Bezpečnostní politika podniku

Karel Minichbauer

Bakalářská práce
2020

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

Ústav bezpečnostního inženýrství

Akademický rok: 2019/2020

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 a Company**

Zásady pro vypracování

1. Seznamte se s pojmem bezpečnostní politika.
2. Stanovte klíčové oblasti bezpečnosti v podniku.
3. Věnujte pozornost problematice GDPR v souvislosti s bezpečnostní politikou.
4. Popište strukturu bezpečnostní politiky pro malé a střední podniky.
5. Demonstrujte návrh struktury na modelovém příkladu.

Rozsah bakalářské práce:
Rozsah příloh:
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: **7. prosince 2019**
Termín odevzdání bakalářské práce: **25. května 2020**

L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

Ing. Jan Valouch, Ph.D.
ředitel ústavu

Jméno, příjmení: Karel Minichbauer

Název bakalářské práce: Bezpečnostní politika podniku

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 a jeden výtisk bude uložen u vedoucího práce;
- 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 – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování 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 11.8.2020

Karel Minichbauer v.r.
podpis diplomanta

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 koronavirové krize. Ing. Jiřímu Minichbauerovi a celé mé rodině za cenné rady a podporu při dokončování mé práce a celého studia.

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

……..…….……..
vlastnoruční podpis autora bakalářské práce

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 mé práci se budu zabývat fiktivní firmou AURORA INOVATIONS jejichž předmětem podnikání je vývoj software na zakázku. Z předmětu podnikání vyplývá že je nutné chránit jak firmu, tak její zákazníky před únikem citlivých informací jako je výrobní tajemství nebo informace o klientech či jejich zakázkách, proto je nutné zpracovat dokumenty, které deklarují bezpečnost podniku. Takový dokument se nazývá „Bezpečnostní politika“.

Bezpečnostní politika řeší hrozby, které mohou vzniknout během chodu podniku a rizika z nich vyplývající. Obsahuje také ale i bezpečnostní opatření, kterými se snaží rizika potlačit nebo alespoň minimalizovat škody jimi způsobené. Celou tuto problematiku popíši v této práci ve dvou částech.

V první teoretické části se budu zabývat bezpečnostní politikou podniků (dále jen BPP), kde si popíšeme klíčové oblasti. V druhé praktické části je uveden vzor dokumentu „Bezpečnostní politika“ vytvořený přímo pro již zmiňovanou firmu AURORA INOVATIONS.

I. TEORETICKÁ ČÁST

1 BEZPEČNOSTNÍ POLITIKA

Každý podnik bez ohledu na svou velikost a předmět podnikání musí dodržovat určité bezpečnostní zásady, které vycházejí z platné legislativní normy ISO/IEC 27001. Tyto 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, jako je např. Provozní řád informačního systému, který bývá součástí dokumentů, kterými se řídí bezpečnost podniku. Souhrn těchto dokumentů obsahuje pravidla, kterými se musí podnik ve vlastním zájmu řídit, aby byl zajištěn jeho bezproblémový chod.

Nedodržování těchto pravidel může vést až k jeho zániku. V zájmu každého podniku je zajistit dodržování všech pravidel uvedených v „Bezpečnostní politice“ a s ní souvisejícími dokumenty. Dodržováním těchto pravidel se minimalizují dopady takzvaných incidentů.[1] Incidenty můžeme kategorizovat dle oblastí ve kterých vznikly [2]:

- **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[22]:

- 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 dodržet danou strukturu, která by měla obsahovat několik částí[23]:

- **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) [22]

- **Personální bezpečnost**

  V části Personální bezpečnost dokumentu „Bezpečnostní politika“ se zabývá například základními požadavky na stávající i nové pracovníky podniku jako jsou např. vzdělání, způsobilost k výkonu dané práce, odborná školení, pravidelná doškolování pracovníků atd. [22]

- **Počítačová bezpečnost**

  V části Počítačová bezpečnost se zabývá deklarováním minimálních požadavků na zabezpečení počítačové sítě dle § 7 a 8 vyhlášky č. 523/2005 Sb. Jinými slovy se v této části bezpečnostní politiky budeme zabývat (například identifikací a autentizací, zabezpečením portů či ochranou utajovaných informací v době servisní činnosti) [22]

- **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. [22]

- **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. [22]

- **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) [22]

- **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) [22]

- **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. [22]

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. [25]
- **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. [25]

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. [25]

Obr. 1 Dokumenty a jejich účel[25]

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 nejzákladnějších bodů zájmu bezpečnostní politiky je objektová bezpečnost. Tento bod se nachází bez výjimky v každé firmě.

