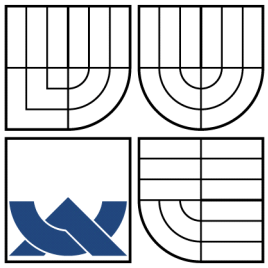
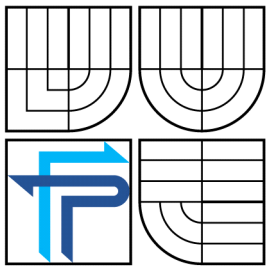


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA PODNIKATELSKÁ
ÚSTAV

FACULTY OF BUSINESS AND MANAGEMENT
INSTITUT OF

HODNOCENÍ ZABEZPEČENÍ OBCHODNÍCH INFORMACÍ

RATING OF SECURITY BUSINESS INFORMATIONS

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — MARTIN VESELÝ, BA
AUTHOR

VEDOUCÍ PRÁCE — PROF. ING. JIŘÍ DVOŘÁK, DRSC.
SUPERVISOR

BRNO 2007

Anotace

Diplomová práce „Hodnocení zabezpečení obchodních informací“ je zaměřena na vytvoření metrik pro vyhodnocování zabezpečení informačního systému firmy Tech4sec, spol.s.r.o.. Aplikací metrik jsou v práci stanovena přesná rizika informačního systému firmy a jejich ekonomický dopad. Součástí práce je též vytvoření dílčí části nové IS/IT strategie firmy, jejímž obsahem je odstranění nalezených rizik.

Annotation

The thesis ”Rating of security business information” is focused on creating metrics in order to assess security of an information system of the company Tech4sec, spol.s.r.o. Risks of the information system and their impact on economy of the company are elaborated by application of the created metrics. To build the part of IS/IT strategy of the company that leads to elimitation of the risks found is dealt with in the thesis as well.

Klíčová slova:

zabezpečení informací, informace, data, informační systém, bezpečnost informačního systému, IS/IT strategie, analýza rizik, bezpečnostní politika, rizika informačního systému, šifrování dat, zálohování dat, ochrana dat, metriky zabezpečení, řízení přístupu k informacím, SWOT analýza, stakeholders

Key words:

security information, information, data, information system, safeguard information system, security information system, IS/IT strategy, risk analysis, security policy, risk of information system, data encryption, data backup, data protection, metrics of security, control of secure access, SWOT analysis, stakeholders

Bibliografická citace diplomové práce:

VESELÝ, M. *Hodnocení zabezpečení obchodních informací.* Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2009. 82 s. Vedoucí diplomové práce prof. Ing. Jiří Dvořák, DrSc.

Prohlášení

Prohlašuji, že diplomová práce na téma „Hodnocení zabezpečení obchodních informací“ je původní a zpracoval jsem ji samostatně. Veškeré zdroje a literaturu, které jsem při práci používal nebo z nich čerpal, v práci řádně cituji a uvádím v seznamu použité literatury, neporušil jsem autorská práva (ve smyslu zákona č. 121/2000 Sb. O právu autorském a o právech souvisejících s právem autorským). Zavazuji se, že nebudu šířit informace získané ve společnosti Tech4Sec, spol. s r.o..

V Brně dne 10. ledna 2009

...…….

Martin Veselý, BA

Poděkování

Rád bych poděkoval touto cestou především prof. Ing. Jiřímu Dvořákovi, DrSc. za cenné rady, konzultace a bedlivý dohled při zpracování diplomové práce. Dále bych chtěl poděkovat také zaměstnancům firmy Tech4Sec, spol.s.r.o. za konzultace, doporučení a vstupní data, které sloužily pro zpracování analýz.

Obsah

Seznam obrázků a tabulek

Seznam obrázků:

Seznam tabulek:

1 Úvod

V posledních několika letech začala stoupat informační vyspělost všech ekonomických subjektů a tím i jejich závislost na datech, informacích, informačních systémech a internetu. A právě tak jak stoupá závislost firmy na informačních systémech a internetu, tak stoupají i všechna rizika z této závislosti vyplývající a je vyžadováno čím dál vyšší zabezpečení. Jak nám dříve stačila disketa na uložení dat, kterou jsme mohli dvakrát zkopírovat a uložit do šuplíků, tak dnes využíváme datové pole v jednotkách terabytů, které zálohujeme daleko složitějším způsobem s přístupem více osob. V případě ztráty diskety by firma fungovala dál, ale v případě výpadku datového pole firma stojí.

V dnešní době v případě ztráty, poškození nebo odcizení firemních dat z informačního systému má tento incident vždy velký dopad na následný chod firmy, pokud jsou data zneužita nebo prodána. Tento incident může trvat několik minut a bez povšimnutí kohokoliv z firmy. Proto je nutné informační systém chránit a zabezpečit, jak před externími hrozbami nebo subjekty jako jsou hackeři, konkurence, viry, cílenými útoky, tak i před interními útoky od zaměstnanců, správců IS, managementem a také před ostatními riziky jako jsou požár, přírodní katastrofy nebo nahodilá závada na zařízení(server,disk) v informačním systému.

Každé riziko nebo ztráta dat z informačního systému se dá vyčíslit, každé odcizení dat a jeho dopad je měřitelné. Tato práce se zabývá obecným stanovením rizik v informačním systému, vytvořením metrik měřitelnosti pro každé riziko, zavedením opatřením na eliminaci těchto rizik a jejich ekonomickým dopadem na firmu.

Vzhledem k rychlému vývoji technologií v oboru IT stoupá stejným způsobem i rychlý vývoj požadavků na informační systém firmy. Proto je více než žádoucí sledovat trendy v oboru a pravidelně investovat do informačního systému a jeho zabezpečení poměrnou část finančních prostředků z rozpočtu firmy. Zaspat v této oblasti může znamenat se neprobudit.

2 Systémové vymezení problému

Obsahem diplomové práce je vytvoření návrhu a aplikace metrik pro hodnocení zabezpečení obchodních informací ve firmě, tak abych mohl provést analýzu zabezpečení obchodních informací a rizik informačního systému firmy.

Na základě provedených výstupu analýz a vyhodnotím stávající zabezpečení obchodních informací a rizik vytvořím nový návrh zabezpečení obchodních informací a informačního systému firmy Tech4Sec spol.s.r.o. Tento návrh zhodnotím a zkomponuji do IS/IT strategie analyzované firmy.

3 Cíl práce

Cílem práce je analyzovat světové trendy bezpečnosti obchodních informací, zúročit vlastní několikaleté praktické a teoretické poznatky z oblasti architektury informačních systémů a komplexního zabezpečení IS firmy.

Vytvořit model funkčních částí komplexního informačního systému firmy a provést analýzu jednotlivých částí IS a současně vytvořit seznam rizik v každé části informačního systému firmy a jejich dopadu v případě zneužití. Na základě výstupu z analýz a nalezených rizik vytvořit seznam opatření především technických a organizačních, tak aby nedošlo ke zneužití obchodních informací a poškození IS firmy neoprávněnou osobou. Vytvořit vhodné metriky na základě těchto opatření pro každou oblast informačního systému.

Aplikovat tyto metriky na konkrétní firmu a stanovit úroveň zabezpečení v každé části informačního systému firmy. Provést další analýzy potřebné k vytvoření komplexního pohledu na celkové zabezpečení daného IS firmy.

A na základě komplexního vyhodnocení aplikace metrik a analýz navrhnout novou koncepci ekonomicky zdůvodněného zabezpečení a strategie IS firmy.

4 Přehled informačních zdrojů světa

4.1 Přehled norem pro řízení bezpečnosti elektronických informací a IS

ČSN ISO/IEC 17799:2005 (ISO/IEC 27002) Informační technologie - **Soubor postupů pro management bezpečnosti informací. Soubor postupů pro řízení bezpečnosti informací**

ISO/IEC 27001:2005 (BS 7799-2) Information security management systems – Requirements. **Požadavky na řízení bezpečnosti informací**

BS 7799-3:2006 Information security management systems – Part 3: Guidelines for information security risk management. **Hodnocení rizik IS**

ISO/IEC 27004 – Information security management measurements. **Definice metrik a indikátorů pro vyhodnocování.**

ČSN ISO/IEC TR 13335-1:2004 Směrnice pro řízení bezpečnosti IT – Část 1: Pojetí a modely bezpečnosti IT. **Úvod k základním pojetím a modelům bezpečnosti.**

ČSN ISO/IEC TR 13335-2:2000 Směrnice pro řízení bezpečnosti IT – Část 2: Řízení a plánování bezpečnosti IT. **Identifikování** vztahu mezi řízením bezpečnosti IT a všeobecným řízením IT.

ČSN ISO/IEC TR 13335-3:1998 Směrnice pro řízení bezpečnosti IT – Část 3: Techniky pro řízení bezpečnosti IT. **Popis řízení činnosti v průběhu projektu zaměřeného na bezpečnostní problematiku.**

ČSN ISO/IEC TR 13335-4:2002 Směrnice pro řízení bezpečnosti IT – Část 4: Výběr ochranných opatření. **Realizace bezpečnostních opatření vůči hrozbám.**

ISO/IEC TR 13335-5:2001 Guidelines for the management of IT security Part 5: Management guidance on network security. **Oblast bezpečnosti počítačových sítí.**

ISO/IEC TR 13569:2005 Banking and related financial services – Information security guidelines. **Problematika bezpečnosti IT společností v bankovním a finančním sektoru.**

ISO/IEC TR 18044:2004 Information security incident management. **Řešení bezpečnostních incidentů ve společnosti.**

4.2 Přehled konferencí se zaměřením na zabezpečení informací

iT security conference - Data v (ne)bezpečí

http://www.dns.cz/ftp/ke_stazeni/dns-program_it_security.pdf

Security Upgrade 2008: Nové trendy v bezpečnosti

http://www.svethardware.cz/art_doc-70390ED042EA0D7BC12575000058DB67.html

VII. Konference Řízení kvality a bezpečnosti informačních systémů ve zdravotnictví

http://wp.czu.cz/cs/index.php/?r=1550&mp=konference.info&idKonference=125

Konference IT underground 2008

http://itunderground.org/

IT Security Workshop 2008

http://www.itsw.cz/

Konference CYTER 2007 (Cyber Terrorism Conference)

https://cythres.mff.cuni.cz/cyter2007/

Security INVEX 2007

http://seminare.idg.cz/seminare.nsf/www/Security-Invex-2007

AEC Roadshow 2007

http://www.aec.cz/index.php?id=424,0,0,1,0,0

4.3 Internetové portály se zaměřením na bezpečnost informací

Bezpečnost IT – Portál o bezpečnosti informací

http://bezpecnost.interval.cz/

SANS - The largest source for information security training, certification & research in the world

http://www.sans.org

crypto-world.info - Novinky ze světa kryptologie

http://crypto-world.info/

ISVS – Informační systém veřejné správy

http://www.isvs.cz/bezpecnost/

Microsoft - Security Center

http://www.microsoft.com/security/default.mspx

Microsoft - Security TechCenter

http://technet.microsoft.com/en-us/security/default.aspx

NETWORKWORLD - Security

http://www.networkworld.com/topics/security.html?tnav=_l317_t1_s

4.4 Odborná periodika se zaměřením na bezpečnost

ICTsecurity - První český on-line magazín o bezpečnosti v ICT

http://www.ictsecurity.cz/

CRYPTO – WORLD - Novinky ze světa kryptologie

http://crypto-world.info/index2.php

DSM - Odborný čtvrtletník zaměřený na problematiku informační bezpečnosti a ochrany dat. http://www.dsm.tate.cz/

SCMagazine - Welcome to the leading industry magazine for IT security professionals

http://www.scmagazine.com/

Security magazíne - http://www.securitymagazine.com/

4.5 Webové prezentace výrobců zabezpečení dílčí části IS

UTIMACO - softwarová ochrana dat, šifrování

http://www.utimaco.com/

PGP - softwarová ochrana dat, šifrování

http://www.pgp.com/

Sophos - antivir, anti-spam, firewall

http://www.sophos.com/

Symantec - antivir, anti-spam, firewall, zálohování, šifrování

http://www.symantec.com/

McAfee, - antivir, anti-spam, firewall, šifrování

http://www.mcafee.com

Essentials security software - šifrování

http://www.essentialsecurity.com/

Aladdin - HW autentizace a PKI

http://www.aladdin.com/

AVG – antivir, antispam, firewall

http://www.grisoft.cz/

CISCO – firewall, IDS, IPS, síťová řešení, VPN, řízení přístupu

http://www.cisco.com

Juniper – firewall, IDS, IPS, síťová řešení, VPN, řízení přístupu

http://www.juniper.net

CheckPoint– firewall, IDS, IPS, síťová řešení, VPN, řízení přístupu

http://www.checkpoint.com

5 Použité metody řešení problému

5.1 Teoretická východiska

5.1.1 Definice a obsah informace

Obecně se slovo informace většinou používá závisle na kontextu bez důrazu na definici - jako příklad lze uvést všudypřítomná slovní spojení „informační věk“, „informační společnost“ a „informační technologie". V teorii informace se informací rozumí zpráva, resp. snížení nejistoty způsobené přijetím určité zprávy. Informace se též používá jako synonymum pro poznání, znalost, dorozumívání, zprávu pravdivou nebo chtěnou v protikladu k dezinformaci nebo šumu, data uložená v paměťových médiích atd.

Etymologicky je slovo informace založeno na myšlence nezávislosti látky a formy. Předpokládá se, že stejnou formu lze vtisknout různým látkám a předmětům, a naopak, že určitý předmět lze vytvarovat do různých forem, aniž by se změnila jeho látková povaha. I když ho již dnes oficiálně přijímaný kvantově mechanický popis přírody nepropaguje, je rozlišování mezi látkou a formou rozšířeným zvykem člověka a možná i nadřazených taxonů. Přitom je vždy předpokládána přinejmenším nějaká definice stejnosti, která nám umožňuje soudit, kdy nesou nestejné předměty stejnou informaci. Tato relace může být založena na tvaru, podobnosti, nebo složitějších přiřazeních, např. pomocí definice znaků a způsobu jejich čtení, a to nejen v obvyklém trojrozměrném prostoru, ale např. i v prostoru chemickém nebo kvantově mechanickém.

Informace z ekonomického hlediska jsou dnes rozhodujícím faktorem jejich úspěchu či neúspěchu, obecně vzato informace a znalosti jsou dnes jediným smysluplným zdrojem. Informace jsou považovány nejen za nezbytný předpoklad manažerských rozhodování, ale i za významný obchodní artikl, investiční oblast a příležitost pro podnikání.

Informace tak jak se používá v tzv. teorii informace

Kmotrem tohohle významu slova informace byl geniální Claude Shannon, který v r. 1948 publikoval průkopnickou publikaci A Mathematical Theory of Communication, v níž se soustřeďuje na přenos zpráv o konečném nebo spočetném množství znaků, např.

písmen nějaké abecedy nebo číslic nějaké číselné soustavy, což souviselo s jeho tehdejší prací pro Bellovy laboratoře. ***Informace je chápána jako míra snížení nejistoty o zprávě po přečtení této zprávy. Zaveden byl též pojem informační entropie.*** *Binární zápis informací ale ze známých osobností dávno před ním propagoval Leibniz, jenž zase obdivoval čínský binární systém I-ťing (易經).*[7]

V počítačové terminologii se formálně udává, že jeden bit, jako číslice dvojkové číselné soustavy, je jednotkou informace. Jeden bit bývá přitom vyčíslen jako znalost výsledku pozorování náhodného jevu, jehož pravděpodobnost je 50 %. To nemá nic společného ze sémantickým významem toho-kterého bitu v tom nebo oném přístroji. Ti, kteří mluví o kvantových počítačích, s oblibou používají jednotku kvantový bit.

5.1.2 Kybernetické a matematické pojetí informace

Z kybernetického hlediska můžeme považovat informace jako tzv. negentropickou veličinu snižující neurčitost rozhodovatele. Kybernetická definice informace je založena na pravděpodobnostním přístupu a můžeme tedy předpokládat:

- Každá rozhodovací situace má konečný počet řešení a rozhodnutí.
- Rozhodnutí se opakuje dostatečně dlouho na to, aby mohl být uplatněn statistický přístup.
- Je známo s jakými pravděpodobnostmi se jednotlivá rozhodnutí vyskytují.

Na základě těchto předpokladů lze potom vypočítávat/měřit množství informace I(X) dle vzorce

$$I(X) = -\log p(X)$$

Kde X je údálost,rozhodnutí

p(X) je pravděpodobnost událostí, rozhodnutí X

Na základě tohoto vztahu lze odvodit, že čím menší je pravděpodobnost p(X) výskytu událostí, rozhodnutí, tím větší je množství informace potřebné pro správné rozhodnutí o jevu X.[4]

5.1.3 Hodnota,obsah a typy informací

Z hlediska ekonomicko-manažerského se stává informace každé sdělení, jako je zpráva nebo data, které usnadňují dané rozhodování ve smyslu jeho správnosti nebo lepšího výsledku rozhodnutí. Toto pojetí informace lze nazývat jako účelové neboli pragmatické. Při tomto pojetí jsou informace získávány nebo odvozovány z dat, které získáváme vhodnými transformacemi a operacemi, jako jsou například filtrace, sumarizace, výběrem na základě vzorců. V dnešní době informace zastarávají velmi rychle a jejich vypovídající informace v daném okamžiku už nemusí být informací ale jen data. Což můžeme definovat tak, že pokud nedokážeme použít doručenou informaci, tak jsou to pro nás pouze „pouhá“data.

Proto v tomto pojetí z pohledu ekonomicko-manažerského potřebujeme zkoumat následující atributy u informací:

- Včasnost, dostupnost, spolehlivost přísunu informací
- Obsah, aktuálnost, relevantnost, pravdivost, objektivnost
- Formát
- Cenu a užitnou hodnotu informací
- Legálnost, utajení

5.1.4 Výpočet informačního obsahu

Když považujeme informace za jakýkoliv údaj o jevech a procesech uvnitř systému i v jeho okolí, tak nám informace zvyšuje uspořádanost systému a tím stoupá narůstání entropie informací, což můžeme charakterizovat jako přechod do méně uspořádaného stavu.

informační obsah = střední množství informace je dán vzorcem, který je shodný s vyjádřením stupně neurčitosti systému, tj. informační entropií

Shannonova entropie

$$H = \frac{I}{n} = -K\sum_{i=1}^{s} P_i \ln P_i$$

= střední hodnota informace na jeden symbol zprávy

Odvození konstanty K:

Nechť A={0,1}, nechť střední množství informace na jeden symbol je rovno jedné. Pak za předpokladu stejné pravděpodobnosti výskytu obou symbolů platí:

$$H = -K[\frac{1}{2}\ln\frac{1}{2} + \frac{1}{2}\ln\frac{1}{2}] = -K\ln\frac{1}{2} = K\ln 2 = 2$$

Odtud: $K = \frac{1}{\ln 2}$

Matematicky korektně:

Entropie je funkce splňující následující axiomy:

1) Je spojitou funkcí pravděpodobnosti na intervalu $0 \le P \le 1$

2) $H(P_1, P_2, ...P_s)$ je symetrickou funkcí svých argumentů

3) Jestliže symbol a_s v původní abecedě lze rozložit na dva dílčí symboly ${}^1a_s$ a ${}^2a_s$ s pravděpodobností výskytu Q_1 a Q_2, kde $P = Q_1 + Q_2$, pak platí

$$H(P_1, P_2, ...P_{s-1}, Q_1, Q_2) = H(P_1, P_2, ...P_s) + P_s H(\frac{Q_1}{P_s}, \frac{Q_2}{P_s})$$

Lze ukázat, že uvedeným podmínkám vyhovuje funkce $H = -K\sum_{i=1}^{s} P_i \ln P_i$ (viz výše)

Z toho vyplývá, že jev jehož pravděpodobnost je veliká nese malé množství informace, jev s malou pravděpodobností má velký informační obsah.[9]

5.1.5 Klasifikace informací

Z ekonomického-manžerského hlediska můžeme klasifikovat informace na tři základní kategorie z pohledu řízení a jejich určení na:

- Strategické informace
- Taktické informace
- Operativní informace

Uvedené kategorie informací se liší charakterem řešených problémů, mírou kompetencí, odpovědnosti při stanovení cílů a úkolů, odpovědnosti za jejich realizaci a dalšími atributy. Zásadní rozdíly mezi jednotlivými vrstvami řízení však existují také v charakteru rozhodování, informací potřebných pro rozhodování a v dopadu kvality na rozhodnutí fungování firmy.[4]

Strategické informace

Mívají na fungování organizace největší a dlouhodobé dopady. Jsou většinou spojeny s neopakovatelnými a unikátními jevy a situacemi. Jejich výskyt a průběh v budoucnu je velmi obtížné předvídat i pro velmi zkušené manažery.

