VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

NÁVRH ISMS V PRŮMYSLOVÉM PROSTŘEDÍ
DESIGN OF ISMS IN INDUSTRIAL ENVIRONMENT

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE
AUTHOR
Bc. Lukáš Kuchařík

VEDOUCÍ PRÁCE
SUPERVISOR
Ing. Petr Sedlák

BRNO 2016

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2015/2016
Ústav informatiky

ZADÁNÍ DIPLOMOVÉ PRÁCE

Kuchařík Lukáš, Bc.

Informační management (6209T015)

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách, Studijním a zkušebním řádem VUT v Brně a Směrnicí děkana pro realizaci bakalářských a magisterských studijních programů zadává diplomovou práci s názvem:

Návrh ISMS v průmyslovém prostředí

v anglickém jazyce:

Design of ISMS in Industrial Environment

Pokyny pro vypracování:

Úvod
Vymezení problému a cíle práce
Teoretická východiska práce
Analýza problému a současná situace
Vlastní návrh řešení, přínos práce
Závěr
Seznam použité literatury

Seznam odborné literatury:

ČSN ISO/IEC 27001, Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky. Praha: Český normalizační institut, 2014.
ČSN ISO/IEC 27002, Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Soubor postupů. Praha: Český normalizační institut, 2014.
DOUCEK P., L. NOVÁK, L. NEDOMOVÁ a V. SVATÁ. Řízení bezpečnosti informací. Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.
JORDÁN, V. a V. ONDRÁK. Infrastruktura komunikačních systémů III: Integrovaná podniková infrastruktura. Brno: CERM, Akademické nakladatelství, 2016. ISBN 978-80-214-5241-1.
ONDRÁK V., P. SEDLÁK a V. MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: CERM, Akademické nakladatelství, 2013. ISBN 978-80-7204-872-4.

Vedoucí diplomové práce: Ing. Petr Sedlák

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2015/2016.

L.S.

doc. RNDr. Bedřich Půža, CSc. Ředitel ústavu	doc. Ing. et Ing. Stanislav Škapa, Ph.D. Děkan fakulty

V Brně, dne 29.2.2016

ABSTRAKT

Diplomová práce je zaměřena na návrh síťové infrastruktury a zavedení systému řízení bezpečnosti informací v průmyslovém prostředí. V úvodu je práce zaměřena na teoretické poznatky z bezpečnosti informací, kde popisuje základní pojmy a obecné postupy systému řízení informační bezpečnosti. Dále se práce zabývá analýzou rizik, kde jsou navržena opatření ke snížení rizik. Následně je proveden návrh nové síťové infrastruktury. Práce čerpá informace převážně z norem ČSN ISO/IEC řady 27000.

ABSTRACT

The master's thesis is aimed at the proposal of network infrastructure and introduction of the managerial system for the safety of information in the industrial environment. At the beginning the work is focused on theoretical knowledge concerning the safety of information wherein it describes basic concepts and common procedures of the managerial system of the safety of information. Further, the work deals with risk analysis in which the measures for reduction in hazard are suggested. The proposal for a new network infrastructure is finally carried out. The work draws the information from CSN standards ISO/IEC, series 27000.

KLÍČOVÁ SLOVA

Systém řízení bezpečnosti informací, bezpečnost, průmysl, síťová infrastruktura, analýza rizik, bezpečnostní opatření, ISO/IEC 27000

KEYWORDS

Information security management systém, security, industry, network infrastructure, risk analysis, security measures, ISO/IEC 27000

BIBLIOGRAFICKÁ CITACE

KUCHAŘÍK, L. *Návrh ISMS v průmyslovém prostředí*. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2016. 82 s. Vedoucí diplomové práce Ing. Petr Sedlák.

ČESTNÉ PROHLÁŠENÍ

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

V Brně dne 19. května 2016 ……..

PODĚKOVÁNÍ

Rád bych poděkoval vedoucímu práce panu Ing. Petru Sedlákovi, který mi poskytoval mnoho důležitých a odborných informací, které jsem mohl uplatnit v této práci, ale také za cenné konzultace a vedení celé práce. Dále bych chtěl poděkovat celé své rodině, která mě po celou dobu studia podporovala.

OBSAH

ÚVOD

Doba jde stále dopředu a s ní i výpočetní oblast. Všude se čím dál více setkáváme s digitalizací dat a informací. Tak je tomu i v oblasti firem, podniků a různých organizací. Proto je nutné tyto data a informace zabezpečit před jejich zneužitím. Firmy jsou ze zákona povinny chránit osobní údaje zaměstnanců, dodavatelů nebo odběratelů. Každá firma potřebuje uchránit před zneužitím své know-how. Aby tomu tak bylo, je zapotřebí se řídit doporučenými dokumenty neboli normami řady 27000. S těmito normami souvisí také zavedení systému řízení bezpečnosti informací, který nám udává postupy, jak nejlépe zavést bezpečnost právě do naší firmy a chránit důležitá data a informace.

V první kapitole jsou sepsány cíle práce a vymezení problému. V následující kapitole budeme seznámeni se základními pojmy, názvoslovím bezpečnosti informací. Dále zde budou uvedeny normy, které jsou nezbytné pro správné vytvoření našeho požadavku. V další kapitole bude popsána současná situace ve firmě, její infrastruktura a celková bezpečnost. Na závěr této kapitoly bude zhodnocení analýzy, kde bude popsáno, co vše je nutné udělat a co je doposud ve firmě špatně zpracované. Poslední kapitola se bude zabývat vlastním návrhem řešení. Jako první bude zpracována analýza rizik, která mohou nastat. Dalším aspektem bude identifikace a ohodnocení aktiv, zranitelností a hrozeb. Na základě této analýzy budeme vědět, v jakých oblastech je nutné zavést ISMS, tedy navrhnout opatření. Dále bude vypracován návrh nové infrastruktury.

1 VYMEZENÍ PROBLÉMU A CÍLE PRÁCE

Diplomová práce se zaměřuje na problematiku systému řízení bezpečnosti informací v průmyslovém prostředí. Na ICS infrastrukturu se klade zvlášť velký důraz, než je tomu u komerčních sítí. Je zapotřebí zvolit si správné prvky infrastruktury a postupovat podle daných norem, aby bylo vše dodrženo. U průmyslového řešení se na první místo staví dostupnost, tudíž je zapotřebí mít síť s maximální dostupností (v reálném čase).

Bezpečnost informací není pouze fyzické zabezpečení zařízení, ale je třeba tento problém řešit komplexněji. Tedy dbát jednak na poučení osob, které mohou přijít do styku s důležitými nebo citlivými informacemi, ale také na fyzickou ochranu budov nebo kamerové systémy.

Práce je tedy zaměřena na návrh ICS infrastruktury, jelikož to je hlavním cílem společnosti. Bude určen rozsah zavedení ISMS, dle požadavků a finančních možností společnosti. Dále se v práci bude provádět analýza rizik a návrh opatření. Cílem práce je tedy navrhnout infrastrukturu, která bude splňovat veškeré podmínky stanovené pro ICS a také bude vyhovovat normám pro průmyslové ISMS.

2 TEORETICKÁ VÝCHODISKA

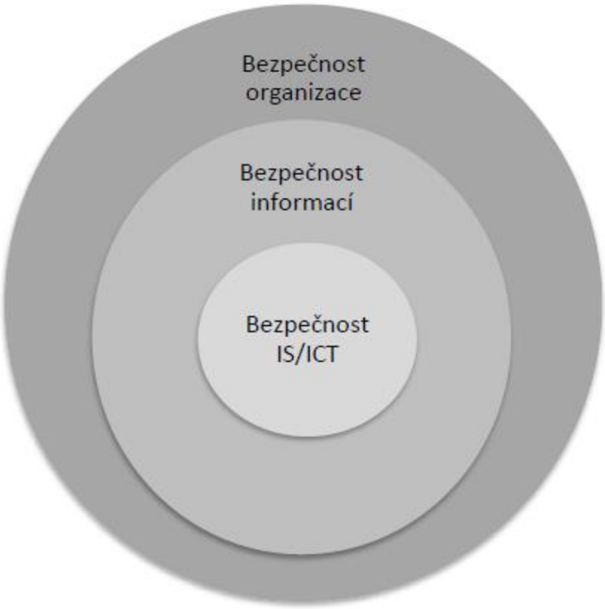
V této části práce budou vysvětleny základní pojmy spojené s bezpečnosti informací a popsány normy. Dále se pak téma bude vztahovat k průmyslovému prostředí.

2.1 Základní pojmy a názvosloví

Na začátek je nutné seznámit se a ujasnit si základní pojmy a názvosloví, které se vyskytuje v oblasti bezpečnosti informací.
V následujících bodech jsou tyto pojmy popsány [1]:

- **ISMS** – systém řízení informační bezpečnosti
- **Informace** – širší pojem, který popisuje reálné prostředí, jeho stav i procesy v něm probíhající ve formě údajů.
- **Data** – jsou plněním informace, kterou vytváří.
- **Přenos dat** – je přenos digitálních zpráv nebo digitalizovaného analogového signálu, a to pomocí fyzického dvoubodového či vícebodového přenosového prostředí (metalický kabel, optický kabel, bezdrátový přenos).
- **Informační systém** – lze chápat jako systém vzájemně propojených informací a procesů.
- **Síťová infrastruktura** – tento pojem zahrnuje veškeré síťové prvky a zařízení použité při realizaci.
- **Počítačová síť** – je součástí síťové infrastruktury a slouží k realizaci komunikačního prostředí mezi uživateli.
- **Bezpečnost informací** – zachování důvěrnosti, dostupnosti a integrity informací.
- **Dostupnost** – zajištění přístupnosti k informaci oprávněnému uživateli v jeho požadovaný okamžik.
- **Důvěrnost** – zajištění přístupnosti k informaci pouze oprávněnému uživateli.
- **Integrita** – zajištění správnosti a úplnosti informace.
- **Aktivum** – veškerý nehmotný i hmotný majetek.
- **Hrozba** – událost, která ohrožuje bezpečnost.
- **Zranitelnost** – slabé místo aktiva.

- **Opatření** – aktivita, která umožňuje snížení hrozby.
- **Riziko** – kombinace zranitelnosti a hrozby s dopadem na aktivum.
- **Dopad** – vznik škody v důsledku působení hrozby.
- **Řízení rizik** – koordinace, která je nutná k řízení a kontrole organizace s ohledem na rizika.
- **Analýza rizik** – systematické používání informací pro odhad míry rizika a také k určení jeho zdrojů.
- **Akceptace rizika** – rozhodnutí o přijetí rizika.
- **Prohlášení o aplikovatelnosti** – dokument, který popisuje opatření ISMS v organizaci.



Obrázek 1: Úroveň bezpečnosti organizace, Zdroj: [19]

Bezpečnost organizace je nejvyšší úrovní bezpečnosti. Do této úrovně spadá zajištění bezpečnosti objektu, nebo majetek organizace. Navíc může pomoci i ostatním úrovním, např. bezpečnost IS/ICT a to tak, že bude kontrolován fyzický přístup do objektu. *Bezpečnost informace* je součást úrovně předchozí. Cílem této úrovně je shrnout zásady bezpečné práce s informacemi. Stará se o digitální data, ale také o způsob uložení, zpracování [20].

Bezpečnost IS/ICT je nejužší úrovní, která pracuje s tzv. neviditelnými daty, informacemi nebo službami. Chrání pouze ta aktiva, která patří k informačnímu systému organizace [20].

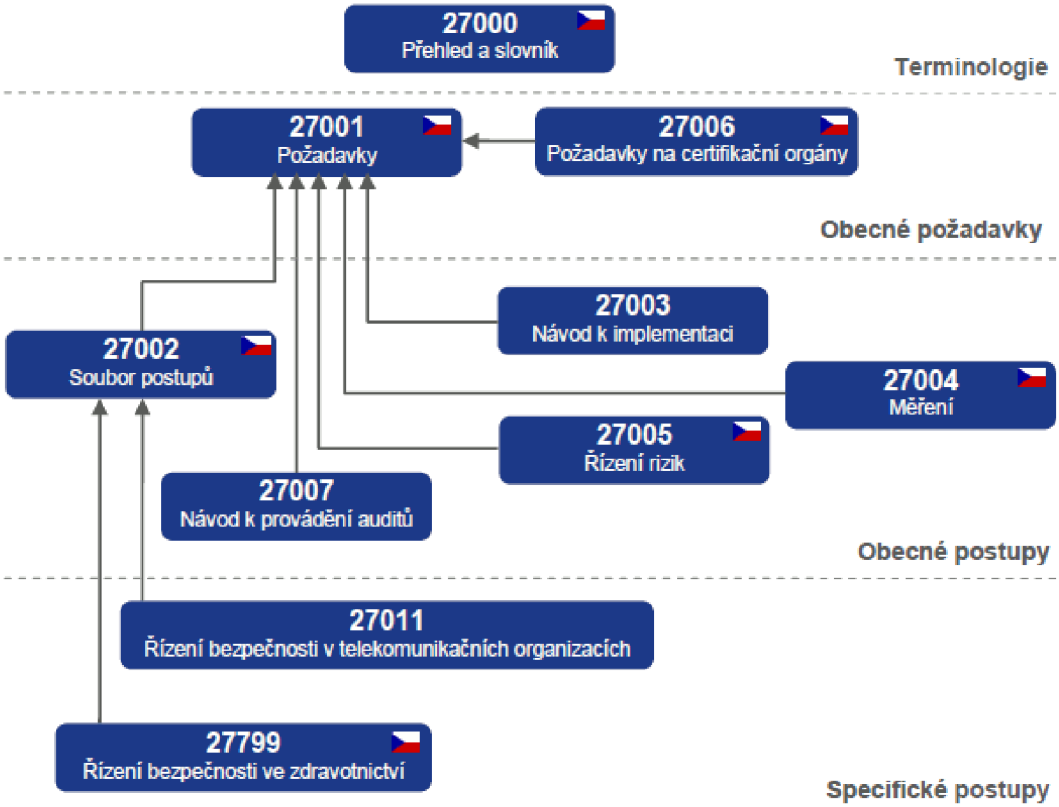
2.2 Normy

Pokud chceme budovat bezpečnost, je nutné brát v úvahu aktuální normy, neboli doporučení, a zákony. Pro obecné ISMS platí normy z řady ISO/IEC 27000.

2.2.1 Normy řady ISO/IEC 27000

Tato řada norem popisuje řízení bezpečnosti informací v organizacích [21]:

- **ISO/IEC 27000** – přehled a slovník
- **ISO/IEC 27001** – požadavky
- **ISO/IEC 27002** – soubor postupů pro opatření bezpečnosti informací
- **ISO/IEC 27003** – směrnice pro implementaci systému řízení bezpečnosti informací
- **ISO/IEC 27004** – měření
- **ISO/IEC 27005** – řízení rizik bezpečnosti informací
- **ISO/IEC 27006** – požadavky na orgány, které provádějí audit a certifikaci systému řízení bezpečnosti informací
- **ISO/IEC 27007** – směrnice pro audit ISMS
- **ISO/IEC 27008** – směrnice pro audit opatření ISMS
- **ISO/IEC 27010** – směrnice pro řízení bezpečnosti informací pro meziodvětvové komunikace a komunikace mezi organizacemi
- **ISO/IEC 27011** – směrnice pro řízení bezpečnosti informací pro telekomunikační organizace
- **ISO/IEC 27013** – návod pro integrovanou implementaci ISO/IEC 27001
- **ISO/IEC 27014** – správa bezpečnosti informací
- **ISO/IEC 27015** – směrnice pro řízení bezpečnosti informací pro finanční služby
- **ISO/IEC 27016** – řízení bezpečnosti informací pro organizační ekonomiku



Obrázek 2: Struktura norem řady 27000, Zdroj: [22]

Norma ISO/IEC 27000

Tato mezinárodní norma obsahuje jakýsi přehled systému řízení bezpečnosti informací a s tím souvisejících termínů, pojmů a definic. Tuto normu lze uplatnit v jakýchkoli typech a velikostech organizací [21].

Norma ISO/IEC 27001

Tato norma udává podporu pro ustanovení, zavedení, provozování, monitorování, udržování a zlepšování systému řízení bezpečnosti informací. Tím patří do strategických rozhodnutí firem, které hodlají zavést systém řízení bezpečnosti informací. Ustavení systému řízení bezpečnosti informací ovlivňuje hned několik faktorů, které se mohou postupem času měnit. Do těchto faktorů patří např.: potřeby a cíle organizace, požadavky na bezpečnost aj. V rámci managementu rizik je velmi důležité a nutné, aby byla zachována důvěrnost, dostupnost a integrita [5].

Norma ISO/IEC 27002

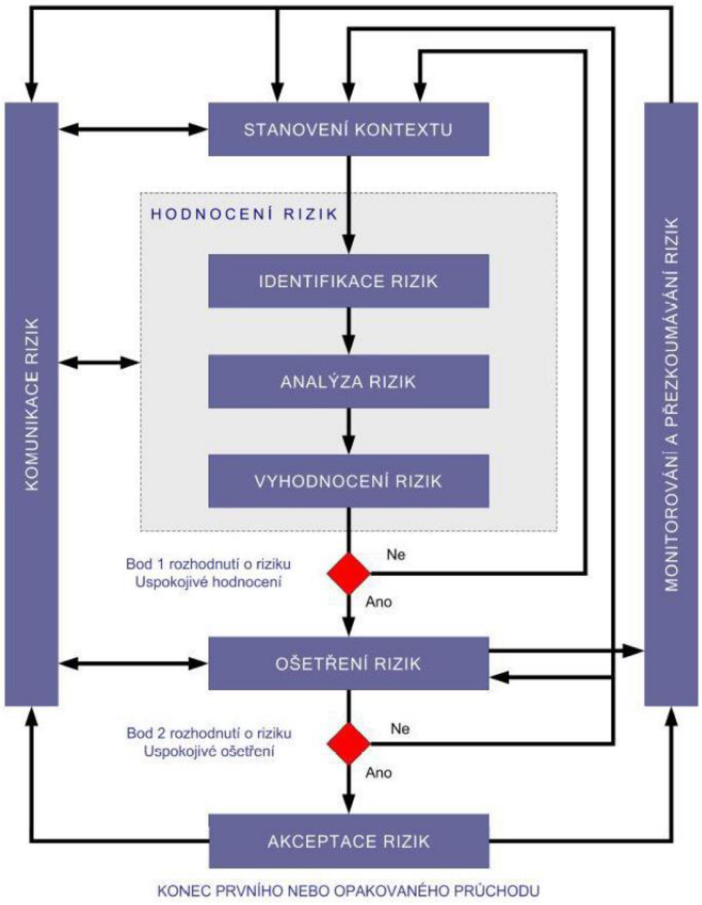
Při zavádění systému řízení bezpečnosti informací slouží jako doporučení tato norma, která obsahuje opatření, která jsou založena na normě ISO/IEC 27001. Zároveň však tato norma může sloužit i jako jakési pokyny pro firmy, které zavádějí opatření bezpečnosti informací. Dále norma může posloužit i k vytvoření směrnic pro řízení bezpečnosti informací v průmyslu. V následující tabulce jsou zobrazeny kapitoly a počet jejich kategorií a opatření [6].

