Návrh IT infrastruktury a informačního systému podniku

Jan Šrubař

Bakalářská práce
2019

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2018/2019

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Jan Šrubař**
Osobní číslo:	**A16634**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**prezenční**
Téma práce:	**Návrh IT infrastruktury a informačního systému podniku**
Téma anglicky:	**A Proposed Design of an IT Infrastructure and Information System for a Company**

Zásady pro vypracování:

1. **Vysvětlete pojem IT infrastruktura a informační systém.**
2. **Popište bezpečnost informačních systémů (zaměřte se na bezpečnou komunikaci zabezpečení dat).**
3. **Navrhněte teorii implementace informačních systémů.**
4. **Analyzujte požadavky podniku.**
5. **Analyzujte rizika.**
6. **Navrhněte vlastní řešení.**
7. **Výsledky konzultujte s vedením podniku.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **BASL, Josef. Podnikové informační systémy: podnik v informační společnosti / Josef Basl, Roman Blažíček. 2012. ISBN 9788024743073.**
2. **GÁLA, Libor, Jan POUR a Zuzana ŠEDIVÁ. Podniková informatika: počítačové aplikace v podnikové a mezipodnikové praxi. 3., aktualizované vydání. Praha: Grada Publishing, 2015, 240 s. Management v informační společnosti. ISBN 978-80-247-5457-4.**
3. **HANÁČEK, Petr. Bezpečnost informačních systémů: metodická příručka zabezpečování produktů a systémů budovaných na bázi informačních technologií / Petr Hanáček, Jan Staudek. 2000. ISBN 8023854003.**
4. **SEVERÝN, Prokop. Šifrovaná VPN (multipoint). Šifrovaná VPN (multipoint) / Prokop Severýn ; vedoucí práce Dan Lukeš ; oponent práce Jiří Calda [online]. 2008 [cit. 2018-10-11].**
5. **TOMÁNEK, Tomáš. Aplikovaná kryptologie v internetové komunikaci. Aplikovaná kryptologie v internetové komunikaci / Tomáš Tománek ; vedoucí práce Martin Souček ; oponent práce Jiří Ivánek [online]. 2008 [cit. 2018-10-11].**

Vedoucí bakalářské práce: **Ing. Lukáš Králík**
Ústav počítačových a komunikačních systémů

Datum zadání bakalářské práce: **20. prosince 2018**

Termín odevzdání bakalářské práce: **15. května 2019**

Ve Zlíně dne 20. prosince 2018

doc. Mgr. Milan Adámek, Ph.D.
děkan

Ing. Jan Valouch, Ph.D.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 27.5.2019 Jan Šrubař, v.r.

ABSTRAKT

Bakalářská práce nesoucí název Návrh IT infrastruktury a informačního systému podniku, se zabývá reálným návrhem u jedné nejmenované firmy. Ta podniká v oblasti stavebnictví. S touto oblastí je spjato mnoho dílčích činností, které se v dnešní době jen těžce provádí bez dobře sestavené IT infrastruktury a vhodně zvolených informačních systémů. Teoretická část poodhaluje zmíněné pojmy. Nechybí ani důraz na zabezpečení jednotlivých systémů a také zejména informací v nich uložených. Popisuje se zde i teorie, jak by se informační systémy daly do různých podniků implementovat v závislosti na IT infrastrukturách. Praktická část popisuje samotný podnik. V práci jsou analyzovány požadavky podniku. Následně jsou analyzovány rizika spjaté s informačními systémy. Z toho vychází navržení vlastního řešení problematiky podniku. Schválený projekt je i dále realizován a patřičně popsán až do provozu schopného stavu.

Klíčová slova:

IT infrastruktura, Informační systém, Analýza rizik, Zabezpečení dat, Počítačová síť, ERP

ABSTRACT

The bachelor thesis entitled The Design of IT Infrastructure and Company Information System of a company deals with a real proposal of one unnamed company. The company deals with businesses in the construction industry. There are many sub-activities associated with this industry, which are difficult to implement today without a well-designed IT infrastructure and appropriately chosen information systems. The theoretical section reveals the mentioned terms. There is also an emphasis on the security of individual systems and the information stored in them. The theoretical section also describes the theory of how different IT infrastructures and information systems could be deployed in a business environment. The practical part then describes the company itself. The thesis analyzes the requirements of the company. Subsequently, the risks associated with the information systems are analyzed. From these results come the design of the company's own solution to the problem. The approved project is further implemented and appropriately described up to the operable state.

Keywords:

IT Infrastructure, Information System, Risk analysis, Data security, Computer network, ERP

Poděkování:

Rád bych poděkoval své rodině za podporu při studiu. Zvláštní poděkování patří zejména mému vedoucímu Ing. Lukášovi Králíkovi, za skvělé vedení, cenné rady a báječnou spolupráci. Mimo jiné za trpělivost a poskytnuté konzultace. Poděkování patří také ostatním akademickým pracovníkům, doprovázejících mne po celou dobu studia. Tímto bych chtěl poděkovat i nejmenovanému podniku, který mi umožnil tuto práci prakticky realizovat.

OBSAH

ÚVOD

Hlavním stavebním kamenem této práce, je návrh a následná realizace IT infrastruktury anonymizovaného podniku. K tomu bude potřeba, se s tímto pojmem nejdříve seznámit a zjistit, co infrastruktura vše zahrnuje. Práce se dále rozvíjí o informační systémy. Je zde opět vysvětlení tohoto pojmu i pojmů s tím spjatých. Je zde i teoretický návrh, jak by mohly být informační systémy do podniku zaváděny. Co je jejich stěžením, a co naopak přínosem.

V práci je dále rozebírána problematika zabezpečení. To se týká jednotlivých prvků infrastruktury, ale i bezpečným používáním informačních systému. Mimo jiné, také bezpečná komunikace elektronickou poštou, nebo bezpečný přístup a manipulace s daty. Co nejde opomenout, je bezpečné provozování bezdrátových sítí. V teoretické části je dále rozebrána problematika související s analýzou rizik. Teoreticky je zde popsána metoda stromu poruch. Analýza nazývaná FTA.

Největší prostor byl věnován praktické části. Ta hned v úvodu popisuje samotnou strukturu řešeného podniku. Ten je následně analyzován po stránce jeho potřeb a požadavků na IT infrastrukturu. Poté přišel prostor pro praktické provedení FTA analýzy, ta poodhaluje vznik hrozby výpadku PC sítě. Následovalo navržení vhodné infrastruktury, která by uspokojila dosavadní potřeby podniku. Samotný návrh, který vedení podniku schválilo, mohl vstoupit do části realizace. Zde je krok po kroku popsán postup sestavení systému, vzájemného propojení a následné základní nastavení jednotlivých komponentů. Poté bylo možno zřízení VPN. To přináší představu o současném a o budoucím nastavení. Závěrem této práce je výsledek snažení, s možnou další představou spolupráce s podnikem, a jeho vizí.

Všechny nastavované údaje jsou smyšlené a slouží pro názornost a vysvětlení, nemají bližší spojitost s nastavením komponentů v samotném podniku.

I. TEORETICKÁ ČÁST

1 IT INFRASTUKTURA

Úvodní kapitola se zabývá vysvětlením pojmu infrastruktury spojovanou s Informačními technologiemi (IT). S těmi se dá nejčastěji setkat v podnikových oblastech, o kterých bude řeč. Dále zde budou popsány a vysvětleny další pojmy související s touto problematikou.

1.1 Pojem IT infrastruktura

IT Infrastruktura je obecně souhrn všech informačních technologií vyskytujících se v tomto prostředí. Patří zde jak samotný hardware, tak i software. Mimo jiné i síťové zdroje či služby. Nelze opomenout ani koncová zařízení uživatelů. V mnoha případech se do IT infrastruktury řadí i samotní správci sítí a samotní uživatelé. IT infrastruktura je pro každý podnik či domácnost rozdílnou záležitostí. Proto je vždy dobré znát potřeby a účel IT infrastruktury již v samotném stádiu návrhu. V podnikovém prostředí se rozdíly jeví zejména na velikosti a rozlehlosti podniku. Také obor podnikání a činnost s tím spojená, je důležitá při návrhu této infrastruktury. Výsledná, dobře sestavená IT infrastruktura, by měla zajistit interní komunikaci mezi zaměstnanci a vedením podniku. Sloužit by měla i k externí komunikaci se zákazníky, či dodavateli. [1],[2],[3],[4]

1.2 Podniková IT infrastruktury

Na pojem IT infrastruktura se dá dívat, jako na souhrn technických prvků neboli informačních systémů, které zabezpečují přenášení informací. V podnikové oblasti jsou tyto informace cennými aktivy, které zefektivňují chod celého podnikání. Infrastruktura informačního systému pro podnik stojí na jednom hlavním pilíři. Tím jsou samotné informační technologie, na kterých běží jednotlivé aplikace. Jejich hlavním úkolem je ukládat data, zpřístupňovat je vybraným lidem a umožňovat jejich další správu. [2]

IT infrastruktura je spojena se dvěma základními aspekty. Jednou z nich jsou zmiňované informační technologie, druhými jsou lidé, které tyto technologie umí spravovat. Tzv. IT management. Tyto dvě odvětví tvoří celek a jedna bez druhé by nemohla existovat. [3],[3]

Zavedení IT infrastruktury v podniku dále s sebou nese pravidelné proškolování zaměstnanců a učení je s technologiemi. V manažerské oblasti pak učení těchto vedoucích pracovníků, jak správně nad zaměstnanci dohlížet a zvyšovat jim produktivitu. Tím vytvářet podniku za pomoci zmiňovaných technologií a technik zisk. [2]

1.2.1 Služby IT infrastruktury

Samotná existence IT infrastruktury v oblasti podnikání nabízí mnoho služeb. Jednou z nich je například společná komunikace. Ne vždy je možné domluvit například sněm všech zaměstnanců na jednom místě a v jeden čas. Proto se zavedením této infrastruktury, je možné například využívat elektronické komunikační kanály, které podnik propojí jak zevnitř mezi zaměstnanci, tak i se zákazníky či partnery. Služby internetu nabízí kupříkladu možnosti e-mailu. Telekomunikace zase služby volání a textových zpráv. Předávání si informací a dat je pak mnohem jednoduší a efektivnější pro podnikání. [2]

Sužby IT infrastruktury, lze rozdělit do dvou hlavních částí. Respektive tří. Ta pak vzniká spojením obou. Dvě základní jsou interní a externí služby. Interní se zabývají zejména vlastními zaměstnanci a jejich potřebami. Externí pak v případě sepsání smlouvy poskytování služeb za úplatu dalším podnikům. Lze k nim přiřadit například nabízení cloudových služeb. Kompromis mezi těmito službami se nazývá sdílená služba a je využito obou variant. [2],[3]

Hlavní služby poskytující IT infrastruktura:

- Komunikační kanály a služby.
- Řízení rizik a bezpečnosti.
- Řízení dat.
- Správa a řízení IT zařízení (hardware).
- Správa softwaru.
- Vzdělávání zaměstnanců. [3]

Významnou službou je zpracovávání dat. Umožňuje tedy řízení dat nezávisle na aplikacích. Dostupnost by měla být zajištěna pro všechny a nejlépe i odkudkoliv. Samozřejmě je cílem docílit vhodného zabezpečení, aby přístup měly jen oprávněné osoby. Jelikož jsou tedy v systému uloženy citlivé údaje zákazníků i samotné firmy, je potřeba je vhodně zabezpečit před únikem či odcizením. [3],[3]

Neméně důležitou oblastí je tedy řízení a zabezpečení jednotlivých dat. S tím souvisí zabezpečení celé infrastruktury. Docílit se tak dá například používáním bezpečných hesel, či bezpečné používání vzdáleného přístupu. Mimo jiné také zálohování dat, šifrování, anebo

firewall. Řeší se zde i například co dělat při dočasném výpadku systému. Tzv Business continuity management (BCM) nebo i Disaster recovery planning (DRP) přinášející plán obnovení při katastrofických událostech. S těmito pojmy úzce souvisí analýza rizik. [3]

Manažeři v oboru IT se musí vypořádávat s rozvíjením podnikové infrastruktury a informačních technologií. Zároveň však musí dohlížet na to, aby celý systém pracoval správně a bezproblémově. Je potřeba zajistit stabilní provoz IT infrastruktury. [2]

1.2.2 Aplikační infrastruktura

Řada rozsáhlých podniků, by svépomocí nezvládala obrovský objem dat a informací zpracovávat samotnými zaměstnanci. Pro tuto práci dnes existuje řada programů, starajících se o činnost zpracovávání dat. Aplikace pak mohou zaměstnancům, či vedení podniku předávat už jen výsledky k dalšímu zpracování. Pro veškeré tyto dále zmiňované aplikace zabývajícími se správou podnikových dat existuje název Enterprise content management (ECM). [2],[4]

Podniky, jejichž byznys stojí na kvalitě plánování, zejména v oblasti výroby, prodeje či servisních prací, jistě ocení aplikace vytvořené pro tuto oblast. Aplikace, které pracují s daty souvisejícími s touto činností, se nazývají Enterprise resource planning (ERP). Účelem těchto aplikací je vytvářet databáze obrovského rozsahu. Ty zahrnují informace o položkách typu zboží, dodavatel, zákazník, zaměstnanec a další s tím spojené. Nedílnou součástí je zpracování těchto údajů, a například pravidelně objednávat výrobní materiál, nebo kontrolovat sklady. Umožňují vytvářet analýzy a statistiky prodeje a další možnosti ulehčující práci lidem. [2],[3],[4]

V mnoha podnicích je snaha komunikovat i se svými zákazníky a mít i jejich evidenci. Pro tyto účely jsou aplikace označovány názvem Customer relationship management (CRM). Tyto aplikace zahrnují databáze zákazníků a řídí komunikaci s nimi. To by mělo vést ke spokojenosti a loajalitě zákazníků. [2],[3],[4]

Rozdělení samotných aplikací je mnoho. Za zmínku stojí například aplikace Supply chain management (SCM), které vedou podnik k maximální efektivitě a optimalizaci řízení. [2],[3],[4]

1.3 Cloud computing

Cloud computing (CC) je ve své podstatě poskytování cloudových služeb jinou společností. Mluvíme tedy často o externích službách. Umožňuje, aby měl uživatel přístup k zařízením připojených k internetu odkudkoliv. Mezi takové zařízení patří například počítač, úložiště dat, celá podniková síť či jednotlivé aplikace. Díky tomuto lze přistupovat k podnikovým datům pohodlně odkudkoliv, kde je alespoň nějaké připojení k internetu. Přístup by měl být možný také z kteréhokoliv zařízení s kterýmkoliv operačním systémem. Tímto je myšleno PC, notebook, nebo i mobilní telefon nezávisle na výrobci. Charakteristikou CC je mimo všestranného síťového přístupu i to, že by měl být samoobslužný. Tedy nemělo by být potřeba znalého technika při změnách. Samozřejmostí by mělo být i sdílení služeb mezi další uživatele. Souvisí zde i pružnost a škálovatelnost. Zákazník si tak určí sám, co ke své práci vyžaduje a co naopak je schopen oželit. Tím si určuje cenu za poskytovanou službu a systém, který sám kontroluje využívané prostředky. [2][3]

1.3.1 Služby CC

Patří zde tři základní poskytované služby. Jedna z nich poskytuje nabízení jen aplikace neboli softwaru. Samozřejmě ve většině případů za úplatek. Této službě se nazývá Software as a service (SaaS). Aplikace je pak buďto provozována přímo na zařízení objednavatele, či na zařízení pronajímatele. Často se takto kupují licence k provozování softwaru. [2],[3]

Druhou skupinou jsou služby poskytující výpočetní platformy. Vlastním názvem Platform as a Service (SaaS). Umožňuje se tak například vyvíjet či provozovat aplikaci na pronajatém zařízení, ke kterému dostane objednavatel přístup přes webové rozhraní. [2],[3]

Do poslední skupiny se řadí přímo pronájem celé infrastruktury, tedy úložiště a výpočetní výkon, dle představ objednavatele. Služba se nazývá Infrastructure as a Service (Iaas). Výhodou je hlavně flexibilita. Zákazník si kdykoliv může změnit kapacitu úložiště či výpočetní výkon. Velkou výhodou je samozřejmě i přístup odkudkoliv. [2],[3]

2 INFORMAČNÍ SYSTÉM

Kapitola pojednávající o Informačním systému (IS), se zabývá tímto pojmem samotným. Je zde tedy uvedeno, co do IS patří a s čím tyto systémy pracují. Jaké jsou základní složky IS, anebo požadavky na IS.

2.1 Pojem Informační systém

Zmiňovaný pojem IS tvoří samotné informační technologie, lidé, data a dílčí procesy. Činnost IS souvisí s přenosem, ukládáním, či zpracováním informací. Informace jsou tvořena z dat. Množina, nebo také složky IS v sobě nese skupinu lidí pracující s těmito technologiemi, samotné technické prostředky pro manipulaci s informacemi a jednotlivé metody zpracování. IS slouží zejména uživatelů, kteří s nimi pracují. [5],[6],[7]

Účelem IS jsou tedy hlavně sběr dat, jejich uchování, přenášení, zpracovávání a poskytování relevantních informací. Samotná architektura IS je založena na informačních a komunikačních technologiích. [5]

2.1.1 Složky IS

Jednotlivé složky informačního systému jsou například hardware či software. Patří zde i databáze, se kterými IS pracují. Nesmí se zapomenout ani na uživatele neboli lidi. S tím souvisí i organizační uspořádání a samotné využití IS. Základními složkami tedy jsou:

- Hardware – jsou základní technické a technologické prvky systému typu počítač, server a prvky sítě jako je router apod. Patří zde i jednotlivé periférie či komponenty jako je myš, klávesnice nebo tiskárna.
- Software – obecně programy řídící správný chod počítače a využívající jeho výpočetní výkon. Zefektivňuje práci uživatelům.
- Orgware – je souhrn pravidel vytvořený podnikem pro pro provoz IS.
- Peopleware – též lidská složka v prostředí IS. [6]

2.1.2 Požadavky na IS

Jako každý jiný systém, musí být i tento spolehlivý. V podnikovém odvětví pak vhodně pružný a snadno rozvinutelný. V neposlední řadě snadno spravovatelný a zejména bezpečný. Efektivně musí být i zužitkovaný náklady na pořízení tohoto systému v porovnání

s přinášejícím užitkem. Přístup k informacím by měl být aktuální a zobrazovat by se měly jen ty relevantní. [6]

2.2 Informace vs. Data

V běžné praxi bývají pojmy informace a data velice snadno zaměňovány. V jednoduchosti lze říci, že data jsou neuspořádané hodnoty, a až po jejich uspořádání se z nich stanou informace. Informace tedy vzniká až samotnou interpretací dat. [6]

Hodnota informace je však relativní. Pro někoho může mít stejná informace vysokou hodnotu, pro někoho jiného zase žádnou. Základním aspektem informace je často její rychlé stárnutí. V čase se dokonce i samotná hodnota informace mění. Informace není hmotného charakteru. [9]

2.3 Zabezpečení IT infrastruktury

Zabezpečení IT infrastruktury a IS, znamená také zabezpečení informací v nich uložených. Kapitola tedy pojednává o tom, jak tyto systémy vhodně zabezpečit před ztrátou či únikem informací. Zejména na co běl být kladen důraz.

2.4 Zabezpečení IS

Abychom zabezpečili data či informace, musíme nejdříve zabezpečit celou IT infrastrukturu. Pro mnohé podniky bývají informace často nejdůležitějším aktivem, který je potřeba chránit. Mnohdy by ztráta citlivých informací vedla i k samotnému zániku podniku. **Chyba! Nenalezen zdroj odkazů.**

Aby vůbec mohl být jakýkoliv systém zabezpečován, je nejdříve potřeba znát hrozby. Mezi nejčastější známé hrozby lze považovat například výpadek výpočetního systému. Ten může být zapříčiněn například selháním některého z hardwaru. Stejně tak i výpadek komunikačního systému. V těchto případech je řešení situace jednoduché, vymění se kus za kus. Často se může stát, že výpadek se stane na straně dodavatele jak už silové energie, tak u poskytovatele internetového připojení. Zde je třeba se obrátit na ně. [10]

Zabezpečení souvisí s vnitřními a vnějšími hrozbami, kterým je třeba se vyvarovat. Vnitřní hrozby vznikají v samotném firemním prostředí mezi zaměstnanci. Například nespokojený zaměstnanec ve výpovědní lhůtě. Nebo jen neznalý zaměstnanec připojený do firemní sítě, který nevědomky nahraje škodlivý software a poškodí celou IT infrastrukturu.

Vnější hrozby pak přicházejí zvenčí. Ať už možnost kybernetického útoku, nebo jen výpadek elektrické energie. [10],[12]

2.4.1 Základní principy zabezpečení

Surová data, nebo již zpracovaná a přeměněná na informace jsou důvodem, proč je potřeba vůbec IS zabezpečovat. Data mají čím dál vyšší finanční hodnotu a v případě ztráty hrozí velké finanční ztráty. Budou-li zabezpečené IS, budou zabezpečené i informace. Dobře zabezpečené systémy a data musí splňovat následující body:

- Přístup k systému a datům smí mít jen oprávněné osoby.
- Ukládat jen důležité a věcné informace.
- Data s sebou musí nést informaci o tom, kdo je vytvořil, upravil nebo případně odstranil a kdy.
- Důvěrné či citlivé informace nesmí být vyzrazeny či zveřejněny.
- Systémy i potřebné informace musí být vždy k dispozici. [10]

2.4.2 Bezpečnost IS

Bezpečnost musí být vždy zajišťována komplexně. Nestačí se tedy chránit jen před vnějšími vlivy, typu výpadku elektrické energie, nebo přírodními vlivy. Chráněná musí být i před vnitřními útočníky, tedy vlastními zaměstnanci. Komplexní zabezpečení je dáno třemi hlavními body: [12]

- Důvěrnost – k údajům mají přístup jen autorizované osoby
- Integrita a autenticita – údaje musí být zpětně dohledatelné, včetně případných změn. Navíc je smějí upravovat jen pověřené osoby
- Dostupnost – údaje jsou po ověření totožnosti vždy dostupné

S těmito body již dnes souvisí i prokazatelnost a nepopíratelnost odpovědnosti či spolehlivost. [12]

Funkce, které se v této oblasti používají, je hned několik. Nejdříve při vstupu do systému probíhá autentizace či identifikace. Poté následuje například autorizace s řízením přístupu, tedy k čemu všemu má uživatel přístup. S tímto odvětvím je i úzce spojená bezpečnostní politika, která je vhodná zřídit, aby byli zaměstnanci obeznámeni s pravidly v podniku a řídili se jimi. [12]

2.5 Bezpečnostní funkce

Bezpečnostní funkce, nebo také bezpečnostní opatření jsou prvky k ochraně zranitelných míst IS. Způsoby jak tyto funkce implementovat je hned několik, například softwarově. Funkce softwarově založené například řídí přístup k systémům, používají kryptografii neboli šifrování. Za zmínku stojí i elektronické podepisování. Nesmíme zapomenout také na dnes už běžný prostředek ochrany, kterým je antivirový software. Samotným testováním bezpečnosti můžeme sami odhalit slabiny systému. Správní zabezpečovací funkce s sebou nese zase školení důvěryhodných osob. Hardwarovým zabezpečením docílíme například autentizací pomocí čipových karet, nebo jen archivací dat mimo IS na papír. Fyzické zabezpečení následně spočívá v pořízení záložního generátoru elektrické energie, trezorů či alespoň bezpečnostních zámků. Vhodnou volnou je také umístění klíčových prvků IS do zabezpečených, střežených a nepřístupných prostor. [12]

2.6 Bezpečná komunikace

Dnešní komunikace elektronickou poštou, která v mnoha podnicích zajišťuje komunikaci s klientelou, tak i mezi samotnými zaměstnanci, nemusí být vždy bezpečnou variantou. Samotná komunikace prakticky nezajišťuje žádnou bezpečnost. Existují však možnosti jak tuto bezpečnost zajistit. Zfalšovat emailovou schránku pod cizí, či vymyšlenou identitou není nijak velký problém. Útočník se pak může vydávat za někoho jiného a rozesílat podvodné emaily. Pro bezpečnou komunikaci je potřeba zajistit tyto body:

- Příjemce musí mít jistotu, kdo zprávu odeslal.
- Zajistit integritu zprávy, tedy že obsah, který odesilatel odeslal, přišel nezměněn i příjemci.
- Možnost skrýt, neboli zašifrovat obsah zprávy. [11]

Způsoby jak zajistit bezpečnou komunikaci, jsou například elektronické podepisování, či šifrování zpráv. [11]

3 IMPLEMENTACE INFORMAČNÍCH SYSTÉMŮ

Kapitola přináší metody, jak je možné IS implementovat do podnikového prostředí. Zdůvodňuje proč je výhodné tyto systémy implementovat a co brzdí jejich implementaci. Také jaké jsou architektury a možnosti IS.

