Ochrana znalostí a údajů v oddělení zákaznické podpory SW společnosti

Knowledge and data protection in the customer service department of the software company

Bc. Ján Pagáč

Diplomová práce
2011

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2010/2011

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

Jméno a příjmení:	**Bc. Ján PAGÁČ**
Osobní číslo:	**A08839**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Ochrana znalostí a údajů v oddělení zákaznické podpory softwarové společnosti**

Zásady pro vypracování:

Diplomová práce se bude zabývat popisem společnosti se zaměřením na oddělení zákaznické podpory (OZP) – jeho struktury a organizačních procesů.

1. **Proveďte shrnutí současného stavu.**
2. **Zaměřte se na identifikaci klíčových SW nástrojů, procesů, zákaznických a firemních údajů, ke kterým mají operátoři OZP přístup.**
3. **Proveďte analýzu možných rizik zneužití těchto nástrojů a údajů.**
4. **Navrhněte preventivní a ochranná opatření snižující toto riziko.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **ČERMÁK, M. Řízení informačních rizik v praxi. 1. vyd. Brno : Tribun EU s.r.o., 2009. 134 s. ISBN 978-80-7399-731-1.**
2. **DOUCEK, P., NOVÁK, L., SVATÁ, V. Řízení bezpečnosti informací. Kamil Mařík – Professional Publishing. 1. vyd. [s.l.] : Professional Publishing, 2008. 239 s. ISBN 978-80-86946-88-7.**
3. **JAŠEK, R. Informační a datová bezpečnost. Zlín : Univerzita Tomáše Bati ve Zlíně. 2006. 140s. ISBN 80-7318-456-7.**
4. **JAŠEK, R. Ochrana znalostí a dat v podnikových informačních systémech. Zlín : Univerzita Tomáše Bati ve Zlíně, 2002. 115 s. ISBN 80-7318-095-2.**
5. **ADAMEC, P., et al. Príručka pre manažéra VII. – Riadenie a audit v informačnej bezpečnosti. 1. vyd. [s.l.] : TATE International Slovakia, s.r.o., 2007. 322 s.**
6. **LOVEČEK, T. Bezpečnostné systémy : bezpečnosť informačných systémov. 1. vyd. Žilina : Žilinská univerzita, 2007. 246 s. Vysokoškolské učebnice. ISBN 978-80-8070-767-5.**
7. **DOSEDĚL, T. Počítačová bezpečnost a ochrana dat. 1. vyd. Brno : Computer Press, 2004. 190 s. ISBN 80-251-0106-1.**

Vedoucí diplomové práce: **Ing. Zuzana Oplatková, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **25. února 2011**

Termín odevzdání diplomové práce: **27. května 2011**

Ve Zlíně dne 25. února 2011

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Táto práca sa zaoberá aplikovaním procesu riadenia informačných rizík ako nástroja na analýzu bezpečnosti informácií a návrh preventívnych opatrení zabezpečujúcich ich ochranu v prostredí zákazníckeho centra softvérovej spoločnosti. Teoretická časť sa venuje úvodu do problematiky informačnej bezpečnosti a popisom organizačnej štruktúry a procesov skúmaného zákazníckeho centra. V praktickej časti sú formou analýzy rizík identifikované a vyhodnotené riziká, na základe ktorých je navrhnutá množina protiopatrení vedúcich k ich zníženiu.

Klíčová slova:

informačná bezpečnosť, riadenie informačných bezpečnostných rizík, analýza rizík, ochrana znalostí, informačné riziko, hodnotenie rizík

ABSTRACT

This diploma thesis deals with the applying of the process of information security risk management as a tool for analysis of information security and for design of preventive measures ensuring the protection of this information in a concrete customer center of a software company. The theoretical part is devoted to an introduction to information security issues and to a description of the organizational structure and processes within the customer center. In the practical part, the risks are analyzed and identified with the help of risk analysis, on the basis of which a set of countermeasures is designed in order to reduce the risks.

Keywords:

information security, information security risk management, risk analysis, knowledge protection, information risk, risk assessment

Na tomto mieste by som sa rád poďakoval svojej, už zosnulej, starej mame za motiváciu k štúdiu. Tak isto ďakujem Ing. Zuzane Oplatkovej, Ph.D za odvahu a ochotu viesť túto diplomovú prácu a za jej cenné rady.

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

Súčasná spoločnosť býva často označovaná ako informačná. Teda spoločnosť, v ktorej vytváranie, používanie, distribúcia a integrácia informácií tvorí značnú časť politických, ekonomických, ale aj kultúrnych aktivít [1]. Spoločnosť, v ktorej informácia ako základ každého procesu či služby predstavuje určitú hodnotu. Jej predchodcom bola spoločnosť industriálna, ktorá sa postupným procesom informatizácie transformovala do dnešnej podoby. Súčasne s informačnou spoločnosťou vznikli a postupne sa vyvíjajú aj informačné technológie (IT), ako nástroj na spracovanie a manipuláciu informácií a zároveň prostredie pre ich šírenie. Tak ako informácie, aj informačné technológie sa postupom času stali životne dôležitými aktívami každého podniku.

Hlavným cieľom tejto práce je navrhnúť účinnú ochranu pred zneužitím procesných znalostí a zákazníckych údajov – informačných aktív, ktorými operátor oddelenia zákazníckej podpory konkrétnej softvérovej spoločnosti disponuje a ku ktorým má prístup. Základným predpokladom pre splnenie tohto cieľa je presná analýza a identifikácia chránených aktív a zároveň hrozieb, ktoré môžu na aktíva negatívne pôsobiť. Len tak je možné odhaliť riziká, ktoré analyzovanému systému hrozia a na ich základe navrhnúť a prijať účinné protiopatrenia. Na dosiahnutie vytýčeného cieľa som sa rozhodol aplikovať proces riadenia informačných rizík, respektíve jeho jeden cyklus. Tento kontinuálny proces, ako súčasť systému riadenie informačnej bezpečnosti, je definovaný súborom noriem, a zároveň sa jeho praktickému použitiu venuje množstvo odbornej literatúry. Hlavný dôraz je v nej predovšetkým kladený na zabezpečenie informačných systémov (IS) a informácií v nich uchovávaných. Avšak iba minimum pozornosti sa venuje ochrane tej istej informácie uchovanej mimo informačný systém, uloženej v mozgu človeka, ktorý ju legitímnym spôsobom zo systému získal. Aj preto je mojou osobnou ambíciou, aby sa predkladaná práca stala akousi príručkou alebo pomocníkom bezpečnostných, operačných a IT manažérov pri zvládaní informačných rizík zameraných na ochranu znalostí, údajov ale aj know-how v malých a stredne veľkých zákazníckych centrách.

Práca je členená do teoretickej a praktickej časti. Prvá kapitola teoretickej časti poskytuje obecný pohľad na informačnú bezpečnosť a potrebu jej štandardizácie. Pojednáva o bezpečnostných hrozbách a rizikách, s ktorými sa v tejto oblasti bežne stretávame a pred ktorými je nutné informačné technológie chrániť. Ďalej nasleduje vysvetlenie problematiky outsourcingu podnikových procesov, ako aj priblíženie

bezpečnostných špecifík tejto formy prevádzky podniku. Po teoretickom úvode je v rámci druhej kapitoly predstavená konkrétna outsourcingová spoločnosť poskytujúca služby zákazníckej podpory, ako objekt riadenia informačnej bezpečnosti. V tejto kapitole je dôraz kladený na popis jej organizačnej štruktúry, kľúčových procesov a používaných informačných systémov.

Praktická časť sa zoberá aplikovaním jedného cyklu procesu riadenia rizík. Jeho prvou fázou je analýza rizík (RK), ktorá prostredníctvom identifikácie a kvantifikácie informačných aktív, ich hrozieb a zraniteľností vytvára podklad pre fázu druhú – vyhodnotenie rizík. V tejto fáze dochádza k vyčísleniu možných rizík. Podľa ich výšky sú navrhnuté účinné a hospodárne opatrenia, ktoré by tieto riziká mali znížiť na akceptovateľnú úroveň. V poslednej fáze sú detailne naplánované konkrétne kroky zabezpečujúce vykonanie definovaných opatrení. Každej fáze procesu riadenia rizík je venovaná samostatná kapitola. Okrem popisu samotnej aplikácie procesu sú v prvých dvoch kapitolách praktickej časti diskutované najčastejšie používané prístupy prevedenia analýzy a vyhodnotenia rizík, a tiež sú v nich popísané účinné spôsoby zberu informácií, ich spracovania, vyhodnotenia a interpretácie. Aj napriek tomu, že sa zväčša jedná o sumár teoretických poznatkov, do praktickej časti sú zahrnuté, aby poskytli čitateľovi širší a zároveň celistvý pohľad na proces riadenia rizík.

I. TEORETICKÁ ČASŤ

1 INFORMAČNÁ BEZPEČNOSŤ

Počítače a internetové technológie (IT) priniesli revolúciu v oblasti výpočtovej techniky a prostredníctvom počítačových sietí umožnili ľudom medzi sebou zdieľať a vymieňať si informácie. Čím sa stáva zdieľanie informácií jednoduchším, tým väčší dôraz je nutné klásť na kontrolu ich toku. Preto vznikla potreba bezpečnosti informačných technológií a s ňou súvisiacich noriem. Každá spoločnosť, ktorá pri svojej činnosti využíva informačné technológie, by mala mať vlastnú bezpečnostnú politiku IT definujúcu tieto normy. Spoločné štandardy a postupy môžu byť aplikované ako na celú spoločnosť, tak na jej jednotlivé organizačné jednotky, čím sa vytvorí efektívne a bezpečné prostredie pre fungovanie IT infraštruktúry. Na ochranu informačných systémov a nimi spracovávaných údajov je ďalej potrebný systém, ktorý zabezpečí vyvážené a hospodárne aplikovanie bezpečnostných metód a techník vyžadovaných definovanými normami [2].

Bezpečnostné normy IT majú za úlohu definovať procesy, procedúry a praktiky nevyhnutné pre implementáciu bezpečnostných programov, ktoré sú špecifické pre jednotlivé oddelenia spoločnosti. Tieto štandardy sa vzťahujú na všetky oblasti aktivít, či už sú realizované pre dané oddelenie, alebo oddelením samotným. Zahŕňajú konkrétne kroky, ktoré musia byť prijaté s cieľom zaistiť bezpečné fungovanie IT infraštruktúry. V oblasti informačnej bezpečnosti je definovaná séria noriem ISO/ IEC 2700x a z nej sú pre účely tejto diplomovej práce dôležité normy ISO/ IEC 27001:2005 (obsahuje špecifikácie certifikačných požiadaviek pre systém manažérstva informačnej bezpečnosti) a predovšetkým ISO/ IEC 27005:2008 popisujúca analýzu a riadenie rizík [3]. Keďže táto diplomová práca je zameraná na úzku oblasť informačnej bezpečnosti a jej riadenia v softvérovej spoločnosti s konkrétnym praktickým využitím, nebudem v ďalšom texte vychádzať priamo z uvedených noriem. Postačí nám dostupná literatúra, ktorá praktické využitie týchto noriem popisuje.

1.1 Základné pojmy informačnej bezpečnosti

Informačná bezpečnosť, ako mladý technický obor zavádza množstvo nových pojmov. Pre jej správne pochopenie si v nasledujúcom texte uvedieme a vysvetlíme tie najzákladnejšie a najdôležitejšie. Keďže sa v oblasti bezpečnosti IS a technológií používa ako univerzálny jazyk anglický, uvádzam aj ich anglické ekvivalenty.

Aktívum (*Asset*). Aktíva sú všetky hmotné i nehmotné statky, všetko, čo má pre majiteľa informačného systému istú hodnotu. Za najcennejšie aktíva sa považujú peniaze, majetok a predovšetkým údaje a informácie, ktorých zneužitie, strata alebo modifikácia by organizácii alebo osobe spôsobili určitú škodu. [4]

Analýza rizík (*Risk Analysis*) je proces zistenia a vyhodnotenia hrozieb pôsobiacich na aktíva s cieľom definovať úroveň rizika, ktorému je systém aktív vystavený. Cieľom je zistenie, či sú bezpečnostné opatrenia dostatočné, aby znížili pravdepodobnosť vzniku škody na prijateľnú úroveň. [4]

Bezpečnosť (*Security*). Pod pojmom bezpečnosť chápeme vlastnosť nejakého objektu alebo subjektu (informačného systému alebo technológie), ktorá určuje stupeň, mieru jeho ochrany možným škodám a hrozbám. [4]

Hrozba (*Threat*) je skutočnosť, udalosť, sila alebo osoby, ktorých pôsobenie (činnosť) môže spôsobiť poškodenie, zničenie, stratu dôvery alebo hodnoty aktíva. Hrozba môže ohroziť bezpečnosť (napr. prírodná katastrofa, hacker, zamestnanec a i.). [4]

Informačný systém (*Information System*) je súbor ľudí, metód a technických prostriedkov zaisťujúcich zber, prenos, uchovanie, spracovanie a prezentáciu údajov s cieľom tvorby a poskytovania informácií podľa potrieb príjemcov informácií činných v systéme riadenia.

Protiopatrenie (Countermeasure) je akýkoľvek proces, činnosť, mechanizmus, technické zariadenie alebo čokoľvek iné, čo chráni aktíva pred pôsobením konkrétnej hrozby, prípadne hrozieb viacerých. Každé protiopatrenie môže chrániť aktíva pred pôsobením hrozby úplne, prípadne jej pôsobenie a vzniknuté škody iba zmierňovať. [4]

Riadenie rizík (*Risk Management*) je celkový proces, pomocou ktorého je možné určiť, kontrolovať a obmedzovať vplyv nepredvídateľných nepriaznivých udalostí – teda hrozieb. Obsahuje predovšetkým analýzu a odhad rizika, analýzu nákladov a výber, implementáciu, testovanie a prevádzkovanie bezpečnosti. [4]

Riziko (*Risk*) je pravdepodobnosť, s akou bude daná hodnota aktíva zničená alebo poškodená pôsobením konkrétnej hrozby, ktorá pôsobí na slabú stránku tejto hodnoty. Je to teda miera ohrozenia konkrétneho aktíva. [4]

Útok (*Attack*), ktorý tiež nazývame bezpečnostný incident, je buď úmyselné využitie zraniteľného miesta k spôsobeniu škôd /strát na aktívach IS, alebo neúmyselné

uskutočnenie akcie, ktorého výsledkom je škoda na aktívach. Pri analýze možných foriem útokov na IT je potrebné riešiť problémy typu: kto útočí, kto môže páchať počítačový zločin, aké riziká súvisia s používaním IT, ako sa chrániť pred útokmi apod. [4]

Zraniteľnosť (*Vulnerablity*) je nedostatok alebo slabina bezpečnostného systému, ktorá môže byť zneužitá hrozbou tak, že dôjde k poškodeniu, alebo zničeniu hodnoty aktív. Každé aktívum je zraniteľné, pretože jeho hodnotu ohrozujú rôzne vplyvy. [5]

1.2 Bezpečnostné hrozby a riziká

Je potrebné si uvedomiť, že hrozby pre informačné technológie a systémy môžu byť výsledkom nielen úmyselnej činnosti „útočníka“, ale aj nedbalosti osoby, ktorá participovala na návrhu, vývoji, implementácií, testovaní, inštalácii, údržbe či prevádzke systémov, alebo je ich oprávneným používateľom, prípadne môžu byť aj dôsledkom výskytu neovládateľných udalostí v okolí systému. Hrozby môžeme deliť podľa hľadísk hlavne na:

- objektívne
  - hrozby plynúce z pôsobenia prírodných živlov, prípadne priemyslových havárií, napr. povodeň, požiar, výpadok dodávky energií, poruchy rôzneho druhu; u týchto hrozieb je prevencia z pohľadu informačnej bezpečnosti obtiažna, preto je nutné skôr riešiť minimalizáciu strát vhodným plánom obnovy,
  - fyzikálne hrozby, napr. elektromagnetické vyžarovanie,
  - technické alebo logické, t.j. porucha pamäti, nesprávne prepojenie inak bezpečných komponentov, nedokonalé zničenie informácie z pamäťového média, jeho krádež apod.,
- subjektívne, t.j. hrozby plynúce z ľudského faktoru,
  - neúmyselné, napr. pôsobením nezaškoleného používateľa alebo správcu informačného systému,
  - úmyselné, ktoré vychádzajú z existencie potenciálneho externého útočníka, napr. špióni, teroristi, hackeri, konkurenti. Predpokladá sa, že až 80% útokov je realizovaných z vnútra, útočníkom, ktorým môže byť prepustený, vydieraný alebo pomstychtivý zamestnanec [4].

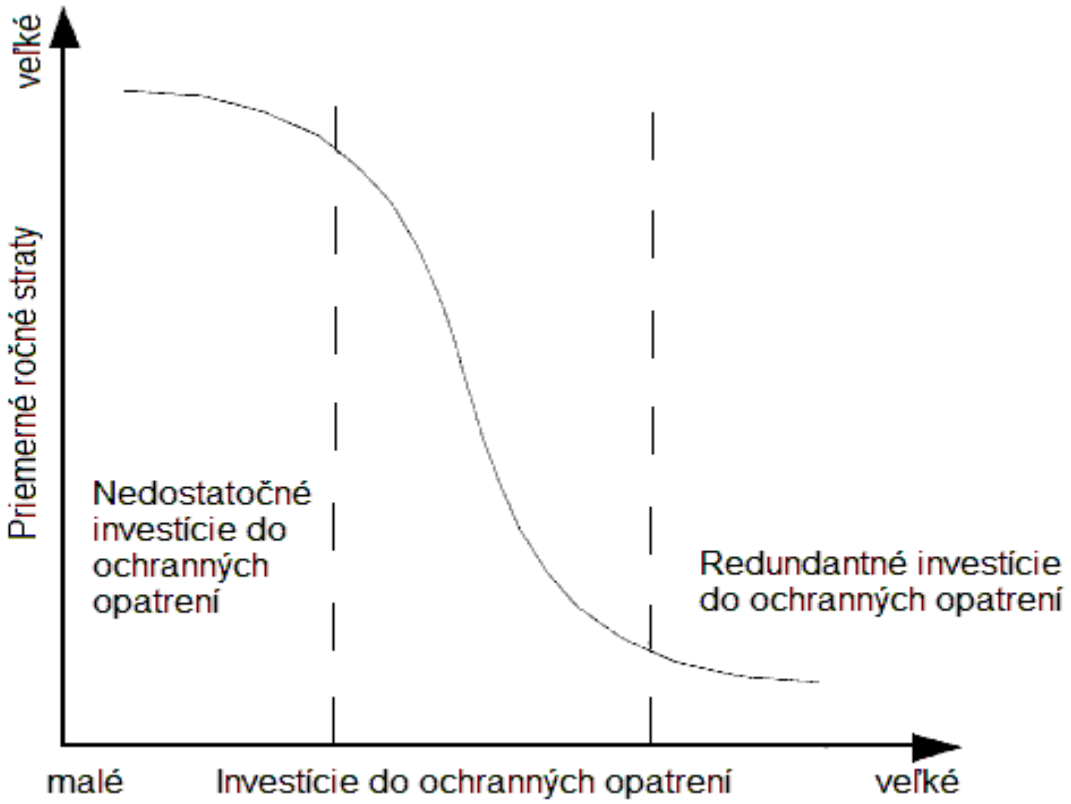
Typické príklady a techniky útoku proti informačným technológiám a systémom sú:

- vizuálna špionáž, sledovanie oprávnených používateľov pri zadávaní prístupových hesiel, alebo sledovanie zobrazovaných výstupov zo systému,
- uvedenie oprávnených používateľov systému do omylu predstieraním identity prevádzkovateľa systému, alebo inej autority, s následným vyžadovaním údajov či iných činností súvisiacich s ich oprávneným prístupom k službám IS,
- sústreďovanie zapožičaných, darovaných, ukradnutých alebo vyradených pamäťových médií a ich preskúmanie s cieľom získať na nich ponechané, resp. nedostatočne zlikvidované údaje,
- monitorovanie alebo úmyselné rušenie komunikácie medzi jednotlivými časťami systému,
- tzv. Trójsky kôň – nezdokumentovaná, pred bežným používateľom skrytá funkcia napohľad užitočného programu; spustením programu môže takto oprávnený používateľ nevedomky iniciovať aj vykonanie škodlivej činnosti,
- „denial-of-service“ útok, teda zablokovanie práce systému vyčerpaním jeho zdrojov, zahltenie komunikačného systému množstvom žiadostí o spojenie či množstvom začatých, ale nedokončených spojení, zahltenie procesora počítača generovaním a spúšťaním stále nových procesov a podobne,
- využitie „štandardných“ (inštalačných) prístupových hesiel. Je známym faktom, že dodávatelia systémov často používajú rovnaké prístupové heslá pre ich inštaláciu alebo údržbu.