Operativní informace

Jsou spojeny s jevy, které se vyskytují opakovaně a jejich výskyt a průběh v budoucnu lze předvídat a je možné se připravit na jejich řešení. Toto řešení bývá zpravidla k dispozici formou návodů, směrnic popřípadě předem definovaných instrukcí. Využívá se zde minulé nebo všeobecně známé situace z předchozích výskytů informace - jevu. Na rozdíl od strategické informace je taktická operace sdělena všem zainteresovaným „stakeholders“. Operativní informace mají střednědobý dopad na fungování organizace.

Taktické informace

Tvoří určitý přechod mezi strategickou a operativní informací. Můžeme to považovat za operativní informace, které mají velký vliv na strategické informace nebo jejich dílčí část. Můžeme si pod nimi představit: poruchy výrobních zařízení, krach významného odběratele, nedostupná výrobní součást, onemocnění odchod klíčových pracovníků, atd…

5.1.6 Data a jejich vztah k informaci

Data je výraz pro údaje, používané pro popis nějakého jevu nebo vlastnosti pozorovaného objektu. Data se získávají měřením nebo pozorováním, a lze je dělit data

spojitá a data atributivní. Data spojitá se přitom vztahují k nějaké spojité stupnici, zatímco data atributivní nikoliv.

Data můžeme považovat za výroky, které popisují realitu a charakterizují určitý jev nebo objekt. Z tohoto pohledu můžeme z akademického hlediska lze zjišťovat zda data(výrok) platí či ne. Jako příklady dat-výroků lze považovat:

- Počet osob v místnosti, počet stran knihy,…
- Jméno a příjmení zaměstnance, datum a místo narození, bydliště,…
- Údaje o objemu prodejů firmy, podílu na trhu, hospodářském výsledku, nákladech,…
- Zpráva o trendech, akciových trzích, vynálezech,…
- Zákony, směrnice, atd…

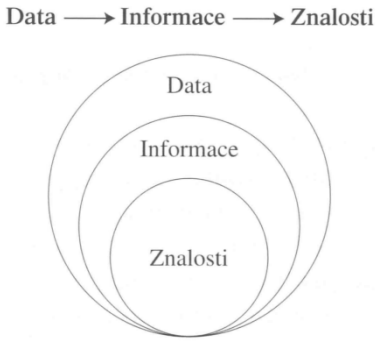
Data jsou

- Vyjádření skutečností formálním způsobem tak, aby je bylo možno přenášet nebo zpracovat (např. počítačem)
- Číselné nebo jiné symbolicky vyjádřené (reprezentované) údaje a hodnoty nějakých entit nebo událostí
- Jakékoli fyzicky (materiálně) zaznamenané znalosti (vědomosti), poznatky, zkušenosti nebo výsledky pozorování procesů, projevů, činností a prvků reálného světa (reality)
- Surovina, z níž se tvoří informace

Vztah mezi daty a informacemi

Nejjednodušeji si lze představit vztah mezi informacemi a daty dle obrázku. Nejprve máme nějaké **data**, např. tabulku s vývoji cen produktu za rok s týdenní periodou aktualizace, což můžeme považovat za jev, který nastal. Když tyto data setřídíme dle určitého algoritmu, tak dostaneme **informaci** o ročním vývoji cen. A na základě této informace **známe** zisk v daném období dle vlastního prodeje.

Vztah mezi Data -> Informace -> Znalosti



Obrázek 1: Vztah mezi daty a informacemi
Zdroj: [2]

5.1.7 Druhy dokumentů

V každé společnosti by měli být dle ISO 27000 rozděleny dokumenty do následujících skupin a každá skupina dokumentů je určena pro určitou skupinu „stakeholders“. Každý druh(skupina) dokumentů vyžaduje přesné vymezení, jak s danou skupinou dokumentů lze nakládat, jako jsou oprávnění pro čtení/zápis, šifrování, utajení a další atributy, které můžeme pro dokumenty, respektive informace nastavit.

Dokumenty můžeme rozdělit na[1]:

a) **Legislativní dokumenty** - dokumenty požadované ze zákona, nebo vydávané vykonavateli státní správy, jako např.:
   - Společenská smlouva, čestné prohlášení jednatele
   - Výpis z obchodního rejstříku, živnostenské listy
   - Výpisy z rejstříku trestů, osvědčení o prověrkách NBÚ

b) **Strategické řídící dokumenty -** Dokumenty definující základní rámec existence společnosti a jsou to všechny tyto dokumenty:
   - Strategie společnosti, která obsahuje:
   - vize a záměry
   - dlouhodobý koncepční plán
   - prospěšnost

[1] Klasifikace dle ISO 27001

- obchodní politika
- personální politika
- politika jakosti, environmentu a bezpečnosti informací
- bezpečnostní politika

- Organizační řád, který obsahuje:
- Organizační strukturu
- Definice hlavních pravomocí a odpovědností
- Zásady firemní kultury

c) **Řídící dokumenty -** Dokumenty, které definují povinnosti, zásady a pravidla práce společnosti a jejich pracovníků. Jsou to:

- Organizační směrnice
- Prováděcí postupy
- Pracovní náplně funkcí
- Strategické cíle

d) **Vzory a šablony -** Podklady a formuláře pro tvorbu dokumentů a prezentací pracovníky společnosti. Jsou to zejména:

- Interní šablony (systém managementu společnosti, zápis z porady apod.)
- Vzory pro prodej (nabídky, smlouvy, obchodní prezentace a pod.)
- Vzory pro realizaci (dotazníky, směrnice, pracovní náplně, školící prezentace apod.)

e) **Evidence -** Aktuální soubory dat vznikajících při práci společnosti např.:

- Seznam potenciálních zákazníků (obchodní aktivita)
- Kontakty pracovníků společnosti
- Základní obchodní evidence
- Přehled odměn
- Přehled řešených projektů
- Pokladní kniha

f) **Záznamy -** Platné dokumenty vydávané příslušně odpovědnými osobami. Jsou to zejména:
   - Roční plán (tržby, náklady, výcvik)
   - Zápisy z porad (vedení, strategická, obchodní, realizační)
   - Záznamy z interních školení
   - Osobní složka zaměstnance
   - Úkoly
   - Platné nabídky
   - Platné smlouvy a objednávky zákazníků
   - Ověřené záznamy z jednání
   - Předávací protokoly
   - Montážní deník
   - Projektová dokumentace
   - Zápis o předání – montážní a kontrolní list

g) **Doklady -** Materiály prokazující vztahy s vnějšími subjekty:
   - Kvalifikační osvědčení zaměstnanců a společnosti (certifikáty, diplomy)
   - Účetní doklady (účty, stvrzenky, faktury, daňová přiznání)
   - Smlouvy a objednávky dodavatelů

h) **Externí dokumentace** - Dokumentace vznikající nezávisle na společnosti, ale ve firmě používaná:
   - Normy
   - Zákony, vyhlášky
   - Učebnice a příručky

i) **Oficiální prezentace -** Informace, které jsou cíleně veřejně dostupné
   - Referenční listiny
   - Reklamní brožury
   - Webové stránky
   - Příručka společnosti

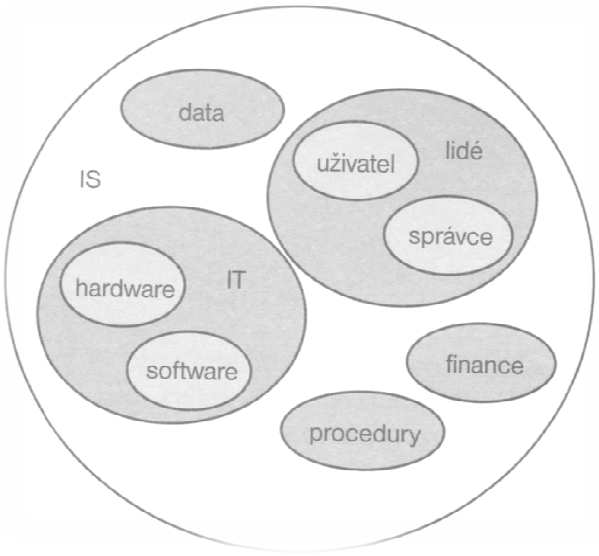
j) **Pracovní dokumentace -** Materiály jejichž platnost souvisí s autorem a účelem, nejsou řízeny a kontrolovány, ale je nezbytné jejich bezpečné uchování:
   - Dokumentace zákazníků

- Metodické koncepty
- Návrhy
- Metodické pokyny

5.1.8 Informační systém a jeho koncepce

Informační systém si můžeme představit jako identifikovatelný funkční celek, zabezpečující cílevědomé a systematické shromažďování, zpracovávání, uchovávání a zpřístupňování informací. IS obsahuje data, technické a programové vybavení, finanční prostředky, procedury(procesy, předpisová základna, směrnice, manuály) a pracovníky (správci a uživatelé).[2]

Schématické znázornění IS včetně komponent je zobrazeno na obrázku 2.



Obrázek 2: Jednotlivé části informačního systému
Zdroj: [2]

Jednotlivé části IS můžeme rozdělit na následovně:

- Data a informace
- Informační technologie (HW a SW)
- Lidé (uživatel a správce IS)
- Procedury
- Finance

Data a informace

Data můžeme z pohledu IS považovat za reprezentaci skutečností, pojmů či údajů, které vznikají, jsou uchovávány a zpracovávány v rámci výkonu činnosti společnosti nebo v přímé souvislosti s ní tak, aby bylo možné jejich zpřístupňování, interpretace či zpracování lidmi nebo automatizovanými prostředky.[ZOI]

Pod pojmem informace vzhledem k IS můžeme definovat data, která jsou především srozumitelná lidem a zejména konkrétním skupinám IS pro které je daná informace určena. Informace jsou nejdůležitější aktiva IS.

Informační technologie (HW a SW)

Informační technologie tvoří v IS veškeré technické vybavení zahrnující hardware, software ale také internetové připojení, WWW prezentace u providera, licence, mobilní telefony, USB disky a veškeré další technické vybavení které dokáže uchovávat, zpracovávat nebo přenášet data.

Lidé (uživatel a správce IS)

Z pohledu IS máme dva typy lidských subjektů vstupujících do IS a to :

Uživatele – který daný systém využívá ke své pracovní činnosti

Správce – který je odpovědný za funkčnost IS. Pod pojmem správce si můžeme představit 3 role:

- Administrátora systému(IT pracovník) – který upravuje, konfiguruje, zavadí nové zabezpečení do IS, je zodpovědný za chod IS.
- Řídící pracovník – dává vizi a strategii IS, dáva pokyny administrátorům systému, řídí směr a vývoj IS. Je zodpovědný za výstupy z IS a jeho celkovou funkčnost.
- Uživatel – je zodpovědný za obsah a aktuálnost dat v IS, které do něj zadává a se kterými pracuje.

Procedury

Pod pojem procedury můžeme zahrnout všechny technické a automatické procesy, které vykonává IS v závislosti mezi všemi částmi IS. Součástí procedur jsou i všechny předpisy a směrnice ve vztahu k IS, které určují jakým způsobem zadávat, reportovat, ukládat, zabezpečit a nakládat s daty v IS.

Finance

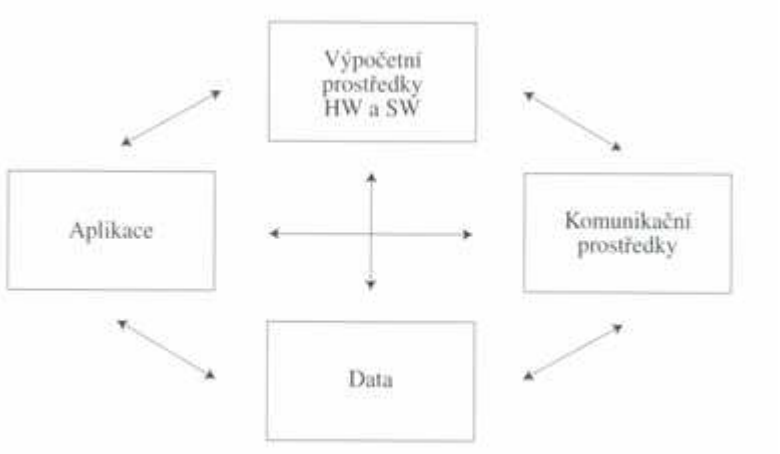
Pod pojmem finance jsou zahrnuty veškeré náklady a hodnoty související se všemi částmi IS (nákup, vývoj, provoz, údržba, know how, hodnota informaci v IS, lidé,…).

5.1.9 Architektura IS

Je zřejmé, že návrh architektury IS patří mezi důležitá a závažná rozhodnutí, které sebou nese vážné důsledky. Proto toto rozhodnutí vyžaduje důkladnou analýzu a speciální znalosti. Proto by na jeho přípravě vždy měli participovat vždy specialisté z požadovaných oblastí IS s adekvátními znalostmi ze svojí oblasti IS.

Celková architektura IS je tvořena dílčími architekturami

- Funkční a procesní architekturou
- Datovou architekturou
- Architekturou programových prostředků
- Architekturou technických prostředků



Obrázek 3: Architektura informačního systému
Zdroj: [2]

5.1.10 Bezpečnostní politika IS

Bezpečnostní politika je základní dokument pro řešení informační bezpečnosti. Tento dokument je schválen nejvyššími představiteli společnosti – managementem a následně je závazný pro všechny zaměstnance společnosti a pro pracovníky externích společností, kteří využívají IS společnosti.

Bezpečnostní politika IS definuje východiska pro všechny další aktivity společnosti v oblasti informační bezpečnosti.

Hlavním cílem bezpečnostní politiky IS je

- Definovat hlavní cíle ochrany informací
- Stanovit způsob řešení bezpečnosti IS
- Určit pravomoci a zodpovědnosti v oblasti IS

Bezpečnostní politika IS by měla řešit následující oblasti bezpečnosti:

- Organizace informační bezpečnosti
- Klasifikace a řízení informačních aktiv
- Personální bezpečnost
- Fyzická bezpečnost a bezpečnost prostředí
- Vývoj a správa systému
- Řízení přístupu uživatelů do IS
- Kontinuita podnikání
- Soulad s právem a legislativou
- Podmínky auditu

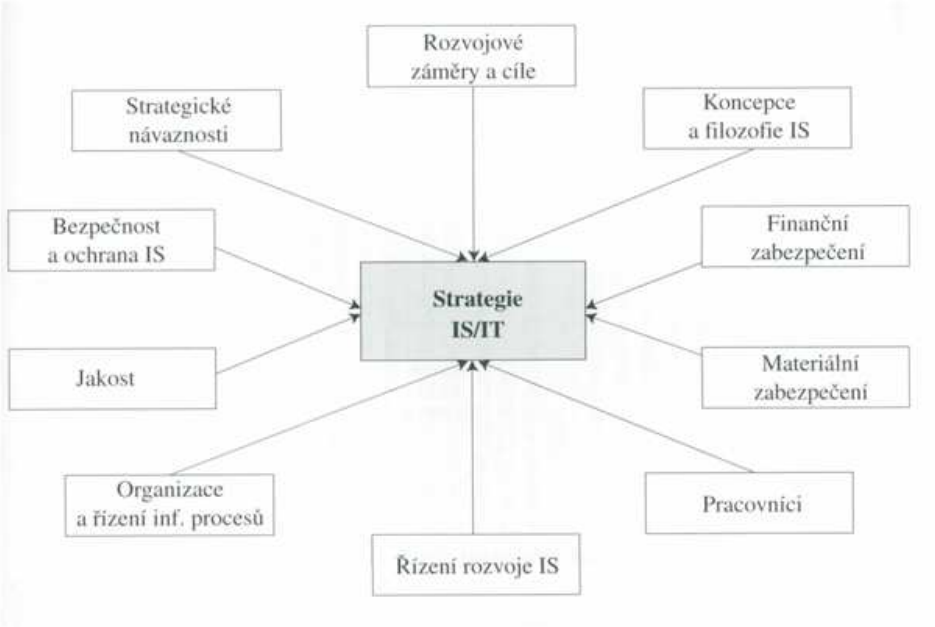
5.1.11 IS/IT strategie IS

IS/IT strategie firmy si můžeme představit jako množinu strategických cílů, plánů, politik, rozpracovaných pro určitou organizační jednotku firmy nebo firmu, které vycházejí ze strategických cílů vytyčených nadřazenou business nebo corporate strategií a zároveň IS/IT strategie vymezuje cestu realizace vytyčených cílů.

Pohled na strukturu strategie IS/IT

Každé strategické cíle, záměry, vize a úkoly můžeme v návrhu strategie kategorizovat a strukturovat podle jednotlivých oblastí a aspektů což můžeme nazvat strukturou neboli obsahem strategie. Názory na jednotlivé kategorie nemusí být vždy jednotné a zároveň se jednotlivé kategorie mohou mezi sebou prolínat.

Základní strukturu a obsahovou strukturu můžeme vidět na následujícím obrázku:



Obrázek 4: Struktura a vymezení IS/IT strategie
Zdroj:[4]

Podle charakteru jednotlivých aspektů budou v některých částech návrhu strategie vyjádřeny spíše strategické cíle, kterých má být dosaženo a v jiných bude převažovat zaměření na vymezení cest a postupné realizace vytyčených strategických cílů. To ale nevylučuje, že i zde mohou být zformulovány specifické strategické cíle pro danou oblast, které však mají spíše charakter kritérií pro hodnocení realizace příslušných záměrů.[11]

5.1.12 Provázání IS/IT strategie na business a corporate strategii firmy

Když se zaměříme na IS/IT strategii tak ji můžeme charakterizovat jako funkční strategii s návaznostmi na nadřazené strategické cíle, které jsou vyjádřeny obchodní

strategií SBU nebo corporate strategií firmy. IS/IT strategie by měla korespondovat s vytyčenými strategickými cíli a způsoby jejich dosažení v oblasti IS/IT.

IS/IT strategie zaujímá mezi funkčními strategiemi zvláštní postavení v tom smyslu, že musí podporovat, jak nadřazenou obchodní strategii, tak i ostatní funkční strategie a měla by s nimi být provázána tak, aby oblast IS/IT maximálně podporovala naplnění dílčích strategických cílů souvisejících funkčních strategií.

5.1.13 Aktiva IS firmy

Aktiva nebo-li Aktivum (asset) můžeme definovat jako nehmotný nebo hmotný statek mající v rámci informačního systému určitou hodnotu.

Identifikace aktiv

Identifikace spočívá ve vytvoření seznamu aktiv, které leží uvnitř hranice AR.Bude se tedy jednat o následující aktiva:

- Informace – databáze, sestavy dat, dokumenty
- HW – servery, pracovní stanice, směrovače, tiskárny, kabely
- SW – operační systémy, aplikační programy
- Budovy a místnosti v nichž se aktiva typu a/ až c/ fyzicky nacházejí

Ocenění aktiv

Při provádění AR potřebujeme znát odhad ceny (významu, důležitosti)jednotlivých aktiv ležících uvnitř hranice analýzy rizik. Stanovení ceny fyzických aktiv je jednoduchá – na základě pořizovací ceny odpovídajícího zařízení. Obtížněji se stanovuje cena datových aktiv – obvykle se stanovuje na základě odhadu velikosti škody, kterou by OS způsobilo vyzrazení a zneužití dat, jejich neoprávněná modifikace, nedostupnost a případné zničení (princip odhadu „Co by se stalo, kdyby …?“. Hodnota je pro tato aktiva odvozována nepřímo přes soustavu nepeněžních měřítek. Doporučuje se vzít v úvahu alespoň následující nepeněžní parametry a z nich vyplývající ztráty:

- Nedodržení legislativy a/nebo předpisů
- Zhoršení výkonu činnosti OS

- Ztráta dobrého jména nebo negativní vliv na pověst OS
- Narušení důvěrnosti spojené s osobními informacemi
- Ohrožení osobní bezpečnosti, nepříznivý vliv na prosazení práva
- Porušení obchodního tajemství
- Narušení veřejného pořádku
- Finanční ztráty, přerušení aktivit činnosti OS
- Zhoršení bezpečnosti prostředí

Seskupování aktiv

Za účelem zjednodušení realizace analýzy rizik se obvykle provádí slučování aktiv do skupin aktiv. Do jedné skupiny zahrneme aktiva stejných vlastností v rámci IS slouží ke stejnému účelu). Například servery obsahující databáze užívané aplikace v OS a umístěné společně v jedné místnosti lze sloučit do jedné skupiny (skupina aktiv „servery“). Podobně pracovní počítačové stanice v rámci celé zkoumané části IS, na nichž je nainstalováno stejné SW prostředí můžeme sloučit do jedné skupiny aktiv „pracovní stanice“.

