Bezpečnostní strategie

Bc. Zuzana Plháková

Diplomová práce
2016

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2015/2016

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

Jméno a příjmení:	**Bc. Zuzana Plháková**
Osobní číslo:	**A14376**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Bezpečnostní strategie**
Téma anglicky:	**Security Strategy**

Zásady pro vypracování:

1. **Pojednejte o účelu, roli a obsahu bezpečnostní strategie.**
2. **Analyzujte systém a způsob zajištění bezpečnosti organizace.**
3. **Specifikujte a analyzujte základní bezpečnostní dokumenty vybraných organizací.**
4. **Navrhněte účel, strukturu a obsah bezpečnostní strategie organizace.**
5. **Vypracujte vzorovou bezpečnostní strategii organizace.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management II. 1. vyd. Zlín: VeRBuM, 2012. ISBN 978-80-87500-19-4.**
2. **LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management III. 1. vyd. Zlín: VeRBuM, 2013. ISBN 978-80-87500-35-4.**
3. **JANOŠEC, Josef. Bezpečnost a obrana České republiky 2015-2025. Praha: Ministerstvo obrany České republiky - Agentura vojenských informací a služeb, 2005. ISBN 80-7278-303-3.**
4. **EICHLER, Jan. Mezinárodní bezpečnost na počátku 21. století. Praha: Ministerstvo obrany České republiky - AVIS, 2006. ISBN 80-7278-326-2.**
5. **ZEMAN, Petr (ed.). Česká bezpečnostní terminologie: výklad základních pojmů. 1. vyd. Brno: Masarykova univerzita, Mezinárodní politologický ústav, 2002. ISBN 80-210-3037-2.**
6. **KHOL, Radek. Evropská bezpečnostní a obranná politika: národní perspektivy. Praha: Ústav mezinárodních vztahů, 2002. ISBN 80-86506-25-8.**
7. **Česká republika a Evropská bezpečnostní a obranná politika. Praha: Ústav mezinárodních vztahů, 2001. ISBN 80-85864-99-1.**

Vedoucí diplomové práce: **doc. Ing. Luděk Lukáš, CSc.**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **5. února 2016**

Termín odevzdání diplomové práce: **16. května 2016**

Ve Zlíně dne 5. února 2016

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

Jméno, příjmení: Bc. Zuzana Plháková

Název diplomové práce: Bezpečnostní strategie

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové 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 práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové 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 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 práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové 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 práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové 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, dne 12.05.2016

.....
podpis diplomanta

ABSTRAKT

Diplomová práce analyzuje problematiku bezpečnostní strategie a její roli, účel a náležitosti z hlediska legislativy ale i funkčnosti v praxi na úrovni státu a organizace. Cílem této práce je specifikace a analýza bezpečnostních dokumentů ve dvou organizacích, poskytnutých pověřenými osobami z analyzovaných firem, externích pracovníků z oblasti bezpečnosti, ale také pozorováním v těchto firmách. Následně byla vyhotovena vzorová bezpečnostní strategie organizace. Vytvořené řešení umožňuje pohled na bezpečnost z globálního hlediska a distancuje se od zajištění firemní bezpečnosti pouze formou bezpečností politiky. Přínosem této práce je zamyšlení se nad dosavadním zajišťováním bezpečnosti v organizacích a upozornění na souvislosti v sestavování strategie a bezpečnosti v rámci strategických rozhodnutí firmy.

Klíčová slova: bezpečnostní strategie, bezpečnostní prostředí, hrozba, riziko, analýza rizik

ABSTRACT

This diploma thesis analyses safety strategy issues, its roles, functions and requirements from the view of legislation and also in common practice at a state and organization levels. The aim of this project is to analyze and specify safety documents in two chosen companies provided by authorized persons in organizations responsible for safety field. Physical observation is the other source of information. Afterwards a model safety strategy of organization was created. This enables to get a global view of safety and also dissociates of handling a company safety with a safety policy. One of main benefits of this project is an evaluation of previous ways of ensuring safety in different companies and pointing out the importance of safety problems when strategic company planning is made.

Keywords: security strategy, security environment, threat, risk, risk analysis

Poděkování:

Velmi ráda bych poděkovala vedoucímu diplomové práce doc. Ing. Luďkovi Lukášovi, CSc. za cenné a moudré rady, vstřícný přístup a věnovaný čas. Velký dík patří také organizacím, které mi zpřístupnily své materiály a poskytly podklady pro vyhotovení diplomové práce.

Motto:

Nezapomeň, že všechno co v životě uděláš, zanechá stopu, a proto si uvědomuj každý svůj krok.

Autor: Paulo Coelho

Prohlašuji, že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Bezpečnostní strategii lze aplikovat na úrovni skupiny států, státu nebo na úrovni organizace. Nejprve bude analyzována Bezpečnostní strategie České republiky. Bezpečnostní strategie ČR patří mezi významné bezpečnostní dokumenty, zpracované na úrovni sátu. Dílčím cílem je provést analýzu tohoto dokumentu, definovat jeho obsah a vývoj, specifikovat bezpečnostní prostředí, zájmy a zmínit strategii vlády pro zajištění bezpečnosti v budoucnu. Další kapitola bude patřit bezpečnostní strategii na úrovni Evropské unie a institucím Společné bezpečnostní a obranné politiky, které se zabývají specifickými otázkami vojenského a civilního krizového managementu. Práce si klade za cíl zejména analyzovat problematiku bezpečnostní situace organizace, specifikovat rozdíly mezi bezpečnostní politikou a bezpečnostní strategií a zmínit legislativu, která danou problematiku upravuje. Oblastí zájmu bude také systém zajištění bezpečnosti, náležitosti bezpečnostního kontroly a přiblížení jednotlivých oblastí bezpečnostní strategie, jako je informační bezpečnost, bezpečnost a ochrana zdraví při práci, personální bezpečnost, požární ochrana a fyzická bezpečnost. Praktická část bude obsahovat analýzu bezpečnostní situace ve dvou organizacích, specifikaci a analýzu jejich bezpečnostní dokumentace a informace o zjištěných nedostatcích. V návaznosti na to se pak bude zabývat návrhem zavedení bezpečnostní strategie na úroveň organizace, jejím obsahem a vhodnou strukturou. V závěru bude vytvořena vzorová bezpečnostní strategii organizace včetně analýzy rizik, která bude využitelná i v praxi.

I. TEORETICKÁ ČÁST

1 BEZPEČNOSTNÍ STRATEGIE

Pojem bezpečnost a strategie jsou vzhledem k momentálnímu dění v České republice i ve světě stále více skloňovány. Obecná definice pojmu bezpečnostní strategie není v odborné literatuře uváděna, můžeme se dočíst pouze o bezpečnostní strategii České republiky, státu, firmy a podobně. V této kapitole si tedy nejprve upřesníme definice jednotlivých slov a poté se budeme věnovat jejich spojení, tedy bezpečnostní strategii. Význam slova strategie můžeme definovat jako koncepční organizaci a řízení určité činnosti za účelem ovlivnění budoucích podmínek a dosažení definovaných cílů. Strategie bývá chápána jako obecný postup či umění koncepčně dosahovat stanovených cílů pomocí identifikovaných prostředků, metod a nástrojů v určitém časovém rozvrhu. Taktika označuje způsob vedení a promýšlení určité činnosti v konkrétní situaci, volbu dílčích prostorově a časově omezených postupů, které jsou implikovány a determinovány obecnými principy a cíli ve shodě se strategiemi či strategickými koncepcemi v dané oblasti či problematice.[1] Pojem bezpečnost má více významů. Nejčastěji označuje stav, kdy referenčnímu objektu nehrozí neakceptovatelná újma, a také soubor opatření, kterým se v případě expozice hrozby tohoto stavu dosahuje. Cílem bezpečnosti jako oboru je zabránit vzniku újmy nebo minimalizovat pravděpodobnost vzniku a velikost újmy ve vybraných oblastech. Újma představuje pro referenční objekt nežádoucí negativní projev, který omezuje naplňování cílové funkce nebo může vést až k jeho zmaru. Uvědomění si velikosti a vlivu újmy na fungování referenčního objektu pro něj má veliký význam. Opatřeními lze vzniku újmy zabránit a tím se vyhnout možným dopadům, s újmou spojeným. Zvládání rizik znamená bránit vzniku neakceptovatelné újmy. [2]

1.1 Role bezpečnostní strategie

Z výše uvedených definic tedy vyplívá, že rolí bezpečnostní strategie je identifikace budoucích bezpečnostních rizik a hrozeb a také změn ve vývoji referenčního objektu, které ho mohou ohrozit, a stanovení cílů a konkrétních kroků pro zajištění jeho bezpečnosti. Jednoduše řečeno, pokud bude kladen důraz na to, co v budoucnu může nastat a co může referenční objekt ohrozit, ať už na životech, zdraví, ztrátě, zničení nebo odcizení majetku, nebo ohrožení státní svrchovanosti a územní celistvosti, ohrožení životního prostředí a podobně, můžou se podnikat kroky k tomu, aby tyto nebezpečné situace nenastaly. Pokud by ale nastaly, bude se vědět, jak je možné se na ně připravit, umět jim čelit a jak je umět vládnout. [2]

1.2 Obsah bezpečnostní strategie

Každá bezpečnostní strategie by měla obsahovat následující body:

- shrnutí aktuálního stavu bezpečnosti daného referenčního objektu,
- analýza bezpečnostních rizik a hrozeb,
- návrh opatření k minimalizaci rizik.

Několikrát jsme zmínili pojmy riziko a hrozba. Rozdíly mezi nimi jsou takové, že riziko by se dalo charakterizovat jako jev, událost, proces, nebo činnost, který vzniká s určitou pravděpodobností, a zároveň má negativní následek. Riziku nelze přiřadit čas, ale pro potřeby modelování mu lze obecně přiřadit místo, objekty a subjekty. Riziko je vlastnost hrozby a má dva parametry:

- míru neurčitosti, která je charakterizována pravděpodobností vzniku jevu, události, procesu, nebo činnosti,
- velikost nebezpečnosti, která je charakterizována možnými následky na osoby, zvířata, majetek, kritickou infrastrukturu a životní prostředí.

Hrozba je hrozivá blízkost něčeho zlého, tedy jevu, události, procesu, který svými projevy, faktory, intenzitou a následky omezuje, ohrožuje, ničí, devastuje a likviduje životy, zdraví, majetek, životní prostředí, či kulturní hodnoty. Hrozba působí neustále a lze ji rozlišit na tři fáze:

- existence hrozby – ví se o existenci jevu, události, procesu, nebo činnosti, ale v daném okamžiku je hmota, síly a energie v rovnováze, pouze může dojít k určitým deformacím, výkyvům, anomáliím, kolísání hmot, sil a energií,
- působení hrozby – vznikla mimořádná událost, nebo krizová situace, je narušena rovnováha hmot, sil a energií jejich akumulací, či úbytkem, nebo došlo k expanzi nárůstu a k neřízenému uvolnění, nebo neřízené, náhlé regresi, či úbytku hmot, sil a energií,
- zánik hrozby – fyzikální, chemické, biologické, informační nebo jiné hrozby přestávají působit. Dochází k odstraňování deformací a adaptaci hmot, sil a energií po jejich uvolnění, či úbytku, je obnovována rovnováha hmot, sil a energií a vzniká nová rovnováha hmot, sil a energií.

Hrozba existuje neustále, riziko definuje, s jakou pravděpodobností dojde k naplnění hrozby. [9]

1.3 Tři roviny zajištění bezpečnosti

Zajištění bezpečnosti lze rozdělit do tří kategorií podle typu referenčního objektu:

- na úrovní státu,
- na úrovni skupiny států,
- na úrovni organizace.

1.3.1 Bezpečnost státu

Základní funkcí bezpečnostního systému státu je řízení a koordinace činnosti jednotlivých složek, odpovědných za zajišťování bezpečnostních zájmů státu. Určitým podílem se na zajištění bezpečnosti státu podílejí také státní orgány, orgány územní samosprávy a právnické a fyzické osoby. Například struktura bezpečnostního systému České republiky zahrnuje prezidenta republiky, Parlament, Vládu ČR, Bezpečnostní radu státu a její pracovní orgány, ústřední správní úřady, krajské a obecní úřady, záchranné sbory a havarijní služby. Funkční bezpečnostní systém představuje nejen nástroj pro účinné zvládání krizových situací vojenského i nevojenského charakteru, ale zajišťuje i prevenci a přípravu na možné krizové situace a jejich včasnou identifikaci a varování. Bezpečnostní systém státu musí neustále reagovat na měnící se podmínky a změny v bezpečnostním prostředí a na nově vzniklé hrozby a rizika. Fungování bezpečnostního systému, výstavba a rozvoj schopností jeho jednotlivých složek a hospodářské a finanční zabezpečení představují dlouhodobý a náročný proces, který čerpá ze zkušeností jednak z řešení různých krizových situací, z přípravy na takové situace a preventivního působení jednotlivých složek. [11]

1.3.2 Bezpečnost skupiny států

Společenství států má bezesporu své výhody i nevýhody. V případě, že by došlo k ohrožení bezpečnosti ČR, je pro ni výhodné být členem společenství jako je například EU nebo kolektivní obrany NATO. Mezi výhody takových společenství patří bezesporu posílení obranných možností země plynoucí z aliančních záruk podle Washingtonské smlouvy. Je v ní uvedeno, že bude případný útok proti jakékoli zemi NATO považován za útok proti všem a tomu bude odpovídat reakce spojenců. Dále je výhodou zapojení do systému kolektivní obrany, například do systému protivzdušné obrany. V případě ohrožení jsou garantovány bezpečnostních konzultace se spojenci, kde může Armáda ČR těžit z jejich zkušeností a posílit tak kvality, schopnosti a prestiž Armády České republiky. Další výhodu je také možnost podílet

se na vytváření politiky Severoatlantické aliance a spolurozhodování o klíčových bezpečnostních otázkách. Pro země, které jsou členem společenství, platí také zapojení do Programu bezpečnostních investic NATO a možnost čerpání finančních prostředků z něj. [11]

1.3.3 Bezpečnost organizace

Systém řízení bezpečnosti v organizaci velmi úzce souvisí s řízením rizik a je zaměřeno na vytvoření takových podmínek, která pomohou předcházet nebo minimalizovat rizika pomocí různých metod, procedur, směrnic, standardů a nástrojů. Cílem řízení bezpečnosti je zajistit bezpečný provoz a zamezit bezpečnostním rizikům a hrozbám, jako jsou ohrožení či poškození života a zdraví nebo hmotných a nehmotných aktiv organizace. Dokument, ve kterém jsou identifikována rizika a hrozby a opatření jak jim předcházet, se nazývá bezpečnostní strategie organizace.

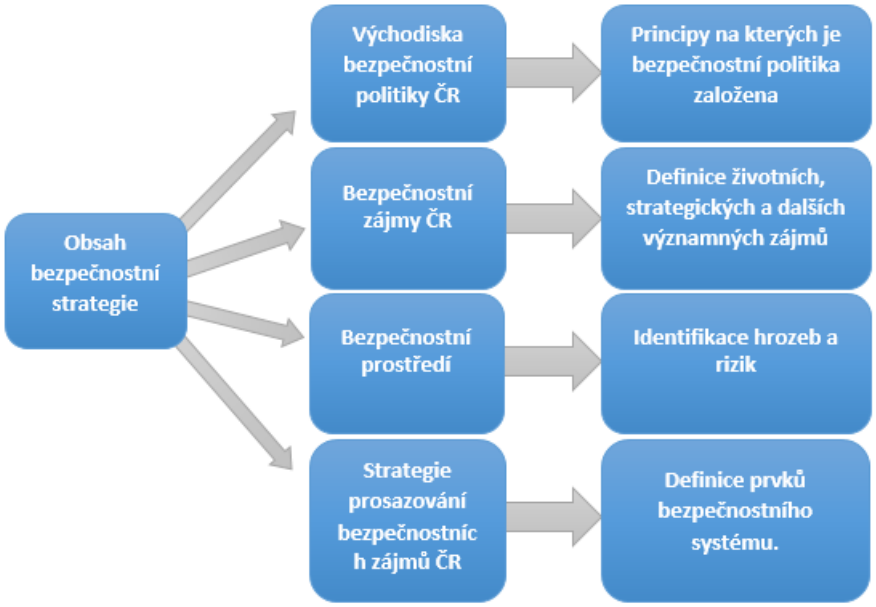
1.4 Bezpečnostní strategie ČR

Základem bezpečnostní politiky je souhrn cílů a nástrojů státu, které usilují o zabezpečení státní svrchovanosti a územní celistvosti, demokratických základů státu, jeho ekonomického a sociálního rozvoje, ale zaměřuje se též na jedince, zejména ohledně ochrany zdraví a života občanů, majetku, kulturních statků nebo životního prostředí a v neposlední řadě o plnění mezinárodních bezpečnostních závazků. Je důležité na začátku zmínit, že Bezpečnostní strategie ČR je dokument. Jedná se o základní dokument bezpečnostní politiky České republiky, jehož obsahem jsou informace o tom, jak ČR vnímá své bezpečnostní prostředí, jak specifikuje své bezpečnostní zájmy a také hrozby a jakým způsobem hodlá daným bezpečnostním hrozbám čelit. Na bezpečnostní strategii navazují další strategické a koncepční dokumenty. Právní rámec tohoto dokumentu vychází z Ústavy ČR, dále pak z Listiny základních práv a svobod a z ústavního zákona č. 110/1998 Sb., o bezpečnosti České republiky. Součástí právního rámce jsou samozřejmě také spojenecké a další mezinárodní závazky, které vyplývají z členství v mezinárodních organizacích, z nichž můžeme jmenovat tyto:

- Organizace Severoatlantické smlouvy (NATO),
- Evropská unie (EU),
- Organizace spojených národů (OSN),
- Organizace pro bezpečnost a spolupráci v Evropě (OBSE). [3]

1.5 Vývoj a obsah dokumentu

První bezpečnostní strategie ČR vznikla v roce 1999. V této době byl předsedou vlády současný prezident Miloš Zeman. Vznik dokumentu úzce souvisí se vstupem ČR do NATO. Aktualizace byla vydána vládou v roce 2001. Dokument byl již přesnější, co se terminologie týče, nicméně v tomtéž roce nastaly teroristické útoky v USA, které se staly důležitými milníky v oblasti zajištění globální bezpečnosti. V roce 2003, před přijetím Evropské bezpečnostní strategie, byla schválena nová verze Bezpečnostní strategie ČR. Vzhledem k dobovým okolnostem byla v této verzi věnována poměrná část problematice mezinárodního terorismu. V roce 2011 po rozhodnutí Bezpečnostní rady státu byla provedena další aktualizace a to v návaznosti na přijetí nových koncepčních dokumentů v NATO a EU. K poslední změně Bezpečnostní strategie ČR došlo začátkem února 2015. Jde ve značné míře o aktualizaci předešlého dokumentu z roku 2011. Tato změna proběhla zejména v důsledku zhoršujícího se bezpečnostního prostředí ve světě, které výrazně ovlivňuje bezpečnost euroatlantického prostoru a klade zvýšené nároky na NATO, EU i jednotlivé členské státy efektivněji na nové bezpečnostní hrozby a výzvy reagovat. Zpřesněna byla například analýza bezpečnostního prostředí, nově jsou v dokumentu vymezeny hrozby a trendy s dopady na bezpečnostní zájmy ČR. Uvádí se zde výčet souvisejících opatření k jejich předcházení. Strategie reflektuje zvýšené nároky na připravenost ČR a ostatních členů NATO a EU reagovat na nové bezpečnostní prostředí a posiluje důraz na plnění našich spojeneckých závazků. Dokument rovněž klade větší důraz na oblast zajištění vnitřní bezpečnosti. Bezpečnostní strategie reaguje na změny bezpečnostního prostředí a snaží se pojmenovat stěžejní hrozby se zaměřením na euroatlantický prostor. Jsou v ní definovány východiska bezpečnostní politiky České republiky, bezpečnostní zájmy, bezpečnostní prostředí a strategie prosazování bezpečnostních zájmů.