Okrem vyššie spomenutých hrozieb, ktoré predpokladajú istú „technickú“ znalosť, nemožno vylúčiť ani hrozby vyplývajúce skôr z opaku, t.j. z neznalosti charakteristík elektronickej komunikácie. Keďže elektronická pošta „je všade“ a „každý ju používa“, niet divu, že jej prostredníctvom sa šíria nie len obyčajné správy, ale aj počítačové vírusy.

Veľkú triedu hrozieb predstavuje aj Internet. Technicky orientované hrozby tejto triedy súvisia spravidla s bezpečnostnými nedostatkami použitých prehliadačov. Hrozby netechnického charakteru, využívajúce neznalosť či bezstarostnosť internetovských „surferov“ alebo dokonca automatické prostriedky hľadania na Internete. Obľúbeným trikom je napríklad zriadenie internetovej stránky, ktorej adresa je syntakticky podobná s adresou cieľovej stránky – je istá šanca, že pri hľadaní cieľovej stránky bude surfer omylom považovať takto vytvorenú stránku za pravú [6].

S každou hrozbou je spojené riziko, ktoré predstavuje pravdepodobnosť uskutočnenia danej hrozby a jej pôsobenia na aktívum. Na zníženie pravdepodobnosti výskytu konkrétnej hrozby, teda miery rizika, je nutné vynaložiť určité úsilie, vykonať množinu konkrétnych činností, krokov. Sadu týchto krokov nazývame protiopatrenie. Čím je protiopatrenie účinnejšie, tým výraznejšie klesá miera rizika. Je nutné si však uvedomiť, že s každým protiopatrením sú spojené náklady na jeho prijatie. Ochrana proti riziku je teda predovšetkým otázkou ceny. Čím vyššia je miera zabezpečenia, tým sú vyššie náklady. Pri návrhu protiopatrení je preto dôležitá cena chránených aktív. Aby proces znižovania rizika mal zmysel, nesmú náklady na prijatie protiopatrení presiahnuť cenu aktív, respektíve škody plynúce z poškodenia/ straty aktív. Vzťah medzi týmito dvomi veličinami je uvedený na obrázku 1.



Obr. 1.1: Funkčný vzťah závislostí medzi investíciami do ochranných opatrení a očakávanými stratami [7]

Na dosiahnutie optimálneho stavu vynaloženia nákladov na protiopatrenia a ochrany proti hroziacemu riziku je nutné vykonať analýzu rizík. Analýza rizík je prvou etapou procesu riadenia rizík. Čo všetko proces riadenia rizík predstavuje a bližší popis všetkých jeho etáp je uvedený v praktickej časti.

1.3 Outsourcovanie podnikových procesov a ich bezpečnosť

Predtým, než sa budem bezpečnosti v tejto oblasti venovať podrobnejšie, je vhodné spomenúť, čo Outsourcing[1] podnikových procesov (OPP) je a aké výhody spoločnostiam prináša. „*OPP je jedna z foriem outsourcingu, ktorá zahŕňa zabezpečenie konkrétnych činností a podnikových procesov spoločnosťou tretej strany na základe uzatvorenej zmluvy, tzv. Service Level Agreement (SLA)*"[8]. OPP sa delí na outsourcing interných procesov, ako riadenie ľudských zdrojov, financie, účtovníctvo a outsourcing externých procesov, kam patrí poskytovanie služieb zákazníkom prostredníctvom kontaktných centier, informačných liniek apod. Hlavnou výhodou pre spoločnosť, ktorá sa rozhodne svoje procesy outsourcovať je zvýšenie jej pružnosti. Flexibilitu spoločnosti môžeme chápať v rôznych súvislostiach a tak isto aj OPP zvyšuje pružnosť spoločnosti rôznymi spôsobmi. Väčšina poskytovateľov[2] OPP poskytuje svoje služby na princípe „poplatok za službu", t.j. výška poplatku závisí od objemu vykonávaných služieb. Spoločnosti to umožní transformáciu fixných nákladov na variabilné. Štruktúra variabilných nákladov zase spoločnosti pomáha reagovať na prípadné zmeny objemu outsourcovaných služieb a nevyžaduje investície do aktív. Tieto závislosti môžu spoločnosti priniesť vyššiu flexibilitu v riadení zdrojov a v konečnom dôsledku pomôcť rýchlejšie reagovať na zmeny dopytu po ich službách [9]. Ďalší spôsob, ktorým môže OPP zvýšiť flexibilitu firmy je sústredenie sa na jej hlavné činnosti. Odľahčí jej kľúčových pracovníkov od množstva administratívnych činností, prípadne byrokratických požiadaviek a umožní im plne sa venovať hlavným oblastiam podnikania firmy[10]. Tretím spôsobom, ktorým OPP dokáže zvýšiť pružnosť spoločnosti, je urýchlenie niektorých podnikových procesov. Toto sa týka hlavne výrobných firiem, ktoré vhodným riadením dodávateľského reťazca a využívaním partnerov môžu urýchliť proces predaja a tým zvýšiť priepustnosť výroby [11].

Hoci vyššie uvedené argumenty podporujú názor, že OPP je pre spoločnosti prínosom, manažment každej z nich by mal byť pri jeho implementovaní opatrný. S OPP sa totiž spája aj niekoľko problémov, ktoré je potrebné vziať do úvahy. Medzi najčastejšie patria nedodržiavanie požadovaných úrovní poskytovaných služieb, špecifické problémy, ktoré nie sú pokryté zmluvou, nepredvídané náklady a paradoxne závislosť na samotnom OPP znižujúca flexibilitu spoločnosti [11]. Najväčším nedostatkom OPP sú však

[1] Outsourcing vznikol v 80. rokoch 20. storočia v USA a označuje proces realizácie subdodávky, ktorá je zabezpečovaná firmou tretej strany.
[2] Poskytovateľ OOP je firma, ktorá outsourcovaný proces/ službu poskytuje.

bezpečnostné hrozby s nim spojené. Pred tým, než sa podnik rozhodne outsourcovať niektoré svoje procesy a služby, dokáže priamo kontrolovať a riadiť vlastných zamestnancov podieľajúcich sa na ich výkone, či dodávke. Po zavedení OPP sa táto priama kontrola stráca, čo prináša rôzne právne, bezpečnostné a iné problémy. Aby sa týmto problémom a hrozbám predišlo, mali by byť riadne ošetrené v zmluve medzi podnikom a dodávateľom OPP. Keďže je táto problematika veľmi široká a zložitá, je vhodné do tohto procesu angažovať poradenskú firmu podnikajúcu v tejto oblasti.

Bezpečnosť v OPP veľmi úzko súvisí s informačnou bezpečnosťou ako takou. Najčastejšie sú to práve informácie a údaje, ktoré sú objektmi páchania trestnej činnosti. Či už to sú prístupové kódy k bankovým účtom, čísla kreditných kariet ale aj kontaktné, osobné údaje a často dôverné informácie o klientoch nadnárodných finančných inštitúcií. V minulosti sa tejto problematike nevenovala dostatočná pozornosť. Až enormný nárast outsourcingových aktivít, ktorých veľká časť je situovaná v Indii a sním spojený zvýšený počet hlásených bezpečnostných incidentov donútili odbornú verejnosť, ale aj jednotlivé spoločnosti venovať bezpečnostnej otázke náležitú pozornosť.

Spoločnosť, ktorá pôsobí vo funkcii dodávateľa OPP typicky prichádza do styku a teda musí chrániť externé údaje dvoch typov. Jednak sú to informácie o samotnom klientovi (spoločnosti, ktorá svoje procesy outsourcuje) – sem patrí prístup do IS klienta, prípadne know-how procesov klienta. Druhým typom sú údaje o zákazníkoch klienta, kam patria už spomínané informácie o účtoch, kreditných kartách alebo osobné údaje. Oba typy dát je nutné chrániť na viacerých úrovniach a tie sú popísané v nasledujúcom texte.

Organizačná vrstva zahŕňa riadenie personálnych zdrojov – ľudí. Proces budovania bezpečnej spoločnosti sa začína už pri nábore nových zamestnancov. Tu by sa mal klásť dôraz na preverovanie týchto ľudí, ich pozadia, predchádzajúcich zamestnaní. Toto sa dá docieliť overovaním referencií, kontrolou dokladov dosiahnutého vzdelania, osobných dokladov ako aj bezúhonnosti. Nový, ale aj stávajúci zamestnanci by mali byť v oblasti informačnej bezpečnosti pravidelne vzdelávaní tak, aby chápali svoje postavenie a zodpovednosť. Tiež aby si plnohodnotne uvedomili, s akým typom údajov pracujú a postihy, ktoré za zneužitie alebo vyzradenie týchto údajov hrozia.

Logická vrstva popisuje bezpečnosť a ochranu na úrovni operačných systémov, informačných systémov a iných aplikácií na nich bežiacich. Definuje dátové toky medzi týmito systémami, čiže používanie zabezpečených spojení, virtuálnych privátnych sietí,

logovanie komunikácie apod. Ďalej popisuje spôsoby ochrany pred škodlivým softvérom (ako sú vírusy, červy a trójske kone), nasadenie brán Firewall a spravuje prístupové oprávnenia do jednotlivých častí informačných systémov.

Fyzická vrstva definuje bezpečnosť na úrovni hardvéru a jeho fyzického uloženia. Patrí sem zabezpečenie počítačov, serverov a UPS záložných systémov. Ďalej spôsob vykonávania záloh dát a samotnú manipuláciu so záložnými pamäťovými médiami. Okrem iného rieši fyzické prepojenie počítačov a serverov v lokálnych sieťach.

Každá spoločnosť poskytujúca outsourcingové služby by mala mať definovanú bezpečnostnú politiku, ktorá ochranu na vyššie uvedených úrovniach bližšie špecifikuje. Tú môže mať spoločnú pre viacerých klientov, ktorým služby a procesy outsourcuje, alebo v prípade špeciálnych požiadaviek klientov sa definuje bezpečnostná politika pre každého klienta zvlášť.

Jeden z praktických príkladov OPP a analýzy ich bezpečnosti je detailne popísaný v nasledujúcich kapitolách.

2 PREDSTAVENIE SPOLOČNOSTI

Spoločnosť Zakaznickapodpora[3] je jedna z najväčších a celosvetovo najuznávanejších spoločností poskytujúca predovšetkým outsourcingové služby, ktoré umožňujú jej klientom plne sa sústrediť na hlavnú oblasť ich podnikania, tzv. core business. Medzi jej klientov patria firmy podnikajúce v oblastiach IT, telekomunikácií, finančných služieb, médií, automobilového priemyslu a mnoho ďalších. Táto spoločnosť má zastúpenie aj v Českej republike v rámci dvoch pobočiek. Pobočka, ktorej sa táto diplomová práca týka, funguje ako callcentrum a momentálne zamestnáva viac ako 150 zamestnancov. Jej hlavnou náplňou je outsourcing rôznych úrovní zákazníckej a technickej podpory niekoľkých významných klientov. Škála cieľových zákazníkov je tvorená domácimi spotrebiteľmi, firmami ale aj distribútormi produktov jednotlivých klientov z krajín strednej Európy. Najväčším klientom z hľadiska objemu poskytovaných služieb je medzinárodná softvérová spoločnosť[4] zaoberajúca sa vývojom a predajom krabicového softvéru. V tejto kapitole si podrobnejšie predstavíme organizačnú štruktúru callcentra, kľúčové role, fungovanie hlavných procesov, metódy ich merania a hodnotenia zo zameraním sa na služby poskytované pre Klient1.

2.1 Organizačná štruktúra

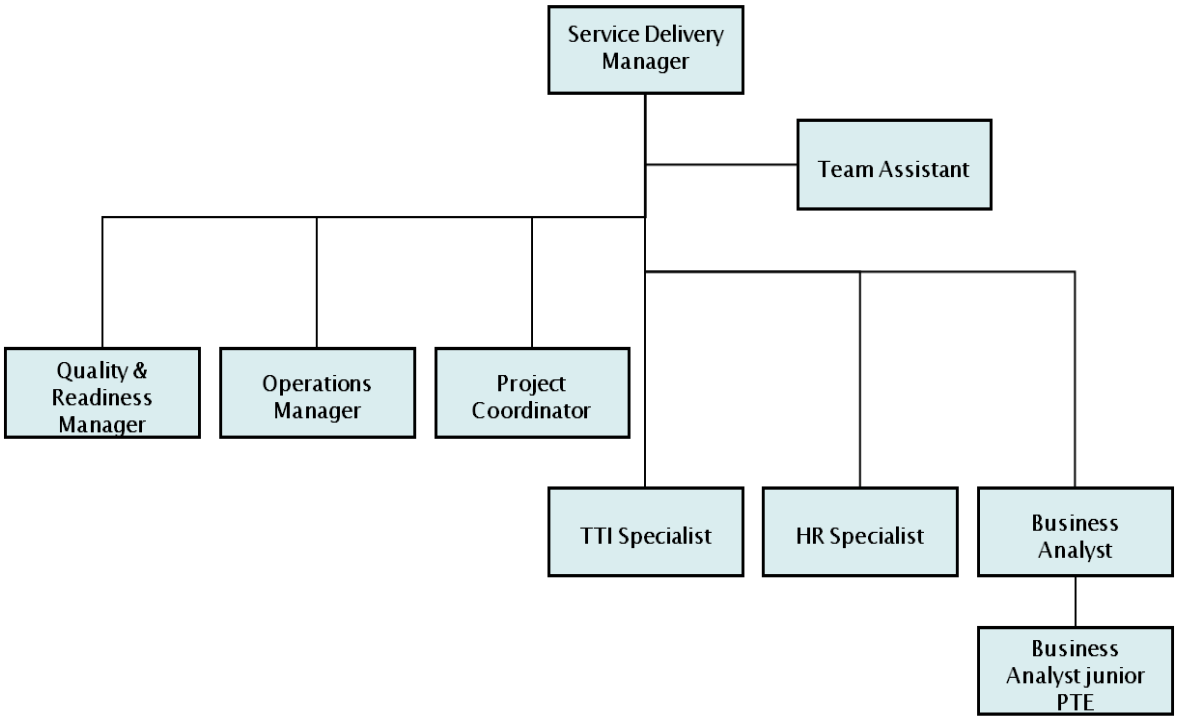
Organizačnú štruktúru callcentra by sme na základe organizácie riadenia mohli rozdeliť do troch organizačných jednotiek, ktoré sú navzájom prepojené. Sú to Management (Obr. 2.1), Quality (Obr. 2.2) a Operations (Obr. 2.3).

V jednotke Management, ktorá je riadená Service Delivery Manager (SDM) vystupuje riadiaci a podporný personál zodpovedný za celkový chod pobočky, zostavovanie rozpočtu, analýzy dát a finančných tokov, personálneho riadenia, vyhľadávanie nových klientov a v neposlednom rade zabezpečenie IT infraštruktúry.

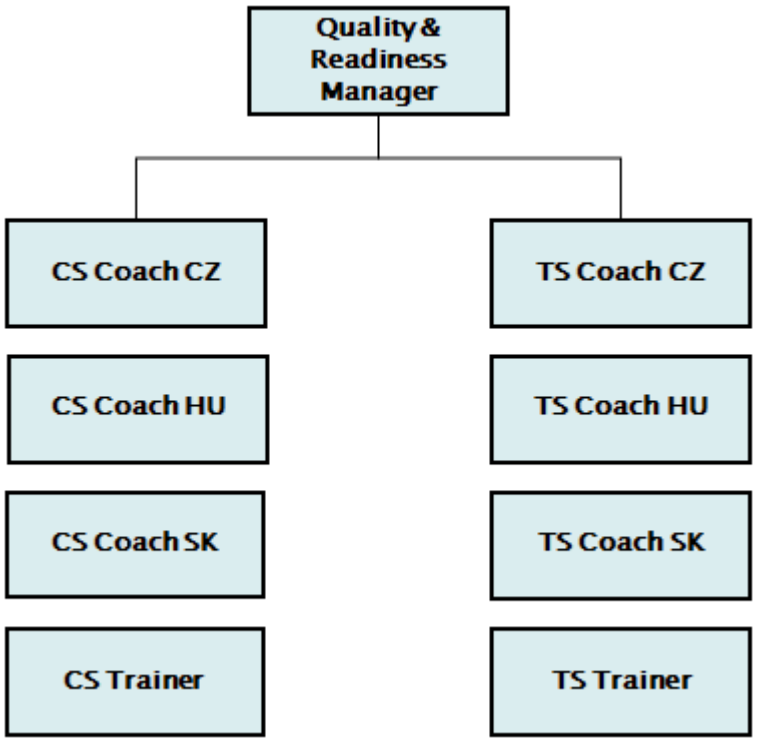
Jednotka Quality vedená Quality and Readiness Manager zabezpečuje riadenie kvality poskytovaných služieb a jej neustále zlepšovanie za účelom dosiahnutia maximálnej spokojnosti klientov a ich zákazníkov. Svoje ciele dosahuje prostredníctvom práce koučov a trénerov, ktorí hrajú kľúčové role vo vzdelávacom procese operátorov. Ich funkciu si podrobne vysvetlíme neskôr.

