel se musí seznámit s pravidly pro práci s informačními systémy v rámci firmy XYZ.

**Mezi základní povinnosti uživatele výpočetní techniky patří:**

- Výpočetní techniku organizace, musí uživatelé využívat pouze k výkonu svých pracovních povinností.
- Uživatel ke své pracovní činnosti používá informace (data), která získává z počítačové sítě v závislosti na přidělené roli či přidělených přístupových oprávnění, pouze pro zajištění pracovních povinností.
- Uživatel nesmí měnit administrátory nastavené prostředí, včetně pomocných a bezpečnostních programů a služeb systému, zastavovat jejich běh, či je odinstalovat a nesmí se pokoušet vlastními silami řešit bezpečnostní problémy.
- Uživatel smí používat svěřený přístup k informačním systémům, internetu a elektronické poště pouze k pracovní činnosti.

**1. Pravidlo používání pouze legálního a schváleného software**

- Uživatel smí používat jen legálně přidělený a schválený software.
- Uživatel je povinen používat pouze počítačové vybavení, které mu bylo zaměstnavatelem přiděleno. Použití k jiným činnostem, než k plnění svých pracovních povinností je zakázáno.

**2. Pravidlo fyzické ochrany svěřených prostředků výpočetní techniky**

- Uživatel má povinnost chránit svěřené prostředky výpočetní techniky před ztrátou, poškozením, zničením či odcizením. Zejména je povinen uzamykat místnosti při nepřítomnosti zaměstnanců v místnosti a přiměřeným způsobem chránit přidělené mobilní prostředky výpočetní techniky.
- Uživatel si musí být vědom, že výpočetní techniku je možné poškodit mechanicky, zvýšenou vlhkostí a teplotou. Při jejím umístění dbá, aby se neumístila v blízkosti zdrojů tepla a vlhkosti.

- Uživatel není oprávněn přemisťovat svěřené počítačové vybavení (kromě přenosných zařízení) bez souhlasu vedení firmy.
- Uživatel není oprávněn měnit, konfigurovat nebo opravovat svěřené počítačové vybavení.

**3. Pravidlo bezpečného užívání prostředků výpočetní techniky**

- Uživatel musí dodržovat všechny bezpečnostní předpisy, opatření a pokyny plynoucí z používání svěřených prostředků výpočetní techniky, tak aby nemohlo dojít k porušení bezpečnosti informací. Uživatel má právo na poskytnutí nezbytných informací formou školení pro použití výpočetní techniky pro výkon své práce a povinnost se jich účastnit.

**5. Pravidlo bezpečného užití a ochrany autentizačních prostředků**

- Uživatel má povinnost chránit své autentizační prostředky (prostředky pro ověření uživatele) před jejich prozrazením (kompromitací) jakýmkoliv jiným.
- Pokud má uživatel podezření na možné zveřejnění, odcizení nebo prolomení svého hesla, je povinen to nahlásit vedení nebo administrátorovi výpočetní techniky k zajištění okamžité změny hesla.

**6. Pravidlo ochrany dat**

- Uživatel musí chránit veškerá data, a zvláště pak data s osobními údaji, před neoprávněným přístupem jiných osob.
- Uživatel musí používat základní ochranné metody, tj. např. „uzamykání“ výpočetní techniky, nebo její vypínání (pokud není z technologických důvodů nařízeno jeho výjimečné ponechání v zapnutém stavu), pokud nemá výpočetní techniku pod svoji přímou kontrolou (např. při opuštění kanceláře).

**7. Pravidlo bezpečného použití elektronické pošty**

- Uživatel je povinen věnovat příchozí poště zvýšenou pozornost a obezřetnost. Zejména se jedná o podezřelé zprávy, zvláště od neznámých odesílatelů, odkazů, od neznámých nebo podezřelých adres v prostoru internetu, nevyžádaných příloh apod. V případě, že uživatel přesto omylem otevře tyto přílohy nebo odkazy a výpočetní technika bude vykazovat nestandartní chování, je toto uživatel povinen nahlásit vedení nebo administrátorovi výpočetní techniky. Nevyžádané emailové zprávy označí jako „Nevyžádanou poštu“.

8. **Pravidlo bezpečné práce v síti Internet**

- Uživatel je povinen zachovávat etický přístup k využívání internetu, je povinen jej využívat pouze k pracovním činnostem.
- Uživatel se musí vyhýbat nebezpečným stránkám, podezřelým odkazům apod.
- Uživatel vystupuje na internetu (např. v oborových diskusích) tak, aby svým chováním nepoškozoval dobré jméno firmy XYZ zejména v případech, kdy uvádí pracovní adresu.

