Bezpečnostní politika podniku

Karel Minichbauer

Bakalářská práce
2021

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav bezpečnostního inženýrství

Akademický rok: 2020/2021

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Karel Minichbauer**
Osobní číslo:	**A16674**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**Kombinovaná**
Téma práce:	**Bezpečnostní politika podniku**
Téma práce anglicky:	**Security Policy in Company**

Zásady pro vypracování

1. Seznamte se s pojmem bezpečnostní politika podniku
2. Stanovte klíčové oblasti bezpečnosti podniku
3. Vysvětlete souvislost GDPR s bezpečnostní politikou
4. Popište strukturu bezpečnostní politiky
5. Demonstrujte návrh struktury na modelovém příkladu

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

Seznam doporučené literatury:

1. NONNEMANN, František. Příručka pověřence pro ochranu osobních údajů. Praha: Klika, 2018. ISBN 978-80-88298-10-6.
2. NULÍČEK, Michal. GDPR – obecné nařízení o ochraně osobních údajů. 2. vydání. Praha: Wolters Kluwer, 2018. ISBN 978-80-7598-068-7.
3. KOLOUCH, Jan a Pavel BAŠTA. CyberSecurity. Praha: CZ.NIC, z.s.p.o., 2019. ISBN 978-80-88168-31-7.
4. MLÝNEK, Jaroslav. Zabezpečení obchodních informací. Brno: Computer Press, c2007. ISBN 978-80-251-1511-4.
5. KINDL, Jiří. Projektování bezpečnostních systémů. Zlín: Univerzita Tomáše Bati ve Zlíně, 2004. ISBN 80-7318-165-7.
6. UHLÁŘ, Jan. Technická ochrana objektů. Praha: Vydavatelství PA ČR, 2001. ISBN 80-7251-076-2.

Vedoucí bakalářské práce: **Ing. Lukáš Králík**
Ústav počítačových a komunikačních systémů

Datum zadání bakalářské práce: **23. července 2021**
Termín odevzdání bakalářské práce: **20. srpna 2021**

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
DĚKAN
L.S.

doc. Mgr. Milan Adámek, Ph.D. v.r.
děkan

Ing. Jan Valouch, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 15. ledna 2021

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně, dne …….

podpis studenta

ABSTRAKT

Bakalářská práce je zaměřena na problematiku bezpečnostní politiky firem. Popisuje základní principy analýzy rizik a zásady pro tvorbu důležitých firemních dokumentů jako je dokument „Bezpečnostní politika“.

Klíčová slova: Bezpečnostní politika, hrozba, riziko, opatření, podnik

ABSTRACT

Bachelor thesis is focused on the security policies of companies. It describes the basic principles of risk analysis and principles for the creation of important company documents such as the document "Safety Policy".

Keywords: Security police, therat, risk, measuer, business, company

Rád bych poděkoval:

Panu Ing. Lukášovi Králíkovi za vedení mé bakalářské práce, za jeho vstřícný přístup, a hlavně za jeho trpělivost v době korona virové krize. Dále bych chtěl poděkovat Ing. Jiřímu Minichbauerovi a celé mé rodině za cenné rady a podporu při dokončování mé práce a celého studia. V neposlední řadě bych chtěl poděkovat Bc. Romaně Novákové za korekci mé práce a její rady.

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

OBSAH

ÚVOD

V každé oblasti podnikání jsou v dnešní době zaměstnavatelé a firmy vystavovány velkému množství rizik, které mohou ohrozit jak chod celého podniku, tak zdraví zaměstnanců. Z těchto důvodů se budou bezpečnostní rizika zásadně lišit podle zaměření podniku.

Každá firma má určitým způsobem specifickou oblast podnikání. Od toho se odvíjí obsah bezpečnostní politiky. Jiná bude bezpečnostní politika firmy, která se zabývá internetovým obchodem a jiná bude u firmy zabývající se autodopravou.

V této práci se budu zabývat firmou Soukromá Škola Hostivař sídlící na Praze 10. Z předmětu podnikání vyplývá, že je nutné chránit jak firmu, tak její zákazníky před únikem citlivých informací jako jsou například informace o klientech a v případě školy jde zejména o osobní údaje, proto je nutné zpracovat dokumenty, které deklarují bezpečnost podniku a zajistit tak bezpečí dat svěřených podniku. Tento dokument se nazývá „Bezpečnostní politika“.

Bezpečnostní politika řeší hrozby, které mohou vzniknout během chodu podniku a rizika z nich vyplývající. Obsahuje také opatření, kterými se snaží rizikům předejít, minimalizovat je, či je zcela potlačit. Celou touto problematikou se bude tato práce zabývat a popisovat jí ve dvou částech.

V první teoretické části se tato bakalářská práce bude zabývat bezpečnostní politikou podniků (dále jen BPP), kde si popíšeme klíčové oblasti této problematiky. V druhé praktické části bude přiblížena analýza rizik výše zmíněného podniku a identifikace jeho zranitelných oblastí. Z těchto výsledků analýzy rizik pak sestavíme ukázku dokumentu Bezpečnostní politika.

I. TEORETICKÁ ČÁST

1 BEZPEČNOSTNÍ POLITIKA

Každý podnik bez ohledu na svou velikost a předmět podnikání by měl dodržovat určité bezpečnostní zásady. Tyto zásady vycházejí z vnitřních směrnic a bezpečnostních politik každé jednotlivé organizace. Bezpečnostní zásady jsou sepsány v jednom z nejdůležitějších dokumentů každého podniku, a to v dokumentu „Bezpečnostní politika (Security Policy)“.

Bezpečnostní politiku jako vnitřní předpis podniku nejčastěji doplňují ještě další interní předpisy podniku. Jedním z takových dokumentů je např. Provozní řád informačního systému, který je většinou součástí dokumentů, kterými se řídí bezpečnost podniku. Souhrn těchto dokumentů obsahuje pravidla, kterými se musí podnik ve vlastním zájmu řídit, aby byl zajištěn jeho bezpečný chod.[1]

Nejvyšším stupněm důvěrnosti vůči svým klientům, kterého mohou firmy dosáhnout z hlediska bezpečnosti je norma ISO/IEC 27001. Což je mezinárodně platný standard, který určuje, jaké požadavky musí systém bezpečnosti informací splňovat. Jedná se zejména o řízení bezpečnosti důvěry informací pro zaměstnance, procesy, IT systémy a strategii firmy. Normu určuje mezinárodní organizace pro normalizaci. Tato norma se doporučuje pro podniky veřejné správy, softwarové firmy, telekomunikační operátory a další. [2] Pokud by podniky nedodržovaly ustanovená pravidla, které plynou z dokumentu „Bezpečnostní politika“ či v případě, že by podnik vlastnil certifikát ISO a nedodržoval by ustanovení, která jsou v normě uvedena, mohlo by takovéto počínání vést až k jeho zániku a to zejména proto že by se mohl stát pro své klienty nedůvěryhodným či by se mohl stát terčem průmyslové špionáže na kterou nebude připraven. Z výše uvedeného tedy vyplývá, že je v zájmu každého podniku zajistit dodržování všech pravidel uvedených v jeho „Bezpečnostní politice“ a dalšími dokumenty, které jsou k tomuto dokumentu přidruženy. Dodržováním těchto pravidel se minimalizují dopady takzvaných incidentů.[3] Incidenty můžeme kategorizovat dle oblastí ve kterých vznikly [4]:

- **Bezpečnostní incidenty**
  situace, při které došlo k ohrožení bezpečnosti informací (krádež, vloupání, fyzický útok či útok hackera).
- **Incidenty kvality**
  dochází ke snižování kvality služeb (Porucha či rozladění výrobní linky, chyba algoritmu).

- **Incidenty týkající se zdraví**

  incident, při kterém dojde k poranění jednoho a více zaměstnanců či klientů v prostorách podniku (úraz na pracovišti, epidemie)

- **Incidenty týkající se poskytovaných služeb**

  situace ve které podnik nemůže poskytovat služby pro své klienty, způsobená jak chybou zaměstnance, tak poruchou podnikového stroje (výpadek proudu)

K zamezení těchto incidentů slouží právě již zmiňovaný dokument „Bezpečnostní politika“. Tento dokument obsahuje následující body[4]:

- Působnosti a platnosti nastavené bezpečnostní politiky,
- Fyzickou a objektovou ochranu,
- Bezpečnost zaměstnanců,
- Informační bezpečnost,
- Odpovědnosti pracovníků.

Při zpracování výše uvedených bodů zájmu bezpečnosti podniku do dokumentu „Bezpečnostní politika“ je zapotřebí postupovat tak aby byly pokryty veškeré kritické body daného podniku dle jeho oboru podnikání, nejčastěji se dokument skládá z těchto bodů[4]:

- **Úvodní ustanovení**

  První část, Úvodní ustanovení, obsahuje základní popis podniku a jeho informačních systémů a slouží k vymezení základních bezpečnostních cílů (například předpokládaný rozsah zpracování důvěrných informací, definice struktury informačního systému, jako jsou počítače či síťové prvky, počet uživatelů systému) [4]

- **Personální bezpečnost**

  Tato část dokumentu se zabývá především základními požadavky na stávající i nové pracovníky, kteří jsou nedílnou součástí podniku. Patří sem zejména vzdělávání, způsobilost k výkonu dané práce, odborná školení, pravidelná doškolování pracovníků jako je např. hlášení bezpečnostních incidentů, bezpečnostní školení informací – upozornění na možné hrozby phishingu či pharmingu, jakým způsobem může dojít k těmto hrozbám a co v takovém případě dělat. atd. [4]

- **Počítačová bezpečnost**

  V části Počítačová bezpečnost, dokument uvádí minimální rozsah požadavků a kroků, které je potřeba udělat k zabezpečení počítačové sítě daného podniku. Tento souhrn požadavků vychází z § 7 a 8 vyhlášky č. 523/2005 Sb. Jinými slovy se v této části dokumentu budeme zabývat např. autorizací a autentizací pracovníků pro přihlášení do podnikové sítě, zabezpečením portů před neoprávněným vniknutím do podnikové sítě zvenčí či ochranou utajovaných informací. Jedná se zejména o níže uvedené typy ochran.[4]

  - **Kryptografická ochrana**

    Část Kryptografické ochrany je zařazována pouze v případě, pokud je využíván v podnikovém informačním systému nějaký certifikovaný kryptografický prostředek podle zákona č. 412/2005 Sb. [4]

  - **Fyzická bezpečnost**

    Část Fyzická bezpečnost upravuje a definuje jakým způsobem je řešena fyzická bezpečnost v daném podniku, v souladu s vyhláškou a zákonem o fyzické bezpečnosti a certifikaci technických prostředků, ve znění vyhlášky č. 19/2008 Sb. a vyhlášky č. 454/2011 Sb., a § 20 vyhlášky č. 523/2005 Sb. [4]

