Bezpečnostní audit ve vybrané firmě

A Security Audit in a Selected Comapany

Radek Zámečník

Bakalářská práce
2015

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2014/2015

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Radek Zámečník**
Osobní číslo:	**A11805**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Bezpečnostní audit ve vybrané firmě**
Téma anglicky:	**A Security Audit in a Selected Company**

Zásady pro vypracování:

1. **Zpracujte krátkou rešerši na téma bezpečnostních auditů.**
2. **Proveďte bezpečnostní audit ve vybrané firmě.**
3. **Zhodnoťte úroveň bezpečnostní politiky firmy na základě výsledků auditu.**
4. **Navrhněte optimální odstranění slabých míst v bezpečnostní politice firmy.**
5. **Při provádění auditu a citování se řiďte příslušnými normami.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **BRABEC, František a kolektiv. Bezpečnost pro firmu, úřad, občana. Praha: Public History, 2001. ISBN 80-86445-04-6.**
2. **BRABEC, František. Ochrana bezpečnosti podniku. Praha: EUROUNION, 1996. ISBN 80-85858-29-0.**
3. **DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat. Brno: Computer Press, 2004. ISBN 80-7226-632-2.**
4. **LUKÁŠ, Luděk a kolektiv. Bezpečnostní technologie, systémy a management II. Zlín: VeRBuM,2013. ISBN 978-80-87500-19-4.**
5. **SEILER, Milan. Bezpečnostní audit v organizaci. Praha: Soukromá vysoká škola ekonomických studií, 2014. ISBN 80-86744-20-5.**
6. **Fryšar, Miroslav a kolektiv. 2006. Bezpečnost pro manažery, podnikatele a politiky. Praha: Public History. ISBN 80-86445-22-4.**

Vedoucí bakalářské práce: **Ing. et Ing. Kateřina Sulovská**
Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce: **6. února 2015**

Termín odevzdání bakalářské práce: **3. června 2015**

Ve Zlíně dne 6. února 2015

L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

Ing. Jan Valouch, Ph.D.
ředitel ústavu

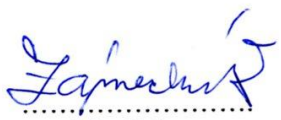
Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně



.....

podpis diplomanta

ABSTRAKT

Cílem bakalářské práce je zjistit skutečný stav implementovaných bezpečnostních pravidel a ochranných mechanizmů v rámci zvolené organizace a porovnat je s požadovaným stavem daným organizací případně stavem ideálním. V praktické části mé bakalářské práce byl proveden audit firmy, analýza rizik a hrozeb. Na základě výsledků těchto analýz bylo provedeno celkové hodnocení bezpečnosti společnosti a navržen optimální způsob odstranění zjištěných slabých míst.

Klíčová slova: bezpečnostní politika, bezpečnostní management, bezpečnostní manažer, bezpečnostní audit, bezpečnostní kontrola

ABSTRACT

The aim of the thesis is to determine the actual state of implemented security policies and protection mechanisms within the selected organization and compare them with the state given by the organization or alternatively with the ideal. In the practical part of my thesis was conducted audit of the company, analysis of risks and threats. Based on the results of these analyzes has been performed an overall evaluation of - its safety and designed the optimal way to overcome the weaknesses - identified previously.

Keywords: security policy, security management, security manager, security audit, security check

Tímto bych rád poděkoval celé své rodině za podporu a trpělivost po celou dobu studia. Velké díky patří mé vedoucí práce Ing. Kateřině Sulovské za velmi cenné rady a trpělivost při psaní mé práce. V neposlední řadě bych rád poděkoval JUDR. Františku Brabcovi za poskytnuté materiály, které byly velkým přínosem při psaní mé bakalářské práce.

Motto:“Důvěřuj, ale prověřuj“

OBSAH

ÚVOD

Každá, i sebemenší firma nebo organizace, aniž si to bezprostředně uvědomuje, má svou bezpečnostní politiku. Je jen otázkou, zdali ji ke své činnosti využívá. Kvalifikovaný a zkušený bezpečnostní management podniku mezi prvními akty řízení při jeho vzniku stanoví svou bezpečnostní politiku. Jde o organizační a řídící akty, normy, pravidla, pokyny a nařízení, jejichž cílem je maximálně ochránit podnik proti ztrátám, rozkrádání a vloupání. Z hlediska řízení podniku sem patří neodmyslitelně informace o ohrožení podniku, stanovení bezpečnostních, odborných, provozních i obchodních rizik.[7] Každá firma by se měla zaměřit na své slabé stránky, vyhodnotit je a následně zabezpečit na takovou úroveň, která ji bude zajišťovat bezpečnost v zásadních oblastech. Odhalení slabých míst a jejich náprava může být v konkurenčním prostředí pro firmu velice zásadní.

V současné době je bezpečnostní politika v určitých oblastech značně podceňována a opomíjena, spíše není nastavena vůbec. Může se lišit činností, kterou se organizace zabývá, nebo směrem jakým se vyvíjí. Jednou ze součástí bezpečnostní politiky organizace je nastavení určitých pravidel, jejich analýza a následná kontrola. V tom nám může být nápomocen bezpečnostní audit, který v konečné fázi implementuje ideální nastavení bezpečnostní politiky v organizaci.

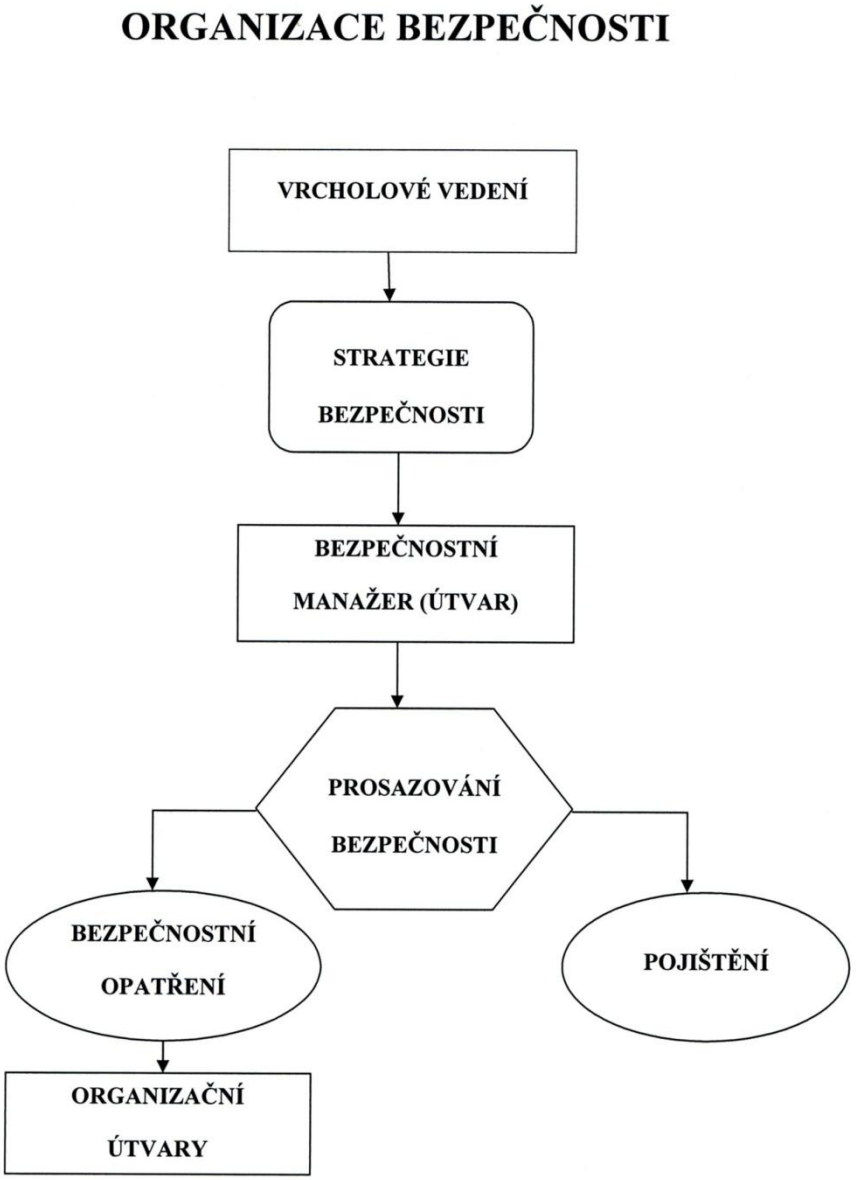
Jelikož pracuji v prostředí, kde je bezpečnostní politika bezprostředně provázána, bylo pro mne téma bakalářské práce velkou výzvou.

V teoretické části bude objasněn význam bezpečnostní politiky, bezpečnostního auditu, druhy auditu, typy auditu a v neposlední řadě jeho průběh a činnosti s tím spojené. V praktické části provedu bezpečnostní audit v několika oblastech, ve které se organizace pohybuje. Dle výsledku navrhnu možné řešení a nastavení takové bezpečnostní politiky, která bude zajišťovat v rámci možnosti organizace její optimální zabezpečení.

I. TEORETICKÁ ČÁST

1 BEZPEČNOSTNÍ POLITIKA PODNIKU

Abychom pochopili bezpečností audit, je třeba alespoň okrajově vysvětlit pojmy bezpečnostní management a bezpečnostní manažer. Bezpečnost v organizaci vyžaduje komplexní a systémový přístup, a je úkolem vrcholového vedení organizace, která za ni nese plnou odpovědnost. V rámci managementu firem a organizací je ve stále větší míře uplatňována zásada bezpečnosti, jako integrální součásti všech řídících procesů.



Obrázek č. 1. : Organizace bezpečnosti [5]

Zásada bezpečnosti vyjadřuje:

- potřebu zahrnout aspekt bezpečnosti do všech strategických koncepčních rozhodnutí
- potřebu zahrnout bezpečnostní aspekty do všech vrstev procesních norem firmy
- potřebu systematicky vytvářet podmínky pro kvalifikované rozhodování v rovině
- bezpečnostní vrstvy řízení provozu

Bezpečnost organizace je bezprostředně spjata se získáváním a zachováním zdrojů pro její existenci. Bezpečnost organizace je dána jejím potenciálem nepoškozovat vlastní prostředí v celku.

Organizace má širokou škálu možností, jak v rámci odpovědnosti osob uvnitř sdružených přispět k vlastní bezpečnosti.

Postup tvorby bezpečnostní politiky může představovat sled následujících činností:

- inventarizace rizik
- vytipování aktuálních rizik
- analýza vytipovaných rizik
- tvorba podkladů pro bezpečnostní projekt
- bezpečnostní projekt a jeho vyhodnocení
- návrh pracovní verze bezpečnostní politiky

Východisko pro tvorbu bezpečnostní politiky:

- bezpečnostní průzkum
- identifikace rizik

Bezpečnostní průzkum

Cílem bezpečnostního průzkumu je zjistit co nejvíce vlivů, které by organizaci mohly buď ohrožovat, nebo ji naopak poskytovat příznivé podmínky k jejím aktivitám. Předmětem bezpečnostního průzkumu budou vlivy klimatogenní, terénní, energetické, dopravní, spojovací, zásobovací, faktory ochrany životního prostředí, ale i další.

Identifikace rizik

Riziko je obecně budoucí, a proto nejistá událost, která může mít nepříznivý účinek na ziskové činnosti podniku, tedy na snížení zisku nebo zvýšení ztráty.

Identifikace rizik je jedním z nástrojů vytváření a udržování systému bezpečnostní organizace. Spočívá ve shromáždění všech typů rizik přicházejících v dané lokalitě, případně v daných souvislostech v úvahu. Při hodnocení rizik je nutné vycházet mimo jiné z analýzy mimořádných událostí v organizaci. Tato analýza je nezastupitelnou pomůckou zejména pro manažery, kteří nemají v oboru dostatečnou zkušenost, respektive s odhadem rizik. [5]

Identifikace rizik je prováděna při:

- vypracování základního bezpečnostního konceptu
- stanovení priorit realizace bezpečnostních opatření
- kontrole realizace bezpečnostních opatření [5]

Hodnocení rizik může probíhat na úrovni:

- celé organizace
- jen určité, vymezené části bezpečnostního systému (subsystému)
- vybraného pracoviště nebo objektu [5]

1.1 Uvedení bezpečnostního systému, kontrola a jeho vyhodnocení

Bezpečnostní systém je předán do provozu a podřízen periodické kontrole, zda realizovaná a implementovaná opatření bezpečnostních politik pracují efektivně a v souladu s tím, jak byla zamýšlena. Postupně jsou procházeny jednotlivé oblasti řešené v bezpečnostních politikách, případné odchylky jsou dokumentovány a odstraňovány nápravnými akcemi. Po jejich vyhodnocení v širším kontextu bezpečnostních politik pak dochází i k případným úpravám příslušných částí bezpečnostního projektu. Vykazuje-li bezpečnostní systém uspokojivý stav, je třeba věnovat se měnícím se podnikatelským požadavkům dané organizace, zachycovat a vyhodnocovat technologické změny a periodicky zkoumat stav hrozeb a zranitelností.

Bezpečnostní systém představující správně vytvořené, realizované a do každodenního fungování organizace implementované bezpečnostní politiky, se stává pevným základem funkčního systému řízení bezpečnosti organizace. Je základním prvkem jistoty managementu, že aktiva organizace jsou dostatečně zabezpečena proti poškození nebo zničení.

Vzhledem k narůstajícímu počtu útoků na data a jiná aktiva řady organizací, může vést podceňování bezpečnostního systému k vážnému porušování povinností při správě majetku a zanedbávání chování dobrého hospodáře. Následky pak mohou být vážné pro organizaci i její vedení. Aktivní práce zaměřené na vybudování bezpečnostního systému organizace

jsou tak pozitivním krokem managementu k zajištění aktiv organizace a čistého svědomí vzhledem k řešení potenciálních rizik. Informace o vytvoření bezpečnostního systému se v současnosti stává konkurenční výhodou na trhu, která deklaruje kvalitu firmy.

1.2 Bezpečnostní management

Je část řízení podniku, která zajišťuje plánování, řízení, organizaci a kontrolu všech oblastí podnikové bezpečnosti. Bezpečnost je z pohledu top manažera složitý problém, který je mnohdy podceňován. Bezpečnostní management ve větším podniku tvoří samostatnou složku, která tvoří nedílnou součást při rozhodování strategie firmy na několik let dopředu.

1.3 Bezpečnostní manažer

Je součástí týmu, který plánuje, organizuje, řídí a kontroluje bezpečnostní situaci ve firmě. U větších organizací je součástí bezpečnostního managementu, která je samostatnou jednotkou ve firmě. Stojí v čele útvaru bezpečnosti a je nadřazený a odpovědný vedení firmy (statutární orgán).

1.3.1 Povinnosti bezpečnostního manažera

1.3.1.1 Popis pravomocí manažera

- je přímo podřízen odpovědné osobě, statutárnímu zástupci nebo pověřenému členovi představenstva
- je přímým nadřízeným všem zaměstnanců bezpečnostního úseku
- v otázkách bezpečnosti metodicky řídí práci všech vedoucích zaměstnanců v odborných manažerských pozicích, a všech odborných úseků organizační struktury firmy
- odpovídá za včasnou identifikaci bezpečnostních rizik, analýzu jejich zdrojů a vývojových trendů
- odpovídá za tvorbu bezpečnostní politiky firmy, za její předložení vedení a její implementaci do praxe po jejím schválení
- odpovídá za tvorbu podkladů pro přijetí rozpočtových opatření v oblasti bezpečnosti, jejich včasné předkládání vedení firmy a po schválení jejich dodržování a hodnocení jejich účinnosti
- má právo navrhovat rozsah outsourcingu v oblasti bezpečnosti, má klíčové postavení v organizaci na výběru dodavatele, smluvním zajištění dodávky

1.3.1.2 Činnosti spojené s uplatněním manažera v organizaci

Navrhuje a vytváří systém bezpečnosti v podniku

Zvládá procesy spojené s analýzou a navrhuje celkovou strategii v oblasti bezpečnosti, její zájmy implementované do organizace a to na úseku personálním, informačním i fyzické ochrany spojené s technickými prostředky. Vše musí být v souladu s bezpečnostní politikou, která je ve firmě nastavena. [5]

Je znalý v právní oblasti bezpečnostní politiky

Bezpečnostní manažer musí být znalý alespoň v základních otázkách právní legislativy a vyhlášek. Nedílnou součástí je ochrana ekonomických a podnikatelských zájmů.

