POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

Fakulta bezpečnostně právní

Katedra managementu a informatiky

Možnosti, formy a nástroje pro zajištění bezpečnosti podniku v současných podmínkách

Bakalářská práce

Possibilities, forms and tools for ensuring the security of the company in current conditions

VEDOUCÍ PRÁCE

Dr. Jindřich NOVÝ, Ph.D.

AUTOR PRÁCE

Jiří DAŠEK

PRAHA

2022

Čestné prohlášení

Prohlašuji, že předložená práce je mým původním autorským dílem, které jsem vypracoval samostatně. Veškerou literaturu a další zdroje, z nichž jsem čerpal, v práci řádně cituji a jsou uvedeny v seznamu použité literatury.

V Chebu, dne 16. 02. 2022

Jiří DAŠEK

…….

ANOTACE

Předmětná práce se zabývá možnostmi, formami a nástroji pro zajištění bezpečnosti podniku v současných podmínkách, a to z hlediska majetkové trestné činnosti spáchané na aktivech podniku. Cílem práce je poukázat na současnou problematiku v rámci bezpečnosti podniku s uvedením možných hrozeb, kterým může být podnik vystaven a možnostem, formám a nástrojům, při jejichž užití mohou být dané hrozby částečně, či zcela eliminovány.

KLÍČOVÁ SLOVA

Bezpečnost, ochrana, podnik, fyzická bezpečnost, informační bezpečnost, zabezpečení

ANOTATION

This written thesis deals with the possibilities, forms and tools for ensuring the safety of the company in the current world conditions. This is from the point of view of property crimecommitted on the assets of the enterprise. The aim of the written work is to highlight the current issues within the security of the enterprise, indicating the possible threats to which the enterprise may be exposed, and the possibilities. Forms and tools used to the threats can be partially or completely eliminated.

KEYWORDS

safety, protection, company, physical security, security and protection of information, security

OBSAH

ÚVOD

Co je to bezpečnost? Pod tímto všeobecně známým pojmem si mnozí z nás představí jeho odlišný výklad. Každý vnímá bezpečnost svým vlastním pojetím, a to od toho nejširšího, kdy se jedná o bezpečnost státu jako celku, po bezpečnost zajišťovanou složkami státu podnikům, organizacím, až po fyzickou bezpečnost konkrétní osoby, tedy toho nejužšího pojetí formy bezpečnosti. Předmětná bakalářská práce se věnuje možnostem, formám a nástrojům sloužícím pro zajištění bezpečnosti podniku, a to v současných, z důvodů celosvětové pandemie onemocnění Covid-19, nepříznivých podmínkách.

Ve vztahu k bezpečnosti se dnešní doba může zdát nepřívětivou, a to již z pohledu jednotlivce, tedy konkrétní fyzické osoby, či z pohledu managera nebo vlastníka zajišťujícího řádný provoz podniku. Výše uvedené je způsobeno mnoha faktory, kdy se jedná například o již zmíněné onemocnění Covid-19 a s ním spojenou řadu nuceně přijatých vládních opatření, dále nepříliš časově vzdálenými teroristickými útoky, které byly spáchány takřka v celosvětovém měřítku a jejich terčem byly jak měkké cíle, tedy občané útokem postižené země, tak i samotné podniky, či vládní instituce. Jako by již tento výčet hrozeb ohrožujících bezpečnost nestačil, fyzické i právnické osoby se musí potýkat s majetkovou trestnou činností, která je páchána různými formami, a to například prostým překonáním fyzických ochranných opatření podniků, nebo nemovitostí náležících soukromým subjektům, tak i sofistikovaným podvodným jednáním, k němuž je v současné době pachateli velmi často využíván internet, či samotné digitální sítě.

Současná doba je synonymem pro aplikování moderních technologií snad do všech aspektů běžného života. S tímto je samozřejmě úzce spjata také modernizace zařízení, systémů a technologií využívaných v podnicích. Nejen současná generace by si jen těžko dokázala představit provádění složitých výpočtů za pomocí pouhé kalkulačky, či opravení jazykové chyby, tedy odchylky od platné pravopisné

kodifikace, v textu psaném na psacím stroji. Řešení těchto problémů dnes poskytují složité algoritmy softwaru instalovaného v počítačích, nebo klávesa backspace situovaná na počítačové klávesnici. Výše uvedené jsou samozřejmě pouhé příklady nespočetného výčtu přínosů, které nám moderní technologie poskytují, ale jak tomu zpravidla bývá i v tomto ohledu platí, že cokoliv, co lidstvu poskytuje užitek, může být zneužito. S rozmachem informačních technologií a jejich aplikací do aspektů běžného života jedinců, podnikových struktur a systémů se k již tradičním bezpečnostním oborům přidružil obor informační bezpečnosti. Z důvodu takového fenoménu, jakým jsou v současné době kybernetické útoky, které cílí jak na fyzické, tak právnické osoby, se informační bezpečnost stala natolik důležitým pojmem, že řada podniků neváhá z důvodu ochrany svých aktiv investovat nemalé finanční prostředky právě do tohoto oboru. Vzhledem k obsáhlému pojetí informační bezpečnosti a důležitosti odborné znalosti této problematiky, která obsahuje mnoho aspektů, a to od managementu, legislativních předpisů, technických řešení a mnohé další, si podniky, v jejichž IT oddělení absentuje specialista na systém řízení bezpečnosti informací (ISMS – Information Security Management Systém), musí najímat externí konzultanty, jejichž rady se následně řídí. Tento fakt pouze umocňuje význam informační bezpečnosti v rámci podniku v současné době a z uvedeného důvodu bude předmětné problematice věnována samostatná podkapitola této bakalářské práce. Ve výčtu rizik, které mohou ohrozit bezpečnost podniku, by neměla být opomenuta možnost vzniku požáru, a to jak úmyslně založeného, tak i toho jehož zahoření může způsobit technická závada na instalovaném zařízení, či nedbalostní jednání osoby, která je v areálu podniku přítomna.

Cílem předmětné bakalářské práce je poukázat na současnou problematiku v rámci bezpečnosti podniku s uvedením možných hrozeb, kterým může být podnik vystaven a možnostem, formám a nástrojům, při jejichž užití mohou být dané hrozby částečně, či zcela eliminovány.

Bakalářská práce je členěna do tří hlavních kapitol, kdy první kapitola pojednává o bezpečnosti jako takové a zároveň má vzhledem k absenci jedinečné definice

bezpečnosti za cíl vysvětlení tohoto pojmu. Druhá kapitola se v rámci předmětné práce zabývá řízením bezpečnosti v podniku, kdy se jedná o komplexní problematiku, která je vzhledem ke svému rozsahu rozdělena do jednotlivých podkapitol. Třetí kapitolou je závěr, ve kterém se nachází shrnutí celé práce, respektive pojednání o problematice zajištění bezpečnosti podniku v souvislosti se současnými podmínkami.

1 BEZPEČNOST

Jak již bylo předestřeno v úvodu předmětné bakalářské práce, je definice pojmu bezpečnost pro každého z nás určitým způsobem specifická. Toto vnímání bezpečnosti je samozřejmě ovlivněno jedinečným pohledem člověka na své okolí, jeho dosavadními životními zkušenostmi, interakcí s ostatními lidmi, či vstřebáváním informací, které nám poskytují hromadné sdělovací prostředky. Pokud bychom se přeci jen chtěli dobrat obecně platné definice, naskýtá se nám několik možností, a to například použití pojmu vymezeného ve Slovníku spisovné češtiny pro školu a veřejnost, který přídavné jméno ke slovu bezpečnost vykládá následující sémantickou definicí:

„Bezpečný je ten, kdo není vystaven nebezpečí, popřípadě poskytuje ochranu před nebezpečím, nebo je nepochybný, zaručený, důvěryhodný.“[1]

Jak již z uvedeného vyplývá, existuje více aspektů v rámci možných definic pojmu bezpečnost, kdy jednou z nich je doporučení Miroslava Mareše, který danou problematiku vymezuje níže uvedeným:

„Bezpečnost je stav, kdy jsou na nejnižší možnou míru eliminovány hrozby pro objekt a jeho zájmy a tento objekt je k eliminaci stávajících i potenciálních hrozeb efektivně vybaven a ochoten při ní spolupracovat.“[2]

Petrem Zemanem a Miroslavem Marešem byla dále definice pojmu bezpečnost více konkretizována, kdy došlo k jejímu rozlišení na subjektivní a objektivní. Subjektivní bezpečností dle jmenovaných autorů rozumíme takový stav, kdy objektem není vnímáno žádné ohrožení bezpečnosti a tou objektivní, kdy objektu reálné ohrožení

[1] KROUPOVÁ, Libuše, FILIPEC, Josef, ed. *Slovník spisovné češtiny pro školu a veřejnost: s Dodatkem Ministerstva školství, mládeže a tělovýchovy České republiky*. Vyd. 4. Praha: Academia, 2005. ISBN 80-200-1347-4. s. 7.

[2] ZEMAN, Petr, ed. *Česká bezpečnostní terminologie: výklad základních pojmů*. Brno: Masarykova univerzita, Mezinárodní politologický ústav, 2002. ISBN 80-210-3037-2. s. 13.

nehrozí. Oba typy bezpečnosti jsou mezi sebou dle konkrétních okolností různě provázané.[3]

Rozjímání o bezpečnosti je lidstvu vlastní již od pradávna. Už naši předci se museli potýkat s hrozbami, a to jak těmi naturogenními, tedy způsobenými přírodními vlivy jako například zemětřesením, povodněmi, či v určitých lokalitách sopečnou erupcí, tak těmi antropogenními, jenž byly zapříčiněny člověkem. Každá z těchto hrozeb vystavovala v nebezpečí životy, či zdraví lidí jako takových, tak jejich hmotný a nehmotný majetek. Z uvedených důvodů byla přijímána různá ochranná, či obranná opatření, která měla za cíl tyto hrozby eliminovat, nebo alespoň co nejvíce zmírnit jejich škodlivost. Výše uvedené citace pouze dokládají fakt, že ačkoliv jsme antropogenezí dospěli do vývojového stádia homo sapiens, úvahy o bezpečnosti byly, jsou a zřejmě také budou vždy aktuálními. Tato skutečnost je samozřejmě umocněna tím, že i přes vývoj moderních technologií, jimiž člověk v současnosti disponuje a které činí jeho život více komfortním, se kromě těch přírodních hrozeb stále musíme potýkat se samotnou povahou člověka jako takového, tedy i jeho negativními vlastnostmi. Jelikož je každý z nás ve své podstatě originálem, tak i základní principy vnímání bezpečnosti nebyly totožné. Toto vedlo ke vzniku konceptů bezpečnosti a samotná bezpečnost se stala ústředním pojmem a zároveň předmětem zájmu bezpečnostních studií.

Samostatnou vědní disciplínou se bezpečnostní studia stala v období po 1. světové válce, kdy vznikla potřeba zkoumat různé aspekty tohoto válečného konfliktu. Jako každá vědní disciplína, tak i bezpečnostní studia prošla určitým vývojem, což dokazuje debata o jejich budoucnosti v 90. letech minulého století.[4] V rámci bezpečnostních studií existují dva úhly pohledu na podstatu této vědní disciplíny, a to ten tradicionalistický, který explicitně vnímá jako objekt stát a soustředí se na jeho obranu, tedy především na jeho ozbrojené síly a dále pohled tzv.

[3] SAK, Petr. *Úvod do teorie bezpečnosti: nekonvenční pohledy na minulost, přítomnost a budoucnost lidstva*. [Praha]: Petrklíč, 2018. ISBN 978-80-7229-652-1. s. 31.

[4] WAISOVÁ, Šárka. *Bezpečnost: vývoj a proměny konceptu*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. Politologické učebnice. ISBN 80-86898-21-0. s. 34.

„rozšiřovatelů“, ti sice z části uznávají pohled tradicionalistů, ale tento rozšiřují o další aspekty v rámci bezpečnosti.

Dle výše uvedeného tak dochází ke střetu mezí „úzkým“ a „širokým“ vnímáním předmětného vědního oboru.[5] Podle Jana Eichlera můžeme pro bezpečnostní studia jako takové použít níže uvedenou definici:

„Bezpečnostní studia jsou jedním z oborů mezinárodních vztahů. Jejich hlavním předmětem jsou koncepce bezpečnosti a jejího místa v zahraniční politice států či mezinárodních organizací. Zabývají se také vzájemnými vazbami mezi bezpečnostní politikou států a mezinárodního bezpečnostního prostředí. Usilují o vytváření teoretických koncepcí pro zajištění bezpečnosti států i celých oblastí. Věnují se i výzkumu charakteru možných válek a z toho vyplývajících úkolů v oblasti výstavby ozbrojených sil a v zaměření jejich bojové přípravy.“[6]

V rámci bezpečnostních studií jsou následně pohledy na bezpečnost jako takovou dále konkretizovány, kdy vedle již výše zmíněné subjektivní a objektivní bezpečnosti můžeme tuto definovat podle ohrožení, které objektu hrozí v závislosti na prostředí, a to na bezpečnost vnitřní a vnější. Problematiku vnější a vnitřní bezpečnosti Petr Zeman a Miroslav Mareš definují následovně:

„Vnitřní bezpečnost je stav, kdy jsou na nejnižší možnou míru eliminovány hrozby ohrožující objekt a jeho zájmy akcemi zevnitř a tento objekt je k eliminaci stávajících i potencionálních vnitřních hrozeb efektivně vybaven a k ní ochoten. Hrozby demokratickému národnímu státu i jeho opatření proti nim se přitom týkají ohrožování demokratického politického systému od extremistů, sociálního systému od masové kriminality, hospodářství od korupce a ekonomické kriminality a

[5] BUZAN, Barry, Ole WAEVER a Jaap de WILDE. *Bezpečnost: nový rámec pro analýzu*. Brno: Centrum strategických studií, 2005. Současná teorie mezinárodních vztahů. ISBN 80-903333-6-2.

