VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

FYZICKÁ BEZPEČNOST V PRŮMYSLOVÉM PODNIKU
PHYSICAL SECURITY IN AN INDUSTRIAL COMPANY

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Bc. Pavel Konečný**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. Petr Sedlák**
SUPERVISOR

BRNO 2017

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Student:	**Bc. Pavel Konečný**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Informační management
Vedoucí práce:	**Ing. Petr Sedlák**
Akademický rok:	2016/17

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává diplomovou práci s názvem:

Fyzická bezpečnost v průmyslovém podniku

Charakteristika problematiky úkolu:

Úvod
Vymezení problému a cíle práce
Teoretická východiska
Analýza současného stavu
Vlastní návrh řešení
Zhodnocení a přínosy práce
Závěr
Seznam použité literatury
Přílohy

Cíle, kterých má být dosaženo:

Pro vybranou společnost (organizaci) na základě analýzy vypracujte metodický postup pro řešení fyzické bezpečnosti v rámci zavádění ISMS.

Základní literární prameny:

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

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

DOUCEK, Petr. Řízení bezpečnosti informací: 2. rozšířené vydání o BCM. 2., přeprac. vyd. Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.

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

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2016/17

V Brně dne 28.2.2017

L. S.

doc. RNDr. Bedřich Půža, CSc. ředitel	doc. Ing. et Ing. Stanislav Škapa, Ph.D. děkan

Abstrakt

Práce je zaměřena na řešení fyzické bezpečnosti organizace působící v segmentu metalurgie. V analytické části jsou identifikovány nedostatky v jednotlivých oblastech fyzické bezpečnosti dle norem ČSN ISO/IEC řady 27 000. Návrhová část je shodně rozčleněna do jednotlivých kapitol obsahujících doporučení k modernizaci, nápravě nedostatků či úpravám systémů. Náplní teoretické části je zejména objasnění pojmů a postupů užitých v návrhu. Hlavní přínos práce spatřuji v návrhu změn, po jejichž správné realizaci bude fyzická bezpečnost podniku na vysoké úrovni.

Abstract

The diploma thesis focuses on physical security solutions in an organization acting in a metallurgy segment. The analytical part identifies the weaknesses in individual areas of physical security according to ČSN/ISO 27 000 regulation. The practical part is divided into individual chapters bringing suggestions for corrections, modernization and modifications of the system. The theoretical part deals mainly with clarification of the terminology and proceses used in the practical part. I see the benefit of my work in the practical suggestions for the changes. If they are implemented correctly, the physical security of the organization will be of high quality.

Klíčová slova

Fyzická bezpečnost, kamerový systém, ochrana perimetru, kontrola vstupů, ISMS, strážní služba, technická ochrana

Key words

physical security, security camera system, perimeter protection, access control, ISMS, guard service utility, technical protection measure

Bibliografická citace

KONEČNÝ, P. Fyzická bezpečnost v průmyslovém podniku. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2017. 86 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 jsou úplné a 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 26. května 2017 .....

podpis

Poděkování

Děkuji vedoucímu práce panu Ing. Petru Sedlákovi za jeho vstřícnost a podporu. Velký vděk patří také panu Ing. Viktoru Ondrákovi, Ph.D., který se ochotně ujal oponentury a poskytnul mi zpětnou vazbu. Dále děkuji všem, kteří mě podporovali a posunuli ke zdárnému odevzdání této práce.

Obsah

ÚVOD

Poptávka firem i jednotlivců po navýšení bezpečnosti v různých oblastech zájmu se v poslední době zvyšuje.[1] [2] Podle mého názoru je tato situace zapříčiněna několika faktory. Mezi nejvýznamnější z nich patří rychlý rozvoj informačních technologií, mediální ruch (terorismus, sabotáže, úniky informací) a inkorporace mezinárodních právních předpisů do českého právního systému.

K tradičním oborům bezpečnosti, mezi které patří bezpečnost práce či požární bezpečnost, se s příchodem informačních technologií připojil obor informační bezpečnosti. Bezpečnost informací byla sice předmětem zájmu již daleko dříve, ale až nástup technologií prudce akceleroval její rozvoj.

Informační bezpečnost je široký pojem, který se dále dělí na rozsáhlé skupiny podoblastí. K návrhu či realizaci opatření z oblastí informační bezpečnosti je důležitá dobrá znalost problematiky, včetně technických řešení, managementu, právních předpisů a práce s lidskými zdroji. Pro IT zaměstnance firem, které nezaměstnávají specialistu na ISMS, je často složité se v této problematice komplexně orientovat. Při řešení problémů nebo při plánovaných změnách se pak podniky musí spoléhat na rady externích konzultantů.

I ke vzniku této práce přispěl fakt, že ve společnosti, se kterou mi bylo umožněno spolupracovat, nebyl v tu chvíli zaměstnán specialista na informační bezpečnost. Má práce se zaměřuje na segment fyzické bezpečnosti informací a základní ochranu aktiv v průmyslovém podniku z oblasti metalurgie. Vzhledem k povaze informací uvedených dále v práci si podnik přál utajit svoji identitu. Protože utajení celé práce již není možné, bude anonymizován její text. To představuje nahrazení identifikovatelných údajů jako např. název nebo poloha podniku vágními a obecnými pojmy. V odkazech na zdroje, které by mohly kompromitovat identitu podniku, jsou uvedeny pouze základní identifikátory a značka „/anonymizováno/“.

[1] Zvyšující se tržby společnosti COMGUARD potvrzují rostoucí poptávku po bezpečnostních i síťových řešeních [online].
[2] Peníze do technologií ano, do vzdělávání lidí ne: firmy riskují, že jim zabezpečení dat selže [online].

CÍLE PRÁCE, METODY A POSTUPY ZPRACOVÁNÍ

Cíle

Cílem práce je analyzovat stav fyzické bezpečnosti zvoleného závodu a na základě zjištěných nedostatků navrhnout nápravná opatření.

Metody

Návrh je zpracován dle doporučení norem řady 27 000, resp. pasáží týkajících se fyzické bezpečnosti. Analytická i návrhová část je členěna do kapitol, jejichž názvy jsou odvozeny z přílohy A normy ČSN ISO/IEC 27 001. Teoretická část se skládá z vybraných pojmů a kontextu důležitého pro výběr opatření v návrhové části.

Analýza byla provedena během několika návštěv podniku, během nichž mi bylo umožněno zkontrolovat většinu oblastí. Zbývající informace jsem doplnil ze záznamů několika rozhovorů, kdy mi na připravené otázky odpovídal odpovědný pracovník.

Plány rozmístění budov, kamer apod. byly zpracovány nad mapovým podkladem serveru mapy.cz, z důvodu zachování měřítka. Ke grafickým úpravám jsem využil volně dostupného softwaru Paint.NET.[3]

Postup zpracování

- Studium literatury a elektronických zdrojů
- Analýza stavu fyzické bezpečnosti podniku
- Instalace potřebného SW
- Návrh změn
- Sestavení teoretické části
- Formální úpravy práce a anonymizace

[3] Paint.NET [online].

1 TEORETICKÁ ČÁST

Pro pochopení vzájemných souvislostí v analytické a návrhové části práce je potřeba objasnit některé pojmy a postupy. Jejich souhrn je náplní této části práce.

1.1 Fyzický bezpečnostní perimetr

Jedním ze základních úkolů při implementaci fyzické bezpečnosti je vymezení chráněných prostor. Za tímto účelem se zřizuje bezpečnostní perimetr. Fyzický bezpečnostní perimetr je prostor chráněný fyzickými bariérami, často v kombinaci s technickými prostředky anebo strážní službou.[4]

1.1.1 Oplocení

Běžná oplocení slouží k vytyčení hranice perimetru a působí spíše jako psychologický varovný prvek, než jako bariéra. Silnější ochrany lze docílit zbudováním robustních plotů např. z betonu anebo instalací dodatečných prostředků jako jsou např. ostnaté dráty či elektronická detekční zařízení. Mezi tato zařízení patří například otřesové kabely, mikrovlnné detektory pohybu nebo infračervené závory.[5]

Při volbě síly oplocení je nutné zvážit rizika v souvislosti s činností podniku, danou lokalitou, finanční hodnotou aktiv atp. Obrázky 1 až 3 zachycují průmyslové oplocení v jeho různých odolnostech.[6] [7]

[4] DRASTICH, Martin. Systém managementu bezpečnosti informací.
[5] GORDON, Adam a Javvad. MALIK. Official (ISC)2® guide to the CISSP® CBK®: Certified Information Systems Security Professional.
[6] Průmyslové ploty. In: PK Mont Moravia s.r.o.: Vrata-brány-pohony-ploty [online].
[7] Betonový plot hladký, SP240 + ostnatý a žiletkový drát. In: Ploty Ostrava [online].

Obrázek 1: Základní průmyslové oplocení (upraveno, Zdroj: Průmyslové ploty [6])

Obrázek 2: Posílené průmyslové oplocení (upraveno, Zdroj: Průmyslové ploty [6])

Obrázek 3: Betonové průmyslové oplocení s žiletkovým drátem (upraveno, Zdroj: Betonový plot [7])

1.1.2 Technické prostředky obvodové ochrany

1.1.2.1 Otřesové kabely

Tento systém využívá koaxiální kabely, které jsou v několika řadách rozvinuty po celé délce pletiva. Kabely je přenášeno elektrické pole, jehož vlastnosti se při změně polohy kabelu v důsledku snahy o překonání plotu mění. Změny jsou detekovány řídící jednotkou a vyvolají alarm. Citlivost systému je nastavitelná tak, aby odpovídala lokálním odlišnostem, které by mohly způsobovat falešné poplachy (např. síla větru). Mezi výhody tohoto řešení patří nízká finanční náročnost, snadné pokrytí rozsáhlých a členitých hranic pozemků, možnost nastavení citlivosti. Problémem může být fakt, že systém je možno provozovat pouze na ohebném oplocení jako je pletivo. Některé druhy kabelů jsou také náchylné k elektromagnetickému rušení.[8] [9]

Zajímavou alternativou koaxiálních kabelů, jsou optické kabely. Jejich předností je, že jsou detekovatelné pouze vizuálně, neboť do prostoru v okolí nic nevyzařují. Rovněž nemohou být rušeny elektromagnetickým polem. Touto technologií může být, při použití laserového zdroje třídy 3b, zabezpečena hranice s délkou až 80 km. K detekci je využíváno dvou detekčních vláken. Při nasazení tří vláken je možno identifikovat i místo narušení s přesností přibližně 25 m.[10]

1.1.2.2 Mikrovlnné detektory pohybu

Zařízení vyzařuje mikrovlnný signál s určitými charakteristikami. Zmíněný signál vytváří trojrozměrný pomyslný útvar, v němž probíhá detekce pohybu. Velikost tohoto útvaru je možno měnit dle potřeby. Změřením charakteristik vyzářeného signálu v době, kdy v chráněném prostoru nedochází k pohybu, získá systém referenční hodnotu pro stav, kdy nedochází k narušení. Odchylka od dané hodnoty způsobí poplach. Mikrovlnné signály prochází materiály jako je beton nebo ocel. Senzory by proto neměly být umístěny v těsné blízkosti komunikací nebo budov. Tím se zabrání častým falešným

[8] GORDON, Adam a Javvad. MALIK. Official (ISC)2® guide to the CISSP® CBK®: Certified Information Systems Security Professional.
[9] Scorpion system: PLOTOVÝ ZABEZPEČOVACÍ SYSTÉM (PZS) SCORPION [online].
[10] Zabezpečovacia technika: Elektronický zabezpečovací systém – EZS časť.2: PRVKY OBVODOVEJ OCHRANY [online].

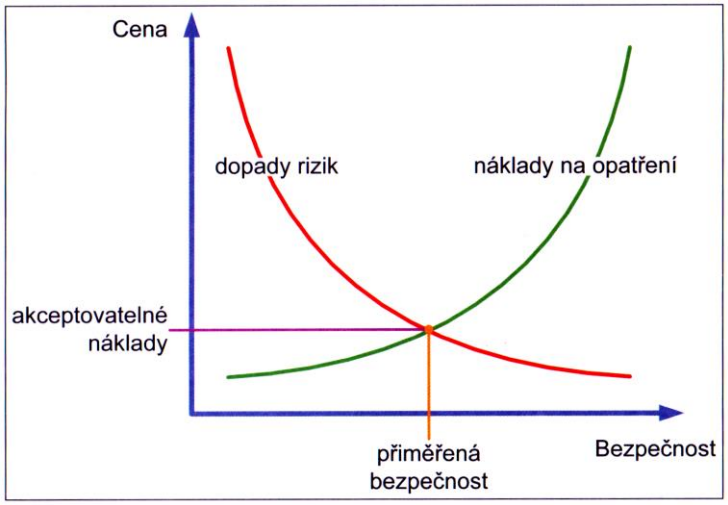
poplachům a zároveň nedojde k ohrožení zdraví osob v důsledku dlouhodobého vystavení mikrovlnám. K výhodám těchto detektorů patří zejména dobrá odolnost proti změnám počasí v porovnání se systémy založenými na detekci laserových paprsků.[11]

1.1.2.3 Infračervené závory

Tato zařízení emitují infračervené paprsky, které jsou rozpoznány snímačem. Při přerušení paprsku je spuštěn poplach. Paprsky jsou obvykle alespoň 2, aby nedocházelo k falešným poplachům. Zařízení je citlivé na vlivy počasí jako déšť nebo mlha. Pro jeho správnou funkci se nesmí mezi přijímačem a emitorem nacházet vysoká tráva nebo jiné podobné překážky, neboť by mimo jiné vlivem větru docházelo k falešným poplachům.[12]

1.2 Přiměřená bezpečnost

Při zavádění bezpečnostních opatření je třeba kromě úrovně dosažené bezpečnosti sledovat také ekonomická hlediska. Výše prostředků investovaných do bezpečnosti by neměla překročit hodnotu chráněných aktiv nebo hodnotu nápravy škod způsobených poškozením aktiva. Koncept přiměřené bezpečnosti znázorňuje následující graf.[13]



Obrázek 4: Graf znázorňující přiměřenou bezpečnost (skenováno s. 36, Zdroj: Problematika ISMS […] [13])

[11] GORDON, Adam a Javvad. MALIK. Official (ISC)2® guide to the CISSP® CBK®: Certified Information Systems Security Professional.
[12] tamtéž
[13] ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. Problematika ISMS v manažerské informatice.

1.3 Síťová bezpečnost

Síťová bezpečnost je širokým pojmem. V následujícím textu zmiňuji pouze první tři síťové vrstvy a stručně také vybrané protokoly či technologie.

Referenční model ISO/OSI, používaný jako názorný příklad řešení komunikace v počítačových sítích, obsahuje 7 vrstev. V rámci každé z nich je možno řešit dílčí bezpečnost. V rámci 1. fyzické vrstvy (L1) lze řešit bezpečnost rozvodů, jejich správné uložení, stínění proti vnějšímu záření apod. Zabezpečení pasivní vrstvy (kabeláže) lze rozdělit do tří stupňů zabezpečení. Jedná se o následující skupiny opatření:[14]

- Identifikační opatření (úroveň 0)
- Blokační opatření (úroveň 1)
- Klíčování portů (úroveň 2)

1.3.1 Network Infrastructure Security Solution

Systém NISS, typický představitel managementu bezpečnosti pasivní vrstvy, pracuje v rámci uvedených úrovní. Nultá úroveň neposkytuje fyzickou ochranu a slouží pouze k zpřehlednění systému. To zajišťují identifikátory kabelů. První úroveň umožňuje blokování datových portů proti připojení nebo proti odpojení kabelu. Také sem patří nejrůznější blokátory přístupu ke kabelovým trasám či rozvaděčům. Úroveň 2 řeší klíčování konektorů a portů.[15]

[14] ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. Problematika ISMS v manažerské informatice.
[15] tamtéž

1.3.2 Vlastnosti kabelů

Kabeláž použitá k výstavbě sítě je součástí fyzické vrstvy. Nejrozšířenější používané kabely jsou klasifikovány jako kategorie 5 nebo kategorie 6. Jedná se o metalické kabely. Kategorie udává jaký frekvenční rozsah je kabel schopen přenést. U kategorie 5 je to hodnota do 100 MHz. U kategorie 6 pak do 250 MHz. Parametr AWG pak udává průměr vodiče bez izolace (čím nižší číslo, tím větší průměr). Kabely kategorie 6 mají obecně větší průměr vodičů než kabely kategorie 5. Díky tomu vydrží kabely kategorie 6 vyšší proudové zatížení. Díky nižšímu elektrickému odporu je tedy při nasazení technologie PoE vhodnější použít kabely kategorie 6.[16]

1.3.3 Power over Ethernet (PoE)

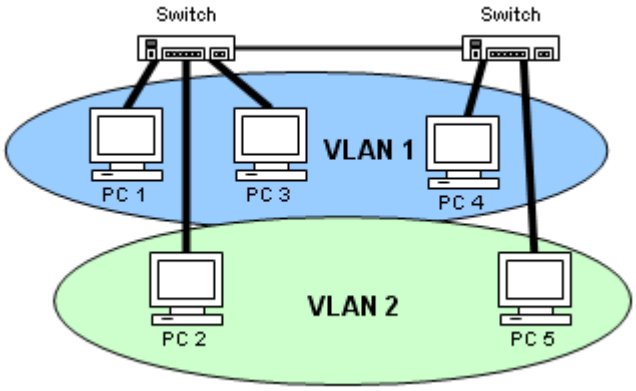
PoE je technologie umožňující elektrické napájení koncového zařízení prostřednictvím datové kabeláže. Mezi výhody tohoto řešení patří zjednodušení připojování zařízení, možnost dálkového restartu zařízení příkazem k vypnutí a opětovnému zprovoznění daného portu, napájení při výpadku (v případě použití systému UPS v rozvaděči) a úspory na jinak nutné elektrické infrastruktuře. Omezujícím faktorem této technologie je příkon napájeného zařízení. Vývoj technologie však stále pokračuje a v nejvyšší třídě (high-power PoE, IEEE 802.3bt) lze připojit zařízení o maximálním příkonu 100 W.[17] [18]

V rámci 2. linkové vrstvy (L2) jsou z pohledu bezpečnosti významné zejména pojmy VLAN (Virtual Local Area Network), MAC (Media Access Control) a topologie fyzické vrstvy z pohledu možností redundance.

[16] JORDÁN, Vilém a Viktor ONDRÁK. Infrastruktura komunikačních systémů I: univerzální kabelážní systémy.
[17] PoE Types: What They Mean and How They're Used [online].
[18] Power over Ethernet (PoE) Explained: Part 2 - Demystifying POE [online].

1.3.4 VLAN

VLAN je technologie sloužící k logickému oddělování sítí a to nezávisle na fyzickém členění. V rámci podnikových sítí je vhodné tohoto nástroje užít mimo jiné k separování datových toků dle jejich účelu. Například vytvořit samostatnou VLAN pro kamerový systém, další pro VoIP atp. Oddělené sítě pak mohou být snáze spravovány s ohledem na potřeby jednotlivých druhů provozu. Komunikace je doručována pouze na porty v rámci dané VLAN. Port, který je zařazen do více VLAN označujeme jako trunk.[19]



Obrázek 5: Dělení na jednotlivé VLAN (převzato, Zdroj: Lupa.cz [20])

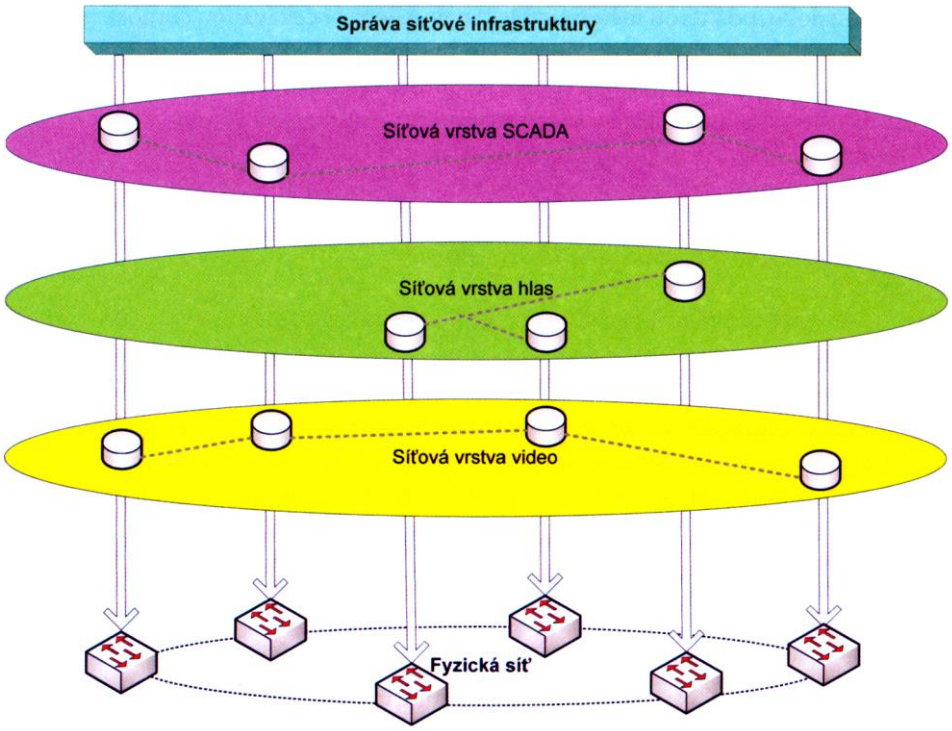
MAC adresa, někdy označovaná jako fyzická adresa, slouží k jednoznačné identifikaci zařízení (jeho síťové karty) v rámci sítě. V sítích Ethernet MAC adresu tvoří 48bitů. Existují také speciální adresy pro všesměrové a skupinové adresování. S adresami lze pracovat v rámci blacklistů a whitelistů, tedy seznamů odepírajících či umožňujících přístup ke konkrétním systémům.[21]

Topologii lze stručně charakterizovat jako způsob propojení jednotlivých uzlů v síti. Mezi nejčastěji používané topologie patří sběrnice, hvězda, kruh a polygon.