3.1 Důvody implementace IS

Informační společnost v dnešní době nabízí podnikům plno nových příležitostí a výzev. Změny, které nově implementovaný IS nabízí, se dotýká nejen samotných zaměstnanců, ale i případných dodavatelů či zákazníků. Samotný přínos je vidět i v manažerském odvětví, kde rozhodnutí jsou čím dál komplikovanější a rizikovější. Pokud jsou však podepřena o výsledek nějakého softwaru, jsou pak lépe obhájitelná v případě vzniklých ztrát. Zavedením IS se zrychluje samotná produktivita podniku. Tím se mění i trh, který musí být daleko flexibilnější a mít vždy něco v záloze. Zavedením IS dostává vedení podniku přehlednou kontrolu nad všemi dílčími činnostmi včetně zisku, či ztrát. [4]

3.2 Teorie implementace IS

Zmiňované IS se v podnikovém prostředí nevyskytují pouze v souvislosti s IT. Ne vždy je totiž informace zaznamenána elektronicky. Stále je spousta informací uložena v papírově podobě a bývají obtížně dostupné. Také se může jednat o informace uložené v samotných zaměstnancích, respektive v jejich mysli a paměti. Těmi jsou například zkušenosti. Je tedy potřeba počítat s tím, že ne všechny informace lze do IS implementovat. [4]

3.2.1 Analýza potřeb konkrétního podniku

Každý podnik je specifický a každý má tedy jiné potřeby. Důležité je, jestli chce podnik implementovat informační systém do stávajících IT a zakoupit si například licenci k provozování této služby, nebo si službu pronajmou externí firmou i s IT. [4]

3.2.2 Architektury IS

Jednotlivé architektury rozdělují podniky do různých oblastí podle jejich zájmů a potřeb. Architektury se zabývají rozvojem IS zejména u rozsáhlých organizací s cílem zefektivnit podnikání. Organizace využívajících dále zmíněných architektur, jsou například banky, rozsáhlé výrobní podniky, nebo telekomunikační společnosti.

- **Business architektura** – Architektura IS zabývající se zejména na tvoření zisku organizace. Zajišťuje kontrolu nad cíli organizace a vede ji k téměř zaručeným úspěchům. Prolíná se zejména s tradičním podnikovým managementem v nejvyšších vrstvách podniku.
- **Informační architektura** – Tato oblast řídí datové toky organizace. Zabývá se zejména informačními potřebami společnosti. Vytváří se tzv. datový model.
- **Aplikační architektura** – V organizaci se zabývá používanými aplikacemi, zejména jejich popisem a evidencí. Dokáže slučovat aplikace mezi různými systémy.
- **Technický architektura** – Tato oblast se zabývá vůbec těmi základními prvky, kterými jsou IT. Tedy hardware a software v procesu podnikání. Probíhá zde strukturování firemní sítě. Tato část patří k nejrychleji dosažitelným z výše zmíněných. [13]

3.2.3 Varianty implementace IS

Různým podnikům připadají různé varianty řešení implementace IS. Jednou z nich je například rozvoj stávajícího IS. To má za následek využití existujících zdrojů a investic. Dá se považovat za levnější a rychlejší variantu s cílem uspokojit stávající potřeby. Nevýhodou je, že vždy nemusí naplnit budoucí požadavky. Po dlouhodobé stránce se tak výrazně zvýší náklady a výsledný systém nemusí dosahovat potřebné kvality. [4]

Druhou variantou je vývoj nového systému přesně na míru požadavků podniku. Řízeným vývojem se tak naplní všechny potřeby podniku. Tato varianta je však obecně časově a finančně náročnější. Rizikem je také to, že další vývoj do budoucna již nebude garantován, jelikož úprava stávajícího řešení, by často byla složitější než vytvoření nového řešení. [4]

Poslední možností je nákup hotového softwarového systému. To s sebou nese z pohledu financí do dlouhodobého hlediska menší náročnost. Velkou výhodou je rychle zavedení a zaručená funkčnost. Funkcionalita je v průběhu času vyvíjena jinou organizací. Nevýhodou tohoto řešení je v tom, že celý systém je závislý na jeho dodavateli, který jej vytváří. Nemusí tak vždy naplnit veškeré požadavky podniku.[4]

3.2.4 Výhody zavedení ERP

Zavádění ERP systému v podniku vede ke značnému zautomatizování podnikání. V podstatě by se dalo říct, že dobře zavedený ERP systém podniká sám. Systém může být zrealizován jako softwarové řešení, které má přístup k většině firemním dat a patřičně je

zpracovává. Dokáže například plánovat logistiku od nákupu až po prodej. Dokáže řídit jednotlivé zakázky a dokonce i komunikovat se zákazníky. Dokáže řídit vlastní výrobu v podniku. V určité míře dokáže spravovat účetnictví. Po implementaci tedy značně ovlivňuje podnikání. Zavedením se tak stává mozkem podniku, který se stará jak o samotnou logistiku, tak i o finance podniku. Mimo to předkládá vedení podniku jasné informace o průběhu podnikání. [2],[4]

Častým stěžením pro implementaci těchto systémů, zejména v prvopočátcích zavádění, jsou samotní zaměstnanci. Ne všichni se rádi učí s novými technologiemi a raději zůstávají u osvědčených věcí. Proto s sebou implementace nových informačních systému, nese řadu školení personálu. Učení s technologiemi a dlouhodobému testování a postupnému zavádění těchto systémů. Často je to běh na dlouhou trať a brzdícím mechanizmem jsou samotní lidé. S tím je spojeno i to, že vize navýšení efektivity práce a tvorby většího zisku nikdy nepřijde okamžitě. Tato skutečnost nese za následek, že řada podniku se od IS stále distancuje. [2],[4]

4 ZÁKLADNÍ POJMY A PRVKY SÍTĚ

V této kapitole jsou popsány základní prvky a pojmy spojeny s IT a počítačovou sítí zaměřenou dále na bezdrátovou komunikaci jednotlivých zařízení. Je zde vysvětleno i rozdělení sítí dle velikostí. Následuje zabezpečení těchto sítí.

4.1 Rozdělení sítí podle velikosti

Sítě se rozdělují do skupin podle velikostí. Nejmenší sítě zaštitují tzv. Personal area networks (PAN), to jsou pro vysvětlení krátké osobní sítě, zejména domácí s dosahem jednotek metrů. Sítě PAN najdeme například ve standardu 802.15, která popisuje známý bezdrátový přenos Bluetooth. V řádech desítek až stovek metrů jsou místní sítě tzv. Local area networks (LAN), ty najdeme téměř v každé domácnosti pokrytými bezdrátovou sítí, která se nazývá Wireless Fidelity (Wi-Fi). Dalšími ještě rozsáhlejšími sítěmi, působícími například v celém městě, či regionu jsou tzv. Metropolitan area networks (MAN), rozlehlost těchto sítí je již v řádech kilometrů. Wide area network (WAN) zaštituje standard 802.16 s komerčním názvem WiMAX. Standard začínal v roce 2001 a popisuje tedy rozsáhle venkovní sítě, oproti tomu Wi-Fi je zaměřeno na vnitřní sítě. [14]

Tabulka 1 – Rozdělení sítí podle velikosti. [14]

Rozdělení sítí podle velikosti		
Název	**Zkratka**	**Rozsáhlost**
Personal area network	PAN	jednotky metrů
Local area network	LAN	desítky až stovky metrů
Metropolitan area network	MAN	kilometry
Wide area netowrk	WAN	rozsáhle sítě

Nejznámějším představitelem WAN sítě je internet. Ten je rozšířený téměř po celém světě. [14]

4.2 Aktivní prvky sítě

Pokud přehlédneme pasivní prvky sítě jako je kabeláž, konektory a různé spojky, zůstanou nám aktivní prvky. Jsou to v podstatě elektrotechnická zařízení, která aktivně pracují s přenosem dat mezi jednotlivými zařízeními, jako je například směrovač, přepínač, rozbočovač či opakovač. [15]

- **Router** – česky označován jako směrovač, je zařízení propojující dvě a více sítí.

- **Switch** – je vlastně přepínač, rozděluje jednotlivá zařízení v sítí k efektivnějšímu využití přenosu dat.
- **Hub** – též rozbočovač sdružuje jednotlivé přípojky zařízení do jednoho místa, dnes nahrazován switchem.
- **Gateway** – je brána zajišťující komunikaci různých zařízení s jinými komunikačními protokoly.
- **Bridge** – přemosťuje zařízení v sítí s různými přenosovými protokoly
- **Repeater** – je označován jako opakovač neboli zesilovač zajišťující správný přenos dat na dlouhé vzdálenosti, aby nedošlo k útlumu signálu (Jak u drátové tak bezdrátové sítě). [15]

4.2.1 Bezdrátová síť

Pojmy a zařízení spojené s bezdrátovým přenosem dat po síti Wi-Fi.

- **Access Point** – je přístupový bod (AP) sloužící k bezdrátovému připojení klientů a zajištění bezpečné komunikace s nimi. V domácnostech jsou AP často integrované přímo do routeru.
- **Client** – Klienti jsou koncová zařízení typu notebook, mobil či bezdrátová tiskárna.
- **Ad-hoc** – Je režim bezdrátové komunikace, kdy neexistuje fyzicky AP, ten nahrazuje první zařízení připojené v sítí, které následně zajišťuje komunikaci s dalšími bezdrátovými zařízeními.
- **Wireles Distribution System** – (WDS) je režimem, kdy je možno propojit bezdrátově více AP. Nevýhodou je zpomalení sítě. Při dvou takto propojených AP je rychlost poloviční. [15]

4.2.2 Metody šifrování bezdrátových sítí

Metody šifrování jsou algoritmy pro bezpečné přenášení dat využívané u bezdrátových sítí Wi-Fi.

- **Wired Equivalent Privacy** – (WEP) zastaralé zabezpečení z roku 1997
- **Wi-Fi Protected Access** – (WPA) reakce na prolomení zabezpečení WEP v roce 2001. Šlo o dočasný standard.
- **W-Fi Protected Access 2** – (WPA2) je standardem 802.11i z roku 2004 a je používán dodnes. Je považován za bezpečný. [15]

4.3 Standardy Institute of Electrical and Electronics Engineers

Rodina standardů Institute of Electrical and Electronics Engineers (IEEE) sahá do historie až k roku 1980. Zejména je řeč o standardu 802. Standardy se zabývají LAN a MAN sítěmi. Počátky standardizace se zabývaly ethernetovým přenosem. Poté se vyvíjel bezdrátový přenos, se kterým souvisí standard IEEE 802.11. [14]

Tabulka 2 – Nejznámější standardy IEEE 802.11. [14]

Standardy IEEE 802.11

Označení IEEE	rok vydání	pásmo	max. rychlost
802.11	1997	2,4 GHz	2 Mbit/s
802.11a	1999	5 GHz	54 Mbit/s
802.11b	1999	2,4 GHz	11 Mbit/s
802.11g	2003	2,4 GHz	54 Mbit/s
802.11n	2009	2,4 a 5 GHz	600 Mbit/s
802.11ac	2014	5 GHz	1 Gbit/s
802.11ad	2012	2,4 , 5 a 60 GHz	7 Gbit/s

Počátky bezdrátové, dnes již zastaralé standardizace sahají do roku 1997. Tehdy vyšel první zmiňovaný standard Wi-Fi 802.11. O dva roky později přišly hned dva nové, výrazně pokročilejší standardy povyšující rychlost v 2,4 GHz pásmu na 11 Mbit/s nesoucí označení 802.11b. V pásmu 5 GHz dokonce s rychlostí 54 Mbit/s označeným jako 802.11a. Pár let později dosáhlo na stejnou rychlost i pásmo 2,4 GHz a označil se tak standard jako 802.11g. Všechny zmíněné standardy pracovaly běžně se šířkou pásma 20 MHz. Poté přišla dlouhá odmlka a vývoj se zdánlivě pozastavil. [14]

Na trůn však v roce 2009 usedl standard nesoucí označení 802.11n. Ten posunul šířku pásma na 40 MHz a samotná maximální rychlost vzrostla na 150 Mbit/s. To však není to jediné, co standard přinesl. Dalším významným posunem byla technologie s názvem Multiple-input multiple-output (MIMO). V překladu více vstupů, více výstupů. Tato technologie umožnovala vysílacím zařízením vlastnit až 4 antény a umožnit tak propustnost až 600 Mbit/s. [14]

Další posun přišel v roce 2014 standardem 802.11ac který umožňoval až 8x8 MIMO. Dokázal navíc využívat šířku pásma až 160 MHz. Maximální rychlost této technologie se blíží k hranici 1 Gbit/s. S touto technologií navíc přichází rozlišení Single User MIMO (SU-MIMO) a Multi User MIMO (MU-MIMO). Předchozí standard 802.11n umožňoval pouze SU-MIMO, tedy při připojení více klientů, vyřizoval přenos střídavě, kdežto u technologie

MU-MIMO umožnoval přenos a komunikaci až u čtyř zařízení současně. Tímto se dosáhlo k dalšímu extrémnímu nárůstu rychlosti bezdrátové komunikace. [14]

4.4 Zabezpečení bezdrátové sítě

Mezi nejznámější zabezpečení bezdrátových sítí patří šifrování přenosu dat metodami WEP, WPA a WPA2. O těchto a dalších metodách zabezpečení, bude pojednávat tato podkapitola.

4.4.1 WEP

Zabezpečení pomocí WEP je nejstarším standardem z roku 1997. Šlo tedy o první možnost zabezpečení bezdrátové komunikace před odposlechy pomocí šifrování. Z názvu Wired Equvivalent Privacy vyplývá, že se mělo jednat o zabezpečení rovnocenné drátovým sítím. K šifrování dat se využívá proudová šifra RC-4. Zmíněná šifrovací metoda patřila k jedné z nejrozšířenějších. Dnes však její používání je na ústupu vzhledem k její poměrně snadné prolomitelnosti. U zabezpečení WEP se používá 40 nebo 104 bitový klíč, ten však navíc obsahoval 24 bitový inicializační vektor (IV). Celková délka klíče tak měla 64 nebo 128 bitů. Existují však i varianty 152 a 256 bitové. Nicméně největší slabina spočívala v onom IV, díky němuž bylo při odposlouchávání přenesených paketů možno uhádnout zbytek klíče. Slabina spočívala tedy v přenášení IV v paketech. [15],[16]

WEP mimo jiné poskytuje dvě metody autentizace. Jedna z nich se nazývá Open system authentication a druhá Shared key authentication. [15]

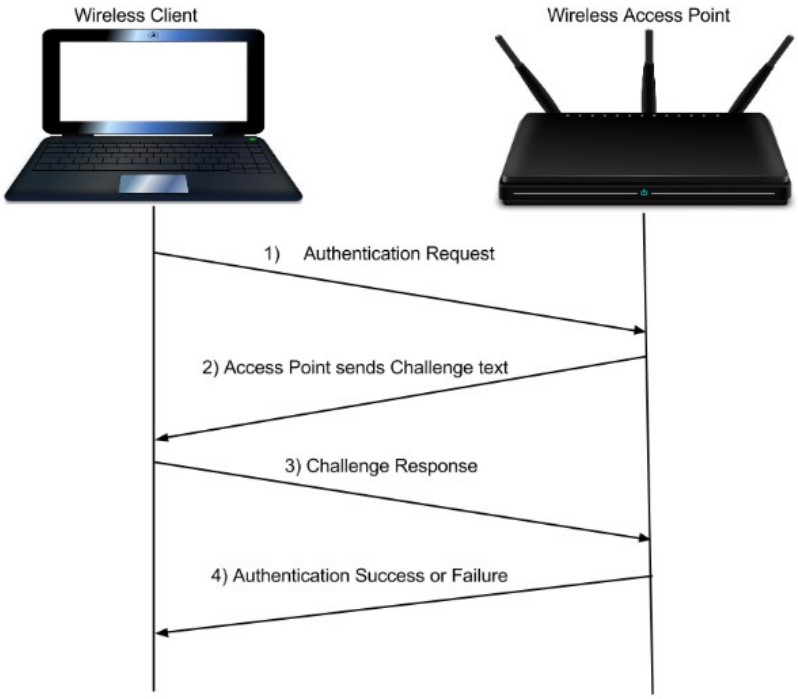
- **Open system authentication -** V tomto případě nedochází k žádné autentizaci klienta s AP, jednoduše pokud má klient správný klíč, může s AP komunikovat po navázání spojení. [15]
- **Shared key authentiation -** Na rozdíl od předchozího otevřeného způsobu autentizace, se zde provádí čtyřfázová autentifikace pomocí WEP klíče. Tento proces se nazývá handshake, nebo také „challenge-response“ což je česky výzva-odpověď. Provádí se tedy k navázání spojení, kdy jedna strana sítě dá otázku druhé straně a ta na ní musí správně odpovědět, obecně řečeno. V praxi to probíhá takto:

(1). Klient, tedy zařízení pokoušející se o navázání spojení vyšle AP žádost o navázání komunikace. (Authentication request)

(2). AP žádost příjme a odešle klientovi tzv. challenge, neboli výzvu. Což je jakýkoliv otevřený text.

(3). Klient, vlastní-li klíč, zprávu tímto klíčem zašifruje a odešle zpět AP, tzv response.

(4). AP nyní přijatou zašifrovanou zprávu dešifruje a porovná z dříve odeslanou zprávou. Pokud se tyto zprávy shodují, dochází k navázání spojení. (Confirm Success). [15]



Obrázek 1 – Handshake. [17][17]

Ačkoliv se zdá bezpečnější druhá metoda za použití procesu výzva-odpověď. Správná odpověď je paradoxně jiná. V tomto případě lze onen handshake odposlechnout někým třetím a pokusit se odvodit používaný klíč. Ten se používá stejný jak k šifrování otevřeného textu při navázání spojení, tak i po celou další dobu komunikace. Jelikož se podařilo WEP prolomit již v srpnu 2001, byl od té doby považován za ne příliš bezpečný. Čas potřebná k prolomení spočíval na vytíženosti sítě, tedy kolik paketů se po sítí během sledování posílá. V případě, že byla nízká vytíženost, bylo navíc možné simulovat provoz sítě generováním vlastních paketů. Prolomení je pak otázkou minut. [14],[16]

4.4.2 WPA

Wi-Fi Protected Access neboli v překladu chráněný přístup k Wi-Fi je nástupcem zabezpečení WEP. WPA se začalo využívat již v roce 2002. V téže době si připravoval nová

standard 802.11i s toto byla jedna z jeho částí, hojně uváděno jako v třetím pracovním návrhu. Jelikož mělo být WPA rychle a snadno implementováno, musela zde být možnost použití stejného hardwaru jako u WEP. V té době tedy stačilo aktualizovat software, respektive firmware produktu, a začít používat nové zabezpečení. Již v době zavádění WPA vědělo IEEE, že se jedná pouze o dočasný prostředek ochrany a pracovalo se na později vydaném WPA2. Nicméně základem WPA bylo eliminování slabých míst, které obsahoval WEP. Zejména tím, že už nešlo tak jednoduše odhalit IV. Jejich přenos byl jak při zahájení komunikace, tak při ní lépe chráněn. O to se zasloužil nově vyvinutý Temporal key integrity protocol (TKIP). [15],[16]

WPA je navržen na použití 128 bitového klíče. Nadále používá IV, v tomto případě 48 bitový. Na rozdíl od WEP používá WPA k práci také Message Integrity Code (MIC) což je jakési počítadlo rámců a znemožňuje, nebo spíše stěžuje odposlouchávání za účelem zopakování předchozí komunikace. [15],[16]

4.4.2.1 TKIP

Ve své podstatě protokol TKIP využívá toho, že na rozdíl od WEP, nepoužívá po celou dobu přenášení dat neboli komunikace stejné klíče. TKIP tedy pro každý paket používá jiný klíč k zašifrování. Tyto klíče se vytvářejí jednak z klíče základního, neboli „Pairwise Transient Key“, navíc pak z MAC adresy přijímacího zařízení, ta by měla být jedinečná. Nakonec se do tvorby klíče přidá pořadové čísla rámce. Sloučením těchto informací vznikne klíč, kterým se paket zašifruje. Tím, že se pořadové číslo mění, mění se tak i celý klíč. Mimo to na koncovém zařízení, tedy klientovi běží na pozadí program tzv. Suplikant, který zajišťuje správnou autentizaci a bezpečnou komunikaci s AP. Na místo TKIP bylo následně po vydání standardu 802.11i možno použit novější šifrovací standard Advanced Encryption Standard (dále jen AES), což je v překladu standard pokročilého šifrování. [15]

4.4.3 WPA2

Již v roce 2004 došlo k implementaci zbytku částí standardu 802.11i. Nyní již byl nahrazen WEP novým standardem WPA2 a ten je od roku 2006 povinný pro certifikací produktů Wi-Fi alliancí. WPA2 nahrazuje proudovou šifru RC-4 novou, již blokovou šifrou AES. Ta je však značně náročnější na výpočetní výkon a neumožňuje funkci na starších zařízeních, které na to nebyly sestavené. Navíc se implementoval nový protokol s názvem Counter Cipher Mode with Block Chaining Message Authentication Code Protocol (dále jen

CCMP). Ten poskytuje v oblasti zabezpečení zejména důvěrnost dat, ověřování a řízení přístupu. Doposud je WPA2 považováno za bezpečné a jeli v případě provozování bezdrátové sítě možno zapnout, mělo by tak i být. [15]

S WPA i WPA2 souvisí také Pre-Shared Key (dále jen PSK) což je v podstatě předsdílený klíč. Tedy klíč, který musí uživatel neboli klient znát k připojení se k AP. Tento klíč by měl být dostatečně dlouhý a hlavně neuhodnutelný. Prolomit lze pouze slovníkovou metodou. [15]

4.4.4 Další možnosti zabezpečení bezdrátové sítě

Existuje mnoho dalších uživatelských typů a rad jak zvýšit bezpečnost bezdrátových sítí. Jednou z nich je například zakázání vysílání Service Set Identifier (dále jen SSID). To je v podstatě název sítě. Pokud jej potenciální útočník nevidí, tak o něm třeba ani neví a musel by se o sítí dozvědět jinak. Poté by teda síť byla přístupná jen těm, kteří o ní vědí. [15]

Dalším tipem a radou je umístit AP tak, aby signál nebyl například vně budovy, to je však u dnešních antén již velice náročné, jelikož jejich dosah roste. [15]

Jednou z nejefektivnějších metod je tzv. MAC control. Tato metoda umožňuje zadat AP jen ty MAC adres zařízení, které mají povoleno po sítí komunikovat. Ostatním zařízením, která by se nenacházela v seznamu, by nebyla komunikace umožněna. [15]

Možnost autentizace je také pomocí Remote authentication dial in user service (RADIUS). To je metoda navazování spojení buďto přes lokálně založený server, nebo i vzdáleně. Uživatel, který se chce připojit do lokální sítě, musí nejdříve požádat o povolení RADIUS server. Na ten odešle požadavek o autentizaci s přihlašovacím jménem, heslem a ID portu, přes který se připojuje. Server tedy vlastní databází uživatelů, kteří mají možnost se do sítě připojit. Pokud se tedy uživatel správně autentizuje, povolí se mu přístup do sítě. V opačném případě se připojení nenaváže. [15]

Velkou výhodu v zabezpečení a vzdálené komunikaci nabízí vytvoření virtuální privátní sítě (VPN). Ta nabízí bezpečné šifrované spojení dvou a více sítí, či koncových zařízení. Uživatel může být fyzicky kdekoliv na světě s připojením k internetu, ale pro zařízení v sítí se tvářit, jako by byl lokálně v ní. Často se tato metoda využívá v podnikových sítích. Metod jak toto propojení vytvořit je mnoho. [18]

5 ANALÝZA RIZIK

Pokud chce někdo něco chránit, musí nejdříve vědět co a jak. K tomu se všeobecně napříč obory používá analýza rizik. Obecně je to tedy proces definování hrozeb, které by mohly poškodit aktiva. Co jsou to aktiva, hrozby, nebo další termíny používané v této oblasti jsou podrobně popsány dále v této kapitole. Analýza rizik by tak měla zodpovědět na co je důležité se v oblasti bezpečnosti zaměřit a na co naopak ne. [20],[22]

Správně postavená analýza rizik ve svém vlastním výsledku odpovídá na tyto otázky:

- Jaké hrozby mohou nastat?
- S jakým rizikem mohou hrozby nastat?
- Jaké budou následky? [20]

5.1 Terminologie používaná v analýze rizik

Pro zdárné vypracování analýzy rizik, je důležitou součástí znalost základních pojmů, které s tímto oborem úzce souvisí a jsou často používané. [20]

5.1.1 Aktivum

Aktivem se rozumí všechno to, co je v našem zájmu, abychom chránili. Pokud by se s naším aktivem něco stalo, například rozbilo, ukradlo, poničilo či jinak porušilo, přišli bychom k finanční újmě. Mezi aktiva patří například veškerý hmotný, či nehmotný majetek firmy, zaměstnanci a vůbec vše to, co chceme chránit. [20]

5.1.2 Nebezpečí

Nebezpečí je pojmem, který představuje děj, jev, faktor, či vlastnosti nějaké látky, které v případě vzniku vykazují negativní jev, tedy pro nás nepříznivý. Nebezpečí nám tedy může způsobit materiální škodu, poškodit životní prostředí, ohrozit zdraví či život, nebo jinak ohrozit. [20]

5.1.3 Hrozby

Hrozbou je v podstatě to, co přímo či nepřímo hrozí našemu chráněnému aktivu. Je to tedy negativní událost a její závažnost je úměrná finanční hodnotě našeho aktiva. Hrozba může být i jevem přírodním, taková se nazývá hrozbou neintencionální. Naopak pokud hrozba vzniká chováním člověka a jeho úmyslným zamýšlením, pak se hovoří o hrozbě in-

tencionální. Hrozby jsou charakterizovány tím, že působí v konkrétním čase, místě a na konkrétní aktivum s určitou mírou nebezpečí, či rizika. Mezi hrozby patří například požár, přírodní katastrofa, ale i krádež, neoprávněné získání informací atd. [20]

5.1.4 Zranitelnost

Pojem zranitelnost udává jakousi citlivost neboli náchylnost systému ke vzniku škody. Dají se mezi ně zařadit například jakákoliv slabá místa. Zranitelnost je tedy to místo, kde může dojít ke vzniku hrozby na naše aktivum. Snížením zranitelnosti lze docílit včasným odhalením slabých míst a zavedení protiopatření. Mirou je tedy její úroveň na určité škále a hodnotí se dle dvou faktorů:

- Citlivost - zranitelnost aktiva danou hrozbou.
- Kritičnost – důležitost námi chráněného aktiva. [20]

5.1.5 Ohrožení

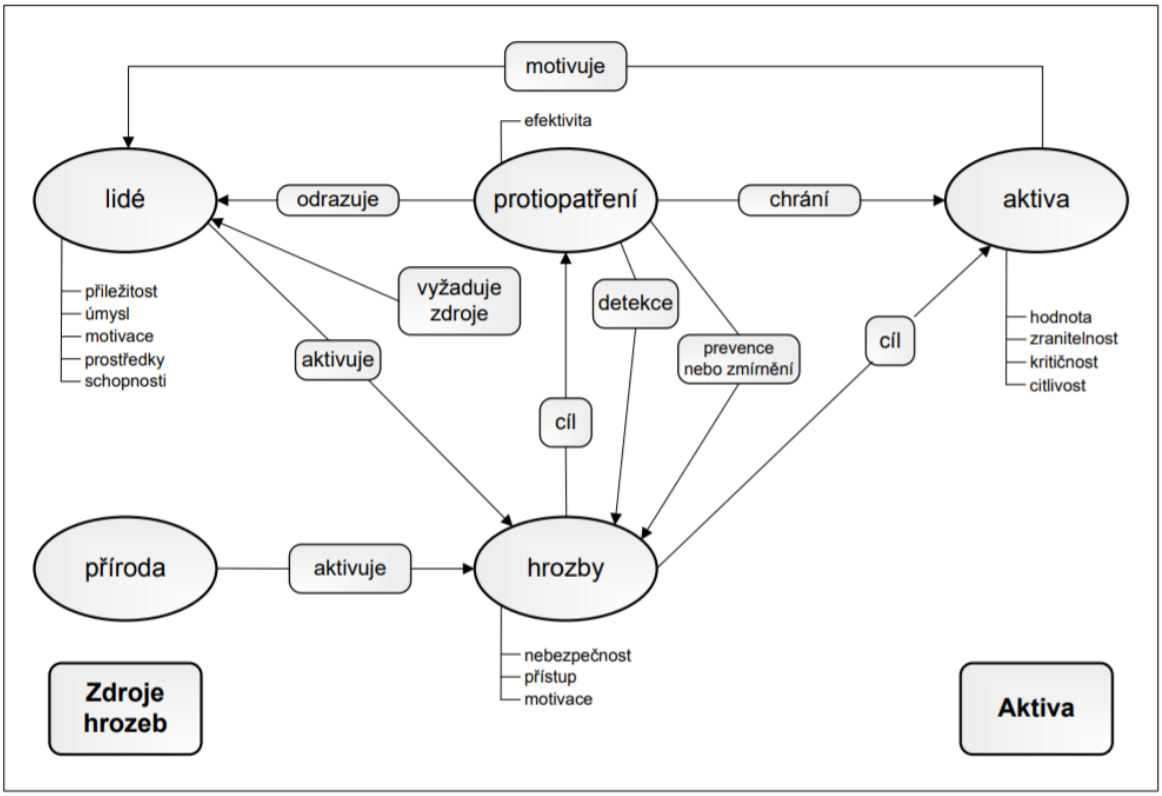
Ohrožení je blízce spjato s hrozbou. Většinou je tedy v technických vědách vyjádřeno matematicky, jako možnost či pravděpodobnost vzniku v daném místě a čase. [20]

5.1.6 Riziko

Riziko je mírou, neboli pravděpodobnosti vzniku nějaké nežádoucí hrozby. Představuje tedy číselně, nebo procentuálně s jakou pravděpodobností daná hrozba může vzniknout. Toto číselné vyjádření pak pomáhá k určení si těch hrozeb, které chceme pokud možno eliminovat, či dosáhnout alespoň minimálních následků při jejich vzniku na chráněné aktivum. [20]

5.2 Analýza a hodnocení rizika

Aby byla analýza rizik provedená správně, je nutné pochopení vztahů v ní. Analýza rizik zpravidla obsahuje identifikaci aktiv, tedy všechno to co je naším primárním cílem chránit. Následuje nalezení jednotlivých hrozeb, která mohou přímo nebo nepřímo působit na naše aktiva. Následuje pak určení míry rizika. Pro lepší orientaci a pochopení analýzy rizik poslouží diagram vztahů jednotlivých činitelů. [19]



Obrázek 2 - Diagram vztahů jednotlivých činitelů v analýze rizik. [20]

Metod jak analýzu rizik provádět je mnoho, obecně se však lze setkat se dvěma skupinami řešení. A to řešením kvalitativním nebo kvantitativním. Tyto na první pohled podobná slovíčka však značně pozměňují pohled na řešenou věc. Pokud se analýza rizik, tedy odhad rizika řeší kvalitativně, míra rizik vzniku jednotlivých hrozeb se určí na předem definované škále, například v rozsahu 1-10 a určí se co je nejhorší riziko a co naopak zanedbatelné riziko. Úroveň se určí kvalifikovaným odhadem. Naopak kvantitativní metody jsou brány například z výpočtů frekvence výskytu hrozeb a následným matematickým výpočtem. Počítá se obvykle s penězi a riziko je tak určováno v předpokládané roční újmě na majetku. [19]

Jakmile jsou známy všechna aktiva, hrozby a jejich rizika, přichází vyhodnocení této analýzy. Nazývá se hodnocením rizik. Je to tedy proces, při kterém dochází k vyhodnocování vzniku nebezpečí a zavádějí se jednotlivá protiopatření. Samozřejmostí zůstává, že ne všechny hrozby lze úplně eliminovat. Také je důležité myslet na to, zdali protiopatření, které by zjevně bylo nutné zavést ke snížení rizika, by svou finanční nákladovou částkou nepřesáhlo samotnou škodu při vzniku této hrozby, pak by zavádění tohoto protiopatření bylo neefektivní. [19]

6 FTA – ANALÝZA STROMŮ PORUCH

Analýza stromu poruch (FTA) se řadí mezi grafické analýzy. Její zpracování bývá ve formě diagramu. Na vrcholu diagramu je onen řešený stav, který bývá často nežádoucí. K tomuto stavu je pak snaha se dopracovat pomocí logických vztahů mezi nimi, čímž ve výsledku vznikne tzv. Strom poruch. [20]

Podstata této analýzy spočívá v určení si hlavního nežádoucího stavu. K tomuto stavu se pak hledají události, díky kterým tento nežádoucí stav nastane. Důležitou částí je vymezením si rozsahu, pro který se bude analýza zpracovávat. Samozřejmostí pro úspěšnou kvalitu zpracování návrhu analýzy rizik je detailní znalost analyzovaného systému. Bez toho se žádná analýza neobejde.[20],[22]

Analýza FTA je také popsána normou ČSN EN 61025, kde lze najít celé znění této normy a jasně popsaný postup a varianty zpracování této analýzy. [20],[21]

6.1 Součásti stromu poruch

Aby se ve výsledném stromu poruch dalo orientovat a vůbec se vědělo jak jej vytvořit, je potřeba znát jeho dílčí aspekty a jejich vzájemné vazby. Zde jsou uvedeny tedy hlavní prvky používané v diagramech. [20]

6.1.1 Hradla

Hradla slouží k definování logických vztahů mezi vstupními a výstupními veličinami diagramu. Nejběžnějšími hradly bývají například hradla OR, AND případně XOR. Hradlo OR si lze představit jako spojku „nebo“. Naopak hradlo AND zase jako spojku „a“ či slovní spojení „a zároveň“. Hradlo XOR pak pracuje se stavy, kdy je pouze jen jedna z variant možná, nikoliv obě. [20]

6.1.2 Události

Událostmi se rozumí nejnižší stavy v onom stromu poruch, které díky provázanosti mezi sebou vedou až k samotnému vzniku nežádoucího stavu. Je třeba tedy najít všechny události, které mohou jakkoliv dovést k nežádoucímu stavu. Nelze opomenout ani přírodní vlivy. Samotný vznik události tak může vést i k více poruchovým stavům. Často požívané značky lze nalézt v příloze P I.:Značky FTA analýzy.

6.1.3 Ostatní

Ostatními prvky grafického znázornění se rozumí například spojovací čáry mezi diagramy, popisky a jiné značky jakou jsou například šipky. [20]

6.2 Postup vypracování

Strom poruch se vytváří směrem od vrchu dolů. Diagram začíná nahoře definovaným nežádoucí stavem v obdélníkové značce. Od něj se pak vyvíjí návazné situace směrem dolů, případně do stran, propojované pomocí hradel, událostí se opět vpisují do obdélníků. Jednotlivé hradla se pak propojují pomocí čar. Postupuje se takto až k samotnému „kořenu“ stromu, kde se nachází událost, která zapříčiní definovaný nežádoucí stav. Konečná, základní událost se označí, či vepíše do značky ve tvaru kruhu. Pokud lze událost dále rozvíjet, ale pro řešení to již není podstatné, dá se událost ukončit značkou čtverce či kosočtverce stojícího na hraně, představující dále nerozvíjenou událost. Pro velké stromy poruch rozdělené například na více částí vedoucí k mnoha událostem a třeba i často opakujících se, lze použít značky jako je například kolečko vepsané v kosočtverci, to značí, že ona událost je již rozebíraná v jiném stromu poruch. Pokud je v jednom stromě poruch více pod událostí vedoucí k jedné a té samé událostí, lze požít tzv. přenos dovnitř nebo ven, a to obrazcem ve tvaru trojúhelníku. Tyto značky se používají zejména tomu, aby se v diagramu zbytečně neobjevovaly jedny a ty samé událostí. [20]

Po celkovém sestavení diagramu přichází jeho vyhodnocení. Pokud je strom poruch sestaven správně, dojde se ke všem základním kořenovým událostem, které vedou k často nežádoucí vrcholné událostí. Ví se tedy na co si dát pozor a na co se zaměřit, což často v tomto typu grafické analýzy stačí a říká se jí kvalitativní. Druhou metodou je metoda kvantitativní, ve které se počítá s pravděpodobnostmi reálného výskytu jednotlivých událostí. [20]

II. PRAKTICKÁ ČÁST

7 POPIS A STRUKTURA PODNIKU

Podnik XY se zabývá činnostmi v oblasti stavebnictví. Zejména tedy zpracováváním požadavků od zákazníků. Zpracováváním projektů a následně hledáním vhodných variant k realizaci. Například sestavením nabídky pro firmy či živnostníky, kteří dále projekt realizují. Dále pak často působí jako stavby vedoucí, kteří dohlížejí na správnou činnost najaté firmy.

K této profesi potřebují zajistit snadnou a rychlou komunikaci mezi svými zaměstnanci, i lidmi mimo podnik XY. Při provádění těchto činností, je dobré mít přístup ke všem podkladům. Je tedy dobré mít veškeré informace, dokumenty a projekty na jednom zabezpečeném místě a mít k těmto datům přístup odkudkoli. Ne jen ze svých kanceláří. Čímž se dále zabývá tato bakalářská práce.

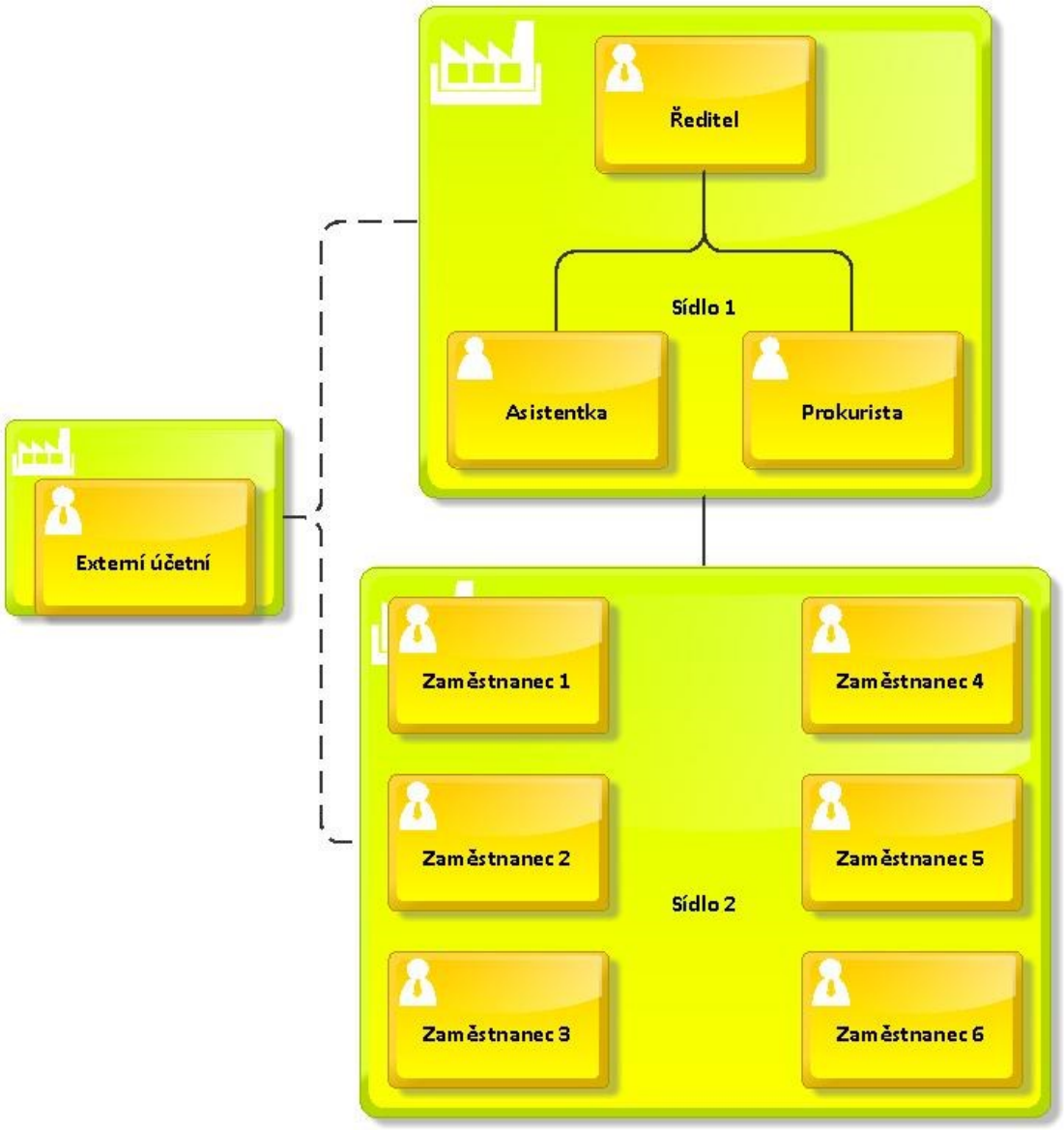
7.1 Struktura podniku

Současná struktura podniku neboli hierarchie je taková, že za vedením podniku stojí majitel. Ten je označován jako ředitel podniku. Dalo by se říct, že ředitelovou pravou rukou je dále prokurista. Ten zajišťuje vše to, co samotný ředitel v jednom čase nestihá. Také jej určitými činnosti ve věci jednání pověřuje. Zkrátka zastupuje ředitele. Mimo jiné, je zde pro všechny situace spojené s vedením podniku a zpracováváním informací asistentka ředitele. Pro tyto tři výše zmíněné je k dispozici sídlo označené číslem jedna.

Další část zaměstnanců pracuje výhradně ze sídla označeným číslicí dva. Zde se setkává šest zaměstnanců. Tito mají na starost zpracovávání jednotlivých projektů pro zákazníky. Udržují se s nimi také v kontaktu. Pokud je potřeba, tak samozřejmě jezdí i po stavbách. Z toho důvodu vzniká potřeba mít přístup k důležitým podkladům ke stavbám i mimo své pracoviště.

Za zmínku stojí, že Sídlo 1 a Sídlo 2 jsou od sebe vzdáleny přibližně 30 km. Sídla se nachází ve dvou odlišných městech. Komunikace probíhá povětšinou telefonicky, případně písemně elektronickou poštou.

S podnikem navíc spolupracuje externí účetní. Ačkoliv se však nachází ve stejném městě jako Sídlo 2, tak jsou tato místa vzdálená v řádech kilometrů.



Obrázek 3 – Struktura podniku

Podnik XY je postaven tak, že pro své stálé zaměstnance, je nedlouho k dispozici výhradně Sídlo 2. V Sídle 1 má ředitel prostory pro své nejbližší zaměstnance a odsud také řídí firmu. Jak již bylo zmíněno, zaměstnanci i vedení podniku často pracuje mimo své kmenové pracoviště, na což je potřeba dále věnovat pozornost. Podoba struktury podniku je vyobrazena na Obrázek 3 – Struktura podniku.

7.2 Potřeby podniku

Vlivem rozrůstání se podniku a migrací části zaměstnanců dříve ze Sídla 1, nově do Sídla 2, vzniká potřeba tyto vzdálená místa jakýmsi způsobem sjednotit. Zejména po stránce předávání si důležitých dat a informací. Přeci jen není ekonomicky ani časově správné řešit

tuto situaci tak, že budou přejíždět z jednoho místa do druhého. Občas jsou situace, kdy je toto řešení samozřejmě nevyhnutelné. Při těch ostatních je však dobrou volbou tento proces přejíždění eliminovat.

Jednou z nabízejících se variant, jak zajistit podniku společnou komunikaci a předávání si důležitých dat a informací, je vytvoření společného úložiště. V dnešní době je zřejmě pro jakýkoliv podnik menší i větší velikosti vhodné mít prostředky pro archivaci, či zpracovávání dat. Možnosti jsou dnes všelijaké. Dalo by se například, pronajmou cloudové úložiště u jiné firmy, která tuto službu nabízí. Přístup k datům by byl tak neomezený. Datová centra bývají často velmi dobře zabezpečená proti všem možným hrozbám. Zálohu dat provádějí automaticky. Kapacita je teoreticky neomezená a vše už pak jen záleží na dohodnuté ceně, kterou je ochoten podnik do datového centra investovat. Dokonce už i u založení firemního emailu, je často možnost využívání cloudových služeb nabízena.

Možnost je samozřejmě také pracovat stále v dobách minulých a vše skladovat v papírové podobě. Skladovat však tak obrovský počet dat, faktur, projektových dokumentací a například i smluv v tištěné papírové podobě, je v dnešní době pomalu nad lidské možnosti. Podnik by tak musel mít pronajatý sklad. Ten by musel vhodně zabezpečit proti případnému požáru. Zároveň by musel vymyslet vhodný systém archivace, aby bylo možné zpětně jakákoliv data dohledat. Dalším negativním aspektem pak určitě působí samotná komunikace se zákazníkem. Pokud za ním přijde někdo se šanony papírů, a neustále v nich hledá to správné, co chce zákazníkovi ukázat, rozhodně celá situace na zákazníka nepůsobí tak, jako když nabízející vytáhne malý, třinácti palcový notebook, a vše již v něm má předem připravené na názornou ukázku. A samozřejmě to co nemá připravené, má dále lehce dohledatelné, jelikož je vše na jednom vzdáleném místě přístupném odkudkoli. Má-li dotyčný v dané situaci samozřejmě přístup k internetu.

Komunikace však neprobíhá pouze se zákazníkem, často se musí zaměstnanci dorozumívat i společně. V dnešní vyspělé společnosti plné elektronických zařízení a výpočetní techniky snad není potřeba zmiňovat mobilní telefony. Podnik by tak měl zajistit možnost neomezené komunikace zaměstnanců mezi sebou, zaměstnancem s vedením podniku, a samozřejmě i zaměstnanců se zákazníkem. Pro potřeby sdílení dat pak například firemní email.

8 ANALÝZA POŽADAVKŮ PODNIKU

Tato kapitola se zabývá soupisem dílčích požadavků podniku kladených na realizaci nové IT infrastruktury a informačních systémů. Ta bude sloužit zejména pro ukládání firemních dokumentů, dat a dalších věcí nezbytných k podnikání.

8.1 Požadavky na IT infrastrukturu

Po konzultacích s vedením podniku, a i samotných zaměstnanců, vznikl požadavek na realizaci nové IT infrastruktury podniku. Ta bude později využívat informační systémy ke správě a řízení projektů a jednotlivých dat, či úkoly zaměstnanců. Návrh spočívá zejména v realizaci firemního úložiště. Vedení podniku hned v prvním sezení zamítlo možnost cloudových služeb. Je dbáno na to, aby firemní data nezpracovávala dále jiná společnost. Často se může jednat o citlivá data, které by mohla zneužít jakákoliv konkurenční firma. Zvýšený požadavek je zejména na bezpečnost a vzdálený přístup.

Z konzultací jasně vyplynulo, že podnik chce vlastnit své uložiště i fyzicky a mít nad ním plnou kontrolu. Z toho jednoznačně vyplývá, že se budeme bavit o úložišti dat s možností jednoduchého ukládání, zálohování a přístupu k němu. Tato zařízení jsou povětšinou síťová. V nabídce zůstává zřízení vlastního serveru. Na tom by běžel operační systém, například Linux, a obsluhoval by tento server. Volit by se musel dostatečně výkonný, s dostatečně velkou kapacitou úložiště a možnosti snadného rozšíření. Server pak patřičně nastavit, dle představ podniku. Dále pak existují zařízení, již přímo sestavené pro práci s velkými množství dat, navíc s možností jednoduchého a zabezpečeného přístupu k nim. Systém je již sestavený výrobcem, ke snadné instalaci a implementaci do prostředí, ve kterém má sloužit. Celým názvem Network Attached Storage (NAS). Na trhu existuje spousta výrobců těchto síťových úložišť a serverů. Bude tedy potřeba blíže specifikovat, co podnik vyžaduje.

8.1.1 Rozpočet pro navrhovanou IT infrastrukturu

Po konzultacích s vedením podniku vyplynulo, že navrhovaná síť bude v rozmezí 50 000 až 100 000 Kč. Jelikož dobře sestavené servery, dosahují samy o sobě těchto a vyšších cenových rozmezí, bez dalších periférií, dohodlo se využití technologií NAS serveru, kdy celkové pořízení produktů, by nemělo přesáhnout 100 000 Kč. Nutno je počítat i s dalšími technickými prostředky pro zřízení spolehlivého IT infrastruktury.

8.1.2 Zálohování a bezpečí uložených dat

Pro podnik je velkou snahou docílit vysokého zabezpečení dat. Zvolit tedy vhodné zabezpečení před únikem, či ztrátou dat. Pro tyto účely existují v samotném úložišti zálohovací aplikace. Mimo to bude implementování zabezpečení jednotlivých disků před zničením. K tomu poslouží vhodně zvolené zabezpečení nazývané Redundant Array of Independent Disks (RAID). To bude záviset na zvoleném počtu disků. V případě pořízení dvou pevných disků, bude prováděno zrcadlení. Tedy RAID 1. Podniku bylo dále navrženo využití vzdáleného zálohování dat. Díky toho, že disponuje dvěma vzdálenými pracovišti, neboli sídly, je možné přes internet provádět pravidelné zálohy, z jednoho místa na druhé. To by zabezpečilo například nejhorší možnou variantu, a tou je požár.

8.1.3 Další prvky IT infrastruktury

Základním prvkem firemní infrastruktury se dá považovat již zmíněný NAS server. Ten však není schopen pracovat samostatně. Přesněji řečeno tedy je, ale nebyl by dále možný přístup odkudkoliv. Proto bylo podniku XY dále navrženo, k maximálnímu uspokojení potřeb, celková rekonstrukce sítě. Do podniku bude, nově implementován router s možností zřízení VPN sítě. Tyto routery by bylo vhodné umístit do obou sídel a zajistit tak propojení nazývané site-to-site. Tedy ačkoliv jsou obě sídla vzdálena několik kilometrů, vzniklo by tak bezpečné spojení těchto míst. Zařízení umístěná v jedné z těchto sítí by se tvářila, jako by byla ve společné LAN sítí. VPN síť tedy zajišťuje bezpečnou šifrovanou komunikaci přes nechráněný veřejný internet. To však zabezpečuje pouze přístup k úložišti z jednoho nebo druhého sídla. Zaměstnanci i vedení podniku, však bude často mimo své pracoviště. Proto potřebují přístup do sítě odkudkoliv, kde je možnost připojení k internetu. Tato možnost naštěstí také existuje. Opět se jedná o VPN využívající však Point-to-Point Tunneling Protokolu (PPTP). V podstatě se jedná o vzdálený přístup. Zde bude pro každého zaměstnance vytvořen účet s přihlašovacím jménem a heslem, pod kterým se do VPN sítě bude moci odkudkoliv připojit. Jedním z takových, kdo bude toto připojení využívat nejčastěji, bude pravděpodobně externí účetní, která tak bude mít přístup k informacím potřebným pro svou činnost.

Vzhledem k tomu, že všichni zaměstnanci využívají přenosná zařízení, kterými jsou notebooky či mobilní telefony, bude i připojení k sítí v rámci lokální sítě prováděno bezdrá-

tově. K tomu bude potřeba zrealizovat vhodný AP pro bezdrátovou komunikaci mezi zařízeními. Wi-Fi následně vhodně zabezpečit proti potenciálnímu napadení zvenčí či infiltrování se do infrastruktury.