9. **Pravidlo bezpečného vzdáleného přístupu a užití mobilních zařízení**

- Pro bezpečný vzdálený přístup do výpočetní techniky je správcem výpočetní techniky technologicky zajištěna bezpečná cesta se šifrovanou komunikací. Pro využití této cesty cestou autorizovaného přístupu zajištěného heslem platí stejná pravidla pro ochranu hesel a zvýšené fyzické ochrany mobilního prostředku.

10. **Pravidlo hlášení závad a podezřelého chování výpočetní techniky**

- Uživatel je povinen provádět veškerá hlášení závad a podezřelého chování výpočetní techniky zaměstnanců vedení nebo administrátorovi výpočetní techniky.

**Provozní a bezpečnostní správy výpočetní techniky**
V případě jakýchkoliv odborných požadavků spojených s výpočetní technikou uživatelé kontaktují nadřízené pracovníky v součinnosti s administrátorem výpočetní techniky.

**Přístup k informačním systémům**
**Připojení k počítačové síti**
Zaměstnanec firmy XYZ je připojen k počítačové síti na základě vzniku pracovněprávního vztahu, v roli „uživatel“ se základním přístupovými právy. Uživateli je vytvořen „uživatelský účet“, kterému je přiděleno „uživatelské jméno“ a je vydáno heslo, které si zaměstnanec může změnit.

**Přidělení přístupových práv k výpočetní technice a aplikacím**
V rámci řízení přístupu k informačním systémům firmy XYZ jsou uplatňována následující pravidla:

- Přístup je přidělen na základě pracovní pozice, přístupová práva musí být v souladu s pracovními povinnostmi.
- Při změně pracovní pozice musí být přístupová oprávnění opětovně nastavena dle nové pracovní pozice na základě požadavků vedení firmy.
- Přístupová oprávnění jsou přidělována na základě žádosti vedoucího pracovníka pro konkrétního zaměstnance (uživatele). Veškerá přístupová oprávnění nad rámec přístupu na základě pracovní pozice (místa), vždy schvaluje vedení firmy XYZ.
- Přístupová práva nastavuje správce výpočetní techniky na základě schválené žádosti.
- Každému uživateli je přidělen pouze jeden uživatelský účet.

**Základní přístupová práva**
Základní přístupová oprávnění k informačním systémům zahrnují přístup a právo používání:

- elektronické pošty (email),
- přístupu k internetu,
- intranetu
- sdílené složky,
- aplikace vyplývající z pracovní funkce (místa),
- docházkového a personálního systému.

Základní přístupová oprávnění jsou nastavena pro každý uživatelský účet při jeho založení, na základě pokynu vedení o zřízení uživatelského účtu pro nového zaměstnance.

Ostatní přístupová práva
**Individuální** – Individuálními přístupovými právy se rozumí ta práva, která jsou uživateli přidělena na základě oprávněné potřeby pro výkon pověřených činností (tzn. případ od případu). O přidělení individuálních přístupových práv žádá přímý nadřízený zaměstnance.

**Přihlašovací údaje uživatele**
Uživatelé, kterým byl přidělen účet a přihlašovací údaje:

- musí udržovat tyto údaje v tajnosti,
- nesmí přihlašovací údaje ukládat v počítači v nezabezpečené podobě jako textový soubor a nesmí být uložena na místě snadno dostupném jiným osobám
-

**Ukončení pracovního poměru**
V případě ukončení pracovního poměru přestává být pracovník uživatelem informačního systému firmy XYZ, tzn., již nemá oprávnění k tomuto systému, jakkoliv přistupovat.
V souvislosti s ukončením pracovního poměru:

- uživatel je povinen předat veškeré informace o rozpracované agendě, tzn. například přeposláním příslušných emailů, překopírování informací uložených na lokálních discích počítače včetně přenosných médií přímému nadřízenému,
- po dni ukončení pracovního poměru je uživateli znepřístupněn a uzavřen jeho uživatelský učet a nelze jej dále v informačním systému využívat,
- uživatel je povinen vrátit všechny přidělené prostředky výpočetní techniky.

**Využívání informačního systému**
**Mobilní výpočetní zařízení a práce na dálku**
V případě přístupu uživatele k informačnímu systému organizace z prostor mimo organizaci mohou být jeho přístupová práva omezena a mohou se lišit od standardních uživatelských práv při připojení z pracoviště, tj. přímo do počítačové sítě na pracovišti.

V případě práce „na dálku“, tzn. je umožněn dálkový přístup k informačnímu systému a informacím organizace, po schválení vedením firmy XYZ.