[19] VLAN - Virtual Local Area Network. SAMURAJ-cz.com - počítačové sítě, Cisco, Microsoft, VMware, administrace [online].
[20] VLAN. In: Lupa.cz: Server o českém internetu: Bráníme se odposlechu: obrana na switchi [online].
[21] MAC adresa [online]. ČR: Západočeská universita v Plzni.

V průmyslových prostředích je nasazován hlavně kruh, v některých případech i polygon a to z důvodu redundance.[22]

Síťová vrstva (L3) se stará o směrování v síti a adresování. Každý host sítě musí mít přidělenu jedinečnou IP adresu. Ta může být zařízení přidělena staticky správcem sítě nebo DHCP serverem. DHCP Server dynamicky přiděluje klientům v síti IP adresy spolu s dalšími údaji. Činí tak pomocí protokolu DHCP (Dynamic Host Configuration Protocol). Z pohledu správy sítě je výhodné vyhrazovat adresní rozsahy, případně vytvářet podsítě, pro zařízení dle jejich účelu. Při tvorbě rozsahů je důležité ponechat dostatečné rezervy pro případ rozšíření počtu prvků v síti.[23] [24]



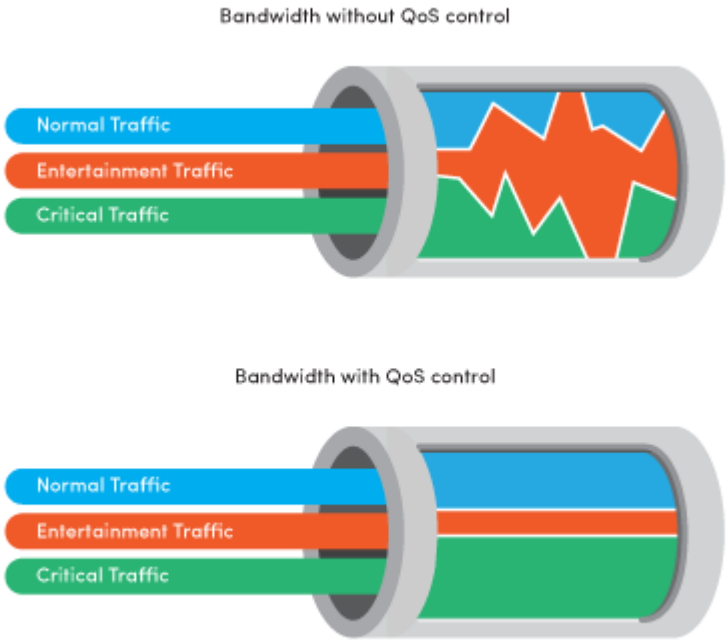
Obrázek 6: Oddělení různých síťových provozů (skenováno s. 253, Zdroj: Problematika ISMS […] [25])

Sítě lze logicky dělit směrováním, spravovat šířku přenosového pásma pomocí technologie QoS (Quality of Service), izolovat nespolehlivé aplikace.[25]

[22] Topologie sítí [online]. ČR: Technická universita Ostrava.
[23] Síťová vrstva [online]. ČR: SPŠ Hradec Králové.
[24] What Is DHCP? [online]. USA: Microsoft.
[25] ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. Problematika ISMS v manažerské informatice.

QoS je síťové řešení sloužící k prioritizaci určitého síťového provozu tak, aby bylo zajištěno, že kritické přenosy dostanou přednost před méně významnými toky v době vysoké zátěže sítě. Příkladem kritických přenosů jsou stream data kamerového systému, VoIP data, výrobní instrukce apod. Naopak mezi méně důležité spadá přístup k webu či přenosy firemních dokumentů.

Pro správnou funkci QoS musí být technologie podporována na všech aktivních prvcích v rámci sítě. Následující obrázek znázorňuje rozdíl v zatížení sítě bez a se zprovozněným QoS.[26]



Obrázek 7: Dopady QoS na rozdělení šířky pásma (převzato, Zdroj: Nehos wiki Communications [26])

Důležitým faktorem v síti je čas evidovaný na jednotlivých zařízeních. K jeho synchronizaci slouží například Network Time Protocol (NTP). Synchronizující

[26] Nehos QoS [online]. USA: Nehos wiki Communications

se zařízení pošle několik dotazů na NTP servery. V odpovědi dostává přesné časy, z nichž pomocí algoritmu určí čas s přesností v řádu milisekund.[27]

Z důvodu omezeného počtu veřejných IPv4 adres a pro možnost seskupit pod jednu veřejnou adresu více prostředků lokální sítě je používána technologie NAT (Network Address Translation). NAT překládá při směrování lokální IP adresy na veřejnou a pomocí dynamických NAT tabulek udržuje v paměti další informace jako čísla portů jednotlivých přenosů apod. Příchozí odpovědi jsou tak díky těmto tabulkám směrovány na konkrétní lokální IP adresu. Téměř všechny routery mají tuto funkcionalitu implementovány. Pro správce sítí je tato technologie důležitá. Pokud ji ale neoprávněně používá některý z uživatelů, značně tím ztíží možnosti rozkrytí struktury sítě za routerem.[28]

1.4 Bezpečnostní prvky

1.4.1 Osvětlení

Osvětlení areálu umožňuje strážní službě vizuální kontrolu prostoru i za tmy. Působí také jako psychologický odstrašující prvek a eliminuje zastíněná místa, na kterých by se mohl ukrývat narušitel. Osvětlení by mělo strážným umožnit rozpoznat osobu na vzdálenost přibližně 20 m. Ze vzdálenosti 10 m pak rozpoznat tvář. Tyto vzdálenosti umožnují adekvátně reagovat na vzniklé situace z bezpečného odstupu. Pomocí světel lze také zlepšit obraz kamer, který bude za tmy zabírat větší prostor anebo bude lépe rozpoznatelný.[29]

[27] NTP Documentation: The NTP FAQ and HOWTO [online].
[28] What Is NAT? [online]. USA: Microsoft
[29] GORDON, Adam a Javvad. MALIK. Official (ISC)2® guide to the CISSP® CBK®: Certified Information Systems Security Professional.

1.4.1.1 Typy osvětlení

Typ použitého osvětlení závisí na bezpečnostních požadavcích. Základní rozdělení osvětlovacích systémů tvoří tyto čtyři skupiny:[30]

- Trvalé osvětlení
- Spínané osvětlení
- Pohyblivé osvětlení
- Nouzové osvětlení

Trvalé osvětlení je nejběžněji používaný systém. Jedná se o skupinu světel, která za snížené viditelnosti osvětluje požadovanou oblast navzájem se překrývajícími kužely světla. Spínané osvětlení je instalováno stejným způsobem jako trvalé, s tím rozdílem, že je spínáno na základě potřeby. To může být prováděno automaticky pomocí čidel pohybu nebo na pokyn strážných. Existuje také varianta náhodného spínání. Tato funkce má vyvolat dojem pohybu zaměstnanců v areálu a odradit tak vnějšího pozorovatele od snahy proniknout do areálu. Pohyblivé osvětlení slouží většinou k doplnění předešlých zmíněných systémů. Tento typ je užíván ve specifických objektech, jako jsou např. věznice. Ovládání může být manuální nebo dálkové, případně automatické, kdy je světlomet zaměřován pomocí infrakamer, které sledují tepelnou stopu osoby v hlídaném prostoru. Nouzové osvětlení slouží při výpadku energie převážně k bezpečné orientaci zaměstnanců v budovách a areálu (nalezení nouzových východů apod.) a jeho funkce je časově omezena v řádu jednotek až desítek minut. Výdrž ovlivňuje zvolená technika napájení. Jedná se o bateriové systémy nebo dieselové elektrocentrály. Systémy nouzového osvětlení je vhodné z výše uvedených důvodů provozovat s co nejvyšší efektivitou. To umožňuje např. technologie LED (Light Emitting Diode). Klasické žárovky dokáží vyzářit světelný tok cca 12 lm/W, lepší hodnoty dosahují kompaktní zářivky s 60 lm/W. LED technologie dosahuje hodnot v rozsahu cca 80 až 160 lm/W.[31] [32]

[30] GORDON, Adam a Javvad. MALIK. Official (ISC)2® guide to the CISSP® CBK®: Certified Information Systems Security Professional.
[31] tamtéž
[32] LED technologie [online]. ČR: LIGHTRONIC

1.4.2 Kontrola přístupu

Primární funkcí systému řízení přístupu je zajistit, aby se do kontrolované oblasti dostaly pouze povolané osoby nebo žádaný materiál. Zaměstnance, zákazníky a návštěvy je vhodné kontrolovat v rozdílné míře, dle konkrétních požadavků na bezpečnost. Kontroly identit mohou být také automatizovány nasazením technologie čipových karet či obdobného řešení. Kontrolovaná oblast by také měla být rozdělena na několik zón, dle bezpečnostních potřeb každé z nich. Například oddělení, kde je nakládáno s citlivými údaji, by mělo mít definované přísnější pravidla vstupu než místnost pro návštěvy.[33]

Základní používané komponenty v systému kontroly vstupu jsou:[34]

- Čtečky karet
- Elektrické zámky
- Alarmy
- Počítačový systém pro monitorování a řízení vstupu
- Další technické a mechanické prostředky jako např. zavírače dveří

Zaměstnanci by také měli být vizuálně identifikovatelní. K tomu slouží karty s fotografií. Systém by měl zaznamenávat pohyb osob a neoprávněné pokusy o vstup. Při nasazení karet je důležité zvážit jejich využití i v dalších systémech podniku. Pro tyto aplikace se používají tzv. smart card (chytré karty), které disponují vlastní pamětí a je možné na ně ukládat data z více systémů. Tyto karty mohou být následně využity při práci s výpočetní technikou jako autentizační tokeny, pro podepisování či šifrování dat apod.[35]

[33] GORDON, Adam a Javvad. MALIK. Official (ISC)2® guide to the CISSP® CBK®: Certified Information Systems Security Professional.
[34] tamtéž
[35] tamtéž

1.4.3 Kamerový systém

Problematika kamerového systému je opět velmi rozsáhlé téma. V této kapitole se pokusím shrnout nedůležitější informace.

Průmyslové kamery dělíme na:[36]

- Barevné
- Černobílé
- Termokamery
- Kombinované kamery

Každá z uvedených má rozdílné výhody. Barevné kamery nabízí více informací (barva vozidla či oblečení sledované osoby) a umožňují tak dohledovým pracovníkům udržovat lepší přehled o dění v chráněném prostoru. Oproti barevným, jsou černobílé kamery schopny pracovat i za špatných světelných podmínek. Termokamery pak mohou pracovat v prostorech zcela neosvětlených, neboť zachycují pouze tepelnou stopu snímaných objektů. Kombinované kamery, např. v provedení barevná – černobílá, poskytují výhody obou. Přes den je snímán barevný obraz, v noci se kamera automaticky přepíná do černobílého módu.[37]

1.4.3.1 Pevné a otočné kamery

Kamery dále dělíme na pevné a otočné. Otočné mohou být ovládané manuálně nebo automaticky. Výhodou otočných kamer je, že obsluha může sledovat i pohybující se zájmový objekt. Nevýhodou pak je, že kamera může být ve chvíli, kdy dochází k incidentu, otočena jiným směrem. Otočné kamery by měly sloužit spíše jako doplňkové nebo musí být po ukončení průzkumu směřovány vždy na konkrétní výchozí místo.[38]

[36] GORDON, Adam a Javvad. MALIK. Official (ISC)2® guide to the CISSP® CBK®: Certified Information Systems Security Professional.
[37] tamtéž
[38] tamtéž

1.4.3.2 Náležitosti systému

Při instalaci kamer je nutno zohlednit také zorné pole kamer tak, aby nebylo zastíněno okolní vegetací či jinými překážkami. Kamery by také měly být nastaveny tak, aby na objektiv nedopadalo přímé sluneční světlo. Rozlišení obrazu by mělo být nastaveno s ohledem na umístění a účel kamery, kapacitu úložného prostoru, atp. Související doporučení obsahuje norma ČSN EN 62676-4. Kamerový systém také musí splňovat legislativní požadavky. Zejména zákon č. 101/2000 o ochraně osobních údajů.[39] [40]

V současné době jsou instalovány převážně IP kamery. Pro konverzi signálu starších, analogových kamer lze použít A/D (analogově/digitální) převodník. A/D převodník je elektronická součástka sloužící k převodu analogového signálu na signál digitální.[41]

1.4.3.3 Ochrana před poškozením

Kamerový systém by měl být chráněn před poškozením. Toho je možné docílit umístěním kamer mimo dosah, vzájemným křížovým snímáním nebo instalací technických prostředků. Je také nutné chránit datové a elektrické přívody ke kamerám.[42]

[39] Zákon č. 101/2000 o ochraně osobních údajů a o změně některých zákonů

[40] GORDON, Adam a Javvad. MALIK. Official (ISC)2® guide to the CISSP® CBK®: Certified Information Systems Security Professional.

[41] AD převodník [online]. ČR: Megapixel

[42] GORDON, Adam a Javvad. MALIK. Official (ISC)2® guide to the CISSP® CBK®: Certified Information Systems Security Professional.

2 ANALÝZA SOUČASNÉHO STAVU

2.1 Popis areálu podniku

Areál analyzovaného podniku se nalézá v průmyslové zóně, kde přímo i nepřímo sousedí s dalšími společnostmi. Uvnitř areálu se nachází několik budov, pronajímané nemovitosti, manipulační plochy a zařízení k vážení nákladních automobilů. Legitimní vstupy do areálu se nachází v severní a západní části. Jedná se o brány (v plánu označené zelenou šipkou jako vstup a) a vstup b)), kterými je umožněn vjezd nákladních a osobních automobilů a o turniket v západní části (v plánu označen zelenou šipkou jako vstup c), kterým vchází zaměstnanci. V jižní části se nachází spojovací brána d), která propojuje areál podniku se sousední společností (dále jen „jižní firma“), pro kterou je tato brána jedinou přístupovou cestou. Veškerý provoz spojený se zásobováním a exportem zboží jižní firmy probíhá přes areál podniku. Rovněž zaměstnanci jižní firmy dochází do práce přes areál podniku. Podnik pronajímá část pozemku a budovu dalším subjektům, pro které musí být zajištěn přístup k těmto nemovitostem.

Budovy jsou užívány k účelům výroby, pro administrativní účely a k zajištění zázemí pro zaměstnance. Na plánu je vyobrazen ucelený blok čtyř na sebe navazujících budov. V první budově ze severní strany probíhá dokončení výroby (expedice), další budova směrem na jih slouží jako administrativní, ještě jižněji je hlavní výrobní hala a východně od ní se nachází budova pískovny. V první ze zmíněných budov dochází k finalizaci výrobků a jejich překlad na kamiony. Budova administrativy také současně slouží jako jídelna pro zaměstnance, serverovna a je v ní umístěna jedna ze dvou rozvoden elektrické energie (rozvodna a serverovna v plánu označeny trojúhelníkem s číslem4). Pomyslné srdce podniku tvoří hlavní výrobní hala, ve které je umístěna elektrická tavící pec (v plánu označena jako trojúhelník s číslem 1), výrobní linka a další náležitosti potřebné pro výrobu. V budově pískovny se kromě strojního zařízení nachází také druhá rozvodna elektrické energie (v plánu označena trojúhelníkem s číslem3). Ostatní budovy slouží ke skladovacím a ostatním účelům nebo jsou pronajímány.

Vyjma hlavních budov se na ploše areálu nacházejí menší objekty. V severní části u každé z bran stojí buňka užívaná jako vrátnice. Další nevyužívaná buňka stojí u turniketu. V jihovýchodní části stojí malá čerpací stanice pohonných hmot (v plánu označená trojúhelníkem s číslem 5). U jihozápadního rohu výrobní haly je zásobník s chladivem (v plánu označen jako trojúhelník s číslem 2).

Fyzická ostraha objektů podniku je zajišťována externí společností. Tato společnost zajišťuje vrátní službu, související činnosti a ostrahu prostoru, k čemuž využívá kamerový systém, který nemá ve svém vlastnictví. Provozovaný kamerový systém vlastní analyzovaný podnik. Jelikož zmíněný systém již není na dnešní poměry dostačující, bude třeba změnit či upravit některé jeho parametry a případně dokoupit další dílčí zařízení. Situační plán je k nahlédnutí v příloze č. 1.

2.2 Fyzická bezpečnost

2.2.1 Hranice fyzického bezpečnostního perimetru

Perimetr areálu tvoří oplocení rozdílné kvality i konstrukčního provedení. Po celé délce severní strany jsou instalovány 3D kovové plotové panely, které jsou uchyceny pomocí hákových šroubů a navzájem propojené panelovými spojkami (tzv. systém nekonečné montáže). Díky vodorovným prolisům a tloušťce jednotlivých prutů má plot dostatečnou tuhost. Jeho bezpečnost dále zvyšují přesahující pruty v horní části, které znesnadňují jeho přelezení. Tento druh oplocení je soudobým prvkem a poskytuje dobrou ochranu. Mezi jeho výhody oproti běžně používanému pletivu patří zvýšená odolnost proti přeštípnutí.

Plot je ve výborné kondici a plní svoji funkci. Severní hranice navíc sousedí s příjezdovou cestou, na jejíž protější straně se rozkládá jiný průmyslový závod, který je rovněž střežen strážní službou. Oblast je přehledná a vrátní jsou schopni kontrolovat celou hranici pohledem ze svého stanoviště (předpokládá se použití dalekohledů).

Obě brány jsou pod permanentním dohledem vrátní služby. Pravděpodobnost neoprávněného vniknutí z této strany je minimální.

Západní strana je chráněna oplocením z litých betonových kvádrových panelů, které jsou vsunuty do drážek dvou sousedících betonových sloupků. Takto je na sebe navršeno přibližně 6 až 8 panelů, které dohromady se sloupky tvoří jeden blok plotu a zmíněné bloky dále tvoří celý plot. Pro znesnadnění překonání plotu je po celé délce instalován ve dvou řadách nad sebou přímý ostnatý drát, který je uchycen na kovové tyči zapuštěné do každého ze sloupků.

Tento plot je vztyčen od jihozápadního rohu k turniketu c) a pokračuje ještě několik metrů severně za turniket, kde je přerušen. Na severní část oplocení navazují budovy skladů, jejichž vnější stěny tvoří část západního perimetru o délce přibližně 135 m. Ovšem oblast mezi sklady a betonovým plotem není chráněna. Částečnou ochranu zde tvoří hustý porost a prudší sráz, což ale nelze považovat za akceptovatelné zabezpečení. Průnik z areálu navazující firmy by byl touto cestou snadný.

Aktuální stav tohoto oplocení není uspokojivý, zřetelně se projevuje vliv povětrnostních vlivů a stáří materiálu. Některé popraskané betonové bloky byly nahrazeny dřevěnými deskami, jiné jsou ponechány roztříštěné na několik kusů. Nevýhodou je, že v betonu nejsou zality roxorové tyče, čímž blok po rozlomení ztratí celistvost a je snáze demontovatelný. Ochrana ostnatým drátem je na několika místech výrazně oslabena. Drát je částečně poškozen korozí, což se mimo ztráty pevnosti projevuje otupením jeho hrotů, a v některých místech je stržen z úchytných tyčí, o což se přičinily větve padající ze stromů v jeho těsné blízkosti. Zmíněné stromy jsou problematické i z toho důvodu, že značně ulehčují překonání plotu oběma směry. Areál z této strany sousedí převážně s rozsáhlými travnatými plochami s minimálním pohybem osob. Pás křovin, z vnější strany plotu, umožňuje nepozorovatelné přiblížení podél celého plotu, jelikož jeho konstrukce neumožňuje pohled ven z objektu a křoviny cloní i pohled z vnější strany. Vchod přes turniket je dozorován pouze nepřímo, pomocí kamerového systému. Neoprávněné vniknutí do areálu z této strany je nejpravděpodobnější.

Obrázek 8: Neuspokojivý stav západního perimetru (Zdroj: autorská fotografie)

Oplocení západní strany průběžně pokračuje jižním směrem až za hranice areálu, kde tvoří západní hranici perimetru jižní firmy. Mezi jižní firmou a areálem podniku je nataženo pletivo, které je upevněno tříbodovým systémem na pozinkované kovové sloupky. V jihovýchodním rohu je plot přerušen bránou a přilehlým turniketem.