  - **Administrativní bezpečnost**

    Tato část dokumentu Bezpečnostní politika řeší administrativní bezpečnost dle vyhlášky č. 529/2005 Sb. (například evidenci a autorizaci administrativních a evidenčních pomůcek či další dokumentaci). [4]

- **Řízení a plánování kontinuity**

  Tato část obsahuje popis, jak je v podniku řešeno a zajištěno řízení kontinuity v krizových situacích (například krizové situace, havarijní plány a řešení bezpečnostních incidentů). [4]

- **Další bezpečnostní dokumentace**

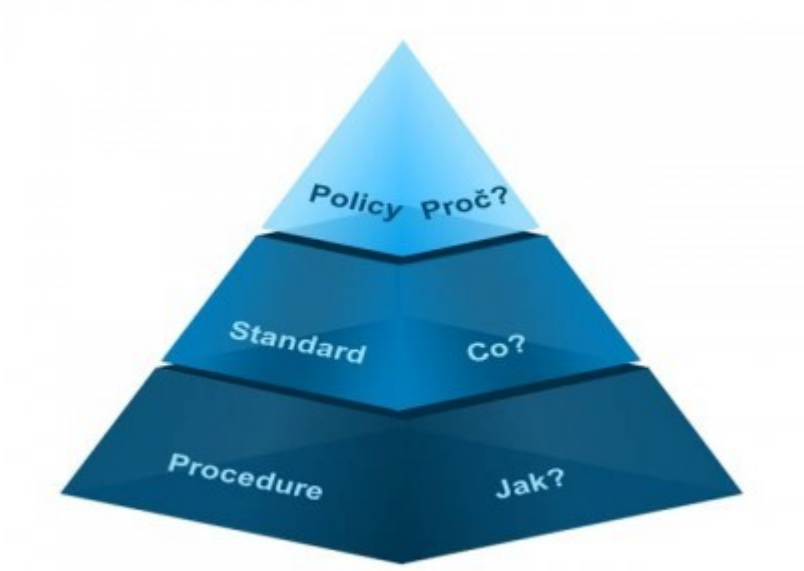
  V této části bezpečnostní politiky je uveden způsob analýzy rizik a opatření v souladu s bezpečnostními požadavky. Dokument „Bezpečnostní politika“ nemusí být jediným dokumentem, který můžeme deklarovat a využívat. Pro zabezpečení informací a chodu podniku se velmi často využívají tři druhy dokumentů spadající do bezpečnostní

politiky celé firmy, a to bezpečnostní politika, standard a postup. Dle normy ISO 9000 nesmí byt tyto dokumenty sloučeny do jednoho. [4]

Další dokumenty rozšiřující bezpečnostní politiku:

- **Bezpečnostní standard** je dokument, upřesňující požadavky uvedené v Bezpečnostní politice. V tomto dokumentu by měly být definovány požadavky na výkon různých prací, například bezpečné zacházení s pracovními nástroji, či jak silné by si měl uživatel nastavit heslo od svého podnikového účtu nebo jak zacházet s magnetickými médii na kterých jsou uloženy důvěrné informace. [5]
- **Bezpečnostní postup** je dokument, popisující přesně, krok za krokem, jak provádět určitou činnost. Důležité je, aby každý proces byl velmi konkrétně popsán a aby minimalizoval riziko chyby například při výrobním postupu, či při práci s informačními systémy. [5]

U obou výše uvedených dokumentů musí být jasně zaznamenáno kdo a kdy daný dokument schválil a kdo zodpovídá za jeho plnění. Každý dokument musí obsahovat datum schválení a datum účinnosti. Stejně jako platí doporučení, že by všechny dokumenty týkající se bezpečnostní politiky měly být jasně a srozumitelně formulovány s použitím striktně příkazových a zákazových formulí (musí/ nesmí) a to zejména z toho důvodu, aby byly lehko zapamatovatelné a srozumitelné všem zaměstnancům, pro které tyto bezpečnostní dokumenty platí. [5]



Obrázek 1: Grafické znázornění významu dokumentů [5]

Každá firma si bezpečnostní politiku vytváří dle svého zaměření. Odlišné body zájmu, pro které podnik bude tvořit svou bezpečnostní politiku např. podnik zabývající se vývojem softwaru, podnik zabývající se výrobou nějakého produktu i supermarket. Představíme si ty nejpoužívanější z nich.

2 OBJEKTOVÁ BEZPEČNOST

Jedním z důležitých bodů zájmu bezpečnostní politiky je objektová bezpečnost. Tento bod by se měl nacházet v každé firmě.

- **Mechanická ochrana**: je zajištění objektů pomocí mechanických zábranných systémů, zamezujících narušiteli vniknout do objektu a poškodit či odcizit ceniny či vybavení podniku uložené v něm. K mechanickému zabezpečení jsou použity například dveře, okna, ploty, závory, brány a mnoho dalších.[6]
- **Režimová opatření**: týká se zejména činnosti pracovníků v objektu, činnosti a pohybu osob přicházejících zvenčí, můžeme je rozdělit do dvou kategorií režimových opatření:
  1. vnější (řeší pohyb osob směrem dovnitř chráněného prostoru ale i ven. Typickým příkladem může být firma Amazon, kontrolující své zaměstnance při vstupu a výstupu do skladových prostor podniku ve snaze zamezit svým zaměstnancům odcizit produkty, se kterými podnik obchoduje).
  2. vnitřní (zabývá se zejména pohybem osob uvnitř chráněného objektu, k zajištění jejich bezpečí a zamezení úniku informací skrze vlastní lidi).
- **Fyzická ochrana**: zájmový objekt je střežen strážným, který má za úkol dohlédnout na to, aby do objektu nevstupovaly nepovolané osoby. Technická ochrana: společně s fyzickou ochranou tvoří základní zabezpečení objektu s celkem vysokou spolehlivostí. Do technické ochrany patří zejména elektronické prvky bezpečnosti jako jsou různá poplachová zařízení, CCTV kamery a vstupní systémy.[6]

3 BEZPEČNOST A OCHRANA ZDRAVÍ PŘI PRÁCI

Důležitým bodem zájmu chránícím jak zaměstnance před pracovními úrazy, tak i podnik před případným soudním sporem mezi ním a zaměstnancem. Úkolem BOZP je předcházet ohrožení nebo poškození lidského zdraví při výkonu práce. Jedná se o soubor pravidel, která jsou dána legislativním rámcem. Nejdůležitějším zákonem z pohledu BOZP je zákon č. 262/2006 Sb. Zákoník práce. Jako další zásadní předpis můžeme zmínit zákon č. 309/2006 Sb. O zajištění dalších podmínek BOZP. Oblastí BOZP se dále zabývá další 104 zákonů a vyhlášek. BOZP se upravuje pomocí dokumentu, který spadá pod Bezpečnostní politiku podniku. Ten zaměstnanec podepisuje v den prvního nástupu na pracoviště, většinou se tak děje v den uzavření pracovní smlouvy [7].

Každý dokument BOZP musí splňovat následující body [8]:

- identifikace a vyhodnocení rizik BOZP vč. následných opatření,
- zpracování dokumentace ke kategorizaci prací,
- zpracování směrnice pro poskytování OOPP, čistících a dezinfekčních prostředků,
- součinnost při řešení a evidenci pracovních úrazů, dodání knihy úrazů,
- zpracování traumatologického plánu vč. plánu první pomoci,
- účast při kontrolách oprávněných orgánů (OIP, HZS apod.),
- zpracování směrnice pro provozování dopravy,
- zpracování provozních řádů,
- zpracování dokumentace pro manipulaci a skladování,
- zpracování další dokumentace BOZP podle typu organizace.

4 POŽÁRNÍ OCHRANA

Požární ochrana je další z nezanedbatelných bodů bezpečnostní politiky. Jedná se o seznam pravidel a opatření k ochraně majetku a osob v případě vzniku požáru. Součástí požární ochrany bývá i seznam pravidel, jak požáru předejít [9]. Požární ochrana v podniku se řídí zákonem č. 133/1985 Sb. o požární ochraně [10].

Každý dokument PO musí splňovat následující body:

- začlenění činností do kategorie podle požárního nebezpečí,
- zpracování organizační směrnice požární ochrany,
- zpracování požární knihy,
- zpracování evakuačního plánu (grafická i textová podoba),
- vypracování dokumentace dle stupně PN (požární řády, organizace apod.),
- zpracování další dokumentace PO podle typu organizace.

5 ZÁSADY KYBERNETICKÉ BEZPEČNOSTI

Hrozby v oblasti kybernetické bezpečnosti rostou každý den a není dne, kdy bychom neslyšeli nové zprávy o kybernetickém útoku nebo krádeži dat. Ti kteří, vlastní nebo řídí malé a střední podniky vědí, že kybernetická bezpečnost je důležitá a že je jí nutné věnovat velkou pozornost. Každý podnik by si měl stanovit body kterými se bude při ochraně dat řídit. [11]

5.1 Zranitelnost infrastruktury podniku

Identifikovat nejdůležitější data podniku je prvním krokem k správnému nastavení zásad kybernetické bezpečnosti. Mohou jimi být údaje o zákaznících a zaměstnancích, finanční informace, ale i zdrojové kódy programů, firemní know-how apod. Je zapotřebí si uvědomit kam všechna tato data ukládáme a jaké je jejich zabezpečení. Jakmile získáme odpovědi na tyto otázky, měli bychom přemýšlet o rizicích, kterým jsou data podniku vystavena. [12]

5.2 Ochrana firemních zařízení

První krok, který zajistí, že systémy nejsou zranitelné vůči kybernetickým útokům, jsou vždy aktuální verze softwaru. [11]

- Ochrana před viry V současné době je zapotřebí investovat do antivirových programů. A to z důvodu ochrany podnikových zařízení před Malware jako jsou např. viry, červy či vyděračský a velice nebezpečný Ransomware. Tyto viry jsou nejvíce používány k napadení malých a středních podniků a to zejména z důvodu, že mnoho podniků podcení nákup kvalitního antivirového programu. (Kompletní průvodce kybernetickou bezpečností pro malé a střední firmy, 2020).[11]
- Aktualizace softwaru V zájmu bezpečnosti informačního systému společnosti je, aby veškerý software instalovaný na zaměstnaneckých počítačích, ale i na firemních serverech a routerech byl pravidelně aktualizován. Tento krok je velmi důležitý, zejména kvůli faktu, že firmy, které software vyrábějí vydávají, odstraňují nedostatky ve svých algoritmech, ty mohou představovat velké bezpečnostní riziko. Příkladem může být třeba firma Microsoft Inc., která průběžně vydává bezpečnostní

balíčky pro svoje produkty, zrovna tak i firma Cisco dodávající hardware pro chod firemní infrastruktury a mnoha dalších. Dalším příkladem toho, proč není radno aktualizace software podceňovat je případ u protokolu IEEE 802.11 (wifi) s názvem KRACK [13], na který museli reagovat všichni výrobci telefonů, notebooků, počítačů a ostatních síťových prvků. Musí být nastaven způsob instalace software a jeho aktualizací a zároveň musí být k této činnosti určen zodpovědný zaměstnanec. [11]

- Nastavení brány firewall Napomáhá zabezpečit firemní počítače a servery, jejím správným nastavením lze útočníkům blokovat přístupy na otevřené porty počítače, zamezit, aby škodlivý program "virus" odeslal data z podnikového počítače k útočníkovi. [11]

5.3 Ochrana firemních údajů

- Uživatelské účty K minimalizaci úniku dat z podniků je třeba určit jaké oprávnění zaměstnancům udělíme a ke kterým datům. Popřípadě do kterých částí firemního informačního systému bude mít zaměstnanec přístup. Obecně platí pravidlo, že zaměstnanec by měl mít přístup pouze k informacím a datům nezbytným k výkonu jeho práce. [14]
- Ochrana a oddělení bezdrátových a počítačových sítí Při tvorbě bezpečnostních sítí bychom měli vytvořit vždy minimálně dvě na sobě nezávislé sítě.
    - Interní síť je síť, ve které jsou připojeny pouze pracovní počítače zaměstnanců a jiná firemní zařízení jako jsou (např. tiskárny, servery a další různá zařízení potřebná pro chod podniku).
    - Síť návštěvníků je síť oddělená od interní a slouží pro připojení například návštěv, či připojení soukromých zaměstnaneckých zařízení k internetu). [9]

6 DOPADY LIDSKÉHO FAKTORU

Z pohledu bezpečnosti informací velmi mnoho malých a středních podniků podceňuje takzvanou vnitřní hrozbu[15].