Identifikace hrozeb

V této části se identifikují hrozby, které mohou ohrožovat některé z uvažovaných aktiv (skupin aktiv). Při identifikaci hrozeb se vychází obvykle ze seznamu hrozeb příslušných pro daný typ aktiva a uvedeného v používané metodě AR nebo z vlastní zkušenosti. Jednotlivým aktivům (skupinám aktiv) jsou přiřazeny konkrétní hrozby.[2]

5.2 Způsoby ochrany dat

5.2.1 Šifrování dat

Šifrování neboli kryptografie je nauka o metodách utajování smyslu zpráv převodem do podoby, která je čitelná jen se speciální znalostí. Slovo kryptografie pochází z řečtiny – kryptós je skrytý a gráphein znamená psát. Někdy je pojem obecněji používán pro vědu o čemkoli spojeném se šiframi jako alternativa k pojmu kryptologie. Kryptologie zahrnuje kryptografii a kryptoanalýzu, neboli luštění zašifrovaných zpráv.

Kryptografie se po staletí vyvíjela k větší složitosti zároveň s lidskou civilizací a mnohokrát ovlivnila běh dějin. Zejména utajení či vyzrazení strategických vojenských

informací může mít zásadní vliv. Ale také prozrazení politických intrik, přípravy atentátů nebo i jen prozrazení milenců a podobně, to vše může úzce záviset na bezpečném přenosu informací a na schopnostech protivníka šifru rozbít.

Symetrická šifra, někdy též nazývaná konvenční, je takový šifrovací algoritmus, který používá k šifrování i dešifrování jediný klíč. Tím se liší od algoritmů s veřejným klíčem, které mají dvojici klíčů – tajný a veřejný.

Podstatnou výhodou symetrických šifer je jejich nízká výpočetní náročnost. Algoritmy pro šifrování s veřejným klíčem můžou být i stotisíckrát pomalejší. Na druhou stranu velkou nevýhodou je nutnost sdílení tajného klíče, takže se odesilatel a příjemce tajné zprávy musí předem domluvit na tajném klíči.

Symetrické šifry se často používají společně s asymetrickými. Obvyklé použití je takové, že otevřený text se zašifruje symetrickou šifrou s náhodně vygenerovaným klíčem. Tento symetrický klíč se zašifruje veřejným klíčem asymetrické šifry, takže dešifrovat data může pouze majitel tajného klíče dané asymetrické šifry.

Symetrické šifry se dělí na dva druhy. Proudové šifry zpracovávají otevřený text po jednotlivých bitech. Blokové šifry rozdělí otevřený text na bloky stejné velikosti a doplní vhodným způsobem poslední blok na stejnou velikost. U většiny šifer se používá blok o 64 bitech, AES používá 128 a 256 bitů. Blokové šifry jsou: AES, Blowfish, DES, GOST, IDEA, RC2, RC5, Triple DES, Twofish.

Nejpoužívanější AES (Advanced Encryption Standard) je schválený standard, amerického úřadu pro standardizaci (NIST), který byl udělen symetrické blokové šifře Rijndael. Šifra byla vyvinuta belgičany Joan Daemen a Vincent Rijmen a zařazena do veřejné soutěže NIST vyhlášené 2.1.1997 o federální šifrovací AES. Šifra využívá symetrického klíče. Tj. stejný klíč je použit pro šifrování i dešifrování. Délka klíče může být 128, 192 nebo 256 bitů. Metoda šifruje data postupně v blocích s pevnou délkou 128 bitů.Šifra se vyznačuje vysokou rychlostí šifrování. Tento standart je nejpoužívanější pro šifrování dokumentů, dat, VPN spojení a emailů.

V současné době není veřejně znám žádný případ plného prolomení této metody ochrany dat.[13]

5.2.2 Zálohovaní dat

O informace v počítači můžete nechtěně přijít mnoha způsoby. Omylem zmáčknete nechtěnou klávesu na klávesnici. Dojde k přepětí nebo výpadku elektrické energie. Zásah blesku. Záplavy. Krádež. A někdy se prostě stane, že zařízení přestane fungovat. **Pravidelné zálohování informací umožňuje obnovit některá (případně všechna) data, pokud dojde ke ztrátě původních informací v počítači.** V následující části je popsáno, které informace bychom měli zálohovat a jak často.

Volba souborů k zálohování

O výběru informací k zálohování rozhoduje každý uživatel sám. Je vhodné začít osobními dokumenty. Na prvním místě by měly být veškeré informace, které nelze snadno nahradit. Informace o bankovních účtech (a další informace o finančních prostředcích), smlouvy, osobní projekty a všechny další dokumenty, které mají pro majitele vysokou hodnotu – to jsou všechno informace, které je vhodné pravidelně zálohovat.

Ve firemním prostředí je nutné zálohovat téměř vše mimo osobních-soukromých dat uživatelů. Musíme zálohovat celý IS a každá část je specifická a tím i zálohování každé části je specifické a různorodé. Omezit nás může pouze velikost prostoru pro zálohování, kterou máte k dispozici.

Ve firemním prostředí bychom měli zálohovat především tyto data:

- Firemní databáze informačního systému (CRM,ERP)
- Nastavení všech zařízení (konfigurace), veškeré hesla, certifikáty, kryptografické klíče
- Veškerou elektronickou komunikaci, která proběhla v posledním období do a z IS (emaily, logy, seznam a obsah vytištěných souborů, seznam všech dat které elektronicky opustily informační systém)
- Účetní data, účetní doklady
- Smlouvy a cenné papíry
- Software nakoupený bez médií, licenční klíče
- Bezpečnostní dokumentaci a směrnice

Vytvoření plánu zálohování

Pro vytvoření plánu zálohování je potřeba stanovit, která data budeme zálohovat a za jakých podmínek a jak často. Podle toho zvolíme správnou strategii zálohování. Volba správné strategie je závislá na tom, jestli je potřeba se zálohami pracovat velmi často nebo je naopak požadována maximální délka archivace zálohovaných dat. Existují i další kritéria, která odrážejí konkrétní specifické podmínky.

Chcete-li zjistit, co pojem často znamená, představte si, jak byste se cítili, kdybyste přišli o veškerou práci, kterou jste v počítači uložili během dneška. Nebo veškerou práci za celý poslední týden nebo za celý poslední měsíc. Jestliže u vás některá z těchto představ vyvolá mírné zděšení, pak jste zjistili, jak často potřebujete zálohovat.

Nejvýhodnější je nastavit zobrazení výzvy k zálohování souborů v kalendáři nebo například při instalaci, inovaci nebo aktualizaci softwaru. Pravidelně a často byste však měli zálohovat všechna data.

Typy záloh

Nestrukturovaná - Nestrukturovaným úložištěm může být větší množství disket, CD, DVD medií s minimem informací o záloze. Tento způsob je nejjednodušší, ale není příliš oblíben u větších firem.

Úplná + Inkrementální - Tento model má za cíl vytvořit více kopií zálohovaných dat vhodnějším způsobem. Nejdříve je provedena úplná záloha všech dat. Posléze je prováděna inkrementální záloha (ukládány jsou pouze soubory, které se změnily od předešlé úplné nebo inkrementální zálohy). Hlavní nevýhodou je, že při obnovení zálohy je potřeba pracovat s úplnou zálohou a následně se všemi inkrementálními zálohami až k požadovanému okamžiku zálohy, což může být velmi náročné na pracovní prostor.

Úplná + Rozdílová - Rozdíl oproti předešlé metodě je v tom, že po úplné záloze se každá částečná záloha zachytí všechny soubory vytvořené nebo změněné od vytvoření úplné zálohy, třebaže některé už jsou obsaženy v předešlé částečné záloze. Výhodou je, že obnova zahrnuje obnovení pouze poslední úplné zálohy a potom její překrytí

poslední rozdílovou zálohou, takže je proces obnovení více odolný vůči defektu média se zálohou.

Zrcadlová + Reverzně přírůstková - Tento model obsahuje zrcadlo reflektující stav systému po poslední záloze a historii přírůstkových záloh. Výhodou je, že máme neustále k dispozici aktuální plnou zálohu a ukládáme pouze historii změn. Každé zálohování se automaticky promítá do zrcadla zrcadla a soubory, které byly změněny, jsou přesunuty do přírůstkové zálohy. Tato metoda se nehodí pro přenosná media, protože každá záloha musí být provedena pomocí srovnání se zrcadlem.

Průběžná ochrana dat - Tato metoda využívá místo plánovaných periodických záloh okamžitý zápis každé změny do žurnálu změn (logu). Provádí se ukládáním bytů nebo celých bloků dat místo ukládání celých změněných souborů. Průběžný záznam změn v žurnálu umožňuje získat obraz dat v minulosti. Naproti tomu prosté zrcadlení dat na druhý disk (např. RAID 1) stav v minulosti nezachycuje.

Pokud soubory pravidelně zálohujete a uchováváte kopie odděleně, můžete některé, možná i všechny, informace získat zpět, jestliže dojde ke ztrátě původních souborů v počítači.

5.2.3 Oprávnění

Většina informačních systémů musí zabezpečit omezení přístupu uživatelů k datům pomocí funkce řízení přístupu. Nastavením oprávnění určíme úroveň přístupu pro uživatele a skupiny.

Nastavení oprávnění k souborům a složkám

Typ přístupu, který chcete udělit uživateli či skupině, můžete definovat pomocí nastavení oprávnění. U souborů můžete například udělit oprávnění pro čtení a zápis celé skupině uživatelů. Chcete-li nastavit oprávnění, je třeba určit úroveň přístupu skupin a uživatelů. Můžete například umožnit čtení obsahu souboru jednomu uživateli, provádění změn v souboru jinému uživateli a všem ostatním uživatelům můžete v přístupu k danému souboru zabránit. Podobná oprávnění lze nastavit také u tiskáren a umožnit, aby určití uživatelé mohli tiskárnu konfigurovat a ostatní uživatelé ji pouze používali k

tisku. Chcete-li u souboru či složky změnit oprávnění, je nutné, abyste byli vlastníkem daného souboru či složky nebo měli oprávnění takové změny provést.[14]

Oprávnění skupiny

Nejlepších výsledků zabezpečení dosáhnete, pokud přidělíte oprávnění skupinám. Tím se vyhnete nutnosti udržovat řízení přístupu u jednotlivých uživatelů. Ve vhodných případech přidělíme Úplné řízení, nikoli individuální oprávnění. Možnost Odepřít u určitého oprávnění použijte, jestliže chcete vyloučit podsadu ze skupiny s oprávněními s hodnotou Povolit nebo jestliže chcete vyloučit jedno určité oprávnění v případě, že jste již uživateli či skupině udělili úplné řízení. Typ oprávnění, které je možné udělit, závisí na typu objektu. Oprávnění k souboru se například liší od oprávnění ke klíči registru. Některá oprávnění jsou však společná, například: číst oprávnění, měnit oprávnění, změnit vlastníka a odstraňovat.

Většina moderních souborových systémů umožňuje kontrolovat přístup k souborům a adresářům pomocí oprávnění, která jsou udělena jednotlivým uživatelům nebo skupinám uživatelů. Na základě těchto oprávnění může operační systém dovolit nebo odepřít čtení nebo zápis do souboru, přejmenování, změnu oprávnění a podobně.

Systémy oprávnění

Tradiční unixová oprávnění - Standard POSIX definuje jednoduchý systém oprávnění, který používají všechny unixové systémy včetně Linuxu a Mac OS X. Proto ho nazýváme jako tradiční unixová oprávnění.

Access control list - Microsoft Windows NT (a všechny jeho následovníci 2000,XP,Vista) stejně jako VMS, OpenVMS a další systémy používají Access control list (ACL), který umožňuje komplexní a variabilní nastavení přístupu. ACL definuje i POSIX, a proto jejich podporu nalezneme v mnoha souborových systémech v Unixu a Linuxu.

Řízení přístupu

Řízení přístupu je proces autorizování uživatelů, skupin a počítačů pro přístup k objektům v síti. Mezi klíčové pojmy, které souvisejí s řízením přístupu patří oprávnění, uživatelská práva a audit objektů.

Oprávnění - určují typ povoleného přístupu k danému objektu nebo vlastnosti objektu určitým uživatelům nebo skupinám. Oprávnění se vztahují na všechny zabezpečené objekty (soubory, objekty služby Active Directory® nebo objekty registru). Oprávnění mohou být přiřazena každému uživateli, skupině, nebo počítači. Oprávnění se většinou přiřazují skupinám.

Vlastnictví objektů - Při vytvoření objektu je tomuto objektu přiřazen vlastník. Výchozím vlastníkem objektu je autor. Vlastník objektu může změnit oprávnění přiřazená objektu vždy, bez ohledu na aktuální oprávnění přiřazená objektu.

Dědičnost oprávnění - správcům usnadňuje přidělování a správu oprávnění. Tato vlastnost způsobuje, že objekty uvnitř kontejneru automaticky dědí všechna dědičná oprávnění tohoto kontejneru. Například soubory vytvořené ve složce dědí oprávnění této složky. Zděděna budou pouze označená oprávnění.

5.2.4 Vzdálený přístup k firemním datům

Jak stoupá v poslední době trend pracovat pro firmu kdekoliv a kdykoliv, tak stoupá i riziko úniku dat, kdykoliv a kdekoliv pomocí nedůvěryhodných osob a při nedostatečném zabezpečení vzdáleného přístupu do firemní sítě pomocí VPN.

VPN (anglicky virtual private network) je prostředek pro propojení několika počítačů na různých místech internetu do jediné virtuální počítačové sítě. I když počítače mohou být v naprosto fyzicky nezávislých sítích na různých místech světa, prostřednictvím virtuální privátní sítě mezi sebou mohou komunikovat, jako by byly na jediném síťovém segmentu.

Prostřednictvím VPN lze zajistit například připojení firemních notebooků kdekoliv na internetu do firemního intranetu (vnitřní firemní sítě). K propojení je třeba VPN server, který má přístup na internet i intranet (může sloužit pouze pro jednoho klienta, nebo sloužit jako koncentrátor a přijímat spojení od více klientů), a VPN klient, který se přes

internet připojí k serveru a prostřednictvím něj pak do intranetu. VPN klient se instaluje jako aplikace na koncovou stanici. VPN server pak plní v podstatě funkci síťové brány.

Zobecněním VPN je síťové tunelování, kdy se prostřednictvím standardního síťového spojení vytvoří virtuální linka mezi dvěma počítači, v rámci které pak lze navázat další síťová spojení.

VPN (Virtual Private Network) pracuje jako bezpečné (autentizované a šifrované) a přitom pro uživatele zcela transparentní spojení mezi dvěma či více sítěmi. Pro spojení mezi uživatelem a požadovanou destinací použita veřejná síť - nejčastěji internet

Požadavky kladené na VPN spojení jsou zajištění integrity dat, nemožnost odposlechu a možnost se bezpečně připojit kdykoliv a kdekoliv nám to síť umožnuje.[12]

Výhody použití VPN spojení:

- Rozšíření hranic působnosti bez nutnosti budovat další síťovou infrastrukturu
- Značné úspory proti budování vlastních WAN sítí
- Dle zvoleného řešení zaručena bezpečnost
- Možnost být stále v kontaktu s daty v lokální síti
- Škálovatelnost (rozšiřitelnost) - možnost růstu úměrně potřebám

5.2.5 Ostatní rizika

Neoprávněný přístup do sítě, útok - patří mezi nejběžnější rizika, kdy se nám kdokoliv kdo přijde do firmy připojí ze svým PC do firemní sítě a má přístup k firemním zdrojům. Nebo se staneme cíleným útokem hackera, který nám ukradne vnitrofiremní data nebo stačí aby se kdokoliv připojil přes bezdrátovou WiFi do naší sítě a využíval zdarma připojení k internetu. Proti těmto rizikům se lze bránit striktním dodržováním bezpečnostní politiky firmy a po technické stránce zavedením nástrojů jako jsou NAC – omezení přístupu do sítě, šifrováním síťového prostředí(složek), zavedením řízení přístupu k síťovým prostředkům a složkám včetně lokálních kopií.

Viry, Spyware, Trojské koně, Rootkity, atd. – proti těmto nežádoucím aplikacím, které dokážou infikovat jednotlivý PC a následně celý IS a udělat zněj nástroj, který se otevře do internetu a ukáže vše co obsahuje nebo zahájí postupnou destrukci dat a operačního systému na něm uložených, lze se bránit účinnými nástroji. Nejlepší

obranou je korporátní řešení Antiviru, Antispyware, Antirootkitu, Firewallu a NAC(Network Admision Control), kde jsou definovány všechny politiky zabezpečení a automatických aktualizací podle předem nastavených schémat, které jsou součástí IS/IT strategie.

V**ada software** – je nahodilý jev,která může být způsoben lidským faktorem nebo chybou kód v software. Toto riziko dokážeme snížit zaměstnáním odborného pracovníka, který dokáže řešit tento druh problémů nebo že budeme mít uzavřenou servisní nebo outsourcingovou smlouvu na zprovoznění IS.

Vada hardware – je nahodilý jev, kterému nelze předcházet, ale dokážeme snížit riziko dopadu vadného zařízení, tím že budeme kritické prvky držet skladem, mít uzavřenou servisní nebo outsourcingovou smlouvu na výměnu zařízení nebo zprovoznění IS.

Krádež – krádeži dat v dobře zabezpečeném informačním systému lze v dnešní době předcházet, je potřeba dodržet všechna důležitá doporučení pro zabezpečení IS jako jsou fyzická bezpečnost, monitoring přístupu, zavedením řízení přístupu k datům, komplexním sledováním anomálii v systému, šifrováním, zálohováním, atd. Úroveň všech zabezpečení je přímo úměrná vloženým investicím, odbornostem správců IS a času věnovanému sledování a zabezpečení IS.

Poškození integrity dat v IS – Může být způsobeno, uživatelem úmyslně nebo neúmyslně, neoprávněnou osobou, závadou v IS nebo jiným způsobem. Tomuto riziku lze předcházet zálohováním, zavedením řízení přístupu, šifrováním, sledováním změn v IS zavedením systémů, které sledují chování uživatelů a vyhodnocují anomálie.

Nedostatek pracovníků – Nedostatek odborných pracovníků provést zásah na zařízení v informačním systému, které má vliv na jeho fungování, neodbornost správců a administrátorů IS. Tomuto riziku lze předcházet outsourcingem, servisní smlouvou a přenést toto riziko na subdodavatele, pokud je to z bezpečnostního hlediska možné.

Výpadek elektřiny – může mít na nás zásadní dopad pokud podnikáme v oblasti, kde má výpadek provozu informačního systému přímý vliv na business firmy (bankovnictví, letectví, výroba, dopravní systémy). Tomuto riziku lze předcházet záložními zdroji na baterie a následně na přepnutí na generátor.

Požár, přírodní katastrofa – jsou rizika, která nelze přímo ovlivnit, ale můžeme je zmírnit vhodným umístěním serverovny, záloho dat mimo objekt firmy, protipožárním systémem firmy, chováním lidí v krizových situacích, vytvořením havarijního plánu

5.3 Použité analýzy informačního systému

5.3.1 Analýza očekávaní a informačních potřeb důležitých „stakeholders“

Má-li být IS úspěšný, je nutno aby nebyl v rozporu se zájmy rozhodujících „stakeholders“. Pod pojem „stakeholders“ můžeme zahrnout následující skupiny, které patří do IS jako jsou zaměstnanci, zákazníci, vlastníci, management, zákazníci, dodavatelé, konkurenti, orgány statní zprávy a další. Znalost požadavků, očekávání a cílů těchto „stakeholders“ ve vztahu k upokojování informačních potřeb a jejich síly je pro návrh IS a jeho analýzu nezbytná, protože právě oni budou tvořit hodnotu IS, jeho obsah a udávat funkčnost a směr IS. Informační systém by měl být navrhován v souladu s očekáváním „stakeholders“, kdybychom ignorovali tyto zajmy nemusel by být IS úspěšný.

Analýza očekavání a uspokojování informačních potřeb pro „stakeholders je důležitou součastí komplexní analýzy, která slouží pro návrh IS a pro formulaci informační strategie. Tvoří jeden ze základních kamenů na kterých lze postavit IS.

Stakeholders a jejich požadavky

V následujících položkách jsou uvedení nejdůležitější „stakeholders“ a jejich očekávání.

Zaměstnanci

- Informace týkající se náplně jejich práce, jejího smyslu a přínosu ke společným cílům.
- Informace o možnostech osobního a profesního rozvoje.
- Stav firmy a její úspěchy, popř. neúspěchy, problémy, s jejichž řešením by mohli pomoci.
- Vyhlídky do budoucna s ohledem na jistotu vlastního zaměstnání.

Manažeři

- Informace potřebné pro jejich manažerská rozhodování o situaci na trhu, o stavu firmy, prostředí v němž se nachází, o výhledech do budoucna a o vývojových trendech.
- Informace o jejich zodpovědnosti, zákonech, normách a předpisech.
- Informace o možnostech profesního a kariérního růstu.

Vlastníci

- Informace o výsledcích hospodaření firmy, informace o tržní hodnotě firmy.
- Informaceo záměrech do budoucna.