Stav oplocení je dobrý, povrchově narezlé pletivo je pevně spojeno se stabilními sloupky. Skrze plot je vidět na jednu z budov jižní firmy a přilehlé pozemky. Na pozemku jižní firmy roste vysoká tráva a osamocené křoviny, které by bylo možno z pohledu vetřelce využít jako maskování při přípravě na překonání plotu, avšak pouze za snížené viditelnosti anebo v nočních či brzkých ranních hodinách. V době mého pozorování byla brána v jihovýchodním rohu otevřená a hlídaná jen nepřímo prostřednictvím kamerového systému. Tato otevřená brána tvoří slabé místo v ochraně jižní hranice, mimo jiné i proto, že neznáme přesný stav zabezpečení perimetru jižní firmy. Do areálu lze také bez větších obtíží vniknout po energo-mostu přes instalované servisní žebříky.

Zřejmě nejspornější je ochrana východní části. Všechny ostatní strany jsou (vyjma neošetřeného severozápadního segmentu) ohraničeny plotem přímo na linii perimetru, což zde není dodrženo. Areál se zde volně prolíná s pozemkem sousedící spřátelené společnosti (dále jen „spřátelená firma“) a hranici tu tvoří pouze násypy, zdi budov a podobné barikády, které jsou na některých místech doplněné kamerovým systémem. Do budoucna je plánována výstavba plotu stejné konstrukce jako v severní části.

Východní strana tedy tvoří nejslabší článek v systému zabezpečení perimetru. Osoby, které získají přístup na pozemek spřátelené firmy (ať již legitimně či protiprávně), jsou schopny s vyvinutím minimálního úsilí překonat pomyslnou „hranici“ a následně se svobodně pohybovat po areálu, až do okamžiku jejich eventuálního odhalení. Zřejmě se tu spoléhá pouze na to, že oplocení spřátelené firmy je celistvé a v relativně dobrém stavu, alespoň tedy v místech, které jsem měl možnost prověřit. Z uvedeného vyplývá, že riziko průniku je přímo závislé na kvalitě zabezpečení spřátelené firmy. Bezpečnost v areálu tedy ovlivňuje cizí subjekt, což nemůže být akceptováno a tento stav je třeba ošetřit.

Tabulka 1: Rekapitulace stavu oplocení (Zdroj: vlastní tvorba)

Tabulka rekapitulace	Strana perimetru			
	Severní	Jižní	Východní	Západní
Viditelnost skrze oplocení	ANO	ANO	ANO	NE
Vyhovující technický stav	ANO	ANO	NE	NE
Odolnost proti poškození	Vysoká	Nízká	NE	Velmi vysoká
Odhadované riziko průniku	Malé	Střední	!!!	Vysoké
Počet vstupů či vchodů	2	1	x	1
Stromy a keře v blízkosti	NE	Téměř ne	ANO	ANO
Doporučit změnu	NE	ANO	ANO	ANO

Popis aktuálního stavu perimetru je tímto naplněn. Dále je potřeba analyzovat prostory uvnitř areálu.

2.2.2 Vnitřní pásmo

Jako další perimetrickou oblast si definuji prostory mezi hranicemi budov a jiných ohraničených objektů a vnějším perimetrem, tedy nezastavěné pozemky podniku (dále jen „vnitřní pásmo“). Hlavní prioritou z pohledu bezpečnosti ve vnitřním pásmu je, co nejvíce zvýšit pravděpodobnost odhalení nepovolaných osob v co nejkratším čase. Za tímto účelem byly v minulosti kolem vnitřní strany jižního a západního perimetru (pouze po turniket) instalovány elektronické závory. Zařízení závor však v současnosti není v provozuschopném stavu. Dokonce již při instalaci závor byly porušeny základní

zásady. Jedná se mimo jiné o fakt, že zařízení infrazávor je instalováno rovnoběžně se stěnou perimetru, přičemž ale není dodržena předepsaná vzdálenost umístění od stěny, tedy alespoň 1 m.[43] Osoba snažící se vniknout do areálu, by po skoku z hrany plotu pravděpodobně dopadla za detekční zónu takto provozovaných závor. V rámci preventivních opatření byl v minulosti jižní úsek také podpořen osvětlením sodíkovými reflektory, které jsou umístěny na střeše nejbližší budovy. Jejich provoz v nočních hodinách mi však nebyl potvrzen. Další prvek ochrany tvoří kamerový systém a dohled strážní služby. Jiné technické prostředky nejsou v areálu nasazeny. Umístění závor a světlometů zachycuje příloha č. 2.

Důležité informace jako výrobní postupy nebo faktury jsou spolu s dalšími citlivými údaji uchovávány v kancelářích na druhém podlaží administrativní budovy. Plášť této budovy tvoří další důležitý perimetr, který by musel být překonán při snaze se fyzicky dostat k informačním zdrojům podniku. Do budovy lze vstoupit pěti vchody. Na západní straně je hlavní vchod, který je odemčen od 6 do 18 hodin. Na téže straně budovy se nachází i vstup pro pracovníky, který je trvale odemčen. V severní a jižní části jsou s administrativní budovou propojeny výrobní prostory. Tyto vstupy jsou trvale přístupné. Na východní straně lze opustit budovu trvale odemčenými dveřmi směrem na dvůr. U žádného z vchodů není zřízena kontrola vstupu nebo kamerový dohled. Vstup na druhé podlaží je chráněn dvoukřídlými, částečně prosklenými dveřmi. Jde o jediný přístup na druhé podlaží. Strážní služba kontroluje uzamčení těchto dveří od cca 17 h až do ranního příchodu zaměstnanců. Každý zaměstnanec administrativy vlastní klíč od těchto dveří a je srozuměn s povinností při odchodu zamykat. Přístupový systém nebo jiná forma evidence není zavedena.

Vybraná okna v prvním podlaží jsou osazena vnější mříží, nicméně zbývající okna nejsou mříží či jinak ošetřena (např. detektory rozbití skla). Jsou tedy selektivně chráněny určité prostory, ale vstupu do budovy touto cestou přímo zabráněno není. Jídelna na prvním podlaží je zaměstnancům k dispozici i mimo pracovní dobu a je dozorována kamerovým systémem v režimu bez záznamu. Ostatní místnosti se na noc zamykají.

Odpovědnost za uzavření oken a uzamčení dveří není předpisem stanovena, zaměstnanci byli o své povinnosti pouze informováni. Případná pochybení by měla při své činnosti

[43] HALOUZKA, Kamil. Fyzická bezpečnost: Perimetrické zabezpečovací systémy [online].

odhalit strážní služba, která provádí obchůzky v intervalu přibližně každé dvě hodiny. Strážní služba při své kontrole prochází na trase místy, kde je umístěn technický prostředek pro autentizaci. Díky tomu, lze zjistit, zda strážný kontrolu provedl a v jakém čase se v konkrétních místech pohyboval. Tím je zvýšena spolehlivost těchto služeb.

Ochrana před požárem není zajištěna detektory žádného druhu. Detektory pohybu, otevření dveří či oken a jiné nejsou nikde v budově instalovány.

2.2.3 Kamerový systém

Aktuálně je v areálu závodu provozováno 11 kamer, z nichž 9 pracuje v režimu se záznamem. Jedná se o kamery značek AirLive, VIVOTEK a TP-Link. O záznam by se měla postarat nedávno zakoupená dohledová stanice značky Synology, která prozatím funguje pouze ve zkušebním provozu pro 2 kamery. Na schématu rozmístění jednotlivých kamer vidíme, že pouze jeden strategicky významný objekt je pod kamerovým dohledem.

Kamery jsou umístěny převážně u vstupů. Z těch ostatních jsou 3 kamery uvnitř budov a ze zbylých tří venkovních, jedna snímá dění u zařízení na vážení vozidel, zbylé dvě pak zabírají příjezdové cesty a okolí. Rozmístění a směřování kamer lze vidět na plánu. Kamery jsou připojeny k nejbližším datovým rozvaděčům a obraz je dále přenášen po společné firemní datové síti (neoddělený provoz) do prostor vrátnice, kde je ukládán na disk záznamového zařízení. Výjimku tvoří některé analogové kamery svedené nejprve do A/D převodníku umístěného na vrátnici a kamera č. 9, jejíž signál je nejprve přenesen bezdrátově do budovy administrace. V cestě přímé viditelnosti bezdrátové trasy bude pravděpodobně v blízké budoucnosti překážet konstrukce postavená na pozemku cizího subjektu. Kabeláž ke kamerám č. 4 a č. 5 je vedena po energo-mostu, který bude v nejbližší době demontován.

Směrová kamera č. 1 je určena pro kontrolu provozu na váhovém zařízení. Snímá zde přibližně z výšky 1,5 m nad zemí registrační značku vážených vozidel. Kamera č. 2 (v otočném provedení) snímá podstatnou část západní strany areálu z výšky přibližně

10 m nad zemí, kde je umístěna na sloupu osvětlení. Slouží k dohledu nad chráněným prostorem z důvodu ochrany majetku a odhalování nepovolaných osob. Třetí kamera dohlíží na provoz vozidel a osob u brány a). Tato směrová kamera je připevněna v rohu na plášti objektu vrátnice ve výšce cca 3 m. Z této pozice snímá prostory až za hranou pozemku, čemuž bude v návrhu změn věnována pozornost. Směrová kamera č. 4 a otočná kamera č. 5 jsou zavěšeny na konstrukci energo-mostu přibližně 6m nad zemí, kde dozorují provoz u brány b). Kamera č. 5 dále slouží k plnění stejných úkolů jako kamera č. 2. Výhled kamer zasahuje za hranice areálu. Otočná kamera č. 6 je umístěna na konstrukci druhého energo-mostu (který bude do budoucna zachován). Plní zde stejné úkoly jako kamera č. 5. Sedmá z kamer visí na zdi pronajímané budovy, kde z výšky asi tří a půl metrů zabírá dění u brány d). Důvodem umístění je sledování provozu a pohybu osob, které překračují hranici areálu. Problémem této kamery, a stejně kamery č. 6 je, že rozvaděč a zdroj energie, na které jsou připojeny, je uvnitř pronajímané budovy. Kamera č. 8 snímá prostory jídelny. Tato kamera je upevněna na zdi ve výšce cca 2,5 m. Kamera č. 9 je umístěna na kovovém sloupku ve výšce přibližně 4,5 m, odkud snímá turniket a slouží ke kontrole pohybu osob. Její záběr však zasahuje za hranici areálu. Nejmodernější z kamer je otočná kamera č. 10. Ta dohlíží na tavnou pec z výšky cca 8 m, kde je upevněna na kovových vaznících pod střechou výrobní budovy. Prostor je monitorován z důvodu kontroly dodržování bezpečnostních pravidel a především stavu tavící pece. Jedenáctá kamera v minulosti snímala prostor u docházkového systému, ale v současnosti není aktivní. Je umístěna přibližně ve výšce 2,5 m. Celou popsanou situaci shrnuje tabulka č. 2.

Tabulka 2: Vlastnosti a účel jednotlivých kamer (Zdroj: vlastní tvorba)

Číslo kamery	Kamera je otočná	Výška nad zemí (odhad)	Výhled ven z areálu	Účel
1	NE	1,5	NE	kontrola provozu na váze
2	ANO	10	sporné	pohyb osob, ochrana majetku
3	NE	3	ANO	kontrola vstupu
4	NE	6	ANO	kontrola vstupu
5	ANO	6	ANO	pohyb osob, ochrana majetku
6	ANO	6	ANO	pohyb osob, ochrana majetku

7	NE	3,5	NE	kontrola vstupu
8	NE	2,5	NE	kontrola mimo pracovní dobu
9	NE	4,5	ANO	kontrola vstupu
10	ANO	8	NE	bezpečnost osob a zařízení
11	NE	2,5	NE	kontrola dodržování předpisů

Systém je provozován na fyzicky neoddělené datové síti, tedy společně s ostatními aplikacemi. V současnosti není oddělen ani v logické rovině např. pomocí VLAN. Záznam je uchováván na zařízeních externí vrátní služby. Jednotliví vrátní mají přístup k záznamům v plném rozsahu a z důvodu topologie i přístup do podnikové sítě. Systém není registrován u ÚOOÚ.

2.2.4 Fyzické kontroly vstupu

O kontrolu vstupu se v současnosti starají pracovníci externí vrátní a strážní služby. Stanoviště vrátnice číslo jedna je umístěno u brány a). Druhá vrátnice je umístěna u brány b). Skrze turniket povolané osoby prochází samostatně po autentizaci ID kartou.

U turniketu c) a brány a) jsou umístěna čtecí zařízení čipových karet, která jsou součástí docházkového systému. Informace o přístupech jsou trvale uchovávány. Databáze osob přítomných v areálu by zároveň měla v nouzové situaci sloužit integrovanému záchrannému systému k zjištění počtu osob. Použité řešení je možno rozšířit dle potřeby.

Citlivá data jsou mimo jiné uložena v místnosti se servery, kde je umístěn i trezor finančního oddělení. Do těchto prostor má přístup personalistka, zaměstnanci účetního oddělení a samozřejmě zaměstnanci IT. Přístup není evidován.

Evidenci návštěv má na starosti vrátní služba. Každý návštěvník obdrží visačku s nápisem návštěva, spolu s předtištěným potvrzením o návštěvě konkrétního pracovníka, jenž slouží jako propustka z areálu. Toto potvrzení musí být podepsáno příslušným pracovníkem. Elektronická kniha evidence návštěv je uložena na disku počítače na vrátnici u brány a), kde je umožněno do ní v případě potřeby nahlédnout. Za její provoz a správu osobních údajů odpovídá externí firma poskytující službu ostrahy.

Zaměstnanci nenosí žádné viditelné identifikátory. Zaměstnanec není schopen na první pohled rozlišit neoprávněnou osobu v areálu, jestliže nezná osobně všechny ostatní zaměstnance společnosti. Každý zaměstnanec má služební průkaz s čárovým kódem, který bez dalšího dokladu nelze použít k identifikaci, neboť jeho součástí není fotografie. Čárový kód byl přibližně před deseti lety využíván docházkovým systémem, v současnosti není nijak využit. Tyto průkazy jsou nadále pro nové zaměstnance generovány podnikovým IS.

Do zabezpečených oblastí přistupují oprávnění zaměstnanci pomocí svěřených klíčů. Je zřízen seznam přidělených klíčů. Přístupová práva jsou přidělována dle potřeb organizace v souladu s platnými normami (např. pouze osoby s určitou kvalifikací či certifikátem mají přístup do rozvodny). Ve spolupráci s personálním oddělením jsou novým zaměstnancům administrativy přidělována přístupová práva k informačním zdrojům. Vzhledem k nižšímu počtu zaměstnanců administrativy a malé fluktuaci je udržován spíše subjektivní přehled o propuštěných zaměstnancích, kdy jsou jim následně zrušena přístupová práva. Formální pravidla ohlášení ze strany personálního oddělení nejsou směrnicí stanovena.

2.2.5 Zabezpečení kanceláří, místností a vybavení

Kanceláře musí být mimo pracovní dobu uzamčeny a v pracovní době, při nepřítomnosti vlastníka kanceláře zajištěny. Jestliže pracuje v kanceláři více osob, zamyká vždy poslední z nich. Tyto povinnosti nejsou formalizovány, v rámci podniku se však důsledně dodržují jako určitá zásada. Od jednotlivých kanceláří vlastní klíče daní zaměstnanci. Mimo ně se do všech kanceláří dostane strážní a úklidová služba a to i bez doprovodu.

2.2.6 Ochrana před vnějšími hrozbami a hrozbami prostředí

Dle údajů ČAP (České asociace pojišťoven) se areál podniku nachází v zóně 1 povodňového nebezpečí, tedy zóně se zanedbatelným nebezpečím výskytu povodně či záplavy.[44]

Problémem však mohou být přívalové deště. V minulosti už došlo k zaplavení areálu vodou přitékající z okolních polí. Větrný atlas České republiky neposkytuje dostatečné rozlišení pro kontrolu stavu rizika přímo na adrese areálu. Ovšem obecně tato oblast patří mezi ty s nejnižšími průměrnými hodnotami rychlosti a nárazů větru.[45] [46]

Index kriminality (jen pro tyto trestné činy: krádeže, vloupání a fyzické útoky) ve sledované oblasti dosahuje nejzávažnějšího z pěti definovaných stupňů (v porovnání s ostatními oblastmi spadajícími pod jednotlivá obvodní oddělení v ČR). V absolutních číslech se jedná o 1 500 až 2 000 zjištěných trestných činů na 10 000 obyvatel za 3 roky. Podnik je proti těmto vlivům pojištěn.[47]

Prevence proti škodám způsobeným přívalovými dešti spočívá v zásobě napytlovaného písku uskladněném v místech, kudy by mohla voda do prostor výroby proniknout. K zastavení výroby dojde při překročení výše vodní hladiny přibližně nad 5 cm. Voda ohrozí mimo jiné pískové výlisky, hydraulické zařízení výrobní linky a elektroniku v jejím dosahu. Historicky nejhorší déšť zaplavil podnik do výšky přibližně 30 cm. Bezpečnost pece je ohrožena kolem stavu hladiny 1m nad zemí.

Ochrana před živly byla konzultována s odborníky. Periodicky jsou prováděny kontroly protipožárních opaření. Požadavky jsou splněny v souladu s normou, za což odpovídá pověřený zaměstnanec.

---

[44] Zpráva o nebezpečí povodně. In: Průvodce pro zjištění nebezpečí výskytu povodně [online]. /anonymizováno/

[45] RNDr. Josef Štekl, CSc., Mgr. David Hanslian a další. Výzkum vhodnosti lokalit v ČR z hlediska zásob větrné energie a zpracování metodiky pro posuzovací a schvalovací řízení při zavádění větrných elektráren. In: Ústav fyziky atmosféry AV ČR [online].

[46] Větrný atlas České republiky. WINDSTORM [online]. /anonymizováno/

[47] MAPAKRIMINALITY.CZ. [online]. /anonymizováno/

2.2.7 Práce v zabezpečených oblastech

Každý externí dodavatel musí při svých implementačních či jiných pracích na informační infrastruktuře společnosti pracovat pod dohledem určeného zaměstnance. Dalšímu dohledu podléhají osoby podle zvláštních právních předpisů. Jedná se např. o práci v režimu některého z paragrafů vyhlášky č. 50/1978 Sb., které určují rozsah kompetencí jednotlivých osob.

Zdvojený dohled v oblastech, kde dochází ke zpracování informací či jiné formy kontroly nejsou formálně stanoveny.

V areálu se vyskytují nevyužívané oblasti. Přístupu do těchto prostor je důsledně zabráněno. U nevyužívaných hal jde například o spojení křídel přístupových dveří svárem. V tomto případě se jedná o bezpečnost a zdraví osob.

2.2.8 Oblasti pro nakládku a vykládku

Expedice zboží probíhá buďto z prostor skladu, který je oddělený od ostatních budov nebo z expediční rampy v budově expedice. Z expediční budovy lze projít do budovy administrace.

Přejímku zboží provádí několik zaměstnanců v závislosti na obsahu dodávky. Při příjezdu dodavatele strážní služba informuje konkrétního odpovědného zaměstnance, který zajistí vážení vozidla a určí místo vykládky. Substance potřebné pro výrobu jsou kontrolovány laboratorně, některé pouze vizuálně. Nebyl zaznamenán případ, kdy by dodávka obsahovala jiné než objednané substance, případně, že by byla jinak sabotována.

2.2.9 Umístění zařízení a jeho ochrana

V administrativní budově platí zákaz kouření. Ke konzumaci jídla a pití je vyhrazena jídelna nebo odpočívárny na halách. V administrativní budově nejsou místa k těmto účelům striktně vyhrazena.

Ochrana budov před bleskem je dle tvrzení podle současných norem.

Přepěťová ochrana je používána v několika stupních. V každé místnosti administrativní budovy se nachází zásuvky opatřené zelenou LED diodou. Zmíněné zásuvky mají zajištěnu zvýšenou ochranu. Další ochrany se nachází v jednotlivých rozvaděčích a další pak v každé z rozvoden.

2.2.10 Podpůrné služby

Elektrická energie je k peci dodávána redundantně z obou rozvoden a při výpadku jedné z nich automatický přepínač okamžitě vybaví záložní přívod.

Serverová místnost je napájena pouze z jedné rozvodny. Dočasný provoz a omezení ztráty dat v důsledku výpadku napájení zajišťuje systém UPS, v kombinaci s řídicím systémem, který při poklesu kapacity jednotlivých baterií pod nastavenou úroveň bezpečným způsobem ukončí provoz daných zařízení. Systém UPS není instalován v datových rozvaděčích, tudíž při výpadku el. energie není datová síť k dispozici. Kamerový systém je částečně jištěn. Kamery napájené koaxiálním kabelem jsou napájeny z vrátní budky i po výpadku el. energie. Jedná se o kamery č. 2, 3, 4 a 5, tedy kamery u obou vrátnic a otočná kamera u váhy. Ostatní kamery nejsou proti výpadku jištěny. Samotné napájení stanovišť strážní služby není zálohované a ani datové připojení nemá redundantní charakter.

Plánované testování funkčnosti záložního systému UPS není prováděno s odvoláním na řídicí systém, který kontroluje životnost baterií a v případě problémů je nastaven tak,

aby správce informoval o rizicích prostřednictvím e-mailu a v akutních případech pomocí SMS zprávy.

V areálu jsou nainstalovány fluorescenční štítky, které označují nouzové východy z budov. Nouzové osvětlení pravděpodobně není instalováno.