Firma může přijít o citlivé údaje o zákazníkovi, nebo o svoje know-how, nebo je útočník může jen využít ve svých cílech, aniž by postižený podnik věděl, že došlo k úniku citlivých dat. Přestože podnik investuje nemalé finanční prostředky do zabezpečení a snaží se držet krok s nejmodernějšími technologiemi v této oblasti, může docházet k úniku citlivých informací. Ačkoliv jsou zabezpečovací systémy velice sofistikované, je nutné si uvědomit, že vznikly až poté, co byla použita konkrétní metoda napadení, tudíž sebelepší zabezpečovací systémy nedokáží ochránit před novými typy hrozeb. [16] Dá se říct, že hackeři jsou vždy o krok napřed. K využití nových metod napadení ze sítě dochází zejména u velkých korporací a firem, kde si hackeři mohou přijít na velmi vysokou finanční odměnu za získané informace [16].

Největší riziko úniku citlivých informací v podnicích však nepředstavují hackeři, ale samotní zaměstnanci. Člověk je de-facto nejslabší článek sebelepšího zabezpečovacího systému a bez vhodné osvěty se zaměstnanci dopouštějí mnoha chyb, které mohou vést ke vzniku nepříjemných situací. Některé z nich vám zde uvedu na základě mých poznatků z kurzu https://www.securityjourney.com/ který jsem zatím absolvoval do třetího levelu s certifikaci „green belt“ [16].

Bezpečnostní hrozby způsobené selháním lidského faktoru [11] [16].:

- Správa hesel,
- Nevyžádaná pošta,
- Oběť sociálního inženýrství,
- Zabezpečení počítačů a přenosových médií,
- Návštěvy nebezpečných stránek,
- Úmyslné vyzrazení firemních informací,
- Zneužití firemních zdrojů.

6.1 Správa hesel

Každý zaměstnanec musí dodržovat předepsané zásady při tvorbě a další správě hesel:

Síla hesla Heslo by mělo být odpovídající nejnovějším bezpečnostním standardům pro tvorbu hesel například minimální rozsah hesla jako je, délka hesla, která se uvádí alespoň 8 znaků, kombinace několika znakových sad (čísla, velká písmena s diakritikou, malá písmena s diakritikou či speciální znaky, jako je křížek, hvězdička apod.) Posledním standardem je například standard NIST [17] Nejnovější studie ukazují, že tento rozsah, který, využívá většina firem již není dostačující a heslo by mělo mít minimální délku 12 – 14 znaků, což je ovšem pro běžného uživatele velice nekomfortní.

Periodická obměna hesel Heslo by mělo být jednou za období určené bezpečnostním či vedoucím pracovníkem změněno. Tato doba může být u každého podniku individuální, ale nejčastěji se používá období 6-12 měsíců. Mnohdy se změna hesla vynucuje přímo informačním systémem.

Unikátní heslo pro přístup do podnikového systému Heslo, které si zaměstnanec vybere pro přístup do podnikového systému či emailu by mělo být unikátní a zaměstnanec by se měl ujistit, zda toto heslo nebylo použito již v minulosti na jiném webu. Většina systémů má nastavenu historii hesel a nedovolí použít stejné heslo. [17].

Uchování hesla v tajnosti Zaměstnanec nesmí za žádných okolností sdělovat heslo jiné osobě. A zaměstnavatel by neměl v zájmu ochrany svého informačního systému v žádném případě žádat své zaměstnance o jejich hesla ani z důvodu jakékoliv údržby. V případě, že zaměstnanci podniku nedodrží správu či volbu hesel dle nařízení podniku, vystavují se možnému postihu ze strany podniku. [11]

6.2 Nevyžádaná pošta

Zaměstnanci podniku se mohou potýkat v denním pracovním režimu s řadou útoků mířených na podnik v kterém, pracují za účelem zcizení důležitých informací podniku. Útok může být realizován pomocí zasílání nevyžádané emailové pošty od útočníků k zaměstnancům podniku. Pomocí zástěrky, například nezaplacené faktury od zdánlivě relevantní emailové adresy donutí zaměstnance kliknout na internetový odkaz či stáhnout soubor přiložený v emailu, který může infikovat počítač zaměstnance nežádoucím programem zvaným malware, který může sledovat, jaké webové stránky zaměstnanec

prohlíží dokonce i jaké klávesy mačká a mnoha dalších. Kromě malware známe ještě druhý nejpoužívanější druh útoku zvaný phishing. Phishing spoléhá na lidskou nepozornost, kdy zaměstnanec klikne na odkaz ve velmi věrohodném emailu, který ho zdánlivě přesměruje na stránky, které velmi dobře zná a navštěvuje je každý den, například stránky www.google.cz. Ve skutečnosti je však zaměstnanec přesměrován na stránky útočníka, které se podobají známým stránkám jak vzhledově, tak i v URL adrese. Pokud uživatel provede přihlášení na takovouto stránku předá nevědomky název uživatelského účtu a heslo útočníkovi. Tímto způsobem si útočníci mohou jednoduše duplikovat firemní web a získat tak přístup do podnikového intranetu, Každý zaměstnavatel by proto měl dbát na pravidelné školení svých zaměstnanců, aby předešel těmto druhům. [16]

6.3 Oběť sociálního inženýrství

Zaměstnanci se také mohou stát oběťmi útoku prostřednictvím takzvaného sociálního inženýrství. Mezi způsoby sociálního inženýrství lze zařadit i případy z bodu nevyžádaná pošta v této práci. Útoky ale mohou mít i jiné podoby, a to například přes telefonní hovor kdy se útočník snaží od zaměstnance zjistit citlivé informace pod zástěrkou falešné identity například IT podpory, či státních dozorčích orgánů. Správné proškolení zaměstnanců a správné nastavení bezpečnostní politiky společnosti může přispět k minimalizaci tohoto rizika. [16]

6.4 Zabezpečení počítačů a přenosových médií

Každé zařízení či přenosové medium společnosti musí být zabezpečeno heslem a zašifrováno jako prevence krádeže. Stejně tak, jako by měly být chráněny porty zaměstnaneckých počítačů či síťových prvků před útokem skrze USB port či proti napojení na intranet společnosti. Zaměstnanci musí být proškoleni k používání podnikových zařízení, aby nedocházelo k úniku informací po vložení infikovaného flashdisku do podnikového zařízeni a naopak. [6]

6.5 Návštěvy nebezpečných stránek

Z pohledu bezpečnosti firemních informací a zamezení jejich úniku skrze zaměstnanecké počítače je velmi dobrým krokem zamezení přístupu zaměstnancům na nevhodné stránky které mohou být zdrojem infikace firemního zařízení. K tomuto kroku v posledních letech přistupuje čím dál více firem. K zabezpečení firemní sítě pomocí firewallu je možné zamezit přístup zaměstnanců na nevhodné stránky. [11]

6.6 Úmyslné vyzrazení firemních informací

Jedním z nejproblematičtějších rizik úniku informací a firemního know-how podniku jsou přímo zaměstnanci, kteří za finanční úplatek dobrovolně poskytnou veškeré informace konkurenčním podnikům. Proti tomuto druhu rizika zatím nemáme úplnou ochranu. K minimalizaci této hrozby mohou podniky udělat dva kroky. [31]

- Prvním krokem je udělovat zaměstnancům oprávnění přístupu pouze k informacím které nezbytně potřebují k výkonu své práce, tím minimalizovat riziko prozrazení firemního know-how. [11] [16]
- Druhým krokem, jak se podnik může pokusit předejít situaci tím, že si svých zaměstnanců bude vážit a nebude jim dávat důvod k těmto činům například správným finančním ohodnocením jejich práce. [11] [16]

6.7 Zneužití firemních zdrojů

Zaměstnanci podniku zejména na pozicích vyššího managmentu se mnohdy dostanou do situace, kdy by pro ně osobně bylo výhodné zneužít firemní zdroje k jejich vlastnímu prospěchu či obohacení. Například převedení podnikové zakázky na jinou či vlastní firmu, přijmutí úplatku za ústupky ve smlouvě znevýhodňující podnik, či poskytování služeb od své osobní firmy pro podnik ve kterém dělá výše postaveného managera. [16]

7 ANALÝZA RIZIK

Součástí každého podniku jsou aktiva jako např. informační systémy, výrobní dokumentace atd. Aktiva jsou právě tím důvodem proč útočníci podniky napadají za účelem špionáže, jsou to například informace, zdrojové kódy, emaily či podnikové know-how. Aktiva jsou pro podnik úplně nejdůležitější položkou a lze je přesně finančně ocenit. Jejich hodnota odpovídá nákladům na jejich znovu-pořízení a částce rovnající se ušlému zisku podniku při jejich ztrátě, odcizení či zneužití. [18] Cílem analýzy rizik nebo bezpečnostních analýz je identifikovat maximum zranitelností a nedostatků obsažených ve zkoumaném objektu nebo podniku, odhadnout hrozby, rizika a možné negativní dopady okolí na zkoumaný objekt, určit efektivitu a funkčnost stávajících ochranných mechanizmů a navrhnout nové tak, aby byla všechna rizika efektivně snížena nebo pokryta na akceptovatelnou úroveň. Pod pojmem zkoumaný objekt si lze představit například počítačové systémy, zařízení, datová aktiva, služby, aplikace, procesy, informační systém organizace jako celek nebo celou organizaci.