Rozdělení:

2.1.1 Mechanická ochrana

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.[14]

2.1.2 Režimová ochrana

týká se zejména činnosti pracovníků v objektu, činnosti a pohybu osob přicházejících zvenčí, můžeme je rozdělit do dvou kategorií režimových opatření:

-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)

-vnitřní (zabývá se zejména pohybem osob uvnitř chráněného objektu, k zajištění jejich bezpečí a zamezení úniku informací skrze vlastní lidi)

2.1.3 Fyzická ochrana

zájmový objekt je střežen strážným, který má za úkol dohlédnout na to, aby do objektu nevstupovaly nepovolané osoby.

2.1.4 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.

3 OCHRANA ZDRAVÍ PŘI PRÁCI

Důležitým bodem zájmu chránícím jak zaměstnance před pracovními úrazy, tak podnik před případným soudním sporem mezi ním a zaměstnancem, který si například zanedbáním svých povinností způsobil vážnější úraz.

BOZP se upravuje pomocí dokumentu, který spadá pod Bezpečnostní politiku podniku, který zaměstnanec podepisuje v den prvního nástupu na pracoviště, většinou se tak děje v den uzavření pracovní smlouvy[27].

Každý dokument BOZP musí splňovat následující body:

- 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.[26]

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. [7]

5.1.1 Určení zranitelných míst v podniku

Identifikovat nejdůležitější data podniku. 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. [11]

5.1.2 Ochrana firemních zařízení

První krok, který zajistí, že systémy nejsou zranitelné vůči kybernetickým útokům, jsou vždy aktuální verze softwaru. [7]

- **Ochrana před viry** V současné době je zapotřebí investovat do antivirových programů. A to z důvodu ochrany podnikových zařízení před. Malware a 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).[7]
- **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, které 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 wifi protokolu s názvem KRACK na který museli reagovat všichny 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. [7]

- **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. [7]

5.1.3 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. [8]
- **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 pro potřebná pro chod podniku)
    - Síť návštěvníků je síť oddělená od interní a slouží pro připojení například návštěv, či připojení soukromých zaměstnaneckých zařízení k internetu) [7]

6 DOPADY LIDSKÉHO FAKTORU

Z pohledu bezpečnosti informací velmi mnoho malých a středních podniků podceňuje takzvanou vnitřní hrozbu[13].

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 nedokážou ochránit před novými typy hrozeb. [8] 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[24].

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“ [13].

Bezpečnostní hrozby způsobené selháním lidského faktoru[8] [24].:

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

6.1.1 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 kombinace několika znakových sad (čísla, velká písmena s diakritikou, malá písmena s diakritikou či speciální znaky, jako je křížek, hvězdička apod.) [7]

- **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.

- **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.

6.1.2 Nevyžádaná pošta

Zaměstnanci podniku se mohou potýkat v denním pracovním režimu s řadou útoků mířených na podnik v kterým, 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 útoků[13].

6.1.3 Oběť sociálního inženýrství

Zaměstnanci se také mohou stát obětmi 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[13].

6.1.4 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 sítových 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[13].

6.1.5 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. [24].

6.1.6 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[13].

- Prvním krokem je udělovat zaměstnancům oprávnění přístupu pouze k informacím které nezbytně potřebují k výkonu své práce, tím minimalizovat riziko prozrazení firemního know-how. [12] [24].
- 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. [8] [24].

6.1.7 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 a 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[13] [24]..

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 znovupořízení a částce rovnající se ušlému zisku podniku při jejich ztrátě, odcizení či zneužití. [12]

Obrázek 1 Proces analýzy rizik [12]

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. [12]

7.1.1 Hrozba

Hrozba je událost, síla nebo osoby jejichž působení mohou způsobit poškození, zničení nebo ztrátu hodnoty aktiv. Hrozba může ohrozit bezpečnost jakéhokoliv systému či podniku. [12] [20]

Jako hrozby ovlivňující podnik můžeme brát například[20]:

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

7.1.2 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 financím ztrátám podniku nebo dokonce k ukončení jeho činnosti. Může mít nepříznivé dopady na obchodní partnery, zákazníky i zaměstnance. Aktiva dělíme do dvou základních skupin[18]:

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

Tabulka hodnocení aktiv:

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

Obrázek 3 Hodnocení aktiv[18]

7.1.3 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 ujmu na zdraví, ztrátu života či způsobit poškození životního prostředí[20].

Riziko je také přímo spjato s místem a časem působením vnějších vlivů. [12]

Obrázek 2 Úroveň rizik [28]

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.