Datové připojení podniku zajišťuje jeden ISP pro „data i hlas“. Výpadek připojení k internetu kratší než 24 hodin neohrozí chod podniku. Připojení k internetu nemá přímý vliv na výrobu, je využíváno k zajišťování procesů souvisejících s plánováním zakázek a prodejů.

2.2.11 Bezpečnost kabelových rozvodů

Vedení ke kamerám je uloženo v korugovaných chráničkách. Vedení ke kamerám č. 1 a č. 2 je uloženo v zemi, ostatní kamerové rozvody jsou umístěny na energo-mostech, s výjimkou kamery č. 9, která je s budovou administrativy spojena bezdrátově.

Tabulka 3: Uložení kabelových rozvodů u jednotlivých kamer (Zdroj: vlastní tvorba)

Číslo kamery	Spojena s rozvaděčem	Typ spoje	Uložení spoje
1	administrativa	kabel	do země
2	administrativa	kabel	do země
3	expedice	kabel	vnitřní stěna vrátnice
4	expedice	kabel	na energo-most
5	expedice	kabel	na energo-most
6	pronajatá budova	kabel	na energo-most
7	pronajatá budova	kabel	vnitřní strana zdi
8	administrativa	kabel	podhledy
9	administrativa	Wi-Fi	prostor
10	hala	kabel	na nosné konstrukci
11	administrativa	kabel	podhledy

Ve výrobní hale jsou dle norem osazeny soudobé datové rozvody a průmyslové síťové prvky. Pronajatá budova, v níž se nachází datový rozvaděč, byla propojena s rozvaděčem v administrativní budově, ještě před zahájením inovace rozvodů ve výrobní hale. Tato trasa je realizována optickými vlákny, která jsou vedena po střechách a energo-mostech.

V pronajaté budově je umístěn rozvaděč elektrické energie, z něhož je napájeno několik kamer. Přístup k němu není zabezpečen a dveře rozvaděče jsou trvale otevřeny. Jistič je označen jako „kamery“ a může tak být snadno cíleně vyřazen. Nevyhovující stav zachycuje následující fotografie.

Obrázek 9: Rozvodná skříň s jističem označeným jako „kamery“ (Zdroj: autorská fotografie)

Budova administrativy (s výjimkou některých rekonstruovaných kanceláří) je spolu s budovou expedice osazena původními datovými rozvody instalovanými před inovací výrobní haly. Trasa mezi administrativou a expedicí je vedena ve sklepních prostorech. Vedení mezi vrátnicemi je uloženo na energo-mostech. Internetové připojení je z bodu bezdrátového spoje na střeše administrativní budovy svedeno optickými kabely do rozvaděče v serverovně.

V areálu jsou přístupné nezaslepené porty datových zásuvek RJ-45, nicméně porty jsou deaktivovány na síťových prvcích. Nejsou instalovány blokátory konektorů směrem ven ani systém klíčování. V minulosti došlo k případům, že zaměstnanec odpojil datový

kabel z počítače a připojil ho na switch přinesený z domu, čímž si rozšířil počet portů. Větší hrozbou je stav, kdy zaměstnanec tímto způsobem připojí do sítě router s aktivovaným DHCP serverem. Obecně takto umístěný router představuje problém, neboť např. pomocí technologie NAT se za něj může skrýt velké množství koncových zařízení, o kterých správce ztratí přehled. V inovované části sítě je tyto neoprávněné zásahy poměrně snadné detekovat díky pokročilé logice průmyslových síťových prvků. V původní komerční síťové infrastruktuře je možno odhadnout přibližné místo problému, ale ve většině případů je nutno fyzicky projít celý postižený segment.

2.2.12 Údržba zařízení

Za údržbu zařízení odpovídají pověření pracovníci. Zařízení jsou servisována v souladu s požadavky. Jednotný formulář pro hlášení oprav není zřízen.

2.2.13 Přemístění aktiv

Zaměstnancům je dovoleno nakládat s firemními notebooky a dokumenty pro práci z domu. Nejsou definovány politiky pro tyto činnosti. Tímto způsobem pracují hlavně obchodníci. Osoby takto pracující jsou poučeny o tom, že data nesmějí ukládat mimo firemní zařízení. To mimo jiné znamená, že nemohou pracovat na soukromých počítačích, s výjimkou webového rozhraní e-mailu, kde mohou e-maily prohlížet a odpovídat na ně. Stahování e-mailů či příloh je zakázáno (uživatelé jsou poučeni, ale tato povinnost není nikde formalizována). Na noteboocích je spuštěn antivirový program společnosti Eset. V minulosti byly zaznamenány bezpečnostní incidenty na těchto zařízeních. V současnosti není prováděno školení zaměstnanců pro zvýšení jejich bezpečnostního povědomí. Podnik je certifikován dle ISO 9001, ale IT procesy byly vyčleněny a certifikací tedy neprošly, což vytváří horší pozici pro prosazování důležitých procesů jako právě zmíněné školení uživatelů.

2.2.14 Bezpečnost zařízení a aktiv mimo prostory organizace

K zápůjčkám nebo pronajímání zařízení pracujícím s informacemi nedochází. Evidence pohybu přenosných zařízení není vedena. U zaměstnanců s přidělenými přenosnými zařízeními je dopředu počítáno, že s nimi budou mimo firmu pracovat v libovolných časech. Výpůjčky dokumentů nejsou evidovány. Zabezpečení firemních přenosných zařízení, jako je šifrování úložišť apod., není směrnicí definováno.

2.2.15 Bezpečná likvidace nebo opakované použití zařízení

Zařízení pro zpracování informací jsou ve firmě používána do konce jejich životnosti či morálního zastarání. Z toho důvodu není nic odprodáváno jiným subjektům. Disková zařízení jsou po vyřazení z provozu demontována a fyzicky nenávratně poškozena pracovníkem podniku. V praxi to znamená vyjmutí datových ploten z disku a jejich destrukci pomocí úderových nástrojů. Takto „upravený“ disk je následně předán společnosti pro ekologickou likvidaci. Papírové dokumenty jsou skartovány jednotlivými pracovníky. Personální a mzdový systém, včetně serveru, spravuje externí dodavatel. Systémy spravované interně šifrování nevyužívají.

2.2.16 Uživatelská zařízení bez přítomnosti obsluhy

Zařízení bez obsluhy jsou v kancelářích chráněna pouze zamezením fyzického přístupu. Zaměstnanci jsou poučeni o rizicích, avšak k dodržování pravidel nejsou formálně zavázáni.

2.2.17 Zásada prázdného stolu a prázdné obrazovky monitoru

Zaměstnanci jsou poučeni o zásadě čistého stolu, nicméně někteří toto pravidlo ignorují, a protože nejsou pravidla stanovena ve směrnici, jsou obtížně vymahatelná. Někteří ze zaměstnanců mají možnost ukládat dokumenty do zamykatelných skříní, případně trezorů. Elektronické dokumenty nejsou jednotlivě ani hromadně šifrovány, povinnost není definována. Neoprávněnému užití tiskárny je zabráněno pomocí PIN kódů tak, aby vytištěné dokumenty nemohl odnést někdo, komu nebyly určeny. Funkcionalita je hojně využívána, ale není přímo definováno, jaké dokumenty musí být tištěny v tomto režimu. O zabezpečení tak rozhodují jednotliví zaměstnanci. Některá oddělení mají tiskárnu fyzicky přímo v místnosti. Tyto tiskárny jsou určeny pro tisk citlivých informací, jako jsou např. mzdové lístky. Trezory chrání aktiva proti vniknutí, protipožární vlastnosti použité trezory nesplňují.

3 NÁVRH ZMĚN

3.1 Fyzický bezpečnostní perimetr

Fyzický bezpečnostní perimetr tvoří vždy nejúčinnější opatření pro zamezení vstupu či vjezdu nepovolaných osob. Všechny další prvky jeho obrany či dohledu jsou spíše podpůrného charakteru, a proto by měl být na kvalitu perimetru kladen největší důraz. Z analýzy vyplývá, že tři ze čtyř stran (zjednodušeno jako světové strany) fyzického bezpečnostního perimetru nesplňují požadavky na bezpečnost. V rámci návrhu změn, zvláště u východní strany, je třeba zohlednit změny, které mimo jiné vyplývají z plánovaných úprav dělení pozemku a demontáže části energo-mostů.

3.1.1 Severní část

Severní část splňuje požadavky a není třeba provádět změny. Část oplocení v severní části bude prodloužena směrem k severovýchodnímu rohu. Tuto problematiku řeším v kapitole „východní část“.

3.1.2 Východní část

Na východní straně doporučuji vybudovat zcela nové oplocení stejného typu, jako je užito na straně severní. Oplocení by mělo být zbudováno navázáním na poslední blok v severovýchodní části současně definovaného perimetru a pokračovat v rovině současného plotu na severní hranici až po panelovou cestu, před kterou se stočí směrem přibližně na jih (rovnoběžně s cestou) a utvoří tak novou východní hranici perimetru. Navázání v jihovýchodním rohu je závislé na přesném průběhu výměry pozemků. Pokud je mi známo mohl by být plot zakončen k fasádě pronajaté budovy, případně k bráně spřátelené firmy, což by mělo být nejlepším řešením.

Délka takto definovaného perimetru je přibližně 605 m. Na vybudování je tedy potřeba přibližně 242 3D plotových bloků a 243 plotových sloupků. Pro představu ekonomické náročnosti tohoto opatření uvádím následující. Při instalaci 3D plotových panelů v pozinkované úpravě o výšce 2 430 mm budou náklady pouze za materiál činit přibližně 360 500,- Kč bez DPH. Zároveň je třeba započítat cenu betonové směsi potřebné k ukotvení sloupků, cenu spojovacího materiálu a především cenu instalace.

3.1.3 Jižní část

V jižní části bylo identifikováno několik nedostatků, které by měly být odstraněny. Slabé místo v zabezpečení tvoří energo-most, který vede nad oplocením z prostor mimo areál do areálu. Na most a dolů z něj je možno dostat se nejsnáze pomocí servisních žebříků. Další problematické místo je poškozená a stále otevřená brána d), která spolu s přilehlým, nepoužívaným turniketem umožňuje bezproblémový vstup do areálu.

Doporučuji žebříky z energo-mostů zcela demontovat, není-li to možné, pak alespoň zkrátit jejich délku tak, aby bylo znesnadněno na ně ze země dosáhnout. Není-li energo-most využíván mimo areál, doporučuji část přesahující mimo areál odstranit nebo alespoň rozdělit mezerou minimálně 2,5m, případně přerušit zábranou. Konstrukce mostu uvnitř areálu je zachována mimo jiné kvůli rozvodům datové sítě.

Problematiku brány d) je možno řešit několika způsoby, v závislosti na řešení přístupu do areálu jižní firmy. V ideálním případě by provoz z a do jižní firmy probíhal mimo areál, po cestě vně východního perimetru. V takovém případě by bylo možno bránu úplně zrušit. Toto řešení doporučuji. Fyzicky by takové opatření bylo možné realizovat s nízkými náklady například svařením křídel stávající brány k sobě a natažením ostnatého drátu nad ní. Podobným způsobem by bylo možno ošetřit i nepoužívaný turniket.

Jestliže bude bránu nutno z jakýchkoli důvodů zachovat, pak je třeba uvést ji do provozuschopného stavu s tím, že bude otevírána jen v případě potřeby. Stejné pravidlo platí i pro přilehlý turniket. Toto řešení bude vyžadovat nezanedbatelné fixní

náklady na provoz. Brána by mohla být otevírána čipovou kartou jednotlivých zaměstnanců či vypůjčenými kartami pro vjezd dodavatelů, popřípadě přímo strážní službou dálkově ze stanoviště u brány b). V každém případě nebude možno zrušit vrátnici u brány b), což je v rozporu s plánem.

3.1.4 Západní část

V západní části by mělo být provedeno několik úprav. Jako první je třeba odstranit stromy a křoviny nebo alespoň jejich větve, které zasahují do prostoru cca 1,5 m až 2 m v každém směru okolo plotu. Poškozené betonové bloky musí být nahrazeny tvarovkou případně kovovým dílcem s podobnou odolností a pevností. V místech, kde plot mění směr (u některých rohových sloupků), vznikly vůle umožňující vytáhnutí bloků ve vodorovném směru ven z areálu. Tato místa je třeba ošetřit např. předsazeným sloupkem z vnější strany či ukotvením jednotlivých bloků k sobě navzájem pomocí šroubů a silného ocelového plechu, a následně z vnitřní strany ke stávajícímu sloupku obdobným způsobem. Po dokončení oprav narušených míst je více než vhodné rozvinout po celé délce horní strany překážku proti překonání plotu. Doporučuji dvouřadý žiletkový drát, jelikož kromě své vynikající zastavovací schopnosti působí na osoby rovněž psychologicky a poskytuje tak výhodu oproti ostnatému drátu, který nevyvolává tento odstrašující pocit v takové míře. Při realizaci tohoto opatření je třeba také počítat s náklady na podpůrné konzole drátu.

Jelikož došlo k odprodeji pozemku v těsné blízkosti západní strany (na obrázku vyznačen modře), dojde k značnému ztížení přístupu zaměstnanců, kteří využívají turniket c), neboť je třeba definovat novou hranici perimetru a patřičně ji zabezpečit, což pro zaměstnance znamená prodloužení současné trasy mezi turniketem a pracovištěm. Avšak v případě, že by nebyl definován nový perimetr, vzniklo by slabé místo a všechna ostatní opatření by pozbyla svého účinku. Dále je třeba vzít do úvahy přerušení perimetru mezi budovami skladů a betonovým plotem. Oplocení vedoucí od jižní stěny budovy skladů, kolem váhy do jihovýchodního rohu odprodaného pozemku a následně probíhající podél jižní hranice odprodaného pozemku směrem

k turniketu c), by dosáhlo délky přibližně 365 m. Takto by byl zcela korektně vytyčen nový perimetr. Jelikož je oblast relativně přehledná, bylo by, dle mého názoru možné, místo průmyslového oplocení, nainstalovat z důvodu úspory nákladů pletivo s tříbodovým uchycením, jak je tomu na jižní straně. Tomuto řešení by však muselo předcházet odstranění křovin a stromů mezi severní částí prodaného pozemku a budovami skladů.

Volba finálního řešení je v tomto případě spíše otázkou strategického rozhodnutí. Nabízí se následující možnosti:

1. Redefinování perimetru a průmyslové oplocení
2. Oddělení prodaného pozemku pletivem
3. Dohoda o spoluúčasti na zabezpečení a smluvní zajištění zákazu pohybu v areálu

První varianta, tedy redefinování perimetru, by vyžadovala přibližně 280 m průmyslového oplocení, nový turniket (případně demontáž turniketu od brány d) a jeho přesazení), a pakliže by nový vlastník pozemku vyžadoval přístup vozidly, pak také bránu pro vjezd vozidel (v plánu označena písmenem n) v zelené šipce). Výhodou je, že problém necelistvosti původního perimetru by byl přesunut na majitele odprodaného pozemku. Zároveň ochrana jihozápadní části žiletkovým drátem by mohla být ukončena přibližně o 90 m jižněji (u nového turniketu), neboť pozemek severně za touto hranicí by se již nacházel za novým perimetrem. Část pozemku (cestu k turniketu c)) by sice stále vlastnil podnik, ale jelikož se v dané oblasti nenalézají zcizitelná aktiva, mohlo by být riziko náhodného průniku osob do tohoto meziprostoru akceptováno.

Varianta č. 2 spočívá v oddělení odprodaného pozemku od prostor areálu pletivem. Tímto způsobem by byla vytvořena nová cesta od turniketu c) k budovám podniku. Realizace by vyžadovala cca 365 m pletiva, okolo 147 sloupků a příslušné množství spojovacího a kotvícího materiálu. Nevýhodou je, že pro přístup na odprodaný pozemek by musela být zřízena branka vedle turniketu c) tak, aby se povolané osoby dostaly pouze na prodaný pozemek a zaměstnanci podniku pouze do areálu podniku. Situace by se dala vyřešit i pouhým odstraněním jednoho plotového bloku severně od turniketu c), tedy severně od nově nataženého pletiva a zabezpečení takto vzniklého průchodu na prodaný

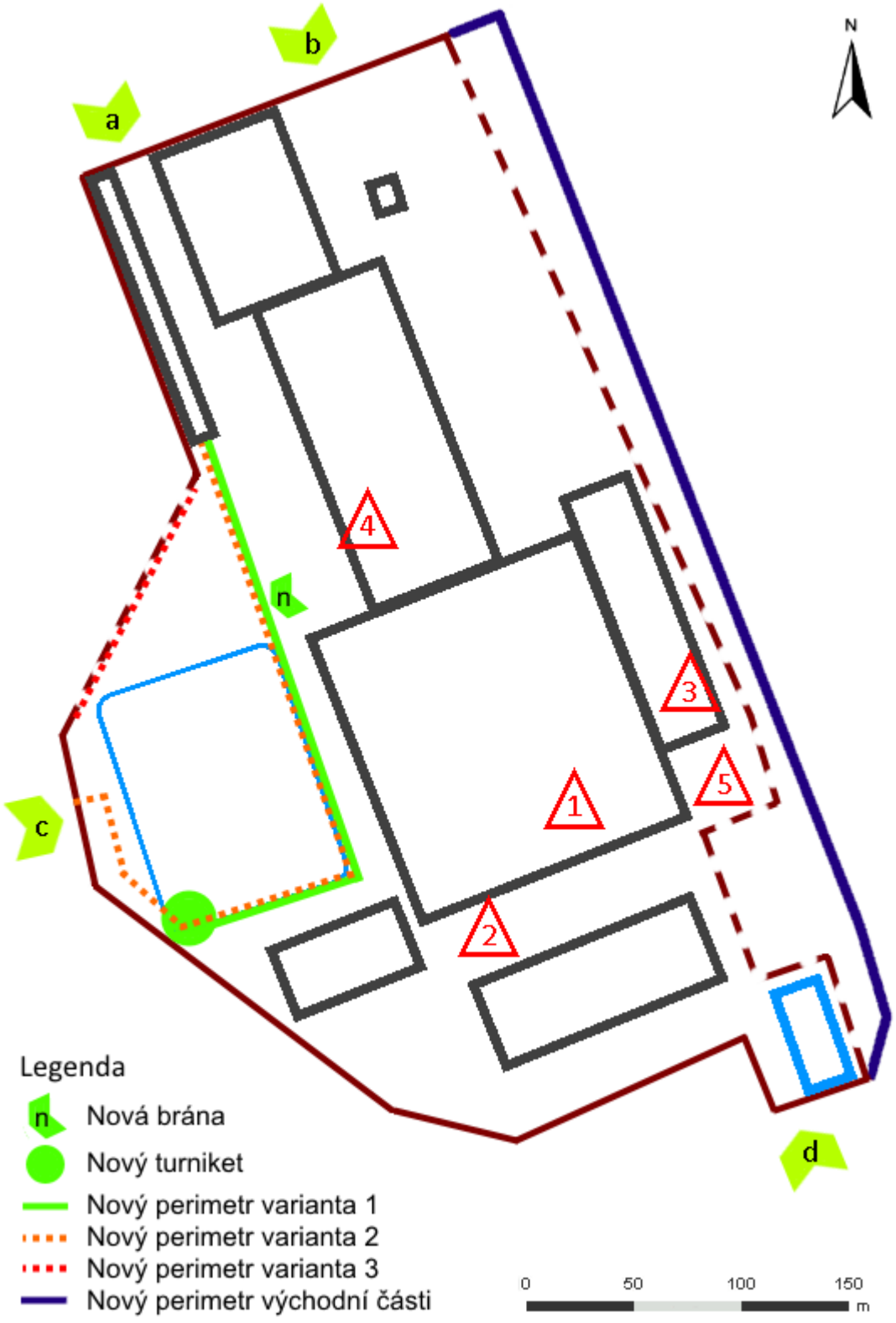
pozemek nechat na jeho vlastnících. Jestliže bude vlastník vyžadovat přístup vozidly, je opět nutné zřídit bránu n). Brána n) by v tomto případě také mohla sloužit jako jediná přístupová cesta a problém s přístupem od turniketu c) by byl v tom případě vyřešen.

Třetí možnost je jakýmsi dočasným a nouzovým řešením. Vzhledem k povaze nového vlastníka je možno očekávat vysokou disciplinovanost a pečlivé dodržování vzájemných dohod. Přijmeme-li tuto premisu, pak je možné uzavřít dohodu, která striktně stanový zákaz pohybu osob mimo jim vyhrazené prostory. Avšak je bezpodmínečně nutné, aby jedna ze stran zbudovala chybějící část oplocení mezi turniketem c) a sklady. Bude-li k této variantě přistoupeno např. z důvodu nedostatku financí, odpovědná osoba musí vzít na vědomí, že se do budoucna vlastník pozemku může změnit a realizace některé z předchozích variant bude nevyhnutelná.

Tabulka 4: Očekávané charakteristiky po provedení změn (Zdroj: vlastní tvorba)

Tabulka rekapitulace	Strana perimetru				
	Severní	Jižní	Východní	Západní (jih)	Západní nový
Viditelnost skrze oplocení	ANO	ANO	ANO	NE	ANO
Plánovány nové vstupy	NE	NE	NE	NE	Dle zvolené varianty
Odolnost proti poškození	Vysoká	Nízká	Vysoká	Velmi vysoká	Dle zvolené varianty
Odhadované riziko průniku	Malé	Střední	Střední	Malé	Dle zvolené varianty
Počet vstupů či vchodů	2	1	0	0	1 až 2

Níže na obrázku č. 10 je k vidění plán s jednotlivými variantami nových hranic.