---

[3] Z procesných a bezpečnostných dôvodov nebude názov spoločnosti ako aj jej klientov uvedený.
[4] V ďalšom texte bude označovaná ako Klient1



Obr. 2.1: Brno Management



Obr. 2.2: Brno Quality

Treťou jednotkou je Operations a tá zabezpečuje samotné služby callcentra volajúcim zákazníkom, t.j. každodenné poskytovanie telefonickej a e-mailovej zákazníckej a technickej podpory. Tvoria ho Operations Manager a Team Manažéri jednotlivých tímov,

ktoré sú rozdelené podľa klienta, technickej úrovne a jazyka poskytovaných služieb. V tejto diplomovej práci sa budeme ďalej zaoberať podporou poskytovanou pre zákazníkov Klient1, ktorú by sme mohli rozdeliť do šiestich virtuálnych tímov:

Zákaznícka podpora (1st level):

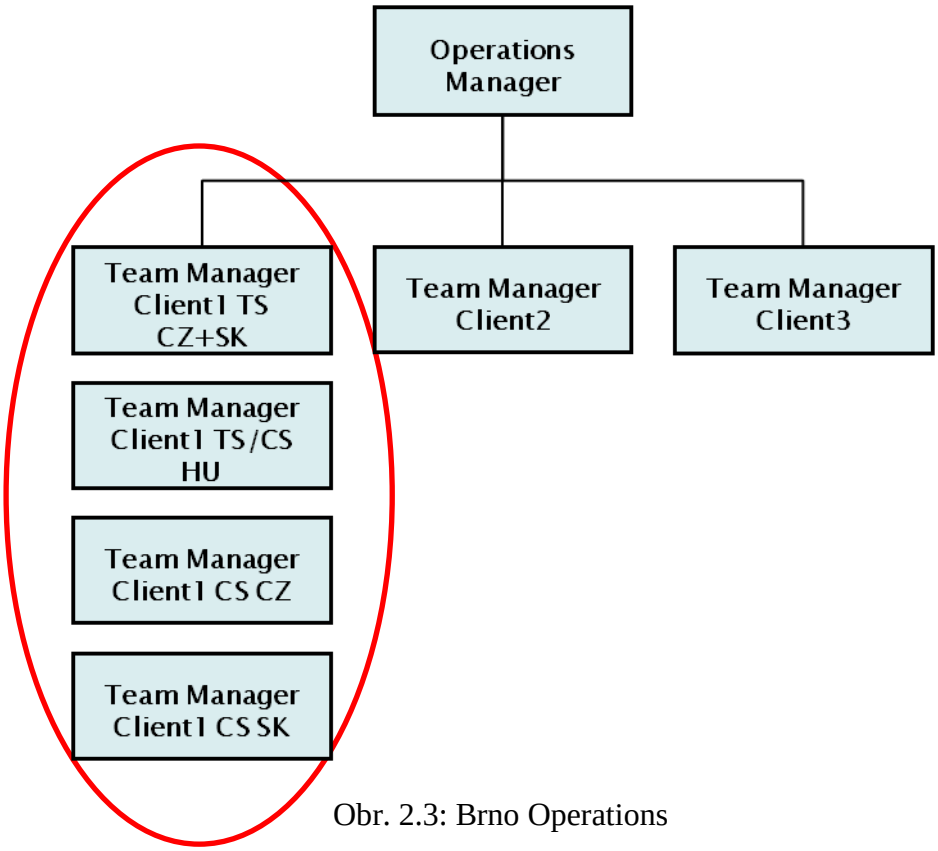
CS CZ – zákaznícka podpora pre Českú republiku

CS SK – zákaznícka podpora pre Slovensko

CS HU – zákaznícka podpora pre Maďarsko

A obdobne technická podpora (2nd a 3rd level[5]):

TS CZ, SK, HU – technická podpora pre Českú republiku, Slovensko a Maďarsko



Obr. 2.3: Brno Operations

2.2 Kľúčové role

Kľúčovými rolami z pohľadu styku s chránenými informáciami a údajmi sú tieto:

[5] Technická podpora sa ďalej delí na domácich zákazníkov (PERsonal – 2nd level) a biznis zákazníkov (PROfessional – 3rd level)

CSR (Customer Service Representative – operátor zákazníckej podpory 1. stupňa) odpovedá na prichádzajúce hovory a e-maily od zákazníkov, zakladá ich profil a pomáha s riešením problémov. Odpovedá na Pre-sales[6] otázky a tiež otázky, ktoré následne rieši technická podpora, prípadne vykonáva oživenie/ aktiváciu produktov. Ďalej je zodpovedný za:

- správne zaevidovanie všetkých zákazníckych dát a pracovných procesov v požadovanom čase,
- v prípade potreby správne prepojenie na vyššiu úroveň podpory,
- evidenciu, prijímanie, spracovávanie a eskaláciu sťažností zákazníka,
- eskaláciu prípadov na team manažéra, ak nepozná správne riešenie,
- vytváranie/ otváranie prípadov – servisných incidentov s pomocou nástrojov dodaných klientom,
- eskaláciu prípadov, ak problém nemôže byť vyriešený v zákazníckom centre a spoluprácu s eskalačným tímom klienta.

Práve táto rola je z pohľadu prístupu a zaobchádzania s citlivými údajmi a informačnými systémami používanými na ich spracovanie najrizikovejšia a preto bude podrobená rizikovej analýze v praktickej časti.

Agent TS PER + PRO (operátor zákazníckej podpory 2nd a 3rd level) poskytuje technickú podporu pre domácich (PER) a firemných (PRO) používateľov a správcov produktov spoločnosti Klient1 a je zodpovedný za:

- prevzatie, identifikáciu, riešenie a vyriešenie servisného incidentu zákazníka,
- správne logovanie všetkých činností spojených s vyššie uvedeným procesom v celosvetovej databáze spoločnosti Klient1,
- eskaláciu servisných incidentov, ak problém nemôže byť vyriešený v zákazníckom centre a spoluprácu so špecializovanými tímami.

Kouč je prostredníctvom monitorovania komunikácie a doručovania pravidelných spätných väzieb zodpovedný za rozvoj technických, komunikačných a iných zručností jednotlivých agentov. Ďalej má na starosti:

[6] Informácie k produktu, o ktorého kúpe zákazník uvažuje.

- koučovanie nových zamestnancov a rozvíjanie ich technických i netechnických zručností a znalostí,
- kontinuálny rozvoj už zapracovaných operátorov,
- proaktívnu komunikáciu a zdieľanie informácií obzvlášť s novými a menej skúsenými operátormi,
- analýzy znalostných medzier jednotlivých členov tímu,
- spoločne s tím manažérmi proaktívne odporúča a iniciuje zdokonaľovanie agentov.

Tréner zodpovedá za systematický rozvoj agentov zákazníckeho servisu a technickej podpory prostredníctvom školení a spätnej väzby. Ďalej má na starosti:

- školenie agentov,
- zostavenie a aktualizácie školiacich materiálov,
- aktívne rozširovanie znalostí agentov zákazníckej a technickej podpory,
- posudzuje potreby školení s koučmi a tím manažérmi,
- testuje znalosti agentov.

Každému tímu je priradený jeden kouč podľa jeho špecializácie (CS/ TS) a jazykovej vybavenosti (CZ/ HU/ SK). Tréneri sú rozdelení iba podľa úrovne podpory (CS/ TS) nezávisle na jazyku jednotlivých tímov.

2.3 Pracovné procesy, ich sledovanie a ochrana

Spoločnosť Klient1 má vypracované procesné manuály a postupy pokrývajúce prakticky všetky situácie a scenáre, ktoré môžu pri obsluhe zákazníkov a s ňou spojenej administratívnej činnosti nastať. Úlohou outsourcingového poskytovateľa – Zakaznickapodpora – je týmito postupmi sa riadiť a podľa nich poskytovať služby koncovým zákazníkom klienta. Aby bolo zabezpečené správne fungovanie a nasledovanie procesov, je nutná ich neustála kontrola a monitoring. Ten sa v spoločnosti Zakaznickapodpora realizuje hlavne prostredníctvom náhodných výberov telefonických hovorov a ich následnou analýzou. Výber a analýzu vykonávajú koučovia, ktorí na jej základe poskytujú operátorom spätnú väzbu o chybách, prípadne nedostatkoch v plnení procesu. Koučovia sú zároveň jediní, ktorí môžu aktívne odhaliť či už úmyselnú alebo nevedomú chybu operátora pri komunikácii so zákazníkom. Okrem analýzy telefonických hovorov, kouč kontroluje správne používanie podporných IS a tiež zaznamenávanie požadovaných údajov a ich štruktúru.

Popri správnom vykonávaní pracovných procesov je spoločnosť Zakaznickapodpora povinná chrániť aj ich dôvernosť. Dôvodom je fakt, že jednotlivé procesy v sebe často skrývajú cenné know-how, ale aj to, že by ich aktívne komunikovanie smerom k zákazníkom nebolo príliš taktické a rozumné z pohľadu imidžu klienta. Okrem samotných procesov je nutné chrániť aj údaje a informácie, s ktorými sa pri vykonávaní pracovných postupov manipuluje. Pracovné procesy a údaje môžeme preto považovať za informačné aktíva firmy. Nevyhnutným predpokladom pre účinnú ochranu aktív je ich identifikácia, ktorá tvorí základ pre úspešnú analýzu rizík. A práve tento predpoklad nie je v spoločnosti Zakaznickapodpora splnený.

2.4 Informačné systémy a citlivé údaje nimi spracovávané

Pri vybavovaní zákazníckych požiadaviek prichádzajú operátori CS oddelení denno denne do styku s rôznymi typmi údajov. Na ich spracovanie a evidenciu využívajú niekoľko informačných systémov. Všetky informačné systémy sú vo vlastníctve klienta Klient1 a ten ako jediný má právo a kompetenciu zasahovať do ich správy a bezpečnostných nastavení. Dovolím si tvrdiť, že úroveň zabezpečenia týchto systémov je na vysokej úrovni. Aj preto ako také nebudú predmetom ochrany. Omnoho dôležitejším a rizikovejším objektom čo do ochrany údajov pred vyzradením, prípadne ich zneužitím je človek – operátor. Ten funguje ako prenosové médium informácie medzi zákazníkom a samotným IS. A práve toto médium je nutné chrániť a zabezpečiť pred únikom informácií.

Pre predstavu čitateľa uvádzam zoznam informačných systémov[7], ich použitie a tiež typy údajov nimi spracovávaných.

[7] Na žiadosť spoločnosti Zakaznickapodpora nebudú skutočné názvy IS uvádzané

Názov IS	Účel použitia
IS1	Evidencia prichádzajúcich tel. hovorov, vrátane irelevantných
IS2	Evidencia prichádzajúcich a odchádzajúcich tel. hovorov a e-mailov súvisiacich s vybavovaním požiadaviek a technických incidentov súvisiacich so SW produktmi spoločnosti Klient1
IS3	Evidencia technických incidentov určených pre 2. úroveň technickej podpory
IS4	Overenie produktových kľúčov a sériových čísiel SW produktov
IS5	Znalostná databáza známych problémov a riešení
IS6	„Oživenie“ SW produktov po ich inštalácii
IS7	Spravovanie multilicenčných a iných typov zmlúv pre firemnú klientelu
IS8	Správa a evidencia sťažností zákazníkov.

Tab. 2.1: Zoznam používaných informačných systémov

Údaje	Popis
PK	Produktový kľúč SW aplikácie (jedno, prípadne viac licenčný)
ID platobných kariet	Identifikačné údaje platobných kariet zákazníkov
Access ID, Multilicencie	Čísla predplatiteľských zmlúv oprávňujúcich prístup k balíkom SW aplikácií uzavretých s korporátnou klientelou
Osobné/firemné údaje	Údaje o domácich a firemných zákazníkoch
Know-how	Know-how interných procesov, ako sú napr. proces overenia a oživenia licencie SW aplikácie, možnosti získania bezplatnej technickej podpory
„Slabé miesta“	Slabé miesta v SW aplikáciách a tiež ich licenčných podmienkach

Tab. 2.2: Zoznam dôležitých spracovávaných typov údajov

II. PRAKTICKÁ ČASŤ – RIADENIE RIZÍK

3 ANALÝZA RIZÍK

Proces riadenia rizík by bolo možné rozdeliť do troch etáp. Prvou, ako som už naznačil v 1.2, je analýza rizík. Po nej nasleduje etapa druhá – vyhodnotenie rizík a na koniec etapa tretia – zvládanie rizík. V tejto kapitole formou analýzy rizík identifikujem riziká plynúce zo spracovania zákazníckych údajov, používania SW nástrojov a postavenia zamestnanca v spoločnosti Zakaznickapodpora. Okrem samotnej AR sú v nej uvedené teoretické základy tejto problematiky a tiež najčastejšie volené prístupy pri jej realizácii.

Analýza rizík (AR) pozostáva z identifikácie a kvantifikácie aktív, hrozieb a zraniteľností. Preto by sa mala opakovať po každej výraznejšej zmene používaných informačných technológií, ako je napríklad nasadenie nového, prípadne úprava stávajúceho informačného systému, objavenie novej hrozby alebo zraniteľnosti. Aktualizácia AR závisí na veľkosti organizácie, zložitosti IT, prípadne miery úpravy IS. Obvykle sa odporúča analýzu rizík aktualizovať v intervale 1 – 4 roky [12]. Pred pristúpením k samotnej AR je potrebné určiť vhodnú metodiku jej prevedenia.

3.1 Výber metodiky analýzy rizík

Určenie vhodnej metodiky je alfou a omegou analýzy rizík. Firmy, ktoré sa AR zaoberajú, si svoju metodiku patrične chránia a považujú ju za svoje Know-how. Spočíva v schopnosti získať čo najviac relevantných informácií, vhodne ich spracovať a interpretovať. Existuje niekoľko SW nástrojov, ktoré dokážu automaticky vygenerovať množstvo analytickej dokumentácie. To by však nemalo byť cieľom tohto procesu. Dôležité je tieto informácie správne interpretovať, orientovať sa v nich, použiť vhodné štatistické a analytické nástroje na ich spracovanie, vhodne ich zobraziť a predovšetkým v nich nájsť súvislosti, ktoré sú pre nás tou onou pridanou hodnotou.

Existujú dva hlavné smery čo do použitia metód AR:

Kvantitatívne metódy. Objavili sa na začiatku 70. rokov a vychádzali z požiadavky formalizácie procesu analýzy rizík informačných systémov. Sú založené na matematickom výpočte rizika z frekvencie výskytu hrozby a jej dopadu. Pre jej vykonanie je nutné disponovať dostatočnou kvalitou a kvantitou vstupných dát. Najznámejšou metódou je ALE (Annualized Loss Expectancy), čiže metóda očakávaných ročných strát [13]. Vychádza z predpokladu veľkosti škody a s ňou súvisiacimi nákladmi na obnovu. Taktiež sa môže jednať aj o finančnú stratu rovnajúcu sa možnému zisku z nevyužitej príležitosti,

alebo naopak zmluvnú pokutu plynúcu z nedodržania záväzkov. Vzorec pre výpočet ALE je nasledujúci:

$$ALE = SLE * ARO$$

kde SLE (Single Loss Exposure) je strata pri jednom výskyte hrozby a ARO (Annualized Rate of Occurence) je pravdepodobnosť, s ktorou sa táto hrozba v priebehu jedného roka vyskytne. Aby sme pokryli všetky straty a hrozby môžeme uvedený vzorec upraviť takto:

$$ALE = \sum_{|=|}^{n} SLE_i * ARO_i$$

Výhodou kvantitatívnych metód je vysoký stupeň formalizácie a teda jednoduchá pochopiteľnosť, jednoznačnosť a presnosť. Výsledkom AR prevedenou týmito metódami sú riziká vyjadrené v spojitej číselnej škále, ktoré predstavujú peniaze. Nevýhodou je zložitosť vykonávanej AR, časová a prostriedková náročnosť. Preto sa pri aplikovaní tejto skupiny metód často využívajú SW nástroje. Najpoužívanejším z nich je CRAMM (CCTA Risk Analysis and Management Methodology). Pri použití SW nástrojov je však potrebné klásť dôraz na spracovanie, interpretáciu a vhodnú vizualizáciu ich výstupov. Zabráni sa tak situácii, kedy výstupom AR je množstvo opatrení, ktoré v konečnom dôsledku skončia založené v archíve alebo v horšom prípade skartované v koši. [13, 14, 15]

„*Nevýhoda týchto metód spočíva v tom, že veľké straty s malou pravdepodobnosťou dávajú rovnaký výsledok, ako malé straty s veľkou pravdepodobnosťou.*“ [15]

Kvalitatívne metódy. Tieto metódy pre popis aktív, hrozieb, zraniteľností a rizík používajú diskrétnu stupnicu (napr. 1 až 5), prípadne slovné vyjadrenie stupňa (napr. nízky až vysoký). Výhodou týchto metód je jednoduchá realizácia, pretože odpadajú výpočty strát a pravdepodobností výskytu hrozieb. Na druhej strane sú však výsledky nejednoznačné a nereprezentujú presné finančné ohodnotenie možných strát a nákladov na ich prevenciu. Pri týchto metódach sa vychádza zo subjektívneho názoru expertov, z čoho plynie náročnosť na veľkosť expertného týmu, aby sa v konečnom dôsledku zaručila objektivita výsledku. [13, 14]

Kombinované metódy. Tieto metódy vychádzajú z číselných údajov. Pri ich použití je možné vďaka kvalitatívnemu hodnoteniu vo väčšom sa priblížiť realite, v porovnaní s predpokladmi, z ktorých vychádzajú kvantitatívne metódy. Je ale potrebné spomenúť, že údaje použité v kvalitatívnych metódach nemusia vždy odrážať priamo pravdepodobnosť

udalostí či výšku ich dopadu, ale môžu byť ovplyvnené mierkou stupnice, ktorá je v konkrétnej metóde použitá [13].

Pre účely tejto DP je využitý kvalitatívny prístup a to z dôvodu nedostatočného množstva dát súvisiacich s frekvenciou výskytu hrozieb a tiež vďaka úzkej oblasti AR, ktorá nemá tak vysokú náročnosť na veľkosť a odbornosť analytického tímu.

3.2 Stanovenie hraníc a hĺbky analýzy rizík

Hranica AR je pomyselná čiara presne určujúca aktíva, ktorými sa budeme v rámci AR zaoberať – ležia vo vnútri hraníc analýzy a ktoré už predmetom analýzy nie sú – ležia za hranicami analýzy. Proces stanovenia hraníc je veľmi dôležitý a preto je mu nutné venovať dostatočné množstvo času a prostriedkov. Nesprávny odhad aktív, ktoré majú byť v projekte AR skúmané, by mohol výraznou mierou narušiť časový harmonogram jeho realizácie, čo by mohlo mať za následok zvýšenie jej nákladov.

U stanovení hĺbky AR sa rozhodujeme, ako podrobne budeme aktíva ležiace vo vnútri hraníc AR skúmať. Podľa [14] hĺbka analýzy rizík vychádza z:

- granulity aktív, teda do akej miery sú aktíva agregované,
- množstva hrozieb, tj. či budeme brať do úvahy iba typické, alebo všetky možné hrozby,
- množstva a skladby respondentov, ktorí budú jednotlivé hrozby a ich možné dopady identifikovať a analyzovať,
- povahy skúmaného systému, ktorý chceme zabezpečiť, s tým súvisí nutná miera dekompozície aktív na menšie elementy; iná bude hĺbka AR pri skúmaní bezpečnosti IS z hľadiska jeho programovej implementácie a použitých komunikačných rotokolov, ako pri analýze procesov definujúcich možnosti používania, správy a prístupu k IS.

Analýza rizík realizovaná v spoločnosti Zakaznickapodpora je zameraná na SW nástroje, resp. procesy, ku ktorým majú operátori CS tímov prístup, resp. ich vykonávajú a zároveň na zákaznícke a firemné údaje, ktoré sú SW nástrojmi pri vykonávaní procesov spracovávané.

3.3 Zostavenie analytického týmu

Na získanie podkladov pre analýzu rizík a jej vlastnú realizáciu je vhodné využiť ako skupinu expertov z oblasti návrhu, správy, konfigurácie a nasadzovania skúmaného IS a podnikových procesov, tak respondentov z radu bežných používateľov a zamestnancov. Obidve tieto skupiny majú pre získanie podkladov značný prínos a netreba ich účasť v procese zhromažďovania vstupných informácií podceňovať. Kým experti dokážu odborne zhodnotiť slabé miesta systému z technického hľadiska, bežný používateľ obohatený každodennými skúsenosťami s jeho používaním prinesie poznatky o tom, ako informácie získané zo systému zneužiť, prípadne priblíži motivačné faktory, ktoré by ho k tejto činnosti mohli viesť.

Zloženie a počet členov týmu sa môže líšiť podľa konkrétneho procesu, ktorý sa práve realizuje. Samotný tým by mohol vyzerať nasledovne (tučným sú vyznačení účastníci zainteresovaní do AR vo firme Zakaznickapodpora):

- používatelia
  - **vlastník systému**
  - **používateľsystému**
  - **vlastník procesu**
  - **vykonávateľ procesu**
- experti
  - **správca systému**
  - **správca aplikácie**
  - správca databázy
  - **správca siete**
  - **pracovník informačnej bezpečnosti**
  - pracovník fyzickej bezpečnosti
  - systémový analytik
  - **pracovník riadenia ľudských zdrojov**

3.4 Metódy získavania podkladov pre AR

Ak máme vybraný okruh pracovníkov, ktorí sa na analýze rizík budú podieľať, je potrebné zvoliť vhodné metódy zberu informácií potrebných pre jej realizáciu. Tento krok je taktiež

dôležitý hlavne z pohľadu adekvátnosti podkladov a efektívnosti ich získavania. V ďalšom sú popísané najvyužívanejšie metódy.

Workshop

Workshop je stretnutie odbornej skupiny, ktoré by malo prebehnúť podľa vopred stanoveného časového harmonogramu. Obvykle sa organizuje v zasadacej miestnosti, pričom účastníci by mali sedieť za pracovným stolom v tvare polkruhu tak, aby mali všetci dobrý výhľad na flipchart, tabuľu, prípadne plátno. U tohto typu schôdzky môže byť definovaných niekoľko rolí, ktoré prispejú k efektívnej organizácii a využitiu času. Sú to: účastníci, facilitátor, zapisovateľ, analytik, expert a asistent/ kontrolór času.