Obrázek 2: Proces analýzy rizik [18]

Úkolem této analýzy rizik je vyhodnocení základních pojmů bezpečnosti. Jedná se převážně o odpověď na otázku “jaká má společnost AKTIVA”. Tím je myšleno, čeho nejvíce si firma cení.

Analýza se následně zabývá zranitelností podniku (hrozby, rizika). Dále následují návrhy opatření (jak eliminovat ohrožení) a jak požadované ochrany docílit. Laicky řečeno, analýza po zjištění informací odpoví na otázky: co chránit, proti čemu a jakým způsobem. [19]

7.1 Analýza obecně

Analýza jako taková je proces rozčlenění či rozboru složitějšího celku nebo skutečností na jednodušší části. Je to rozbor vlastností, vztahů, faktů postupující od celku k částem. Na rozdíl od syntézy, při které se postupuje od části k celku. V této kapitole se zaměřím konkrétně na analýzy týkající se bezpečnosti chodu podniku. V souvislosti s bezpečnostní politikou podniku je analýza rizik prvním krokem, který by měl udělat každý podnik, před tím než začne vytvářet své vnitřní předpisy týkající se bezpečnostní politiky podniku.

7.2 Hrozba

Hrozba je událost, síla nebo osoby jejichž působení mohou způsobit poškození, zničení nebo ztrátu hodnoty aktiv. Může ohrozit bezpečnost jakéhokoliv systému či podniku. [19] [20]

Jako hrozby ovlivňující podnik můžeme brát například[16]:

- politické hrozby,
- ekonomické hrozby,
- sociální hrozby,
- lidský faktor,
- kybernetické hrozby,
- legislativní hrozby,
- ekologické hrozby,
- přírodní katastrofy.

7.3 Aktivum

Aktiva podniku mají vždy určitou hodnotu která je ve většině případů pro organizaci z hlediska jejího fungování kritická. V případě její ztráty či poškození může dojít k finančním ztrátám podniku nebo dokonce k ukončení jeho činnosti. Může mít nepříznivé dopady na obchodní partnery, zákazníky i zaměstnance. Aktiva dělíme do dvou základních skupin [20]:

- hmotná aktiva (např. hardware, komunikační zařízení, auta apod.),
- nehmotná aktiva (např. informace, výrobní tajemství, software apod.).

Tabulka hodnocení aktiv:

Tabulka 1: Hodnocení aktiv

Číselná hodnota	**Slovní hodnota**
1	Nízký
2	Střední
3	Vysoký
4	Kritický

Riziko

Riziko je chápáno jako potenciální nebezpečí, že daná hrozba využije zranitelnosti aktiva nebo bezpečnosti podniku a způsobí škody na majetku či jiných aktivech podniku. Lze jí také charakterizovat jako kombinaci pravděpodobností nežádoucích hrozeb, které mohou způsobit škody na majetku či újmu na zdraví, ztrátu života či způsobit poškození životního prostředí. [18]

Riziko je také přímo spjato s místem a časem působení vnějších vlivů. [18]

Tabulka 2: Stanovení rizik [18]

	Dopady				
Pravdeporosbnos	1 - Nepatr	2 - Malý	3 - -Středı	4 - Význam	5 - Extrém
5 - Častý	Střední riziko	Vysoké riziko	Vysoké riziko	Velmi vysoké riziko	Velmi vysoké riziko
4 - Pravděpodobný	Střední riziko	Střední riziko	Vysoké riziko	Vysoké riziko	Velmi vysoké riziko
3 - Možný	Nízké riziko	Střední riziko	Střední riziko	Vysoké riziko	Velmi vysoké riziko
2 - Nepravděpodobný	Nízké riziko	Střední riziko	Střední riziko	Střední riziko	Vysoké riziko
1 - Vzácný	Nízké riziko	Nízké riziko	Střední riziko	Střední riziko	Vysoké riziko

Každý člověk vnímá a hodnotí riziko odlišným způsobem. Úroveň rizika je možno seřadit podle akceptovatelnosti. Projevené riziko může svými dopady vyvolávat příčiny ke vzniku nových rizik.

7.4 Bezpečnostní opatření

Bezpečnostní opatření jsou taková opatření, která snižují riziko. Je to například nastavení povinné změny hesla k přístupu do důležitých informačních systémů. [18]

7.5 Analýza dopadů na podnikání

Analýza dopadů na podnikání nebo-li Business Impact Analysis (dále jen BIA) Je analýza podniku zaměřená zejména na jeho činnost a na dopady způsobené jejím výpadkem a následným narušením dodávek produktů podniku. Při hodnocení dopadů na organizaci v případě narušení kritických činností se berou v úvahu spíše následky než příčiny. Dopady na organizaci a jejich vývoj v čase se posuzuje dle vhodných vodítek. Vybraná vodítka musí

být vhodná pro danou organizaci; vodítka finanční instituce se budou lišit od vodítek orgánu státní správy. Vodítka pro hodnocení dopadů mohou být například finanční ztráta, dopad na dodávky služeb, poškození nebo ztráta pověsti, nesplnění zákonných nebo regulačních povinností, atd.

Závěry z analýzy dopadů společně s hodnocením rizik narušení kritických činností organizace jsou základem pro strategie řízení kontinuity činností, které umožňují identifikovat různé varianty a způsoby obnovy kritických činností organizace v požadovaných časech v případě jejich narušení [21].

Postup při analýze BIA:

- identifikovat činnosti, které zajišťují dodávku klíčových produktů a služeb,
- ohodnotit dopady, pokud dojde k narušení těchto činností, a vývoj těchto dopadů v čase,
- určit pro každou identifikovanou činnost maximální tolerovanou dobu narušení činnosti MTPD po kterou jsou dopady pro organizaci ještě akceptovatelné,
- identifikovat a určit priority jejich obnovy činností na základě MTPD. Za kritické činnosti lze považovat činnosti s největšími dopady v nejkratších časech,
- pro každou kritickou činnost určit lhůtu její obnovy RTO. Pro jeho stanovení je nutné zvážit s tím spojené náklady na obnovu. RTO kritické činnosti musí být však menší než její maximální doba tolerance MTPD,
- určit minimální úroveň zdrojů potřebných k obnově každé kritické činnosti.

7.6 Technická bezpečnostní analýza

Technická bezpečnostní analýza neboli RAC Information System Security Examination Cycle.

RAC ISSEC je metodika vyvinutá společností RAC za účelem na zkoumání informačních systémů, ve všech fázích jeho životního cyklu, přímo v prostorách a na zařízeních zákazníků, včetně penetračního testování přes Internet. RAC ISSEC se primárně zaměřuje na IT technologie, ale zkoumá bezpečnost jejich implementace a provozu i ve všech ostatních vrstvách bezpečnosti fyzické, personální, administrativní a zejména organizační.

RAC ISSEC se řídí standardy ISO/IEC 27002 a ISO/IEC 27001 a slouží jako diagnostický a podpůrný proces pro provádění analýz rizik informačních systémů, klade důraz na implementaci ochranných opatření bezpečnostní audity[22] .

Při zpracování této metody se využívají zejména tyto druhy analýz

- Bezpečnostní analýza,
- Penetrační testování,
- Bezpečnostní audit.

Diferenční analýza

Diferenční analýzu nebo-li Gap Analysis je analýza zaměřená na zjištění nějakého nedostatku či mezery mezi současným a požadovaným stavem. Lze porovnávat i stav v dané problematice oproti konkurenčnímu podniku. Gap analýza byla navržená ruským matematikem Igor Ansoffsem a má velmi široké spektrum využití v různých oborech jako například k analýze tržních a marketingových mezer, legislativní analýze odpovídající za to jestli podniková politika a jeho postupy jsou v souladu s platnými zákony nebo například při bezpečnostní analýze kdy zkoumáme a posuzujeme nedostatky například v oblasti fyzické či informační bezpečnosti. [23]

Postup při Gap analýze:

- Popis stávajícího stavu,
- Stanovení cílového stavu,
- Určení rozdílů mezi stávajícím a cílovým stavem,
- Návrh postupů a opatření k dosažení cílového stavu,
- Zhodnocení návrhů a výběr nejlepšího z nich,
- V případě potřeby se celý postup opakuje, dokud není dosaženo cílového stavu.

7.7 PEST analýza

PEST analýza slouží k podrobnému posouzení faktorů, které působí na společnost. Jednotlivá písmena v názvu této techniky značí rozličné sféry, které je nezbytné brát v potaz při vypracování analýzy. [24]

- P – politické,
- E – ekonomické,
- S – sociální,
- T – technologické.

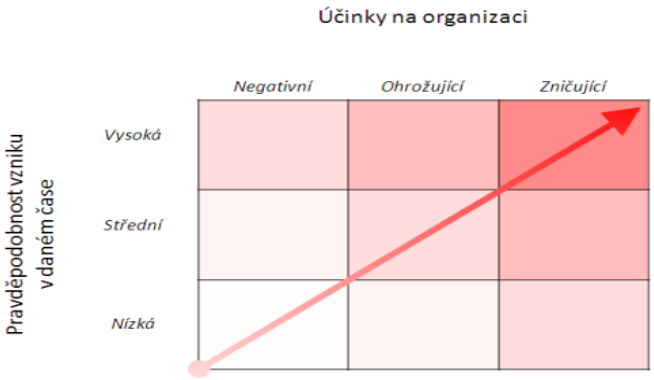
Smysl této metody spočívá v určení (pro každou z výše uvedených skupin) co nejvíce možných rizik, faktorů a okolností, která budou mít přímý, či nepřímý vliv na chod společnosti. Následně je nutno posoudit, jaký konkrétně vliv budou mít jednotlivé faktory a podnik a určit nejkritičtější body tohoto seznamu. Při zpracování analýzy je zapotřebí brát na vědomí vzájemné propojení jednotlivých sfér, kdy jakákoliv změna v jedné sféře neodmyslitelně vede k různě markantním změnám v ostatních sférách.

Winterlingova krizová matice

Winterlingovu krizovou matici vymyslel Klaus Winterling, jako jednoduchý, ale praktický nástroj k posouzení rizik[25].

K tomuto účelu pracujeme pouze se dvěma parametry:

- Pravděpodobnost vzniku rizika v daném čase.
  - Tento parametr nabývá tří hodnot (nízká, střední, vysoká).
- Účinek rizika na společnost.
  - tento parametr rovněž pracuje se třemi hodnotami (negativní, ohrožující, zničující).



Obrázek 3: Posouzení rizik Winterlingova matice [25]

Analýza rizik pomocí metody FMEA

FMEA nebo-li Failure Mode and Effect Analysis, je univerzánlní analytická metoda, která nachází uplatnění v mnoha odvětvích jako je například řízení rizik, řízení kvality nebo řízení bezpečnosti. Základem metody je systematická identifikace všech možných vad výrobků, procesů jejichž dopady mají vliv na vznik vad bezpečnostních rizik. [26]

Při zpracovávání metody FMEA postupujeme postupně dle několika bodů, [26]:

- analýza současného stavu,
- hodnocení současného stavu,
- analýza vlivu rizik či vad na podnik či zákazníka,
- analýza příčin a stávajících opatření,
- zhodnocení pravděpodobnosti,
- výpočet rizikového čísla,
- návrh opatření,
- opětovná analýza,
- posouzení účinnosti jednotlivých opatření.