Obrázek 10: Plán areálu s vyznačenými variantami průběhů jednotlivých hranic. (Zdroj: vlastní tvorba)

* Červené trojúhelníky znázorňují strategické body (viz. kapitola 2.1 Popis areálu podniku).

3.2 Vnitřní pásmo

Ochrana vnitřního pásma je závislá na přijatých opatřeních pro vnější perimetr. Dodatečná ochrana by měla být instalována v místech, kde existuje zvýšené riziko překonání vnější perimetrické ochrany. Například západní část, bude-li chráněna žiletkovým drátem, by měla poskytnout přiměřenou bezpečnost a instalování dodatečných prvků přímo na perimetr by nepřineslo vyšší efektivitu ochrany vzhledem k investovaným prostředkům. To ovšem neznamená, že by v západní části vnitřního pásma neměly být v žádném případě instalovány dodatečné prvky ochrany jako např. kamery, případně čidla apod. Naopak tento přístup je v rámci prevence vhodným doplňkem silného perimetru.

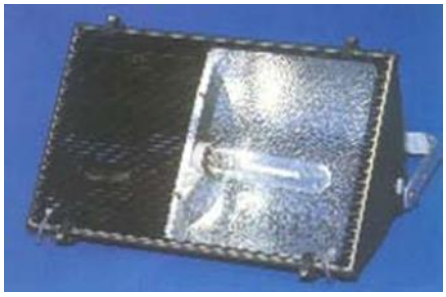
V rámci ochrany vnitřního pásma je účelné vytvořit souvislé, přehledné, kamerovým systémem dozorované plochy, které budou v nočních hodinách osvětleny tak, aby bylo možno kontrolovat pohyb osob alespoň v oblastech se zvýšeným rizikem (například významné objekty 1 až 5). Realizace takového opatření vyžaduje úpravu kamerového systému a jeho doplnění reflektory, případně dalšími dodatečnými prvky. Snaha osvětlit některé prostory areálu (jižní část) byla již v minulosti započata, avšak stav zařízení a jejich energetická efektivita nedosahuje hodnot dnešních prostředků.

3.2.1 Podpůrné prostředky

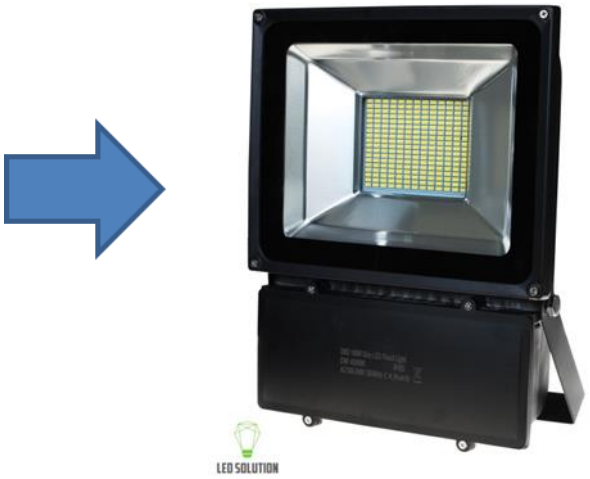
Jižní perimetr by bylo vhodné posílit elektronickými závorami nebo otřesovými detekčními kabely. Montáž by z důvodu spolehlivosti systému měla být provedena odbornou firmou. Jako pasivní prvek doporučuji nainstalovat (obměnit) reflektory, které nasvítí oblast podél perimetru.

3.2.2 Náhrada reflektorů

Měněné nefunkční a nově instalované reflektory by měly být založeny na technologii LED, která nabízí vysokou efektivitu. Starý reflektor o výkonu do 500W může být (dle výrobce) nahrazen reflektorem LED o výkonu 100W při zachování stejné intenzity osvětlení. Životnost LED reflektoru se pohybuje okolo hodnoty 50 000 hodin.[48] [49]



Obrázek 12: Původní reflektor (převzato, Zdroj: Venkovní průmyslové reflektory […][49])



Obrázek 11: Navrhovaná náhrada – LED (převzato, Zdroj: Černý LED reflektor […] [48])

3.2.3 Ochrana budov

V rámci konceptu přiměřené bezpečnosti a vzhledem k současnému stavu budov není možné nasadit plášťovou ochranu budov plošně, a to z důvodu vysoké finanční náročnosti i neúčelnosti takového řešení. Aktiva nacházející se v halách jsou totiž z větší části těžko odcizitelná (pro svou vysokou hmotnost) a jejich poškození také téměř vždy vyžaduje strojní podporu. Výrobní prostory by proto měly být zabezpečeny především z důvodů bezpečnosti osob, zajištění kontinuity výroby a ochrany citlivých strojních zařízení spolu s informacemi o výrobních postupech. Zvláštní pozornost je třeba věnovat ochraně informací v budově administrativy.

[48] Černý LED reflektor 100W SMD: Parametry. LED Solution [online].
[49] Venkovní průmyslové reflektory VM 150 VR, VM 250 VR, VM 400 VR. VYSTO [online].

V administrativní budově jsou kritická aktiva přechovávána v kancelářích na druhém podlaží. K ochraně budovy lze přistoupit dvojím způsobem:

1. Zabezpečení budovy jako celku (1 zóna)
2. Rozčlenění budovy na 2 zóny (podlaží) a zvolit rozdílnou míru zabezpečení

V případě první varianty existuje několik limitujících faktorů jako například větší počet vstupů do budovy či okna v prvním podlaží, což zapříčiní razantní zvýšení nákladů na jednotlivá opatření anebo snížení celkové bezpečnosti. V druhém případě jsou pro druhé podlaží stanovena přísnější bezpečnostní pravidla než pro první. Tento přístup doporučuji, jelikož poskytne potřebnou úroveň bezpečnosti při zachování akceptovatelných nákladů.

3.2.3.1 Varianta 1

Při volbě první varianty by bylo nutné přehodnotit, zda je aktuální počet vstupů do budovy možno snížit nebo jsou všechny využívané a nenahraditelné. Dveře zbylých vstupů by musely být upraveny tak, aby mohly být otevřeny jen oprávněnými osobami. Například montáží mechanického zavírače dveří v kombinaci s elektrickým otevíráním dveří, které by bylo inicializováno pomocí rozšíření používaného docházkového systému a zavedení směrnice, která by stanovila zaměstnancům za povinnost nevpustit do objektu administrativy další osoby. Průchody jednotlivých zaměstnanců by byly zaznamenány na serverech s ostatními daty, která se týkají docházky (v log souborech). Vedení by tak mělo ucelený přehled o pohybu osob v rámci budovy. Musí být dodrženy požadavky požární bezpečnosti v souvislosti s únikovými trasami, vzhledem k počtu osob dle ČSN 73 0818.

Problematické je, že do budovy vstupují mimo jiné řidiči, kteří nemají vlastní přístupovou kartu. Někdo ze zaměstnanců by je tedy musel jednotlivě vpouštět nebo by muselo být na vrátnici zřízeno několik přístupových karet pro návštěvy, které by strážní služba zapůjčovala. Pakliže by byli vpouštěni konkrétním zaměstnancem, bylo by nutné instalovat u dveří kamery a v kanceláři daného zaměstnance zařízení pro otevření jednotlivých dveří a obrazovky s náhledem dění přede dveřmi, v ideálním

případě interkom. V případě přidělování karet by strážní službě přibyla administrativa spojená s evidencí zapůjčovaných karet, a jestliže by měla být vedena v elektronické podobě, centralizovaně na serverech společnosti, muselo by dojít k úpravě systému nebo alespoň nasazení nové aplikace, kde by se zápůjčky evidovaly separátně.

Na prvním podlaží je také nutné zabezpečit okna. Na některá z nich byla již z vnější strany instalovaná mříž, ta zbylá nejsou chráněna. Ochrana oken by byla v rámci této varianty nejnákladnějším opatřením. Veškerá okna na prvním podlaží by měla být osazena mříží, další okna pak opatřena fólií proti průrazu a v místnostech s kritickými aktivy podniku by měly být instalovány detektory uzavření oken, společně s detektorem tříštění skla (druhý zmíněný lze vynechat v případě instalace detektoru pohybu).

3.2.3.2 Varianta 2

Prostory budovy by měly být rozděleny do dvou zón. Každé podlaží tvoří jednu zónu. Prioritou je ochrana majetku a informací na druhém podlaží.

Vstupní dveře na druhé podlaží by bylo vhodné opatřit elektrickým otevíráním kartou docházkového systému anebo alespoň z vnější strany dveří nahradit kliku koulí a nainstalovat zavírač dveří. Pakliže skleněné výplně dveří nemají od výroby ochranu proti průrazu, doporučuji opatřit je bezpečnostní fólií. Tato opatření zajistí, že dveře bude moci otevřít pouze osoba s kartou či klíčem. Protože se jedná o jediný vstup na druhé podlaží, nabízí se možnost preventivní pasivní ochrany – instalace kamery. I kdyby kamera fungovala pouze v omezeném režimu nebo bez záznamu, poskytne strážní službě přehled o situaci a možnost rychleji reagovat.

Detektory pohybu by měly být instalovány alespoň v místnostech s kritickými aktivy. Především místnosti finančního oddělení, serverovny a dalších kanceláří, kde jsou uchovávány dokumenty spojené s výrobou či osobními údaji. V ideálním případě i na přístupových chodbách.

3.2.3.3 Společná doporučení pro obě varianty

Měly by být formalizovány povinnosti zaměstnanců týkající se bezpečnosti, stanoveny odpovědnosti a sankce, například formou směrnice. V rámci fyzického přístupu se jedná o uzavření oken, uzamčení dveří, manipulace s přístupovou kartou, vpouštění osob do budovy/areálu, spouštění a deaktivace poplachových systémů (budou-li instalovány), kontroly dodržování stanovených pravidel a podobně.

V budově by měl být zaveden systém elektrické požární signalizace (EPS). Obsluhu ústředny by měla provádět strážní služba ze svého stanoviště u brány a), kam by měla být ústředna instalována. Tento systém dle vyhlášky č. 246/2001 Sb. vyžaduje pravidelné kontroly.

3.3 Kamerový systém

Kamerový systém je v podniku provozován již delší dobu. Na jeho tvorbě a úpravách se podílelo několik různých správců, což se mimo jiné projevilo nesystematickým umístěním některých kamer, rozvaděčů či kabelových tras, spolu s nesourodostí celého systému.

3.3.1 Obměna systému

V rámci modernizace, ještě před mou účastí v podniku, byla zakoupená stanice Synology Surveillance. Toto zařízení poskytuje možnost připojit dvě kamery bez poplatku, což umožňuje testování. Pro každou další připojenou kameru je třeba zakoupit licenci. Při testování bylo zjištěno, že některé z kamer nejsou stanicí podporovány, byť byly uvedeny na stránkách prodejce jako kompatibilní. Stanice skutečně podporuje všechny 3 použité značky kamer, ale pouze některé modely daných značek. U jedné z podporovaných kamer se vyskytl problém. Stanice dokáže zobrazit živý náhled této kamery, avšak při pokusu o záznam dojde k nespecifikované chybě. Tuto situaci jsem se na místě pokusil vyřešit v kooperaci s panem správcem. Nejprve bylo ověřeno a upraveno nastavení

kamery a stanice Synology. Problémy někdy způsobuje rozdílný čas na zařízeních, což se v tomto případě nestalo, neboť kamera i stanice mají synchronizován čas proti NTP serveru. Příčinou mohou být také nedostatečná přístupová práva k zápisu na disk z internetu.[50] V tomto případě to ovšem není pravděpodobné, protože obraz z ostatních kamer zaznamenat lze. Před prověřováním dalších hypotéz časově velmi náročným systémem pokus/omyl, byl aktualizován firmware na obou zařízeních. Ani tento zásah nepomohl a kameru se nepodařilo pro záznam zprovoznit.

V rámci úpravy systému bude nutné vyřešit především následující úkoly:

1. Sjednotit platformu (kamery od stejného výrobce)
2. Oddělit datový tok z kamer od ostatního trafiku v rámci sítě
   a. Fyzicky – vybudováním nových kabelových tras nebo
   b. Logicky – v rámci stávající sítě
3. Přehodnotit pracovní režimy jednotlivých kamer (se záznamem či bez záznamu)
4. Upravit umístění kamer
   a. Změna snímaného prostoru (legislativní změny, zvýšení přehlednosti)
   b. Změna upevnění kamer (odprodej budov, změna tras konektivity)
5. Zrušit kamery, které nesplňují požadavky (neúčelnost, zastaralost, nekompatibilita)
6. Navrhnout umístění nových kamer
7. Vytvořit dokumentaci ke kamerovému systému a zhodnotit právní hledisko
8. Sjednocení platformy

Výrobci kamer a záznamových zařízení se od sebe navzájem odlišují mírou poskytovaných služeb. Rozdíly často nejsou na první pohled patrné. Může se jednat o různé přístupy k jednotlivým kamerám, doplňkový SW (např. rozeznávání osob) či „low-levelové“ nuance na úrovni síťových protokolů. Z těchto důvodů jsou spolu v lepším případě jednotlivá zařízení kompatibilní pouze částečně (částečně přicházíme o funkcionalitu), v horším případě vůbec (kameru nelze v systému vůbec použít).

[50] NEJČASTĚJŠÍ DOTAZY - FAQ. Apexis.cz [online].

Nasazení prvků od jednoho výrobce značně usnadňuje instalaci, ovšem nejvíce se výhody tohoto řešení projeví při správě systému, který by měl umožnit bezproblémovou obsluhu, rozšiřitelnost a plnou funkcionalitu.

Opět zde existují minimálně dvě možná řešení. Zavést zcela nový systém s využitím minima použitých prvků nebo zachovat stávající systém a postupně ho upravit do požadovaného stavu. Každá z metod sebou nese výhody i úskalí. V prvním případě získáme systém, který bude zcela kompatibilní a od jeho zprovoznění plně využitelný, avšak za cenu vysoké jednorázové investice. V druhém případě můžeme očekávat komplikace při úpravách, ale náklady na změnu mohou být rozloženy do delšího časového období (tím však není vyloučeno, že celkové náklady nebudou ve výsledku vyšší než v případě 1. možnosti).

3.3.2 Oddělení datových toků

V rámci kamerového systému jsou uchovávány osobní údaje. Z toho důvodu je třeba učinit taková opatření, aby byl do této sítě a k samotným datům co nejvíce omezen přístup. Jedním z nástrojů, jak toho docílit, je oddělení provozu od ostatního ve firemní síti. V každém případě musí být úložiště umístěno v rámci serverovny a strážní službě umožněn pouze náhled.

Fyzické oddělení představuje zbudování nového kabelážního systému určeného výhradně pro bezpečnostní přenosy, v našem případě dat z kamerového systému. Vzhledem k rozloze areálu by toto řešení vyžadovalo investici nejen do kabelů, ale také do aktivních prvků, kterých by muselo být odhadem okolo pěti a více kusů. Toto řešení je technicky čisté, jeho nevýhodou jsou značné náklady na realizaci, neboť se prakticky jedná o výstavbu sítě, nehledě na ceny výkopových prací.

V rámci logického řešení oddělení provozu se nabízí technologie VLAN. Prvky související s kamerovým systémem by měly být vyčleněny do vlastní podsítě na úrovni L3 a do vlastní VLAN na úrovni L2. V rámci L1 bude v tomto případě využito existujícího kabelážního systému, resp. bezdrátového přenosu.

3.3.3 Pracovní režimy kamer

Kamery musí mít definován účel nasazení. Především by mělo být jasné, před čím se touto technologií chráníme, co chráníme a kdo je zodpovědný za zásah v případě vzniku incidentu. Na základě toho je třeba učinit rozhodnutí, zda provozovat systém v režimu se záznamem, bez něj či kombinovaně. Záznam může dobře posloužit např. v rámci vnitropodnikového vyšetřování či učení se z chyb, u soudu však do budoucna jako důkaz nemusí obstát.[51]

V systému nedochází ke zpracování citlivých údajů, neboť je získáván pouze prostý kamerový záznam, který je používán a zpracováván obvyklým způsobem. Tzn., že nejsou vyhodnocovány biometrické charakteristiky, identifikace lidských tváří apod. Dochází však ke zpracování osobních údajů. Z toho důvodu je třeba registrovat nový systém pomocí webového formuláře, který je k nalezení pod následujícím odkazem. (www.uoou.cz/oznameni-o-zpracovani-osobnich-udaju.asp). Doporučuji podat současně žádost o vydání osvědčení o zápisu do registru. O režimu kamer musí být subjekty informovány pomocí cedulí ještě před zónou snímání.[52]

3.3.4 Umístění kamer

Kamerový systém je provozován vždy ke konkrétním účelům a chrání definované právní zájmy provozovatele. Na tuto skutečnost je třeba myslet při umisťování jednotlivých kamer. Kamery by měly monitorovat především chráněná aktiva a dále nezasahovat do soukromí nezúčastněných osob. Důležitou součásti je i ochrana samotných kamer. Například jejich vzájemný dohled, umístění mimo dosah, ochranné kryty apod. Umístění kamer musí být mimo jiné v souladu se zákonem č. 101/2000 Sb., o ochraně osobních údajů. Při přemisťování by mělo být pamatováno na zásadu sjednocení platformy a kamery, které nevyhovují nepřemisťovat, ale rovnou nahradit.

[51] Video musíme sami zfalšovat, abychom dokázali podvod, vysvětluje expert. Technet-cz [online].
[52] BURIAN, David, ed. Provozování kamerových systémů: metodika pro splnění základních povinností ukládaných zákonem o ochraně osobních údajů [online].

Kamera č. 1 snímá v nepřítomnosti vozidel na váze i příjezdovou cestu. Jelikož není provozována se záznamem a zabírá pouze oblast areálu, kde strážní službě může sloužit jako podpůrná kamera, nevidím v jejím umístění problém. Kamera je upevněna poměrně nízko nad zemí. Jako prevence jejího poškození slouží mimo jiné kamera č. 2.

Z důvodu dohledu mimo areál je třeba upravit polohu některých kamer. Jedná se o kamery č. 2 až č. 6 a č. 9. Kamera č. 2 má zastíněn výhled směrem na západ sloupkem a elektrorozvaděčem. Pakliže se odstínění na snímku projeví jako nedostatečné, může být doplněno např. upevněním plechu dále do výhledu. Její dohled mimo areál může však spíše hrozit v severní části, kde je ovšem hranice areálu vzdálená cca 200 m. Doporučuji ověřit, zda rozlišení kamery umožňuje dohlédnout za hranici areálu takovým způsobem, aby byli na obrazu rozeznatelné jednotlivé osoby. Pakliže ano, je třeba tento prostor odstínit. Zde je také třeba počítat, že po stržení energo-mostů bude do prostoru za areál viditelnost značně usnadněna.

Kamera č. 3 je upevněna na stěně vrátnice. Snímaný prostor lze omezit sklopením kamery směrem k zemi anebo natočením kamery směrem více do areálu. Další možností je zastínění části obrazu kamery fyzickou či SW cestou. Pakliže ani jedna z možností nepovede k nápravě, bude třeba kameru přemístit. Na tomto místě se však pravděpodobně nelze zcela vyhnout zastínění některých míst jako je např. brána, skrze kterou lze vidět z areálu.

Čtvrtá a pátá kamera musí být nainstalována na vlastní sloupek, neboť energo-most, na kterém jsou umístěny, bude demontován. V té souvislosti bude také třeba zřídit nové přívody. Řešením je uložení do země a připojením do budovy expedice. Zastínění závisí na zvolené výšce umístění. Kamera č. 4 ve výšce cca 3 m by mohla být namířena na bránu se záběrem její spodní třetiny, což zabrání monitorování osob mimo areál. Kamera č. 5 je otočná a měla by dohlížet na pohyb v severovýchodní části areálu. Umístění kamery by z toho důvodu mělo být co nejvýše, třeba i na témže sloupku s kamerou č. 4. V této pozici však musí být kamera ze severní části zastíněna a kompromisně upraven úhel snímání na přibližně 80°. Přemístění kamery přibližně 50 m východním směrem by umožňovalo pohled ze severního rohu hlouběji do areálu s úhlem snímání cca 90°. Severní a východní část mimo areál, by musela být zastíněna. Pro detailnější kontrolu nad oblastí se zdá nejvýhodnější přemístit kameru č. 5 na úroveň středu mezi severní stěnou

haly a bránou b), tedy zhruba úroveň kamery č. 8, přičemž v západovýchodním směru co nejblíže východní hranici a ve výšce alespoň 4 m. V tom případě by stačilo zastínit pohled za východní hranici a vznikla by kontrolovaná oblast s úhlem pohledu 180°. Poslední dva zmíněné návrhy však vyžadují zbudování nových přívodů v délce nad 50 m.

Otočnou kameru č. 6 by dle mého názoru bylo vhodné přemístit směrem na sever do prostoru mezi budovami. Kamera by tak ztratila výhled do cizího areálu a navíc by byl zajištěn dohled nad chladícím ostrůvkem a čerpací stanicí, přičemž by bylo možno monitorovat i cestu k bráně d), kterou kamera snímá nyní. Řešení vyžaduje instalaci L konzoly ke spodní hraně energo-mostu a prodloužení přívodů. Vzhledem k budování nového rozvaděče u pronajaté budovy by neměl být problém rozvod upravit.