Brainstorming

V oblasti analýzy rizík sa zvykne využívať upravená metóda klasického brainstormingu. Spočíva v tom, že účastníci dostanú v dostatočnom časovom predstihu zadanie, ktoré si budú môcť v pokoji súkromia preštudovať a navrhnúť vlastné riešenie. To potom zdokumentujú a vytlačené prinesú na naplánovaný brainstorming. Počas samotného stretnutia organizátor prednesie všetky návrhy, ku ktorým môžu všetci účastníci zaujať svoj vlastný postoj. Výsledkom bude to najlepšie riešenie, prípadne sa na základe predložených návrhov vytvorí riešenie nové. [15]

Dotazníkový formulár

Na získanie informácií od väčšieho počtu respondentov sa s obľubou využíva dotazníkový formulár, alebo tiež dotazník. Jedná sa o časovo a nákladovo nenáročnú metódu. Aby mali takto získané informácie požadovanú výpovednú hodnotu, je nutné aby otázky v ňom položené boli pre respondentov zrozumiteľné a jednoznačné. Dotazníky môžeme jednoducho distribuovať v tlačenej forme, ideálne však elektronicky e-mailom, alebo prostredníctvom webových formulárov.

Delfská metóda

Tiež známa ako metóda Delphi. Tejto prognostickej metódy sa spravidla zúčastňujú skupiny expertov, ktorí nezávisle na sebe reagujú na dotazníkový prieskum a vyplnené dotazníky posielajú organizátorovi. Tento prijaté návrhy sumarizuje a spätne distribuuje medzi respondentov. Tento proces sa opakuje tak dlho, kým sa experti nezhodnú na spoločnom riešení. Ideálny počet iterácií sa v praxi udáva 2 až 3, väčší počet by bol neefektívny [15]. Medzi respondentmi by nemali chýbať používateľ, správca a gestor

hodnoteného systému. Distribúcia dotazníkov prebieha obdobným spôsobom, ako u predchádzajúcej metódy.

Pohovor

V prípade potreby detailnej analýzy je vhodné využiť metódu pohovoru, alebo tiež Interview. Aby sa získali otvorené, objektívne a nikým neovplyvňované názory, stretnutie by sa malo konať v neutrálnom prostredí a mala by ho viesť nezávislá osoba, nie respondentov priamy alebo nepriamy nadriadený. Interview by sa mal zúčastniť každý typický používateľ systému, vždy však samostatne a samozrejmosťou by malo byť zachovanie anonymity účastníkov.

Papierový kolotoč

Medzi účastníkmi koluje papier, v záhlaví ktorého je popísaný problém, prípadne už samotné riešenie. Každý z účastníkov k nemu zaujme vlastné stanovisko. Obdobnou metódou je diskusná štafeta. Jej súčasťou môže byť navyše hodnotenie, alebo preferenčné usporiadanie navrhnutých riešení.

Diablov advokát

V tejto metóde, v angličtine nazývanej Devil's advocate, hrá expert rolu „diablovho advokáta“, ktorého jediným cieľom je jasnými, presnými a logickými argumentmi vyvrátiť každú myšlienku/ nápad jednotlivých účastníkov. V diskusii, ktorá sa nesie v prísne vecnej rovine nesmie dochádzať k napádaniu osôb, ale iba ich názorov.

3.5 Analýza a ďalšie spracovanie získaných informácií

Aby sme mohli získané informácie spracovať a použiť na analýzu rizík, je potrebné zabezpečiť ich normalizáciu podľa požiadaviek vstupov AR. Túto úlohy si vieme do značnej miery zjednodušiť už pri príprave procesu získavania informácií navrhnutím štandardizovaných formulárov a dotazníkov. Respondentom by sme mali jasne povedať, v akom formáte výsledky očakávame, v akých merných jednotkách apod. Veľmi efektívnym spôsobom je využitie webových formulárov, u ktorých vieme vykonať validáciu vyplnených údajov ešte pred ich odoslaním. Takto získané informácie by sme mali účelne analyzovať, aby sme oddelili odpovede, ktoré sa odlišujú od tých väčšinových a na tieto sa zamerať. V ďalšom by sme mali zistiť prečo sú vytypované odpovede odlišné od tých ostatných. Dôvodom môže byť nepochopenie otázky respondentom, schválne uvádzanie nezmyselných informácií, ale často sa môže jednať o jediné a správne riešenie.

Ak máme získané informácie vhodne štandardizované, je na mieste riešiť otázku ich interpretácie a vizualizácie. Existuje na to množstvo SW nástrojov, ktoré sú schopné generovať profesionálne vyzerajúce grafy a reporty. Tu je dôležitá úloha analytika, aby tieto výstupy vhodne upravil do jednoznačnej a zrozumiteľnej podoby. Toto je nevyhnutné pre podporu manažmentu spoločnosti pri rozhodovaní o prijímaní ďalších krokov súvisiacich s AR a tiež, aby zistené skutočnosti nebral na ľahkú váhu.

Na záver je potrebné všetky získané podklady pre ďalšie použitie dôkladne zdokumentovať:

Názov dokumentu	Obsah Dokumentu
Zoznam aktív	Zoznam všetkých procesov a ich aktív, zoznam vlastníkov aktív, ich ohodnotenie a vizuálne modely analyzovaného systému.
Zoznam hrozieb	Zoznam všetkých hrozieb a ich miery.
Zoznam zraniteľností	Zoznam všetkých zraniteľností pre dvojicu aktívum X hrozba.
Zoznam rizík	Zoznam všetkých rizík.
Zoznam opatrení	Zoznam už zavedených opatrení a opatrení, ktoré majú byť zavedené.
Analýza rizík	Vzniká z predchádzajúcich dokumentov.
Analýza rizík	Podklad pre prezentáciu výsledkov AR vlastníkovi analyzovaného systému.

Tab. 3.1: Zoznam dokumentov AR

3.6 Aktíva

Aktívom označujeme všetko, čo má pre našu organizáciu hodnotu, ktorá môže byť pôsobením hrozieb znížená. Aktíva delíme na hmotné a nehmotné. V oblasti riadenia informačných rizík je chápanie týchto dvoch pojmov odlišné od bežného. Medzi hmotné aktíva patrí HW, SW apod. Nehmotnými aktívami označujeme napr. know-how alebo informácie. Proces spracovania aktív pozostáva zo štyroch etáp: identifikácia aktív, dekompozícia aktív, zoskupenie aktív a kvantifikácia, čiže zhodnotenie aktív.

3.6.1 Identifikácia aktív

Identifikáciou aktív rozumieme zistenie hlavných aktív (ležiacich vo vnútri hraníc AR) a určenie ich vlastníkov. Na zistenie aktív využijeme BPA (Business Process Analysis). Predmetom tejto analýzy sú všetky hlavné procesy, v ktorých vystupuje používanie IS,

prípadne nakladanie s údajmi z neho získanými. Spravidla platí vzťah „jeden proces = jedno aktívum“. Dôležitým predpokladom pre realizáciu procesne orientovanej analýzy je dobrá znalosť organizácie a samotných obchodných procesov. Preto je vhodné, aby sa na identifikácii aktív podieľali interní zamestnanci pobočky. V našom prípade to boli CS tím manažéri a CS koučovia formou dotazníkového prieskumu. E-mailom im bol zaslaný formulár so sprievodnými informáciami o jeho vyplnení. Po sumarizácii vyplnených formulárov a vylúčení duplicitných položiek sa k jednotlivým aktívam priradia ich vlastníci. Vlastník aktíva je väčšinou vlastník procesu, v ktorom aktívum vystupuje. Vlastníkom procesu rozumieme nariaďovateľa vykonávania procesu, tj. osoba (manažér), ktorá vykonávanie procesu požaduje. V našom prípade má každý analyzovaný proces rovnakého vlastníka – tím manažér CS a preto ho nebudem uvádzať.

3.6.2 Dekompozícia aktív

Vo fáze dekompozície aktív delíme (dekomponujeme) hlavné aktíva (jednotlivé procesy) na objekty (jednotlivé zdroje a IS), ktoré budeme neskôr označovať ako aktíva. Tento postup opakujeme, až kým nedostaneme požadovanú úroveň dekompozície aktív. Stupeň úrovne závisí na zložitosti systému a požiadavky na hĺbku AR.

3.6.3 Zoskupenie aktív

Ak máme určené všetky aktíva, s ktorými budeme v AR pracovať, mali by sme sa zamyslieť nad vhodným zoskupením (agregáciou) aktív. Aktíva zoskupujeme hlavne preto, že v ďalších fázach budeme hodnotiť, aké hrozby na jednotlivé aktíva pôsobia a aká je zraniteľnosť jednotlivých aktív voči hrozbe. Je zrejmé, že čím viac aktív budeme hodnotiť, tým bude AR časovo náročnejšia. Aktíva zoskupujeme podľa účelu a ich spoločných vlastností [14].

3.6.4 Hodnotenie aktív

Kvantifikácia aktív, čiže stanovenie hodnoty jednotlivých aktív je poslednou etapou dokumentácie aktív. Existuje niekoľkou metód určenia hodnoty aktív. My použijeme metódu BIA (Business Impact Analysis). Jedná sa o metódu hodnotenia dopadu, tzn. že riešime otázky typu „čo by sa stalo, ak by došlo k narušeniu integrity, dôvernosti alebo dostupnosti aktíva“. Na vyjadrenie stupňa dopadu sa u tejto metódy využíva diskrétna stupnica, ktorej slovné vyjadrenie môže vyzerať napr. žiadny – nízky – stredný – vysoký – kritický. Ja som volil stupnicu so štyrmi úrovňami. Domnievam sa, že párny počet stupňov

je vhodnejší, pretože eliminuje častý výber strednej hodnoty (3 u 5 stupňovej škály), ku ktorému môžu respondenti pri hodnotení inklinovať. Hodnotiaca stupnica je uvedená v Tab. 3.2.

Stupeň	Skratka	Výška dopadu	Popis dopadu	Škoda od – do
1	N	nízka	malé škody	0 – 0,3
2	S	stredná	vážne škody	0,3 – 3
3	V	vysoká	veľmi vážne škody	3 – 30
4	K	kritická	prežitie je ohrozené	30 – 100

Tab. 3.2: Stupnica hodnôt aktív

Ohodnotenie aktív sa v našom prípade vykonalo na základe stupňa negatívnych dopadov niekoľkých typov, ktoré by vznikli ako možný následok narušenia základných bezpečnostných charakteristík aktíva – dostupnosti, dôvernosti a integrity realizáciou ľubovoľnej hrozby. Typy dopadov ako aj slovné vyjadrenie ich stupňov sú znázornené v Tab. 3.3.

Stupeň	Businessflow	Cashflow	Imidž klienta	Dôvera klienta
1	malé škody	0 – 0,3	nenarušený	nenarušená
2	vážne škody	0,3 – 3	čiastočne narušený	klient nerozšíri spoluprácu
3	veľmi vážne škody	3 – 30	narušený v národnom meradle	klient uvažuje o zmene dodávateľa služieb
4	prežitie je ohrozené	30 – 100	narušený v medzinárodnom meradle	klient ruší spoluprácu

Tab. 3.3: Typy hodnotených dopadov

Businessflow (BF) – dopad na existenciu spoločnosti Zakaznickapodpora pobočka Brno.

Cashflow (CF) – dopad na celkový finančný príjem spoločnosti Zakaznickapodpora pobočka Brno uvádzaný v % z celkového obratu.

Imidž klienta (IK) – dopad na imidž klienta u verejnosti.

Dôvera klienta (DK) – dopad na dôveru klienta, a teda možnosti ďalšieho rozšírenia spolupráce.

Samotnú kvantifikáciu aktív realizovali Operations manažér a SDM podľa typu dopadu. Výstupom tejto fázy je dokument „Zoznam aktív“, ktorý je znázornený v Tab. 3.4.

Pre lepšiu ilustráciu sú aktíva zoskupené do dvoch kategórií (nástroje – IS a informácie – zdroje – metriky) a stupne dopadov vyjadrené číselne.

#	Aktívum	BF	CF	IK	DK
	Nástroje – IS				
1.	IS1 + IS2	2	3	3	3
2.	IS3	2	3	3	3
3.	IS4	2	3	1	3
4.	IS5	1	1	1	1
5.	IS6	1	2	1	2
6.	Poštový klient (doména @klient1.com)[8]	1	2	3	2
7.	IS7	2	3	2	3
8.	IS8	1	2	1	2
	Informácie – zdroje – metriky				
9.	Identifikačné údaje platobnej karty	3	4	4	4
10.	Jednolicenčný PK	1	2	2	2
11.	Multilicenčný PK	2	3	2	2
12.	Dôvera a spokojnosť zákazníka – CSAT	2	3	2	2
13.	Service Level[9]	1	2	1	1
14.	SA/Access ID/Multilicencie a iné čísla zmlúv	2	3	2	3
15.	Kontaktné a osobné/firemné údaje o zákazníkovi	2	3	3	3
16.	Interné KNOW-HOW callcentra	2	3	1	1
17.	Informácie o chybách v produktoch a ich licenciách	1	2	1	2
18.	Know-how aktivácie	1	2	1	2
19.	Know-how získania bezplatného SRX	1	1	1	2

Tab. 3.4: Zoznam aktív

3.7 Hrozby

Hrozba je akákoľvek udalosť, ktorá môže negatívne pôsobiť na dôvernosť, integritu alebo dostupnosť aktíva. Tieto udalosti môžu byť vyvolané vedome s cieľom poškodiť aktívum, ale tiež nevedome – chybou pracovníka, prípadne živelnou pohromou. Pre naše účely budeme brať v úvahu hrozby vyvolané človekom – pracovníkom, či už úmyselne alebo

[8] Každý operátor má k dispozícii e-mailové konto s doménou @Klient1.
[9] Zmluvou definovaný čas telefonickej, alebo e-mailovej odozvy operátora počas prevádzkovej doby infolinky.

neúmyselne. Hrozby, podobne ako aktíva, musíme najskôr identifikovať. Výstupom tejto fázy bude zoznam všetkých hrozieb, ktoré následne ohodnotíme, čiže kvantifikujeme. Po kvantifikácii hrozieb bude zrejmé, ktoré z nich ohrozujú spoločnosť najviac, ktoré menej a ktoré vôbec – tieto môžeme z ďalšieho priebehu AR vypustiť.

3.7.1 Identifikácia hrozieb

Pri tomto procese je kľúčové identifikovať všetky hrozby. Prehliadnutie jedinej vážnejšej hrozby môže mať za následok znehodnotenie celkového výsledku AR a v konečnom dôsledku neefektívne vynaloženie značných prostriedkov na prijatie opatrení. Preto je vhodné do tohto procesu zainteresovať čo najväčšiu skupinu ľudí napr. formou dotazníkového prieskumu. Dôležitý je tiež výber cieľovej skupiny respondentov. Keďže cieľom tejto DP je odhaliť možné riziká zneužitia postavenia operátora zákazníckej podpory, ako ideálna osoba na odhalenie hrozieb sa naskytá práve samotný operátor. Preto som oslovil všetkých CS operátorov so žiadosťou o vyplnenie dotazníka. V ňom boli operátori inštruovaní vložiť sa do role útočníka a vymyslieť čo najviac možných spôsobov útokov na vypísané aktíva.

Najväčším problémom, s ktorým som sa stretol, bol nezáujem respondentov. Napriek tomu sa našlo niekoľko pracovníkov, ktorí boli ochotní sa zamyslieť a aktívne sa zapojiť do prieskumu. Po obdŕžaní vyplnených dotazníkov som jednotlivé hrozby zosumarizoval, vylúčil duplicitné položky a doplnil vlastnými návrhmi. Tieto som spätne poslal aktívnym zúčastneným na opätovné zamyslenie. Nakoniec sme usporiadali spoločné stretnutie, na ktorom sme si ujasnili význam jednotlivých hrozieb a doplnili niekoľko ďalších. Výsledkom bolo 19 konkrétnych dvojíc aktívum – hrozba. Jednotlivé hrozby som zoskupil do piatich kategórií – Zneužitie/ prezradenie informácií (ZI), Zneužitie SW nástroja (ZN), Krádež (K), Úmyselné poškodenie (US) a Chyba používateľa (CH). V Tab. 3.5 je zobrazená matica aktív a hrozieb, ktoré na jednotlivé aktíva pôsobia.

#	Aktívum	ZI	ZN	K	UŠ	CH
	Nástroje – IS					
1.	IS1 + IS2		X			
2.	IS3		X			
3.	IS4		X			
4.	IS5		X			
5.	IS6		X			
6.	Outlook, resp. domena @klient1.com		X			
7.	IS7		X			
8.	IS8		X			
	Informácie – zdroje – metriky					
9.	Identifikačné údaje platobnej karty			X		
10.	Jednolicenčný PK			X		
11.	Multilicenčný PK			X		
12.	Dôvera a spokojnosť zákazníka – CSAT				X	X
13.	Service Level				X	X
14.	SA/Access ID/Multilicencie a iné čísla zmlúv			X		
15.	Kontaktné a osobné/firemné údaje o zákazníkovi			X		
16.	Interné KNOW-HOW callcentra	X				
17.	Informácie o chybách v produktoch a ich licenciách	X				
18.	Know-how aktivácie	X				
19.	Know-how získania bezplatného SRX	X				

Tab. 3.5: Matica aktív a hrozieb

3.7.2 Kvantifikácia hrozieb

Po identifikácii možných hrozieb je potrebné stanoviť ich hodnotu. Pri hodnotení hrozieb sa analyzuje každá dvojica hrozba – aktívum samostatne. To znamená, že pre každú dvojicu hrozba – aktívum je nutné stanoviť vlastnú hodnotu úrovne hrozby. Na kvantifikáciu hrozieb neexistuje presný a jednoznačný algoritmus, a preto výsledná hodnota ešte viac, ako hodnota dopadu (viď 3.6.4), závisí na úsudku osoby, ktorá sa na hodnotení podieľa. Pre účely kvantifikácie hrozieb si tieto rozdelíme do dvoch skupín na:

- úmyselné – hrozby (škody) spôsobené vedomou činnosťou operátora,
- neúmyselné – hrozby (škody) spôsobené nevedomou činnosťou operátora – preklepy, chyby pri zadávaní dát do IS spôsobené neznalosťou problematiky a pod.

Každá skupina hrozieb bude hodnotená podľa jej príznačných kritérií tak, aby stanovená hodnota hrozby čo najviac odzrkadľovala reálnu skutočnosť. Pri hodnotení hrozieb označených ako úmyselné vychádzam z faktorov, ktorými som sa nechal inšpirovať z [15]:

- atraktivita aktíva,
- znalosti a schopnosti potrebné na uskutočnenie hrozby,
- čas a námaha potrebné na uskutočnenie hrozby.

Pri hodnotení neúmyselných hrozieb prichádza do úvahy jediný faktor, a to pravdepodobnosť výskytu hrozby. Pri určovaní pravdepodobnosti je možné vychádzať z interných štatistík, prípadne aj štatistík iných firiem pôsobiacich v rovnakej sfére. Predmet činností, ktoré v tejto analýze hodnotíme je natoľko špecifický, že budeme vychádzať výlučne z interných štatistických zdrojov. Podobne ako u kvantifikácie aktív je aj tu potrebné stanoviť si hodnotiacu stupnicu, ktorá bude pre všetky typy hrozieb rovnaká. Opäť bude postačovať diskrétne hodnotenie v štyroch stupňoch. Podrobný popis jednotlivých stupňov je zrejmý z Tab. 3.6.

Stupeň	Skratka	Úroveň hrozby	Popis hrozby	Od [%]	Do [%]
1	N	nízka	nepravdepodobná	0	25
2	S	stredná	pravdepodobná	25	50
3	V	vysoká	vysoko pravdepodobná	50	75
4	K	istá	istá	75	100

Tab. 3.6: Stupnica hodnôt hrozieb

V nasledujúcich podkapitolách 3.7.2.1 a 3.7.2.2 sú jednotlivé faktory vysvetlené podrobne. Na konci tejto kapitoly je potom uvedený zoznam dvojíc aktívum – hrozba s ich dielčimi ako aj celkovými úrovňami. Na ich hodnotení som sa podieľal ja spoločne s TTI špecialostom a oddelením Q&R

3.7.2.1 *Úmyselné škody*

Ako som už spomenul, úroveň hrozieb plynúcich z úmyselných škôd hodnotím z pohľadu troch faktorov. Pre každú dvojicu aktívum – hrozba je stanovená čiastková hodnota hrozby pri uvažovaní každého faktoru zvlášť. Výsledná úroveň hrozby je vypočítaná ako aritmetický priemer čiastkových hodnôt.