7.1.4 Bezpečnostní opatření

Bezpečnostní opatření jsou taková opatření, která snižují riziko. Je to například nastavení povinné změny hesla k přístupu do důležitých informačních systémů. [12]

7.1.5 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[21].

Při zpracovávání metody FMEA postupujeme postupně dle několika bodů[21]:

- 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.

7.1.6 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. [10]

- **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 ovlivňující dané riziko. [10]

Všechny tyto body se určují v rozsahu od **1-5**. [17]

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

Tabulky hodnot pro tvorbu analýzy PNH[9]:

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 3 Stupně hodnocení rizik metody PNH [9]

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 4 Míra rizika [9]

7.1.7 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.[3]

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.[3]

Obrázek 5 SWOT analýza .[3]

8 GDPR A BEZPEČNOSTNÍ POLITIKA PODNIKU

General Data Protection Regulation do češtiny přeloženo jako Obecná nařízení na ochranu osobních údajů (dále jen GDPR). Toto nové 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.

8.1.1 Definice Osobních údajů

Aby BPP mohla fungovat v souladu s GDPR musí každá organizace seznámit všechny pracovníky, kteří zpracovávají osobní údaje s tím, co to vlastně osobní údaje jsou a jak se mají chránit. Osobní údaje jsou definovány jako veškeré informace vztahující se k identifikovatelné fyzické osobě. Jako obecné osobní údaje bereme věk a datum narození, osobní stav, IP adresu, fotografický záznam, tzv. organizační údaje (e-mailová adresa, telefonní číslo či různé identifikační údaje vydané státem).

Naopak z působnosti GDPR jsou vyloučeny anonymizované údaje, údaje zemřelých osob a údaje získané v rámci činnosti čistě osobní povahy, které nemají obchodní či institucionální charakter. Týká se to tedy údajů, které zpracováváme pro osobní potřebu a s nikým je nebudeme sdílet.[6]

8.1.2 GDPR ve vztahu k osobním údajům zaměstnanců

S novým nařízením evropské unie GDPR vzniká každému podniku povinnost zpracovávat osobní data svých zaměstnanců v souladu s tímto nařízením a dodržovat při tom veškeré povinnosti správy osobních vycházející z této evropské směrnice zejména u zpracování těchto dat.

Personální a mzdová agenda je pro tuto oblast základní oblastí zpracování údajů, ke které není třeba souhlasu se zpracováním, neboť se odbývá téměř výlučně na základě plnění zákonných povinností zaměstnavatele, nebo v rámci plnění pracovní smlouvy, eventuálně

v rámci naplňování oprávněného zájmu zaměstnavatele. Zahrnuje v sobě činnost [6]

8.1.3 Před vznikem pracovního poměru

Nastávají situace, kdy podnik potřebuje shromáždit a zpracovat osobní údaje ještě před tím než mezi podnikem a osobou vznikne jakýkoliv právní vztah. Jedná se zejména o náborové řízení, kdy podnik potřebuje zpracovat životopis dané osoby obsahující citlivé osobní údaje. Tento proces lze zařadit pod personálně-mzdovou agendu a není tedy pro ně nutný souhlas subjektů údajů. [5] V případě, že mezi uchazečem a podnikem nevznikne jakýkoliv právní vztah, je podnik povinen tyto údaje bezpečně zlikvidovat.[5]

8.1.4 V průběhu pracovního poměru

Přijímací řízení jehož nedílnou součástí nyní práce s osobními údaji zaměstnanců, bez níž si nelze realizaci pracovněprávního vztahu vůbec představit. Součástí je nejen evidence mezd, dalších odměn, dávek sociálního zabezpečení a sociálního pojištění, dovolené nebo evidence docházky zaměstnanců, jejich služebních cest a podobně, ale i činnost jako je použití fotografií nebo biometrických prvků na průkazech zaměstnanců nebo v jejich přístupových údajích, evidence pracovní docházky nebo vstupů zaměstnanců do jednotlivých prostor organizace zaměstnavatele, evidence pracovních úrazů, nemocí z povolání,
vyřizování stížností zaměstnanců nebo povinné uchovávání dokumentace po ukončení pracovněprávního vztahu. Zpravidla půjde o zpracování kvůli právní povinnost, plnění smlouvy, nebo z důvodu oprávněného zájmu (ochrana majetku apod.).[5]

8.1.5 Po ukončení pracovního poměru

Při ukončení pracovního poměru podnik postupně ztrácí důvody pro zpracování některých údajů zaměstnanců, podnik je povinen veškeré tyto údaje bezpodmínečně odstranit.