**Schválený software a konfigurace počítače**
Uživatel smí používat pouze schválený a evidovaný software. Je přísně zakázáno individuální nahrávání, instalace, modifikace nebo spouštění neschváleného software do výpočetní techniky. Veškeré případné oprávněné požadavky uživatele je nutno, po odsouhlasení přímého nadřízeného, adresovat k administrátorovi výpočetní techniky.
Uživatel je povinen používat pouze již nakonfigurované počítačové vybavení, které mu bylo přiděleno. Uživatel nesmí provádět žádné změny na zařízení, konfigurovat je nebo je fyzicky opravovat.

**Interní počítačová síť**
Uživatelé s přístupem do počítačové vnitřní sítě firmy XYZ odpovídají za svoje činnosti prováděné v této síti. Z důvodu zajištění bezpečnosti informací uživatelé nesmí zejména:

- zneužívat síťové prostředky pro osobní účely,
- stahovat a šířit data chráněná autorským právem,
- šířit soubory a e-maily u nichž je pravděpodobný výskyt škodlivého softwaru nebo u nich není možné ověřit jejich původ,
- připojovat do sítě neschválená zařízení,
- měnit síťové konfigurace koncových a síťových zařízení,
- bez pracovního důvodu exportovat data,
- využívat nástroje sloužící k maskování identity,
- provádět jakoukoliv formu skenování portů, monitorování počítačové sítě, které může vést k zachycení dat, která nejsou určena pro počítač příslušného zaměstnance,
- obcházet autentizaci uživatele nebo obcházet zabezpečení jakéhokoliv počítače, počítačové sítě nebo uživatelského účtu,
- provádět jakékoliv aktivity vedoucí k omezování nebo odepírání služeb jiným uživatelům,
- užívat jakékoliv programy, skripty nebo příkazy nebo zasílat zprávy v jakékoliv formě s úmyslem omezit nebo znemožnit poskytování služeb nebo terminálových relací, lokálně nebo přes počítačovou síť.

**Přístup na internet**
Uživatelé, kteří mají přístup k internetu prostřednictvím internetové přípojky jsou povinni internet využívat pouze k pracovní činnosti po nezbytně dlouhou dobu.

Z důvodů zajištění dostupnosti výpočetní techniky a zajištění dostatečné internetové konektivity je zakázáno používání následujících kategorií služeb internetu:

- internetové video kanály (mimo přenosů sloužící k pracovním činnostem),
- hudební kanály,
- online televizní přenos (mimo přenosů sloužící k pracovním činnostem),
- internetová rádia,
- sociální sítě,
- online hry,
- sdílení fotografií (mimo přenosů sloužící k pracovním činnostem),

- pornografie a erotické stránky,
- veřejná úložiště (mimo příjmu pracovních dat),
- maskování identity uživatele,
- P2P sítě (např. BitTorrentové služby).

**Elektronická pošta / komunikace**

Uživatel, který má zřízen „pracovní" e-mail, je povinen tuto elektronickou poštu používat pouze k pracovní činnosti. „Pracovní" e-mail není určen pro soukromé účely. Pro zajištění správné funkcionality elektronické pošty, je uživatel povinen kontinuálně udržovat volnou kapacitu emailové schránky, tzn. emaily odmazávat, popřípadě je přesouvat do osobního archivu.

Při přijímání e-mailu uživatel musí být mimořádně opatrný při otevírání elektronické pošty, protože mohou obsahovat viry nebo jiné škodlivé kódy. Pozornost je třeba věnovat zejména emailům:

- jejichž příjemce nebo odesílatel vykazují nestandardní znaky (nesprávné použití jazyka, neznámí odesílatelé, nesprávné adresy odesílatele),
- text zprávy obsahuje gramatické a pravopisné chyby,
- jejichž přílohy obsahují spustitelné soubory, popřípadě nestandartní názvy souborů
  v příloze
  - požadující nějaký druh finanční platby nebo zadání bankovních nebo osobních údajů,
  - odkazují na webové stránky.

Pokud uživatel přijal v emailové poště takové informace, které mají dlouhodobou platnost, jsou důležité pro rozhodování firmy XYZ nebo mají jinou hodnotu pro organizaci (např. souvisí s agendou zajišťovanou uživatelem), je povinen tuto informaci uchovat (např. formou archivace nebo uložení na sdílené disky).

V případě, že uživatel do své emailové schránky přijal poštu soukromé povahy (soukromý email), musí tyto informace vymazat ze své emailové schránky.