Faktor č. 1 – atraktivita aktíva

Pri posudzovaní atraktivity aktíva vychádzame z hodnoty, ktorú pre páchateľa samotné aktívum predstavuje, ako mieru motivácie uskutočnenia hrozby. To znamená, aký zisk pre škodcu plynie zo zneužitia konkrétneho aktíva. Hodnotiaca stupnica je zobrazená v Tab. 3.7.

Stupeň	Skratka	Atraktivita aktíva	Od [%]	Do [%]
1	N	Realizácia hrozby neprinesie útočníkovi žiadne finančné prostriedky, prípadne iný hmotný úžitok.	0	25
2	S	Relizáciou hrozby je možné získať minimálne finančné prostriedky v rádoch sto Kč	25	50
3	V	Realizáciou hrozby je možné získať finančné prostriedky v rádoch tisíc Kč	50	75
4	K	Realizáciou hrozby je možné získať značné finančné prostriedky v rádoch desaťtisíc Kč.	75	100

Tab. 3.7: Hodnotiaca stupnica pre atraktivitu aktíva

Faktor č. 2 – znalosti a schopnosti

Pri posudzovaní tohto faktoru vychádzame z úrovne znalostí a schopností, ktorými musí páchateľ disponovať, aby bol schopný hrozbu uskutočniť. Posudzujeme pri tom ako fyzické, tak mentálne schopnosti a zručnosti. Hodnotiacu stupnicu u tohto faktora som zvolil podľa [15] a je zobrazená v Tab. 3.8.

Stupeň	Skratka	Znalosti, schopnosti a zručnosti	Od [%]	Do [%]
1	N	K realizácii hrozby je potrebné mať také znalosti, ktoré nie je možné bežne dosiahnuť.	0	25
2	S	K realizácii hrozby je potrebné mať nadpriemerné znalosti.	25	50
3	V	K realizácii hrozby je potrebné mať priemerné znalosti.	50	75
4	K	K realizácii hrozby postačujú základné znalosti a tá tak môže byť realizovaná kýmkoľvek.	75	100

Tab. 3.8: Hodnotiaca stupnica úrovne potrebných znalostí, schopností a zručností

Faktor č. 3 – čas a námaha

Pri posudzovaní tohto faktoru vychádzame z množstva času a námahy, ktoré páchateľ musí vynaložiť na uskutočnenie hrozby. Hodnotiaca stupnica je zobrazená v Tab. 3.9.

Stupeň	Skratka	Čas a námaha	Od [%]	Do [%]
1	N	Čas realizácia hrozby sa pohybuje rádovo v hodinách	0	25
2	S	Čas realizácia hrozby sa pohybuje rádovo v desiatkách minút	25	50
3	V	Čas realizácia hrozby sa pohybuje rádovo v minútach	50	75
4	K	Hrozba môže byť uplatnená okamžite.	75	100

Tab. 3.9: Hodnotiaca stupnica množstva času a námahy

3.7.2.2 *Neúmyselné škody*

Neúmyselné hrozby sú spôsobené nevedomou činnosťou operátora. Môže to byť nesprávne zaevidovanie a zaradenie technického incidentu do nesprávnej rúry, použitie nevhodnej šablóny pri zakladaní technického incidentu, prípadne chybné prepojenie zákazníka na nesprávne oddelenie. Na prvý pohľad by sa zdalo, že tieto chyby nemajú negatívny vplyv na objekt rizikovej analýzy. Z prieskumných dotazníkov spokojnosti zákazníka však vyplýva, že aj tieto, na prvý pohľad, „maličkosti“ zákazník vníma a zohľadňuje pri ich vypĺňaní. Pozorný čitateľ si určite všimol, že spokojnosť zákazníka je jedným z hodnotených aktív, aj preto je týmto chybám nutné venovať náležitú pozornosť. Keďže pri hodnotení tohto typu hrozieb sa môžeme oprieť iba o pravdepodobnosť ich výskytu, problémom môže byť nedostatok alebo celková absencia štatistických údajov potrebných pre určenie pravdepodobností. V prípade tejto analýzy sa o reálne štatistické údaje opieram iba z časti a vychádzam tiež z vlastných skúseností, prípadne skúsenosti kolegov, ktorí sa na hodnotení hrozieb podieľali. Stupnica neúmyselných hrozieb, podľa ktorej dvojice aktívum – hrozba hodnotím je uvedená v Tab. 3.10.

Stupeň	Skratka	Pravdepodobnosť	Od [%]	Do [%]
1	N	nepravdepodobná	0	25
2	S	pravdepodobná	25	50
3	V	vysoko pravdepodobná	50	75
4	K	istá	75	100

Tab. 3.10: Hodnotiaca stupnica pravdepodobnosti výskytu neúmyselnej hrozby

3.7.2.3 *Výpočet úrovní hrozieb*

Na výpočet celkovej úrovne hrozby pre každú dvojicu aktívum – hrozba som použil aritmetický priemer dielčich hodnôt odpovedajúcich uvažovaným faktorom. V niektorých prípadoch by sa vyjadrenie celkovej úrovne hrozby dalo spresniť pridelením rôznych váh jednotlivým faktorom, prípadne pridaním ďalších faktorov, ako je napríklad zodpovednosť alebo poctivosť potenciálneho útočníka – operátora. Domnievam sa, že pri uvažovaní týchto „sociálnych“ činiteľov, by boli úrovne jednotlivých hrozieb globálne nižšie a reálnejšie. Avšak posúdiť faktory takéhoto typu, prípadne im priradiť odpovedajúcu váhu presahuje možnosti tejto práce a preto ich nebudem brať do úvahy. V Tab. 3.11 sú uvedené hodnoty čiastočných a im odpovedajúcich celkových hrozieb.

#	Aktívum	Hrozba	Úroveň hrozby				
			AA	**ZS**	**ČN**	**P**	**C**
1.	IS1 + IS2	ZN	3	3	2	–	3
2.	IS3	ZN	3	3	2	–	3
3.	IS4	ZN	4	3	3	–	3
4.	IS5	ZN	1	2	2	–	2
5.	IS6	ZN	2	4	3	–	3
6.	Outlook, resp. domena @klient1.com	ZN	1	3	2	–	2
7.	IS7	ZN	4	3	3	–	3
8.	IS8	ZN	2	2	2	–	2
9.	Identifikačné údaje platobnej karty	K	4	3	3	–	3
10.	Jednolicenčný PK	K	2	3	3	–	3
11.	Multilicenčný PK	K	2	3	3	–	3
12.	Dôvera a spokojnosť zákazníka – CSAT	UŠ	1	3	2	–	2
13.	Dôvera a spokojnosť zákazníka – CSAT	CH	–	–	–	1	1
14.	Service Level	UŠ	2	3	2	–	2
15.	Service Level	CH	–	–	–	1	1
16.	SA/Access ID/Multilicencie a iné čísla zmlúv	K	3	3	3	–	3
17.	Kontaktné a osobné/firemné údaje o zákazníkovi	K	2	3	2	–	2
18.	Interné KNOW-HOW callcentra	ZI	3	2	2	–	2
19.	Informácie o chybách v produktoch a ich licenciách	ZI	1	3	2	–	2
20.	Know-how aktivácie	ZI	1	4	4	–	3
21.	Know-how získania bezplatného SRX	ZI	2	4	4	–	3

Tab. 3.11: Hodnoty čiastočných a celkových hrozieb

Legenda:

AA – atraktivita aktíva

ZS – znalosti a schopnosti

ČN – čas a námaha

ZI – Zneužitie/ prezradenie informácií

ZN – Zneužitie SW nástroja

K – Krádež

US – Úmyselné poškodenie

CH – Chyba používateľa

3.8 Zraniteľnosť

Zraniteľnosť chápeme ako slabé miesto aktíva, ktoré môže byť zneužité hrozbou za účelom narušenia dostupnosti, integrity alebo dôvernosti aktíva. Miera zraniteľnosti určuje, nakoľko je aktívum voči pôsobeniu hrozby odolné. Podobne ako u aktív a hrozieb, aj zraniteľnosti identifikujeme a hodnotíme. Postup však bude v tomto prípade odlišný. V predošlých fázach sme identifikovali aktíva a hrozby priamo. Zraniteľnosti identifikujem a hodnotím prostredníctvom prijatých opatrení, ktoré by ich mieru mali znižovať.

3.8.1 Identifikácia opatrení

V tejto fáze projektu je dôležité starostlivo identifikovať všetky opatrenia, ktoré sú v súčasnosti prijaté a aplikované na ochranu aktív. Aj tejto časti je potrebné venovať zvýšenú pozornosť s cieľom skutočne odhaliť všetky opatrenia. Aby sa niektoré z nich neopomenuli, pomôžem si podrobným zoznamom možných opatrení z [16]. V nasledujúcom je uvedený ich výpis. Tučným písmom sú vyznačené tie, ktoré sú už nejakým spôsobom zavedené a funkčné. Na identifikácii sa podieľali Operations Manager, TTI Specialist, HR Specialist a tím manažéri CS oddelení.

1. Personálne – je potrebné zaistiť dostatočný počet kvalitných pracovníkov

1.1 Pri prijímaní zamestnancov

1.1.1 Referencie – referencie uvádzané v životopise by mali byť overené.

1.1.2 Vzdelanie – doklady o dosiahnutom vzdelaní by mali byť overené.

1.1.3 Totožnosť – totožnosť by mala byť overená pomocou ďalšieho dokladu.

1.1.4 Bezúhonnosť – bezúhonnosť uchádzača o zamestnanie by mala byť overená.

1.1.5 Zmluva – súčasťou zmluvy by mala byť klauzula o zachovaní dôvernosti.

1.2 Pri trvaní a ukončovaní pracovného pomeru

1.2.1 Vzdelávanie – malo by byť zaistené sústavné vzdelávanie v oblasti informačnej bezpečnosti.

1.2.2 Dodržiavanie politiky – bezpečnostná politika by mala byť dodržiavaná.

1.2.3 Kontrola – mala by prebiehať pravidelná kontrola, či je bezpečnostná politika dodržiavaná.

1.2.4 Hlásenia – všetky neštandardné stavy, incidenty a podozrenia na ne by mali byť hlásené.

1.2.5 Šetrenia – v prípade porušenia, alebo podozrenia na nedodržiavanie bezpečnostnej politiky zahájiť šetrenie.

1.2.6 Vyvodenie dôsledkov – v prípade porušenia bezpečnostnej politiky by mali byť vyvodené dôsledky.

1.2.7 Koučing – mal by byť zabezpečený neustály koučing zamestnancov s upozornením na chyby a v prípade ich opakovania vyvodiť dôsledky.

1.2.8 Odobranie práv pri ukončovaní pracovného pomeru – prístupové práva do systému by mali byť odobrané.

2. Logické — prístup k informáciám by mal byť riadený princípom need to know

2.1 Správa prístupových oprávnení

2.1.1 Malo by byť určené, kto môže žiadať, schvaľovať, zriaďovať a rušiť prístup do IS.

2.1.2 Požiadavka na zriadenie, zrušenie a zmenu prístupu by mal existovať v písomnej podobe.

2.1.3 Prístupové práva by mali byť jasne stanovené a dokumentované pre jednotlivca a skupinu.

2.1.4 Nepoužívané účty by mali byť zrušené alebo zablokované – pravidelne kontrolovať.

2.1.5 Odoberať práva zamestnancom, ktorí odchádzajú do iného oddelenia alebo končia.

2.1.6 Užívateľ by mal podpísať, že mu bol prístup zriadený a rozumie podmienkam prístupu.

2.1.7 Užívateľ by mal mať možnosť zistiť, kam má pridelené prístupy.

2.1.8 Pridelené prístupové oprávnenia by mali byť pravidelne kontrolované.

2.2 Správa a používanie hesiel

2.2.1 K overeniu identifikácie užívateľa by malo byť použité heslo.

2.2.2 Heslá by si užívatelia mali pravidelne meniť.

2.2.3 Heslá by mali byť udržiavané v tajnosti a užívatelia by ich nemali nikomu prezrádzať.

2.2.4 Heslá by si užívatelia nemali nikam zapisovať s výnimkou bezpečného uloženia.

2.3 Zásada prázdnej obrazovky

2.3.1 Pri krátkodobom prerušení práce by mal užívateľ počítač SW uzamknúť.

2.3.2 Pri ukončení práce by sa mal užívateľ odhlásiť.

2.3.3 Nepoužívaný počítač by sa mal po určitej dobe nečinnosti sám uzamknúť.

2.4 Riadenie prístupu k sieti a sieťovým prvkom

2.4.1 Do siete by nemalo byť možné pripojovať neautorizované zariadenia.

2.4.2 Prevádzka na sieti a prístup do Internetu by mali byť filtrované na základe dokumentovaných pravidiel.

2.4.3 Prístup do iných sietí a Internetu by mal byť povolený iba vybraným užívateľom.

2.5 Riadenie prístupu k operačným systémom (OS)

2.5.1 OS by mal vynútiť kvalitné heslá a obmedziť ich platnosť.

2.5.2 OS by mal po prihlásení užívateľovi zobraziť dátum posledného prihlásenia.

2.5.3 OS by mal po prihlásení užívateľovi zobraziť počet neúspešných pokusov o prihlásenie.

2.6 Riadenie prístupu k výstupným zariadeniam

2.6.1 Právo zapisovať na vymeniteľné média by malo byť povolené len vybraným osobám.

2.6.2 Právo obstarávať tlačové kópie by malo byť povolené len vybraným osobám.

3. Administratívne

3.1 Vlastná organizácia

3.1.1 Mala by existovať osoba zodpovedná za riadenie bezpečnosti.

3.1.2 Mala by existovať Bezpečnostná politika a mal by byť určený jej vlastník.

3.1.3 Bezpečnostná politika by mala byť pravidelne revidovaná.

3.1.4. Mali by byť jednoznačne definované povinnosti a zodpovednosti všetkých zamestnancov.

3.1.5. Zamestnanci organizácie by mali potvrdiť svojím podpisom, že boli s politikou zoznámení.

3.2 Auditovanie a monitoring práce na PC a s IS

3.2.1 Úroveň auditovania a monitorovania by mala byť stanovená na základe vykonanej AR.

3.8.2 Kvantifikácia zraniteľností

Pri stanovení úrovne zraniteľností je nutné posúdiť prostredie a zavedené protiopatrenia, ktoré túto úroveň znižujú. Podľa [17] je okrem samotných implementovaných opatrení potrebné zohľadniť aj ich správnosť a schopnosť efektívne znižovať mieru zraniteľností. Toto sa dá v tak rýchlo meniacom sa prostredí docieliť analýzou procesu zavádzania, dokumentovania a kontroly týchto opatrení. Podľa [15] je pre tento účel vhodné použiť upravenú stupnicu zrelosti procesov CMM[10]:

1. Žiadne opatrenie nie je zavedené – ak nie je žiadne opatrenie zavedené, je takmer isté, že hrozba sa uplatní a môžeme preto hovoriť o kritickej zraniteľnosti.
2. Opatrenia nie sú zdokumentované – opatrenia sú zavedené, ale tým že nie sú zdokumentované, je pravdepodobné, že ich ani nikto všetky neskontroluje. Dá sa preto predpokladať, že so značnou pravdepodobnosťou dôjde k uplatneniu hrozby – zraniteľnosť je vysoká.
3. Opatrenia sú zdokumentované – vzhľadom k tomu, že neprebieha kontrola funkčnosti týchto opatrení a už vôbec nedochádza k ich zlepšovaniu, dá sa predpokladať, že môže dôjsť k uplatneniu hrozby – zraniteľnosť je stredne vysoká.
4. Opatrenia sú zdokumentované, kontrolované – dá sa predpokladať, že nefunkčné opatrenia sa podarí včas odhaliť a hrozba nebude mať príležitosť sa uplatniť. Vzhľadom k tomu, že nedochádza k zlepšovaniu opatrení, tieto nebudú dostatočne účinné voči novým zraniteľnostiam – zraniteľnosť je stredná.
5. Opatrenia sú zdokumentované, kontrolované a dochádza k ich priebežnému zlepšovaniu – hrozba nebude mať s najväčšou pravdepodobnosťou príležitosť sa uplatniť – zraniteľnosť je nízka.

Na kvantifikáciu aktív a hrozieb sme použili stupnicu so štyrmi diskrétnymi stupňami. Aby bol pri hodnotení zraniteľností zachovaný CMM model, volím päť stupňovú hodnotiacu škálu. Jednotlivé stupne zodpovedajú stupňu zrelosti procesu modelu CMM a sú znázornené v Tab. 3.12.

[10] Capability Maturity Model definuje 5 úrovní zrelosti procesu. Bol vyvinutý v Software Engineering Institute na Carnegie Mellon University v Pittsburghu.

Stupeň	Skratka	Prijaté opatrenia	Od [%]	Do [%]
1	N	Sú zdokumentované, kontrolované a dochádza k ich priebežnému zlepšovaniu	0	20
2	S	Sú zdokumentované a kontrolované	20	40
3	SV	Sú zdokumentované, ale nie sú kontrolované	40	60
4	V	Sú zavedené, ale nie sú zdokumentované	60	80
5	K	Žiadne opatrenie nie je zavedené	80	100

Tab. 3.12: Hodnotiaca stupnica zraniteľností

Pri hodnotení zraniteľností konkrétnych aktív, na ktoré pôsobia konkrétne hrozby vychádzame z Tab. 3.13. V tejto tabuľke je vo štvrtom stĺpci pre každú dvojicu aktívum – hrozba vypísaný zoznam aktuálne zavedených opatrení. Na hodnotení jednotlivých opatrení sa podieľali Operations Manager, TTI Specialist, HR Specialist a tím manažéri CS oddelení. Po posúdení úrovne každého opatrenia (číslo v zátvorke) konkrétnej dvojice sme spoločne s TTI špecialistom podľa vlastného úsudku určili výslednú hodnotu jej zraniteľnosti. Tá je v uvedenej tabuľke zobrazená v piatom stĺpci.