Tabulka 1: Hlavní oblasti opatření dle ISO/IEC 27002, Zdroj: upraveno dle [6]

Označení	Kapitola	Počet kategorií	Počet opatření
A.5	Politiky bezpečnosti informací	1	2
A.6	Organizace bezpečnosti informací	2	7
A.7	Bezpečnost lidských zdrojů	3	6
A.8	Řízení aktiv	3	10
A.9	Řízení přístupu	4	14
A.10	Kryptografie	1	2
A.11	Fyzická bezpečnost a bezpečnost prostředí	2	15
A.12	Bezpečnost provozu	7	14
A.13	Bezpečnost komunikací	2	7
A.14	Akvizice, vývoj a údržba systémů	3	13
A.15	Dodavatelské vztahy	2	5
A.16	Řízení incidentů bezpečnosti informací	1	7
A.17	Aspekty řízení kontinuity činnosti organizace z hlediska bezpečnosti informací	2	4
A.18	Soulad s požadavky	2	8

Norma ISO/IEC 27005

Tato norma se zabývá doporučením k řízení rizik bezpečnosti informací. Opět souvisí s normou ISO/IEC 27001 tím, že podporuje její obecný koncept. Norma je vytvořena strukturovanou formou a podporuje implementaci informační bezpečnosti, která je založena na přístupu řízení rizik [2].



Obrázek 3: Znázornění procesu řízení rizik bezpečnosti informací, Zdroj: [2]

2.3 Definice, klasifikace a hodnocení aktiv

Aktivum je cizí slovo pro majetek, kde se jedná o veškerý hmotný i nehmotný majetek. Pro ohodnocení aktiv je třeba si nejprve aktiva identifikovat. Tedy seskupit veškerá aktiva, která k sobě logicky patří (programová aktiva, bezpečnostní aktiva, obchodní aktiva apod.). Dále identifikovat vlastníka (pověřenou osobu, která je plně zodpovědná za dané aktivum) každého aktiva, se kterým se následně určuje konkrétní hodnota aktiva [1].

K hodnocení aktiv buď můžeme využít softwarový nástroj, nebo si vytvořit tabulku např. v Excelu. Nyní si musíme stanovit stupnici a hodnotící kritéria, která použijeme k přiřazení ohodnocení určitého aktiva. Tuto stupnici si můžeme určit buď jako peněžní vyjádření, nebo kvalitativními hodnotami. Tato volba závisí na zvážení vedení organizace. Peněžní stupnice vyjadřuje v místní měně hodnotu určitého aktiva.

Kvalitativní vyjádření určuje hodnotu v termínech, jako jsou např. stupnice od velmi nízké, až po kritické [1].

Dalším důležitým aspektem je barevné odlišení. Pokud bychom měli rozsáhlé tabulky s hodnocením aktiv, tak nám vhodně zvolené barvy mohou pomoci k jednodušší orientaci. Výběr a rozsah termínů závisí na organizaci, jak si je zvolí, dále to závisí na bezpečnostních potřebách organizace, nebo její velikosti apod. Pokud má organizace např. zaveden systém řízení kvality (ISO 9001), je možné tento stávající model využít k ohodnocení aktiv. Hlavním principem při ohodnocení aktiv jsou náklady, které by mohly vzniknout při porušení důvěrnosti, dostupnosti a integrity. Tato tři kritéria nám poskytují podklady pro ohodnocení aktiv [1].

Ohodnocení aktiv je zapotřebí provádět s majitelem aktiv. Jeho hodnocení může být subjektivní a je dobré provést interview také s uživatelem daného aktiva. Křížová kontrola je velmi důležitým aspektem k upřesnění hodnoty aktiva. Tuto kontrolu je doporučeno provádět u všech aktiv, která mají pro organizaci vysoké hodnoty [1].

2.3.1 Výpočet hodnoty aktiva

Pro výpočet ohodnocení aktiv můžeme využít různé způsoby. Tím nejjednodušším a nejpoužívanějším je tzv. **součtový algoritmus** [1].

Principem je součet [1]:

$$\frac{Dostupnost + Důvernost + Integrita}{3}$$

Takovýto součtový algoritmus nám poskytuje nejrychlejší způsob, kterým lze získat hodnotu daného aktiva. Dále nám také určuje dopad pro organizaci, který nastane při zničení, popř. poničení daného aktiva [1].

2.4 Bezpečnostní hrozby

Hrozba má potenciální schopnost způsobit nežádoucí incident. Tento incident může mít za následek poničení systému, nebo organizace, popř. jejich aktiv [1].

2.4.1 Základní rozdělení hrozeb

Dělení hrozeb dle původu [1]:

- *Přírodní* – zemětřesení, požár, povodně
- *Způsobené lidským faktorem* – odposlech, chyba uživatele

Dále hrozby rozlišujeme dle úmyslu [1]:

- *Náhodné* – vymazání souboru, zapomenuté dokumenty s důvěrnými daty
- *Úmyslné* – krádež, úmyslné poškození

Z hlediska bezpečnosti je nutné, aby náhodné i úmyslné hrozby byly identifikovány a také odhadnuta jejich úroveň a pravděpodobnost [1].

Hrozby můžeme dělit i podle toho, na jaké aktivum působí [1]:

- *Operační systém*
- *Aplikace*
- *Databáze*
- *Síť*
- *Klient*

2.4.2 Posouzení hrozeb

Hrozby posuzujeme vždy na základě následujících otázek [1]:

- *Ztráta důvěrnosti* – může vést ke ztrátě důvěry vůči zákazníkům, právní odpovědnosti, finanční ztrátě apod.
- *Ztráta integrity* – může vést k přijetí nesprávných rozhodnutí

- *Ztráta dostupnosti* – může vést k neschopnosti vykonávat kritické činnosti
- *Ztráta individuální odpovědnosti* – může vést k podvodu, špionáži, krádeži
- *Ztráta autentičnosti* – může vést k použití neplatných dat, která vedou k neplatným výsledkům
- *Ztráta spolehlivosti* – může vést k nespolehlivým dodavatelům, demotivaci zaměstnanců

Ovšem nesmíme zapomenout na následné efekty hrozby. Pokud uvedeme příklad výpadku elektrické energie, tak ta nemá za následek pouze nedostupnost dat, ale při dlouhodobém výpadku může vést k ohrožení činnosti organizace, nebo fyzické integrity člověka (nemocnice, hasiči, policie) [1].

Mezi nejčastější hrozby můžeme řadit [1]:

- *Selhání dodávky energie*
- *Škodlivý software*
- *Selhání hardwaru*
- *Selhání komunikačních služeb*

2.5 Analýza rizik

Tato analýza se provádí za účelem identifikace zranitelných míst v organizaci. Dále zachycuje hrozby, které působí na informační systém a stanovuje rizika, která jsou příslušná každému zranitelnému místu a hrozbě [1].

Rizikem se rozumí nebezpečí vzniku škody, poškození, ztráty, zničení apod. Tuto skutečnost lze chápat jako možnost odlišného a hlavně nežádoucího vývoje od předpokládaného [3].

S rizikem jsou úzce spjaty tyto pojmy [3]:

- *Neurčitý výsledek* – vždy musí existovat množina variant vývoje
- *Minimálně jedna varianta musí být nežádoucí* – pokud by žádná nebyla, nejedná se o riziko, ale o jistotu žádaného směru vývoje

Rizika rozlišujeme na [1]:

- *Bezvýznamné riziko* – u tohoto rizika není vyžadováno žádné zvláštní opatření. Riziko možno přijmout.
- *Akceptovatelné riziko* – toto riziko je přijatelné se souhlasem vedení. Je zde nutno zvážit náklady na případné řešení nebo zlepšení. Možné riziko, zvýšit pozornost.
- *Mírné riziko* – urgentnost opatření není tak závažná jako u nežádoucích rizik, ovšem je nutno zpravidla bezpečnostní opatření zrealizovat dle zpracovaného plánu vedení firmy. Potřeba nápravné činnosti.
- *Nežádoucí riziko* – tento typ rizika vyžaduje urychlené provedení odpovídajících bezpečnostních opatření, které by riziko snížilo na přijatelnější úroveň. Vysoké riziko, bezprostřední bezpečnostní opatření.
- *Nepřijatelné riziko* – jak je již z názvu patrné, jedná se o nepřípustné, značné, kritické riziko, permanentní možnost úrazu, závažné nehody, nutnost okamžitého zastavení činnosti, odstavení z provozu do doby, než se provedou nezbytná opatření. Práce se nesmí zahájit, nebo pokračovat, dokud se riziko nesníží. Velmi vysoké riziko, zastavit činnost!

2.5.1 Stanovení hranic revize

Stanovení hranic revize se provede ještě před identifikací a hodnocením aktiv. Pokud toto stanovení provedeme pečlivě, umožní nám to vyvarovat se zbytečných činností. Budeme tedy definovat, kterých prvků se analýza rizik bude týkat (např. HW, SW) [1].

2.5.2 Identifikace a ohodnocení aktiv

Tato problematika je blíže popsána v již zmíněné kapitole 2.3.

2.5.3 Hodnocení hrozeb

Hrozba může představovat možnost poškodit zkoumaný systém IT a jeho aktiva. Hrozby mohou být přírodního nebo lidského původu [1]. Blíže popisuje kapitola 2.4.

2.5.4 Odhad zranitelnosti

Odhad zranitelnosti nám odhalí slabá místa ve fyzickém prostředí, organizaci, postupech, personálu managementu, administraci HW, SW, nebo v komunikačním zařízení. Tato místa pak mohou být využita zdrojem hrozby a působit tak škodu na aktivech [1].

2.5.5 Identifikace plánovaných a existujících ochranných opatření

Identifikace plánovaných a existujících ochranných opatření je součástí analýzy rizik. Výsledkem tohoto kroku je seznam všech existujících a plánovaných bezpečnostních opatření [1].

2.5.6 Výběr ochranných opatření

Ochranná opatření slouží k minimalizaci případných rizik. Usnadněný popis různých typů ochranných opatření, jsou zavedeny v rámci normy kategorie ochranných opatření. Mezi nejdůležitější patří tzv. všeobecně aplikovatelná ochranná opatření [1].

Základní kategorie [1]:

- Řízení a politiky bezpečnosti IT
- Kontrola bezpečnostní shody
- Řešení incidentů
- Personální opatření
- Provozní problémy
- Plánování kontinuity činnosti organizace
- Fyzická bezpečnost

2.5.7 Odhad rizik

Tento krok slouží k identifikaci a odhadu rizik, které ohrožují aktiva. Tedy musíme zjistit, co a proč nám hrozí [1].

2.5.8 Přijetí rizik

Po identifikaci a odhadu rizik, po výběru a revizi ochranných opatření nám vždy zůstanou zbytková rizika. Úplně bezpečný systém je jen teoretická hypotéza, ke které se můžeme v reálném provozu pouze limitně přiblížit. Tato zbytková rizika se dělí na akceptovaná nebo neakceptovaná rizika. Pokud riziko neakceptujeme, musí proběhnout znovu výběr ochranných opatření a odhad rizika [1].

2.5.9 Politika bezpečnosti systému IT

Tato část by měla obsahovat podrobnosti požadovaných ochranných opatření a také popis, proč jsou nezbytná [1].

2.5.10 Plán bezpečnosti IT

Shrnující dokument, který ve stručnosti popisuje veškeré akce, které musí být uskutečněny, aby mohla být ochranná opatření implementována [1].

2.6 Management bezpečnosti pasivní vrstvy

Management pasivní vrstvy využívá kombinaci softwaru, elektroniky a produktů strukturované kabeláže, a tím umožňuje uživatelům sledování a správu jejich investic od fáze plánování, přes návrhy, instalaci, až po případný upgrade infrastruktury. Typickým příkladem Managementu bezpečnosti pasivní vrstvy je NISS (Network Infrastructure Security Solution) a definuje tři stupně zabezpečení [1].

2.6.1 Stupeň 0 – identifikátory

Stupeň 0 nezajišťuje žádnou fyzickou ochranu komunikace. Usnadňuje pouze správu systému a naviguje správce sítě, jak správně zapojit pomocí barevného rozlišení prvků.

U metalických i optických konektorů, propojovacích kabelů, popisových štítků a zejména barevných značkovacích kroužků na všechny druhy propojovacích kabelů lze využít celou řadu barev [1].

Základními identifikačními prvky jsou [1]:

- Barevné propojovací kabely
- Barevné značkovací kroužky

Obrázek 4: Kabelové identifikátory, barevný patch cord, Zdroj: [1]

2.6.2 Stupeň 1 – blokátory

Tento stupeň už zajišťuje základní fyzickou ochranu tím, že blokuje porty (proti připojení, nebo proti odpojení) a blokuje přístup (do kabelových tras a datových boxů) [1].

Blokátory dělíme [1]:

- Blokování portu (datového metalického, optického nebo USB portu)
  - Kabeláže
  - Aktivního prvku
- Uzamčení portu proti neoprávněnému odpojení
- Blokování datového boxu proti neoprávněnému přístupu a připojení nežádoucího zařízení
- Blokování kabelových tras proti neoprávněnému přístupu ke kabelovým svazkům

Obrázek 5: Blokátor optického konektoru LC a datového portu RJ-45, Zdroj: [1]

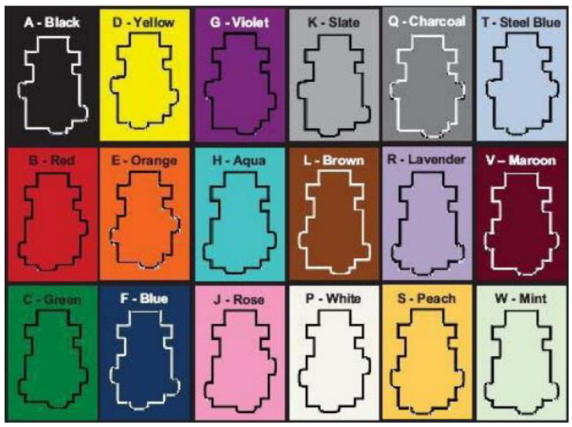
2.6.3 Stupeň 2 – klíčování konektorů

V tomto stupni jsou umístěny prostředky znemožňující připojení skupin metalických propojovacích kabelů a optických duplexních propojovacích kabelů do nepovolených portů. Jedná se o technické řešení využívající klíčování konektorů [1].

Princip bezpečnostního opatření je postaven na následujících bodech [1]:

- Neklíčovaný plug nelze zasunout do žádného klíčovaného jacku
- Klíčovaný plug nelze zasunout do neklíčovaného jacku, ani do jacku s jiným typem klíče
- Stejný princip platí také pro optické konektory

Klíč, který je na konektorech umístěn v pozitivní i negativní formě, je postaven na principu tvarové úpravy konektorů v trojrozměrném provedení.



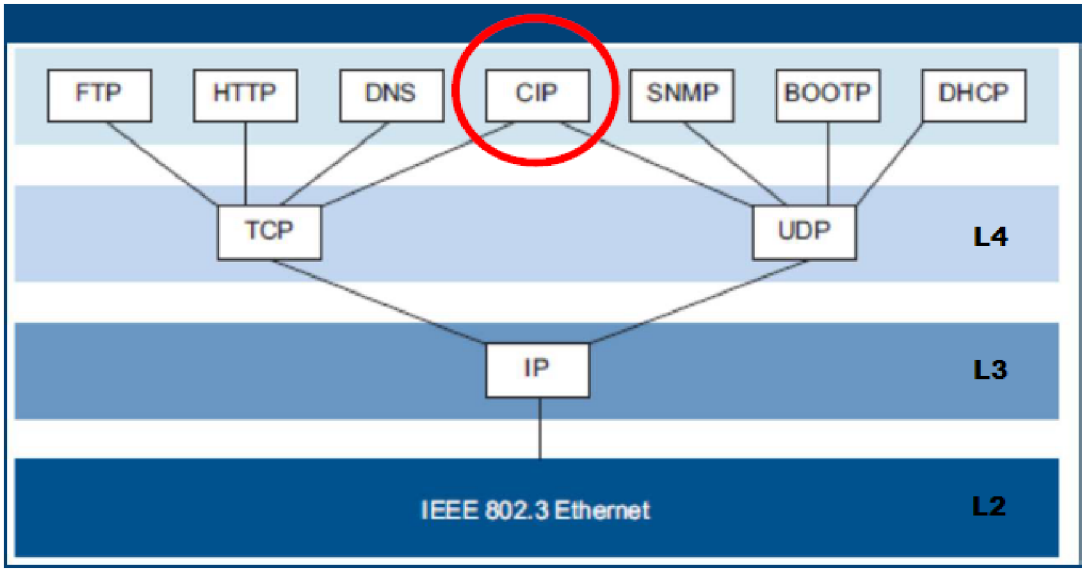
Obrázek 6: Různé tvary konektorů LC v klíčovaném provedení, Zdroj: [1]

2.7 Průmyslová bezpečnost

Bezpečnost v průmyslu je zkráceným názvem pojmu bezpečnost průmyslového prostředí ICT. Bezpečnost ICT v průmyslu je klíčovým prvkem a je dosahována maximálními možnostmi aplikovaných doporučených bezpečnostních doporučení. Základním parametrem průmyslových aplikací je práce v reálném čase, proto jsou požadavky na průmyslovou síťovou infrastrukturu tak specifické a nekompromisní. Tímto splňuje průmyslová infrastruktura také požadavky na síť s maximální dostupností [1].

2.7.1 Industrial Ethernet

Protokol EtherNet/IP byl založen na bázi Ethernetu. EtherNet/IP byl celosvětově standardizován jako průmyslový komunikační protokol. Protokol využívá standardizovaných transportních protokolů TCP/IP a UDP/IP [1].
CIP (Common Industrial Protocol) je na bázi EtherNet/IP a rozšiřuje ethernetovské použití pro oblast aplikací pro průmyslovou automatizaci [1].