Jedná se například o biometrické údaje zaměstnance či údaje o rodině. Podnik ovšem nemůže na ráz odstranit veškeré údaje o zaměstnanci, ale musí si zachovat údaje nutné pro případné dokazování zdanitelných položek pro FÚ, jako jsou služební cesty, výplatní pásky, mzdové listy docházka zaměstnance či informace o jeho úrazech na pracovišti. Tyto údaje je firma dokonce povinna si uschovat nejméně po dobu promlčecí doby danou zákonem.[5]

8.1.6 Sankce

Za nedodržení správných postupů při práci s GDPR může být podnik pokutován. Podle článku 83 odst. 4 nařízení GDPR může výše pokut dosáhnout až 10 000 000 EUR. Jedná-li se o korporátní podnik pokuty mohou být až do výše 2 % celosvětového ročního obratu, a to například při porušení postupů povinností týkajících se jmenování pověřence pro ochranu osobních údajů a výkonu jeho činnosti, podmínek a náležitostí smluvního vztahu mezi správcem a zpracovatelem osobních údajů.

Dále podle článku 83 odst. 5 nařízení GDPR může úřad v určitých případech uložit ještě vyšší pokuty, a to až do výše 20 000 000 EUR nebo, jde-li o korporátní podnik, tak až do výše 4 % celosvětového ročního obratu. Tyto nejvyšší možné sankce může úřad ukládat například při porušování (resp. nedodržování) základních zásad zpracování osobních údajů stanovených nařízením.

II. PRAKTICKÁ ČÁST

9 MODELOVÝ PŘÍKLAD BEZPEČNOSTNÍ POLITIKY PODNIKU

Celou problematiku bezpečnostní struktury a bezpečnostní politiky podniku Vám představím v praktické ukázce.

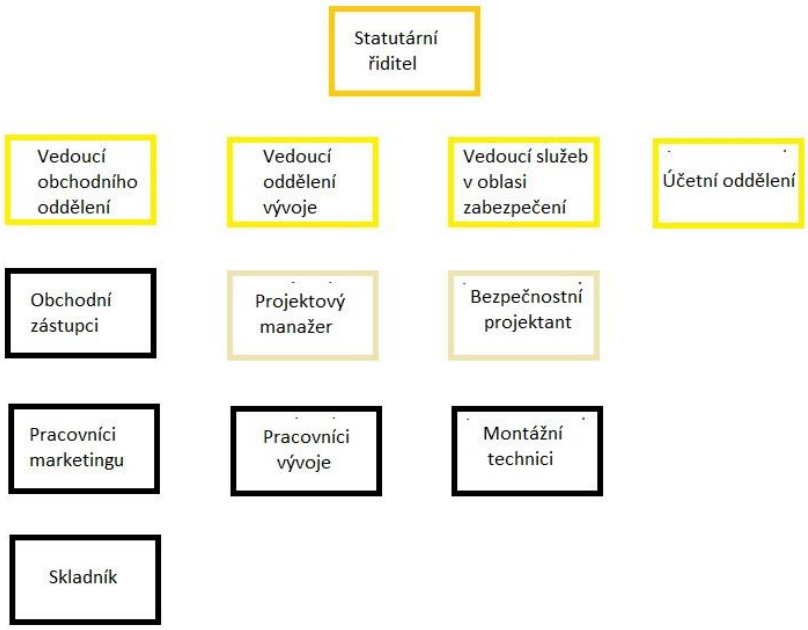
9.1 Popis virtuálního podniku

Pro ukázku bezpečnostní politiky podniku jsem vytvořil fiktivní firmu s názvem AURORA INOVATION, s.r.o. zabývající se zakázkovým vývojem softwaru, obchodem, technickým zabezpečením objektů a vývojem IoT technologií. Jedná se o malý podnik[19] s dvaceti pěti zaměstnanci sídlící v kancelářské budově s recepcí v mimo zátopové oblasti v Praze, Hostivaři.

9.1.1 Organizační struktura podniku

Zaměstnanci podniku AURORA INOVATION, s.r.o. jsou rozděleni do čtyř oddělení každé oddělení má svého vedoucího který se zodpovídá statutárnímu řediteli.