[6] EICHLER, Jan. Bezpečnostní studia. In ZEMAN, Petr, ed. *Česká bezpečnostní terminologie: výklad základních pojmů*. Brno: Masarykova univerzita, Mezinárodní politologický ústav, 2002. ISBN 80-210-3037-2. s. 36.

sociálního, hospodářského a politického systému celkově od organizovaného zločinu.“[7]

Vnitřní bezpečností podle jmenovaných autorů tedy rozumíme stav, kdy určenému objektu v rámci bezpečnosti nehrozí či je minimalizováno ohrožení, a to z důvodu částečné, či úplné eliminace faktorů, které toto ohrožení způsobují. Mezi faktory majícími vliv na vnitřní bezpečnost objektu, kterým pro účely tohoto vysvětlení ustanovím stát, můžeme zařadit například různá extremistická hnutí, či radikalizované politické strany, tedy takové hrozby, jenž na bezpečnost státu působí z jeho vnitřního prostředí.

„Vnější bezpečnost je stav, kdy jsou na nejnižší možnou míru eliminovány hrozby zvnějšku pro objekt a jeho zájmy a tento objekt je k eliminaci stávajících i potenciálních hrozeb efektivně vybaven a ochoten.“[8]

Na základě výše uvedeného vyplývá, že ve věci bezpečnosti jako takové, či v rámci jejího vnitřního a vnějšího rozdělení, je jako k zásadnímu objektu nejčastěji přistupováno z hlediska státu, či mezinárodních organizací. Toto je způsobeno absencí jedinečné relevantní definice, která by byla legislativně, či terminologicky explicitně ukotvena. Proměnlivost chápání významu pojmu bezpečnost, respektive variabilita její definic, se tedy může zdát v určitých aspektech odlišná. Pro účely předmětné bakalářské práce je nicméně důležitá skutečnost z výše uvedených definic vyplývající, a to nezbytnost ustanovení objektu, jehož bezpečnost hodláme zajistit. Všeobecně bychom z primárního hlediska pod pojmem objekt v rámci bezpečnosti samozřejmě mohli stanovit stát jako takový, ale tímto objektem může být například také konkrétní člověk, základní územní samosprávné společenství občanů, tedy obec, kraje, či politické a ekonomické nadnárodní uskupení, jakým je

[7] ZEMAN, Petr, ed. *Česká bezpečnostní terminologie: výklad základních pojmů*. Brno: Masarykova univerzita, Mezinárodní politologický ústav, 2002. ISBN 80-210-3037-2. s. 17.

[8] ZEMAN, Petr, ed. *Česká bezpečnostní terminologie: výklad základních pojmů*. Brno: Masarykova univerzita, Mezinárodní politologický ústav, 2002. ISBN 80-210-3037-2. s. 18.

Evropská unie. S ohledem na téma bakalářské práce a pro její účely bude jako objekt bezpečnosti ustanoven podnik.

2 Řízení bezpečnosti v podniku

S bezpečností podniku úzce souvisí pojem řízení bezpečnosti (Security Management). Jen těžko v současném světě můžeme počítat s pouhým štěstím a bez přiměřených důvodů spoléhat na to, že se nám každá hrozba obloukem vyhne. Jak již bylo v předchozím textu uvedeno, antropogenní hrozby svým způsobem ohrožují každého z nás a jejich riziko může být přímo úměrné majetku, kterým disponujeme. Lidská závist, či touha po zisku vede určité osoby k páchání trestné činnosti, čímž dochází v souvislosti s podniky k ohrožení jejich aktiv, tedy majetku či hospodářských prostředků. V rámci zajištění bezpečnosti, a to samozřejmě nejen z důvodu antropogenních hrozeb, byla řadou podniků přijata určitá opatření, mezi kterými je právě řízení bezpečnosti, s nímž je velmi těsně spjat Business Continuity Management, tedy řízení kontinuity činnosti organizace (podniku).[9] V rámci definování pojmu řízení bezpečnosti můžeme aplikovat níže uvedené:

„Řízení bezpečnosti je soustavná, opakující se sada navzájem provázaných činností, jejichž cílem je zajistit bezpečný provoz a zamezit bezpečnostním rizikům a hrozbám, jako jsou ohrožení či poškození života a zdraví, hmotných a nehmotných aktiv organizace.“[10]

Z předmětné definice vyplývá, že do pojmu řízení bezpečnosti v rámci organizace, v našem případě podniku, je absorbována jak bezpečnost vnější, tak i ta vnitřní. Tato konkrétní problematika, respektive adekvátní zajištění bezpečnosti, pro podniky znamená vynaložení mnohdy nezanedbatelných investic, které financují ze svých zdrojů. Předmětnou skutečnost deklaruje analytický report provedený v roce 2020 společností Cisco. Konkrétní report cílil na oblast kybernetické bezpečnosti, tedy počítačové bezpečnosti nebo též ICT bezpečnosti, která je významným okruhem informační bezpečnosti a zjišťoval prostředky potřebné k vynaložení do

[9] Řízení bezpečnosti (Security Management) - ManagementMania.com. [online]. Copyright © 2011 [cit. 17.02.2022]. Dostupné z: https://managementmania.com/cs/rizeni-bezpecnosti

[10] Řízení bezpečnosti (Security Management) - ManagementMania.com. [online]. Copyright © 2011 [cit. 17.02.2022]. Dostupné z: https://managementmania.com/cs/rizeni-bezpecnosti

minimálního nutného zabezpečení organizací a dále také skutečnost, zda si tyto organizace mohou potřebné investice dovolit. Z uvedeného reportu vyplynulo, že 84 % organizací si může dovolit jen část minimálního potřebného zabezpečení, ale existují i takové, které mají desítky bezpečnostních řešení, a přesto se necítí zcela ochráněny. Ve věci vynaložených investic byly dotazovány organizace čítající mezi 250 a 1000 zaměstnanci, kdy 46 % z nich uvedlo, že nejčastěji za zabezpečení ročně utratí částku do 250 000 dolarů, 43 % investuje částku mezi 250 000 a 1 milionem dolarů a 11 % vynaloží prostředky přesahující 1 milion dolarů. I přes tyto finanční zdroje vložené do kybernetické bezpečnosti si většina organizací uvědomuje skutečnost, že v rámci této problematiky je potřeba přijmout další efektivní prvky.[11]

Dle výše předestřeného, je řízení bezpečnosti komplexním systémem provázaných činností, které se ze své podstatné části zabývá oprávněným přístupem osob k aktivům podniku a na druhou stranu zabráněním přístupu osobám neautorizovaným. Jednou z možností, která se podniku v rámci zajištění své bezpečnosti v tomto ohledu naskýtá, je zaměstnání osoby odpovědné za řízení bezpečnosti. Jak již z uvedeného textu vyplývá, s každým učiněným opatřením je potřeba počítat s určitými finančními zdroji, které jsou k jeho realizaci nutné. Z tohoto důvodu musíme vzít v potaz velikost podniku, aktiva, kterými daný podnik disponuje a náklady vynaložené na zaměstnání specializovaného manažera, jehož náplní práce řízení bezpečnosti bude. Na uvedeném základě tedy není pro malé podniky příliš efektivní předmětného manažera zaměstnávat na plný úvazek, tuto úlohu zde plní statutární orgán a při potřebě řešit situaci v rámci řízení bezpečnosti se tyto podniky následně spoléhají na externí poradce či společnosti, které dané poradenství poskytují. V případě některých středních a velkých podniků, které si mohou dovolit zaměstnávat specializovaného pracovníka, tuto pozici zastává

[11] Jaké jsou dostatečné investice do kybernetické bezpečnosti? - CIO Business World. CIO Business World [online]. Copyright © 2020 [cit. 17.02.2022]. Dostupné z: https://www.cio.cz/clanky/jake-jsou-dostatecne-investice-do-kyberneticke-bezpecnosti/

manažer bezpečnosti (CSO – Chief Security Officer[12]), což pro vlastníka podniku, či statutární orgán samozřejmě neznamená, že by se odpovědnosti za bezpečnost zcela zbavili. Vlastník či statutární orgán nesou vždy tu nejvyšší odpovědnost za bezpečnost podniku, zaměstnání specializovaného manažera jim však umožní delegování určitých aspektů této odpovědnosti na osobu, která je v této konkrétní problematice specializována. Náplní práce manažera bezpečnosti je odpovědnost za plánování rozvoje bezpečnosti podniku, realizace analýzy bezpečnosti, stanovení strategie a bezpečnostní politiky v podniku a samozřejmě také sledování aktuálních trendů v rámci možného zabezpečení. V souvislosti s velikostí podniku a aktiv, kterými disponuje, exponenciálně vzrůstají možnosti ve věci zajištění bezpečnosti. Z tohoto důvodu je ve větších podnicích zřízena také pozice manažera informační bezpečnosti (CISO – Chief Information Security Officer[13]), kdy se tento v rámci podniku soustředí na jeho informační bezpečnost. Manažer informační bezpečnosti zastává v podnicích obdobné úkoly jako manažer bezpečnosti, avšak ve specifické oblasti, a to v rámci informační bezpečnosti. Specializuje se tedy na ochranu informací na organizační a technologické úrovni.

Řízení bezpečnosti je obsáhlou a s ohledem nejen na současnou dobu důležitou oblastí řízení, která podnikům zprostředkovává možnosti, jak ochránit svá aktiva, a to jak ve fyzické, tak i v digitální rovině. Stejně jako pachatelé trestných činů, zejména kybernetických útoků, kteří neustále inovují způsoby, jejímž prostřednictvím realizují odcizení zdrojů z napadených podniků, musí i podnik neustále inovovat svá bezpečnostní opatření. Pro představu o komplexnosti

[12] CSO (Chief Security Officer) - ManagementMania.com. [online]. Copyright © 2011 [cit. 18.02.2022]. Dostupné z: https://managementmania.com/cs/cso-chief-security-officer

[13] CISO (Chief Information Security Officer) - Manažer informační bezpečnosti - ManagementMania.com. [online]. Copyright © 2011 [cit. 18.02.2022]. Dostupné z: https://managementmania.com/cs/ciso-chief-information-security-officer-manazer-informacni-bezpecnosti

problematiky řízení bezpečnosti, která musí reagovat na různé typy hrozeb, je tato rozdělena do níže uvedených klíčových okruhů[14]:

- Fyzická bezpečnost,
- Informační bezpečnost,

V rámci fyzické bezpečnosti je následně zahrnuta bezpečnost majetku, hotovosti a cenností nevyjímaje, bezpečnost budov, jejich ostraha a samozřejmě také osobní bezpečnost společně s řízením lidských zdrojů. Informační bezpečností je obsažena také ICT bezpečnost (Computer security – počítačová bezpečnost).

2.1 Fyzická bezpečnost

Jak již bylo výše uvedeno, fyzická bezpečnost je jedním z klíčových okruhů řízení bezpečnosti. Samotná fyzická bezpečnost v sobě obsahuje výčet možností, forem a nástrojů, jenž podnikům slouží k zabezpečení jejich aktiv. Zároveň je také tou základní formou bezpečnosti v podnicích, jelikož například zabraňuje vstupu neautorizovaným osobám do objektu, a to již jeho prostým uzamčením. Důležitou skutečností v souvislosti s fyzickou bezpečností je specifikace objektu, který hodláme bezpečnostním opatřením chránit. Před realizací instalace bezpečnostního systému, či bezpečnostních opatření, je potřeba, aby podnik provedl vyhodnocení faktorů v rámci zabezpečovaných aktiv, tedy jejich sumarizaci, hodnotu, potenciál jejich zneužití, respektive dostupnost předmětných aktiv na trhu. Následně by měla být podnikem učiněna analýza možných rizik, tedy hrozeb, které zabezpečovaným aktivům hrozí. V tomto ohledu má svůj význam stav aktuálního zabezpečení, charakteristika samotného objektu, subjekt vlastnící předmětný podnik a

[14] Řízení bezpečnosti (Security Management) - ManagementMania.com. [online]. Copyright © 2011 [cit. 18.02.2022]. Dostupné z: https://managementmania.com/cs/rizeni-bezpecnosti

samozřejmě také lokalita.[15] Lokalita je v rámci fyzické bezpečnosti objektu významným aspektem. Je rozdíl, zda má podnik své sídlo v místě, kde dochází k vyššímu počtu trestné činnosti majetkového charakteru, či je situován v sousedství policejního oddělení a v prostoru s minimálním nápadem trestné činnosti.

V závislosti na vyhodnocení výše uvedených faktorů, a to zejména úrovně rizika, kterému je objekt vystaven, je možné, aby se podnik v rámci fyzické bezpečnosti řídil doporučením normy ČSN P CEN/TS 14383-3. Předmětná norma stanovuje preventivní opatření právě v závislosti na míře rizika a celkovou míru rizika klasifikuje do pěti úrovní.[16]

Tabulka úrovní rizika a způsobů zabezpečení:[17]

Úroveň zabezpečení	**Úroveň rizika**	**Preventivní opatření**
1	velmi nízké	Jednoduché mechanické zabezpečení
2	nízké	Zvýšené mechanické zabezpečení
3	střední	Zvýšené mechanické zabezpečení a minimální elektronické zabezpečení
4	vysoké	Rozsáhlé mechanické zabezpečení a střední elektronické zabezpečení
5	velmi vysoké	Rozsáhlé mechanické zabezpečení a vysoké elektronické zabezpečení

[15] KYNCL, Jaromír. Bezpečnost objektu ve světle moderních technologií. Praha: Komora podniků komerční bezpečnosti České republiky, 2014. ISBN 978-80-260-7115-0.