Obrázek 7: Ethernet CIP v ISO/OSI referenčním modelu, Zdroj: [7]

2.8 Parametry průmyslové síťové infrastruktury

Typické parametry jsou zakotveny a zabudovány v samotné standardizaci Industrial Ethernet [1].

Tato zařízení jsou určená pro nasazení ve specifických podmínkách [1]:

- Teplotní odolnost
- Odolnost vůči vodě a vlhku
- Odolnost vůči agresivnímu prostředí
- Odolnost vůči mechanickým vlivům
- Odolnost vůči elektromagnetickému rušení

Veškeré tyto požadavky se následně projeví na konstrukci jednotlivých komponentů (pasivní i aktivní vrstva) [1].

Prvky pasivní vrstvy [1]:

- *Kabely* – zodolněné, speciální či pancéřované plášťování
- *Konektory* – standardní v odolném provedení (krytí) nebo speciální (např. M12)
- *Datové rozvaděče* – 19“ ve specifickém provedení či s lištami DIN

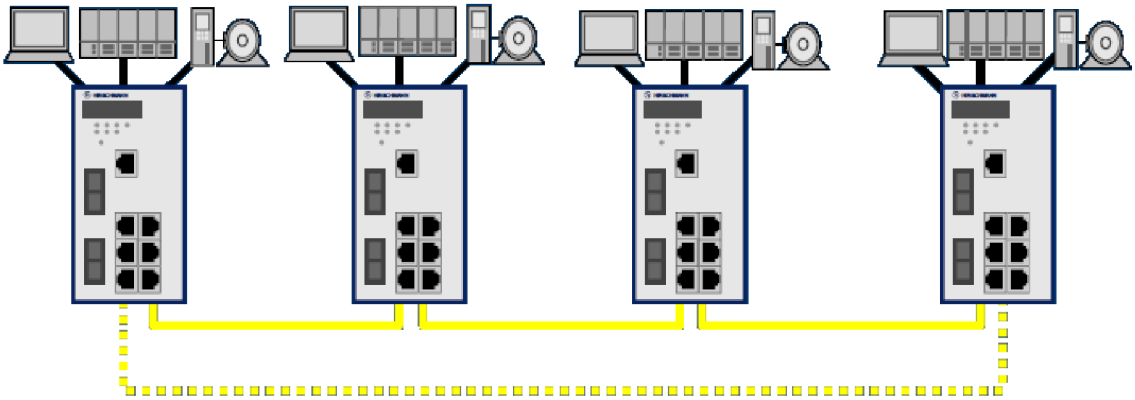
Aktivní prvky [1]:

- Bezventilátorové provedení
- Provedené pro montáž na DIN lišty
- „coating“ elektroniky (máčení ve speciálních odolných lacích)
- Speciální odolné vodotěsné plášťování

2.8.1 Topologie

Vývoj topologie v průmyslovém prostředí byl dříve dán zařízeními, která komunikovala s dohledovými pracovišti pomocí sériové komunikace (sběrnicová topologie), poté přichází Ethernet/IP pro průmysl (topologie hvězda) a na závěr při požadavku na topologickou redundanci vznikla kruhová topologie s různými úrovněmi zabezpečení [1].

V dnešní době je standardní průmyslová topologie ve většině případů kruhová (ring). Vzniká z liniové topologie, a to tak, že se propojí počáteční a koncové zařízení, viz následující obrázek [1].



Obrázek 8: Vznik kruhové topologie z linkové pomocí redundantní trasy, Zdroj: [7]

Rozšiřování topologie kruh může být řešeno několika způsoby [1]:

- Napojením dalších kruhů (Sub-ring) na zařízení v hlavním kruhu
- Napojením kruhů pomocí linek v redundantním provedení – Couplink
- V některých případech se používá typické topologie hvězdy při napojení na koncové přepínače

2.8.2 Redundance

Redundance je dalo by se říct nadbytečností, ovšem slouží ke zvýšení bezpečnosti provozu ICT zařízení [1].

Výběrová kritéria pro volbu redundance [1]:

- Použití napojení pomocí jednoho zařízení je úsporné, ale při výpadku tohoto zařízení není napojení mezi sítěmi.
- Použití napojení pomocí dvou zařízení je praktičtější, jelikož při výpadku kteréhokoli zařízení stále existuje napojení.
- Použití napojení pomocí dvou zařízení s kontrolní linkou nemá žádný vliv na provoz v žádném kruhu. Řeší pouze komunikaci mezi redundantními zařízeními.

Redundance topologická

Základní topologie u linkových tras je kruh. Ten vzniká, jak již bylo zmíněno, uzavřením linkové topologie redundantní trasou [1].

Základní parametry [1]:

- Síťová vzdálenost 3000 km
- Vzdálenost mezi dvěma zařízeními do 120 km
- Doba reakce dle základního nastavení < 10 ms nebo < 200 ms
- Síť může obsahovat cca 50 zařízení typu switch
- Pracuje na sítích 10 Mbps až 10 Gbps

Redundance zařízení

Tato redundance je podporována na všech úrovních. Základem je redundance zařízení při napojení dvou kruhů pomocí kontrolní linky. Extrémní redundantní zapojení je paralelní, neboli duplikovaná síť [1].

Redundance napájení

Tento typ redundance je většinou řešen různými způsoby napájení průmyslových ICT zařízení [1]:

- Zdvojené standardní napájení 230 V/50 Hz v rozsahu 90 až 265 V AC – typicky 2 zdroje
- Napájení 24 nebo 48 DC v rozsahu 18 až 60 V
- Kombinace napájení AC a DC s automatikou, neboli přepínaní

2.9 Mission Critical Network

Pojmem Mission Critical je označen požadavek na plnou funkčnost systémů životně důležitých pro fungování organizace. Pro komunikační sítě se používá pojem Mission Critical Network (MCN) [3].

Tři základní pravidla pro MCN [1]:

- *Jednoduchost*
  - V návrhu síťové infrastruktury snížení komplexního použití
  - Zrychlení odstraňování závad a údržba
  - Snížení rizika snížením komplexnosti infrastruktury a nákladů na školení
  - Předcházení lidským chybám
- *Separátní rutinní provoz*
  - Logické oddělení sítí s odlišným použitím
  - Správa šířky přenosového pásma
  - Izolování vadných či nespolehlivých aplikací
- *Spolehlivost*
  - Činnost síťové infrastruktury ve ztížených podmínkách – prach, teplota …
  - Minimální výpadky sítě
  - Životnost síťové infrastruktury minimálně 15 let
  - Nadčasovost
  - Dosažení spolehlivosti maximální dostupností

Základní požadavky na odolnost systému vůči vlivům prostředí [3]:

- *Rozsah pracovních teplot* – u prvků komerčních bývá rozsah 5 °C až 40 °C, u prvků MCN je obvyklým požadovaným rozsahem 0 °C až 60 °C, nebo -40 °C až 70 °C, někdy dokonce i více.
- *Odolnost proti chemickým vlivům prostředí* – vlhkost, voda, olej, benzin, odmašťovadla, působení různých chemikálií. Kvůli těmto vlivům je potřebná vysoká odolnost materiálů plášťů kabelů, kontaktů konektorů a u aktivních prvků ochrana elektroniky speciálním lakem.
- *Odolnost vůči povětrnostním podmínkám* – prašnost, vlhkost, voda, UV záření

- *Odolnost vůči ostatním vlivům prostředí* – prašnost (až velmi vysoká), vibrace a rázy, ultrazvuk, rentgenové nebo radiační záření (potřebná odolnost materiálů a u aktivních prvků potřebná verze bez ventilátorů).

2.10 Propojení sítí se zabezpečeným oddělením

Integrovanou komunikační infrastrukturu podniku navrhujeme jako fyzicky oddělené sítě se vzájemným zabezpečeným propojením. Pokud bychom se chtěli napojit do vnějších veřejných sítí, můžeme u většiny případů použít pro oddělení sítí Security Router nebo Firewall. Pro oddělení sub-sítí v rámci hierarchické infrastruktury se používají aplikační firewally [4].

I v rámci typické struktury integrované sítě podniku potřebujeme mít často lokálně zabezpečená připojení, např. pro údržbu, diagnostiky apod. V mnoha případech je dobré mít takové zabezpečené připojení i se vzdáleným přístupem, což urychlí diagnostiku a není potřeba čekat na příchod servisního technika. Kolikrát se může stát, že servisní technik na dálku zjistí, že žádná porucha nenastala a stav zařízení byl vyvolán chybou obsluhy. Takovýmto způsobem uvede zařízení do správného stavu nebo informuje obsluhu o případných úkonech [4].

Integrovanou podnikovou komunikační infrastrukturu je potřebné oddělit nejen z pohledu aplikačního, ale i z hlediska systémového členění vnějších a vnitřních napojení. Jednotlivé sub-sítě se většinou oddělují pomocí aplikačních firewallů. To platí především v případech oddělení řízení kritických aplikací od administrativní sítě (kamerový systém), nebo kritického výrobního procesu (výrobní linky, stroje) [4].

2.11 Napájení a integrovaná infrastruktura

Současná komunikační infrastruktura umožňuje také integraci napájení. Dnes je již běžnou záležitostí napájení vybraných koncových zařízení po síti v prostředí EtherNet. Tento typ napájení se nazývá Power over EtherNet – PoE [4].

Systém napájení po ethernetu je běžně používanou funkcí u mnoha zařízení, pro která dostačuje poskytovaný příkon. Standardní napětí PoE je minimálně 48 V DC. Ovšem pozor na to, že některé zařízení mají možnost napájení z externího zdroje, které se liší napětím (např. 12 V DC nebo 24 V DC). Tato napětí nemají s PoE nic společného [4].

Nejčastější zařízení napájená PoE [4]:

- IP telefony
- IP kamery
- Přístupové body Wi-Fi sítí
- Zobrazovací jednotky času
- Kontrolní panely různých systémů
- Prodejní automaty
- Hrací automaty
- A spoustu dalšího

V poslední době proniká PoE i do oblastí, jako je napájení různých zařízení, která nemají s komunikační infrastrukturou nic společného (např. nabíječky mobilních telefonů, tabletů, ale i holicích strojků apod.) [4].

Definice [4]:

- *PSE (Power Sourcing Equipment)* – zařízení, které napájí (zdroj PoE)
- *PD (Powered Device)* – zařízení, které je napájeno

Po připojení síťového zařízení na PSE, musí nejdříve PSE určit, zda je připojené zařízení PD nebo nikoli. Zjišťuje, zda je protější zařízení kompatibilní s PoE, pokud by nebylo, hrozí poškození. Pokud je kompatibilita v pořádku, může se zapnout napájecí napětí [4].

2.12 Profinet Input / Output

Koncepce architektury komunikačního systému Profinet je modulární, tedy lze jeho funkční schopnosti do jisté míry volit dle povahy dané úlohy [3].

Rozlišujeme varianty [3]:

- *Profinet CBA* – koncept modulární výstavby komunikačního systému z předem připravených komponent.
- *Profinet IO* – varianta určená k realizaci propojení decentralizovaných periferií především v cyklickém režimu komunikace.

2.12.1 Profinet IO

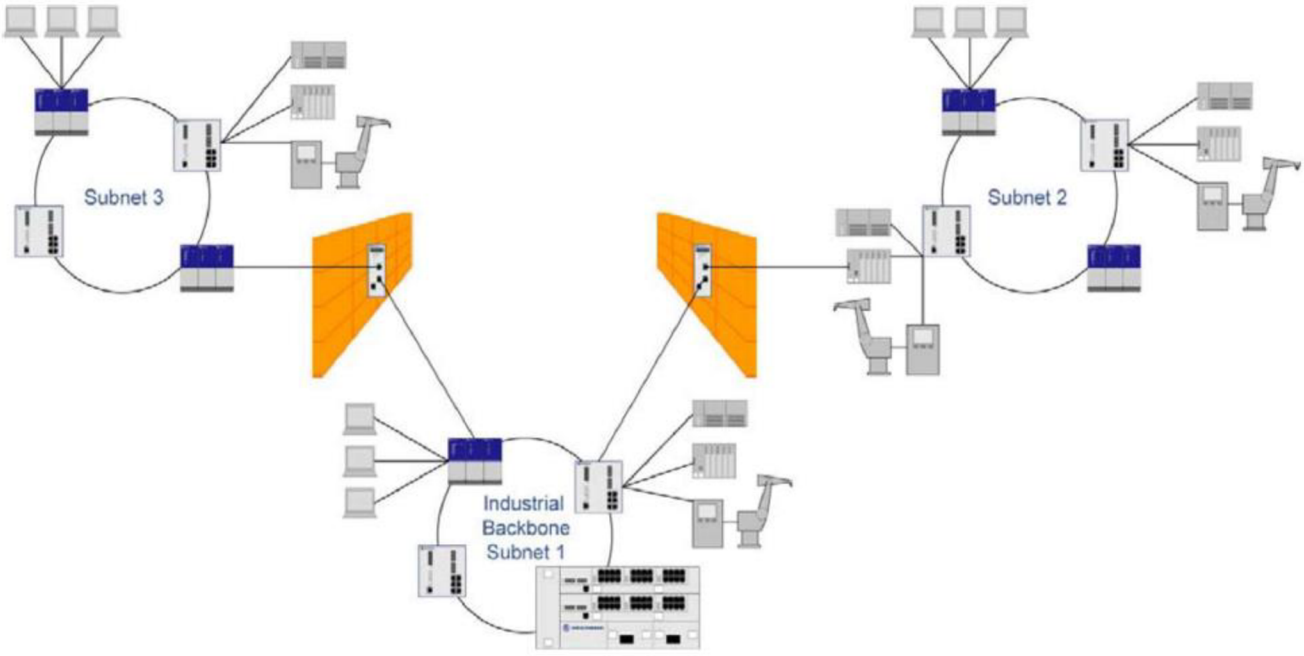
Je vlastní fyzické provedení průmyslového Ethernetu. Jeho úkolem je zajistit rychlé a spolehlivé přenosy dat mezi decentralizovanými moduly Input / Output a řídícími stanicemi po síti Ethernet [3].

Profinet IO musí zajistit tyto funkce [3]:

- Cyklickou výměnu dat mezi moduly Input / Output a řídícími stanicemi
- Přenos s velkou prioritou a kvitování výstražných hlášení nesoucích informaci o stavu zařízení
- Přenos acyklických dat v režimu bez reálného času
- Rychlou výměnu dat přímo mezi koncovými stanicemi bez zásahu řídících stanic
- Synchronizaci stanic pracujících v režimu reálného času
- Automatické přidělení adres zařízením

2.13 Zónové zabezpečení

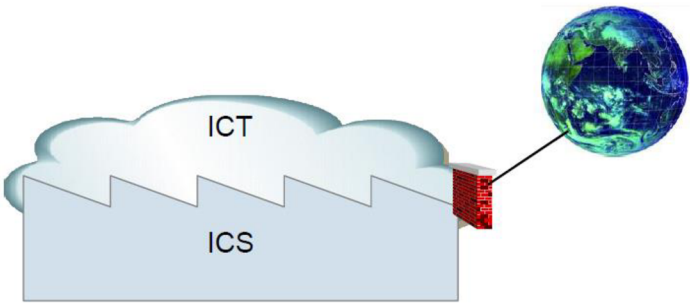
Síť se rozdělí na pracovní skupiny, které spolu mají něco společného a navzájem se oddělí. Po tomto oddělení platí správa jednotlivé buňky pouze pro tu danou buňku a neplatí pro ostatní. Je to důležité hlavně z toho důvodu, že pokud máme zařízení od různých výrobců, tak každé zařízení má jiný způsob spravování [7].



Obrázek 9: Příklad zónového řešení, Zdroj: [7]

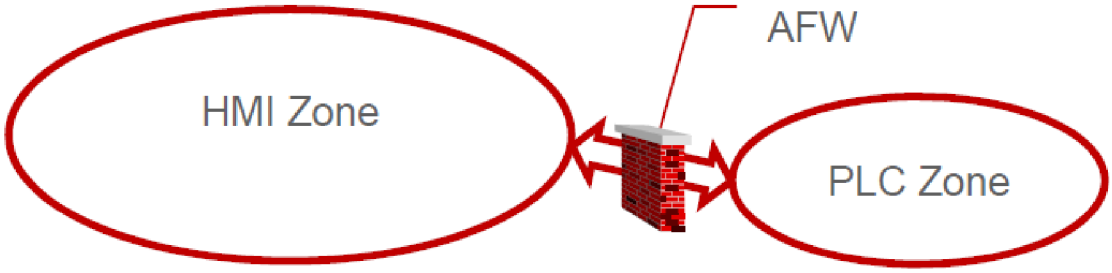
2.13.1 Aplikační firewall

Pokud budeme brát standardní aplikace a oddělení zón, tak nám postačí router, který má v sobě zabudovaný základní firewall [7].



Obrázek 10: Standardní aplikace, Zdroj: [7]

Ovšem pro ICS řešení oddělení zón nám lépe poslouží samotný aplikační firewall, např. při oddělení průmyslových výrobních systémů. Ideální aplikační firewall je dvouportové Tofino Xenon, které má pomocí škálovatelných softwarových modulů mnoho funkcionalit. Hlavní nasazení tohoto firewallu je do průmyslových zónových řešení. Může nám např. oddělovat kamerový systém, nebo kritické výrobní procesy [7].



Obrázek 11: Zónové řešení pomocí aplikačního firewallu, Zdroj: [7]

3 ANALÝZA SOUČASNÉ SITUACE

V této kapitole budu popisovat současnou situaci ve společnosti. Budou zde uvedeny současné prvky infrastruktury, kabeláž a také celková bezpečnost.

3.1 Popis společnosti

Vybraná společnost si nepřeje být v této práci jmenována z důvodu ochrany citlivých informací a údajů. Uvedu tedy pouze stručný popis podniku.