Státní instituce a úřady

- Povinné informace pro úřady správy daní, zdravotního a sociálního pojištění.
- Informace týkající se bezpečnosti práce, životního prostředí.

Dodavatelé

- Specifikace objednávek a s tím související informace.
- Výhledy další spolupráce, předpoklad poptávky.

Zákazníci

- Informace o programech péče o zákazníka.
- Nabídka nových produktů, informace o účasti firmy na veletrzích a obdobných akcích.
- Informace vytvářející žádoucí image firmy a výrobku.

Konkurence

- Informace vedoucí k vytvoření žádoucího obrazu o firmě vzhledem k přijaté strategii.

Místní komunita

- Informace vytvářející příznivý obraz firmy v místním kontextu.

- Informace, které činí firmu atraktivní pro potenciální zaměstnance.

Odbory, ochránci životního prostředí, atd.

- Informace s preventivní působností proti případnému vměšování ze strany těchto a podobných organizací.[6]

5.3.2 Analýza stávající firemní kultury z hlediska zabezpečení firemního IS „7S“

Firemní kulturu má podobu psaných nebo nepsaných pravidel, která mají svůj původ v myšlení, chování všech důležitých stakeholders firmy. Je výsledkem působení vnitřních koordinačních sil i vlivů vnějšího prostředí. Jejich spolupůsobením se vytvářejí a upevňují pravidla, normy a postupy řešení vyskytujících se problémů, které se pak přenášejí různými formami i na nové členy organizace v procesu jejich adaptace. Proto můžeme firemní kulturu považovat za komplexní jev. Dále firemní kultura je identita firmy odrážející firemní hodnoty, názory a filozofii, prostředí v němž firma působí, charakter používaných technologií a výrobních postupů,neformální komunikaci a komunikační kanály, postoje vlastníků, managementu a řadových pracovníků ke kulturním a etickým hodnotám a společenské zodpovědnosti, image a důvěryhodnost, historii firmy, formality,a rituály a některé další aspekty. Mezi firemní kulturou, IS/IT strategii a IS musí být definován vztah.

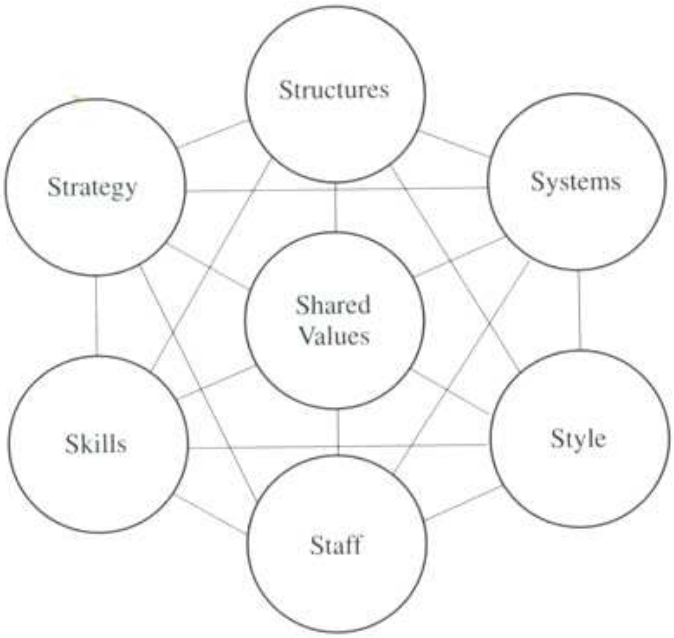
Analýza firemní kultury spočívá v kritickém zhodnocení současného vztahu a v návrhu pro firmu přínosných změn. Při analýze se uplatňují běžné metody a techniky průzkumu potřeb, postojů a názorů. Je potřeba zajistit aby fakta byla pravdivá a objektivní. Je doporučováno, aby průzkum dělala externí organizace nebo osoba nezávislá na firmě. Analýzu je potřeba zpracovat z pohledu formulace IS/IT strategie a zabezpečení IS.

Během samotné analýzy by měl být rovněž posouzen soulad přijaté IS/IT strategie organizace a firemní kultury. Pro tuto analýzu lze použit nástroj firmy McKinsey, tzv. model „7S“. Metodika tohoto nástroje nám zaručuje strategické řízení, organizaci, firemní kulturu a další rozhodující faktory pojímat a analyzovat v celistvosti, ve vzájemných vztazích a působení, tzn. systémově.

V tomto pojetí budeme pohlížet na každou organizaci jako na množinu sedmi základních faktorů (aspektů), které se vzájemně podmiňují, ovlivňují a ve svém souhrnu rozhodují o tom, jak bude vytyčená firemní, respektive IS/IT strategie naplněna.

Model „7S“ zahrnuje těchto 7 faktorů:

- Strategy (strategie)
- Structure (struktura)
- Systems (systémy řízení)
- Style (styl manažerské práce)
- Staff (spolupracovníci)
- Skills (schopnosti)
- Shared Values (sdílené hodnoty)



Obrázek 5: Model "7S" firmy McKinley
Zdroj: [4]

Obsah jednotlivých faktorů z hlediska pohledu IS a IS/IT strategie

Strategy (strategie) - Strategie IS a firmy nám udává koncepci filosofii IS a jeho soulad s business strategií, způsob jak provést materiální a finanční zabezpečení, systém rozvoje IS, bezpečnosta a ochranu IS a další strategické návaznosti.

Structure (struktura) - Je obsahově, funkční uspořádání organizace ve smyslu nadřízení a podřízení a spolupráce. Pod pojmem struktura jsou zahrnuty i kontrolní mechanismy a sdílení informací.

Systems (systémy řízení) - Jsou prostředky, procedury a systémy, které slouží řízení, např. komunikační, dopravní, informační a bezpečnostní.

Style (styl manažerské práce) – Je vyjádření toho jak management přistupuje k řízení a k řešení vyskytujících se problémům. Je potřeba si uvědomit rozdíl mezi formální a neformální (nepsanou) formou řízení.

Staff (spolupracovníci) – Se rozumí lidé, řídící a řadoví spolupracovníci, jejich vztahy, funkce, chování, motivace, loajalita a přístup k firmě. Je přitom nutné rozlišit mezi kvantifikovanými a nekvantifikovanými aspekty.

Skills (schopnosti) – Je míněna profesionální zdatnost celého pracovního kolektivu firmy jako celku. Je nunto brát v úvahu, kladné i záporné synergetické efekty dané kvalifikační strukturou pracovního kolektivu, úrovní organizace práce a řízením.

Shared Values (sdílené hodnoty) – Můžeme považovat za ideje, skutečnosti a principy respektované pracovníky a některými dalšími stakeholders firmy bezprostředně zainteresovanými na úspěchu firmy. V dobře fungujících firmách jsou základní sdílené hodnoty patřičným způsobem vyjádřeny v jejich misích.

5.3.3 Analýza rizik IS firmy

Analýza IS firmy slouží k odhadu ztrát, jež mohou vzniknout působením hrozeb na IS a dává přehled o stupni nezabezpečenosti jednotlivých hrozeb, slabých míst zranitelnosti a rizicích, jímž je hodnocený systém vystaven. Provedení analýzy rizik je klíčovým krokem při budování zabezpečeného IS. Bezpečnost nelze řešit komplexně, aniž je provedena analýza rizik IS. Cílem analýzy není provedení kontroly jednotlivých částí IS, ale zmapovat v jakém stavu se daný IS nachází a na základě zjištěných skutečností doporučit další postup.

Hrozby obvykle neexistují izolovaně, často se jedná o kombinace hrozeb, které představují riziko pro daný subjekt. Při provádění analýzy rizik je zapotřebí určit priority z pohledu dopadu a pravděpodobnosti jejich výskytu a zaměřit se na klíčové rizikové oblasti.

Nejčastěji uvažované hrozby pro firmu a IS

- Infiltrace neoprávněné osoby do IS, nepovolené užití aplikace
- Porucha počítače, serveru, hardwarového zařízení
- Porucha síťových služeb
- Porucha software
- Chyba uživatele IS
- Nedostatek pracovníků
- Výpadek dodávky elektřiny
- Porucha klimatizace
- Poškození vodou
- Poškození požárem
- Krádež
- Přírodní katastrofa (zemětřesení, vichřice, záplavy)
- Teroristická akce

Identifikace cílů hrozeb aktiv z hlediska pohledu částí IS:

- Informace
- Hardware
- Software
- Komunikační kanály
- Dokumentace
- Personál

Opatření pro zvládnutí rizik

Opatření zahrnují:

- aplikování vhodných opatření;

- vědomé a objektivní akceptování rizik za předpokladu, že naplňují politiku společnosti a kritéria pro akceptaci rizik;
- vyhnutí se rizikům; a
- přenesení rizik spojených s činností organizace na třetí strany, např. na pojišťovny, dodavatele.

Hodnocení rizik a opatření:

Samotná míra rizika pomocí vzorce:

$$R = (A * T * V) / 3,$$

kde: - R je míra rizika,

- A je hodnota aktiva,
- T je pravděpodobnost vzniku hrozby,
- V je zranitelnost daného aktiva.

5.3.4 SWOT analýza IS zaměřená na ochranu dat a rizik v IS

Při SWOT analýze IS se identifikují faktory a skutečnosti, které pro daný objekt analýzy představují jeho silné (Strenghts) a slabé (Weaknesses) stránky, příležitosti (Opportunities) a hrozby (Threats) v tomto případě zaměřené na ochranu dat a rizik v IS. Tytoklíčové faktory jsou potom zaznamenány, případně blíže charakterizovány a ohodnoceny ve čtyřech kvadrantech tabulky SWOT.

Fakta pro SWOT lze shromažďovat pomocí nejrůznějších technik, např.převzetím závěrů z dílčích analýz, porovnáním s konkurenty, metodou interview, řízené diskuse expertů. Analýza SWOT je zpravidla zpracovávána za účelem posouzení aktuálního stavu.[4]

Zásady pro zpracování SWOT

- SWOT analýza by měla být zpracována na konkrétní účel
- SWOT analýza by měla být zaměřená na podstatná fakta a jevy
- SWOT analýza je součástí strategické analýzy, pak by při ní měla být identifikována pouze strategická fakta.

- SWOT analýza by měla být objektivní a neměla by vyjadřovat jenom subjektivní názory zpracovatele
- Síla působení jednotlivých faktorů by měla být v tabulce SWOT, nějakým způsobem ohodnocena podle významu, např. bodově
- Jednotlivá fakta v tabulce SWOT by měla být identifikována nebo označena

5.4 Stanovení metrik pro jednotlivé analýzy

5.4.1 Metrika pro vyhodnocení analýzy očekávání „stakeholders“

Metrika pro vyhodnocení obsahuje vymezení skupin „stakeholders“ firmy dle kapitoly 5.3.1. a pro každou skupinu „stakeholders“ stanovujeme splnění úrovně očekávání od informačního systému firmy. Data získáváme pomocí interview, vyplněním dotazníků od všech skupin nebo „e-formuláři“. Úroveň očekávání skupin ohodnotíme číslem v rozsahu 0 – 9, kde 0 znamená nesplnění očekávání od IS a 9 znamená plné uspokojení očekávání (požadavků) na IS. V případě odpovědí ve skupině budeme brát výsledný průměr odpovědí skupiny. Následné hodnoty zobrazíme ve spojnicovém grafu, kde nám výsledný obrazec ukáže splnění očekávání od IS dle mezi jednotlivými skupinami „stakeholders“.

Metrika pro vyhodnocení zabezpečení informací dle jednotlivých skupin „stakeholders nám vypovídá o způsobu zabezpečení informací, omezení přístupu k informacím v IS. Čim více je skupina „stakeholders“ nežadoucí, riziková nebo má dopad na zneužití informací v IS tím více aplikujeme restrikce a omezení práce s daty. Vstupním údajem pro vyhodnocení je součet všech omezení, které jsou na danou skupinu aplikována a konkrétní data o skupině dodají správci jednotlivých dílčích částí IS. Metrika pro vyhodnocení je stanovena následovně:

Čím více jsou použity restrikce a omezení na skupinu, tím vyšší číslo v rozsahu 0 – 9 je použito a zaneseno do tabulky. Následně zaneseme údaje do stejného grafu jako v analýze očekávání stakeholders.

Výsledné zobrazení ve spojnicovém grafu nám zobrazuje míru očekávání stakeholders a zároveň míru omezení přístupu stejné skupiny k informacím a do informačního systému firmy.

5.4.2 Metrika vyhodnocení analýzy firemní kultury „7S“

Metrika pro vyhodnocení analýzy firemní kultury „7S“ ve vztahu k informačnímu systému obsahuje 7 kategorií definovaných analýzou „7S“ a v každé kategorii jsou definovány otázky s jednobodovou hodnotou z dané kategorie. Dotazníkovou metodou a analýzou firemního IS vyhodnotíme, zda na otázku můžeme odpovědět kladně, pokud ano přičteme do hodnocení kategorie 1 bod. Pokud při dotazníkové formě nebudeme mít jednoznačnou odpověď použijeme vyhodnocená, tak že při 80% a více kladných odpovědí přičteme bod.

Sečteme body za kategorii, a když získáme 2 nebo 3 body za kategorii můžeme považovat, že **informační systém je v dané kategorii v souladu s analyzovanou kategorií**.

Pokud je součet bodů za kategorii 0 nebo 1 bod můžeme konstatovat, že **informační systém není v souladu s danou analyzovanou kategorií.**

Metrika pro vyhodnocení analýzy „7S“ obsahuje následující kategorie a otázky:

- Strategy (strategie) – 3b
  - Firma má stanovenou a definovanou business strategii – 1b
  - Firma má stanovenou a definovanou IS/IT strategii – 1b
  - IS/IT strategie je v souladu s business strategií – 1b
- Structure (struktura) – 3b
  - Firma má definovanou firemní organizační strukturu – 1b
  - Firma má definované odpovědnosti za každou část IS – 1b
  - Firma provádí pravidelné audity, kontroly v předem stanovených cyklech – 1b
- Systems (systémy řízení) – 3b
  - Firma má zaveden účetní a CRM systém(popř.ERP) – 1b
  - Firma má stanovenou a aplikovanou bezpečnostní politiku řízení přístupu k informacím – 1b
  - Jsou přesně definované odpovědnosti za správu dílčích částí IS – 1b
- Style (styl manažerské práce) – 3b

- Management využívá aktivně výstupu dat z IS a pravidelně navrhuje změny úprav v IS – 1b
- Firma má plánovanou koncepci rozvoje IS která je v souladu s koncepcí rozvoje firmy – 1b
- Management pravidelně investuje v požadované výši do obnovy a údržby IS – 1b

- Staff (spolupracovníci) – 3b
  - Uživatelé jsou spokojeni s práci v IS, IS je uživatelsky přívětivý – 1b
  - IS umožňuje snadnou a rychlou dostupnost firemních informací uživatelům – 1b
  - IS zkracuje dobu potřebnou pro vykonání pracovního úkolu a tím i snižuje očekávaný pracovní čas zaměstnance a zvyšuje jeho produktivitu – 1b
- Skills (schopnosti) – 3b
  - Počítačová gramotnost uživatelů dostačuje k plnění jejich pracovních úkolů v IS – 1b
  - Uživatelé jsou uvědomělí při nakládání s firemními daty a minimalizují jejich zneužití – 1b
  - Zaměstnancům je umožněno vzdělávání v používání aplikací, které jsou součástí IS formou školení, e-lerningu nebo certifikací – 1b
- Shared Values (sdílené hodnoty) – 3b
  - IS usnadňuje možnost uživatelům jeho efektivního využívání pro teamovou práci – 1b
  - Systém obsahuje kontrolní mechanizmy mezi skupinami uživatelů, které zabezpečují dodržování firemních procesů – 1b
  - IS obsahuje inteligentní prvky, které se individuálně přizpůsobují jednotlivým uživatelům a usnadňuje jejich práci a tím snižuje pracovní čas pro vykonání pracovního úkolu – 1b

5.4.3 Metriky pro vyhodnocení analýzy rizik

Pro stanovení metrik pro hodnocení rizik byla zvolena upravená metodika *„Analýza rizik využívající matice aktiv, hrozeb a zranitelností“*.[9] Upravená metoda využívá čtyři matice (tabulky) nutné pro provedení postupu hodnocení.

Identifikace, ohodnocení aktiv a určení vlastníků (A) :

Prvním krokem je identifikace aktiv, ohodnocení dostupnosti, důvěrnosti a integrity aktiv. **Identifikovaná a evidovaná aktiva nesmí být vyjmuta z evidence bez schválení managera bezpečnosti informací.**

K ohodnocení byla použita následující empirická stupnice.

Tabulka 1: Stupnice hodnocení rizik

Stupnice hodnocení	
5	Velmi vysoká
4	Vysoká
3	Střední
2	Nízká
1	Zanedbatelná

Zdroj: vlastní

Hodnota aktiva je určena jako součin hodnocení dostupnosti, důvěrnosti a integrity tohoto aktiva. Význam hodnoty aktiva je rozdělen do čtyř úrovní dle následující tabulky:

Tabulka 2 : Význam hodnoty aktiva

Význam hodnoty aktiva		
65	**125**	**Vysoká**
28	**64**	**Střední**
9	**27**	**Malá**
1	**8**	**Zanedbatelná**

Zdroj: vlastní

Identifikace hrozeb a pravděpodobnost vzniku hrozby (T):

Druhým krokem je stanovení pravděpodobnosti vzniku hrozby. Pravděpodobnost je vyjádřena stejnou empirickou stupnicí hodnocení použité u 1. tabulky.

Míra zranitelnosti aktiv hrozbou (V):

Třetí krokem je stanovení míry zranitelnosti jednotlivých aktiv konkrétními hrozbami. Ne všechny buňky jsou v tabulce vyplněny. Tyto buňky zůstávají prázdné, protože mezi odpovídajícím aktivem a hrozbou není žádný vztah. Jinak řečeno aktivum není touto hrozbou zranitelné. Míra zranitelnosti je vyjádřena stojnou empirickou stupnicí hodnocení použité u 1. tabulky.

Hodnocení rizik a opatření:

Čtvrtým krokem se vypočítá samotná míra rizika pomocí vzorce:

$$R = (A * T * V) / 3,$$

kde:

- R je míra rizika,
- A je hodnota aktiva,
- T je pravděpodobnost vzniku hrozby,
- V je zranitelnost daného aktiva.

Tímto výpočtem dojde k naplnění následující tabulky. Ohodnocení rizika je určeno následující tabulkou:

Tabulka 3 : Ohodnoceni rizika

Ohodnocení rizika (dopad):		
534	1042	Vysoké riziko
226	533	Střední riziko
68	225	Malé riziko
1	67	Nevýznamné riziko

Zdroj: vlastní

6 Současny stav řešené problematiky

6.1 Informace o analyzované firmě

Společnost TECH4SEC, spol.s.r.o. je systémový integrátor poskytující svým zákazníkům kompletní zajištění implementace a dodávky od úvodní analýzy problémů přes projekční činnosti, realizace dodávek systémů, až po zaškolení obsluhy a následné servisní služby.

Společnost TECH4SEC, spol.s.r.o. se od svého počátku profilovala jako firma se zaměřením na služby spojené s budováním komunikačních infrastruktur zejména v oblasti metalických a optických sítí LAN, značkových aktivních technologií včetně jejich správy a diagnostiky. Dnes, po devíti letech působení TECH4SEC, spol.s.r.o. na českém trhu lze říci, že patří k lídrům v oboru komunikačních technologií.

Společnost TECH4SEC, spol.s.r.o. je díky strategickému řízení moderní organizací s pevným postavením na tuzemském trhu. Dobře víme, že moderní společnost musí být plně orientována na potřeby zákazníka za dodržování zásad řízení jakosti a procesů uvnitř společnosti, které zabezpečují neustále se zlepšující kvalitu a efektivitu poskytovaných služeb.

Společnost byla založena v roce 1997 a za dobu své existence prošla cestou, která odráží rychlý vývoj trhu ICT v posledních deseti letech.

Díky správnému pochopení zákonitostí tohoto vývoje managementem firmy se na našem trhu rychle prosadila. Už ve druhém roce své existence postoupila podle hodnocení společnosti Deloitte & Touche mezi 50 nejdynamičtěji se rozvíjejících firem v regionu Moravy.