Obr. 1 Struktura Bezpečnostní strategie ČR

1.6 Bezpečnostní zájmy

V Bezpečnostní strategii ČR je uvedeno, že Česká republika vychází z předpokladu, že v dohledné budoucnosti lze vyloučit možnost rozsáhlého přímého vojenského útoku proti jejímu území i území jejích spojenců. Zároveň dochází k prohlubování integračních a demokratizačních procesů v euroatlantickém prostoru. Na straně druhé, se však na globální úrovni, především mimo euroatlantický prostor, v posledních dvou letech, zhoršilo bezpečnostní prostředí. Vzrostlo riziko realizace hrozeb asymetrického charakteru, zvláště v podobě teroristických útoků. [3] Nikde v tomto dokumentu ale není analyzována a zhodnocena situace na Ukrajině, kdy v roce 2014 v důsledku rozsáhlé vlny protestů známé jako Euromajdan v Kyjevě, došlo ke svržení vlády prezidenta Viktora Janukovyče a k rozšíření nepokojů napříč celou zemí. Toto období nejistoty a nestability bylo využito Ruskou federací k započetí vojenských operací vedoucím k jednostrannému vyhlášení nezávislosti Krymu na Ukrajině a jeho následné inkorporace do Ruské federace. Ukrajina není členem NATO, ani EU. Existuje však množství smluv a dohod chránících teritoriální integritu Ukrajiny, mezi něž patří Charta spojených národů, Závěrečný akt Konference o bezpečnosti a spolupráci v Evropě, protokol k ustanovujícímu prohlášení Společenství nezávislých států a Budapešťské memorandum o bezpečnostních zárukách. Západní země uvalily na Rusko v reakci na jeho naru-

šení teritoriální integrity Ukrajiny ekonomické sankce. Krym je ale stále, navzdory úsilí západních států o přinucení Ruska k podřízení se mezinárodně uznávaným normám a upuštění od nezákonného jednání prostřednictvím ekonomických sankcí, součástí Ruské federace, jejíž oficiální pozice vzhledem k této problematice zůstává nezměněná. [4] Česká republika rozlišuje své bezpečnostní zájmy podle stupně důležitosti. V Bezpečnostní strategii jsou zájmy rozděleny do tří kategorií: životní, strategické a další významné zájmy. Nejdůležitějšími jsou životní zájmy. [3]

1.6.1 Životní zájmy

Mezi nejdůležitější životní zájmy patří především zajištění existence České republiky, její suverenity, územní celistvosti a politické nezávislosti. Dále je to obrana demokracie a právního státu a ochrana základních lidských práv a svobod obyvatel. Životní zájmy zabezpečuje stát rozsáhlými opatřeními bezpečnostní strategie, kterou provádí pomocí zahraniční, obranné a hospodářské politiky a politiky v oblasti vnitřní bezpečnosti a veřejné informovanosti. [3]

1.6.2 Strategické zájmy

Uskutečňování strategických zájmů je úzce spjato s ochranou životních zájmů. Napomáhají k zajištění společenského rozvoje a prosperity ČR. Mezi strategické zájmy řadíme především bezpečnost a stabilitu nejen v ČR, ale i v euroatlantickém prostoru. Důležitá je též prevence a zvládání místních a regionálních konfliktů a zmírňování jejich následků. Pro ČR je do budoucna důležité členství v mezinárodních organizacích, posilování soudržnosti a efektivnosti NATO a EU a naplňování strategického partnerství mezi NATO a EU, včetně posilování jejich spolupráce v rámci obranných a bezpečnostních schopností. Stejně tak rozvíjení role OBSE v oblasti prevence ozbrojených konfliktů, demokratizace a posilování vzájemné důvěry a bezpečnosti. Strategické zájmy se též zaměřují na spolupráci s partnerskými zeměmi v oblasti mezinárodní stability. Zaměřují se na ochranu demokracie, základních svobod a principů právního státu a také na zajištění vnitřní bezpečnosti a ochrany obyvatelstva, stejně jako na zajištění ekonomické bezpečnosti ČR a posilování konkurenceschopnosti ekonomiky.[3]

1.6.3 Další významné zájmy

Účelem prosazování dalších významných zájmů je přispět k zajištění životních a strategických zájmů ČR a zvyšovat odolnost společnosti vůči bezpečnostním hrozbám. Mezi další

významné zájmy zejména patří snižování kriminality, posilování zpravodajské ochrany a obrany ČR, potlačování extremismu a jeho příčin, zvyšování efektivity a profesionality státních institucí a soudnictví, rozvoj občanských sdružení a nevládních organizací působících v oblasti bezpečnosti nebo ochrana životního prostředí. [3]

1.7 Charakteristika bezpečnostního prostředí

Bezpečnostní prostředí lze označit jako pojem, zahrnující jak přírodní, tak společenskou stránku reality. Zabývá se možnými ohroženími a zranitelností zkoumaného prostředí. Bezpečnostní prostředí je jak vnější, tak vnitřní, ovlivňující bezpečnost státu. U vnějšího bezpečnostního prostředí jde o prostor nacházející se vně státních hranic České republiky, ve kterém se realizují a střetávají zájmy našeho státu se zájmy jiných aktérů mezinárodních vztahů a v němž se odehrávají procesy, které mají významný vliv na úroveň bezpečnosti České republiky. Události odehrávající se v prostředí mimo území České republiky se pak přímo i nepřímo promítají do prostoru České republiky. Prostor na území České republiky považujeme za vnitřní bezpečnostní prostředí. Působením na dané podmínky lze dosáhnout minimalizaci rizik, zabránění vzniku nežádoucích událostí, omezení jejich negativních dopadů, včetně rekonstrukce následků způsobených případnou nežádoucí událostí. Potřeba prognóz zde vyvstává do popředí, protože v této oblasti je důležité vytvoření představy o bezpečnostním prostředí v budoucnosti a na jejím základě, protože není jednoznačně determinována a vychází ze subjektivních pohledů, ji lze určitým způsobem ovlivňovat, nebo se na ni připravit. [11]

1.7.1 Hrozby a rizika pro Českou republiku

Bezpečnostní strategie v souvislosti s charakterizací bezpečnostního prostředí používá dva základní pojmy:

- hrozbu jako vnější fenomén s potenciálem poškodit zájmy ČR,
- riziko jako pravděpodobnost vzniku událostí, považované z bezpečnostního hlediska za nežádoucí,
- ekonomické.

Mezi současné nejzávažnější hrozby pro Českou republiku patří teroristé, teroristické skupiny a hnutí. Ti působí nejen lokálně, ale i globálně a koordinovaně. Ve spojení s extremistickými skupinami a v kombinaci se snahou o získání zbraní hromadného ničení vytváří pro

Českou republiku hrozbu strategického významu. Používají asymetrickou strategii, což znamená, že se vyhýbají přímému střetu. Za objekty útoku si vybírají převážně civilní cíle především ve městech, používají prostředky hromadné destrukce, usilují nejen o získání zbraní hromadného ničení, ale i nově vyvíjené druhy zbraní. Dalšími hrozbami jsou nestabilita a regionální konflikty v euroatlantickém prostoru a jeho okolí, oslabování mechanismu kooperativní bezpečnosti, migrace nebo extremismus. Lze identifikovat čtyři typy možných konfliktů, které mají potenciál vyústit do ozbrojených střetů:

- etnické,
- teritoriální,
- politické,

V době kdy je svět takřka závislý na informačních technologiích se stále zvyšuje také hrozba kybernetických útoků. Bezpečnostní strategie též zmiňuje mezi hrozbami ohrožení funkčnosti kritické infrastruktury, přerušení dodávek strategických surovin, energie nebo také organizovaný zločin.

Hrozby mohou mít také přírodní a antropogenní původ. Nežádoucí stav mohou způsobit extrémní výkyvy počasí. U antropogenního původu jde především o infekční nemoci s pandemickým potenciálem. [3]

1.8 Dlouhodobá strategie vlády pro prosazování bezpečnosti v ČR

Pro ČR je do budoucna stěžejní především účast v mezinárodních organizacích, zejména systému kolektivní obrany NATO. ČR je trvale zapojena do aliančního integrovaného systému protivzdušné obrany, známého také pod zkratkou NATINADS, který je jedním ze základních pilířů obrany ČR. ČR vytváří podmínky pro aktivní účast v misích NATO, EU a OSN při řešení celého spektra krizí – ať již před konflikty, během nich či po nich. ČR přispívá k posilování schopností třetích zemí poskytováním výcviku místním silám či asistencí v oblasti reformy bezpečnostního a obranného sektoru. ČR se zapojuje do Společné zahraniční a bezpečnostní politiky EU a v jejím rámci do Společné bezpečnostní a obranné politiky a jejích misí. Podílí se na financování a realizaci evropské rozvojové spolupráce a humanitární pomoci. Současně těží ze vzrůstající spolupráce zemí EU v oblasti vnitřní bezpečnosti, ochrany obyvatelstva, ochrany kritické infrastruktury, kybernetické bezpečnosti, při potlačování a zmírňování následků, plynoucích z nelegální migrace, organizovaného zločinu, terorismu a nestability dodávek klíčových energetických a jiných surovin.

Kromě zapojení v mezinárodních organizacích ČR prosazuje své bezpečnostní zájmy také prostřednictvím budování vztahů zejména se sousedními zeměmi a regionální spolupráce včetně Visegrádské skupiny. Podrobně jsou jednotlivé body dlouhodobé strategie popsány v bezpečnostní strategii. Česká republika zpracovává i další strategické dokumenty, které jsou uvedeny v tabulce 1.

Rok vzniku	Název dokumentu
2001	Doktrína Armády České republiky
2002	Koncepce výstavby profesionální AČR a mobilizace ozbrojených sil ČR
2003	Bezpečnostní strategie ČR
2003	Koncepce výstavby profesionální AČR a mobilizace ozbrojených sil ČR
2004	Národní strategie vyzbrojování
2006	Zpráva o zajištění obrany ČR
2007	Transformace resortu Ministerstva obrany České republiky
2008	Dlouhodobá vize resortu MO
2008	Principy obrany ČR 2030
2008	Vojenská strategie ČR
2011	Bezpečnostní strategie České republiky - září 2011
2011	Plán obrany ČR
2012	Obranná strategie ČR - září 2012
2015	Bezpečnostní strategie České republiky - únor 2015
2015	Dlouhodobý výhled pro obranu 2030
2015	Koncepce výstavby armády České republiky 2025

Tab. 1 Další strategické dokumenty ČR [5]

Tabulka 1 obsahuje přehled dalších strategických dokumentů v oblasti bezpečnosti a obrany, které Česká republika v této oblasti zpracovává.

1.9 Bezpečnostní strategie na úrovni EU

Evropská unie v roce 2003 schválila svoji první bezpečnostní strategii, která vymezuje evropské představy o vlastní roli ve světové bezpečnosti a o hrozbách, kterým musí EU a její členské státy čelit. Po vstupu Lisabonské smlouvy v platnost je možné mezi některými členskými státy navázat prohloubenou spolupráci v oblasti obrany, která se označuje termínem stálá strukturovaná spolupráce. Stálá strukturovaná spolupráce musí být povolena Radou, která o ní na žádost zúčastněných států rozhoduje kvalifikovanou většinou. Mezi instituce EU řadíme Evropský parlament. Za otázky bezpečnostní a obranné politiky v Parlamentu odpovídá Podvýbor pro bezpečnost a obranu, který patří pod Výbor zahraničních věcí. Dále mezi ně řadíme Evropskou komisi - politicky za oblast Společné bezpečnostní a obranné politiky odpovídá Vysoká představitelka Unie pro zahraniční věci a bezpečnostní politiku. Poslední institucí je Evropská rada - v oblasti SBOP vymezuje zásady a obecné směry jejich dalšího rozvoje. Společná bezpečnostní a obranná politika byla založena v roce 1999. Do vstupu Lisabonské smlouvy v platnost se označovala jako Evropská bezpečnostní a obranná politika (SZBP). Zahrnuje spolupráci v oblasti vojenství a zvládání krizí v rámci širší Společné zahraniční a bezpečnostní politiky EU. V rámci politik si drží zvláštní postavení. Od svého založení Evropská unie v rámci Společné bezpečnostní a obranné politiky EU zrealizovala několik desítek zahraničních vojenských a civilních operací.[15]

1.9.1 **Instituce SBOP**

Společná bezpečnostní a obranná politika vychází z obecného rámce Společné zahraniční a bezpečnostní politiky. Specifické otázky vojenského a civilního krizového managementu vedly k vytvoření řady specifických institucí jako je například Politický a bezpečnostní výbor (COPS), který funguje jako přípravný orgán pro Radu. Mezi hlavní funkce patří sledování mezinárodní situace a pomoci při definování politiky v rámci společné zahraniční a bezpečnostní politiky. Hlavní rozhodovací práva má Rada pro vnější vztahy, jejímiž členy jsou ministři zahraničí členských států. Setkání probíhá jednou do měsíce, což pro operativní rozhodování, které je při řízení probíhajících misí zapotřebí, nestačí. Každodenní rozhodnutí tedy přijímá COPS. Jeho členy jsou zástupci členských států na úrovni velvyslanců, kteří sídlí nastálo v Bruselu. Scházejí se obvykle dvakrát týdně, v případě potřeby i častěji. Vojenský výbor Evropské unie (EUMC) je nejvyšší vojenský orgán zřízený v rámci Rady a je složen z náčelníků generálních štábů členských států, kteří se scházejí a doporučují další postup COPS v otázkách vojenství a využití vojenské síly v operacích. Výbor pro civilní

aspekty řešení krizí asistuje ostatním institucím při civilních operacích. Vojenský štáb EU slouží k dlouhodobějšímu strategickému plánování a včasnému varování. Stálé operační centrum na úrovni EU je útvar schopnosti civilního plánování a provádění, označovaný anglickou zkratkou CPCC. Ředitelství pro řízení a plánování krize, které zajišťuje, aby EU dokázala účinně využívat své nejsilnější stránky, jako je schopnost integrovat vojenský a civilní přístup ke krizovému managementu. Při přibližování a sjednocování bezpečnostních politik členských států spolupracuje celá řada samostatných institucí a agentur. Mezi nejdůležitější patří Evropská obranná agentura. Ta má za úkol hledat cesty, jak harmonizovat a koordinovat vyzbrojování armád členských států. Agentura má čtyři hlavní funkce:

- rozvoj obranného potenciálu,
- spolupráci ve vyzbrojování,
- evropské obranné technologické a průmyslové základny a trh s obranným vybavením,
- výzkum a technologie. [15]

1.9.2 Vztahy s NATO

Členská základna Evropské unie a Severoatlantické aliance se z velké části překrývá. 21 států je součástí obou organizací, tedy tři čtvrtiny z 28 členů EU a 28 členů NATO. Není proto divu, že byl způsob spolupráce s Aliancí vždy důležitým tématem při vývoji SBOP.

1.10 Shrnutí

Pokud se zaměříme na význam slova strategie, vyplyne nám skutečnost, že bezpečnostní strategie ČR ne zcela naplňuje význam tohoto slova. Je velmi obecná a i když jsou v ní uvedeny cíle, kam by měla Česká republika ve snaze zajistit svoji bezpečnost směřovat, nejsou v ní uvedeny konkrétní kroky, jak toto zajistit. Je určitě důležité zabývat se budoucností bezpečnostní situace ČR, nicméně dle mého názoru by bylo možné vyhotovit efektivnější výstup v rámci postupů pro dosažení stanovených cílů. Bezpečnost České republiky je z velké části závislá také na okolních státech a společenstvích, kterých je členem, což nese pozitivní, ale i negativní důsledky. V případě možného mezinárodního konfliktu bychom se sami těžko bránili. Proto je pro Česko přínosem společenství v mezinárodních organizacích. V rámci společenství se ale musíme podřizovat a přijímat nastavená pravidla, což nemusí být vždy v absolutní shodě s našimi záměry a myšlenkami.

2 BEZPEČNOSTNÍ STRATEGIE ORGANIZACE

Bezpečnost je stav, kdy je velikost všech rizik v organizaci na akceptovatelné úrovni. Nástrojem pro zajištění bezpečnosti je bezpečnostní systém. Firmy musí chránit svůj majetek a dbát na bezpečnost svých zaměstnanců. Dnes je také samozřejmostí, že veškeré důležité informace, se kterými organizace pracují, jsou převáděny do digitální podoby a firmy by se bez svých informačních systémů a sítí jen těžko obešly. Tato skutečnost je ale spojena s možnými bezpečnostními riziky. Proto by v každé firmě měla být vypracována souhrnná bezpečnostní strategie, která upozorní na konkrétní bezpečnostní hrozby a rizika a povede k zajištění ochrany majetku, osob, zaměstnanců, jejich zdraví, ochrany dat a samozřejmě také kontinuity podnikání.