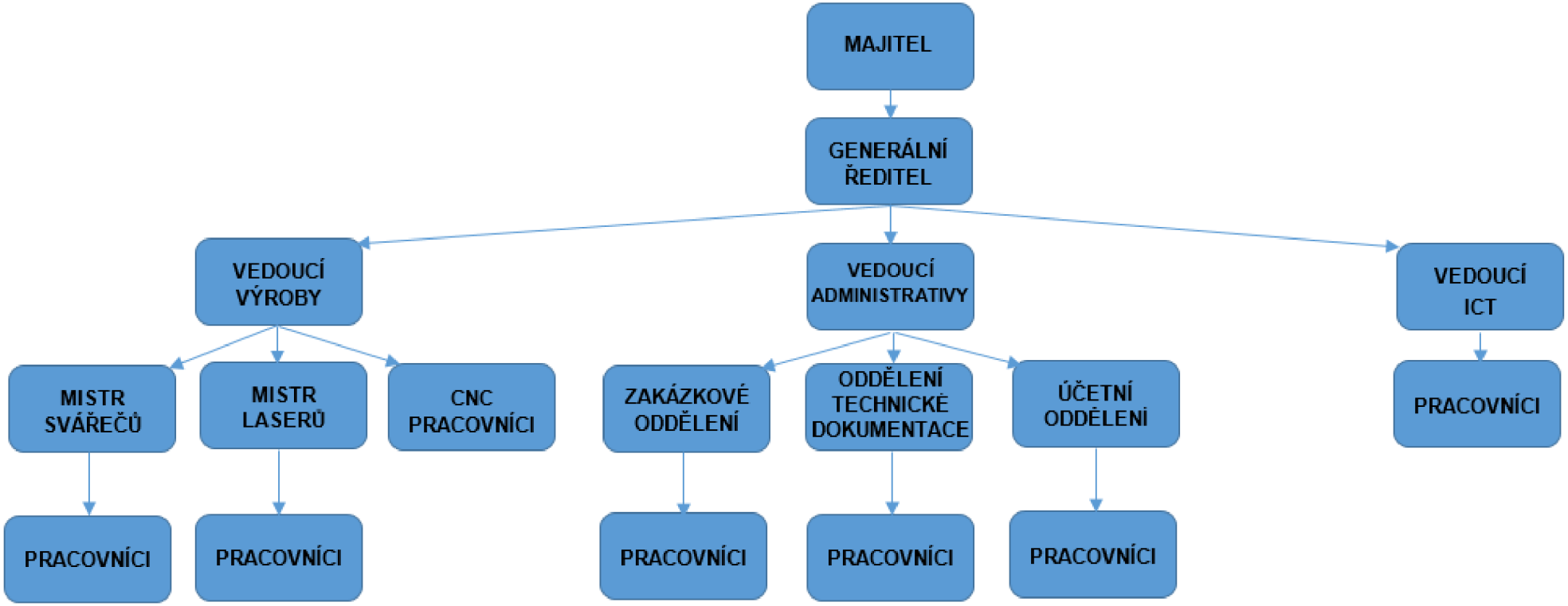
Jedná se o společnost XY, s.r.o., která se zabývá strojírenskou výrobou se zaměřením na zpracování plechů, řezání laserem a ohýbání CNC stroji. Provádí se zde také svářečské, zámečnické a lakýrnické práce. Společnost sídlí v Brně a má 50 zaměstnanců. Firma disponuje tím, že dodává své výrobky po celém území České republiky a částečně i na Slovensko. V budoucnu není vyloučeno, že firma bude expandovat na zahraniční trhy, zejména pak rakouský a polský. K dodávkám svých výrobků používají vlastní vozový park, díky němuž mohou rozvést většinu výrobků ke svým zákazníkům, pokud si zákazník nezajistí vlastní dopravu.

Prosperita firmy závisí na spokojenosti zákazníků, proto je kvalita výrobků tím nejdůležitějším aspektem. Firma má zaveden systém řízení jakosti dle ISO 9001, který neustále zlepšuje.

ICT správa je řešena pověřenými pracovníky, kteří se starají o chod a správu ICT prvků a celé síťové infrastruktury včetně serveru. ICT oddělení má veškerou zodpovědnost za chod a funkčnost sítě.

Společnost vede jeden majitel, který řídí obecný chod firmy, dále také generální ředitel, který kontroluje a dbá na spolehlivost firmy. Dále je zde oddělení administrativy, již zmíněné ICT oddělení a oddělení výroby, pod kterou spadá řezání laserem, ohýbání na CNC strojích, svářečské a zámečnické práce a také lakovna.

3.1.1 Organizační struktura



Obrázek 12: Organizační struktura, Zdroj: [Vlastní]

3.1.2 Strojní park

Jak jsem již zmínil, firma má k dispozici lasery pro přesné dělení různých kovů dle požadavků zákazníka. Data do laserů se přivedou pomocí PLC (Programmable Logic Controller), který tato data zpracuje a následně nastaví laser pro správné vykonání řezu.

Firma vlastní dva typy řezacích laserů:

1) *CNC laserový řezací stroj Trumpf Trumatic 3030 TLF 3200W*

Obrázek 13: Laser Trumpf 3030, Zdroj: [8]

Tento laser disponuje výkonem 3200 W a řeznou plochou 3000 x 1500 mm. S přesností cca 0,2 mm a šířkou spáry řezu 0,2 – 0,5 mm. Hmotnost polotovaru, který se na stroji vyřeže, je maximálně 710 kg.

Na tomto stroji se mohou zpracovávat materiály:

- Oceli konstrukční uhlíkové a nízkolegované do tloušťky 20 mm
- Oceli legované, korozivzdorné (neboli nerez) do tloušťky 12 mm
- Slitiny hliníku do tloušťky 6 mm

2) *CNC laserový řezací stroj Trumpf TruLaser 3530 TLF 3200W*

Obrázek 14: Laser Trumpf 3530, Zdroj: [9]

Laser tohoto typu se nějak zvlášť neliší od výše zmíněného, má stejné schopnosti až na pár výjimek, a to:

- Přesnost cca 0,1 mm (oproti 0,2 mm)
- Šířka spáry řezu 0,2 – 0,4 mm (oproti 0,2 – 0,5 mm)
- Slitiny hliníku do tloušťky 8 mm (oproti 6 mm)

Dále firma vlastní dvě CNC ohýbačky, které si pracovník sám nastaví a následně vykonává potřebný ohyb.

1) *CNC ohraňovací hydraulický lis Trumpf Trumabend V85*

Obrázek 15: CNC ohýbačka Trumpf V85, Zdroj: [10]

Tento stroj disponuje lisovací sílou 850 kN a maximální ohýbanou délkou 2000 mm.

2) *CNC ohraňovací hydraulický lis Trumpf Trumabend V130*

Obrázek 16: CNC ohýbačka Trumpf V130, Zdroj: [11]

Tento stroj má lisovací sílu vyšší než předchozí, a to 1300 kN. Maximální délku ohýbaného materiálu má též jinou, v tomto případě je to 3060 mm.

Firma má také k dispozici přístroj, kterým provádí spektrální analýzu výrobků z plechů, tedy plechů z materiálů na bázi železa a hliníku. Jedná se o vysoce přesný, jiskrový, mobilní, optický, emisní spektrometr Belec Compact Port. Zařízení slouží k velmi přesné chemické analýze nebo k rychlému třídění kovových materiálů přímo v provozu. Spektrometr poskytuje velmi přesnou analýzu vysokolegovaných materiálů i prvků s nízkými koncentracemi a to včetně obsahu uhlíku pod hodnotami 0,1% koncentrace. Výsledky analýz jsou pak zobrazovány v přehledném rozhraní. Z těchto výsledků lze pak vytvořit statistiky, jako průměr a odchylku, nebo zatřídění materiálů. Následně je možné si tyto statistiky uložit ve formátu PDF k uschování, nebo vytištění.

Obrázek 17: Belec Compact Port, Zdroj: [12]

3.2 Popis infrastruktury

Hlavní nedostatky:

- Komerční infrastruktura
- Nekontrolovaná manipulace s daty

Interní síť ve firmě není řešena příliš profesionálně. Pro kabeláž jsou zde použity komerční typy metalických kabelů, dokonce nestíněné. Kabeláž je vedena zčásti v lištách umístěných na zdech, zčásti v drátěných žlabech. Tudíž agresivní prostředí průmyslu a elektromagnetické záření se v tomto případě nebere v potaz. Některé části kabeláže vedené v lištách jsou již ztrouchnivělé a rozpadlé, kabely jsou někde i volně visící, což není příliš profesionální, natož bezpečné. Centrálním místem je technická místnost, kde jsou soustředěny veškeré aktivní prvky infrastruktury a také server.

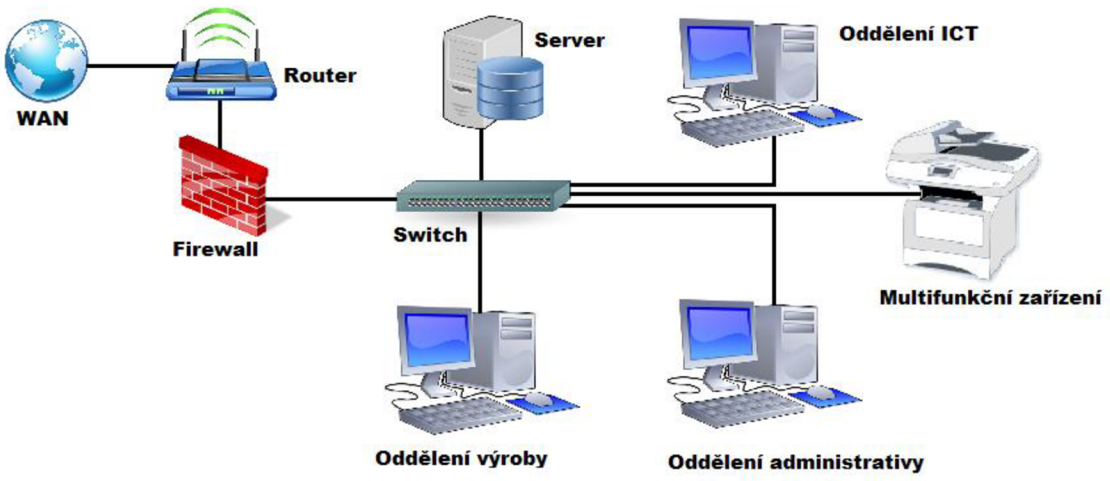
Aktivní prvky firemní sítě jsou komerční produkty, které neodpovídají náročnosti a požadavkům průmyslového prostředí. Prvky jsou uloženy v datovém rozvaděči, který je opatřen ventilátorem. I samotné prvky mají ventilátorové řešení, což je v průmyslu vyloučeno. I když není datový rozvaděč umístěn přímo v prostorách výrobních hal, je značně zanesen vodivým prachem a ostatními nečistotami, které zkracují životnost prvků.

V administrativní oblasti má každý pracovník svoji pracovní stanici. Na těchto stanicích je nainstalován operační systém Microsoft Windows 7, do kterého se každý pracovník přihlašuje pomocí svého jména a hesla. Na stanicích je nainstalován antivirový program od společnosti Kaspersky, kde se pravidelně aktualizují virové databáze (každou hodinu). Veškerá data, která potřebují pracovníci z administrativní oblasti ke své práci, jsou uložena na jediném serveru. Tedy k serveru má přístup každý pracovník a může si zkopírovat jakákoli data a uložit si je na svůj disk v počítači, popř. flash disk apod. Nikdo pracovníky nekontroluje, jaká data si stahují a kam si je ukládají. Pracovní stanice jsou napojeny na záložní UPS, které dokáží udržet napájení při výpadku elektrické energie až na 20 minut. Díky této technologii mají pracovníci čas uložit veškeré rozpracované úkony a řádně vše ukončit. Pracovní stanice jsou do interní sítě připojeny přes kabel. Wi-Fi připojení ve firmě sice existuje, ale není využíváno žádným oddělením ke své činnosti. V administrativní části se také nachází multifunkční zařízení, které je rovněž zapojeno do interní sítě. K tomuto zařízení mají přístup všichni pracovníci ze všech oblastí.

V oblasti výroby je umístěn jeden stolní počítač, na kterém běží firemní informační systém. Tento počítač je také komerčního provedení a není nijak uzavřen nebo chráněn před nepříznivými účinky výroby. Tento počítač je také zapojen do firemní sítě přes kabel. Do informačního systému pracovníci z oblasti výroby zaznamenávají ukončení zadané práce, které má několik atributů. Tento počítač není vybaven nijak zvlášť výkonným hardwarem, proto často dochází k výpadkům, což má ale obvykle za následek vodivý prach, který se dostává do počítače.

V oddělení ICT je umístěn již zmíněný datový rozvaděč s aktivními prvky sítě. Je zde umístěn také server, na kterém je nainstalován operační systém Microsoft Windows Server 2008 R2. Server je opatřen diskem o kapacitě 1 TB. Dále má firma k dispozici síťové úložiště NAS o velikosti 2 TB, které ovšem slouží pouze pro zálohování serveru. Emailová a webová komunikace je řešena externě přes internetového poskytovatele. Dále je zde umístěna jedna pracovní stanice pro správce sítě, na této stanici je rovněž nainstalován operační systém Microsoft Windows 7 s antivirovým programem od společnosti Kaspersky.

Síťová infrastruktura ve firmě je zapojena do topologie hvězda, což v průmyslovém prostředí není obvyklé. Ideálně by měla být infrastruktura zapojena do topologie kruh. Na následujícím obrázku je zobrazena zjednodušená topologie sítě ve firmě.



Obrázek 18: Infrastruktura ve firmě, Zdroj: [Vlastní]

3.3 Zhodnocení analýzy současné situace

Z provedené analýzy současné situace ve firmě je zřejmé, že je nutné navrhnout a vybudovat novou síťovou infrastrukturu a zavést systém řízení bezpečnosti informací. Je zapotřebí pravidelně kontrolovat pracovní stanice a aktivní prvky sítě. Dále je potřeba, aby citlivá data nebyla přístupná všem zaměstnancům firmy, kde hrozí jisté nebezpečí odcizení důležitých dat a informací. Tato rizika je nutné eliminovat na minimum, aby nemohlo dojít ke zneužití nezabezpečené sítě.

Velké nebezpečí také hrozí v napadení sítě malwarem nebo virem, který by mohl způsobit značné škody. Je nezbytné školení všech zaměstnanců v oblasti systému řízení bezpečnosti informací, aby nedocházelo k situacím, kdy hrozí firmě existenční dopad. Firma má sice firewall, který brání v přístupu určitých paketů nebo webových stránek, ale není nastaven až do takové míry, aby zabránil všemu, a především není tak kvalitní, jak by do průmyslového prostředí měl být.

V další části práce se budu zabývat analýzou rizik, návrhem řešení ke snížení daných rizik a návrhem síťové infrastruktury.

4 VLASTNÍ NÁVRHY

V této kapitole se budeme zabývat vlastním návrhem řešení. Bude zde zpracována analýza rizik, identifikace a ohodnocení aktiv, hrozeb a zranitelností. Dále bude zpracována míra zavedení ISMS s návrhem infrastruktury.

4.1 Analýza rizik

V kapitole analýza rizik si nejdříve zpracujeme identifikaci a ohodnocení aktiv. Následně pak identifikaci hrozeb a zranitelností, kde si sestavíme matici zranitelností a stanovíme míru rizika.

4.1.1 Identifikace a hodnocení aktiv

Nejprve je důležité určit správné ohodnocení aktiv tak, aby bylo na první pohled jasné, jak jsou daná aktiva pro firmu důležitá. Zpracování těchto ohodnocení můžeme vidět v následující tabulce.

Tabulka 2: Ohodnocení aktiv, Zdroj: [Vlastní]

Hodnota aktiva	Slovně	Význam
1	nevýznamné	Nemá dopad na firmu, lehce nahraditelné, nízké náklady
2	málo významné	Lehký dopad na firmu, aktiva s určitou hodnotou, potřebné
3	významné	Finanční ztráta, či potíže při chodu firmy
4	cenné	Větší finanční problémy, vážné problémy, které mohou vést k omezení chodu firmy
5	velmi cenné	Klíčová aktiva, bez kterých by firmě hrozili existenční potíže

V další tabulce jsou uvedena aktiva, která byla identifikována. Nejsou zde uvedena veškerá aktiva firmy, pouze ty nejdůležitější z pohledu firmy. U aktiv se hodnotí dopad na dostupnost, důvěrnost a integritu. Hodnotu aktiva dostaneme tak, že sečteme všechny tři komponenty a poté ji vydělíme jejich počtem, tím dostaneme celkovou hodnotu aktiva.

Z tabulky můžeme vidět, že pro firmu jsou nejdůležitějšími aktivy data, informační systém, data z AutoCadu. Z hardwaru to jsou samozřejmě stroje a síťová infrastruktura. Ze služeb pak serverová komunikace, jelikož k serveru se připojují všichni zaměstnanci, aby mohli plnit svoji práci.

Tabulka 3: Identifikovaná a ohodnocená aktiva, Zdroj: [Vlastní]

Aktivum (A)	Zdroj	Hodnota
Data	IS	5
	Data	5
	AutoCad	5
	DB zákazníků	4
HW	Server	4
	NAS	4
	PC	2
	Kamerový systém	3
	Stroje	5
	Síťová infrastruktura	5
SW	OS	1
	MS Office	2
	AutoCad	3

4.1.2 Identifikace hrozeb a zranitelností

Abychom mohli sestavit matici zranitelností, je nutné si nejdříve identifikovat a sepsat hrozby a určit jejich pravděpodobnost, s jakou mohou nastat. V následující tabulce je zobrazeno ohodnocení hrozeb a zranitelností.

Tabulka 4: Ohodnocení hrozeb, Zdroj: [1]

Pravděpodobnost	Slovně	Význam
1	žádný dopad na organizaci	bezvýznamné riziko
2	zanedbatelný dopad na organizaci	akceptovatelné riziko
3	potíže či finanční ztráty	mírné riziko
4	vážné potíže či podstatné finanční ztráty	nežádoucí riziko
5	existenční potíže	nepřijatelné riziko

Nyní je nutné vybrat hrozby, které by mohly ohrozit firemní aktiva a omezit tím chod celé firmy. Vybrány byly podle nejrůznějších doporučení, zkušeností nebo názorů. Standardní hrozby jsou brány z normy ČSN ISO/IEC 27005, přílohy C. V následující tabulce vidíme identifikované hrozby a jejich ohodnocení.