[16] ÚNMZ – ÚŘAD PRO TECHNICKOU NORMALIZACI, METROLOGII A STÁTNÍ ZKUŠEBNICTVÍ [online]. Copyright © [cit. 18.02.2022]. Dostupné z: https://www.unmz.cz/files/Sborn%C3%ADky%20TH/DEF_TNI-2-A4%20-%20pro%20www.pdf

[17] ÚNMZ – ÚŘAD PRO TECHNICKOU NORMALIZACI, METROLOGII A STÁTNÍ ZKUŠEBNICTVÍ [online]. Copyright © [cit. 18.02.2022]. Dostupné z: https://www.unmz.cz/files/Sborn%C3%ADky%20TH/DEF_TNI-2-A4%20-%20pro%20www.pdf

Je podstatné podotknout, že předmětná norma, či preventivní opatření související s mírou rizika, jež jsou specifikována ve výše uvedené tabulce, jsou pouze doporučujícího charakteru. Pro pojmy mechanické a elektronické zabezpečení se v rámci předmětné práce spokojíme s vysvětlením, že v případě mechanického zabezpečení se jedná o prvky klasické ochrany, kterými jsou například oplocení, mříže a v rámci elektronického zabezpečení o prvek technické ochrany, kdy se jedná o kamerové systémy, poplachové zabezpečovací a tísňové systémy, či elektrickou požární signalizaci.

Fyzickou bezpečnost můžeme dále rozlišit dle pasivních a aktivních prvků. V případě těch pasivních se jedná o již zmíněné oplocení, zámky, či například trezory, tedy o takové prvky, které zamezují přístup do objektu a tento chrání proti vniknutí do něj. Účelem aktivních prvků fyzické bezpečnosti je samozřejmě také snaha o zamezení přístupu do objektu, ale zároveň disponují možností upozornit již na případný pokus o vniknutí. Mezi aktivní prvky fyzické bezpečnosti řadíme kamerový systém, pohybová čidla, teplotní čidla, ostrahu atd.[18]

Z výše uvedeného vyplývá, že v rámci zajištění bezpečnosti podniku je problematika fyzické bezpečnosti důležitou a komplexní oblastí, která zahrnuje výčet bezpečnostních prvků, či také ochran. V případě, že podnik bude realizovat bezpečnostní opatření proti trestné činnosti majetkového charakteru, která není páchána prostřednictvím digitálních sítí, tedy zejména proti přímým fyzickým útokům pachatele na aktiva podniku, v tomto konkrétním případě na nemovitosti a aktiva v nemovitostech uložených, je důležité vymezení chráněných prostor.

Z uvedeného důvodu se zřizuje bezpečnostní perimetr, kdy se jedná o prostor, jenž je chráněn fyzickými zábranami, které jsou mnohdy doplňovány adekvátními technickými prostředky, či strážní službou.[19] V souvislosti s daným příkladem, tedy

[18] Fyzická bezpečnost (Physical Security) - ManagementMania.com. [online]. Copyright © 2011 [cit. 18.02.2022]. Dostupné z: https://managementmania.com/cs/fyzicka-bezpecnost

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

zajištěním bezpečnosti, či ochranou nemovitosti, je fyzickou bezpečnost možné rozdělit do níže uvedených druhů ochran:

- Klasická ochrana,
- Technická ochrana,
- Fyzická ochrana,
- Režimová ochrana.

V rámci snahy o dosažení maximální úrovně bezpečnosti je nutné přistoupit k adekvátní kombinaci výše uvedených typů ochran. Všeobecně se dá konstatovat, že žádný bezpečnostní systém není neprolomitelný, tedy stoprocentní. Hlavním účelem bezpečnostního systému je snížení rizika, kterému je objekt vystaven, a to na určitou přijatelnou míru.[20]

2.1.1 Klasická ochrana

S prvky klasické ochrany se lidé setkávají již od nepaměti, jelikož je nejstarším a zároveň základním aspektem bezpečnostního systému. Jejím účelem, jak již bylo předestřeno výše, je snaha o zabránění, či alespoň podstatné ztížení vstupu neautorizované osoby do vytyčeného bezpečnostního perimetru, nebo do nemovitosti. Mezi prvky klasické ochrany zahrnujeme mechanické zábranné systémy, které svou ochranu poskytují na základě mechanické pevnosti, a to prostřednictvím jejich průlomové odolnosti.

Průlomovou odolností ve smyslu mechanických zábranných systémů rozumíme takovou dobu, kterou musí neautorizovaná osoba ke zdolání jejich pevnosti vynaložit. Toto se samozřejmě odvíjí od znalostí dané osoby o konkrétním

[20] KYNCL, Jaromír. *Bezpečnost objektu ve světle moderních technologií*. Praha: Komora podniků komerční bezpečnosti České republiky, 2014. ISBN 978-80-260-7115-0.

mechanickém zábranném systému, druhu nástrojů použitých k jeho překonání, vynaložené energie atd. V rámci mechanického zábranného systému se poté průlomová hodnota stanovuje pro částečný, či úplný průlom, kdy je vyjádřena nejvyšším možným prodloužením časového intervalu, jenž pachatel k překonání překážky potřebuje, a to dle níže uvedené rovnice[21]:

$$\Delta t = t_1 - t_2 \text{ [min]}$$

- Δt časový interval, jenž je k překonání překážky potřeba,
- t_1 čas započetí překonávání překážky,
- t_2 čas finálního překonání překážky.

Na základě průlomové odolnosti jsou poté mechanické zábranné systémy rozděleny do šesti bezpečnostních tříd. V zásadě se účel realizace mechanických zábranných systémů dá považovat také za preventivní. Pokud se totiž bude jednat o takového pachatele, který na základě aktuálních okolností zvažuje možnost vniknutí do objektu, vhodně zvolené mechanické zábranné systémy ho mohou od jeho záměru odradit. Avšak v případě odhodlaného pachatele, jenž má úmysl vniknout do bezpečnostního perimetru, či nemovitosti, na předmětnou trestnou činnost se důkladně připravil a je odhodlán k jejímu spáchání, stále platí, že žádná z ochran není vždy stoprocentní. V daném případě mají mechanické zábranné systémy funkci zdržujícího faktoru, který má za úkol zajistit, aby do jejich překonání musel pachatel vložit značné úsilí, tedy zvyšují časovou náročnost, jenž je zapotřebí k dokonání protiprávního jednání. Výše uvedená skutečnost pouze deklaruje, že pro komplexní zajištění bezpečnosti objektu je zapotřebí kombinace různých typů ochran a také prvků v nich obsažených. Požadavky na prvky mechanických zábranných systémů jsou uvedeny v normách ČSN EN 1627, ČSN EN 1628, ČSN

[21] IVANKA, Ján. *Mechanické zábranné systémy*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2010. ISBN isbn978-807-3189-105.

EN 1629 a ČSN EN 1630. Jak již z výše uvedeného vyplývá, jsou mechanické zábranné systémy prvky klasické ochrany, kterou následně můžeme rozdělit do níže uvedených typů:[22]

- Obvodová ochrana,
- Plášťová ochrana,
- Předmětová ochrana,
- Speciální ochrana.

2.1.1.1 Obvodová ochrana

Obvodová ochrana vymezuje hranici bezpečnostního perimetru a tím chráněný prostor, či objekt odděluje od ostatních pozemků. Jedná se o první mechanický zábranný systém, který musí neautorizovaná osoba, tedy pachatel, v rámci snahy o vniknutí do takto ohraničeného prostoru překonat. Zároveň může mít vybudování robustní obvodové ochrany také psychologický varovný efekt na potencionálního pachatele, což lze umocnit instalací dodatečných, či také doplňkových prvků v rámci obvodové ochrany, a to například vrcholových zábran, jako jsou bariéry s žiletkovým drátem, či nástavce s ostnatým drátem, dále také instalací infračervených závor, otřesových kabelů atd. Mezi prvky obvodové ochrany náleží oplocení, podhrabové zábrany, vrcholové zábrany, vstupy a vjezdy.[23]

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

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

Oplocení

Samotné oplocení, nebo také plotní systémy má dvojí efekt. Instalací oplocení dáváme najevo, že určitý prostor, či v případě podniku jehož bezpečnost zajišťujeme, bezpečnostní perimetr, není veřejnosti přístupný, tedy vstup neautorizovaných osob je v tomto ohledu nežádoucí. K tomuto účelu adekvátně postačí živý plot, tedy oplocení pozemku živými stromky, či křovinami, které případnému pachateli sice ztíží vstup na pozemek, ale k jejich překonání není potřeba vynaložení přílišného úsilí. V rámci zajištění vyššího stupně bezpečnosti v dané oblasti je pro podnik potřeba analyzovat míru rizika ohrožujícího chráněná aktiva, tedy vyhodnotit skutečnosti již konkretizované v úvodu části 2.1 Fyzická bezpečnost. Na základě vyhodnocení předmětné analýzy a v případě potřeby zvýšení úrovně zabezpečení, se nabízí instalace umělého plotního systému. V rámci umělého plotního systému poté rozeznáváme klasické drátěné oplocení, bezpečnostní oplocení, či vysoce bezpečnostní oplocení.[24]

S klasickým drátěným oplocením se můžeme setkat téměř všude. Předmětný druh oplocení je instalován soukromými subjekty v rámci vymezení hranic jejich pozemků, tedy u rodinných domů, zahrad, či také u podniků, které nemají zapotřebí realizovat mechanické zábranné systémy vyššího stupně. Nižší pořizovací hodnota a jednoduchá montáž přispívají k celkové oblíbenosti předmětného plotního systému, avšak pro jeho nízkou průlomovou odolnost není vhodný pro podniky, které mají v úmyslu realizovat vyšší stupeň zabezpečení svých aktiv. Překonání drátěného oplocení vhledem k jeho obvyklé výšce od 1 m do 2 m neznamená pro fyzicky průměrně zdatného pachatele ve většině případů žádný problém, jelikož je možné jej prostě přelézt. V rámci eliminace, či ztížení možnosti překonání drátěného oplocení uvedeným způsobem, je možné v kombinaci s daným oplocením instalovat dodatečné prvky obvodové ochrany, tedy vrcholové zábrany tvořené například bariérou s žiletkovým drátem, či nástavcem s ostnatým drátem.

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

Z důvodu slabého průměru železného drátu, kterým je klasické drátěné oplocení tvořeno, a to 2,5 mm, nepředstavuje při užití standartních nástrojů, například štípacích, či kombinačních kleští, překážku, která by razantně zvýšila časový interval potřebný k jejímu překonání. V rámci klasického drátěného oplocení rozeznáváme čtvercové pletivo, uzlové pletivo a svařované pletivo.[25]

Bezpečnostní oplocení má na rozdíl od klasického drátěného oplocení značně vyšší průlomovou hodnotu, což je dáno převážně použitými materiály, jako je ocel, či beton. Ke zvýšení pasivní bezpečnosti předmětný plotní systém přispívá jak svou výškou, která může dosahovat 2,6 m, tak i svým tvarem a tloušťkou.[26] Z uvedených důvodů je tento mechanický zábranný systém vhodný především pro podniky, které iniciují bezpečnostní zajištění svých aktiv, jelikož splňuje náročnější požadavky na vymezení bezpečnostního perimetru. I v případě bezpečnostního oplocení platí, že vyššího stupně ochrany může podnik docílit jeho kombinací s instalací vrcholových, či podhrabových zábran, které účinnost předmětného mechanického zábranného systému zvyšují. Samotné bezpečnostní oplocení je více odolné vůči snaze o jeho přestřihnutí, či průrazu. Za předmětný plotní systém můžeme pokládat například mřížové oplocení, pevné bariéry, svařované zvlněné pletivo, pletivo z vlnitého drátu, drátěné panelové oplocení a palisádové oplocení.[27]

Vysoce bezpečnostní oplocení se značnou průlomovou odolností je konstruováno pro objekty, u kterých je kladen velký důraz na zajištění jejich bezpečnosti, kdy se jedná například o věznice, jaderné elektrárny, podniky s vysokou mírou rizika atd. V rámci plotních systémů vysoce bezpečnostní oplocení poskytuje nejvyšší možné zajištění bezpečnostního perimetru, což je dáno jak jeho výškou, jenž dosahuje až 5 m, tak jeho pevností. U předmětného oplocení je velmi častá jeho kombinace

[25] UHLÁŘ, Jan. *Technická ochrana objektů*. Praha: Vydavatelství PA ČR, 2000. ISBN isbn80-7251-046-0.