- Oddělení vývoje: Jeho vedoucí odpovídá za chod celého oddělení a několik projektových managerů, kteří se starají o rozdělení prací mezi vývojáře a o úspěšné dokončování projektů.
- Obchodní oddělení: Jeho vedoucí odpovídá za chod oddělení, jehož úkolem je vyhledávání a zpracování maloobchodních a velkoobchodních zakázek. Prodej mají na starost obchodní zástupci podniku společně se skladníkem. Marketingoví pracovníci mají na starost prezentování podniku a tvorbu propagačních materiálů.
- Oddělení bezpečnostního technického zabezpečení služeb: Jeho vedoucí odpovídá za technický provoz, výrobu a montáž mají na starost projektanti zabezpečovacích systémů a montážní dělníci.
- Účetní oddělení dohlíží na zpracování a archivaci faktur a veškerých důležitých podnikových dokumentů.



Obrázek 6 Organizační struktura podniku

9.2 Analýza rizika

Pro analýzu rizik jsem provedl identifikaci ke zjištění, která aktiva podniku jsou nejdůležitější a je třeba zabránit jejich poškození ztrátě či znehodnocení.

V dalším kroku identifikuji hrozby podniku, které jakýmkoliv způsobem ohrožují podniková aktiva a provedu nad nimi analýzu PNH.

9.2.1 Identifikace a hodnocení aktiv

V následující tabulce jsem vybral a ohodnotil nejzásadnější aktiva výše uvedeného podniku.

Typ aktiv	**Aktivum**	**Slovní ohodnocení**
Nehmotné	Informace/data	Kritické
	Zdrojové kódy	Kritické
	Dokumenty	Vysoký
Hmotná	Hardware	Střední
	Vybavení laboratoře	Nízký
	Servery	Střední
	Datová uložiště	Kritický
	Firemní auta	Nízký
	Vybavení techniků	Nízký
	Uskladněné zboží	Vysoké
Lidské zdroje	Zaměstnanci (management, technici, vývojáři …)	Kritické

Tabulka 1 Identifikace aktiv

9.2.2 Identifikace hrozeb

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

Hrozby	Pravděpodobnost hrozby	Příklad související se zranitelností
Požár	Vysoká	Přítomnost elektrotechniky a laboratoř vybavená pájecí stanicí
Vloupání do podniku	Vysoká	Uložení dokumentací a smluv v podniku
Selhání techniky	Střední	Náchylnost techniky na prach a vlhkost
Únik dat	Vysoká	Podnik provádí práci na vývoji software a hardware
Ztráta dat	Střední	Provoz cloudu navázaného na podnikové aplikace
Terorismus/ sabotáž	Nízká	Konkurenční či politický boj
Výpadek energie	Střední	Vyřazení všech služeb a provozů podniku
Epidemie	Střední	V souvislosti s onemocněním COVID-19
Výpadek internetu	Střední	Vyřazení části služeb a provozů podniku
Vykradení skladu	Nízké	Uskladněné zboží vyšší hodnoty

Tabulka 2 Identifikace Hrozeb

9.2.3 Analýza rizik dle metody PNH

Pomocí metody PNH vypočítáme rizika vyplívající s identifikovaných hrozeb. [17]

Hrozby	P	Z	H	Riziko	Přijatelnost	Opatření
Požár	3	5	5	75	Nežádoucí riziko	Protipožární systém
Vloupání do podniku	2	3	3	18	Mírné riziko	Čipové karty, bezpečnostní zámky, kamera u vchodu
Selhání techniky	2	3	3	18	Mírné riziko	Přepěťové zásuvky
Únik dat	3	4	5	60	Nežádoucí riziko	Dodržování zásad kybernetické bezpečnosti
Ztráta dat	1	4	5	20	Mírné riziko	Záloha dat
Terorismus/ sabotáž	1	5	5	25	Mírné riziko	Kontrola návštěv podniku
Výpadek energie	1	3	5	15	Mírné riziko	Záložní zdroj UPS
Epidemie	3	3	3	9	Akceptovatelné riziko	Dodržování hygieny
Výpadek internetu	1	2	3	6	Akceptovatelné riziko	Sekundární poskytovatel připojení
Vykradení skladu	1	3	3	9	Akceptovatelné riziko	Alarm

Tabulka 3 Analýza rizik

9.2.4 Výsledky analýzy rizik

Na základě identifikace aktiv a hrozeb jsem sestavili analýzu rizik pomocí metody PNH, která nám ukázala na nejproblematičtější části podniku a dala nám možnost zamyslet se nad tím jaké kroky udělat pro minimalizaci či úplné odstranění rizik.

Nejproblematičtější částí podniku, kde riziko přerostlo v nežádoucí byly:

- Riziko vzniku požáru
- Riziko úniku dat

Proti kterým byla podniku navrhnuta opatření.

