Bezpečnostní politika firmy

The Security Policy of a Company

Bc. Jan Rochovanský

Diplomová práce
2012

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2011/2012

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

Jméno a příjmení:	**Bc. Jan ROCHOVANSKÝ**
Osobní číslo:	**A10927**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Bezpečnostní politika firmy**

Zásady pro vypracování:

1. **Charakterizujte bezpečnostní politiku podnikatelské společnosti.**
2. **Proveďte analýzu platné legislativy a její praktické dopady.**
3. **Popište činnosti firmy Marius Pedersen a.s. především z pohledu dosud uplatňovaných bezpečnostních postupů.**
4. **Konkretizujte slabé články v bezpečnostních opatřeních a navrhněte způsob řešení.**
5. **Analyzujte rizika skládek a navrhněte sjednocení v rámci této společnosti.**
6. **Práci doplňte obrazovou a grafickou dokumentací.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **KINDL,Jiří.Projektování bezpečnostních systémů I.díl.Zlín:Univerzita Tomáše Bati ve Zlíně,2004.ISBN 80-7318-165-7.**
2. **LAUCKÝ,Vladimír.Technologie komerční bezpečnosti I.Zlín:Univerzita Tomáše Bati ve Zlíně,2004.ISBN 80-7318-194-0.**
3. **LAUCKÝ,Vladimír.Speciální bezpečnostní technologie.1.vydání.Zlín:Univerzita Tomáše Bati ve Zlíně,2009.ISBN 978-80-7318-762-0.**
4. **LUKÁŠ,Luděk a kolektiv.Bezpečnostní technologie, systémy a management I.1.vydání.Zlín:VeRBuM,2011.ISBN 978-80-87500-05-7.**
5. **KAMENÍK,Jiří. BRABEC,František a kolektiv.Komerční bezpečnost.Praha:ASPI,2007.ISBN 978-80-7357-309-0.**
6. **UHLÁŘ,Jan.Technická ochrana objektů I.díl - Mechanické zábranné systémy.Praha:Policejní akademie České republiky,2000.ISBN 80-7251-046-0.**
7. **UHLÁŘ,Jan.Technická ochrana objektů I.díl - Elektrické zabezpečovací systémy.Praha:Policejní akademie České republiky,2001.ISBN 80-7251-076-2.**

Vedoucí diplomové práce: **JUDr. Josef Čejka**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **24. února 2012**

Termín odevzdání diplomové práce: **15. května 2012**

Ve Zlíně dne 24. února 2012

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Diplomová práce je zaměřena na bezpečnostní politiku obecně a na konkrétní bezpečnostní politiku podniku Marius Pedersen Group. V práci je bezpečnost podniku rozdělena do oblastí IT ochrany, bezpečnosti a ochrany zdraví při práci, ochrany budov a majetku a požární ochrany Jednotlivé oblasti bezpečnosti byly posuzovány z hlediska legislativy a současného stavu u firmy. Závěrem byl navržen dokument bezpečnostní politiky podniku Marius Pedersen Group a doporučená opatření (standard).

Klíčová slova: bezpečnostní politika podniku, bezpečnost a ochrana zdraví při práci, IT ochrana, ochrana osob a majetku, požární ochrana

ABSTRACT

This thesis is focused on security policy in general and the specific security policy of the Marius Pedersen Group. The work is divided into the security business areas of IT security, health and safety at work, the protection of buildings and property, fire safety measures and individual safety procedures are assessed in terms of legislation and the current state of the company. Finally a document on the safety policy of the Marius Pedersen Group is proposed as well as recommended measures (standard).

Keywords: specific security policy, health and safety at work, IT security, protection of persons and property, fire safety measures.

Poděkování, motto

Tímto bych chtěl poděkovat vedoucímu mé diplomové práce JUDr. Josefu Čejkovi za pomoc a připomínky, které mi poskytl při psaní této diplomové práce.

Chci také poděkovat za podporu mých kolegů z firmy Marius Pedersen, kteří mně seznámili s některými firemními pravidly a poskytli mi k nastudování interní materiály.

Současně chci poděkovat mé rodině za trpělivost a toleranci nejen tvorbě této mé práce, ale také za podporu po celou dobu mého studia.

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 s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- 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 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 11. 5. 2012

.....
podpis diplomanta

OBSAH

ÚVOD

Pro dnešní společnost se stala bezpečnost součástí běžného každodenního života. Nejinak je tomu i v rámci podnikání a možná právě při podnikatelských aktivitách nabývá pojem bezpečnosti ještě většího významu. Tuto skutečnost potvrzuje i poměrně nový pojem bezpečnostní politika podniku. Alespoň některá z částí bezpečnostní politiky bývá součástí interních předpisů všech podnikatelských subjektů. Jedná se o banky, obchodní, dopravní, telekomunikační, bezpečnostní firmy a také průmyslové podniky. Liší se pouze rozsahem, formou, obsahem a zpracováním.

Každopádně důležité je, jak která firma k zajišťování své bezpečnosti přistupuje a jak se staví celkové k otázce bezpečnostní politiky.

Tato práce si klade za úkol zjistit, jak je to s bezpečnostní politikou v praxi. Proto byla vybrána konkrétní firma, kde s pomocí zjištění současného stavu bezpečnosti, na základě provedení analýzy bude možné posoudit stav její bezpečnosti a příp. navrhnout opatření ke zlepšení stavu v souladu se zadáním této práce.

I. TEORETICKÁ ČÁST

1 BEZPEČNOSTNÍ POLITIKA

O bezpečnostní politice mluvíme tehdy, pokud se bezpečností zabývá stát, organizace, instituce nebo podnik.

Pro naše potřeby se na ni můžeme podívat ze dvou hledisek. Jedním je bezpečnostní politika obecně a druhým pak bezpečnostní politika vztahující se k podnikatelským subjektům.

1.1 Globální bezpečnostní politika

Globální bezpečnostní politika má svoji historii ve vojenských konfliktech od nejstarších civilizací. Tyto vojenské konfrontace vycházely z mocenských ambicí, především velkých států, ale válečné konflikty se dotýkaly se vlastně všech národů a jejich státních uspořádání.

Na současné lidstvo působí kombinované účinky hrozeb a zdaleka se nejedná pouze o hrozby vojenských konfliktů jako v minulosti. Tyto stále zůstávají velkým nebezpečím, především s ohledem na civilizační pokrok ve vyzbrojování, konkrétně např. zbraní hromadného ničení, ale i ozbrojené konflikty vychází z jiných aspektů.

I na vojenské hrozby se ale musíme dívat především z pohledu současných hrozeb, jakými jsou např. extremismus ať už státní politiky nebo při prosazování náboženských směrů.

Globálním hrozby současnosti můžete rozdělit do několika oblastí:

- mezinárodní vztahy
- extremismus
- IT hrozby
- změny klimatických podmínek
- ekonomické hrozby

1.1.1 Mezinárodní vztahy

Při sledování mezinárodních vztahů v současnosti si uvědomíme, jak jsou rozdílné a zároveň stejné jako v minulosti. Na jedné straně lidská civilizace vyspěla, snaží se řešit mezinárodní konflikty mírovou cestou, vytváří se multikulturní města a státy. Dochází ke sbližování mezi národy a vazby mezi jednotlivými státy jsou užší. Dokladem toho je např. rozšiřování Evropské unie. Na straně druhé toto může vést k podcenění možných hrozeb, které už známe nebo k přehlížení dosud skrytých hrozeb.

U globálních hrozeb se většinou neřeší aktuální hrozby současnosti, ale úkolem globální bezpečnostní politiky je globální hrozby předvídat a hledat s předstihem možnosti jejich řešení.

Některé konflikty v mezinárodních vztazích jsou dlouhodobé a řeší se několik desetiletí mezi tyto konflikty a tedy i potencionální hrozby patří např. rozdělení Korejského poloostrova, problém Falklandských nebo Kurilských ostrovů. Evropě je pak nejblíž rozdělení Kypru. Které je od roku 1974 rozděleno na řeckou a tureckou část.

Z globálního hlediska jsou ale mnohem nebezpečnější politika některých států, jež má přímý vliv na mezinárodní vztahy. Jedná se např. o státní politiku Íránu a jeho jaderný program. Íránský jaderný program je již delší dobu jedním z hlavních témat v mezinárodně bezpečnostní oblasti. Írán ale tvrdí, že se v jaderné oblasti zaměřuje výhradně na energetiku a oficiálně odmítá tvrzení o vývoji jaderných zbraní. Tvrdí, že jaderný výzkum je zaměřen na mírové využití jádra především v oblasti energetiky.

Další klasickou ukázkou státní politiky, která je potencionálním nebezpečím je politika Pákistánu. Politická situace v Pákistánu je dlouhodobě ovlivňována dvěma hlavními aspekty. Jsou to armáda na jedné straně a islámské náboženství na straně druhé. Podle toho jak jsou si tyto aspekty blízké, či vzdálené je politická situace v zemi nebezpečná i pro mezinárodní vztahy. Pákistán s ohledem na silné proislámské myšlení vystupuje jako přirozený spojenec islámských extremistů, ale chce zůstat také spojencem západních zemí, především USA. Tato rozpolcenost státní politiky Pákistánu vede k nečitelnosti jeho mezinárodních vztahů. Nezanedbatelným faktorem jeho hrozby je také to, že se jedná o jednu z jaderných mocností, která disponuje jaderným arsenálem a zároveň o jednu z nejlidnatějších zemí světa. K bezproblémovým mezinárodním vztahům v oblasti

nepřispívá, ani dlouholetý spor se sousední Indií, která je mj. dalším státem disponujícím jadernými zbraněmi, o území Kašmíru, které si nárokují obě strany konfliktu.

Posledním konfliktem, který mněl přímý dosah na mezinárodní vztahy v globálním měřítku byla tzv. severoafrické revoluce. Tunisko, Alžírsko, Libye, Jemen, Jordánsko, Egypt, to jsou státy, v kterých průběhu roku 2011 došlo k velkým politickým změnám, ke svržení předchozích vládních garnitur. Toho bylo dosaženo lidovými protesty, které přerostly v otevřenou revoltu a postupně i ozbrojený odpor s cílem svrhnout nenáviděné diktatury. Jednalo se o revoluci, která si dala za cíl prosadit svobodu a demokracii, jejím prvotním důvodem byly dlouhodobé ekonomické problémy.

Tyto severoafrické nepokoje se rozšířily také na blízký východ a mimo pokračujících nepokojů v Sýrii, tak můžeme sledovat i výbušnou situaci např. v Bahrajnu.

Jak bylo zmíněno v úvodu, úkolem globální bezpečnosti je především předpovídání možných problémů. Takovým problémem může být do budoucna např. nedostatek nerostných surovin. Přesto v poslední době bývá v souvislosti s možnou globální nebezpečností zmiňován nedostatek vodních zdrojů.

1.1.2 Extremismus

Mezi hrozby, které významně ovlivňující globální bezpečnost se řadí bezesporu extremismus. Extremismus není jednoduché definovat, neexistuje ani jeho právní vymezení a dokonce existují názory, že pojem samotný zjednodušuje konkrétní problematiku. Přesto ho můžeme definovat jako krajní názory od většinové populace, která vytváří určitou střední normu, tyto extrémní názory mohou být posunuty směrem doprava i doleva od pomyslného středu názorů a s ohledem na jejich míře odchylky pak můžeme hodnotit závažnost extremismu.

Nejednoduší definici můžeme najít ve slovníku cizích slov, kde se o extremismu hovoří jako o krajně radikálním, výstředním postoji.

V České republice je pak pojem extremismus označován jako vyhraněné ideologické postoje, které vybočují z ústavních, zákonných norem, vyznačují se prvky netolerance, a útočí proti základním demokratickým ústavním principům, jak jsou definovány v českém ústavním pořádku. [1]

Extremistické skupiny prosazují své názory většinou nedemokratickou cestou. Pro bezpečnostní politiku je pak nevýznamnějším faktorem stupeň jakým chtějí jednotlivé extremistické uskupení své názory prosazovat.

V souvislosti s extremismem můžeme zmínit také pojmy jako radikalismus, fanatismus, fundamentalismus, terorismus, některé, většinovou společností nesdílené formy nacionalismu, fašismu, xenofobie a rasismu, nátlakové akce environmentálních či ekologistických aktivistů (tzv. ekoterorismus) atd.

Extremismus bývá dělen na politický a náboženský, ale můžeme se o něm zmiňovat např. i v souvislosti s ekologií nebo národnostními zájmy.

Politický extremismus můžeme rozdělit na pravicový a levicový.

V pravicovém spektru zaujímají výrazný prostor nacionalisté, jejichž společným rysem je upřednostňování národnostního principu před občanským. Odmítají rovné uplatňování lidských a občanských práv a v jejich programech se objevují otevřené nebo skryté prvky rasismu, xenofobie a antisemitismu.

V levicovém extremismu zaujímají významné místo vyznavači marxisticko-leninské revoluční ideologie, vyzývající k diktatuře proletariátu, tedy k organizovanému, systematicky uplatňovanému násilí, jehož cílem a smyslem je likvidace aktivních odpůrců i veškeré možné názorové opozice. Součástí levicového extremismu je i tzv. anarchoautonomní hnutí, které spojuje anarchisty s příznivci tzv. autonomního neideologického proudu, odmítajícího respektovat jakýkoliv společenský řád a jeho struktury. [2]

IT hrozby

Pro rok 2012 předpovídají experti větší zaměření hrozeb v oblasti IT na sofistikovanější cílené útoky. Jedná se tak o odklon od masivních útoků, jejichž pokles můžeme v posledních letech sledovat. Nejčastěji jsou zmiňována následující trendy:

- Počet útoků na PC bude nadále kopírovat stávající trend, ovšem výrazný nárůst zaznamenají především útoky na uživatele mobilních zařízení. Nejvíce ohrožení budou uživatele s operačním systémem Android, ale ani uživatelé ostatních

platforem nebudou moci cítit o mnoho bezpečněji. Útoky vedené prostřednictvím sociálních sítí budou nadále slavit svůj úspěch.

- Stále vice útoků bude vedeno již nikoliv pouze na finanční instituce a velké organizace, ale i na malé a střední podniky zkr. SMB[1]. Pro průnik do systémů velkých společností bude vzhledem k jejich poměrně kvalitnímu zabezpečení stále častěji používáno sofistikovaných technik sociálního inženýrství. A SMB, které doposud stály spíše stranou zájmu organizovaného zločinu, budou nuceni se více zajímat o bezpečnost, a to pro většinu z nich bude představovat značný problém.

- K útokům bude mimo jiné využíváno i soukromých mobilních zařízení, na kterých nejsou mnohdy aplikovány vůbec žádné bezpečnostní politiky, a které budou v mnoha firmách využívány v rámci programu BYOD[2], od kterého se očekává, že přinese větší spokojenost na straně zaměstnanců, zvýší efektivitu práce a především sníží náklady na nákup těchto koncových zařízení. V souvislosti s nezvládnutím deprovisioningu[3] však lze očekávat, že těch citlivých informací, které si zaměstnanci na svých zařízeních odnesou, bude podstatně vice než dřív. Kromě toho je zřejmé, že zaměstnanci budou na svá zařízení instalovat nejrůznější aplikace a spolu s nimi se na ně dostane i malware[4].

- Pokud jde o malware[5] pro smartphony[6] jako takový, tak i nadále se budou objevovat na marketu aplikace, které se budou snažit uživatele okrást o jeho peníze, ale stále častěji se bude moci setkat i s malwarem, který bude cílen na konkrétní firmy a bude se snažit získat přístupové údaje, kontakty, seznam klientů, citlivé

---

[1] **SMB**- malé a střední podniky (Small and Medium Business)

[2] **Bring Your Own Device** - zaměstnanci si nosí svá vlastní "chytrá" zařízení do firemního prostředí.

[3] **Provisioning** - slouží k automatickému nastavení zařízení, udržování jeho firmwaru a nastavení v aktuální ověřené verzi.

[4] **Malware** - počítačový program určený ke vniknutí nebo poškození počítačového systému.

[5] **Malware** - počítačový program určený ke vniknutí nebo poškození počítačového systému.

[6] **Smartphone** - chytrý telefon, který poskytuje pokročilé funkce, jako například připojení k internetu.

dokumenty a know-how. Tento bude velice obtížné odhalit, neboť bude využívat zranitelností nultého dne a jeho komunikace s řídícím serverem se na první pohled nebude příliš lišit od běžného provozu. Pokročilá inspekce odchozích paketů a nasazení nástrojů umožňující analýzu chování síťového provozu, se tak stane nutností.

- Pokud jde o zcela nové hrozby, dají se očekávat první útoky na NFC[7], protože tato poměrně nová technologie, je stále více oblíbenější a tím i rozšířenější. [4]

Největší slabinou webových aplikací jsou bezpečnostní chyby, které překonaly všechny ostatní hrozby a dle dostupných informací, představují až 55 všech známých slabin. Tato procenta nemusí být, ale konečná, protože nezahrnují webové aplikace vyvinuté na zakázku. Podle odhadů se tak může jednat až o dvě třetiny všech hrozeb.

Podniky bojují se stále důmyslnějšími útoky na své počítačové sítě, včetně tzv. vyspělých perzistentních hrozeb, s využitím metod skrytých útoků, které rostou co do četnosti i složitosti.

Dalším konkrétním příkladem hrozby je zneužívání formátu PDF, které od roku 2009 narůstá v důsledku nalezení nových způsobů, jak oklamat uživatele. Aktuálně tento způsob tvoří až tři z pěti běžně používaných možností napadení prohlížečů.

Obecně předpokládáme nárůst všech typů útoků a hrozeb, především se ale očekává ústup např. od klasických spamů, protože jak již bylo několikrát zmíněno, jsou útoky mnohem propracovanější, adresnější a tedy sofistikovanější. U určitých hrozeb tak dochází k jejich poklesu. V bankovním sektoru se tak jedná se např. o phishing 8, jehož útoky meziročně klesají o desítky procent. Přesto se finanční instituce musejí mít i nadále na pozoru a to především s ohledem na útoky na kreditní karty, které přebírají primát co do četnosti ohrožení.

---

[7] **Near Field Communication** - technologie umožňuje bezdrátový přenos dat na krátkou vzdálenost.

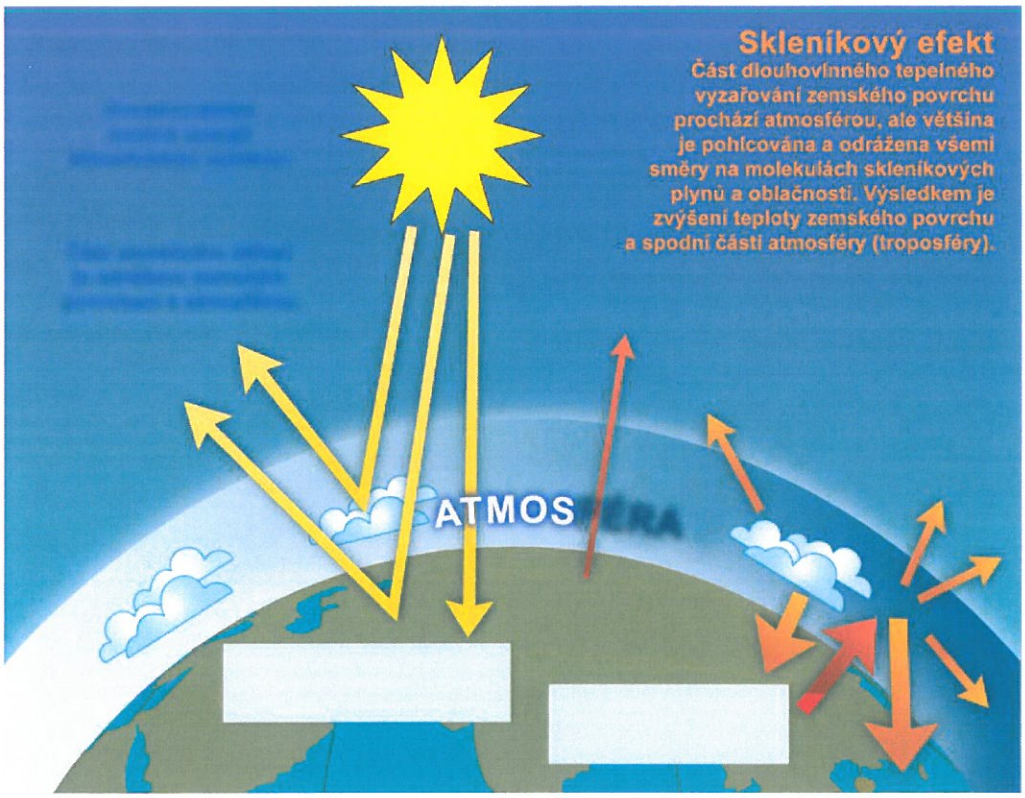
[8] **Phishing** - podvodná technika používaná na Internetu k získávání citlivých údajů (hesla, čísla kreditních karet apod.) v elektronické komunikaci.

Mezi nejvýznamnější hrozby se dále mohou řadit: nevyžádaná pošta, viry na USB flashdiscích, podvržené certifikáty, neodhalitelné viry, nebezpečné přílohy a útoky na mobilní zařízení.

1.1.3 Změny klimatických podmínek

- globální oteplování

Je způsobeno především nerovnováhou "skleníkových plynů". Skleníkových plyny samy o sobě nejsou problémem, problémem je jejich únik do zemské atmosféry, jako produkt skleníkového efektu. Bez skleníkového efektu a jeho odpovídajících plynů by průměrná teplota na Zemi klesla k 0°C. Četné vědecké práce prokazují, že obsah CO_2 v atmosféře, je aktuálně mnohem vyšší než v minulosti a dále se dá předpokládat jejich zvýšení.