8.2 Zabezpečení před výpadkem elektrické energie

Častým problémem, se kterým se síťové zařízení, zejména tedy navrhované úložiště NAS potýká, je nečekaný výpadek dodávky elektrické energie. Pokud k takovéto události dojde, často se může poškodit část dat, která byla danou chvíli jakkoliv zpracovávána, či přenášená. Pro tyto situace existují záložní zdroje napájení, známe pod názvem Uninterruptible Power Supply (UPS). Ty zaručí, že v případě výpadku elektrické energie začnou okamžitě napájet připojená zařízení. Tyto zařízení primárně slouží k bezpečnému vypnutí veškerých připojených komponentů po zpracování nezbytných operací, které na zařízeních byly spuštěny. Pokud je však záložní zdroj UPS dobře dimenzován, dokáže napájet zařízení při výpadku v řádech desítek minut, někdy i hodin. Často jsou UPS připojena přímo do lokální sítě, aby připojeným zařízením předala informaci o výpadku dodávky elektrické energie. Ty pak bezpečně ukončení svou činnost. Komunikace probíhá povětšinou přes rozhraní USB, anebo kroucenou dvojlinkou s koncovkou RJ45.

Vhodně dimenzované zařízení UPS bude do navrhovaného systému implementováno k zajištění bezpečné činnosti zejména NAS serveru.

8.3 Umístění úložiště

Samotné úložiště se všemi komponenty bude po dohodě fyzicky umístěno v Sídle 2. Mimo jiné existuje mnoho variant provedení NAS serveru, například v provedení Tower, které se umisťuje na polici či stůl. Toto provedení je vhodné spíše pro domácnost. Pro podnikové prostředí jsou často vhodnější Racková provedení. Ty umožňují vložení a připevnění do 19“ skříně. Stejně tak jsou ve stejném duchu vyráběná i UPS. Když už tedy má být takovýto systém někde fyzicky umístěn, je vhodné mít všechny tyto potřebné komponenty v jedné uzavřené nebo i uzamčené skříni. Mimo výše zmíněný hardware lze do skříně samozřejmě vložit router, případně switch a další komponenty.

Racková skříň navíc umožňuje snadnější propojení jednotlivých komponentů, s možnosti schování kabeláže do vzhledné podoby. Jednou z výhod je také kontrola nad chlazením celého systému. Pokud je zřejmé, že se zařízení nadměrně zahřívají, dá se často přímo do skříně implementovat ventilátor či dokonce klimatizace. Lépe vybavené Rackové skříně,

spíše pro datová centra a velké serverovny, dokonce disponují i hasebním systémem pro případ vznícení některého zařízení a následně rychlého uhašení.

8.4 Dodatečná zabezpečení

Mimo zmiňovanou skutečnost, že může občas dojít k výpadku elektrické energie, jsou zde i další hrozby související s bezpečným provozováním firemní IT infrastruktury. Zejména je důležité myslet na to, že celkové zabezpečení jakéhokoliv systému v jakémkoliv oboru se odvíjí od nejslabšího prvku v systému. Když už tedy bude provozováno co nejlépe zabezpečené firemní úložiště, bude potřeba zabezpečit i jednotlivá zařízení na kterých zaměstnanci pracují a budou se do sítě připojovat. Přece jen může být kdykoliv, jakékoliv zařízení ztraceno, či dokonce odcizeno. Pokud by tedy takovéto nezabezpečené zařízení dostal do rukou nesprávný člověk, který by se dostal až k citlivým firemním informacím, mohl by je zneužít. Je tedy kladen důraz, i na takovéto hrozby se připravit. Ačkoliv jejich pravděpodobnost vzniku není příliš vysoká, dopad by pro podnik mohl byt až zničující.

8.4.1 Zabezpečení firemních zařízení

Jednou z nejjednodušších, nejlevnějších a zároveň nejpraktičtějších metod jak zabezpečit obsah počítačů, notebooků či mobilních telefonů je tyto zařízení zašifrovat. Obsluha sice bude muset pravidelně, například při startu zařízení, zadávat například heslo, nebo se jinak autentizovat. Na druhou stranu takto zabezpečené zařízení, se při ztrátě nebo odcizení stává z hlediska obsahu dat bezcenné. Jedinou reálnou možností pro pachatele, je formátování disků a přeinstalování systému. V tomto případě již budou veškerá citlivá data ztracena. Není dokonce potřeba šifrovat ani celý obsah disku. Pokud se dohodne, že se bude pro firemní účely využívat například jen jeden z oddílu logicky rozděleného disku, lze zašifrovat pouze tento oddíl a autentizace by probíhala pouze při přístupu k těmto datům. Šifrovat lze i již zmíněné mobilní telefony.

Další nedílnou součástí veškerých zařízení je používání prověřených a aktuálních antivirových programů. Ty by z velké části měly ochránit zařízení před útoky hackerů. Pokud by takto nezabezpečené a napadané zařízení vstoupilo do sítě, mohlo by poškodit celou infrastrukturu a způsobit velké škody.

8.4.2 Přístup k datům

Jelikož má každý zaměstnanec ve firmě svou roli, používá tak pro svou práci jen omezenou část dat. Není tedy potřeba, aby měl přístup k veškerým informacím. Tímto se za spolupráce s vedením podniku, bude moci sestavit hierarchie jednotlivých uživatelských účtů vytvořených na NAS serveru. Takto strukturovaný systém vede k větší bezpečnosti a utajenosti firemních dat před potenciálními „škůdci“. Ačkoliv je odcizení zařízení za účelem vytěžení informací z něho málo pravděpodobně, více pravděpodobné, je již odcizení a použití citlivých dat zaměstnancem z vlastních řad. Může se například jednat o nespokojeného zaměstnance ve výpovědní lhůtě. Také může být zmanipulován konkurenční firmou a informace o vlastní firmě například prodat. Scénářů může být hodně. Proto je vhodné v každém případě uvažovat o omezování přístupu k jednotlivým citlivým údajům.

8.4.3 Přístup do sítě

Přístup k samotnému NAS serveru, kde budou dostupná veškerá data, předchází připojení se do lokální sítě. Tento přístup musí být z hlediska bezpečnosti také omezován a musí se nad ním dohlížet. Dostane-li nezvaný host přístup do lokální sítě, může se pak snadno pokusit dostat i do úložiště nebo jiného zařízení v síti. Existuje několik možností jak přístup zabezpečit. U bezdrátového připojení pomocí Wi-Fi v Sídle 2 či 1, bude nejvíce záležet na nastavení samotného AP s dostatečným šifrováním a vytvořením dostatečně dlouhého a složitého klíče. O provozování VPN se budou starat routery. I zde bude nutno nastavit jasná pravidla i pro firewally.

9 ANALÝZA RIZIK IT INFRASTRUKTŮRY

Kapitola zabývající se analyzováním rizik IT infrastruktury, bude nahlížet na riziko spojené s hrozbou, kterou je výpadek této infrastruktury. Budou se tedy hledat příčiny těchto událostí, ve snaze najít poté vhodné řešení k minimalizování případných ztrát, či samotných vzniků negativních událostí.

9.1 Analýza počítačové sítě pomocí FTA

Pro implementaci analýzy FTA do problematiky počítačové sítě je důležité vědět, v jakém rozsahu bude řešena. Pro tuto práci je vybrána problematiku výpadku počítačové sítě jako takové. Onym nežádoucím stavem je tedy **výpadek počítačové sítě,** neboli IT infrastruktury. Postupným vytvářením diagramu se zjišťuje, co výpadku může předcházet a dojde se až k samotným jednotlivým událostem, které výpadek mohou zapříčinit. Strom poruch je vyobrazen v příloze P II.: FTA Strom poruch.

9.2 Vyhodnocení analýzy

Touto analýzou, ve které byl řešen výpadek PC sítě, bylo dosaženo nalezení mnoha událostí, které by mohly vést k samotnému výpadku IT infrastruktury. Některé události byly již dále nerozvíjené, jakým způsobem k nim došlo. Jelikož pro naši potřebu nejsou potřeba znát další detaily. První jednoznačnou události vedoucí k výpadku PC sítě, je mimo jiné výpadek elektřiny. Ta může vzniknout odpojením napájecího kabelu k serveru (A). Proti tomu se dá bránit například uzamčením prvku do samostatné skříně či místnosti.

Druhou událostí, je výpadek napájení jednoho ze síťových prvků (Switche, HUB, apod.). Ten může vést k výpadku jen části sítě, nebo i dokonce celé sítě (B). Opět je vhodné omezit přístup k těmto zařízením.

Jednoznačně za přerušením dodávky elektrické energie, stojí porucha vlivem počasí (C), rekonstrukce vedení rozvodné sítě (D), či vyhozený jistič (E) z jakéhokoliv důvodu. Tyto událostí jsou většinou nepředvídatelné a těžce zamezitelné. Ztráty se však dají eliminovat zřízením vlastního záložního zdroje napájení. Ať už myšleno UPS nebo záložní generátor.

Netrápí nás však jen výpadek elektřiny, ale také i selhání samotné systému. K přerušení spojení může vést samotný výpadek serveru (N). Ve spojení s chybou v komunikaci, pak vznikají události, jako je přerušený drát či optický kabel (K). Chybná adresace (L), nebo

zarušení signálu (M). Selhání systému také vede k špatnému nastavení sítě (F), nebo kybernetický útok (G). Všechny výše zmíněné, musí proti vzniku zabezpečit samotný správce sítě. Jsou tedy vyžadovány odborné znalosti v oblasti IT, aby byl na tyto události dostatečně připraven a předcházel jim.

V poslední řadě se může stát, že selže přenos dat. Ten vlivem pomalého přenosu může vzniknout například nedostatečným pokrytím bezdrátové sítě, tedy velké vzdálenosti Wi-Fi vysílače a přijímače (H), nebo přetížením sítě vlivem připojení mnoha uživatelů (O), či stahováním objemných dat (P). Přenos dat také ovlivní špatný signál opět velké vzdálenosti Wi-Fi (I), anebo vlivem počasí, tedy povětrnostními podmínkami (J). Opět je vznik těchto situací často nahodilý a obtížně předvídatelný. Výsledky se opět odráží na zkušenostech a znalostech správce sítě.

10 ANALÝZA SOUČASNÉHO STAVU INFRASTRUKTŮRY A INFORMAČNÍHO SYSTÉMU

Kapitola popisuje, jak je na tom podnik s dosavadní IT infrastrukturou, v době před realizací. Jaké využívá zařízení. Jak komunikují zaměstnanci, či jak probíhá archivace dat.

10.1 Současný stav zařízení v podniku

Každý zaměstnanec disponuje alespoň dvěma firemními přenosnými výpočetními zařízeními, neboli notebookem a chytrým mobilním telefonem. V Sídle 1 je mimo jiné k dispozici stolní počítač pro asistentku ředitele. Ta tedy využívá jak přenosný, tak stolní počítač a mobilní telefon. Navíc se v onom sídle nachází tiskárna připojená k lokální síti a plotr, který je rovněž síťově připojitelný. Prokurista společně s ředitelem vlastní notebooky a mobilní zařízení.

Sídlo 2 disponuje taktéž síťovou tiskárnou a plotrem. Plotr zejména pro tisk výkresů k projektům. Šestice zaměstnanců, stále obývající tyto prostory, opět ke své činnosti využívají notebooky a mobilní zařízení. Navíc je zde stolní počítač v druhé místnosti.

Na všech zmíněných pracovních stanicích, ačkoliv jsou různých značek, běží nejnovější operační systém Windows 10. Mobilní telefony jsou rovněž od různých výrobců. Nejčastěji se systémem Android. Výjimku tvoří prokurista společně s ředitelem, ti vlastní mobilní telefony iPhone od výrobce Apple s aktuálním operačním systémem iOS. Na všech koncových zařízeních je instalován antivirový program ESET s firemní licencí.

10.2 Připojení k internetu

Vznik nové IT infrastruktury sebou nese i zvýšení nároků na internetové připojení. V obou sídlech je dle smlouvy s poskytovatelem internetového připojení provoz omezen na 24 Mbit/s stahování a 3 Mbit/s nahrávání. To jsou hodnoty, v dnešní době běžně dostačující, pro malou domácnost. V nově navrhovaném systému, by s takovýmto připojením mohl být problém. Zvlášť pak v situacích, kdy dojde ke špičce, a budou se chtít připojit například k úložišti všichni zaměstnanci najednou. V tomto případě by se nedočkal uspokojivého výsledku asi ani jeden z nich. Pokud by se měla provádět i pravidelná záloha dat, mezi jednotlivými sídly, tak ačkoliv by byla prováděna zejména v nočních hodinách, kdy nebudou zařízení využívána, byl by i tento přenos dat velice zdlouhavý. Není tedy jiné řešení, než dojednat s poskytovateli internetového připojení rychlejší přenos dat.

11 NÁVRH VLASTNÍHO ŘEŠENÍ

Po konzultacích s vedením podniku a zjištění dílčích požadavků, bylo možno připravit návrh komponentů. Návrh se skládá ze dvou částí, jedna řeší nedostatky v Sídle 1 a druhá v Sídle 2. Oba tyto návrhy později budou tvořit celek vhodný pro provoz této firemní sítě.

11.1 Základní prvky návrhu IT infrastruktury v Sídle 2

Základním prvkem celého navrhovaného systému bude firemní úložiště. Toto úložiště bude realizováno NAS serverem umístěným v prostorech podniku v Sídle 2. Mimo to je požadavek na přístup k úložišti odkudkoliv, kde je přístup k internetu. S tím tedy úzce souvisí zřízení VPN. K tomu bude potřeba router, který tuto službu bude nabízet. Jednotliví zaměstnanci v prostorách Sídla 2, kteří zde budou pracovat ze svých zařízení, budou připojeni k lokální síti i k internetu pomocí AP, tedy bezdrátově skrze Wi-Fi. V lokální síti se nachází navíc tiskárna a plotr, ty se do sítě připojí pomocí kabelu, k tomu je navíc vhodné do návrhu zanést rozbočovač neboli switch. Mimo tyto základní komponenty budou síťové prvky elektricky zálohovány vhodným záložním zdrojem UPS. Celý tento systém bude uzavřen a uzamčen v Rackové skříni.

Tabulka 3 – Souhrn komponentů návrhu systému v Sídle 2

Komponenty	**Název**	**ks**	**cena bez DPH**
NAS	QNAP TS-873U-RP-8G	1	43 679 Kč
Hard-Disk	WD 8TB Ultrastar DC HC320 SATA HDD	2	14 058 Kč
Router	UBNT EdgeRouter 6P	1	4 923 Kč
Access Point	UBNT UniFi AC Long Range	1	2 202 Kč
Switch	UBNT EdgeSwitch 10XP	1	2 613 Kč
UPS	Eaton 5P 1150i	1	13 079 Kč
Rack	LEXI 19" Rozvaděč 15U	1	2 793 Kč
Cena celkem:			**83 347 Kč**

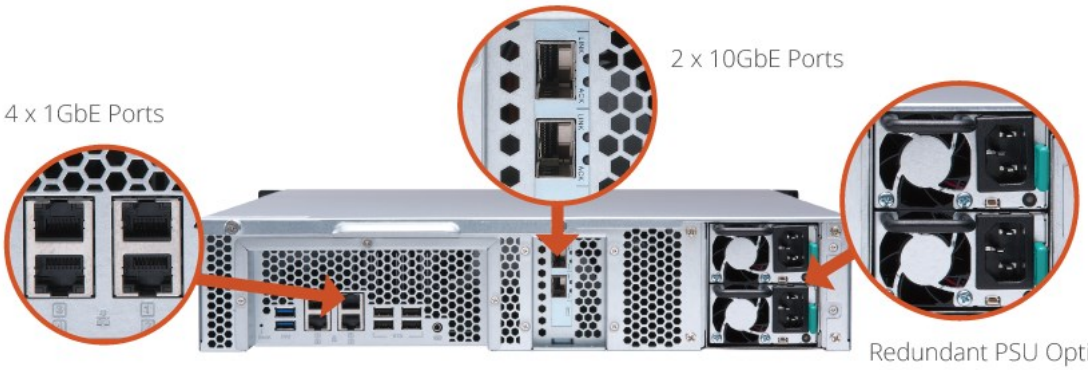
11.1.1 NAS server

Dnešní trhy s elektronikou jsou doslova přesyceny různými komponenty a je opravdu z čeho vybírat. Základním stavebním kamenem byl vhodný výběr NAS serveru. Společnost QNAP je svými produkty proslavena po celém světě. Nabízí různé třídy produktů v provedení Tower i RACK. V tomto navrhovaném systému se budeme poohlížet po RACK provedení, které umožní vložení a uzamčení do Rackové skříně. Je potřeba myslet do budoucna,

kdy se objem dat bude stále zvětšovat a pravděpodobně i požadavky podniku se budou v průběhu času měnit, měly by se komponenty lehce předimenzovat. Vhodným kandidátem vzešel model TS-873U-RP s 8 GB RAM pamětí, která v případě potřeby, lze dále rozšířit až na 64 GB.

Obrázek 4 – QNAP 873U-RP-8G_čelo

Toto zařízení se řadí samotnou společností k vyšší střední třídě. Je vybaveno čtyřjádrovým procesorem AMD řady R. Jak už bylo zmíněno, lze rozšířit až na 64 GB DDR4 RAM. Velkou výhodou je také to, že je vybaven osmi kazetami pro harddisky 2,5“ s redukcí a běžně 3,5“ HDD SATA. Disky samozřejmě nejsou součástí. NAS mimo jiné umožňuje řadu RAID zabezpečení disků. Označení RP v názvu znamená to, že je server vybaven redundantními napájecími zdroji s možností rychlé výměny za nový. Dva zdroje jsou výhodou. Jeden bude zapojen do navrhované UPS a druhý přímo do silové sítě. Ačkoliv samotné UPS dokáže generovat vyhlazené výstupní napětí bez špiček, což přispívá stabilnějšímu provozu, často jsou tyto zařízení označována za nejporuchovější. Proto je v případě výpadku UPS napájeno i z klasické zásuvky na 230V. Montáž do Rackové skříně zabere 2U jednotky.



Obrázek 5 - QNAP 873U-RP-8G_záda

Mimo jiné je NAS vybavena čtveřicí gigabitových portů. Lze tedy do routeru či switche připojit všechny čtyři a zajistit tak maximální možnou rychlost komunikace až 4 Gbit/s.

Do budoucna s možností využití dokonce optických kabelů. Pro tyto kabely je zde síťová karta se dvěma 10 Gbit/s porty. Mimo dále může NAS komunikovat s dalšími externími zařízeními přes USB. To je vybaveno 2x USB 3.0 a 4x USB 2.0.

Zařízení je dále vybaveno spolehlivým a uživatelský přívětivým operačním systémem QTS aktuálně ve verzi 4.3. Zde je k dispozici řada aplikaci pro účely firem i domácností. Jednou z velkých výhod tohoto zařízení je konektivita s nejznámějšími operačními systémy operačními systémy Windows®, Mac®, Linux®/UNIX®. Je zde také možnost virtualizace jakéhokoliv systému, přes řadu softwaru. Aplikace pro zálohu o obnovení dat, jsou v tomto zařízení samozřejmostí. Samotný výrobce také klade důraz na vysokou bezpečnost. Dokonce i na samotném NAS, lze využívat zabezpečený přístup přes VPN či proxy server. Pro firmu pak centralizovaná správa emailů a kontaktů bude jistě výhodou. Funkcí má tedy opravdu mnoho a výrobce celý systém neustále vyvíjí. Neposlední výhodou je také alespoň částečné přeložení operačního systému do češtiny.

11.1.2 Hard-Disk

S výběrem vhodného pevného disku do NAS serveru to taky není zdaleka jednoduché, jelikož i zde, je kladen důraz na spolehlivost a vysokou rychlost zápisu i čtení. Dále svou roli hraje i hlučnost, či vyzařovaný tepelný výkon. Pevný disk pro toto zařízení byl volen ve velikosti 3,5“. Zlatou střední cestou pak vzešel disk od výrobce Western Digital nesoucí označení HC320. Kapacita vybraného disku je 8 TB. Rozhraní je SATA 3. Rychlost otáčení disku je 7 200 otáček za minutu. Vyrovnávací paměť Cache o velikosti 256 MB. Tento pevný disk je svými parametry předurčen pro použití v serverech a tedy i úložištích. Vyznačuje se vysokou spolehlivostí a kvalitním zpracováním.

Obrázek 6 - WD 8TB Ultrastar DC HC320 SATA HDD

Do NAS serveru jsou prozatím navrženy dva tyto disky, které budou zrcadleny. Funkce se nazývá tedy RAID 1. V případě selhání jednoho z disků nedojde ke ztrátě dat. Cena v Tabulka 3 – Souhrn komponentů návrhu systému v Sídle 2 zahrnuje oba tyto disky.

11.1.3 Router

Vzhledem tomu, že navrhovaný router bude řídit celý provoz infrastruktury, nelze ani zde sáhnout po jakékoliv variantě. Router musí být rychlý a umožňovat realizaci VPN. V této oblasti existuje ještě větší množina výrobců než v předešlých případech. Funkce routeru jsou dnes také velmi rozsáhlé, čímž je výběr velice náročný. Důraz byl však kladen na to, aby již celá nová síť byla homogenní, tedy tvořena prvky jednoho výrobce. Dalším atributem pro výběr vhodného routeru bylo umístění do Rackové skříně. Vhodným kandidátem se stal nakonec výrobce Ubiquity Networks (UBNT). Od tohoto výrobce pak byl vybrán produkt EdgeRouter 6P.

Obrázek 7 - UBNT EdgeRouter 6P

Tento router, disponuje opět do budoucna možností připojení optického kabelu. Mimo to také pěti ethernetovými porty a jedním portem „console“ pro zaběhlejší konfigurátory. Jak uvádí samotný výrobce, USB port je zatím ve vývinu a využití pro externí zařízení přijde s dalšími aktualizacemi firmwaru. Mimo jiné umí router využívat zapínatelnou funkci Power over Ethernet (PoE) pro všech pět ethernetových portů. To znamená, že některé zařízení typu AP může být zároveň napájeno napětím 24 V a proudem 1 A. Každý z ethenertových portů dokáže komunikovat rychlostí 1 Gbit/s. V zařízení tepe čtyř-jádrový procesor. Taktován je na 1 GHz a disponuje pamětí 1 GB RAM typu DDR3. V případě použití montážních lišt zabere v Rackové skříni 1U.

Rozhodujícím faktorem pro výběr tohoto produktu, bylo uživatelské prostředí s operačním systémem EdgeOS. To působí velice přívětivě, snadno se v něm router nastavuje a učí se s ním. Komunita pro správu je již taky velice rozšířená a náročnější operace lze zvládnout i v příkazovém řádku. Výhodou je kompatibilita a jednoduchá správa všech zařízení od tohoto výrobce. Zejména pak software Ubiquiti Network Management System (UNMS). Ten slouží pro dohled nad zařízeními a případnou jednoduchou správu kteréhokoliv síťové prvku podporujícího tento software. Software je k dispozici pro Linuxové distribuce, Android a iOS.

11.1.4 Access Point

Přístupový bod pro tento navrhovaný systém je nedílnou součástí. Jak už bylo zmíněno, je dobré dodržet homogenitu sítě a volit prvky stejného výrobce. Od výrobce UBNT, byl zvolen přístupový bod nazývaný UniFi AC Long Range. AP působí svým vzhledem trochu futuristicky a připomíná Unidentified Flying Object (UFO). Důležité je však to, co má uvnitř. Zařízení podporuje pásma 2,4 a 5 GHz. Disponuje maximální rychlostí až 1 317 Mbit/s. Velkou výhodou, jsou uvnitř zakomponované tři antény pro 2,4 GHz pásmo. Využívá tedy technologie 3x3 MIMO. Pro pásmo 5 GHz pak antény dvě, se kterými lze využívat 2x2 MIMO technologii.

Obrázek 8 - UBNT UniFi AC Long Range

Samotné AP je napájeno pasivním PoE 24V přes ethenetový kabel. Nastavení AP je také velice jednoduché. Provádí se přes grafické rozhraní nazývané UniFi Controller. Mimo to, že lze vytvořit účet hosta, lze také vytvořit více SSID s různými typy zabezpečení. Poté například i dle SSID omezovat provoz. Lze také sledovat připojené klienty a jejich provoz po síti. Montáž tohoto AP je výhradně do vnitřních prostor a lze umístit jak na stěnu, tak i na strop kde zmíněné UFO svým designem vážně připomíná.

11.1.5 Switch

Pro rozšíření lokální sítě se nabízí použití switche. Toto zařízení rozšiřuje počet portů pro lokální síť. Zvolený produkt byl opět od stejného výrobce UBNT. Ten nese označení EdgeSwitch 10XP. Tento switch disponuje osmi ethernetovými 1 Gbit/s porty a dvěma porty pro připojení optického kabelu do budoucna. Na všech osmi ethenertových portech lze povolit PoE napájení 24V pro připojená zařízení. Pro správu zařízení lze použít již zmíněný software UNMS který poskytuje vzdálenou konfiguraci či dohled nad síti. Switch lze instalovat jak na stěnu tak za pomocí montažní sady i do Racku.

Obrázek 9 - UBNT EdgeSwitch 10XP

Switch bude používán pro připojení síťové tiskárny a plotru. Případně pak samotného NAS serveru či jiných zařízení. Ačkoliv působí minimalisticky, pro potřeby podniku by měl prozatím dostačovat. Vyznačuje se zejména nízkou spotřebou elektrické energie pohybující se okolo 8W. Montážní sada je stejná jako u routeru a zabere 1U.

11.1.6 UPS

Záložní zdroj pro spolehlivý provoz NAS serveru zejména při výpadku elektrické energie je v dobře navrženém systému nedílnou součástí. Opět existuje na trhu spousta výrobců a druhů UPS. Liší se zejména typologií napájení, kapacitou baterií a komunikačním rozhraním s dalšími zařízeními. Pro tento navrhovaný systém byl zvolen výrobce Eaton. Z jeho modelových řad byl nakonec zvolen model s označením 5P 1150i. Tento model se opět vyrábí ve dvou variantách. Tedy Tower a Rack. Pro náš systém bylo zvoleno Rackové provedení.