9.2.5 Odstranění rizik

Pro omezení rizik vyplývajících z analýzy rizik je nutné podle závažnosti provést opatření, která odstraní nebo minimalizují rizika. opatření by nemělo finančně převyšovat hodnotu chráněného aktiva.

- Nejúčinnějším způsobem odstranění rizika ztráty dat je například změna technologie jako je změna ukládání dat z podnikových diskových polí do cloudu.
- Pro minimalizaci rizika požáru můžeme udělat celou řadu opatření. Nejdůležitějším opatřením je instalace protipožárního systému v místech, kde je nebezpečí vzniku požáru vysoké, je nutné pravidelně dělat revize elektrických zařízení používaných v prostorách podniku a dbát na správné proškolení zaměstnanců o bezpečnosti práce.
- Zabezpečení informací a dat proti úniku lze realizovat v následující bodech. Nejdůležitějším bodem je dbát na dodržování zásad kybernetické bezpečnosti. Dalšími důležitými body je dostatečné proškolení zaměstnanců, správné nastavení interních předpisů podniku a zamezení kopírování dat na soukromá média.

9.3 Dokument Bezpečnostní politika

Ukázka dokumentu [23] „ Bezpečnostní politika“ pro podnik AURORA INOVATION

Úvodní ustanovení

1. Vedení společnosti AURORA INOVATION, s.r.o. (dle jen AI) stanovuje bezpečnostní politiku, která je platná pro všechny zaměstnance společnosti, kteří pracují s důvěrnými informacemi podniku nebo k nim mají z jakéhokoliv důvodu přístup. Tato bezpečnostní politika obsahuje zásady bezpečnosti informací.
2. K zajištění bezpečnosti informací ve společnosti AI se touto bezpečnostní politikou:
    a. popisuje bezpečnost informací
    b. stanovuje cíle bezpečnosti
    c. stanovuje bezpečnostních zásady
3. Bezpečnost informací je definována jako důvěrnost, integrita a dostupnost informací v podniku.
    a. důvěrnost je zajištěna tím, že jsou jednotlivým pracovníkům zpřístupněny takové informace, které potřebují k výkonu své práce a mají k nim přiděleno potřebné oprávnění.
    b. integrita je zabezpečena přesnosti a kompletnosti informací a metod jejich zpracování
    c. dostupnost zajištění přístupnosti všem pověřeným osobám ke všem informacím a datům, ke kterým mají povolen přístup v době, kdy je potřebují.

4. Cílem bezpečnostní politiky informací je bezpečnost informací ve společnosti AI a zajištění dostupnosti informačních aktiv pouze oprávněným osobám a ochrana informací proti náhodnému nebo neoprávněnému zničení, zneužití, či ztrátě, proti neoprávněnému přístupu, změnám nebo šíření, a to v souladu se zákony a jinými právními předpisy ČR.
5. Bezpečnost informací pokrývá celou strukturu společnosti AI.
6. Tato politika se 1x ročně podrobuje posouzení aktuálnosti.
7. Za posouzení aktuálnosti dokumentu bezpečnostní politiky informací jsou odpovědní vedoucí pracovníci jednotlivých oddělení.
8. Tento dokument byl vypracován se záměrem vedení společnosti AI k ochraně informačních aktiv v souladu se zákony a jinými právními předpisy ČR.

Zásady bezpečnosti informací

1. Zaměstnancům a klientům společnosti AI v zájmu dodržení bezpečnosti informací vedení podniku zaručuje[23]:
    a. ochranu práv a svobod jednotlivců, zejména právo na soukromí uznané v článku 7 Úmluvy o ochraně lidských práv a základních svobod, usnesení předsednictva ČNR č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky.
    b. ochranu osobních údajů dle zákona.
    c. ochranu obchodního tajemství podle zvláštního právního předpisu a obsahu smluv obchodně závazkových vztahů, pokud se k tomu společnosti AI v uzavřené smlouvě zavázala.
    d. ochranu listovního tajemství atd.

Organizace bezpečnosti

1. Ve společnosti AI vedení společnosti dohlíží a koordinuje implementaci bezpečnostních opatření uvnitř podniku dle stanovené působnosti a odpovědnosti vedoucích zaměstnanců. Cílem je zlepšení řízení a koordinace bezpečnosti informací ve společnosti dle normy ČSN ISO/IEC 27 001.
2. Kontrola dodržování implementace bezpečnostních opatření se provádí pravidelnými audity.
3. Dodržování a plnění bezpečnostní politiky zajišťují všichni vedoucí zaměstnanci společnosti AI dle stanovené působnosti a odpovědnosti.