[Zdroj: Le Treut]

Obr. 1 Zjednodušený model skleníkového efektu

- klimatické změny

Světová banka vydala seznam pěti hlavních hrozeb vyplývajících z klimatické změny: sucho, povodně, bouře, zvyšující se hladina moří a větší problémy v zemědělství.
V seznamu dvanácti nejohroženějších zemí figurují čtyři z nejchudších zemí světa. Seznamu vévodí Malawi, Bangladéš, Vietnam, Súdán a Filipíny.

Malawi, jihoafrická země s nízkým příjmem, jejíž obyvatelé žijí převážně ve venkovských oblastech a vydělávají 975 amerických dolarů či méně za rok, je podle zprávy země nejvíce ohrožená suchem. Ta by měla přicházet častěji a měly by trvat déle. V uplynulých dvaceti letech Malawi zažilo již dvě vážná období sucha, naposledy v roce 2004.

Bangladéš zase pro změnu vévodí seznamu zemí nejohroženějších záplavami. Himalájské ledovce tající v důsledku zvyšování globálních teplot hrozí rozvodnit řeky Ganga a Brahmaputra i stovky jejich přítoků a cestou na jih do Bengálského zálivu zaplavit každoročně 30 až 70 procent země. Bengálský záliv je mimochodem ohrožen i zvyšující se hladinou moří.

Zvyšující se hladina moří ohrožuje nejvíce Vietnam. Další studie Světové banky uvádí, že pokud by se hladina moře zvýšila o pět metrů, zasáhlo by to až 16 procent území Vietnamu, 35 procent jeho populace a dotklo se to 35 procent hrubého domácího produktu.

Súdán, největší africký stát, jehož území tvoří převážně vyprahlá půda či poušť, je zemí nejvíce ohroženou nedostatkem potravin v důsledku dopadu klimatické změny na zemědělství. Leží v Sahelu, regionu, který Mezinárodní panel pro klimatickou změnu (IPCC) popsal jako oblast nejnáchylnější k suchu vůbec.

Filipíny, země se středním příjmem ležící v jihovýchodní Asii, jež zároveň tvoří na 7000 ostrovů, vede seznam zemí ohrožených častějšími a silnějšími bouřkami. Podle ženevského Centra pro výzkum epidemiologie pohrom to byla v roce 2008 jedna ze tří zemí nevíce zasažených přírodními katastrofami. [4]

- ekologické katastrofy

Sopečné erupce

Jako o jedné z posledních sopečných katastrof se můžeme zmínit např. o erupci islandských sopek v březnu 2010, kdy se na jihu země Islandu probudila sopka Eyjafjöll a Katla. Erupce začala po několika týdnech silné seizmické aktivity a terénních deformací. V důsledku erupce došlo také k rozsáhlým záplavám. Silná aktivita sopek má také vliv na změnu klimatických podmínek především v Evropě. Přímým důsledkem aktivity sopek bylo chrlení popela a dýmu, které vytvořilo velký oblak popelu, který ovlivnil leteckou dopravu v celé severní části Evropy. Zrušení letů se týkalo také zbytku Evropy a také letů ze Severní Ameriky. Došlo k uzavření letišť v Británii a ve Skandinávii.

Vlny tsunami

V březnu 2011 postihla Japonsko velká přírodní katastrofa v podobě vlny tsunami, která byla vyvolána zemětřesením o síle až 8,9° Richtera. Otřesy způsobené zemětřesením vyvolaly velké až 23 metrové vlny, které zasáhly pobřeží Japonska. Katastrofa po sobě zanechala téměř 30 tis. mrtvých a pohřešovaných osob. Další desetitisíce osob zůstali bez přístřeší. Velké ekonomické ztráty zaznamenala celá ekonomika státu. Z globálního hlediska se největším nebezpečím ale stalo poškození japonských jaderných elektráren. K největšímu poškození, v důsledku silného zemětřesení, došlo na jaderné elektrárně Fukušima 1. V důsledku tohoto poškození začal selhávat chladící systém a v okolí města Okuma na severovýchodě Japonska došlo k úniku radiace. Havárie v elektrárně otevřela ve světě diskuzi o bezpečnosti výroby elektřiny z jádra.

Další tragédií z poslední doby byla vlna Tsunami v Indickém moři v prosinci 2004, vlna tsunami se zrodila u ostrova Sumatra. Silné zemětřesení zvedlo mořské dno a následná vlna se dala do pohybu a rychlostí až 800 kilometrů v hodině se řítila Tichým oceánem. Během půl hodiny zasáhla Sumatru, po hodině od prvních otřesů začala decimovat Thajsko a postupovala do dalších oblastí – Indonésie, Srí Lanku, Maledivy, Somálska, Barmu, Seychely. Během pár hodin tak o život přišlo více jak 200.000 lidí. Celková hodnota pomoci se v prvních měsících po tragédii vyšplhala až k sedmi miliardám dolarů. Kromě

vysokého počtu obětí je třeba připočítat zdravotní rizika, environmentální a ekonomické dopady. Šířily se nemoci spojené s velkým počtem usmrcených a zraněných osob.

Jde o přímé nakažení, kontaminaci pitné vody apod. Byly závažně poničeny ekosystémy korálových útesů a pralesních porostů. Velmi utrpěl rybářský průmysl a cestovní ruch.

Ropné havárie

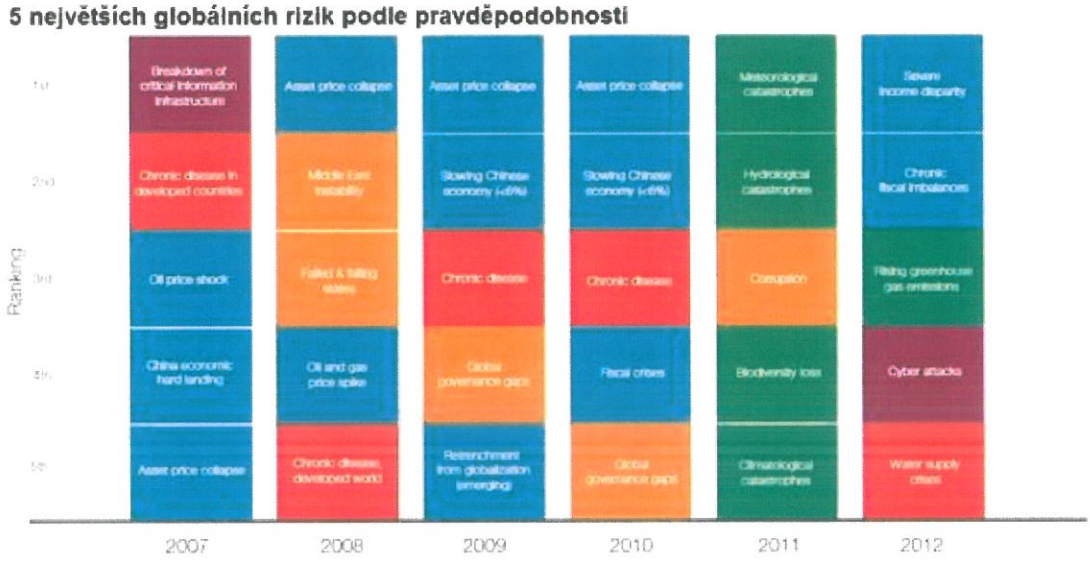
Exploze ropné plošiny britské společnosti BP[9] v dubnu 2010 v Mexickém zálivu způsobila jednu z největších ekologických katastrof a vůbec největší ekologickou katastrofu v dějinách USA. Než se podařilo výbuchem poškozený ropný vrt uzavřít, došlo podle posledních odhadů, během 3 měsíců k úniku přibližně 757 mil. litrů ropy. To má přímý vliv na životní prostředí, ale také na průmysl. Především rybolov, turistiku, ubytovací a stravovací služby. V neposlední řádě má tato katastrofa vliv především na samotný těžební průmysl.

Hlavním důvodem úniku ropy bylo nedodržení bezpečnostních pravidel, porušení deklarovaných zásad monitorování a vyhodnocování sledovaných ukazatelů. Dostatečná pozornost se nevěnovala používaným vrtným prostředkům, především z pohledu bezpečnosti. Tato činnost byla evidentně podceněna.

1.1.4 Ekonomické hrozby

Světová banka ve svém nedávném výhledu na globální rizika pro letošní rok nezapomněla na světová finanční rizika ani na nedostatek vody. Za nejpravděpodobnější považuje nerovnost příjmů lidí, chronické fiskální nerovnováhy, růst emisí skleníkových plynů, kybernetické útoky a nedostatek vody.

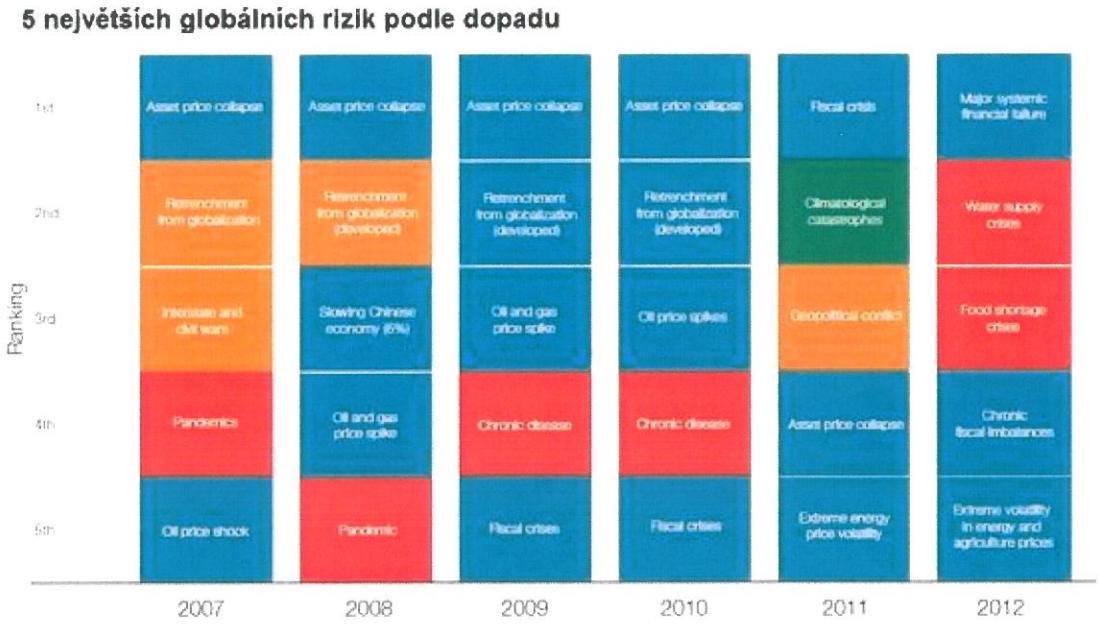
[9] British Petroleum



[Zdroj: investicniweb]

Obr. 2 Ekonomická globální rizika – pravděpodobnost

Jako největší rizika co do dopadu vidí velký systémový finanční kolaps, nedostatek vody a potravin, chronické fiskální nerovnováhy a extrémní kolísání cen zemědělských komodit a energií. [5]



[Zdroj: investicniweb]

Obr. 3 Ekonomická globální rizika - dopad

K udržení globální bezpečnosti v 21. Století je nutná restrukturalizace pohledů na hrozby a revize postupů jejich řešení.

1.2 Bezpečnostní politika podniku

Bezpečnostní politiku musíme chápat jako komplex opatření. V žádném případě se nejedná pouze o samostatné zajištění určitých částí, které chceme mít ošetřené z hlediska bezpečnosti a jak ji ještě v současné době chápe většina firem. Bezpečnostní politika podniku vyžaduje systémové řešení s celkovým pohledem na všechny bezpečnostní oblasti jako celek. Nejedná se tedy pouze např. o zabezpečení IT oblasti nebo obvodové ochrany objektů.

Bezpečnostní politika podniku má za úkol zvýšit jeho bezpečnost. Bezpečnost je ochrana podnikových aktiv pomocí technologií, procesů a školení, proti poškození, krádeži nebo jiné hrozbě.

I přesto, že je bezpečnostní politika koncepční a systémovou záležitostí, je třeba provádět její pravidelnou aktualizaci. Tu je nutno provádět rovněž před zásadními zásahy do technologie, očekávanými vnějšími vlivy, které mohou vážně ovlivnit chod podnikatele (orgánu státu) i po větších haváriích a katastrofách a jiných mimořádných událostech.

1.2.1 Definice bezpečnostní politiky

V předchozí kapitole byla popsána bezpečnostní politiku z obecného hlediska prostřednictvím globální bezpečnosti. Co to ale je bezpečnostní politika podniku? Jedná se o dokument, který v písemné podobě obsahuje prohlášení společnosti, tedy plán na ochranu aktiv společnosti (majetku, osob, prostředí). Bezpečnostní politika je neuzavřený, tzv. „živý dokument“, který může být průběžně aktualizován s ohledem na nové požadavky zaměstnanců, legislativní změny nebo zavádění nových technologií na trh.

Bezpečnostní politika je strategický dokument, který definuje, čeho chce společnost v konkrétní oblasti bezpečnosti dosáhnout, ale nespecifikuje už, jakým způsobem toho má být dosaženo. Proto jsou součástí bezpečnostní politiky bezpečnostní procesy a postupy, které upřesňují konkrétně, jak toho má být dosaženo. Konkrétně tak bývá bezpečnostní

politika rozšířena o vnitronormy , konkrétní návrhy zabezpečení, politiku BOZP, pravidla PO.

V odborné literatuře se uvádí, že:

„Bezpečnostní politika organizace je ve své podstatě souhrn odpovědí vrcholového vedení organizace především na tři základní otázky:

- Co má organizace v oblasti bezpečnosti činit a z jakého důvodu?
- Jakých cílů v oblasti bezpečnosti chce dosáhnout?

Jak bude řídit jednotlivé podnikové činnosti a jaká provede opatření, aby stanovených bezpečnostních cílů bylo dosaženo?“ [6]

1.2.2 Obsah bezpečnostní politiky

Jednotlivé oblasti bezpečnostní politiky se liší podle konkrétních činností firmy. Proto se jsou požadované oblasti zabezpečení firem různé. Mezi nejčastěji zabezpečované oblasti patří:

- ochrana objektů a majetku
- ochrana bezpečnosti a zdraví při práci
- ochrana IT
- požární ochrana

Obsah bezpečnostní politiky můžeme měnit v závislosti na potřebách zaměstnanců, požadavcích majitelů nebo okolních vlivů.

Bezpečnostní politika může zahrnovat zásady užívání, popis toho, jak společnost plánuje vychovávat své zaměstnance o tom, jak chrání majetek společnosti a vysvětlení, jak oblasti bezpečnosti kontrolovat a vymáhat správné provádění vč. postupu pro hodnocení účinnosti zavedení bezpečnostní politiky. Toto je nutné pro nutné změny a aktualizace bezpečnostní politiky tak aby byla účinná.

Součástí bezpečnostní politiky podniku je její rozšíření o interní dokumenty konkrétní návrhy zabezpečení, politiku BOZP, pravidla PO a jiné interní dokumenty.

V dokumentu bezpečnostní politiky podniku můžou být konkrétně zmiňovány tyto informace: mimo představení firmy, závazek aplikace nových trendů, specifikace aktiv, které chce firma zabezpečit, identifikace rizik, závazek ke kontrole (auditům), personální výhody, soulad bezpečnostní politiky podniku s mateřskou firmou, deklarace podpory systému řízení, informace o doplňujících dokumentech.

1.2.2.1 Ochrana objektů a majetku

První z oblastí, která jako součást bezpečnostní politiky je předmětem požadavku na zabezpečení je ochrana majetku podniků. Pod pojmem majetek podniku si v této souvislosti můžeme představit venkovní prostory, budovy, vnitřní prostory firmy, příp. stroje a zařízení. Na tuto ochranu se můžeme podívat z několika pohledů, některé zdroje uvádějí např. vnější a vnitřní ochranu. Jiné zdroje uvádějí dělení na 4 základní formy ochrany objektů:

- klasická ochrana
- režimová ochrana
- fyzická ochrana
- technická ochrana

Klasická ochrana – založena na zajištění objektu pomocí mechanických zábran a zařízení, které znemožňují odcizení nebo poškození objektů, jejich částí nebo cenných předmětů uvnitř objektů.

Režimová ochrana – představuje organizačně administrativní opatření a postupy. Z hlediska opatření můžeme režimovou ochranu dále dělit na vnější a vnitřní opatření.

Fyzická ochrana – prováděná fyzickou ostrahou objektu (hlídací služba).

Technická ochrana – založená na automatickém monitorování objektu pomocí technických prostředků objektové bezpečnosti. Technickou ochranu můžeme dělit podle prvků použitých k zabezpečení na mechanické, elektronické (elektrické), kombinované (mechatronické) a speciální prvky bezpečnosti. [6]

1.2.2.2 Bezpečnost a ochrana zdraví při práci

Zajišťování bezpečnosti ochrany zdraví při práci je základní povinností zaměstnavatele vůči zaměstnanci. Tato povinnost je dána legislativně, ale současně má sociální charakter, kdy na základě projednání problematiky s odborovým orgánem podniku, mohou být některé specifické podmínky zajištění bezpečnosti formulovány např. v rámci kolektivní smlouvy se zaměstnanci.

Povinnosti bezpečnosti a ochrany zdraví při práci jsou směřovány k základním požadavkům na dodržování bezpečnostních a hygienických předpisů, používání předepsaných bezpečnostních postupů, používání bezpečných zařízení a výstroje předepsanými osobními ochrannými pracovními prostředky pro danou činnost. [6]

Za tímto účelem jsou sepsána pravidla BOZP. Cílem tohoto snažení je, aby se zaměstnanci vraceli domů z práce zdraví.

1.2.2.3 Ochrana IT

Ochrana zabezpečení IT, je oblastí bezpečnosti, která je chápána většinou organizací jako nejohroženější oblast podnikání. Proto jí většina firem přikládá velký význam. „Hovoříme-li o problematice ochrany informací dat, komunikačních a datových systémů v podniku, můžeme jinými slovy hovořit o obranném zpravodajství, či podnikové kontrašpionáži." [11]

Při ochraně IT se všeobecně jedná o dva typy hrozeb, lidský faktor, který je rozhodujícím faktorem při ochraně dat a technický faktor, který je v mnoha případech ovlivněn také lidským faktorem.

Škody, které nám mohou vzniknout, můžeme rozdělit na přímé a nepřímé ztráty:

„Přímé ztráty- vyzrazení obchodních záměrů, výsledků výzkumu či možnosti uplatnění výsledku, důsledky nelegálních finančních transakcí, zvýšené náklady na obnovení ztracených informací či obnovení výroby v důsledku nuceného přerušení výroby či expedice zboží aj.

Nepřímé ztráty – ztráta dobrého jména podniku, protože nebyly dodrženy dohodnuté podmínky, čímž dochází k finančním ztrátám aj." [11]

Velké a střední firmy vynakládají na zabezpečení této oblasti nemalé částky, to jim ale nezaručuje, že mají tuto oblast dobře zabezpečenou. Velké investice není zárukou velké záruky bezpečnosti.

1.2.2.4 Požární ochrana

Požární ochrana slouží k prevenci před hrozbou požáru. Jejím úkolem je tedy předcházet škodám na zdraví osob nebo škodám na majetku. K prevenci slouží soubor pravidel požární ochrany.

Požární prevence zahrnuje tyto požadavky:

- udržování volné únikové cesty (chodby, schodiště, východy, ...)
- elektrické spotřebiče a zdroje tepla nesmí být ponechány v provozu bez dozoru
- dodržovat bezpečné vzdálenosti pro hořlavé materiály od zdrojů tepla
- uniklé hořlavé kapaliny musí být ihned zachyceny vhodným sorbentem a tento zlikvidován uložením v předepsaných nádobách
- kontrolovat, aby všechny hasící přístroje byly na místě , v provozu schopném stavu a byl k nim volný přístup, aby byl přístup ke všem požárním hydrantům, a kontrolovat neporušenost požárních hlásičů
- být seznámen s evakuačními plány v případě mimořádné události

zachovávat správný systém záznamů a hlášení [6]

Dokument pravidel požární ochrany slouží jednak k prevenci, ale také k seznámení s postupem při požáru, tak s činnostmi po něm bezprostředně navazujících.

1.2.1 Účel bezpečnostní politiky

„Význam bezpečnostní politiky organizace spočívá právě v tom, že podává ostatním subjektům informaci o vztahu organizace k výše uvedeným hodnotám a současně je základním účinným nástrojem k formulaci konkrétních problémů v oblasti bezpečnosti organizace a jejich následné realizaci.“ [6]

Účelem bezpečnostní politiky je tak podle obecně přijímaných hledisek:

- snížit riziko lidské chyby, krádeže, podvodu nebo zneužití prostředků organizace

- zajistit, aby si uživatelé byli vědomi bezpečnostních hrozeb a otázek s nimi spjatých a byli připravení se podílet na dodržování politiky bezpečnosti informací v průběhu své běžné práce
- minimalizovat škody způsobené bezpečnostními incidenty a chybami, sledovat je a učit se z nich

Mimo uvedený účel by měla bezpečnostní politika podniku zabezpečit čtyři cíle:

- zajistit bezpečnost firmy
- posilovat její důvěryhodnost
- zajistit dostupnost informací, při zachování jejich ochrany
- posilovat konkurenceschopnost

1.2.2 Obecný postup při zpracování bezpečnostní politiky

Při zpracování bezpečnostní politiky podniku se musíme nejdříve rozhodnout, kdo bezpečnostní politiku zpracuje.