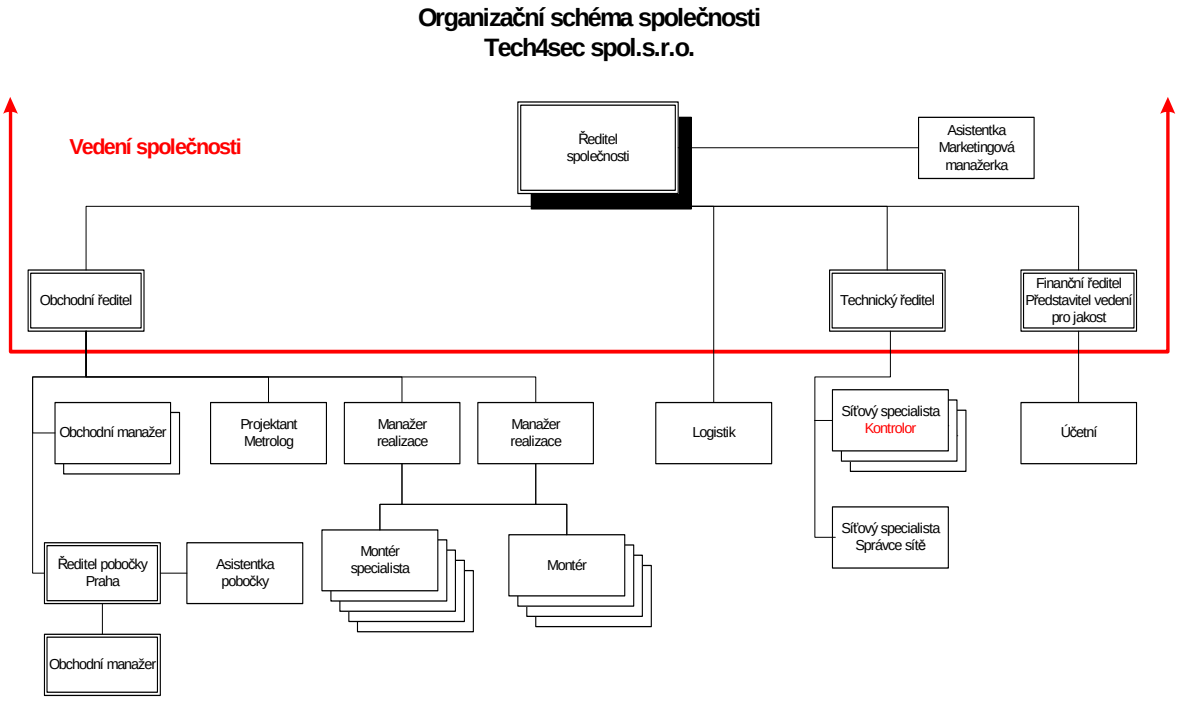
Dynamičnost jejího rozvoje dosvědčí fakt, že už během prvních dvou let svého působení na českém trhu se zařadila mezi přední společnosti v oblasti telekomunikací s pravidelným obratem přes 200 mil. Kč. Díky neustálému rozvoji dosahuje v současnosti roční obrat převyšující 150 mil. Kč.

Je to dáno i tím, že se od počátku orientovala především na potřeby zákazníka a zároveň vysokou kvalitu nabízených služeb, která vychází ze stále rostoucí odbornosti zaměstnanců, jak z obchodními, tak technickými zkušenostmi.

V rámci strategického řízení začala společnost TECH4SEC, s.r.o. poskytovat další služby v oblasti telekomunikací a dodávek slaboproudých technologií. V následujících

Obrázek 6: Organizační struktura společnosti

letech úspěšného rozvoje firma rozšířila portfolio svých služeb zejména v oboru



projektování, systémové integrace (slaboproudých technologií), outsourcingu a nabídky dalších ICT technologií, především pak bezpečnosti na bázi produktů UTIMACO a technologií MICROSOFT.

Zdroj: firemní interní směrnice

Oblast působení firmy

Po produktové a technologické stránce se společnost soustřeďuje na renomované značky v každé oblasti.

O oblasti **aktivních síťových technologií** produkty CISCO, 3COM, Hewlett-Packard, Nortel Network, včetně zabezpečení návrhů, analýz a instalací na těchto technologiích prostřednictvím vlastních certifikovaných pracovníků se zkušenostmi z praxe.

V oblasti **bezpečnosti** se pak společnost profiluje tvorbou bezpečnostních analýz a komplexních návrhů bezpečnosti od průmyslové EZS, EPS, CCTV, a po datovou šifrování a zabezpečení přístupu na bázi produktů UTIMACO a MICROSOFT.

V oblasti **metalických a optických systémů LAN a WAN** s společnost zaměřuje na systémy TYCO-AMP a SCHRACK.

V rámci **systémové integrace** slaboproudých technologií pak společnost nabízí dodávky a instalace systémů EZS, EPS, CCTV, rozvodů elektro do 1000V, budování serveroven včetně dodávek docházkových a přístupových systémů.

Další služby poskytované zákazníkům

Pro všechny dodávané technologie dále poskytujeme následující služby:

- **technické konzultace** – jsme schopni poradit zákazníkům v základních otázkách a napomoci mu k orientaci v problematice datových komunikací,
- **projektové poradenství** – zpracováváme oponentní posudky a vedeme oponentní řízení na již zpracované projekty,
- **služby hot line** – pomáhají zákazníkům s řešením aktuálních, konkrétních problémů,
- **přímá servisní podpora zákazníkům** – jak ve formě servisního zásahu přímo na místě nebo tzv. dálkovým dohledem – připojením do jeho datové sítě;

SWOT analýza
Silné a slabé stránky společnosti TECH4SEC - shrnutí stávajícího stavu

Tabulka 4: SWOT analýza firmy

S - silné stránky	W - slabé stránky
- Stabilní vlastnická struktura - Finanční stabilita - Dobrý management - Široké portfolio produktů - Používání a zavádění nejmodernějších technologií - Vysoká úroveň znalostí a zkušeností - Reference renomovaných firem - Vysoká kvalita poskytovaných služeb za dostupné ceny - Znalost českého prostředí a trendů - Servisní zázemí - Obecně fungující povědomost o	- Pokles státních zakázek kvůli úsporám ve veřejných financí - Nedostatek investic pro podstatně rychlejší zavádění nových technologií - Úzký obchodní tým - absence koncepce rozvoje společnosti - schází důsledné prosazování jednotných představ pro úspěšnost, není vidět za horizont, - slabá mediální podpora - podcenění příchodu nových spolupracovníků a jejich pohledu na věc - Neztotožňovaní se s cíli společnosti jak

zaměření společnosti - Určitý podíl na trhu - Technické zázemí - Odborná znalost	krátkodobých tak dlouhodobých - Slabší obchodní oddělení
O – příležitosti	**T – hrozby**
- Stálí zákazníci - Noví zákazníci - Hospodářský růst ČR - Reforma státního sektoru a školství - Pokračování zahraničních investic v ČR - Noví zákazníci - Vznikající technologie - Strategické aliance - Rozšíření obchodního týmu - Požadavek trhu na outsourcing IT služeb - Požadavek zákazníků na větší bezpečnost - Větší objem přenášených dat - Mezinárodní terorismus - Vstup na nové trhy - urychlené zabezpečení základních zdrojů a finanční jistoty - analýza potřeb a možností stávajícího týmu - přesná definice úkolů a kontrola jejich plnění	- Politické změny - Znalost trhu - Vstup nových firem - Ztráta části zákazníků - Lidské zdroje - zkušenost pracovníků, fluktuace, atd… - Nutnost další certifikace "ISO" - Nehodná strategie - Cash flow - Nízká vymahatelnost práva - Omezení trhu předpisy EU - Sílící kurz koruny - Přírodní pohromy - Vstup asijských firem na trh ČR - Vliv globalizace - nedostatek důvěry spolupracovníků - nedostatek finančních příjmů - destabilizace společnosti

Zdroj: Vlastní

Jako vždy se při projednání týmu projevovala určitá neochota odkrýt slabé stránky firmy, nicméně výsledná tabulka SWOT vyjadřuje relativně dobře situaci ve firmě.

Zarážející byl konstatovaný nezájem o vzdělávání a získávání nových technologií a slabé provázání marketingu s obchodem. Jako vždy členové týmu vyjadřovali pocit, že jsou v porovnání s jinými firmami málo motivováni.

6.2 Současné zabezpečení IS

Fyzická bezpečnost

Firma využívá zděné pronajaté prostory, sídlo má v nadzemním podlaží, okna do serverovny jsou chráněna mříží, přístupová cesta obsahuje 2 dveře s bezpečnostními zámky a za posledními dveřmi je mříž. Celý prostor je napojen na EZS s připojením na centrální pult.

Požární bezpečnost

S požárního hlediska lze firmu klasifikovat jako standardní kancelářské prostory bez senzorů na požár. Ve firemních prostorech jsou rozmístěny a označeny kontrolované hasící přístroje.

Přistup ke zdrojům dat

Ve firmě je aplikována politika uživatelského hesla do všech aplikací a uživatel je zařazen do skupiny dle jeho pozice. Každá skupina má předem nadefinované přístupy do sdílených dokumentů dle oprávnění a ostatních aplikací. V systému CRM má přístup jen dle oprávnění skupiny.

Zabezpečení pracovního PC

Každý zaměstnanec má osobní počítač zabezpečen heslem do operačního systému. Na každém PC je nainstalováno šifrování disku, emailové komunikace (příloh) a zapnuto šifrování všech připojených médií. Někteří uživatelé využívají biometrické přihlášení prstem. Lokalní replika systému CRM, vyžaduje při každém spuštění zadání přihlašovacích údajů.Každý PC má nainstalován firewall, antivir, NAC, antispyware a antirootkit řešení, které je propojeno s centrální správou firmy.

Zabezpečení serveru a sítě

Počítačová síť je chráněna z vnější strany (z internetu): 2 firewally 1x HW firewall, kde se nastavují pravidla pro celou síť, 1xSW uživatelský firewall, kde jsou definovány omezení, kde skupiny kam uživatel spadá. Dále je v cestě do internetu WEB gateway pro kontrolu obsahu, email gateway, která slouží jako spam filtr.

Ve vnitřní síti nejsou definována, téměř žádná omezení.

Technická zdatnost zaměstnanců

Většina technických zaměstnanců jsou profesionálové z oblasti IT, kterým nedělá používání IS žádný problém. Ostatní zaměstnanci z oblasti obchodu, vedení a logistiky využívají IS bez problémů.

Zálohováni

Zálohování všech dat je prováděno pouze na serverech, uživatelé mají povinnost všechna firemní data z lokálních PC ukládat do IS na serveru. Servery jsou pravidelně zálohovány duplicitně 2x na pásku. Jedna kopie pásek je ukládána mimo firemní prostory u vedení společnosti.

Směrnice, bezpečnostní strategie a krizové plány

Firma má definovány směrnice pro využívání IS, návod a dokumentaci pro uživatele IS, má vypracované dokumenty pro bezpečnostní politiky částí IS, má vypracovaný krizový plán včetně řešení krizových situací.

6.3 Současná IS/IT strategie firmy

6.3.1 Firemní strategie

Firma má zpracovanou firemní strategii, která byla vytvořena na základě vize a cílů firmy, které jsou rozepsány níže.

Cíle strategie

- Maximalizace výnosnosti kapitálu ve střednědobém a dlouhodobém výhledu
- Maximální orientace na zákazníka
- Efektivita veškerých procesů se zaměřením na čas a náklady
- Poskytnutí vyšší přidané hodnoty zákazníkům
- Stanovení mise spol.TECH4SEC

Pro vnitřní komunikaci mezi pracovníky společnosti zásadní motto

„Krok před konkurencí – krok k zákazníkovi“.

Směrem k okolnímu prostředí se spol.TECH4SEC prezentuje misí

„… komunikace mezi námi“.

K dosažení cílů v rámci změn okolí a růstu společnosti jsou nutné změny v oblastech:

- Organizační struktury
- Přístupu k zákazníkům

- Volbě technologií
- Procesů
- Kontroly
- Zavádění nových technologií
- Zvyšování podílu na trhu
- Plánování
- Rozvoj vzdělávání a inovací

6.3.2 Stanovení vize společnosti

Společnost TECH4SEC, s. r. o. je českou společností, která působí v oblasti budování síťových komunikačních infrastruktur, bezpečnostních a signalizačních systémů. Naše služby budeme poskytovat na území České republiky zákazníkům z oblasti průmyslu, státní správy, zdravotnictví, školství a služeb.

Soustřeďuje se výhradně na značková řešení předních světových výrobců, zejména Hewlett-Packard, Nortel Network, 3Com, Avaya, Netgear, Microsoft, DELL, Utimaco, APC, Allied Telesyn, MICROSOFT, IMC, Proxim, Cisco, AMP Netconnect, Schrack. Díky strategickým spojením s řadou z nich disponuje vysokými odbornými znalostmi v oblasti nabízených technologií a jsme schopni garantovat maximální funkčnost a špičkovou kvalitu všech projektů a tím i záruku vložených investic.

Díky těmto předpokladům je společnost zákazníkům schopna poskytovat maximální podporu, a sice od úvodní analýzy problematiky přes projekční činnosti, realizace dodávek systémů, až po zaškolení obsluhy a následné servisní služby (přímá servisní podpora na místě nebo dálkovým připojením, služby hot-line, technické konzultace) v následujících oblastech :

- Cisco, Microsoft, UTIMACO, bezpečnost
- aktivní technologie 3COM, Hewlett Packard, Avaya, Nortel Networks
- komunikační infrastruktury (metalické a optické kabeláž, wireless, …)
- Outsourcing, pobočka Ostrava, systémová integrace, komplexní řešení
- EZS, EPS, CCTV, bezpečnostní systémy
- projekce (projektování slaboproudých systémů v různých stupních dokumentace)

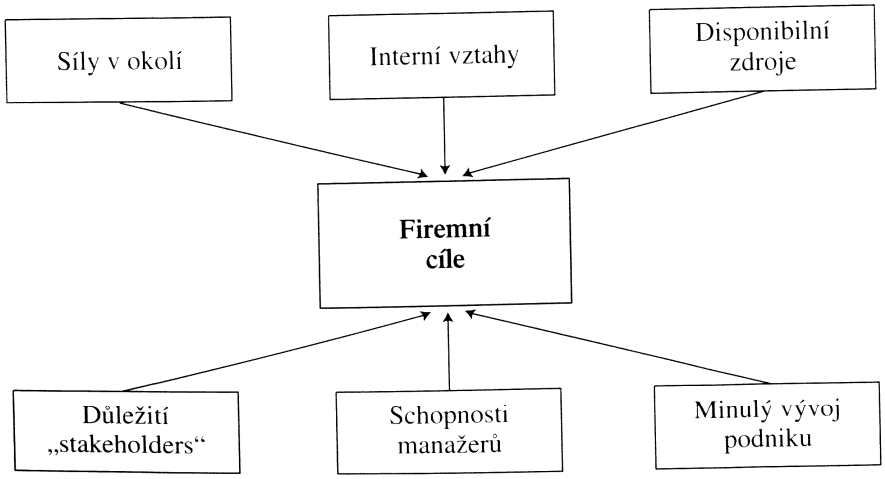
Společnost bude každodenně usilovat o to, aby její zákazníci byli díky poskytovaným službám a řešením zákazníky spokojenými. Toho chce dosáhnout přístupem pracovníků na všech úrovních jejich úctou, vstřícností, rychlostí, spolehlivostí a kvalifikovanými odbornými znalostmi.

Společnost tvoří vysoce výkonný tým, který tvoří odborníci a profesionálové. Práce v takovém týmu je založena na osobním přístupu a důvěře v to, že všem jde o špičkový výsledek. Snahou každého je pak i neustálé zlepšování, motivace a sebeinspirace.

Tyto zásady bude společnost uplatňovat tak, abych mohla svým zákazníkům přinášet špičková moderní řešení jejich potřeb - současných i budoucích.

6.3.3 Stanovení cílů společnosti

Cíle společnosti vycházejí z následujícího schématu:



Obrázek 7: Firemní cíle
Zdroj:[2]

Krátkodobé cíle do 6 měsíců

- stabilizace chodu společnosti, v oblasti obchodu
- zlepšení nastartování příjmů s ohledem na způsob financování a zvýšení obratu společnosti jak v oblasti dodávek, tak především služeb včetně přenosu těchto požadavků mezi všechny spolupracovníky
- plnění cílů společnosti, které je potřeba zaměřit na dvě hlavní věci a to obchod a úpravou vnitřních procesů, snížení provozních nákladů společnosti, hlavně v části vozového parku.
- nastartovat růst příjmů, vypracování reálných obchodních plánů a realizací min. 2 zakázek nad 10 mil. Kč
- přehodnocení způsobu obchodního oddělení včetně odměňování
- stabilizace a max. vytěžení stávajících projektů v oblasti služeb
- zabezpečení stabilních příjmů na pokrytí finančních potřeb společnosti a plnění úkolů stanovených koncepcí rozvoje
- zpracování střednědobé koncepce rozvoje společnosti
- zavedení ISO 14 000
- vytvoření bezpečnostní politiky společnosti

Střednědobé cíle 6-18 měsíců:

- Rozšíření povědomosti o záměrech společnosti mezi všechny spolupracovníky (ztotožnění se)
- Stabilizace a maximální zhodnocení všech stávajících projektů
- Hledání optimálních projektů, které mohou zahrnovat služby
- Získání dlouhodobých partnerství
- Zvýšit obrat na službách na 15 mil/rok, min. však 10mil.
- Obrat přes 100 mil.Kč

Dlouhodobé cíle

- Získání výraznějšího podílu na trhu u větších zákazníků
- Zabezpečení mediálního povědomí

- Přehodnocení nákladových položek společnosti se záměrem jejich snižování

6.3.4 IS/IT strategie firmy

Při tvorbě strategie firmy se rovněž projevily značné nedostatky vnitrofiremní komunikace. Tyto problémy by měly být řešeny v rámci implementace strategie přechodem na novou organizaci firmy. Dále byla konstatována slabá sounáležitost se strategickými cíli firmy a celkový slabý zájem o strategii firmy.

IS/IT strategie firmy byla tvořena na základě firemní strategie firmy, tak aby dokázala korespondovat s cíly firmy. Mezi hlavní cíle IS/IT strategie patří:

- Zavedení nového systému CRM, tak aby korespondoval se stávajícími a plánovanými procesy a toky informací a dat ve firmě.
- Zvýšit zabezpečení firemních dat a zavést ISO 27000.
- Průběžně zvyšovat kvalifikaci odborných pracovníků a získat vyšší stupeň partnerství a specializaci u společností CISCO, MICROSOFT, VMWARE a UTIMACO.

7 Analýza problému

7.1 Analýza „stakeholders“

Analýza očekávání požadavků na IS od skupin „stakeholders“ jsem prováděl pomocí interview, dotazníků, webových anket, formulářů s každou skupinou, která je součástí informačního systému. Hodnota splnění očekávání byla stanovena na základě metrik uvedených v kapitole 5.4.1. Čím větší číslo, tím většího očekávání bylo dosaženo.

Míra zabezpečení informačního systému vůči skupinám „stakeholders“ nám stanovuje, jak je informační systém zabezpečen vůči dané skupině, tzn. jaký má daná skupina přístup k informacím v informačním systému. Čím větší je hodnota zabezpečení pro danou skupinu, tím má menší přístup k informacím daná skupina „stakeholders“. Příkladem tohoto zabezpečení je že zaměstnanci nemají plný přístup k účetním informacím i když je IS jimi disponuje.

Úroveň zabezpečení IS definujeme organizačně interní směrnicí, bezpečnostními politikami a vnitrofiremními procesy. Úroveň zabezpečení IS z technického hlediska nastavuje administrátor nebo správce na základě interních směrnic, bezpečnostních politik firmy a procesů firmy, které odsouhlasilo vedení společnosti. Technické prostředky zabezpečení jsou uvedeny v kapitole 5.2.

Splnění očekávání skupin „stakeholders“ od informačního systému a úrovně zabezpečení jednotlivých skupin najdeme v následující tabulce.