Výpočet rizikového čísla: R= Z*V*O

Z – znamená závažnost a nabývá hodnot v intervalu <0,10>.

V – znamená výskyt a nabývá hodnot v intervalu <0,10>.

O – znamená odhalitelnost a nabývá hodnot v intervalu <0,10>.

Rizikovost je vyjádřena hodnotou rizikového čísla:

- Rizikovost 0-125 malé riziko,
- Rizikovost 126-768 střední riziko,
- Rizikovost 769-1000 vysoké riziko.

7.8 Hodnocení rizik pomocí metody PNH

Jednou z nejpoužívanějších a také z nejjednodušších metod pro hodnocení rizik je polo-aktivní metoda PNH neboli **(P)** pravděpodobnost vzniku, **(N)** pravděpodobnost následků a **(H)** názor hodnotitele. [27]

- **Pravděpodobnost vzniku:** posouzení rizika na základě možnosti a četnosti vzniku rizik.
- **Pravděpodobnost následků:** posouzení rizika na základě míry jeho dopadů na podnik.
- **Názor hodnotitele:** hodnotitel zohledňuje míru závažnosti rizik na základě počtu ohrožených osob, délce ohrožení, technického stavu objektů či strojů, vlivu pracovního systému, prostředí a podmínek a dalších vlivů ovlivňujících dané riziko. [27]

Všechny tyto body se určují v rozsahu od **1-5**.

Pro stanovení rizika jako takového **(R)** používáme vzorec **R = P x N x H**

P – pravděpodobnost vzniku a existence nebezpečí

Nahodilá	1
Nepravděpodobná	2
Pravděpodobná	3
Velmi pravděpodobná	4
Trvalá	5

N – možné následky ohrožení

Poškození zdraví bez pracovní neschopnosti	1
Absenční úraz (s pracovní neschopností)	2
Vážnější úraz vyžadující hospitalizaci	3
Těžký úraz a úraz s trvalými následky	4
Smrtelný úraz	5

H – názor hodnotitelů

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

Obrázek 4: Stupně hodnocení rizik PNH [27]

Rizikový stupeň	R	Míra rizika
I.	> 100	Nepřijatelné riziko
II.	51 ÷ 100	Nežádoucí riziko
III.	11 ÷ 50	Mírné riziko
IV.	3 ÷ 10	Akceptovatelné riziko
V.	< 3	Bezvýznamné riziko

Obrázek 5: Určení míra rizika PNH [27]

7.9 SWOT Analýza

K analýze rizik můžeme také využít druhou analytickou metodu zvanou SWOT. Analýza SWOT je díky jejímu integrujícímu charakteru vyhodnocených poznatků jednou z nejpoužívanějších metod a to převážně v ekonomice. V rámci analýzy rizik by byla použita SWOT analýza jako komplexní metoda kvalitativního vyhodnocení všech klíčových stránek vhodná nejen pro strategické řízení, ale aplikovatelná v jakékoliv oblasti. Zejména proto, že SWOT analýza hodnotí vnitřní a vnější vlivy zkoumaného jevu. Vnitřní faktory se zabývají hodnocením silných a slabých stránek, vnější faktory zahrnují hodnocení příležitostí a hrozeb. [28]

SWOT je anglická zkratka

- S = Strengths (Silné stránky),
- W = Weaknesses (Slabé stránky),
- O = Opportunities (Příležitosti),
- T = Threats (Hrozby).

po vytvoření této analýzy se definují doporučení, která by měla zlepšit současný stav bezpečnosti podniku. [28]

8 OBECNÁ NAŘÍZENÍ NA OCHRANU OSOBNÍCH ÚDAJŮ

General Data Protection Regulation do češtiny přeloženo jako Obecná nařízení na ochranu osobních údajů (dále jen GDPR). Toto nařízení Evropské Unie vyšlo v platnost dne 25. května 2018 a upravuje všeobecný přístup k osobním údajům občanů žijících v Evropské Unii. Podle nařízení Evropského parlamentu a Rady (EU) 2016/679 (GDPR) v českém právním systému podle zákona 110/2019 Sb. o zpracování osobních údajů ze dne 12. března 2019. Tímto zákonem se musí řídit všichni, kteří jakýmkoliv způsobem zpracovávají či shromažďují osobní údaje. Cílem tohoto nařízení je zvýšit bezpečnost citlivých dat zaměstnanců, zákazníků, dodavatelů či běžných občanů a chránit je tak před zneužitím. [29]

8.1 Osobní údaje

Za osobní údaje dle GDPR lze ve zkratce považovat jakékoliv informace, které lze použít k identifikaci konkrétní žijící fyzické osoby. Za takové lze považovat i jednotlivé zdánlivě nesouvisející informace, které v kombinaci napomáhají identifikovat konkrétní osobu. Tyto informace lze zařadit do dvou kategorií:

- obecné osobní údaje,
- citlivé osobní údaje.

8.2 Povinnosti subjektů

Povinnost subjektů zpracovávajících osobní údaje vyplývající z GDPR:

- získání souhlasu se zpracováním osobních údajů správce osobních údajů musí doložit, že získal od fyzické osoby souhlas se zpracováním osobních údajů. V praxi to znamená podpis listiny, ve které je ve srozumitelné formě deklarováno, jak a k jakým účelům, budou osobní údaje využity. Tato listina musí obsahovat také informace o odvolání souhlasu se zpracováním osobních údajů.
- oznamovací povinnost v případě, že dojde k úniku citlivých informací, je správce těchto dat povinen do 72 hodin tuto událost oznámit kontrolním orgánům a také osobám, jejichž údaje byly zasaženy.
- Plánování strategie zpracování osobních údajů správce osobních údajů je podle GDPR povinen utvořit strategii pro zpracování a ochranu osobních údajů v souladu s GDPR dříve, než dojde k samotnému zpracování informací.

Je nezbytné přihlédnout k tomu, že jakékoliv osobní údaje dětí spadají do kategorie citlivých údajů a je potřeba s nimi zacházet jako odpovědným způsobem.

  - Vypracování posouzení vlivu na ochranu osobních údajů - tato povinnost se týká zpracovatelů, kteří osobní informace zpracovávají systematicky a v rozsáhlém měřítku
  - určení osoby zodpovědné za ochranu osobních údajů (Data protection officer) - tato povinnost se týká zpracovatelů, kteří osobní informace zpracovávají systematicky a v rozsáhlém měřítku

- pseudonymizace, případně anonymizace osobních údajů. Zpracovatel je povinen osobní údaje uchovávat nebo s nimi pracovat, pokud možno v pseudonymizované podobě, to znamená, že je nutno data rozdělit takovým způsobem, aby na první pohled nebylo možné identifikovat konkrétní osobu. Zpětná identifikace je ovšem možná (za použití specifického klíče který je nezbytné uchovávat odděleně od zašifrovaných informací). Anonymizace je proces podobný pseudonymizaci. Liší se pouze v tom, že i klíč k identifikaci je odstraněn a tudíž neexistuje způsob zpětné identifikace konkrétní osoby(jedná se o nevratný děj) [30].
- vedení záznamů o zpracování osobních údajů.
  - jméno a kontaktní údaje zpracovatele,
  - jméno a kontaktní údaje správce osobních údajů,
  - účel zpracování,
  - druh osobních údajů,
  - informace o subjektech, jimž byly osobní informace zpřístupněny,
  - informace o mezinárodním předávání osobních údajů,
  - lhůty pro výmaz jednotlivých údajů,
  - popis technických a organizačních opatření.

II. PRAKTICKÁ ČÁST

9 PŘÍKLAD BEZPEČNOSTNÍ POLITIKY SOUKROMÉ ŠKOLY

Celou problematiku bezpečnostní struktury a bezpečnostní politiky podniku Vám představím v praktické ukázce. Jako příklad jsem si vybral se souhlasem majitele reálně fungující firmu, ve které působím také jako správce sítě. Na tomto reálném podniku Vám představím bezpečnostní analýzu podniku s návrhem řešení nalezených potenciálních bezpečnostních problémů.

9.1 Popis podniku

Název podniku, na kterém budu předvádět analýzu rizik je Soukromé Školy Hostivař. Škola se nachází na kopci mimo zátopovou oblast a je rozdělena do dvou částí. Každá část je umístěna v jednom patře té samé budovy. V přízemí se nachází mateřská škola s jídelnou, menší tělocvičnou a kanceláří managementu. V patře se nachází 5 tříd prvního stupně základní školy, šatna a kantorská sborovna. Škola má kapacitu přibližně 140 dětí a zaměstnává 13 lidí kteří se starají o její chod.

9.1.1 Aktuální stav

V současném řešení jsou některé bezpečnostní a funkční prvky vyvinuty přímo na míru pro potřeby školy. Zdrojové k těmto prvkům jsou uloženy na školním serveru. Pro ochranu dětí slouží vstupní dveře na čipovou kartu pro vchod do budovy, které zamezují příchodu neautorizovaných lidí do prostor školy.

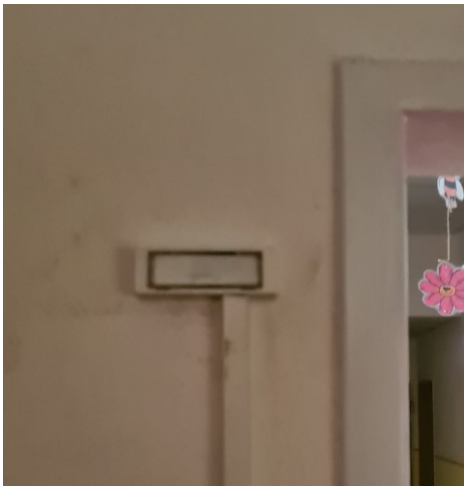
Obrázek 6: Vstupní čtečka karet

Pro otevření dveří ze vnitřních prostor objektu je ve výšce 1,9 metru umístěno tlačítko pro otevření dveří. Tato výška tlačítka je zvolena z důvodu toho aby žáci mateřské školy či prvního stupně základní školy nedosáhli na tlačítko dveří a nemohli tak svévolně opustit prostor školy.

Obrázek 7: Tlačítko na otevření vstupních dveří z vnitřní strany

Stejným způsobem jsou jištěny dveře od tříd mateřské školy.