Můžeme si vybrat ze tří možností:

- vypracování externí firmou
- vypracování vlastními zaměstnanci
- kombinací obou

Vypracování externí firmou

První možností, která se jeví zdánlivě nejjednodušší, je možnost zadání zpracování bezpečnostní politiky externí firmě. Tedy organizace se nemusí o nic starat, poskytne externistům pouze potřebné údaje, ti vše vyhodnotí, zpracují, a výsledek předají zadavateli. Tato varianta má, ale samozřejmě svá úskalí. Externí firma si nechá za své služby zaplatit, to je ale ten nejmenší problém. Mnohem závažnějším problémem je, existence možnosti, že externí firma ze zadání správně nepochopí požadavky a potřeby firmy. Firma se může dostat k informacím, které můžou ohrozit know-how podniku, příp. charakteru obchodního tajemství což může v případě úniku informací ohrozit podnikatelské aktivity. V neposlední řadě pak může externí firma zpracovat takovou bezpečnostní politiku, s kterou se neztotožní zaměstnavatelé podniku, tím pádem bude téměř nemožné ji prosadit, tak aby

efektivně fungovala. Pokud se organizace rozhodneme pro tuto možnost, je velmi důležitá správná volba zpracovatele.

Vypracování vlastními zaměstnanci

Druhou možností je využití vlastních zaměstnanců. Toto řešení má nesporné výhody, především z ekonomických a personálních důvodů. Využití vlastních zaměstnanců má výhodu i v kontinuitě zpracování dalších navazujících dokumentů, které jsou součástí bezpečnostní politiky podniku např. interní předpisy nebo pravidla požární ochrany. Hlavní výhodou ale je znalost prostředí a potřeb firmy. Další výhodou je snížení rizika úniku informací mimo firmu. Ale i toto řešení má své nevýhody, na jedné straně to může být nezkušenost a nekvalifikovanost zaměstnanců k takovým úkolům, na straně druhé pak, pokud se jedná o běžné zaměstnance, nedostatek autority pro prosazení zpracovaných materiálů. Pokud se organizace rozhodne pro tuto možnost, musí si být jista, že pověření pracovníci zadaný úkol zvládnou a celý projekt zpracování a zavedení bezpečnostní politiky musí být zastřešen firemní autoritou.

Vypracování kombinací

Třetí možností je zpracování bezpečnostní politiky podniku je kombinace obou výše uvedených možností s využitím jejich výhod. Pracovní skupina je složena ze zaměstnanců podniku a zaměstnanců externí organizace. Vytvořením takovéto pracovní skupiny je zajištěna patřičná autorita závěrů této skupiny, protože úkol je chápán jako samostatný projekt a jako takový je zaštítěn garantem z řad vedoucích pracovníků firmy.

Kombinace členů pracovní skupiny zajišťuje na jedné straně znalost potřeb firmy s detailní znalostí pracovních činností garantovanou zaměstnanci a na straně druhé je odborná znalost garantovaná externími pracovníky.

Výsledek závisí od spolupráce všech členů, ale tady je také největší úskalí, protože pracovní skupina nemusí být týmem, který je schopen spolupracovat na požadované úrovni a výsledek tak může zůstat za očekáváním, protože všichni si splní pouze svoji smluvně upravenou povinnost, ale nic navíc.

1.2.2.1 Seznam činností zpracování

Důležitým aspektem při zpracování bezpečnostní politiky podniku je komplexnost dané problematiky. Žádná z jednotlivých oblastí by neměla být upřednostňována, ale všechny oblasti by měly být brány jako rovnocenné a tvořit jeden celek.

Při samotném zpracování bezpečnostní politiky je vhodné dodržovat následující postup:

- zjistit výchozí stav
- zpracovat zadání požadavku na bezpečnostní politiku
- provést analýzu rizik
- vypracovat bezpečnostní politiku podniku
- realizovat odsouhlasenou bezpečnostní politiku
- zpracovat bezpečnostní dokumenty nižší úrovně
- provádět kontrolu a vyhodnocování bezpečnostní politiky

Výchozí stav

Zjištění výchozího stavu se doporučuje, ale není nutné. Jedná se o finančně nenáročnou studii, která ale může významně zkrátit proces vypracování bezpečnostní politiky a tím ho i zlevnit. Může sloužit také k přesnější formulaci požadavků. Tato jednoduchá studie by měly především zjistit aktuální stav právního rámce bezpečnostní politiky, zjistit případná nová rizika, které mně nutí bezpečnostní politiku zpracovat nebo aktualizovat a v neposlední řadě by měla odpovědět, jaký je současný stav zabezpečení firmy a zda již organizace bezpečnostní politiku má.

Zadání

Předmětem zadání je definice konkrétních požadavků na vypracování bezpečnostní politiky podniku, toto zadání je možné na základě připomínek zpracovatele doplnit či upravit a takto odsouhlasené zadání slouží jako základní podklad pro vypracování bezpečnostní analýzy.

Analýza rizik

Úkolem analýzy rizik je vyhodnocení základních pojmů bezpečnosti. Především se jedná o odpověď na otázku jaké má společnost aktiva, čeho si nejvíc cení. V této souvislosti se analýza zabývá zranitelností podniku, jaké hrozby mu hrozí, jaké z toho vyplývají rizika. Navrhují se opatření, jak tyto ohrožení eliminovat a jak má být požadované ochrany dosaženo. Na základě určení rizik se určuje také stupeň ohrožení.

[Zdroj: Systemonline]

Obr. 4 Analýza rizik

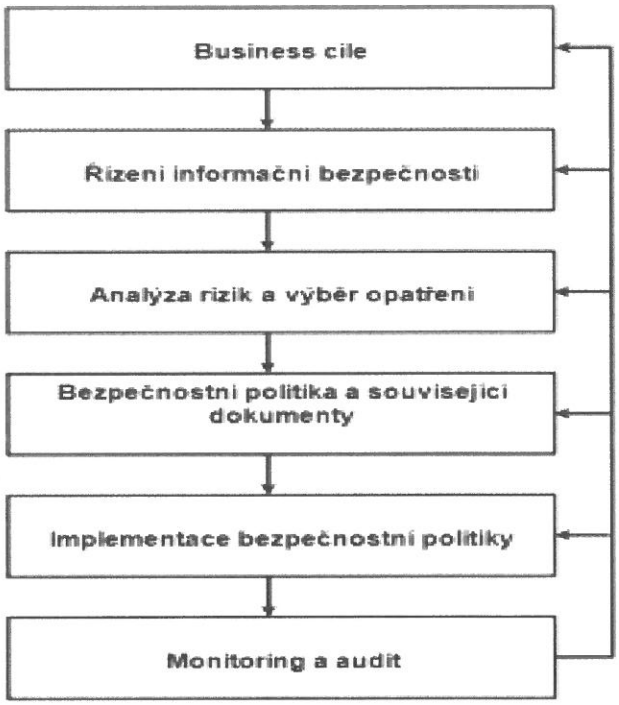
Zjednodušeně řečeno, analýza na základě zjištěných informací odpoví na otázky, co chránit, proti čemu a jakým způsobem.

Vypracování bezpečnostní politiky

Pro zpracování bezpečnostní politiky musíme mít na zřeteli, že jejím obsahem z obecného hlediska musí být stanovení účelu, závaznost pro zaměstnance garance ze strany vedené

podniku, předpisy, havarijní plány a definici požadovaných zabezpečení vč. jejich úrovně, interní normy.

Na začátku vypracování bezpečnostní politiky je požadavek vedení podniku na novou bezpečnostní politiku nebo na její aktualizaci. Po zjištění stávající úrovně zabezpečení, ověření právního rámce (legislativy), jsou poskytnuty zpracovateli informace o specifických činnostech podniku. Následuje provedení vstupní analýzy a zpracování vlastní bezpečnostní politiky.



[Zdroj: Smardcart]

Obr. 5 Schéma tvorby bezpečnostní politiky

Bezpečnostní politika je souhrn cílů, nástrojů, aktiv, systémových požadavků a normativ, bezpečnostního managementu, určení zodpovědností a taxativní uvedení legislativy.

Po vypracování jednotlivých kapitol musí být tyto předloženy k posouzení vedení podniku., jejich připomínky zapracovány a teprve následně může dojít k odsouhlasení dokumentu bezpečnostní politiky podniku. K úplnému dokončení vypracování bezpečnostní politiky je nutné zpracovat veškeré doklady pro technickou i netechnickou oblast organizace.

Realizace bezpečnostní politiky

Realizace bezpečnostní politiky je jeho nedílnou součástí, která bývá často neprávem podceňována. Součástí realizace je zavedení vypracované bezpečnostní politiky BP do praxe nemusí být snadné. Při bezpečnostních opatřeních dochází z hlediska zaměstnanců k zavádění nových opatření, která je svým způsobem omezují a částečně zatěžují i po pracovní stránce. Proto je velmi důležité věnovat velké úsilí seznámení zaměstnanců z důvody zavádění nových opatření, provádět jejich kvalitní proškolení a počítat s tím, že zavedení nové bezpečnostní politiky může trvat 1-5 měsíců. Vlastní provozování bezpečnostní politiky je jednou z jejích nejdůležitějších částí.

Zpracování bezpečnostní dokumentace nižší úrovně

Součástí realizace bezpečnostní politiky je také zpracování dokumentace, která navazuje na samotný dokument bezpečnostní politiky podniku. Jedná se především různé interní normy, zpracování pravidel BOZP, zpracování pravidel PO aj. Tato dokumentace nižší úrovně je zpracovávána téměř vždy zaměstnanci podniku. Objednání zpracování externí firmou je zcela vyjímečné. Důvodem je skutečnost, že se jedná o dokumenty, popisující konkrétní opatření a činnosti v podniku, které nejlépe znají zaměstnanci.

Vyhodnocování a provádění kontrol bezpečnostní politiky

Další součástí realizace bezpečnostní politiky je její soustavná kontrola a vyhodnocování monitoringu. Zavedením bezpečnostní politiky začíná její druhá etapa. Je nutné sledovat dodržování bezpečnostní politiky, provádět pravidelné kontroly a vyhodnocovat získané informace.

Úkolem kontrol je zjistit nakolik jsou zavedená opatření efektivní a odpovídají zadaným požadavkům, zda byly vynaložené náklady použity správně. Sleduje se také kvalita a účinnost opatření bezpečnostní politiky.

1.2.3 Bezpečnostní audit

Bezpečnostní audit je systematické hodnocení bezpečnostní politiky firem podle toho jak dobře odpovídá souboru stanovených kritérií. Důkladnou kontrolou obvykle hodnotí

bezpečnost systému fyzické ochrany. Bezpečnostní audity jsou často používány k určení právního souladu, v návaznosti na právní předpisy a ostatní doklady firemní bezpečnosti.

„Cílem bezpečnostního auditu je poskytnout managementu o stavu bezpečnosti organizace, které umožní managementu, aby při dosahování základních cílů organizace mohl přijmout opatření, která eliminují nebo alespoň minimalizují zjištěná bezpečnostní rizika."

Tyto audity mohou být pravidelné, ale z hlediska vypovídající schopnosti je vhodné také do systému zavést audity nepravidelné. Auditem můžou být pověření vlastní zaměstnanci nebo externí pracovníci. Podle toho rozdělujeme audity na interní a externí. U auditů interních musíme dbát na to, aby auditoři z řad zaměstnanců byli řádně proškolení a seznámeni s bezpečnostní politikou podniku.

Správným vyhodnocováním auditů dochází k ověření aktuálnosti bezpečnostní politiky, zjištění neshod. Díky tomu může dojít k úpravám bezpečnostního projektu, jeho aktualizaci, případně k odstranění chyb.

II. PRAKTICKÁ ČÁST

2 LEGISLATIVA BEZPEČNOSTNÍ POLITIKY

Legislativa bezpečnostní politiky není v současné době v právním řádu ČR upravená žádným samostatným zákonem. Proto legislativa komplexní bezpečnostní politiky podniku vychází z různých právních předpisů a na právní rámec této problematiky se proto musíme dívat také komplexně. To můžeme učinit ze dvou pohledů. Prvním pohledem je oblast základních právník norem a druhým oblast jednotlivých oblastí bezpečnostní politiky z pohledu platné legislativy.

2.1 Základní právní normy

Jak jsem již uvedl, není legislativa bezpečnostní politiky upravena samostatným zákonem. To ale neznamená, že se nemusí řídit legislativou a že není regulována právními předpisy. Mezi základní právní předpisy, kterými se musí řídit bezpečnostní politika podniku, patří:

- Listina základních práv a svobod
- Občanský zákoník
- Občanský soudní řád
- Obchodní zákoník
- Trestní zákon
- Trestní řád

Uvedené základní právní normy musíme chápat jako vyšší formu právní síly.

Mezi další právní předpisy, kterými se řídí bezpečnostní politika podniku, patří např.:

- Zákoník práce
- Zákon o bezpečnosti a ochraně zdraví při práci
- Zákon o požární ochraně
- Zákon o integrovaném záchranném systému
- Zákon o odpadech

Uvedené zákony však neřeší komplexní bezpečnost, ale pouze část chráněných zájmů. Integrujícím prvkem bezpečnosti by měla být právě bezpečnostní politika v oblasti ochrany osob, majetku a informací. Takovou bezpečnostní politiku má Česká

republika, a také řada resortů státní správy, krajských úřadů a organizací státní správy. Bezpečnostní politika je součástí interních předpisů bank, průmyslových podniků, obchodních, dopravních, telekomunikačních a bezpečnostních společností.

2.1.1 Listina základních práv a svobod

Byla vyhlášena ustanovením zákona č. 2/1993J a můžeme ji považovat za právní východisko bezpečnostní politiky. Je součástí ústavního pořádku České republiky. Protože, se jedná o vyšší právní normu je nutné v rámci Bezpečnostní politiky firmy, respektovat a dodržovat.

Z hlediska bezpečnostní politiky vymezuje Listina základních práv a svobod právní východiska práva na ochranu majetku a osob, tedy i bezpečnosti podniku a současně vymezuje rámec této ochrany, který nesmí být překročen, tak aby nedošlo k neoprávněnému zásahu do garantovaných práv a svobod osob. [6,10]

Konkrétně můžeme zmínit články, které mají přeneseně vliv i na bezpečnostní politiku podniků, jedná se např. o:

Článek 1: „Lidé jsou svobodní a rovní v důstojnosti i právech. Základní práva a svobody jsou nezadatelné, nezcizitelné, nepromlčitelné a nezrušitelné“

Článek 11: „Každý má právo vlastnit majetek“

Článek 12: „Obydlí je nedotknutelné.“

Článek 14: „ Svoboda pohybu a pobytu je zaručena.“

Článek 15: „ Svoboda projevu a práva na informace je zaručena.“

Článek 14: „ Každý se může domáhat zaručeným postupem svého práva u nezávislého a nestranného soudu a ve stanovených případech u jiného orgánu.“ [6]

2.1.2 Občanský zákoník

Další právní normou, která je z pohledu bezpečnostní politiky významná, je Občanský zákoník, zákon č. 40/1964 v jeho dosud platném znění. Poslední publikace všech jeho změn a doplňků byla uveřejněna ve sbírce zákonů pod č. 47/1992. Občanský zákoník

deklaruje ochranu práv občana i právnických osob. V souvislosti s bezpečnostní politikou podniku, z něho můžeme zmínit následující ustanovení:

§ 6: „Jestliže hrozí neoprávněný zásah do práv bezprostředně, může jej ten, kdo je takto ohrožen, přiměřeným způsobem odvrátit…"

§ 123: „Vlastník je v mezích zákona oprávněn předmět svého vlastnictví držet, požívat jeho plody a nakládat s ním."

§ 126: „Vlastník má právo na ochranu proti tomu, kdo do jeho vlastnických práv neoprávněně zasahuje…"

§ 415: „…Každý je povinen počínat si tak, aby nedošlo ke škodám na zdraví, na majetku, na přírodě a životním prostředí…"

§ 417: „…Komu hrozí škoda, je povinen k jejímu odvrácení zakročit způsobem přiměřeným okolnostem ohrožení…" "

U občanského zákoníku dojde s účinností od 1. ledna 2014 k významné změně, protože vejde v účinnost Nový občanský zákoník. Ten podepsal 20. 2. 2012 prezident republiky Václav Klaus. Nová norma občanského práva má 3081 paragrafů a provádí změny ve 238 právních předpisech.

Občanský zákoník je tematicky rozdělen do pěti částí – Obecná část, Rodinné právo, Absolutní majetková práva, Relativní majetková práva a Ustanovení společná, přechodná a závěrečná.

V obecné části jsou především vymezeny jednotlivé pojmy, se kterými následně text občanského zákoníku pracuje.

Část Rodinné právo v sobě zahrnuje dnešní zákon o rodině. Dotýká se jak institutu manželství, tak vztahů mezi příbuznými, zejména pak vztahů mezi rodiči a dětmi.

Část Absolutní majetková práva v sobě skrývá definici vlastnictví, práva k cizím věcem a problematiku dědění.

Čtvrtá část nazvaná Relativní majetková práva je nejobsáhlejší. Zahrnuje v sobě různé druhy smluv, stejně tak jako závazky z deliktního jednání (tedy i odpovědnost za škodu).

Poslední část se zabývá především legislativně technickou problematikou, mimo jiné tím, které dosavadní zákony budou novým zákonem zrušeny. [10]

Občanský soudní řád

Občanský soudní řád je zákonem č. 99/1963 Sb., který je základním pramenem občanského práva procesního.

Obsahuje právní úpravu civilního procesu: sporného i nesporného nalézacího řízení, řízení smírčích a zajišťovacích a řízení vykonávacího. Je tedy základní procesním nástrojem, jehož prostřednictvím soudy poskytují ochranu narušeným nebo ohroženým subjektivním právům a jiným zákony chráněným zájmům fyzických a právnických osob.

Mezi jeho základní ustanovení patří:

§ 1

Občanský soudní řád upravuje postup soudu a účastníků v občanském soudním řízení tak, aby byla zajištěna spravedlivá ochrana práv a oprávněných zájmů účastníků, jakož i výchova k zachovávání zákonů, k čestnému plnění povinností a k úctě k právům jiných osob.

§ 2

V občanském soudním řízení soudy projednávají a rozhodují spory a jiné právní věci a provádějí výkon rozhodnutí, která nebyla splněna dobrovolně; dbají přitom, aby nedocházelo k porušování práv a právem chráněných zájmů fyzických a právnických osob a aby práv nebylo zneužíváno na úkor těchto osob.

§ 3

Občanské soudní řízení je jednou ze záruk zákonnosti a slouží jejímu upevňování a rozvíjení. Každý má právo domáhat se u soudu ochrany práva, které bylo ohroženo nebo porušeno.

§ 5

Soudy poskytují účastníkům poučení o jejich procesních právech a povinnostech.

§ 6

V řízení postupuje soud v součinnosti se všemi účastníky řízení tak, aby ochrana práv byla rychlá a účinná a aby skutečnosti, které jsou mezi účastníky sporné, byly spolehlivě zjištěny.

Z hlediska bezpečnostní politiky občanský soudní řád není normou přímo zakotvující její podstatu, ale ovlivňuje a řídí samotný praktický výkon ochrany osob a majetku, především se dotýká externí spolupráce se soukromými, příp. detektivními firemními službami, jedná se především o shromažďování případných důkazů, výpovědí svědků a zastupováním firmy u projednání kriminálních deliktů. Jedná se o § 22, § 28, § 31, § 123, § 125 a § 126. [6]

U občanského soudního řádu došle k poslední novely zákona č. 7/2009 Sb. Hlavním cílem novely, která nabyla účinnosti 1. července 2009, bylo zjednodušení procesních postupů, snížení zatížení soudů a zamezení průtahů v soudním řízení.

V průběhu letošního roku dojde opět k projednání návrhu novely občanského soudního řádu. Jednou ze změn má být zpřísnění podmínek pro podání dovolání. Podle ministerstva spravedlnost se pak Nejvyšší soud bude zaobírat jen skutečně závažnými případy. [6]

2.1.3 Obchodní zákoník

Zákon č. 513/1991 Sb. (obchodní zákoník) upravuje postavení podnikatelů, obchodní závazkové vztahy (tzv. obchodní právo), jakož i některé jiné vztahy s podnikáním související, a zapracovává příslušné předpisy Evropských společenství. Zákon je rozdělen na čtyři části, které jsou kromě obecných ustanovení věnovány zejména ustanovením týkajícím se obchodních společností a družstev, obchodním závazkovým vztahům, zejména různým druhům smluv a ujednání. [7]

Z hlediska bezpečnostní politiky podniku má svůj význam obchodní zákoník, právě proto že upravuje podnikatelskou činnost viz. **§ 1**. Ta se dále řídí v obchodních vztazích především ustanoveními: [6]

§ 2 odst. 1 Podnikání se rozumí soustavná činnost prováděná samostatně podnikatelem vlastním jménem a na vlastní odpovědnost za účelem dosažení zisku.

§ 2 odst. 2 Podnikatelem podle tohoto zákona je:

a) osoba zapsaná v obchodním rejstříku,
b) osoba, která podniká na základě živnostenského oprávnění,
c) osoba, která podniká na základě jiného než živnostenského oprávnění podle zvláštních předpisů,

d) osoba, která provozuje zemědělskou výrobu a je zapsána do evidence podle zvláštního předpisu.