2.1 Bezpečnostní strategie a bezpečnostní politika

Bezpečnostní strategie je základní dokument celkového zabezpečení organizace. Umožňuje koncepční a konzistentní budování a zajištění bezpečnosti v organizaci. Tento dokument v obecné rovině popisuje cíle organizace v oblasti jejího zabezpečení a konkrétní kroky jak jich dosáhnout. V zájmu vedení firmy pak musí být prosazování bezpečnostní politiky vyplívající ze strategie a všech jejích částí. Účelem těchto bezpečnostních činností je nastolit fungující bezpečnostní politiku a udržovat požadovanou míru fyzické, informační, požární i personální bezpečnosti a BOZP, v celé firmě všemi zaměstnanci i externími subjekty.

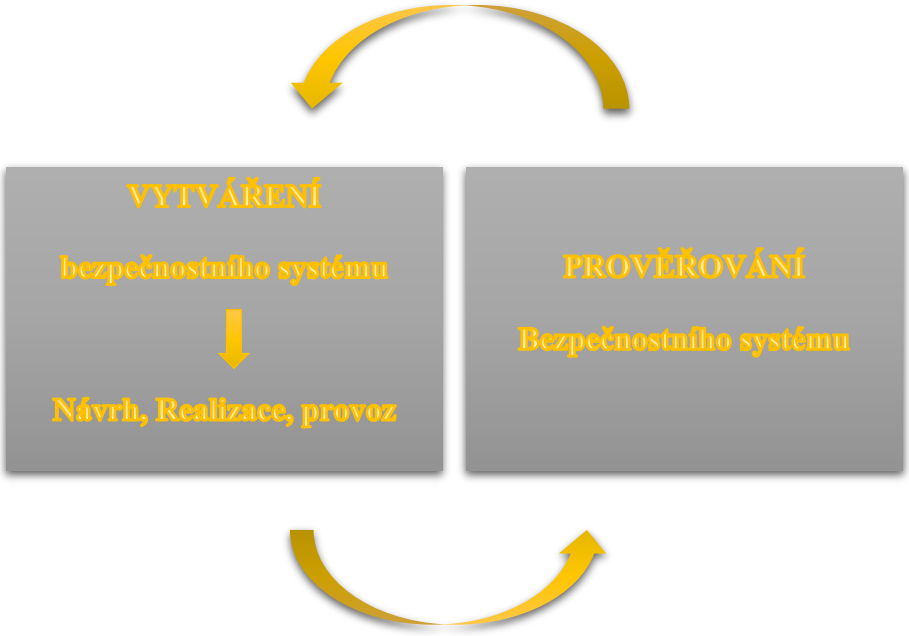
2.2 Otázky zajištění bezpečnosti

Bezpečnostní strategie organizace musí odpovědět na tyto otázky:

- Jaké jsou cíle organizace v oblasti ochrany aktiv?
- Jaká aktiva musí být chráněna?
- Jaká je cena těchto aktiv?
- Kdo za ně nese zodpovědnost?
- Jaká opatření budou efektivní?
- Jak bude jejich dodržování vynuceno, jaká penalizace bude za jejich nedodržení?
- Kdy a jak bude Bezpečnostní strategie zavedena do praxe?
- Jaký je cílový stav bezpečnostního systému?
- Jak a které osoby budou proškoleny?
- Jak zajistit osobní odpovědnost zaměstnanců?

2.3 Bezpečnostní systém organizace

Bezpečnostní systém se vyznačuje dynamikou a vliv na něj mají různé proměnlivé činitele zasahující do procesů, které v něm probíhají. Tyto činitelé mohou působit jak zevnitř, tak z vnějšího prostředí. Společným faktorem změn pro většinu bezpečnostních systémů je zejména právní rámec, ve kterém působí, protože způsob ochrany bezpečnostních zájmů organizace musí být vždy v souladu s pravidly danými právním řádem. K zajištění optimální funkce bezpečnostního systému je zapotřebí, aby v jeho životních cyklech byla udržována rovnováha mezi dynamikou systému ovlivňovaného nestálými podmínkami, na straně jedné a potřebou zachování jeho účinnosti nebo efektivnosti, na straně druhé. Řízení bezpečnostního systému proto vyžaduje dohled nad procesy, které v něm probíhají. Jedním z velmi účinných nástrojů k trvalému udržování efektivnosti a účinnosti bezpečnostního systému je jeho systematické prověřování, na základě něhož by měly být prováděny potřebné kvalifikované a systémově orientované korektury. Prověřování proto musí být součástí životního cyklu bezpečnostního systému. Cyklus, který se řídí obecnými principy řídicího cyklu, má dvě základní fáze, které jsou vyobrazeny níže.



Obr. 2 Životní cyklus bezpečnostního systému

2.4 Kontrola způsobu zajištění bezpečnosti

Způsob prověřování bezpečnostního systému můžeme zajistit například pomocí dozoru, revize, posouzení, kontroly, revize nebo bezpečnostním auditem. Bezpečnostní kontrola je jedním z neúčinnějších způsobů prověřování bezpečnostního systému organizace. Ověřuje totiž nejen funkčnost systému ale i správnost jeho nastavení v organizaci, což znamená soulad s obecně závaznými předpisy a dosažení optimalizace rizik. Kontrolu bezpečnosti lze provádět pouze tam, kde již existuje nějaký bezpečnostní systém. Kontrola vyhodnotí současný stav systému z hlediska shody s bezpečnostními standardy. Jejím účelem je především předcházet chybám a teprve v druhé řadě napravovat chyby, které již nastaly. Zaměřuje se tedy na prevenci systémových nedostatků a na jejich vyhledávání ve stávajícím systému bezpečnosti podniku. [13]

2.4.1 Průběh bezpečnostní kontroly

Průběh bezpečnostní kontroly se řídí principy organizačního cyklu v obecném smyslu.

Obr. 3 Průběh bezpečnostního kontroly

Prověření probíhá shromážděním všech dostupných údajů známými metodami, jako je pozorování, seznámení s dokumentací, srovnávání nebo modelování. Analýza probíhá vyhodnocením stavu z hlediska rizik. Tvoří hlavní fázi celého procesu. Kvalita analýzy rizik určuje platnost závěrů a doporučení. Doporučení pak obsahuje návrh protiopatření pro optimalizaci rizik.

2.4.2 Formy bezpečnostní kontroly

Bezpečnostní kontrola může mít několik forem a můžeme ji dělit například dle časového kritéria nebo věcného kritéria. Dle časového kritéria jde o plánovanou, mimořádnou a následnou kontrolu. Dle věcného kritéria jde o zaměření kontroly na jednotlivé oblasti bezpečnosti v organizaci a o její rozsah, tedy zda bude komplexní nebo dílčí. [13]

2.5 Legislativa

Při zpracování návrhu bezpečnostní strategie organizace musíme klást důraz mimo výsledků analýzy rizik také na požadavky, které vyplývají z platné legislativy. Základní přehled zákonů, norem a systémů jakosti, které se vztahují k bezpečnostní politice organizace, uvádím níže v této kapitole. Pojem bezpečnost organizace zahrnuje široké spektrum oblastí napříč firmou, kterých se dotýká a která musí být legislativně ošetřena.

2.5.1 Zákony

Důležitými zákony pro tuto oblast jsou:

- Zákon č. 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů v platném znění,
- Zákon č. 499/2004 Sb. o archivnictví a spisové službě a o změně některých zákonů v platném znění,
- Zákon č. 240/2000 Sb. o krizovém řízení a o změně některých zákonů v platném znění,
- Zákon č. 106/1999 Sb. o svobodném přístupu k informacím v platném znění,
- Zákon č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti v platném znění,
- zákon č. 262/2006 Sb. Zákoník práce,
- Zákon č. 309/2006 Sb., o zajištění dalších podmínek bezpečnosti a ochrany zdraví při práci,
- Zákon č. 133/1985 Sb., o požární ochraně.

2.5.2 Normy

V mezinárodní normě ISO/IEC 17799 je uvedena specifikace požadavků na systém řízení v oblasti bezpečnosti informací. Jde o stěžejní normu pro zavádění a certifikaci systémů řízení organizace. Systém managementu bezpečnosti informací je uveden v Normě BS 7799-2. Norma ČSN ISO/IEC 27001 stanoví požadavky na systém managementu bezpečnosti informací tak, aby byla organizace schopna vyhodnocovat svá rizika a uplatňovat náležité kontrolní a řídící mechanismy k zachování důvěrnosti, integrity a dostupnosti informací. Norma ČSN ISO/IEC 15408 se týká informačních technologií, bezpečnostní techniky a kritérií pro hodnocení bezpečnosti IT. Norem týkajících se bezpečnosti je celá řada, mezi další důležité patří také Norma ČSN EN 5 130, týkající se poplachových systémů a mnohé další.

2.5.3 Ostatní právní předpisy v rámci Evropské Unie

Zde bychom mohli zmínit například Směrnici rady č. 1991/250/EHS o právní ochraně počítačových programů nebo Směrnici EU 1995/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Další důležitou je Směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací. Směrnice rady č. 2001/264/EC, kterou se přijímají bezpečnostní předpisy Rady

a Nařízení Evropského parlamentu a Rady 2001/45/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů také patří mezi ty, které bychom zde měli jmenovat.

2.5.4 Výhody na nevýhody použití norem při zajištění bezpečnosti

Standardy vytvářejí vzor řešení určitého problému, není tedy nutné dané problémy řešit vždy znovu. Tím se šetří čas i prostředky. Pokud se problémy řeší pomocí stejného standardu, povaha výsledků je vždy stejná, a je tak možné je sdílet, nebo používat stejným způsobem. K výhodám užívání norem v organizaci patří zejména sjednocení provedení výrobků, zajištění vyměnitelnosti součástí na strojích při opotřebování nebo poškození, zvýšení sériovosti, hromadnosti a plynulosti výroby, čímž se přispívá k její zrychlení a zlevnění. Další výhodou je bezesporu zhospodárnění výroby a snížení ceny výrobků, zobecnění způsobů provádění výpočtů, projektování, konstruování a metody zkoušení materiálů a výrobků. Normy též pomohou zobecnit značky, symboly nebo názvy jednotek. Za nevýhody můžeme označit to, že standardizace omezuje uživatele na předem dané postupy a případy určené standardem. Standardizací není možné postihnout všechny možné případy. Vývoj a udržování standardu vyžaduje financování a někdo je tedy musí hradit. Standardy mohou být předmětem patentů a za jejich používání je nutné platit licenční poplatky.

2.6 Bezpečnostní management

Cílem bezpečnostního managementu je správa bezpečnosti v organizaci, zajišťující její požadovaný stav. Přijímaná bezpečnostní opatření musí být cílená. Opatření můžeme rozdělit na preventivní a represivní. Cílem preventivních opatření je působit proti příčinám, řešit příčiny expozice bezpečnostních hrozeb. Represivní opatření nastupují v případě akutní možnosti expozice bezpečnostních hrozeb a při jejich expozici. Represivní opatření působí vůči škodícímu účinku, brání vzniku újmy nebo alespoň zmírňují její velikost. Pro konkrétní obsah bezpečnostního managementu je důležité provést potřebnou analýzu rizik, potřeb zajištění bezpečnosti a z toho vyvodit odpovídající požadavky na bezpečnostní management. Významný vliv na charakter bezpečnostního managementu bude mít i to, jedná-li se o bezpečnost vůči záměrným nebo nezáměrným hrozbám. Zabezpečení vůči záměrným hrozbám vyžaduje silové působení a trvalou připravenost. Při zabezpečení vůči nezáměrným hrozbám

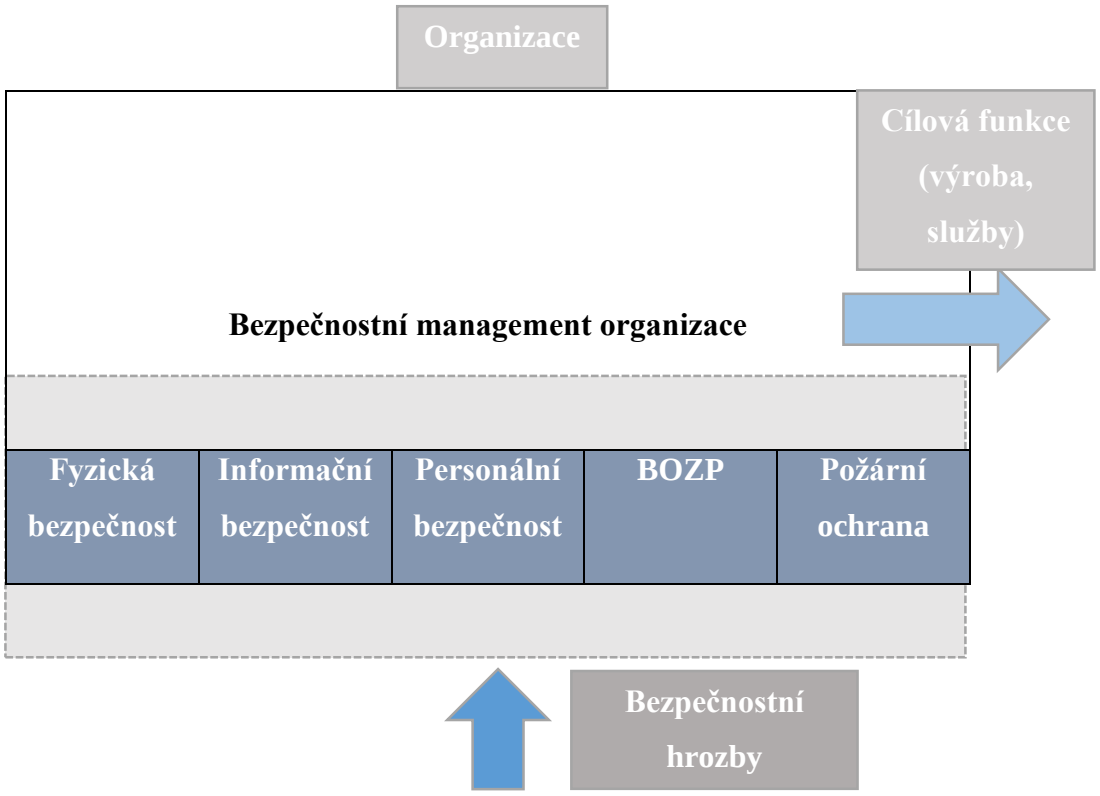
je kladen důraz na kontrolu stavu a podmínek, dodržování pravidel i připravenost ochranných opatření. Mezi základní požadavky na bezpečnostní systém a tím i zprostředkovaně bezpečnostní management patří:

- připravenost
- reakce-schopnost
- adekvátnost
- vytrvalost
- pružnost
- řiditelnost
- ekonomická efektivnost [2]

2.7 Oblasti bezpečnostní strategie organizace

Bezpečnostní strategii organizace mohou tvořit zejména následující oblasti:

- fyzická bezpečnost,
- informační bezpečnost,
- personální bezpečnost,
- bezpečnost a ochrana zdraví při práci,
- požární ochrana. [5]



Obr. 4 Bezpečnostní management v organizaci [5]

Z těchto oblastí budeme vycházet v praktické části, při analýze bezpečnostní politiky v organizacích.

2.8 Shrnutí

Obsahem bezpečnostní strategie je zejména stanovení cílů a popis způsobu zajištění celkové bezpečnosti informačního systému ve vztahu k bezpečnosti organizace. Je to výběr bezpečnostních zásad a předpisů splňující bezpečnostní politiku organizace a všeobecně definujících bezpečné používání systémů v rámci organizace. Jedná se tedy o detailní normy, pravidla, praktiky, předpisy konkrétně definující způsob zajištění bezpečnosti organizace. Dokumenty celkové bezpečnostní strategie by měly být předloženy zaměstnancům organizace a to ve formě, která je relevantní, přístupná a pochopitelná.

Praktické zavedení jednotlivých opatření do každodenního provozu fungující organizace vždy přináší určité restrikce vůči zaměstnancům a klade na ně požadavky, na něž dosud nebyli zvyklí. Zatímco restriktivní složka těchto opatření je patrná hned a pracovník ji pocítí s okamžitou platností, přínos daných opatření už tak snadno a jasně vidět není a obvykle se projeví až po určitém časovém úseku. Je zřejmě v lidské přirozenosti se všem změnám bránit, a tak je prosazení nových opatření a zavádění nových struktur nesnadný úkol. Od zodpovědných pracovníků vyžaduje velkou dávku trpělivosti, asertivity a znalosti lidských vztahů.

II. PRAKTICKÁ ČÁST

3 ANALÝZA BEZPEČNOSTNÍ POLITIKY FIREM

V praktické části budeme analyzovat bezpečnostní politiku ve dvou organizacích. Obě se zabývají stejnou činností. Tyto organizace působí ve strojírenství. Firmy byly dotazovány v rámci zjištění informací o zajištění bezpečnostní politiky v oblasti personální, informační, fyzické, požární a BOZP a byly od nich vyžádány veškeré dokumenty spojené s bezpečností pro provedení analýzy. Kompletní analýzu provedeme u firmy A, obecnou analýzu vyhotovíme pro druhou firmy, označenou písmenem B.

3.1 Organizace A

Organizace A se zabývá průmyslovou výrobou, patří do kategorie velkých firem a má historii 165 let. V Česku patří mezi nejlepší firmy ve svém oboru. Pro tuto společnost nyní pracuje cca 800 zaměstnanců. Její produkty jsou žádány jak na tuzemském, tak i zahraničním trhu.

Obr. 5 Sídlo společnosti a výrobní hala organizace A

Analýza bezpečnostní situace v organizaci A proběhne na základě rozdělení podle charakteru chráněného aktiva, tedy podle rozdělení na fyzickou, personální, informační bezpečnost, bezpečnost a ochranu zdraví při práci a požární ochranu. Následně bude zhodnocena bezpečnostní dokumentace firmy a ve shrnutí budou uvedeny zjištěné nedostatky.

3.1.1 Fyzická bezpečnost

Ve firmě probíhá kontrola oprávněnosti vstupu osob a evidence návštěv, kterou zajišťuje vrátnice provedením zápisu do návštěvní knihy. Firma plánuje koupit SW na evidenci návštěv z důvodu zlepšení přehlednosti, historie a také BOZP. Objekty jsou oploceny, aby se zamezilo neoprávněnému vniknutí osob do objektu. Vrátní mají seznam nepovolených návštěv.

Vrátnice je zodpovědná za:

- kontrolu obsahu zavazadel,
- kontrolu nákladů vozidel podle dokladu,
- kontrolu vynášení předmětů,
- klíčový režim,
- kontrolu firemních aut,
- pochůzkovou činnost po areálu,
- obsluhu centrálního telefonu.