**Odesílání emailu**

Uživatel se při odesílání emailu chová eticky a dodržuje pravidla pro rozesílání elektronické pošty, zejména:

- nesmí neautorizovaně (Skrytá kopie) používat nebo padělat zprávy elektronické pošty,
- neoprávněně zasílat informace jiným subjektům,
- nesmí zatěžovat počítačovou síť zasíláním spamu, obchodních sdělením, hromadnými emaily atd.,
- musí v případě odesílání informací s vyšším stupněm důvěrnosti ověřit identitu příjemce (např. ověřením kvalifikovaného certifikátu),

- musí za účelem výměny dat, která nelze zaslat pomocí pracovního e-mailu (zpravidla přílohy o velikosti 10 MB a více), využívat pouze interní úložiště pro sdílení/výměnu dat.

Uživatel při odesílání emailu dodržuje následující etická pravidla elektronické pošty:

- uživatel nešíří „humorné“ či „poplašné“ zprávy,
- uživatel dodržuje pravidla slušnosti i při elektronické komunikaci
- uživatel dodržuje pravidla ochrany autorských práv, tzn., nerozesílá dílo s autorskými právy bez souhlasu autora,
- emailová zpráva má vždy vyplněn předmět zprávy, který musí být relevantní k obsahu zprávy,
- uživatel nerozesílá nepřiměřeně velká data.

**Přenosné počítače**

Uživatel, kterému byl svěřen přenosný počítač je povinen vynaložit úsilí k tomu, aby mu toto zařízení nebylo odcizeno nebo poškozeno. Uživatel při používání přenosného počítače mimo prostory organizace je povinen v rámci možností zabránit, aby informace byly odpozorovány z monitoru neoprávněnou osobou. Přístup k přenosnému počítači (operačnímu systému) musí být zabezpečen stanoveným způsobem, tj. minimálně zadáním přihlašovacích údajů (uživatelské jméno a heslo).
Při ztrátě nebo krádeži takového zařízení vzniká bezpečnostní incident. Uživatel je povinen neprodleně tuto skutečnost oznámit přímému nadřízenému.

**Antivirová ochrana**

Antivirová ochrana, resp. ochrana počítačové sítě a informačních systémů proti škodlivým kódům je jedním z bezpečnostních opatření. Antivirová ochrana počítačové sítě a výpočetní techniky je zajišťována centrálně v rámci organizace, odpovídá za ni administrátor výpočetní techniky. Uživatel není oprávněn vypnout nebo měnit nastavení antivirové ochrany. Uživatel nesmí připojovat k počítačové síti zařízení, které nemá nainstalovaný antivirový software. Uživatel po povinen oznámit jakékoliv podezření na výskyt viru nebo jiného škodlivého software vedení nebo administrátorovi výpočetní techniky. Uživatel má zakázáno pracovat na počítači, dokud není virus nebo škodlivý software odstraněn.

**Zálohování dat**

Zálohování dat na sdílených discích/serverech a řídících prvcích sítě je v odpovědnosti administrátora výpočetní techniky. Zálohování na pracovních stanicích a noteboocích je v odpovědnosti uživatele.

**Přenášení, výměna informací (média)**

Uživatelé využívají jen taková přenosná zařízení (flash disky, externí disky apod.) a externí média (CD, DVD apod.), která byla zaměstnanci oficiálně zaregistrována do evidence a připravena k použití v síti firmy XYZ. Jakékoliv jiná zařízení bez registrace musí být do sítě a zařízení připojována a ihned překontrolována antivirovým programem. Bez této antivirové kontroly nesmí být přenosné zařízení nebo externí médium používáno prostředky výpočetními prostředky.

**Provozní problémy**
V případě, že uživatel zjistí jakýkoliv problém v rámci provozu počítačového systému nebo přiděleného počítače (příp. jiného zařízení výpočetní techniky), oznámí tuto závadu nadřízenému nebo administrátorovi výpočetní techniky.

**Povinnosti při bezpečnostní události nebo incidentu**
Uživatel má odpovědnost za bezpečnost informací v rámci své činnosti s informačním systémem. Z tohoto důvodu je povinen oznámit bezpečnostní událost nebo bezpečnostní incident nadřízenému nebo administrátorovi výpočetní techniky.
Za bezpečnostní událost nebo incident se považují situace, kdy může dojít, a/nebo již došlo k narušení bezpečnosti informací. Jedná se zejména o následující situace nebo stavy systému:

- neoprávněný přístup do systému nebo k informacím,
- zneužití oprávnění přístupu do systému,
- krádež, zničení, poškození nebo ztráta informací,
- ztráta, krádež, neoprávněné použití, poškození nebo zničení například souborů, databází, zařízení IT,
- incident způsobený škodlivým programem nebo kódem (zavirování systému).