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

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

s instalací dodatečných prvků obvodové ochrany. V souvislosti s vysoce bezpečnostním oplocením rozeznáváme rovný bezpečnostní plot a zakřivené bezpečnostní oplocení. Druhý z daných typů je specifický vyhnutím své horní části, a to ve směru předpokládaného neoprávněného přístupu.[28]

Podhrabové zábrany

Jak již ze samotného názvu vyplývá, podhrabovými zábranami rozumíme takové bezpečnostní prvky, které plotní systémy doplňují o ochranu proti podhrabání, či podlezení. Předmětný bezpečnostní prvek má své opodstatnění zejména v místě, kde je plotní systém situován v měkkém podloží. Zde je instalován až do hloubky 1 m. V rámci podhrabových zábran je v závislosti na účelu tohoto dodatečného prvku využíváno desek, které jsou z plastu, či armovaného betonu s tím, že k instalaci desek z plastu se přistupuje zejména z důvodu zabránění přístupu zvěře. Podhrabové zábrany jsou důležitou součástí hodnotného plotního systému a poskytují podniku další možnost k zajištění jeho bezpečnosti.[29]

Vrcholové zábrany

Vrcholovými zábranami rozumíme další doplňující prvek plotních systémů, který zvyšuje úroveň zajištění bezpečnostního perimetru v rámci pasivní bezpečnosti. Jak již bylo výše uvedeno, mezi vrcholové zábrany náleží například bariéry s žiletkovým drátem, nástavce s ostnatým drátem, ale dále také pevné hroty, otočné válce, či otočné hroty. Vrcholové zábrany se instalují na vrchní část plotního systému, zejména bezpečnostního oplocení a vysoce bezpečnostního oplocení, ale můžeme se s nimi setkat i v rámci klasického drátěného oplocení. V případě klasického

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

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

drátěného oplocení mají však vrcholové zábrany na odhodlaného a běžnými nástroji vybaveného pachatele spíše psychologický efekt, a to z důvodu nízké průlomové hodnoty předmětného plotního systému. Samotné vrcholové zábrany poskytují plotnímu systému, na němž jsou instalovány, doplňující bezpečnostní faktor, a to ochranu proti přelezení.[30]

Vstupy a vjezdy

V rámci bezpečnostního perimetru je důležité správné situování a zvolení počtu přístupů do tohoto prostoru, kdy k tomuto účelu jsou určeny právě vstupy a vjezdy. Jedná se o důležitou součást obvodové ochrany, která podnikům umožňuje provedení kontroly osob, či dopravních prostředků, a to v rámci samotného vstupu do bezpečnostního perimetru, či dokonce ještě před ním. V rámci bezpečnostních perimetrů, ve kterých je kladen maximální důraz na jejich zabezpečení je možnost užití dvoutaktních vstupních systémů, kde je vstupující subjekt vpuštěn první branou, či vjezdem do kontrolního prostoru, ta se za ním uzavře a po provedení kontroly je subjekt do bezpečnostního perimetru vpuštěn další branou, či vjezdem, který je situován naproti tomu původnímu. Předmětný dvoutaktní systém je využíván například ve věznicích, či ve významných strategických podnicích, tedy v místech, kde je vstup neautorizované osoby považován za vysokou míru rizika. V takových případech je tento prvek obvodové ochrany poskytující pasivní bezpečnost doplněn prvkem aktivní bezpečnosti, a to například ostrahou v rámci fyzické ochrany. Jak již bylo předestřeno, vstupy a vjezdy v tomto ohledu rozumíme různé typy bran, branek, turniketů, závor, či bezpečnostních propustí, které v případě vjezdů pro dopravní prostředky mohou být doplněny přídavnými bezpečnostními prvky, jakými jsou mobilní zastavovací pásy, či hřebové pásy. Ke snížení rychlosti dopravních prostředků se v rámci jejich vjezdu do bezpečnostního perimetru, či průjezdu ním, dají využít další technické prostředky, jakými jsou různé

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

zpomalovací zábrany, kdy se jedná o druhy umělých pevných překážek umístěných na vozovce, které svou konstrukcí přinutí řidiče zpomalit, či o průjezdové retardéry, které tvoří betonové bloky, jenž jsou situovány po obou stranách vozovky a v určitých místech jsou zúženy takovým způsobem, aby byl průjezd mezi nimi umožněn pouze při výrazném snížení rychlosti. V rámci realizace adekvátní obvodové ochrany by rovněž žádný podnik neměl opomenout existenci tzv. technologických vstupů, kdy se jedná například o kanalizaci v rámci bezpečnostního perimetru, či procházející pod ním, průlezy s kabely, či také větrací šachty.[31]

2.1.1.2 Plášťová ochrana

Za plášťovou ochranu považujeme takovou ochranu nemovitosti, která je poskytována jejími samotnými konstrukčními prvky, tedy obvodovým zdivem, střechou, či podlahou a otvorovými výplněmi jakými jsou například okna, dveře, či různé šachty. V rámci zajištění bezpečnosti nemovitosti by podnik měl vzít v potaz samotnou existenci bezpečnostního perimetru, který je vymezen obvodovou ochranou. V tomto případě je plášťová ochrana druhým stupněm ochrany. V případě, že podniku byla z určitých důvodů znemožněna realizace obvodové ochrany, a to například z důvodu nemovitosti stojící v klasické zástavbě, kde je obklopen veřejně přístupným prostranstvím, či přímo sousedí s okolními budovami, je plášťová ochrana primárním bezpečnostním prvkem, se kterým případný pachatel při pokusu o vniknutí do nemovitosti setká. Účelem plášťové ochrany je tedy samotná eliminace, či podstatné ztížení možnosti vstupu do nemovitosti neautorizovaným osobám. V případě budovy, která se zabezpečovanou nemovitostí sousedí alespoň po její jedné straně, je potřeba vzít v potaz materiál použitý v rámci této předmětné obvodové zdi a jeho tloušťku. Za určitý minimální standard v rámci

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

odolnosti u konstrukčních prvků lze považovat například cihelné zdivo o tloušťce alespoň 30 cm, které má adekvátní odolnost.

V rámci otvorových výplní plášťové ochrany se jedná o neodmyslitelné součásti budovy, které nám zaručují, jak vstup do ní, tak například její přirozené osvětlení, či větrání. Vstupní body do nemovitosti jsou dány umístěním dveří, kdy se jedná o komplexní mechanický zábranný systém, který je tvořen dveřním křídlem, které je uchyceno v závěsech, dále zárubní, uzamykacím systémem a kováním, kdy se jedná o ochranný štít zámku. Z důvodu komplexnosti a provázanosti jednotlivých prvků dveřního systému je důležité, aby každá z jeho výše uvedených částí disponovala totožnou, či alespoň velmi podobnou průlomovou odolností, jelikož i v tomto případě platí, že komplexní bezpečnostní systém je pouze tak odolný, jako jeho nejslabší část.

Význam oken jako takových byl zmíněn již výše, tedy tato otvorová výplň nám poskytuje přirozené prosvětlení nemovitosti, které je dáno propouštěním denního světla a možnost odvětrání. Existuje velké množství typů oken, které se navzájem odlišují nejen rozměry, či způsoby jejich otevírání, ale také například skleněnou výplní, která může být tvořena i dvojskly, nebo také trojskly s izolačními vlastnostmi. V rámci zajištění bezpečnosti podniku by měla být zvážena možnost zvýšení úrovně bezpečnosti nemovitosti, a to ochranou předmětných otvorových výplní, které lze docílit například instalací mříží, jejichž jednotlivé ocelové, či duralové pruty by měly disponovat takovou odolností, jenž zabrání jejich roztažení. Zároveň by mříže měly být ukotveny v konstrukčním prvku nemovitosti způsobem, který eliminuje možnost jejich vytržení. Odolností mříží proti jejich vytržení se rozumí taková vlastnost, která možnému pachateli za užití běžných nástrojů eliminuje, či podstatně znesnadní možnost neoprávněného vstupu do nemovitosti. Specifikaci a požadavky na mříže jsou stanoveny v normě ČSN EN 1627. Za další možné prvky sloužící k zabezpečení oken jsou považovány například bezpečnostní fólie, které se lepí na skleněnou výplň okna, což v případě rozbití skleněné výplně zajistí její dodatečnou celistvost, a to konkrétně udržením střepů z poškozené skleněné výplně v předmětné fólii. Podniku se rovněž nabízí možnost užití bezpečnostního skla

v oknech, což výrazně navýší bezpečnostní faktor, který nemovitosti plášťová ochrana poskytuje. Dle výroby bezpečnostních skel tato rozdělujeme na tvrzená bezpečnostní skla a vrstvená bezpečnostní skla. K zabezpečení otvorových výplní může podnik využít instalaci bezpečnostních rolet, které fungují na podobném principu jako například navíjecí mříže a mimo bezpečnostní ochranu poskytují také určité odhlučnění od venkovního prostředí, či fungují jako další faktor ovlivňující tepelnou izolaci. V rámci snahy o co nejvyšší zabezpečení objektu je tedy potřeba zvážit použití pouze některých, či kombinaci různých výše uvedených bezpečnostních prvků.[32]

2.1.1.3 Předmětová ochrana

Předmětovou ochranou se rozumí takové ochranné prvky, které zabezpečují aktiva podniku v podobě úschovy předmětů, cenných listin atd. Do uvedené ochrany tedy můžeme zařadit úschovné prostředky jakými jsou například komorové trezory, bezpečnostní schránky, či úschovné objekty.

V rámci komorových trezorů se jedná o bezpečnostní objekty, které jsou určeny k uložení a zabezpečení určitých aktiv. Ochranu předmětů v nich uložených zajišťují více jak 1 m silné obvodové stěny komorových trezorů, kdy je samotný trezor zpravidla součástí konstrukčních prvků budovy, ve které je situován. Dveře komorového trezoru poté disponují komplexním uzamykacím systémem, který je vícebodový a je také opatřen několika zámky. V rámci jejich konstrukce lze komorové trezory rozdělit na monolitické, panelové a kombinované. V případě bezpečnostních schránek jsou tyto umístěny v interiérové části komorových trezorů, kdy jsou zpravidla pronajímány různým subjektům k uložení jejich cenností. Mezi úschovné objekty dále považujeme široké spektrum bezpečnostních úložišť, a to od

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

přenosných schránek po skříňové trezory, či ohnivzdorné skříně. Jak již bylo předestřeno, předmětová ochrana poskytuje nejen fyzickým, ale také právnickým osobám, tedy podnikům, zajištění bezpečnosti jejich aktiv a v případě, že tyto subjekty nedisponují předmětovou ochranou v rámci jejich nemovitostí, mohou využít pronájem již zmíněných bezpečnostních schránek, které nabízejí například bankovní instituce. V rámci realizace předmětové ochrany je samozřejmě důležitý záměr, s jakým je tato ochrana budována, tedy jaké předměty, či aktiva budeme předmětovou ochranou zabezpečovat. Z uvedeného důvodu jsou účelové trezory rozděleny na zabudované trezory, zbraňové trezory a trezory vhozové.[33]

2.1.1.4 Speciální ochrana

Speciální ochrana neposkytuje ceninám, či předmětům, na kterých je užita zabezpečení proti přímému odcizení, či znehodnocení. V rámci speciální ochrany se užívají chemické, či mechanické prvky, kterými se chráněné ceniny, či předměty, označí, což umožňuje například následné ověření jejich pravosti. Speciální ochrana dle výše uvedeného může zajistit určitou formu bezpečnosti specifických aktiv podniku, avšak neposkytuje bezpečnost podniku jako takovému a z tohoto důvodu se v rámci této práce není potřeba problematice speciální ochrany více věnovat.

2.1.2 Technická ochrana

Technická ochrana je nejnovějším okruhem fyzické bezpečnosti, jenž je specifický použitím různých typů detekčních, monitorovacích, či poplachových a

[33] UHLÁŘ, Jan. *Technická ochrana objektů*. 2. vyd. Praha: Policejní akademie České republiky v Praze, 2009. ISBN 978-80-7251-312-3.

zabezpečovacích systémů, které například umožňují zachytit vstup neautorizované osoby do bezpečnostního perimetru a upozornit na něj akustickým, či vizuálním způsobem. Přidanou hodnotou technické ochrany je možnost archivace záznamů, které mohou v rámci šetřeného protiprávního jednání, či určité mimořádné události, sloužit orgánům činným v trestním řízení jako důkazní prostředek. Na uvedeném základě je patrné, že v rámci bezpečnostního perimetru je technická ochrana velice účinným doplňkem ochrany klasické a fyzické, a to zejména v případech, kdy je tento perimetr rozsáhlý. Z hlediska zdrojů, které hodlá podnik v rámci zajištění své bezpečnosti investovat, poté předmětná ochrana snižuje náklady vynaložené na ochranu fyzickou, tedy například umožňuje redukci počtu členů ostrahy, a to při zachování stávající úrovně bezpečnosti.[34]

Stejně jako prvky klasické ochrany, má i technická ochrana na případného pachatele trestné činnosti psychologický faktor. Z uvedeného důvodu je nutné zvážit, zda prvky technické ochrany budeme situovat takovým způsobem, aby byly zřetelně viditelné, či je umístíme skrytě. V závislosti na umístění prvků technické ochrany v prostoru tuto dělíme do níže uvedených druhů:

Obvodová ochrana

Obvodovou ochranou v rámci technické ochrany rozumíme takové technické prvky, jež jsou situovány po obvodu bezpečnostního perimetru a poskytují doplňkové zabezpečení plotních systémů, vstupů a vjezdů atd. Předmětné prvky mohou monitorovat případné protiprávní jednání v rámci pokusu o překonání zabezpečení, či například prostřednictvím čidel upozornit na samotné vniknutí do bezpečnostního perimetru.

Plášťová ochrana

Plášťová ochrana v rámci technické ochrany má totožný princip jako ochrana obvodová. V tomto případě však poskytuje doplňkové zabezpečení konstrukčním

[34] UHLÁŘ, Jan. *Technická ochrana objektů*. 2. vyd. Praha: Policejní akademie České republiky v Praze, 2009. ISBN 978-80-7251-313-0.

prvkům budovy, či otvorovým výplním v rámci plášťové ochrany, tedy například oknům, či dveřím, kdy upozorňuje na narušení opláštění budovy.