Pro účel podnikání bezpečnostních služeb v rámci bezpečnostní politiky podniku jsou důležitá také ustanovení podle § 261 a § 269. Tyto části zákona upravují závazkové vztahy mezi podnikateli a upravují typy smluv pro zabezpečení dohodnuté činnosti, tedy i služeb v rámci bezpečnostní politiky podniku. [6]

2.1.4 Trestní zákon

Trestní zákon je trestním kodexem, který popisuje jednotlivé trestné činy a tresty. Od 1. ledna 2010 nabyl účinnosti nový trestní zákoník. Jedná se o zákon č. 40/2009 Sb. Jedná se o právní normu trestního práva hmotného.

Trestní zákon má již ve svém ustanovení § 1 a § 2 deklarovánu ochranu práv a osob, neboť jeho prostředky mají ochránit důležité společenské vztahy, tedy i ochranu majetku a osob, mají porušovatele této ochrany od jednání odradit. Přesto se takové činy dějí a jsou označovány v § 3 jako činy trestné. [6]

Trestní zákon je důležitým pramenem práva také pro bezpečnostní politiku, protože definuje pojmy jako nutná obrana v § 13 a krajní nouze v § 14: „Čin, jinak trestný, kterým někdo odvrací nebezpečí přímo hrozící nebo trvající útok na zájem chráněný tímto zákonem, není trestným činem. Nejde o nutnou obranu, byla-li ochrana zcela zjevně nepřiměřená způsobu útoku. Čin jinak trestný, kterým někdo odvrací nebezpečí přímo hrozící zájmu chráněnému tímto zákonem, není trestným činem. Nejde o krajní nouzi, jestliže bylo možno toto nebezpečí za daných okolností odvrátit jinak anebo způsobený následek je zřejmě stejně závažný nebo ještě závažnější než ten, který hrozil. [6]

Obecně lze říci, že nový trestní zákon klade větší důraz na ochranu života, majetku a dalších individuálních práv, když tyto zájmy staví před zájmy společnosti a státu. To se projevuje i v systematice zákona, kde jsou (na rozdíl od současného trestního zákona) na první místo řazeny trestné činy proti životu a zdraví, rodině a dětem, svobodě a lidské důstojnosti. [6]

2.1.5 Trestní řád

Trestní řád je zákonem č. 141/1961 Sb., stejně jako u občanského soudního řádu je trestní řád právním pramenem pro přímý výkon bezpečnostních metod. Trestní řád upravuje normy trestního řízení. Tímto právním předpisem se zejména vymezuje postup a činnost orgánů činných v trestním řízení při zjišťování trestných činů, jejich pachatelů a potrestání těchto pachatelů. Zákon také stanoví práva a povinnosti osoby, proti které se řízení vede, a dalších osob zúčastněných na řízení (svědci, obhájci, znalci, tlumočníci apod.). [6,10]

§ 1 odst. 1Účelem trestního řádu je upravit postup orgánů činných v trestním řízení tak, aby trestné činy byly náležitě zjištěny a jejich pachatelé podle zákona spravedlivě potrestáni. Řízení přitom musí působit k upevňování zákonnosti, k předcházení a zamezování trestné činnosti, k výchově občanů v duchu důsledného zachovávání zákonů a pravidel občanského soužití i čestného plnění povinností ke státu a společnosti.

§ 1 odst. 2 Pomáhat k dosažení účelu trestního řízení je právem a podle ustanovení tohoto zákona i povinností občanů.

Trestní řád rozvíjí některá práva deklarovaný Listinou základních práv a svobod, kterým je např. právo na obhajobu viz. § 2 odst. 13. Dále opět v souvislosti především s činností bezpečnostních služeb můžeme zmínit § 42, § 43, § 50 a § 76 odst. 2, které upravují zadržení pachatelů při trestném činu, právo na obhajobu, práva poškozené osoby, vč. práva zvolit si zmocněnce a práva obhájce.

Původní podoba trestního řádu byla mnohokrát měněna a upravována pozdějšími zákony, od listopadu 1989 do poloviny roku 2006 došlo k 38 novelizacím a do textu zákona rovněž šestkrát zasáhl svými nálezy Ústavní soud.

Trestní řád je označení pro zákoník, který uceleným způsobem upravuje normy trestního řízení. Jde o zákoník trestního práva procesního. Tímto právním předpisem se zejména vymezuje postup a činnost orgánů činných v trestním řízení při zjišťování trestných činů, jejich pachatelů a potrestání těchto pachatelů. Zákon také stanoví práva a povinnosti osoby, proti které se řízení vede, a dalších osob zúčastněných na řízení (svědci, obhájci, znalci, tlumočníci apod.).

2.1.6 Legislativa ochrany informačních technologií

Současná legislativa ČR ukládá povinnost zpracovávání bezpečnostní politiky pouze v několika případech. Mezi nejdůležitější právní předpisy v uvedené oblasti patří zejména o zákony č. 101/2000 Sb. o ochraně osobních údajů a o změně dalších zákonů který upravuje ochranu osobních údajů, zákon č. 227/2000 Sb. a zákon č. 412/2005 Sb., o ochraně utajovaných informací.

zákon č. 101/2000 Sb.

Tento zákon v souladu s právem Evropských společenství, mezinárodními smlouvami, kterými je Česká republika vázána, a k naplnění práva každého na ochranu před neoprávněným zasahováním do soukromí upravuje práva a povinnosti při zpracování osobních údajů a stanoví podmínky, za nichž se uskutečňuje předání osobních údajů do jiných států.

zákon č. 227/2000 Sb.

Tento zákon upravuje v souladu s právem Evropských společenství používání elektronického podpisu, elektronické značky, poskytování certifikačních služeb a souvisejících služeb poskytovateli usazenými na území České republiky, kontrolu povinností stanovených tímto zákonem a sankce za porušení povinností stanovených tímto zákonem.

zákon č. 412/2005 Sb.

Tento zákon upravuje zásady pro stanovení informací jako informací utajovaných, podmínky pro přístup k nim a další požadavky na jejich ochranu, zásady pro stanovení citlivých činností a podmínky pro jejich výkon a s tím spojený výkon státní správy.

Další legislativou, která upravuje definici bezpečnostní politiky podniku v oblasti IT je:

- zákon č. 56/2006 Sb., o prevenci závažných havárií.
- zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících právem autorským (tzv. autorský zákon)
- zákon č. 127/2005 Sb. o elektronických komunikacích
- zákon č. č. 206/2005 Sb., o ochraně některých služeb v oblasti rozhlasového a televizního vysílání a služeb informační společnosti

- zákon č. 480/2004 Sb., o některých službách informační společnosti
- ÚOOÚ [10]vyhláška č. 366/2001 Sb. k zákonu o elektronickém podpisu
- další legislativa (vyhlášky, standardy atd.) MV ČR, ÚOOÚ, NBÚ[11] apod.

Přímým dopadem na podnik je např. ustanovení dle novely zákona č. 480/2004 Sb., o službách informační společnosti, které stanoví po úpravě pokutu až do výše 10.000 000,- Kč, kterou může Úřad pro ochranu osobních údajů udělit právnické osobě, která hromadně nebo opakovaně šíří elektronickými prostředky obchodní sdělení:

- bez souhlasu adresáta
- neoznačené jasně a zřetelně jako obchodní sdělení
- skrývající nebo utajující totožnost odesílatele, jehož jménem se komunikace uskutečnila
- neobsahující platnou adresu, na niž by adresát mohl odeslat žádost o ukončení takové komunikace
- nebo bez toho, že by zákazníkovi poskytla možnost jasně, zřetelně, jednoduchým způsobem, zdarma nebo na svůj účet udělit či odmítnout souhlas s využitím jeho elektronického kontaktu při zaslání každé jednotlivé zprávy

Některé z uvedených povinností nejsou jen předmětem ochrany z pohledu IT, ale dotýkají se také jiných oblastí. Tak je tomu např. u zákona na ochranu osobních údajů, který řeší ochranu osobních dat a nakládání s osobními údaji vč. jejich zneužití také v oblasti personální a mzdové. Především tím, že v rozsahu působnosti tohoto zákona stanoví, kdo je oprávněn ověřovat osobní údaje a jak s nimi musí nakládat, aby nemohly být zneužity.

---

[10] ÚOOÚ- Úřad pro ochranu osobních údajů

[11] NBÚ – Národní bezpečnostní úřad

Nově byla do zákona o službách informační společností vložena možnost postihovat za šíření nevyžádaných obchodních sdělení i fyzické osoby, které nejednají v rámci jejich podnikatelské činnosti, a které poruší výše uvedené podmínky pro zasílání obchodních sdělení. Pokuta je v tomto případě až do výše 100.000,- Kč.

Dne 1. ledna 2012 nabyl účinnosti zákon č. 468/2011 Sb., o elektronických komunikacích, kterým došlo mj. k novelizaci zákona o elektronických komunikacích, zákona o ochraně osobních údajů a zákona o službách informační společnosti.

V rámci legislativy Evropské unie je problematika ochrany IT řešena směrnicí 1995/46/ES o ochraně osobních dat a informační bezpečnost převzala tuto směrnici také do norem ČSN ISO/IEC.

Pro rok 2012 jsou avizovány změny, které jsou připraveny Evropskou komisí v oblasti ochrany osobních údajů, kde se očekává v souladu s materiálem vypracovaným v roce 2010, revize směrnice o ochraně osobních údajů z roku 1995, která je již zastaralá.

2.1.7 Legislativa bezpečnosti a ochrany zdraví při práci

Oblasti BOZP se týkají stovky právních předpisů - zákonů, vyhlášek a nařízení vlády, stejně jako směrnic EU. Z množství právních nařízení je zřejmé, že se jedná o významnou oblast nejen bezpečnostní politiky podniku, ale také pracovního práva vůbec.

Legislativní povinnosti v oblasti bezpečnosti a ochrany zdraví při práci, vyplývají především z ustanovení Zákoníku práce, kde se v § 101 odst. 1 vysloveně uvádí:

„ Zaměstnavatel je povinen zajistit bezpečnost a ochranu zdraví zaměstnanců při práci s ohledem na rizika možného ohrožení jejich života a zdraví, které se týkají výkonu práce…“ [6]

Základní zákony a právní předpisy, které upravují BOZP:

- 262/2006 Sb., zákoník práce
  Toto je hlavní předpis ošetřující mj. základní otázky bezpečnosti a ochrany zdraví při práci.

- 309/2006 Sb., zákon o zajištění dalších podmínek BOZP

Doplňuje zákoník práce dalšími povinnostmi, zejména technického a kvalifikačního charakteru.

- 251/2005 Sb., zákon o inspekci práce
  Zde jsou stanoveny práva a povinnosti inspektora inspekce práce a také sazebník pokut za nedodržení povinností v oblasti BOZP.

- 174/1968 Sb., zákon o státním odborném dozoru nad BOZP
  Stále platný a účinný zákon o státním odborném dozoru. Po všech novelách určuje spíše jen obecný rámec, konkrétní podmínky jsou v zákoně o inspekci práce.

Přímým dopadem legislativy v oblasti BOZP jsou povinnosti podnikatelů k zaměstnancům. Především se jedná o následující povinnosti:

- Identifikovat rizika možného ohrožení zdraví zaměstnanců, zjišťovat jejich příčiny a zdroje a přijímat opatření k jejich odstranění
- Nelze-li rizika odstranit, je zaměstnavatel povinen je vyhodnotit a přijmout opatření k omezení jejich působení tak, aby ohrožení bezpečnosti a zdraví zaměstnanců bylo minimalizováno
- Poskytovat zaměstnancům osobní ochranné pracovní prostředky a ochranné nápoje
- Provádět kategorizaci prací a informovat zaměstnance o tom, do jaké kategorie byla jím vykonávaná práce zařazena
- Určit osoby zodpovědné za provoz a údržbu tlakových nádob, zdvihacích zařízení, manipulačních vozíků s vlastním pohonem, …
- Stanovit a rozvrhnout pracovní dobu
- Vést evidenci pracovní doby
- Plnit povinnosti týkající se pracovních úrazů a nemocí z povolání, vyšetřovat příčiny vzniku úrazu, vést evidenci, zajišťovat opatření proti vzniku úrazu

- Zajistit periodické školení zaměstnanců v oblasti BOZP dle aktualizované osnovy školení
- Sdělit zaměstnancům, které zdravotnické zařízení jim poskytuje závodní preventivní péči a umožnit zaměstnancům účastnit se lékařských preventivních prohlídek a mimořádných preventivních prohlídek
- Zajistit zaměstnancům poskytnutí první pomoci
- Zajistit, aby stroje, technická zařízení, dopravní prostředky, přístroje a nářadí byly z hlediska BOZP vhodné pro práci, při které budou používány
- Zajistit, aby pracoviště byla prostorově a konstrukčně uspořádána a vybavena tak, aby pracovní podmínky pro zaměstnance z hlediska BOZP, odpovídaly bezpečnostním požadavkům a hygienickým limitům na pracovní prostředí a pracoviště
- Umístit bezpečnostní značky a zavést signály, které poskytují informace nebo instrukce týkající se BOZP a seznámit s nimi zaměstnance
- Zaměstnavatel je povinen organizovat práci a stanovit a provádět pracovní postupy tak, aby byly dodržovány zásady bezpečného chování na pracovišti

Přímým dopadem je také to, že za nesplnění povinností a porušení právních předpisů v oblasti BOZP hrozí podniku sankce až do výše 2.000.000,- Kč.

S účinností od 1. 4. 2012 bylo ve Sbírce zákonů zveřejněno nařízení vlády č. 93/2012 Sb., kterým se mění nařízení vlády č. 361/2007 Sb., kterým se stanoví podmínky ochrany zdraví při práci.

Hlavním důvodem novelizace nařízení vlády č. 361/2007 Sb., kterým se stanoví podmínky ochrany zdraví při práci, je povinnost harmonizovat český právní předpis s právem Evropské unie a sice implementovat třetí směrný seznam chemických látek podle směrnice Komise 2009/161/EU ze dne 17. prosince 2009.

Souběžně s touto úpravou se dává do souladu oblast problematiky chemických látek a nově i směsí ve smyslu chemického zákona. S tím souvisí i úpravy v části věnující se karcinogenům, mutagenům a látkám toxickým pro reprodukci.

Dále se upravuje, co se v tomto nařízení vlády rozumí rizikovými faktory pracovních podmínek. Samostatně se vymezuje výklad zátěže teplem v § 3, který upřesňuje, jakými kritérii je zátěž teplem vyjadřována. Za § 3 se vkládá nový § 3a - vymezení pojmů a § 3b, který upravuje zátěž teplem na pracovišti s neudržovanou a udržovanou teplotou a na venkovním pracovišti včetně hygienických limitů. Stanovují se hodnoty nastavení a chlazení pro klimatizovaná pracoviště, kde bude vykonávána pouze práce třídy I a IIa, tj, práce vsedě a dále přípustné hodnoty zátěže teplem pro klimatizovaná pracoviště, kde důvodem zavedení klimatizace jako technologického požadavku je ochrana výrobku, produktu nebo výroby.

Nově se zavádí dělení pracovišť třídy I a IIa podle nároků na kvalitu vnitřního prostředí na pracoviště kategorie A (vysoké nároky), kategorie B (střední nárok) a C (běžné podmínky).

Upravuje se i vyjádření dlouhodobě a krátkodobě únosné doby práce, jako doby přípustné a to včetně důlních pracovišť.

Pokud dojde k překračování přípustných hodnot zátěže teplem, uplatní se jako doposud režim střídání práce a bezpečnostní přestávky, což platí převážně na pracovišti, na němž je vykonávána práce s vyšší fyzickou zátěží, na pracovišti s trvalou technologicky nezbytně nutnou přítomností sálavé složky tepla a na venkovních pracovištích. U práce třídy I a IIa se naopak zdůrazňuje, že takový režim není nutný až do teploty 36 °C. Opatření k ochraně zdraví při práci i u těchto tříd však bude aplikováno ve formě náhrady ztráty tekutin prostřednictvím ochranného nápoje již za podmínky překročení teploty 31 °C.

Dále se upřesňují pojmy aklimatizovaný a neaklimatizovaný zaměstnanec. Za aklimatizovaného zaměstnance se považuje zaměstnanec vykonávající práci po dobu alespoň 3 týdnů od nástupu na posuzované pracoviště. U neaklimatizovaného zaměstnance vykonávajícího práci zařazenou do třídy IIb až V, pokud jsou při ní na pracovišti překračovány přípustné hodnoty zátěže teplem, uvedené v příloze č. 1 k tomuto nařízení, části A, tabulce č. 2, se po dobu 3 týdnů od nástupu na takové pracoviště dlouhodobě

přípustná doba práce upravená v příloze č. 1 k tomuto nařízení, části B, tabulkách 1a až 2c sníží o 30 %.

Nově se pak stanoví limit ztráty tekutin na pracovištích s délkou směny delší než 8 hodin, kde nesmí ztráta tekutin potem a dýcháním v důsledku pracovní a tepelné zátěže za směnu překračovat přípustný limit ztráty tekutin o více než 20 % a zároveň s tím nesmí být překračovány krátkodobě přípustné doby práce.

Ztráta tekutin nahrazovaná ochranným nápojem je nově odstupňovaná jak v měřené teplotě pro danou třídu práce, tak v náhradě tekutin. U náhrady ztráty tekutin pro třídu I až IIIa není striktně uváděno, že poskytovaný ochranný nápoj musí být vždy jmenovaná balená voda, ale že tyto druhy vod mohou být i ve formě jiné, tedy čerpány přímo ze zdroje.

V části věnující se větrání (§ 41) se upřesňují druhy větrání a stanoví se nový limit minimálního objemu vzduchu pro práce třídy I a IIa na pracovišti nevýrobního a výrobního charakteru. Přidává se další druh větrání – kombinované větrání.

Nově se upravuje osvětlování venkovního pracoviště.

Novela upravuje frekvenci úklidu a malování pracovišť a jejich sanitárních a pomocných zařízení.

2.1.7.1 Evropská legislativa bezpečnosti a ochrany zdraví při práci

V rámci evropské legislativy jsou pro bezpečnost práce směrodatné především Rámcové a Dílčí směrnice Rady, jedná se především o směrnice 89/391 EHS, o zavádění opatření pro zlepšení bezpečnosti a ochrany zdraví při práci a 89/654, o minimálních požadavcích na bezpečnost a ochranu zdraví na pracovišti.

2.1.8 Legislativa požární ochrany

Legislativa, která upravuje pravidla požární ochrany je dána zákonem č. 133/1985 Sb., zákon o požární ochraně, kde najdeme základní povinnosti fyzických i právnických osob v požární ochraně. Vyhláškou, která upřesňuje a doplňuje zákon o požární ochraně je vyhláška č. 246/2001 Sb., vyhláška o požární prevenci

Tyto dva základní právní předpisy, stanovují nejen postupy z hlediska bezpečnostní politiky podniku, ale také povinnosti státních orgánů, právnických i fyzických osob vztahující se k prevenci, ohlašování i likvidaci požáru či jiného požárního nebezpečí. Dále vymezuje status, povinnosti a postupy všech jednotek požární ochrany na území ČR. Zákon o požární ochraně také udává podmínky a výše sankcí při jeho porušení.

„Právnické osoby a podnikající fyzické osoby plní povinnosti na úseku požární ochrany ve všech prostorách, které užívají k provozování činnosti. Za plnění povinností na úseku požární ochrany u právnických osob odpovídá statutární orgán a u podnikajících fyzických osob tyto osoby nebo jejich odpovědný zástupce. Provozuje-li činnost v prostorách více právnických osob nebo podnikajících fyzických osob, plní povinnosti na úseku požární ochrany na místech, která užívají společně, vlastník těchto prostor, není-li smlouvou mezi nimi sjednáno jinak. Součástí smlouvy musí být i určení osoby odpovědné za plnění povinností na úseku požární ochrany.“ [7]

Další seznam právních předpisů, které se vztahují k požární ochraně:

Zákony

Zákon č. 133/1985 Sb., o požární ochraně ve znění pozdějších předpisů

Zákon č. 183/2006 Sb., o územním plánování a stavebním řádu (stavební zákon)

Zákon 11/ 2002 Sb., stanovuje vzhled a umístění bezpečnostních značek a zavedení signalizace

Zákon 238/ 2000 Sb., zákon o hasičském záchranném sboru ČR

Zákon 239/ 2000 Sb., o integrovaném záchranném systému a změně některých zákonů

Nařízení vlády

Nařízení vlády č. 91/2010 Sb., o podmínkách požární bezpečnosti při provozu komínů, kouřovodů a spotřebičů paliv

Vyhlášky

Vyhláška č. 246/2001 Sb., o stanovení podmínek požární bezpečnosti a výkonu státního požárního dozoru (vyhláška o požární prevenci)

Vyhláška č. 268/2009 Sb., o technických požadavcích na stavby

Vyhláška č. 23/2008 Sb., o technických podmínkách požární ochrany staveb

Vyhláška č. 202/1999 Sb., kterou se stanoví technické podmínky požárních dveří, kouřotěsných dveří a kouřotěsných požárních dveří

Vyhláška č. 499/2006 Sb., o dokumentaci staveb

Vyhláška 73/ 2010 Sb., o stanovení vyhrazených technických zařízeních

Vyhláška 87/ 2000 Sb., kterou se stanoví podmínky požární bezpečnosti při svařování a nahřívání živic v tavných nádobách

Z uvedeného přehledu legislativy vyplývají tyto konkrétní povinnosti pro právnické osoby a podnikající fyzické osoby:

- Začlenit provozované činnosti do kategorie dle § 4 zákona 133/1985 Sb.
- Obstarávat a zabezpečovat v potřebném množství a druzích požární techniku, věcné prostředky požární ochrany a požárně bezpečnostní zařízení se zřetelem na požární nebezpečí provozované činnosti a udržovat je v provozuschopném stavu. U vyhrazené požární techniky, věcných prostředků požární ochrany a požárně bezpečnostních zařízení, kromě výrobků stanovených podle zvláštních právních předpisů, 1i) lze instalovat a používat pouze schválené druhy.
- Vytvářet podmínky pro hašení požárů a pro záchranné práce, zejména udržovat volné příjezdové komunikace a nástupní plochy pro požární techniku, únikové cesty a volný přístup k nouzovým východům, k rozvodným zařízením elektrické energie, k uzávěrům vody, plynu, topení a produktovodům, k věcným prostředkům požární ochrany a k ručnímu ovládání požárně bezpečnostních zařízení.
- Dodržovat technické podmínky a návody vztahující se k požární bezpečnosti výrobků nebo činností.
- Označovat pracoviště a ostatní místa příslušnými bezpečnostními značkami, příkazy, zákazy a pokyny ve vztahu k požární ochraně, a to včetně míst, na kterých se nachází věcné prostředky požární ochrany a požárně bezpečnostní zařízení.
- Pravidelně kontrolovat prostřednictvím odborně způsobilé osoby, technika požární ochrany nebo preventisty požární ochrany dodržování předpisů o požární ochraně a neprodleně odstraňovat zjištěné závady.
- Umožnit orgánu státního požárního dozoru provedení kontroly plnění povinností na úseku požární ochrany, poskytovat mu požadované doklady, dokumentaci a

informace vztahující se k zabezpečování požární ochrany v souladu s tímto zákonem a ve stanovených lhůtách splnit jím uložená opatření.