V případě vzniku bezpečnostní situace nebo incidentu uživatel oznámí tuto skutečnost vedení nebo administrátorovi výpočetní techniky. V případě zavirování nepokračuje dále v práci na tomto počítači.

**Oprávnění organizace**
Zaměstnavatel je oprávněn kontrolovat, zda zaměstnanci plně využívají pracovní dobu, a zda jsou prostředky výpočetní techniky a informační systémy využívány pouze k pracovním účelům.

Uživatelé jsou si vědomi, že provoz všech informačních systémů firmy XYZ může být monitorován. Takto pořízené informace mohou být použity k řešení kybernetických bezpečnostních událostí, a to v souladu s platnou legislativou.

Nedodržování pravidel provozu informačních systémů a bezpečnosti informací, stanovených touto směrnicí a dalšími vnitřními předpisy, může být kvalifikováno jako porušení pracovní kázně a bude řešeno v souladu s vnitřními předpisy organizace a příslušnými zákony ČR.

**Příloha II**

# Konfigurace VPN typu SSTP

### Konfigurace SSTP VPN serveru a SSTP klienta

Nastavení je rozděleno do dvou částí, konfigurace serveru a konfigurace klienta.

## 1. Konfigurace SSTP serveru v routeru Mikrotik

Nastavení SSTP serveru proběhlo ve třech krocích, tvorba TLS certifikace, spuštění a konfigurace SSTP serveru a vytvoření uživatelů pro samotný přístup přes VPN.

### Vytvoření TLS certifikátu

Konfigurace SSTP serveru vyžaduje vytvoření TLS certifikace z důvodu zabezpečené komunikace. Operační systém Mikrotiku router OS umožňuje vytvoření, uložení a správu certifikátu v úložišti. SSTP server vyžaduje dva typy certifikátů:

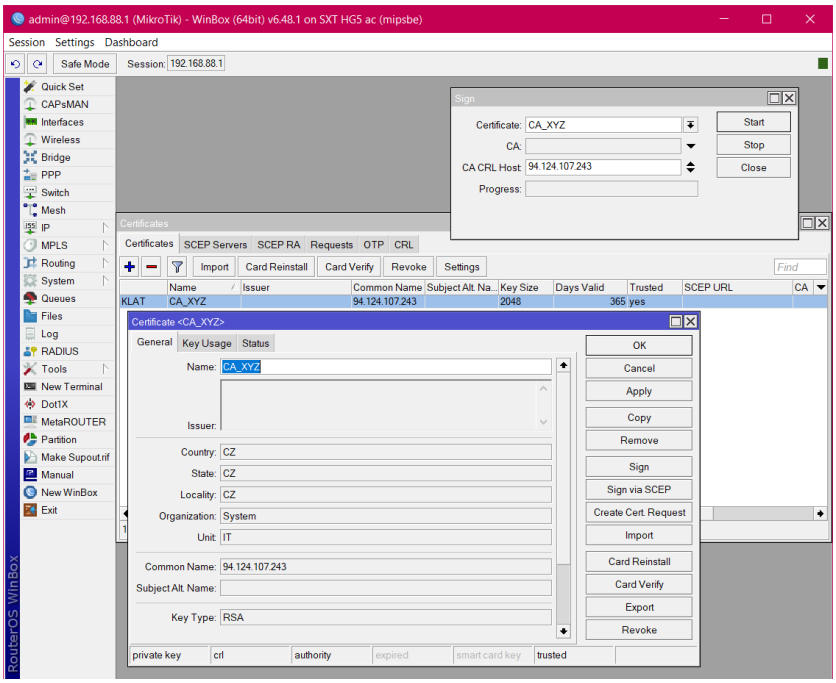
a) CA (certifikační autorita) certifikát
b) serverový certifikát.

a) Vytvoření CA certifikační autority

Mikrotik router OS umožňuje vytvořit vlastní certifikační autoritu pro podepsání a vygenerování svých serverových certifikátů. Tyto certifikáty jsou následně instalovány v SSTP klientských zařízeních, které se nimi ověřují vůči serveru. Na záložce certifikáty v menu systém jsem přidala nový certifikát (znaménkem plus). Název certifikační autority jsem zvolila CA_XYZ a do pole Common Name vložila adresu hlavního routeru 94.124.107.243. Na záložce Key Usage musí být zatrženo ctr sign a key cert sign. Po stisku tlačítka sign jsem vložila veřejnou adresu 94.124.107.243. do políčka CA CRL Host. Tlačítkem Start spustíme certifikační autoritu.