Musí mít dobré znalosti v oblasti technických prostředků

Je schopen na základě znalosti technických prostředků mít přehled o jejich využití, a hlavně možnosti případného zneužití ve firmě, ve které zastává jednu z nejvyšších pozic podniku a je plně odpovědný za správné nasazení těchto systémů a prostředků. [5]

Vytváří vnitřní předpisy

V součinnosti s vedením podniku (statutárním orgánem) vydává potřebné směrnice, jako např. poplachové směrnice. Dále vydává metodické pokyny. Řídí oblast technických a režimových standardů a podpory provozu a provozu bezpečnostního řešení pracovišť. [5]

Aplikuje plánování podniku a řízení krizových situací v součinnosti IZS

Podílí se na řízení krizových situací, realizuje opatření k mimořádným událostem, zjišťuje a analyzuje jejich příčiny i následky, a s příslušnou úrovní managementu navrhuje přijetí nápravně-preventivní opatření. Musí ovládat alespoň základní pravidla pro provádění bezpečnostních auditů. [5], [6]

Zajišťuje bezpečnostní školení zaměstnanců a vzdělávání zaměstnanců

Zajišťuje školení v oblasti manažerů v oblasti IT na zabezpečení počítačového systému. Dále různá další školení, jako např. BOZP (Bezpečnost a ochrana zdraví při práci), školení řidičů, školení na nákladní výtahy. V rámci školení je možné jmenovat požární hlídku, která absolvuje v pravidelných horizontech školení.

Nastavuje zásady ochrany informací v rámci organizace

Do této oblasti patří ochrana utajovaných skutečností, obchodního a bankovního tajemství. V této fázi je velice těžké pro bezpečnostního manažera zaručit jejich utajení. Informace se dávají jen nezbytné pro samotný výkon pracovních povinností. [5]

1.4 Rozdíl mezi auditem a kontrolou

Bezpečnostní politika má dva skoro totožné a velmi zaměnitelné pojmy a to kontrola – audit. Pokud to budeme chtít vysvětlit hodně jednoduše, tak použijeme toto srovnání. Kontrolu provádí osoba, která přímo odpovídá za danou oblast, nebo tím může pověřit třetí osobu, která má přikazovací pravomoc (nepřímá závislost) [5]. Kdežto pokud mluvíme o auditu, jde o dohled, který je vykonáván osobami nebo organizací, které nemají vůči sledovaným procesům žádnou odpovědnost, ani nejsou na ní nějak závislá. Kontrola a audit se liší svými cíly. Rozdíly nám může ukázat následující tabulka.

Tabulka č. 1.: Rozdíly kontroly a auditu [5]

	Vnitřní kontrola	Interní audit
Zařazení	součást všech úrovní řízení	nástroj vrcholového vedení organizace
Spočívá	ve zjišťování odchylek stavu skutečného od stavu žádoucího	v nezávislém ověřování všech činností probíhajících v organizaci, jehož podstatou je zjišťování rizik a jejich následné řízení
Provádí	všichni řídící pracovníci	pracoviště interního auditu
Cíl	odstranění zjištěných nedostatků	zvyšování efektivnosti, vytváření přidané hodnoty

2 BEZPEČNOSTNÍ AUDIT

Je metoda přezkoumání bezpečnostní situace ve firmě, nebo systematický proces objektivního získávání a vyhodnocování důkazů, které se týkají takových činností v podniku, které je třeba zkoumat. Cílem je zjistit rozdíl mezi skutečným a požadovaným stavem bezpečnosti. Závěrem bezpečnostního auditu je poskytnout vedení společnosti výsledek auditu. Pokud se výsledek auditu neztotožňuje s bezpečnostní politikou firmy, je třeba navrhnout takový model, který organizaci zaručí její ochranu, a to ve všech oblastech, které organizace využívá. Dalším možným cílem bezpečnostního auditu je ukázat vedení firmy, že prostředky vložené na ochranu bezpečnosti organizace jsou v dostatečné míře využity.

2.1 Na základě výsledku auditu můžeme využít těchto modelů

2.1.1 Auditní osnova

Je to nejjednodušší vzor při provádění auditu, který obsahuje běžný seznam úkolů, které je třeba vykonat, a stanoven cíl, který má být auditem dosažen. [7]

2.1.2 Auditní model

V této fázi je zpracován reálný model situace v podniku, jak má vypadat, aby v konečné fázi a ve výsledku obstál „vyhovuje bez výhrad“. [7]

2.1.3 Auditní matrice

Je nejpřesnější stanovení úrovně bezpečnosti. V tomto modelu je zpracována přesná matrice, která nepřipouští sebemenší odchylky. Pokud se naleznou v konečné fázi nějaké, i sebemenší nejasnosti, tak v tomto modelu je označujeme „nevyhovuje“. Lze připustit, že po rychlém odstranění je výsledkem „vyhovuje bezpodmíněně“. Pokud vyhovuje plně „bez výhrad“ je zjištěn skutečný stav v tu danou chvíli, kdy je audit vykonáván. [7]

2.2 Druhy auditu

2.2.1 Externí audit

Tento audit vykonává na základě požadavku bezpečnostního managementu externí specializovaná firma, která se zabývá činností auditu komerční bezpečnosti. [5]

2.2.2 Interní audit

Je interní záležitostí firmy, kterou provádí bezpečnostní manažer firmy na základě podkladů poslední prověrky určité části podniku. Je třeba říci, že bezpečnostní audit nemůže vykonávat bezpečnostní manažer na úseku, který je bezprostředně pod jeho dohledem, nebo má nějaký vliv na jeho vedení. Pokud jde o jednodušší variantu auditu, je možné, že bezpečnostní manažer jmenuje jiného zaměstnance, který není spjat s konkrétním úsekem, a má dostatečné zkušenosti v oblasti bezpečnostních auditů, včetně návrhu konkrétních řešení. [5]

2.2.3 Komplexně bezpečnostní audit

Pokud je ve firmě nastavena bezpečnostní politika, je třeba provádět pravidelné kontroly již nastavených konkrétních opatření, zda stále odpovídají realitě a zdali jsou skutečně efektivní, a jsou-li správným způsobem naplňovány všechny cíle bezpečnostní politiky. Zaměřuje se na hrozby spojené s nastavenou bezpečnostní politikou a průběžně ověřuje, zda jsou navržená bezpečnostní opatření dostatečná a zda pokrývají všechny oblasti podniku, kterého se týkají. Další důležitou částí je ověření, je-li využití dostatečné, nebo naopak nadsazené. V obou případech je to špatně. V prvním případě je nedostatečná, a proto je třeba navrhnout řešení na vyšší zabezpečení bezpečnostní politiky firmy. Na druhou stranu to podnik může stát spoustu zbytečných financí, které by mohl investovat v jiné oblasti. Ale obecně je pravidlo takové, že i v této oblasti je lépe bezpečnostní politiku předimenzovat. [1],[5]

2.2.4 Specializovaný bezpečnostní audit

Je zaměřen na konkrétní činnosti v podniku. Na základě analýzy z předešlých kontrol se můžeme zaměřit právě na revizi těchto úseků v dané firmě a zjistit skutečný stav, který nám napoví v jaké pozici je na trhu a jestli nám nehrozí nějaké hrozby jak zvenčí, tak i uvnitř firmy. Můžeme je rozdělit na několik nejdůležitějších oblastí, u kterých je bezpečnostní audit nejvíce důležitý. Jsou to oblasti organizační, fyzické, personální, informační, požární bezpečnost, bezpečnost a ochrana zdraví při práci, atd. [5]

2.3 Oblasti bezpečnostního auditu

2.3.1 Organizační bezpečnost

V této oblasti se posuzuje kontinuita jednotlivých úseků firmy, které spolupracují s jinými celky podniku. Zkoumají, zda dané kompetence jsou v souladu s metodickými pokyny dané firmy, zkoumá funkčnost jednotlivých oddělení a to hlavně, zda je dostatečná komunikace mezi jednotlivými zaměstnanci, kde je komunikace mezi zaměstnanci třeba. [1] V neposlední řadě řeší systém vnitřních předpisů, jejich úplnost a hlavně provázanost v jednotlivých úsecích, kde je to nezbytně nutné [5]. Vychází z podmínek zadaných klientem s vazbou na charakter provozu respektive na typy činností, ke kterým je objekt využíván. Jedná se zejména o provozní dobu, oprávněnost osob ke vstupu, vjezd-výjezd vozidel, vnášení-vynášení materiálu apod.

2.3.2 Fyzická bezpečnost

Zde se prověřuje stav v oblasti fyzické bezpečnosti. Předmětem auditu je efektivnost uplatňování fyzické bezpečnosti [5]. Můžeme zde dělat revizi činnosti v oblasti kontroly vstupu na jednotlivá pracoviště, součástí jsou i pravidla pohybu osob v objektu. Na základě zjištěných skutečností je třeba nasazení odpovídajících režimových opatření.

Audit se může týkat oblastí:

- ochrana perimetru podniku a vytyčení možných hrozeb
- PZTS (poplachový zabezpečovací a tísňový systém)
- ESKV (systémy kontroly vstupu)
- EPS (elektrická požární signalizace)
- přístupové a docházkové systémy
- klíčový režim
- směrnice pro režim provozu
- krizový plán ochrany objektu [5]

V případě, že organizace nakládá s utajovanými informacemi, je povinna zabezpečit všechny objekty, kterých se to týká dle příslušné vyhlášky Národního bezpečnostního úřadu - NBÚ (č.339/1999 Sb.). Je třeba mít zpracovanou „Dokumentaci objektové bezpečnosti“. Dále je třeba, aby byl subjekt podroben bezpečnostní prověrce prováděné Národním

bezpečnostním úřadem. Velký význam je třeba dbát při manipulaci s osobními údaji, a tím předejít jejich zneužití.

2.3.3 Personální bezpečnost

V této oblasti je třeba brát na zřetel, že středem zájmu je člověk, nikoliv technika. K tomu slouží pravidelná kontrola splněných úkolů.

Představuje nejméně spolehlivý faktor bezpečnostního prostředí. Člověk, coby základní článek personální oblasti, je vysoce subjektivně ovlivnitelný, a tedy přirozeně nestabilní prvek. A v každodenní praxi nejsou v našem podnikatelském prostředí nijak neobvyklé snahy motivovat člověka k nekalému jednání ať už v podobě lákavé finanční nabídky („každý má svou cenu“), tak třeba i formou nátlaku (například vydíráním) [2]. Bezpečnost personální je možno metodicky členit do dvou relativně samostatných oblastí – do oblasti personálního výběru předpokladatelně vhodných osob a do oblasti personální práce s těmito osobami. [5]

Personální výběr vychází z kritérií požadovaných k výkonu činností na konkrétních pozicích. Rozhodujícím faktorem při něm je samozřejmě schopnost budoucího zaměstnance zastávat požadované pracovní povinnosti, včetně jeho osobnostní způsobilosti a bezúhonnosti.

Personální práce představuje především vstupní školení a následnou péči o další prohlubování nezbytných profesních znalostí, konkretizovanou v související dokumentaci s prokázáním nejen rozsahu a kvality odborné přípravy, výchozích pramenů, účasti školených zaměstnanců, ale i prokazatelné adekvátní odborné kvalifikace školitelů. Součástí personální práce je rovněž průběžné hodnocení a kontrola zaměstnanců, a to jak jejich získaných teoretických znalostí, tak i prakticky vykonávaných služebních povinností (včetně dokumentace s výsledky tohoto hodnocení, kterou si vedou nadřízení). [5]

V personální bezpečnosti může být audit zaměřený:

- na spolehlivost zaměstnanců
- na úroveň odborné přípravy zaměstnanců
- na jazykovou bariéru na pozicích, kde je to třeba (dá se např. řešit doškolením pracovníků a nabídnutím jazykových kurzů)
- na duplicitu pracovních pozic

Personální bezpečnost je výhradně součástí aktivit spadající pod řízení lidských zdrojů a proto je jasné, že se týká všech řídících a vedoucích pracovníků.

2.3.4 Logická bezpečnost

Zabývá se problémem zpracováním dat, jejich integrity, dostupnosti a důvěryhodnosti. K tomu využijeme nějaký software. Běžně se jedná o operační systém. V lepším případě slouží ke zpracování dat, která se např. využijí v personální činnosti. Je třeba zařídit její nedotknutelnost v rámci zneužití. Jelikož jde mnohdy o velmi citlivá „osobní" data, je třeba k nim zřídit přístup. V lepším případě charakterizovat pracovníky, kteří se mohou dostat k přístupu ke konkrétní databázi celého systému. [5]

2.3.5 Informační bezpečnost

Zde je opět třeba zdůraznit, že lidé jsou klíčovým faktorem při ochraně informací. Dá se říci, že v současné době je ochrana počítačových stanic a sítí na prvním místě ze všech oblastí, u kterých se koná bezpečnostní audit. Je to logické, je to technika, která jde neustále dopředu. A její viditelné zastavení v jejím rozvoji je takřka vyloučené. [3]

Proto na tuto fázi auditu je třeba brát významný zřetel. Musíme se zvláště při auditu soustředit na možnosti napadnutelnosti sítě jak zvenku, tak i zevnitř podniku.

Podniky mají za úkol:

- bezpečně zabezpečit veškerou manipulaci se všemi informacemi. Jedná se hlavně o informace typu státní, obchodní, bankovní a služební tajemství, ochrana osobních údajů. [5]
- veškeré své zaměstnance upozornit na zachování mlčenlivosti o skutečnostech, které by mohli poškodit jméno firmy. [5]

Součástí informační bezpečnosti je ochrana technických prostředků, které se využívají ke zpracování a následnému přenášení. Bezpečnostní politika v IT je obdobná, jako u všech ostatních. Proto je třeba, aby strategie ochrany byla stanovena v základním dokumentu, který je nedílnou potřebnou dokumentací při tvorbě auditu v této oblasti.

V této oblasti, stejně jako v jiné, je třeba stanovit určitá pravidla, opatření, přiřazení odpovědnosti jednotlivých pracovníků, jejich přístup např. na určité servery, sdílené disky, help desky. Hlavní úloha IT je zabezpečení sítě proti škodlivým vlivům. V rámci bezpečnostní

politiky je třeba brát velký důraz při bezpečnostním auditu na stáří jednotlivých technických počítačových komponentů, jako např. servery, počítačové pracovní stanice.

V oblasti IT bezpečnostních auditů můžeme především:

- analyzovat a určovat pracovníkům jejich přístupová práva do určitých částí IT systémů
- pravidla zálohování dat
- ochrana uložených dat
- ochrana dat při výpadku napájení
- zjištění bezpečnosti na úrovni vnitřní sítě (zabezpečení sítě, vedení a typy kabelů, rychlost sítě, uživatelská práva jednotlivých stanic, zabezpečení bezdrátových sítí)
- zjištění bezpečnosti z hlediska vnější sítě (kontrola rizik spojený se vzdáleným připojením do sítě „intranet nebo internet“, dále je třeba zjištění možného napadení sítě) [5]

Nejdůležitější částí informačního auditu je zjištění nedostatků při napadnutí IT systému. Toto se zjišťuje tzv. penetračním testem. Jeho snahou je vniknutí do informačního systému, zjištění co možná nejvíce možných děr a cest, kterou může být napaden. Tento test má svoje náležitosti a pravidla. Pokud je zadáván externí firmou, je třeba zaručit ochranu dat a to za účasti někoho z IT a společně zabezpečit bezpečný průběh testu, tzv. nepoškození dat. [3]

Komunikační bezpečnost, jako součást informačního auditu

V komunikační fázi auditu je třeba vzít v úvahu, že data jsou přenášena po síti a mohou být, pokud nebude síť dostatečně zabezpečena, napadena snadněji bez velkých obtíží neznámým útočníkem.