#	Aktívum	Hr	Zavedené opatrenia	Zr.
1.	IS1 + IS2	ZN	1.1 (1), 1.2 (5), 2.1 (2), 2.2 (4), 2.3 (4), 2.4 (3), 2.5 (2), 2.6 (3), 3.1(3), 3.2 (3)	4
2.	IS3	ZN	1.1 (1), 1.2 (5), 2.1 (2), 2.2 (4), 2.3 (4), 2.4 (3), 2.5 (2), 2.6 (3), 3.1(3), 3.2 (3)	4
3.	IS4	ZN	1.1 (1), 1.2 (5), 2.1 (2), 2.2 (4), 2.3 (4), 2.4 (3), 2.5 (2), 2.6 (3), 3.1(3), 3.2 (3)	2
4.	IS5	ZN	1.1 (1), 1.2 (5), 2.1 (2), 2.2 (4), 2.3 (4), 2.4 (3), 2.5 (2), 2.6 (3), 3.1(3), 3.2 (3)	4
5.	IS6	ZN	1.1 (1), 1.2 (5), 2.1 (2), 2.2 (4), 2.3 (4), 2.4 (3), 2.5 (2), 2.6 (3), 3.1(3), 3.2 (3)	4
6.	Outlook, resp. domena @klient1.com	ZN	1.1 (1), 1.2 (5), 2.1 (2), 2.2 (4), 2.3 (4), 2.4 (3), 2.5 (2), 2.6 (3), 3.1(3), 3.2 (3)	4
7.	IS7	ZN	1.1 (1), 1.2 (5), 2.1 (2), 2.2 (4), 2.3 (4), 2.4 (3), 2.5 (2), 2.6 (3), 3.1(3), 3.2 (3)	4
8.	IS8	ZN	1.1 (1), 1.2 (5), 2.1 (2), 2.2 (4), 2.3 (4), 2.4 (3), 2.5 (2), 2.6 (3), 3.1(3), 3.2 (3)	4
9.	Identifikačné údaje platobnej karty	K	1.1 (1), 1.2 (5), 2.6 (3), 3.1(4), 3.2 (1)	5
10.	Jednolicenčný PK	K	1.1 (1), 1.2 (5), 2.3 (3), 2.4 (5), 2.6 (4), 3.1 (4)	5
11.	Multilicenčný PK	K	1.1 (1), 1.2 (5), 2.3 (3), 2.4 (5), 2.6 (4), 3.1 (4)	5
12.	Dôvera a spokojnosť zákazníka – CSAT	UŠ	1.1 (1), 1.2 (3), 3.2 (3)	3
13.	Dôvera a spokojnosť zákazníka – CSAT	CH	1.1 (1), 1.2.7 (2)	2
14.	Service Level	UŠ	1.1 (1), 1.2.7 (3)	3
15.	Service Level	CH	1.1 (1), 1.2.7 (2)	2
16.	SA/ Access ID/ Multilicencie a iné zmluvy	K	1.1 (1), 1.2 (5), 2.1 (5), 2.3 (3), 2.4 (5), 2.6 (4), 3.1 (4)	5
17.	Osobné/ firemné údaje o zákazníkovi	K	1.1 (1), 1.2 (5), 2.3 (3), 2.4 (5), 2.6 (4), 3.1 (4)	5
18.	Interné Know-how	ZI	1.1 (1), 1.2 (5), 2.4 (5), 3.1 (4)	5
19.	Informácie o chybách v produktoch a licenciách	ZI	1.1 (1), 1.2 (5), 3.1 (4)	5
20.	Know-how aktivácie	ZI	1.1 (1), 1.2 (5), 3.1 (4)	5
21.	Know-how získania bezplatného SRX	ZI	1.1 (1), 1.2 (5), 3.1 (4)	5

Tab. 3.13: Tabuľka aktívum+hrozba X opatrenia s úrovňou zraniteľnosti

4 VYHODNOTENIE RIZÍK

Vyhodnotenie rizík je druhou etapou procesu riadenia rizík a pozostáva z niekoľkých fáz. V prvej sa vyčíslujú jednotlivé riziká. Hodnota rizika sa stanoví na základe úrovne každého člena trojice aktívum – hrozba – zraniteľnosť (AHZ). Výstupom tejto fázy je výška rizika pre každú trojicu AHZ, na základe ktorej sa v ďalšej fáze vyberajú opatrenia. Úlohou vybratých opatrení je znížiť každé riziko na akceptovateľnú úroveň. V poslednej fáze procesu vyhodnotenia rizík sa vykonáva analýza vybraných opatrení, posudzuje sa ich vhodnosť, schopnosť efektívne znižovať riziká a ich hospodárnosť. Pre potreby tejto práce sú fázy výberu a posudzovania opatrení zlúčené do jednej. Každá z fáz je ďalej rozpracovaná v samostatnej podkapitole.

4.1 Kvantifikácia rizík

Úroveň rizika sa stanovuje pre každú trojicu aktívum – hrozba – zraniteľnosť. Podľa [18] je úroveň rizika definovaná takto: „*Riziko vyjadruje v číselnej hodnote mieru zneužitia určitej zraniteľnosti konkrétnou hrozbou, ktorého dôsledkom je dopad na uvažované aktíva.*“ Čím je hodnota aktíva, hrozby a zraniteľnosti vyššia, tým vyššia bude aj úroveň rizika. Matematicky môžeme riziko vyjadriť ako funkciu týchto troch vstupných premenných: $R = f(A, H, Z)$. Pre výpočet rizika potom použijeme vzorec:

$$R(A, H, Z) = a \times h \times z,$$

kde a je hodnota aktíva A, h je výška hrozby H pôsobiacej na aktívum a z je hodnota zraniteľnosti Z aktíva voči hrozbe H.

Keďže sme v analýze rizík pri hodnotení aktív uvažovali štyri typy dopadov – Businessflow, Costflow, Imidž klienta a Dôvera klienta – je nutné pre každý typ dopadu stanoviť riziko zvlášť. Výška miery rizík podľa jednotlivých typov dopadov je zobrazená v Tab. 4.2, Tab. 4.3, Tab. 4.4 a Tab. 4.5. Pri výpočte miery rizík sa riadim nasledovnými pravidlami:

- aby sa s hodnotami vstupných premenných dobre pracovalo a zároveň boli vypočítané riziká na prvý pohľad zrozumiteľné, vstupy prepočítam na hodnoty z nasledovných intervalov:
    - pre hrozby a zraniteľnosti <0, 1>,

- pre aktíva <0, 100>,
- miera rizika tak bude z intervalu <0, 100>[11],

- u každého vstupu (A, H, Z) sa počíta s hornou hraničnou hodnotou, viď Tab. 4.1,
- hodnoty aktív sú prepočítané takto:
  - $s \times \frac{100}{4}$,

  kde *s* je hodnota aktíva z tabuľky Tab. 3.4,

- hodnoty hrozieb sú prepočítané takto:
  - $s \times \frac{1}{4}$,

  kde *s* je hodnota hrozby z Tab. 3.11; u hrozieb sa navyše počíta s presnou nezaokrúhlenou celkovou hodnotou vypočítanou aritmetickým priemerom čiastkových hrozieb,

- hodnoty zraniteľností sú prepočítané takto:
  - $s \times \frac{1}{5}$,

  kde *s* je hodnota zraniteľnosti z tabuľky Tab. 3.13.

#	Aktívum	Hrozba	Zraniteľnosť
1	25	0, 25	0,2
2	50	0, 50	0,4
3	75	0,75	0,6
4	100	1	0,8
5			1

Tab. 4.1: Konverzná tabuľka stupňa A, H, Z na hodnotu z definovaných intervalov

[11] Z dôvodu toho, že pri výpočte rizika uvažujem horné hraničné hodnoty intervalov jednotlivých diskrétnych stupňov aktív, hrozieb a zraniteľností (viď Tab. 4.1), môže jeho miera fakticky nadobudnúť hodnoty z intervalu <1,25; 100>

Aktívum	**Hrozba**	**A_{BF}**	**H**	**Z**	**R_{BF}**
IS1 + IS2	ZN	50	0.67	0.8	27
IS3	ZN	50	0.67	0.8	27
IS4	ZN	50	0.83	0.4	17
IS5	ZN	25	0.42	0.8	8
IS6	ZN	25	0.75	0.8	15
Outlook, resp. domena @klient1.com	ZN	25	0.50	0.8	10
IS7	ZN	50	0.83	0.8	33
IS8	ZN	25	0.50	0.8	10
Identifikačné údaje platobnej karty	K	75	0.83	1	63
Jednolicenčný PK	K	25	0.67	1	17
Multilicenčný PK	K	50	0.67	1	33
Dôvera a spokojnosť zákazníka – CSAT	UŠ	50	0.50	0.6	15
Dôvera a spokojnosť zákazníka – CSAT	CH	50	0.25	0.4	5
Service Level	UŠ	25	0.58	0.6	9
Service Level	CH	25	0.25	0.4	3
SA/Access ID/Multilicencie a iné čísla zmlúv	K	50	0.75	1	38
Kontaktné a osobné/firemné údaje o zákazníkovi	K	50	0.58	1	29
Interné KNOW-HOW callcentra	ZI	50	0.58	1	29
Informácie o chybách v produktoch a ich licenciách	ZI	25	0.50	1	13
Know-how aktivácie	ZI	25	0.75	1	19
Know-how získania bezplatného SRX	ZI	25	0.83	1	21

Tab. 4.2: Výška miery rizika dopadu na Businessflow

Aktívum	**Hrozba**	**A_{CF}**	**H**	**Z**	**R_{CF}**
IS1 + IS2	ZN	75	0.67	0.8	40
IS3	ZN	75	0.67	0.8	40
IS4	ZN	75	0.83	0.4	25
IS5	ZN	25	0.42	0.8	8
IS6	ZN	50	0.75	0.8	30
Outlook, resp. doména @klient1.com	ZN	50	0.50	0.8	20
IS7	ZN	75	0.83	0.8	50
IS8	ZN	50	0.50	0.8	20
Identifikačné údaje platobnej karty	K	100	0.83	1	83
Jednolicenčný PK	K	50	0.67	1	33
Multilicenčný PK	K	75	0.67	1	50
Dôvera a spokojnosť zákazníka – CSAT	UŠ	75	0.50	0.6	23
Dôvera a spokojnosť zákazníka – CSAT	CH	75	0.25	0.4	8
Service Level	UŠ	50	0.58	0.6	18
Service Level	CH	50	0.25	0.4	5
SA/Access ID/Multilicencie a iné čísla zmlúv	K	75	0.75	1	56
Kontaktné a osobné/firemné údaje o zákazníkovi	K	75	0.58	1	44
Interné KNOW-HOW callcentra	ZI	75	0.58	1	44
Informácie o chybách v produktoch a ich licenciách	ZI	50	0.50	1	25
Know-how aktivácie	ZI	50	0.75	1	38
Know-how získania bezplatného SRX	ZI	25	0.83	1	21

Tab. 4.3: Výška miery rizika dopadu na Costflow

Aktívum	**Hrozba**	**A_{IK}**	**H**	**Z**	**R_{IK}**
IS1 + IS2	ZN	75	0.67	0.8	40
IS3	ZN	75	0.67	0.8	40
IS4	ZN	25	0.83	0.4	8
IS5	ZN	25	0.42	0.8	8
IS6	ZN	25	0.75	0.8	15
Outlook, resp. domena @klient1.com	ZN	75	0.50	0.8	30
IS7	ZN	50	0.83	0.8	33
IS8	ZN	25	0.50	0.8	10
Identifikačné údaje platobnej karty	K	100	0.83	1	83
Jednolicenčný PK	K	50	0.67	1	33
Multilicenčný PK	K	50	0.67	1	33
Dôvera a spokojnosť zákazníka – CSAT	UŠ	50	0.50	0.6	15
Dôvera a spokojnosť zákazníka – CSAT	CH	50	0.25	0.4	5
Service Level	UŠ	25	0.58	0.6	9
Service Level	CH	25	0.25	0.4	3
SA/Access ID/Multilicencie a iné čísla zmlúv	K	50	0.75	1	38
Kontaktné a osobné/firemné údaje o zákazníkovi	K	75	0.58	1	44
Interné KNOW-HOW callcentra	ZI	25	0.58	1	15
Informácie o chybách v produktoch a ich licenciách	ZI	25	0.50	1	13
Know-how aktivácie	ZI	25	0.75	1	19
Know-how získania bezplatného SRX	ZI	25	0.83	1	21

Tab. 4.4: Výška miery rizika dopadu na Imidž klienta

Aktívum	**Hrozba**	**A_{DK}**	**H**	**Z**	**R_{DK}**
IS1 + IS2	ZN	75	0.67	0.8	40
IS3	ZN	75	0.67	0.8	40
IS4	ZN	75	0.83	0.4	25
IS5	ZN	25	0.42	0.8	8
IS6	ZN	50	0.75	0.8	30
Outlook, resp. domena @klient1.com	ZN	50	0.50	0.8	20
IS7	ZN	75	0.83	0.8	50
IS8	ZN	50	0.50	0.8	20
Identifikačné údaje platobnej karty	K	100	0.83	1	83
Jednolicenčný PK	K	50	0.67	1	33
Multilicenčný PK	K	50	0.67	1	33
Dôvera a spokojnosť zákazníka – CSAT	UŠ	50	0.50	0.6	15
Dôvera a spokojnosť zákazníka – CSAT	CH	50	0.25	0.4	5
Service Level	UŠ	25	0.58	0.6	9
Service Level	CH	25	0.25	0.4	3
SA/Access ID/Multilicencie a iné čísla zmlúv	K	75	0.75	1	56
Kontaktné a osobné/firemné údaje o zákazníkovi	K	75	0.58	1	44
Interné KNOW-HOW callcentra	ZI	25	0.58	1	15
Informácie o chybách v produktoch a ich licenciách	ZI	50	0.50	1	25
Know-how aktivácie	ZI	50	0.75	1	38
Know-how získania bezplatného SRX	ZI	50	0.83	1	42

Tab. 4.5: Výška miery rizika dopadu na Dôvera klienta

Legenda k Tab. 4.2, Tab. 4.3, Tab. 4.4 a Tab. 4.5:

Aktívum – slovný popis aktíva

Hrozba – skratka hrozby (ZI – zneužitie informácií, ZN – zneužitie SW nástroja, K – krádež, US – úmyselné poškodenie, CH – chyba používateľa)

$\mathbf{A_{BF}}$, $\mathbf{A_{CF}}$, $\mathbf{A_{IK}}$, $\mathbf{A_{DK}}$ – hodnota aktíva z pohľadu dopadu na Businessflow, Costflow, Imidž klienta, Dôveru klienta

H – hodnota hrozby

Z – výška zraniteľnosti

$\mathbf{R_{BF}}$, $\mathbf{R_{CF}}$, $\mathbf{R_{IK}}$, $\mathbf{R_{DK}}$ – výška rizika dopadu na Businessflow, Costflow, Imidž klienta, Dôvera klienta

Každé riziko môžeme podľa jeho výšky označiť ako nízke, stredné, vysoké alebo kritické. V závislosti na tejto kategórii je nutné k riziku pristupovať a odpovedajúcim spôsobom ho zvládať. Kritickým rizikom by sme sa mali zaoberať bezodkladne – žiada si okamžitý zásah manažmentu. U rizík označených ako vysoké, prípadne stredné je možné ich zvládanie naplánovať. Kým riziko nízke môžeme akceptovať a ďalej ho iba monitorovať. Riziko sa obvykle zvláda prostredníctvom protiopatrení, prípadne podstúpením rizika tretej strane – v praxi sa to realizuje napríklad poistením proti riziku alebo prenosom vysoko rizikových procesov na dodávateľský subjekt [13]. V našom prípade nie je prenos rizika na tretiu stranu možný, preto je nutné stanoviť účinné a hospodárne protiopatrenia.

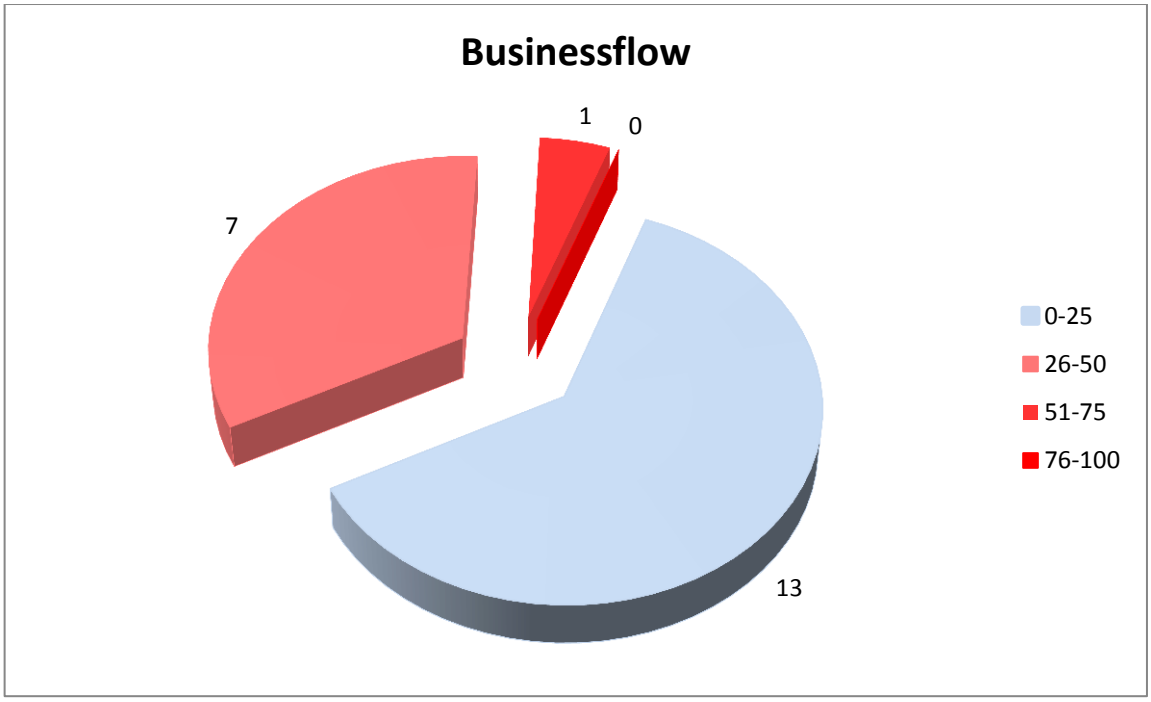
Aj keď sa zdajú výsledky hodnotenia rizík uvedené v Tab. 4.2, Tab. 4.3, Tab. 4.4 a Tab. 4.5 na prvý pohľad alarmujúce, je nutné podotknúť, že uvedené hodnoty rizík nepredstavujú reálnu pravdepodobnosť negatívneho dopadu na aktíva. Ich globálne vyššiu úroveň pripisujem predovšetkým faktu, že hodnoty hrozieb do určitej miery nezodpovedajú reálnemu stavu z dôvodov uvedených v 3.7.2.3. Navyše skutočnosť, že dôjde k uplatneniu nejakej hrozby voči aktívu, v našom prípade ešte neznamená, že dôjde aj k negatívnemu dopadu na aktívum samotné. Napríklad, ak operátor zákazníckej linky odcudzí produktový kľúč a zneužije ho na komerčné účely, hrozba „Krádež“ bude voči aktívu „Produktový kľúč“ uplatnená, no v prípade, že sa Klient1 túto skutočnosť nedozvie, nedôjde k žiadnemu zo štyroch sledovaných negatívnych dopadov. Keďže pravdepodobnosť odhalenia uskutočnenej hrozby nie je v rámci tejto práce možné presne

určiť, ba ani odhadnúť, nie je ako taká zahrnutá do analýzy rizík. Preto je nutné vypočítané hodnoty miery rizík vnímať skôr relatívne než absolútne a hľadieť na ne ako na priority, podľa ktorých budú zvládané.

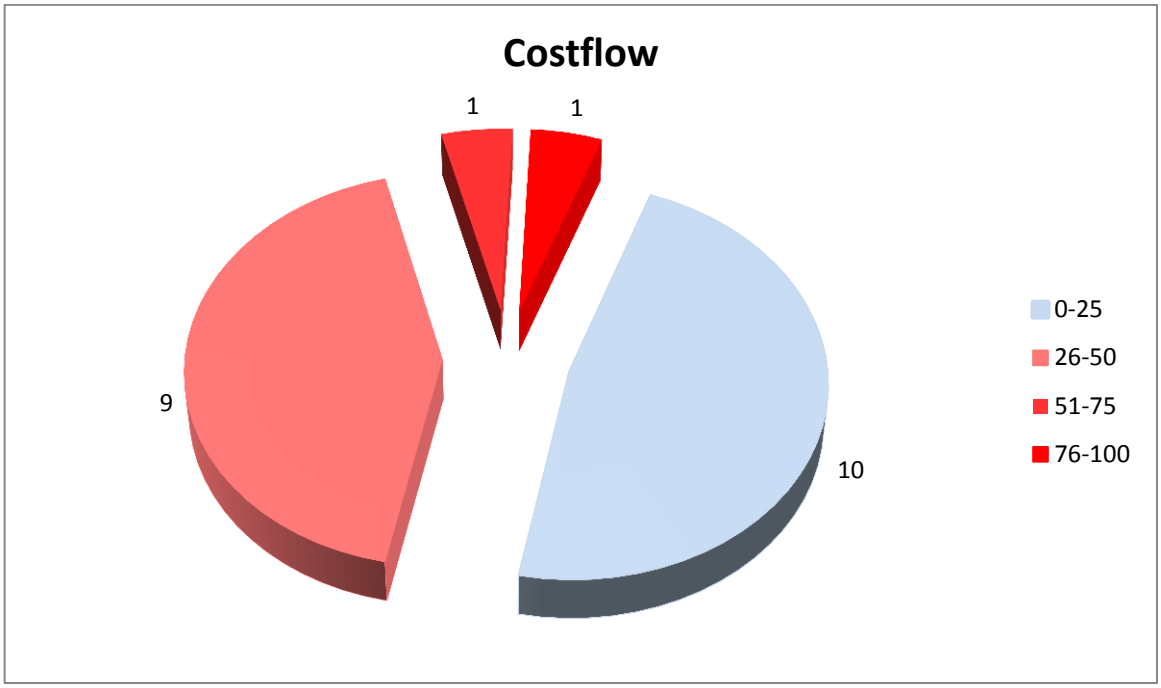
Na základe vyššie uvedeného a po konzultácii s vedením spoločnosti Zakaznickapodpora som pre naše účely zvolil delenie rizík uvedené v Tab. 4.6. Grafické znázornenie počtu rizík v jednotlivých kategóriách je na Obr. 4.1, Obr. 4.2, Obr. 4.3 a Obr. 4.4.