Prostorová ochrana

Prostorovou ochranu v rámci technické ochrany poskytuje soustava čidel, které detekují pohyb neautorizované osoby. Výhodou prostorové ochrany je právě možnost konkretizace místa s narušitelem, tedy jeho lokalizování a předání tohoto poznatku ostraze, či přivolané hlídce policie. Prostorová ochrana tedy usnadňuje následný zákrok proti pachateli.

Předmětová ochrana

Předmětovou ochranou v rámci technické ochrany rozumíme takové technické prostředky, zpravidla čidla, které signalizují neoprávněný pokus, či vniknutí do ochranných úschovných prvků, tedy například trezorů atd.

Klíčová ochrana

Klíčová ochrana má v rámci technické ochrany obdobný význam jako ochrana prostorová. Specifikací klíčové ochrany je však předchozí vytyčení míst, kde se předpokládá pohyb neautorizované osoby, například schodiště, chodby, vestibuly atd.

V rámci zajištění maximální úrovně bezpečnosti je vhodné využít kombinaci výše uvedených prvků technické ochrany v bezpečnostním perimetru, kdy tímto realizujeme vícestupňovou ochranu.

Technická ochrana podnikům poskytuje více možností pro zajištění jejich bezpečnosti, a to nejen proti hrozbám, antropogenním, kdy se jedná o úmyslné trestné činy spáchané určitou fyzickou osobou, ale také například v rámci elektrické požární signalizace (EPS), která při detekci požáru umožňuje spuštění s ní kombinovaných protipožárních opatření jako je například hasící, či odvětrávací systém a prostřednictvím pultu centralizované ochrany vyrozumí o vzniklém požáru

operátora hasičského záchranného sboru. Mezi prvky technické ochrany řadíme níže uvedené:

Poplachové zabezpečovací a tísňové systémy

V případě poplachového zabezpečovacího systému, či tísňového systému se jedná o komplexní bezpečnostní systém, který je tvořen tzv. zabezpečovacím řetězcem, a to detektory, ústřednou, přenosovými prostředky a signalizačním zařízením. Základním principem těchto systémů je samotná detekce narušení zabezpečované budovy, a to jak již ve stádiu pokusu, tak v rámci jeho dokonání a následné předání poplachového signálu akustickým, či vizuálním způsobem oprávněné osobě, kdy se může jednat například o člena ostrahy objektu, či prostřednictvím pultu centralizované ochrany bezpečnostní agentuře, či policii.

V závislosti na způsobu předání poplachového signálu rozlišujeme lokální, autonomní a dálkové poplachové zabezpečovací a tísňové systémy. V rámci lokálního předání poplachového signálu detektor iniciuje optickou, či vizuální signalizaci konkrétně v napadeném objektu, autonomní předání poplachového signálu vede k předání signálu do ústředny, kde je přítomen člen ostrahy a dálkový přenos poplachového signálu vede k vyrozumění externího dohledového a poplachového centra, které není v prostoru zabezpečovaného objektu.[35]

Uzavřený televizní okruh

Uzavřený televizní okruh (CCTV – Closed Circuit Television), nebo také kamerový systém, je důležitou součástí technické ochrany. Jak již bylo výše předestřeno, vhodně situovaný kamerový systém působí také odstrašujícím psychologickým faktorem a může potencionálního pachatele odradit od úmyslu vniknout do

[35] UHLÁŘ, Jan. *Technická ochrana objektů*. 2. vyd. Praha: Policejní akademie České republiky v Praze, 2009. ISBN 978-80-7251-313-0.

bezpečnostního perimetru již svou přítomností. Kamerový systém je tvořen komplexním systémem technických zařízení, zejména libovolným počtem kamer a má za účel monitorování bezpečnostního perimetru, v rámci určitých kamerových systémů automatickou detekci narušení bezpečnostního perimetru, zaznamenávání a archivaci záznamu, či v souvislosti s poplachovými zabezpečovacími a tísňovými systémy také ověřování předmětného poplachového signálu.[36]

V rámci kamerového systému se v současné době jedná o jeden z nejrozšířenějších bezpečnostních prvků, kromě preventivního účelu, tedy výše uvedeného psychologického odstrašujícího faktoru, disponuje kamerový systém, respektive záznam pořízený kamerovým systémem, pro orgány činné v trestním řízení neocenitelnou důkazní hodnotou. Vzhledem k jeho situování můžeme předmětný systém rozlišit na vnitřní a venkovní.

Elektrická požární signalizace

V souvislosti se zajištěním bezpečnosti podniku je důležitá instalace elektrické požární signalizace, jelikož požár, a to jak ten úmyslně, nedbalostně, či technickou závadou způsobený, je závažným ohrožením života a zdraví v místě přítomných osob a také podnikových aktiv. Z ekonomického hlediska je pro podnik rozhodně výhodnější investice do předmětné signalizace, a to v porovnáním s pokrytím škod způsobených požárem. Základním účelem elektrické požární signalizace je neprodlená detekce ohniska požáru, a to konkrétně již ohniska zahoření a včasné upozornění na vzniklé nebezpečí prostřednictvím akustických a vizuálních signálů. Uvedený signalizační systém je tvořen hlásiči, přenosovými prostředky a signalizačními zařízeními.[37]

[36] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management*. Zlín: Radim Bačuvčík - VeRBuM, 2015. ISBN 978-80-87500-05-7.

Systém kontroly vstupu

Účelem předmětného komplexního systému je zejména evidence osob, či dopravních prostředků, které vstupují do bezpečnostního perimetru, či do zón, které jsou v rámci perimetru předem definovány s možností zabránění, či povolení vstupu, a to například na základě identifikační karty, kterou autorizované osoby disponují.[38]

Systém kontroly vstupu je vhodný například pro podniky, které čítají vyšší počet zaměstnanců s odlišnou bezpečnostní prověrkou, či které z důvodu zajištění bezpečnosti svých aktiv chtějí znemožnit přístup určitých zaměstnanců do předem definované zóny. V rámci nastavených parametrů předmětný systém umožňuje vstup předem určeným osobám v určitém časovém intervalu, nebo zabránění opakovanému průchodu v takto definovaných zónách.[39]

2.1.3 Fyzická ochrana

Stavba hradišť, nebo oplocení důležitých míst, či objektů a jejich následné střežení provází lidstvo již od nepaměti. Z uvedeného vyplývá, že kombinace klasické ochrany s ochranou fyzickou je tou nejstarší a osvědčenou metodou v rámci zajištění bezpečnosti. Ať již jsou moderní zabezpečovací systémy schopny detekovat pokus, či průnik neautorizované osoby do bezpečnostního perimetru a upozornit na něj, pouze lidský faktor v rámci bezpečnosti umožní realizovat adekvátní zákrok proti narušiteli, a to samozřejmě v souladu s platnou legislativou.

---

[37] UHLÁŘ, Jan. *Technická ochrana objektů*. Praha: Vydavatelství PA ČR, 2006. ISBN 80-7251-235-8.

[38] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management*. Zlín: Radim Bačuvčík - VeRBuM, 2015. ISBN 978-80-87500-19-4.

[39] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management*. Zlín: Radim Bačuvčík - VeRBuM, 2015. ISBN 978-80-87500-05-7.

Z uvedeného důvodu je v rámci zajištění bezpečnosti mnoha středními a velkými podniky přistupováno k realizaci ostrahy objektu, která je vykonávána například vrátnými, pracovníky soukromých bezpečnostních služeb, hlídači, či v rámci specifických podniků se strategickým významem také Policií České republiky. Ačkoliv je přínos fyzické ochrany v rámci bezpečnosti nepopiratelný, je také pro podniky z ekonomického hlediska nejvíce zatěžující. V rámci snížení předmětné ekonomické zátěže je pro podniky výhodné kombinovat daný typ ochrany s již uvedenými prvky ochrany klasické, či technické ochrany, kdy tato kombinace při adekvátním rozložení jednotlivých prvků zachová stávající úroveň bezpečnosti, a to s výsledným snížením potřebných nákladů. Výše uvedené umocňuje skutečnost, že každý policista v rámci Policie České republiky má na základě iniciativy dle ustanovení § 10 odstavce 1 zákona číslo 273/2008 Sb. o Policii České republiky níže uvedenou povinnost:

„V případě ohrožení nebo porušení vnitřního pořádku a bezpečnosti, jehož odstranění spadá do úkolů policie, je policista ve službě nebo zaměstnanec policie v pracovní době povinen provést úkon v rámci své pravomoci nebo přijmout jiné opatření, aby ohrožení nebo porušení odstranil.“[40]

Z výše uvedeného vyplývá, že zaměstnanec ostrahy objektu, který zjistil narušení bezpečnostního perimetru, či mu předmětné narušení bylo signalizováno systémem v rámci technické ochrany, může provést určitá opatření sám, či zjištěné protiprávní jednání oznámit Policii české republiky. V konkrétním případě protiprávního jednání, tedy narušení bezpečnostního perimetru, či vniknutí do střežené nemovitosti neautorizovanou osobou, je zaměstnanec ostrahy oprávněn podezřelou osobu zadržet, a to dle ustanovení § 76 odstavce 2 zákona číslo 141/1961 Sb. o trestním řízení soudním (trestní řád), kde je taxativně uvedeno:

[40] 273/2008 Sb. Zákon o Policii ČR. Zákony pro lidi - Sbírka zákonů ČR v aktuálním konsolidovaném znění [online]. Copyright © AION CS, s.r.o. 2010 [cit. 22.02.2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/2008-273

„Osobní svobodu osoby, která byla přistižena při trestném činu nebo bezprostředně poté, smí omezit kdokoli, pokud je to nutné ke zjištění její totožnosti, k zamezení útěku nebo k zajištění důkazů. Je však povinen tuto osobu předat ihned policejnímu orgánu; příslušníka ozbrojených sil může též předat nejbližšímu útvaru ozbrojených sil nebo správci posádky. Nelze-li takovou osobu ihned předat, je třeba některému z uvedených orgánů omezení osobní svobody bez odkladu oznámit.“[41]

V oblasti fyzické ochrany jsou ostrahou objektu vykonávány činnosti vedoucí k ochraně aktiv podniku, zabezpečení pořádku, kontrola bezpečnostního perimetru, tedy také kontrola vstupu, či odchodu osob nebo vjezdu a výjezdu dopravních prostředků. Na základě uvedeného spektra povinností, které jsou na členy ostrahy kladeny a s ohledem na možný zákrok proti pachateli protiprávního jednání, jsou členové ostrahy mnohdy vybaveni obrannými a ochrannými prostředky. V rámci držení střelných zbraní se na členy ostrahy vztahuje ustanovení § 8 zákona číslo 119/2002 Sb. o střelných zbraních a střelivu, kde je uvedeno:

„Nabývat do vlastnictví, s výjimkou dědění, a držet nebo nosit zbraň nebo střelivo může pouze ten, kdo je držitelem zbrojního průkazu nebo zbrojní licence, pokud zákon nestanoví jinak.“[42]

V souvislosti s držením střelných zbraní pro členy ostrahy vyplývá povinnost, být držitelem zbrojního průkazu skupiny D, který danou osobu k tomuto opravňuje v rámci výkonu zaměstnání nebo povolání.

[41] 141/1961 Sb. Trestní řád. Zákony pro lidi - Sbírka zákonů ČR v aktuálním konsolidovaném znění [online]. Copyright © AION CS, s.r.o. 2010 [cit. 22.02.2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/1961-141

[42] 119/2002 Sb. Zákon o střelných zbraních a střelivu. Zákony pro lidi - Sbírka zákonů ČR v aktuálním konsolidovaném znění [online]. Copyright © AION CS, s.r.o. 2010 [cit. 22.02.2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/2002-119

2.1.4 Režimová ochrana

Ve snaze o zajištění vyšší bezpečnosti se podniku nabízí zavedení režimové ochrany, kdy se jedná o realizaci a následné dodržování konkrétních norem v rámci podnikové struktury. Režimová ochrana se zejména týká vstupu/vjezdu osob/dopravních prostředků do bezpečnostního perimetru a jejich odchodu/výjezdu z něj, ale také například oprávněním konkrétních osob ke vstupu do předem definovaných zón. Ke zvýšení efektivity režimové ochrany se nabízí možnost jejího kombinování s prvkem technické ochrany, a to konkrétně systémem kontroly vstupu. Základní princip kombinace režimové ochrany se systémem kontroly vstupu je totiž doplňujícího charakteru, kdy v rámci režimové ochrany podnik přijme určité závazné normy, které se týkají vstupu, odchodu a pohybu osob, či manipulací s jeho aktivy, kterými se rozumí například cenné listiny, či pro podnik významné informace. Dle úrovně potřebného zajištění bezpečnostního perimetru, zón, či aktiv poté podnik stanoví bezpečnostní úroveň, kterou v souvislosti s pohybem, či manipulací s aktivy konkrétní osoby potřebují, tedy jim udělí určitá oprávnění a následně těmto osobám v rámci systému kontroly vstupu poskytne například identifikační karty stanovené bezpečnostní úrovně, které jejich držitele k výše uvedenému opravňují. Prostřednictvím režimové ochrany mohou být konkrétní osoby oprávněny k výkonu výše uvedeného jako celku, či pouze k jeho určitých dílčích částí, a to právě na základě jejich bezpečnostní úrovně. Na uvedeném základě lze konstatovat, že efektivní režimová ochrana je v rámci zajištění bezpečnosti pro podnik přínosem.[43]