Obrázek 10 - Eaton 5P 1150i_čelo

Typologie této UPS se nazývá Interaktivní vysokofrekvenční. Zařízení lze zatížit až na 1150/770 VA/W. Vstupní napětí, se kterým dokáže pracovat, se nachází v rozmezí 160-294 V, bez nutnosti použít baterie. Z tohoto vstupního napětí dokáže generovat výstupní nastavitelné napětí 200 V, 208 V, 220 V, 230 V nebo až dokonce 240 V. V zařízení se nacházejí čtyři baterie.

Obrázek 11 - Eaton 5P 1150i_záda

Vstupní napájení se z běžné zásuvky připojuje do vstupního konektoru označeného jako IEC-320-C14. Pro napájení zařízení má UPS celkově 6 výstupních zásuvek IEC-320-C13. Tyto zásuvky jsou rozděleny do dvou skupin, z nichž každá dokáže dodávat

proud 10 A. Při maximálním zatížení dokáže zařízení pracovat spolehlivě po dobu čtyř minut. Zařízení je však předimenzováno, aby zajistilo provoz NAS serveru po značně delší dobu.

Pro komunikaci s dalšími zařízeními, je zde možnost propojení pomocí sériového portu RS 232, nebo pomocí USB portu. Bohužel však ne současně. K zařízení je dodáván i softwarový balíček, pro snadnou kontrolu nad zařízením. Vložením do Rackové skříně zabere 1U pozici.

11.1.7 RACK

Racková rozvodná skříň pro navrhovaný systém musí být zejména vhodně dimenzovaná, aby se zde vešly veškeré komponenty včetně kabeláže. Existuje celá řada Rackových skříní o různých rozměrech či provedeních. Některé se věší na zeď, jiné se zase pokládají na zem. Šířka je pevně stanová, jelikož se bavíme o 19“ Racku. Počítat se musí zejména s hloubkou, které má naše největší zařízení. UPS má hloubku 509 mm a NAS dokonce 534 mm. Výběr se musí tedy odvíjet od NAS serveru. V úvahu přichází hloubka Rackové skříně alespoň 600 mm.

Dalším parametrem, na který je potřeba myslet, je výška celé skříně. Ta se počítá v jednotkách „U“. Spočítáme-li si jednotlivá „U“ navrhovaných komponentů do Rackové skříně, tedy NAS (2U), routeru (1U), switche (1U) a UPS (1U), jsme na 5U jednotkách. Taková skříň by sice byla dostačující, avšak poněkud malá a těžce by se komponenty instalovaly. Prostor pro kabeláž, by byl velmi stísněný a jednotlivá zařízení by byla velmi blízko u sebe, což by mohlo vést k přehřívání jednotlivých komponent, při vyšším zatížení. Proto je vhodné i tento parametr značně předimenzovat, alespoň na 15U. Neposledním parametrem je samotná nosnost skříně.

Při konzultacích s vedením podniku, se navrhovalo umístění skříně na stěnu. Proto byl navrhován takto strukturovaný RACK. Jelikož i samotné zařízení mají displeje nebo indikační LED, je vhodné volit skříň s prosklenými a průhlednými hlavními dvířky. Zvoleným produktem byl tedy 19“ rozvaděč 15U od výrobce LEXI.

Obrázek 12 - LEXI 19" Rozvaděč 15U

Rozměry této skříně jsou 600x600 mm. Je tvořený za studena válcovanou ocelí tloušťky konstrukčních dílů 2,0 mm a ostatních dílů 1,2 mm. Díly jsou svařované. Celková nosnost této skříně je dimenzovaná na 60 Kg.

11.2 Příslušenství k IT infrastruktuře v Sídle 2

Ačkoliv základní prvky navrhované IT infrastruktury máme navržené, je potřeba myslet i na okolnosti spojenými s těmito produkty. Například UPS je již dodávaná s kolejnicemi pro uchycení do 19“ racku, ovšem takový NAS server ne, a je potřeba tento komponent dokoupit zvlášť. NAS server bude umístěn v Rackové skříni na dostatečně velké a zatížitelné polici. Dalšími potřebnými komponenty pro správné sestavení a upevnění do Rackové skříně jsou montážní sady k routeru a switchi. Ty jsou pro obě tyto zařízení konstruovány stejně.

Tabulka 4 – Příslušenství k návrhu systému v Sídle 2

Příslušenství	**Název**	**ks**	**cena bez DPH**
Patch panel	Datacom Patch panel 19" UTP 24, 1U	1	879 Kč
PDU lišta	DIGITUS 1U hliníkové PDU	1	1 110 Kč
Montážní sady	K routeru/switchi - UBNT ER-RMKIT	2	616 Kč
	K NAS serveru	1	573 Kč
Police	LEXI 19“ 250mm	1	239 Kč
Cena celkem:			**3 417 Kč**

Dalšími prvky, které ačkoliv nejsou úplně důležité, je dobré je pro případ rozšiřování systému ve skříni mít. Mezi takovýto komponent patří Patch panel od výrobce Datacom. Ten umožňuje strukturování kabeláže uvnitř skříně, jakýkoliv ethernetový kabel se zde dovede, jednotlivé dráty se zařežou do patřičných svorkovnic připojených k zásuvkám RJ45, a ty se dále připojí k routeru či switchi. Výhoda je snadnější uspořádání kabeláže, popis jednotlivých kabelů a esteticky přijatelnější provedení v případě rozsáhlých systémů. Panel obsahuje celkem 24 zásuvek pro UTP kabel.

Významným komponentem je dále PDU lišta. Ta se připojí k UPS záložnímu zdroji a dokáže tak napájet další zařízení, skrz tento panel. Lišta se připojuje k UPS pomocí IEC-320-C14 zásuvky. Do lišty se pak další aktivní prvky připojují přes, u nás běžně používanou, zásuvku SCHUKO. Těch má k dispozici osm. Mimo to je lišta navíc vybavená 10 A pojistkou.

Posledním alternativním doplňkem pro jakýkoliv další komponent, či jen odložení si nářadí při servisní práci, je malá police o hloubce 250 mm. Police má nosnost až 40 Kg.

11.3 Návrh IT infrastruktury v Sídle 1

Mimo základní prvky obsažených v návrhu IT infrastruktury v Sídle 2, se dále navrhuje do Sídla 1 zakomponovat nové síťové prvky, aby byla celá síť homogenní a nedocházelo k problémům. Tyto síťové prvky budou sloužit k připojení do VPN sítě a sloužit NAS serveru k zálohování dat, do této lokality. Návrhem a realizací vzdáleného zálohování se již tato práce nezabývá.

Tabulka 5 – Souhrn komponentů k návrhu sytému v Sídle 1

Komponenty	**Název**	**ks**	**cena bez DPH**
Router	UBNT EdgeRouter X SFP	1	1 625 Kč
Access Point	UBNT UniFi AC Long Range	1	2 202 Kč
Cena celkem:			**3 827 Kč**

11.3.1 Router

Jelikož zde není plánována Racková skříň, bude navrhovaný router umístěn pravděpodobně na stole, případně pověšen na zdi. Navrhovaný router je opět od výrobce UBNT označený jako EdgeRouter X SFP. Není sice již tak výkonný jako v Sídle 2, avšak i tak je

pro svou budoucí činnost vhodně dimenzován. Pro případné dotažení optické kabeláže je zde i port pro tento kabel. Pětice ethernetových portů je konstruována na provoz 1 Gbit/s.

Obrázek 13 - UBNT EdgeRouter X SFP

Router je taktován na 880 MHz a řizen je dvou-jádrovým procesorem. Všech pět portů dále umožňují pasivní napájení PoE s 24 V. Pro účely běžného provozu vedení podniku, kdy navíc bude zřízená VPN síť, pro vzdálený přístup do Sídla 2, navíc prováděná vzdálená záloha dat, je plně dostačující.

11.3.2 Access Point

Rozšíření přístupu k internetu a síťovým prvkům pomocí bezdrátové sítě Wi-Fi bude i zde použit stejný přístupový bod jako v Sídle 1. Tedy UBNT UniFi AC Long Range. Ten bude komunikovat, a taktéž napájen, přímo z výše zmíněného routeru přes ethernetový kabel.

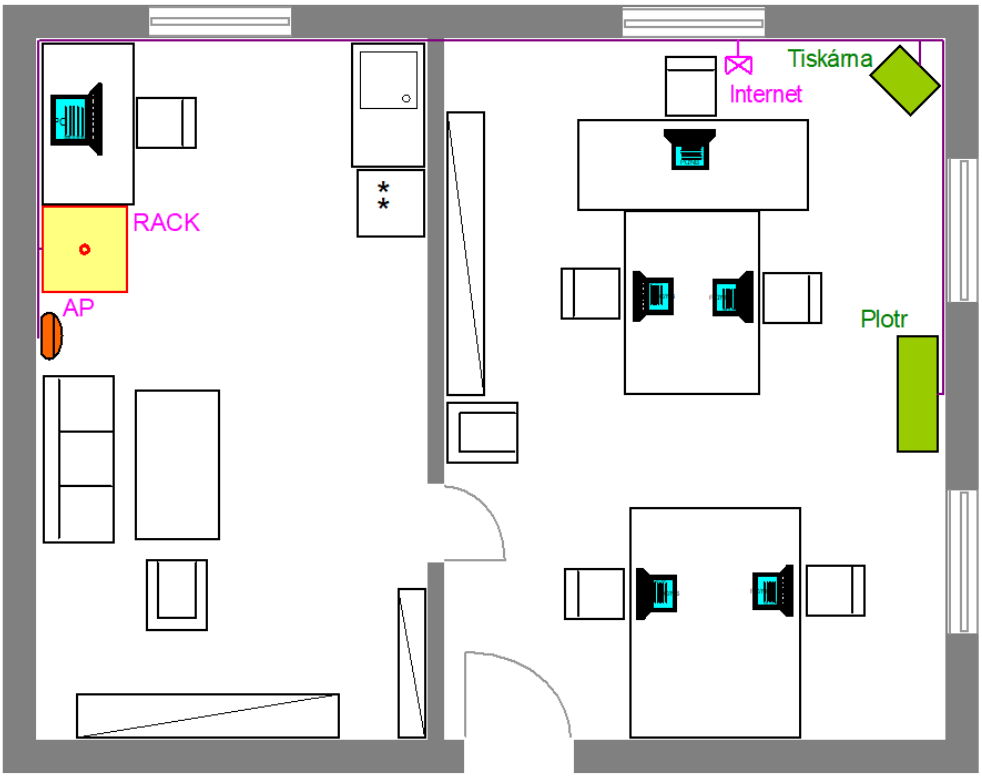
12 REALIZACE IT INFRASTRUKTURY

Jakmile byl navrhovaný systém představen vedení podniku a následně schválen, přišla vlna objednávání jednotlivých komponentů. Poté co veškeré komponenty byly dopravci úspěšně doručeny na Sídlo 2, přišla nejtěžší a časově nejnáročnější část tohoto projektu. Tedy sestavení celého systému a postupným uváděním do provozu.

Realizace IT infrastruktury v této práci, bude spočívat v sestavení Rackové skříně a implementaci jednotlivých komponentů. Ty pak nastaveny a spuštěny do testovacího provozu s tím, že bude zřízen na routeru VPN přístup PPTP. Práce se již tedy nebude zabývat realizací sítě v Sídle 1 a zřízení VPN propojení site-to-site z důvodu rozsáhlosti a časové náročnosti této práce.

12.1 Kompletace sytému

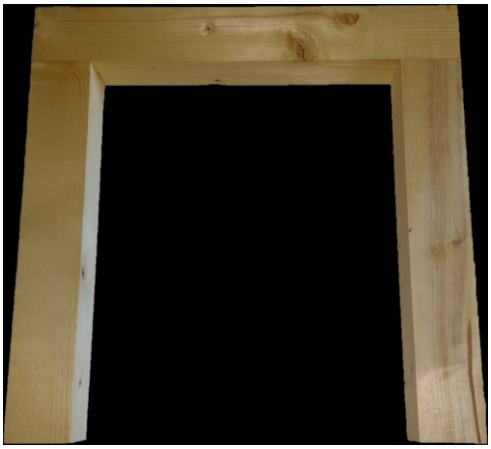
Samotné sestavování systému spočívalo nejdříve v rozbalení Rackové skříně. Ta se pak umístila na své místo a postupně se začalo s kompletací. Pro bližší představu, jak Sídlo 2 s novými prvky bude vypadat, slouží vizualizace tohoto prostředí, tedy Obrázek 14 – Vizualizace Sídla 2.



Obrázek 14 – Vizualizace Sídla 2

12.1.1 Montáž RACK rozvaděče

Racková skříň bude umístěná v levé místnosti, vedle stolu se stolním počítačem. Ten bude do budoucna možno využít, k lokální správě celého systému, v případě havárie, kdy nebude možná vzdálená správa systému. Jelikož je však zakoupený RACK primárně určen k montáži na zeď, stojí prozatím v současné době na svépomocí vytvořeném dřevěném podstavci ve tvaru U s rozměry 600 x 600 x 85 mm.



Obrázek 15 – Podstavec pod RACK

Samotná racková skříň byla samozřejmě již složená. Instalace tedy spočívala především ve zvolení vhodné vzdálenosti vertikálních posuvných lišt k instalaci dalších zařízení.

Obrázek 16 – RACK – v továrním stavu (bez bočnic a dveří)

Díky možnosti vyjmutí předních i bočních dvířek šla práce poměrně snadno. Bylo potřeba naměřit si podle instalovaných komponentů, jaká vzdálenost lišt bude asi ta nejvhodnější. Lišty byly dány v téměř maximální rozestup mezi sebou. Velikost Rackové skříně byla

na hraně s tím, aby se do něj vůbec komponenty vešly. Jednotlivé lišty se tedy umístily do vyměřených vzdáleností tak, aby šla zavřít dvířka a zároveň aby v zadní části zbylo místo pro kabeláž.

12.1.2 Montáž UPS

Jako první zařízení instalované do Rackové skříně, byl záložní zdroj UPS. Zejména z toho důvodu, že pravděpodobně bude vyzařovat nejvíce tepelné energie, tak je vhodné jej umístit co nejvýše. Sestavení spočívalo v umístění kolejnic do skříně a usazení samotné UPS. Spolu se zařízením byly dodány komponenty k připojení a CD se softwarem. V této části se připravila kabeláž pro připojení k NAS a PDU liště. Dále se připojil kabel USB pro budoucí nastavení záložního zdroje.

12.1.3 Montáž NAS serveru

Ještě před samotným umístěním NAS serveru do Rackové skříně, bylo potřeba upevnit připravené pevné disky do kazet nacházejících se v NAS serveru.

Obrázek 17 - NAS – Montáž pevných disků do kazet

Do Rackové skříně se nainstalovala dostatečně dlouhá a zatížitelná police. Na ni se položil NAS server. Police je upevněna jak na zadních tak i na předních vertikálních lištách. Pomocí šroubů je možné i k předním lištám NAS server napevno přišroubovat Umístěný byl o pár pozic pod UPS.

Poté byl NAS osazen dvěma pevnými disky o kapacitě 8 TB. Připravil se ethernetový kabel přibalený výrobcem. Ten se umístil do portu číslo jedna a připravil se pro budoucí připojení k routeru či switchi. Mimo jiné, se zapojil jeden z redundantních zdrojů napřímo do připravené UPS a druhý silový kabel do elektrické zástrčky, hned za Rackovou skříní. Tímto byl NAS server připraven k provozu.

12.1.4 Montáž routeru

Samotnému umístění routeru do Rackové skříně, předcházelo připevnění montážní sady k routeru. Tato sada je univerzální a instalace je velice jednoduchá. V balení montážní sady se nacházely kromě lišty k upevnění i šroubky pro přichycení k routeru. Ten se připevňoval pomocí osmi malých křížových šroubků. Poté, co se připevnila lišta k routeru, bylo možné jej umístit do Rackové skříně. Nyní je naopak zvolené místo pro router ve spodní části skříně. Jelikož veškerá kabeláž je do skříně přivedena ze spodní zadní části, tak aby byla co nejblíže a lépe se s ní pracovalo. Samotný router se tedy umístil do nejnižší pozice. Ze zadní části se přivedl napájecí adaptér, který se připravil pro pozdější spuštění. Prozatím se router s ničím nepropojoval.

12.1.5 Montáž switche a patch panelu

Obdobně jako u routeru, se k samotnému switchi připevnila nejdříve lišta, která umožní montáž do Rackové skříně. Postup byl totožný, jelikož se jedná o stejnou montážní sadu. Zároveň s tím byl připraven k montáži patch panel, ten se jako všechno ostatní rozbalil z krabice, přichystaly se montážní součástky a pokračovalo se v instalaci komponentů do Rackové skříně. Patch panel slouží k možnému pozdějšímu využití pro strukturování kabeláže. V současné době jej nebude potřeba využít. Ke switchi se následně připojil ze zadní strany napájecí adaptér a pokračovalo se v montáži.

12.1.6 Výsledná sestava

Po umístění veškerých komponent do Rackové skříně, mohlo přijít na řadu postupné zapojování a propojování prvků. Na Obrázek 18 – Výsledná sestava lze vidět celkové sestavení Rackové skříně společně s komponenty.

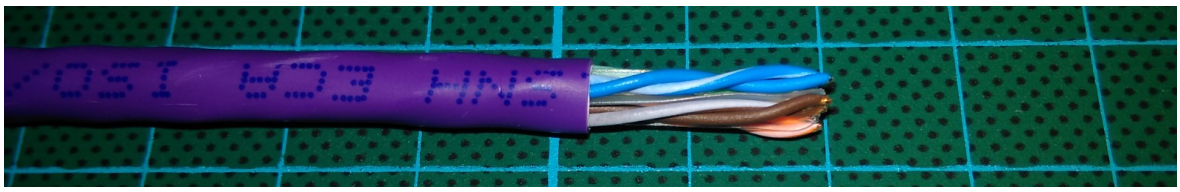
Obrázek 18 – Výsledná sestava

12.2 UTP kabel – krimpování

Ještě před samotným propojováním síťových prvků, bylo potřeba si vytvořit potřebnou kabeláž. K propojování se používá UTP kabel. Pro tento podnik byl zvolen UTP kabel kategorie 6. Ten svými vlastnostmi dokáže pracovat až s frekvencí 250 MHz a je vhodný pro 1 Gbit sítě. Pořízen byl nestíněný kabel v provedení lanko. S tím byl spojený i vhodný výběr konektorů RJ45 pro tento typ vodiče. K připojení konektoru ke kabelu je potřeba speciálních kleští. Mimo to je důležité dodržet správné pořadí barviček při zasouvání do konektoru.

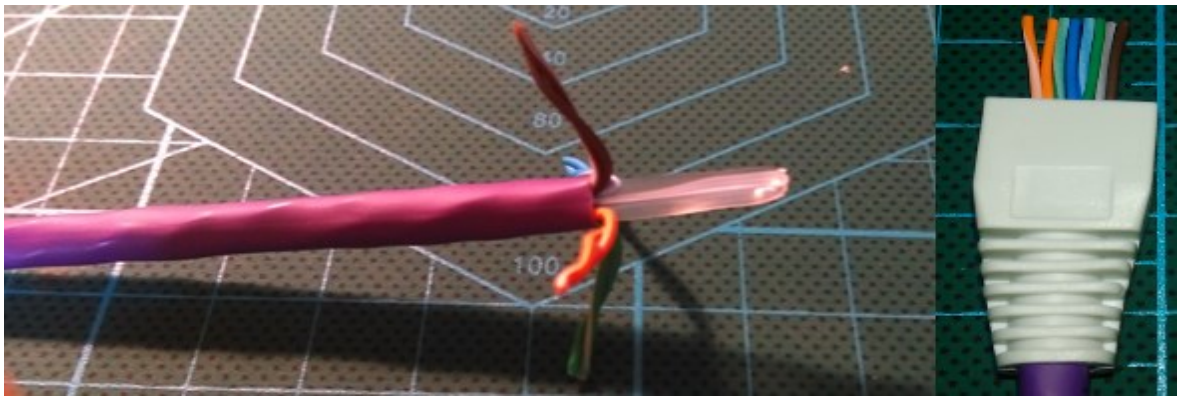
12.2.1 Postup krimpování

Ze všeho nejdříve bylo potřeba si kabel mezi zařízeními odměřit a připravit tak vhodnou délku. Poté kleštěmi ustřihnout. Nyní se jeden konec kabelu odizoloval v délce asi 2 cm. Nejlépe pomocí na to určeného nářadí, tedy pomocí odizolovacích kleští.



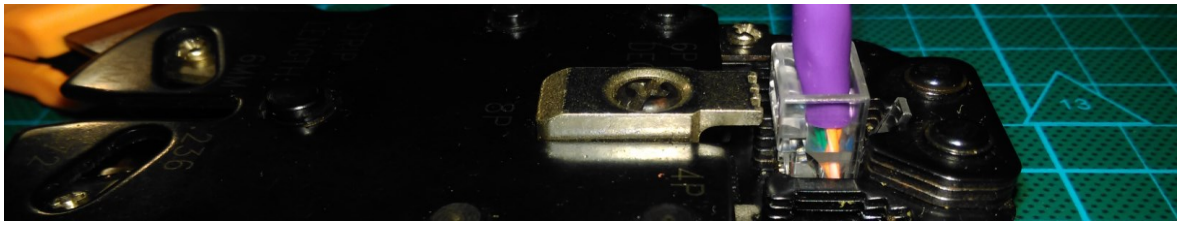
Obrázek 19 - UTP – Odizolování

Poté se čtyři kroucené páry přehnuly do pravého úhlu a zastřihlo se lanko těsně k drátům. Poté se jednotlivé drátky rozdělily a přeskládaly podle barev. Pořadí, dle kterého se uspořádávají, je označované jako T568B. To slouží ke standartní, běžně používaným propojením síťových prvků. Standardně se používá toto pořadí drátů: oranžovo-bílý, oranžový, zeleno-bílý, modrý, modro-bílý, zelený, hnědo-bílý a hnědý. Před vytržením drátů z koncovky se navíc používá i ochrana pro tento konektor. Ta se může na kabel nasunout a připravit ještě před samotným uspořádáváním drátů.



Obrázek 20 – UTP – přeskládání drátů

Následně se konce drátů zarovnaly do stejné roviny. Pak byla vložena správně koncovka RJ45 a znova se ověřilo pořadí barev včetně toho, jsou-li všechny dráty zasunuty až do konce koncovky. Do krimpovacích kleští, se následně konektor vložil a kleště se silně zmáčkly. Tímto došlo jednotlivými zoubky v konektoru k prořízntutí izolace v každém z vodičů. Zároveň se stiskem přimáčkl i konektor k izolaci kabelu, čímž by měli být pevně spojeni.



Obrázek 21 – UTP – krimpování

Následně se jen navlékla ochrana konektoru na konektor a jedna strana kabelu byla hotová. Stejně se postupovalo i s druhým koncem kabelu a i se všemi dalšími kabely.

Obrázek 22 – UTP – Hotový kabel s konektorem RJ45

12.2.2 Kontrola správného zapojení

Po připojení koncovek ke kabelu, je vhodné ještě před samotným zapojováním a používáním kabelu ověřit ještě jednou jeho správnost zapojení. Pro ověření se používá tester, který se připojí na oba konce kabelu. Jedna část zařízení nazývaná Master, pouští postupně do každého vodiče signál, který pak druhá část zařízení zachytí a zobrazí pomocí LED na stupnici 1-8. Stupnice tedy obsahují obě tyto částí testeru a pořadí musí na obou stranách probíhat od jedné do osmi. Pokud se obě stupnice shodují, jsou koncovky kabelu zapojený správně. Pokud je na jedné, či druhé straně zaznamenáno vynechání položky, přehození pořadí, či obrácený směr přepínání LED zobrazení, stala se v zapojování chyba a je potřeba ji najít. V opačném případě by připojena zařízení vzájemně nekomunikovala.

Obrázek 23 – UTP – kontrola krimpování

12.3 Spuštění a nastavení jednotlivých prvků systému

Po kompletaci celého systému přišla druhá část práce, tedy zapojení, spuštění a nastavení systému. Na počátku stálo zprovoznění UPS. Ta bude sloužit k napájení NAS serveru, z PDU lišty i routeru a switche. Poté bylo potřeba zprovoznit samotný router, ke kterému se následně připojil switch a AP. Poté co se uvedla síť do provozu, bylo možno nastavit NAS server.

12.3.1 Zapojení a spuštění UPS

Samotné zapojení UPS bylo velice jednoduché. Přívodní silový kabel se ze zásuvky zpoza Rackové skříně dovedl do vstupu UPS. Poté, jelikož záložní zdroj disponuje dvěma skupinami výstupů, byla jedna zdířka ze skupiny použita pro napájení NAS serveru. Z druhé skupiny zdířek byla napájená PDU lišta, která je samostatně jištěná deseti ampérovou pojistkou. Ta byla instalována do pozice mezi NAS server a patch panel do zadní části, aby byla přístupná a zároveň nepřekážela. Z této PDU lišty byly dále napájeny router a switch.

Obrázek 24 – PDU lišta – napájení routeru a switche

V případě, že by záložní zdroj selhal a běžná silová síť fungovala, je v Rackové skříní k dispozici i běžný prodlužovací kabel s třemi zdířkami a přepěťovou pojistkou. Ta je umístěná ve spodní části Rackové skříně.

Na UPS se při uvádění do provozu pomocí tlačítek a displeje nastavilo požadované výstupní napětí, tedy 230V. Zařízení dále ukazovalo stav baterií, teplotu, či parametry vstupního a výstupního signálu. Dodatečně bylo možno nainstalovat software na počítač, pro vzdálenou kontrolu nad zařízením v případě připojení do sítě. UPS byla následně připojena pomocí rozhraní USB k NAS serveru.