Tabulka 5: Identifikace a ohodnocení hrozeb, Zdroj: [Vlastní]

Hrozba			Pravděpodobnost
Fyzické poškození	1	Požár	2
	2	Voda	1
	3	Zničení zařízení	3
	4	Prach	4
Dostupnost služeb	5	Výpadek elektrické energie	4
	6	Výpadek internetu	3
	7	Výpadek IS	3
	8	Výpadek serveru	2
	9	Výpadek interní sítě	4
Důvěrnost služeb	10	Neoprávněný přístup do sítě	3
	11	Neoprávněný přístup do IS	3
	12	Neoprávněný přístup na server	3
	13	Škodlivý software	3
	14	Zneužití nebo krádež disků	2
	15	Krádež technického vybavení	4
	16	Získání dat z vyřazených médií	3
Lidský faktor	17	Fyzické poškození zařízení	3
	18	Nedodržování směrnic	4
	19	Nedbalost při obsluze zařízení	3
	20	Nedostatečná dokumentace	2
	21	Ztráta důvěrných dat	3
Technické selhání	22	Selhání serveru	3
	23	Selhání pracovních stanic	3
	24	Selhání strojů	2
	25	Selhání diskového úložiště NAS	2
	26	Selhání síťových prvků	2
Neoprávněné činnosti	27	Neoprávněné zkopírování dat	4
	28	Neoprávněný přístup do budovy	2
	29	Porušení mlčenlivosti pracovníků	4
	30	Zneužití uživatelských práv	3
	31	Zneužití administrátorských práv	2

Tabulka 6: Matice zranitelnosti, Zdroj: [Vlastní]

Zranitelnost		IS	Data	AutoCad (data)	DB zákazníků	Server	NAS	PC	Kamerový systém	Stroje	Síťová infrastruktura	OS	MS Office	AutoCad
Fyzické poškození	Požár	5	5	5	5	5	5	5	5	5	5	5	5	5
	Voda	3	3	3	3	4	4	4	2	4	3	3	3	3
	Zničení zařízení	2	2	2	2	4	4	4	3	4	3	2	2	2
	Prach	2	2	2	2	4	4	4	3	2	2	2	2	2
Dostupnost služeb	Výpadek elektrické energie	1	1	1	1	2	1	2	1	3	1	1	1	1
	Výpadek internetu	1	1	1	2	2	1	3	1	1	3	1	1	1
	Výpadek IS	3	2	1	3	1	1	1	1	2	1	1	1	1
	Výpadek serveru	1	4	1	3	4	4	2	2	2	1	1	1	1
	Výpadek interní sítě	1	2	2	2	3	2	3	3	2	4	1	1	1
Důvěrnost služeb	Neoprávněný přístup do sítě	4	4	3	4	3	3	3	2	3	5	1	1	1
	Neoprávněný přístup do IS	4	1	1	4	1	1	1	1	1	1	1	1	1
	Neoprávněný přístup na server	1	4	3	4	2	2	1	2	2	1	1	1	1
	Škodlivý software	1	2	1	2	3	2	4	2	1	3	2	1	1
	Zneužití nebo krádež disků	1	3	3	2	2	2	2	1	1	1	1	1	1
	Krádež technického vybavení	2	2	3	2	2	2	4	1	2	1	1	1	1
	Získání dat z vyřazených médií	3	3	3	3	3	1	1	1	1	1	1	1	1
Lidský faktor	Fyzické poškození zařízení	1	2	3	1	3	3	4	2	4	3	1	1	1
	Nedodržování směrnic	1	3	3	3	2	2	2	1	3	2	1	1	1
	Nedbalost při obsluze zařízení	1	2	2	1	2	2	3	1	4	2	2	1	1
	Nedostatečná dokumentace	3	3	4	4	2	2	2	2	4	1	1	1	1
	Ztráta důvěrných dat	1	3	3	4	2	2	2	1	2	2	1	1	1
Technické selhání	Selhání serveru	1	4	3	2	1	3	1	1	2	1	1	1	1
	Selhání pracovních stanic	1	1	1	1	1	1	3	1	1	1	1	1	1
	Selhání strojů	1	1	1	1	1	1	1	1	4	1	1	1	1
	Selhání diskového úložiště NAS	1	2	2	1	2	3	1	2	1	1	1	1	1
	Selhání síťových prvků	1	2	1	1	1	1	1	1	1	4	2	1	1
Neoprávněné činnosti	Neoprávněné zkopírování dat	2	5	4	2	2	2	2	1	1	1	1	1	1
	Neoprávněný přístup do budovy	1	3	3	1	2	2	3	1	2	1	2	1	1
	Porušení mlčenlivosti pracovníků	1	3	2	2	1	1	1	1	1	1	1	1	1
	Zneužití uživatelských práv	2	3	2	3	2	2	3	1	1	1	2	2	2
	Zneužití administrátorských práv	3	4	3	4	2	2	2	1	1	3	2	1	1

4.1.3 Ohodnocení míry rizika

Hranice rizika jsou rozděleny do pěti skupin, a to na riziko:

- Bezvýznamné
- Akceptovatelné
- Mírné
- Nežádoucí
- Nepřijatelné

Ohodnocení je popsáno v následující tabulce.

Tabulka 7: Ohodnocení rizik, Zdroj: [1]

Hranice	Riziko
0 - 10	bezvýznamné riziko
11 - 20	akceptovatelné riziko
21 - 30	mírné riziko
31 - 60	nežádoucí riziko
61 a více	nepřijatelné riziko

4.1.4 Míra rizika

V této analýze rizik jsme si nejdříve určili tabulky pro aktiva, následně pro hrozby, které mohou ve firmě nastat a následně zranitelnost aktiv na základě hrozeb. V tomto případě se tedy jedná o metodu se třemi parametry. V následující tabulce jsou uvedeny výsledné hodnoty míry rizika a těmto hodnotám je přiřazena patřičná barva z předchozí tabulky.

Tabulka 8: Matice rizik, Zdroj: [Vlastní]

Riziko		IS	Data	AutoCad (data)	DB zákazníků	Server	NAS	PC	Kamerový systém	Stroje	Síťová infrastruktura	OS	MS Office	AutoCad
Fyzické poškození	Požár	50	50	50	40	40	40	20	30	50	50	10	20	30
	Voda	15	15	15	12	16	16	8	6	20	15	3	6	9
	Zničení zařízení	30	30	30	24	48	48	24	27	60	45	6	12	18
	Prach	40	40	40	32	64	64	32	36	40	40	8	16	24
Dostupnost služeb	Výpadek elektrické energie	20	20	20	16	32	16	16	12	60	20	4	8	12
	Výpadek internetu	15	15	15	24	24	12	18	9	15	45	3	6	9
	Výpadek IS	45	30	15	36	12	12	6	9	30	15	3	6	9
	Výpadek serveru	10	40	10	24	32	32	8	12	20	10	2	4	6
	Výpadek interní sítě	20	40	40	32	48	32	24	36	40	80	4	8	12
Důvěrnost služeb	Neoprávněný přístup do sítě	60	60	45	48	36	36	18	18	45	75	3	6	9
	Neoprávněný přístup do IS	60	15	15	48	12	12	6	9	15	15	3	6	9
	Neoprávněný přístup na server	15	60	45	48	24	24	6	18	30	15	3	6	9
	Škodlivý software	15	30	15	24	36	24	24	18	15	45	6	6	9
	Zneužití nebo krádež disků	10	30	30	16	16	16	8	6	10	10	2	4	6
	Krádež technického vybavení	40	40	60	32	32	32	32	12	40	20	4	8	12
	Získání dat z vyřazených médií	45	45	45	36	36	12	6	9	15	15	3	6	9
Lidský faktor	Fyzické poškození zařízení	15	30	45	12	36	36	24	18	60	45	3	6	9
	Nedodržování směrnic	20	60	60	48	32	32	16	12	60	40	4	8	12
	Nedbalost při obsluze zařízení	15	30	30	12	24	24	18	9	60	30	6	6	9
	Nedostatečná dokumentace	30	30	40	32	16	16	8	12	40	10	2	4	6
	Ztráta důvěrných dat	15	45	45	48	24	24	12	9	30	30	3	6	9
Technické selhání	Selhání serveru	15	60	45	24	12	36	6	9	30	15	3	6	9
	Selhání pracovních stanic	15	15	15	12	12	12	18	9	15	15	3	6	9
	Selhání strojů	10	10	10	8	8	8	4	6	40	10	2	4	6
	Selhání diskového úložiště NAS	10	20	20	8	16	24	4	12	10	10	2	4	6
	Selhání síťových prvků	10	20	10	8	8	8	4	6	10	40	4	4	6
Neoprávněné činnosti	Neoprávněné zkopírování dat	40	100	80	32	32	32	16	12	20	20	4	8	12
	Neoprávněný přístup do budovy	10	30	30	8	16	16	12	6	20	10	4	4	6
	Porušení mlčenlivosti pracovníků	20	60	40	32	16	16	8	12	20	20	4	8	12
	Zneužití uživatelských práv	30	45	30	36	24	24	18	9	15	15	6	12	18
	Zneužití administrátorských práv	30	40	30	32	16	16	8	6	10	30	4	4	6

4.1.5 Zhodnocení analýzy

Informační systém spravují pouze pracovníci z ICT oddělení, kteří vše nejdříve konzultují s majitelem a generálním ředitelem. Ostatní zaměstnanci podávají návrhy na změny, nebo poznatky, jak vylepšit informační systém. Zálohování dat probíhá pravidelně každý den, ovšem zálohovaná data se nacházejí ve stejné místnosti jako server s daty. Fyzickou bezpečnost má firma celkem podchycenou, u vjezdu do areálu firmy sedí vrátný, který ovládá závoru a zároveň určuje, kdo do firmy vstoupí. V areálu firmy jsou také nainstalovány kamery, které sledují vnější i vnitřní prostor. Podle provedené analýzy můžeme odhalit některé nedostatky, které se musí eliminovat, nebo alespoň snížit.

4.2 Návrh síťové infrastruktury

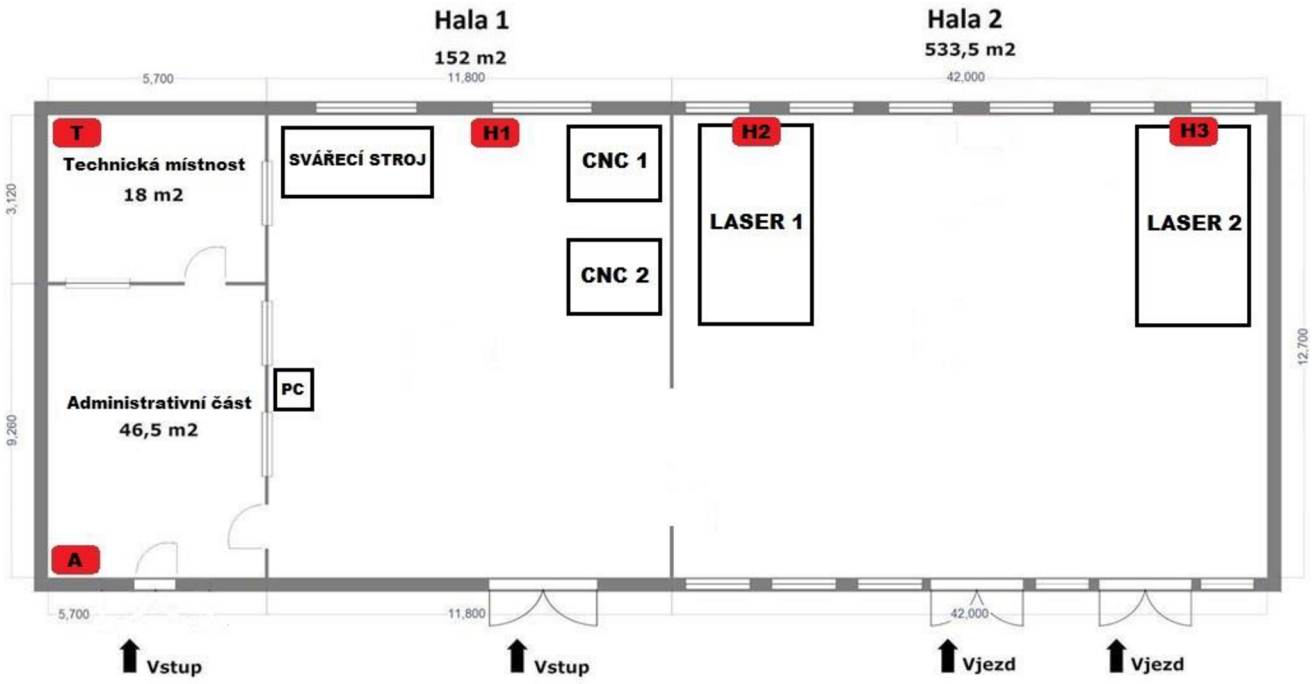
V této kapitole se budeme zabývat návrhem ICS řešením pro naši firmu. Budou vybrány správné síťové prvky pro průmyslové prostředí, určeny kabelové trasy a rozmístění uzlových bodů. Nová infrastruktura bude napojena na stávající, nová infrastruktura se bude realizovat za provozu.

Je zapotřebí navrhnout a vytvořit síť s maximální dostupností, vybrat správnou jednotnou platformu aktivních prvků a kabeláže (konektory, kabely). Dále spolu s novou infrastrukturou vytvořit redundanci, která odpovídá požadavkům sítě s maximální dostupností. Za další je nutná modularita pasivní i aktivní vrstvy. Je zapotřebí, aby pasivní vrstva byla od jednoho výrobce, to samé platí i pro aktivní vrstvu. Tedy v jednotlivých uzlových bodech budeme mít stejné aktivní prvky neboli typizované řešení. Firma požaduje centrální řízení provozu a výroby. Nyní hlavní pracovníci oddělení výroby chodí po hale a kontrolují, zda vše probíhá tak, jak má.

Topologie ICS sítě se bude provádět jako optická páteř do kruhu. V průmyslovém prostředí se jedná o nejlepší řešení. Dále je zapotřebí zastřešit infrastrukturu jednotným managementem, kterým se bude provádět dohled nad celou sítí.

4.2.1 Určení páteřních uzlových bodů

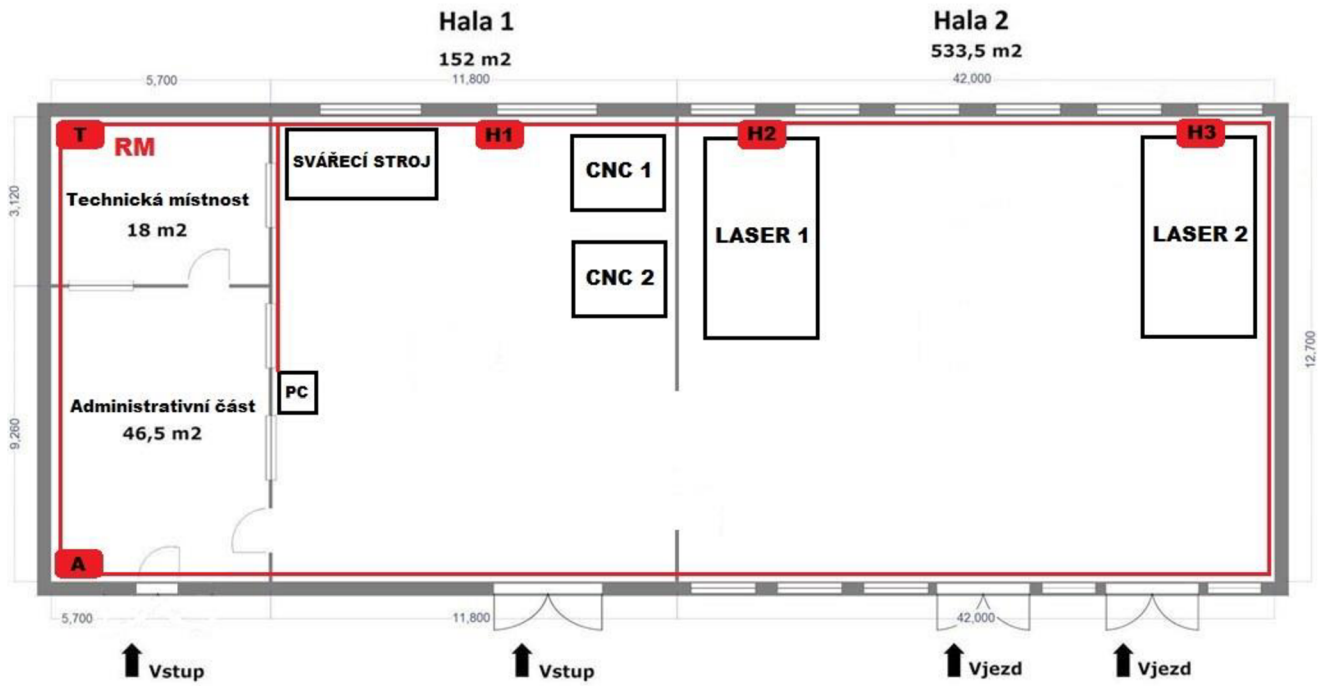
Uzlové body se musí vybrat takovým způsobem, aby byly dobře přístupné a vydržely na daném místě dlouhou dobu při provozu. Datové rozvaděče je nutné umístit výš, aby nedocházelo k mechanickému poškození rozvaděče, nebo aby nebyl zasažen agresivní látkou. Na následujícím obrázku je znázorněno umístění uzlových bodů.



Obrázek 19: Rozmístění uzlových bodů, Zdroj: [Vlastní]

4.2.2 Návrh optické páteřní sítě

Vedení kabeláže je nutné umístit tak, aby byl z dosahu veškerých jeřábů a vysokozdvižných vozů, které manipulují s materiály. Následně se spojí optickými kabely uzlové body do kruhové topologie. Bude se jednat síť s rychlostí 1 Gb/s. Ring master celé topologie je umístěn v uzlovém bodě v technické místnosti. Dále je nutné pojmenovat si jednotlivé uzlové body z důvodu správné identifikace, pokud by se všechny uzlové body jmenovaly stejně, postrádalo by toto značení smysl.



Obrázek 20: Návrh tras optické páteře, Zdroj: [Vlastní]

Nyní je nutné spočítat počet vláken jednotlivých tras. Jelikož se síť bude tvořit za chodu firmy, je nutné tyto uzlové body zapojovat postupně a pokaždé, až bude daný uzlový bod zprovozněn, tak se síť přepne ze staré na novou. Proto je nutné nejprve udělat trasu z bodu **T** do bodu **H1**, což jsou dvě vlákna, poté z bodu **T** do bodu **H2** a takhle postupně až do bodu **A**. Celkově se tedy jedná o osm vláken a samozřejmě nesmíme zapomenout na redundanci minimálně 50%. Tím se dostáváme na dvanáct vláken, která se vrátí zpět do uzlového bodu **T**. Celková délka segmentu nepřesáhne 300 m. Je potřeba počítat se svody z vedení trasy k jednotlivým datovým rozvaděčům a také k rezervě, která bude v datových rozvaděčích. Poté jsme schopni za provozu postupně zprovoznit síť do topologie hvězdy a po zprovoznění posledního segmentu nastavit Ring master a přepnout síť na redundantní kruh. Takto to lze vyřešit bez přerušení provozu ve firmě.