2.3.6 Požární bezpečnost

V rámci organizace provádí kontrolu odborně způsobilá osoba v požární ochraně, dle zákona ve smyslu dodržování podmínek požární bezpečnosti. Dohled nad dodržováním podmínek požární bezpečnosti provádí orgán státního požárního dozoru. Na rozdíl od předcházejících typů bezpečností, jsou ustanovení k požární ochraně závazná ve smyslu uvedených předpisů objekty na základě v nich provozovaných činností rozděleny na:

- objekty bez zvýšeného požárního nebezpečí (bez ZPN)

- objekty se zvýšeným požárním nebezpečím (se ZPN)
- objekty s vysokým požárním nebezpečím (s VPN)

Do požárního auditu můžeme zařadit kontrolu:

- systém požární ochrany
- kontrola prostředků požární ochrany - vyhrazených/nevyhrazených
- kontrola označení únikových cest a východů při mimořádných a krizových událostech
- bezpečnostní značky a značení
- volný přístup k prostředkům požární ochrany
- zpracování dokumentace dle požadavku zákona PO

2.3.7 Bezpečnost a ochrana zdraví při práci

Požadavky na bezpečnost a ochranu zdraví při práci (dále BOZP) jsou stanoveny zákonem, kde jsou obsaženy bezpečnostní požadavky na organizaci. Všichni zaměstnanci v rámci svých činností, musí tyto požadavky dodržovat. Celé spektrum bezpečnostních opatření tvořících systém BOZP je dáno riziky jednotlivých typů činností vykonávaných v rámci pracovního procesu.

Jedná se o čtyři kategorie souvisejících hodnocení rizik:

- kategorie pracovních rizik 1 - nejde o žádná podstatnější rizika ohrožující zaměstnance
- kategorie pracovních rizik 2 - přestavuje rizika přijatelná
- kategorie pracovních rizik 3 - se vztahuje k rizikům, jejichž omezení vyžaduje používat v průběhu pracovní doby osobní ochranné pracovní pomůcky (dále jen OOPP), v podmínkách bezpečnostních služeb mohou být do této kategorie zařazeni psovodi, případně pracovníci eskort doprovázejících peněžní či jiné významné zásilky.
- kategorie pracovních rizik 4 - týká se takových pracovních činností, u nichž může dojít i přes použití dosažitelných OOPP ke škodlivé expozici organismu, ať už vlivem fyzikálních (záření, vibrace), biologických, chemických, psychických či jiných druhů nadprahových zátěží.

BOZP můžeme rozdělit na 3 části:

1. kontrola systému řízení BOZP
2. kontrola stavu plnění v jednotlivých úsecích BOZP
3. přímá kontrola pracovišť, zvláště vedoucích pracovníků

Předmětem auditu je:

- bezpečnost a hygiena práce
- péče o technická zařízení a VTZ (vyhrazená technická vyhledávání a odstraňování zařízení)
- kontrola všech pracovišť
- kontrola a ověření správnosti dokumentů
- roční prověrka BOZP
- pracovně lékařská péče
- prevence rizik
- osobní ochranné pracovní pomůcky
- nebezpečné látky nacházející se na pracovišti
- školení zaměstnanců na všech stupních pracovní činnosti [5]

2.4 Druhy auditu z hlediska časového

2.4.1 Plánovaný audit

Audit, který se provádí v pravidelných předem domluvených časových intervalech. Interní i externí auditoři musí vědět v dostatečném předstihu termín auditu z důvodu prostudování bezpečnostní politiky organizace.

2.4.2 Mimořádný audit

Provádí se při mimořádné události ve firmě, jako například změna bezpečnostní politiky firmy, obměna bezpečnostního managementu, změna majitelů firmy, mimořádná obměna vedoucích pracovníků na důležitých pozicích z hlediska bezpečnosti.

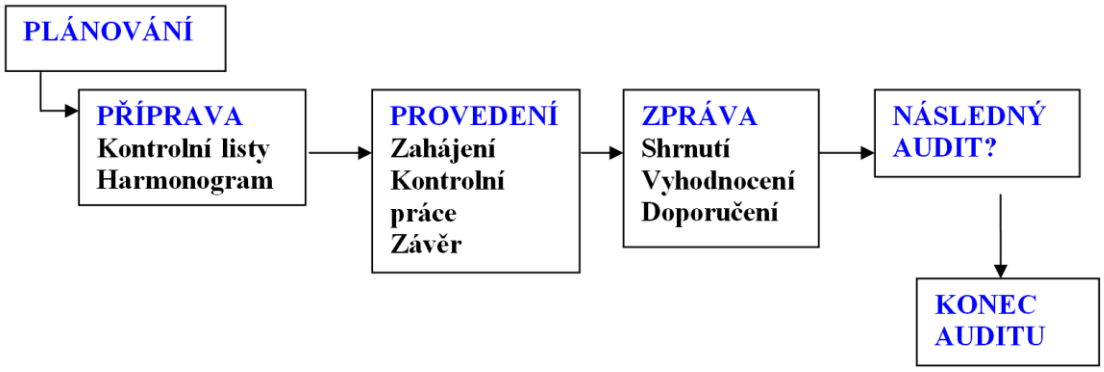
2.4.3 Následný audit

Tento audit se provádí na doporučení auditora, v případě, že plánovaný a mimořádný audit vykazoval nesrovnalosti s bezpečnostní politikou firmy [5]. Na základě zprávy z auditu, vydá auditor v závěrečné zprávě doporučení na sjednání nápravy.

3 PRŮBĚH AUDITU

3.1 Plánování auditu

V praxi se vykonává audit dle potřeb a požadavku firmy, proto není nikde stanoveno, v jakých časových intervalech se má audit opakovat. Pokud má firma více útvarů, je výhodnější dělat audit průběžně a mít přehled o možných rizikách, na základě závěru auditu a jeho vyhodnocení a návrhu řešení postupně bude odstraňovat díry v bezpečnosti organizace.



Obrázek č. 2: Organizační cyklus bezpečnosti [5]

3.2 Příprava auditu

Před samotným auditem je třeba mít jasno, kterých oblastí se bude bezpečnostní audit týkat. Zvážit, zda nemůže audit provést pracovník bezpečnostního managementu, bezpečnostní manažer, nebo někdo znalý problému auditů. Musí to být zaměstnanec, který nemá přímou vazbu na dění v úseku, který chceme kontrolovat. Toto je samozřejmě lepší varianta z hlediska možného úniku zásadních informací z firmy. U externí firmy, která se zabývá auditorskou činností, bude větší šance, že bude audit více objektivní a nasazení prostředku bude více transparentní.

Ve chvíli, kdy je jasné, kdo bude audit vykonávat, bude třeba, aby se seznámil s dostatečným předstihem s dokumenty a oblastí, kterou bude kontrolovat.

3.3 Příprava auditu obsahuje:

- určení auditorského týmu
- vypracování postupu na základě podnikových směrnic
- vyžádání dokumentace předchozích auditů (pokud se nějaké uskutečnili)
- vypracování harmonogramu
- zajištění přístupu na pracoviště, kde se bude konat audit [5]

3.3.1 Seznam náležitostí spojený s úvodní listinou

1. Identifikace

- název firmy, kde bude audit vykonán
- popis auditovaného objektu pracoviště
- auditované období
- termín realizace a stanovení konce auditu
- jméno vedoucího a členy auditu

2. Cíl auditu – tím je myšlen konkrétní plán, kterého má ve výsledku auditem docíleno

3. Postupy a techniky auditu

4. Časový harmonogram zpracování konečné auditní zprávy [5]

3.4 Zahájení auditu

Zahájení auditu začíná pohovorem, kterého se účastní:

- vedení auditovaného pracoviště společně s bezpečnostním manažerem
- auditor a celý jeho tým

Záměrem je:

- vysvětlit záměry, cíle celé akce a uklidnit všechny zúčastněné, hlavně z řad podniku, kde bude audit probíhat, že nejde např. o personální audit, a tím už na počátku stanovit a jasně definovat účel a proč se bude konat právě na tom konkrétním pracovišti.

- z důvodů časté neinformovanosti, je třeba i doladit s vedením firmy způsob oznámení i na dalších pracovištích z hlediska zbytečného, možného šíření tzv. nepravdivých zpráv.

Setkání je obvykle důvodem na doladění posledních nezbytných záležitostí mezi auditorem a vedoucími pracovníky, kde bude audit probíhat. O všem musí proběhnout zápis, který bude úvodním dokumentem a bude součástí bezpečnostního auditu. [5]

Dále je třeba systémově:

- určit jasně místa, kde bude audit probíhat, jakými způsoby
- organizačně zajistit plnění jednotlivých fází, jasně definovat skupiny, osoby, úkoly a pravomoce
- jako poslední se musí vymezit, v jakých hodinách bude audit probíhat (ve dne, v noci, za provozu, za účasti jen některých zaměstnanců) [5]

Jako poslední je třeba vymezit a určit implementované techniky, které budou jednotliví auditoři uplatňovat. Toto bývá součástí úvodního pohovoru, kde se jasně tyto techniky vymezí a nastaví tak, aby splnily svůj účel, tzv. dostálo se požadovaných výsledků.

3.5 Techniky auditorské práce

Při výběru metod a postupů auditu musí být použity takové techniky, které zabezpečí požadované výsledky.

3.5.1 Rozhovor (Interview)

Jde o nejběžnější část při auditech, která je zároveň nejúčinnější. Tato technika je mnohdy velmi obtížná, hlavně z důvodu obavy, že zaměstnanec odpoví něco, co by mohlo být pro podnik z hlediska osobních údajů nepříjemné a zneužitelné. Proto je třeba předem jasně vymezit před jeho provedením samotný obsah, otázky … např. bezpečnostním manažerem společně a auditorem, aby dotazy byly jen otázky týkající se skutečně záležitosti auditu.

3.5.2 Porovnání analýzy

Kontroluje během auditu odchylky, nebo neobvyklé situace.

3.5.3 Pozorování

Systematické sledování konkrétních činností. Jejím výsledkem je popis skutečností, ale i její vysvětlení. V této fázi se můžeme setkat s tzv. experimentem. Jde o pozorování, které provádíme za kontroly, nebo řízených podmínek, které jsou předem vymezené.

3.5.4 Analogie

Podstatou je srovnání. Jde o myšlenkový postup, při němž na základě shody některých znaků několika předmětů či jevů usuzujeme na přibližnou shodu i u ostatních předmětů nebo jevů či shody v ostatních znacích. [5]

3.5.5 Indukce a dedukce

Zde se na základě např. pozorovací analýzy mohou vyvodit obecné závěry na základě mnoha získaných poznatků. Dedukcí můžeme dojít od obecných ke konkrétnějším závěrům. [5]

3.5.6 Modelování

Jeho činností se vytváří zjednodušený obraz skutečnosti, který reprodukuje vlastnosti dané skutečnosti [5].

3.6 Oprávnění a povinnosti auditorů

Určitou samozřejmostí jsou určitá práva a povinnosti, které je třeba respektovat, bez kterých není možno audit realizovat. Mohou být vymezeny na základě domluvy, kde budou řádně sepsány vymezené pravomoci.

3.6.1 Oprávnění auditora

- je oprávněn navštěvovat v doprovodu zástupce společnosti nebo s členem auditní komise všechna pracoviště, která byla vymezena pro audit
- vyžádat si veškeré podklady týkající se auditu a pořizování jejich kopií, které může následně využít pouze v rámci auditu [5]
- vést pohovory se zaměstnanci

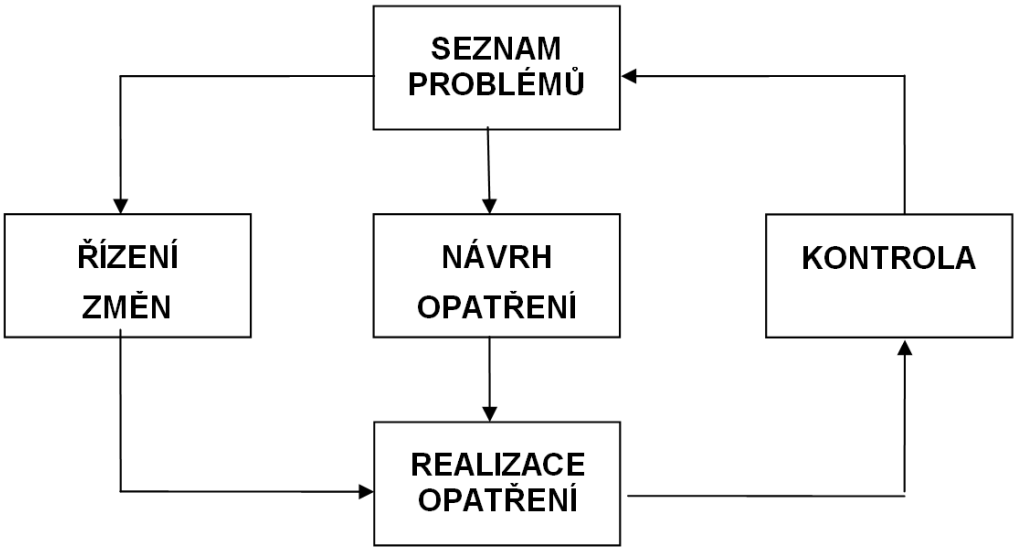
- provádět veškeré úkony podle metodiky vedení auditu, kde může využívat techniku a prostředky jako např. prověrka, inspekce a posuzování
- vyžádání veškeré technické a provozní dokumentace

3.6.2 Povinnosti auditora

- uskutečňování své činnosti podle předem nastaveného programu
- dodržování obecně platných předpisů (provozních a bezpečnostních)
- seznámit vedoucí jednotlivých pracovišť - účel, typ a účel auditu, jeho zahájení a ukončení
- při zjištění různých informací musí auditor zachovat mlčenlivost
- je povinen nezasahovat do výkonu práce jednotlivých pracovníků
- nesmí manipulovat se zařízením, které slouží ke každodenní činnosti pracovníků
- na základě dohody s vedoucím pracovníkem, je třeba respektovat pohyb a bezpečnost na pracovišti [5]

3.7 Postupy a zpracování závěrečné zprávy auditu

Po ukončení jednotlivých etap auditu je sestavena takzvaná předběžná zpráva, která není zprávou konečnou. V této fázi je třeba s výsledkem auditu seznámit auditované pracoviště a společně s auditorem na jeho doporučení, společně konzultují případné nedostatky. Po seznámení s obsahem je možné, aby se každá z osob, které se audit bezprostředně týká, k předběžné zprávě vyjádřila. Společně hledají řešení nápravy. Je třeba si uvědomit, že pokud by byla zpráva jako definitivní předána rovnou zadavateli, vedení, nebo majiteli organizace, byla by v tu chvíli pravděpodobnost spolupráce auditovaných osob daleko složitější. Obvykle si dá vedení organizace dobu, kdy je možné o zprávě diskutovat (obvykle 15-30 dní). Po tomto období auditor předá závěr auditu, včetně doporučení vedení podniku, který si audit vyžádal.



Obrázek č. 3: Návrh řízení procesu změn v systému bezpečnosti organizace [5]

3.7.1 Předpisy pro psaní konečné zprávy

- psát nejstručněji, tj. je třeba vyloučit nepotřebné informace a detaily, ale zároveň vypsat důrazně jasné nedostatky, které je třeba do zprávy dát na první místo
- používat jednoduchá slova, aby byla zpráva jasná a bez jakýchkoliv možných dvojsmyslných výkladů
- vyhnout se slovům, která by mohla auditované jakkoliv urazit
- je možné udělat změny na základě diskuze ke zprávě, pokud o ně auditovaní požádají

Je třeba věnovat pozornost:

- pravopisu
- obsahové i formální stránce zprávy
- logické struktuře zprávy

3.7.2 Obsah závěrečné zprávy

Konečná zpráva by měla obsahovat tyto části:

Obsah

- vnitřní ucelené členění zprávy

Úvodní část

- podstata provedené práce, jasně definováno pro adresáta zprávy
- druh auditu
- účastníci auditu
- kontaktní údaje
- použité postupy [5]

Posudek

- zde se uvádí seznam nedostatků, které byly zjištěny v průběhu auditu [5]

Doporučení

- jasná definice opatření k nápravě
- pokud jsou v doporučení zavedeny podstatné změny v bezpečnostním systému, musí být po realizaci opatření jejich následná kontrola mnohem častější

Povinností auditora je seznámit o výsledku závěrečné zprávy kontrolované organizační celky. Seznámení se zprávou a její převzetí potvrzují svým podpisem vedoucí pracovníci. [5]

3.7.3 Vyhodnocení auditu

Organizace by se měla z výsledku auditu poučit a řídit se plně doporučením auditora. Vedoucí pracovníci mohou pravidelnými kontrolami v určitém horizontu kontrolovat činnosti, které byly v průběhu auditu kontrolovány – analyzovány a navrhnout případně v rámci bezpečnostní politiky firmy jejich postupnou inovaci. K tomu dochází zvláště pří změně bezpečnostní politiky a navýšení jejích aktiv. Mnohdy si toho nemusí vedení podniku ani povšimnout. Pokud je v organizaci více změn, je třeba následný audit.