Stupeň	Skratka	Výška rizika	Slovné vyjadrenie rizika	Od – do
1	N	nízke	Riziko môžeme akceptovať a ďalej ho monitorovať	0 – 25
2	S	stredné	Riziko musí byť zvládané podľa plánu	26 – 50
3	V	vysoké	Riziko musí byť zvládané podľa plánu	51 – 75
4	K	kritické	Riziko musí byť naplánované a zvládané okamžite	76 – 100

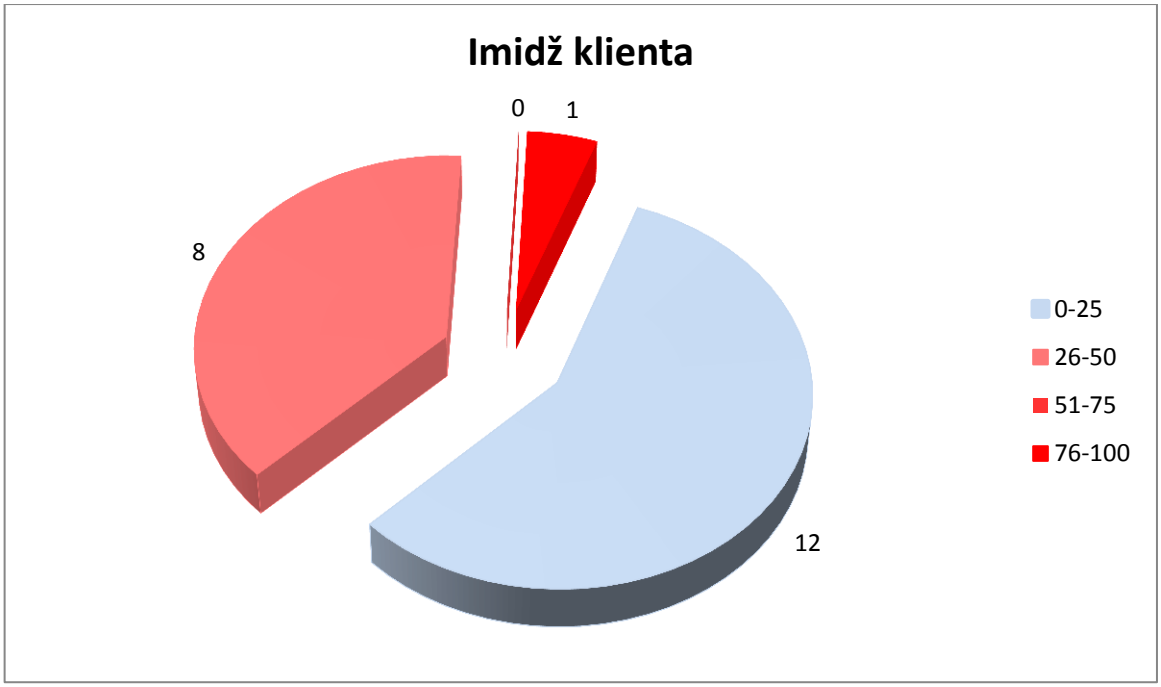
Tab. 4.6: Klasifikácia rizík



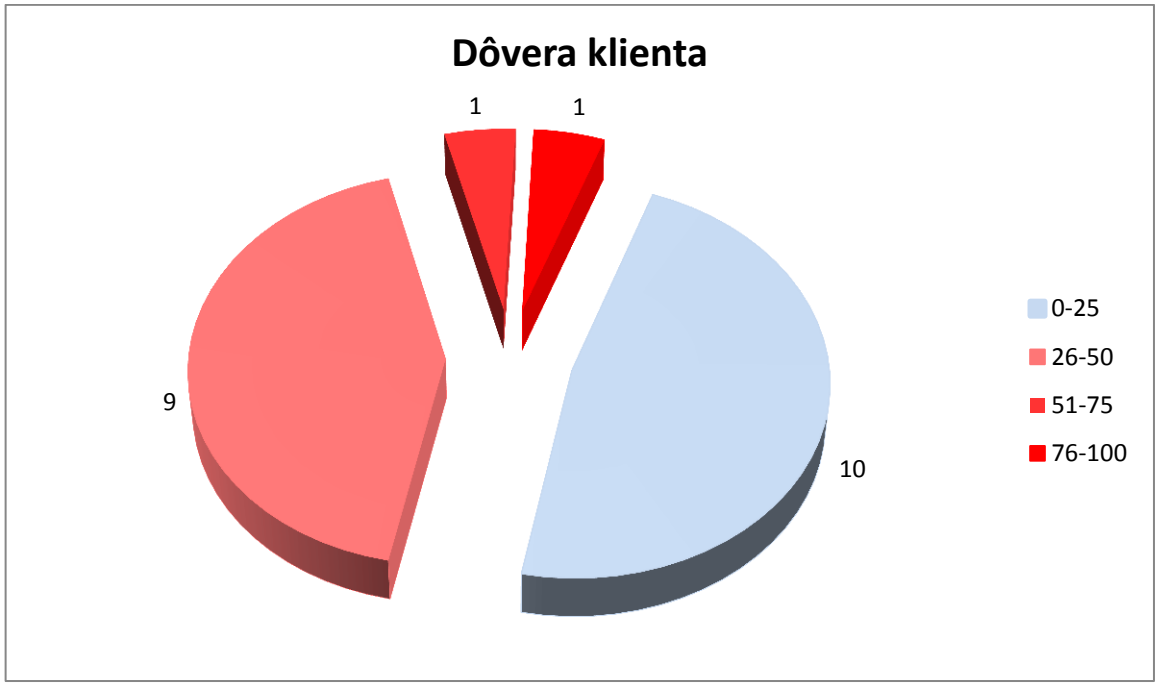
Obr. 4.1: Množstvo rizík pôsobiacich na Businessflow a ich rozdelenie



Obr. 4.2: Množstvo rizík pôsobiacich na Costflow a ich rozdelenie



Obr. 4.3: Množstvo rizík pôsobiacich na Imidž klienta a ich rozdelenie



Obr. 4.4 Množstvo rizík pôsobiacich na Dôveru klienta a ich rozdelenie

4.2 Identifikácia opatrení

Po ohodnotení miery rizík je potrebné definovať účinné protiopatrenia, ktoré existujúce riziká znížia. Pri identifikácii opatrení je nevyhnutné uvažovať ich efektivitu, hospodárnosť ale aj použiteľnosť na chránený systém. Naskytuje sa totiž hneď niekoľko účinných a zároveň hospodárnych opatrení, ktoré značným spôsobom zasahujú do slobody a pohodlia zamestnancov, čo môže viesť k ich nespokojnosti, prípadne ukončeniu pracovného pomeru. Všetky opatrenia je preto nutné vyberať s prihliadnutím na ich pozitívne ale aj negatívne stránky.

Po konzultácii s manažmentom sme vybrali sadu opatrení, ktoré je možné rozdeliť do hlavných kategórií totožných s 3.8.1. Uvažované boli iba opatrenia účinné a hospodárne. Keďže z povahy aktív a hrozieb nebolo možné definovať konkrétne opatrenie pre každé riziko zvlášť, väčšina z opatrení pôsobí na viacero rizík súčasne. Miery rizika je zohľadnená ako v opatreniach samotných, tak aj v časovom horizonte ich realizácie.

4.2.1 Personálne opatrenia

1.1 Referencie – referencie uvádzané v životopise by mali byť overené a zdokumentované u každého prijatého uchádzača o zamestnanie.

1.2 Zodpovednosť **(kratkodobe)** – používatelia by mali byť upovedomení o svojich právach a povinnostiach v súvislosti s používaním informačných systémov, bezpečnosti používateľského vybavenia a nakladania s dôvernými údajmi, ako aj know-how procesov spoločnosti Zakaznickapodpora a jej klienta Klient1. Mali by byť jasne definované všetky typy dôverných údajov, ktoré bude operátor spracovávať a ktoré máme v úmysle chrániť – viď identifikácia aktív. Operátori by si taktiež mali byť vedomí možných postihov v prípade porušenia týchto nariadení.

Súčasťou tohto opatrenia by mal byť dodatok k pracovnej zmluve o zachovaní dôvernosti. Tento dodatok bude okrem povinnosti o zachovaní dôvernosti tiež zakazovať používanie akýchkoľvek e-mailových adries pridelených zamestnávateľom na vybavovanie inej, než firemnej korešpondencie a korešpondencie súvisiacej s vybavením zákazníckych požiadaviek. Dôvodom tohto zákazu je možnosť jednoduchšej kontroly a monitorovania e-mailovej komunikácie zo strany zamestnávateľa – toto opatrenie je podrobnejšie popísané v rámci logických opatrení.

4.2.2 Logické opatrenia

2.1 Riadenie prístupu k sieti, sieťovým prvkom a výstupným zariadeniam – do siete by nemalo byť možné pripojiť neautorizované zariadenia. Taktiež by malo byť operátorom odoprené použitie akýchkoľvek zapisovacích médií a HW prostriedkov, ako sú CD/DVD nosiče, USB kľúče a pamäťové karty. Použitie CD/DVD nosičov je povolené pre jednosmerný tok údajov a to smerom do PC. Toto sa dá docieliť vhodnou konfiguráciou skupinovej politiky aplikovanej na doménové účty skupiny operátorov.

Na používateľských staniciach operátorov by mali byť povolené iba tie **sieťové protokoly**, ktoré sú potrebné pre správne fungovanie autorizovaných SW nástrojov a IS. Všetky ostatné protokoly, predovšetkým komunikačné – využiteľné napr. v MS Outlook (SMTP, POP3, IMAP) by mali byť zablokované.

Prístup do **siete Internet** by mal byť filtrovaný. Predovšetkým by mali byť obmedzené stránky poskytujúce online služby typu Instant Messaging, e-mailové služby a iné online služby umožňujúce komunikáciu s okolím a zhromažďovanie, prípadne ukladanie údajov. Zároveň by však nemalo dôjsť k obmedzeniu prístupu a plnej funkčnosti webových stránok, ktoré operátor potrebuje pre každodenné vybavovanie telefonických a e-mailových požiadaviek zákazníkov. Konkrétne sa jedná o nalsedujúce webové stránky:

- oficiálna stránka technickej podpory a pomoci Klient1,
- stránka diskusných skupín Klient1,
- oficiálne stránky priamych partnerov spoločnosti Klient1,
- oficiálne stránky venované jednotlivým hlavným SW produktom, prevádzkovanými spoločnosťou Klient1 a jej oficiálnymi partnermi,
- stránky pod doménou zakaznickapodpora.com/ .cz.

Systém kontroly a filtrovania webového obsahu by mal byť flexibilný, aby ho bolo možné jednoducho a rýchlo meniť.

Na používateľských staniciach by mali byť blokované všetky neautorizované **SW programy a nástroje** vrátane ich tzv. „portable“ verzií, ktoré nie je nutné inštalovať.

Podrobný zoznam blokovaných sieťových protokolov a filtrovacích pravidiel vypracuje a zdokumentuje TTI manažér v spolupráci s IT oddelením materskej organizácie spoločnosti Zakaznickapodpora.

4.2.3 Administratívne opatrenia

3.1 Školenie a priebežná informovanosť (dlhodobe) – malo by byť zabezpečené úvodné školenie v oblasti informačnej bezpečnosti, ktoré okrem bodov uvedených v opatrení Zodpovednosť (viď Personálne opatrenia) pokrýva aj nasledujúce témy:

- zoznámenie sa s bezpečnostnou politikou spoločnosti,
- typy údajov, s ktorými príde pracovník do styku a aké informačné systémy sa na spracovanie údajov používajú.

Všetkým používateľom by malo byť tiež oznámené, aby:

- udržovali heslá v dôvernosti,
- vyvarovali sa držania záznamu hesiel na papieri, ak takýto záznam nemôže byť bezpečne uložený,
- zmenili heslá vždy, keď existuje akákoľvek indícia ohrozenia systému alebo hesla,
- po ukončení práce, prípadne dočasnom opustení pracovného miesta uzamkli pracovnú stanicu.

Ďalej by mala byť zabezpečená kontinuálna informovanosť pracovníkov o význame a potrebe informačnej bezpečnosti s dôrazom na benefity, ktoré

jednotlivcom ako aj celej spoločnosti prináša. K zvýšeniu povedomia v tejto oblasti môže byť využitý firemný bulletin.

3.2 *Zásada čistého stola a čistej obrazovky (strednedobo)* by mala zabezpečiť, aby operátori riadne ukončovali otvorené relácie IS po vybavení požiadavky zákazníka a tiež uzamykanie pracovnej stanice po prerušní, prípadne ukončení práce. Cieľom tohto nariadenia je obmedziť riziká neautorizovaného prístupu, straty a poškodenia informácií počas alebo mimo normálneho pracovného času. Toto opatrene by ďalej malo v maximálnej miere zamedziť možnosti zachytenia chránených údajov z obrazovky pomocou záznamových zariadení, ako sú fotoaparáty, mobilné telefóny a pod. Vedenie spoločnosti Zakaznickapodpora by preto malo zvážiť zákaz používania takýchto prostriedkov v priestoroch „openspace“. Operátori by si zakázané zariadenia mohli ukladať v uzamykateľných skrinkách, ktoré sú umiestnené v chodbičke pred vstupom do „openspace“. Som si vedomý, že každé takéto nariadenie alebo zákaz, ktorý zasahuje do komfortu a voľnosti pracovníkov, môže byť z ich strany vnímaný veľmi negatívne. To sa týka hlavne operátorov, ktorí v spoločnosti pracujú už dhlšie a majú tým pre ňu vyššiu hodnotu. Aj preto musí manažment spoločnosti prijatie podobných opatrení citlivo posúdiť a prípadne vyvážiť inými zamestnaneckými výhodami.

3.3 *Riadenie elektronickej a telefonickej komunikácie* – akákoľvek elektronická komunikácia medzi zákazníkom a operátorom môže prebiehať iba prostredníctvom informačného systému určeného na vybavovanie zákazníckych požiadaviek – CAP. V odvôvodnených prípadoch môže zodpovedný tím manažér udeliť výnimku. Na internú komunikáciu, ako aj komunikáciu so zástupcami Klient1 môže operátor použiť informačný systém IS1, pridelenú e-mailovú adresu, prípadne SW nástroj Office Communicator. Všetky formy elektronickej komunikácie budú archivované po dobu minimálne jedného roku, aby boli k dispozícii pri šetrení bezpečnostného incidentu alebo pre prípad náhodnej kontroly.

Na prenos objemných dát je možné použiť na to určenú online aplikáciu prevádzkovanú Klient1 dostupnú prostredníctvom VPN.

Telefonická komunikácia by mala byť uskutočňovaná výhradne prostredníctvom telefónneho prístroja na to určeného a zároveň každá telefónna stanica by mala byť zabezpečená proti neautorizovanému použitiu.

3.4 Auditovanie práce na PC a s IS (okamzite) – práca operátorov na PC by mala byť zaznamenávaná, tzv. screening, vhodným SW nástrojom. Zaznamenávanie by sa malo aktivovať v týchto prípadoch:

- pri započatí každého telefonického hovoru a trvať minimálne do doby ukončenia hovoru,
- pri každom prihlásení operátora do IS7 a trvať až po jeho odhlásenie.

Všetky záznamy by mali byť uchovávané po dobu jedného roka pre prípad šetrenia bezpečnostného incidentu. Na tento účel je vhodné použiť SW nástroj NICE, ktorý spoločnosť už využíva na monitorovanie telefonických hovorov a teda nie je nutný nákup nových licencií.

3.5 Monitoring práce na PC a s IS – Súčasne s monitorovaním telefonických hovorov by mala byť kontrolovaná aj práca na PC – video záznam obrazovky zosnímaný v čase tel. hovoru. Okrem náhodného výberu telefonátov by sa mali kouči vo väčšej miere zamerať na hovory týkajúce sa zmlúv s korporátnou klientelou a prístupov do IS7. Navyše by však mal byť preskúmaný každý rozhovor, v ktorom zákazník poskytol indentifikačné údaje platobnej karty.

3.6 Riadenie a správa bezpečnostných incidentov (stredne/dlhodobo) – za bezpečnostný incident môžeme považovať každé úmyselné ale aj neúmyselné zneužitie informačných systémov – a údajov nimi spracovávaných – pracovníkom spoločnosti, a zároveň aj jeho postavenie, ktoré by viedlo k negatívnemu dopadu na hodnotu sledovaných aktív.

Všetci pracovníci, počnúc operátormi, cez koučov a trénerov až po tímových manažérov, by si mali byť vedomí nutnosti všímať si a čo najrýchlejšie hlásiť bezpečnostné incidenty. Špeciálnu rolu v tomto prípade zohrávajú práve kouči, ktorí každodenne monitorujú telefonické hovory operátorov. Práve oni by mali byť vedením spoločnosti motivovaní, aby k monitoringu pristupovali zodpovedne a aby sa zamerali na najviac rizikové procesy a činnosti operátora.

Manažment spoločnosti by preto mal zaistiť komplexný program odhaľovania, hlásenia a správy bezpečnostných incidentov, ktorý podporuje ochranu proti incidentom, ich detekciu a hlásenie a primerané reakcie na ne. Na príprave tohto programu by sa mali podieľať TTI Manager v spolupráci s Operations Manager a oddelením Quality.

5 ZVLÁDANIE RIZÍK

Zvládanie rizík je poslednou etapou procesu riadenia rizík. Nemali by sme ju však považovať za etapu konečnú, keďže proces riadenia rizík by mal byť procesom kontinuálnym a pravidelne sa v čase opakovať. V tejto etape sa budú navrhnuté protiopatrenia vhodne plánovať a realizovať. Ďalej je tiež nevyhnutné, aby realizáciu a dodržiavanie opatrení niekto kontroloval. V maximálnej miere sa tak predíde situáciám, kde by boli dodržiavanie, prípadne realizácie opatrení vykonávané inak, než bolo pôvodne zamýšľané. Plán realizácie protiopatrení je spracovaný v nasledujúcej podkapitole. Záverečnou fázou každého cyklu riadenia rizík by malo byť vyhodnotenie prijatých opatrení, to však už nie je súčasťou tejto diplomovej práce a preto nebude bližšie popísaná.

5.1 Plán zavádzania opatrení

Pri plánovaní realizácie jednotlivých protiopatrení budeme prihliadať jednak na dostupnosť ľudských zdrojov, ale aj na výšku miery rizík, ktorá má byť opatreniami znížená na akceptovateľnú hodnotu. V nasledujúcom texte je každé protiopatrenie naplánované:

- definovaním RACI[12] matice (viď Tab. 5.1), ktorá popisuje kto dané opatrenie zrealizuje, kto je za neho zodpovedný, s kým sa bude opatrenie konzultovať a kto bude o ňom informovaný,

	R	A	C	I
Rola 1	X	X		
Rola 2			X	
Rola 3				X
Rola 4	X		X	

Tab. 5.1: Príklad RACI matice

- tabuľkou zobrazujúcou konkrétne úlohy, kto je za ne zodpovedný – kto ich má zrealizovať, a tiež prioritu, s akou sa majú vykonať, prípadne periodicitu kontroly. Priority sú rozdelé do troch úrovní a predstavujú časový úsek, v ktorom majú byť jednotlivé opatrenia a ich dielčie úlohy zrealizované – viď Tab. 5.2.