Tabulka 5: Stakeholders a jejich požadavky
Zdroj: vlastní výpočet

Stakeholders a jejich požadavky	Splnění očekávání "stakeholders" od IS	Míra zabezpečení IS vůči "stakeholders"
Zaměstnanci	6	4
Manažeři	7	2
Vlastníci	8	1
Státní instituce a úřady	5	7
Dodavatelé	5	5
Zákazníci	7	5
Konkurence	2	9
Místní komunita	4	8
Odbory, ochránci životního prostředí, atd.	7	9

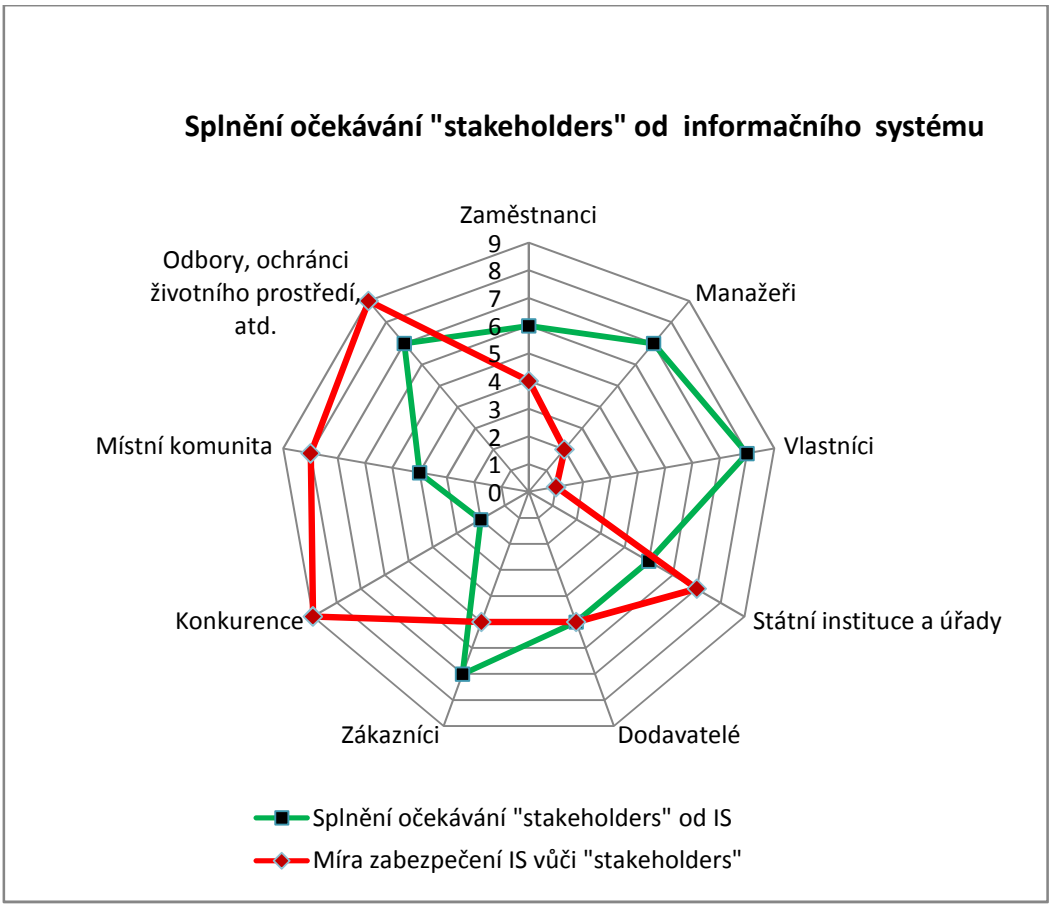
Po vynesení obou hodnot do spojnicového grafu můžeme konstatovat následující závěry vyplývající z této analýzy:

Informační systém koresponduje s očekáváním vlastníků, manažerů, zákazníků, odborů a splnil očekávání jejich potřeb. Tyto skupiny uživatelů mají pozitivní přístup při práci s IS.

Pro skupinu zaměstnanci, dodavatelé, statní instituce a úřady je systém nastaven, tak aby jim poskytoval jen to nejnutnější, co potřebují k práci a jen ty výstupy informací, které jsou nezbytně nutné pro jejich pracovní činnosti. Z tohoto důvodu tyto skupiny hodnotí IS jako průměrný.

Pro skupiny konkurence a místní komunita je IS nastaven tak, aby byl minimalizován výstup informací z IS.

Když vyhodnotíme zabezpečení skupin „stakeholders“ IS firmy můžeme konstatovat, že zabezpečení je nastaveno, tak aby se eliminovalo zneužití informací v IS.



Obrázek 8: Graf - splnění očekávání "stakeholders"
Zdroj: vlastní výpočet

7.2 Analýza firemní kultury „7S“ ve vztahu k IS

Na základě všech dostupných informací o firmě, byla aplikovaná metrika na jednotlivé oblasti firemní kultury, zda korespondují s využíváním IS firmy. Po zodpovězení všech otázek bylo zjištěno, že firma má 2 slabá místa v oblastech „Staff“ a „Style“.

V oblasti „Staff“ je to způsobeno tím, že práce s IS je zdlouhavá a zaměstnanec musí vyplňovat stejná vstupní data do více aplikací, formulářů. A dalším problémem je přílišné reportování managementu a množství procesů, což zaměstnancům odebírá pracovní čas, který by mohli věnovat produktivnějším úkolům.

V oblasti „Style“ jsou 2 slabiny a to:

- Management řeší v IS jen operativní změny a nemá vytvořen, dlouhodobý plán rozvoje IS.

- Management nevyužívá všechny výstupy z IS v plné míře ke svému rozhodování, ale při tom jsou ve firemních procesech nastaveny a zaměstnanci musí tyto vstupy do systému zadávat, tím dochází k neefektivnosti využívaní času zaměstnance.

Výsledky tabulky jsou uvedeny v následující tabulce.

Tabulka 6 : Analýza firemní kultury ve vztahu k IS "7S"

Oblasti analýzy 7S	Výsledek	Body
Strategy (strategie)	V SOULADU	3
Firma má stanovenou a definovanou business strategii	ANO	1
Firma má stanovenou a definovanou IS/IT strategii	ANO	1
IS/IT strategie je v souladu s business strategií	ANO	1
Structure (struktura)	V SOULADU	3
Firma má definovanou firemní organizační strukturu	ANO	1
Firma má definované odpovědnosti za každou část IS	ANO	1
Firma provádí pravidelné audity, kontroly v předem stanovených cyklech	ANO	1
Systems (systémy řízení)	V SOULADU	3
Firma má zaveden účetní a CRM systém(popř.ERP)	ANO	1
Firma má stanovenou a aplikovanou bezpečnostní politiku řízení přístupu k informacím	ANO	1
Jsou přesně definované odpovědnosti za správu dílčích částí IS	ANO	1
Style (styl manažerské práce)	NENÍ V SOULADU	1
Management využívá aktivně výstupu dat z IS a pravidelně navrhuje změny úprav v IS	NE	0
Firma má plánovanou koncepci rozvoje IS, která je v souladu s koncepcí rozvoje firmy	NE	0
Management pravidelně investuje v požadované výši do obnovy a údržby IS	ANO	1
Staff (spolupracovníci)	NENÍ V SOULADU	1
Uživatelé jsou spokojeni s práci v IS, IS je uživatelsky přívětivý	NE	0
IS umožňuje snadnou a rychlou dostupnost firemních informací uživatelům	ANO	1
IS zkracuje dobu potřebnou pro vykonání pracovního úkolu a tím i snižuje očekávaný pracovní čas zaměstnance a zvyšuje jeho produktivitu	NE	0
Skills (schopnosti)	V SOULADU	2
Počítačová gramotnost uživatelů dostačuje k plnění jejich pracovních úkolů v IS	ANO	1
Uživatelé jsou uvědomělí při nakládání s firemními daty a minimalizují jejich zneužití	ANO	1
Zaměstnancům je umožněno vzdělávání v používání aplikací, které jsou součástí IS formou školení, elearningu nebo certifikací	NE	0

Shared Values (sdílené hodnoty)	V SOULADU	2
IS usnadňuje možnost uživatelům jeho efektivního využívání pro teamovou práci	ANO	1
Systém obsahuje kontrolní mechanizmy mezi skupinami uživatelů, které zabezpečují dodržování firemních procesů	ANO	1
IS obsahuje inteligentní prvky, které se individuálně přizpůsobují jednotlivým uživatelům a usnadňuje jejich práci a tím snižuje pracovní čas pro vykonání pracovního úkolu	NE	0

Zdroj: vlastní výpočet

7.3 Analýza rizik

Analýza rizik byla zpracována v souladu s využitím norem ISO 17999, ISO 27001 a aplikací ISMS (Information Security Management Systém/**Systém řízení bezpečnosti informací**) a využívá všech matic aktiv, hrozeb a zranitelností uvedených v těchto normách.

Analýza obsahuje tyto tabulky:

- Identifikace, ohodnocení aktiv a určení vlastníků
- Identifikace hrozeb a pravděpodobnost vzniku hrozby
- Míra zranitelnosti aktiv hrozbou
- Hodnocení rizik a opatření

7.3.1 Identifikace, ohodnocení aktiv a určení vlastníků

Tabulka obsahuje vyhodnocení dostupnosti, důvěrnosti, integrity aktiv a vypočítává součinem hodnotu aktiva.
Pro hodnocení aktiva se využívá hodnocení dle následující tabulky č.X a v tabulce č. Y. máme úrovně, které určují celkovou význam hodnoty aktiva:

Tabulka 7: Stupnice hodnocení rizika aktiva

Stupnice hodnocení	
5	Velmi vysoká
4	Vysoká
3	Střední
2	Nízká
1	Zanedbatelná

Tabulka 8: Význam hodnoty aktiva

Význam hodnoty aktiva		
65	**125**	**Vysoká**
28	**64**	**Střední**
9	**27**	**Malá**
1	**8**	**Zanedbatelná**

Zdroj: vlastní výpočet

Tabulka 9 : Identifikace, ohodnocení aktiv a určení vlastníků

Název aktiva	Dostupnost	Důvěrnost	Integrita	Hodnota aktiva	Vlastník aktiva
Nehmotná informační aktiva					
Elektronicka pošta - údaje o poptávky, nabídky, objednávky	4	4	5	**80**	Obchodníci/ prodejci
Skladovací systém - údaje	4	5	5	**100**	Logistik
Účetní systém - údaje	4	5	5	**100**	Účetní
Nehmotná softwarová aktiva					
Operační systém Windows Server	5	5	5	**125**	administrátor
Operační systém Windows XP - PC	4	4	4	**64**	uživatel
SW Antivirová ochrana PC, server, Smart phone	3	3	3	**27**	uživatel
NAVISION	5	5	5	**125**	administrátor
Firewallová ochrana PC	3	2	3	**18**	uživatel
Webmaster (www stránky)	3	2	2	**12**	administrátor
Ostatní evidovaný SW	2	2	4	**16**	administrátor
MS Office	4	2	2	**16**	uživatel
Hmotné aktiva					
Servery	5	5	5	**125**	administrátor
NAVISION - server	5	5	5	**125**	administrátor
Firewallová ochrana serverů	4	4	4	**64**	administrátor
Server el. pošta (tř. kpt. Jaroše)	4	4	4	**64**	administrátor
EZS	3	1	3	**9**	MBI (LARN)
Síťové prvky	5	3	3	**45**	administrátor
Přenosná výpočetní technika	5	5	4	**100**	uživatel
Pracovní stanice PC	4	5	4	**80**	uživatel
Ostatní hardware (tiskárny, scaner ..)	3	1	2	**6**	administrátor
Externí HDD, datová media	3	5	4	**60**	administrátor
MS Exchange	4	4	4	**64**	administrátor

Aktiva - externí služby					
Připojení do sítě Internet a ostatní služby, SW+HW	4	3	2	**24**	SkyNet
Dodávka elektrické energie	4	3	3	**36**	Reko
Dodávka ostatních energií	4	3	3	**36**	Reko
Poštovní služby - dopravci	2	2	2	**8**	PPL
Webhosting, WWW stránky	2	3	3	**18**	administrátor

Zdroj: vlastní

7.3.2 Identifikace hrozeb a pravděpodobnost vzniku hrozby

Následující tabulka nám určuje pravděpodobnost vzniku hrozby pro dané aktivum.

Tabulka 10: Identifikace hrozeb a pravděpodobnost vzniku hrozby

Identifikace hrozby:	předstírání identity uživatele	použití softwaru neautorizovanými uživateli	zneužití privilegií – použití SW neautorizovaným způsobem	popření (anonymita prováděných	prozrazení dat během přenosu	prozrazení dat na paměťovém mediu	modifikace dat na paměťovém mediu	modifikace dat v databázi	modifikace dat při přenosu	technické selhání síťových	selhání hardware	poškození paměťového media	zemětřesení	povodeň a voda z potrubí	požár	selhání dodávky energie	selhání klimatizace	krádež, násilný trestný čin	škodlivý software (viry, trojské koně)
Nehmotná informační aktiva	H1	H2	H3	H4	H5	H6	H7	H8	H9	H11	H11	H12	H13	H14	H15	H16	H17	H18	H19
Elektronicka pošta - údaje o poptávky, nabídky, objednávky	3	3	3	2	4	3	3	2	3	2	2	1	1	1	2	1	1	3	3
Skladovací systém - údaje	3	3	4	2	3	2	1	2	2	2	2	2	1	1	2	1	1	4	2
Účetní systém - údaje	3	3	4	2	3	2	1	2	2	2	2	2	1	1	2	1	1	4	2
Operační systém Windows Server	H1	H2	H3	H4	H5	H6	H7	H8	H9	H11	H11	H12	H13	H14	H15	H16	H17	H18	H19
Operační systém Windows 2003 Server	3	2	2	2	2	2	2	2	2	2	2	2	1	1	2	1	1	1	3
Operační systém Windows XP - PC	3	3	3	3	2	2	2	3	3	3	3	2	1	1	2	1	1	1	4
SW Antivirová ochrana PC, server,	1	1	2	1	2	1	1	1	1	1	1	1	1	1	2	1	1	1	3
NAVISION	3	2	2	2	2	3	3	2	2	2	2	2	1	1	2	1	1	1	3
Firewallová ochrana PC	1	1	2	1	2	1	1	1	1	1	1	1	1	1	2	1	1	1	3
Webmaster (www stránky)	2	2	2	2	2	2	2	2	2	2	2	2	1	1	2	1	1	1	3
Ostatní evidovaný SW	1	1	1	1	2	1	3	2	1	1	1	1	1	1	2	1	1	1	2
MS Office	1	2	2	3	2	3	4	3	2	1	1	1	1	1	2	1	1	1	3
Servery	H1	H2	H3	H4	H5	H6	H7	H8	H9	H11	H11	H12	H13	H14	H15	H16	H17	H18	H19
Servery	3	2	2	3	3	2	2	3	2	2	2	2	1	1	2	2	2	2	2
NAVISION – server	3	2	2	3	1	2	2	3	2	2	2	2	1	1	2	2	2	2	2
Firewallová ochrana serverů	2	2	2	2	1	1	1	1	1	2	2	2	1	1	2	2	2	1	2
Server el. pošta	2	2	3	2	1	1	1	1	1	2	2	2	1	1	2	2	2	2	3
EZS	2	1	1	1	1	1	1	1	1	2	2	2	1	1	2	2	2	2	1
Síťové prvky	2	2	2	2	1	1	1	2	1	2	2	2	1	1	2	2	2	2	1

Přenosná výpočetní technika	3	4	3	2	2	2	2	2	1	3	3	2	1	1	2	2	1	4	3
Pracovní stanice PC	3	3	2	2	2	2	2	2	2	2	2	2	1	1	2	2	1	2	2
Ostatní hardware (tiskárny, scaner ..)	2	2	1	2	2	1	1	1	1	2	2	1	1	1	2	2	1	2	1
Externí HDD, datová media	1	2	1	2	2	3	3	1	1	1	2	2	1	1	2	2	1	4	3
MS Exchange	1	2	1	2	1	1	1	1	1	3	2	2	1	1	2	2	2	2	3
Aktiva - externí služby	H1	H2	H3	H4	H5	H6	H7	H8	H9	H11	H11	H12	H13	H14	H15	H16	H17	H18	H19
Připojení do sítě Internet a ostatní služby, sw + hw	2	2	2	1	1	1	1	1	2	2	2	1	1	1	2	2	2	3	1
Dodávka elektrické energie	1	1	1	1	1	1	1	1	1	2	2	1	1	2	2	2	1	1	1
Dodávka ostatních energií	1	1	1	1	1	1	1	1	1	2	2	1	1	1	2	2	1	1	1
Poštovní služby - dopravci	1	1	1	1	1	1	1	1	1	1	2	1	1	2	2	1	1	2	1
Webhosting, WWW stránky	1	1	1	1	1	1	1	1	1	2	3	2	1	1	2	2	1	2	2

7.3.3 Míra zranitelnosti aktiv hrozbou

Následující tabulka určuje jaká je míra zranitelnosti pro dané aktivum od uvedených hrozeb.

Tabulka 11: Míra zranitelnosti aktiv hrozbou

Popis hrozby:	předstírání identity uživatele	použití softwaru neautorizovanými uživateli	zneužití privilegií – použití SW	popření (anonymita provádějících	prozrazení dat během přenosu	prozrazení dat na paměťovém mediu	modifikace dat na paměťovém	modifikace dat v databázi	modifikace dat při přenosu	technické selhání síťových	selhání hardware	poškození paměťového media	zemětřesení	povodeň a voda z potrubí	požár	selhání dodávky energie	selhání klimatizace	krádež, násilný trestný čin	škodlivý software (viry, trojské
Nehmotná informační aktiva	**H1**	**H2**	**H3**	**H4**	**H5**	**H6**	**H7**	**H8**	**H9**	**H10**	**H11**	**H12**	**H13**	**H14**	**H15**	**H16**	**H17**	**H18**	**H19**
Elektronicka pošta - údaje o poptávky, nabídky, objednávky	3	3	3	3	3	3	3	2	3	2	2	2	2	1	3	1	2	4	3
Skladovací systém - údaje	3	2	2	1	2	2	2	2	2	2	2	2	2	1	3	1	2	3	2
Účetní systém - údaje	3	2	2	1	2	2	2	2	2	2	2	2	2	1	3	1	2	3	2
Nehmotná softwarová aktiva	**H1**	**H2**	**H3**	**H4**	**H5**	**H6**	**H7**	**H8**	**H9**	**H10**	**H11**	**H12**	**H13**	**H14**	**H15**	**H16**	**H17**	**H18**	**H19**
Operační systém Windows 2003 Server	3	2	2	2	2	2	2	2	1	2	2	2	2	1	3	1	1	1	4
Operační systém Windows XP - PC	3	3	2	2	2	2	2	2	1	2	2	2	2	1	3	1	1	1	4
SW Antivirová ochrana PC, server,	1	1	2	1	2	1	1	1	2	1	2	2	2	1	3	1	1	1	3
NAVISION	2	3	2	2	2	2	2	2	2	2	2	2	2	1	3	1	1	1	3
Firewallová ochrana PC	1	1	2	1	2	1	1	1	1	1	1	1	2	1	3	1	1	1	3
Webmaster (www stránky)	2	2	2	2	2	2	2	2	2	2	2	2	2	1	3	1	1	1	3
Ostatní evidovaný SW viz I1.3	1	1	1	1	2	1	1	1	1	1	1	1	2	1	3	1	1	1	1
MS Office	2	2	2	3	2	2	2	3	3	1	1	2	2	1	3	1	1	1	3
Hmotné aktiva	**H1**	**H2**	**H3**	**H4**	**H5**	**H6**	**H7**	**H8**	**H9**	**H10**	**H11**	**H12**	**H13**	**H14**	**H15**	**H16**	**H17**	**H18**	**H19**
Servery	3	2	2	2	2	2	2	3	1	2	2	2	2	2	3	3	2	2	2
NAVISION - server	3	2	2	2	2	2	2	2	1	2	2	2	2	2	3	2	2	2	2
Firewallová ochrana serverů	3	3	2	1	2	1	1	1	1	2	2	2	2	2	3	3	2	2	2
Server el. pošta	2	1	2	1	2	2	2	1	1	2	2	2	2	2	3	2	2	2	2

EZS	2	2	2	2	2	1	1	1	1	2	2	2	2	2	4	2	2	3	2
Síťové prvky	2	2	2	2	2	1	1	1	1	2	2	2	2	2	3	3	2	2	2
Přenosná výpočetní technika	3	4	2	1	2	2	2	1	1	2	3	2	2	2	2	3	2	3	2
Pracovní stanice PC	3	3	2	1	2	2	2	1	1	2	2	3	2	2	4	3	2	2	2
Ostatní hardware (tiskárny, scaner ..)	2	2	1	1	2	1	1	1	1	2	2	1	2	2	4	3	2	3	2
Externí HDD, datová media	2	2	2	1	2	3	2	1	1	2	2	3	2	2	2	3	1	2	3
MS Exchange	2	3	2	2	2	2	2	2	2	2	2	2	2	2	3	1	1	1	3
Aktiva - externí služby	**H1**	**H2**	**H3**	**H4**	**H5**	**H6**	**H7**	**H8**	**H9**	**H10**	**H11**	**H12**	**H13**	**H14**	**H15**	**H16**	**H17**	**H18**	**H19**
Připojení do sítě Internet a ostatní služby, sw + hw	1	1	1	2	2	1	1	1	1	3	3	2	2	2	2	3	2	2	1
Dodávka elektrické energie	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2	1	1	1
Dodávka ostatních energií	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	3	1	1	1
Poštovní služby - dopravci	2	1	1	1	1	1	1	1	1	1	1	1	2	2	3	3	1	2	1
Webhosting, WWW stránky	2	2	1	2	1	2	2	2	2	2	2	2	2	2	2	3	2	3	2