b) Vytvoření serverového certifikátu

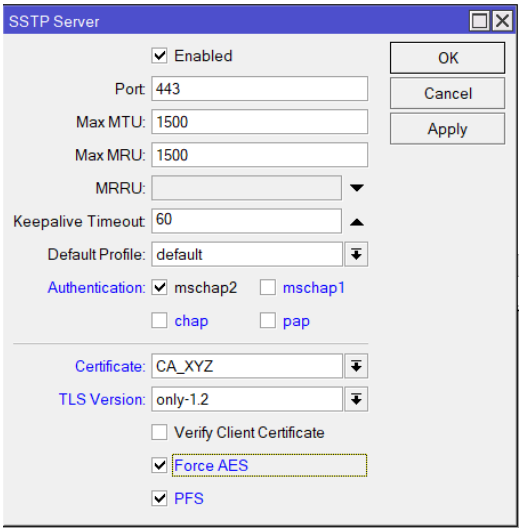
Po vytvoření certifikační autority jsem vytvořila serverový certifikát, který je touto certifikační autoritou podepsán. Tento certifikát bude využíván SSTP serverem.




**Obrázek 12: Vytvoření certifikace**
(Zdroj: vlastní zpracování)

## Spuštění a konfigurace SSTP serveru

V menu PPP na záložce interface jsem zvolila SSTP server. Políčko Enabled musí být zaškrtnuto, dále jsem vybrala port pro zabezpečenou komunikaci 443. V sekci Authentification zůstane zaškrtnuto pouze mschap2. V políčku Certification je vybrán náš ceritifikát CA_XYZ a v poli TLS version only-1.2. Musí být zašrtnuto Force AES a PFS.



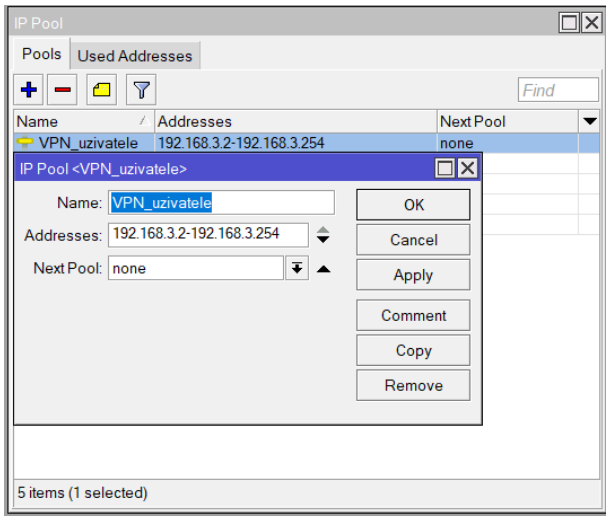

**Obrázek 13: Konfigurace SSTP serveru**
(Zdroj: vlastní zpracování)

SSTP server nyní běží na routeru Mikrotik a pro úspěšné připojení je potřeba vytvořit pouze uživatelská jména a heslo pro VPN připojení.

### Vytvoření přístupových jmen a hesel v routeru Mikrotik pro přístup přes VPN

Mikrotik SSTP používá uživatelská jména a hesla pro ověření připojení, z tohoto důvodu je nutné vytvořit seznam uživatelů, kteří se budou připojovat přes VPN. Protože k Mikrotiku jsou připojení uživatelé jak z vnitřní sítě, tak uživatelé z vnější sítě, je lepší pro uživatele z vnější sítě vytvořit samostatný adresní rozsah.

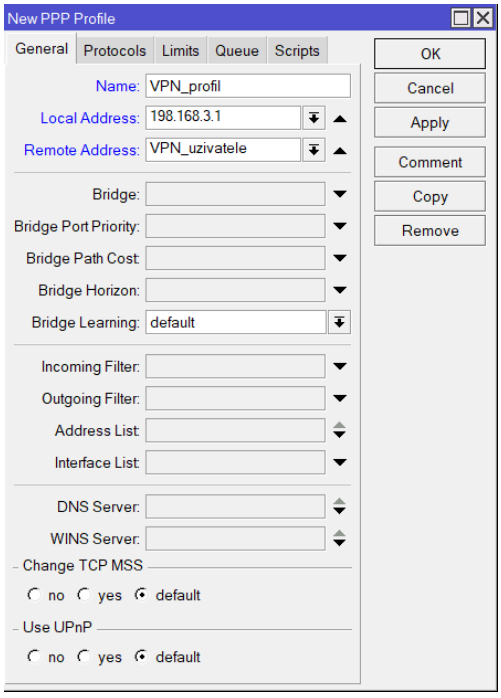
V menu IP jsem vybrala sekci Pool a kliknutím na znaménko plus vytvořila nový rozsah IP adres pro uživatele připojující se přes VPN 192.168.3.2 - 192.168.3.254.