[43] Režimová ochrana :: Bezpečnostní poradenství JŠ. Bezpečnostní poradenství JŠ [online]. Copyright © 2015 Všechna práva vyhrazena. [cit. 22.02.2022]. Dostupné z: https://www.bp-js.cz/fyzicka-ochrana/rezimova-ochrana/

2.1.5 Bezpečnost a ochrana zdraví při práci

Pojmem bezpečností a ochranou zdraví při práci se rozumí soubor takových opatření různého charakteru, které podnik stanovuje za účelem zajištění bezpečnosti zaměstnanců, kdy tato opatření snižují riziko vedoucí k ohrožení zdraví, nebo ztrátám na životě. V rámci definování předmětného pojmu se může použít také níže uvedené:

„Bezpečnost a ochranu zdraví při práci chápeme jako souhrn práv a povinností účastníku pracovně právních vztahů, jakož i orgánu dozoru nad bezpečností a ochranou zdraví při práci a právních institutů, které směřují k zabezpečení opatření a technických zařízení potřebných k zajištění bezpečnosti a ochrany zdraví při práci.“[44]

Z výše předestřeného vyplývá, že bezpečnost a ochrana zdraví při práci prostřednictvím norem vydaných v rámci předmětné problematiky, zastává zejména funkci preventivního, ale také produkčního charakteru, a to v zájmu snahy o vytvoření optimálních pracovních podmínek, či pracovního prostředí. Preventivním charakterem v rámci podnikové struktury rozumíme taková opatření, která vedou ke snížení rizika ohrožení zdraví a ztrát na životech, a to v kontextu se zákoníkem práce, kde je taxativně uvedeno:

- Ustanovení § 101 odstavce 1 zákona číslo 262/2006 Sb. zákoník práce

„Zaměstnavatel je povinen zajistit bezpečnost a ochranu zdraví zaměstnanců při práci s ohledem na rizika možného ohrožení jejich života a zdraví, která se týkají výkonu práce.“[45]

---

[44] GALVAS, Milan. *Pracovní právo*. 2., doplněné a přepracované vydání. Brno: Masarykova univerzita, 2015. ISBN 978-80-210-8021-8. s. 607.

[45] 262/2006 Sb. Zákoník práce. Zákony pro lidi - Sbírka zákonů ČR v aktuálním konsolidovaném znění [online]. Copyright © AION CS, s.r.o. 2010 [cit. 22.02.2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/2006-262

- Ustanovení § 102 odstavce 1 zákona číslo 262/2006 Sb. zákoník práce

„Zaměstnavatel je povinen vytvářet bezpečné a zdraví neohrožující pracovní prostředí a pracovní podmínky vhodnou organizací bezpečnosti a ochrany zdraví při práci a přijímáním opatření k předcházení rizikům.“[46]

V rámci preventivního charakteru je předcházení rizikům pro podnik přínosné nejen z důvodu zajištění bezpečnosti jeho zaměstnanců, ale také z ekonomického hlediska. Každý podnik chce mít na svém pracovišti kvalifikované zaměstnance, kdy z důvodu jejich absence, způsobené například pracovním úrazem, musí podnik přistoupit ke školení zaměstnance nového, či překvalifikování některého ze stávajících a zároveň mu vzniká povinnost uhrazení nákladů souvisejících s odškodněním pracovního úrazu. Podnik zároveň adekvátním realizováním bezpečnosti a ochrany zdraví při práci zajišťuje bezpečnost svých aktiv, která mohou být například neodbornou manipulací s technikou ohrožena možností vzniku požáru. Produkční charakter bezpečnosti a ochrany zdraví při práci má vliv na samotnou produkci podniku, který má samozřejmě snahu o dosažení permanentního a kvalitativně stabilního pracovního režimu.

2.2 Informační bezpečnost

V souvislosti s rozvojem moderních technologií, v rámci předmětné práce zejména s digitalizací podniků, je informační bezpečnost klíčovým okruhem v oblasti řízení bezpečnosti. Význam dané problematiky neustále roste, což deklaruje také report provedený společností Cisco, jenž je uveden v kapitole 2 Řízení bezpečnosti. Téměř žádný podnik se v současné době neobejde bez informačních technologií, které umožňují realizaci zpracování informací, kdy se často jedná o osobní, či citlivé

[46] 262/2006 Sb. Zákoník práce. Zákony pro lidi - Sbírka zákonů ČR v aktuálním konsolidovaném znění [online]. Copyright © AION CS, s.r.o. 2010 [cit. 22.02.2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/2006-262

údaje, nebo v rámci podnikové struktury také o aktiva, jakými jsou například informace o bezpečnosti podniku, před konkurencí chráněné výrobní procesy, vnitropodnikové analýzy, nebo plány jejich případné budoucí expanze. Jedná se rovněž o tzv. know-how, čímž rozumíme souhrn vědomostí, odborných znalostí, výrobních znalostí a postupů získaných dlouholetou zkušeností v daném oboru. Dle výše předestřeného vyplývá, že zpracování informací, v tomto případě přenos výše uvedených citlivých dat, je důvěrné, tedy žádná ze zainteresovaných stran, a to odesílatel, či adresát předmětných dat, nechce, aby tyto informace unikly ke konkurenci, či k neautorizované osobě a tímto vystavit předmětná data riziku odcizení, či zneužití.

Snaha o eliminaci rizika ztráty, či zneužití dat, případně jeho razantního snížení, není pro podniky v rámci informační bezpečnosti jediným hnacím faktorem. V souvislosti se zpracováváním osobních údajů, jsou podniky k jejich zabezpečení také legislativně povinovány, a to konkrétně na základě ustanovení § 46 odstavce 1 zákona číslo 110/2019 Sb. o zpracování osobních údajů, kde je v souvislosti s povinnostmi osob při zabezpečení osobních údajů taxativně uvedeno:

„Správce je povinen přijmout taková technická a organizační opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení, ztrátě, neoprávněnému přenosu nebo jinému neoprávněnému zpracování nebo zneužití. Tato povinnost platí i po ukončení zpracování osobních údajů.“[47]

Výše uvedená povinnost je stanovena rovněž pro zpracovatele osobních údajů, a to v návaznosti na ustanovení § 46 odstavce 5 zákona číslo 110/2019 o zpracování osobních údajů.

V rámci realizace informační bezpečnosti v podniku by ochrana dat měla být koncipována na organizační a technologické úrovni, a to právě s cílem zajištění

[47] 110/2019 Sb. Zákon o zpracování osobních údajů. Zákony pro lidi - Sbírka zákonů ČR v aktuálním konsolidovaném znění [online]. Copyright © AION CS, s.r.o. 2010 [cit. 23.02.2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/2019-110

bezpečné práce s informacemi. Na základě organizační úrovně by měly být podnikem ustanoveny autorizované osoby, tedy zaměstnanci s oprávněním k manipulaci s chráněnými informacemi, či daty. Výše uvedené může být řešeno například smluvním zavázáním mlčenlivosti. Ochranu informací na technologické úrovni v rámci informační bezpečnosti podnik realizuje prostřednictvím ICT bezpečnosti, někdy také nazývané jako počítačová bezpečnost, která zahrnuje použití specializovaného bezpečnostního softwaru, či hardwarových opatření.[48]

2.2.1 Systém řízení bezpečnosti informací

Řízení bezpečnosti informací (ISMS – Information Security Management Systém) je komplexním systémem v rámci standardů stanovených Mezinárodní organizací pro standardizaci (International Organization for Standardization), které jsou vydávány pod zastřešující normou ISO/IEC 27000 a soustředí se na jednotlivé aspekty informační bezpečnosti.[49] Klíčovou normou je však norma ISO/IEC 27001, kdy předmětná norma nabízí komplexní stanovisko k informační bezpečnosti a stanovuje tři principy ochrany informací, a to:

- Důvěrnost
- Celistvost
- Dostupnost

Na základě důvěrnosti je zaručen přístup k chráněným informacím pouze autorizovaným osobám, celistvost zaručuje integritu informací a stanoví oprávnění

[48] Bezpečnost a ochrana informací (Security and Protection of Information) - ManagementMania.com. [online]. Copyright © 2011 [cit. 23.02.2022]. Dostupné z: https://managementmania.com/cs/bezpecnost-a-ochrana-informaci

[49] ISO 27000 - ManagementMania.com. [online]. Copyright © 2011 [cit. 23.02.2022]. Dostupné z: https://managementmania.com/cs/iso-27000

v kontextu s jejich pozměňováním a dostupnost zajišťuje, že potřebné informace jsou pro autorizované osoby v případě potřeby k dispozici.[50]

V souvislosti s definicí systému řízení bezpečnosti informací lze užít níže uvedené:

„Systém řízení bezpečnosti informací představuje soubor pravidel, jejichž cílem je zachovat důvěrnost, integritu a dostupnost informací aplikováním procesu řízení rizik a dát jistotu zainteresovaným stranám, že jsou rizika přiměřeně řízena. V rámci ISMS jsou chráněna aktiva, řízena rizika bezpečnosti informací a již zavedená opatření jsou kontrolována.“[51]

Systém řízení bezpečnosti informací analyzuje rizika v souvislosti s nakládáním s informacemi a vzhledem k jeho komplexnosti je ho možné dělit do níže uvedených fází:

- Zavádění a provozování
- Monitorování a přezkoumávání
- Udržování a zlepšování

V rámci fáze zavádění a provozování systému řízení bezpečnosti informací podnik implementuje řadu opatření souvisejících se zvládáním rizik. Fází monitorování a přezkoumávání rozumíme detekci bezpečnostních incidentů v rámci jejich pokusů, či samotného dokonání, nebo monitoring činnosti autorizovaných osob při nakládání se zabezpečovanými informacemi. Fáze udržování a zlepšování je preventivního a nápravného charakteru, kdy na výše uvedených základech provedenými analýzami dochází k odstraňování zjištěných nedostatků a jsou přijímána protiopatření.[52]

[50] ISO 27001 Systém managementu bezpečnosti informací - ManagementMania.com. [online]. Copyright © 2011 [cit. 24.02.2022]. Dostupné z: https://managementmania.com/cs/iso-27001

[51] KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88168-31-7. s. 253

2.2.2 ICT bezpečnost

ICT bezpečnost (Information and Comunication Technologies), nebo také počítačová bezpečnost je jednou ze součástí informační bezpečnosti, a to v rámci informačních a komunikačních technologií.[53] V souvislosti s definováním pojmu ICT bezpečnost lze konstatovat, že předmětný pojem je souhrnným označením problematiky, která řeší, či spravuje využití technických prostředků pro komunikaci a manipulaci s informacemi, tedy zajišťuje ochranu dat proti ohrožujícímu nahodilému, či škodlivému jednání, a to na softwarové, či hardwarové úrovni.

Specifikací současné doby je celosvětově rozšířené používání moderních technologií snad ve všech aspektech života. Z tohoto důvodu si jen velmi těžko dokážeme představit, že by užívání moderních technologií absentovalo také v podnikových strukturách. Digitalizace podniků je významný přínosem, který zvyšuje efektivitu výroby a mimo jiné také umožňuje archivaci aktiv, respektive cenných informací i v jiné než tiskové podobě uložené ve skříni. Na výše uvedeném základě je tedy patrné, že samotná digitalizace má pozitivní aspekt na komplexní podnikovou strukturu, avšak s jejím rozšířením, a to konkrétně v souvislosti s internetovým připojením jednotlivých zařízení, také exponenciálně vzrostlo riziko kybernetických útoků, které podnikům hrozí. Stejně jako by měl mít podnik snahu ochránit svá aktiva v rámci fyzické bezpečnosti, tedy zejména učinit taková bezpečností opatření, jež by eliminovala, či snížila riziko přímého vniknutí pachatele do bezpečnostního perimetru, měl by přijmout také určitá bezpečnostní opatření v rámci informační bezpečnosti, a to právě na základě ICT bezpečnosti. Předmětnými opatřeními se rozumí například zajištění antivirové bezpečnosti podnikových sítí, bezpečné nakládání s hesly, řádné aktualizace, zajištění ochrany proti spywaru atd.

---

[52] DOUCEK, Petr. *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM*. 2., přeprac. vyd. Praha: Professional Publishing, 2011. ISBN n978-80-7431-050-8.

[53] Počítačová bezpečnost (Computer security) - ManagementMania.com. [online]. Copyright © 2011 [cit. 24.02.2022]. Dostupné z: https://managementmania.com/cs/pocitacova-bezpecnost

Současná doba je zejména v souvislosti s pandemií onemocnění Covid-19 spojována s rozmachem práce z domova (tzv. home office). I přes výše uvedené je stále potřeba zachování kontinuity v rámci řádné komunikace se zaměstnanci, kteří vykonávají své povolání právě prostřednictvím uvedeného způsobu. To však znamená zvýšení rizika kybernetického útoku spojeného s ohrožením podnikových aktiv, respektive cenných informací a o to větší opodstatnění v současné době ICT bezpečnost má.