Je zapotřebí vybrat správný druh optického vlákna. V našem případě a v naší vzdálenosti tras, budeme volit druh optického kabelu OM2. Optický kabel je nutné uložit do kovové chráničky, zvláště v oblasti výrobních hal. Pro vedení optických tras využijeme registry napájecích rozvodů. Je to nejjednodušší způsob vedení tras, jelikož se kabel k registrům přiváže ocelovými vázacími páskami tam, kde jsou velké výkyvy

teplot. Tam, kde se vyšší teploty nevyskytují, nám postačí plastové vázací pásky, ovšem černé, které jsou odolné vůči UV záření.

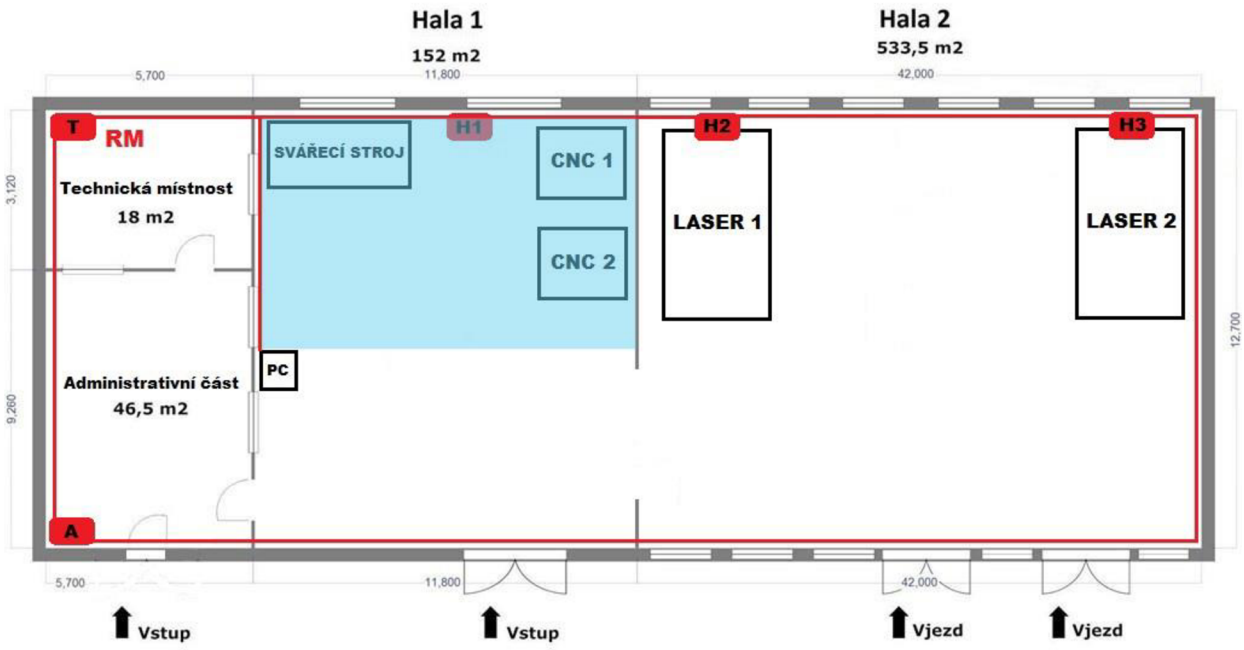
Nyní musíme dle požadavků vybrat správné datové rozvaděče pro uzlové body. Bude se jednat opět o typizované řešení. Je nutné použít zodolněné datové rozvaděče pro použití v těžkém průmyslu, které budou odolné vůči vodě a prachu.

Bude se jednat o řešení:

- *19“ montáž* – zde musíme počítat s připojením jednotlivých pracovišť, dohledů, PLC, strojů metalickým vedením, tudíž metalické rozvody pro patch panely a záložní zdroje UPS.
- *DIN montáž* – na DIN lištu bude připevněn optický modulární rozvaděč, dále napájecí zdroj pro aktivní prvky PoE (Power of Ethernet) s napětím 48V DC.

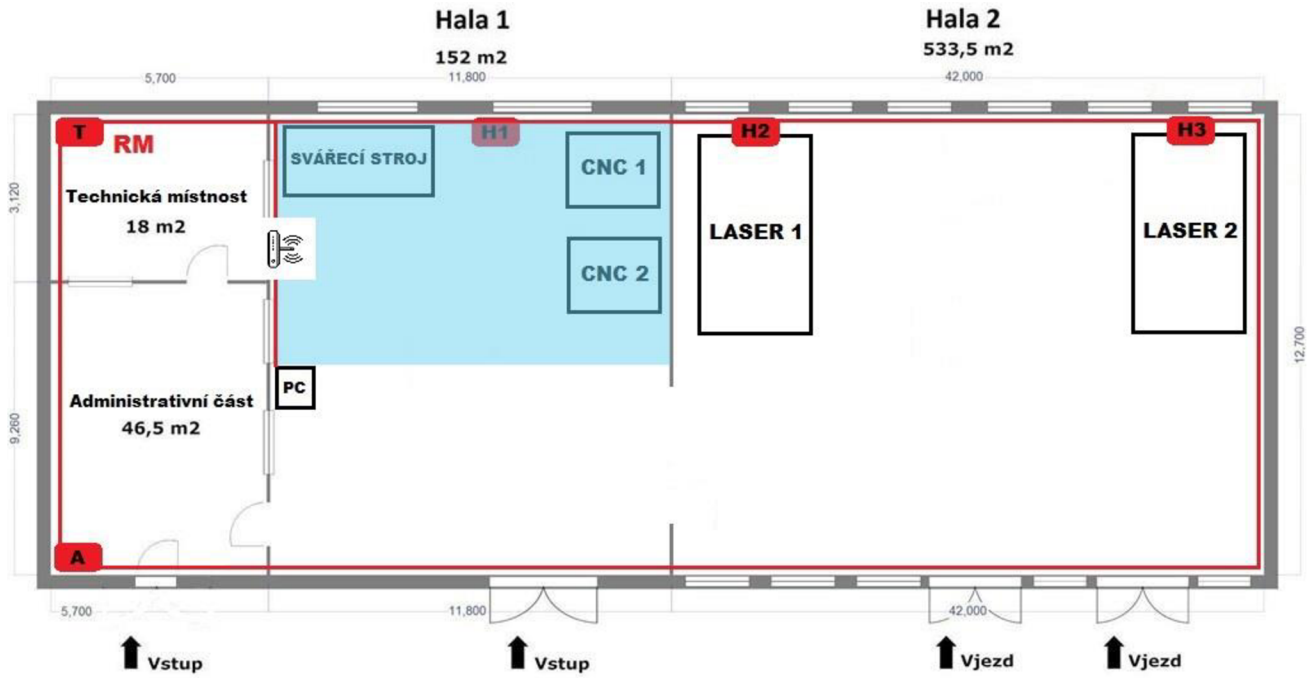
4.2.3 Wi-Fi pokrytí

Pokud chceme pokrýt nějakou část haly Wi-Fi signálem, musíme použít průmyslové Wi-Fi technologie. Nejprve je nutné určit si požadovanou plochu, která má být pokryta signálem. Pro majitele bylo nejdůležitější, aby signálem byly pokryty dva CNC ohraňovací stroje, které leží v hale 1. Na následujícím obrázku je modrou barvou zobrazeno pokrytí Wi-Fi signálem.



Obrázek 21: Požadovaná plocha pokrytí, Zdroj: [Vlastní]

Nyní je nutné správně umístit Wi-Fi prvek. Umístěn bude v prostoru mezi svářecím strojem a PC haly v ideální výšce cca 6 metrů od země. Je zapotřebí prvku nastavit správný vyzařovací výkon. Ten se musí řídit povolenými hodnotami v rámci České republiky. Proto musíme na zařízení nastavit vyzařovací výkon pro Českou republiku. Musíme Wi-Fi prvky napojit metalickým kabelem pomocí funkce PoE. Pro menší úbytky napětí použijeme metalické kabely profinet typ lanko, který je mnohem odolnější a ohebnější a je stíněný, a který bude navíc umístěn v kovové chráničce. Jelikož budeme mít použitý pouze jeden Wi-Fi prvek, nemusíme řešit kanálové řešení. Na následujícím obrázku je zobrazeno umístění prvku pro bezdrátový přenos.



Obrázek 22: Umístění Wi-Fi prvku, Zdroj: [Vlastní]

4.2.4 Pasivní vrstva

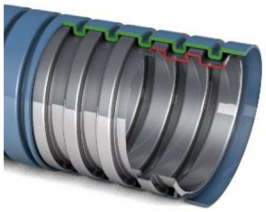
V této části budou popsány jednotlivé prvky pasivní vrstvy, jako jsou kabely, chráničky, datové rozvaděče apod.

Optická páteř

Pro vedení páteře budou použity více plášťové optické kabely od firmy Belden. Tento kabel je chráněn materiálem polyuretan, který má výborné vlastnosti a je odolný vůči UV záření.

Obrázek 23: Více plášťový optický kabel, Zdroj: [7]

Tyto kabely budou uloženy do speciální kovové chráničky, která kabel uchrání před mechanickým poškozením, dále pak před agresivním prostředím průmyslu (oleje, chemikálie) a vodou. Tato chránička má obal také z polyuretanu.



Obrázek 24: Kovová chránička, Zdroj: [17]

Zakončení optických tras bude pomocí zodolněných konektorů určených pro průmyslové prostředí.

Obrázek 25: Zodolněné optické konektory, Zdroj: [7]

Datové rozvaděče

Datový rozvaděč pro průmysl musí mít jiné atributy, než komerční rozvaděč. Průmyslové provedení rozvaděče nemá ventilátor ani žádné průduchy.

Obrázek 26: Průmyslový datový rozvaděč, Zdroj: [18]

Tento celokovový datový rozvaděč má odolnost vůči vodě a prachu. Je určen pro montáž přímo na zeď. Ovšem datový rozvaděč, ve kterém bude umístěn Wi-Fi aktivní prvek, bude plastový, ale musí splňovat veškeré požadavky pro průmysl. Plastový musí být z toho důvodu, aby nepohlcoval bezdrátový signál.

ProfiNet pro připojení Wi-Fi

Jedná se o dvoupárový metalický kabel typu lanko, který je mnohem odolnější a ohebnější. Navíc je stíněný a bude umístěn v kovové chráničce.

Obrázek 27: Průřez profinet kabelu, Zdroj: [7]

Zakončení profinetního kabelu bude pomocí zodolněného RJ-45 konektoru, který splňuje požadavky průmyslu (kovový plášť).

Obrázek 28: Zodolněný konektor RJ-45, Zdroj: [7]

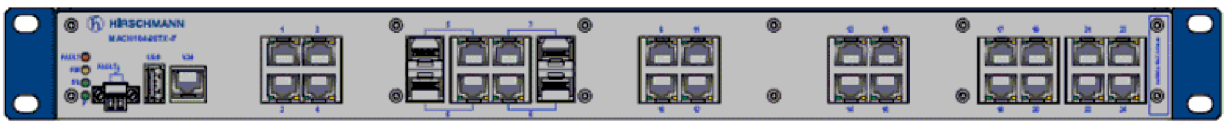
4.2.5 Výběr aktivních prvků

Vybrat správné a vhodné aktivní prvky pro průmyslové prostředí je velmi důležité. Zde se nemůže jednat o komerční prvky, jelikož nápor průmyslu a agresivního prostředí nezvládnou. Je zapotřebí, aby se jednalo o bezventilátorové, zodolněné prvky.

Aktivní prvky, které jsem vybral, budou od společnosti Hirschmann. Jedná se o německou firmu ležící nedaleko Stuttgartu, která se specializuje na tyto prvky. Osobně jsem viděl, s jakou pečlivostí a přesností se prvky vyrábí a jaký důraz kladou na kvalitu provedení. Z toho důvodu nevidím jiné řešení, než použít aktivní prvky právě od firmy Hirschmann.

Páteřní switch

Po dohodě s majitelem naší společnosti jsme dospěli k názoru, že použijeme plnohodnotný switch s rychlostí 1 Gb/s. Tedy na všech portech, které switch obsahuje, bude rychlost1 Gb/s.

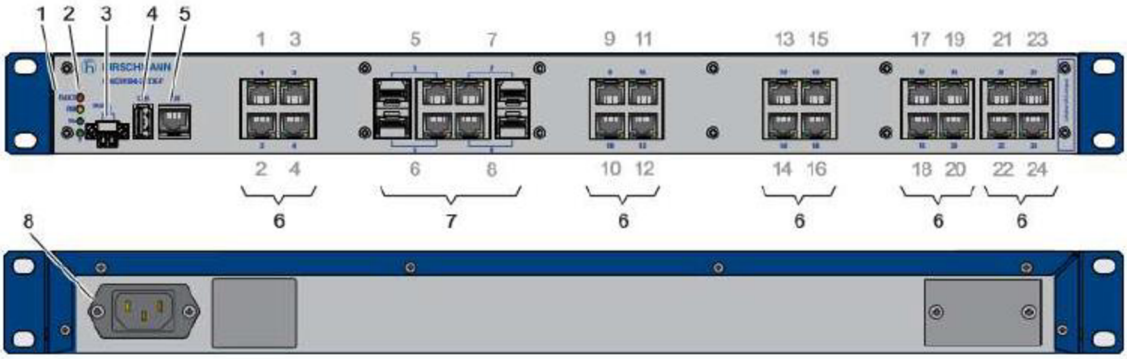


Obrázek 29: Switch Mach 104, Zdroj: upraveno dle [13]

Požadavky:

- 24 gigabitových portů
- 4 combo porty
- Podpora plného managementu
- Podpora ring topologie
- 19“ provedení

Tento switch obsahuje 24 gigabitových portů a k tomu 4 combo porty. U combo portů se zásuvným modulem lze jednoduše přejít z gigabitového metalického portu na gigabitový optický port. Dále switch podporuje plný management, což byla podmínka. Switch podporuje také ring topologii. Jedná se o 19“ montáž, jelikož vybrané datové rozvaděče mají možnost 19“ montáže.



Obrázek 30: Popis portů Mach 104, Zdroj: upraveno dle [7]

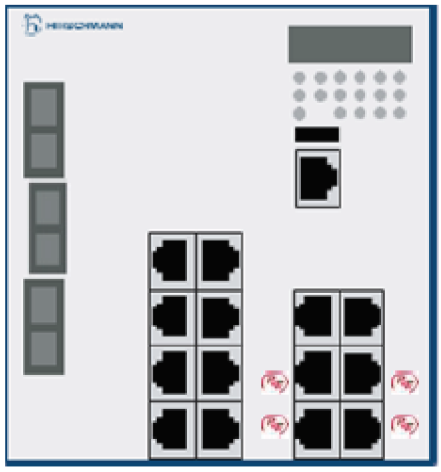
Na tomto obrázku můžeme vidět, jak v Hirschmannu číslují porty. Porty číslo 1 až 4 jsou klasické porty RJ-45, porty 5 až 8 jsou combo porty a dále 9 až 24 jsou opět klasické RJ-45 porty.

Další označení:

1. Název zařízení
2. LED diody
3. Signál kontaktu
4. USB rozhraní
5. V. 24 připojení pro externí management
6. RJ-45 porty
7. Combo porty
8. Napájecí konektor

PoE switch

Pro další aktivní prvek je nutné, aby měl funkcionalitu PoE. V tomto případě se bude jednat o prvek, který bude připevněn na DIN lištu.

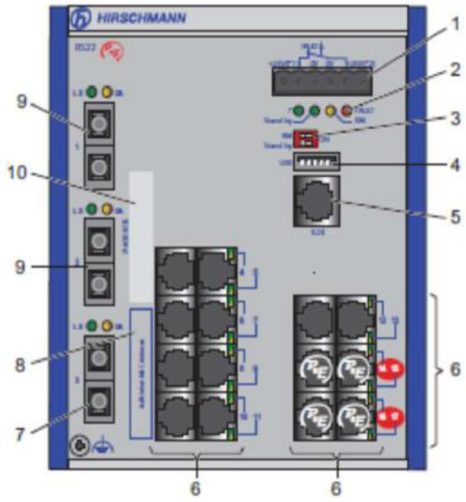


Obrázek 31: Prvek RS 22 PoE, Zdroj: [7]

Požadavky:

- 14 portů s rychlostí 100 Mb/s
- 4 porty s funkcionalitou PoE
- 3 optické porty s rychlostí 100 Mb/s
- Podpora plného managementu
- DIN provedení

Tento prvek má elegantní řešení na úrovni 3 optických portů, což může být do budoucna výhoda. Následně má řadu 14 metalických portů, z nichž 4 porty podporují funkci PoE. Toto řešení má velkou výhodu pro připojení bezdrátových prvků jedním kabelem.



Obrázek 32: Popis portů RS 22, Zdroj: [7]

Jak již bylo zmíněno, jedná se o provedení switche pro montáž na DIN lištu. Popis portů je také popsán výše.

Prvek dále obsahuje:

1. Napájení 48 V DC
2. LED diody
3. Konfigurační port
4. USB rozhraní
5. V. 24 připojení pro externí management

Wi-Fi prvky

Bezdrátové řešení jsou jednorádiové, ale umí i dvourádiové s tím, že se musí přepínat, tudíž nejedou obě zaráz, musíme si zvolit sami. Tento prvek má provedení se třemi vyzařovacími anténami, kterými můžeme nastavovat směr vyzařování signálu.