II. PRAKTICKÁ ČÁST

4 SEZNÁMENÍ S AUDITOVANOU FIRMOU

Pro svou bakalářskou práci jsem si vybral společnost, která se jako komplex zabývá činností spojenou s filmovým průmyslem. Vytváří podmínky pro filmové produkce k natáčení filmových projektů a reklamních spotů. Dále se zabývá pronájmem budov a kanceláří pro produkční společnosti.

Zadáním bakalářské práce bylo zpracování bezpečnostního auditu organizace. Jelikož se jedná o velký komplex, není možné do bakalářské práce obsáhnout veškeré činnosti, které se týkají bezpečnostní politiky firmy. V rámci ochrany celé firmy nebyly při auditu zpřístupněny některé z prostor, všechna data a informace. Tím tedy nebylo možné udělat komplexní audit celé firmy. Některá citlivá data nebylo možné zveřejnit. Proto jsem v rámci auditu vybral ve firmě dvě oblasti.

V první části se budu zabývat fyzickou ochranou vybraných částí areálu, společně s technickými prostředky ochrany. Pro druhou část jsem si vybral jeden z objektů, kde byl proveden v několika oblastech bezpečnostní audit.

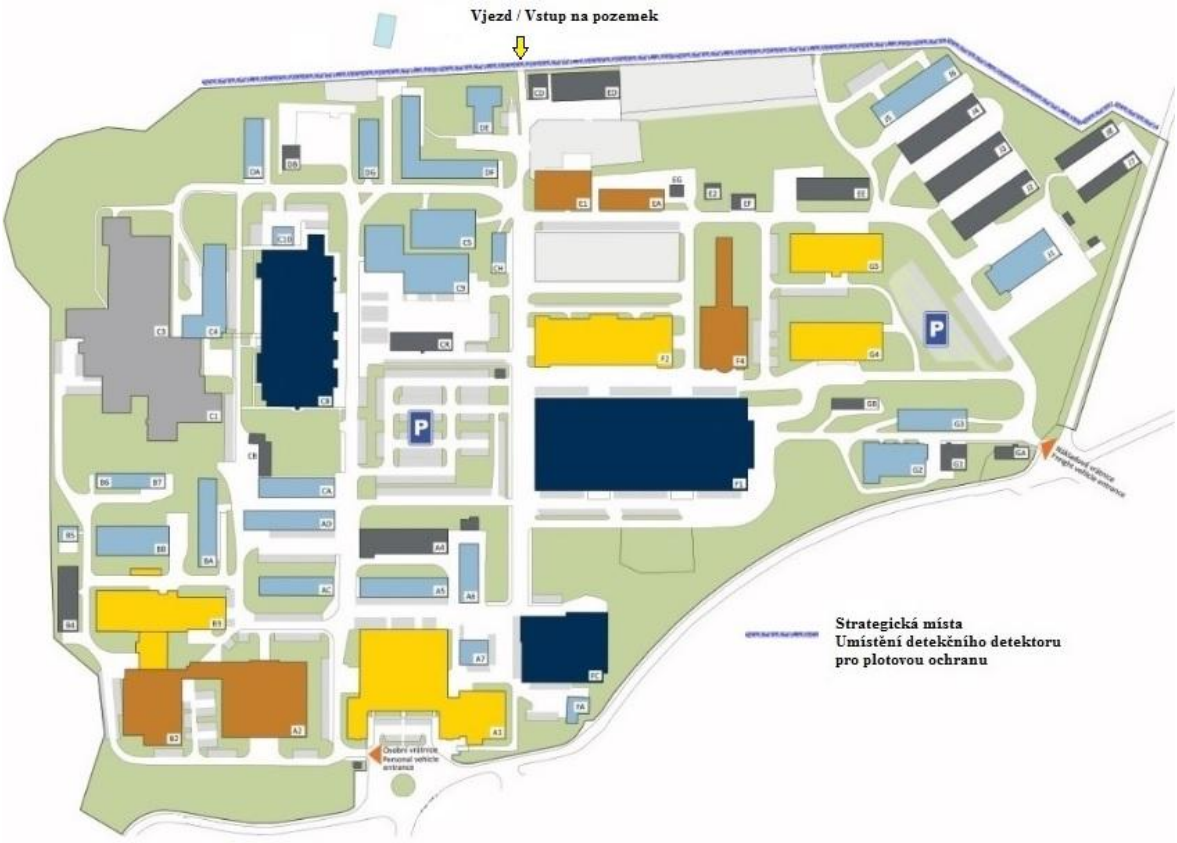
V době psaní bakalářské práce má firma cca 150 zaměstnanců. Firma je rozdělena na několik divizí. Jelikož jde o firmu středního typu, má své IT oddělení a bezpečnostního technika. Objekt, ve kterém jsem provedl bezpečnostní audit, má v době psaní práce 8 zaměstnanců interních a 3 externí nájemce.

5 AUDIT FYZICKÉ BEZPEČNOSTI V AREÁLU

V rámci celého areálu je třeba posoudit v rámci auditu jeho slabé stránky, včetně překonání barier a kontrolu osob pohybujících se po areálu, včetně režimového opatření celého areálu.

5.1 Základní seznámení s areálem

Areál a objekty jsou umístěny v klidnější části města v uzavřeném areálu s obvodovým oplocením a navýšeným ostnatým drátem. Ke vstupu do hlavní administrativní budovy slouží jeden osobní vchod s recepční službou zajišťovanou zaměstnanci společnosti. Do dalších prostor je nainstalován elektronický systém kontroly vstupu (ESKV). Všechny prostory v budově jsou přístupné až po splnění základních administrativních a bezpečnostních náležitostí na osobním vchodu s recepcí. Ke vstupu/výstupu osob, vjezdu/výjezdu vozidel z/do lokality slouží dvě vrátnice s fyzickou ostrahou a instalovaným vnějším uzavřeným televizním okruhem (CCTV). Lokalita není zajištěna kompletním elektronickým poplachovým zabezpečovacím a tísňovým systémem (PZTS). Objekty s určitou důležitostí jsou zajištěny lokálními PZTS s výstupy na dohledové a přijímací poplachové centrum (DPPC). Totéž se týká elektronického požárního systému (EPS). Charakteristická je v lokalitě velká frekvence pohybu osob v pondělí až pátek v době od 8:00 do 17:00 hodin.



Obrázek č. 4.: Plánek areálu [archiv autora, upraveno pro potřeby BC práce]

5.2 Perimetr areálu

5.2.1 Kontrolní propustková služba - vrátnice

Pro vstup/výstup a vjezd/výjezd do/z areálu je využíváno dvou vrátnic, z nichž jedna je definována jako nákladová - pro nákladní automobily a druhá jako osobní. V současné době je testováno v rámci vrátnicového vjezdu nové zabezpečení v rámci pohybu vozidel v celém komplexu areálu. Je jasně definováno, kde a za jakých podmínek budou vozidla parkovat. V rámci celého systému bude jasně definován každý vjezd automobilu. To se netýká jednorázových - občasných zákazníků. V rámci kamerového systému, který snímá každou ze značek, bude jasně definován konkrétní automobil. Pokud je v systému vozidlo nalogováno, je automaticky vpuštěno do areálu. Zaměstnanci externí bezpečnostní agentury (majitelem nebylo povoleno zveřejnění firmy, která zabezpečuje ve firmě bezpečnost) zajišťují zdvojení provozu tohoto systému při jeho nečinnosti. V jejich kompetenci je informovat zákazníky o možných komplikacích v areálu. Dále jsou nepřetržitě ve spojení s DPPC, aby mohli na případné mimořádné události ze svých pozic zasáhnout.

Uživatele vjezdového systému můžeme rozdělit do tří kategorií:

- zaměstnance
- stálé nájemce areálu
- jednorázové, občasné zákazníky

Zjištění

V testování nového systému vjezdu/výjezdu automobilu se ukázalo v rámci zadavatele projektu, že je vše v pořádku. V důsledku stále většího pohybu vozidel po celém areálu, to byla jedna ze zásadních investicí.

Doporučení

Vjezd/výjezd, vstup/výstup, do/z je zdvojen kontrolní propustkovou službou. Je proto třeba, aby bylo jednorázové a občasné zákazníky možné v areálu identifikovat. Proto je doporučeno při vjezdu do areálu tyto zákazníky vpustit jen po nahlášení SPZ, jména majitele vozidla a kontaktu – následně bude vpuštěn do areálu. Kontakt bude sloužit správě areálu např. při špatném parkování v areálu. Při opouštění areálu vozidlem, zaplacení příslušné částky v parkovacím automatu a průjezdu ven z areálu přes vrátnici se data v systému promažou. Při příštím vjezdu stejného vozidla bude probíhat stejný průběh. Dále bylo zjištěno, že zákazníci, kteří vchází do areálu, nejsou kontrolováni vůbec. Jedno z dalších doporučení je kontrola každého zákazníka, který vstupuje do areálu a jeho evidence do systému. Z hlediska snížení rychlosti jízdy automobilu v areálu, navrhuji montáž zpomalovacích pásu, tzv. retardérů.

5.2.2 Obvodová ochrana - plot

Z hlediska firmy je plot jedno z nejzranitelnějších míst celého areálu. Po téměř celém obvodu areálu je namontován plot. Plot je napnut a upevněn k pevným kovovým stojanům zapuštěných do betonu, na některých místech je kovový stojan zabetonován do sloupku. K vypnutí plotu slouží napínací drát umístěný ve spodní, střední a vrchní části. Plot je na některých místech 1 metr vysoký, někde 2 metry vysoký. Na některých místech je rozšířen o vrcholovou ochranu z jednoho až tří pramenů ostnatého drátu a to ve vodorovné rovině.

Obrázek č. 5.: Ukázka plotu z jedné části pozemku [archiv autora]

Doporučení

Sjednocení plotu na stejnou velikost 2 metrů po celém obvodu celého areálu a jeho vrchní část rozšířit o vrcholovou ochranu ze tří pramenů ostnatého drátu vykloněného o 45 stupňů z chráněného prostoru.

Vzhledem k velikosti areálu by bylo příliš nákladné např. rozšíření o některý z perimetrických systémů, jako např. detekčními kabely nebo senzorovými kabely. Nicméně na určitá strategická místa (naznačeno v plánku areálu, obrázek č.4) bych to doporučil. Jelikož je areál vybaven kamerovým systémem tak by to byla v kombinaci, např. s detekčním kabelem typu Umirs QUADROSENSE wire z hlediska bezpečnosti dobrá investice. Kabel je vysoce citlivý pro plotovou ochranu - koaxiální struktura vodičů (maximálně 250 m délky na každý alarmový vstup). Má extrémně nízký šum, odolnost vůči UV záření a má vysokou životnost. Dále bylo zjištěno, že část areálu není oplocena vůbec, kvůli častým výjezdům na další část pozemku (v mapce areálu je označen jako Vjezd/Vstup na pozemek). V tomto případě bych doporučil vyhotovení vrat s klíčem, kde by byla jasně definována režimová opatření v podobě klíčového režimu. Kamerový systém zde již nainstalován je. Nicméně bych doporučoval určitou část kolem nově opatřených vrat opatřit detekčním kabelem typu Umirs QUADROSENSE wire, který bude detekovat pohyb plotu. Při jeho přestřihnutí, narušení bude vyvolán poplach. V neposlední řadě bych detekční kabel rozšířil o meteostanici, která významně omezí falešné poplachy, které vznikají např. při velkém

větru. Detekční kabely jsou UV odolné -30°C až + 70°C, jejich cena se pohybuje okolo 130,- na běžný metr.

Obrázek č. 6.: Detekční kabel Umirs Quadrosense wire [12]

5.3 Kamerový systém

V rámci ochrany celého komplexu je na zranitelných místech nainstalován v areálu kamerový systém, který monitoruje pohyb vozidel a osob v areálu. Záznam z těchto kamer je posílán na dohledové a poplachové přijímací centrum - DPPC (dříve pult centralizované ochrany) nahráván na pásku a uchováván po dobu 10 dnů na úložném disku v serverovně IT oddělení pro případ potřeby dohledání záznamu. Ochrana podniku nezasahuje do veřejného prostranství. Na kamerový systém je vypracován projekt, který je pravidelně rozšiřován na základě změn v režimových opatřeních. Kamerový systém je rozšířen i na veřejné chodby objektů.

V areálu jsou nainstalovány jak kamery analogové, tak i IP kamery. Z analogových kamer od firmy Bosch je záznam přenášen po koaxiálních kabelech a následně přenášen do koncového zařízení, tj. převodníku na digitální signál, a dále je záznam ukládán na disk. Nicméně od analogových kamer se již v tuto chvíli ustupuje a přechází se pouze na digitální IP kamery. Analogové kamery se již v podstatě nechávají tzv. dosloužit. Informace o výskytu kamerového systému v rámci celého areálu se vyskytuje u vjezdu, formou velké informační tabule. Více rozšířeny jsou IP kamery, kde jejich signál komunikuje po síti a je

přímo po optickém kabelu veden do ústředny. Jelikož to není areál typu banka ani atomová elektrárna, neřeší se zde možná sabotáž kamer. Areál nevykazuje hrozbu terorismu, proto se ochrana kabelových tras a přemostění nehlídá. Nestandardní jevy v areálu jsou hlídány fyzickou ostrahou, která je zajištěna strážní službou. Z hlediska citlivosti a rozlišení jsou IP kamery instalovány v prostorách s horší viditelností. Jsou schopny veškerých operací, jako je digitalizace záznamu, kterou vykonává samotná kamera. Ovládání kamer, např. natáčení, je v kompetenci přímo pracovníků ostrahy na DPPC, kteří zajišťují jejich obsluhu. Napájecí systém je zálohován pro případ výpadku elektrické energie z hlavního zdroje.

Doporučení

Dle projektových plánů zhodnotit situaci a navrhnout rozšíření kamerového systému i do slabých míst a tím více zmapovat celý areál, zvláště ve spojitosti s perimetrem (plotem) celého obvodu areálu.

Fyzická ostraha objektu by si kromě teoretického zabezpečení měla vést i statistiku potencionálních útoků pachatelů na objekt. Vyhodnotit jejich možnou škodu a na základě toho posílit perimetrickou ochranu areálu o sledování kritických míst dalšími kamerovými a případně záznamovými či dohledovými prostředky, nebo řešit vhodnými opatřeními.

5.4 Fyzická ochrana

Fyzickou ochranu celého areálu zajišťuje externí firma a to nepřetržitě 24 hodin denně. V rámci ochrany podniku se neobejde fyzická ochrana bez technických prostředků a zároveň technické prostředky se neobejdou bez fyzické ochrany.

Činnosti, které v rámci areálu vykonává bezpečnostní firma

- kontrolní propustková služba
- zajištění bezpečnosti celého areálu
- kontrolní pochůzková činnost
- obsluha DPPC
- realizace zásahu při mimořádné události, na základě poplachu na DPPC
- výjezdová skupina
- požární asistence, požární hlídka
- klíčový režim

Povinnosti a kompetence pracovníků ostrahy (výtažek ze strážního řádu firmy)

- pracovník ostrahy lokalit s pracovním nasazením „strážný“ je při plnění pracovních úkolů přímo podřízen veliteli směny
- pracovník ostrahy lokalit s pracovním zařazením „velitel směny“ je při plnění pracovních úkolů přímo podřízen veliteli lokalit celého podniku

Tabulka č. 2.: Obsazení stanovišť

Stanoviště	Pracovní zařazení	Zaměst./směna	Obsazení
č. 1 osobní vrátnice	Strážný	1	Po – Ne nepřetržitě
	Strážný	1	Po – Pá 08.00 – 16.00
č. 2 nákladní vrátnice	Strážný	1	Po – Ne nepřetržitě
Autohlídka	Strážný	2	Po – Ne nepřetržitě
Dispečink	Velitel směny	1	Po – Ne nepřetržitě
Velitelství	Velitel ostrahy BS	1	Po – Pá dle potřeby 8,00 hod.

Tabulka č. 3.: Začátek a konec pracovní doby

Osobní /nákladní vrátnice	Zahájení směny	Ukončení směny
Ranní směna	07:00 hod.	19:00 hod.
Noční směna	19:00 hod.	07:00 hod.

Doporučení

Vzhledem k velikosti areálu, je třeba zvýšit pozornost pracovníků bezpečnostní agentury na jednotlivých stanovištích, tj. kontrola osob při vchodu do areálu, jejich evidence v systému. Co se týká plnění samotných úkolů zaměstnanců bezpečnostní agentury, které byly dohodnuty se zákazníkem, jsou v pořádku.