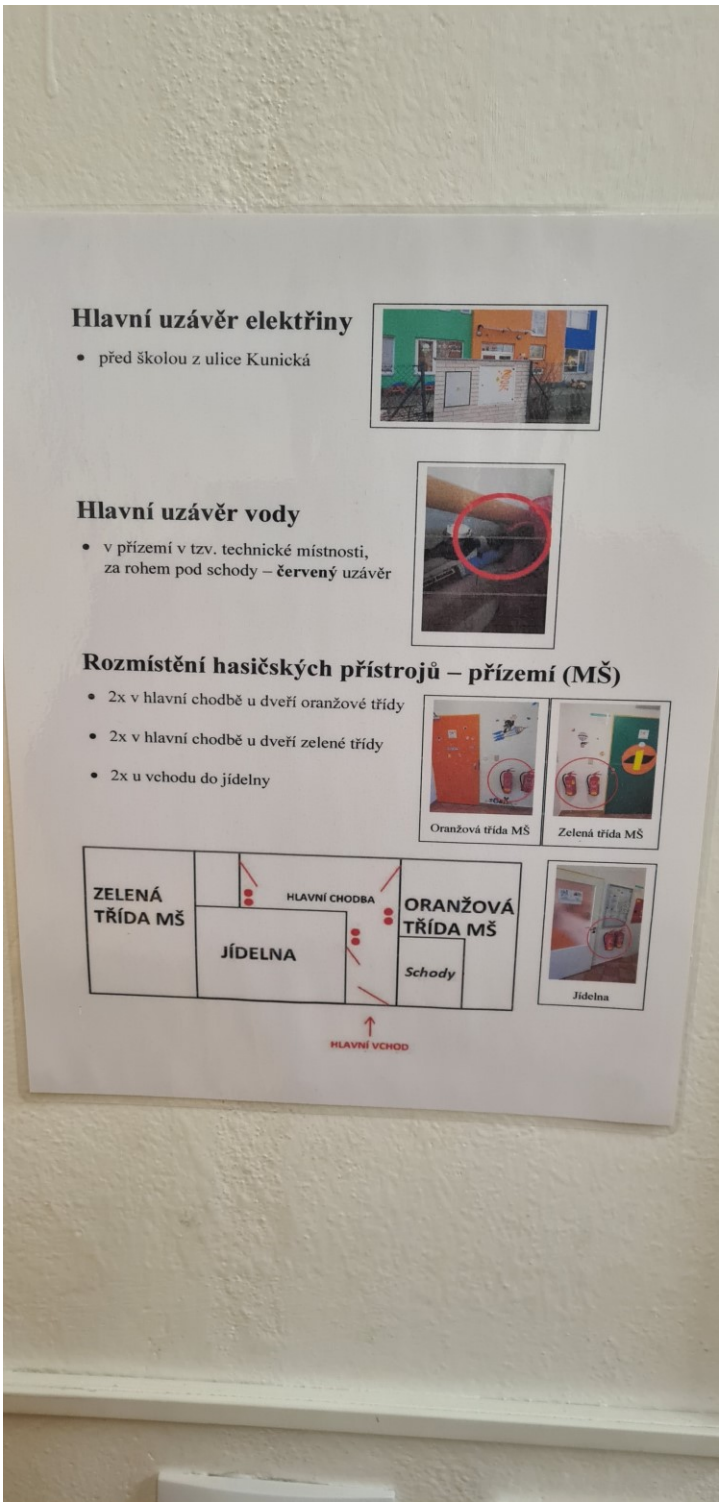
Obrázek 8: Čtečka karet pro otevření dveří do školky



Obrázek 9: Tlačítko pro otevření dveří od školky z vnitřních prostor

V případě mimořádné situace jako je například požár, je škola vybavena únikovými východy, požárními čidly a plánky.

Obrázek 10: Únikový východ z prvního patra



Obrázek 11: Plánek rozmístění hasičských přístrojů v přízemí

9.1.2 Identifikace a hodnocení aktiv

Tabulka 3: Identifikace a hodnocení aktiv

Typ aktiv	**Aktivum**	**Slovní ohodnocení**
Nehmotné	Studijní materiály	Kritické
	Internetové připojení	Vysoké
Hmotná	Kantorské notebooky	Kritické
	Notebooky žáků	Vysoké
	Server	Vysoké
	Služební automobil	Kritické
	Dotykové televize	Kritické
	Vybavení jídelny	Střední
	Uskladněné zboží	Nízké
	Učební a sportovní pomůcky	Nízké
Lidské zdroje	Zaměstnanci (management, učitelé, pomocný personál …)	Kritické

9.1.3 Identifikace hrozeb

V následující tabulce je uvedena identifikace největších hrozeb, se kterými se v našem podniku můžeme setkat. [17][9]

Tabulka 4: Identifikace hrozeb soukromé školy

Hrozby	Pravděpodobnost hrozby	Příklad související se zranitelností
Požár	Nízké	Přítomnost elektroniky, která může být potenciálním zdrojem požáru, instalován protipožární systém
Vloupání do podniku	Střední	Uložení smluv, osobních údajů a drahého vybavení v podniku
Selhání techniky	Střední	Náchylnost techniky na prach a vlhkost
Únik dat	Střední	Osobní údaje klientů
Ztráta dat	Střední	Výukové materiály
Terorismus/ sabotáž	Nízká	Konkurenční politický či náboženský motiv
Výpadek energie	Vysoká	Vyřazení všech služeb a provozů podniku
Epidemie	Vysoká	V souvislosti s onemocněním COVID-19
Výpadek internetu	Vysoká	Vyřazení části služeb a provozů podniku
Odcizení firemního auta	Střední	Parkuje na nezabezpečeném parkovišti

9.1.4 Identifikace rizik ohrožující zdraví

Seznam zdraví ohrožujících nehod, kterým je třeba se pokusit předejít nejen v BOZP ale i úpravami prostor ve kterých se zaměstnanci i klienti pohybují.

Tabulka 5: Identifikace rizik ohrožující zdraví

Riziko	**Chráněno**	**Způsob ochrany**
Kontakt s ostrou hranou	Chráněno	Odstraněny ostré hrany i předměty
Pád ze schodů	Nechráněno	Označení schodů značkou i pruhy

9.1.5 Analýza rizik dle metody PNH

Pomocí metody PNH vypočítám rizika vyplývající s identifikovaných hrozeb [17]. Nyní spočítám rizikový stupeň a dle tabulky obsažené v kapitole 6.10.2 Hodnocení rizik pomocí metody PNH a zjistím které z hrozeb se stávají akceptovatelným rizikem a které potřebují zásah či investici k jejich odstranění.

Při výpočtu se řídíme tabulkami na straně 33 a 34 uvedenými v teoretické části této práce.

Tabulka 6: Analýza rizik soukromé školy

Hrozby	**P**	**N**	**H**	**Riziko**	**Přijatelnost**	**Opatření**
Požár	1	5	5	25	Mírné riziko	Protipožární systém je již instalován. Žádoucí opatření je přidat záložní zdroj k napájení rozhlasu a přepracování elektronického zámku vstupních dveří
Vloupání do podniku	2	3	3	18	Mírné riziko	Čipové karty instalovány, alarm instalován s napojením na pult centrální ochrany. Žádoucí opatření je instalace bezpečnostního zámku a ochrana kamerovým systémem proti vandalismu
Selhání techniky	2	3	3	18	Mírné riziko	Přepěťové zásuvky
Únik dat	2	2	3	12	Mírné riziko	Dodržování zásad kybernetické bezpečnosti
Ztráta dat	2	2	3	12	Mírné riziko	Doporučení zálohy dat
Terorismus/ sabotáž	1	5	2	25	Akceptova-telné riziko	Vstup pouze s přístupovou kartou, okolo školy plášťová ochrana s 50 cm vysokou zdí s plotem.
Výpadek energie	1	3	3	15	Akceptova-telné riziko	Žádoucí instalace UPS na nejdůležitější systémy
Epidemie	3	3	3	9	Akceptova-telné riziko	Dodržování hygieny
Výpadek internetu	1	2	3	6	Akceptova-telné riziko	K řešení doporučena smlouva se sekundárním poskytovatelem připojení
Odcizení firemního auta	1	3	3	9	Akceptova-telné riziko	Alarm

9.2 Stanovení bezpečnostních cílů

V prvním kroku je zapotřebí stanovit bezpečnostní cíle které jsou očekávány

- Zajistit přiměřenou bezpečnost informací získaných od klientů a smluvních partnerů (v tomto případě od dětí a jejich rodičů), tj. zachovat jejich důvěrnost, zajistit požadovanou dostupnost, integritu a spolehlivost obsahu informací v celém procesu jejich zpracování.
- Splnit legislativní požadavky na ochranu informací, zejména:
  - Legislativní a zákonné povinnosti dle zákona o zpracování osobních údajů č.110/2019Sb. který provádí nařízením EU č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (dále jen GDPR)
  - Občanský zákoník, Zákon č. 513/1991 Sb.
  - Obchodní zákoník a Zákon o účetnictví č. 563/1991 Sb.
- Splnit požadavky na ochranu informací dodavatelů a smluvních stran,
- Požární ochrana,
- Zajistit maximální bezpečnost dětí.

9.2.1 Návrh eliminace rizik

Z mé analýzy plyne že Soukromá škola Hostivař splňuje a má v tomto okamžiku vyhovující ochranu proti aktuálně hrozícím hrozbám. Včetně zajištění prostor tak aby nedocházelo ke zranění osob pohybujících se v prostorách školy. Nalezl jsem však určité kroky, které by škola mohla udělat pro lepší ochranu majetku a zdraví osob v prostorách školy.

- Zvýšení plášťové a objektové ochrany kamerovým systémem, který bude chránit majetek školy před odcizením či vandalstvím.
- V současné době je instalována na škole protipožární ochrana formou hlásičů a zvukového signálních zařízení. Doporučení pro zlepšení požární ochrany ve smyslu evakuace osob bych navrhoval koupi záložního zdroje pro rozhlasový systém školy.
- Dále bych doporučil, aby elektronické zámky u vstupních dveří byly automaticky nastaveny na NO (normaly open) a zefektivnila se tak evakuaci osob, které by v

případě požáru a výpadku proudu nemusely rozbíjet sklo s klíčkem u dveří nebo hledat přímo únikový východ.

9.3 Ukázka dokumentu Bezpečnostní politika

Jak by měl vypadat dokument Bezpečnostní politiky pro konkrétně tuto základní a mateřskou školu je zpracováno v této části bakalářské práce.

Úvodní ustanovení

Vedení společnosti vyhlašuje zásady bezpečnosti a bezpečnosti informací v podniku. Tato politika je závazná pro všechny zaměstnance společnosti a slouží k zajištění bezpečnosti a podpoře bezpečnosti informací.

1) tato politika popisuje a vysvětluje bezpečnost informací uvnitř společnosti,
2) stanovuje bezpečnostní cíle,
3) uvádí stručný výklad bezpečnostních zásad,
4) stanovuje kritéria, kterými bude hodnoceno riziko.

Zajištění bezpečnosti informací je charakterizováno jako zachování:

1) Důvěrnosti (zajištění přístupnosti k informacím pouze povolaným pracovníkům),
2) Integrity (zaručuje přesnost a kompletnost informací),
3) Dostupnosti (zajišťuje přístupnost k informacím v době potřeby).