U kamery č. 9 je problém dohledu mimo areál nejpalčivější. Navíc přemístění kamery brání fakt, že blízký pozemek je pronajímán. Ke kameře není zřízeno datové vedení a bezdrátový spoj z důvodu výstavby pravděpodobně není schopen do budoucna plnit svoji funkci. Nejvýhodnější by zde bylo monitorovat prostor z opačné strany přístupové cesty, tedy ze severu na jih, kdy by v levé části záběru byla nevyužívaná vrátnice, na středu přístupová cesta a turniket c) pak v pravé části. Při dostatečné výši sloupku (cca 4 m) a patřičném sklonu kamery, by bylo možno monitorovat procházející osoby, avšak za oplocení areálu by již kamera nedohlédla. Toto řešení by vyžadovalo přemístění stávajícího nebo montáž nového sloupku spolu s přivedením rozvodů. Opět závisí na rozhodnutí v oblasti změn perimetru.

V průběhu psaní této práce byla pronajímaná budova odprodána. Kamera č. 7 se tedy již nachází na fasádě cizí budovy. Protože účelnost monitorování těchto prostor také závisí na zvolené variantě řešení přístupu do jižní firmy, měla by kamera být prozatímně demontována, dokud nebude o tomto rozhodnuto. V případě, že průchod zůstane aktivní, doporučuji přemístit kameru na podpěrný sloupek plynového vedení do výšky alespoň 3 m, zaměřenou na spodní třetinu brány d). V opačném případě by mohla být využita na kontrolu cesty u jižního perimetru.

Osmá kamera by měla nadále působit v režimu bez záznamu nebo být demontována.

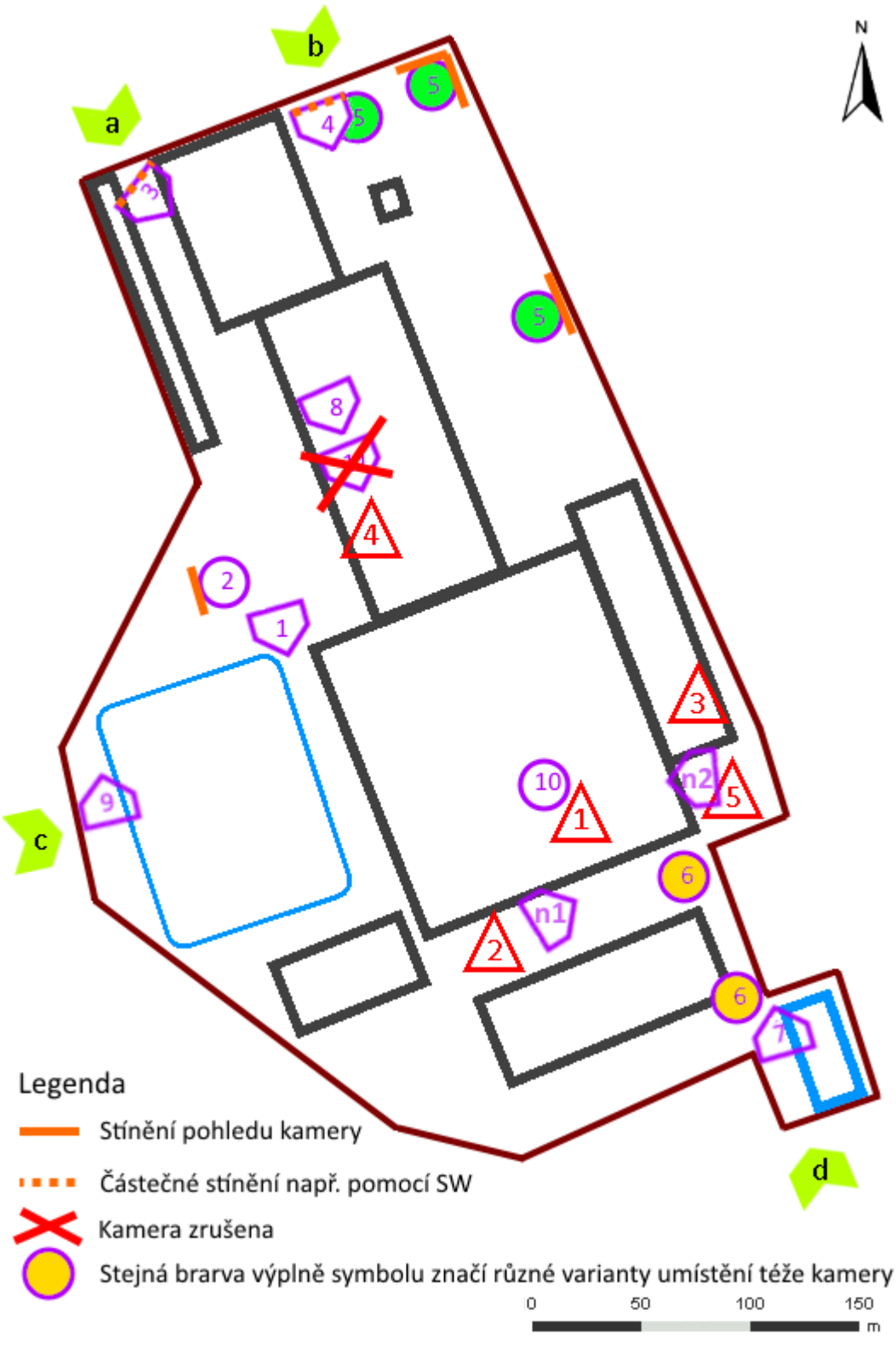
Kamera č. 10 dohlíží především na bezpečnost pece, na kterou by měla být zaměřena vždy, pokud není zkoumána jiná riziková situace na hale.

3.3.5 Rušené kamery

Kamera č. 11 snímající docházkový systém, již neplní svůj původní účel a měla by být demontována. S ohledem na výše popsanou situaci potenciálně také kamera č. 7.

3.3.6 Návrh na nové kamery

Nejméně jištěná část je jihozápadní roh areálu. Zřejmě vzhledem k tomu, že se v dané oblasti nenachází cenná aktiva. Nasazení kamerového systému s křížovým hlídáním a pokrytím významné části celého objektu zde není možné z důvodu obrovské plochy areálu a s tím související neúměrné náklady, které by bylo třeba vynaložit na vybudování datové a energetické infrastruktury ke kamerovým základnám. Systém by měl především dohlížet na kritická místa. Ostatní prostory pak průběžně kontroluje strážní služba během pravidelných obchůzek. S ohledem na to navrhuji dozorovat kamerovým systémem strategický bod číslo 2, a pakliže nebude přesunuta kamera č. 6, tak i strategický bod č. 5. Připojení kamer je zde možné do rozvaděčů v hale. Kamera snímající bod 2 může být umístěna na jižní stěně haly. Kamera snímající bod 5 pak na straně východní. Při použití směrových kamer nehrozí snímání vnějších prostor. Kamery jsou v plánu přemístění (obrázek 14) značeny jako n1 (nová u chladícího ostrůvku) a n2 (nová u čerpací stanice).



Obrázek 13: Návrh přemístění kamer (Zdroj: vlastní tvorba)

* Červené trojúhelníky znázorňují strategické body (viz. kapitola 2.1 Popis areálu podniku).
* Směr pohledu kamer viz. legenda přílohy č. 3

3.3.7 Dokumentace a právní hledisko

Ke kamerovému systému musí být k dispozici dvojí dokumentace – návrhová a provozní. V rámci návrhové dokumentace by měla být k dispozici analýza variant ochrany, projektová dokumentace s analýzou rizik, dokumentace organizačních opatření a smluvní dokumentace. V rámci provozní dokumentace jsou velmi důležité informační cedule u sledovaných prostor. Dále pak na vyžádání podrobnější informace o provozovateli a dokumentace o přístupech a práci se získanými záznamy.[53]

Vzhledem k tomu, že projektová dokumentace ke kamerovému systému by rozsahem stačila na samostatnou práci a s přihlédnutím k faktu, že definitivní polohy jednotlivých kamer závisí na řadě rozhodnutí vedení podniku, rozhodl jsem se uvést pouze takové informace, které mohou napomoci změně systému k lepšímu, provozuschopnějšímu stavu tak, aby byla posílena fyzická bezpečnost podniku. Tato práce tedy může při tvorbě dokumentace částečně posloužit.

Z právního hlediska je nejprve potřeba rozhodnout zda mohou být zaměstnanci skrytě či otevřeně monitorováni v souladu s §316 odst. 2 zákoníku práce. Jedná se o kogentní úpravu. Nejsou-li tedy jeho podmínky naplněny, nelze zaměstnance monitorovat, byť by k tomu dali souhlas.[54]

„Zaměstnavatel nesmí bez závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele narušovat soukromí zaměstnance na pracovištích a ve společných prostorách zaměstnavatele tím, že podrobuje zaměstnance otevřenému nebo skrytému sledování, odposlechu a záznamu jeho telefonických hovorů, kontrole elektronické pošty nebo kontrole listovních zásilek adresovaných zaměstnanci.“[55]

Mezi prostory, které odpovídají této definici, a které jsou pod dohledem kamer se záznamem, patří pouze hala. Venkovní prostory by bylo možno považovat za pracoviště strážní služby, což je externí subjekt, kterým se budu věnovat níže.

[53] BURIAN, David, ed. Provozování kamerových systémů: metodika pro splnění základních povinností ukládaných zákonem o ochraně osobních údajů [online].
[54] KUČEROVÁ, Alena a František NONNEMANN. Ochrana osobních údajů v praktických příkladech.
[55] Zákon č. 262/2006 Sb. Zákoník práce [online].

Domnívám se, že dohled nad stavem tavící pece je závažným důvodem opravňujícím sledování, nicméně doporučuji toto konzultovat s právníkem.

Předpokládejme, že se jedná o oprávněný důvod. V takovém případě musíme zaměstnance o provozu kamery informovat dle §316 odst. 3 zákoníku práce.[56]

Na ostatní osoby, které nemají k provozovateli zaměstnanecký poměr, se uplatňuje zákon ochraně osobních údajů. Z toho důvodu musí správce najít některý právní titul uvedený v §5 odst. 2 zákona o ochraně osobních údajů, na jehož základě lze osobní údaje zpracovávat. Nabízí se §5 odst. 2 písm. e), na jehož základě lze zpracovávat záznamy i bez souhlasu snímaných osob, avšak musí být posouzeno, zda je nutné monitorovat prostory, kudy musí dodavatelé procházet např. do kancelářských prostor.[57] [58]

Kamerový systém podléhá registraci (dle §16 zákona o ochraně osobních údajů) jako celek. Během registračního řízení může být řešena detailnější specifikace kamerového systému jako umístění jednotlivých kamer, nastavení kamer, jejich počet aj.[59]

3.4 Fyzické kontroly vstupu

Primární funkcí fyzických kontrol vstupu je zabránění vstupu nepovolaných osob. Mezi další důležité činnosti patří identifikace vstupujících (zejména návštěv), vedení záznamů o vstupech a odchodech, vstupní kontrola (např. kontroly vnášených předmětů), kontrola způsobilosti osob (např. ovlivnění návykovými nebo psychotropními látkami), odchodová kontrola (např. prevence krádeží) a další, dle požadavků na bezpečnost v odlišných objektech. Tyto kontroly mohou být z velké části podpořeny elektronickými systémy.

Aby kontroly poskytovaly dostatečnou efektivitu, je také potřeba nastavit pravidla tohoto procesu. Pouhé umožnění vstupu a odchodu všem zaměstnancům sebou nese značná rizika. Při nesprávném nastavení pravidel by se mohl dělník z výroby dostat např.

[56] Zákon č. 262/2006 Sb. Zákoník práce [online].
[57] Zákon č. 101/2000 o ochraně osobních údajů a o změně některých zákonů [online].
[58] KUČEROVÁ, Alena a František NONNEMANN. Ochrana osobních údajů v praktických příkladech.
[59] Zákon č. 101/2000 o ochraně osobních údajů a o změně některých zákonů [online].

do místnosti se servery. Proto je důležité definovat, nejenom kdo se dostane do podniku, ale i kam a v jakou denní dobu. Pokročilé systémy umožňují i dynamické odepření přístupu např. v době dovolené daného zaměstnance nebo v případě delší služební cesty, tak aby HW klíč nemohl být zneužit jinou osobou.

Úprava systému kontroly také závisí na rozhodnutí, která z výše navrhovaných opatření (zvláště těch upravujících perimetr), budou přijata. Ideálním stavem je zachování pouze vrátnice u brány a), ze které budou dozorovány ostatní vstupy pomocí kamerového systému, v součinnosti s docházkovým systémem. Bude-li nadále nutné strpět průchod zaměstnanců jižní firmy od turniketu c) přes areál podniku k turniketu d), pak doporučuji smluvně zajistit odpovědnost za bezpečnost osob a jimi způsobené škody přímo s jižní firmou. Dále stanovit maximální čas, během kterého musí tyto osoby opustit areál. Především vzhledem k tomu, že jejich pohyb v areálu je omezen pouze na cestu od turniketu c) k turniketu d) a zpět. Delší pobyt v areálu je nezdůvodněný, a protože zvyšuje míru rizik, měl by být eliminován. Nejlepším řešením by však bylo zřízení vlastního vstupu v západní části jižní firmy (tuto činnost by zajistila jižní firma na své vlastní náklady). Jejich zaměstnanci by tak procházeli podél vnější strany západního perimetru našeho podniku a vstupovali za hranicí jižního perimetru přímo do prostor svého zaměstnavatele. Pokud tomuto řešení nebrání smluvní dohody, doporučuji toto řešení předložit jižní firmě k akceptaci.

V rámci pravidel vstupů navrhuji rozdělit areál na několik zón. První přístupovou zónu můžeme chápat jako vnitřní pásmo, tedy venkovní prostory uvnitř areálu. Další zóny pak budou představovat jednotlivé budovy, případně zóny v rámci budov. Nejpřísnější pravidla pro vstup pak budou nasazena v rámci chráněných pracovišť. Příklad možného rozdělení zachycuje následující tabulka č. 5.

Tabulka 5:Návrh možného rozdělení na zóny a jejich kódové značení (Zdroj: vlastní tvorba)

Kód oblasti	Oblast	Podoblast	Pracoviště
1	Vnitřní pásmo		
2a	Budova administrativy	1. podlaží	
2b	Budova administrativy	2. podlaží	

2b–S	Budova administrativy	2. podlaží	Serverovna
2b–F	Budova administrativy	2. podlaží	Kanceláře FO
3	Hala výroby		
3a	Hala výroby	Prostory u tavné pece	
4	Expedice		
5	Budova pískovny		
6	Sklady		
7	Stanoviště strážní služby		

Dále musí být kategorizovány osoby pohybující se v areálu do logických skupin, dle jejich potřeb přístupu a stanoveny časy, ve kterých jejich oprávnění platí. Při pečlivém dělení by vzniklo neprakticky velmi mnoho skupin. Tomuto stavu je možno částečně předejít pomocí omezení a výjimek pro jednotlivé případy. Následuje tabulka s demonstrativním návrhem možného řešení.

Tabulka 6: Kategorizace osob s pravidly pro vstup do vymezených oblastí (Zdroj: vlastní tvorba)

Osoba	Časy	Oblasti	Omezení a výjimky
Pracovníci úklidu	5:00 až 17:00	1, 2a, 2b, 2b–S, 2b–F 6, 7	Kanceláře a chráněná pracoviště pouze v doprovodu
Pracovníci výroby linka	6:00 až 18:00	1, 2a, 3	2a – po 16hod pouze jídelna
Pracovníci výroby tavná pec	vždy	1, 2a, 3, 3a	2a – po 16hod pouze jídelna
Pracovníci výroby expedice	6:00 až 18:00	1, 2a, 4, 6	2a – po 16hod pouze jídelna
Pracovníci výroby pískovna	6:00 až 18:00	1, 2a, 4, 5	2a – po 16hod pouze jídelna, 4 – pouze manipulační technici
Zaměstnanci úseku financí	8:00 až 16:00	1, 2a, 2b, 2b–F, 4, 6	
Zaměstnanci úseku IT	8:00 až 16:00	1, 2a, 2b, 2b–S, 7	2b–S – vstup jen pro správce

Zaměstnanci obchodního oddělení	8:00 až 16:00	1, 2a, 2b, 4, 6	
Návštěvy	8:00 až 16:00	1, 2a	1 – pouze přesun od brány k budově administrativy a zpět
Zaměstnanci jižní firmy	6:00 až 18:00	1	Pouze průchod, doba strávená v areálu max. 15 minut

Časy stanovené v tabulce přibližně reflektují pracovní doby jednotlivých osob. Při nasazení systému musí být zohledněno, že zaměstnanci mohou přijít dříve, aby se ustrojili atp., a zároveň z podobných důvodů mohou odejít o něco později. Situaci lze ošetřit paušálním navýšením časů o přiměřenou rezervu cca 45 min. Příchody v jiné časy musí být hlášeny strážní službě.

Oblasti musí být rovněž upraveny tak, aby nevznikaly nadbytečné požadavky pro přístup dalších osob. Problematická je z tohoto pohledu oblast serverovny (2b–S), neboť je v ní umístěn trezor finančního oddělení. Tento musí být bezpodmínečně přesunut do kanceláří finančního oddělení (2b–F). V prostoru serverovny tak zůstanou pouze aktiva IT oddělení. Jelikož oblasti 2b–S a 2b–F jsou chráněnými pracovišti, bylo by vhodné (v závislosti na přijetí opatření zabezpečení administrativní budovy) zajistit u nich evidenci vstupů nebo alespoň umožnit vstup pouze vybraným odpovědným zaměstnancům s tím, že ostatní osoby zde mohou provádět své činnosti pouze pod dozorem. V případě pracoviště 2b–S je tento přístup důležitý, jelikož jsou zde uchovávány citlivé osobní údaje a zároveň důležitá infrastruktura pro chod celé společnosti.

Evidenci návštěv provádí svědomitě strážní služba, proces je dobře ošetřen a případné změny by měly být implementovány jen v rámci modernizace, spočívající například v zavedení přístupových karet, což je jedno z opatření navrhnutých výše. Existuje zde prostor pro vyšší automatizaci a zvýšení komfortu, kdy by potvrzení o návštěvě příslušný navštívený mohl podat vrátní službě elektronicky a tím by odpadla nutnost tisknout tato potvrzení.

Jak bylo řečeno, návštěvy mají za povinnost nosit visačku „návštěva“ na viditelném místě, což je odlišuje od ostatních zaměstnanců. Pokud však svoji povinnost nesplní nebo do budovy pronikne cizí osoba, nemají zaměstnanci možnost ji bezprostředně odhalit, neboť sami nenosí žádný viditelný identifikátor. Mohou si tak cizí osobu splést s kolegou z jiného pracoviště. To je jeden z důvodů proč by měli všichni zaměstnanci nosit viditelný identifikátor. Optimálním řešením situace by mohla být čipová karta s potiskem, která by sloužila k autentizaci do všech podnikových systémů. Fotografie, jméno a zařazení vyobrazené na přední straně karty by umožnili rychlou identifikaci zaměstnanců. Potisk může také kvůli zpětné kompatibilitě s některými systémy obsahovat dříve používané čárové kódy. Povinnosti jako nosit kartu neustále viditelně, hlásit pohyb osoby bez karty strážní službě apod. musí být formalizovány. Problém s vydáváním nových karet komplikuje HR systém, který v současnosti pro nové zaměstnance generuje průkazy jen s čárovým kódem bez fotografie, který by bylo třeba upravit či implementovat úplně nový. Fotografie by také musely být uloženy v databázi splňující podmínky pro ochranu osobních údajů.

Mezi personálním a IT oddělením by měla vzniknout dohoda, ve které se personální oddělení zaváže předávat neprodleně IT oddělení informace o propuštěných zaměstnancích z důvodu zrušení jejich přístupových práv do systémů společnosti. Pakliže bude zaveden navrhovaný systém přístupů, mělo by IT oddělení v součinnosti s ostatními pracovišti prověřovat aktuálnost seznamu a provádět úpravy oprávnění dle potřeb v pravidelných intervalech, jejichž maximální délka bude součástí směrnice.

3.4.1 Uplatnění čipových karet v rámci podniku

Čipové karty nacházejí uplatnění napříč firemními procesy a výše byly zmíněny jen možnosti jejich nasazení v rámci přístupů. Vedení by mělo učinit v oblasti bezpečnosti strategické rozhodnutí a zvážit zda je nasazení karet vhodné lokálně v rámci dílčích řešení nebo plošně všude tam, kde to přispěje k bezpečnosti, urychlení a zvýšení přehlednosti procesů, což může mít pozitivní dopady i na ekonomiku daných procesů.

Karty mohou být využity velmi rozmanitě od plateb v kiosku, jako náhrada za klíče až po jejich nasazení coby HW klíče k přihlášení k počítači.