- Poskytovat bezúplatně orgánu státního požárního dozoru výrobky nebo vzorky nezbytné k provedení požárně technické expertizy ke zjištění příčiny vzniku požáru.
- Bezodkladně oznamovat územně příslušnému operačnímu středisku hasičského záchranného sboru kraje každý požár vzniklý při činnostech, které provozují, nebo v prostorách, které vlastní nebo užívají.
- Právnické osoby a podnikající fyzické osoby nesmí vypalovat porosty.
- Při spalování hořlavých látek na volném prostranství, se zřetelem na rozsah této činnosti, stanovit opatření proti vzniku a šíření požáru.
- Spalování hořlavých látek na volném prostranství včetně navrhovaných opatření předem oznámit územně příslušnému hasičskému záchrannému sboru kraje, který může stanovit další podmínky pro tuto činnost, popřípadě může takovou činnost zakázat.
- Vlastník nebo uživatel zdrojů vody pro hašení požárů je povinen tyto udržovat v takovém stavu, aby bylo umožněno použití požární techniky a čerpání vody pro hašení požárů.
- Vlastník nebo uživatel lesů v souvislých lesních porostech o celkové výměře vyšší než 50 hektarů je povinen zabezpečit v době zvýšeného nebezpečí vzniku požáru opatření pro včasné zjištění požáru v lesích a proti jeho rozšíření pomocí hlídkové činnosti s potřebným množstvím sil a prostředků požární ochrany, pokud tak neučiní Ministerstvo zemědělství podle zvláštního zákona.

Pro právnické osoby a podnikající fyzické osoby provozující činnosti se zvýšeným požárním nebezpečím a s vysokým požárním nebezpečím jsou dále povinny:

- Stanovit organizaci zabezpečení požární ochrany s ohledem na požární nebezpečí provozované činnosti.
- Prokazatelným způsobem stanovit a dodržovat podmínky požární bezpečnosti provozovaných činností, případně technologických postupů a zařízení, nejsou-li

podmínky provozování činností a zabezpečování údržby a oprav zařízení stanoveny zvláštním právním předpisem.

- Zajišťovat údržbu, kontroly a opravy technických a technologických zařízení způsobem a ve lhůtách stanovených podmínkami požární bezpečnosti nebo výrobcem zařízení.
- Stanovit z hlediska požární bezpečnosti požadavky na odbornou kvalifikaci osob pověřených obsluhou, kontrolou, údržbou a opravami technických a technologických zařízení, pokud to není stanoveno zvláštními právními předpisy, a zabezpečit provádění prací, které by mohly vést ke vzniku požáru, pouze osobami s příslušnou kvalifikací.
- Mít k dispozici požárně technické charakteristiky vyráběných, používaných, zpracovávaných nebo skladovaných látek a materiálů potřebné ke stanovení preventivních opatření k ochraně života a zdraví osob a majetku.
- Prostřednictvím odborně způsobilé osoby zabezpečit posouzení požárního nebezpečí z hlediska ohrožení osob, zvířat a majetku a plnění dalších povinností na úseku požární ochrany. [7]

2.1.9 Legislativa ochrany objektů

Kromě základních právních předpisů, které byly zmíněny již v předchozích kapitolách, můžeme vymezit i další vybranou legislativu, která určuje podmínky ochrany objektů, jedná se především o zákon č. 239/2000 Sb., o integrovaném záchranném systému, který vymezuje integrovaný záchranný systém, zákon č. 258/2000 Sb., o ochraně veřejného zdraví, který vymezuje práva a povinností fyzických a právnických osob v oblasti ochrany a podpory veřejného zdraví, zákon č. 353/1999 Sb., o prevenci závažných havárií, který vymezuje širokou oblast havárií, jejich postupů a analýz vč. jejich prevence s ohledem na jejich současné technologie.

Z hlediska krizových situací musí bezpečnostní politika podniku počítat např. s již uvedeným zákonem o integrovaném záchranném systému, který stanoví pro právnické osoby možnost povinnosti poskytnout věcné zdroje, které jsou poskytnuty dobrovolně nebo povinně na základě žádosti o věcnou pomoc nebo z hlediska povinnosti toho, kdo způsobil

havárii, nebo činnost občanských sdružení se záchranářským nebo humanitárním zaměřením. Jde o to, využít pro záchranné a likvidační práce v potřebný okamžik každého, kdo je provádět záchranné a likvidační práce povinen, kdo pomoci může a kdo pomoci chce.

Z hlediska přímého dopadu na ochranu objektů, je však nutné zmínit především technické normy objektů.

Níže uvedený výběr technických norem řeší rozdělení a požadavky na prostředky zabezpečovacích systémů jedná se např. o:

- ČSN EN 50131-1

  Poplachové systémy - Elektrické zabezpečovací systémy uvnitř a vně budov.

  - tato evropská norma specifikuje elektrické zabezpečovací systémy. Popisuje čtyři stupně zabezpečení a čtyři třídy vlivu prostředí, dále popisuje sestavování zabezpečovacích systémů. Norma je určena jako vodítko pro pojišťovací společnosti, dodavatele elektrických zabezpečovacích systémů, uživatele a policii při stanovování kompletní a přesné specifikace ochrany pro konkrétní objekty.

- ČSN EN 50132-2-1

  Poplachové systémy - CCTV sledovací systémy pro použití v bezpečnostních aplikacích.

  - norma stanovuje minimální požadavky na specifikaci a zkoušení černobílých kamer používaných v systémech sledovacích systémů pro bezpečnostní aplikace.

- ČSN EN 50133-1

  Poplachové systémy - Systémy kontroly vstupů v bezpečnostních aplikacích.

  - tato norma popisuje všeobecné požadavky na funkčnosti systému kontroly vstupů pro použití v zabezpečovacích aplikacích.

- ČSN EN 50134-1

  Poplachové systémy - Systémy přivolání pomoci.

  - norma obsahuje doporučení poskytovatelům pro efektivní a účinné řídicí a organizační postupy pro instalaci, testování, obsluhu a údržbu systému přivolání pomoci včetně technického vybavení a organizování pomoci.

- ČSN EN 50136-1-1

  Poplachové systémy - Poplachové přenosové systémy a zařízení.

- norma stanovuje základní požadavky na provedení, spolehlivost a charakteristické bezpečnostní znaky poplachových přenosových systémů. Zahrnuje všeobecné požadavky spojení s podmínkou signalizace mezi poplachovým systémem a poplachovým přijímacím centrem.

Dále se jedná o normy upravující konkrétní zařízení s ohledem na bezpečnost objektu:

- ČSN 74 7731
  Dveře odolnější proti vloupání

- ČSN P ENV 1627
  Okna, dveře, uzávěry – odolnost proti násilnému vniknutí.
  - požadavky a klasifikace

- ČSN EN 1143-1
  Bezpečnostní úschovné objekty
  - požadavky, klasifikace a metody zkoušené odolnosti proti vloupání [10]

2.1.10 Ostatní legislativa

Předchozí uvedený přehled legislativy nepatří mezi vyčerpávající, ani dle uvedeného rozdělení nemohl obsáhnout všechny oblasti. Proto je nutné zmínit i legislativu některých dalších oblastí důležitých z pohledu bezpečnostní politiky podniku. Mezi takové patří hygiena práce nebo nakládání s odpady.

2.1.10.1 Hygiena práce

Z dalších oblastí, které můžeme zmínit jako součást bezpečnostní politiky je oblast hygieny práce. Tato problematika je upravena nařízením vlády 361/2007 Sb., podmínky ochrany zdraví při práci. Tato nařízení vlády nahradilo předchozí předpis 178/2001 Sb. Velkým dopadem na podniky může být požadavek na dodržení všech požadavků v rámci tohoto nařízení, vyžadovaná kontrolními orgány a následné sankce za jejich nedodržení. [7]

2.1.10.2 Nakládání s odpady

Důležitou oblastí legislativy, která má přímý vliv na činnost všech podniků, je oblast nakládání s odpady. Odpadové hospodářství firem je součástí environmentálních aspektů a jako takové ho můžeme zařadit do bezpečnostní politiky podniků. [9]

Povinnosti podniků vyplývají v současné době především ze zákona č. 185/2001 sb., o odpadech. Zákon se ale nevztahuje na všechny druhy odpadů. Samostatnou právní úpravu pak mají odpady, které neupravuje předchozí zákon.

Jedná se např. o:

- odpadní vody
- odpady z hornické činnosti
- odpady drahých kovů
- lidské ostatky
- konfiskáty živočišného původu
- nezachycené emise do ovzduší
- trhaviny, výbušniny a munice
- léky a návykové látky

Obecné povinnosti se týkají všech, kteří s odpadem v některé fázi nakládají. Základní povinnosti jsou:

- nakládat s odpady a zbavovat se jich pouze v souladu se zákonem
- předávat odpady do vlastnictví jen oprávněným osobám
- zajistit třídění odpadů a jejich nemíšení
- povinnost mít odpadového hospodáře pro podniky, které v uplynulých dvou letech nakládaly s více než 100 tunami ročně nebezpečného odpadu

Dále jsou povinnosti v oblasti nakládaní s odpady rozděleny podle fáze nakládaní s nimi např. pro původce, přepravce, zpracovatele apod.

Obecnou povinností je také odlišit výrobky, které podléhají zpětnému odběru výrobků a tím snížit celkové množství produkovaných odpadů. K této problematice byla vydána prováděcí vyhláška č. 352/2005 Sb. o nakládání s elektrozařízeními a elektroodpady. Tato povinnost je také plně v souladu se směrnicí Evropského parlamentu a Rady č. 2002/96/EC

o odpadních elektrických a elektronických zařízeních a směrnice Evropského parlamentu a Rady č. 2002/95/EC o omezení aplikací jistých nebezpečných látek v elektrických a elektronických zařízeních.

3 PŘEDSTAVENÍ SPOLEČNOSTI

Marius Pedersen A/S je přední dánskou společností, která se zabývá především moderními metodami nakládání se všemi druhy odpadů, výstavbu silnic s výstavbou sportovních zařízení, výstavbou a renovací speciálních povrchů na těchto objektech, a to nejen v Dánsku, ale i v dalších zemích Evropy.

3.1 Historie společnosti Marius Pedersen

Firma Marius Pedersen byla založena v roce 1925 jako společnost pro výstavbu silnic panem Marius Pedersenem, který byl v té době jediným vlastníkem firmy a ta se do konce šedesátých let zabývala převážně touto činností. Zajímavostí také je, že společnost vlastní několik patentů na technologie používané při realizaci silnic. Jedno z prvních osvědčení je i patent z roku 1935. V místním muzeu je umístěn jeden z prvních strojů na hutnění cest z roku 1935, který se dodnes dochoval. Dnes jsou samozřejmě společností patentovány podstatně modernější technologie, které se používají v celém světě. [3]

Začátkem sedmdesátých let, kdy se v Dánsku začaly seriózně řešit otázky spojené s likvidací a využitím odpadů, byla firma Marius Pedersen mezi prvními společnostmi, které se touto problematikou začaly zabývat.

V roce 2001 uzavřel Fond Marius Pedersen Dánsko s divizí odpadového hospodářství VIVENDI Environnement – ONYX holdingovou společnost. Marius Pedersen / ONYX Holding A/S.

Fond Marius Pedersen, jako vlastník stejnojmenné společnosti, se rozhodl zajistit ekonomickou stabilitu a pokračování dynamického rozvoje společnosti pro budoucí léta právě vytvořením společnosti s ONYX.

ONYX tímto potvrzuje pozici vedoucí společnosti v oblasti nakládání s odpady v Evropě a poskytuje služby ve více než 40 zemích světa. To řadí toto holdingové uskupení na třetí příčku na světě.

V prosinci 2002 získala VIVENDI Environnement nezávislost a díky důvěře významných investorů, akcionářů, samosprávných celků a průmyslových partnerů se výhradně koncentruje na poskytování služeb v oblasti vodohospodářství, odpadů, energetiky

a přepravy osob. V dubnu 2003 přijala firma rovněž novou identitu v podobě nového jména – VEOLIA Environnement. [3]

3.2 Marius Pedersen v ČR

Marius Pedersen navázala své první kontakty v tehdejším Československu v roce 1990. Hlavním předmětem podnikání bylo moderní řešení nakládání s odpady a jejich doprava. Zpočátku se firma zaměřila na oblast východních Čech a za své sídlo si zvolila město Hradec Králové, kde působí dosud. [3]

[Zdroj: Marius Pedersen]

Obr. 6 Sídlo společnosti v České republice

Firma, především ve svých začátcích, využila mnohaleté zahraniční zkušenosti i finanční zdroje k tomu, aby vytvořila systém nakládání s odpady, který by splňoval náročná evropská kritéria.

Během poměrně krátké doby se Marius Pedersen vypracoval v České republice na přední místo mezi subjekty zabývajícími se nakládáním s odpady.

V současné době provozuje firma v České republice 16 řízených skládek odpadů s ročním objemem uložených odpadů téměř 700 tis. Tun, dále zařízení na úpravu a zneškodňování

nebezpečných odpadů, solidifikační linky, vlastní recyklační a třídící zařízení a zařízení pro biodegradaci materiálů kontaminovaných ropnými produkty.

Díky vzniku holdingové společnosti Marius Pedersen / ONYX Holding A//S v polovině roku 2001 zaujímá společnost Marius Pedersen na českém trhu klíčovou pozici s celoplošnou působností.

Skupina firem nyní zaměstnává přes 2500 kvalifikovaných pracovníků.

Organizačně je společnost Marius Pedersen Group členěna na mateřskou společnost Marius Pedersen a.s. a 29 dceřiných společností. Skupina firem Marius Pedersen Group má více než 50 provozoven po celé České Republice. [13]

V současné době vstupuje firma Marius Pedersen v České republice na trh nakládání s odpady dvěma základními formami:

- formou společných podniků založených jak s municipálními partnery, tak s komerčními právnickými osobami,
- přímými aktivitami jako samostatná právnická osoba.

Všechny tyto subjekty velice úzce spolupracují při řešení a zajišťování jednotlivých projektů v rámci celé skupiny firem Marius Pedersen Group.

V rámci dalšího rozvoje svých aktivit je společnost Marius Pedersen a.s. připravena nabízet své služby prakticky ve všech regionech České republiky a současně dále zkvalitňovat a rozšiřovat rozsah nabízených služeb ve stávajících oblastech.

Firemní filosofie spočívá v poskytování efektivních a kvalitních služeb v komunální a komerční sféře při maximálně šetrném přístupu k životnímu prostředí. Přitom také úzce spolupracujeme s orgány státní správy a samosprávy působícími v oblasti životního prostředí. [2]

3.2.1 Činnosti společnosti Marius Pedersen

Do náplně činností společnosti Marius Pedersen patří všechny systémy nakládání s odpadem a to především:

- **výstavba a provozování zabezpečených a řízených skládek, včetně skládek s využitím bioplynu,**
- sběr, svoz a doprava průmyslových i domovních odpadů,
- různé systémy separovaného sběru domovního odpadu, vč. separovaného sběru nebezpečného odpadu z domácností, wet/dry systému,
- provozování skartačních systémů sběru, svozu a likvidace pro důvěrné dokumenty,
- výstavba a provozování zařízení pro kompostování „zelená frakce" odpadu,
- výkup, třídění a zpracování druhotných surovin,
- recyklace a znovuvyužití odpadů, včetně výstavby a provozování recyklačních závodů,
- systémy sběru, svozu a termické likvidace pro zdravotnická zařízení a další druhy nebezpečných odpadů,
- sanace starých ekologických zátěží,
- facility management,
- propracovaný počítačový systém evidence a sledování všech systémů nakládání s odpadem, jehož výstupy jsou cenným zdrojem informací nejen pro zákazníka, ale i pro firmu a především pro orgány státní správy a místních samospráv zabývajících se odpady,
- poradenská a konzultační činnost pro zákazníky,
- inženýrská a přípravná činnost spojená s přípravou a výstavbou těchto zařízení a systémů. [3]

4 SOUČASNÝ STAV BEZPEČNOSTNÍ POLITIKY MARIUS PEDERSEN

Přesto, že firma MPG patří ve svém oboru k leadrům na trhu a obratově se řadí k nejvýznamnějším firmám v rámci ČR, bylo zjištěno, že v otázce bezpečnostní politiky tomu tak rozhodně není. Firma nemá ucelenou koncepci zabezpečení svých firem a nemá dokonce ani vypracovaný dokument bezpečnostní politiky podniku. O tom, že je uvedená problematika u zmíněné firmy, tzv. „ na vedlejší koleji", svědčí také skutečnost, že neexistuje, ani přímá odpovědnost za tuto oblast. S tím souvisí i fakt že MPG nemá v rámci své personální struktury pozici obsazenou pozici bezpečnostního manažera. Pro zjištění současného stavu bezpečnostní politiky podniku MPG, byla s ohledem na nekomplexnost zvolena forma rozhovorů s vedoucími pracovníky a studium aktuálních interních materiálů (směrnic, nařízení, postupů, organizačních pokynů, ...). Pro lepší přehled a návaznost na předchozí kapitoly, je popis současného stavu bezpečnostní politiky podniku MPG členěn na ochranu objektů a majetku, bezpečnost a ochrana zdraví při práci, IT ochrana a požární ochranu.

4.1 Ochrana objektů a majetku

Jako první bylo provedeno seznámení se se zabezpečením ochrany objektů a majetku. V rámci MPG neexistuje závazný pokyn pro postup při zajišťování objektů, areálů a majetku. Součástí některých interních dokumentů jsou pouze kusé informace k této problematice. V organizační směrnici Organizační a pracovní řád je tak např. částečně upraven režim zabezpečení v rámci budovy centrály v Hradci králové. Konkrétně se jedná o klíčový režim a zabezpečení EZS. Není zde však již žádným způsobem řešeno zabezpečení jednotlivých provozoven MPG a k zabezpečení dceřiných společností je uvedena pouze odpovědnost ředitelů společností za toto zabezpečení. V provozních řádech skládkových zařízení pak zase můžeme v rámci popisu areálů nalézt zmínku o oplocení.

4.1.1 Klíčový režim

V organizační směrnici je uvedena odpovědnost za evidenci a výrobu klíčů a ukládání rezervních klíčů. Schéma oprávněných vstupů k systému generálního klíče schvaluje GŘ.

Každý zaměstnanec obdrží klíč, kterým lze odemknout zaměstnanecké vchody. Další úrovně přidělovaných klíčů umožňují odemykat kromě vstupů i příslušné povolené místnosti. Běžné provozní místnosti (kanceláře, zasedací místnosti, kuchyňky, sociální zařízení, jídelna) se nezamykají. Ztrátu klíče musí zaměstnanec neprodleně oznámit odpovědné osobě. Zaměstnancům je zakázáno pořizovat kopie klíčů.

4.1.2 Elektronický zabezpečovací systém

V rámci organizační směrnice je uvedený pouze postup přidělování bezpečnostních kódů a návaznost EZS na docházkový systém, především z pohledu povinností pro zaměstnance. Organizační směrnice neřeší požadavky na EZS. Ke schématu oprávnění EZS, jejich úrovně zabezpečení a rozsahu oprávnění je určena odpovědná osoba.

Kódy jsou rozděleny na stálé kódy (zaměstnanci, úklid, IT, technici, ...) a dočasné kódy (auditoři, příp. dle potřeby). Příslušné bezpečnostní kódy jsou sdělovány při předávání klíčů.