Za poskytování základních informací návštěvám a zejména poučení o bezpečnosti a chování v areálu firmy odpovídá osoba, která si návštěvu pozvala. Existuje formulář poučení o BOZP a chování v areálu. Je v plánu tuto odpovědnost převést na vrátnici. Budovy jsou opatřeny kódováním, externí firma provádí dálkový monitoring a provádí výjezdy při poplachu. Přestože je zde nepřetržitý provoz vrátnice, v noci je zdvojen systém ostrahy. Vyhodnocování poplachu z poplachového systému probíhá přes externí firmu. V případě vzniku závažné události na objektu volá vrátný nebo externí firma na správu majetku. Pokud se nedovolá na správu majetku, tak osobě odpovědné za provozovnu. Správa majetku všechny incidenty hlásí správnímu řediteli nejpozději následující pracovní den. Celý tento úsek zajištění bezpečnosti spadá pod správního ředitele. Mezi zjištěné nedostatky patří skutečnost, že se nedodržuje pravidlo vyzvednutí návštěvy pracovníkem, za kterým návštěva přišla, jak je uvedeno v provozní dokumentaci. Návštěva bývá vpuštěna do areálu bez doprovodu pověřené osoby, bez poučení o chování a bezpečném pohybu po objektu. Za toto poučení zodpovídá osoba, která si návštěvu pozvala. Existuje formulář o poučení o BOZP a chování v areálu, nikdo ho ale nepoužívá. Toto by mělo být v kompetencích vrátnice. Kontrolu firemních aut neprovádí vrátnice důsledně. Auta prohlíží namátkově a auta některých zaměstnanců vůbec.

3.1.2 Personální bezpečnost

Každý zaměstnanec má přístup pouze k těm informacím, které potřebuje k vykonávání své práce. Ve firmě je používán MS Dynamics Axapta, přístup by měl být povolen pouze k práci s daty, která jsou nezbytná pro práci jednotlivých lidí. Za toto zodpovídá správní ředitel a ředitel pro strategii a projekty. U tištěné technické dokumentace je její výdej vázán pravidly a zodpovídá za ni výrobní ředitel. Datovou technickou dokumentaci spravuje technický

úsek. U smluvní dokumentace aktuálně probíhá projekt na její evidenci a zabezpečení. Informace o dodavatelích a odběratelích jsou spravovány v programu Axapta. Zodpovědnost je na řediteli nákupu a obchodním řediteli. Zde by bylo vhodné prověřit natavení přístupů jednotlivých zaměstnanců k stěžejním datům. Neexistuje dokument, který by jasně definoval, kdo má jaká oprávnění a z jakého důvodu. Je zde též zmíněno, že u smluvní dokumentace právě probíhá projekt na její evidenci a zabezpečení. Z toho vyplývá, že aktuálně žádná forma evidence, ani zabezpečení této dokumentace neexistuje. Přitom smluvní dokumentace obsahuje citlivé údaje, jako jsou informace o dodavatelích, odběratelích, bankovních účtech a částkách, nebo informacích zajímavých pro konkurenční firmy.

3.1.3 Informační bezpečnost

Problematika datových přenosů je popsána v organizačním řádu sítě, je ale spíše obecná a málo popisující. Ochrana počítačových sítí, kabelových i bezdrátových propojení a ochrana před vnějšími i vnitřními útoky v tomto řádu není blíže specifikovaná. Identifikace a analýza rizik ve vztahu k informační bezpečnosti neproběhla. Stejně tak zajištění dat a zálohování je uvedeno v organizačním řádu sítě pouze v obecné podobě. Scénáře obnovy dat nejsou v řádu specifikovány. Definování a dodržování bezpečnostních směrnic není nastaveno. Systém pro správu námětů a připomínek, který můžeme také nazvat jako helpdesk, není nastaven. Pro tyto účely je zřízena pouze emailová adresa, u které ale není dohledatelná korespondence ze strany uživatele. Firemní informace z hlediska bezpečnosti podle jejich hodnoty, právní citlivosti, nebo jejich kritičnosti nejsou nijak klasifikovány. Zodpovědnou osobou pro tuto oblast je správní úsek. Z výše uvedených poznatků je možné zhodnotit zajištění informační bezpečnosti jako absolutně nedostatečné ve všech směrech. Organizační řád sítě je zpracován pouze na obecné úrovni, což můžeme u tak velké firmy označit jako hazard. V případě ztráty důležitých strategických dat by to mohlo vést k ohrožení chodu firmy, dokonce k ohrožení její existence. Dále je zde absence systému podávání stěžejních informací zainteresovaným osobám. Informace o rozhodnutích vedení, které mají dopad na oblast bezpečnosti, musí být poskytnuty osobám zodpovědným za bezpečnost organizace. Pokud to tak není, nemůže být tento systém fungující a aktuální. Také není zajištěna informační bezpečnost v rámci klasifikace firemní dokumentace.

3.1.4 Bezpečnost a ochrana zdraví při práci

Základní normou, kterou se BOZP ve firmě řídí, je zákon č. 262/2006 Sb., zákoník práce. Dalším je zákon č. 309/2006 Sb., o zajištění dalších podmínek bezpečnosti a ochrany zdraví

při práci. Firma se také drží standardu OHSAS 18001. BOZP ve firmě zajišťuje externista. Pro zaměstnance je pořádáno vstupní a pak periodické školení, které se řídí podle zákonů a vyhlášek a podrobně je rozpracováno v řídící dokumentaci. Pro kontrolu proškolení zaměstnanců jsou ve firmě pořádány audity. Za školení zodpovídá správní a personální ředitel. Osobní ochranné pracovní pomůcky zajišťuje výrobní úsek. Kontrolu provádí vedoucí ne všech stupních řízení a interní audity. Výrobní ředitel odpovídá za seznámení vedoucích a mistrů s řídící dokumentací pro poskytování osobních ochranných pracovních, mycích, čistících a dezinfekčních prostředků a s provozními řády pracovišť. V praxi to bohužel nefunguje a bylo by vhodné provést audit na seznámení zaměstnanci s dokumentací. Pracovní podmínky pro zaměstnance, jako je pracovní doba, směny, pauzy a podobně, jsou uvedeny v pracovním řádu. Tento řád ale nebyl již dva roky aktualizován a je nefunkční. Ve firmě jsou vypracovány evakuační plány, požární a poplachové směrnice, pracovní, bezpečnostní, ekologický, organizační řád a bezpečnostní pokyny.

RIZIKO	OOPP	OBLAST
Poranění hlavy	Ochranná přilba	Práce na úseku výroby
Tržné, řezné, bodné rány na rukou	Ochranné rukavice	Veškeré pracovní činnosti spojené s uvedeným rizikem
Poranění očí	Ochranné brýle	Brusičské práce, manipulace s CHLP
Popáleniny, poranění kůže a očí	Svářečské kukly, oděvy a obuv	Svařovací práce
Rozdrcení prstů na nohou	Pracovní obuv s kovovou špičkou	Manipulace na živých částech zařízení
Poranění el. proudem	Elektrostatický oblek	Manipulace na živých částech zařízení
Nadýchání výparů	Respirátor s filtrací	Práce s CHLP, lakování

Tab. 2 Přehled používaných OOPP v organizaci A

V této firmě je velkým problémem nedodržování bezpečnostních opatření na úsecích výroby. Jde o používání ochranných osobních pracovních prostředků. Na teoretické úrovni je veškerá tato problematika zpracována dobře, praxe ale vypadá opačně. Někteří zaměstnanci odmítají používat OOPP. Porušují tak firemní směrnice, ale hlavně hazardují se svým zdravím. Bohužel zde není zpracován systém postihů v případě nedodržování směrnic a panuje zde velká benevolence od vedoucích pracovníků, které zodpovídají za jejich dodržování.

3.1.5 Požární ochrana

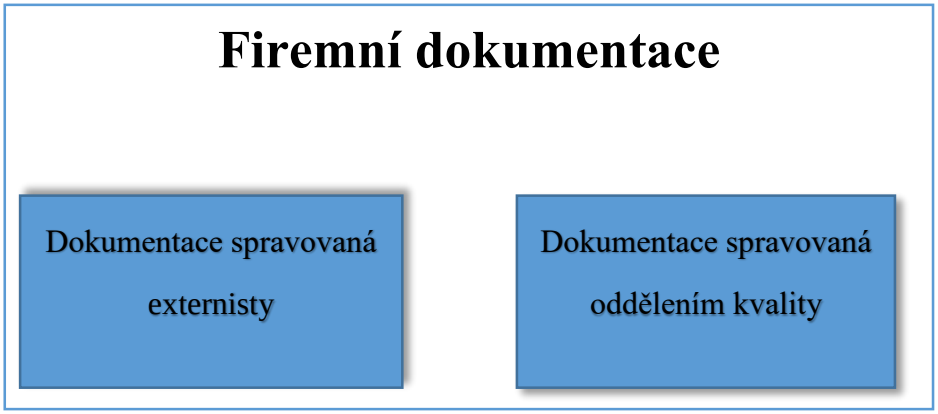
Požární ochrana je ve firmě zajištěna podle platné legislativy, kterou je:

- zákon č. 133/1985 Sb., o požární ochraně,
- vyhláška č. 246/2001 Sb., o požární prevenci,
- vyhláška č. 247/2001 Sb., o organizaci a činnosti jednotek požární ochrany.

Zákon č.133/1985Sb. o požární ochraně má za sebou spoustu novelizací. Je to stěžejní dokument, podle kterého se vůbec řídí celý výkon státního požárního dozoru. Vyhláška o požární prevenci stanovuje především požadavky na rozsah a obsah dokumentace požární ochrany, což jsou požární řády, knihy, požární bezpečnostní řešení apod. Mimo jiné stanovuje statut osoby odborně způsobilé v oblasti požární ochrany. Důležitou je také vyhláška č.23/2008Sb., o technických podmínkách požární bezpečnosti staveb která je novelizována vyhláškou č. 268/2011Sb. Vyhláška č. 247/2001 Sb., o organizaci a činnosti jednotek požární ochrany byla novelizována vyhláškou č.226/2005Sb. Každý pracovní úsek firmy má vyhotoven svůj požární řád. Aktualizace požárních řádů proběhla v roce 2014. Firma má také vypracované pokyny pro činnost preventivní požární hlídky pro každé pracoviště, plán požárních kontrol a začlenění provozovaných činností do kategorií podle požárního nebezpečí. Požární ochranu zde zaštiťuje externista. Pro jednotlivé úseky jsou vytvořeny orientační plány, které obsahují schéma a v něm označená místa uložení hasicích přístrojů, hydrantů, chemických látek, odpadů, únikových cest a lékárniček pro poskytnutí první pomoci. U této oblasti zajištění bezpečnosti nebyly shledány žádné nedostatky. Zde by bylo doporučením pouze prověření znalostí vedoucích pracovníků z jednotlivých úseků firmy o požární ochraně.

3.2 Specifikace dokumentů – organizace A

V organizaci není zpracována bezpečnostní strategie. Jsou zde zpracovány pouze dílčí korky pro zajištění bezpečnosti. Firma například prošla certifikací OHSAS 18001, která stanovuje požadavky bezpečnosti a ochrany zdraví při práci. Tato norma umožňuje organizaci, aby odpovědně řídila rizika a zlepšovala bezpečnost a ochranu zdraví svých zaměstnanců. Na základě této certifikace probíhá jedenkrát ročně dohledový audit a jedenkrát za tři roky recertifikační audit. Ve firmě bezpečnostní politiku zajišťuje správní úsek a externí firma. Zodpovědnost za bezpečnostní politiku firmy nese správní úsek, ten ji řídí a externisté ji pouze spravují. Dokumentace firmy se dělí na dvě skupiny.



Obr. 6 Struktura firemní dokumentace organizace A

Aktualizace firemních dokumentů probíhá buď na základě požadavku firmy, nebo z iniciativy samotného externisty. Externista zpravidla sám poukazuje na aktualizace v případě legislativních změn vázajících se k zajištění bezpečnosti. Proces probíhá tak, že externista předá požadavek na aktualizaci ke schválení na úsek správy. Tam začne připomínkové řízení, kde se rozhoduje, který zaměstnanec bude mít odpovědnost za danou aktualizaci. Oddělení kvality zajišťuje uložení dokumentů v elektronické podobě a také to, aby byly fyzicky uloženy a vyvěšeny na jednotlivých pracovištích, kterých se to týká.

3.3 Analýza dokumentů

DOKUMENTACE

ZÁVAZNÉ ŘÍDICÍ AKTY	ZÁZNAMY DOKUMENTACE NA PRACOVIŠTÍCH
Kolektivní smlouva, metodické pokyny, organizační směrnice, pracovní instrukce, řády	OOPP a hodnocení rizik, havarijní připravenost, evakuační plány, hodnocení ekologické újmy, kategorizace práce, požární ochrana, registr rizik, pracovní úrazy, energie, odpady

Obr. 7 Dělení dokumentace organizace A

Z obrázku je patrné, jak organizace řídí a spravuje svoji dokumentaci. Seznámení zaměstnanců s dokumentací, spadající do závazných řídích aktů, provádí samotná pracoviště, odbory a divize. Pro dokumenty spadající do druhé skupiny platí, že je do firmy implementuje externista. Ten při tvorbě těchto dokumentů a jejich aktualizací vychází z procedurálně schválených formulářů. Tato dokumentace není podřízena oficiální schvalovací proceduře a vychází z požadavků legislativy.

3.3.1 Bezpečnostní řády

Bezpečnostní řád obsahuje pracovní a bezpečnostní řád firmy, který vznikl v roce 2009 a od té doby nebyl aktualizován. Účelem pracovního a bezpečnostního řádu je zabezpečení správného provozu, pracovních postupů a bezpečnosti práce na oddělení, pro které byl vyhotoven. Za proškolení zaměstnanců a dodržování této směrnice zodpovídá mistr pracoviště. Kontrolu dodržování této směrnice provádí vedoucí výrobního úseku.

3.3.2 Havarijní plán

Podle § 39 zákona č. 254/2001 Sb., o vodách a o změně některých zákonů, vodní zákon, mají uživatelé závadných látek povinnost vypracovat plán opatření pro případy havárie, tedy havarijní plán. Havarijní plán slouží k prevenci úniku závadných látek do vod a současně připravuje uživatele těchto látek na případ havárie. Závadné látky vodní zákon definuje v ustanovení § 39 odst. 1 jako látky, které mohou ohrozit jakost povrchových nebo podzemních vod, nepatří však mezi ně odpadní a důlní vody. Nakládání s těmito látkami a náležitosti havarijního plánu jsou definovány ve vyhlášce č. 450/2005 Sb., o náležitostech nakládání se závadnými látkami a náležitostech havarijního plánu, způsobu a rozsahu hlášení havárií, jejich zneškodňování a odstraňování jejich škodlivých následků, v platném znění. Havarijní plán obsahuje tyto části:

- identifikaci objektu a vymezení území,
- seznam závadných látek, jejich vlastnosti a užívané množství,
- seznam zařízení, popis kanalizace až po výpust do veřejné kanalizace,
- cesta havarijního odtoku a preventivní opatření – signalizace,
- preventivní opatření, stavební, technologické, konstrukční včetně jejich parametrů,
- popis organizačních preventivních opatření a technických prostředků včetně situace uložení těchto prostředků,

- postup při vzniku havárie,
- zásady ochrany a bezpečnosti práce při havárii,
- personální zajištění,
- kontakty na správní orgány,
- postup předávání hlášení o vzniklé havárií,
- plán školení, výcviku a aktualizace,
- údaje o umístění kopií havarijního plánu,
- vedení záznamu,
- odpovědné osoby.

Tento dokument je ve firmě platný od roku 2013 a dosud nebyl aktualizován. Přílohami tohoto dokumentu jsou bezpečnostní listy, plán kanalizace, rozmístění prostředků na likvidaci havárie, formulář – záznam o havárii, fotodokumentace a dokumentace polohy firmy. Údaje, uvedené ve schváleném havarijním plánu, by se měly aktualizovat do jednoho měsíce po každé změně, která může ovlivnit účinnost a použitelnost havarijního plánu. Havarijní plán této organizace obsahuje veškeré nutné informace a přílohy, uvedené ve vyhlášce zmíněné výše.

3.3.3 Organizační řád

Organizační řád byl vyhotoven v roce 2007 a jeho poslední aktualizace proběhla v roce 2012. Účelem Organizačního řádu je stanovit organizační uspořádání společnosti a určit základní odpovědnosti a pravomoci jednotlivých organizačních útvarů. Organizační řád je základním organizačním dokumentem společnosti, který schvaluje představenstvo společnosti. Je výchozím dokumentem pro tvorbu nižší organizačně řídící dokumentace. Za zpracování organizačního řádu a jeho případné změny je zodpovědný představitel vedení pro jakost. Za promítnutí změn provedených v organizačním řádu do ostatní řídící dokumentace jsou odpovědni zpracovatelé řídící dokumentace.

3.3.4 Požární řády

Pro každé oddělení firmy je zvlášť vypracován požární řád. Každý z těchto dokumentů obsahuje stručný popis vykonávané činnosti a charakteristiky požárního nebezpečí provozované činnosti, dále požárně technické charakteristiky hořlavých látek, nejvýše přípustné množství látek, které se mohou v daném prostoru vyskytovat a stanovení podmínek bezpečnosti k zamezení vzniku a šíření požáru nebo výbuchu s následným požárem. Obsahují také

vymezení oprávnění a povinnosti osob při zajišťování stanovených podmínek požární bezpečnosti, a to pro zahájení, průběh, přerušení a ukončení činnosti. Upravují podmínky pro bezpečný pobyt a pohyb osob a způsob zabezpečení volných únikových cest. V každém z těchto řádů je také vyznačena odpovědná osoba. Dále jsou v něm uvedeny informace o umístění výstražných a bezpečnostních značek, o požární technice a věcných prostředcích a zařízeních požární ochrany.

3.3.5 Pracovní řád

Pracovní řád byl vyhotoven v prosinci roku 2015, je přílohou kolektivní smlouvy a jeho účelem je informovat zaměstnance o právech a povinnostech vyplývajících z pracovního poměru. Za obsah, zpracování a aktualizaci tohoto řádu je odpovědný personální ředitel. Za uplatnění práv a povinností, vyplývajících z pracovního řádu, odpovídají vedoucí zaměstnanci na všech úrovních řízení. V řádu je dále vymezena pracovní doba a pracovní režim a jejich evidence. Jsou zde také popsány bezpečnostní přestávky, nebo práva a povinnosti zaměstnanců i zaměstnavatele při vzniku pracovních úrazů nebo při odpovědnosti za způsobenou škodu. Pracovní řád také obsahuje informace o tom, že zaměstnavatel i zaměstnanci jsou povinni řídit se v zájmu BOZP platnými ustanoveními zákoníku práce. Přílohou tohoto dokumentu je Žádost o změnu pracovní doby.