2.2.2.1 Kybernetické útoky a jejich příklady

V souvislosti se současnou modernizací a vývojem nových technologií je spojována také problematika kybernetických útoků, které jsou nyní mnohem sofistikovanější, než kdy dříve byly. V rámci definice pojmu kybernetického útok se nám nabízí níže uvedené vysvětlení Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB):

„Kybernetickým útokem je jednání, které má za cíl způsobit škodu omezením či vyřazením služeb počítačových systémů z provozu, získání či podvržení dat v elektronické podobě bez autorizace nebo získání neautorizovaných práv na cizím počítačovém systému.“[54]

Vzhledem k současné době je nebezpečí kybernetického útoku vystaven každý uživatel internetu, tedy daná problematika s sebou nese riziko jak pro fyzické, tak i právnické osoby a vzhledem k závažnosti způsobených následků, je pro podnik žádoucí realizace ICT bezpečnosti v rámci své struktury. V souvislosti s kybernetickými útoky jsou podniky nejčastěji vystaveny níže uvedeným hrozbám:

[54] Národní úřad pro kybernetickou a informační bezpečnost - Doporučení pro případ napadení DDoS útokem - jak se zachovat a jak postupovat. Národní úřad pro kybernetickou a informační bezpečnost - Úvodní stránka [online]. Dostupné z: https://www.nukib.cz/cs/infoservis/doporuceni/1452-doporuceni-pro-pripad-napadeni-ddos-utokem-jak-se-zachovat-a-jak-postupovat/

Malware

V rámci počítačové terminologie považujeme malware za souhrnný název pro všechny typy škodlivého počítačového softwaru. V tomto souhrnném názvu se nachází celý výčet škodlivého softwaru, kdy se jedná například o trojské koně, počítačové viry, spyware atd. Ve většině případů je infikování počítače malwarem způsobeno nepozorností, či lehkomyslností jeho uživatele, který například otevře přílohu v nevyžádaném e-mailu, navštíví nezabezpečené stránky, nebo klikne na neznámý odkaz atd. Prostřednictvím uvedeného jednání malware spustí instalaci určitého škodlivého softwaru do počítačového systému. V závislosti na typu takto instalovaného škodlivého softwaru může dojít například k odepření přístupu ke kritickým součástem sítě, získání informací o uživateli, či podniku v rámci načtení dat z pevného disku, narušení systému, nebo způsobení nefunkčnosti systému.[55]

Z důvodu rozšířenosti malwaru by měl být každý uživatel obezřetný, a to jak v rámci internetového prostředí, tak i v dodržování bezpečnostních zásad na pracovišti, tedy by například neměl odcházet od počítače, na kterém zůstal přihlášen a takto jej nechat bez dozoru. Další alternativou, jak snížit riziko infikování počítače malwarem, jsou také řádné aktualizace operačního systému a aplikací v něm instalovaných. Mezi nejběžnější typy malwaru řadíme například následující škodlivý software[56]:

Počítačový virus

Počítačový virus je škodlivý software, jehož účelem je šíření sebe sama bez vědomí uživatele a následné ohrožení, poškození, či zničení dat uložených v počítači. V rámci infikování počítače virem dochází k jeho připojení k inicializační sekvenci a následné replikaci do jiných spustitelných souborů či dokumentů, čímž počítačový

[55]Slovníček pojmů | IST | České vysoké učení technické v Praze. IST | České vysoké učení technické v Praze [online]. Copyright © 2018 [cit. 24.02.2022]. Dostupné z: https://ist.cvut.cz/bezpecne-it/slovnicek-pojmu/

[56] Slovníček pojmů | IST | České vysoké učení technické v Praze. IST | České vysoké učení technické v Praze [online]. Copyright © 2018 [cit. 24.02.2022]. Dostupné z: https://ist.cvut.cz/bezpecne-it/slovnicek-pojmu/

virus infikuje další kód v počítačovém systému. Zpravidla se počítačové viry také mohou připojit ke spustitelnému kódu nebo se přidružit k souboru, a to vytvořením škodlivého souboru se stejným názvem, ale s příponou .com, či .exe, kdy tímto dochází k vytvoření spustitelného infikovaného souboru, který běžný uživatel bez použití například antivirového softwaru neodhalí. Ke svému šíření mimo infikovaný počítač je potřeba ve druhém počítači opět spustit instalační škodlivý soubor. K samotnému přenosu viru tedy ve většině případů dochází jeho přenesení prostřednictvím CD, DVD či počítačové sítě.

Trojské koně

Trojský kůň je software se škodlivými účely, jenž se ukrývá uvnitř užitečného programu. Na rozdíl od virů se trojský kůň nereplikuje a běžně se používá k vytvoření vzdáleného přístupu do systému, který je následně kybernetickými útočníky využíván k další záškodnické činnosti.

Počítačový červ

Počítačový červ je škodlivý software, který je na rozdíl od počítačového viru schopen samostatné replikace do dalších počítačových systémů a následného vzdáleného spuštění jeho tímto způsobem vytvořených kopií. Jedná tedy s určitou mírou nadsázky o autonomní software, který ke svému šíření již nepotřebuje úmyslné, či neúmyslné jednání ze strany uživatele. Počítačový červ se často do systému instaluje prostřednictvím e-mailových příloh a následně posílá svou kopii každému kontaktu v e-mailovém seznamu infikovaného počítače. Běžně se používají k přetížení e-mailového serveru a dosažení kybernetického útoku typu denial-of-service.

Ransomware

Dalším typem malwaru je ransomware, kdy se jedná o tzv. vyděračský škodlivý software, který po své instalaci do systému odepírá přístup k datům uživatele napadeného počítače a tohoto ve většině případů pod pohrůžkou zveřejnění, či

výmazu dat následně vydírá, kdy zpravidla žádá o zaplacení určité finanční hotovosti. Ransomware vstupuje do počítačového systému obdobně jako trojský kůň či počítačový červ. Pokročilý ransomware je využíván také v rámci tzv. kryptovirového vydírání, které zašifruje data napadeného počítače, které nelze dešifrovat bez dešifrovacího klíče. Uživatel napadeného počítače je poté kriptovirem vyrozuměn o potřebě zakoupení dešifrovacího klíče, který mu výše uvedeným způsobem znepřístupněná data opět odemkne.

Spyware

Spyware je typ škodlivého softwaru, jenž po jeho instalaci do systému napadeného počítače shromažďuje informace o uživatelích, jejich systémech, zvyklostech při prohlížení webových stránek, kdy následně získaná data odesílá vzdálenému uživateli. Kybernetický útočník poté může získané informace použít pro účely cílené reklamy, vydírání, nebo ke stažení a instalaci dalších škodlivých programů z webu. Významný rizikem pro uživatele napadeného počítače jsou poté výše uvedeným způsobem získaná hesla, přihlašovací údaje, nebo také čísla kreditních karet, kterými nyní kybernetický útočník disponuje.

Adware

Adware je typ škodlivého softwaru, který znepříjemňuje manipulaci s určitou aplikací, a to neustálým zobrazováním reklam ve formě bannerů, či vyskakujících oken. Adwarem je také často samovolně měněna domovská stránka internetového prohlížeče. Adware je zpravidla přidáván do bezplatných aplikací jejich samotnými vývojáři, kteří za zobrazování reklam financují vývoj předmětné aplikace.

Základní ochranu počítačových systémů proti malware poskytují například antivirové programy, kdy se jedná o počítačový software, jenž dokáže malware identifikovat a následně eliminovat. Jak již bylo předestřeno, význam ICT bezpečnosti v současné době v rámci podnikové struktury opodstatňuje jednak množství kybernetických

útoků, kterým jsou podniky vystaveny, tak jejich sofistikovanost. Níže je uveden výčet nejběžnějších typů kybernetických útoků[57]:

Phishing

Phishingové útoky jsou běžnou podvodnou technikou kybernetických útočníků, která zahrnuje rozesílání značného počtu podvodných e-mailů nic netušícím uživatelům, kdy se tyto e-maily více, či méně sofistikovaně prezentují jako pocházející z důvěryhodného a spolehlivého zdroje. Podvodné e-maily často vypadají jako legitimní, ale svého příjemce po kliknutí na v nich uvedený odkaz spojí se škodlivým souborem nebo skriptem, které jsou navrženy tak, aby kybernetickým útočníkům poskytl vzdálený přístup k zařízení napadeného uživatele. Předmětného vzdáleného přístupu kybernetičtí útočníci následně využijí k ovládnutí zařízení, shromažďování dat, instalaci škodlivých skriptů/souborů nebo k extrakci takových dat, jako jsou například informace o uživateli, informace o internetovém bankovnictví a další. Phishingové útoky mohou probíhat také prostřednictvím sociálních sítí a dalších online komunit, a to prostřednictvím přímých zpráv jiných uživatelů se skrytým záměrem. Kybernetičtí útočníci často využívají sociální inženýrství a další veřejné informační zdroje ke shromažďování informací o zaměstnání, zájmech, či aktivitách napadeného uživatele, kdy je tyto získané informace zvýhodňují při následných útocích. Phishingové útoky mohou probíhat také prostřednictvím telefonního hovoru (voice phishing) a prostřednictvím textové zprávy (SMS phishing).

[57] Jaké jsou nejčastější typy kybernetických útoků? – KYBEZ. KYBEZ – Platforma kybernetické bezpečnosti [online]. Copyright © [cit. 27.02.2022]. Dostupné z: https://www.kybez.cz/jake-jsou-nejcastejsi-typy-kybernetickych-utoku/

Man-in-the-Middle (MitM) útoky:

Předmětné útoky nastanou, když útočník zachytí komunikaci dvou stran a jako prostředník se do předmětné komunikace připojí. Ve většině případů je k provedení MitM útoků zneužito slabých míst v zabezpečení sítě, jako je například nezabezpečená veřejná WiFi. Z takto nezabezpečené sítě mohou kybernetičtí útočníci odcizit data a manipulovat s nimi přerušením provozu tím, že se vloží mezi zařízení uživatele a síť. Problém s daným druhem útoku je ten, že je velmi obtížně odhalitelný, jelikož si napadený uživatel myslí, že informace směřují na legitimní místo určení. Phishingové nebo malwarové útoky jsou často využívány k provedení útoku MitM.

Denial of Servise (DOS) útoky

Principem útoků DOS je zahlcení systémů, serverů nebo sítě, kdy toto vede k přetížení zdroje a odepření žádané služby. Předmětný výsledek znemožňuje systému zpracovávat a plnit legitimní požadavky. Kromě útoků typu denial of service (DoS) existují také distribuované útoky typu denial of service (DDoS – distributed denial of service). Útoky DoS saturují systémové prostředky s cílem bránit reakci na požadavky dané služby. Na druhou stranu je útok DDoS spuštěn z několika infikovaných hostitelských počítačů s cílem dosáhnout odmítnutí služby a odpojení systému, čímž se připraví cesta pro další útok, který vstoupí do sítě.

SQL injections

K tomuto napadení dochází, když kybernetický útočník vloží škodlivý kód na server pomocí jazyka SQL (Serves query language), čímž server donutí doručit mu chráněné informace. Tento typ útoku obvykle zahrnuje předchozí odeslání škodlivého kódu do nechráněného komentáře na webu nebo vyhledávacího pole. Účinným způsobem, jak zabránit SQL injections jsou postupy bezpečného kódování, jako je například použití připravených příkazů s parametrizovanými dotazy.

Zero day Exploit

Zero day Exploit se týká zneužití zranitelnosti nové, nebo nedávno oznámené sítě, a to před vydáním, či implementací opravy dané zranitelnosti, tedy například před vydáním opravné aktualizace. Prevence těchto útoků tedy vyžaduje neustálé monitorování, proaktivní detekci a agilní postupy v rámci správy hrozeb.

Útok prostřednictvím hesel

Hesla jsou nejrozšířenější metodou ověřování přístupu k zabezpečenému informačnímu systému, díky čemuž jsou atraktivním cílem pro kybernetické útočníky. Přístupem k heslu uživatele může útočník získat přístup k důvěrným nebo kritickým datům a systémům, a to včetně získání schopnosti s těmito daty a systémy manipulovat.

K identifikaci jednotlivých hesel používají kybernetičtí útočníci nespočet metod, a to včetně sociálního inženýrství, tedy manipulace osob s cílem získat konkrétní informace, či navedení těchto osob k provedení určité akce, získání přístupu k databázi hesel, testování síťového připojení k získání nezašifrovaných hesel, či prostým hádáním. Poslední zmíněná metoda se provádí systematickým způsobem známým jako „útok hrubou silou“. K útoku hrubou silou využívá útočník program, který zkouší všechny možné alternativy, tedy varianty a kombinace k uhádnutí hesla.

Cross-site Scripting (XSS)

Útok cross-site Scripting, tedy skriptování mezi weby, vkládá škodlivé kódy do obsahu ze spolehlivých webových stránek. Škodlivý kód se následně připojí k dynamickému obsahu, který je odeslán do prohlížeče napadeného uživatele. Obvykle se tento škodlivý kód skládá ze skriptovacího jazyka Javascript, který je spuštěn prohlížečem napadeného uživatele, ale taktéž může zahrnovat Flash, HTML. XSS a bývá útočníky využíván například u již zmíněného phishingu, kde je

právě díky cross-site Scripting uživateli vyobrazen odlišný obsah na jinak spolehlivé webové stránce.

Rootkity

Rootkity jsou nainstalovány uvnitř legitimního softwaru, kde mohou získat vzdálenou kontrolu a přístup k systému na úrovni správy. Kybernetický útočník poté pomocí rootkitu maskuje přítomnost veškerého škodlivého softwaru v napadeném systému, kdy se jedná například o počítačový virus, trojského koně atd. Rootkity zůstávají skryty v legitimním softwaru a vyčkávají na povolení uživatele, které danému softwaru umožní provádět změny v operačním systému, čímž se rootkit instaluje do systému a zůstane nečinný do té doby, než je útočníkem aktivován.