Při odchodu z pracoviště každý zaměstnanec zkontroluje, zda jsou zavřená okna. Při odchodu z budovy mimo pracovní dobu recepce je každý zaměstnanec povinen zkontrolovat na obrazovce umístěné vedle docházkového terminálu, zda se ještě někdo nachází v budově. Pokud není na monitoru zobrazeno žádné jméno, je povinen budovu zakódovat a vchod, kterým odchází, uzamknout. Klávesnice bezpečnostního systému je umístěna v recepci vedle docházkového terminálu. Po zakódování budovy je nutno do 30 sekund budovu opustit.

V případě setrvání v budově po stanovené hodině, je zaměstnanec povinen nahlásit svou přítomnost na PPC. V případě spuštění poplachu chybnou manipulací je třeba zadat bezpečnostní kód, který sirénu vypne. Zároveň je nutno vyrozumět pracovníky PPC na uvedeném telefonním čísle o tom, že se jednalo o planý poplach a zabránit tím zbytečným placeným výjezdům ostrahy.

Každý zaměstnanec je povinen zaznamenat příchod do budovy nebo odchod z budovy přihlášením se do docházkového systému v recepci.

4.1.3 Oplocení areálů

Text Jak bylo výše uvedeno, oplocení areálů je zmiňováno pouze popis areálů např. skládek, kde je tímto oplocením splněna pouze zákonná povinnost vyplývajících ze zákona č. 185/2001 Sb.

Jedná se o oplocení výšky 2 m z ocelového pletiva s využitím železobetonových nebo ocelových sloupků v betonových patkách po 3 metrech, se 2-3 řadami vrchních ostnatých drátů. Vjezdy a vstupy do areálů jsou zajištěny především mechanickým uzamykáním.

4.2 Bezpečnost a ochrana zdraví při práci

Bezpečnost a ochrana zdraví při práci je jednou ze základních činností, s kterou se setkáváme v rámci činnosti všech firem. Nejinak je tomu i u skupiny firem MPG.

Směrnice definuje rozsah základních činností v oblasti BOZP podle požadavků OHSAS[12] 18001 a je platná pro všechny dceřiné společnosti a generálního ředitele skupiny Marius Pedersen Group.

4.2.1 Zajišťování BOZP

Za zajišťování BOZP a dodržování předpisů zodpovídají všichni vedoucí zaměstnanci v rozsahu svých funkcí. Uvedená zodpovědnost se vztahuje i na vznik pracovních úrazů a havárií. Zajištění BOZP je nedílnou součástí plnění pracovních úkolů.

Funkce bezpečnostního technika není u organizace ustavena, plnění požadavků na úseku BOZP zajišťuje na základě smlouvy odborná firma jako kontrolní a poradní orgán vedoucího organizace (vedoucí provozu, resp., Provozní náměstek).

Kontrolní činnost na úseku BOZP je zajišťována průběžně všemi vedoucími zaměstnanci organizace. Jedenkrát za 3 měsíce zajistí odborná firma na úseku BOZP kontrolu na všech pracovištích.

---

[12] OHSAS – systém managementu bezpečnosti a ochrany zdraví při práci

Pro GŘ zajišťuje funkci bezpečnostního technika technik organizace, který následně plní požadavky na úseku BOZP. Kontrolu na pracovišti GŘ provádí tento pracovník 1x za 3 měsíce.

Jednou za rok organizuje vedoucí organizace prověrky bezpečnosti práce v souladu se Zákoníkem práce.

Vedoucí zaměstnanci odpovídají za plnění úkolů zaměstnavatele v péči o bezpečnost a ochranu zdraví při práci.

4.2.2 Školení BOZP

Systém periodických školení je součástí kvalifikace pro výkon práce. Každý zaměstnanec je povinen se zúčastnit školení. Neúčast bez řádné omluvenky, je považováno za hrubé porušení pracovní kázně.

Školení zaměstnanců o bezpečnosti práce a ochraně zdraví při práci se provádí zvlášť pro zaměstnance a zvlášť pro vedoucí zaměstnance. Školení jsou povinni absolvovat všichni zaměstnanci dle pracovního zařazení.

Jedná se o tyto druhy školení:

- vstupní (při nástupu do organizace)
- školení na daném pracovišti (při nástupu na dané pracoviště)
- opakované školení zaměstnanců (1 x za 2 roky)
- opakované školení vedoucích zaměstnanců (1 x za 3 roky)
- speciální školení řidiče z povolání (1 x za rok), řidič vysokozdvižného vozíku (1 x za rok), řidič referent (1 x za 2 roky), obsluha tlakových nádob (1 x za 3 roky)

O provedeném školení se musí vést záznam, který musí obsahovat osnovu školení (dle pracovního zařazení), datum školení, časový rozsah školení, podpis školeného, podpis školitele.

4.2.3 Ochranné pomůcky

Osobní ochranné pracovní prostředky (dále OOPP) jsou prostředky osobní ochrany, schválené příslušnou autorizovanou zkušebnou a určené k tomu, aby se zaměstnanci jejich

používáním chránili před riziky, která by mohla ohrozit jejich život, bezpečnost nebo zdraví při práci. Osobní ochranné pracovní prostředky jsou na základě legislativních předpisů používány všude tam, kde není možné zajistit bezpečnost při práci technickým řešením (technologie výrobního procesu, konstrukční provedení, organizační opatření apod.). Pro jednotlivé druhy prací jsou zaměstnanci vybavováni ochrannými pracovními pomůckami před započetím přidělené práce na základě vyhodnocených rizik.

Společnost zajistí osobní ochranné pracovní prostředky pracovníkům transportních divizí, pracovníkům skládky, v omezeném množství i technikům, kteří zajišťují kontrolu přidělených úkolů.

4.3 IT ochrana

Ke správě, řízení a zabezpečení v oblasti IT je vytvořený speciální oddělení. Jako u většiny firem je této oblasti věnována velká pozornost a nejinak je tomu také u firmy MPG. Všechny činnosti jsou podrobně popsány v interních dokumentech firmy, jakými jsou konkrétně např. organizační směrnice SPRÁVA ICT, organizační směrnice POUŽÍVÁNÍ ICT, pracovní postup PLÁNY KONTINUITY ICT.

4.3.1 Popis zabezpečení

V rámci uvedených dokumentů, dochází k přesnému popisu oblasti IT, od nákupu HW a SW až po jeho likvidaci. Interní dokumenty konkrétně popisují evidenci každého zakoupeného HW, kdy je ke každému novému hw přiřazeno evidenční číslo. Pořizování HW a SW, je standardní a jednotné.

Součástí zabezpečení je **zálohování dat**, které se provádí pomocí zálohovacího SW, který po zápisu vykoná automatickou verifikaci zapsaných dat. Ověření konzistence provedených záloh jsou prováděny dle Plánu monitoringu a kontrol ICT[13].

[13] ICT - Information and Communication Technologies

Dále standardně probíhá **ověřování identity uživatelů** a zařízení. Tyto funkce provádějí specializovaná ověřovací zařízení nebo software (servery) a ověřovací služby (ActiveDirectory) síťové infrastruktury - směrovačů, přepínačů, firewallů, VPN[14] koncentrátorů, bezdrátových přístupových bodů.

Mezi standardní zabezpečení patří v rámci nákupu licencí a platby poplatků patří např.: antivirová ochrana stanice, antivirová ochrana pošty, antispamová ochrana pošty, ochrana přístupu do Internetu.

Součástí ochrany IT je proces řízení přístupu, proces přidělování a odebírání přístupových oprávnění, vzdálený přístup. K zabezpečení přístupu a jednotlivých aplikací také standard při **nastavení hesel**, který obsahuje následující pokyny:

- vynucená délka hesla - minimálně 8 znaků
- vynucená obnova hesla systémem v cyklu 90 dnů
- heslo nelze opakovat 3x po sobě jdoucí
- heslo musí být komplexní

Součástí zabezpečení jsou i tzv. **podpůrná zařízení**, která mají zajistit např. nepřetržitou dodávku energie. Ta je zabezpečena generátorem a UPS. Na zálohované okruhy jsou napojeny zařízení a systémy, které zajišťují chod ICT a nejsou ohroženy obchodně-provozně aktivity společnosti. Protiproudová ochrana je zabezpečena proudovými chrániči. Teplota v prostorech serveru je monitorována podle Plánu monitoringu a kontrol.

Podpůrná zařízení	Zajišťuje	Kontroluje
_UPS zdroje	Desktop Administrator IT	Desktop Administrator IT
Generátor el. napětí	IRIUM s.r.o	IRIUM s.r.o
Klimatizace - server	A-Z Chlazení s.r.o.	A-Z Chlazení s.r.o.

[Zdroj: Marius Pedersen]

Tab. 1 Přehled podpůrných zařízení

[14] VPN - virtual private network

4.3.1.1 Ochrana proti škodlivým programům a mobilním kódům

Skupina MPG používá kombinovanou antivirovou ochranu. Používaný SW má předplacenou aktualizaci tak, že detekční AV systém odpovídá s minimálním zpožděním aktuálnímu stavu, který nabízí dodavatel. Odpovědnost za správu, rozsah nastavení a kontrolu má vedoucí administrátor IT (včetně desktopů a přenosných zařízení).

Eset NOD32

AV firmy Eset Software je používán k ochraně serverů i jednotlivých PC. Touto ochranou je detekována virová infiltrace, která již pronikla až na cílové zařízení. U tohoto AV je aktuálnost verzí i antivirové databáze hlídána centrálním softwarovým managementem výrobce instalovaným v GŘe. I přes aktivní funkce rezidentní ochrany je automaticky spuštěn detekovací proces skenování nejdůležitějších oblastí, jako jsou boot sektory, zavaděče systému, části operační paměti a systémové soubory podílející se na běhu relace. Tento proces je proveden při každém přihlášení uživatele, tedy při vytvoření nové relace.

Symantec Corporation

AV firmy Symantec Corporation je používán v rámci komplexní ochrany mailové komunikace v 1. stupni, tj. ochrana před nákazou příchozích mailů z vnějšího prostředí firmy. Díky kontinuálnímu aktualizování virových definic umíme čelit virové nákaze skryté v příchozích mailech.

ForeFront Security

AV firmy Microsoft je komplexním in-bandovým řešením v samotném mailovém serveru a tudíž poskytuje maximální ochranu mailové komunikace v 2. stupni, tj. vnitrofiremní komunikace, a výkon v rychlém vyhodnocení potenciální nákazy. ForeFront je obchodní označení produktu, který v sobě obsahuje více různorodých AV enginů, díky kterým se pokryje maximální možné riziko nákazy.

4.3.1.2 Obrana proti útokům

Ochranu zajišťují aplikační stavové firewally, Intrusion Protection systémy, software pro ochranu koncových stanic a serverů, systémy chránící před rozprostřenými útoky proti službám, bezpečnostní služby obsažené v síťové infrastruktuře - zejména ve směrovačích a přepínačích. Podstatnou roli v aktivní obraně hraje i systém pro monitorování bezpečnosti sítě. Tyto technologie zajišťují ochranu sítě a koncových zařízení před napadením.

Celkově můžeme konstatovat, že zabezpečení v oblasti IT je na potřebné úrovni. Problémem může být, ale samotné tvrzení o nezbytnosti uvedených kroků, o vytváření dojmu o nenahraditelnosti apod.

4.3.1.3 Bezpečný přenos dat

MPG používá k elektronické výměně dat vyhrazené datové linky uskupené do virtuální privátní sítě (VPN) produktově označeno MPLS. Každá lokalita DS nebo mobilní uživatel je bezpečně připojen do sítě. VPN je tvořena pomocí aktivních prvků CISCO po vyhrazených datových okruzích za použití technologií (SDSL, ADSL), tudíž je chráněna před vnějším prostředím. Službu VPN provozuje, zabezpečuje, monitoruje smluvní poskytovatel datových služeb,

4.3.1.4 Obrana proti útokům

Ochranu zajišťují aplikační stavové firewally, Intrusion Protection systémy, software pro ochranu koncových stanic a serverů, systémy chránící před rozprostřenými útoky proti službám, bezpečnostní služby obsažené v síťové infrastruktuře - zejména ve směrovačích a přepínačích. Podstatnou roli v aktivní obraně hraje i systém pro monitorování bezpečnosti sítě. Tyto technologie zajišťují ochranu sítě a koncových zařízení před napadením.

4.3.1.5 Ověřování identity uživatelů a zařízení

Tyto funkce provádějí specializovaná ověřovací zařízení nebo software (servery) a ověřovací služby (ActiveDirectory) síťové infrastruktury - směrovačů, přepínačů, firewallů, VPN koncentrátorů, bezdrátových přístupových bodů.

4.3.1.6 Ochrana dat pro testování

K ochraně produkčních aplikací a dat je použita identická kopie, tedy testovací prostředí, které odráží aktuální stav produkčního prostředí. V tomto prostředí jsou prováděny testovací činnosti k zjištění funkční či technologické změny v aplikačním SW či databázích. Testování provádí pověřená testovací skupina pro danou oblast. Na základě výstupu skupiny, tedy pokud provedené testy byly úspěšné, se provede uvolnění změny do produkčního prostředí. Po nasazení změny je zvýšena aktivita technické podpory ze strany dodavatele, který změnu dodal. Celou činnost koordinuje a schvaluje jednotlivé kroky

Manažer pro rozvoj IS. Každé kopírování provozních informací do testovacího systému je schváleno Manažerem ICT nebo Manažerem pro rozvoj IS a zaznamenáno do administrátorského deníku.

Trvale připojené testovací databáze na produkčním prostředí pro operativní simulace (MPG99New, MPGMainTest), jsou dostupné pouze v síti MPG na hlavním DB serveru, s řízeným přístupem

4.3.1.7 Umístění zařízení a jeho ochrana

Všechna zařízení jsou umístěna v uzamykatelných prostorách. Zvláště důležitá zařízení (servery, aktivní prvky, zálohovací zařízení), která přímo souvisí s nepřetržitým provozem infrastruktury a její bezpečností jsou chráněna ve vyhrazených uzamykatelných prostorách, které byly za tímto účelem vybudovány a splňují jak bezpečnostní tak technické parametry.

4.3.1.8 Bezpečnost kabelových rozvodů

Kabelové rozvody a jejich změny jsou možné pouze na základě projektu. Jejich rozvod je realizován v chráněných trasách tj. parapetní žlaby, trubkové vedení, který je zakončen na jedné straně datovou zásuvkou a na straně druhé patch panelem v rozvaděči umístěném ve vyhrazeném prostoru. Propojení zařízení na tyto rozvody je prováděno přes volně ležící síťový kabel o délce max. 3m, jehož narušení neohrožuje kabelový rozvod.

4.4 Požární ochrana

V rámci požární ochrany se MPG řídí zákonem č. 133/1985 Sb. o požární ochraně v platném znění a vyhláškou MV č. 246/2001 Sb., kterou se provádějí ustanovení zákona o požární ochraně. Tato směrnice byla vydána za účelem řízení a organizaci požární ochrany.

V souladu s tímto zákonem vydala firma organizační směrnici 22 Bezpečnostní předpis, jehož součástí jsou i ustanovení k požární ochraně. Ve směrnici jsou podrobně popsány

Problémem požární ochrany je skutečnost, že tato existuje především v písemné podobě, přispívá k tomu fakt, že všechny povinnosti jsou přeneseny na externí firmy a firma je tak z velké části odkázána na kvalitu dodavatelů požadovaných služeb. Jsou tak zajišťovány školení, návrh požárních opatření nebo prokázání shody.

4.4.1 Organizační směrnice

Organizační směrnice se vztahuje na všechny dceřiné společnosti a zařízení MPG. Účelem této směrnice je stanovit povinnosti pracovníků, jejich působnost na úseku požární ochrany, jakož i postavení při řízení požární ochrany tak, aby byly vytvořeny podmínky pro účinnou ochranu života a zdraví pracovníků a majetku před požáry.

4.4.2 Požární řád

Požární řád pracoviště upravuje základní zásady zabezpečování požární ochrany na místech, kde se provozují činnosti se zvýšeným požárním nebezpečím. Je zpracován dle vyhlášky MV ČR 246/2001 Sb., § 31, pro konkrétní zařízení jsou vypracovány požární řády skladů, skladů NO, hala, lisů, manipulačních ploch atd. V souladu se směrnicí jsou dále vydávány řády ohlašovny, záznamy o školení aj. dokumenty vztahující se k PO.

4.4.3 Odpovědnost za zajištění

Za zajištění požární ochrany v MPG odpovídá generální ředitel. Ve své působnosti je povinen soustavně pečovat o zabezpečení požární ochrany ve všech užívaných objektech jako o součást plnění pracovních úkolů. Řídí se přitom platnými předpisy o požární ochraně a pokyny územně příslušného Hasičského záchranného sboru.

Za zajištění požární ochrany na jednotlivých pracovištích odpovídající vedoucí pracovníci na všech stupních řízení v rozsahu svých funkcí. Jsou povinni řídit se pokyny generálního ředitele akciové společnosti a předpisy stanovenými pro vykonávanou pracovní činnost, právními a ostatními předpisy k zajištění požární ochrany.

4.4.4 Organizační zabezpečení

Organizační zabezpečení zajišťují na svých úrovních ředitelé, preventisté, členové požárních hlídek.

4.4.4.1 Ředitelé

Ředitel akciové společnosti a vedoucí pracovníci jsou povinni ve své působnosti soustavně pečovat o požární ochranu ve všech užívaných objektech jako o rovnocennou a

neoddělitelnou součást při plnění pracovních úkolů. Řídí se přitom platnými předpisy o požární ochraně. Pro řádné plnění těchto úkolů jsou povinni zejména:

- jmenovat preventisty požární ochrany příp. požární hlídku pracoviště, pokud by se jednalo o pracoviště se zvýšeným požárním nebezpečím
- stanovit organizaci požární ochrany
- stanovit povinnosti na úseku požární ochrany vedoucím a ostatním pracovníkům
- ustavovat do funkcí a činností na úseku požární ochrany pracovníky s požadovanou odbornou kvalifikací a způsobilostí
- jednou za tři roky zabezpečovat pravidelné školení na úseku požární ochrany vedoucích zaměstnanců odborně způsobilou osobou
- uložených orgány státního požárního dozoru projednávat hodnocení činnosti v požární ochraně, rozbory požárů vzniklých v organizaci a pokut
- podávat zprávy o případných požárech
- požadovat dodržování požadavků na požární ochranu v dlouhodobé výstavbě a dokumentaci staveb
- ch)uložit postihy pracovníkům, kteří hrubě porušují předpisy o požární ochraně

4.4.4.2 Preventisté požární ochrany

Preventisté požární ochrany jsou povinni:

- provádět preventivní prohlídky provádí v určeném úseku 1 x měsíčně, výsledek kontroly zapíše do požární knihy, kterou vždy min. 1x za 6 měsíců předloží k podpisu odpovědnému zástupci společnosti. Pokud zástupce zjistí závažné závady, bude s preventistou dohodnut způsob a termíny jejich odstranění
- účastnit se školení požární ochrany vedoucích zaměstnanců
- dbát, aby na všech pracovištích bylo prováděno školení při nástupu do zaměstnání a periodické školení zaměstnanců 1 x za 2 roky v souladu se směrnicí o požární ochraně a tématickým plánem školení požární ochrany

4.4.4.3 Požární hlídky pracoviště

V případě výskytu pracovišť se zvýšeným požárním nebezpečím jsou zřizovány požární hlídky. Jejich početní stav určí odpovědný zástupce společnosti.

Hlídka plní tyto úkoly:

- dohlíží na dodržování předpisů o PO na pracovišti se zvýšeným požárním nebezpečím
- provádí nutná opatření v případě vzniku požáru, zejména záchranu ohrožených osob, přivolání pomoci a zdolávání požáru.

4.4.5 Povinnosti konkrétních osob

Mimo povinností v rámci organizačního zajištění ukládají interní dokumenty také povinnost vedoucím pracovníkům a zaměstnancům společnosti MPG.

4.4.5.1 Povinnosti vedoucích pracovníků

Vedoucí pracovníci na všech stupních řízení jsou povinni zabezpečovat požární ochranu pracovišť v souladu s obecně závaznými pracovními předpisy, technickými předpisy a dbát na stav pracovišť tak, aby nemohlo dojít k požáru. Jsou zejména povinni:

- prokazatelně školit podřízené pracovníky s předpisy o požární ochraně
- zúčastňovat se školení požární ochrany
- dbát na to, aby po skončení pracovní doby bylo pracoviště zanecháno v požárně nezávadném stavu
- upozorňovat vedení společnosti na požárně bezpečnostní závady a činit v mezích své pravomoci opatření k jejich odstranění
- při revizi hasicích přístrojů předložit všechny přístroje rozmístěné na pracovištích k překontrolování odbornému pracovníku
- udržovat prostředky požární ochrany v akce schopném stavu a nepoužívat je k jiným účelům

4.4.5.2 Povinnosti všech zaměstnanců

Pracovníci na všech pracovištích jsou v zájmu zajištění požární bezpečnosti povinni počínat si tak, aby při své činnosti nezpůsobili požár nebo svým jednáním z nedbalosti příp. opomenutím nevytvořili nebezpečí vzniku požáru. Jsou zejména povinni:

- dodržovat předpisy platné pro jejich pracoviště

- při odchodu z pracoviště provést všechna opatření k zamezení vzniku požáru (vypnout el. proud, uzavřít přívod plynu, zabezpečit hořlavé látky, uhasit oheň v kamnech apod.)
- hlásit svému nadřízenému požární závady zjištěné na pracovišti a podle svých schopností se zúčastnit jejich odstraňování
- účastnit se školení požární ochrany
- znát rozmístění hasicích prostředků na pracovišti a umět je ovládat
- uhasit podle svých schopností zpozorovaný požár dosažitelnými prostředky, není-li účinný hasební zásah možný, bezodkladně to oznámit způsobem určeným v požárních poplachových směrnicích
- poskytnout za účelem zdolání požáru a na výzvu orgánů k tomu oprávněných, osobní a věcnou pomoc.