Cílem bezpečnosti informací ve společnosti je zajištění kompletnosti, správnosti a dostupnosti informačních aktiv povolaným osobám. Jejich ochrany před náhodným nebo neoprávněným zničením, ztrátě či zneužití. Při zachování bezpečnosti informací musí být dodrženy veškeré zákony a právní předpisy ČR. Zajištění důvěrnosti a bezpečnosti jejich zpracování a ochrany informací proti náhodnému, neoprávněnému zničení, náhodné ztrátě, proti neoprávněnému přístupu, změnám nebo šíření, a to v souladu se zákony a jinými právními předpisy ČR. Zajištění bezpečnosti informací pokrývá celou strukturu společnosti a veškeré spolupracující podniky, které přichází do styku se zabezpečenými informacemi spravovaných společností. Bezpečnost informací pokrývá všechna důležitá informační aktiva společnosti.

Dokument Bezpečnostní politika podléhá pravidelné revizi v intervalu jeden krát ročně. Za revizi dokumentu Bezpečnostní politika odpovídá statutární zástupce společnosti. Záměrem Organizace je udržovat přiměřenou ochranu informačních aktiv.

Cíle a zásady bezpečnosti informací

Zaměstnanci společnosti v rámci dodržování bezpečnosti informací zajišťují:

1) ochranu práv a svobod jednotlivců, zejména právo na soukromí uznané v článku 7 Úmluvy o ochraně lidských práv a základních svobod, usnesení představenstva ČNR č. 2/1993 Sb. o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky.
2) ochranu osobních údajů a citlivých údajů podle zvláštního zákona upraveného evropským nařízením GDPR,
3) ochranu obchodního tajemství podle zvláštního právního předpisu a obsahu smluv,
4) ochranu listovního tajemství,
5) vedení společnosti vyjadřuje touto bezpečnostní politikou svoji strategii trvalého zajišťování bezpečnosti informací jako nedílné součásti řídících procesů.

Organizace bezpečnosti

Záměrem organizace bezpečnosti je řízení a koordinace bezpečnostních opatření dle působnosti a odpovědnosti vedoucích zaměstnanců v oblasti bezpečnosti informací a personální bezpečnosti. Povinnosti spojené s řízením bezpečnosti informací ve společnosti zajišťuje statutární zástupce společnosti nebo pověřený pracovník, a to ve spolupráci s pověřeným pracovníkem pro ochranu osobních údajů, který přezkoumává a sleduje bezpečnostní incident a schvaluje a navrhuje kroky vedoucí ke zvýšení bezpečnosti informací. Za dodržování bezpečnostní politiky zodpovídají všichni vedoucí zaměstnanci společnosti dle jejich působnosti.

Klasifikace informačních aktiv

Účelem klasifikace a řízení informačních aktiv je udržovat jejich přiměřenou ochranu. V rámci Společnosti je zavedena a udržována evidence osobních údajů u nichž je minimálně určena identifikace osobního údaje, jeho zdroj, kategorie, subjekt údajů, účel zpracování, operace zpracování a jednoznačně stanoveny osoby pověřené k nakládání s těmito osobními údaji v souladu s platnými předpisy. Osobní údaje ve společnosti musí být kategorizovány tak, aby byl přesně stanoven účel jejich zpracování, zákonnost a kategorie. Kategorizaci stanoví statutární zástupce Společnosti, nebo Pověřenec pro ochranu osobních údajů, popřípadě pověření pracovníci, kteří odpovídají za periodické přezkoumávání této klasifikace a její aktualizaci. Kategorizace určuje způsob zacházení s informacemi s ohledem na jejich ochranu a citlivost.

Personální bezpečnost

Cílem personální bezpečnosti je snížení rizika způsobené lidským selháním, krádeží či zneužití zdrojů společnosti. Záměrem společnosti je eliminovat rizika spojená s lidským faktorem:

1) přijímacím řízením zaměstnance (posouzení zaměstnance při přijímacím řízení),
2) formou školení zaměstnanců dostat do povědomí pravidla bezpečnosti informací a nakládání s nimi,
3) nedodržení bezpečnostních zásad zaměstnancem může být kvalifikováno jako porušení jeho povinnosti či porušení pracovní kázně zaměstnance s příslušnými důsledky ve smyslu zákona č. 262/2006 Sb., zákoník práce. Týká-li se pochybení zaměstnance porušení ochrany osobních údajů prošetří incident společnost ve spolupráci s pověřencem pro ochranu osobních údajů a provede o něm záznam.

Fyzická bezpečnost a bezpečnost prostředí

Záměrem fyzické bezpečnosti společnosti je zamezení neoprávněnému přístupu k informačním aktivům společnosti formou fyzického porušení, narušení nebo odcizení. Bezpečnostním cílem je zajištění fyzické ochrany:

1) vymezením zabezpečených oblastí kde se informace nacházejí, zpracovávají a uchovávají (např.: kontrola vstupů, zamykatelné kanceláře apod.),
2) zabezpečením zařízení proti odcizení a zničení, poškození, zahrnujícím bezpečné umístění zařízení, zajištěním podpůrných služeb pro provoz zařízení (dodávky energie, klimatizace atd.), zabezpečením kabeláže a zajištěním pravidelné bezpečné údržby a revizí systémů a zařízení,
3) uplatnění zásad čistého stolu a čisté obrazovky (zodpovídá vedoucí pracovník),
4) zajištění požární bezpečnosti podle zákonů a jiných právních předpisů v společnosti (požárním hlásičem, zvukovým signalizačním zařízením a ukazateli únikových východů),
5) stanovení režimu vstupu a výstupu osob do budovy a zajištění zabezpečených oblastí formou:
    a) zajištění autorizovaného vstupu do budovy je realizováno pomocí dveřního systému otevírajícího dveře na bezkontaktní RFID kartu,
    b) omezení vstupu do zabezpečené oblasti je realizováno uzamykatelnými dveřmi.

Řízení bezpečnosti komunikací a provozu

Účelem řízení bezpečnosti komunikací a provozu je zajistit bezpečný provoz systému pro zpracování informací a minimalizovat jejich selhání. Bezpečnostním cílem je zajištění ochrany informací prostřednictvím:

1) ochrany proti škodlivým programům
    a) užíváním antivirového programu a jeho pravidelným aktualizováním ve všech zařízení společnosti,
    b) nastavením brány firewall,
    c) omezením přístupu na nevhodné a nebezpečné stránky ze všech zařízení v síti pomocí přesměrováním na DNS od společnosti https://www.i-bezpecne.cz/.
2) zálohování, tak aby byla zajištěna obnova dat a systémů
    a) zálohování 3x týdne do online uložiště od poskytovatele CESNET,
    b) server společnosti využívá jako ochranu dat před selháním disků RAID 1.
3) zpracování postupů obnovy systému po jejich selhání nebo výpadku se provádí v několika krocích
    a) kontrola připojení k internetu (max do 5 minut),
    b) každý samostatný reproduktor určený k rozhlasu automaticky vydá zvukovou signalizaci o jeho úspěšném propojení s hlavním serverem (max do 3 minut),
    c) dveřní systémy plně obnoví svou funkci a zahlásí jejich připravenost dlouhým zvukovým signálem (max do 3 minut),
    d) požární hlásič má na sobě zelenou a červenou diodu při správné funkci hlásiče dioda 2x problikne každých 30 sekund dle příručky výrobce (okamžitě),
    e) přístupnost k interním webovým stránkám (do 3 minut).
4) správy bezpečnosti počítačových sítí
    a) síť rozdělena na 4 podsítě (zaměstnanecká, síť pro žáky, síť pro zařízení (reproduktory, dveřní systém, obědový systém), síť pro hosty).
5) zajištění důvěrnosti informací pomocí kryptografické ochrany
    a) zaměstnanecké počítače užívají funkci bit locker,
    b) pro přístup povolaným zaměstnancům k serveru je použit SSH klíč.

6) ochrany před neautorizovanými zásahy dodržováním principu oddělení povinnosti a odpovědnosti při přidělování uživatelských práv
    a) o přidělení práv uživatelů se stará pověřený vedoucí pracovník a řídí se interní směrnicí.
7) zajištěním bezpečnosti elektronické pošty
    a) proškolením zaměstnanců a žáků školy tak aby dokázali rozeznat nevyžádanou či nebezpečnou poštu.
8) bezpečným zacházením s paměťovými médii.
    a) zaměstnanci jsou proškoleni v problematice zacházení s paměťovými médii,
    b) pro přenos dat mimo pracoviště zaměstnanci mohou využít flashdisky společnosti zamykatelné službou Locker+.
9) zajištění důvěryhodnosti informací před jejím přenosem do jednotlivých systémů společnosti.

Řízení přístupů

Účelem řízení přístupů bezpečnosti je omezeni přístupu k informacím společnosti, aby k nim měli přístup pouze oprávnění uživatelé.

1) Správa přístupů do systémů
    a) přístupy uživatelům zajišťuje a přiděluje povolaný vedoucí pracovník,
    b) při přidělování přístupů se řídí interní směrnicí pro přidělení přístupů dle zařazení uživatele žádajícího o přístup (žák, administrativní pracovník, učitel, zákonný zástupce žáka).
2) Přidělení přístupů do prostor s osobními informacemi
    a) je přidělován pouze pověřeným pracovníkům pro práci s osobními údaji.
3) Přístupy na síť a použití VPN pro vzdálenou práci
    a) pro přístup do vnitřního systému zaměstnanci používají open VPN, přístup jim je přidělován po konci zkušební doby.

Vývoj a údržba systémů

Účelem je prosadit bezpečnost informací jak při softwarovém upgradu, tak při hardwarovém upgradu informačního systému. Bezpečnostním cílem je zajištění ochrany

1) analýza a specifikace bezpečnostních požadavků společnosti při výběru nového hardwaru i softwaru,
2) zajištění přesnosti a spolehlivosti zpracování dat upravovaných v aplikacích a kryptografická opatření,
    a) Zajištění, aby veškeré aktualizace a zásahy do systémů nevedly ke snížení bezpečnosti informací společnosti.
3) bezpečnost systémových souborů a procesu vývoje a podpory (zdrojové kódy, hesla, klíče).
    a) Společnost používá zajištění svého chodu zařízení vyrobená na míru pro jejich specifické potřeby. Zdrojové kódy spadají pod vlastnictví společnosti a společnost zajišťuje jejich bezpečnost zálohováním na externí uložiště mimo běžící systém školy.

Řízení kontinuity činností

Bezpečnostním cílem je zajištění přípravy, proškolení a připravenosti zaměstnanců společnosti po odborné stránce k výkonu činností spojených s řešením krizových situací, ochranou zdraví, života zaměstnanců a ochranou majetku.