Zdroj: vlastní

7.3.4 Hodnocení rizik a opatření

Následující tabulka vypočítává hodnotu rizika pro firmu a informační systém**.**

Tabulka 12: Hodnocení rizik a opatření

Popis hrozby:	předstírání identity uživatele	použití softwaru neautorizovanými uživateli	znežití privilegií – použití SW neautorizovaným způsobem	popření (anonymita prováděných akcí)	prozrazení dat během přenosu	prozrazení dat na paměťovém mediu	modifikace dat na paměťovém mediu	modifikace dat v databázi	modifikace dat při přenosu	technické selhání síťových komponent	selhání hardware	poškození paměťového media	zemětřesení	povodeň a voda z potrubí	požár	selhání dodávky energie	selhání klimatizace	krádež, násilný trestný čin	škodlivý software (viry, trojské koně)
Nehmotná informační aktiva	H1	H2	H3	H4	H5	H6	H7	H8	H9	H10	H11	H12	H13	H14	H15	H16	H17	H18	H19
Elektronicka pošta - údaje o poptávky, nabídky, objednávky	240	240	240	160	320	240	240	107	240	107	107	53	53	27	160	27	53	320	240
Skladovací systém - údaje	300	200	267	67	200	133	67	133	133	133	133	133	67	33	200	33	67	400	133
Účetní systém - údaje	300	200	267	67	200	133	67	133	133	133	133	133	67	33	200	33	67	400	133
Nehmotná softwarová aktiva	H1	H2	H3	H4	H5	H6	H7	H8	H9	H10	H11	H12	H13	H14	H15	H16	H17	H18	H19
Operační systém Windows 2003 Server	375	167	167	167	167	167	167	167	83	167	167	167	83	42	250	42	42	42	500
Operační systém Windows XP - PC	192	192	128	128	85	85	85	128	64	128	128	85	43	21	128	21	21	21	341
SW Antivirová ochrana PC, server, Smart phone	9	9	36	9	36	9	9	9	18	9	18	18	18	9	54	9	9	9	81
NAVISION	250	250	167	167	167	250	250	167	167	167	167	167	83	42	250	42	42	42	375
Firewallová ochrana PC	6	6	24	6	24	6	6	6	6	6	6	6	12	6	36	6	6	6	54
Webmaster (www stránky)	16	16	16	16	16	16	16	16	16	16	16	16	8	4	24	4	4	4	36
Ostatní evidovaný SW viz I1.3	5	5	5	5	21	5	16	11	5	5	5	5	11	5	32	5	5	5	11
MS Office	11	21	21	48	21	32	43	48	32	5	5	11	11	5	32	5	5	5	48

Hmotné aktiva	H1	H2	H3	H4	H5	H6	H7	H8	H9	H10	H11	H12	H13	H14	H15	H16	H17	H18	H19
Servery	375	167	167	250	250	167	167	375	83	167	167	167	83	83	250	250	167	167	167
NAVISION - server	375	167	167	250	83	167	167	250	83	167	167	167	83	83	250	167	167	167	167
Firewallová ochrana serverů	128	128	85	43	43	21	21	21	21	85	85	85	43	43	128	128	85	43	85
Server el. pošta	85	43	128	43	43	43	43	21	21	85	85	85	43	43	128	85	85	85	128
EZS	12	6	6	6	6	3	3	3	3	12	12	12	6	6	24	12	12	18	6
Síťové prvky	60	60	60	60	30	15	15	30	15	60	60	60	30	30	90	90	60	60	30
Přenosná výpočetní technika	300	533	200	67	133	133	133	67	33	200	300	133	67	67	133	200	67	400	200
Pracovní stanice PC	240	240	107	53	107	107	107	53	53	107	107	160	53	53	213	160	53	107	107
Ostatní hardware (tiskárny, scaner ..)	8	8	2	4	8	2	2	2	2	8	8	2	4	4	16	12	4	12	4
Externí HDD, datová media	40	80	40	40	80	180	120	20	20	40	80	120	40	40	80	120	20	160	180
MS Exchange	43	128	43	85	43	43	43	43	43	128	85	85	43	43	128	43	43	43	192
Aktiva - externí služby	H1	H2	H3	H4	H5	H6	H7	H8	H9	H10	H11	H12	H13	H14	H15	H16	H17	H18	H19
Připojení do sítě Internet a ostatní služby, sw + hw	16	16	16	16	16	8	8	8	16	48	48	16	16	16	32	48	32	48	8
Dodávka elektrické energie	12	12	12	12	12	12	12	12	12	24	24	12	24	48	48	48	12	12	12
Dodávka ostatních energií	12	12	12	12	12	12	12	12	12	24	24	12	24	24	48	72	12	12	12
Poštovní služby - dopravci	5	3	3	3	3	3	3	3	3	3	5	3	5	11	16	8	3	11	3
Webhosting, WWW	12	12	6	12	6	12	12	12	12	24	36	24	12	12	24	36	12	36	24

Zdroj: vlastní

Ohodnocení míry rizika jednotlivého aktiva a hrozby je v následující tabulce:

Tabulka 13: Ohodnocení rizika

Ohodnocení rizika (Míra rizika):		
534	1042	Vysoké riziko
226	534	Střední riziko
68	226	Malé riziko
1	68	Nevýznamné riziko

Zdroj: vlastní

7.4 SWOT analýza

V následující SWOT analýze jsou shrnuty veškeré výstupy z předcházejících analýz, současného stavu firmy a mých vlastních teoretických a praktických zkušeností při provádění analýz. Výsledná SWOT analýza je jedním z hlavních podkladů pro vytvoření návrhu řešení.

Tabulka 14: Shrnutí zabezpečení pomocí SWOT analýzy

S - silné stránky	**W - slabé stránky**
- Stabilní síťová a serverová infrastruktura - Firma využívá řízení přístupu k informacím - Veškeré PC stanice a síťové úložiště je šifrované - IS splňuje očekávání „stakeholders“ - Firma používá a zavádí nejmodernější technologie - Vysoká úroveň znalostí a zkušeností pracovníků - Vlastní servisní zázemí - Obecně fungující povědomost o zaměření společnosti - Vlastní technické zázemí - Odborná znalost technologií	- Není definována koncepce rozvoje IS - Nedostatek investic pro podstatně rychlejší zavádění nových technologií - Nejsou využívány pro rozhodování všechny výstupy, které by rozhodnutí usnadnili - Přílišné reporty zaměstnanců k managementu - Žádná část IS není outsourcována, stoupají požadavky na vlastní IT oddělení - Vysoké náklady na IT oddělení
O – příležitosti	**T – hrozby**
- IS lze využívat kdekoliv a kdykoliv pomocí vzdáleného přístupu do firemní sítě - Firma má definovanou bezpečnostní politiku - Firma je partnerem předních světových výrobců zabezpečení IS - Požadavek trhu na outsourcing IT služeb - Požadavek zákazníků na větší bezpečnost - přesná definice úkolů a kontrola jejich plnění - Firma může poskytovat vlastní systém outsourcingem pro jiné firmy - Čerpání benefitů z partnerských smluv dodavatelů (licence, HW, SW, školení)	- Velké množství vstupů, které musí zaměstnanci reportovat, aniž by se následně využily - Odchod důležitých technických pracovníků - Vynesení informací mimo IS zaměstnancem - Cílený útok hackera - Přírodní pohromy - nedostatek důvěry spolupracovníků - nedostatek finančních příjmů do IS - destabilizace společnosti - Výpadek IS - Předstírání identity uživatele - Vyzrazení hesel uživatelů - Není zaveden monitoring tisku

Zdroj: vlastní

8 Návrh řešení

8.1 Návrh zabezpečení IS firmy na základě výsledků analýz

Když zhodnotíme aktuální stav firmy na základě současného stavu a provedených analýz, tak jej můžeme vyhodnotit jako velmi dobrý, který splňuje zabezpečení obchodních informací u českých firem nebo i v některých případech i za nadstandardní po technické stránce. Pokud byly nalezeny nedostatky, tak to bylo v především v oblastech organizačních a lidských zdrojů.

Nalezené nedostatky ve stávajícím IS jsou:

- Chybějící koncepce rozvoje IS
- Nejsou plánovány investice v souladu s plánem rozvoje IS
- Firma se nezaměřuje na outsourcing částí IS
- Není zde ochrana proti vyzrazení hesla uživatele
- Duplicita zadávaných vstupů od zaměstnanců
- Vedení nevyužívá nebo nedokáže využít zobrazení všech výstupů potřebných pro usnadnění rozhodování z IS
- Není zabezpečeno vynesení informací z IS
- Není zaveden monitoring tisku
- Přílišný manuální reporting zaměstnanců
- Vysoké náklady na IT oddělení

Chybějící koncepce rozvoje IS

Firma nemá definovanou koncepci rozvoje informačního systému. Řešením bude vytvořit novou koncepci rozvoje IS, která bude obsahovat krátkodobé, střednědobé a dlouhodobé cíle rozvoje, které budou v souladu s IS/IT strategii a business strategií. Plán rozvoje bude zaměřen na upgrade infrastruktury IS a postupné zvyšování zabezpečení obchodních informací v IS.

Nejsou plánovány investice v souladu s plánem rozvoje IS

Na základě nově vytvořené koncepce rozvoje IS bude nutné stanovit plán investic, takovým způsobem, aby pokrýval koncepci rozvoje IS. Plán investic musí být v souladu s firemní strategií, takovým způsobem, aby bylo možné finanční prostředky v daném termínu vyčlenit.

Firma se nezaměřuje na outsourcing částí IS

Firma nevyužívá outsourcingu dílčích částí IS a tím stoupají náklady na odbornost, čas a zkušenosti na IT oddělení. Se stoupajícími požadavky stoupají náklady, odpovědnost, počet zaměstnanců, počet systémů a klesá rentabilita vložené investice. Bezpečnostní prvky, servery a další aplikace jsou vytíženy v jednotkách procent a efektivnost takových systémů je nízká. Vhodnější je využít některé systémy jako službu za mnohonásobně nižší náklady než si systém koupit a samostatně spravovat.

Není zde ochrana proti vyzrazení hesla uživatele

V případě, že uživatel prozradí své heslo, třetí osobě nebo bylo odchyceno při zadávání, tak není ochrany, jak tomu zabránit, aby nebylo zneužito. Řešením je zavést generované heslo pro každé přihlášení. Toho lze dosáhnout implementací tokenů do IS. Pro každé přihlášení nám token po zadání pinu vygeneruje nové heslo.

Duplicita zadávaných vstupů od zaměstnanců

Pro odstranění zadávání duplicitních informací do různých aplikací, je nutné vytvořit datové konektory mezi aplikacemi a stanovit výměnu dat a synchronizaci mezi aplikacemi. Toto řešení zvýší efektivnost zadávání dat do systému a sníží časovou náročnost administrativních úkonů od uživatelů.

Vedení nevyužívá nebo nedokáže využít zobrazení všech výstupů potřebných pro usnadnění rozhodování z IS

Vedení nevyužívá z manažerského hlediska všechny výstupy z IS, proto je nutné zautomatizovat výstupy a reporting, vytvořit nové komplexnější výstupy, které dokážou sumarizovat více vstupů.

Není zabezpečeno vynesení informací z IS

Uživatelé si nyní mohou vynést z IS téměř všechny informace ke kterým mají přístup následujícími způsoby: vypálení na CD/DVD, uložením na USB disk zasláním přes freeemail a firma to nezjistí. Z tohoto důvodu je nutné zavést systém SafeGuard LeakProof, který umožňuje hlídat kompletní správu a nakládaní s dokumenty a umožňuje blokovat zkopírování, přesunutí, vytištění dokumentů.

Není zaveden monitoring tisku

Ve firemním informačním systému je potřeba implementovat systém, který monitoruje všechny vytištěné dokumenty z IS. Tento systém nám umožní hlídat uživatele, tak aby nezneužívali firemní prostředky a zároveň eviduje všechny dokumenty, které IS opustily.

8.2 Ekonomický dopad nalezených nedostatků zabezpečení IS firmy

V následující tabulce je souhrn ekonomických dopadů nalezených rizik, na základě předchozích analýz, při zabezpečení obchodních informací a IS firmy.

Tabulka 15 : Ekonomický dopad nalezených nedostatků zabezpečení IS firmy

Nalezený nedostatek v zabezpečení informací nebo v IS	Ekonomický dopad nalezeného nedostatku
Chybějící koncepce rozvoje IS	Informační systém nemá definovanou koncepci, což může mít za následek vyšší výdaje při provádění následných změn. IS se může ubírat jiným směrem než, který byl nastaven, což může snižovat jeho efektivitu.
Nejsou plánovány investice v souladu s plánem rozvoje IS	Firma nemá v plánování a kalkulací nákladů stanoveny výdaje na investice na IS, ale pouze provozní náklady na IS
Firma se nezaměřuje na outsourcing částí IS	Náklady na IT oddělení a IS mohou být několikanásobně vyšší, než kdyby firma využila outsourcingu
Není zde ochrana proti vyzrazení hesla uživatele	V případě vyzrazení hesla mohou nastat firmě finanční ztráty podle úrovně, jak bylo heslo zneužito a které informace byly získány a jak bylo s nimi naloženo
Duplicita zadávaných vstupů	Když musí zaměstnanec duplicitně zadávat

od zaměstnanců	vstupy do několika aplikací, klesá jeho efektivita a stoupají jeho náklady vzhledem k odvedené práci
Vedení nevyužívá nebo nedokáže využít zobrazení všech výstupů potřebných pro usnadnění rozhodování z IS	Když vedení nebude sledovat, všechny důležité procesy v IS a zpětnou vazbu těchto procesů nebo nebude využívat výstupy z IS pro rozhodování, tak může docházet k finančním ztrátám a strategickým chybám
Není zabezpečeno vynesení informací z IS	Každý uživatel si může odnést jakýkoliv dokument, ke kterému má přístup, což může mít dopad na obchod, pokud jsou dokumenty předány třetí straně(konkurence, úřady, hackeři,média) .
Není zaveden monitoring tisku	Firma nemá monitorováno, jaké dokumenty opustí firmy a jaká je jejich hodnota. Náklady na tisk jsou dnes nezanedbatelnou položkou v případě tisku pro osobní potřebu uživatelů.

Zdroj: vlastní

8.3 Návrh IS/IT strategie pro aplikaci změn IS firmy

Nová IS/IT strategie by měla obsahovat odstranění nalezených koncepčních nedostatků, měla by navrhnout směr IS, jak v krátkodobém, tak i v dlouhodobém horizontu. Všechny cíle definované v nové IS/IT strategii by měly být SMART a měly by směřovat k postupnému zvyšování zabezpečení obchodních informací v informačním systému firmy.

Návrh strategie IS/IT by měl obsahovat následující cíle:

Krátkodobý horizont

- Vytvoření strategii rozvoje IS, včetně plánu investic
- Vytvořit lepší datové propojení mezi aplikacemi, tak aby se snížilo zatížení zaměstnanců při zadávání vstupů a stoupla jejich efektivita.
- Zavést pravidelné kontroly a audity v IS za účelem stanovení, zda IS koresponduje s IS/IT strategií, jeho zabezpečení nevyžaduje změnu a neklesá spokojenost a očekávání uživatelů IS.

Dlouhodobý horizont

- Zavedení systému kontroly dokumentů, tak aby bylo možné sledovat pohyb dokumentů ve firmě a mimo ni.
- Zavést dynamické přihlašování uživatelů pomocí tokenů, které generují jednorázové heslo. Do všech aplikací zavést jednotné přihlašování na základě identifikace uživatele, tímto heslem.
- Zavést monitoring tisku, pošty, navštívených WWW stránek a sledovat vytížení firemních prostředků.
- Navrhnout a spočítat, které části IS by bylo vhodnější použít outsourcing
- Pro vedení a management navrhnout lépe vypovídající výstupy IS s vyšší sumarizací všech informací a procesů v IS

9 Zhodnocení návrhu řešení

Návrh řešení nás směruje do úplně nové oblasti a to k řízení přístupu a oprávnění k dokumentům. Tento nový trend správy dokumentů můžeme zařadit mezi ty nejžádanější a nejspolehlivější na trhu. Firma nyní disponuje technologiemi na velmi vysoké úrovní a tento systém by ji mohl posunout dále v oblasti zabezpečení obchodních informací.

Návrh a implementace systémů řízení dokumentů vyžaduje plánovat v dlouhodobém horizontu. Samotná implementace je stejně dlouhá jako např. implementace CRM systému, tzn. jednotky až desítky měsíců. Tuto implementaci musíme navrhnout do návrhu IS/IT strategie a plánu rozvoje IS. Proto je velmi důležité vytvořit návrh rozvoje zabezpečení IS, který bude součástí IS/IT strategie. Nedílnou součástí rozvoje musí být i plán investic v dlouhodobém a krátkodobém horizontu.

Co se týče nalezených rizik, můžeme konstatovat, že firma má dobře zmapovaná rizika firmy a IS a zároveň vytvořeny opatření proti těmto rizikům. Rizika jsou ohodnocena a je zřejmá jejich váha, četnost, pravděpodobnost výskytu a možně jejích následky.

Z analýz je zřejmé, že se firma velmi dobře věnuje technické části IS, ale už opomíjí lidský faktor a některé procesy. Firma by se měla více věnovat zaměstnancům a managementu a jejich potřebám a jejich vztahu k IS. Vhodné by bylo zavést monitoring práce zaměstnanců, managementu a dalších skupin, tak abychom mohli tyto potřeby předvídat a zavádět do IS průběžně.

10 Závěr

Metodika, principy a analýzy pro hodnocení zabezpečení obchodních informací použité v v této práci mi dává nástroje, pomocí kterých můžu analyzovat kteroukoliv jinou firmu a její zabezpečení obchodních informací. Zaměření firmy může být jakékoliv. Výsledek analýz a metodik mi poskytne stejně hodnotný výstup hodnocení zabezpečení obchodních informací kterékoliv firmy.

Na základě výstupu analýzy rizik v této práci jsem schopen přesně definovat, jaké riziko pro danou dílčí část informačního systému představuje hrozbu, jaký má tato hrozba dopad na danou část informačního systému a jaká je pravděpodobnost výskytu této hrozby. Když provedu součin všech těchto atribut hrozeb, tak dostanu výslednou hodnotu hrozby daného rizika pro informační systém.

Následně mohu navrhnout novou IS/IT strategii, která je založena na eliminaci nalezených rizik informačního systému a výstupu analýz, takovým způsobem, aby odstraňovala tyto nedostatky, dávala směr v rozvoji informačního systému a zároveň rostla úroveň zabezpečení obchodních informací. Ekonomický dopad nalezených rizik, musí být zakomponován do této strategie.

V poslední řadě je třeba brát v úvahu, neustále se zrychlující tempo rozvoje v oblastech informačních technologií, jejich trendech, bezpečnosti a firemních informačních systému. Z tohoto hlediska je nutné sledovat, implementovat a neustále aktualizovat informační systém a jeho zabezpečení.

V dnešní informační a zrychlené době může znamenat zneužití obchodních informací i zánik firmy nebo nepředstavitelné problémy vůči všem „stakeholders“.

A proto platí v této oblasti: ***Zaspat, může znamenat se neprobudit.***

11 Seznam použitých informačních zdrojů

[1]SODOMKA,P.: *Informační systémy v podnikové praxi*. 1.vyd. Brno: Computer Press, 2006. 352s. ISBN: 80-251-1200-4.

[2]MLÝNEK,J.: *Zabezpečení obchodních informací*. 1.vyd. Brno: Computer Press, 2007. 154s. ISBN: 978-80-251-1511-4.

[3]SMEJKAL,V.,RAIS,K.: *Řízení rizik*. 1.vyd. Praha: Grada, 2003.

[4]KEŘKOVSKÝ,M., DRDLA,M.: *Strategické řízení firemních informací*: teorioe pro praxi. 1.vyd. Praha: C.H.Beck, 2003. 187s. ISBN: 80-7179-730-8.

[5]KOCH,M., DOVRTĚL,J.,: *Management informačních systémů*, Brno: Vysoké učení technické Brně, Fakulta podnikatelská, 2006. ISBN: 80-214-3262-4.

[6]MOLNÁR, Z.: *Efektivnost informačních systémů*. 1. vyd. Praha: Grada, 2000. 142 s. ISBN 80-7169-410-X.75.

[7] WIKIPEDIA .ORG: *Informace*.[online], poslední aktualizace 15. 12.2008, [cit. 2008-12-23], Dostupné z WWW:< http://cs.wikipedia.org/wiki/Informace>

[8] WIKIPEDIA .ORG: *Data*.[online], poslední aktualizace 23. 9.2008, [cit. 2008-12-23], Dostupné z WWW:< http://cs.wikipedia.org/wiki/Data>

[9] W. Weaver and C. E. Shannon, *The Mathematical Theory of Communication*, Urbana, Illinois: University of Illinois Press, 1949, republished in paperback 1963.