Obrázek 33: Wi-Fi prvek BAT-R, Zdroj: [14]

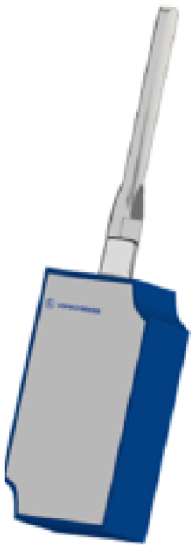
Požadavky:

- Podpora PoE
- Nastavitelné vyzařovací charakteristiky
- Podpora plného managementu
- DIN provedení

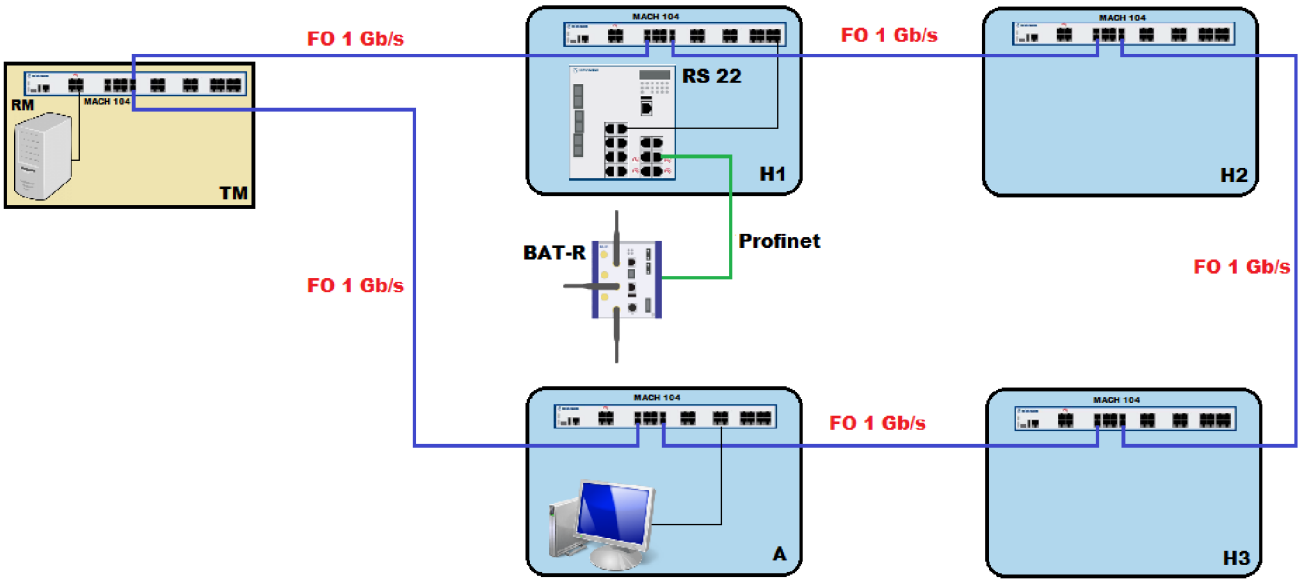
Zvolil jsem variantu takovou, která má pouze vstup na PoE a integrovaný datový vstup, více není potřeba. Zařízení tedy bude napájeno pomocí PoE, což je velmi jednoduchý a elegantní způsob. Dále byl požadavkem plný management, což je nutné. Tento prvek má provedení pro umístění na DIN lištu. Vyobrazené zadní rozhraní je viditelné na následujícím obrázku.

Obrázek 34: BAT-R porty, Zdroj: [23]

Dále je zapotřebí mít na druhé straně pevného klienta, který bude obsahovat podporu plného managementu. Musí být zodolněný, jelikož bude umístěn na ohraňovacích strojích.



Obrázek 35: Wi-Fi klient, Zdroj: [7]



Obrázek 36: Blokové schéma osazení aktivními prvky, Zdroj: [Vlastní]

Na výše uvedeném obrázku můžeme vidět blokově zapojené aktivní prvky. Jak je z obrázku zřejmé, tak technická místnost i jednotlivé páteřní uzlové body jsou provedeny 19“ zástavbou. Modré propojení jednotlivých prvků je gigabitová optická páteř. Zeleně je propojen PoE switch s prvkem bezdrátového signálu pomocí profinetu. Celé zapojení vychází z jednoho typu páteřního switche, dále máme jeden switch s podporou PoE, ale pokud bychom někdy použili další, vybereme stejný typ. To stejné platí u bezdrátového řešení.

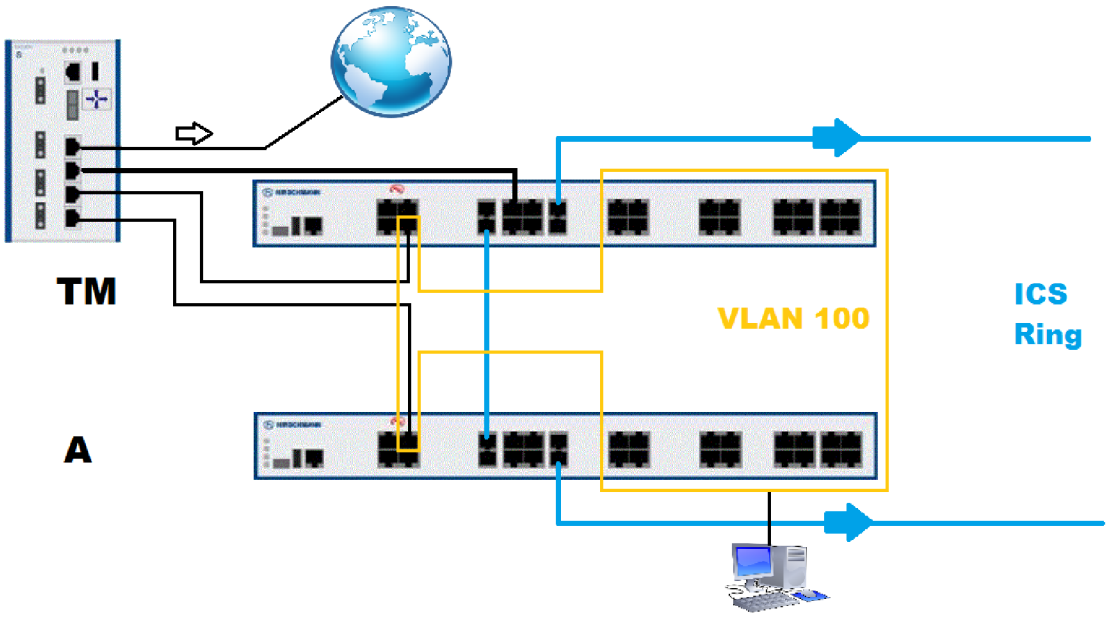
4.2.6 Oddělení sítí

V dalším kroku je možné nastavovat různé funkcionality. Je zapotřebí oddělit administrativní síť od průmyslové. Momentálně se ve firmě nenachází žádné routování, jedná se o tzv. plochou síť. Postup je takový, že se nastaví VLANy.

VLAN můžeme nastavit dvojím způsobem:

- Staticky
- Dynamicky

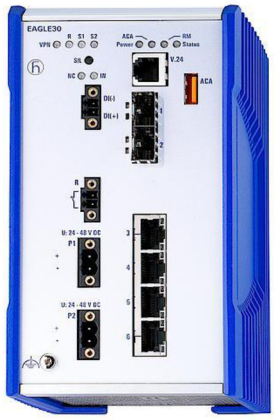
Statické nastavení je takové, že se každý port ručně v managementu nadefinuje. Je to velmi dobré řešení, jelikož v okamžiku kdy máme port ve VLAN a jsme v té dané VLAN, tak vše vidíme a vše funguje, jakmile ho ale posuneme do jiné VLANy tak nevidíme nic. Je nutné rozdělit sítě také na vrstvě L3. Hrozilo riziko, že by nemusel stačit adresní prostor ve firmě, proto je zapotřebí rozšířit adresní prostory. Tedy před VLANy je umístěn víceportový router od firmy Hirschmann.



Obrázek 37: Oddělení adresních prostorů, Zdroj: [Vlastní]

Jeden port routeru je určen pro přenos směrem ze sítě, další port je pro páteřní připojení, u dalších portů se jedná o aplikační připojení, jako např. kamerový systém. Tedy díky předřazenému routeru a vytvořením VLAN se dá dosáhnout oddělení jednotlivých sítí.

Použitý router Eagle 30 je, jak již bylo zmíněno, od firmy Hirschmann, a je to kombinace routeru a základního firewallu. Jedná se o čtyřportovou verzi, která nabízí veškeré funkcionality průmyslového řešení. Obsahuje gigabitové řešení včetně optických portů, dále pak překlad adres NAT, VPN přístupy, DPI (Deep Packet Inspection) a WAN port, který umí komunikovat s jakýmkoli providerem směrem ven ze sítě.



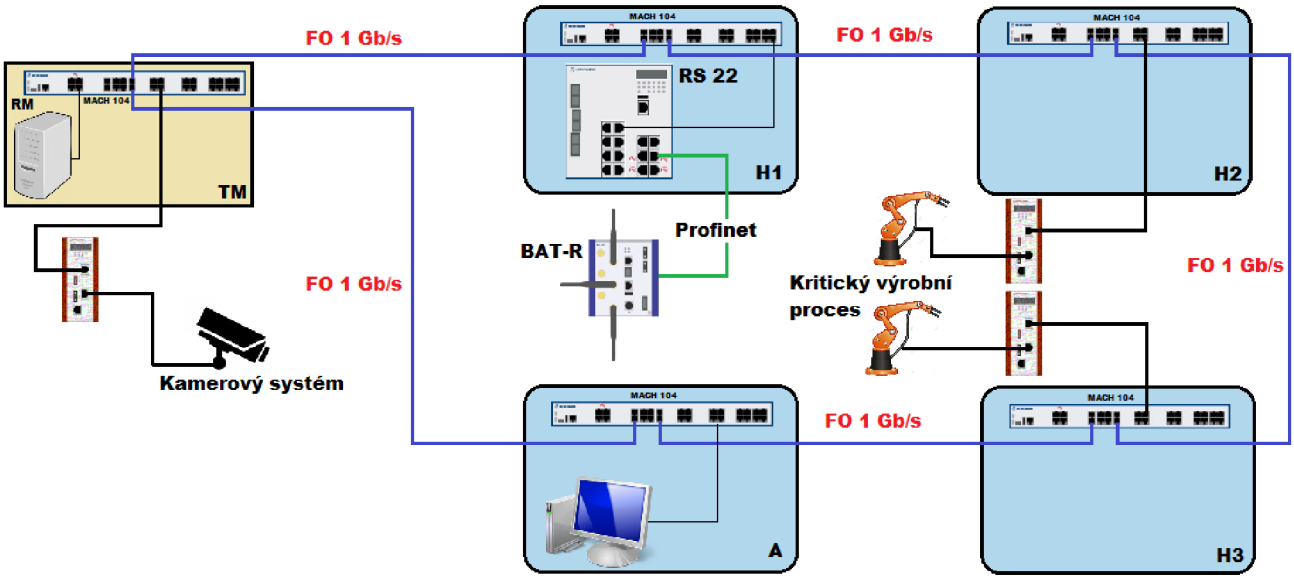
Obrázek 38: Router Eagle 30, Zdroj: [15]

4.2.7 Aplikační firewall

V této části se budeme zabývat aplikačním firewallem z důvodu zónového řešení ICS sítě. Bude zde použit čistě pouze firewall, ne žádná kombinace s routerem, tím pádem zde nefungují žádné překlady adres apod. Jako aplikační firewall bylo vybráno dvouportové Tofino, které bylo vyvíjeno v Kanadě. Hlavní nasazení tohoto firewallu je převážně do průmyslového prostředí, a to na zónové řešení. Firewall má mnoho funkcionalit, je to provedení pro montáž na DIN lištu.

Obrázek 39: Tofino Xenon, Zdroj: [16]

Na následujícím obrázku je zapracovaný aplikační firewall Tofino do naší sítě, kde bude oddělovat kamerový systém a kritické výrobní procesy.



Obrázek 40: Zabudování aplikačního FW do sítě, Zdroj: [Vlastní]

4.2.8 Management software

V této části bude vybrán managementový software pro dohled nad sítí, který bude zaznamenávat veškerou činnost. Jedná se o nejdůležitější část celé infrastruktury. Aktivní prvky v sobě mají zabudovaný výstup pro sériové propojení přes konektor RJ-11. Takovýmto způsobem to provádíme, chceme-li do zařízení nahrát např. unikátní konfiguraci a nechceme to řešit přes síť. Máme k dispozici několik softwarových možností, jak síť monitorovat. Jedná se o produkty firmy Hirschmann.

První modul je **HiDiscovery**, který umí najít zařízení v síti pomocí MAC adresy. Tento modul je volně stažitelný na internetu.

Obrázek 41: HiDiscovery modul, Zdroj: [7]

Dalším modulem na podobné úrovni je **HiView**, který zprostředkovává grafický pohled sítě.

Obrázek 42: HiView modul, Zdroj: [7]

Následující modul můžeme nazvat jako managementový software, jedná se o **HiVision**, který umí pracovat na různých úrovních a umožní interaktivní zásah při monitorování sítě.

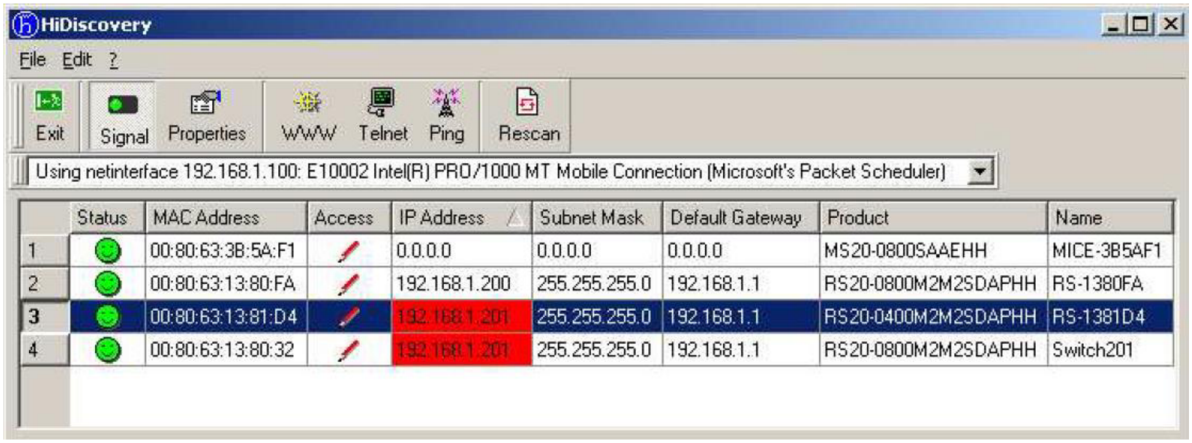
Obrázek 43: HiVision modul, Zdroj: [7]

Dalším z produktů je modul **HiFusion**, který umí pracovat s MIB databázemi hlavně s databázemi třetích stran. Tento modul je vhodný pro řízení výrobních procesů.

Obrázek 44: HiFusion modul, Zdroj: [7]

Zajímavým modulem je tzv. **HiMobile**, který umí zobrazit stav sítě přes smartphone, nebo tablet pokud se nacházíte např. v terénu. Tento modul je dalším z volně stažitelných, ovšem musíme si zakoupit produkt HiVision.

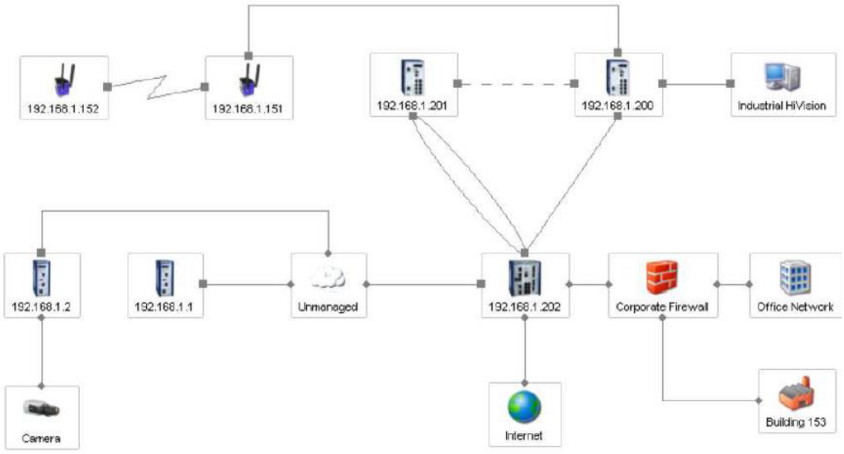
Obrázek 45: HiMobile modul, Zdroj: [7]



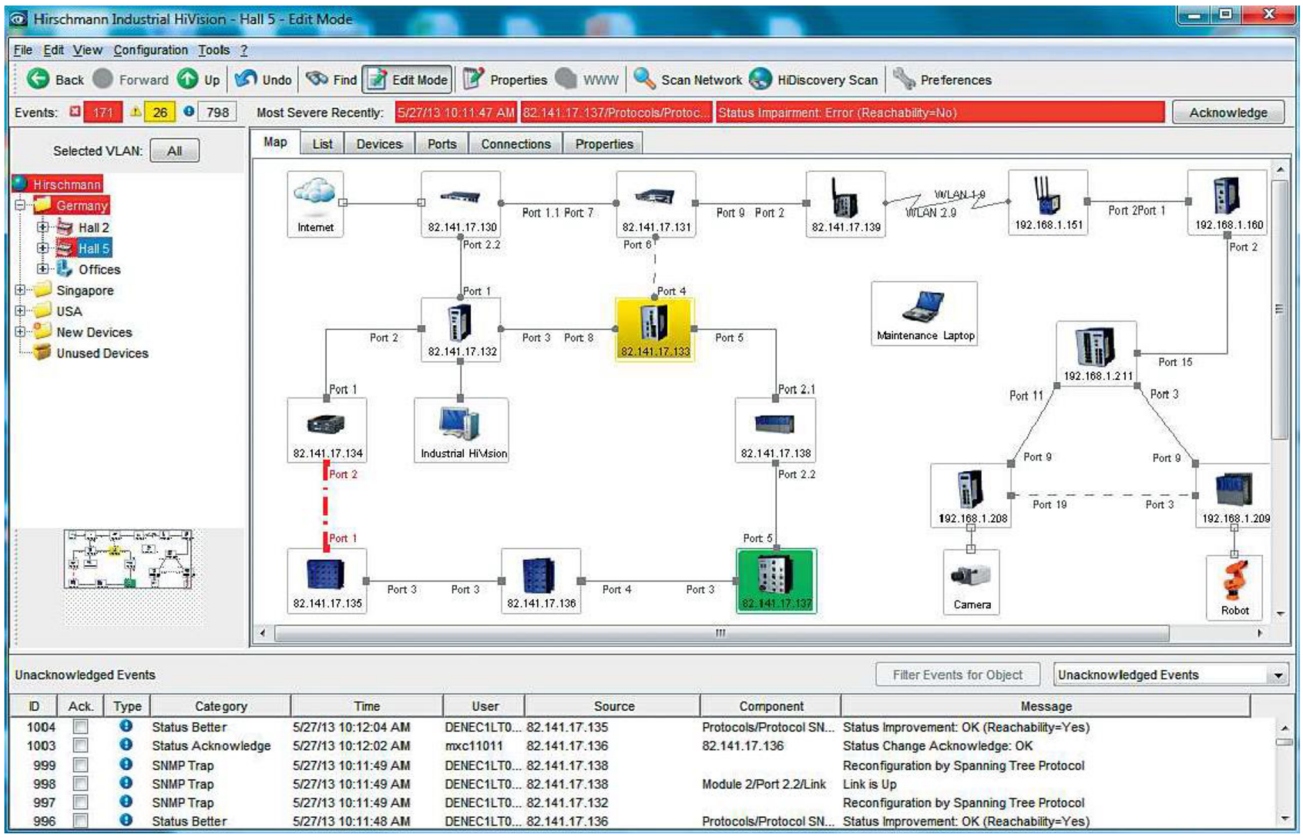
Obrázek 46: Ilustrační zobrazení modulu HiDiscovery/HiView, Zdroj: [7]

Na výše zobrazeném obrázku můžeme vidět ilustrační prostředí modulu HiDiscovery/HiView. Obsahuje detekci kolizí adres, aby nedošlo k zahlcení sítě. Další výhodou je detekce duplicitních adres.