Politika mobilních zařízení

1. Cílem této vnitřní úpravy je zajistit bezpečnost informací při užívání mobilních zařízení.
2. Každé firemní mobilní zařízení je evidováno a má instalovanou proaktivní ochranu před hrozbami.
3. V případě potřeby je zajištěno šifrování dat v zařízení kvůli případnému odcizení.

Politika práce na dálku

1. AI plně podporuje umožňující vykonávat plnohodnotnou práci mimo pracoviště po jejím schválení vedoucím příslušného oddělení.
2. Podmínkou pro výkon práce mimo kanceláře podniku dodržení veškerých bezpečnostních pravidel, tak aby nemohlo dojít k ohrožení informační bezpečnosti.

Bezpečnost lidských zdrojů

1. Cílem zabezpečení lidských zdrojů je snížení rizika lidské chyby, krádeže, podvodu nebo zneužití prostředků organizace ku vlastnímu prospěchu.
2. Prověření a posouzení uchazečů o zaměstnání z hlediska bezpečnosti je součást výkonu personálních činností dle Pracovního řádu a v souladu s obsahem pracovněprávních dokumentů.
3. Zaměstnanci společnosti AI před nástupem na svou pracovní pozici podepisují prohlášení o mlčenlivosti formou závazku zaměstnance ve smyslu zákonem uložené povinnosti.

4. Zaměstnanci AI jsou povinni zachovávat mlčenlivost o skutečnostech a systémových řešeních, se kterými se seznámili při plnění úkolů ve společnosti AI. Tato povinnost přetrvává i po skončení pracovního vztahu, pokud zvláštní právní předpis nestanoví jinak. V návaznosti na tuto skutečnost musí být zaměstnanec seznámen s povinnostmi a odpovědností z hlediska bezpečnosti informací při skončení nebo změně pracovního vztahu.
5. Zaměstnanci jsou seznámeni s bezpečnostní politikou podniku vždy při nástupu a poté periodicky zpravidla jednou za rok.
6. Každý zaměstnanec je povinen nahlásit veškeré bezpečnostní incidenty a musí znát přesný postup hlášení těchto incidentů.
7. Nedodržení bezpečnostních zásad může být kvalifikováno jako porušení povinností zaměstnance příp. porušení pracovní kázně s příslušnými důsledky pro zaměstnance. Případné vyšetřování porušení bezpečnostních zásad je v kompetenci vedoucího oddělení podniku, o jehož výsledku je vedoucí oddělení povinen v co nejkratší době obeznámit ředitele AI.

Klasifikace a řízení informačních aktiv

1. Za účelem udržení přiměřené ochrany aktiv stanovujeme zásady jejich klasifikace a řízení.
2. Data a informace společnosti AI jsou řízena a uchovávána podle předchozího posouzení hrozeb, zranitelností a rizik.
3. Dle klasifikace je určen způsob zacházení a ochrany daných informací.
4. Jsou stanovena pravidla pro manipulaci s médii obsahujícími důvěrné a utajované informace, včetně jejich likvidace.
5. Při ukončení pracovního poměru se zaměstnancem jsou přesně stanovené postupy týkající se ochrany informací svěřených zaměstnanci a navrácení aktiv.

Fyzická bezpečnost a bezpečnost prostředí

1. Účelem fyzické bezpečnosti a bezpečnosti prostředí je zejména předcházet neoprávněnému přístupu k informacím nebo jejich poškození či narušení.
2. Cílem fyzické bezpečnosti podniku je zajištění fyzické ochrany informací a prostředí, ve kterém se informace nacházejí pomocí:
    a. Kontroly vstupů a upřesnění způsobu práce mimo kanceláře či zasedací místnosti.
    b. Zabezpečení kanceláří a všech místností.
    c. Ochrany proti vnějším hrozbám
    d. Bezpečnostních prvků k zamezení odcizení či zničení informací,
    e. Zajištění služeb energie (dodávky energie, záložní zdroje elektrické energie, klimatizace atd.), zabezpečení kabeláže a zajištění pravidelné a bezpečné údržby zařízení
    f. Zajištění bezpečnosti informací mimo objekty společnosti AI
    g. Zabezpečení oblasti a definování fyzického bezpečnostního perimetru
3. Zajištění požární bezpečnosti podle zákonů a jiných právních předpisů (čidla, automatické hlásiče požáru včetně samo hasicích zařízení)
4. Uplatnění zásad čistého stolu a čisté obrazovky spadá do kompetence všech zaměstnanců na jejichž dodržování dohlíží vedoucí zaměstnanci.