5.5 Objekty a kanceláře v nájmu

V pronajatých budovách a kancelářích je zabezpečovací systém montován jen na přání nájemce. Je na zvážení každého, jestli jeho aktiva je třeba nějakým způsobem chránit. Nicméně už jenom to, že má někdo v kanceláři PC s nějakými informacemi, je důvod se nad tím alespoň zamyslet. Po napojení CCTV, PZTS nebo ESKV je třeba napojení na pult, v tomto případě DPPC, kam se vysílají záznamy CCTV nebo signály o zastřežení objektu. V těchto případech jsou tu možnosti dvě. Za prvé si může zákazník nechat napojit některé z technických prostředků přímo na DPPC celé společnosti, nebo jsou zde další menší bezpečnostní agentury, které disponují též s DPPC a je tudíž možné, aby si zákazník vybral.

Doporučení

Bylo zjištěno, že pracovištěm DPPC je monitorována celá firma 24 hodin, což jsem zmiňoval již dříve. Některé z pronajímaných kanceláří a budov v areálu jsou napojeny z hlediska zabezpečení na externí, menší bezpečnostní agentury, kteří mají své zaměstnance na DPPC jen v určitém časovém rozpětí a signály o narušení si nechávají posílat přes GMS na mobilní telefony. V tomto případě se ukázalo, že toto je velmi nepraktické a mnoho případů, spojených s narušením objektu, i tak řeší hlavní dispečerské DPPC firmy. Navíc hlavní DPPC a ostraha je tímto značně přetížena.

6 AUDIT VE VYBRANÉM OBJEKTU

Budova objektu, která byla postavena v 70. letech 20. století, se skládá z tří pater a suterénních prostor. Součástí budovy je nákladová rampa, která je z hlediska bezpečnosti ohraničena řetězy. V budově jsou skladovací prostory, kanceláře a dílny. Budova dále disponuje dvěma nákladními výtahy.

6.1 Plášťová ochrana

Plášťová ochrana je řešena v suterénních a přízemních prostorách mřížemi na oknech budovy, které jsou montovány vždy 10 cm zvenku od okenního rámu. Vchodové celokovové dveře budovy jsou opatřeny bezpečnostní vložkou typu R1, skleněnou výplní, která je zabezpečena z vnější strany po celém obvodu skleněné výplně pevnou kovovou mříží. Vstup do vrchních pater a suterénních prostor je opatřen roletovou mříží, která prochází každoroční revizí.

Doporučení:

Z hlediska celkového dalšího technického zabezpečení je plášťová ochrana zabezpečena dostatečně. Ale jen v případě realizovatelných opatření v oblasti PZTS, která jsou uvedena v dalších kapitolách.

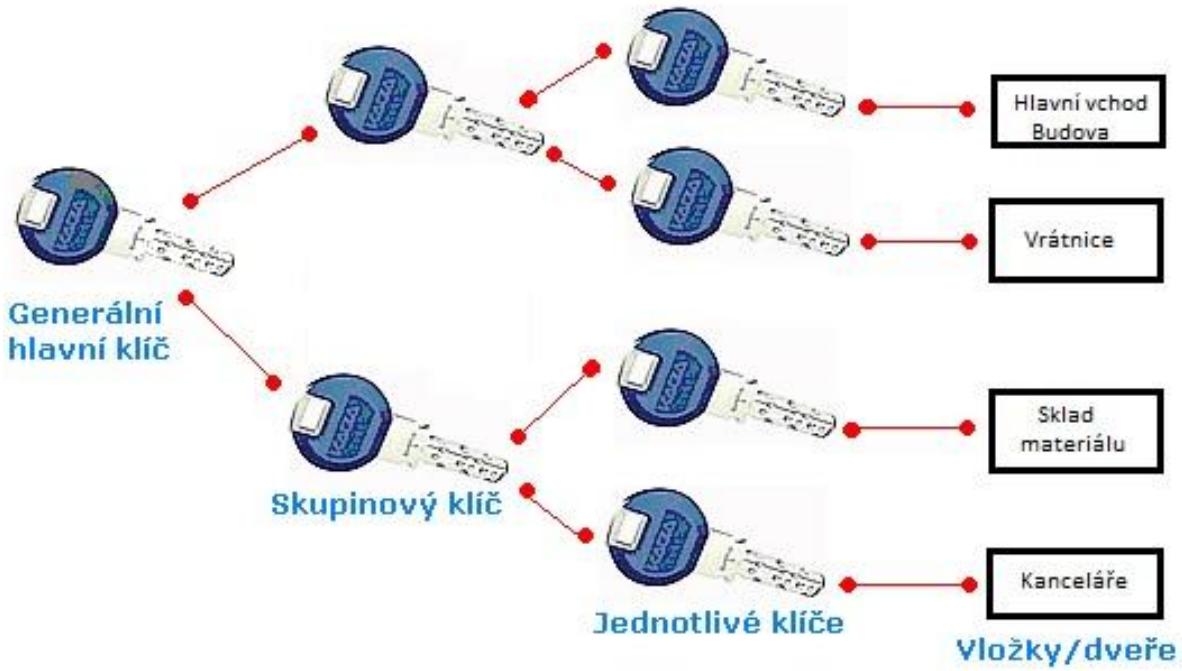
6.2 Klíčový režim

Zde je nastaveno jasné režimové opatření. Hlavní klíče od budovy mají všichni zaměstnanci pohybující se po budově. O tom je sepsán seznam „Seznam pracovníků vlastnících klíče od budovy a dalších prostor“. Součástí seznamu je datum předání klíče, jméno a příjmení zaměstnance a jeho podpis. Přidělení jednotlivých klíčů má v pravomoci vedoucí celého oddělení, který zároveň seznam aktualizuje. Při rozvázání pracovního poměru se zaměstnancem je ze seznamu vymazán, a zároveň je povinen všechny klíče od budovy a místností vrátit vedoucímu oddělení. Vedoucí pracovníci mají přístup téměř do všech prostor v budově a současně od téměř všech prostor mají klíče. Bohužel v budově není zaveden pro vedoucí pracovníky systém generálního klíče, proto všichni nosí potřebné klíče od všech místností u sebe. Na základě seznamu pracovníků a soupisu všech klíčů je vypracována obecná směrnice, která jasně definuje rozsah klíčového režimu. Změnou se nepřepisuje směrnice, ale aktualizuje se seznam pracovníků, nebo v soupisu všech klíčů jejich změna.

Hlavní vchod je zabezpečen bezpečnostní cylindrickou vložka značky FAB 100D - bezpečnostní třída BT2.

Doporučení

Dá se říci, že v tomto případě je klíčový režim závislý na systému vstupu. Pravidlo je takové, že kdo má přístupová práva do místností, které jsou opatřeny technickým opatřením, v tomto případě – pasivní infračervený detektor (PIR), magnetický kontakt, klávesnice, má přístup do skoro všech místností v objektu. To je přímo definováno v dokumentu „ Seznam pracovníků vlastnících klíče od budovy a dalších prostor“. Přiřazením příslušného kódu (který si každý zaměstnanec volí sám a s tím je spojena častá obměna hesla) při vstupu do prostor, má zároveň pravomoc se pohybovat po všech místnostech. Proto bych doporučoval v tomto případě, pro tyto pracovníky systém skupinového klíče, který je nastíněn na obrázku viz. - níže.



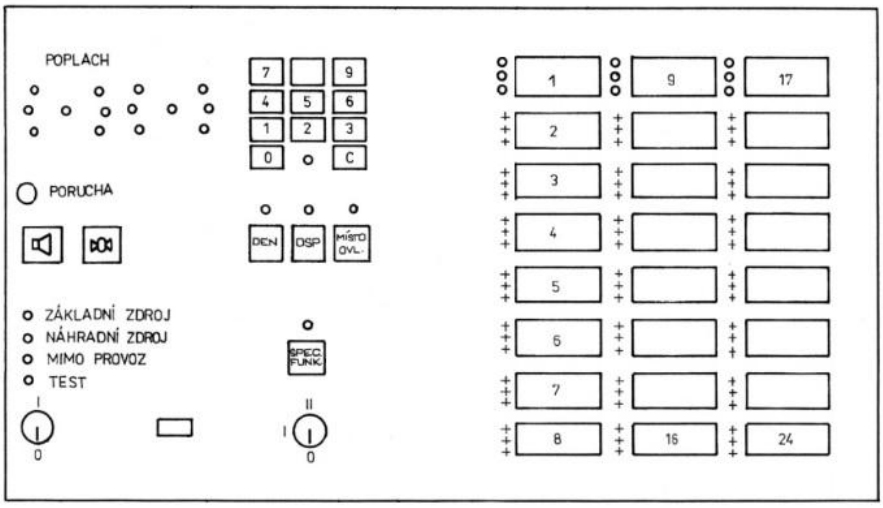
Obrázek č. 7.: Návrh systému režimového opatření [8, upraveno dle potřeb autora]

6.3 Elektrická požární signalizace (EPS)

Budova je zabezpečená jako celek elektrickou požární signalizací. Jelikož jde o budovu, kde má EPS velký význam, bude tato kapitola popsána podrobněji. Zařízení EPS je tuzem-

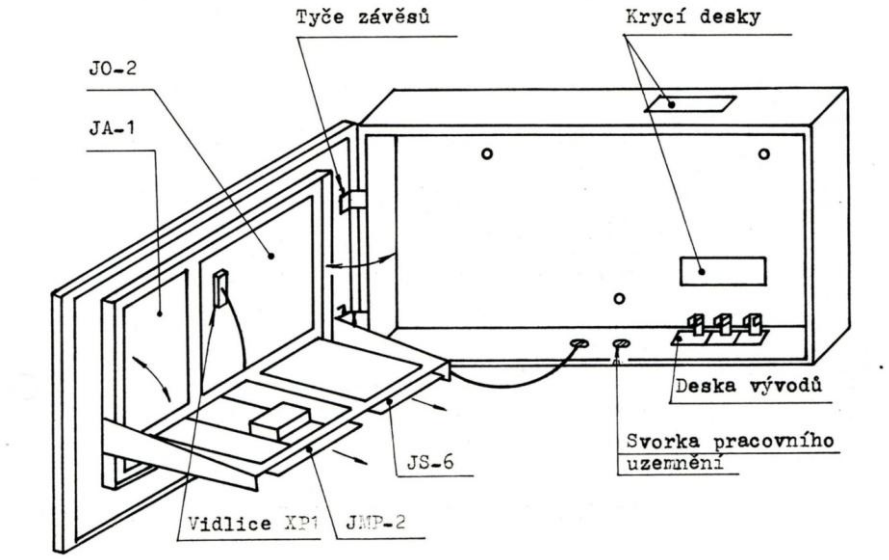
ské výroby TESLA Liberec. Systém je decentralizovaný a navazuje na zavedený systém v areálu od firmy TESLA Liberec.

Ústředny typu MHU 106 jsou umístěny v objektu skladu v přízemní místnosti naproti vrátnici. Signály o stavu jednotlivých smyček jsou přenášeny na tabla MHS 805, která jsou umístěna v místnosti ostrahy společně s DPPC.



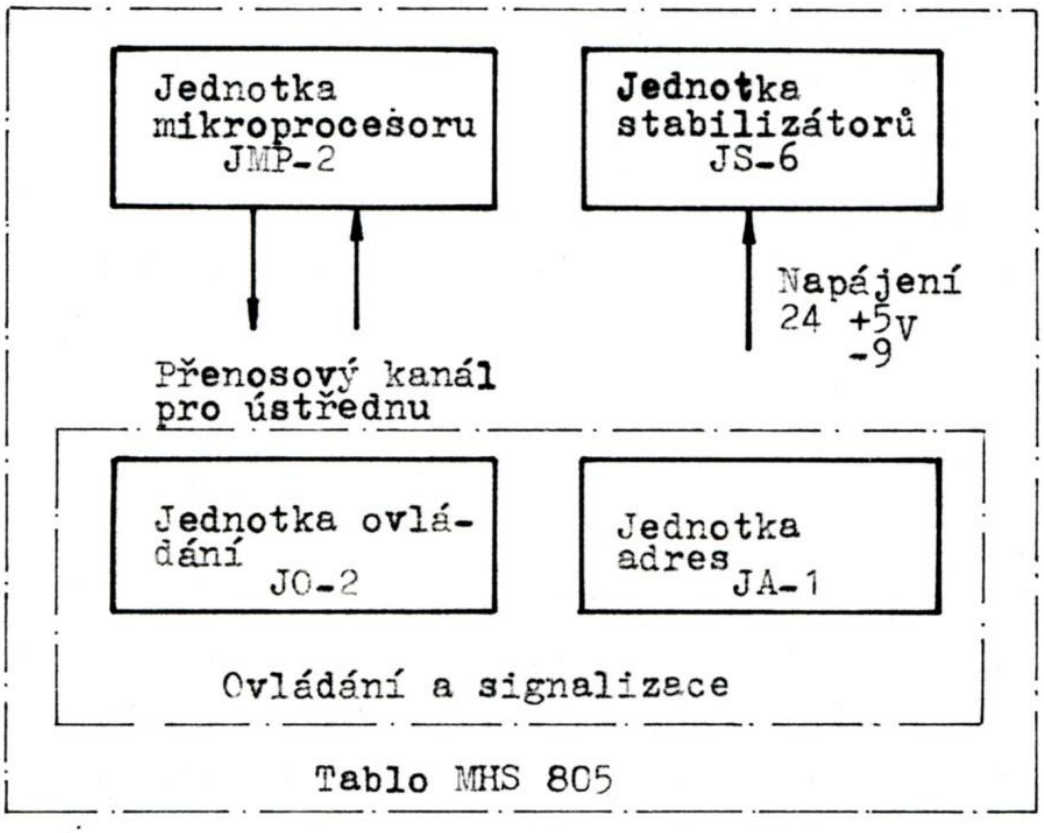
Obrázek č. 8: Vnější ovládání a signalizační prvky TABLA MHS 805

[13, upraveno dle potřeb autora]



Obrázek č. 9.: Pohled na tablo MHS 805 s otevřenými dveřmi

[13, upraveno dle potřeb autora]



Obrázek č. 10.: Blokové schéma tabla

[13, upraveno dle potřeb autora]

6.3.1 Napájecí napětí

Napájecí napětí ústředen je 220V a je přivedeno z hlavního rozvaděče objektu samostatně jištěným a v průběhu trasy neodpojitelným vedením. Náhradním zdrojem, který se zapíná automaticky při výpadku 220V je akumulátorová baterie, umístěná přímo pod ústřednou. Akumulátorová baterie je volně přístupna nepovolaným osobám, viz obrázek č. 11 a 12.

Obrázek č. 11.: Akumulátorová baterie, zavřená [archiv autora]

Obrázek č. 12.: Akumulátorová baterie, otevřená [archiv autora]

6.3.2 Kabelové rozvody

Hlavní stoupací vedení je provedeno kabely SYKFY 20×2×0,5. Kabely použité pro jednotlivé smyčky jsou SYKFY 5×2×0,5. Kabely jsou vedeny dle charakteru místnosti na roštech.

6.3.3 Typy signalizačních prvků

V prostorách celé budovy jsou namontovány hlásiče ionizační "MHG 181" a termodiferenciální "MHG 381". Hlásiče jsou umístěny v místnostech na stropech. Tyto hlásiče jsou opatřeny paralelními signalizačními svítidly MHY 104 umožňující rychlou orientaci osob provádějících preventivní prohlídku nebo zásah. Svítidla jsou umístěna vždy nad vstupy do

hlavních skladovacích prostor na každém patře. Svítidla od hlásičů umístěných ve strojovnách výtahů, jsou umístěna nad dveřmi nákladního výtahu v každém patře. Na únikových cestách, schodištích, chodbách a u vstupu do objektu jsou umístěny tlačítkové hlásiče požáru MHA 101 a MHA 102. Jsou umístěny v zorném poli unikajících osob ve výšce 140 cm nad podlahou.

Obrázek č. 13: Ionizační hlásič požáru M 181 [archiv autora]

Obrázek č. 14: Signalizační svítidlo MHY 104 [archiv autora]

Obrázek č. 15: Vnitřní tlačítkový hlásič požáru MHA 101 [archiv autora]

Obrázek č. 16: Venkovní tlačítkový hlásič požáru MHA 102 [archiv autora]

Ústředna typu MHU 106 prochází každý měsíc kontrolou. Hlásiče požáru se testují a kontrolují v pravidelných intervalech jednoho roku. K tomu je třeba zkušební hlavice MHU 506, která se pomocí redukce nasazuje na teleskopickou tyč GAR 290. V hlavici se používá zkušební plyn TEST Aerosol SOLO, který se při revizi zařízení vpustí do hlásiče

Obrázek č. 17 : Ústředna MHU 106 [archiv autora]

Obrázek č. 18.: Zkušební hlavice MHU 506 [9]

Obrázek č. 19.: Teleskopická tyč GAR 290 [10]

Obrázek č. 20.: Redukce k MHU 506 [11]

Zjištění

Systém je již zastaralý, nicméně funkční. Kontroly hlásičů probíhají v pravidelných ročních intervalech. Kontrola ústředny MHU 106 probíhá v horizontu jednoho měsíce interními zaměstnanci.