1) Řízení společnosti v krizovém režimu při vzniku krizového incidentu
    a) Proškolení zaměstnanců v případě epidemie/pandemie
        1) Zaměstnanci musejí dbát na dodržování všech doporučení a nařízení hygienické stanice pod kterou společnost spadá,
        2) V případě potřeb je škola vybavena na provozování online výuky (každý žák má přidělený vlastní školní notebook či tablet).
    b) Proškolení zaměstnanců s vedením výuky v případě výpadku proudu, havárie vody, selhání klimatizace či jiných důležitých systémů pro plynulý chod společnosti,
    c) Seznámení zaměstnanců i žáků s evakuačním plánem v případě požáru nebo jiného živelného ohrožení.

Legislativní a smluvní požadavky na bezpečnost informací

Bezpečnost informací i celková bezpečnostní politika je realizována v souladu s legislativními a smluvními požadavky zákonů a jiných právních předpisů. V rámci společnosti musí být veden přehled platných norem a předpisů.

1) Dodržení ustanovení o autorském právu a licenčních podmínek svých dodavatelů.
    a) Veškerý software i hardware společnost používá v souladu s licenčními podmínkami dodavatelů a platí případné licence pro jeho použití.
2) Společnost přijímá a provádí opatření k zajištění ochrany osobních a citlivých údajů dle zákona 110/2019 Sb.

Společnost dokládá potvrzení o shodě s reálným stavem zabezpečení a dokumentem Bezpečnostní politika.

Kritéria hodnocení rizik

Bezpečnostní opatření byla stanovena na základě hodnocení aktiv společnosti, následnému hodnocení rizik a provedené analýze rizik. Hodnocení rizik je prováděno na základě následujících kritérií:

1) dle požadavků na dostupnost, důvěrnost a integritu osobních údajů,
2) určení dopadů identifikovaných hrozeb dle ohrožení firemních aktiv a zisků,
3) reálné pravděpodobnosti identifikovaných hrozeb,
    a) při posuzování pravděpodobnosti byla hodnocena geografická poloha společnosti,
    b) zaměření společnosti její zájem podnikání.
4) určení akceptovatelné úrovně rizika dle metody PNH.

Stanovení obecných a specifických odpovědností pro osobní údaje

Odpovědnost pro oblast bezpečnosti informací společnosti jsou pro její zaměstnance uzpůsobeny vnitřními směrnicemi. Bezpečnostní politiku jsou povinni dodržovat všichni zaměstnanci společnosti a za kontrolu jejich plnění odpovídají vedoucí zaměstnanci dle pracovního zařazení. Odpovědnost pro bezpečnost informací osobních údajů je dále upravena zákonem a evropským nařízením GDPR.

Závěrečná ustanovení

Tento dokument bezpečnostní politiky nabývá účinnosti dnem 1. 9. 2021

10 ZÁVĚR

Cílem této bakalářské práce bylo popsat bezpečnostní politiku a demonstrovat ji na modelovém příkladu. Jako modelové příklady jsem si vybral Soukromou Školu Hostivař, která se nachází na Praze 10. Z této školy je pro účely této bakalářské práce pořízeno několik fotek na základě, kterých je demonstrován aktuální stav zabezpečení školy.

Pro vybraný podnik v praktické části této práce byla provedena identifikace aktiv, identifikace hrozeb a následná analýza rizik podle metody PNH. Výsledkem praktické části je zjištění nejcitlivějších částí podniku a návrh opatření pro minimalizaci či úplné potlačení analyzovaných rizik. Z této práce vyplynulo několik připomínek k bezpečnostnímu řešení Soukromé Školy Hostivař, které byly díky této bakalářské práci sděleny vedoucím pracovníkům školy a mají možnost tyto připomínky zapracovat a vylepšit tak bezpečnost svého podniku. Pro tento podnik byl také na míru vytvořen dokument Bezpečnostní politika, ve kterém byla podchycena identifikovaná rizika z analýzy rizik a zpracována protiopatření kterými, by se podnik měl řídit, aby zachoval svou důvěryhodnost a předešel problémům při případném vzniku bezpečnostního incidentu.

V teoretické části této práce je popsán úvod do problematiky bezpečnostní politiky firem, vysvětlen význam dokumentu Bezpečnostní politika a detailně popsána jeho struktura. V další částí byla rozebrána analýza rizik podniku a popsány metody, kterými lze bezpečnostní analýzu rizik provádět, jako je analytická metoda SWOT, PNH, GAP, BIA nebo FMEA. Dále se tato práce zabývá problematikou GDPR v souvislosti s bezpečností podniku. A v neposlední řadě v teoretické části jsou zmíněny a popsány další dva zásadní dokumenty podniku. Požární ochrana a Bezpečnost a ochrana zdraví při práci. Při studiu materiálů k této bakalářské práci jsem pochopil, že investovat do odborného zpracování bezpečnostní politiky podniku může být pro podnik velmi výhodná investice, protože pokuty za nedodržení legislativy, případně výdaje za škodné události, které pojišťovna neproplatí z důvodu nevyhovujícího zabezpečení, mohou značně převýšit cenu za odborné zpracování Bezpečnostní politiky podniku

SEZNAM POUŽITÉ LITERATURY

[1] Bezpečnostní politika podniku [online]. [cit. 2020-07-06]. Dostupné z: https://managementmania.com/cs/bezpecnostni-politika-security-policy

[2] BP implementace ISO 27001 [online]. [cit. 2021-08-06]. Dostupné z: https://is.ambis.cz/th/yz387/Cegan_BP_Implementace_ISO_27001.pdf

[3] Bezpečnostní politika podniku [online]. [cit. 2020-07-06]. Dostupné z: https://managementmania.com/cs/incident

[4] Zásady tvorby bezpečnostní dokumentace informačních systémů určených k nakládání s utajovanými informacemi [online].[cit. 2020-6-08] Dostupné z: https://www.nbu.cz/download/bezpecnost-informacnich-systemu/DokumentaceIS-vzor.docx

[5] Bezpečnostní politika a související dokumenty [online].[cit. 2020-4-08] Dostupné z: https://www.cleverandsmart.cz/bezpecnostni-politika-a-souvisejici-dokumenty/

[6] KINDL,Jiří.Projektování bezpečnostních sysémů 1.díl.Zlín:Univerzita Tomáše Bati ve Zlíně,2004ISBN 80-7318-165-7.

[7] Co je BOZP? Definice, cíle, legislativa a principy [online].[cit. 2020-4-08] Dostupné z: https://www.bozp.cz/aktuality/co-je-bozp/

[8] Základní dokumentace BOZP v podniku [online].[cit. 2021-4-08] Dostupné z: https://zsbozp.vubp.cz/bozp-obecne/599-zakladni-dokumentace-bozp-v-podniku

[9] Dokumentace PO [online].[cit. 2020-4-08] Dostupné z: https://zsbozp.vubp.cz/pozarni-ochrana/dokumentace-po/490-jak-zpracovat-dokumentaci-pozarni-ochrany

[10] Zákon o požární ochraně [online].[cit. 2021-6-08] Dostupné z: https://www.zakonyprolidi.cz/cs/1985-133

[11] Kompletní průvodce kybernetickou bezpečností [online]. [cit. 2020-27-07]. Dostupné z: https://cs.vpnmentor.com/blog/kompletni-pruvodce-kybernetickou-bezpecnosti-pro-male-stredni-firmy/

[12] RIZIKA A JEJICH ANALÝZA [online]. [cit. 2020-27-07]. Dostupné z: https://fei1.vsb.cz/kat420/vyuka/Magisterske%20nav/prednasky/web/RIZIKA.pdf

[13] KRACK [online]. [cit. 2021-27-06]. Dostupné z: https://cs.wikipedia.org/wiki/KRACK

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

[15] Hrozba [online]. [cit. 2021-27-06]. Dostupné z: https://managementmania.com/cs/hrozba-threat

[16] Securityjourney. 808 Ribbonleaf Lane Fuquay Varina, North Carolina 27526, 2020. Do-stupné z: https://www.securityjourney.com/

[17] Heslo [online]. [cit. 2021-27-06]. Dostupné z: zdroj https://www.internetembezpecne.cz/internetem-bezpecne/navody/heslo

[18] Analýza podnikatelských rizik [online]. [cit.2020-01-08]. Dostupné https://is.ambis.cz/th/yu9i6/Jan_Petira_management_organizaci.pdf

[19] Metodika analýzy rizik [online]. [cit. 2020-01-08]. Dostupné http://download.microsoft.com/documents/cs-cz/Priloha-1_Metodika-analyzy-rizik_health.pdf

[20] Metodika pro identifikaci a hodnocení aktiv a rizik [online]. [cit. 2020-03-08]. Dostupné z: https://mestokladno.cz/assets/File.ashx?id_org=6506&id_dokumenty=1474792

[21] Bussines impact analysis [online]. [cit. 2021-03-06]. Dostupné z: https://cs.wikipedia.org/wiki/Business_Impact_Analysis

[22] RAC ISSEC: RAC Information System Security Examination Cycle [online]. [cit. 2021-03-06]. Dostupné z: https://macek.rac.cz/rac/homepage.nsf/CZ/ISSEC

[23] Diferenční analýza [online]. [cit. 2021-03-06]. Dostupné z: https://managementmania.com/cs/diferencni-analyza

[24] PEST analýza [online]. [cit. 2021-03-06]. Dostupné z: https://edolo.cz/clanky/pest-analyza/

[25] Winterlingova krizová matice [online]. [cit. 2021-03-06]. Dostupné z https://managementmania.com/cs/winterlingova-krizova-matice

[26] FMEA. [cit. 2021-03-06]. Dostupné z: https://cs.wikipedia.org/wiki/FMEA

[27] ANALÝZA RIZIK V PRMYSLOVÉM PODNIKU [online]. [cit. 2021-03-06]. Dostupné z https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=54380

[28] SWOT Analýza [online]. [cit. 2020-013-06]. Dostupné z: https://cs.wikipedia.org/wiki/SWOT

[29] Evropské nařízení GDPR [online]. [cit. 2020-16-06]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:32016R0679

[30] Příručka GDPR pro malé a střední podniky [online]. [cit. 2020-016-06]. Dostupné z:https://www.gdpr-experts.cz/userfiles/docs/prirucku_pro_pripravu_malych_a_s.pdf

[31] Interní zaměstnanci jako hrozba pro vaši firmu [online].[cit. 2020-4-08] Dostupné z: https://computerworld.cz/securityworld/ohrozuji-vas-hrozby-od-internich-za-mestnancu-54597

[32] Pomůcka pro určení velikosti podniku [online]. [cit. 2020-01-08]. Dostupné http://prahafondy.ami.cz/cz/oppa/pro-prijemce/325_pomucka-pro-urceni-velikosti-podniku.html

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

IoT	Internet of things.
IT	Information technology
KRACK	Key Reinstallation Attacks
PO	Požární ochrana
SSH	Secure Shell
RAID	Redundant Array of Inexpensive Disks
RFID	Radio Frequency Identification

SEZNAM OBRÁZKŮ

SEZNAM TABULEK