12.3.2 Zapojení síťových komponentů

Přívodní UTP kabel od poskytovatele internetového připojení v objektu byl dotažen z druhé místnosti do Rackové skříně. Zde byl připojen do routeru na první pozici označenou jako eth0. Poté ze zdířky eth1 byl vyveden kabel do AP. Pozice eth2 slouží k propojení se switchem.

Switch je s routerem propojen na poslední pozici označené číslem 8. Dále poskytuje propojení s tiskárnou. Ta je připojena do portu č.1. Následující port slouží k propojení plotru, tedy na pozici č.2. Port označený číslem 7 slouží k připojení samotného NAS serveru. Propojení jsou zobrazena na oObrázek 25 – Síť – propojení síťových komponentů.

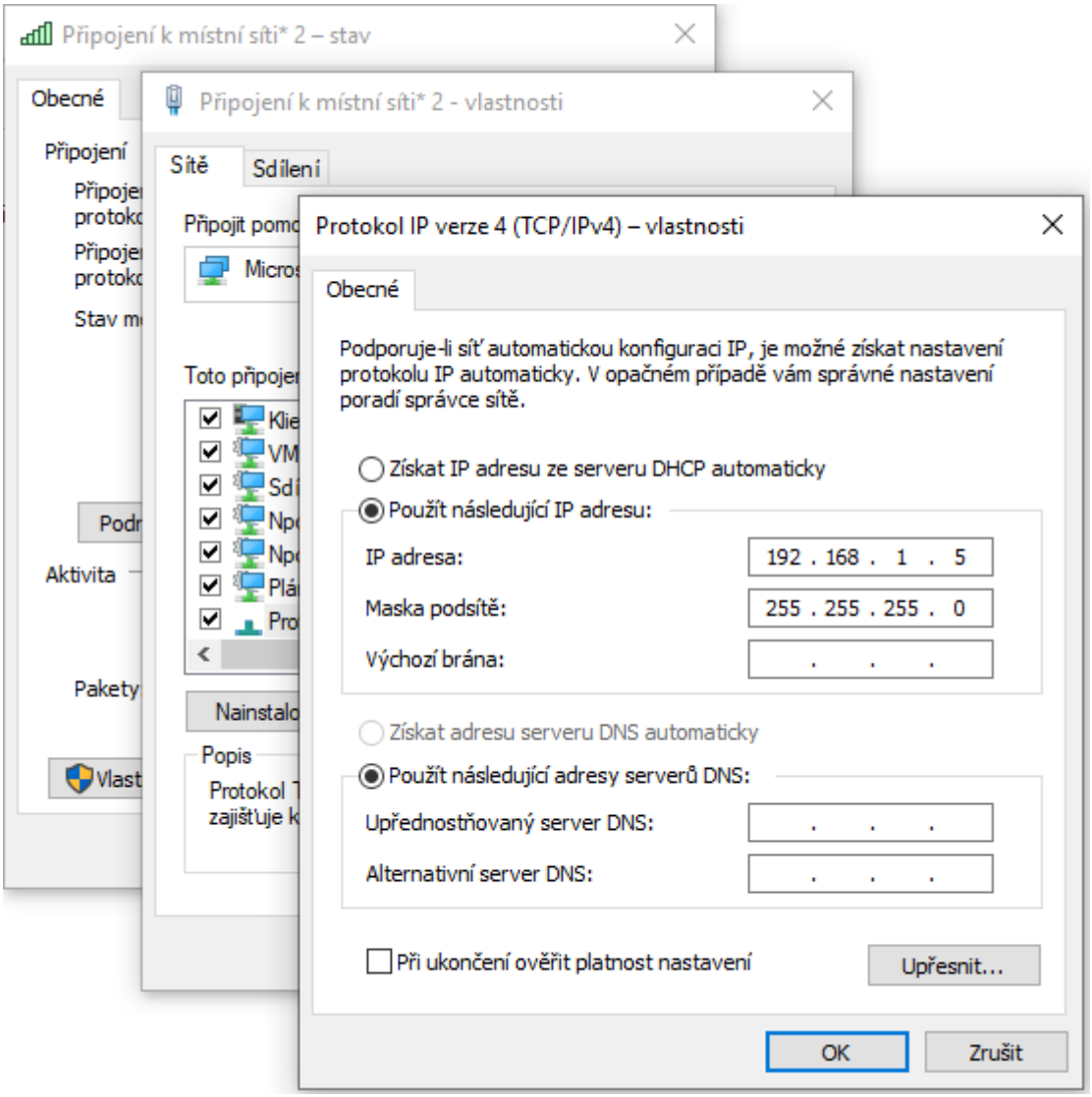
Obrázek 25 – Síť – propojení síťových komponentů

Oba tyto síťové prvky jsou, jak již bylo výše zmíněno, napájeny z UPS.

12.3.3 Nastavení routeru

S poskytovatelem internetového připojení, který i dříve nabízel tuto službu podniku, bylo ujednáno nové připojení. Aby bylo možné nastavit i vzdálený přístup přes VPN, bylo nutno si vyžádat veřejnou IP adresa. Poté co byly tyto údaje získány, mohly se začít nastavovat jednotlivé komponenty.

Nejdříve bylo potřeba nastavit router. Připojil se tedy k němu počítač přes port eth0. Router byl v továrním nastavení a nacházel se dle výrobce na adrese 192.168.1.1. Na počítači bylo ještě nutno nastavit statickou IP adresu na ethernetové zdířce. Například 192.168.1.5 a maska podsítě, která je 255.255.255.0. Následně zmáčknout tlačítko „OK“.

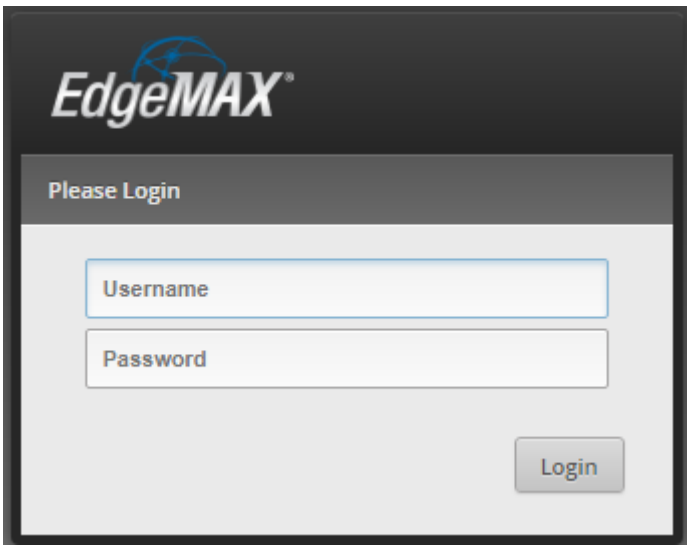


Obrázek 26 – Nastavení PC k propojení s routerem

Po chvilce strpení, kdy se PC s routerem spojil, bylo možno zadat adresu routeru do kteréhokoliv prohlížeče a pokusit se připojit.

Obrázek 27 – Router – Defaultní adresa

Poté co se podařilo navázat s routerem spojení, vyskočilo na obrazovce přihlašovací okénko. Zde se vyplnily výchozí přihlašovací údaje, tedy jméno a heslo.

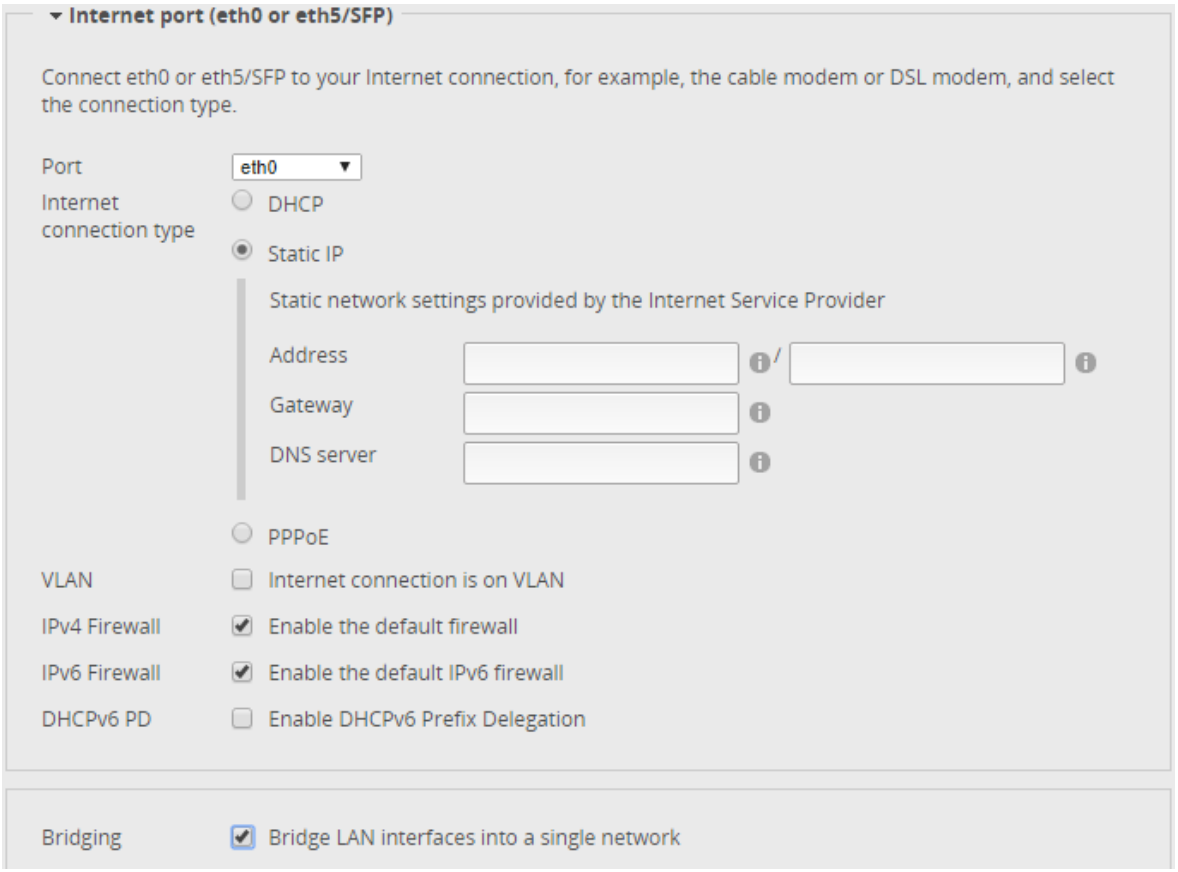


Obrázek 28 – Router – Přihlášení

Po úspěšném přihlášení se do routeru a seznámením se s prostředím, následovalo zadání údajů získaných od poskytovatele internetového připojení. V průvodci nastavení WAN se vybral port, do kterého bude po restartu zařízení, připojen přívodní internetový kabel. V našem případě tedy eth0. Od poskytovatele byla k dispozici statická adresa, maska podsítě, výchozí brána a DNS server.

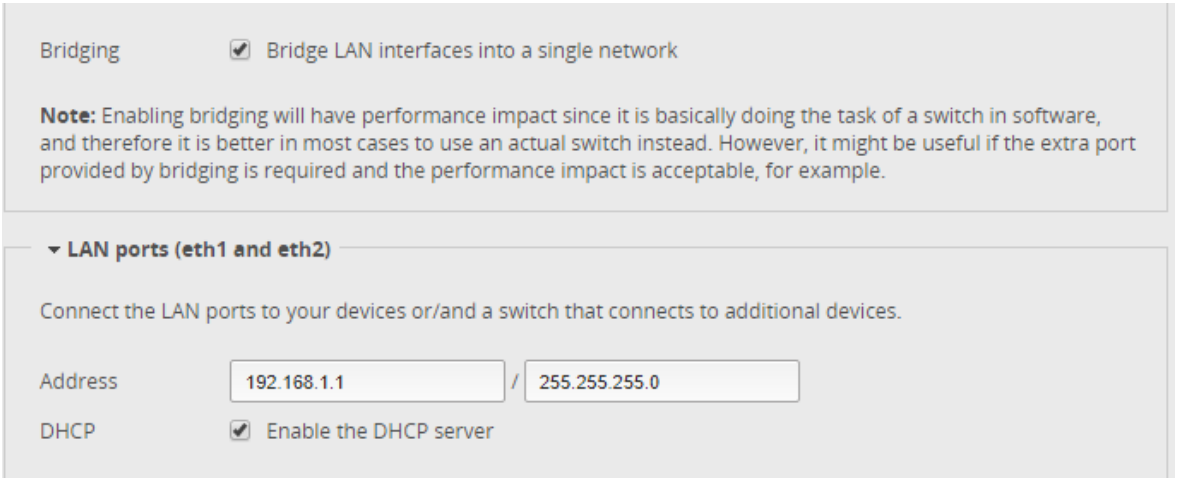
Vzorový příklad:

- IP adresa: 192.168.11.5
- Maska: 255.255.255.0, ta je možno zadat také tzv. prefixem /24
- Výchozí brána: 192.168.11.1
- DNS server 8.8.8.8



Obrázek 29 – Router – Nastavení WAN

Po zadání patřičných údajů do routeru přes webové rozhraní, bylo možno tyto údaje uložit a nechat router restartovat. Ještě předtím však bylo vhodné změnit přihlašovací údaje, na což sám router upozorňoval v průběhu ukládání nového nastavení. Přihlašovací jména a heslo bylo tedy změněno, aby se nikdo nepovolaný do něj nedostal. Povolený byl také „Bridging“, neboli přemostění.



Obrázek 30 – Router – Nastavení LAN

Poté byla v routeru vytvořena podsíť LAN. Například s IP adresou 192.168.1.1. pod kterou bylo možno v lokální síti router nalézt a spravovat.

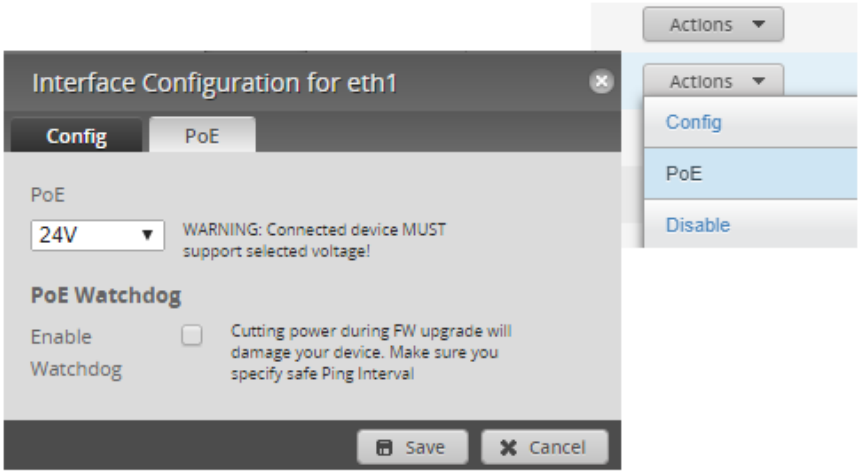
Průvodce si sám nastavil i DHCP server pro námi vytvořenou podsíť. Zde se tedy pro kontrolu v nabídce routeru kliklo na kolonku „Services“ kde byl již vidět vytvořený DHCP server. V našem případě bylo nastavení upraveno pro jasně daný rozsah přidělování IP adres zařízením. Do kolonek „Range Start“ a „Range Stop“ se zapsaly IP adresy rozsahu, podle kterých bude DHCP server přidělovat IP adresy připojeným klientům.

Vzorový příklad:

- DHCP Name: LAN_BR
- Subnet: 192.168.1.1
- Range Start: 192.168.1.50
- Range Stop: 192.168.1.199

Tímto nastavením jsme si upravili nastavení DHCP serveru s názvem „LAN_BR“ pro lokální podsíť 192.168.1.1 a rozsahem až 150 přidělitelných IP adres neboli klientů.

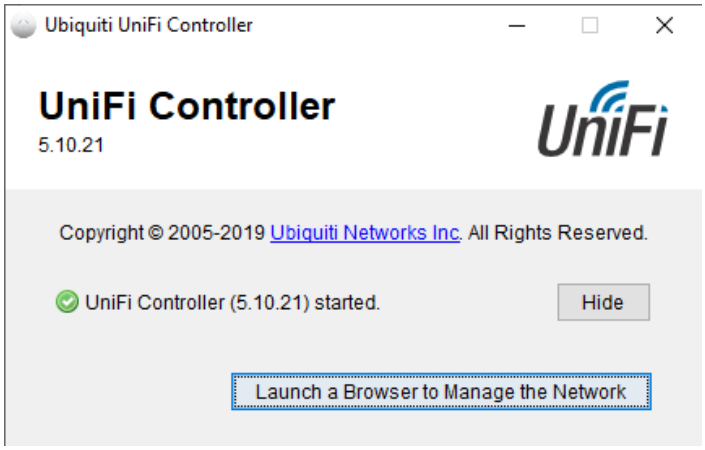
Následovalo povolení PoE napájení pro AP na portu eth1. Díky tomu bylo možno dále spustit a nastavovat AP pro bezdrátové připojení Wi-Fi.



Obrázek 31 – Router – Povolení PoE u eth1 pro AP

12.3.4 Nastavení AP

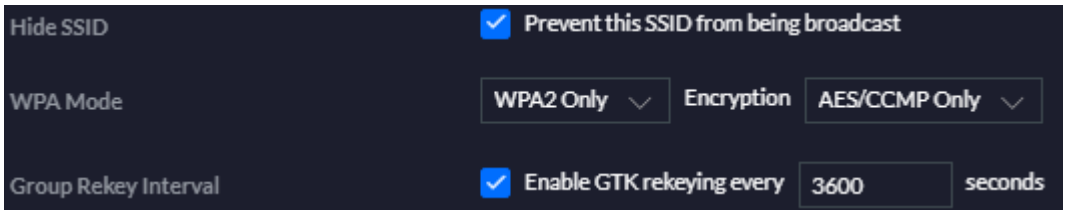
Jak již sám manuál napovídal, bylo nejdříve do počítače nutno nainstalovat software UniFi Controller, který slouží k připojení a správě tohoto zařízení.



Obrázek 32 – AP – UniFi Controller

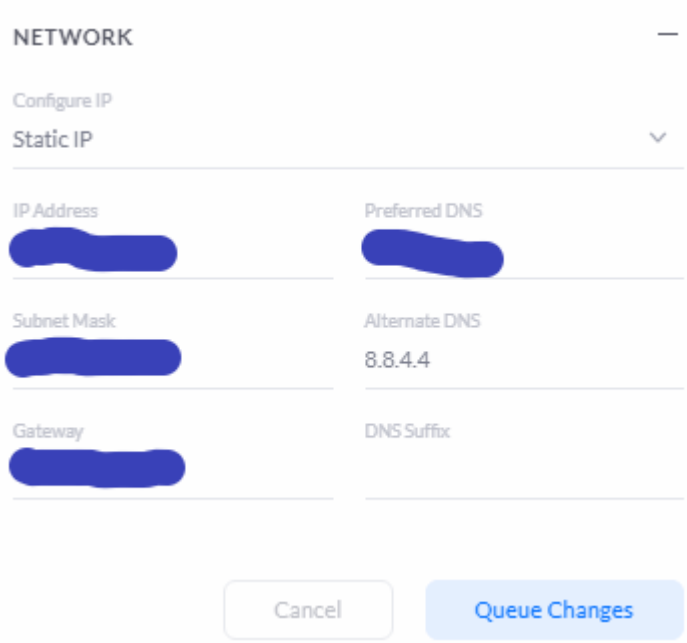
Byl-li dále počítač připojen k sítí, například do routeru pomocí kabelu, bylo následně možné se k AP připojit a provést prvotní nastavení, které sebou neslo například údaje o časovém pásmu. Poté bylo potřeba vytvořit si účet majitele tohoto zařízení pro další správu, nebo pro případné sjednocování dalších zařízení do toho účtu.

Samotné nastavení AP pak probíhalo dle průvodce. Zadal se název SSID, pod kterým lze Wi-Fi síť vyhledat, ten byl poté skryt před náhodnými útočníky. Šrifrování přenášených dat bylo nastaveno na WPA2 a šifrování metodou AES a protokolem CCMP. Před-sdílený klíč k přístupu do bezdrátové sítě byl zvolen vhodně složitý a dostatečně dlouhý.



Obrázek 33 – AP – Nastavení šifrování

Mimo ostatní nastavení byla ještě AP přidělená statická adresa. Ta by podle vzoru byla nastavena například na 192.168.1.2. Tedy jako druhé zařízení v naši podsíti. Adresa zařízení lze samozřejmě zvolit i jiná mimo rozsah DHCP serveru. Maska v tomto případě je 255.255.255.0.

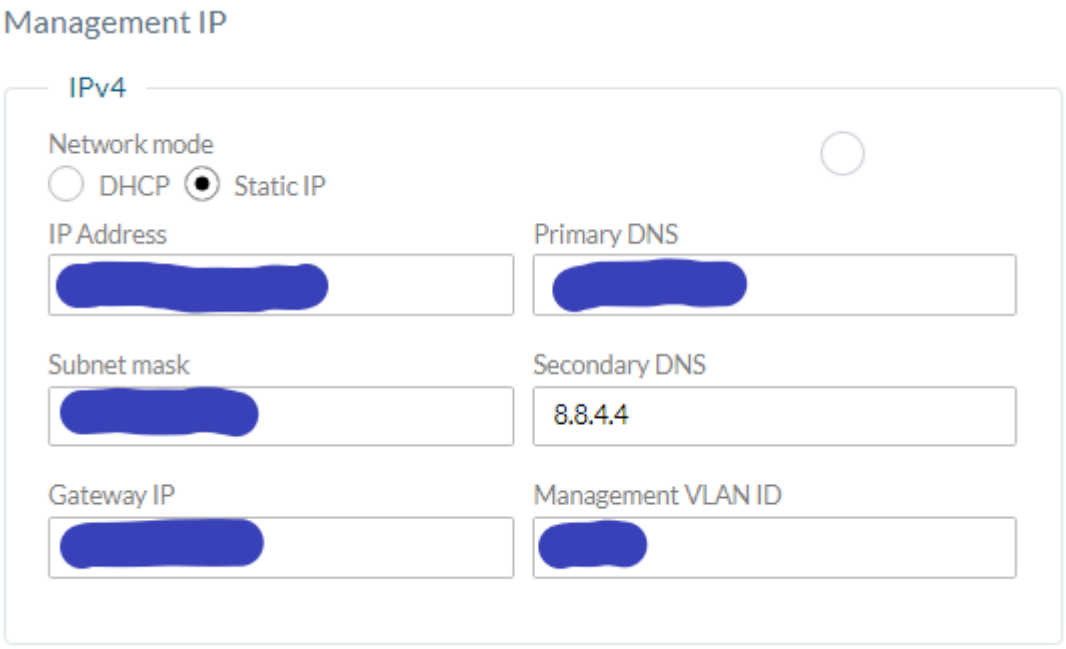


Obrázek 34 – AP – Statická IP

Po uložení nastavení a restartování zařízení bylo možné se již připojovat k bezdrátové síti pomocí Wi-Fi. Grafické rozhraní AP je velice přívětivě a umožňuje spoustu funkcí. Těmi jsou například sledování provozu po sítí připojených klientů. Nebo vytvoření více bezdrátových sítí například pro hosty. Také lze omezovat rychlost připojení pro jednotlivé bezdrátové sítě či klienty a spoustu dalšího

12.3.5 Nastavení switche

Switch byl připojen k routeru do portu eth2. Na switchi vycházel nejblíže port označený číslem 8. Poté bylo možno dostat se do uživatelského rozhraní a nastavení switche. Zde byla vepsána adresa IP. Například 192.168.1.3. Jednalo by se tedy o třetí prvek v sítí. Následně bylo možno zkontrolovat propojení s tiskárnou a plotrem na portech 1 a 2. Obě tiskárny mají také nastavenou statickou IP adresu pro snadnější vyhledání v sítí a navázání spojení například s počítačem. Adresa tiskárny by byla například 192.168.1.10 a adresa plotru 192.168.1.11. Maska v obou případech je 255.255.255.0.



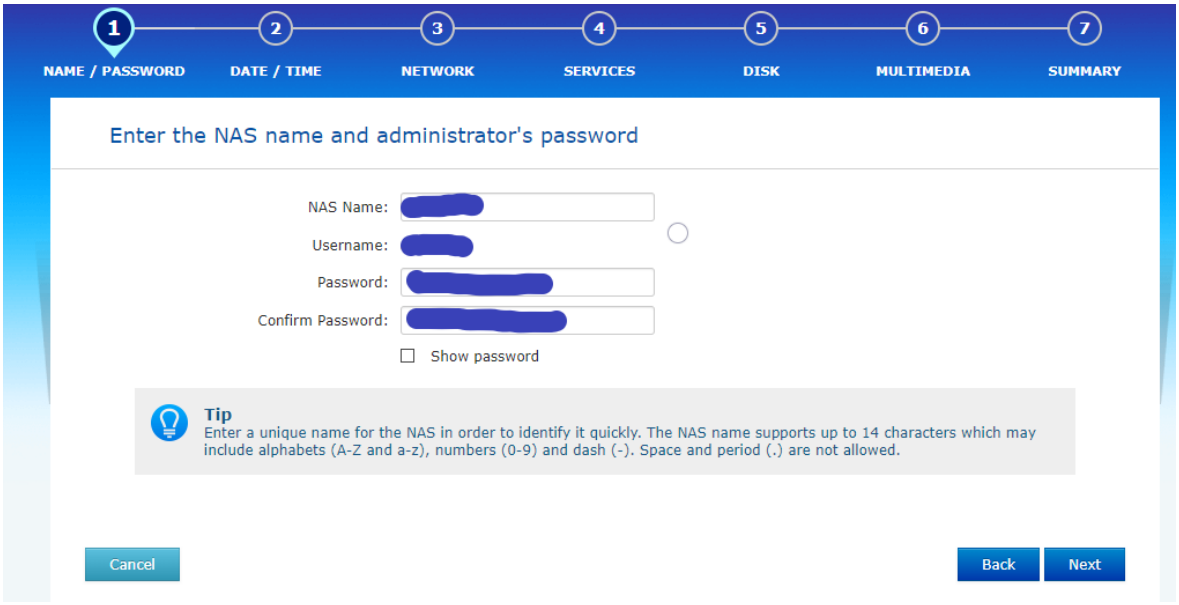
Obrázek 35 – Switch – Statická IP

Tímto jsou v základním, provozu schopném režimu, nastaveny veškeré síťové prvky.