4.4.6 Dokumentace požární ochrany

Základní dokumentaci požární ochrany tvoří na všech pracovištích:

- požární kniha
- požární poplachové směrnice
- směrnice k řízení a organizaci požární ochrany
- záznamy o provedených školeních vedoucích zaměstnanců a zaměstnanců

Tato dokumentace musí být soustředěna tak, aby byla dostupná, dobře viditelná a trvale přístupná pracovníkům i v případě nepřítomnosti pracoviště.

Požární kniha obsahuje přehled o hasicích přístrojích a jejich kontrole, zápisy z kontrol požárního dozoru, záznamy o provedených školeních PO, údaje o případných požárech, přehled preventivních úseků, další doklady vyžadující předpisy požární ochraně.

Požární poplachové směrnice je nutné každý rok prověřit a podle potřeby upravit (zkontrolovat, zda uvedená telefonní čísla jsou platná, atd.). Za správnost uvedených údajů odpovídají vedoucí jednotlivých pracovišť. O provedené prověrce požárních poplachových směrnic bude pořízen zápis do požární knihy. S obsahem požárních poplachových směrnic musí být seznámeni všichni pracovníci.

5 ANALÝZA

K zajištění bezpečnosti podniku je vhodné provést v návaznosti na popis současného analýzu. K vlastnímu provedení analýzy si můžeme vybrat mezi několik typy. Jedná se např. o GAP[15] analýza, PEST[16] analýzu, SWOT[17] analýzu, analýzu rizik. Pro potřeby analýzy MPG byla zvolena SWOT analýza silných a slabých stránek společnosti.

5.1 SWOT analýza

SILNÉ STRÁNKY	SLABÉ STRÁNKY
Lidské zdroje Finanční zajištění Kvalitní technologie a kvalifikovanost v oboru Zázemí silné nadnárodní firmy (mateřského podniku).	Absence bezpečnostní politiky podniku Nedostatečné procesy bezpečnosti Nepokrytí některých oblastí zabezpečení Diverzifikovanost podnikatelských aktivit a lokalit umístění
PŘÍLEŽITOSTI	**HROZBY**
Přístup managementu Zpracování bezpečnostní politiky podniku Nastavení standardů bezpečnosti Možnost využití zkušeností ze zahraničí, především v rámci předpisů EU	Bezpečnostní rizika obecně. Nové rizika ve vztahu k bezpečnosti podniku. Změny právního rámce v rámci legislativy ČR a směrnic EU.

[Zdroj: vlastní]

Tab. 2 SWOT analýza Marius Pedersen

[15] GAP - Group-Analytic Practice

[16] PEST - Political, Economic, Social, and Technological analysis

[17] SWOT – Strengths, Weaknesses, Opportunities, Threats

SWOT analýza je posuzována z celkového pohledu na firmu Marius Pedersen Group.

Marius Pedersem Group je představitelem velkého podniku, který není typickým příkladem pro svou širokou škálu poskytovaných služeb. Tato diverzifikace nepřináší z pohledu bezpečnosti zvýšenou míru rizika, ale z pohledu zpracování bezpečnostní politiky, především nastavení účinných standardů je náročnější.

Geograficky je rozdělen skupina firem Marius Pedersen Group v rámci celé České republiky na menší celky, kterými jsou jednotlivé provozovny a společné podniky MPG s obcemi a městy.

Přes zjištěné nedostatky, nelze hodnotit stav jako kritický. Nevyhnutelná je ale změna přístupu k bezpečnostní politice, především uvnitř samotné společnosti, ale také vůči svému okolí.

Do budoucna můžeme doporučit provedení následujících kroků:

- Provedení celkového bezpečnostního auditu externí firmou
- Schválení bezpečnostní politiky podniku
- Vytvoření bezpečnostních standardů pro všechny oblasti

6 NÁVRH BEZPEČNOSTNÍ POLITIKY

Zjištěním současného stavu bezpečnostní politiky firmy MPG bylo mj. zjištěno, že firma nemá zpracovaný základní dokument bezpečnostní politika podniku, tedy písemného dokumentu, který určuje rámec bezpečnosti firmy a je po schválení představenstvem společnosti závazný pro všechny zaměstnance a je směrodatná také pro všechny externí subjekty, které spolupracují s firmou.

Bezpečnostní politika podniku musí být v souladu s politikou celé firmy, definuje, základní cíle a postoje k bezpečnosti. Vychází z platných interních směrnic.

6.1 Bezpečnostní politika podniku

Konkrétní návrh dokumentu bezpečnostní politiky podniku:

BEZPEČNOSTNÍ POLITIKA PODNIKU MARIUS PEDERSEN GROUP

- Společnost Marius Pedersen Group si dala za cíl chránit své zaměstnance, majetek, obchodní aktivity, jakož i veškeré informace obchodního i soukromého rázu. Jako prostředek k zajištění toho cíle si zvolila bezpečnostní politiku podniku.
- Bezpečnostní politika je závazná pro všechny zaměstnance, kteří jsou v souladu s úrovní svého pracovního zařazení školeni a odpovědni za bezpečnost, všichni zaměstnanci jsou tak součástí procesu řízení bezpečnosti
- Při použití prvků a prostředků ochrany, pro dosažení cílů bezpečnosti, je brán vždy zřetel na přiměřenost a zákonnost. Současně je garantována ochrana základních lidských práv a svobod, etika a respekt k soukromí osob.
- Pro řízení bezpečnosti jsou vytvořeny bezpečnostní standardy, které stanoví závazná pravidla pro celou společnostní. Standardy zohledňují specifika jednotlivých lokalit a zařízení a minimalizují vyjímky z pravidel.
- Kontrola bezpečnosti a opatření s tím souvisejících je prováděna pravidelně prostřednictvím auditů a přezkoumání, vyhodnocuje přijatá opatření z hlediska jejich úrovně a efektivity. Na základě závěrů přijímá opatření k nápravě zjištěných chyb za účelem neustálého zlepšování stavu a prevence bezpečnosti.
- Společnost průběžně hodnotí stávající a identifikuje nová rizika související s bezpečností, vyhodnocuje je a zaváděním přiměřených opatření, tyto řídí.
- Bezpečnostní politika Marius Pedersen Group jako součást skupiny Veolia Enviroment Services je plně v souladu s bezpečnostní politikou mateřské firmy a respektuje všechny zákonné a smluvní požadavky, kterými je povinna se řídit.
- Bezpečnostní politiku dále rozvádí organizační směrnice např. OS 22 Bezpečnostní předpis a ostatní interní dokumenty společnosti.
- Vydáním tohoto dokumentu vedení společnosti jednoznačně deklaruje svou podporu systému řízení bezpečnosti.

V Hradci Králové dne .....2012 .....

předseda představenstva

7 POPIS SKLÁDEK

Firma Marius Pedersen Group, dále jen MPG zajišťuje v rámci celé České republiky celkem 17 řízených skládek k odstraňování odpadu. Z kapitálového hlediska je můžeme rozdělit na provozovny, kde má MPG 100% majetkový podíl a dceřiné společnosti, kde má MPG majetkový podíl v rozmezí 52-98% a jedná se o společné podniky s obcemi nebo městy.

7.1 Rozdělení skládek

Z geografického hlediska můžeme skládky rozdělit podle oblastí, kde se nacházejí a které odpovídají i organizační struktura v rámci řízení skládkové činnosti společnosti MPG.

- **Oblast východních Čech** - MP Dolní Branná (Vrchlabí), MP Křovice (Dobruška), Bohemian Waste Management a.s., EKOLA České Libchavy s.r.o., Růžov a.s., Společnost Horní Labe a.s.,
- **Oblast severozápadních Čech** - MP Košťálov (Semily), MP Modlany (Teplice), MP Rožany (Šluknov), MP Vysoká (Plzeň), MP Vysoká Pec (Jirkov), Skládka Tušimice, Technické služby Děčín a.s.
- **Oblast Morava** - EKO-Chlebičov a.s., ELIO Slezsko a.s., Moravská Skládková společnost a.s., SOMA Markvartovice a.s.

7.2 Popis činnosti skládek

Skládky odpadu zcela ekologicky a bezpečně zajišťují konečnou ukládku již nevyužitelného odpadu.

Konstrukce skládek se řadí mezi technické stavby a musí splňovat vysoké nároky, např. na trvalou odolnost proti mechanickým, fyzikálním, chemickým a biologickým vlivům nebo začlenění skládky do okolního reliéfu krajiny.

Podmínky pro provozování skládky určuje Zákon o odpadech č. 185/2001 Sb. v platném znění a musí být plně v souladu s legislativou Evropské unie.

Provoz skládky je definován provozním řádem a integrovaným povolením, které shrnuje veškeré provozně-legislativní podmínky. Provozovatel je povinen pravidelně provádět monitoring pro státní úřady s následným vyhodnocením.

Areály skládek doplňují další provozní zařízení, která jsou začleněna do tzv. „Centra pro komplexní nakládání s odpady".

Součástí areálu skládek jsou také:

- prostor pro příjem a deklaraci dováženého odpadu,
- systém pro jímání skládkových plynů s jejich využitím v kogenerační jednotce na výrobu elektrické energie,
- uzavřený systém k jímání průsakových vod,
- kompostárna,
- shromažďovací místa k získání využitelných komodit odpadu,
- biodegradační plocha.

Ve všech skládkových provozech jsou ukládány odpady kategorie „O" nebo „N", které jsou přijímány podle standardizovaného seznamu společnosti MPG a odpady pro konkrétní zařízení jsou schvalovány příslušnými krajskými úřady pro jednotlivé skládky.

8 POPIS ZABEZPEČENÍ SKLÁDEK

Pro popis zjištěného současného stavu zabezpečení skládek, byly vybrány jako reprezentativní vzorek 4 skládky z oblasti Morava:

- EKO-Chlebičov a.s. - Zařízení pro nakládání s odpady
- ELIO Slezsko a.s. - Řízená skládka odpadů Holasovice II
- Moravská Skládková společnost a.s. - Centrum pro komplexní nakládání s odpady Kvítkovice
- SOMA Markvartovice a.s. - Centrum pro nakládání s ostatními odpady

8.1 Bezpečnost pracovníků, hygiena práce a požární ochrana

Předpisy bezpečnosti práce, ochrany zdraví a požární ochrany, tedy i opatření v této oblasti jsou pro všechny skládky v podstatě shodné. Nejedná se však o samostatné dokumenty jak by si tato problematika zasluhovala, ale jsou pouze zmíněny v menší, či větší míře v provozních řádech skládek.

8.1.1 Bezpečnost a ochrana zdraví při práci

V areálu zařízení se mohou pohybovat pouze zaměstnanci provozovatele, dále dodavatelé odpadů a jejich dopravci, a to po dobu nezbytně nutnou k odbavení jejich odpadu a v místech určených obsluhou zařízení. V případě provádění investičních akcí provozovatele (stavební a montážní práce apod.) v areálu zařízení budou samostatně stanovena pravidla pohybu dodavatelů investičních akcí na základě povahy a místa prováděné investiční akce při předání staveniště nebo pracoviště.

Pracovníci zařízení jsou povinni absolvovat vstupní lékařskou prohlídku a dále jsou pracovníci povinni se podrobovat ověřování zdravotní způsobilosti periodicky (včetně povinného očkování). Termíny těchto preventivních prohlídek jsou dány pracovním zařazením pracovníka (pracovní činností) a právními předpisy.

Způsobilost pracovníků k práci nesmí být žádným způsobem snížena (nemoc, požití alkoholu nebo omamných látek, apod.). Pracovníci tedy nesmí nastupovat pod vlivem alkoholických nápojů nebo jiných návykových látek na svá pracoviště a v pracovní době i mimo tato pracoviště.

Pracovníci zařízení musejí nejméně 1 x za 2 roky absolvovat školení BOZP a PO, (včetně

zásad první pomoci). Dále jsou pracovníci povinni se účastnit vstupních a periodických školení bezpečnosti práce a ochrany zdraví při práci a školení požární ochrany, s periodou a náplní odvislou od pracovního zařazení a pracovní činnosti. Součástí školení je také seznámení s provozním řádem zařízení.

Pracovníci jsou povinni používat při práci příslušné ochranné pracovní prostředky dané dle seznamu OOPP vypracovaném pro jednotlivá pracovní zařazení na základě zhodnocení rizik.

Zařízení je vybaveno jednou lékárničkou pro poskytování první pomoci.

V prostoru skládkového tělesa je přísně zakázáno jíst, pít a kouřit. Toto je povoleno pouze v prostorách zařízení, které jsou pro to určeny.

Případné provádění deratizačních a desinfekčních prací je povoleno pouze odborným pracovníkům specializovaných firem.

V případě výskytu toulavých zvířat platí zákaz kontaktu s nimi.

Povrch plochy pro denní ukládku odpadů bude pravidelně podle potřeby zakrýván vhodným materiálem nebo odpadem (zemina, stavební suť, škvára) proti množení hmyzu, hlodavců a ptáků. Prašnosti bude zamezováno kropením překrytého povrchu vodou.

Při zpětné recirkulaci průsakových vod na skládkové těleso budou využívány pouze ty části skládkového tělesa, kde se momentálně nepracuje. [9]

8.1.2 Požární ochrana

Protipožární opatření skládky jsou specifikována v tzv. „Požární směrnici skládky" schválené ředitelem společnosti. Uvedená „Požární směrnice skládky" nespadá do žádného schvalovacího řízení ve spojitosti s tímto provozním řádem. [9]

8.2 EZS a mechanické zábranné systémy

Stejně jako pro celou skupinu MPG ani pro popisované skládky není zpracován standard pro požadavky k zajištění areálů pomocí zábranných systémů.

8.2.1 Vniknutí cizích osob

Ochrana skládek proti vniknutí cizích osob, příp. proti krádežím je zmíněno v provozních řádech jednotlivých skládek se uvádí:

„ V případě zjištění skutečnosti nebo podezření, že do areálu skládky nebo do některého objektu někdo neoprávněně vniknul, je nutno s ničím nehýbat a přivolat telefonicky Policii ČR a do doby jejího příjezdu nesmí nikdo do dotčeného prostoru anebo objektu vstoupit."

Areály skládek jsou oploceny a jediná možnost vstupu a vjezdu do areálu bez překonání překážky v provozní době zařízení je vjezdová brána.

Obsluha zařízení pravidelně (min. v týdenních intervalech) kontroluje stav neporušenosti oplocení zařízení.

V provozní době zařízení se mohou v areálu zařízení vyskytovat a pohybovat pouze osoby, které jsou zařazeny do obsluhy zařízení, osoby, které vykonávají činnost v areálu zařízení na základě smlouvy nebo objednávky a to pouze s vědomím obsluhy zařízení a na místech určených obsluhou zařízení. Dále se v provozní době v areálu zařízení mohou vyskytovat pracovníci dodavatelů odpadů, a to po dobu nezbytně nutnou pro řádné předání odpadu k odstranění.

V mimoprovozní době je vjezdová brána uzavřena a uzamčena a ve vážním objektu a vybraných prostorech zařízení je aktivována elektronická zabezpečovací signalizace.

Ve dnech pracovního klidu a pracovního volna provádí určený pracovník zařízení v rámci pracovní pohotovosti prohlídku zařízení. Obsahem prohlídky je:

- kontrola stavu provozního objektu a garáží z hlediska protipožární ochrany a zajištění proti vniknutí nepovolaných osob
- kontrola vstupní brány a oplocení kolem celého areálu zařízení
- kontrola výškové úrovně hladiny v jímce průsakových vod
- kontrola technického stavu mechanismů používaných v zařízení, jejich uzamčení (případný únik ropných látek)
- kontrola skládkového tělesa zejména z hlediska možného zahoření odpadu a znečišťování ovzduší
- kontrola funkčnosti čerpadla (čerpadel) pro čerpání průsakových vod
- kontrola stavu zásobníku na naftu vč. výdejního stojanu

Stav zjištěný v průběhu prohlídky zapíše pracovník provádějící prohlídku do provozního deníku. V případě zjištění nedostatku či závady provede nezbytná opatření k jejich odstranění, případně uvědomí příslušné osoby a orgány dle provozního řádu. [3]

8.2.2 Zabezpečení odpadů před odcizením

S ohledem na funkci skládek je zabezpečení odpadů jednou z nejdůležitějších oblastí bezpečnosti skládek. Nejedná se jen o možnost zcizení, ale také o možné nežádoucí účinky, především s ohledem na ekologickou nebezpečnost se jedná o úniky nebezpečných látek způsobených neodbornou manipulací s odpady.

Zabezpečení odpadů před odcizením je zajištěno pravidelnou kontrolou oplocení zařízení, které znemožňuje volný přístup do areálu zařízení. Všechny objekty jsou mimo provozní dobu uzamčeny. Dále jsou odpady uložené na skládce zabezpečeny tak, že jsou řádně zhutněny, rozdrceny a překryty.

Úniku odpadů do okolního prostředí je zabráněno řízeným skládkováním, postupy řízeného skládkování jsou popsány v provozním řádu a dále také technickým vybavením a zabezpečením skládky (těsnící konstrukce apod.). [3]

8.3 EZS a mechanické zábranné systémy

Pro elektrické ani mechanické zábranné systémy nemají skládky ani jiná zařízení MPG zpracovány samostatně ani jako součást jiných interních dokumentů žádná jednotná pravidla. Přesto jsou jednotlivé skládky částečně zabezpečeny.

8.3.1 EKO - Chlebičov

Skládka Chlebičov je zabezpečena čtyřmi kamerami (3xEKO, 1xMP) s možností on-line sledování provozu a se záznamem s venkovními a vnitřní prvky EZS. Tyto jsou napojeny na pult EZS poskytovatele – operátor non-stop. V případě narušení prvků EZS se na pultu zobrazí poplach, operátor vyhodnotí, zda je planý, nebo ne, v případě podezření na narušení volá odpovědné osobě (EKO, MP) a po dohodě s ní případně zajistí výjezd zásahovky. Nově byly v závěru minulého roku instalovány závory na vjezdu do areálu a vjezdu na těleso skládky. Schéma areálu viz Příloha č. 1 a fotografie areálu č. 2.

8.3.2 SOMA Markvartovice

Skládka v Markvartovicích je vybavena jednou kamerou se záznamem a vnitřními a venkovní prvky EZS, ty jsou napojeny na pult Městské policie v Hlučíně, v případě poplachu je realizován výjezd zásahové jednotky.

8.3.3 Moravská skládková společnost

Na skládce v Kvítkovicích jsou instalovány vnitřní prvky EZS jednak v administrativní budově a jednak v garáži mechanismů. Tyto jsou napojeny na pult EZS poskytovatele – operátor non-stop.

V případě narušení prvků EZS se na pultu zobrazí poplach, operátor vyhodnotí, zda je planý, nebo ne, v případě podezření na narušení volá odpovědné osobě (MSS) a po dohodě s ní případně zajistí výjezd zásahové jednotky.

8.3.4 ELIO Slezsko

V areálu skládky ELIO jsou instalovány vnitřní prvky EZS ve vážní místnosti provozní budovy, poplachové hlášení je prostřednictvím EZS napojeno na telefon vedoucího skládky.

9 NÁVRH ZABEZPEČENÍ SKLÁDEK

Návrh zabezpečení skládek vychází ze zjištěného současného stavu zabezpečení bezpečnosti firmy MPG, provedené SWOT analýzy a aktuálního stavu zabezpečení na skládkách. Z hlediska zákonných povinností se snaží společnost dodržet všechny předepsané náležitosti v rámci interních dokumentů. Jedná o oblast bezpečnosti a ochrany zdraví při práci, hygieny práce a požární ochrany.

Nejvíce zabezpečenou oblastí je oblast IT

Pro ostatní oblasti takové interní dokumenty chybí nebo jsou nedostatečné. Není tak standardizována oblast zabezpečení areálů, budov, příp. majetku. Nejsou tak nastaveny ani požadavky na mechanické nebo elektronické zabezpečení skládek.

9.1 Návrh standardů

9.1.1 BOZP, PO

S ohledem na výše uvedené a závěry předchozích zjištěních je zřejmé, že přesto, že existují interní dokumenty, které ve své podstatě splňují zákonné povinnosti, ale neodpovídají zcela potřebám bezpečnosti. Proto doporučuji zavedení jednotných standardů pro všechny společnosti v rámci firmy MPG. Jedná se o vytvoření samostatných standardu pro jednotlivé oblasti. Tedy vytvoření směrnice pro BOZP, pro PO a pro další navazující oblasti jakými jsou např. Hygiena práce. Tyto samostatné standardy budou závazné pro všechny provozovny a doporučující pro všechny dceřiné společnosti MPG.

Dalším doporučením pro oblast BOZP je zavedení standardu OHSAS 18001 pro zařízení skládek. Tento standard je dosud uplatňován pouze u jedné z provozoven v rámci provozoven MPG. Což je s ohledem na současné požadavky nedostatečné.