3.5 Zabezpečení kanceláří, místností a vybavení

Do kanceláří by nemělo být povoleno vstupovat bez dozoru nikomu, kromě pracovníků, jimž byly přiděleny. Z toho důvodu je třeba přehodnotit přístupy úklidového personálu mimo běžnou pracovní dobu. V rámci prevence selhání jednotlivce je také třeba uvážit nutnost přístupu strážní služby. Kontrolu kanceláří lze provést jen pohledem přes skleněné výplně dveří. Na druhou stranu zaměstnanci strážní služby během své kontroly kanceláří mohou uzavřít okna, pokud na to některý ze zaměstnanců při odchodu zapomněl apod. Pakliže by měla být situace vyřešena bez kompromisů, bylo by nutné osadit veškerá okna detektory uzavření a zároveň upravit dveře tak, aby elektronický systém nedovolil odchod, pakliže okno není uzavřeno. Takto sofistikovaný systém by si však podle mého názoru vyžádal příliš mnoho financí v poměru k nárůstu míry bezpečnosti.

Úklidoví pracovníci vstupují nejčastěji za účelem vynášení komunálního odpadu. Dříve bylo v podniku nastoleno pravidlo, že pokud si přeje majitel kanceláře odpad vynést, tak postaví při odchodu koš s odpadem za dveře. Toto pravidlo by mělo být opět zavedeno a formalizováno.

Každá kancelář, kde se pracuje s citlivými dokumenty, by měla být vybavena schránkou na dokumenty. Provedení může být ve formě zamykatelného šuplíku stolu či zamykatelné skříňky na dokumenty. V nepřítomnosti vlastníka citlivých dokumentů budou dokumenty ochráněny před nahodilým zneužitím.

3.6 Ochrana před vnějšími hrozbami a hrozbami prostředí

Z analýzy vyplynulo, že největší riziko představuje voda z přívalových dešťů a vysoká míra majetkové trestné činnosti v dané lokalitě. Podnik má již určité zkušenosti s těmito vlivy. Průniky do areálu také dokladují grafity na několika místech budovy výrobní haly, kam se sprejeři pravděpodobně dostali po servisních žebřících. Problémem těchto vniknutí je, že pachatelé bývají nezletilí a v případě, že by si přivodili zranění při odchytu strážní službou, existuje možnost poškození dobrého jména společnosti např. skrze média, z důvodu nedostatečné ochrany perimetru. Doporučuji i z tohoto důvodu zabezpečit servisní žebříky na střechy budov alespoň jejich zkrácením, tak aby nebyly ze země na dosah.

Před přívalovou vodou se podnik brání aktivně. V areálu se nachází zásoba pytlů s pískem, které jsou v případě potřeby použity k utěsnění exponovaných míst. Voda ohrožuje areál nejvíce z východní strany. Zde spatřuji možnost pro zbudování pasivní ochrany – ochranného příkopu, který by mohl být zbudován současně s nově vytyčeným západním perimetrem. Riziko by tímto bylo téměř zcela eliminováno a náklady na opatření by dle mého názoru i vzhledem k přidruženým pracím na západním perimetru byly akceptovatelné oproti variantě zabezpečit proti vodě jednotlivé budovy zvlášť.

Podnik vzorně plní nařízení týkající se pravidelných požárních a jiných kontrol a shody s normami, v čemž by měl prostřednictvím pověřeného zaměstnance pokračovat a provádět potřebné inovace. O modernizacích a průběžném zvyšování bezpečnosti by měli být informováni i pracovníci, kteří odpovídají za pojištění podniku pro případ škod, jelikož pojišťovny často nabízí pro různé úrovně bezpečnosti různé cenové tarify, může podnik touto cestou ušetřit finance.

3.7 Práce v zabezpečených oblastech

Je-li to možné z pohledu počtu zaměstnanců, pak by měla být povinnost dohledu v zabezpečených oblastech rozšířena tak, aby v místnosti byli vždy minimálně dva

zaměstnanci. V případě prací externích dodavatelů vždy alespoň jeden ze zaměstnanců firmy. V přítomnosti externích pracovníků by měly být v přímém dosahu pouze dokumenty, které jsou nezbytné pro výkon jejich činnosti. Ostatní materiály musí být dle okolností uschovány ve skříni na dokumenty nebo trezoru.

Jak bylo navrženo výše, mimo pracovní dobu, je prioritou kontrola uzamčení a monitoring vnitřních prostor (pohyb, požár, …). I když je pořizování fotografií zakázáno v celém areálu, je vhodné tuto povinnost zdůraznit i zde, obzvláště externím pracovníkům. Kromě toho by v těchto oblastech měl platit zákaz pořizování všech ostatních záznamů a používání komunikačních prostředků, vysílačů apod.

3.8 Oblasti pro nakládku a vykládku

Oblasti pro nakládku a vykládku jsou uvnitř areálu, takže přístupu náhodných osob je zabráněno fyzickými kontrolami vstupu. Oblasti jsou také odděleny od prostor, kde jsou zpracovávány informace. Výše navržená opatření týkající se zabezpečení budovy administrativy také zabraňují vstupu neoprávněných osob do těchto prostor.

Kontroly příchozího materiálu a informovanost zaměstnanců o postupech jsou na dostatečné úrovni.

3.9 Umístění zařízení a jeho ochrana

Cílem opatření je „*zabránit ztrátě, poškození, odcizení nebo kompromitaci aktiv a přerušení provozu organizace.*“ [60]

Opatření jsou částečně pokryta návrhem vyčlenění pracovišť 2b–S a 2b–F. V rámci oblasti 2b–S doporučuji zavést zákaz vnášení jídla a pití. Zařízení a dokumenty, které nepodléhají zpřísněnému režimu a ke kterým potřebují přistupovat ostatní zaměstnanci,

[60] ČSN ISO/IEC 27002. Informační technologie - Bezpečnostní techniky - Soubor postupů pro opatření bezpečnosti informací.

by měly být uloženy mimo chráněná pracoviště tak, aby bylo sníženo množství přístupů na dané pracoviště.

Ochranu před bleskem a přepěťové ochrany zajišťují pověření elektrotechnici dle aktuálních norem.

Jelikož kamerový systém nelze považovat za ochranu, ale pouze podporu, nejsou dle mého názoru některé strategické objekty (v plánu označeny jako 1 až 5) chráněny dostatečně.

1. Tavící pec

U tavící pece je zejména třeba zabránit vniku vody do prostoru pece, její nepřerušené zásobování elektrickou energií a dodávání chladiva. Tyto kritické úlohy jsou dobře zvládnuty a prováděny. Na pec také dohlíží jedna z kamer.

2. Ostrůvek s chladivy

Minimálně dva sloupky oplocení nejsou ukotveny, čímž je narušena celistvost ochrany. Stav pletiva a sloupků působí na pohled akceptovatelně a oprava by mohla být provedena upevněním sloupků do betonového ostrůvku pomocí kovových konzol. Pakliže se stav při bližším ohledání ukáže jako nevyhovující nebo při příští komplexnější rekonstrukci, doporučuji nasadit robustnější řešení spodního hrazení, či ideálně předsazení ukotvených betonových zátaras (např. typ CITY BLOC - TP159), aby bylo zabráněno nárazu vozidla do nádrží s chladivem.[61] Oplocení by mělo být posíleno dvouřadým ostnatým, případně žiletkovým drátem. Tento systém je kritický z pohledu kontinuity výroby, a proto by měla být věnována maximální pozornost jeho ochraně a na realizaci opatření vyčleněno odpovídající množství prostředků. Zohledníme-li fakt, jakou finanční ztrátu představuje znovu zprovoznění tavící pece, výpadek výroby na několik dní a související náklady, pak jsou investice do fyzické bezpečnosti ostrůvku chlazení marginální.

Prostor v okolí ostrůvku by měl být v noci permanentně osvětlen a po celý den snímán bezpečnostní kamerou nebo více kamerami.

[61] Svodidla betonová CITY BLOK - TP159 [online]. ČR: SVODIDLA a jednotliví autoři, ©1996-2011 [cit. 2017-05-11]. Dostupné z: http://www.svodidla.cz/svodidlo_city_blok.php

3. Rozvodna elektrické energie

Zabezpečení vstupů do rozvodny je realizováno kovovými dveřmi. Zabezpečení je přiměřené, nicméně lze doporučit nasazení podpůrných prvků jako detektory pohybu uvnitř prostor.

4. Serverovna a 2. rozvodna elektrické energie

Serverovna byla vyčleněna jako chráněné pracoviště 2b–S, ve kterém platí zpřísněná opatření. Druhá rozvodna se nachází uvnitř budovy administrativy. Vstup do rozvodny je chráněn uzamčenými dveřmi. Vzhledem k umístění rozvodny v budově by bylo vhodné, pakliže nebude přijato opatření instalace EPS jako celku, instalovat detektory požáru alespoň v těchto prostorech.

5. Čerpací stanice pohonných hmot

Ochrana stanice by měla být realizována např. instalací přístupové branky či uzamčením jednotlivých pistolí do stojanu. Stanice by měla být monitorována z důvodu odhalení neoprávněného tankování nebo sabotáže. Technicky lze situaci řešit připojením další kamery, případně čidel do systému.

V průběhu psaní diplomové práce došlo k úpravě výdeje nafty prostřednictvím identifikačních čipů

3.10 Podpůrné služby

Podnik má k dispozici dvě nezávislé elektrorozvodny, avšak redundantní spoj vede pouze k peci. Rozšíření tohoto napájení na další systémy, vzhledem k vysokým nákladům, lze doporučit pouze výhledově a po zvážení přínosů.

Důležitějším systémem, který by měl být nasazen, je systém UPS. Při výpadku proudu je nyní paralyzována datová síť, na které je (pakliže nebylo rozhodnuto o fyzickém vyčlenění) závislý kamerový systém a případné další detekční systémy komunikující

skrze IP. Systémy nejvíce ohrožují transientní a krátké výpadky (poklesy napětí a neplánované výpadky), které mohou vznikat i opakovaně v krátkých časových sledech, což může vést k restartu konfigurace některých zařízení nebo přinejmenším vyřazení systémů na dobu, než dojde k jejich opětovnému načtení (re-boot). Dlouhodobé výpadky jsou většinou oznamovány předem a systémy tak lze bezpečně včas odpojit.[62]

Vybavení datových rozvaděčů systémy UPS, by mělo tyto výpadky překlenout. Pro jednodušší nasazení je výhodné přes datovou síť napájet i koncová zařízení jako jsou kamery pomocí technologie PoE. Vybrané body napájené pomocí PoE by měly být propojeny se zdroji kabelem kategorie 6. V případě nasazení systému musí být systém schopen informovat správce o stavu prostřednictvím sítě nebo musí být prováděny periodické kontroly stavu fyzicky.

V prostorech jako rozvodny, serverovna, rozvaděče a další, kde se nachází kritické systémy, by mělo být zřízeno nouzové osvětlení. Nejlevnější realizaci lze zajistit instalací LED svítilen a procesním opatřením, které stanoví intervaly výměny baterií a pověřené osoby.

„Data i hlas“ jsou do areálu přivedeny spojem, na jehož trase se vyskytuje SPOF. Protože chod podniku není přímo závislý na připojení k internetu, je současné řešení připojení skrze jednoho ISP a smluvním zajištěním akceptovatelné. Telefonické spojení je možné při výpadku zastoupit mobilními telefony.

3.11 Bezpečnost kabelových rozvodů

Vedení kamer č. 1 a č. 2 je bezpečně uloženo do země. Nicméně část přívodu nad zemí (délková rezerva kabelu) u kamery č. 1 není chráněna. Měla by být rovněž uložena do chráničky či krabice pro rezervy kabelu. Vedení od kamery č. 2 svedené po vnější straně sloupu osvětlení, na kterém je umístěna, by mělo být ochráněno do výšky přibližně

[62] PROKOP, Lukáš, Zdeněk MEDVEC a Zdeněk ZMEŠKAL. Problematika oceňování nedodané energie v průmyslu [online].

2,5 m nad zemí odolnější chráničkou tak, aby nemohlo dojít k přeštípnutí kabelu nástroji, kterými by mohl být náhodně vybaven narušitel (např. kapesní nůž atp.).

Zbývající rozvody kamer jsou, s výjimkou kamery č. 9, umístěny na energo-mostech. Vhodným řešením změn by bylo uložení kabelů do země. Tam kde to nebude možné, doporučuji vést kabeláž v armovaných chráničkách.

Další rozšiřování síťové infrastruktury by mělo být realizováno po vzoru sítě instalované ve výrobní hale, která splňuje veškeré požadavky pro správnou funkci v průmyslovém prostředí.

Nespornějším místem z pohledu bezpečnosti kabelových rozvodů je pronajatá budova. Přístup do budovy není chráněn. Přístup k datovému rozvaděči omezuje pouze kryt rozvaděče. Skříň s elektrickými jističi je pak přímo přístupná. Jelikož, je budova pronajata, doporučuji zřídit z vnější strany nezávislou elektro-skříň, ze které budou napájeny přilehlé kamery a rovněž zřízení vnějšího datového rozvaděče s využitím stávajících tras. Tyto dva rozvaděče by měly být zamykatelné a přístupné pouze pověřeným osobám.

Rozvody mezi vrátnicemi je třeba upravit, neboť energo-most v severní části bude demontován.

Jako reakci na neoprávněné používání routerů doporučuji instalovat blokátory síťových portů směrem ven. Tedy tak, aby síťový kabel propojoval vždy konkrétní port zásuvky s konkrétním koncovým zařízením a nebylo možno ho přepojit bez příslušného klíče. Toto opatření rovněž zabrání opotřebování zlacených kontaktů portů (zhoršení parametrů sítě) a připojování zařízení pokaždé na jiný port zásuvky (při správě vzniká chaos). Nevyužívané porty by pak měly být zaslepeny. I když jsou nevyužité porty elektricky odpojeny, zaslepení přispívá jejich ochraně před nečistotami a uživateli, kteří by se mohli pokoušet nefunkčním portem připojit. Zbývá vyřešit otázku připojení mobilních zařízení. Pro notebooky by mohly být vyhrazeny kabely blokované pouze na jednom konci do vyhrazených portů, které budou určeny pro přenosná zařízení. Avšak dnes již spousty zařízení síťovým portem nedisponuje a komunikují pouze skrze bezdrátovou technologii. Zde je třeba učinit rozhodnutí na kterých místech a jakým způsobem je potřeba s těmito zařízeními pracovat a příslušná místa pokrýt signálem Wi-Fi. Tento provoz by měl být

oddělen pomocí technologie VLAN. Wi-Fi pokrytí by mělo umožňovat přístup k internetu a přístup k vnitřní síti by měl být umožněn pouze schváleným zařízením. Při modernizaci sítě v rámci budovy administrace by měl být navýšen počet datových portů tak, aby nebyly jako dosud lokálně využívány soukromé switche či jiné prvky mimo rozvaděče. Pravidla užívání sítě by měla být formalizována a zaměstnanci zaškoleni.

3.12 Údržba zařízení

O údržbě by měla být vedena dokumentace a to ideálně na jednotném formuláři, ze kterého jasně vyplyne kdo, kdy, co a jakým způsobem opravoval. Chyby na zařízeních musí být neprodleně hlášeny zaměstnancům, kteří jsou oprávněni provádět servis. Tito následně učiní záznam do formuláře a odevzdají ho na určené místo. Formuláře by měly mimo jiné sloužit jako doklady osvědčující plnění závazků vyplývajících z pojistných smluv.

3.13 Přemístění aktiv

Dokumenty a mobilní výpočetní zařízení podniku by nadále měly být zapůjčovány pouze zaměstnancům, kteří je nezbytně potřebují k výkonu své práce mimo areál. Jedná se tedy hlavně o obchodníky. Zaměstnanci by měli být pravidelně školeni v oblasti bezpečnosti s ohledem na používání šifrování disků mobilních firemních zařízení, způsobu manipulace s dokumenty, zacházení s podezřelými daty a aktualizací software. To vše v rámci širšího školení zahrnující informace o jejich dalších povinnostech v rámci fyzické bezpečnosti a zvyšování bezpečnostního povědomí v reakci na nové hrozby. Samozřejmě by i tyto povinnosti měly být formalizovány.

3.14 Bezpečnost zařízení a aktiv mimo prostory organizace

Přemisťovaná aktiva by měla být namátkově kontrolována, zda nedošlo k porušení povinností souvisejících s jejich zacházením. Disky mobilních zařízení by měly být plně šifrovány. V případě ztráty mobilního zařízení pak nehrozí unik citlivých dat. U antivirového software by měl být kladen největší důraz na prevenci, tedy citlivost ochran (testování na přítomnost PUP atp.) pracujících v reálném čase jako jsou webové a e-mailové štíty spolu se štíty souborového systému. Nevyužívané služby by měly být zastaveny. Je-li to možné, neukládat data pouze do zařízení, ale synchronizovat v rámci firemní infrastruktury.

Při zapůjčení citlivých firemních dokumentů by měl být o této skutečnosti pořízen záznam zahrnující údaje o tom kdo a za jakým účelem si který daný dokument půjčil.

3.15 Bezpečná likvidace nebo opakované použití zařízení

Proces bezpečné likvidace je funkčně dobře nastaven. Doporučuji zavést dokumentaci likvidovaných zařízení obsahujících citlivá data.

3.16 Uživatelská zařízení bez přítomnosti obsluhy

Zaměstnanci by měli být pravidelně proškoleni o zásadách bezpečného odchodu od zařízení. Zejména by mělo být vyžadováno odhlašování se z aplikací, které nejsou využívány, ukončování relací a ochrana účtu při odchodu (v systémech MS Windows je za tímto účelem zřízena klávesová zkratka WIN + L). Požadavky na zaměstnance by měly být začleněny do směrnice.

3.17 Zásada prázdného stolu a prázdné obrazovky monitoru

V rámci výše navrženého opatření zavést do kanceláří uzamykatelné skříně na dokumenty může být definován požadavek ukládat citlivé dokumenty do skříní vždy, když se s nimi nepracuje a ostatní dokumenty pak při odchodu zaměstnanců po skončení pracovní doby.

Do školení zaměstnanců by měla být zahrnuta i zásada čistého stolu s tím, že budou formalizovány sankce za její porušení. Rovněž je třeba definovat, které druhy dokumentů mají být tištěny v režimu kdy je nutné zadání PIN kódu.

3.18 Ekonomické zhodnocení

Finanční náročnost realizace navržených opatření bude dle mého odhadu v řádech stovek tisíc až jednotek milionů. Návrat investic do bezpečnosti se dá obtížně vyčíslit, neboť zde hrají roli přírodní živly a další náhodné jevy. Vezmeme-li však v úvahu navrhovanou výši pokut v GDPR (General Data Protection Regulation), která je pro mnohé podniky likvidační, je investice do bezpečnosti v navrhované výši ospravedlnitelná. Jak bylo uvedeno výše, podnik také může po zavedení opatření získat výhodnější cenu pojistného.

Fyzická bezpečnost je nutná pro plánování a udržení kontinuity výroby. Strategicky důležitá zařízení musí být bezpodmínečně chráněna před poškozením či sabotáží. Protože při odstávce těchto zařízení by vznikly podniku škody převyšující náklady na realizaci bezpečnostních opatření, dovolím si tvrdit, že navržená opatření splňují předpoklad přiměřené bezpečnosti.

4 ZÁVĚR

Problematika byla stručně uvedena a rozebrána v teoretické části práce. Důležité pojmy byly dle mého názoru objasněny.

V analytické části byla identifikována slabá místa zabezpečení a neshody s normami. Identifikované problémy byly popsány v rámci jednotlivých kapitol.

V návrhové části se podařilo navrhnout několik variant změn hranic perimetru, z nichž si může vedení podniku zvolit tu, která bude nevíce odpovídat budoucím záměrům. Dále byla doporučena režimová opatření, které může podnik převzít a začlenit do bezpečnostní směrnice. Bylo předloženo demonstrativní řešení rozdělení areálu do bezpečnostních zón. Toto řešení může být převzato a upraveno dle nově vzniklých potřeb organizace. Problematice kamerového systému byla věnována samostatná kapitola, ve které jsou navrženy úpravy systému a návrhy na budoucí zlepšování. V důležitém tématu bezpečnosti strategických bodů byla navržena opatření k nápravě současných nedostatků.

Hlavní inovace tedy představují změny kamerového systému, hranic perimetru a režimová opatření. Cílem práce bylo analyzovat stav fyzické bezpečnosti závodu a navrhnout opatření k nápravě nevyhovujícího stavu. Dle mého názoru byl cíl naplněn. Hlavní přínos práce spatřuji v možnosti využití danou firmou v praxi.

Vedení společnosti bylo již delší dobu znepokojeno zhoršeným stavem fyzické bezpečnosti. Nyní mají k dispozici tuto práci, která může sloužit jako podklad pro výběrové řízení na dodávku systému zabezpečení.

SEZNAM POUŽITÉ LITERATURY

DRASTICH, Martin. Systém managementu bezpečnosti informací. Praha: Grada, 2011. Průvodce (Grada). ISBN 978-80-247-4251-9.

GORDON, Adam a Javvad. MALIK. Official (ISC)2® guide to the CISSP® CBK®: Certified Information Systems Security Professional. Fourth edition. London: (ISC)2 Press, 2015. (ISC)2 Press series. ISBN 978-1482262759.

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

KUČEROVÁ, Alena a František NONNEMANN. Ochrana osobních údajů v praktických příkladech. Praha: BOVA POLYGON, 2013. ISBN 978-80-7273-173-2.