12.3.6 Nastavení a spuštění NAS serveru

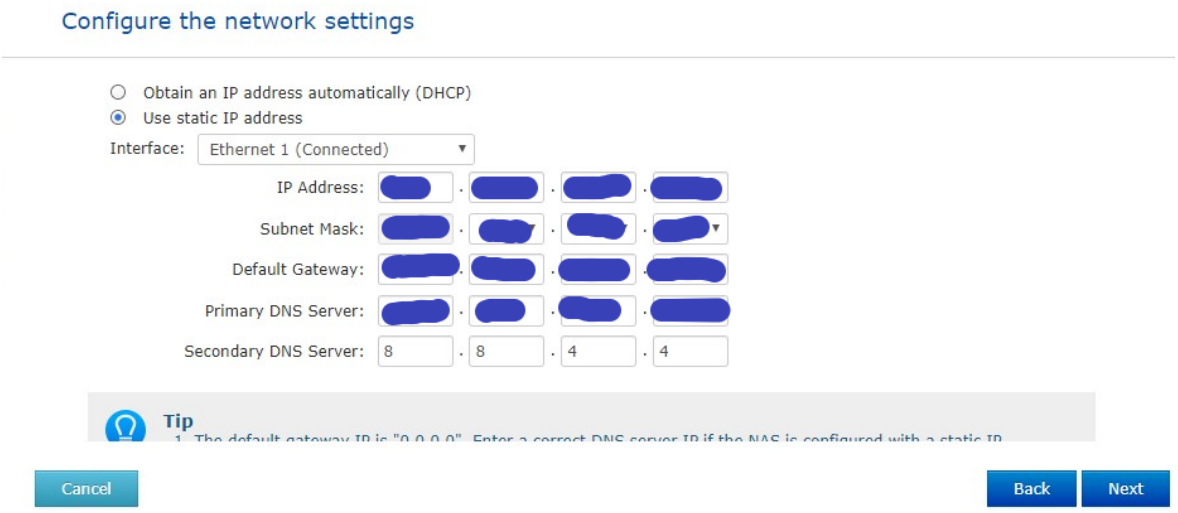
Úspěšné nastavení síťových zařízení a UPS, vedlo dále k nastavování NAS serveru. Ten je napájen, jak již bylo zmíněno, dvěma redundantními zdroji, jak z UPS, tak z běžné silové sítě. Pomocí USB portu bylo propojeno UPS s NAS serverem.

NAS server disponuje čtyřmi ethernetovými porty. Pro potřeby nastavení, byl prozatím propojen první z těchto portů s portem switche na pozici označené číslem 7. Následovalo zapnutí NAS serveru a vyčkání, až se zařízení spustí. Poté přišlo nastavení při prvotním spuštění. Nejdříve bylo požadováno vytvoření administrátorského účtu.



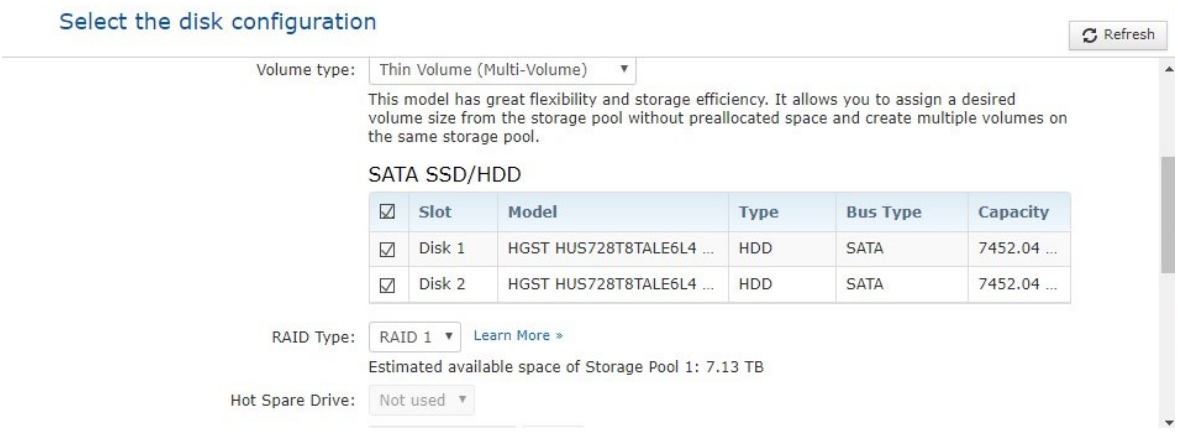
Obrázek 36 – NAS – prvotní spuštění

Pomocí průvodce, se zařízení vhodně nastavovalo pro budoucí používání. Vybralo se časové pásmo, kde bude NAS používán, datum a čas. U třetí části nastavení „Network“ byla zadána statická IP adresa tohoto ethernetového portu. V našem vzorovém příkladu, by to bylo například 192.168.1.5 s maskou 255.255.255.0.



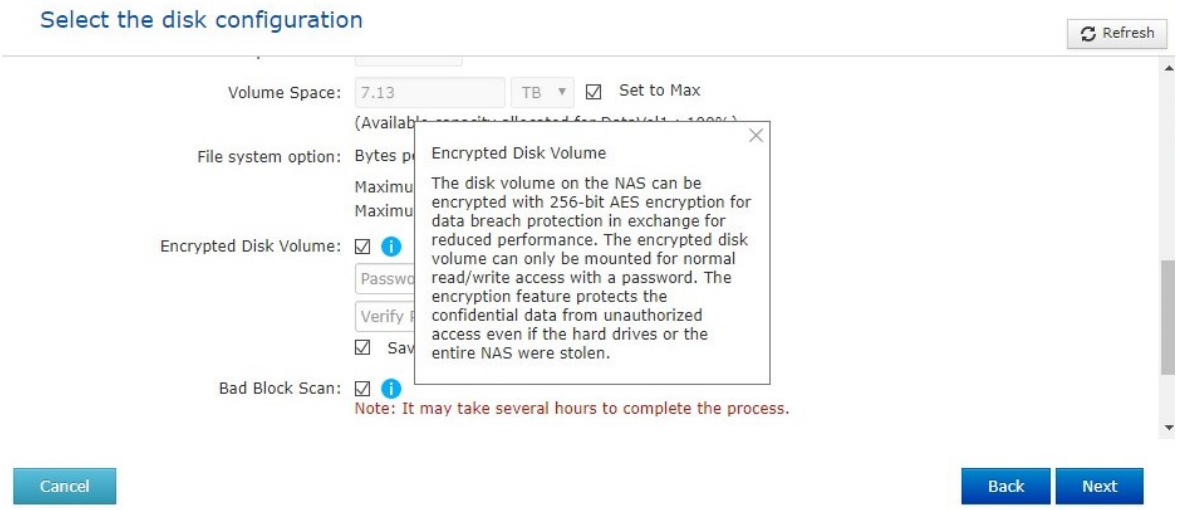
Obrázek 37 – NAS – nastavení statické IP

Pokračováním dále v průvodci se vyskytl dotaz, jak chceme disky zabezpečit, respektive data v nich, proti nechtěné ztrátě. Jelikož jsou prozatím k dispozici pouze dva disky, byl vybrán RAID 1. To znamená zrcadlení disků. To co je na jednom, je tedy i na druhém disku.



Obrázek 38 – NAS – Nastavení RAID 1

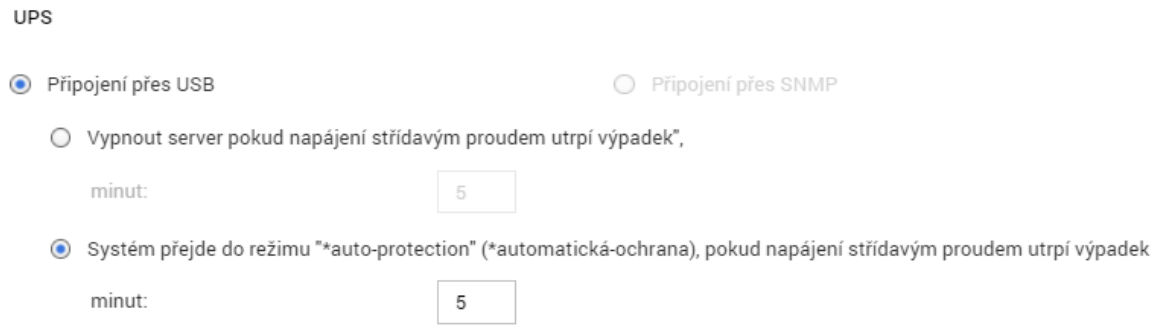
V této části průvodce bylo dále nastaveno šifrování dat na disku. Zvolená metoda byla AES s 256 bitovým klíčem. Vyšší typ zabezpečení prozatím NAS nepodporuje.



Obrázek 39 – NAS – Šifrování disků

Tímto bylo základní nastavení NAS serveru úspěšně dokončeno a po uložení nastavení a restartování, byl NAS server nalezen na své statické IP adrese. Nyní se stačilo přihlásit a pokračovat v dílčích nastaveních.

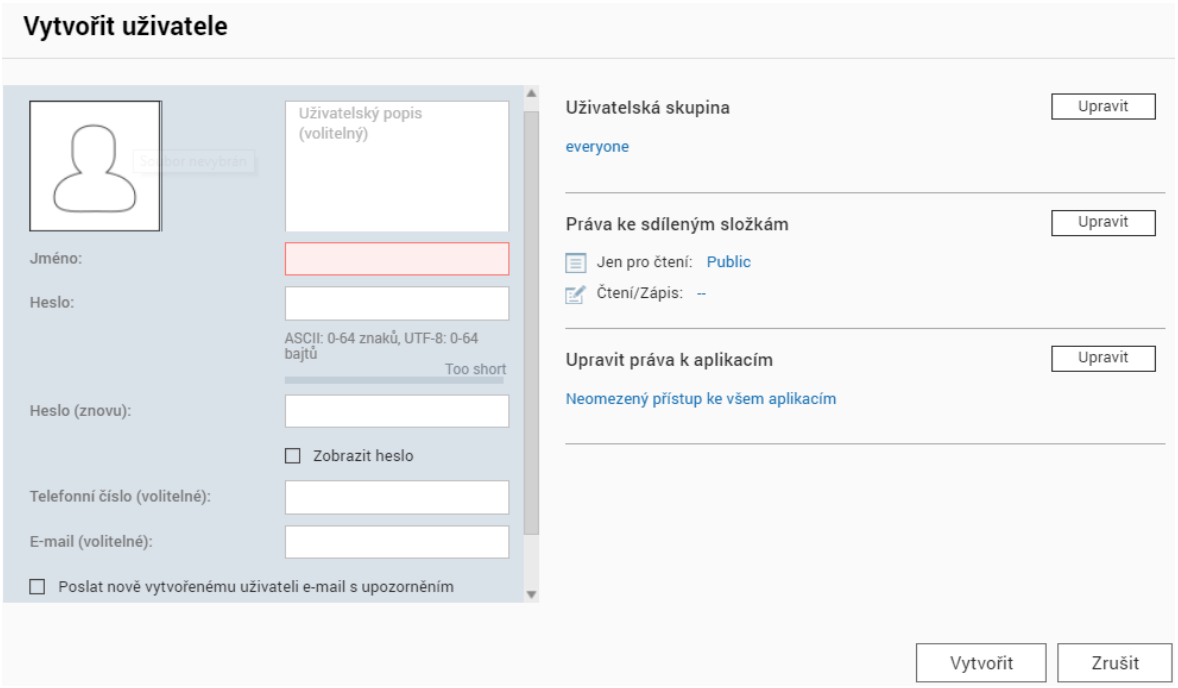
Ihned po staru NAS serveru, byl samovolně spuštěn průvodce grafickým prostředím a následovalo seznamování se se zařízením. Během toho bylo detekováno externí zařízení připojené pomocí USB. Tím bylo již zmiňované UPS.



Obrázek 40 – NAS – Nastavení UPS

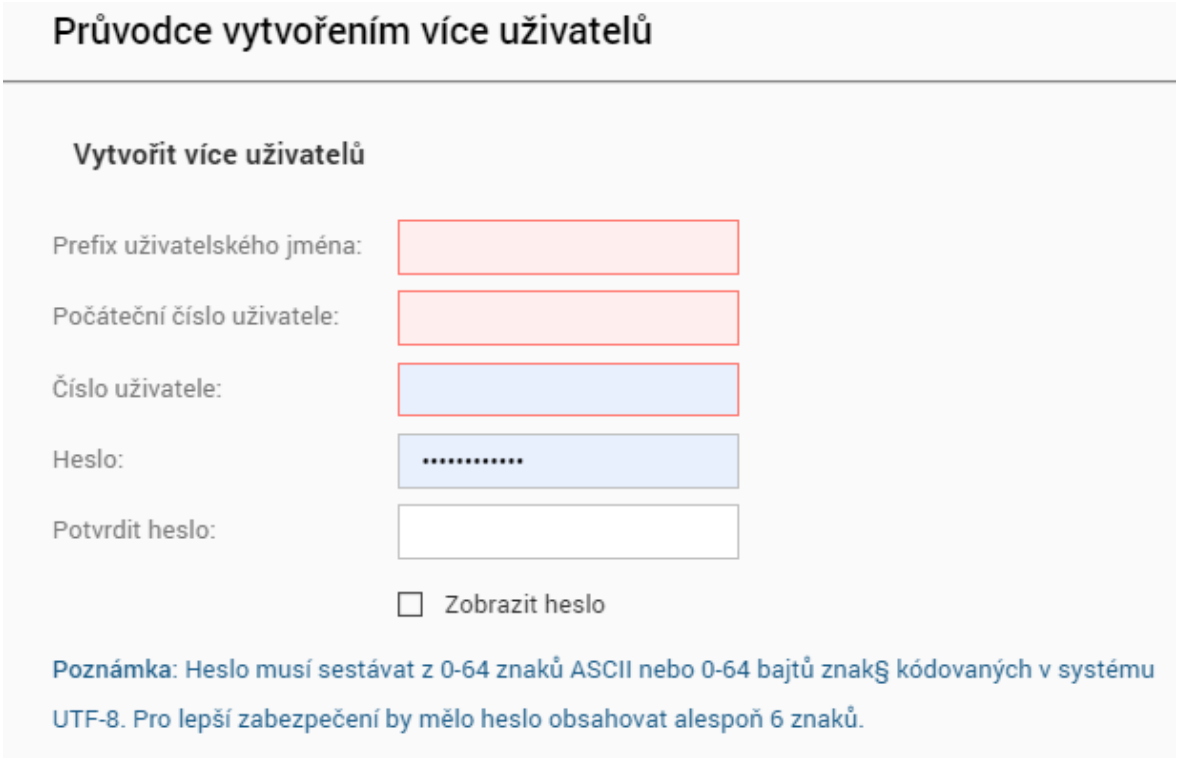
Nastavení UPS umožnuje buďto okamžité vypnutí NAS serveru po uplynutí nastavené doby, nebo přechod do režimu „auto-protection“. To znamená, že NAS server zastaví veškeré služby a odpojí všechny svazky. Poté co se obnoví napájení střídavým proudem, se zařízení restartuje, a samo uvede zpět do provozu. Nastavenou dobu je třeba zvážit s ohledem na UPS, tedy po jak dlouhou dobu vydrží připojená zařízení napájet. To je předmětem testování.

Jakmile bude dále NAS server vhodně nastaven a zabezpečen, přijde část vytváření účtů pro každého zaměstnance, který zde bude mít přístup. Mimo to se každému udělí práva pro přístup k jednotlivým složkám. Většina pak nebude mít právo například soubory, či složky mazat. Někteří budou mít i možnost pouze čtení, aby například do dokumentů nijak nezasahovali.



Obrázek 41 – NAS – vytváření uživatelských účtů

Pro usnadnění vytváření účtů existuje i možnost vytvářet rovnou skupiny uživatelů. To dokáže zjednodušit práci u rozsáhlejších podniků. Zároveň to vede k jasné organizaci uživatelů, například podle čísel.

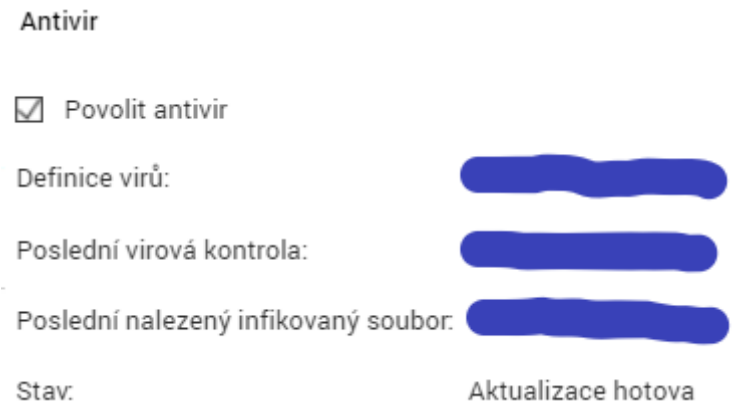


Obrázek 42 – NAS – vytváření více uživatelských účtů

Následně pak umožní průvodce každému uživateli vytvořit vlastní složku pro ukládání svých dat pro potřeby výkonu práce. Po vytvoření se mu udělí práva do jakých sdílených složek a souborů může nahlížet, případně je upravovat. Stejně tak lze omezit i přístup k aplikacím běžících na serveru.

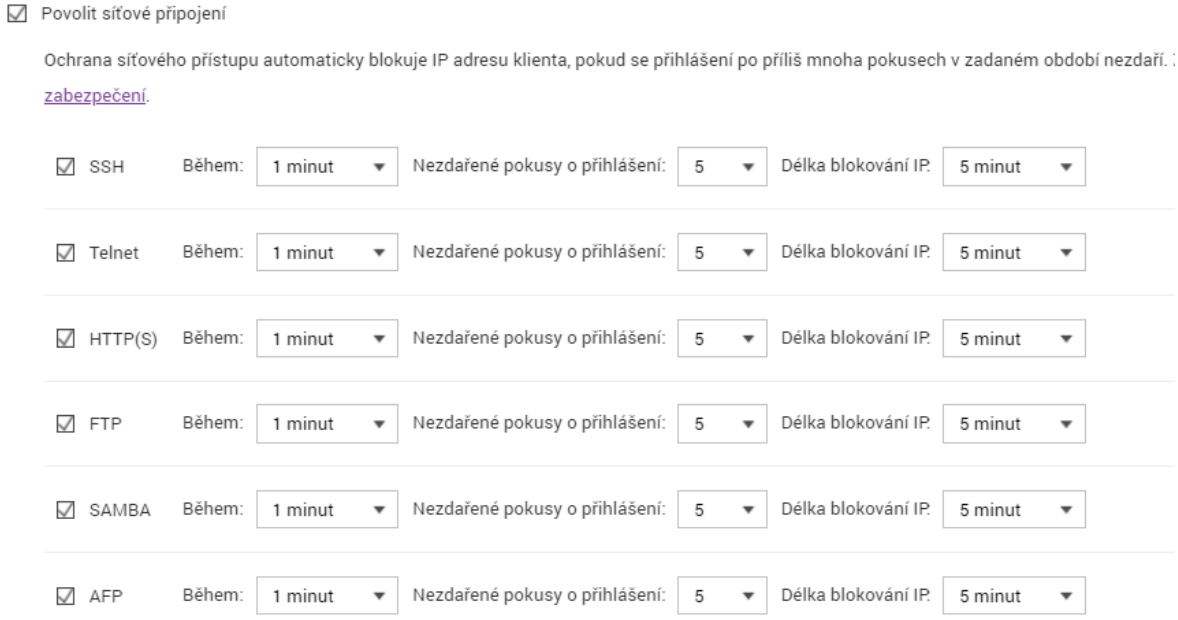
12.3.7 Zabezpečení NAS serveru

Existuje spousta věcí, které jsou třeba nastavit ještě před samotným používáním NAS serveru v podniku. Jednou z nich je například aktivace antivirového programu. Ať už je tento program jakýkoliv, vždy je lepší mít aspoň nějaký, než žádný.



Obrázek 43 – NAS - Antivir

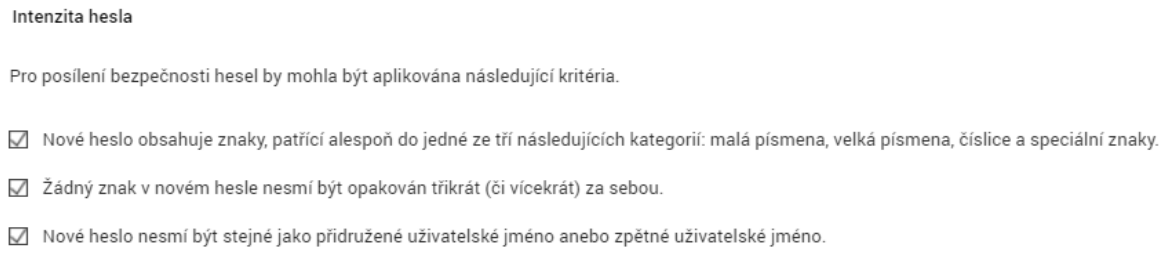
Jednou z metod, jak zabezpečit NAS server proti útoku z venčí, které sám běžně nabízí, je například ochrana přístupu k sítí. Nastavení, která běžně zpracovává firewall a měla by být součástí nastavení routeru, lze nastavit i na NAS serveru. Na Obrázek 44, je pro ukázku nastavení blokování IP adresy, při pěti špatně zadaných pokusech na dobu pěti minut. Tím je z velké části omezen slovníkový útok, ve snaze nabourat se do zařízení a prolomit zabezpečení.



Obrázek 44 – NAS – Zabezpečení – Blokování přístupu

Mimo to lze vytvořit seznam IP adres, které budou mít oprávnění se k serveru připojit. Nebo naopak seznam zakázaných zařízení. Pro podnik by bylo vhodnější zvolit první variantu, kdy by se NAS server zpřístupnil jen pro určitá zařízení.

Jelikož bude mít každý zaměstnanec vytvořený vlastní přihlašovací účet, a dostane se pouze k datům, ke kterým má přístup, je dobré i na ně apelovat, aby volili vhodné hesla a případně je i pravidelně aktualizovali. Mimo jiné je také nevolit stále stejná hesla.



Obrázek 45 – NAS – Zabezpečení – Intenzita hesel

Nastavení umožňuje i vyžadovat změnu hesla po uplynutí nastaveného intervalu, třeba co 90 dní.

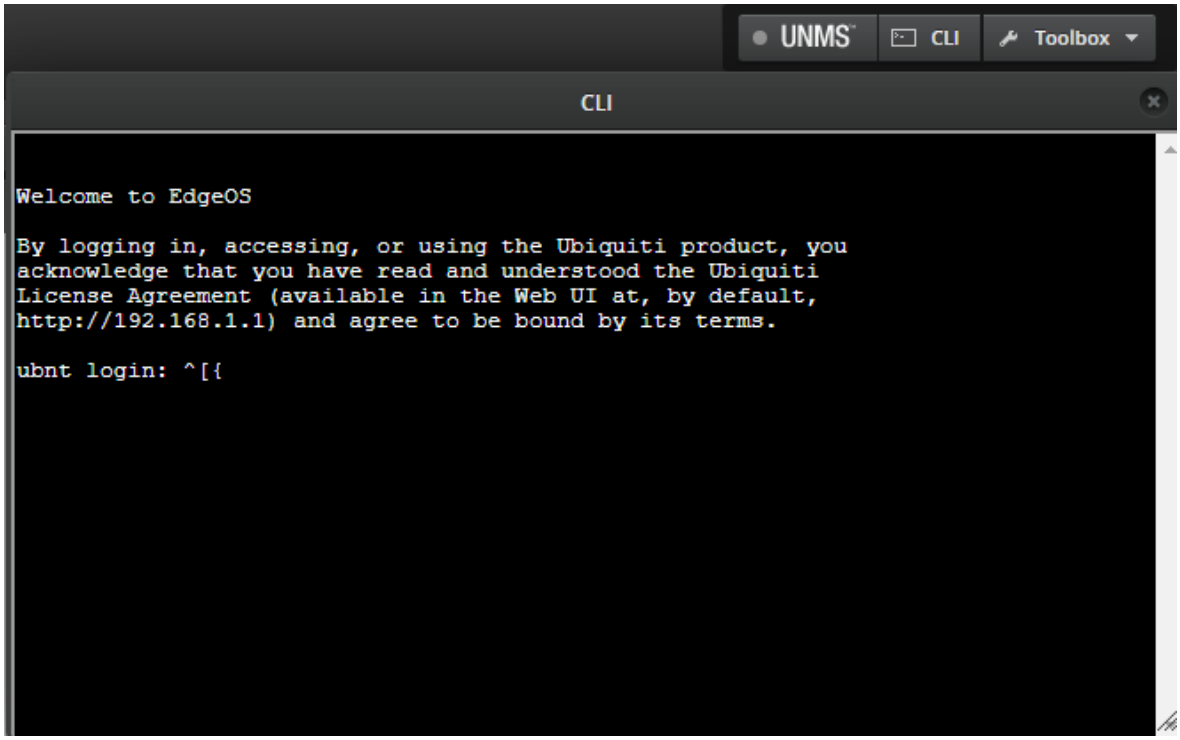
Další možností jak povýšit zabezpečení firemního úložiště, je zakázání přístupu zařízení ke cloudovým funkcím. Zařízení tak neobchází nastavení routeru a není možné se k němu jinak připojit, než z lokální sítě.