9.2 Zabezpečení areálů a budov

Hlavní oblastí bezpečnosti skládek, kde má firma MPG nedostatky, je zajištění ochrana areálů proti vniknutí cizích osob, zcizení odpadu, příp. poškození zařízení firmy. Důvodem je chybějící dokumentace. K uvedeným hrozbám můžeme najít pouze krátké odstavce o jedné až dvou větách v rámci provozního řádu.

Současně jsem ohledáním na místě zjistil i nedostatky v provádění režimových opatřeních, kdy sice odpovědní pracovníci mají povinnost pravidelné kontroly např. oplocení, ale na místě bylo zjištěno a zdokumentováno jeho poškození, což znamená i neplnění povinností pracovníků. I proto by bylo vhodné doplnit oplocení o systém ochranných prvků. Obrazová dokumentace oplocení viz. Příloha č. 3.

9.2.1 Návrh zabezpečení areálů

Ke stávajícímu mechanickému zabezpečení areálů, které tvoří především oplocení a vjezdové brány, doporučuji zabezpečení rozšířit o perimetrické ochranné prvky a záznamová zařízení.

Konkrétní zajištění areálu si můžeme představit např. na zajištění skládky v Kvítkovicích, schéma areálu viz. Příloha č. 4.

9.2.1.1 Navrhované řešení

Základní charakteristika systému:

- účel nasazení - monitorování vjezdu do objektu a na parkoviště, monitoring pohybu osob hlavně v nočních hodinách, kontrola při vyhlášení poplachu
- provedení systému - barevný, vysoké rozlišení (1Mpix), záznam při pohybu a při narušení prvků perimetrické ochrany, IR přísvit kamer, záznam po dobu 7-14 dní
- záznamové zařízení - obraz z kamer bude ukládán do síťového záznamového zařízení MXR 6004, zařízení budou dvě, aby se měla kam ukládat pátá kamera
- Avermedia MXR6004 má podporu megapixelových kamer a kompresního formátu h. 264 což uspoří spoustu místa na HDD oproti ostatním kompresním algoritmům
- HDD na jedno zařízení jsem zvolil 1000GB což by mělo stačit pro záznam ze 4 1,3MP kamer se snímkováním 10 snímku za sekundu a vysoké kompresní kvalitě na dobu 1-2 týdnů
- IP[18] licence je již obsažena v ceně produktu
- vzdálený přístup

[18] IP – Internet Protocol

9.2.1.2 Požadavek na dodávku

Požadavek na montáž IP kamerového systému:

- 1. kamera: monitorovat prostor vjezdu do areálu s rozlišovací schopností kamery (detail)
- 2. kamera a 3. kamera: monitorovat prostor v okolí nádrží kde parkují popelářské vozy
- 4. kamera: monitoring prostoru oplocení a brány v blízkosti multifunkční plochy
- 5. kamera: monitoring prostoru oplocení v blízkosti multifunkční plochy

Obrazová dokumentace k návrhu viz. Příloha č. 5.

9.2.1.3 Ostatní

Pro zlepšení komfortu řidičů doporučuji vybavit vjezdové, především nákladní brány automatickým otevíráním.

Z hlediska zjednodušení standardů bezpečnosti doporučuji dodržování jednotných standardů a požadavků na zabezpečení skládek.

9.2.2 Návrh zabezpečení budov

Zabezpečení areálů musí odpovídat také požadavky na zabezpečení budov, které jsou součástí skládek. Tyto můžeme hodnotit stupněm průměrného rizika. Tomu musí odpovídat i požadované zabezpečení. Předpokladem pro účelnost a přiměřenou nákladovost zabezpečení je kombinace mechanických systémů s ostatními formami ochrany, především EZS. U mechanických zábranných systémů se jedná především o dveřní systémy. V případě EZS se očekává vytvoření standardů vnitřní ochrany objektů s využitím především PIR detektorů. V požadavku na zajišťování zabezpečení musí být zmíněna také možnost napojení na ACS přístupový a docházkový systém. Samozřejmostí by měla být kombinace EZS s EPS. Kombinací těchto systémů můžeme také snížit náklady na instalaci zabezpečení.

Předpokladem pro správnou funkci přijatých opatření je dodržování režimových opatření, klíčového režimu a přidělování bezpečnostních kódů.

Správné nastavení požadavků na zabezpečení skládek nám může poskytnout kvalitně zpracovaný standart požadavků na zajištění bezpečnosti.

9.3 Ostatní zabezpečení

V návaznosti na doporučení zavedení zabezpečení areálů skládek pomocí EZS můžou být tyto návrhy rozšířeny i na ostatní zařízení areálů skládek.

9.3.1 Čerpací stanice

Jedním ze zařízení, kde je možné využít zabezpečení EZS a která bývají součástí areálu skládek, jsou čerpací stanice. Tyto čerpací stanice jsou umístěny na dvou ze čtyř hodnocených skládek a to konkrétně na skládce v Kvítkovicích a na skládce Chlebičov. V návaznosti na doporučení zavedení zabezpečení areálů skládek pomocí EZS můžou být tyto návrhy rozšířeny i na ostatní zařízení areálů skládek.

ZÁVĚR

Cílem mé diplomové práce bylo popsat bezpečnostní politiku podniku konkrétní firmy se zaměřením na konkrétní podnikatelskou aktivitu. Při studiu materiálů k dané problematice jsem zjistil, že většina dokumentů zabývajících se bezpečností je zaměřena na ochranu v oblasti IT, oblasti utajovaných informací, příp. činnosti strážných, bezpečnostních a detektivních služeb.

Práce je rozdělena na část teoretickou a část praktickou.

V první kapitole teoretické části byla popsána bezpečnostní politika obecně a to nejprve z globálního pohledu. Globální hrozby ovlivňují nepřímo také všechny ostatní oblasti bezpečnosti a to na všech úrovních. V druhé kapitole pak byla popsána bezpečnostní politika, její účel, obsah, postup při zpracování, jeho průběh až po bezpečnostní audit.

V praktické části byla v souladu se zadáním diplomové práce v první kapitole nastíněna problematika legislativy bezpečnostní politiky jednak z pohledu právních předpisů a jednak z pohledu posuzovaných oblastí bezpečnosti podniku. V druhé kapitole a třetí kapitole byla pro potřeby posouzení bezpečnostní politiky stručně představena společnost Marius Pedersen Group a její podnikatelské aktivity a popsán současný stav bezpečnosti podniku v členění na ochranu osob a majetku, bezpečnost a ochranu zdraví při práci, IT ochranu a požární ochranu.
V dalších kapitolách byl s využitím provedení SWOT analýzy navržen konkrétní dokumentu bezpečnostní politiky podniku. Poslední tři kapitoly byly věnovány, opět v souladu se zadáním diplomové práce, konkrétnímu zabezpečení skládek od jejich popisu, přes stav současného zabezpečení až po návrh standardu jejich zabezpečení.

Zajímavou oblastí bezpečnosti je zabezpečení podniku v IT oblasti. Této problematice je v současnosti věnována velká pozornost. Otázkou, ale je, zda jsou všechny prostředky vynaloženy účelně. IT problematika a zainteresovaní pracovníci jsou v mnoha případech, obtížně kontrolovatelní a mohou vytvářet pocit nepostradatelnosti. Principem by mělo být, aby i tato oblast bezpečnosti podniku podléhala celkové bezpečnosti podniku a

bezpečnostnímu managementu. Dodržení tohoto principu může mít i pozitivní vliv na vynakládané finanční prostředky.

Závěrem mohu konstatovat, že tato práce potvrdila všeobecnou skutečnost, podceňování významu bezpečnostní politiky a tedy i samotné bezpečnosti podniku. Především se jedná o nedocenění významu ze stran vrcholového managementu a také z jejich neznalosti uvedené problematiky. Tento fakt je částečně způsobený také malou dostupností ucelených studijních materiálů k bezpečnostní politice podniku. Proto doufám, že tato diplomová práce může být malým vodítkem k tomu, z jakého pohledu se na bezpečnost podniku můžeme také podívat.

CONCLUSION

The aim of the thesis was to describe the security policy of a particular company, focusing on specific business activities. In the study of literature on this issue, the author found merely documents dealing with security aims for protecting the IT sphere, areas concerning classified information and security guard work operations, security and detective services.

The work is divided into theoretical and practical parts.

The first section describes the theoretical part of security policy in general, initially from a global perspective. Global threats indirectly affect all other areas of security at all levels. The second section then describes the security policy in place at Marius Pedersen, its purpose, content, procedures for processing, and consideration within the security audit.

The practical part, in accordance with the specifications of the thesis, in the first section outlines the issues of security policy and legislation, both in terms of regulations and areas assessed in terms of company safety. The second section and the third briefly assessed the requirements of security policy for the Marius Pedersen Group and its business activities, and describe the current state of security in the company's structure to protect people and property, health and safety at work, IT security and fire safety measures. Subsequent parts, using the SWOT analysis, featured a proposal of a safety policy document for this particular company. The last three sections are devoted, again in accordance with the specifications of the thesis, to particular security as regards a description of the landfill sites, and a suggestion as to future standard policy.

An interesting area of security concerns IT. This issue is currently the subject of much attention. The question is whether any funds are spent effectively. IT issues and staff, involved in many cases, prove difficult to monitor and these persons may create a sense of indispensability. The principle should be that this area of security becomes subject to the enterprise's management of overall safety and security. Adherence to this principle can have a positive impact on expenditure.

Finally, the author believes that this work confirmed the general status quo an underestimation of the importance of security policy and, therefore the actual security of the company. In particular, it is a failure to appreciate the importance of it by senior management and their oversight of the issue. This fact is partly due to the limited availability of comprehensive study materials that inform company security policy. Therefore, the author hopes that this thesis may be of some guidance as to what view of security the company can further investigate.

SEZNAM POUŽITÉ LITERATURY

Publikace:

[1] KINDL, Jiří. *Projektování bezpečnostních systémů I. díl.* Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2004. 134 s. ISBN 80-7318-165-7.

[2] LAUCKÝ, Vladimír. *Technologie komerční bezpečnosti* I. Vyd. 2. Zlín: Univerzita Tomáše Bati ve Zlíně, 2004. 64 s. ISBN 80-7318-194-0.

[3] LAUCKÝ, Vladimír. *Technologie komerční bezpečnosti* II. Vyd. 2. Zlín: Univerzita Tomáše Bati ve Zlíně, 2004. 122 s. ISBN 80-7318-231-9.

[4] LUKÁŠ, Luděk a kol. *Bezpečnostní technologie, systémy a management I.* Vyd. 1. Zlín: VeRBuM, 2011. 105 s. ISBN 978-80-87500-05-7.

[5] LAUCKÝ, Vladimír. *Speciální bezpečnostní technologie.* Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2009. 223 s. ISBN 978-80-7318-762-0.

[6] KAMENÍK, Jiří. BRABEC, František a kol. *Komerční bezpečnost. Soukromá bezpečnostní činnost detektivních kanceláří a bezpečnostních agentur.* Vyd. 1. Praha: ASPI, a.s. 2007. 340 s. ISBN 978-80-7357-309-6.

[7] UHLÁŘ, Jan. *Technická ochrana objektů I. díl - Mechanické zábranné systémy.* Vyd. 1. Praha: Policejní akademie ČR, 2000. 150 s. ISBN 80-7251-046-0.

[8] UHLÁŘ, Jan. *Technická ochrana objektů II. díl - Elektrické zabezpečovací systémy.* Vyd. 1. Praha: Policejní akademie ČR, 2001. 205 s. ISBN 80-7251-076-2.

[9] HADRABOVÁ, Alena. *Enviromentální aspekty podnikání.* Vyd. 1. Praha: Vysoká škola ekonomická v Praze, 2010. 120 s. ISBN 978-80-245-1709-4.

[10] BRABEC, František. *Ochrana bezpečnosti podniku.* Vyd. 1. Praha: EUROUNION, 1996. 203 s. ISBN 80-85858-29-0.

[11] BRABEC, František a kol. *Bezpečnost pro firmu, úřad, občana.* Vyd. 1. Praha: Public History, 2011. 348 s. ISBN 80-86445-04-06.

[12] IVANKA, Ján. *Systematizace bezpečnostního průmyslu I.* Vyd. 3. Zlín: Univerzita Tomáše Bati ve Zlíně, 2009. 123 s. ISBN 978-80-7318-850-4.

[13] IVANKA, Ján. *Systematizace bezpečnostního průmyslu II.* Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2009. 86 s. ISBN 978-80-7318-863-4.

[14] IVANKA, Ján. *Mechanické zábranné systémy.* Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2010. 151 s. ISBN 978-80-7318-910-5.

[15] ČANDÍK, Marek. *Objektová bezpečnost II.* Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2004. 100 s. ISBN 80-7318-217-3.

Internetové zdroje:

[1] Ministerstvo vnitra ČR - http://www.mvcr.cz

[2] Bezpečnostní informační služba - http://www.bis.cz

[3] Marius Pedersen a.s. - http://intranet

[4] Člověk v tísni - http://www.rozvojovka.cz

[5] IW zpravodajský server - http://www.investicniweb.cz

[6] Pro právo - http://www.propravo.cz

[7] Ing. Marek Zeman - http://www.bozpzeman.cz

[8] Ministerstvo spravedlnosti - http://www.justice.cz

Ostatní zdroje:

[2] Interní materiály Marius Pedersen a.s.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

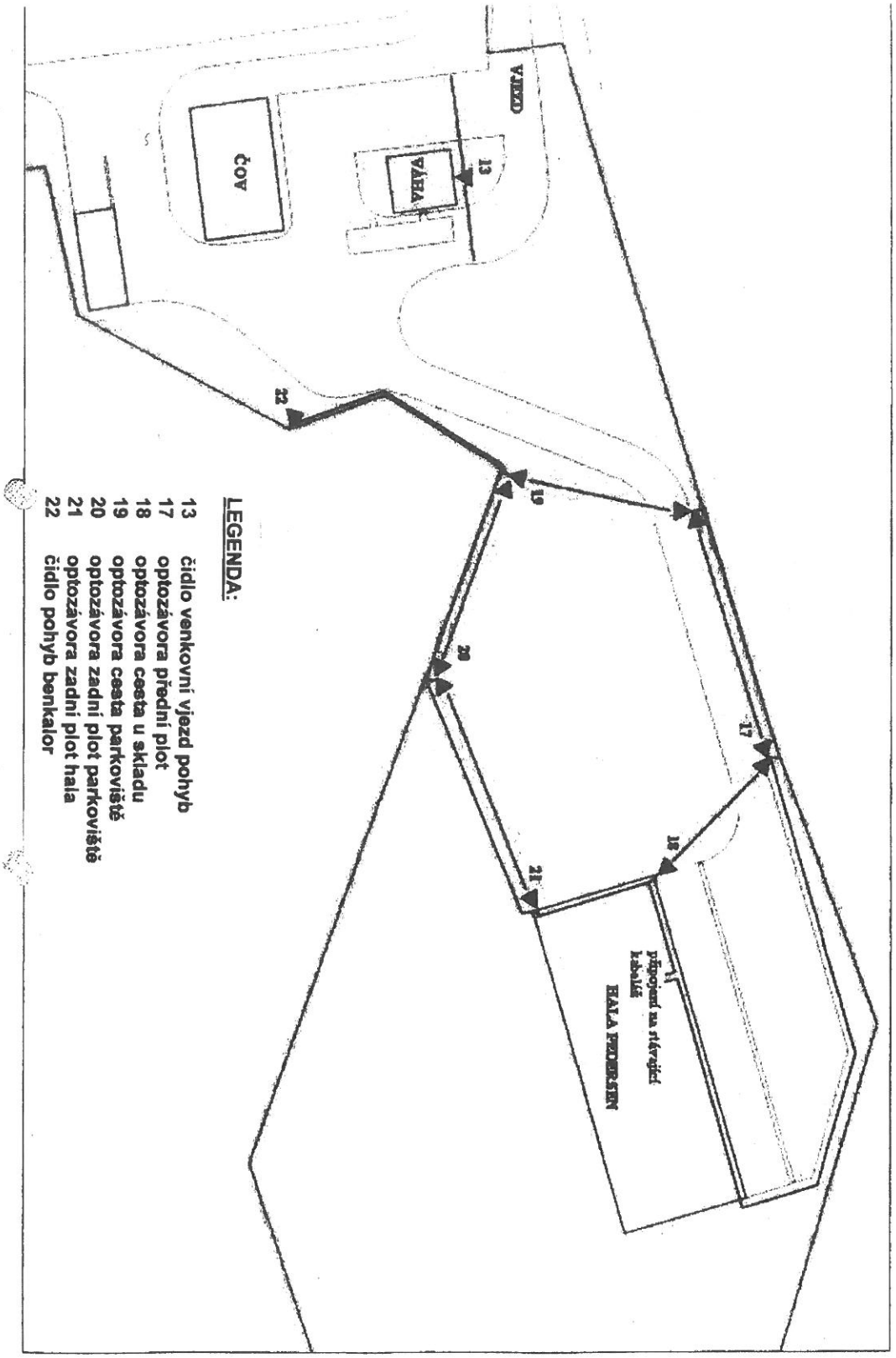
IT/ICT	Informační technologie / Informační a komunikační technologie.
BYOD	Systém přístupu soukromých zařízení zaměstnanců do podnikové sítě.
NFC	Bezdrátový přes dat na krátkou vzdálenost.
BOZP/OHSAS	Bezpečnost a ochrana zdraví při práci.
PO	Požární ochrana.
ČR	Česká republika.
ÚOOÚ	Úřad pro ochranu osobních údajů.
EU	Evropská unie.
ČSN EN	Evropská norma přejatá do národního systému norem ČR.
EZS	Elektrická zabezpečovací signalizace.
MPG	Marius Pedersen Group.
PPC	Poplachové přijímací centrum.
GŘ	Generální ředitel.
OOPP	Osobní ochranné pracovní prostředky.
VPN	Virtuální privátní síť.
MV	Ministerstvo vnitra.
GAP	Srovnávací analýza.
PEST	Analýza politiky, ekonomiky, sociální oblasti a technologií.
SWOT	Analýza slabých a silných stránek, příležitostí a hrozeb.
PIR	Pasivní infračervený detektor pohybu prostorové ochrany.
CCTV	Uzavřený televizní okruh.
ACS	Přístupový a docházkový systém.
EPS	Elektrická požární signalizace.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P 1 SCHÉMA AREÁLU EKO CHLEBIČOV



PŘÍLOHA P 2 AREÁL SKLÁDKY EKO CHLEBIČOV

Obrázek 1 Vjezd do areálu

Obrázek 2 Vážní domek

Obrázek 3 Pohled na skládku

PŘÍLOHA P 3 UKÁZKA OPLOCENÍ SKLÁDKY KVÍTKOVICE

Obrázek 4 Poškozené oplocení

Obrázek 5 Chybějící oplocení

Obrázek 6 Neudržované oplocení

PŘÍLOHA P 4 DOPLNĚNÍ K NÁRVHU ZABEZPEČENÍ SKLÁDKY

1. stanoviště - IP kamera (brána): Kamera má velmi široký rozsah zoomu, což umožní ji přiblížit tak, že půjde rozpoznat osoba stojící u brány. Kamera se po setmění umí přepnout do monochromatického (černobílého) režimu a zapnout IR přísvit pro lepší záznam v noci. Vnitřní vyhřívání. Kamera bude připojena drátově pomocí již nainstalované strukturované kabeláže a přívodu napájení.

Technické parametry: 1.3 megapixel kamera, LOW-LUX, DEN/NOC do 50m, venkovní se ZOOM motorickým objektivem 5.2-58.8mm DC vprovedení "válec", 0.2 / 0.0001 lux, 1280x1024 @25fps, H.264, 2DNR, IP67, IR-Cut filter,12VDC

Bezdrátový přenos - přenos obrazových a jiných dat z kamer 2,3,4,5 bude realizován pomocí Bezdrátové sítě (zařízení owl410- Wi-Fi 802.11 n/a). Na administrativní budově bude hlavní jednotka na zbylých dvou kamerových stanovištích budou podružné jednotky. Možná regulace výkonu. Reálná uživatelská přenosová rychlost se pohybuje mezi 60 až 90 Mb/s v závislosti na prostředí.

2. stanoviště - IP kamer 2 a 3 (parkoviště popelářských vozů): Zde jsou navrženy dvě kamery aby alespoň trochu pokryli žádaný prostor, kde parkují popelářské vozy. Kamera Vivotek ip7361 má rozlišení 2Mpx, což zvyšuje šanci na rozpoznání případné osoby, protože má kamera 5x větší rozlišení než běžná analogová kamera. Druhou použitou kamerou je Samsung SNO- 5080R. Rozlišení 1Mpix.

Technické parametry: Vivotek ip7361 IP kamera, IP7361 MPEG-4/MJPEG, CMOS (1/3), max. 1600×1200 (2 Mpix), až 15 sn/s, DI/DO, PoE, prohlížení na MT (RTSP), IR-Cut, IP66,DC drive, objektiv 3- 9mm, F1.2

Samsung SNO- 5080R Kompaktní den/noc (mech.) IP kamera srozlišením HD 720p (1280x1024) je vybavena IR přísvitem do 30m avarifokálním objektivem. Tato kamera je vhodným řešením hlavně do venkovních aplikací s neosvětlenými prostorami. Své uplatnění určitě najde také zabudovaná inteligentní video analýza.

3. stanoviště - IP kamer 4 a 5 (perimetr v blízkosti multifunkční plochy): Zde jsou také navrženy dvě kamery, aby alespoň trochu pokryli žádaný prostor. Jsou zde navrženy kamery Samsung SNO- 5080R s rozlišením 1Mpix (viz. předchozí odstavec)