**Obrázek 14: Konfigurace rozsahu adres pro uživatele**
(Zdroj: vlastní zpracování)

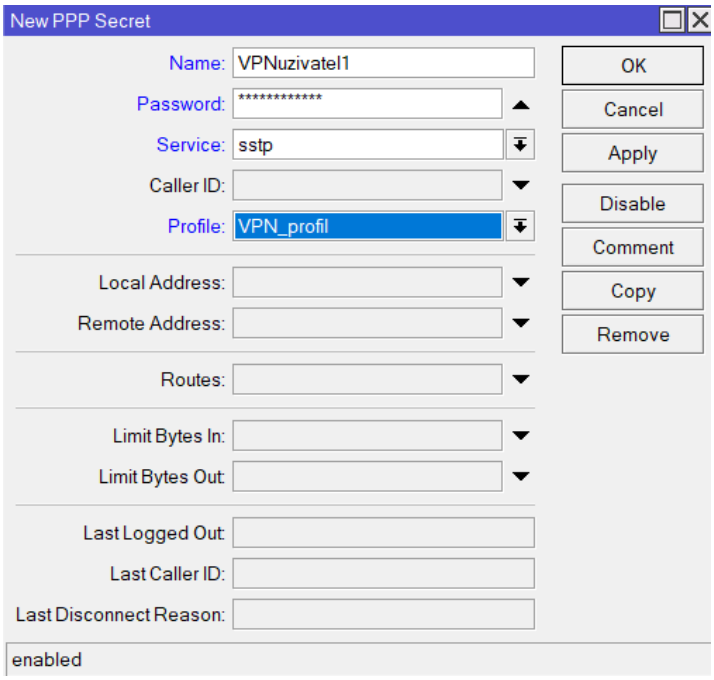
Po vytvoření adresního rozsahu pro VPN uživatele jsem vytvořila profil uživatelů VPN.

V PPP byla zvolena záložka Profil a založila jsem nový přes znaménko plus.




**Obrázek 15: Konfigurace profilu**
(Zdroj: vlastní zpracování)

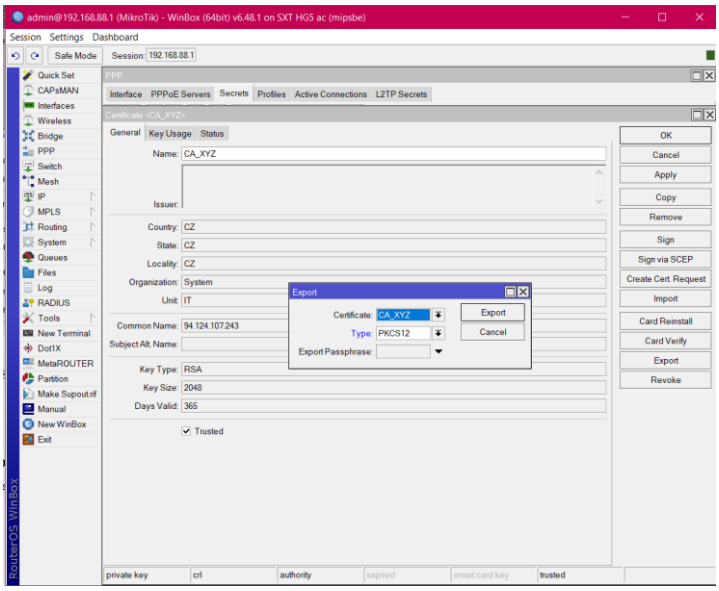
Po vytvoření profilu budou vytvoření uživatele SSTP serveru. V menu PPP v záložce Secrets znaménkem plus přidáme uživatelské jméno. Stejným způsobem se vytvoří všichni uživatelé, kteří se připojují přes VPN.