3.3.6 Provozní řád

Provozní řád je dokument, který je součástí provozní dokumentace. Popisuje souhrn určitých pravidel, která stanovují způsoby, jakými bychom se měli chovat k objektu/zařízení a jak jej správně užívat. Tento souhrn a jeho hlavní obsah stanovuje osnova, která určuje několik základních aspektů, které by měl provozní řád obsahovat, např. mechanickou odolnost a stabilitu, požární bezpečnost, úsporu energií a další. Dále se obsah provozního řádu liší podle toho, zda se jedná o provozní řád objektu, zařízení či provozu. A vzhledem k tomu, že každý z těchto provozních řádů má svá specifika a celkově je tvorba provozního řádu multidisciplinární záležitostí, je důležité, aby osoba či osoby, které tyto řády tvoří, měly znalosti z oborů nejen technických, ale taky ekonomických, zároveň ale musí mít přístup k informacím k danému problému. Provozní řád by měl zajišťovat plynulý a bezpečný provoz a měl by regulovat všechny předvídatelné provozní situace. Tato společnost disponuje celkem třiceti bezpečnostními řády. Každé pracoviště musí mít vyhotovený vlastní provozní řád.

3.3.7 Řád sítě

Řád sítě vznikl v roce 2008 a prošel několika změnami, z nichž poslední proběhla v červnu roku 2012. Účelem dokumentu je definování a popis systému řízení sítě včetně jejich prvků. V tomto řádu je popsána infrastruktura sítě firmy, která je tvořena osobními počítači, terminály, notebooky, servery, aktivní prvky a datovými rozvody. Terminál je zařízení, které slouží k připojení k terminálovému serveru. Terminálem jsou vybaveni uživatelé, kteří nepotřebují k výkonu své funkce žádný speciální software. K zajištění chodu sítě jsou použity terminálové, aplikační, databázové, poštovní, webové a datové servery. Aktivní prvky slouží k propojení všech lokálních sítí k serverům a internetu, k rozbočení uzlových bodů na více přípojných bodů sítě a k nastavení primárního zabezpečení. Rozvody slouží k propojení uzlových bodů sítě. Pro rozvody po budovách jsou použity kabely minimálně třídy 5e a vyšší, rozvody mezi budovami jsou provedeny optickým kabelem. Použití kabelových žlabů k jiným účelům než k datovým vedením je závislé na schválení správce sítě. Řád sítě obsahuje také informace o garantované provozní době sítě, o typech serverů a jejich využití, zabezpečení domény a typy Hardware. Je zde také popsáno zajišťování servisů serverů, aktivních prvků sítě a prevence a kontroly. Proškolení uživatelů pro aplikace potřebné k výkonu jejich funkce zajišťují jednotliví vedoucí prostřednictvím personálního úseku. V pravidlech užívání výpočetní techniky ve firmě jsou popsány pravidla pro užívání sdílených složek, čerpání dat, elektronická komunikace, zálohování a užívání internetu.

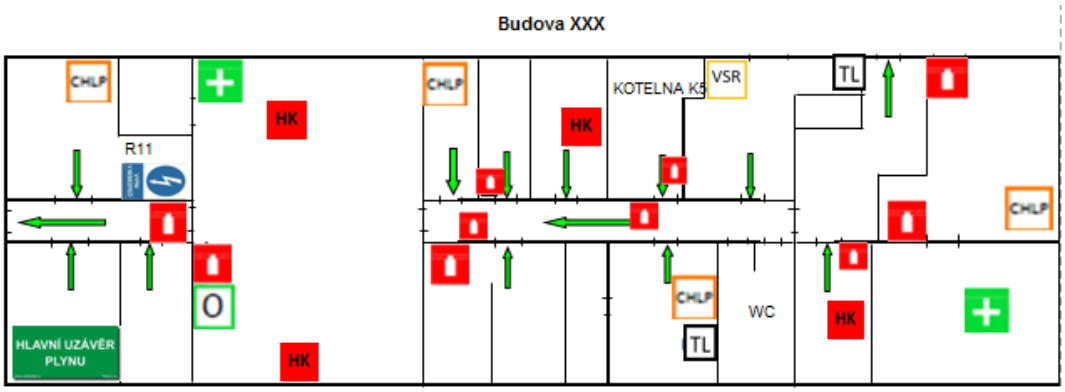
3.3.8 Evakuační plány

V případě vzniku mimořádné události (požár, povodeň, porucha technologického zařízení, atd.) nebo jiné nebezpečné situace v objektu, je evakuace jedním z účinných nástrojů řešení této situace. Povinnost mít evakuační plány vyplývá především ze zákona č. 133/1985 Sb., o požární ochraně a dále dle zákona č. 262/2006 Sb., zákoník práce. Plán se dále musí zpracovávat, pokud tak stanoví dokumentace PO zpracovaná na základě stanovení podmínek požární bezpečnosti „Stanovení organizace zabezpečení požární ochrany“. Dokumentaci PO, tedy i evakuační plány, smí zpracovávat pouze technik PO nebo odborně způsobilá osoba v PO. Požární evakuační plán se skládá z textové a grafické části. Textová část obsahuje:

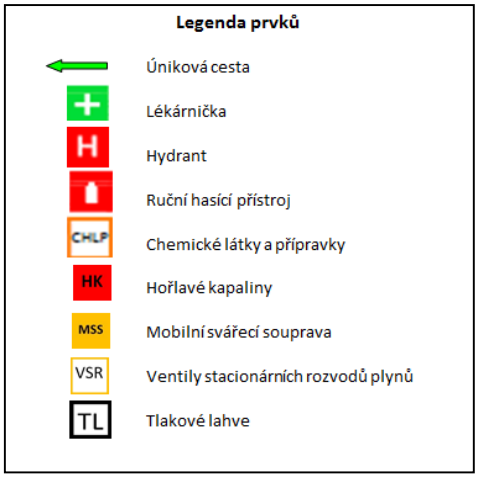
- osobu, která bude evakuaci organizovat,
- místo, ze kterého bude evakuace řízena,
- osoby a prostředky, s jejichž pomocí bude evakuace řízena,

- cesty a způsob evakuace,
- místa, kde se evakuované osoby, popřípadě zvířata budou soustřeďovat,
- určení zaměstnance, který provede kontrolu počtu evakuovaných osob,
- způsob zajištění první pomoci postiženým osobám,
- určení místa, na kterém se bude soustřeďovat evakuovaný materiál a způsob jeho střežení.

Grafická část slouží ke znázornění směru únikových cest. Evakuační plán musí být umístěn na dobře viditelném a trvale přístupném místě. Podrobné požadavky na vzhled a obsah únikového a evakuačního plánu jsou v ČSN ISO 23601.



Obr. 8 Evakuační plán budovy XXX (interní zdroj organizace A)



Obr. 9 Legenda evakuačních plánů
(interní zdroj organizace A)

3.3.9 Shrnutí

Na základě analýzy dokumentů organizace A můžeme bezpečnostní dokumentaci ohodnotit vcelku pozitivně. Dokumenty jsou zpracovány ve všech oblastech napříč celofiremní strukturou, některé jsou ale zastaralé a potřebovaly by projít revizí a aktualizací. Pokud bychom měli zhodnotit provázanost teorie zajištění bezpečnosti s praxí, situace již není tak pozitivní. Ve firmě existuje bezpečnostní politika, ale strategie ne. Veškeré kroky k zajištění bezpečnosti jsou zatím prováděny spíše na základě nutnosti z důvodu nařízení legislativy a norem, chybí však její komplexní zajištění, není na ni pohlíženo jako na stejně důležitou oblast zájmu v rámci tvorby celofiremní strategie. Je zřejmé, že náklady na bezpečnost mohou být vysoké a zajištění bezpečnosti firmě nepřináší žádný zisk, v konečném důsledku jí ale může ušetřit velké peníze.

Jako nejzávažnější prohřešek z oblasti bezpečnosti je působení subdodavatelských firem na úseku výroby, které poskytují dílčí služby na finálním produktu. Tyto firmy jsou objednávány oddělením kooperací na základě požadavku úseku výroby. Neexistuje systém evidence, kontroly a proškolování těchto externích firem. Často jde i o zahraniční subdodavatele, jejichž zaměstnanci nemluví česky. V některých případech se dokonce externisté nacházeli v objektu, vykonávali své práce, aniž by o nich někdo z firmy věděl.

V případě bezpečnostního incidentu tito pracovníci neznají postupy, jak se zachovat v případě vzniku nebezpečí, komu incident nahlásit a v některých případech díky jazykové bariéře ani nemohou oznámit, co se stalo. Postihy pro firmu v případě závažného nebezpečí mohou být v těchto případech obrovské. Další prostor pro zlepšení vidím v nedostatečné kontrole práce externisty. Externista je podřízený správnímu úseku. Zaměstnanci správního úseku nezahrnují žádného odborníka na bezpečnost, který by dokázal kontrolovat externí práce. Správní úsek je tedy absolutně závislý na práci externisty a vkládá do něj maximální důvěru. Zde bych navrhla zaměstnat bezpečnostního odborníka s praxí, který by kontroloval jeho činnost ve firmě.

Ve firmě je velkým problémem nedodržování bezpečnostních opatření na úsecích výroby ve smyslu používání ochranných osobních pracovních prostředků. Zaměstnanci působící ve firmě delší období dříve nebyli zvyklí používat tyto prostředky, dnes se to od nich vyžaduje a jejich přístup je spíše odmítavý. Neuvědomují si důsledky svého chování.

Obr. 10 Správná a špatná praxe použití OOPP (interní zdroj organizace A)

Fotka z výroby vlevo ukazuje, jak vypadá správná praxe za použití OOPP, na pravé fotce je zachycen pracovník firmy A bez veškerých prvků ochrany. Zde bych doporučila nastavit systém postihů za nedodržení nastavených pravidel. Nešvarem této firmy je absence systému podávání stěžejních informací zainteresovaným osobám. Pokud se informace o rozhodnutích vedení, které mají dopad na změny v bezpečnosti firmy, nedostanou k osobám zodpovědným za bezpečnost organizace, nikdy nemůže být tento systém fungující a aktuální. Také není zajištěna informační bezpečnost v rámci klasifikace firemní dokumentace.

3.4 Organizace B

Tato firma působí ve stejném oboru již 22 let a také patří ke špičkám ve zmiňovaném odvětví. Pro tuto společnost v současné době pracuje kolem 150 zaměstnanců, spadá tedy do kategorie středních podniků.

Obr. 11 Sídlo a výrobní hala organizace B (interní fotodokumentace organizace A

Stejně jako u analýzy předchozí organizace, i zde bude postup obdobný. Nejprve proběhne zhodnocení bezpečnostní situace podle rozdělení na fyzickou, personální, informační bezpečnost, bezpečnost a ochranu zdraví při práci a požární ochranu. Poté bude zhodnocena bezpečnostní dokumentace firmy. Shrnutí bude obsahovat zjištěné nedostatky.

3.4.1 Fyzická bezpečnost

Za kontrolu oprávněnosti vstupu osob a evidenci návštěv pro výrobní úsek v této organizaci zodpovídá zaměstnanec vrátnice. Co se týče administrativní budovy, zde odpovídá za své návštěvy osobně každý vedoucí sám. Zamezení vniknutí neoprávněných osob do objektu je řešeno oplocením objektu a uzamykatelnou bránou a vrátnicí. Objekt je zabezpečen pomocí kamerového systému. Za poskytnutí základních informací návštěvám je zodpovědná asistentka společnosti. Každý vedoucí zodpovídá za funkční obsluhu telefonu a faxu na svém pracovišti. Ostraha zajištěná externí firmou zodpovídá za:

- kontrolu oprávněnosti vjezdu vozidel,
- kontrolu nákladu podle dokladu na vozidlech,
- vedení režimu vydávání klíčů,
- pochůzkovou činnost,
- kontrolu vynášení předmětů,
- kontrolu firemních aut.

Budovy jsou opatřeny kódováním, externí firma provádí dálkový monitoring a provádí výjezdy. Vyhodnocování poplachu z poplachových systémů probíhá přes externí firmu. V případě vzniku závažné události na objektu volá externí firma jednatelům společnosti. Informování o závažných událostech na objektu jsou povinni zaměstnanci nebo externisté hlásit vedení firmy v případě jejich přítomnosti osobně nebo telefonicky. V této firmě se jeví zajištění fyzické bezpečnosti, jako fungující, nicméně by bylo dobré provést kontrolu vrátnice nezávislou osobou, zda opravdu dodržuje stanovené postupy. Mohlo by se stát, že zaměstnanec vrátnice se dohodne například se zaměstnancem výrobního úseku, který spáchá krádež, že jej pustí přes vrátnici s ukradeným předmětem a po zpeněžení takového předmětu se společně rozdělí.

3.4.2 Personální bezpečnost

Personální bezpečnost je zajištěna ve smyslu snížení rizika lidského faktoru, tedy rizika chyby, krádeže, podvodu nebo nesprávného užití či zneužití informací a informačního systému. Přístupy k informacím a strategickým a dalším dokumentům jsou ošetřeny podle toho, jak je zaměstnanci potřebují k výkonu své pracovní činnosti. Ve firmě je používán databázový informační systém SAP, přístup by měl být povolen pouze k práci s daty, která jsou nezbytná pro práci jednotlivých lidí. Za tuto skutečnost se ale odpovědná osoba nechce zaručit. Bylo by vhodné provést kontrolu oprávnění zaměstnanců pro přístup k důležitým datům.

3.4.3 Informační bezpečnost

Ochrana počítačových sítí, kabelových i bezdrátových propojení nebo ochrana před vnějšími i vnitřními útoky probíhá na vstupu přes Firewall a doménovou síť. Problematika datových přenosů je řešena vnitřní doménovou zabezpečenou sítí. Databáze klientů firmy jsou zabezpečeny heslem, přístupová práva mají vedoucí pracovníci. Databáze formulářů dodávaných v rámci produktů jsou taktéž zabezpečeny heslem, které znají pouze pověření zaměstnanci. Systém pro správu námětů a připomínek ve firmě neexistuje. Firemní účetnictví je zabezpečeno heslem a samostatným serverem se samostatným přístupem. Pracovní stanice jednotlivých uživatelů jsou chráněny přístupovým heslem. Ve firmě funguje rozhraní Wi–Fi sítě. Firemní informace nejsou nijak klasifikovány z hlediska bezpečnosti, to znamená podle jejich hodnoty, právní citlivosti, podle jejich citlivosti nebo podle jejich kritičnosti. Bylo by vhodné klasifikaci dat nastavit. Jak je patrné ze zjištěných informací uvedených výše, jediným autentizačním mechanismem v organizaci je kombinace uživatelského jména a hesla. Autentizace je kritickým místem bezpečnosti počítačových systémů a dat, které tyto systémy obsahují. Největší nebezpečí může způsobit únik citlivých firemních dat, kterými jsou střednědobá a dlouhodobá strategie firmy, databáze klientů a dodavatelů, informace o pojištění, bankovních účtech a podobně. Za standard v zabezpečení přístupu k datům a systémům je považována dvou faktorová autentizace (2FA). Před jejím zavedením se provádí analýza rizik. Ztráta nebo krádež stěžejních informací může v konečném důsledku znamenat i konec podnikání. Zaměstnancům se do telefonu nainstaluje aplikace chráněná PIN kódem. Pro přístup pak budou uživatelé vyzváni k zadání jména, hesla a jednorázového hesla, které se po zadání PIN kódu zobrazí v telefonu. Teprve po této autentizaci budou mít přístup k datům, firemním údajům, případně citlivým informacím.[16]

3.4.4 BOZP

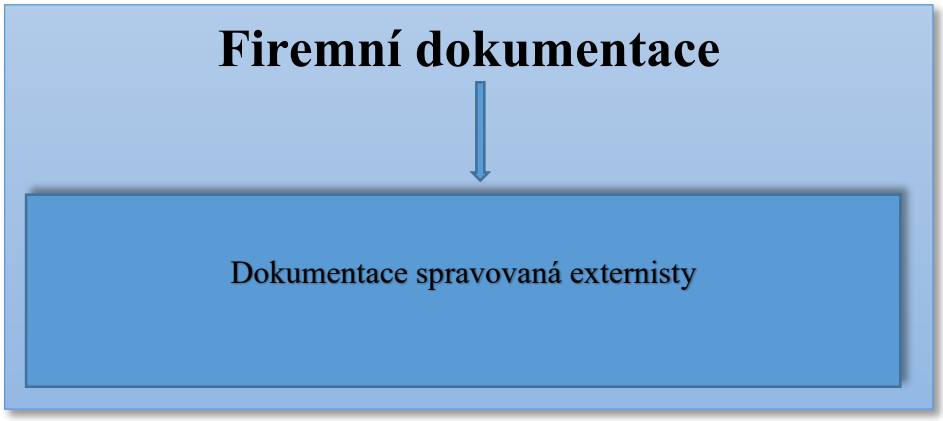
Zodpovědnou osobou za zajištění bezpečnosti a ochrany zdraví při práci je pracovník externí firmy a určený pracovník společnosti. Školení zaměstnanců na veškeré dokumenty spojené s BOZP probíhá jedenkrát ročně a provádí ho pracovník externí firmy. Školí se všichni zaměstnanci, tedy vedení společnosti, dělníci i externí pracovníci, kteří pracují ve výrobních halách. Kontrola proškolení zaměstnanců na BOZP probíhá dle prezenční listiny. Úprava dokumentů v návaznosti na změny zákonů, norem popř. situace ve firmě se děje dle aktuálních změn a po kontrolách dle navržených opatření. Za služby externisty za zajištění BOZP tato firma platí 10 000,- Kč měsíčně. Nákup osobních ochranných pracovních pomůcek zajišťuje nákupní oddělení. Zaměstnancům jsou přidělovány dle směrnice a smluvně. Kontrolu jejich používání na dílnách provádí vedoucí dílen, pracovník společnosti společně s externím pracovníkem. Pracovní podmínky zaměstnanců, jako je pracovní doba, směny, pracovní přestávky a podobně jsou nastaveny v souladu se zákoníkem práce. Dodržování bezpečnosti a ochrany zdraví při práci je v organizaci B fungujícím procesem. Zde nebyly shledány žádné nedostatky.

3.4.5 Požární ochrana

Každé oddělení firmy musí mít svůj požární řád. Firma má také vypracované pokyny pro činnost preventivní požární hlídky pro každé pracoviště, plán požárních kontrol a začlenění provozovaných činností do kategorií podle požárního nebezpečí. Požární ochranu zaštiťuje externista dle platné legislativy, která je blíže popsána v odstavci požární ochrany firmy A.