Modul HiVision je profesionální management software síťové verze. Je možné ho použít i pro dohledové SCADA systémy a podporuje prostředí Windows i Linux. Po zakoupení softwaru je nutná registrace, bez které program na daném prvku nespustíme. Nebo můžeme program nainstalovat na server a potom si k monitorování sítě můžeme připojit libovolný počet monitorovacích stanic. Pomocí funkce **Scan Network** zmapuje program celou síť a vyobrazí topologii sítě. Poté si můžeme pomocí editoru ikon zvolit, jak se nám má co zobrazit (redundantní trasy, bezdrátové spojení, rychlost mezi danými uzly apod.). Můžeme si poskládat topologii podle sebe, aby reálně odpovídala skutečnému zapojení, program nám ji automaticky zmapuje, ovšem neuspořádá podle reálného zapojení.



Obrázek 47: Ilustrační zmapování sítě, Zdroj: [7]



Obrázek 48: Ilustrační zobrazení prostředí HiVision, Zdroj: [7]

Z důvodu, že nová síťová infrastruktura ve firmě zatím není zrealizována, jsem nucen používat ilustrační ukázky prostředí management softwaru.

Z management softwaru jsme schopni dostat výstupy v různých podobách, ze kterých můžou být sestaveny statistické formuláře. Program umí vytvořit výstup buď do souboru PDF, který si můžeme uložit, nebo vytisknout a založit, umí ale také výstup ve formátu MS Excel. A jak již bylo zmíněno, můžeme si nechat zobrazit stav sítě i na chytrém zařízení.

4.3 Zavedení nejkritičtějších částí ISMS

Z důvodu některých velmi kritických oblastí bezpečnosti ve firmě, které plynou z analýzy rizik, je zapotřebí zavést některé části ISMS. Tato část se bude řídit normou ČSN ISO/IEC 27001, příloha A.

4.3.1 A.5.1.1 Dokument bezpečnostní politiky informací

Pověřená osoba: majitel podniku

Vedení firmy by mělo vytvořit bezpečnostní politiky, se kterými následně seznámí veškeré zaměstnance, popř. externí dodavatele či odběratele. Vytvoření tohoto dokumentu by nemělo přesáhnout 24 hodin.

4.3.2 A.6.1.1. Přidělení odpovědností a A.6.1.2 Koordinace bezpečnosti informací

Pověřená osoba: majitel firmy, bezpečnostní manažer, vedoucí jednotlivých oddělení

Je nutné do firmy zavést směrnici, která bude stanovovat způsob koordinace bezpečnosti informací mezi jednotlivými odděleními. Současně musí být ve směrnici stanoveny odpovědnosti v oblasti bezpečnosti informací. Díky této směrnici se vedoucí oddělení stávají spoluodpovědnými osobami za vzájemnou koordinaci při řešení bezpečnostních incidentů. Při nastání bezpečnostního incidentu hlásí podřízení pracovníci svému vedoucímu oddělení daný problém, který ho řeší dle předem daného postupu. Vedoucí oddělení tento problém následné hlásí bezpečnostnímu manažerovi, který ho zpracovává dál. Každý incident nebo bezpečnostní problém musí být řádně zdokumentován.

4.3.3 A.6.1.5 Ochrana důvěrných informací

Pověřená osoba: vedoucí jednotlivých oddělení

Ve firmě jsou stanoveny jisté dohody, které udávají, jakým způsobem se mají chránit důvěrné informace. Je v nich uvedeno, jací pracovníci mají přístup k daným informacím, a co s nimi mohou provádět. Dále mají povinnost zachovat mlčenlivost o důvěrných datech. Za porušení těchto dohod jsou uděleny sankce, se kterými byli všichni zaměstnanci řádně seznámeni. Pracovníci by měli mít přístup pouze k takovým datům, která úzce souvisí s náplní jejich práce.

4.3.4 A.7.2.2 Povědomí, vzdělávání a školení bezpečnosti informací

Pověřená osoba: bezpečnostní manažer

Formou školení bude zaměstnancům sděleno, proč se buduje nová síťová infrastruktura, jaký to bude mít vliv na funkčnost firmy a co nového je čeká. Následovat bude seznámení s bezpečností informací, jak mají s daty zacházet, jak se chovat na pracovní stanici apod. Dále budou seznámeni s novými funkcionalitami, které přináší nová infrastruktura. Na závěr školení bude zaměstnancům rozdán test, ve kterém budou otázky na dané školení, a pokud by snad někdo neuspěl, je nutná náprava.

4.3.5 A.7.2.3 Disciplinární řízení

Pověřená osoba: majitel firmy

Pokud by některý ze zaměstnanců porušil firemní směrnice, je nutné, aby existoval formální proces disciplinárního řízení pro zaměstnance, kteří se dopustili narušení bezpečnosti informací.

4.3.6 A.11.2.4 Údržba zařízení

Pověřená osoba: vedoucí oddělení ICT

Je nutné vytvořit plán pro pravidelnou revizi a kontrolu pracovních stanic, serverů a aktivních prvků síťové infrastruktury. Pro tyto úkony je stanoven odpovědný pracovník oddělení ICT, který pravidelně provádí fyzické kontroly a revize zařízení používaných ve firmě. Po každé kontrole nebo revizi sepíše dokument o provedení kontroly, a pokud by došlo k nálezu chyb nebo nedostatků, sdělí tuto skutečnost svému vedoucímu a ten pak majiteli. Pro UPS zdroje se musí vytvořit plán pro pravidelné testování funkčnosti, které se bude provádět každý měsíc. Pravidelné kontroly pracovních stanic, serverů a aktivních prvků infrastruktury také zahrnuje čištění od prachu.

4.4 Ekonomické zhodnocení

Ve firmě bylo nutné udělat kompletní síťovou infrastrukturu, která bude splňovat podmínky průmyslového řešení. Oblast zabezpečení v průmyslu není levná záležitost, jsou zde použity speciální prvky, které musí zvládnout náročnost prostředí. V následující tabulce jsou uvedeny veškeré prvky, které jsou nutné k vybudování nové infrastruktury.

Tabulka 9: Rozpočet, Zdroj: [Vlastní]

Položka	Množství	Cena za mj bez DPH	Cena celkem bez DPH
Pasivní vrstva			
Optický kabel OM2	200 m x 12 vláken	45,00 Kč	9 000,00 Kč
ProfiNet kabel	17 m	33,00 Kč	561,00 Kč
Kovová chránička	185 m	98,00 Kč	18 130,00 Kč
Odolné optické konektory	12 ks	499,00 Kč	5 988,00 Kč
Odolné RJ-45 konektory	2 ks	366,00 Kč	732,00 Kč
Datový rozvaděč uzlových bodů	5 ks	9 670,00 Kč	48 350,00 Kč
Datový rozvaděč pro Wi-Fi	1 ks	2 980,00 Kč	2 980,00 Kč
Kovové vázací pásky	150 ks	9,00 Kč	1 350,00 Kč
Plastové vázací pásky černé	50 ks	2,00 Kč	100,00 Kč
Aktivní vrstva			
Páteřní switch Mach 104	5 ks	64 890,00 Kč	324 450,00 Kč
PoE switch RS 22	1 ks	39 770,00 Kč	39 770,00 Kč
Wi-Fi prvek BAT-R	1 ks	34 330,00 Kč	34 330,00 Kč
Wi-Fi klient	2 ks	9 640,00 Kč	19 280,00 Kč
Router Eagle 30	1 ks	29 950,00 Kč	29 950,00 Kč
Aplikační firewall Tofino Xenon	3 ks	58 890,00 Kč	176 670,00 Kč
Management software			
HiView	1 ks	zdarma	-
HiVision pro 32 zařízení	1 ks	65 300,00 Kč	65 300,00 Kč
HiFusion	1 ks	zdarma	-
HiMobile	1 ks	zdarma	-
Práce			350 000,00 Kč
Cena celkem bez DPH a práce			776 941,00 Kč
DPH 21%			163 158,00 Kč
Cena celkem s DPH a prací			**1 290 099,00 Kč**

Jak z tabulky můžeme vidět, celkový rozpočet na vybudování nové infrastruktury i s prací činí 1 290 099 Kč. Nejdražší položky jsou z aktivní vrstvy, jelikož to jsou velmi kvalitní produkty od společnosti Hirschmann. Pokud by se taková síťová infrastruktura realizovala v oblastech jako je IT, účetnictví, školství apod., tak by jistě rozpočet nevystoupal až na takovéto hodnoty. Ceny jednotlivých komponent jsem převzal z praxe od jednotlivých společností a výrobců daných prvků pasivní a aktivní vrstvy.

Díky tomuto řešení se mi podařilo vybudovat novou síťovou infrastrukturu v průmyslovém podniku, která splňuje veškeré požadavky průmyslového řešení. Vybral jsem takové prvky, které jsou kvalitní a spolehlivé. Pasivní vrstva musí být odolná hlavně vůči mechanickému poškození a jiným vlivům, které se v průmyslu objevují. Aktivní prvky musí zvládat náročnost průmyslové sítě, ale také musí být odolné vůči nepříznivým vlivům, jako je prach, výkyvy teplot apod. Dále bylo nutné celou infrastrukturu zastřešit management softwarem, který dokonale zmapuje síť a má dobré uživatelské rozhraní. Tento management byl vybrán opět od společnosti Hirschmann a je určen pro připojení 32 zařízení, což nám bude v tomto případě stačit.

ZÁVĚR

Diplomová práce je rozdělena na dvě hlavní části a to teoretická východiska a vlastní návrh řešení. Kapitola teoretická východiska se zabývá základními pojmy a názvoslovím z oblasti informační bezpečnosti, dále jsou zde uvedeny normy, ze kterých se vycházelo. Uvedena byla také problematika analýzy rizik a popis bezpečnostních hrozeb. Další část teoretických východisek se zaměřovala na průmyslovou bezpečnost a její řešení jako např. management pasivní vrstvy, industrial ethernet, vysvětleny byly také parametry průmyslové infrastruktury, její topologie a pojem redundance. Dalším pojmem byla síť s maximální dostupností a problematika napájení zařízení po síti, neboli Power over Ethernet a závěr teoretických východisek se zaměřoval na zónové řešení pomocí aplikačního firewallu.

Praktická část diplomové práce se skládá z části, kde byl popsán současný stav firmy, ve které se návrh realizoval. V této analýze byl popsán současný stav síťové infrastruktury a zařízení, které firma využívá. Z výsledků pak byly vyvozeny nedostatky, které se musely napravit. V další části byla provedena analýza rizik, kde se nejprve identifikovala aktiva firmy a vhodně ohodnotila. Následně byl sestaven seznam hrozeb a zranitelností. Z těchto seznamů byla poté sestavena matice rizik, která poukázala na nejkritičtější části ve firmě, tedy jaká aktiva jsou nejzranitelnější. Samotný návrh síťové infrastruktury měl několik částí. Nejprve musely být správně rozmístěny uzlové body sítě a také vedení optických tras. Následně bylo vybráno vhodné místo pro umístění bezdrátového prvku pro pokrytí vymezené oblastí Wi-Fi signálem. Po těchto úkonech se musely vybrat vhodné prvky pasivní a aktivní vrstvy. Veškeré prvky těchto vrstev byly vybrány pečlivě a hlavně podle kvality a požadavků na průmyslové řešení. V další části bylo nutné oddělit průmyslovou a administrativní síť a udělat zónové řešení pomocí aplikačního firewallu. Celá síťová infrastruktura se na závěr zastřešila management softwarem, který bude celou síť monitorovat a upozorňovat na výpadky, nebo nedostatky. V poslední části návrhu byly zavedeny nejkritičtější oblasti ISMS, které byly z analýzy rizik vyhodnoceny. Celý návrh síťové infrastruktury byl zhodnocen v ekonomické rozvaze, kde jsou popsány jednotlivé komponenty s příslušnou cenou.

Hlavním přínosem práce pro firmu je funkční a spolehlivá síťová infrastruktura, která splňuje veškeré požadavky průmyslového řešení, a také zavedení některých částí ISMS. Výběr prvků, které jsem použil, byl hlavně z důvodu, že jsem osobně navštívil společnost Hirschmann, která tyto prvky vyrábí, a na vlastní oči jsem viděl, s jakou precizností jsou vyráběny a kontrolovány, než jsou poslány k odběratelům. V práci bylo také poukázáno na rizikovou situaci, která by mohla nastat, pokud by se nevybudovala nová síťová infrastruktura. Pokud by daná situace nastala, mohlo by to mít fatální následky na fungování firmy. Díky nové infrastruktuře a také návrhům zavedení informační bezpečnosti byla firmě poskytnuta metodika pro zavádění informační bezpečnosti a k její následné správě, plně v souladu s doporučeními ISMS.

SEZNAM POUŽITÉ LITERATURY

[1] ONDRÁK V., P. SEDLÁK a V. MAZÁLEK. *Problematika ISMS v manažerské informatice*. 1. vyd. Brno: CERM, Akademické nakladatelství, 2013. ISBN 978-80-7204-872-4.

[2] *ČSN ISO/IEC 27005. Informační technologie - Bezpečnostní techniky – Řízení rizik bezpečnosti informací - Přehled a slovník*. Praha: Český normalizační institut, 2014.

[3] JORDÁN, V. a V. ONDRÁK. *Infrastruktura komunikačních systémů II: Kritické aplikace*. 1. vyd. Brno: CERM, Akademické nakladatelství, 2015. ISBN 978-80-214-5240-4.

[4] JORDÁN, V. a V. ONDRÁK. *Infrastruktura komunikačních systémů III: Integrovaná podniková infrastruktura*. Brno: CERM, Akademické nakladatelství, 2016. ISBN 978-80-214-5241-1.

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

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

[7] SEDLÁK, P. *Technologická bezpečnost ICT*. Přednáška. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská: akademický rok 2015/2016.

[8] LASER TECHNOLOGY. *lasertechnology.cz* [online]. © 2008-2016 [cit. 2016-4- 27]. Dostupné z: http://www.lasertechnology.cz/img/pic-laser-paleni5.jpg

[9] TOP KONTAKT. *produkty.topkontakt.idnes.cz* [online]. © 1999-2016 [cit. 2016-4-27]. Dostupné z: http://s.topkontakt.cz/images//img_product/200/02422/02422002_foto_200_8818952783.jpg

[10] EMS. *engineeredmechanicalsystems.com* [online]. © [cit. 2016-4-27]. Dostupné z: http://98.130.116.9/images/V85new.jpg

[11] HOLL. *holl-online.de* [online]. © 2016 [cit. 2016-4-27]. Dostupné z: http://www.holl-online.de/file/image/7d7739dc22302374a0ab83b174ecaaa4.png/f

[12] BELEC. *belec.de* [online]. © 2016 [cit. 2016-4-27]. Dostupné z: https://www.belec.de/fileadmin/_processed_/csm_Belec_compct_port_wagen_blau125_02_536bbca312.jpg

[13] DACEL. *dacel.com.tr* [online]. © 2016 [cit. 2016-5-9]. Dostupné z: http://www.dacel.com.tr/upload/data/images/inet_ethernet/mach104_ailesi.gif

[14] GAE. *gae.co.id* [online]. © 2016 [cit. 2016-5-9]. Dostupné z: http://www.gae.co.id/userdata/uploads/product/910109d58c5baecda1f2636e8c6545b8.png

[15] MI GROUP. *mi-group.eu* [online]. [cit. 2016-5-10]. Dostupné z: http://www.mi-group.eu/fileadmin/_processed_/csm_p_ik_EAGLE_30_5702cfa58a.jpg

[16] INS. *industrialnetworking.com* [online]. © 2016 [cit. 2016-5-10]. Dostupné z: http://www.industrialnetworking.com/Tofino-Xenon-Security.jpg?resizeid=-2&resizeh=240&resizew=240

[17] GUMEX. g*umex.cz* [online]. © 2015 [cit. 2016-5-10]. Dostupné z: http://www.gumex.cz/index.php?ma=ajax&sid=pimage&pid=26049

[18] TRITON. *triton.cz* [online]. © [cit. 2016-5-10]. Dostupné z: http://www.triton.cz/userfiles/image/SAD/2015/SAD_1.jpg

[19] DOCPLAYER. *docplayer.cz* [online]. © 2016 [cit. 2016-5-13]. Dostupné z: http://docplayer.cz/docs-images/25/5901189/images/13-0.png

[20] DOUCEK, P. et al. *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM*. 2. vyd. Praha: Professional Publishing, 2011, 286 s. ISBN 978-80-7431-050-8.

[21] *ČSN ISO/IEC 27000. Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnostní informací - Přehled a slovník*. Praha: Český normalizační institut, 2014.

[22] QCOM. *qcom.cz* [online]. © 2016 [cit. 2016-5-13]. Dostupné z: http://www.qcom.cz/home/cesky/systemy_rizeni/isms/struktura_27k.gif

[23] PROFITEK. *profitek.co.za* [online]. © 2015 [cit. 2016-5-13]. Dostupné z: http://profitek.co.za/wp-content/uploads/2016/02/Hirschmann-OpenBAT-R.jpg

SEZNAM TABULEK

SEZNAM OBRÁZKŮ