10 ZÁVĚR

Cílem mé bakalářské práce bylo popsat bezpečnostní politiku a demonstrovat ji na modelovém příkladě. Pro demonstraci jsem si vytvořil malý fiktivní podnik AURORA INOVATION, s.r.o. zabývající se především vývojem softwaru, na kterém jsem v praktické části této práce demonstroval identifikaci aktiv, identifikaci hrozeb a následnou analýzu rizik podle metody PNH.

Výsledkem praktické části je návrh opatření zjištění nejcitlivějších částí podniku a návrh opatření pro minimalizaci či úplné potlačení analyzovaných rizik. Na základě výsledků analýzy rizik uvádím praktický příklad dokumentu „Bezpečnostní politika“.

V teoretické části této práce popisuji úvod do problematiky bezpečnostní politiky firem, vysvětluji význam dokumentu bezpečnostní politika a detailně popisuji jeho strukturu. V další částí rozebírám analýzu rizik bezpečnostní politiky a popisuji metody kterými lze bezpečnostní analýzu rizik provádět jako je analytická metoda SWOT, PNH nebo FMEA.

Dále se v této práci zabývám problematikou GDPR a jeho dopadem na bezpečnost podniku.

V neposlední řadě v teoretické části zmiňuji a popisuji další dva zásadní dokumenty podniku. Požární Ochrana a Bezpečnost a Ochrana Zdraví Při Práci.

Při studiu dokumentů pro zpracování mé práce jsem přišel na to že hrozba způsobená zevnitř podniku vlastními zaměstnanci může být tou nejzákeřnější, a to z jednoho prostého důvodu. Neumíme se jí bránit tak efektivně jako ostatním hrozbám.

SEZNAM POUŽITÉ LITERATURY

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

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

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

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

[5] 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

[6] Osobní údaje GDPR [online]. [cit. 2020-26-07]. Dostupné z: https://www.gdpr.cz/gdpr/osobni-udaje/

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

[8] Bezpečnost informačních systémů – rizika (3. díl) [online]. [cit. 2020-27-07]. Dostupné z: https://www.businessinfo.cz/clanky/7-zasad-pro-kyberneticke-zabezpeceni-male-firmy/

[9] Analýza rizik ve společnosti HART PRESS[online]. [cit. 2020-16-06]. Dostupné z: http://digilib.k.utb.cz/bitstream/handle/10563/34380/eli%E1%20ov%E1_2015_dp.pdf?sequence=1

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

[11] Pět zásad kybernetické bezpečnosti [online]. [cit. 2020-01-08]. Dostupné z: https://www.chip.cz/novinky/5-zasad-kyberneticke-bezpecnosti/

[12] Analýza personálních rizik ve vybrané organizaci [cit. 2020-01-08]. Dostupné z: http://digilib.k.utb.cz/bitstream/handle/10563/42942/vla-chov%C3%A1_2018_dp.pdf?sequence=1

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

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

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

[16] UHLÁŘ, JAN. Projektování bezpečnostních systémů.Praha: Vydavatelství PA ČR, 2001. ISBN 80-7251-076-2

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

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

[19] 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

[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] Analýza použití metody FMEA a přístupů ke snižování rizik [online]. [cit. 2020-4-08] Dostupné z: https://dspace.vsb.cz/bitstream/handle/10084/109122/KOP212_FMMI_N3922_3902T041_2015.pdf?sequence=1

[22] 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

[23] Bezpečnostní politika společnosti ČEZ [online]. [cit. 2020-4-08] Dostupné z: https://www.cez.cz/cs/o-cez/cez/bezpecnost

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

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

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

[27] Co obsahuje dokumentace BOZP? Přehled toho nejdůležitějšího [online].[cit. 2020-4-08] Dostupné z: https://www.dokumentacebozp.cz/aktuality/co-obsahuje-dokumentace-bozp-prehled-toho-nejdulezitejsiho

[28] Personální informační systém Policie ČR při mimořádných událostech [online].[cit. 2020-4-08] Dostupné z: https://docplayer.cz/12912530-Personalni-informacni-system-policie-cr-pri-mimoradnych-udalostech-bc-jiri-minichbauer.html

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

SWOT Strengths Weaknesses Opportunities Threats.

FMEA Failure Mode and Effect Analysis.

IoT Internet of Things

PNH Druh analýzy (Pravděpodobnost, Následky, Hodnotitelé).

SEZNAM OBRÁZKŮ

SEZNAM TABULEK