Útoky IoT

Zatímco připojení k internetu přes téměř všechna představitelná zařízení přináší jednotlivcům a společnostem komfort, představuje také rostoucí a téměř neomezený počet přístupových bodů, které mohou kybernetičtí útočníci zneužít. Vzájemná provázanost těchto zařízení umožňuje útočníkům prolomit vstupní bod a použít jej jako vstupní bránu ke všem zařízením připojených k dané síti. IoT útoky jsou stále populárnější kvůli rychlému růstu IoT zařízení a (obecně) nízké prioritě, která je dána implementovanému zabezpečení v těchto zařízeních a jejich operačních systémech. Mezi osvědčené postupy, které pomáhají předcházet útokům IoT, náleží aktualizace operačního systému a udržování silného hesla pro každé zařízení v IoT v síti a časté změny těchto hesel.

3 ZÁVĚR

Cílem předmětné práce bylo poukázání na současnou problematiku v rámci bezpečnosti podniku s uvedením možných hrozeb, kterým může být podnik vystaven a možnostem, formám a nástrojům, při jejichž užití mohou být dané hrozby částečně, či zcela eliminovány.

V první kapitole byla věnována pozornost zejména pojmu bezpečnosti jako takové, a to na základě její důležitosti v rámci této práce. Bezpečnost lze vnímat, či chápat na základě mnoha faktorů, které na člověka působí. Situace, či okolnost, jenž se některému jedinci jeví jako bezpečná, může odlišnému jedinci připadat jako krajně nebezpečná. Každý z nás jsme individualitou, a to způsobuje výčet mnohdy protichůdných postojů ve vnímání dané problematiky. Tento fakt umocňuje absence jedinečné definice pojmu bezpečnost v rámci platné legislativy, či literatury obecně. Jak již bylo předestřeno, protichůdné vnímání bezpečnosti není jen otázkou současné doby, což potvrzuje skutečnost, že samotná bezpečnost se stala předmětem zkoumání bezpečnostních studií, kterým je v rámci první kapitoly rovněž věnována pozornost. V kontextu s cílem předmětné práce tedy byly představeny definice bezpečnosti, které se nejblíže přibližují vnímání bezpečnosti z pohledu podniku, jenž v rámci své struktury aspiruje o její zajištění.

V rámci druhé kapitoly byla soustředěna pozornost na komplexní problematiku řízení bezpečnosti v podniku, která byla z důvodu jejího rozsahu rozdělena do jednotlivých podkapitol. Řízení bezpečnosti je v souvislosti se současnými podmínkami natolik významné, že samozřejmě s ohledem na finanční možnosti podniku a po vyhodnocení míry rizika, kterému jsou jeho aktiva vystaveny, lze podnikům doporučit zaměstnání specializovaného pracovníka na pozici manažera bezpečnosti. Pracovní náplní manažera bezpečnosti je odpovědnost za plánování rozvoje bezpečnosti podniku, realizace analýzy bezpečnosti, stanovení strategie a bezpečnostní politiky v podniku a samozřejmě také sledování aktuálních trendů

v rámci možného zabezpečení. Podnikům, pro něž by se přijetí uvedeného opatření jevilo jako neefektivní, bylo v rámci řízení bezpečnosti doporučeno konzultovat danou problematiku s externími poradci, či společnostmi, které předmětné poradenství poskytují.

Jedním z klíčových okruhů řízení bezpečnosti je fyzická bezpečnost, které byla věnována samostatná podkapitola. Předmětná problematika se zabývá snížením míry rizika hrozícího podniku v souvislosti s antropogenními, či naturogenními hrozbami, a to s ohledem na hrozby současné. Uvedená podkapitola byla dále členěna v závislosti na formu jednotlivých ochran, respektive na ochranu klasickou, technickou, fyzickou a režimovou, které byly blíže specifikovány, a to včetně konkrétních možností, které může podnik v rámci zajištění své bezpečnosti využít. Z uvedeného vyplynula skutečnost, že ideálním řešením fyzické bezpečnosti podniku je kombinace bezpečnostních prvků jednotlivých forem ochran, které ve vzájemném kontextu disponují doplňujícím charakterem. Z důvodu zajištění bezpečnosti podniku, respektive jeho zdrojů, mezi něž náleží také zdroje lidské, byla v rámci členění fyzické bezpečnosti věnována pozornost také bezpečnosti a ochraně zdraví při práci.

Druhým klíčovým okruhem řízení bezpečnosti byla v rámci předmětné práce definována informační bezpečnost, při jejíž realizaci bylo podnikům doporučeno tuto koncipovat jak na organizační, tak technologické úrovni. Informační bezpečnost nabyla svého současného významu zejména v souvislosti s vývojem moderních technologií a s tím spojenou digitalizací podniků, kdy je mnoho podniků vystaveno riziku ztráty, odcizení, či zneužití jejich aktiv, a to především informací a dat. Vzhledem ke komplexnosti informační bezpečnosti byla tato členěna do jednotlivých podkapitol. V souvislosti se zajištěním bezpečnosti podniku v dané problematice byla doporučena implementace systému řízení bezpečnosti informací a s ohledem na finanční možnosti daného podniku také zaměstnání specializovaného manažera informační bezpečnosti, či spolupráce s externími poradci. V podkapitole ICT

bezpečnost byla věnována pozornost riziku spojenému s kybernetickými útoky, které jsou závažným rizikem současné doby. Předmětné riziko navyšuje skutečnost, že z důvodu pandemie onemocnění Covid-19 mnoho podniků přistoupilo k práci jejich zaměstnanců vykonávané z domova, a to mnohdy bez adekvátního zabezpečení případné elektronické komunikace. Na základě uvedeného byla doporučena určitá bezpečnostní opatření, a to například zajištění antivirové bezpečnosti podnikových sítí, bezpečné nakládání s hesly, řádné aktualizace, zajištění ochrany proti spywaru atd. V rámci závažnosti kybernetických útoků jejichž sofistikovanost narůstá v souvislosti s vývojem moderních technologií byla poslední podkapitola věnována právě výčtu škodlivého malwaru, se kterým se podnik v rámci kybernetického útoku může setkat a také možným způsobům jejich provedení.

SEZNAM POUŽITÉ LITERATURY:

1) BUZAN, Barry, Ole WAEVER a Jaap de WILDE. *Bezpečnost: nový rámec pro analýzu*. Brno: Centrum strategických studií, 2005. Současná teorie mezinárodních vztahů. ISBN 80-903333-6-2.

2) DOUCEK, Petr. *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM*. 2., přeprac. vyd. Praha: Professional Publishing, 2011. ISBN n978-80-7431-050-8.

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

4) EICHLER, Jan. Bezpečnostní studia. In ZEMAN, Petr, ed. *Česká bezpečnostní terminologie: výklad základních pojmů*. Brno: Masarykova univerzita, Mezinárodní politologický ústav, 2002. ISBN 80-210-3037-2.

5) GALVAS, Milan. *Pracovní právo*. 2., doplněné a přepracované vydání. Brno: Masarykova univerzita, 2015. ISBN 978-80-210-8021-8.

6) IVANKA, Ján. *Mechanické zábranné systémy*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2010. ISBN isbn978-807-3189-105.

7) KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88168-31-7.

8) KROUPOVÁ, Libuše, FILIPEC, Josef, ed. *Slovník spisovné češtiny pro školu a veřejnost: s Dodatkem Ministerstva školství, mládeže a tělovýchovy České republiky*. Vyd. 4. Praha: Academia, 2005. ISBN 80-200-1347-4.

9) KYNCL, Jaromír. Bezpečnost objektu ve světle moderních technologií. Praha: Komora podniků komerční bezpečnosti České republiky, 2014. ISBN 978-80-260-7115-0.

10) LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management*. Zlín: Radim Bačuvčík - VeRBuM, 2015. ISBN 978-80-87500-05-7.

11) SAK, Petr. *Úvod do teorie bezpečnosti: nekonvenční pohledy na minulost, přítomnost a budoucnost lidstva*. [Praha]: Petrklíč, 2018. ISBN 978-80-7229-652-1.

12) UHLÁŘ, Jan. *Technická ochrana objektů*. Praha: Vydavatelství PA ČR, 2000. ISBN isbn80-7251-046-0.

13) UHLÁŘ, Jan. *Technická ochrana objektů*. 2. vyd. Praha: Policejní akademie České republiky v Praze, 2009. ISBN 978-80-7251-312-3.

14) WAISOVÁ, Šárka. *Bezpečnost: vývoj a proměny konceptu*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. Politologické učebnice. ISBN 80-86898-21-0.

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

Webové stránky a elektronické zdroje:

1) Bezpečnost a ochrana informací (Security and Protection of Information) - ManagementMania.com. [online]. Copyright © 2011 [cit. 23.02.2022]. Dostupné z: https://managementmania.com/cs/bezpecnost-a-ochrana-informaci

2) CISO (Chief Information Security Officer) - Manažer informační bezpečnosti - ManagementMania.com. [online]. Copyright © 2011 [cit. 18.02.2022]. Dostupné z: https://managementmania.com/cs/ciso-chief-information-security-officer-manazer-informacni-bezpecnosti

3) CSO (Chief Security Officer) - ManagementMania.com. [online]. Copyright © 2011 [cit. 18.02.2022]. Dostupné z: https://managementmania.com/cs/cso-chief-security-officer

4) Fyzická bezpečnost (Physical Security) - ManagementMania.com. [online]. Copyright © 2011 [cit. 18.02.2022]. Dostupné z: https://managementmania.com/cs/fyzicka-bezpecnost

5) ISO 27000 - ManagementMania.com. [online]. Copyright © 2011 [cit. 23.02.2022]. Dostupné z: https://managementmania.com/cs/iso-27000

6) ISO 27001 Systém managementu bezpečnosti informací - ManagementMania.com. [online]. Copyright © 2011 [cit. 24.02.2022]. Dostupné z: https://managementmania.com/cs/iso-27001

7) Jaké jsou dostatečné investice do kybernetické bezpečnosti? - CIO Business World. CIO Business World [online]. Copyright © 2020 [cit. 17.02.2022]. Dostupné z: https://www.cio.cz/clanky/jake-jsou-dostatecne-investice-do-kyberneticke-bezpecnosti/

8) Jaké jsou nejčastější typy kybernetických útoků? – KYBEZ. KYBEZ – Platforma kybernetické bezpečnosti [online]. Copyright © [cit. 27.02.2022]. Dostupné z: https://www.kybez.cz/jake-jsou-nejcastejsi-typy-kybernetickych-utoku/

9) Národní úřad pro kybernetickou a informační bezpečnost - Doporučení pro případ napadení DDoS útokem - jak se zachovat a jak postupovat. Národní úřad pro kybernetickou a informační bezpečnost - Úvodní stránka [online]. Dostupné z: https://www.nukib.cz/cs/infoservis/doporuceni/1452-doporuceni-pro-pripad-napadeni-ddos-utokem-jak-se-zachovat-a-jak-postupovat/

10) Počítačová bezpečnost (Computer security) - ManagementMania.com. [online]. Copyright © 2011 [cit. 24.02.2022]. Dostupné z: https://managementmania.com/cs/pocitacova-bezpecnost

11) Režimová ochrana :: Bezpečnostní poradenství JŠ. Bezpečnostní poradenství JŠ [online]. Copyright © 2015 Všechna práva vyhrazena. [cit.

22.02.2022]. Dostupné z: https://www.bp-js.cz/fyzicka-ochrana/rezimova-ochrana/

12) Řízení bezpečnosti (Security Management) - ManagementMania.com. [online]. Copyright © 2011 [cit. 17.02.2022]. Dostupné z: https://managementmania.com/cs/rizeni-bezpecnosti

13) Slovníček pojmů | IST | České vysoké učení technické v Praze. IST | České vysoké učení technické v Praze [online]. Copyright © 2018 [cit. 24.02.2022]. Dostupné z: https://ist.cvut.cz/bezpecne-it/slovnicek-pojmu/

14) ÚNMZ – ÚŘAD PRO TECHNICKOU NORMALIZACI, METROLOGII A STÁTNÍ ZKUŠEBNICTVÍ [online]. Copyright © [cit. 18.02.2022]. Dostupné z: https://www.unmz.cz/files/Sborn%C3%ADky%20TH/DEF_TNI-2-A4%20-%20pro%20www.pdf

15) 110/2019 Sb. Zákon o zpracování osobních údajů. Zákony pro lidi - Sbírka zákonů ČR v aktuálním konsolidovaném znění [online]. Copyright © AION CS, s.r.o. 2010 [cit. 23.02.2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/2019-110

16) 119/2002 Sb. Zákon o střelných zbraních a střelivu. Zákony pro lidi - Sbírka zákonů ČR v aktuálním konsolidovaném znění [online]. Copyright © AION CS, s.r.o. 2010 [cit. 22.02.2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/2002-119

17) 141/1961 Sb. Trestní řád. Zákony pro lidi - Sbírka zákonů ČR v aktuálním konsolidovaném znění [online]. Copyright © AION CS, s.r.o. 2010 [cit. 22.02.2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/1961-141

18) 262/2006 Sb. Zákoník práce. Zákony pro lidi - Sbírka zákonů ČR v aktuálním konsolidovaném znění [online]. Copyright © AION CS, s.r.o. 2010 [cit. 22.02.2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/2006-262

19) 273/2008 Sb. Zákon o Policii ČR. Zákony pro lidi - Sbírka zákonů ČR v aktuálním konsolidovaném znění [online]. Copyright © AION CS, s.r.o. 2010 [cit. 22.02.2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/2008-273