[12] Model používaný pre definovanie rolí a zodpovedností. RACI je skratka anglického Responsible (realizuje), Accountable (zodpovedá), Consult (konzultovaný), Informed (informovaný) [19]

Priorita	Časový úsek	Slovný popis
1	týždeň	okamžite
2	mesiac	strednedobo
3	3 mesiace	dlhodobo

Tab. 5.2: Úroveň priorít a im odpovedajúci časový úsek

5.1.1 Personálne opatrenia

5.1.1.1 *Referencie*

	R	A	C	I
SDM				X
Operations Manager				X
HR	X	X		
Team Managers			X	

Tab. 5.3: RACI opatrenia 1.1

Časový horizont prijatia opatrenia

Opatrenie by malo byť prijaté okamžite a aplikované pri výbere nových pracovníkov. Na súčasných zamestnancov sa toto opatrenie nevzťahuje.

Úloha/ výstup	Zdroje	Priorita/ Periodicita
Realizácia opatrenia	HR	okamžite
Kontrola opatrenia	SDM	ročne

Tab. 5.4: Plán zavedenia opatrenia 1.1

5.1.1.2 *Zodpovednosť*

	R	A	C	I
SDM		X		
HQ	X			
HR	X			
Operations Manager				X
Team Managers				X
Coaches and Trainers			X	
TTI	X			
Agents				X

Tab. 5.5: RACI opatrenia 1.2

Časový horizont prijatia opatrenia

Opatrenie by malo byť prijaté v horizonte jedného týždňa, kedy by mala byť vypracovaná smernica vymedzujúca práva a povinnosti súvisiace s používaním informačných systémov, kde budú tiež jasne definované všetky typy dôverných údajov. Ďalej bude vypracovaný dodatok k pracovnej zmluve. So smernicou a dodatkom sa zoznámia a svojím podpisom potvrdia novo prijímaní opeátori CS, ako aj všetci stávajúci.

Úloha/ výstup	**Zdroje**	**Priorita/ Periodicita**
Vypracovanie smernice práv a povinností v súvislosti s používaním IS a styku s chránenými údajmi	TTI, HR	okamžite
Vypracovanie dodatku o dôvernosti	Právnik	okamžite
Podpis dodatku	HR, operátori	okamžite
Kontrola opatrenia	SDM	jednorázovo

Tab. 5.6: Plán zavedenia opatrenia 1.2

5.1.2 Logické opatrenia

5.1.2.1 *Riadenie prístupu k sieti, sieťovým prvkom a výstupným zariadeniam*

	R	A	C	I
SDM				X
Operations Manager				X
Team Managers				X
Coaches and Trainers	X			
TTI	X	X		
IT Department			X	

Tab. 5.7: RACI opatrenia 2.1

Úloha/ výstup	**Zdroje**	**Priorita/ Periodicita**
Blokovanie ext. HW zariadení a zapisovateľných médií	TTI	okamžite
Analýza IS a podporných SW nástrojov, požadovaných protokolov/ portov a webových stránok potrebných pre vykonávanie pracovných procesov	TTI, tréneri	strednedobo
Blokovanie neautorizovaného SW, nepovolených protokolov a portov	TTI, IT oddelenie	strednedobo
Filtrovanie webových stránok	TTI, IT oddelenie	strednedobo
Kontrola opatrenia	SDM, tréneri	ročne

Tab. 5.8: Plán zavedenia opatrenia 2.1

5.1.3 Administratívne opatrenia

5.1.3.1 *Školenie a priebežná informovanosť*

	R	A	C	I
Trainers	X			
TTI			X	
Q&R Manager		X		
Team Managers	X			
Agents				X

Tab. 5.9: RACI opatrenia 3.1

Úloha/ výstup	**Zdroje**	**Priorita/ Periodicita**
Príprava a realizácia školenia	Tréneri, TTI	strednedobo
Kontinuálne vzdelávanie v oblasti inf. bezpečnosti	TTI	dlhodobo
Kontrola opatrenia	Q&R Manager	6 mesiacov

Tab. 5.10: Plán zavedenia opatrenia 3.1

5.1.3.2 *Zásada čistého stola a čistej obrazovky*

	R	A	C	I
SDM		X	X	
HR	X			
TTI	X			
Operations Manager				X
Coaches	X			
Team Managers	X			
Agents				X

Tab. 5.11: RACI opatrenia 3.2

Úloha/ výstup	Zdroje	Priorita/ Periodicita
Smernica vymezujúca zakázané zariadenia	TTI, HR	strednedobo
Príprava podkladov pre školenie (viď 5.1.1.4)	TTI	strednedobo
Kontrola opatrenia	Tím manažéri, kouči	priebežne

Tab. 5.12: Plán zavedenia opatrenia 3.2

5.1.3.3 *Riadenie elektronickej a telefonickej komunikácie*

	R	A	C	I
Operations Manager		X		
Team Managers	X			
Coaches	X			
TTI	X			
Agents				X

Tab. 5.13: RACI opatrenia 3.3

Úloha/ výstup	Zdroje	Priorita/ Periodicita
Archivovanie elektronickej komunikácie	TTI	okamžite
Vypracovanie smernice a komunikácia pravidiel operátorom	Tím manažéri	okamžite
Kontrola opatrenia	Kouči	priebežne

Tab. 5.14: Plán zavedenia opatrenia 3.3

5.1.3.4 *Auditovanie práce na PC a s IS*

	R	A	C	I
Operations Manager				X
Team Managers				X
Coaches			X	
TTI	X	X		
IT Department			X	

Tab. 5.15: RACI opatrenia 3.4

Úloha/ výstup	Zdroje	Priorita/ Periodicita
Nastavenie a archivácia video záznamov obrazoviek operátorov	TTI	okamžite
Kontrola opatrenia	Operations manažér	ročne

Tab. 5.16: Plán zavedenia opatrenia 3.4

5.1.3.5 *Monitoring práce na PC a s IS*

	R	A	C	I
Operations Manager				X
Team Managers				X
Coaches	X			
Q&R Manager		X		
Agents				X

Tab. 5.17: RACI opatrenia 3.5

Úloha/ výstup	Zdroje	Priorita/ Periodicita
Monitoring video záznamov a telefonických hovorov	Kouči	okamžite
Kontrola opatrenia	Q&R manažér	mesačne

Tab. 5.18: Plán zavedenia opatrenia 3.5

5.1.3.6 *Riadenie a správa bezpečnostných incidentov*

	R	A	C	I
SDM				X
Operations Manager			X	
Team Managers				X
Coaches and Trainers			X	
TTI	X	X		
Q&R Manager			X	

Tab. 5.19: RACI opatrenia 3.6

Úloha/ výstup	**Zdroje**	**Priorita**
Systém riadenia a správy bezpečnostných incidentov	TTI, Operations manažér, Q&R manažér	dlhodobo
Kontrola opatrenia	SDM	

Tab. 5.20: Plán zavedenia opatrenia 3.6

ZÁVER

V tejto diplomovej práci som sa venoval popisu konkrétnej outsourcingovej spoločnosti (callcentra) zabezpečujúcej dodávku služieb telefonickej a e-mailovej zákazníckej podpory pre klientov medzinárodnej softvérovej spoločnosti. Cieľom práce bolo navrhnúť a iniciovať opatrenia, ktoré by v čo najväčšej miere zamedzili možnosti zneužívania zákazníckych údajov, SW nástrojov a znalostí vyplývajúcich z pozície operátora callcentra. Na dosiahnutie tohto cieľa som zvolil aplikovanie procesu riadenia informačných rizík. Tento proces som rozdelil do troch fáz. V prvej prebehla analýza rizík, druhou fázou bolo vyhodnotenie rizík a v tretej som sa pokúsil navrhnúť spôsoby a opatrenia na ich zvládanie.

V rámci analýzy rizík, u ktorej som volil kvalitatívny prístup, sme spoločne so zástupcami callcentra identifikovali a kvantifikovali jej tri základné veličiny, ktorými sú aktíva (SW nástroje, znalosti a údaje), hrozby (negatívne pôsobiace na aktíva) a zraniteľnosti (aktív voči hrozbám). Keďže sa na identifikácii a hodnotení týchto veličín podieľalo nezávisle viacero osôb, bolo potrebné zvoliť jednoduchú a jednoznačnú hodnotiacu stupnicu. Z tohto dôvodu som volil štyri, respektíve päť stupňovú diskrétnu škálu, ktorej súčasťou je aj slovný popis jednotlivých stupňov. Domnievam sa, že hodnotenia aktív, hrozieb a zraniteľností boli jednotné a nevznikli žiadne výrazné odchýlky, ktoré by mohli byť spôsobené rôznou interpretáciou hodnotiacej stupnice. Odchýlka od reálneho stavu však mohla nastať pri kvantifikácii hrozieb u konkrétnych dvojíc „aktívum – hrozba“ z dôvodu ich nedostatočného posúdenia. Každá z dvojíc bola hodnotená z pohľadu troch sledovaných faktorov – atraktivita aktíva, znalosti a schopnosti (k uskutočneniu hrozby), čas a námaha. Výsledná úroveň každej dvojice bola vyrátaná ako aritmetický priemer čiastkových hodnôt. Domnievam sa, že pridelením odpovedajúcich váh jednotlivým faktorom, prípadne posúdením ďalších činiteľov, ako je napr. zodpovednosť, alebo „poctivosť útočníka“ (operátora), by vypočítaná úroveň hrozieb presnejšie odrážala reálny stav. Súčasne predpokladám, že by to viedlo k jej celkovému zníženiu. Na realizáciu tejto myšlienky však nebol v predkladanej práci priestor.

Vo fáze vyhodnotenia rizík som vypočítal úrovne rizika pre každú trojicu aktívum – hrozba – zraniteľnosť ako súčin týchto troch veličín. Vstupné veličiny som vhodne prepočítal tak, aby výsledné hodnoty rizík spadali do intervalu 0 – 100 a boli teda na prvý pohľad zrozumiteľné. Celkovo vysokú mieru jednotlivých rizík pripisujem už zmieňovanej odchýlke pri posudzovaní hrozieb. Samotné riziká preto neboli prezentované

ako pravdepodobnosti poškodenia alebo zničenia aktív. Mali by však byť vnímané skôr ako vyjadrenie priorít, podľa ktorých je potrebné riziká zvládať. Následným krokom bola identifikácia opatrení. V tomto kroku som navrhol jednak úpravy existujúcich kontrolných procesov a mechanizmov, ale aj nové opatrenia, ktoré by mali viesť k účinnejšej ochrane aktív. Pri ich identifikácii som okrem výšky jednotlivých rizík zohľadnil tiež náklady spojené s ich realizáciou, ale aj možnú negatívnu odozvu na ich prijatie zo strany operátorov.

V rámci poslednej fázy procesu riadenia rizík som vypracoval plán, podľa ktorého by mali byť identifikované opatrenia realizované. Hlavným posudzovaným kritériom boli hodnoty zvládaných rizík, ktoré určovali prioritu a časový horizont aplikovania jednotlivých opatrení. Poslednou etapou tejto fázy je ich samotná realizácia. Táto však nie je súčasťou predkladanej práce a ostáva na zodpovednosti manažmentu analyzovaného callcentra.

Výstupom tejto diplomovej práce je množina konkrétnych opatrení s ich popisom a odporúčaným plánom zavádzania. Sú uvedené v kapitolách 4.2. a 5.1 Až čas a rozhodnutia manažmentu callcentra však ukážu, či predkladaná práca bola úspešná. Domnievam sa, že mieru úspechu nemožno hodnotiť iba z pohľadu celkového zníženia analyzovaných rizík, ale aj z pohľadu operátorov a miery ich, či už pozitívneho alebo negatívneho vnímania realizovaných opatrení.

Okrem návrhu preventívnych a ochranných opatrení by som si za prínos tejto práce dovolil označiť aj možnosť jej využitia ako príručky pri aplikovaní procesu analýzy, vyhodnotenia a zvládania informačných rizík v prostredí zákazníckych callcentier.

ZÁVĚR V ANGLIČTINĚ

In this thesis, I described a particular outsourcing company (call center) which ensures the supply of telephone services and e-mail customer support for clients of an international software company. The goal was to design and initiate measures which would be able to prevent an abuse of customer data, software tools and knowledge resulting from the position of call center operator. To achieve this objective, I chose to apply the process of information security risk management. I divided this process into three phases. In the first phase, the risk analysis was realized, the second phase contained the risk assessment and in the third phase I tried to suggest ways and measures for their management.

In the risk analysis, where a qualitative approach was chosen, some representatives of the call center and I identified and quantified, three basic variables called assets (software tools, knowledge and data), threats (negatively influencing assets) and vulnerability (of the assets against threats). Due to the fact the identification and the assessment of these variables were contributed by more people independently, it was necessary to choose a simple and unambiguous assessment scale. For this reason, I chose four- or five-level discrete scale, which also includes a verbal description of particular grades. I believe the assessment of assets, threats and vulnerabilities was unified, and no significant deviations, which could be caused by different interpretation of the assessment scale, occured. Deviation from the real situation could arise, however, within the quantification of specific threats' couples "asset – threat" because of the lack of their assessment. Each pair was assessed from the perspective of three monitored factors – attraction of assets, knowledge and skills (required for the realization of threats), time and effort. The resultant value of each pair was calculated as the arithmetic mean of partial values. I believe that by assigning of corresponding weights to each factor, or by considering and assessing other factors, such as responsibility, or "righteousness of the attacker" (call center agent), the calculated level of threat would better reflect the reality. At the same time I suppose that it would lead to its overall decrese. However, there was no space to implement this idea in this thesis.

In the phase of risk assessment I calculated risk level for each trio: the asset - the threat - the vulnerability as a product of these three variables. I recalculated input variables appropriately so that the resulting risk values were within the range 0 to 100 and therefore understandable at first sight. I assign the overall high degree of particular risks to the

difference in assessing of the alleged threats. The real risks were therefore not presented as the likelihood of damage or destruction of assets. However, they should be seen rather as an expression of priorities by which it is necessary to manage risks. The next step was to identify measures. In this step, I proposed not only modifying of existing control processes and mechanisms, but also new measures, which should lead to more effective protection of assets. When I identified them, I regarded the amount of particular risks and the costs associated with their implementation, but also their possible negative acceptance by operators.

In the last phase of the risk management process, I developed a plan according to which should the identified measures be implemented. The main criteria under consideration were the values of managed risk, which determined the priority and timing of application of specific measures. The last stage of this phase is their mere realization. This is however not part of this paper and it remains in the responsibility of the call center management.

The outcome of this thesis is a set of concrete measures with their descriptions and recommended implementation plan. They are listed in chapter 4.2. and 5.1. Only the time and call center management decisions will show whether the presented work was successful. I believe that the succession rate cannot be evaluated only in terms of overall reduction of analyzed risks, but also from the perspective of operators and their positive or negative perceptions of the realized measures.

As a contribution of this thesis, besides the proposal of preventive and protective measures, I would like to indicate the possibility to use it as a manual for applying the process of information risk analysis, assessment and cope in the environment of customer call centers.

SEZNAM POUŽITÉ LITERATURY

[1] BENIGER, James R. The Control Revolution: Technological and Economic Origins of the Information Society. Cambridge, Mass.: Harvard University Press, 1986.

[2] DOSEDĚL, T. Počítačová bezpečnost a ochrana dat. 1. vyd. Brno : Computer Press, 2004. 190 s. ISBN 80-251-0106-1.

[3] ADAMEC, P., et al. Príručka pre manažéra VII. - Riadenie a audit v informačnej bezpečnosti. 1. vyd. [s.l.] : TATE International Slovakia, s.r.o., 2007. 322 s.

[4] POŽÁR, Jozef. Informační bezpečnost. Plzeň : Vydavatelství a nakladatelství Aleš Čeněk, 2005. 309 s. ISBN 80-86898-38-5.

[5] JAŠEK, R. Informační a datová bezpečnost. Zlín : Univerzita Tomáše Bati ve Zlíně. 2006. 140s. ISBN 80-7318-456-7.

[6] VYSKOČ, Jozef. Bezpečnosť informačných systémov [online]. Bratislava : 1999 [cit. 2010-02-14]. Dostupný z WWW: <http://www.valdner.com/school_public/FM%20UK%20BA/4roc%20-%20Ochrana%20informacii/skripta.rtf>.

[7] LOVEČEK, T. Bezpečnostné systémy : bezpečnosť informačných systémov. 1. vyd. Žilina : Žilinská univerzita, 2007. 246 s. Vysokoškolské učebnice. ISBN 978-80-8070-767-5.

[8] TAS, JEROEN, SUNDER, SHYAM. Financial Services Business Process Outsourcing. 2004. COMMUNICATIONS OF THE ACM Vol. 47, No. 5.

[9] WEERAKKODY, VISHANTH, CURRIE, WENDY, EKANAYAKE, YAMAYA. Re-engineering business processes through application service providers - challenges, issues and complexities. Business Process Management Journal. 2003, Vol. 9 No. 6: 776-794.

[10] Fisher, L.M. Strategy+Business. In From vertical to Virtual : How Nortel's Supplier Alliances Extend the enterprise [online]. 2001 [cit. 2010-02-05]. Dostupné z WWW: <http://www.strategy-business.com/press/16635507/11153>.

[11] VAUGHAN, Michel; GUY, Fitzgerald. The IT outsourcing market place: vendors and their selection. Journal of Information Technology. 1997, 12, s. 223-237.

[12] JAŠEK, R. Ochrana znalostí a dat v podnikových informacních systémech. Zlín : Univerzita Tomáše Bati ve Zlíne, 2002. 115 s. ISBN 80-7318-095-2.

[13] SMEJKAL, Vladimír; RAIS, Karel. Řízení rizik ve firmách a jiných organizacích. 3. vyd. Praha : Grada Publishing, 2009. 360 s. ISBN 978-80-247-3051-6.

[14] PELTIER, Thomas, R. Information Security Risk Analysis. CRC Press, 2005. ISBN 0849333466.

[15] ČERMÁK, M. Řízení informačních rizik v praxi. 1. vyd. Brno : Tribun EU s.r.o., 2009. 134 s. ISBN 978-80-7399-731-1.

[16] BS 7799-3:2006, Information Security Management Systems, British Standard Institution.

[17] ČSN ISO/IEC TR 13335-4, Český normalizační institut 2009.

[18] DOUCEK, P., NOVÁK, L., SVATÁ, V. Řízení bezpečnosti informací. Kamil Mařík - Professional Publishing. 1. vyd. [s.l.] : Professional Publishing, 2008. 239 s. ISBN 978-80-86946-88-7.

[19] RANCE, Stuart; HANNA, Ashley. ITIL V3 : Slovníček termínů, definic a zkratek. 2. Praha : ItSMF Czech Republic, 2010. 72 s. Dostupné z WWW: <http://www.best-management-practice.com/officialsite>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AR	Analýza rizík
BIA	Business Impact Analysis (analýza funkčných dopadov)
BPA	Business Process Analysis (analýza podnikových procesov)
CCTA	Central Computer and Telecommunications Agency
CMM	Capability Maturity Model (model zrelosti procesov)
CS	Customer Support (oddelenie zákazníckej podpory 1. úrovne)
CSAT	Customer Satisfaction (spokojnosť zákazníka)
CSR	Customer Service Representative (operátor zákazníckej podpory)
HR	Human Resources Specialist (špecialista oddelenia ľudských zdrojov)
IS	Informačný systém
OPP	Outsourcing podnikových procesov
Q&R	Quality and Readiness (oddelenie kvality)
SDM	Service Delivery Manager
SL	Service Level (úroveň služby)
SLA	Service Level Agreement (dohoda o úrovni služby)
SRX	Service Request (technický incident)
TS-PER	Technical Support on Personal Level (oddelenie technickej podpory 2. úrovne)
TS-PRO	Technical Support on Professional Level (oddelenie technickej podpory 3. úrovne)

SEZNAM OBRÁZKŮ

SEZNAM TABULEK