Obrázek 46 – NAS – Zakázání Cloudových funkcí

Pokud však bude tato funkce zapnuta, bude potřeba ji vhodně zabezpečit. Jedním z problému neslučitelným s požadavky firmy je, že se data ukládají na cizí server. Ten by však měl být vhodně zabezpečený proti případným únikům, je zde ale toto potenciální riziko stále, proto tato služba pravděpodobně nebude využívána.

12.4 Nastavení VPN na routeru

Pro vzdálený a zabezpečený přístup do podnikové sítě odkudkoliv, bylo potřeba zrealizovat nastavení VPN. To spočívalo ve vytvoření PPTP protokolu. Pro potřeby virtuální privátní síťě, je nezbytné vlastnit veřejnou IP adresu. Ta byla přidělena poskytovatelem internetového připojení. Nastavení pak probíhalo následovně přes příkazový řádek v routeru. Ten se spustil ve webovém rozhraní, v pravém horním rohu kliknutím na tlačítko „CLI“



Obrázek 47 – VPN – Spuštění příkazového řádku

Ze všeho nejdříve, bylo potřeba se přihlásit pod administrátorským účtem, aby bylo možno provádět změny v nastavení. Po úspěšném přihlášení, následovalo zadání příkazu „configure“, díky kterému se mohl router dále konfigurovat. Poté přišla vlna příkazů k samotnému nastavení.

Nejdříve bylo potřeba zadat pravidla, které povolovaly firewallu provozování tohoto protokolu. Příkazy se zapisovaly jeden po druhém a vždy se ověřilo jejich přijetí. Bez těchto pravidel pro firewall by nebyl vzdálený přístup možný.

```
set firewall name WAN_LOCAL rule 50 action accept
set firewall name WAN_LOCAL rule 50 description PPTP
set firewall name WAN_LOCAL rule 50 destination port 1723
set firewall name WAN_LOCAL rule 50 protocol tcp
```

Obrázek 48 – VPN – PPTP – pravidla Firewallu

Další vlna příkazů sloužila k nastavení autentifikačního serveru. Tedy které klienty bude pouštět a které ne. V tomto případě bude docházet k lokálnímu ověřování pomocí dále vytvořeného jména a hesla.

```
set vpn pptp remote-access authentication mode local
set vpn pptp remote-access authentication local-users username "jméno" password "heslo"
```

Obrázek 49 – VPN – PPTP – lokální autentizace

Zadáním prvního příkazu byl tedy zřízen přístup pomocí lokální autentizace. Druhým příkazem se poté vytvořil účet, který by dále umožnoval přístup do zabezpečené VPN.

Následovaly další dva příkazy, pomocí kterých byl stanoven rozsah přidělitelných IP adres pro klienty připojujících se k VPN. V případě, že tedy máme síť 192.0.2.0 a DHCP server přiděluje adres v rozsahu 50 – 199, pro VPN pak můžeme použít například rozsah 200-250.

```
set vpn pptp remote-access client-ip-pool start 192.0.2.200
set vpn pptp remote-access client-ip-pool stop 192.0.2.250
```

Obrázek 50 – VPN – PPTP – Rozsah adres

Nyní je tedy vytvořen rozsah IP adres pro 50 klientů, kteří budou mít přístup do VPN.

V dalším kroku je potřeba nastavit DNS servery. Jeden tedy přímo našeho routeru a druhý například společnosti Google, který je veřejný.

```
set vpn pptp remote-access dns-servers server-1 192.0.2.1
set vpn pptp remote-access dns-servers server-2 8.8.8.8
```

Obrázek 51 – VPN – PPTP- DNS servery

Posledním bodem je nastavení IP adresy WAN portu, kterou nám přidělil poskytovatel internetového připojení. V našem vzorovém případě je to tedy 192.168.11.5. Zadáme tedy následující příkaz se zmíněnou IP adresou.

```
set vpn pptp remote-access outside-address 192.168.11.5
```

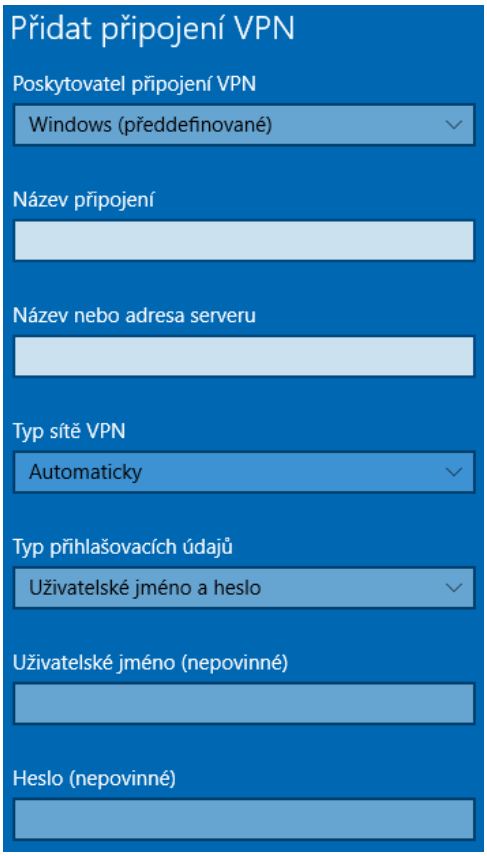
Obrázek 52 – VPN – PPTP – IP Providera

Nyní už jen stačí zadat příkazy „commit“ a „save“ čímž ukončíme konfigurační nastavení a uložíme změny do nastavení routeru.

Nyní si můžeme nastavení ověřit v samotném grafickém prostředí routeru. Kliknutím v horní liště na kolonku VPN. Zde pak vidíme aktuální nastavení PPTP protokolu VPN.

Obrázek 53 – VPN – PPTP – Úspěšné nastavení

Úspěšně byla tedy zřízená VPN síť s protokolem PPTP. Nyní je možno například připojit počítač k této síti. V systému Windows 10 stačí vyhledat nastavení sítě VPN pomocí nabídky start. Poté kliknout na kolonku přidat připojení a zadat patřičné údaje.



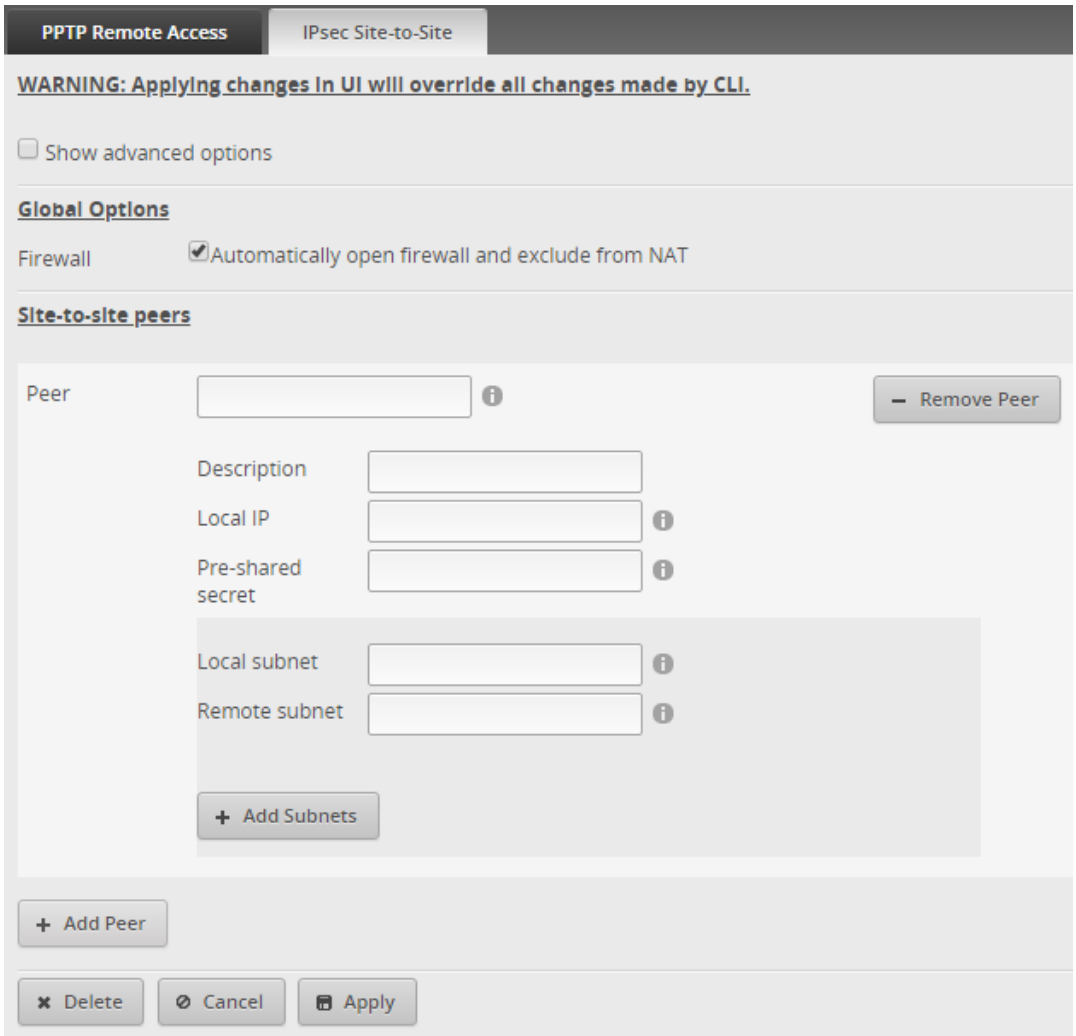
Obrázek 54 – VPN – Windows - Připojení počítače

Název připojení si uživatel zvolí sám. Název nebo adresa serveru je v tomto případě veřejná IP adresa (vzorová 123.213.231.211). Na závěr jen zadat uživatelské jména a heslo.

12.4.1 Nastavení IPsec site-to-site

V budoucnu bude probíhat zřízení propojení obou sídel pomocí VPN site-to-site. To bude mít za následek to, že zařízení v obou sídlech, se budou tvářit, jakoby byla v jedné lokální síti. Uživatelé v Sídle 1 tak budou mít stejně jednoduchý přístup k NAS serveru, jako uživatelé v Sídle 2.

Poté co bude poskytovatelem internetového připojení v Sídle 1 poskytnuta veřejná IP adresa, budou se moct oba tyto routery vzdáleně propojit a spárovat. Na obou stranách se zadají veřejné IP adresy těch protějších. Lokální IP adresy a dostatečně složitý před-sdílený klíč.



Obrázek 55 – VPN – site-to-site – Budoucí nastavení

Výše zmíněné nastavení bude dalšího snažení nad rámec této práce.

13 VÝSLEDKY A KONZULTACE S VEDENÍM PODNIKU

Výsledkem snažení v této práci, bylo prakticky navrhnout a zrealizovat IT infrastrukturu nejmenovaného podniku. Ten je s dosavadním průběhem práce, zdá se spokojen. Po úplné kompletaci infrastruktury v Sídle 1 i Sídle 2, bude na řadě implementace těchto technologií do každodenního procesu podniku. NAS server čeká přírůstek, v podobě dalšího pevného disku, ten přinese změnu v zabezpečovaných discích. Nově bude zvolen RAID 5. To vše však přináší ještě spoustu společné práce. Bude potřeba veškeré zaměstnance s technologiemi seznámit a například zavést i bezpečnostní politiku, pro bezpečné provozování těchto technologií. Svůj čas si vezme i postupné zavádění provázaní s koncovými zařízeními. Administrativa a hierarchie celé této koncepce ukládání a správy dat, musí být také vhodně navržena s ohledem na bezpečnost. Zdárným výsledkem práce, je sestavení celého systému, který funguje a snad bude i zaměstnancům ulehčovat práci. Zvolený koncept s vybraným NAS serverem společnosti QNAP, přináší podniku nové možnosti a cíle v podnikání. Vše je nyní jen otázkou času a vhodně navrženého IS, aby práci zaměstnanců zefektivňoval, zjednodušoval a zpříjemňoval. Nikoliv naopak.

13.1 Vize do budoucna

V současnosti je s vedením podniku probírán návrh implementace informačních systémů. Nejen tedy společné firemní úložiště, ale i správa nad informacemi v něm uložených. Bude se tedy nějakým způsobem zavádět ERP systém k ulehčení činnosti v oblasti podnikání. Systém bude řídit práci zaměstnanců. Aby tedy jasně věděli, co mají dělat, kdy to mají mít hotové, nebo kdo je za co zodpovědný. Zároveň například v provázanosti s elektronickou poštou, zautomatizovat komunikaci se zákazníky. Provázání s kalendářními aplikacemi, bude snaha o jasné plánování práce. Možností jsou už nyní rozsáhlé a vedení podniku tento systém zautomatizování vřele vítá a těší se výsledků.

ZÁVĚR

Obsahem této práce, bylo z hlavní části ukázat, jak se dá poměrně jednoduše zřídit podniku IT infrastruktura a na ní pak postupně navázat informační systémy. Jak bylo v práci zmíněno, požadavky každého podniku jsou individuální. To co je pro zmiňovaný podnik vhodnou variantou, může být pro jiný podnik naprosto nedostačující. Práce v teoretické části rozebírala pojmy spojené s touto problematikou. Od samotné IT infrastruktury, přes pojem Informační systém a jeho možná implementace do podnikového prostředí. Za zmínku v této oblasti patřilo jednoznačně zabezpečení, jak jednotlivých prvků infrastruktury, tak bezpečné komunikace, nebo bezdrátového přenosu dat. V práci byl teoretický popsán i postup při analyzování rizik, za použití grafické metody FTA.

Praktická část následovala teoretickou. V úvodu stálo seznámení se s podnikem XY a jeho strukturou. Následovalo analyzování potřeb podniku, který má snahu zrealizovat novou infrastrukturu podniku a následně zavést informační systémy. Poté přišlo modelové analyzování rizik, respektive tedy hledání příčin vzniku hrozby výpadku PC sítě. Poté co byly požadavky podniku zanalyzovány. Došlo k samotnému návrhu skladby infrastruktury. Podnik zmiňovaný návrh přijal, což vedlo k samotné realizaci. Ta je v práci popsána od sestavení jednotlivých komponentů do Rackové skříně, až po nastavení a prvotní spuštění komponent. Byla podniku také zřízená virtuální privátní síť, s možností vzdáleného a bezpečného přístupu. Práci navíc zavírá vize další spolupráce s podnikem do budoucna. Spolupráce měla zatím kladný přínos na obou stranách. Podniku se nově otevřely nové možnosti.

SEZNAM POUŽITÉ LITERATURY

[1] IT Infrastruktura. *It-slovník.cz* [online]. [cit. 2019-05-22]. Dostupné z: https://it-slovnik.cz/pojem/infrastruktura

[2] GÁLA, Libor, Jan POUR a Zuzana ŠEDIVÁ. Podniková informatika: počítačové aplikace v podnikové a mezipodnikové praxi. 3., aktualizované vydání. Praha: Grada Publishing, 2015, 240 s. Management v informační společnosti. ISBN 978-80-247-5457-4.

[3] KŘENA, Martin. *Charakteristika IT infrastruktury*. Fakulta informatiky a statistiky, 2014. Diplomová práce. Vysoká škola ekonomická v Praze.

[4] BASL, Josef. Podnikové informační systémy: podnik v informační společnosti / Josef Basl, Roman Blažíček. 2012. ISBN 9788024743073.

[5] Informační systém podniku. *Managementmania.com* [online]. 2015 [cit. 2019-05-22]. ISSN 2327-3658. Dostupné z: https://managementmania.com/cs/informacni-system-podniku-enterprise-information-system

[6] *Informační systém* [online]. Vysoká škola báňská, 2011 [cit. 2019-05-22]. Dostupné z: http://homel.vsb.cz/~dan11/rd_is_skripta.htm

[7] BUŠEK, Petr. *Implementace podnikového informačního systému ve vybrané firmě* [online]. České Budějovice, 2016 [cit. 2019-05-25]. Dostupné z: https://theses.cz/id/6s15gc/BP_Bu_ek_Petr.pdf. Bakalářská práce. Jihočeská univerzita v Českých Budějovicích. Vedoucí práce Ing. Petr Hanzal, Ph.D.

[8] PETRTÝLOVÁ, Barbora. *Správa podnikových informací z pohledu podnikových informačních systémů*. Praha, 2009. Diplomová práce. Univerzita Karlova v Praze. Vedoucí práce Prof., Ing. Josef Basl CSc.

[9] Informace. *Managementmania.com* [online]. 2017, 14.12.2017, , 1 [cit. 2019-05-22]. ISSN 2327-3658. Dostupné z: https://managementmania.com/cs/informace

[10] Informační systém a ochrana dat. *IS systems* [online]. systemonline.cz, 8.2001, 1 [cit. 2019-05-22]. ISSN 1802-615X. Dostupné z: https://www.systemonline.cz/clanky/informacni-systemy-a-ochrana-dat.htm

[11] Bezpečná komunikace. *Www.solnet.cz* [online]. [cit. 2019-05-26]. Dostupné z: https://www.solnet.cz/files/manual/webis/mail_secure.html

[12] HANÁČEK, Petr. Bezpečnost informačních systémů: metodická příručka zabezpečování produktů a systémů budovaných na bázi informačních technologií / Petr Hanáček, Jan Staudek. 2000. ISBN 8023854003.

[13] PAVLÍK, Lukáš. *Informační systémy* [online]. Olomouc, 2017 [cit. 2019-05-22]. Dostupné z: https://mvso.cz/wp-content/uploads/2018/02/Informa%C4%8Dn%C3%AD-syst%C3%A9my-studijn%C3%AD-text.pdf. Studijní materiál. Moravská vysoká škola Olomouc.

[14] VÁCLAVÍK, LUKÁŠ. HISTORIE WI-FI SE ZAČALA PSÁT PŘED 25 LETY. PŘIPOMEŇTE SI HLAVNÍ MILNÍKY. CNEWS.CZ [ONLINE]. 2015 [CIT. 2019-05-13]. DOSTUPNÉ Z: HTTPS://WWW.CNEWS.CZ/HISTORIE-WI-FI-SE-ZACALA-PSAT-PRED-25-LETY-PRIPOMENTE-SI-HLAVNI-MILNIKY/

[15] KERŠLÁGER, MILAN. BEZDRÁTOVÉ SÍTĚ [ONLINE]. CREATIVECOMMONS.ORG, 2016 [CIT. 2019-05-13]. DOSTUPNÉ Z: HTTPS://WWW.DROPBOX.COM/SH/YGLE7LU2FK85ZAG/AAAGG-W2TKMZTTNVEEHOQZLBA?PREVIEW=BEZDR%C3%A1TOV%C3%A9_S%C3%ADT%C4%9B.ODP#

[16] TOMÁNEK, Tomáš. *Aplikovaná kryptologie v internetové komunikaci* [online]. Praha, 2008 [cit. 2019-05-26]. Dostupné z: https://is.cuni.cz/webapps/zzp/detail/58821/. Diplomová práce. Univerzita Karlova v Praze. Vedoucí práce Ing. Martin Souček.

[17] SHARED KEY AUTHENTICATION. ITFELLOVER.COM [ONLINE]. 2015 [CIT. 2019-05-13]. DOSTUPNÉ Z: HTTPS://ITFELLOVER.COM/6-SHARED-KEY-AUTHENTICATION-SKA/

[18] SEVERÝN, Prokop. *Šifrovaná VPN (multipoint)* [online]. Praha, 2008 [cit. 2019-05-26]. Dostupné z: https://is.cuni.cz/webapps/zzp/detail/46356/?lang=en. Bakalářská práce. Univerzita Karlova v Praze. Vedoucí práce Dan Lukeš.

[19] *BARIŠ, Dušan. Komplexní bezpečnost obchodního centra* [online]. Ostrava, 2010 [cit. 2018-12-02]. Dostupné z: <https://theses.cz/id/k3llra/>. Diplomová práce. Vysoká škola báňská - Technická univerzita Ostrava, Fakulta bezpečnostního inženýrství. Vedoucí práce Michail Šenovský.

[20] ROMAN, Mahel. analýza stromu poruchových stavů (FTA) a analýza možných vad a jejich důsledků (FMEA) procesu pájení a vodivého lepení v elektronice [online].

ČVUT, 2016 [cit. 2019-05-20]. Dostupné z: https://dspace.cvut.cz/handle/10467/64869. Magisterská práce. ČVUT. Vedoucí práce Mach Pavel.

[21] Technické normy [online]. internet: Normy ČSN, 2007 [cit. 2019-05-20]. Dostupné z: http://www.technicke-normy-csn.cz/010676-csn-en-61025_4_79666.html

[22] FTA (Fault Tree Analysis) - Analýza stromu poruchových stavů. *Managementmania.com* [online]. 24.7.2015 [cit. 2019-05-26]. ISSN 2327-3658. Dostupné z: https://managementmania.com/cs/fault-tree-analysis

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

IT	Informační technologie
BCM	Business Continuity Management
DRP	Disaster Recovery Planning
ECM	Enterprise Content Management
ERP	Enterprise Resource Planning
SCM	Supply Chain Management
CC	Cloud Computing
SAAS	Software as a Service
PAAS	Platform as s Service
IAAS	Infrastuctuce as a Service
IS	Informační systém
PAN	Personal Area Network
LAN	Local Area Network
MAN	Metropolitan Area Network
WAN	Wide Area Network
MIMO	Multiple-input Multiple-output
SU-MIMO	Single User MIMO
MU-MIMO	Multiple User MIMO
AP	Access Point
WDS	Wireles Distribution systém
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
MIC	Message Integrity Code
AES	Advanced Encryption Standard

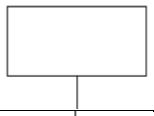
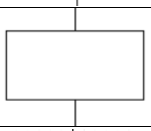
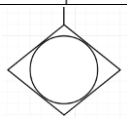
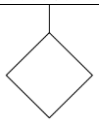
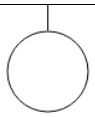
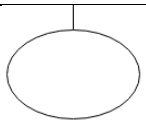
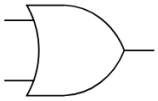
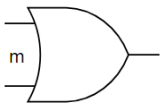
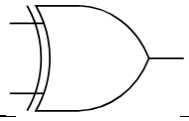
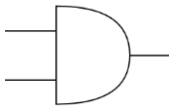
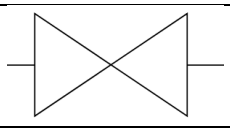
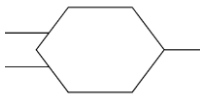
WPA2	Wi-Fi Protected Access 2
CCMP	Counter Cipher Mode with Block Chaining Message Authentication Code Protocol
PSK	Pre.Shared Key
SSID	Service Set Identifier
RADIUS	Remote Authentication Dial In User Service
VPN	Virtuální privátní síť
FTA	Analýza stromu poruch
NAS	Network Attached Storage
RAID	Redundant Array of Independent Disks
PPTP	Point-to-Point Tunneling Protocol
UPS	Uninterruptible Power Supply
UBNT	Ubiquity Networks
POE	Power over Ethernet
UNMS	Ubiquiti Network Management Systém
UFO	Unidentified Flying Object

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: ZNAČKY FTA ANALÝZY

Značka	Název	popis
	Vrcholová událost	Vrcholová událost, řešený stav, ke kterému směřují všechny ostatní události.
	Událost	Blok s popisem události směřující k vrcholové události za nějaké podmínky.
	Událost analyzovaná jinde	Událost, která je dále rozvíjená v jiném stromu poruch.
	Nerozvíjená událost	Událost, která se dále podrobněji nerozvíjí. (Nebývá potřeba dále rozvíjet).
	Základní událost	Základní primární událost, která se dále nerozvíjí.
	Podmínková událost	Událost, která bývá podmíněná jinou událostí.
	Transfer (přenos dovnitř)	Hradlo, které naznačuje rozvíjení událostí v jiné části diagramu (používá se k eliminacím duplicit událostí).
	Transfer (přenos ven)	Hradlo naznačující opakování událostí, která je rozvíjená jinde v diagramu.
	Logický součet OR	Hradlo nahrazující spojku a případně anebo. Platí, když nastane alespoň jedna z předcházejících událostí.
	Majoritní hradlo	Hradlo, které platí, jestliže nastane alespoň m z n vstupních událostí.
	XOR	Hradlo XOR platí tehdy, nastane-li jedna z událostí, nebo druhá. Nikdy ne současně.
	Logický součin AND	Hradlo and nahrazuje slovní spojení a zároveň. Platí tehdy, jestliže nastanou oba, či více vstupních stavu současně.
	Negace NOT	Hradlo, při níž výstupní událost nastane tehdy, jestliže vstupní nenastane.
	Blokování INHIBIT	Podmínkové hradlo, výstupní událost nastane tehdy, jestliže vstupní události splní určitou podmínku.

PŘÍLOHA P II: FTA STROM PORUCH