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

NORMY

ČSN ISO/IEC 27001. Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

ČSN ISO/IEC 27002. Informační technologie - Bezpečnostní techniky - Soubor postupů pro opatření bezpečnosti informací. 2. vyd. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

Seznam použitých elektronických zdrojů

AD převodník [online]. ČR: Megapixel, 2017 [cit. 2017-05-25]. Dostupné z: https://www.megapixel.cz/ad-prevodnik

Betonový plot hladký, SP240 + ostnatý a žiletkový drát. In: Ploty Ostrava [online]. ČR: Ploty Ostrava - Vítězslav Kanclíř, ©2015 [cit. 2017-05-21]. Dostupné z: http://www.ploty-ostrava.cz/ploty/betonovy-plot-hladky-sp240-ostnaty-a-ziletkovy-drat

BURIAN, David, ed. Provozování kamerových systémů: metodika pro splnění základních povinností ukládaných zákonem o ochraně osobních údajů [online]. Brno: Pro Úřad pro ochranu osobních údajů vydala Masarykova univerzita, 2012 [cit. 2017-05-18]. ISBN 978-80-210-6017-3. Dostupné z: https://www.uoou.cz/files/metodika_provozovani_kamerovych_systemu.pdf

Černý LED reflektor 100W SMD: Parametry. LED Solution [online]. ČR: LED Solution, 2016 [cit. 2017-04-27]. Dostupné z: https://eshop.ledsolution.cz/LED-reflektor-100W-cerny-smd-tepla-bila-3000K?tab=parameters

HALOUZKA, Kamil. Fyzická bezpečnost: Perimetrické zabezpečovací systémy [online]. Brno [cit. 2017-05-11]. Dostupné z: https://moodle.unob.cz/pluginfile.php/18075/mod_resource/content/2/10_Perimetrick%C3%A9%20zabezpe%C4%8Dovac%C3%AD%20syst%C3%A9my.pdf

LED technologie [online]. ČR: LIGHTRONIC, ©2015 [cit. 2017-05-24]. Dostupné z: http://www.lightronic.cz/led-technologie.php

MAC adresa [online]. ČR: Západočeská universita v Plzni, 2012 [cit. 2017-05-20]. Dostupné z: http://home.zcu.cz/~dachova/ZPS/Mac%20Adresa.htm

MAPAKRIMINALITY.CZ. MAPAKRIMINALITY.CZ [online]. ČR: Projekt Otevřené společnosti, 2012 [cit. 2017-01-13]. Dostupné z: http://www.mapakriminality.cz/

Nehos QoS [online]. USA: Nehos wiki Communications, 2016 [cit. 2017-05-24]. Dostupné z: http://wiki.nehos.net/?p=517

NEJČASTĚJŠÍ DOTAZY - FAQ. Apexis.cz [online]. ČR: Apexis.cz, 2017 [cit. 2017-01-11]. Dostupné z: https://www.apexis.cz/FAQ-IP-kamer-apexis

NTP Documentation: The NTP FAQ and HOWTO [online]. Cambridge: Free Software Foundation, ©1999-2005 [cit. 2017-05-22]. Dostupné z: http://www.ntp.org/ntpfaq/NTP-s-algo.htm

Paint.NET [online]. dotPDN LLC and Rick Brewster, 2010 [cit. 2017-05-24]. Dostupné z: https://www.getpaint.net/

Peníze do technologií ano, do vzdělávání lidí ne: firmy riskují, že jim zabezpečení dat selže [online]. ČR: COMPUTERWORLD, 2016 [cit. 2017-04-15]. Dostupné z: http://computerworld.cz/aktuality/do-technologii-ano-do-vzdelavani-lidi-ne-firmy-riskuji-ze-jim-ochrana-selze-53394

PoE Types: What They Mean and How They're Used [online]. Belden, 2016 [cit. 2017-05-22]. Dostupné z: http://www.belden.com/blog/datacenters/poe-types-what-they-mean-and-how-they-re-used.cfm

Power over Ethernet (PoE) Explained: Part 2 - Demystifying POE [online]. Prestwick: Veracity UK, 2016 [cit. 2017-05-22]. Dostupné z: http://www.veracityglobal.com/resources/articles-and-white-papers/poe-explained-part-2.aspx

PROKOP, Lukáš, Zdeněk MEDVEC a Zdeněk ZMEŠKAL. Problematika oceňování nedodané energie v průmyslu [online]. Ostrava: VŠB-TU, 2009 [cit. 2017-05-15]. ISBN 978-80-248-2099-6.

Průmyslové ploty. In: PK Mont Moravia s.r.o.: Vrata-brány-pohony-ploty [online]. ČR: PK Mont Moravia, ©2017 [cit. 2017-05-21]. Dostupné z: http://www.vrata-brany.eu/12670/prumyslove-ploty

RNDr. Josef Štekl, CSc., Mgr. David Hanslian a další. Výzkum vhodnosti lokalit v ČR z hlediska zásob větrné energie a zpracování metodiky pro posuzovací a schvalovací řízení při zavádění větrných elektráren. In: Ústav fyziky atmosféry AV ČR [online]. ČR: Ústav fyziky atmosféry, 2004 [cit. 2017-01-13]. Dostupné z: www.ufa.cas.cz/vavf320f08f03.html

Scorpion system: PLOTOVÝ ZABEZPEČOVACÍ SYSTÉM (PZS) SCORPION [online]. ČR: International Scorpion Security, ©2010 [cit. 2017-05-21]. Dostupné z: http://www.zabezpeceni-fve.cz/zabezpecovaci-plotovy-system.php

Síťová vrstva [online]. ČR: SPŠ Hradec Králové, 2000 [cit. 2017-05-22]. Dostupné z: http://www.gybon.cz/~rusek/vyuka/site/site006.html

Topologie sítí [online]. ČR: Technická universita Ostrava [cit. 2017-05-20]. Dostupné z: http://www.cs.vsb.cz/grygarek/PS/lect/topologie.html

Venkovní průmyslové reflektory VM 150 VR, VM 250 VR, VM 400 VR. VYSTO [online]. ČR: Vysto Kobylí, c2011 [cit. 2017-04-27]. Dostupné z: http://www.vysto.cz/svitidla/vybojkova-svitidla-vm-elektro/venkovni-prumyslove-reflektory-vm-150-vr-vm-250-vr-vm-400-vr

Větrný atlas České republiky. WINDSTORM [online]. ČR: WINDSTORM, 2016 [cit. 2017-01-13]. Dostupné z: http://www.windstorm.estranky.cz/fotoalbum/vetrna-mapa-cr/

Video musíme sami zfalšovat, abychom dokázali podvod, vysvětluje expert. Technet-cz [online]. ČR: převzato z časopisu IN ZOOM, 2016 [cit. 2017-05-06]. Dostupné z: http://technet.idnes.cz/banky-nekdy-nevedomky-pomahaji-zlocincum-f1v-/veda.aspx?c=A160307_140749_veda_mla

VLAN. In: Lupa.cz: Server o českém internetu: Bráníme se odposlechu: obrana na switchi [online]. ČR: Lupa.cz, 2006 [cit. 2017-05-23]. Dostupné z: https://i.iinfo.cz/urs/VLAN-115615665392667.GIF

VLAN - Virtual Local Area Network. SAMURAJ-cz.com - počítačové sítě, Cisco, Microsoft, VMware, administrace [online]. ČR: Petr Bouška, 2007 [cit. 2017-05-20]. Dostupné z: http://www.samuraj-cz.com/clanek/vlan-virtual-local-area-network/

What Is DHCP? [online]. USA: Microsoft, 2003 [cit. 2017-05-22]. Dostupné z: https://technet.microsoft.com/en-us/library/cc781008(v=ws.10).aspx

What Is NAT? [online]. USA: Microsoft, ©2017 [cit. 2017-05-24]. Dostupné z: https://technet.microsoft.com/en-us/library/cc753373(v=ws.10).aspx

Zabezpečovacia technika: Elektronický zabezpečovací systém – EZS časť.2: PRVKY OBVODOVEJ OCHRANY [online]. Vranov nad Topľou: NET4ALL, 2016 [cit. 2017-05-22]. Dostupné z: http://www.net4all.sk/zabezpecovacia-technika/elektronicky-zabezpecovaci-system/

Zákon č. 101/2000 o ochraně osobních údajů a o změně některých zákonů [online]. In: . ČR, 2016-aktuálníznění, s. 32 [cit. 2017-05-17]. Dostupné z: https://portal.gov.cz/app/zakony/download?idBiblio=49228&nr=101~2F2000~20Sb.&ft=pdf

Zákon č. 262/2006 Sb. Zákoník práce [online]. In: . ČR: Sbírka zákonů, 2017-aktuálníznění, s. 235 [cit. 2017-05-17]. Dostupné z: https://portal.gov.cz/app/zakony/download?idBiblio=62694&nr=262~2F2006~20Sb.&ft=pdf

Zpráva o nebezpečí povodně. In: Průvodce pro zjištění nebezpečí výskytu povodně [online]. ČR: Intermap Technologies, 2016 [cit. 2017-01-13]. Dostupné z: /anonymizováno/ (riskportal.intermap.cz)

Zvyšující se tržby společnosti COMGUARD potvrzují rostoucí poptávku po bezpečnostních i síťových řešeních [online]. ČR: COMGUARD, 2015 [cit. 2017-04-15]. Dostupné z: https://www.comguard.cz/novinky/aktuality/zvysujici-se-trzby-spolecnosti-comguard-potvrzuji-rostouci-poptavku-po-bezpecnostnich-i-s/

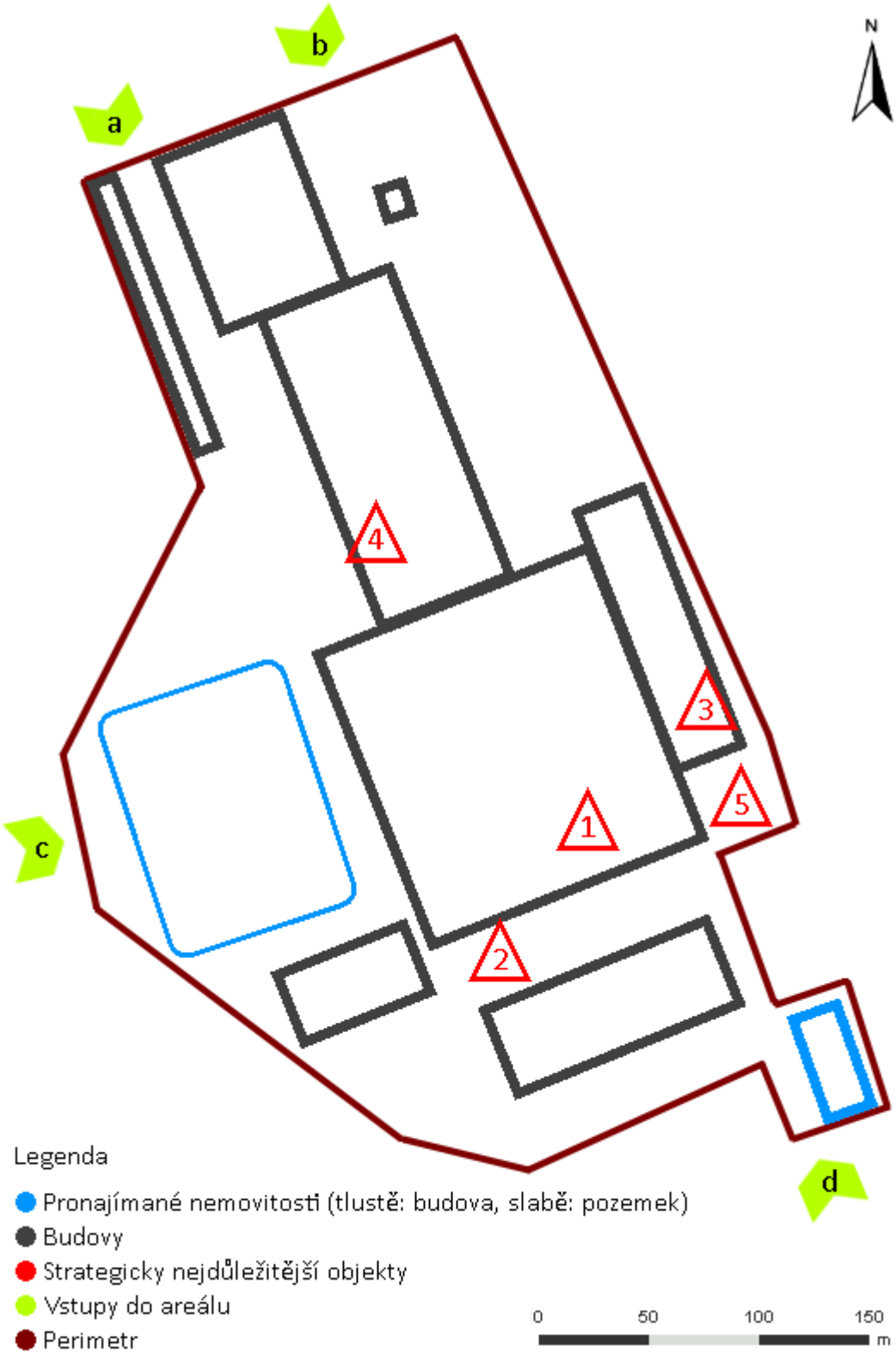
SEZNAM PŘÍLOH

SEZNAM OBRÁZKŮ

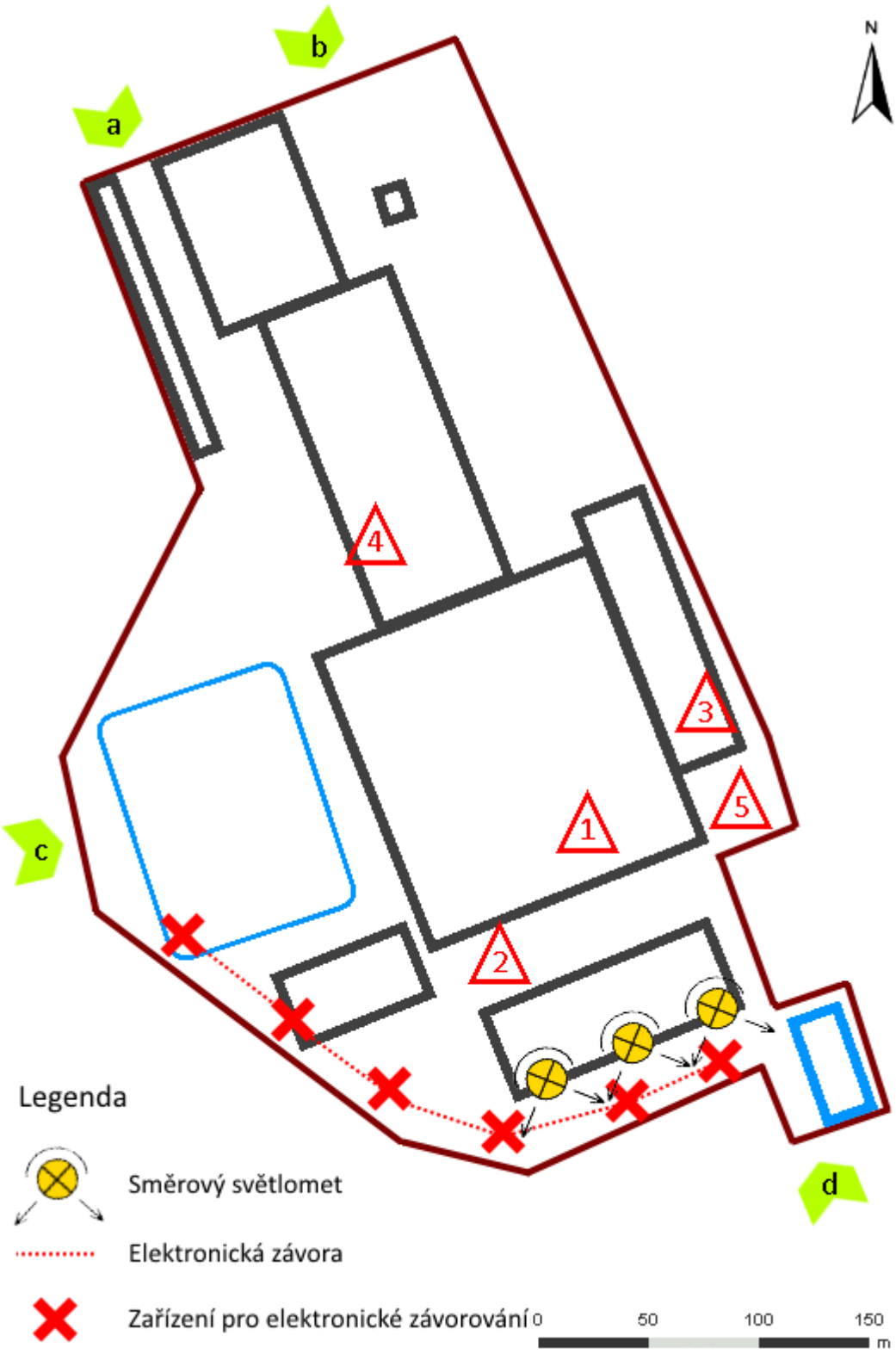
SEZNAM TABULEK

Přílohy

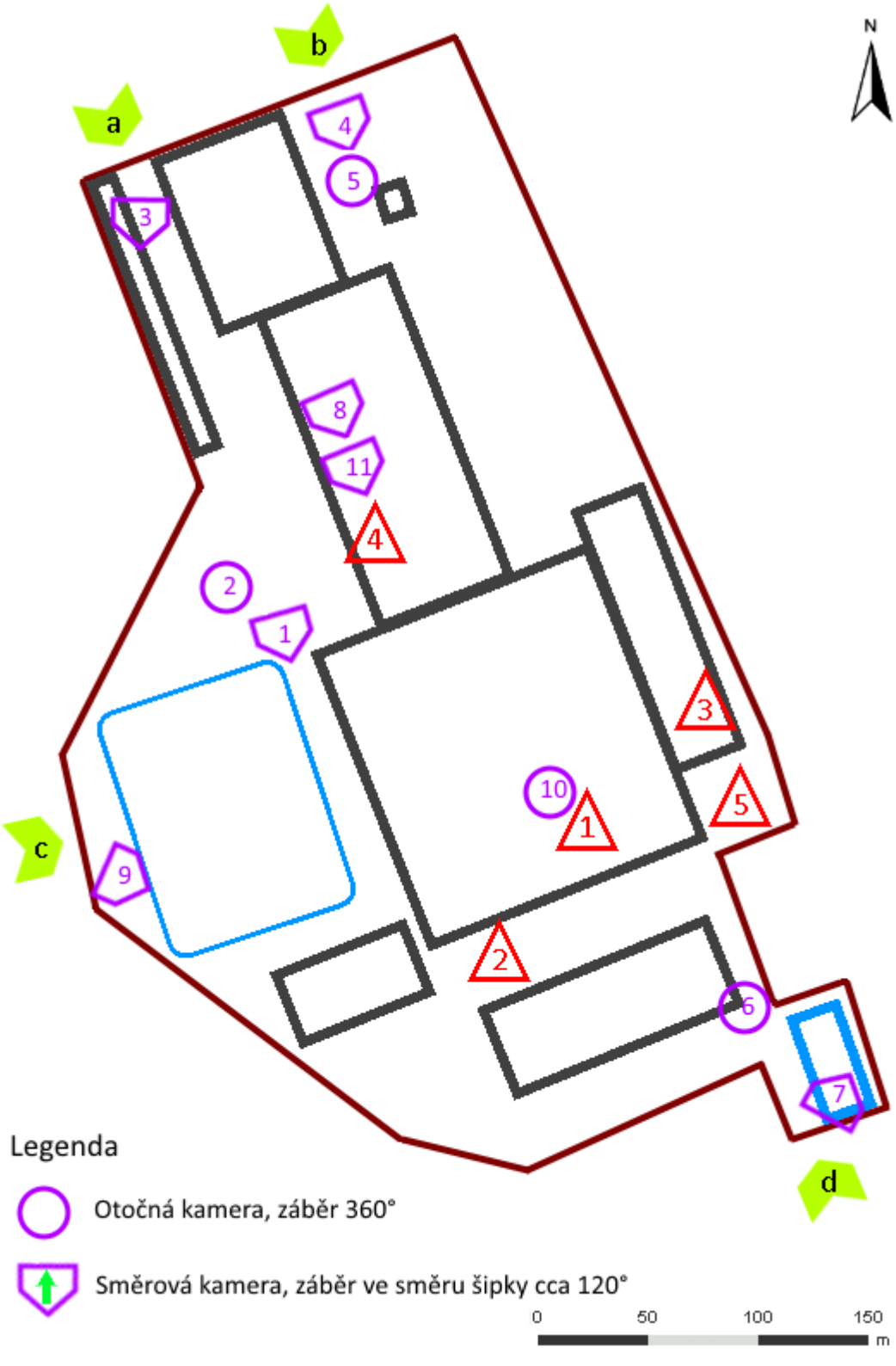
Příloha 1: Plán areálu podniku (Zdroj: vlastní tvorba)



Příloha 2: Umístění elektronických závor a světlometů (Zdroj: vlastní tvorba)



Příloha 3: Rozmístění kamerového systému před úpravami (Zdroj: vlastní tvorba)



Příloha 4: Fotografie demonstrující stáří a stav budov (Zdroj: autorská fotografie)