Doporučení

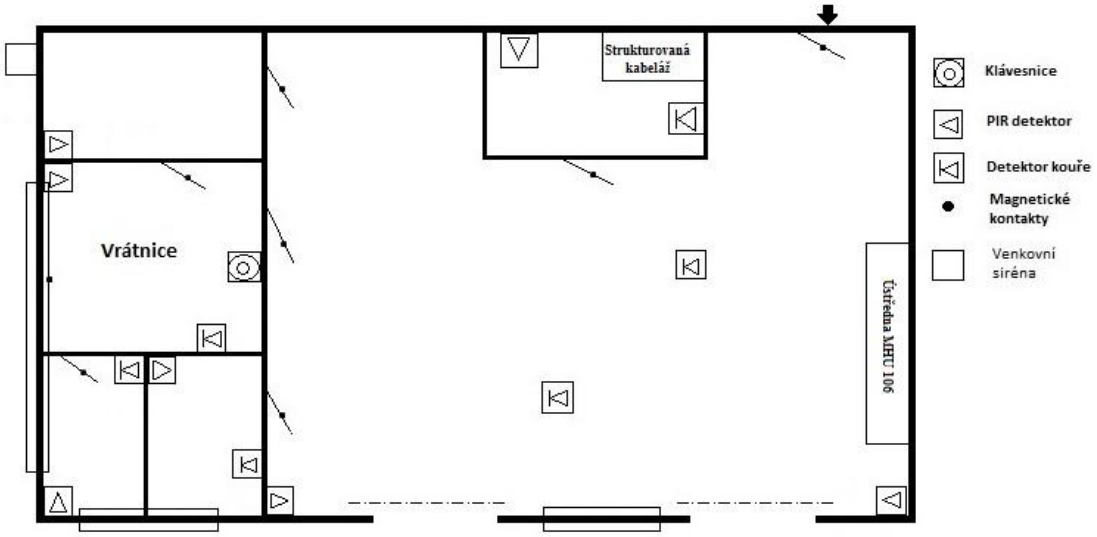
Testování proběhlo v pořádku. Některé z hlásičů po testu zkušebním plynem musely být vyměněny. Z důvodů už špatně sehnatelných náhradních dílů z hlediska bezpečnosti a důležitosti maximálního zabezpečení této budovy, doporučuji výměnu za novější typy hlásičů. Doporučuji instalaci nových opticko-kouřových a teplotních hlásičů požáru od výrobce Tyco. V případě opticko-kouřového hlásiče doporučuji detektor 601P, který je schopen detekovat viditelný kouř, který produkují materiály, které hoří velmi pomalu, nebo při hoření doutnají (nábytek, plastické hmoty). Detektor je vhodný instalovat, kde hrozí přehřátí elektrických instalací. Konstrukce a řídící elektronika je odolná vůči falešným poplachům, které mohou být způsobeny prachem. V případě teplotního hlásiče doporučuji typ 601H-R (fixní teplota 58°C), který je určen k detekci prudkého nárůstu teploty. Pracuje na principu vyhodnocování rychlosti nárůstu teploty, na které reaguje detektor svitu LED diody a překlopením relé. [15] Z hlediska bezpečnosti je momentální umístění akumulátorové baterie ústředny na veřejně přístupném místě naprosto nepřípustná. Umístění akumulátorových baterii pod ústřednou je třeba umístit do uzamykající místnosti. V tomto případě ideální do místnosti kde je strukturovaní kabeláž. V době psaní bakalářské práce probíhá revize stávajících komponentů, a to hlavně hlásičů.

6.4 Poplachový zabezpečovací a tísňový systém (PZTS)

Je to jedna z budov celého areálu, kde je PZTS zabezpečena komplexně. Budovu je třeba rozdělit na skladovou část, administrativní kanceláře, dílenské prostory, vrátnici. Na obrázku č. 21 je znázorněno schéma PZTS z jedné z částí přízemních prostor.

Prvky obsažené v budově

- PIR detektory
- magnetické kontakty
- kabeláž
- klávesnice
- ústředna



Obrázek č. 21.: Schéma PZTS [archiv autora]

Obrázek č. 22 : PIR detektor [archiv autora]

Obrázek č. 23 : Ovládací prvek – klávesnice [archiv autora]

Dveře vrátnice jsou osazeny magnetickým kontaktem. Dalším zabezpečením vrátnicového prostoru je PIR detektor, který snímá narušitele. Klávesnice je umístěna za dveřmi kanceláře. Jak již bylo zmíněno, okno vrátnice je opatřeno venkovní mříží, která je zabetonovaná ve vzdálenosti 10 cm zvenčí od okenního rámu. Okno je zabezpečeno magnetickým kontaktem. Součástí tohoto zabezpečení je venkovní siréna, která se spustí po časové prodlevě nečinnosti při kódování klávesnice.

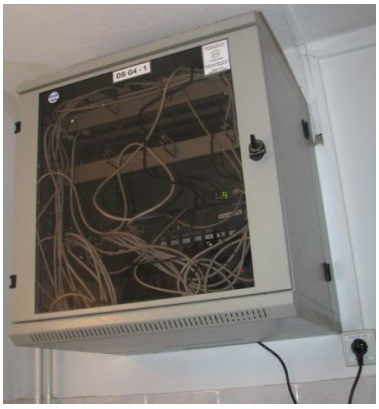
Obrázek č. 24: Venkovní siréna [archiv autora]

V přízemí budovy se nachází dva skladovací prostory spojené s administrativní kanceláří, které jsou z hlediska zabezpečení zabezpečeny stejně. Jen je zde použito více PIR detektorů pohybu ve skladovacích prostorách a jeden PIR detektor v kanceláři, který je namířen na okno kanceláře. Klávesnice je pro odkódování a zakódování v ideální vzdálenosti od vchodových dveří skladu.

Suterénní prostor, 1. patro a 2. patro jsou zabezpečeny také PIR detektory pohybu, které jsou ovládány z vrátnice, případně paralelně z administrativní kanceláře. Skladovací prostory v 1. a 2. patře jsou po stranách opatřeny únikovými východy - kovové dveře, venkovní podesta - žebřík. Klíče od těchto dveří jsou umístěny na veřejně přístupném místě z vnitřní části budovy, hned vedle dveří v malé skříňce. Malá skříňka je uzamčena a opatřena zpředu sklem a zámkem. Vstupy těchto dveří jsou zabezpečeny PIR detektory pohybu a magnetickým kontaktem. Ovládací prvek je klávesnice, která je umístěna ve vrátnici budovy a paralelně opět v jedné z kanceláří odkud je ovládán. Venkovní část na straně bočních únikových východů je chráněna z obou stran kamerovým systémem.

6.4.1 Kabeláž

Od PIR detektoru ke klávesnicím a od klávesnic k ústředně je použito tzv. UTP kabelů. Signál o zakódování, odkódování, případné sabotáži z klávesnice a ústředny, je přenášen dále po telefonní analogové lince na DPPC. Na obrazovce má dispečink v DPPC rozlišené informace o zabezpečení následujícími barvami zelená-zakódováno, červená-odkódováno, šedivá-nezapojeno, tj. momentálně odpojeno od provozu, žlutá-sabotáž, tj. začne probliká-vat a spustí se zároveň na DPPC siréna o narušení objektu. Několikrát denně je pevná linka na ústřednu kontrolována pomocí tzv. impulsu s nutnou zpětnou reakcí zpět na DPPC.



Obrázek č. 25 : Strukturovaná kabeláž [archiv autora]

6.4.2 Režimová opatření

Přístup do těchto prostor nemají všichni zaměstnanci objektu. Je zavedený přísný režim otevírání zabezpečených prostor podle jasného harmonogramu, kdy každá z odpovědných osob má sama zvolený bezpečnostní kód, který je navolen na každou z klávesnic s pracov-níkem servisní firmy a dále předány informace na DPPC. Ten je na DPPC hlášen pouze dle čísla např. 1- př. 1-Novák-XXXXXX. Tj. na DPPC se rozsvítí zelený signál zaměstnance č. 1, který právě zakódoval.

Zjištění

Na PZTS dříve EZS nejsou žádné technické plány. V současné chvíli při psaní bakalářské práce probíhá revize, kontrola stávajícího zabezpečení. V testování systému, při kterém jsem byl přítomen společně s pracovníkem DPPC byla ověřena funkčnost systému. Při průchodu mezi sklady, při zabezpečení hlavních dveří skladu (zamčeny), kde je magnetic-

ký kontakt se automaticky spustila venkovní siréna a poplach byl zaznamenán na DPPC, po odkódování se siréna vypnula. O sabotáži byl udělán zápis s pracovníkem DPPC.

Doporučení

Dodání chybějících technických plánů na celý objekt v oblasti PZTS. Navrhuji lepší zabezpečení bočních únikových východů např. otřesovými čidly, na všechna okna kanceláří v přízemních prostorách by byla vhodná instalace kontaktních detektorů tříštění skla, které se umísťují přímo na sklo a zachycují každý abnormální otřes. Jelikož se v jedné z dílen pracuje s vysokotlakovými láhvemi a svařuje se zde, doporučuji montáž detektoru úniku plynu typu SINDA CG 102, který díky citlivým senzorům velmi rychle reaguje na přítomnost nebezpečných plynů, jako např. metan, propan, butan, acetylen. Bezpečné napájení 12V umožňuje napojení detektoru do systému centrálního zabezpečení EPS a PZTS. Detektor obsahuje sirénu pro zvukovou signalizaci při překročení koncentrace plynu. Doporučuji také pořízení tísňového tlačítka do kanceláře vrátnice pro případné vyvolání mimořádné události na DPPC. Navrhuji drátové tísňové tlačítko s aretací PB68, které je propojitelné se zabezpečovací ústřednou. Po stisku zůstává stlačené do doby odemčení resetovacím klíčkem.

Obrázek č. 26.: Drátové tísňové tlačítko s aretací PB68 [14]

6.5 Požární ochrana (PO)

Jak již bylo popsáno technické zabezpečení PO je řešeno formou EPS. V budově se nachází další prostředky včasného zásahu při mimořádné události, v našem případě požáru, požární hydranty, které se nachází na každém patře dva. Dále se na každém patře nachází celkem 6 hydrantů, které jsou umístěné vždy před vstupem do skladovacích prostor.

Typy stabilně instalovaných hasicích přístrojů v budově:

Pěnový hasicí přístroj

Kontrola probíhá 1x za rok, hasicí přístroj je opatřen samolepkou o této informaci, tlaková zkouška probíhá 1x za pět let a je opatřena samolepkou, který na přístroj lepí revizní požární technik. V případě této budovy provádí tlakové zkoušky a revizi požární technik firma Horelica.

Vodní hasicí přístroj

Jelikož s tímto typem hasicího přístroje není možné hasit v blízkosti elektrického zařízení, je v prostorách auditované budovy skoro nevyužitelný. Kontrola probíhá 1x za rok, hasicí přístroj je opatřen samolepkou o této informaci, tlaková zkouška probíhá 1x za tři roky a je opatřen samolepkou, který na přístroj lepí revizní požární technik.

Práškový hasicí přístroj

Jelikož se tento typ hasicího přístroje používá mimo jiné i na elektrická zařízení, je v této budově využíván nejvíce. Kontrola probíhá 1x za rok, hasicí přístroj je opatřen samolepkou o této informaci, tlaková zkouška probíhá 1x za pět let a opatřena samolepkou, který na přístroj lepí revizní požární technik.

Obrázek č. 27 : Hasicí přístroje [archiv autora]

Požární hydrant

Kontrola probíhá 1x za rok, hasicí přístroj je opatřen samolepkou o této informaci, tlaková zkouška probíhá 1x za pět let a opatřena samolepkou, který na přístroj lepí revizní požární technik.

Obrázek č. 28 : Požární hydrant [archiv autora]

V prostorách mezi jednotlivými sklady jsou prostupy vycpány protipožárním sáčkem na grafitové bázi – Intumex PS 300, který slouží k rychlému bezprašnému zatěsnění prostoru. Je určen pro aplikaci do stěn a stropů. Snižuje riziko šíření kouře a ohně. Jelikož jsem byl u testování těchto protipožárních sáčku, tak mohu potvrdit, že jsou plně dostačující na vycpání prostupů a skutečně zabraňují dalšímu šíření požáru. Vstupní dveře do skladovacích prostor jsou na každém patře opatřeny plechy po celé ploše z obou stran, čímž zvyšující odolnost proti šíření případného požáru.

Obrázek č. 29 : Prostup skladovacích prostor Intumex PS [archiv autora]

6.5.1 Revize a kontrola přístrojů

Na všechny typy hydrantů probíhá pravidelný servis a kontrola externí firmou. Každé ze zařízení je opatřeno plombou a revizním štítkem a s informací, kdo revizi prováděl a za jak

dlouho musí proběhnout další. O revizích a kontrolách je sepsán záznam s termínem další kontroly, u hydrantů pravidelné tlakové zkoušky (informace o jednotlivých typech zařízení, viz úvod kapitoly 6.5). Záznam je uložen u bezpečnostního technika, který hlídá další nutné revize a kontroly.

6.5.2 Školení zaměstnanců

Jak jsem již uvedl v úvodu praktické části, firma má svého bezpečnostního technika, který zajišťuje mimo jiné školení zaměstnanců v oblasti PO. V budově je zvolena 3členná hlídka z řad středního a nižšího managementu. Z 3členné požární hlídky je zvolen jeden velitel a dva členové požární hlídky, kteří jsou každým rokem proškoleni bezpečnostním technikem v PO. O školení je vytvořen záznam s podpisy všech účastníků školení.

Doporučení

V této oblasti nebyly zjištěny žádné významné - zásadní závady pro činnost a bezpečnost firmy. Revize, kontroly a tlakové zkoušky probíhají v pravidelných termínech a to vždy s měsíčním předstihem – osobně prověřena skutečnost (dle informace záznamu z protokolu požárního technika a štítku na hasicích přístrojích). Kontrola pěnového hasicího přístroje proběhla i po praktické stránce, vše v pořádku. Ale je nutné vytknout, že v budově v době psaní bakalářské práce chybí směrnice požární ochrany, kde je mimo jiné nutné vypsat veškeré důležité kontakty, včetně základních informací pro ostatní zaměstnance a zákazníky budovy. V příloze je vytvořen návrh požární poplachové směrnice a to jak v české tak i anglické verzi.

6.6 Bezpečnost a ochrana zdraví při práci

Jak již bylo zmíněno v úvodu praktické části a minulé kapitole, firma má svého bezpečnostního technika, který má za úkol pravidelná školení všech zaměstnanců firmy. Vede důkladnou evidenci všech zaměstnanců a dohlíží nad jejich včasné proškolení z hlediska BOZP.

Bezpečnostní technik v rámci BOZP ve firmě zajišťuje:

- průběžné školení BOZP a na všech stupních (provozech)
- zajišťuje školení nově příchozích zaměstnanců
- školení pro provoz v nákladním výtahu
- zajišťuje a vytváří tvorbu směrnic

- konzultuje bezpečnostní situaci, v rámci změn v podniku vytváří bezpečnostní opatření
- prochází pravidelně pracovištěm a vedoucí zaměstnance upozorňuje na nedostatky
- kontroluje umístění lékárniček na místech tomu určených
- eviduje knihu všech pracovních úrazů v rámci celé organizace (veškeré pracovní úrazy v rámci auditovaného objektu jsou sepisovány do knihy úrazů, následně předány písemně bezpečnostnímu technikovi)
- zajišťuje školení na referenční vozidla

O všech školeních je společně se všemi zúčastněnými vytvořen záznam s podpisy a s termínem dalšího školení.

Jak jsem již uvedl, v budově je dílna, kde se sváří hořlavými látkami. Na dveřích dílny a budovy je umístěna cedule s informací o jaké typy plynů jde a v jakém množství. Pokud se svařuje, v rámci budovy v místě ne tomu určeném, je třeba o tom sepsat protokol - zajišťuje bezpečnostní technik. V době sváření a nejméně po dobu osmi hodin od konce svařování je potřeba, aby byla přítomna požární hlídka – funguje, osobně prověřeno.