3.5 Specifikace dokumentů organizace B

Stejně jako předešlá firma, i tato prošla certifikací OHSAS 18001, která stanovuje požadavky bezpečnosti a ochrany zdraví při práci. Ve firmě bezpečnostní politiku řídí pouze externí firma, která spolupracuje se všemi odděleními napříč firmou. Na každém oddělení je pověřená osoba, zodpovědná za podání veškerých potřebných podkladů a informací externistovi a za implementaci bezpečnostních opatření na svém oddělení.



Obr. 12 Struktura firemní dokumentace organizace B

Aktualizace firemních dokumentů probíhá stejně jako v organizaci A na základě požadavku firmy, nebo z iniciativy samotného externisty. Proces probíhá tak, že externista tvoří dokumenty v úzké spolupráci s odpovědnou osobou za daný úsek. Externista poučí pověřenou osobu o náležitostech uložení dokumentů ve fyzické i elektronické podobě a o poučení zaměstnanců. Za splnění těchto požadavků nese zodpovědnost pověřená osoba.

3.6 Analýza dokumentů organizace B

Firma B disponuje menším počtem zaměstnanců a struktura bezpečnostní politiky se oproti organizaci A výrazně liší. Organizace B zajišťuje svoji bezpečnost výhradně přes externí firmu. Zaměstnanec externí firmy je přímo podřízený řediteli firmy. Stejně jako organizace A, i tato firma prošla certifikací OHSAS 18001. Dokumenty spojené se zajištěním bezpečnosti a ochrany zdraví při práci tedy upravuje podle ní.

3.6.1 Organizační směrnice

Účelem této směrnice je stanovit zásady pro zaměstnance pro dodržování bezpečnosti při práci, dále je obsahem postup při řešení pracovních úrazů, pravidla poskytování ochranných pracovních prostředků a pro zabezpečení požární ochrany. Směrnice byla vydána v roce 2010 a od této doby nebyla aktualizována. Organizační řád obsahuje matici odpovědnosti pro bezpečnost práce a zajištění požární ochrany.

Číslo	Název činnosti	1	2	3	4	5	6
1	**Dodržování bezpečnosti práce**		S		Z	S	
2	**Dodržování požární ochrany (požárního řádu)**		S	Z	S		
2	**Hlášení pracovních úrazů**		Z			Z	
3	**Odškodnění pracovních úrazů**	Z					
4	**Požární ochrana při svařování**			S	S		
5	**Uzavření smluv pro kontrolu hydrantů**			S			Z
6	**Školení o požární ochraně**			Z			
7	**Školení z bezpečnosti práce**		Z				

Tab. 3 Matice odpovědnosti pro BOZP a PO (interní zdroj organizace B)

Obsah:

- 1 – ředitel
- 2 – bezpečnostní technik
- 3 – požární preventista
- 4 – mistr
- 5 – technolog svařování
- 6 – ekonom

Symboly:

- Z – zodpovídá
- S – spolupracuje

3.6.2 Bezpečnost a ochrana zdraví při práci

Pro bezpečnost a ochranu zdraví při práci existuje v této organizaci dokument, označený jako metodický pokyn pro výchovu a vzdělávání v oblasti BOZP. Byl vyhotoven 2. 1. 2013 a prozatím nebyla provedena žádná jeho aktualizace. V tomto dokumentu jsou uvedeny informace o vstupním školení, kdo je povinen být proškolen a kdo zodpovídá za proškolení

právě přijatých zaměstnanců do pracovního poměru. Dalším bodem je popis průběhu a odpovědností v rámci periodického, mimořádného, odborného a speciálního profesního školení.

3.6.3 Osobní ochranné pracovní prostředky

Tento vnitřní předpis stanovuje rozsah a bližší podmínky poskytování osobních ochranných pracovních prostředků. Tento dokument obsahuje náležitosti uvedené v zákoně č. 495/2001 Sb. zákoník práce. Pro evidenci výdeje těchto prostředků slouží dokument „Záznam o přidělení OOPP“. V dokumentu jsou uvedeny odpovědnosti a pravomoci. Přílohou je seznam OOPP pro jednotlivé profese, seznam poskytovaných mycích, čistících a desinfekčních prostředků pro jednotlivé profese ve společnosti, dále tabulka pro vyhodnocení rizik pro výběr a použití OOPP a záznam o přidělení OOPP. Osobní ochranné prostředky musí chránit zaměstnance před riziky, nesmí ohrožovat jejich zdraví, nesmí bránit při výkonu práce a musí splňovat požadavky stanovené prováděcím předpisem.

3.7 Shrnutí

V této firmě se jeví bezpečnostní politika lépe fungující, než v organizaci A. Je to také tím, že v menší firmě jsou nedostatky v rámci zajištění bezpečnosti lépe viditelné a odhalitelné. Vyšší forma zabezpečení vyplývá také z důraznějších kontrol a častých návštěv majitele firmy. Pokud ten shledá nějaký nedostatek, například ve formě nedodržení bezpečnostních pokynů, absence pracovních pomůcek a podobně, vyžaduje okamžité řešení situace, dohledání odpovědných osob, určení postihů a vyžádá si nápravné řešení, aby se situace neopakovala. Co se týče fyzické bezpečnosti, by bylo vhodné nastavit systém kontrol zaměstnance vrátnice, zda opravdu dodržuje nastavené postupy. Fungování fyzické bezpečnosti se jeví bez větších nedostatků, nicméně žádný systém pravidelných či namátkových kontrol, provedených nezávislou osobou, není v této oblasti nastaven. V případě personální bezpečnosti by bylo vhodné provést kontrolu přístupů zaměstnanců a oddělení k důležitým a strategickým informacím. Přístupy by sice měly být omezené podle potřeby informací k vykonávání pracovní činnosti zaměstnanců, zodpovědná osoba se ale za toto odmítá zaručit a sama navrhuje provést kontrolu. Jak je též patrné ze zjištěných informací uvedených výše, vztahujících se k informační bezpečnosti, jediným autentizačním mechanismem je kombinace uživatelského jména a hesla. To je však metoda, na niž by se firma rozhodně neměla spoléhat. Autentizace je kritickým místem bezpečnosti počítačových systémů a dat, které tyto systémy

obsahují. Za standard v zabezpečení přístupu k datům a systémům je považována dvou faktorová autentizace (2FA). Před jejím zavedením je nutné provést precizní analýzu rizik, před nimiž má tento způsob zabezpečení firmu chránit. Analýza rizik zahrnuje kvalifikace dat v závislosti na riziku, kterému by firma musela čelit v případě jejich ztráty. Ztráta informací, které jsou součástí například interních firemních plánů a procesů, může pro společnost znamenat konkurenční nevýhodu, případně nutnost vynaložení nákladů spojených s jejich opětovným vypracováním. Největší nebezpečí může způsobit únik citlivých firemních dat, kterými jsou střednědobá a dlouhodobá strategie firmy, databáze klientů a dodavatelů, informace o pojištění, bankovních účtech nebo účetnictví firmy. Ztráta nebo krádež tohoto typu informací může v konečném důsledku znamenat i konec podnikání. Může být také narušena důvěra zákazníků, kteří budou zvažovat spolupráci s někým, kdo nedokáže ochránit například jejich osobní údaje. Aktuální trend Bring your own device (BYOD), je jedním z nejčastějších důvodů, proč čím dál více firem sahá v rámci bezpečnostních opatření po dvou faktorové autentizaci. Umožňuje při práci využívat soukromá přenosná zařízení zaměstnanců. Tento trend podle průzkumu z roku 2012 využívalo v USA 80 % firem. To s sebou přináší i bezpečnostní problémy, kdy firmy prakticky nemohou kontrolovat, kdo má přístup k jejich interním datům. 2FA dokáže spolehlivě zajistit, že se k firemním aplikacím a citlivým datům dostanou pouze pověřené osoby. Jedním z uživatelsky přijatelných a finančně nenáročných řešení, je autentizace prostřednictvím jednorázových hesel zasílaných na mobilní telefon. Zaměstnancům se do telefonu nainstaluje aplikace chráněná PIN kódem. Pro přístup pak budou uživatelé vyzváni k zadání jména, hesla a jednorázového hesla, které se po zadání PIN kódu zobrazí v telefonu. Teprve po této autentizaci budou mít přístup k datům, firemním údajům, případně citlivým informacím. [14]

Organizace v oblasti zajištění bezpečnosti maximálně využívá služeb externisty, který také zodpovídá za její nastavení v této firmě. Přitom u organizace A bylo zjištěno, že odpovědnost je na správním úseku. Nicméně i v této společnosti je otázka bezpečnosti řešena bezpečnostní politikou. Neexistuje zde strategie vývoje zajištění bezpečnosti organizace, tedy bezpečnostní strategie.

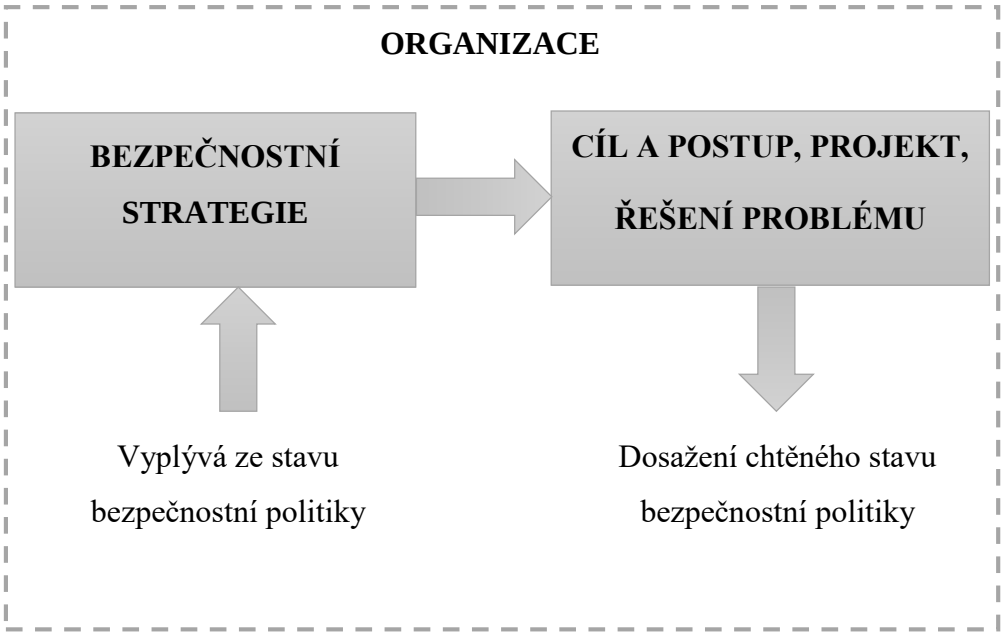
4 NÁVRH BEZPEČNOSTNÍ STRATEGIE ORGANIZACE

Systém řízení bezpečnosti je neodmyslitelnou součástí systému řízení organizace. Představuje zejména plnění funkcí na manažerské úrovni. Na začátku tvorby takového systému se stanoví bezpečnostní požadavky, jejichž nejobecnější formou jsou správně stanovené bezpečnostní cíle. Ty vycházejí z obchodních cílů organizace, legislativy, smluv, ale také z interních požadavků. Pokud jsou jasné cíle, je třeba určit strategii ukazující principy a rámcové postupy pro jejich dosažení. Je výhodné vytvářet bezpečnostní politiky jako více provázaných hierarchických dokumentů, které na své úrovni řeší vždy příslušné oblasti bezpečnosti.

4.1 Účel bezpečnostní strategie

Účelem bezpečnostní strategie je zajištění ochrany veškerého hmotného i nehmotného majetku firmy na požadované úrovni, ochrana jejího dobrého jména a předmětu činnosti organizace. Dokument musí obsahovat veškeré aspekty a kroky při zabezpečení ochrany organizace, počínaje ochranou budov přes definování jednotlivých skupin zaměstnanců, zálohování dat nebo požární ochrany. Obsah schvaluje vedení organizace a její schválená podoba je závazná pro všechny její zaměstnance. Prostřednictvím smluv s třetími stranami se pak mohou jednotlivé požadavky přenášet i na smluvní partnery organizace a jejich zaměstnance. Je třeba dbát na to, aby se na všechny složky řešení bezpečnosti kladl stejný důraz a vzniklo tak vyvážené a celistvé řešení. Tvorba kvalitní bezpečnostní strategie a navazující řešení bezpečnosti zasáhne více či méně do všech organizačních struktur, projeví se ve většině stávajících psaných i nepsaných norem organizace. Zavedení a udržení požadované míry úrovně bezpečnosti vyžaduje pravidelné školení mezi zaměstnanci na všech úrovních. Nutné je mít plnou podporu ze strany vedení organizace. Kvalitní bezpečnostní strategii je možné vyhotovit pouze po provedení kvalitní analýzy rizik. Ta by měla předcházet jakýmkoliv finančním investicím do bezpečnosti. Jen tak bude zaručeno jejich maximálně efektivní využití. Analýza rizik poskytne odpovědnému týmu odpovědi na otázky, co chránit, proti čemu a jakým způsobem. Nedostatečně či špatně provedená analýza rizik může mít pro organizaci fatální následky.

4.2 Struktura bezpečnostní strategie



Obr. 13 Struktura bezpečnostní strategie organizace

U bezpečnostní strategie jde o stanovení projektů, postupů a dílčích cílů, které zajistí naplnění strategických cílů bezpečnosti a dosažení žádoucího stavu bezpečnostní politiky. Při tvorbě bezpečnostní strategie se vychází ze stávajícího a chtěného stavu bezpečnostní politiky.

4.3 Obsah bezpečnostní strategie

Vzorová bezpečnostní strategie bude vyhotovena v následující kapitole a bude obsahovat tyto body:

- určení vazeb mezi globální a bezpečnostní strategií organizace,
- analýza dosavadního vývoje bezpečnostního systému v organizaci,
- analýza a prognóza vývoje bezpečnostních systémů organizací,
- analýza změn bezpečnostního prostředí a požadavků bezpečnostní politiky,
- plán rozvoje bezpečnostního systému v střednědobém a dlouhodobém horizontu,
- objem finančních prostředků a dalších zdrojů pro podporu bezpečnostní strategie,
- návrh standardů uplatňovaných v bezpečnostním systému firmy,
- návrh organizačních změn a měřítek k dosažení plánovaných cílů,
- zásady pro vyhodnocování účinnosti bezpečnostní strategie a bezpečnostního systému organizace.

4.4 Shrnutí

Kvalitní bezpečnostní strategie musí obsahovat zejména výhled zajištění bezpečnosti v určeném časovém horizontu, vzhledem ke strategii firmy, měnícím se hrozbám a měnícímu se stavu referenčního objektu. Bezpečnostní strategie by měla být závazná pro všechny zaměstnance a vedení organizace by na její dodržování mělo klást důraz. Důležitou stránkou fungující bezpečnostní strategie je také deklarace souladu řešení bezpečnosti s platnou legislativou a normami.

5 VZOROVÁ BEZPEČNOSTNÍ STRATEGIE

V této kapitole bude vypracována vzorová bezpečnostní strategie firmy. Při její tvorbě se bude vycházet ze strategických cílů firmy a také ze zjištěných nedostatků v rámci bezpečnostní politiky organizace A.

5.1 Určení vazeb mezi globální a bezpečnostní strategií

Pro určení vazeb mezi globální a bezpečnostní strategií musíme nejprve znát výhledy a cíle společnosti. V našem případě vycházíme především z obchodní strategie. V tuto chvíli má společnost podepsány kontrakty na dodávky svých výrobků, jejichž objem je o třetinu vyšší než nyní a trendy trhu predikují v horizontu následujících deseti let rostoucí tendenci. Pro splnění závazků vyplívajících z kontraktů je nutné v příštím roce vybudovat novou výrobní halu, což znamená zabývat se otázkami zajištění prostoru, finančních prostředků, technologií, logistiky a zásobování, zajištění personálu a nastavení koncepce zajištění bezpečnosti nejen v nové hale, ale i v celé firmě. Musí tedy proběhnout identifikace a analýza rizik. Pro provoz nové haly je potřeba znát veškeré potřeby a souvislosti, což znamená:

- zabezpečení prostoru,
- zajištění pracovní síly,
- zajištění technologického vybavení haly,
- zajištění organizace pracoviště,
- nákup, logistika a skladování.

Vzhledem k tomu, že nová výrobní hala bude součástí stávajícího areálu firmy, její zajištění, klíčový režim, kontroly zaměstnanců, návštěv, kontroly nákladů aut dle dokumentů, kontroly vjezdu a výjezdu aut, budou zpočátku zajištěny stávajícími externími zaměstnanci vrátnice. Přístup do haly budou mít pouze odpovědní pracovníci na základě identifikačního čipu. Pro novou halu bude v projektové dokumentaci zakreslen kamerový systém. Pro zabezpečení požární ochrany bude hala vybavena požárními hlásiči, automaticky hasícím systémem a hasicími přístroji. Pro všechny úseky bude vyhotoven požární řád dle platné legislativy. V hale budou vytvořeny únikové cesty a bezpečnostní koridory pro pohyb osob a materiálu, označeny na podlaze příslušným typem a barvou čáry. Výše uvedené zabezpečení prostoru zajistí správní úsek s nově vytvořeným úsekem bezpečnosti a externí firmou. Personální ředitel je zodpovědný za nábor požadovaných zaměstnanců dle požadavků výrobního úseku.

Po přijetí zaměstnanců do pracovního poměru, musí být tito proškoleni, vybaveni ochrannými osobními pracovními prostředky. Musí být seznámeni s pracovištěm, pracovními podmínkami a BOZP. Musejí být proškoleni na jednotlivé stroje a zařízení. Hala bude vybavena stroji a zařízeními dle požadavku výrobního úseku a úseku technologie. Rozmístění strojů bude odpovídat toku výrobního procesu a materiálu. Na vstupu a výstupu bude probíhat kontrola jakosti a kvality. Zajištění organizace pracoviště bude blíže specifikováno v organizačních řádech a směrnicích. Před dodáním materiálu na výrobu bude tento materiál skladován v příslušném skladu, který je součástí této haly.

5.2 Analýza dosavadního vývoje zajištění bezpečnosti (organizace A)

Dle analýzy bezpečnostní situace v organizace jsme zjistili následující nedostatky:

- chybí koncept zajištění bezpečnosti v rámci firemní strategie, existuje pouze bezpečnostní politika, nikoli strategie,
- absence systému evidence, kontroly, a proškolení zaměstnanců externích firem vykonávající svou pracovní činnost v objektu firmy,
- absence kontroly externisty, který firmě A zajišťuje bezpečnost,
- absence zajištění informační bezpečnosti,
- nedodržování bezpečnostních opatření zavedených v dokumentaci ve formě používání ochranných osobních pracovních prostředků,
- absence systému předávání informací, které mají vliv na změny v oblasti bezpečnosti, zainteresovaným osobám.