[10] ISO/IEC 27001:2005 (BS 7799-2) Information security management systems – Requirements.

[11]KEŘKOVSKÝ,M.: *Moderní přístupy k řízení výroby*.Praha: C.H.Beck, 2001. ISBN 80-7179-471-6

[12] PRÚCHA,O.:Návrh realizace VPN řešení pro KIV.[online], , [cit. 2008-12-23], Dostupné z WWW:< http://home.zcu.cz/~ondrous/>

[13] PETERKA,J.: Backup. [online], [cit. 2008-12-23], Dostupné z WWW:< http://www.earchiv.cz/a93/a330c120.php3 >

[14] MICROSOFT: Omezení přístupu uživatelů k souborům pomocí funkce řízení přístupu. [online], [cit. 2008-12-22], Dostupné z WWW: <http://www.microsoft.com/cze/windows/xp/pro/using/howto/security/accesscontrol.mspx>

[15] DRDLA, M.,RAIS, K.: *Řízení změn ve firmě*.Praha:Computer Press,2001.ISBN 80-7226-411-7.

[16]KEŘKOVSKÝ,M., VYKYPĚL,O.: *Strategické řízení – teorie pro praxi*.Praha: C.H.Beck, 2002. ISBN 80-7179-578-X

[17]KOTLER, P.: *Marketing Managment*. Prentice Hall, Engelwood Cliffs, 1984 (český překlad:Marketing managment.10.rozšířené vydání.Praha:Grada publishing, 2001.ISBN 80-247-0016-6).

[18]MOLNÁR, Z.: *Efektivnost IS/IT*.Zlín:FAME UTB, 2001.

[19]RODRYČOVÁ, D., STAŠA, P.: *Bezpečnost informací-jako podmínka prosperity firmy*. Praha: Grada publishing, 2000.ISBN 80-7169-144-5.

[20]VOŘÍŠEK, J.: *Strategické řízení informačního systému*.Praha: Managment press, 1997. ISBN 80-85943-40-9.

[21]GROŠEK, O., PORUBSKÝ, Š.: Šifrovanie-algoritmy, metódy,prax, Grada, Praha, 1992.

[22]MLÝNEK, J.: *Klasifikace informací a vlastníci informací v obchodní společnosti*, 5.konference Bezpečnost informací ve finančním sektoru, Tatranská Lomnica, březen 2003.

[23]MLÝNEK, J.: *Securing of Business Information*, *23rd International Konference Mathematical Methods in Economics 2005*, Hradec Králové, September 2005.

[24]PELTIER, T. R.: *Information Security Risk Analysis*, Taylor & Francis Group, Boca Raton, USA, 2005.

[25]SMEJKAL, V., RAIS, K.: *Řízení rizik*, Grada, Praha: 2003. ISBN 80-7169-842-7.

[26] COVEY, S.R.: *Sedm návyků vůdčích osobností*.Praha: Pragma, 1994. ISBN 80-85213-41-9.

[27] MAJER, J.: *Principy procesně řízené organizace za pomocí informačních systémů*. In Svět informačních systémů 2006: sborník příspěvků z mezinárodní konference, Zlín, 10.-11.dubna 2006. Ed.Roman Bobák a Petr Sodomka. Zlín: FaMe, UTB ve Zlíně, CVIS – odborná sekce ČSSI, 2006, s. 238- 245. ISBN 80- 7318- 400-1.

[28] POLÁK, J., MERUNKA, V., CARDA, V.: *Umění systémového návrhu*. Praha: Grada Publishing, 2003. ISBN 80-247-0424-2.

[29] TVRDÍKOVÁ, M.: *Závádění a inovace informačních systémů ve firmách*. Praha: Grada Publishing, 2000. ISBN 80-7169-703-6.

[30] HAMMER, M.: *Agenda 21*: *co musí každý podnik udělat pro úspěch v 21.století*. Praha: Managment Press, 2002. ISBN 80-7261-074-0.

12 Seznam zkratek a odborných termínů

Seznam odborných termínů a zkratek z oblasti bezpečnosti informačních systémů a rizik

Akceptace rizika / Risk acceptance - Rozhodnutí vedení přijmout existující úroveň rizika.

Aktivum / Asset - Vše, co má pro organizaci hodnotu hmotnou (zaměstnanci, počítač, materiál, finanční hotovost apod.) nebo nehmotnou (programy, data, kvalita personálu apod.).

Analýza rizik (AR) / Risk analysis - Proces, který slouží k odhadu ztrát, jež mohou vzniknout působením hrozeb na systém, a dává přehled o nebezpečnosti jednotlivých hrozeb, jejich zdrojích, zranitelnostech hodnoceného systému a rizikách, kterým je hodnocený systém vystaven.

Autentizace / Authentification - Poskytnutí záruky týkající se identity subjektu nebo objektu, např. ujištění, že konkrétní uživatel je skutečně ten, za koho se prohlašuje, resp. schopnost zjistit, kdo vydal daný příkaz nebo požadavek.

Autorizovaný uživatel / Accredited user - Uživatel, který má určité právo nebo povolení pracovat v IS a s aplikacemi podle stanovených zásad přístupu.

Bezpečnost informací / Information security - Vlastnost nebo stav ochrany informací proti potenciálním ztrátám. Opatření k zachování důvěrnosti, integrity, dostupnosti, autentičnosti, odpovědnosti, nepopiratelnosti, spolehlivosti a správnosti.

Bezpečnost IS / IS security - Ochrana IS a informací, které jsou v nich uchovávány, zpracovávány a přenášeny. Stav IS, ve kterém jsou hrozící rizika pomocí vhodných opatření snížena na přijatelnou úroveň.

Bezpečnostní cíle / Security aims - Stav bezpečnosti, který má daný systém nebo produkt dosáhnout.

Bezpečnostní funkce / Safety function - Funkce provádějící požadovanou činnost, zajišťující realizaci bezpečnostních požadavků.

Bezpečnostní incident / Safety incident - Jedna nebo více nechtěných bezpečnostních událostí s vysokou pravděpodobností kompromitace činnosti organizace nebo informačního systému.

Bezpečnostní manažer / Security manager - Zaměstnanecká role pro výkon odpovědnosti gestora IS za bezpečnost s definováním odpovědností a pravomocí.

Bezpečnostní mechanismus / Safety mechanism - Logika nebo algoritmus, který implementuje příslušnou funkci prosazující bezpečnost, nebo pro bezpečnost relevantní funkci v hardwarové nebo softwarové podobě.

Bezpečnostní opatření / Safety measures - Souhrn prostředků a opatření, kterými je prosazována bezpečnostní politika s cílem navodit požadovaný stupeň bezpečnosti.

Bezpečnostní politika IS / IS security policy - Celkový záměr vedení a směr řízení bezpečnosti informací se stanovením kriterií pro hodnocení rizik.

Bezpečnostní rada kraje (BRK) / District security council - Koordinační orgán kraje pro přípravu na krizové situace

Bezpečnostní rada určené obce (BRUOb) / Municipality security council - Koordinační orgán určené obce pro přípravu na krizové situace

Bezpečnostní rada státu (BRS) / National security council - Stálý pracovní orgán vlády ČR pro koordinaci bezpečnosti ČR a přípravu návrhů opatření k jejímu zajištění

Bezpečnostní událost / Security event - Identifikovaný stav systému, služby nebo sítě, ukazjící na možnost porušení bezpečnostní politiky nebo selhání bezpečnostních opatření.

Biologické zbraně (BZ) / Biological weapons - Druh zbraní, které patří mezi zbraně hromadného ničení. Využívají škodlivých účinků biologických látek na lidský nebo jiný živý organismus. Skládají se z biologických látek a prostředků jejich dopravy na cíl. Zahrnují rovněž využití infikovaných hlodavců, hmyzu apod.

Citlivá data / Sensitive data - *Chráněná data* mající pro chod organizace zásadní význam. Jejich vyzrazením, zneužitím, neautorizovanou změnou nebo nedostupností by vznikla organizaci škoda, případně by organizace nemohla řádně plnit svoje poslání.

Civilní nouzové plánování (CNP) / Civil emergency planning - "Proces plánování opatření k zajištění ochrany vnitřní bezpečnosti a veřejného pořádku, ochrany obyvatelstva, ochrany ekonomiky, trvalé funkčnosti státní správy, přijatelné úrovně společenské a hospodářské činnosti státu a obyvatelstva"

Civilní ochrana (CO) / Civil protection - Souhrn činností a postupů určených k ochraně civilního obyvatelstva před nebezpečím a k pomoci obyvatelstvu při odstraňování bezprostředních účinků krizových situací a mimořádných událostí a při vytváření nezbytných podmínek pro jejich přežití

Číselník nezbytných dodávek (CND) / Numerical catalogue of necessary - Přehled jednotného číselného označení zavedených položek nezbytných dodávek, navazující na číselník standardní klasifikace produkce

Dostupnost / Availability - Zajištění, že informace a důležité služby jsou dostupné uživateli, když je třeba a v potřebném rozsahu.

Důvěrnost / Confidentiality - Zajištění, že informace jsou přístupné nebo sděleny pouze tomu, kdo je k jejich přístupu oprávněn.

EPS / EPS - Electric Fire Alarm - Elektrická požární signalizace

Evakuace / Evacuation - Souhrn opatření zabezpečující přemístění (odsun) osob, zvířat, kulturních hodnot a věcných prostředků v daném pořadí priority, z ohroženého prostoru na jiné území, ve kterém je zajištěno náhradní ubytování, stravování a nezbytné služby pro obyvatelstvo, ustájení pro hospodářská zvířada a uložení pro věcné a kulturní prostředky

EZS / EZS - Electronical Alarm System - Elektronický zabezpečovací systém

Firewall / Firewall - Bezpečnostní prvek ochrany sítě

Fyzická bezpečnost / Physical security - Fyzická (objektová) bezpečnost – ochranná opatření zajišťující přístup a kontrolu do zabezpečených prostorů a objektů, kontrolu neautorizovaných narušení bezpečnostních perimetrů a ochranu před vlivy provozního prostředí.

Havárie / Average - Nežádoucí mimořádná, částečně nebo zcela neovládaná, časově a prostorově ohraničená událost, která vznikla nebo jejíž vznik bezprostředně hrozí v souvislosti s provozem technických zařízení, výrobou, užitím, skladováním, zneškodňováním nebo přepravou nebezpečných látek, která vede ke ztrátě života, poškozenínebo ohrožení zdraví lidí, živých organismů nebo životního porstředí nebo k prokazatelné újmě na majetku.

Havarijní plán (HP) / Emergency plan - Dokument, v němž jsou uvedeny popisy činností a opatření prováděných při vzniku závažné mimořádné události nebo havárie vedoucí k minimalizaci jejích následků

Havarijní připravenost / Emergency preparedness - Příprava opatření na odvrácení dopadů havárií nebo alespoň na jejich zmírnění.

Hmotné rezervy / Material reserves - Vybrané základní suroviny, materiály, polotovary a výrobky určené pro zajištění obranyschopnosti státu a obrany státu, pro odstranění následků krizových situací a pro ochranu důležitých hospodářských zájmů státu

Hodnota aktiv / Assets value - Objektivní vyjádření obecně vnímané ceny nebo subjektivní ocenění důležitosti (kritičnosti) aktiva, popř. kombinace obou přístupů.

Hodnocení rizik / Risk rating - Celkový proces analýzy a vyhodnocení rizik, tj. porovnávání odhadnutého rizika vůči daným kriteriím pro určení jeho významu.

Hospodářské opatření pro krizové stavy (HOPKS) / Economic measure for emergenies - Organizační, materiální nebo finanční opatření přijímaná správním úřadem (státem) v krizových stavech pro zabezpečení nezbytné dodávky výrobků prací a služeb, bez nichž nelze zajistit překonání krizových stavů

Hrozba / Threat, Hazard - Potenciálně ničivá fyzikální událost, jev nebo lidská aktivita, která může zapříčinit ztrátu životů nebo zranění, škody na majetku, sociální a ekonomické poruchy nebo environmentální znehodnocení

HW / Hardware - Technické vybavení

Chemické zbraně (CHZ) / Chemical weapons - Chemické zbraně jsou zbraně hromadného ničení, jejichž účinek je založený na toxických vlastnostech chemických látek. Hlavní komponenty chemických zbraní jsou bojové otravné látky a prostředky jejich použití, včetně nosičů, přístrojů a zařízení pro navedení na cíl

ICT / Information and Communication Technology - Informační a komunikační technologie

ID / ID, Identification - identifikátor uživatele

Informační bezpečnost / Security of information - Bezpečnost při manipulaci s informacemi, především vzhledem k požadavkům na důvěrnost, integritu a dostupnost informací.

Integrita / Integrity - Zajištění správnosti, úplnosti a aktuálnosti informací a softwaru k jejich zpracování.

Internet / Internet - celosvětová síť počítačů komunikujících prostřednictvím IP protokolů

Interoperabilita / Interoperability - Schopnost společně působit při plnění stanovených cílů nebo-li schopnost systémů, jednotek či organizací poskytovat služby jiným systémům, jednotkám či organizacím a akceptovat je od nich a používat takto sdílené služby pro efektivní společnou činnost

IS / IS, Information system - Informační systém

ISMS / Information Security Management System - Systém řízení bezpečnosti informací. Součást řízení organizace, zaměřená na řízení rizik a zlepšování bezpečnosti IS organizace.

ISO / International Organization for Standardization - Mezinárodní organizace pro normalizaci

IT / Information Technology - Informační technologie

Integrovaný záchranný systém (IZS) / Integrated rescue systém - Koordinovaný postup jeho složekm při přípravě na mimořádné události a při provádění záchranných a likvidačních prací.

Jaderné zbraně (JZ) / Nuclear weapens - Jaderné zbraně jsou zbraně hromadného ničení, založené na využití vnitrojaderní energie, vznikající při štěpných reakcích dělení těžkých jader některých izotopů uranu a plutonia nebo při termojaderných reakcích syntézy lehkých jader izotopů vodíku (deuteria a tritia).

Katastrofa, Pohroma / Catastrophe, Disaster - Náhlá událost s velkými ztrátami na životech a zdraví obyvatelstva, velkými škodami na majetku a životním prostředí, včetně životně důležitém zásobování obyvatelstva značného rozsahu vyžadující centrální řízení

KM / Crisis management - Krizový management

Komunikační bezpečnost / Communication security - blast bezpečnosti, která se věnuje technickým otázkám realizace bezpečnosti komunikačních prostředků.

Kritická infrastruktura (KI) / Critical infrastructure - Výrobní i nevýrobní systém, jehož nefunkčnost by mohl mít vážné dopady na bezpečnost, ekonomiku a zachování nezbytného rozsahu dalších základních funkcí státu

Krizová situace (KS) / Crisis, emergency situation - Mimořádná událost, při níž je vyhlášen tzv. krizový stav

Krize / Crisis - Situace, v niž je významným způsobem narušena rovnováha mezi základními charakteristikami systému na jedné straně a postojem okolního prostředí na straně druhé

Krizové plánování / Crisis planning - Aktivita příslušných orgánů krizového řízení zaměřená na minimalizaci (prevenci) možnosti vzniku krizových situací. Hledání nejvhodnějších způsobů protikrizové intervence, optimalizaci metod a forem zvládání těchto nežádoucích jevů (tj. redukci dopadů krizových situací) a stanovení nejracionálnějších a ekonomicky nejvýhodnějších cest obnovy postižených systémů a jejich návratu do nového běžného stavu.

Krizová připravenost / Crisis preparedness - Příprava opatření k řešení vlastních krizových situací a k podílu na řešení krizových situací ve svém okolí

Krizové řízení (KŘ) / Crisis managment, emergency - Soubor řídících činností věcně příslušných orgánů zaměřených na analýzu a vyhodnocení bezpečnostních rizik, plánování, organizování, realizaci a kontrolu činností prováděných v souvislosti s řešením krizové situace

Krizový management (KM) / Crisis management - Krizový management zahrnuje systém a metody řešení řízení mimořádných událostí / krizových situací specializovanými odborníky, kteří tvoří skupinu souhrnně nazývanou krizový management

Krizový plán (KP) / Crisis plan - Souhrnný plánovací dokument, který zpracovávají zákonem stanované subjekty, a který obsahuje souhrn opatření a postupů k řešení krizových situací

Krizový stav (KS) / Crisis state - Legislativní opatření vyhlašované Parlamentem ČR (stav ohrožení státu a válečný stav), vládou ČR (nouzový stav) nebo hejtmanem kraje / primátorem (stav nebezpečí) za účelem řešení krizové situace

Krizový štáb kraje (KŠK) / Crisis district staff - Pracovní orgán kraje (hejtmana) k řešení krizových situací

Krizový štáb určené obce (KŠKUOb) / Crisis municipality staff - Pracovní orgán určené obce (starosty) pro řešení krizových situací

LAN / Local Area Network - Lokální počítačová síť

Likvidační práce (LP) / Salvage, clearance operations - Činnosti k odstranění následků způsobených mimořádnou událostí / krizovou situací

Management rizik / Risk managment - Řízené činnosti, zaměřené k plánování, organizování a kontrole organizace vzhledem k existujícím rizikům.

Mimořádná událost (MU) / Extraordinary incident - Škodlivé působení sil a jevů vyvolaných činností člověka, přírodními vlivy, a také havárie, které ohrožují život, zdraví, majetek nebo životní prostředí a vyžadují provedení záchranných a likvidačních prací

Nezbytná dodávka (ND) / Necessary delivery - Dodávka výrobků, prací a služeb, zajišťována prioritně právnickou osobou a podnikající fyzickou osobou (dodavatelem nezbytné dodávky). Dalším zdrojem můžou být zásoby vytvořené v rámci státních hmotných rezerv, případně v rámci mezinárodní spolupráce a pomoci, bez níž nelze zajistit překonání krizových stavů

Obnovovací (asanační) práce / Renovation works - Činnosti spočívající v revitalizaci životního prostředí a činnosti směřující k únosné obnově životního prostředí, společenského života a materiálních hodnot

Oddělení odpovědností / Responsability department - Postup ochrany, který zajistí provedení některých operací rozdílnými uživateli. Hlavním pravidlem oddělení odpovědností je, že osobě odpovědné za určitou přesně zformovanou operaci nesmí být povoleno tuto operaci i vykonávat.

Odmítnutí služby / Dismissing of service - Ztráta dostupnosti způsobená náhodnou nebo úmyslnou činností uživatele nebo výpadkem systému, které ovlivňují funkčnost IS.

Ochrana obyvatelstva (OO) / Civil protection - Plnění úkolů civilní obrany v době ozbrojeného konfliktu a civilní ochrany mimo něj. Jedná se zejména o varování, evakuaci, ukrytí, zabezpečení nouzového přežití obyvatelstva a další opatření k zabezpečení ochrany života, zdraví a majetku obyvatel ČR

OS / Operating system - Operační systém

Produkt / Product - Softwarový nebo hardwarový výrobek IT zabezpečující funkce, navržené pro přímé využití nebo k začlenění do různých systémů.

Provozovatel systému / System operator - Subjekt, který provádí alespoň některé informační činnosti související s informačním systémem.

Přístupové právo / Access right - Uživateli nebo subjektu přidělené oprávnění uskutečňovat typ přístupu.

Riziko / Risk - Nekvantifikovatelná náhoda, při které je aktivum vystaveno možnosti vzniku škody. Vyjadřuje pravděpodobnost ohrožení aktiva, míru nebezpečí, že se uplatní hrozba a dojde k nežádoucímu výsledku vedoucímu ke vzniku škody.

Role / Role, Status - Určená množina funkčně příbuzných činností a potřebných autorizací pro provádění těchto činností, jež může být přidělena uživatelům.

Server / Server - Uzlový počítač sítě

Severoatlantická aliance (NATO) / North Atlantic Treatment Organization - Organizace Severoatlantické smlouvy, jejímž hlavním cílem je vytvoření společenství kolektivní obrany k ochraně svobody, bezpečnosti a stability členů severoatlantické aliance

Správce systému / System administrator - Subjekt, který zabezpečuje zpracování informací a informační systém provozuje

SW / Software - Programové vybavení

UPS / Uninterruptible Power Supply - Nepřerušitelný zdroj napájení

Uživatel / User - Součást systému, která v rozsahu přidělených pravomocí využívá informace (služby, funkce) systému, zajišťuje vstupní informace potřebné pro identifikaci objektu nebo prostředku.

VPN / Virtual Private Network - Virtuální privátní síť

Zbytkové riziko / Residual risk - Riziko, zbývající po uplatnění bezpečnostních opatření ke zvládání rizik.

Zranitelnost / Vulnerability - Slabina v systému, která umožňuje působení hrozby na slabá místa bezpečnosti IS

Zvládání rizik / Risk managing - Proces výběru a přijímání opatření pro snížení rizik.

13 Přílohy

1x Systém řízení přístupu k dokumentům UTIMACO LeakProof