Doporučení

Školení zaměstnanců probíhá v pravidelných termínech. Nicméně nikde v budově nejsou vyvěšeny aktuální směrnice BOZP, což je z mého hlediska závažné pochybení. Je nutné, z hlediska bezpečnosti označit vždy první a poslední schod tučně viditelnou žlutou čárou, nebo žlutou páskou.

6.7 Informační bezpečnost

Jedna z nejdůležitějších oblastí bezpečnosti každé firmy je bezpečnost informačních systémů a informační a komunikační technologie (IS/ICT). Je to taky jedna z nejrizikovějších oblastí ochrany firmy, zejména z hlediska jejich aktiv a informací. Důležitá je především hodnota hardware, hlavně serverového a vlastních dat firmy. Toto je určující pro míru zabezpečení.

Budova je z hlediska IT rozdělena na dvě části, a to na administrativní pracoviště a skladové pracoviště. Během auditu byla přezkoumána oblast a zabezpečení serverovny, ochrana dat, práva uživatelů, hesla a zabezpečení PC, pracovní stanice, internet.

6.7.1 Servery a jejich fyzické zabezpečení

V této oblasti je nutné rozdělit ochranu zabezpečení na ochranu proti fyzikálním vlivům a na zaměření lidského faktoru, který může být zdrojem škod jak úmyslně, tak neúmyslně.

Veškeré servery, využívající auditovaná budova jsou umístěny v hlavní administrativní budově, kde sídlí IT oddělení. Pro servery je vyčleněná jedna místnost, která je řádně označena. Do serverovny, mají vstup pouze uživatelé IT oddělení, pověřená osoba ze správy areálu a úklidová firma, dle přesně vymezených režimových opatření. Místnost je klimatizovaná, teplota je nastavena mezi 15 °C - 17 °C. Ochrana serverovny je z hlediska EPS napojena na stávající vedení celé budovy. Místnost je zabezpečena z hlediska EPS dvěma hlásiči. První reaguje na změnu teploty pro případ poruchy klimatizačního systému, druhý hlásič reaguje na oheň a kouř. Hlásiče mají samostatný okruh, kde následná informace o případné mimořádné události je posílána přímo na tablo, které je umístěno v místnosti ostrahy DPPC. Místnost je zabezpečena PIR detektorem pohybu a na dveřích a rámu je umístěn magnetický kontakt. Ovládacím prvkem je klávesnice. Informace o vstupech a kolísání teploty je přenášen na DPPC. Celá serverovna je napojena na záložní UPS, kvůli nenadálému výpadku elektrického proudu, který je umístěn v jiné místnosti, která je zabezpečena z hlediska EPS a PZTS obdobně.

Doporučení

Z hlediska fyzického zabezpečení je serverovna zabezpečena na dostačující úrovni. Nicméně, opět chybí detailní zpracování směrnic. Je zpracováno pouze režimové opatření na přístup do místnosti. Není zpracován plán mimořádných událostí pro případ požáru a není zpracován plán celého hardwarového rozmístění celé serverovny, včetně rozmístění kabeláže. Některá kabeláž nebyla řádně označena a tím je celá serverovna dosti nepřehledné.

6.7.2 Ochrana dat

Ochrana dat je jedna z nejkomplikovanějších oblastí celé IT bezpečnosti. Jejich ztráta, nedostupnost může mít z hlediska uživatelů pracovních stanic nedozírné následky. V této oblasti byl audit ve firmě zaměřen na pracovní stanice a diskové pole. U všech sdílených disků, probíhá zálohování vždy jednou denně v určitou noční hodinu. Na některých sdílených discích probíhá záloha jen u určitých důležitých složek.

Každá pracovní stanice má své interní úložiště, v podobě interních harddisků propojených SATA kabelem. Dále má každý uživatel – zaměstnanec v síti zaveden tzv. svůj odkládací prostor, tj. určitou vymezenou část na jednom z lokálních disků, kam si může, ukládat datově malé zálohy, jako jsou např. dokumenty. Většina pracovníků používá pro ukládání dat přenosné flash disky s kapacitou max. 16GB. Dále zaměstnanci využívají přenosná externí zařízení WD Elements Desktop 2000GB, na ukládání dat kapacitou 2TB. Zaměstnanci mají zakázáno tyto externí zařízení s firemními daty odnášet mimo firmu. V současné době se již ve firmě upustilo od ukládání dat na optické disky CD, DVD, CD-RW, DVD-RW. Vedoucí zaměstnanci proškolují své podřízené v oblasti ochrany dat a upozorňují na nutnost vytváření častých záloh.

Doporučení

Ochrana dat v rámci oddělení – budovy je na dobré úrovni. Zaměstnanci a IT oddělení dělají pravidelné zálohy. Sdílené lokální disky ve velikosti obvykle 1.6 TB, jsou zálohovány jednou denně v nočních hodinách. Nejsou vytvořena jasná pravidla pro zaměstnance. IT oddělní, resp. správce sítě musí vytvořit směrnice v oblasti ochrany dat a poté s nimi seznámit všechny zaměstnance. Vidím jako velkou výhodu, že bylo upuštěno od ukládání dat na optická média. Jejich poruchovost má vysoké procento, zvláště v horizontu několika let. Existují programy typu Nero, které po vypálení zkontrolují nahrané stopy a jejich čitelnost. Nastavení práv uživatelů v tomto případě neříká, na kterých stanicích je možno s paměťovými médii pracovat. Je třeba se zamyslet, na které stanici je třeba zamezit úniku dat, možné napadení a komunikaci přes externí zařízení zcela zakázat a využívat pouze sdílených lokálních disků.

6.7.3 Práva uživatelů

Práva a přístupy jednotlivých pracovníků jsou rozdělena na základě rozdělených a přiřazených kompetencí hardware a software (HW/SW) IT oddělením. Auditem jsem zjistil, že práva uživatelů nejsou přesně vymezena a na některých klientských stanicích jsou nainstalovány programy, které nemají licenci. Zjistil jsem, že firma nemá vůbec nastavenou IT bezpečnostní politiku v oblasti práv uživatelů, a nejsou v dostatečné míře zpracovány směrnice, které by jejich práva jasně definovala.

Standardní uživatel, po zřízení a nastavení účtu administrátorem nemá právo na instalaci žádného z programů. Tím je zamezeno šíření nelegálních software na pracovní stanice. Ale tak je tomu pouze u běžného uživatele. Administrátorský účet dovoluje provádět změny,

které ovlivňují ostatní uživatele, jako např. konfigurace systémových nastavení nebo instalace příslušného software. Někteří pracovníci mají nastaveny práva administrátora bezdůvodně. Každý zaměstnanec se může přihlásit na jakoukoliv pracovní stanici v rámci celé firemní sítě. Tohoto je využíváno jen výjimečně. Uživatel při přihlášení na jiném PC pod svým účtem, má k dispozici pouze základní obrazovku - prostředí Windows, ale už nejsou nastavena další zařízení, která jsou nutná pro provoz samotného pracoviště, jako je nastavení tiskáren, sdílení atd. Po přihlášení do takovéto pracovní stanice, může na svůj odkládací prostor - disk s velmi malým prostorem a úložištěm, který se po přihlášení přiřadí k jeho účtu ukládat datově malé zálohy. Tohoto typu přihlášení do systému se využívá jen zřídka a ve výjimečných případech. Více je využíváno tzv. připojení vzdálené plochy, která je administrátorem nastavena všem uživatelům v rámci sítě. Někteří vybraní uživatelé mají právo přihlášení do firmy zvenčí, což je řešeno externími notebooky, které jsou do firemní sítě patřičně zabezpečeny a nastaveny.

Doporučení

Práva a přístupy jednotlivých uživatelů nejsou IT oddělením jasně nastavena. Práva musí být nastavena jen v nezbytně nutném rozsahu pro činnost uživatele, nebo procesu. O přidělení se musí přihlásit každý sám. Je třeba se zaměřit na odebírání práv nejen v případě odchodu ze zaměstnání, ale hlavně při přeřazení na jinou pozici. Zde bylo zjištěno, že je tady jistá prodleva a práva uživatelů se řeší dodatečně. Jelikož ve firmě je oddělení IT o dvou pracovnících, nejsou nastaveny žádné směrnice z hlediska bezpečnostní politiky. V této oblasti je nutné se cíleně zaměřit na tvorbu směrnic, která budou jasně definovat práva jednotlivých uživatelů, jejich přístupy do jednotlivých stanic a přístupy z venkovní sítě. Je třeba se zaměřit na kontrolu nadbytečných práv. Dále je nutné redukovat práva uživatelů na minimum, což může mít na druhou stranu za následek navýšení pracovníků v oblasti IT. V neposlední řadě je nutné odebrat práva administrátora běžným uživatelům. Přidělování práva „administrátor“ přiřazovat jen správci sítě a jeho spolupracovníkům, kteří po rozdělení kompetencí správu sítě zabezpečují. Současným trendem je to, že vedoucí pracovníci mají práva administrátora. Nicméně v tomto ohledu bych byl opatrnější. Prvně je třeba zjistit, jaká práva a pravomoci má každý vedoucího pracovník a následně mu buď přidělit práva administrátora "admin", nebo práva standardního "users" uživatele.

6.7.4 Hesla a zabezpečení PC

Nový uživatel dostává od IT oddělení PC se svým uživatelským přihlášením a universálním heslem, které je třeba ihned po prvním přihlášení změnit. Zadávání hesel do klientských pracovních stanic, nemá vůbec žádný řád a pravidla. Jejich obměna vůbec neprobíhá, hesla na některých stanicích jsou nastavena již několik let stále stejná. Zabezpečení pracovních stanic je zabezpečeno podporou antivirového programu. V současné době je ve firmě antivirový program AVG, který je aktualizován na pracovní stanice průběžně, bez upozornění uživatelů. Aktualizace systému Windows si musí každý z uživatelů instalovat sám. V tomto případě jsou vyhrazená práva instalace i pro běžného "users" uživatele. Systém Windows má ve firmě tzv. multilicenci na všechny PC. V nedávné době proběhla revize všech pracovních stanic a bylo zjišťováno, které programy jsou v PC navíc a bez licencí.

Doporučení

Z hlediska uživatelů je zabezpečení na pracovních stanicích nedostatečné. Na některých účtech bylo zjištěno, že původní heslo od IT oddělení, nebylo změněno vůbec. Na některých PC je heslo staré několik let. Správce sítě musí dbát na kontrolu obměny hesel v určitém časovém horizontu, který je třeba dodržovat. V této firmě bych navrhoval obměnu hesel v horizontu 1x za 2 měsíce. Jelikož jsou zde PC, na kterých pracuje více uživatelů, je třeba důsledně dbát na pravidelné odhlášení. Zde bych řešil situaci tak, že po nějaké časově prodlevě a při nečinnosti, by proběhlo automatické odhlášení ze systému, kde musí uživatel počítat s možnou ztrátou dat. Případně PC nastavit po určité době do spánkového režimu.

Příklad pravidel zabezpečení hesel:

- obměna hesla minimálně jednou za dva měsíce
- minimum znaků je 7 – maximum 30 znaků
- heslo musí obsahovat alespoň jedno velké písmeno
- součástí hesla musí být alespoň jedna číslice
- hesla do klientských stanic nikomu nesdělovat

Jelikož jde o ochranu dat firmy, je třeba věnovat zabezpečení hesel stejnou důležitost, jako u přihlášení do bankovnictví.

6.7.5 Pracovní stanice

Pracovní stanice uživatelů jsou rozděleny na administrativní a skladové pracoviště. Administrativní pracoviště využívají pracovníci PC stanice ke komunikaci se zákazníky. Na skladových pracovištích je PC vybaven jen základními programy, nezbytně nutné pro skladovou evidenci. Tyto PC jsou zároveň bez přístupu na internet. V současné chvíli probíhá ve firmě obměna většiny hardwaru, tj. PC a tiskáren. Je zde ještě mnoho PC s Windows XP. Jejich ochrana je z hlediska napadení dosti problematická, protože již neexistují pro tento systém aktualizace. Nové počítačové stanice, většinou od firmy Dell, jsou již opatřeny operačními systémy Windows 7. Stejně tak je to u Office, kde na některých PC je ještě Office 2003 a na nových PC Office 2007, což je mezi jednotlivými verzemi problém z hlediska synchronizace. Pro komunikaci se zákazníkem je využíváno Office 360, kde při používání Light verze využívají zaměstnanci sdílené kalendáře, např. dovolená. Pracovní stanice „Vrátnice“ má pouze jeden účet, na který se pracovníci hlásí pod jedním přihlášením.

Seznam programů

- Windows XP Professional (s balíky Service Pack 2), Windows 7 - multilicence
- Microsoft Office 2003, Microsoft Office 2007, Microsoft Office 20010 (kancelářské aplikace)
- Microsoft Office 365, v současné chvíli pro uživatele rozšířena ze 2GB na 50GB.
- Nero 9, jen na některých PC stanicích
- Ashampoo Burning Studio free - frewarové verze programu
- Zoner Photo Studio 10 – licence (některé PC)
- Adobe Photoshop 7 – licence (některé PC), Adobe Reader
- Internet Explorer 7, Internet Explorer 10, Google Chrome

Doporučení:

Hardwarové vybavení, zvláště PC jsou různého typu. Liší se zásadně svým stářím. Programy a operační systém, které jsou instalovány v jednotlivých PC, mají licenční čísla, některé programy jsou instalovány do PC jako freewarové verze. Jsou zde dva typy operačních systémů. Což z hlediska aktualizací Windows XP je nešťastné. Z hlediska bezpečnosti je třeba průnik do sítě ještě více zabezpečit. Jelikož v současné době probíhá obměna hardwarového zařízení lze předpokládat, že do budoucna se operační systémy sjednotí do všech PC. Zaměstnancům, kteří mají nové PC a využívají Microsoft Office 2007 a vyšší

verze doporučuji nastavit na PC správcem IT oddělení synchronizaci přes Microsoft Office 360 a Microsoft Office 20xx. Dle mého hlediska je prostředí Office 360 naprosto nepřehledné. Pokud si nenastavíte Light verzi tohoto systému, nemůžete využívat ani sdílené kanceláře, která je jedinou výhodou. Dále je nezbytně nutné, ohledně skladového programu, který je programován na jeden typ prohlížeče, sjednotit všechny počítačové stanice na jeden typ internetového prohlížeče a to Internet Explorer 10.

6.7.6 Internet a jeho připojení

Jak již bylo výše zmíněno, nastavení internetového připojení je přesně vymezeno na administrativní a skladové pracoviště. Na administrativních pracovištích je internet povolen, na skladových pracovištích je internet zakázán. Důvodem je doporučení externí firmy, která dodává do firmy skladovací program. Dále je umožněn zákazníkům připojení internetu přes wiffi router na svá zařízení. Toto připojení je řešeno od wiffi vysílače kabelem UTP do ústředny a dále po metalickém vedení. Wifi síť je zabezpečena silným heslem a pokrývá hlavně přízemní část budovy. Zařízení Ubiquiti UniFi AP Professional je znázorněno na obrázku č. 30 a je to anténa s integrovaným WiFi 802.11, který má funkci AP/Hotspot. Je určen pro frekvenci 2,4 GHz, tak 5 GHz, jedná se o Dual-Band zařízení. Pro interní potřebu zaměstnanců je řešena druhá wiffi, která je napojena na stávající firemní síť a opatřena též silným zabezpečením - heslem. Instalované zařízení se nazývá WiFi router 802.11b/g/n ASUS RT – N 12.

Obrázek č. 30.: Anténa s integrovaným WIFI [archiv autora]

Obrázek č. 31.: WiFi router ASUS RT – N12 [16]

Doporučení

Internet a jeho napadení zvenčí je zabezpečeno dostatečně. Jediná výtka je přejmenování názvu sítě, pro snadnější orientaci rozlišení a to firemní-zákaznická.