V rámci výstavby nové haly se bude řešit komplexní zajištění bezpečnosti napříč celofiremní strukturou. Bude se postupovat tak, aby došlo k vyvarování se chyb, které byly odhaleny analýzou bezpečnostní situace firmy A, která je podrobněji vypracována v kapitole 3.

5.3 Analýza a prognóza vývoje bezpečnostních systémů organizace

Zde se budeme zabývat otázkou, jak další organizace zajišťují svoji bezpečnost a jaké jsou trendy v zabezpečení. Možností, jak zabezpečit firmu na jednotlivých úsecích, je mnoho. Většina firem, stejně jako námi analyzovaná organizace A, již využívá různé formy poplachových zabezpečovacích a tísňových systémů (PZTS). Otázka ale zní, jakým způsobem.

Zřizování PZTS má svá pravidla. Mělo by se řídit základními etapami, uvedenými v ČSN CLC/TS 50131-7, kterými jsou:

- návrh systému,
- příprava realizace,
- montáž.

Výstupy ve formě dokumentů v jednotlivých etapách jsou:

- návrh skladby systému,
- plán montáže,
- dokumentace skutečného stavu. [6]

5.3.1 Etapa 1 – návrh systému

Návrh systému obsahuje stanovení rozsahu PZTS, volbu komponent a zpracování návrhu systému. Účastníky této etapy jsou objednatel, dodavatel a provozovatel. Dalšími subjekty mohou být pojišťovny, provozovatelé telekomunikačních služeb nebo Policie ČR a bezpečnostní agentury ve smyslu napojení na dohledové přijímací centrum. V procesu zřizování PZTS představuje v návrhu systému první krok v rámci první etapy bezpečnostní posouzení. Bezpečnostní posouzení je založeno na vyhodnocení čtyř základních oblastí zájmu, kterými jsou zabezpečované hodnoty, budova a vnější a vnitřní vlivy. Analýza rizika, obsahující posouzení zabezpečovaných hodnot a budovy, je zpracovávána s cílem stanovení požadovaného stupně zabezpečení v souladu s ČSN EN 50131-1 ed.2.

Druhá skupina oblastí zájmů bezpečnostního posouzení představuje posouzení ostatních vlivů. Cílem posouzení ostatních vlivů je vyhodnocení stávajících nebo budoucích podmínek uvnitř a vně střežených prostorů z hlediska následného výběru a umístění komponent. Význam bezpečnostního posouzení objektu spočívá zejména v získání a zpracování informací potřebných pro vytvoření návrhu PZTS.

Výstup je využitelný zejména v:

- stanovení rozsahu systému,
- východisko pro volbu komponentů,
- vymezení potencionálních hrozeb,
- charakteristika potencionálního narušitele,
- stanovení stupně zabezpečení,
- stanovení pojistné třídy,
- určení třídy prostředí,
- návrh řešení systému (počty, typy detektorů),
- umístění komponent v objektu,
- redukce planých poplachů.

Výstup bezpečnostního posouzení představuje Zápis o bezpečnostním posouzení, jehož struktura odpovídá výše popisovaným oblastem zájmu. Návrh skladby systému představuje výstupní dokument první etapy zřizování PZTS a obsahuje následující body:

- údaje o klientovi,
- údaje o střežených objektech,
- stupeň zabezpečení,
- třída okolního prostředí,
- seznam materiálu,
- konfigurace systému,
- hlášení poplachu.

Tento dokument slouží ve fázi nabídky k upřesnění rozpočtu dodávky a jako podklad k jednání se zákazníkem. V další fázi může být také podkladem pro tvorbu projektové dokumentace. [6]

5.3.2 Etapa 2 - Příprava realizace

Etapa příprava realizace zahrnuje zpracování projektové dokumentace PZTS. Zde je využit dokument - Návrh skladby systému z předešlé etapy, který je dále rozpracován do podoby projektové dokumentace. Ta musí odpovídat požadavkům na následnou realizaci montáže

PZTS. Příprava realizace zahrnuje ověření úplnosti a realizovatelnosti, schválení zákazníkem, zpracování změn a projekci. Nedílnou součástí je technické posouzení, které již probíhá přímo v prostorách objektu.

Obsahová náplň projektové dokumentace je následující:

- dokumentace pro ohlášení stavby,
- dokumentace pro provádění stavby,
- dokumentace pro výběr dodavatele,
- dokumentace skutečného provedení stavby. [6]

5.3.3 Etapa 3 – montáž PZTS

Etapa montáže PZTS začíná převzetím objektu a je ukončena předáním systému PZTS do trvalého provozu. Jako vstupní dokument je zde považována projektová dokumentace obsahující technickou zprávu, výkresovou část a rozpis materiálu. Výstupem je nainstalovaný systém PZTS, který prošel požadovanými zkouškami. Důležitým aspektem je také proškolení obsluhy, která musí být seznámena s jednotlivými kroky:

- jak systém provozovat,
- jak měnit a nastavovat příslušné kódy,
- jak reagovat v jednotlivých situacích,
- jak často a jakým způsobem systém testovat,
- koho a jak kontaktovat v případě technických potíží a závad,
- jak vést provozní knihu PZTS.

Za zabezpečení pravidelných revizí odpovídá vlastník PZTS. Mezi vlastníkem PZTS a kompetentní firmou musí být uzavřena servisní smlouva. [6]

5.3.4 PZTS, EZS a IPS

PZTS je možné kombinovat s elektrickými zabezpečovacími systémy (EZS). Komponenty EZS/PZTS podle standardů obsahují minimálně:

- ústřednu,
- jeden nebo víc detektorů,
- jedno nebo víc signalizačních zařízení, případně poplachových přenosných systémů,
- jedno nebo víc napájecích zařízení.

Počet použitých komponentů závisí například na rozloze budovy, požadované úrovni zabezpečení a podobně. Elektrický zabezpečovací a tísňový poplachový systém se může skládat z více podsystémů. Podsystém je umístěn v jasně definované části chráněného prostoru a je schopen samostatné činnosti. EZS i PZTS musejí mít stanovený stupeň zabezpečení, jak je definováno v ČSN EN 50131-1 ed.2, tedy:

- stupeň 1 - nízké riziko,
- stupeň 2 - nízké až střední riziko,
- stupeň 3 - střední až vysoké riziko,
- stupeň 4 - vysoké riziko.

Od stupně zabezpečení se pak dají odvodit parametry komponentů EZS a PZTS a požadavky na ně kladené. Při volbě komponentů je důležité zabývat se vhodným prostředím jejich použití, které je také definováno do čtyř tříd. U všech stupňů EZS musí také existovat čtyři stupně úrovní přístupu k jejich funkcím:

- úroveň 1 - přístup pro každou osobu,
- úroveň 2 - přístup pro uživatele systému,
- úroveň 3 - uživatelský přístup pro servisní techniky,
- úroveň 4 - přístup pro výrobce zařízení.

Jednotlivé úrovně definují konkrétní práva osoby užívající EZS a PZTS prostřednictvím uživatelského rozhraní. Nastavení stavu střežení a pohotovostního režimu musí být umožněno pouze uživatelům s příslušnou přístupovou úrovní. Uvedení do stavu střežení nebo pohotovostního režimu je podmíněné správným fungováním EZS/ PZTS při minimalizaci nesprávné činnosti.

Integrace poplachových systémů představuje moderní způsob využití současných technologických prvků zabezpečovacích, kamerových, přístupových, tísňových systémů a systémů přivolání pomoci. Uvedené aplikace je možné integrovat navzájem a tím zabezpečit efektivní aplikaci automatizačních procesů v průmyslových a jiných objektech. Mezi poplachové aplikace patří již zmíněné PZTS, systémy přivolání pomoci (SAS), elektrická požární signalizace, systémy kontroly vstupů pro použití bezpečnostních aplikacích a podobně. Ty se dají integrovat navzájem například se systémy vytápění, osvětlení, klimatizace nebo řízení ener-

getických systémů. Hlavní výhodou integrovaných systémů je zvýšení účinnosti jednotlivých poplachových systémů a zvýšení přehledu o situaci v objektu. Významnou výhodou je také finanční úspora. [6]

5.4 Analýza změn bezpečnostního prostředí a požadavků bezpečnostní politiky

Tento bod bezpečnostní strategie popisuje, jakým způsobem se mění bezpečnost ve společnosti a na co je důležité se zaměřit při tvorbě bezpečnostní strategie organizace. Je nutné nepodceňovat změny bezpečnostního prostředí, naopak by se s nimi mělo neustále aktivně pracovat, sledovat například zahraniční trendy nebo využít specializované firmy zabývající se touto problematikou. Je důležité připravovat firmu na důsledky takovýchto změn.

V této kapitole jsem se rozhodla popsat kybernetickou bezpečnost, která je v dnešní době velmi podceňovaná a měl by na ni být kladen větší důraz. Do této kapitoly ale spadá například také problematika zaměstnávání zahraničních pracovníků nebo nedostatek kvalifikovaného personálu. Firmy v České republice podceňují hrozby, spojené s kybernetickými útoky. Věnují jim nedostatečnou pozornost. V případě napadení mohou pachatelé vyřadit z provozu například významné servery, ale také ukrást citlivá data, peníze na účtech či strategické informace firem, které mohou následně zneužít.

Výkonnostní problémy v oblasti IT, chyby důležitých aplikací nebo narušení bezpečnosti systémů a dat vedou k finančním ztrátám, poškození dobrého jména, nespokojenosti zaměstnanců a ztrátě zákazníků. Ze studie EY Global Information Security Survey vyplývá, že zhruba 85 procent českých firem má nevyhovující nebo jen částečně vyhovující zabezpečení podnikových informací. Ve světě je podíl podniků s nevyhovujícím zabezpečením ještě o tři procenta vyšší. Kvůli nízkým investicím do kybernetické bezpečnosti a absenci odborníků jsou firmy v Česku pomalejší v odhalování bezpečnostních incidentů. Do hodiny dle této studie odhalí útok 33 procent českých firem, ve světě je to polovina. Vylepšení zabezpečení svých systémů v Česku plánuje 55 procent firem, ve světě chystá bezpečnostní opatření 78 procent společností. Priority kybernetické bezpečnosti jsou v ČR odlišné od okolních zemí, hlavní hrozby se však neliší. Mezi ty patří především demotivovaní zaměstnanci a phishing.

Phishing je metoda podvodného získání citlivých údajů na internetu a následné krádeže peněz. České firmy příliš nevnímají zvyšující se hrozby vyplývající z mobilních technologií či

zneužití sociálních sítí. Rozpočet na kybernetickou bezpečnost chce v roce 2017 zvýšit alespoň o pět procent zhruba pětina českých firem, ve světě je to polovina podniků. Obavy z organizovaného zločinu zesílily, naopak slábnou obavy z incidentů způsobených nevědomostí či nedbalostí zaměstnanců či zastaralostí systémů. Tato studie společnosti Global Information Security Survey vychází z odpovědí 1755 firem z celkem 67 zemí světa včetně ČR. [16]

5.5 Plán rozvoje bezpečnostního systému v střednědobém a dlouhodobém horizontu

Každá firma by měla provádět identifikaci a analýzu rizik, jak je uvedeno v zákoníku práce a související legislativě. Tento bod je při tvorbě bezpečnostní strategie klíčový. Cílem je na základě analýzy rizik a změn v bezpečnostní politice formulovat koncept změn v zabezpečení organizace. Pro vyhotovení analýzy rizik je nutné znát střednědobé cíle ve vývoji bezpečnosti. V následující tabulce jsou uvedeny střednědobé cíle organizace A.

č.	Název projektu	Druh bezpečnosti	Popis projektu	Doba realizace	Odpovědná osoba
1	Převod zajišťování FB a BOZP z externí firmy na interní oddělení bezpečnosti	FB, BOZP	Tvorba bezpečnostního oddělení společnosti, převedení činností týkajících se bezpečnosti z externích firem na vlastní/vlastního zaměstnace (specialisty/specialistu).	7/2015 - 12/2015	personální ředitel
2	Zavedení motivačního systému v oblasti BOZP	BOZP	Nastavení systému kontrol v oblasti BOZP - používání OOPP - dodržování technologických postupů Nový motivační systém s cílem snížit úrazovost na pracovišti na 30% roku 2015	7/2015 - 12/2015	bezpečnostní specialista, správní a personální ředitel
3	Zavedení systému informační bezpečnosti a jeho implementace do firmy	IB, PERS.B.	Zajištění bezpečnosti informačních a komunikačních technologií a systémů pomocí dvoufaktorové autentizace, Patch management, stanovení kategorizace dat, manipulace s nimi, sledování jejich pohybu, autorizace přístupu k nim, periodické kontroly a audit, systém pro řízení změn a ukládání do konfigurační data-	1/2016 - 12/2016	správní ředitel, vedoucí IT odd. , bezpečnostní specialista

			báze, klasifikace dokumentace, zajištění archivace dokumentace dle platných zákonů a norem.		
4	Monitoring externích firem v objektech společnosti, revize návštěvního systému	FB	Návrh a implementace systému evidence a kontroly zaměstnanců externích firem vykonávajících svou pracovní činnost v objektu firmy. Zavedení evidence návštěv přes vrátnici.	1/2017 - 6/2017	personální ředitel, výrobní ředitel, vedoucí nákupu a logistiky, bezpečnostní specialista
5	Revize a nasazení systému kontroly vstupu s integrovaným docházkovým systémem.	FB	Přechod na nový docházkový systém, čipové přívěšky pro zaměstnance.	7/2017 - 12/2017	personální ředitel, výrobní ředitel, bezpečnostní specialista
6	Revize a nasazení nového kamerového systému	FB	Přechod ze stávajících analogových kamer na nové AHD kamery v HD rozlišení, zajištění stěžejních úseků firmy kamerovým systémem Rozšíření systému o bezpečnostní rám a skener.	1/2018 - 12/2018	správní ředitel, výrobní ředitel, bezpečnostní specialista
7	Zajištění objektu mechanickým zabezpečovacím systémem	FB	Revize stávajícího MZS firmy - nové oplocení	1/2019 - 6/2019	správní ředitel, bezpečnostní specialista
8	Posouzení a případné zavedení Cloud uložiště.	IB	Analýza vhodnosti provozování softwaru organizace v Cloudu, vyhodnocení přínosů systému s cílem doporučit nebo zamítnout jeho zavedení.	7/2019 - 12/2019	správní ředitel, vedoucí IT odd.

Tab. 4 Projekty v rámci bezpečnostní strategie ve střednědobém horizontu

Tabulka obsahuje výčet projektů ve vztahu k bezpečnostní strategii, které budou v horizontu pěti let ve firmě realizovány.

5.5.1 Kritéria vyhodnocení rizik

Pro vyhodnocení závažnosti rizik jsou stanovena následující kritéria:

5.5.1.1 P – pravděpodobnost ohrožení

1	Nahodilá
2	Nepravděpodobná
3	Pravděpodobná
4	Velmi pravděpodobná
5	Trvalá

Tab. 5 Pravděpodobnost ohrožení

5.5.1.2 N – následky - závažnost, pravděpodobnost

1	Zanedbatelné
2	Nezávažné
3	Méně závažné
4	Závažné
5	Vysoce závažné

Tab. 6 Následky, závažnost, pravděpodobnost

5.5.1.3 H – subjektivní názor hodnotitelů

1	Zanedbatelný vliv na míru nebezpečí a ohrožení
2	Malý vliv na míru nebezpečí a ohrožení
3	Větší, nezanedbatelný vliv na míru nebezpečí a ohrožení
4	Velký a významný vliv na míru nebezpečí a ohrožení
5	Více významných a nepříznivých vlivů na závažnost a následky ohrožení a nebezpečí

Tab. 7 Subjektivní názor hodnotitelů

Pro posouzení a vyhodnocení rizika použijeme termín míra rizika (mR). Při vyhodnocování závažnosti musí nejprve dojít ke konsensu hodnotitelů u jednotlivých kritérií. Výsledná míra rizika se vypočítá podle:

$$mR = P \times N \times H$$

přičemž znamená, že:

1	nepřijatelné riziko	R > 100	velmi vysoké riziko vzniku úrazu nebo závažné nehody, nutné okamžité zastavení činnosti, odstavení z provozu do realizace nezbytných opatření.
2	nežádoucí riziko	R 51-100	nutnost urychleného provedení opatření ke snížení rizika v nejkratším možném termínu
3	mírné riziko	R 30-50	opatření ke snížení realizovat v programu prevence (plánované revize, servisní prohlídky, plánovaná údržba)
4	akceptovatelné riziko	R 10-30	riziko přijatelné s ohledem na potřebné náklady nutné k zajištění technických a jiných opatření
5	zanedbatelné riziko	R < 10	není nutnost zvláštních opatření, realizace výcvikových programů

Tab. 8 Hodnocení rizik

5.5.1.4 Z – hodnocení řízení rizik

Kategorie	**Významnost rizika**	**Úkoly**	**Body od - do**
A	Příliš vysoké riziko	Musí být opatření i cíl	76 – 125
B	Akceptovatelné riziko	Musí být opatření a může být cíl	26 – 75
C	Zanedbatelné riziko	Může být opatření	1 - 25

Tab. 9 Hodnocení řízení rizik

5.5.2 Četnost identifikace a hodnocení rizik

Hodnocení rizik se bude provádět vždy při změně:

- technologie,
- při mimořádné události,
- organizační změně,
- konstrukční změně na stroji,
- výrobních a pracovních prostředků,
- v případech, které mají nebo mohou mít podstatný vliv na bezpečnost a ochranu zdraví při práci,
- po každé nehodě, skoro-nehodě a po pracovním úrazu,
- vždy min. 1 x ročně.

Cílem tohoto procesu je podchytit nová rizika, která mohou vzniknout. Pro vyhotovení analýzy rizik bude sestavena komise. Na závěr hodnocení odsouhlasí všichni členové provedenou analýzu.

5.5.3 Analýza rizik

Pro vyhodnocování závažnosti rizik daných projektů bude použita bodová metoda, při které je vyhodnocené riziko označeno s přihlédnutím k pravděpodobnosti vzniku a následků, stupni závažnosti, počtu ohrožených osob, kvalifikaci pracovníků a času působení rizika případně i jiným vlivům potencujícím riziko.