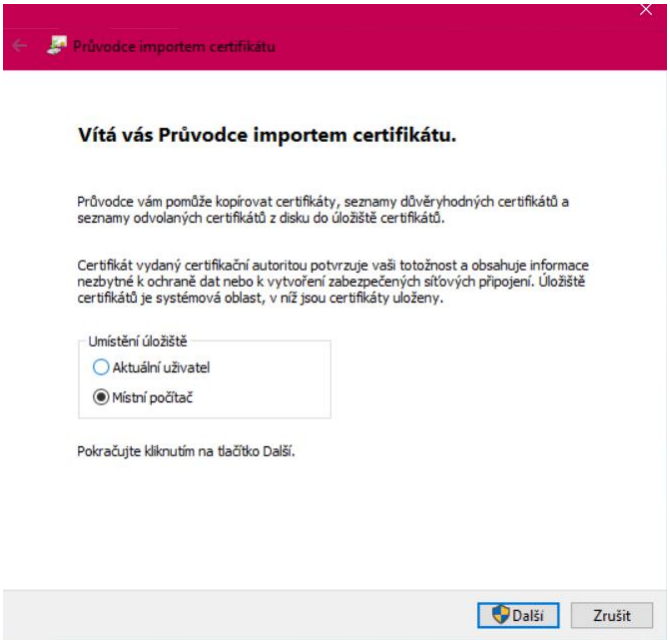

**Obrázek 16: Konfigurace nového uživatele VPN**
(Zdroj: vlastní zpracování)

## 2. konfigurace SSTP klienta v klientském počítači s Windows 10

Pro klienty se na hlavním routeru vyexportuje certifikát včetně CA. V menu System je vybrán Certificates a klikneme na tlačítko export. Dále v menu Files najdeme vyexportovaný certifikát cert_export_CA_XYZ. Tento certifikát naimportuji pomocí certifikačního průvodce, kde zvolím volbu Místní počítač.

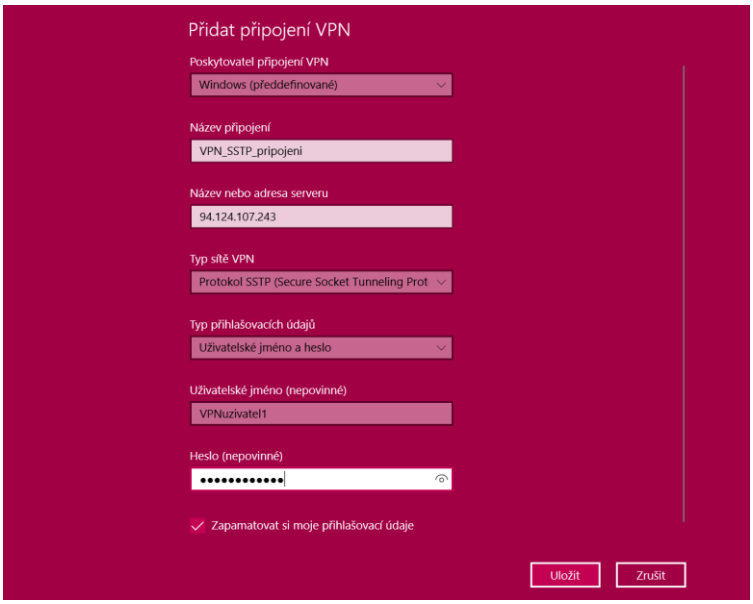



**Obrázek 17: Export certifikační autority**
(Zdroj: vlastní zpracování)




**Obrázek 18: Import certifikace**
(Zdroj: vlastní zpracování)

V počítači v nastavení Síť a internet zvolím položku přidat VPN, kam vložíme veřejnou IP adresu hlavního firemního routeru a uživatelské jméno a heslo příslušného uživatele VPN.




**Obrázek 19: Přidání připojení VPN**
(Zdroj: vlastní zpracování)

Konfigurace byla otestována připojením testovacího notebooku přes datové připojení mobilního operátora k firemní síti, která je připojená přes wifi operátora. Také byla vytištěna testovací stránka na tiskárně ve firemní síti.

**Příloha III**

## Uživatelské skupiny

Majitel = majitel firmy

Zastupce = zástupce majitele firmy

Vedouci = vedoucí sedmi jednotlivých odděleních

IT = externí IT specialista, který bude administrátorem

Zamestnanci = zaměstnanci na výrobních halách u strojů

Ucetni = externí účetní

SAP = externí specialista na SAP

Administrátor přiděluje jednotlivým skupinám následující oprávnění:

X = none (žádný přístup)

R = read (pouze pro čtení)

RW = read write (čtení i zápis)

**Tabulka 17: Přístupová oprávnění skupin ke sdíleným datům**

(Zdroj: Vlastní zpracování)

| | Majitel | Zastupce | Vedouci | IT | Zamestnanci | Ucetni | SAP |
|---|---|---|---|---|---|---|---|
| Data ohledně odběratelů | RW | RW | R | X | X | RW | X |
| Data o zaměstnancích | X | RW | X | X | X | RW | X |
| Data o dodavatelích | RW | RW | R | X | X | RW | X |
| Zálohy dat | R | R | X | RW | X | X | X |
| Účetnictví | RW | RW | X | RW | X | RW | X |
| Firemní politika a metodiky | RW | RW | R | X | R | X | X |
| Záznamy o výrobcích a produktech | RW | RW | RW | X | R | R | R |
| Výrobní dokumentace | RW | RW | R | X | R | X | X |