6.7.7 Režimová opatření IT

Obecně je informační technologie (IT) z hlediska síťového zabezpečení na velmi dobré úrovni. Hodnota aktiv IS/ICT je na střední úrovni, kdy stačí důsledná aplikace procesů a nastavení, které je již obsaženo v operačních systémech, aktivních prvcích apod. Nejsou proto potřeba drahá řešení třetích stran. Velký problém je z hlediska jednotlivých uživatelů, kteří nemají nastavené žádné režimové opatření. Vedoucí pracovníci nemají jasné instrukce od správce sítě formou vnitřních směrnic. Proto bych doporučoval, aby byl jasně definován pojem správce sítě a jeho pravomoci. Dále je nutné jmenovat někoho z managementu firmy, který by společně se správcem sítě definoval a vytvořil směrnice IT/ICT. S těmito směrnicemi dále seznámit zaměstnance, kteří se jimi musí řádně řídit. Nezbytně nutná je po určité době kontrola jejich plnění. Závěrem je potřeba ze všech směrnic vytvořit dokument bezpečnosti organizace v oblasti IS/ICT.

7 SHRNUTÍ NEDOSTATKŮ AUDITU

Komplexní audit probíhal za účasti jednotlivých zodpovědných a pověřených osob z řad firmy. K některým informacím a datům nebyl umožněn přístup. V současné chvíli firma prochází v několika oblastech zásadní obměnou, což vnímám velice pozitivně z hlediska konkurenčního prostředí.

Auditem byly zjištěny méně, ale i více závažné skutečnosti.

V první části auditu bylo v rámci areálu zjištěno, že zkušební provoz monitorovacího systému v rámci vjezdu a výjezdu do areálu není plně funkční - zvláště v oblasti vjezdu občasných a jednorázových zákazníků. Dále na vrátnicích není řešena evidence zákazníků při vstupu do areálu. Velké nedostatky jsem zjistil v oplocení celého areálu. Ploty jsou různých velikostí, na většině míst není navýšen o ochranný drát k větší obtížnosti překonání plotu. Na vjezd a výjezd na zadní část pozemku není plot instalován vůbec. Kamerový systém instalován v areálu a ve společných prostorách budov je nyní na dobré úrovni, ale v rámci mapování celého areálu a navyšování pohybujících se zákazníků je každý rok řešena otázka možného navýšení kamer. Analýzu možných rizik zpracovává a předává velitel ostrahy vedení společnosti.

Ve druhé části auditu jsem zjistil následující nedostatky. Vedoucí pracovníci, kteří mají vstup do všech kanceláří a prostor mají od každých dveří jiný klíč - není zaveden systém generálního klíče. V auditu EPS bylo zjištěno, že kompletní rozvod celého systému je z 80. let, a je již zastaralý. Zastaralé hlásiče, ústředna i tablo jsou tak zastaralé, že je již v tuto chvíli jejich údržba značně problematická a komplikovaná. V PZTS nejsou, ke stávajícímu vedení žádné plány a výkresy. Další nedostatky jsou ve vybavení některých technických prostředků přízemních prostor a kanceláří, jako například chybějící kontaktní detektory na tříštění skla.

Nedostatky se vyskytly i u auditu požární ochrany. V místnosti, kde jsou umístěny vysokotlaké láhve propan butanu a acetylenu, není umístěn detektor na únik možného plynu. Větším nedostatkem je zjištění, že v budově nejsou vyvěšeny požární poplachové směrnice. V příloze bakalářské práce je vložen návrh „Směrnice požární ochrany“. V auditu BOZP bylo zjištěno, že v budově nejsou rozvěšeny aktuální směrnice BOZP pro zaměstnance a zákazníky.

V oblasti auditu bezpečnosti IT je asi nejvíce nedostatků. Pro serverovnu nejsou zpracovány žádné směrnice, ani plán mimořádných událostí pro případ požáru. Dále chybí plán rozmístění hardwarových komponentů.

Není nastavena jasná komunikace mezi počítačovými stanicemi a externími zařízeními. Práva uživatelů nejsou jasně definovány. Jejich rozsah je v některých případech u vedoucích a některých dalších pracovníků zbytečně nastaven na účet "administrátor".

Zabezpečení pracovních stanic jednotlivých uživatelů nejsou dostatečně zabezpečeny. Za prvé dlouhá prodleva obměny hesel jednotlivých uživatelů do pracovních stanic a za druhé - hardware na několika pracovních stanicích je již zastaralý (operační systém Windows XP). Na těchto PC není již možnost aktualizací. Zároveň jsou již nedostačující pro samotný výkon práce zaměstnanců.

U každé z auditovaných oblastí bylo v případě zjištění pochybení a nedostatků na tyto skutečnosti upozorněno a navrhnuto optimální řešení.

ZÁVĚR

Bezpečnostní audit je jedna z nejdůležitějších oblastí z hlediska bezpečnosti každé větší firmy, zvláště pro střední a velké podniky. Každý podnik má z hlediska zabezpečení jiné priority. Zjištění nedostatků v oblasti bezpečnosti by mělo být pro každou firmu prioritou. Následná kontrola je povinností.

Cílem bakalářské práce bylo se seznámit se základními informacemi v oblasti bezpečnostního auditu. Dále byl popsán stávající stav firmy v určitých „vybraných" oblastech, ve kterých se z hlediska bezpečnosti nachází. Je nutné říci, že z hlediska bezpečnosti, zvláště oblasti PZTS, EPS, CCTV bylo splněno vše, co bylo zadavatelem "firmou" zadáno - bylo ověřeno u bezpečnostní agentury, která bezpečnost firmě zajišťuje.

V každé kapitole byl udělán bezpečnostní audit, následně bylo navrhnuto opatření, pro zajištění větší bezpečnostní politiky firmy. Nicméně v určitých oblastech, zvláště v oblasti IT má jisté rezervy, které je nutné odstranit. Např. implementováním návrhy opatření popsaných v auditu a v pravidelných intervalech, vykonávat jejich kontrolu.

V předchozí kapitole jsem definoval nedostatky z hlediska bezpečnosti v několika oblastech. Zásadním problémem je, že některá zařízení a technické prostředky jsou již zastaralá a tím samozřejmě méně spolehlivá. Z hlediska bezpečnosti jde např. o stáří požárních hlásičů, které jsou z 80. let minulého století.

Nicméně v současné době prochází firma v několika oblastech revitalizací. Je to hlavně důsledkem stále většího objemu zákazníků, kteří se po areálu pohybují. V tomto případě je nutno zmínit například obnovu parkovacího systému, obnovu kamerového systému pro vjezd/výjezd do areálu. Dále mohu uvést obnovu technického zabezpečení. Jako například obnovu elektrické požární signalizace v auditované budově, která se má konat v horizontu několika týdnů.

Dle mého názoru má firma obrovský potenciál a bezpečnostní prvky jsou v součinnosti s bezpečnostní firmou v určitých časových intervalech přezkoumávány. Ze všech doporučení z každé kapitoly vyplývá, že nemá firma přímo vyčleněného pracovníka, který by se staral o celkovou bezpečnost firmy.

V tomto případě bych z hlediska velikosti firmy nedoporučoval najmutí externího bezpečnostního manažera. Bezpečnostní manažer jako zaměstnanec firmy by shromažďoval kompletní informace - materiály z každé oblasti a s jednotlivými vedoucími pracovníky

vytvářel, přezkoumával, a následně implementoval režimová opatření. V neposlední řadě by rozhodoval o potřebě vykonání bezpečnostního auditu.

Zpracovaný audit byl předán vedení společnosti a správci areálu. Některé z nedostatků již jsou napraveny, některé jsou v době psaní bakalářské práce rozpracovány. Pro příklad v současné chvíli probíhá přezkoumání některých nedostatků a to zvláště oblasti HW/SW v oblasti IT. Dále v oblasti PZTS je přezkoumáván z hlediska dostatečného zabezpečení stav implementovaných prvků v rámci auditované budovy.

CONCLUSION

Safety audit is one of the most important areas for the safety of bigger companies, particularly for medium and large enterprises. Each business has in terms of security other priorities. It should be a priority for every company to identify deficiencies in security. Subsequent inspection is a duty.

The aim of this thesis was to introduce the basic information of the security audit. In addition, it was described current state of the company in certain "selected" areas from the point of view of safety. It is necessary to say that in terms of safety, especially areas PZTS, EPS, CCTV everything has been fulfilled what the contracting authority "the enterprise" specified - it has been verified by the security agency that provides its security.

In each chapter a security audit was made, it were subsequently suggested measures to ensure better security policies of the company. However, in certain areas, particularly in the field of IT, there are some imperfections, which must be removed. For example - by implementing proposals for measures described in the audit and carry out their control in regular intervals.

In the previous chapter, I defined the shortcomings in terms of security in the zone of the multiple-tech. The fundamental problem is that some of the equipment and technical resources are obsolete and therefore less reliable. In terms of safety we can mention goes e.g. the age of the fire alarms, which are from the 80s of the last century.

However, the company is currently undergoing revitalization in several areas. This is mainly due to the increasing volume of customers who are moving around the premises. In this case it is necessary to mention - for example parking system restoration, renovation of the CCTV system for entry / exit to the premises. Furthermore, I can mention renewal of technical security. As for example - restoration of the fire alarm (EPS) in the audited building, that will take place in the next few weeks.

In my opinion, the company has huge potential and safety elements are reviewed in cooperation with security firm in certain intervals. This is mainly due to the proper deployment and possible subsequent innovations. From the recommendations of each chapter implies that the company doesn't have any worker directly dedicated to take care of the overall security of the entire company.

In this case I don't recommend hiring an external security manager. Security manager, a company's employee could gather complete information - materials from each area and he would - in collaboration with each individual executives - create, review, and subsequently implement regime measures. Finally, he would decide if another safety audit is needed.

Processed audit was forwarded to the company's management and administrator’s complex. Some of the shortcomings are corrected already; some are at the time of the writing of this thesis elaborated. For example, at the moment ongoing review of certain deficiencies and especially HW / SW in the IT field. Furthermore, in PZTS is reviewed in terms of adequate security status implemented elements within the audited buildings.

SEZNAM POUŽITÉ LITERATURY

[1] BRABEC, František a kolektiv. Bezpečnost pro firmu, úřad, občana. Praha: Public History, 2001. ISBN 80-86445-04-6.

[2] BRABEC, František. Ochrana bezpečnosti podniku. Praha: EUROUNION, 1996. ISBN 80-85858-29-0.

[3] DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat. Brno: Computer Press, 2004. ISBN 80-7226-632-2.

[4] LUKÁŠ, Luděk a kolektiv. Bezpečnostní technologie, systémy a management II. Zlín: VeRBuM, 2013. ISBN 978-80-87500-19-4.

[5] SEILER, Milan. Bezpečnostní audit v organizaci. Praha: Soukromá vysoká škola ekonomických studií, 2014. ISBN 80-86744-20-5.

[6] Fryšar, Miroslav a kolektiv. 2006. Bezpečnost pro manažery, podnikatele a politiky. Praha: Public History. ISBN 80-86445-22-4.

[7] LAUCKÝ, Vladimír. Technologie komerční bezpečnosti II. Vyd. 2. Zlín:

Univerzita Tomáše Bati ve Zlíně, 2007, ISBN 978-80-7318-631-9.

[8] Návrh tvorby generálního klíče. [online]. [cit. 2015-04-19]. Dostupné z: http://www.marak.cz/infopage/vyroba-sghk-na-generalni-klic/

[9] Zkušební hlavice MHY 506. [online]. [cit. 2015-04-19]. Dostupné z: http://www.variant.cz/zbozi/1007-012-zkusebni-hlavice-mhy-506

[10] Tyč teleskopická GAR 290. [online]. [cit. 2015-04-19]. Dostupné z: http://www.variant.cz/zbozi/1007-014-tyc-teleskopicka-gar-290

[11] Redukce sestavná k MHY 506. [online]. [cit. 2015-04-19]. Dostupné z: http://www.variant.cz/zbozi/1007-013-redukce-sestavna-k-mhy-506

[12] Detekční kabel Umirs Quadrosense wire. [online]. [cit. 2015-05-07]. Dostupné z:

http://www.jhcomp.cz/katalog/umirs-quadrosense-wire-detekcni-kabel

[13] Elektrická požární signalizace. Tesla Liberec, Tablo Obsluhy MHS 805

[14] Drátové tísňové tlačítko s aretací PB65. [online]. [cit. 2015-05-08]. Dostupné z:

http://www.ampertech.cz/tisnova-tlacitka/326-dratove-tisnove-tlacitko-s-aretaci-pb68.html

[15] Kouřové a teplotní hlásiče požáru.[online]. [cit. 2015-05-08]. Dostupné z:

http://www.kelcom.cz/tyco/

[16] WiFi router ASUS RT – N 12. [online]. [cit. 2015-05-14]. Dostupné z:

https://www.alza.cz/asus-rt-n12-ver-d-d390719.htm

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

BP	bezpečnostní politika
BA	bezpečností audit
EPS	elektrická požární signalizace
PZTS	poplachové a zabezpečovací tísňové systémy
BOZP	bezpečnost a ochrana zdraví při práci
CCTV	uzavřený televizní okruh
DPPC	dohledové a přijímací poplachové centrum
ESKV	elektronický systém kontroly vstupu
PIR	pasivní infračervený detektor
PO	požární ochrana
IS/ICT	informační systémy/informační a komunikační technologie
IT	informační technologie
HW	hardware
SW	software
PC	počítač
NBÚ	Národní bezpečnostní úřad
Atd.	a tak dále
Např.	například

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

Příloha P1: Požární poplachová směrnice – česká verze

NÁZEV FIRMY, ADRESA PODNIKÁNÍ

POŽÁRNÍ POPLACHOVÁ SMĚRNICE

V případě vzniku požáru

P	Požární poplach je vyhlašován : voláním **„HOŘÍ“** Proveďte záchranu osob z ohrožených prostor. Prvotní zásah proveďte hasicími přístroji nebo vodou z požárního hydrantu.
O	Ohlaste požár na OHLAŠOVNU POŽÁRU společnosti tel. **2 42 05 5555 nebo 5555** případně tlačítkem hlásiče „Elektrické požární signalizace“ V hlášení uveďte : kdo volá, kde hoří, co hoří
M	Máte-li požárem znemožněn únik osob z objektu, použijte dalších únikových cest a nouzových východů vedoucích do volného prostoru.
O	Osobní pomoc veliteli jednotky hasičů je Vaší zákonnou povinností !! Po evakuaci a příjezdu jednotek oznamte hasičům všechny informace o místě a druhu požáru, charakteru objektu, umístění uzávěrů médií apod.
C	**Tísňová telefonní čísla** **V objektu společnosti: NON STOP** **Mimo objekt společnosti** **Hasiči** 2 42 05 5555 **Hasiči** 150 **Ochranná služba** 2 4205 2268 **Policie ČR** 158 **Poruchy el.sítě** 2 4205 1071 **Záchranná služba** 155 **Poruchy plynu** 2 4205 1071 **Městská policie** 156 **Poruchy vody** 2 4205 1071 **Tísňová linka** 112 **Hlášení poruch vnitřní telefonní linka společnosti 1071**
Účinnost :	Ode dne účinnosti Požární poplachové směrnice - datum
Zpracoval :	Bezpečnostní technik
Schválil :	Majitel firmy, generální ředitel

Příloha P2: Požární poplachová směrnice – anglická verze

COMPANY NAME AND ADDRESS

FIRE ALARM INSTRUCTIONS

in the case of fire

H	Shout **„FIRE“** to notify others Help evacuate personnel from areas that are in danger. Use a fire extinguisher or water from the fire hydrant in first attempts to douse the fire.
E	Notify the **FIRE NOTIFICATION CENTER** of the company by dialing **2 4205 5555 or 5555** or by pushing the „Elektronic Fire systém“ buton. When calling, specify : who ic calling, where the fire is, and what is burning.
L	If the departure of personnel from the threatened area is restricted by the fire, use other escape route – any exits or emergency routes that lead to safety ares.
P	It is your legal responsibility to provide personal assistance to the fire brigade leader! After the premises have been evacuated and the fire brigade has arrived, provide the fire fighters with all available information regarding the location and type of fire, the characteristics of the building, the location of all shut – off valves, etc.
	Important Telephone Numbers **Internal : NON STOP** — **External : NON STOP** **Fire Notification Center** 2 4205 5555 — **Fire Brigade** 150 **Security Service** 2 4205 2268 — **Police of the Czech Republic** 158 **Electricity Problems** 2 4205 1071 — **Emergency Rescue Service** 155 **Cas Line Problems** 2 4205 1071 — **Municipal Police** 156 **Water Line Problems** 2 4205 1071 — **Emergency Line** 112 **Malfunction reporting - internal telephone line 1071**
Effective:	**Date of effectiveness of fire alarm instructions**
Executed: **Members of the patrols**	**Safety technician** **Commander, 2x member**
Authorized:	**Chief Executive**