Subsystém	Identifikace nebezpečí	Vyhodnocení závažnosti rizika					Opatření
		P	N	H	R	Z	
Převod zajišťování FB a BOZP z externí firmy na interní oddělení bezpečnosti	• snížená kontrola BOZP, • nedodržování BOZP - zvýšená úrazovost, - krádeže, - neoprávněné vznikání do objektu, - úniky dat.	3	3	4	36	B	• využívání služeb současné externí firmy pro překlenovací období, • vytipovat vhodného interního pracovníka, zajištění jeho rekvalifikace, • zácvik nového bezpečnostního specialisty, • zachování četnosti kontrol BOZP za přítomnosti nového bezpečnostního specialisty a externí firmy.

Zavádění informační bezpečnosti	• krádeže dat externí zaváděcí firmou, • nekompatibilita s informačním systémem, • školení zaměstnanců – snížení produkce v době školení, • nedostatečná kvalifikace stávajících zaměstnanců.	2	4	3	24	C	• detailní audit, prověření a reference externích společností, • ověření kompatibility zamýšlených softwarů a aplikací, • efektivní školení zaměstnanců po jednotlivých odděleních a dle přesně stanoveného navazujícího harmonogramu, • test kvalifikace zaměstnanců školení pro zvýšení kvalifikace.
Pohyb neproškolených externích firem v objektech společnosti	• nedodržování OOPP, • úrazy při výkonu práce, • úrazy při pohybu na pracovišti, • dopravní nehody, • krádeže, • neoprávněná obsluha pracovních strojů, zdvihacích prostředků a technologií, • úniky dat a informací.	4	4	4	64	B	• proškolení externích firem pro vstup a pohyb v objektu a na pracovištích, • jmenování zodpovědných osob externích firem, • jmenování interních zodpovědných osob firmy, • vymezení pracovišť, • proškolení, • monitoring externích firem, • audity, kontroly.
Systém kontroly vstupu s integrovaným docházkovým systémem.	• ztráta čipu, • odcizení a zneužití vstupu do objektu - úrazy, - krádeže, - neoprávněné vznikání do objektu, - úniky dat.	2	4	4	32	B	• pokuta za ztrátu čipu, • ověření vlastníka čipu otisky prstů.
Revize a nasazení nového kamerového systému	• rozpor se zákony, • ztráta soukromí, • nervozita a menší koncentrace na práci - škody na zdraví a na majetku, • únik dat z kamerového systému.	2	2	2	8	C	• právní audit kamerového systému před instalací, • komunikace se zaměstnanci – proč snímáme, v čem jim to může pomoci, • vhodná volba prověřeného zaměstnance pro práci s kamerovým systémem.
Zavedení Cloud uložiště.	• bezpečnost dat, • únik dat, • nekompatibilita s informačním systémem.	4	4	3	48	B	• detailní audit a reference poskytovatele, • detailní ověření kompatibility, simulace.

Tab. 10 Analýza rizik pro plánované projekty

Díky této analýze rizik jsme si definovali možné hrozby a pravděpodobnost jejich výskytu. Pomocí bodového hodnocení v rámci stanovené komise jsme určili jejich závažnost a dopady. Pro zjištěné skutečnosti jsme nastavili soubor navrhovaných opatření, který je uveden v posledním sloupci naší tabulky. Hodnocení řízení rizik se pohybuje mezi kategorií B a C. Pro kategorii B platí, že jde o akceptovatelné riziko, pro které musíme vytvořit opatření a můžeme určit cíl. Pro kategorii C platí, že jde o zanedbatelné riziko, pro které můžeme nastavit opatření. Závažné riziko, které by spadalo do kategorie A, jsme neodhalili.

5.6 Objem finančních prostředků pro podporu bezpečnostní strategie

Součástí tvorby bezpečnostní strategie musí být také stanoven finanční rozpočet. Tyto prostředky zpravidla činí významnou část rozpočtu, což je ve výsledku vyváženo bezpečností majetku, osob, firemních dat a podobně. Finanční položka bezpečnosti je často přijímána negativně, protože nepřináší zisk, jeví se tedy pouze jako nákladová položka. Nicméně otázka bezpečnosti je jednou z nejdůležitějších pro zajištění chodu firmy. Při tvorbě rozpočtu se lze inspirovat zkušenostmi z dosavadního provozu výrobních hal s přihlédnutím na nové trendy v oblasti zajištění bezpečnosti.

5.7 Návrh standardů uplatňovaných v bezpečnostním systému firmy

Výsledkem bezpečnostní kontroly jsou organizační opatření ve formě závazných interních dokumentů organizace, které označujeme jako bezpečnostní standardy. V bezpečnostních standardech jsou podrobně definovány postupy pro jednotlivé oblasti bezpečnosti. Při implementaci bezpečnostních standardů do firmy zvolíme vhodnou strategii řízení rizik:

- přijetí rizika – nepřijetím žádných opatření akceptuje organizace bezpečnostní důsledky pro ohrožená aktiva,
- zmírnění rizika – snížení hrozby pro aktivum,
- přenesení rizika – přenesení části rizik na třetí stranu.

Externista, správní úsek a úsek kvality, a dále nově vytvořený úsek bezpečnosti, odpovědný za bezpečnostní standardy organizace, dbá na jejich aktualizaci a na jejich dostupnost konkrétním oddělením a zaměstnancům. V organizaci probíhají vstupní a pravidelná školení pro seznámení zaměstnanců s bezpečnostními standardy. Pravidelná školení probíhají v intervalech uvedených v příslušné legislativě. Ve firmě také probíhají pravidelné i nahodilé kontroly dodržování pravidel a zásad bezpečnosti uvedených v bezpečnostních standardech.

5.8 Návrh organizačních změn k dosažení plánovaných cílů

Dle zjištěných poznatků na základě analýzy v organizaci A musí být provedeny následující organizační změny:

- nastavení kompletní bezpečnostní strategie se zavedením bezpečnostních systémů do praxe napříč firmou, nejlépe za pomoci renomované externí firmy nebo specialisty, zabývajícího se touto problematikou,
- převedení zodpovědnosti za bezpečnost v organizaci z právního úseku na externistu, ten bude přímo podřízený řediteli firmy,
- nastavit systém kontroly pracovní činnosti externisty odborníkem na bezpečnost z řad zaměstnanců firmy. Vzhledem k tomu, že nikdo takový ve firmě nyní zaměstnán není, doporučením je vyhlásit výběrové řízení na tuto pozici a obsadit ji vhodným odborníkem s praxí.
- musí být jasně definovány odpovědnosti a pořádání pravidelných kontrol, jak u zaměstnanců, kteří mají prostředky používat, tak ve skladu, odkud jsou tyto OOPP distribuovány. V případě, že by pracovník neměl na sobě povinné OOPP v době vykonávání pracovní činnosti, toto bude zdokumentováno a postih bude nastaven formou srážky ze mzdy.
- nastavení systému evidence, kontroly, a proškolení zaměstnanců externích firem vykonávající svou pracovní činnost v objektu firmy. Zatím v této věci nejsou ve firmě podnikány žádné kroky pro nastavení systému a přitom se jedná o nejzávažnější bezpečnostní pochybení.
- vyhodnocování a nastavení předávání stěžejních informací, které mají vliv na změny v oblasti bezpečnosti, zainteresovaným osobám, tak aby mohla být komplexně, včas a funkčně zajištěna bezpečnostní politika v organizaci.
- nastavení klasifikace firemní dokumentace z hlediska přístupů oprávněných osob, nebo z hlediska opatření pro úniky strategických informací. Dokumentace musí být spravována také podle hodnoty, podle právní citlivosti, podle jejich citlivosti a podle jejich kritičnosti.

5.9 Zásady pro vyhodnocování účinnosti bezpečnostní strategie a bezpečnostního systému organizace

Doporučením je realizace nezávislých přezkoumání bezpečnosti v organizaci na všech úrovních formou auditů. Nezávislá přezkoumání jsou důležitá pro zajištění toho, že přístup organizace k řízení bezpečnosti je vyhovující, přiměřený a dostatečně účinný. Součástí přezkoumání bude také zhodnocení možností pro zlepšení a změny v přístupu k bezpečnosti, včetně přezkoumání bezpečnostní politiky a cílů opatření. Tato přezkoumání se budou provádět nezávislou autoritou a budou poskytovat nezaujaté hodnocení stavu bezpečnosti. Při každém dalším přezkoumání bezpečnosti, vznikne řada údajů, které by měly doložit, že se vývoj v oblasti ochrany bezpečnosti u organizace zlepšuje. Hodnocení, audit a monitoring stavu bezpečnosti v organizaci je nedílnou součástí procesu řízení bezpečnosti. Východiskem jsou vždy bezpečnostní cíle stanovené v bezpečnostní strategii. Nezávislá organizace provádí analýzu požadavků, rizik a hodnocení současného stavu zabezpečení. Výstupní dokument obsahuje rozhodnutí, zdali vyhovuje, vyhovuje s výhradami anebo nevyhovuje. Dále je v něm také uveden popis problémových oblastí včetně opatření pro odstranění bezpečnostních rizik. Audity budou probíhat také na interní úrovni, v tomto případě je provede subjekt zcela nezávislý na bezpečnostním oddělení. Neprovádění hodnocení, auditu nebo nedostatečná úroveň monitoringu bude mít za následek neodhalení bezpečnostních incidentů a způsobení vyšší škody než při včas odhalených incidentech. Důležitým prvkem pro řízení bezpečnosti bude také ponaučení z bezpečnostních incidentů. Bezpečnostní incidenty budou detekovány, aby informace o stavu bezpečnosti, které incident s sebou přináší, neprošly bez povšimnutí.

Druh bezpečnostního incidentu	Počet výskytů	Finanční újma v Kč
Výpadek proudu	5	2 357 000
Porucha technologií – výrobních strojů	23	978 000
Počítačový virus	15	157 000
Chyba lidského faktoru	39	1 511 000
Krádeže do 5 000 Kč	9	36 000
Krádeže nad 5 000 Kč	4	112 000
Pracovní úrazy	25	784 000
celkem	**120**	**5 935 000**

Tab. 11 Přehled bezpečnostních incidentů ve společnosti A

V tabulce 11 jsou uvedeny bezpečnostní incidenty, které se udály v roce 2015. Z tabulky jasně vyplývá, čím je důležité se zabývat a co v budoucnu zlepšit. Důležité je hledat řešení jak incidentům předejít a jak snížit jejich četnost. Bezpečnostní incident jako jediný poskytuje informaci o skutečném stavu bezpečnosti informací, protože je odrazem chování skutečné reálné situace a nikoli jen výsledkem modelování. U bezpečnostního incidentu je potřeba minimalizovat jeho škodlivé dopady, k čemuž jsou potřebné bezpečnostní struktury stanovené v bezpečnostní politice a bezpečnostních postupech. Velmi důležitou fází je vyhodnocení příčin vzniku bezpečnostního incidentu a vyvození příslušného ponaučení z bezpečnostního incidentu, kvůli zabránění opakování tohoto bezpečnostního incidentu. Právě ponaučení z bezpečnostních incidentů definováním preventivních opatření představuje hlavní bezpečnostní přínos, který lze z bezpečnostního incidentu vytěžit. Pokud bezpečnostní incident proběhne nepovšimnut, jediné, co z něj získáme, je incidentem způsobená škoda.

ZÁVĚR

Zajištění bezpečnosti je nedílnou součástí tvorby celofiremní strategie. Zabezpečení fungování procesů a systémů napříč všemi odděleními a dodržování nařízených bezpečnostních opatření je závislé na několika faktorech. Především jde o kvalitu zpracování, ale i o to, jak jsou odpovědné osoby schopné toto efektivně implementovat dovnitř firmy.

Tato práce zkoumá a hodnotí především důležitost firemní bezpečnosti v globálním měřítku. Dále poukazuje na absenci komplexního zabezpečení firem napříč celofiremní strukturou.

Příkladem je analýza bezpečnostní situace a dokumentace ve dvou organizacích, včetně popisu zjištěných nedostatků, díky čemuž byl získán ucelený pohled na firemní bezpečnost v praxi. Byla odhalena pochybení ve formě chybějícího konceptu zajištění bezpečnosti v rámci firemní strategie a to, že ve firmě existuje pouze bezpečnostní politika, nikoli strategie. Dále byla zjištěna absence systému evidence, kontroly, a proškolení zaměstnanců externích firem vykonávajících pracovní činnost v objektu firmy. Úplně chybí také kontrolní mechanizmus externisty, který firmě zajišťuje bezpečnost. Řešeno není ani zajištění informační bezpečnosti.

V současné době je koncepčním dokumentem v oblasti bezpečnosti bezpečnostní politika firmy. Dokument obvykle popisuje způsob zajištění bezpečnosti v jednotlivých oblastech a druzích bezpečnosti. Na základě analýzy bylo zjištěno, že by bylo vhodné vyhotovit dokument typu bezpečnostní strategie. Přínosem dokumentu je specifikace cílů v oblasti zlepšení bezpečnosti a kroky, které povedou k naplnění daných cílů.

Při tvorbě dokumentu se vycházelo ze střednědobých cílů společnosti, především v rámci obchodní strategie, kdy již má společnost podepsány kontrakty na dodávky svých výrobků, jejichž objem je o třetinu vyšší než nyní a trendy trhu predikují v horizontu následujících deseti let rostoucí tendenci. Pro splnění závazků vyplívajících z těchto kontraktů je nutné vybudovat novou výrobní halu, což s sebou nese mimo jiné také požadavky na zajištění bezpečnosti. Nedílnou součástí je také nutnost nastavení pravidel pro dodržování bezpečnostní strategie všemi zaměstnanci, ale také externisty pohybujícími se v objektu firmy, nebo jakoukoliv osobou z řad zákazníků či návštěv. Součástí je samozřejmě také doporučení nastavení systému kontrol a auditů pro pravidelné zjišťování bezpečnostní situace a fungování bezpečnostních systémů a standardů, které budou provádět jak interní zaměstnanci firmy, tak externisté.

SEZNAM POUŽITÉ LITERATURY

[1] ZEMAN, Petr (ed.). Česká bezpečnostní terminologie: výklad základních pojmů. Brno: Masarykova univerzita, Mezinárodní politologický ústav, 2002. ISBN 80-210-3037-2.

[2] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management V*. Zlín: Radim Bačuvčík - VeRBuM, 2015. ISBN 978-80-87500-67-5.

[3] *Bezpečnostní strategie ČR* [online]. Praha: Kolektiv autorů pod vedením Ministerstva zahraničních věcí ČR, 2015 [cit. 2016-05-12]. Dostupné z: http://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf

[4] Anexe Krymu Ruskou federací. *Www.politikaspolecnost.cz* [online]. Policy Paper, 2016 [cit. 2016-05-12]. Dostupné z: http://www.politikaspolecnost.cz/wp-content/uploads/2016/01/Matzek_Anexe-Krymu-Ruskou-federac%C3%AD_%C4%8CJ.pdf

[5] České strategické dokumenty. *Www.mocr.army.cz* [online]. 2016 [cit. 2016-05-12]. Dostupné z: http://www.mocr.army.cz/ministr-a-ministerstvo/odkazy/odkazy-46088

[6] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management III*. Zlín: VeRBuM, 2013. ISBN 978-80-87500-35-4.

[7] DRASTICH, Martin. *Systém managementu bezpečnosti informací*. 1. vyd. Praha: Grada, 2011. Průvodce (Grada). ISBN 978-80-247-4251-9.

[8] *Bezpečností politika IS: sborník příspěvků ke konferenci pořádané u příležitosti 10. výročí založení společnosti EUNIS-CZ : Špindlerův Mlýn 20.-22.5.2007*. 1. vyd. V Plzni: Západočeská univerzita, 2007. ISBN 978-80-7043-554-0.

[9] ADAMEC, Vilém, David ŘEHÁK a Lenka ČERNÁ. *Základy organizace a řízení bezpečnosti v České republice*. 1. vyd. V Ostravě: Sdružení požárního a bezpečnostního inženýrství, 2012. Spektrum (Sdružení požárního a bezpečnostního inženýrství). ISBN 978-80-7385-123-1.

[10] EICHLER, Jan. *Bezpečnostní a strategická kultura mezinárodních organizací a ČLR*. Vyd. 1. Praha: Oeconomica, 2013. ISBN 978-80-245-1992-0.

[11] NOVÁK, Jaromír. *Vnitřní a vnější bezpečnost státu*. 1. vyd. V Olomouci: Univerzita Palackého, 2014. ISBN 978-80-244-4371-3.

[12] SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 4., aktualiz. a rozš. vyd. Praha: Grada, 2013. Expert (Grada). ISBN 978-80-247-4644-9.

[13] NEČAS, Stanislav a Milan HÁLA (eds.). *Bezpečnost v podmínkách organizací a institucí ČR: sborník z mezinárodní konference, Praha 20. května 2005*. Vyd. 1. Praha: Soukromá vysoká škola ekonomických studií, 2005. ISBN 80-86744-49-3.

[14] Drtivá většina firem má v Česku nevyhovující zabezpečení dat. *Novinky.cz* [online]. ČTK, 2015 [cit. 2016-04-30]. Dostupné z: http://www.novinky.cz/internet-a-pc/bezpecnost/388118-drtiva-vetsina-firem-ma-v-cesku-nevyhovujici-zabezpeceni-dat.html

[15] Bezpečnostní a obranná politika. *Www.euroskop.cz* [online]. [cit. 2016-05-02]. Dostupné z: https://www.euroskop.cz/8715/sekce/bezpecnostni-a-obranna-politika/

[16] Dvoufaktorová autentizace. *Www.computerworld.cz* [online]. 2013 [cit. 2016-05-03]. Dostupné z: http://computerworld.cz/securityworld/je-dvoufaktorova-autentizace-vhodna-pro-male-a-stredni-firmy-50117

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

BS	Bezpečnostní strategie
BP	Bezpečnostní politika
EU	Evropská unie
NATO	Organizace Severoatlantické smlouvy
OBSE	Organizace pro bezpečnost a spolupráci v Evropě
SBOP	Společná bezpečnostní a obranná politika
SZBP	Společná zahraniční bezpečnostní politika
NATINADS	Alianční integrovaný systém protivzdušné obrany
AČR	Armáda České republiky
ČSN	Česká technická norma
ISO	Mezinárodní organizace pro standardizaci
COPS	Politický a bezpečnostní výbor
EUMC	Vojenský výbor Evropské unie
CPCC	Útvar schopnosti civilního plánování a provádění
OOPP	Ochranné osobní pracovní prostředky
BOZP	Bezpečnost a ochrana zdraví při práci
IT	Informační technologie
2FA	Dvoufaktorová autentizace
BYOD	Užívání soukromých přenosných zařízení zaměstnanců k práci

SEZNAM OBRÁZKŮ

SEZNAM TABULEK