



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA PODNIKATELSKÁ
ÚSTAV INFORMATIKY

FACULTY OF BUSINESS AND MANAGEMENT
INSTITUTE OF INFORMATICS

METODIKA ZAVEDENÍ SÍŤOVÉ BEZPEČNOSTI V SOFTWAREOVÉ SPOLEČNOSTI

IMPLEMENTATION METHODOLOGY OF NETWORK SECURITY IN THE SOFTWARE COMPANY

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

AUTOR PRÁCE

AUTHOR

Ing. JAKUB TOMAGA

VEDOUCÍ PRÁCE

SUPERVISOR

Ing. PETR SEDLÁK

BRNO 2013

ZADÁNÍ DIPLOMOVÉ PRÁCE

Tomaga Jakub, Ing.

Informační management (6209T015)

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách, Studijním a zkušebním řádem VUT v Brně a Směrnicí děkana pro realizaci bakalářských a magisterských studijních programů zadává diplomovou práci s názvem:

Metodika zavedení síťové bezpečnosti v softwarové společnosti

v anglickém jazyce:

Implementation Methodology of Network Security in the Software Company

Pokyny pro vypracování:

Osnova zadání:

Úvod

Vymezení problému a cíle práce

Teoretická východiska práce

Analýza problému a současná situace

Vlastní návrhy řešení, přínos návrhů řešení

Závěr

Seznam použité literatury

Přílohy

Seznam odborné literatury:

ČSN ISO/IEC 27001 Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnostiinformací - Požadavky. Praha: Český normalizační institut, 2006.

ČSN ISO/IEC 27002 Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnostiinformací - Soubor postupů. Praha: Český normalizační institut, 2008.

ISO/IEC 27033-1 Network security overview and concepts. 2009

ISO/IEC 27033-2 Guidelines for the design and implementation of network security. 2012

POŽÁR, J. Informační bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005.

ISBN 80-86898-38-5.

Vedoucí diplomové práce: Ing. Petr Sedlák

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2012/2013.

L.S.

doc. RNDr. Bedřich Půža, CSc.
Ředitel ústavu

doc. Ing. et Ing. Stanislav Škapa, Ph.D.
Děkan fakulty

V Brně, dne 23.05.2013

Abstrakt

Diplomová práce se zabývá problematikou síťové bezpečnosti a možnostmi jejího zavedení v prostředí existující softwarové společnosti. Popisuje nasazení managementu bezpečnosti informací s úzkou specializací právě na počítačové sítě. Pro analyzovanou společnost je navrhnutá síťová bezpečnostní politika a možné úpravy v síťové infrastruktuře za účelem zvýšení bezpečnosti. Ke všem částem je vytvořené také finanční zhodnocení.

Abstract

This thesis deals with network security and its deployment in the real environment of the software company. The thesis describes information management framework with a specific concentration on computer networks. Network security policy is designed as well as network infrastructure modifications in order to increase the level of security. All parts of the solution are also analyzed from financial point of view.

Klíčová slova

ISMS, bezpečnost, síťová bezpečnost, bezpečnostní politika, ISO 27001, ISO 27033, síťová infrastruktura, data.

Keywords

ISMS, security, network security, security policy, ISO 27001, ISO 27033, network infrastructure, data.

Citace

TOMAGA, J. *Metodika zavedení síťové bezpečnosti v softwarové společnosti*. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2013. 78 s. Vedoucí diplomové práce Ing. Petr Sedlák.

Prohlášení

Prohlašuji, že předložená diplomová práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

.....

Jakub Tomaga

24. mája 2013

Poděkování

Děkuji vedoucímu diplomové práce Ing. Sedlákovi za metodické vedení, pedagogickou a odbornou pomoc při zpracování mé diplomové práce.

Obsah

Úvod	8
Vymedzenie problému a ciele práce	9
1 Analýza súčasného stavu	10
1.1 Popis spoločnosti	10
1.2 Zhodnotenie stavu	10
2 Teoretické východiská riešenia	13
2.1 Model PDCA	13
2.2 Systém riadenia bezpečnosti informácií	15
2.2.1 Ustanovenie ISMS	15
2.2.2 Zavádzanie a prevádzka ISMS	18
2.2.3 Monitorovanie a preskúvanie ISMS	21
2.2.4 Údržba a zlepšovanie ISMS	23
2.2.5 Sústavné zlepšovanie ISMS	23
2.2.6 Odstraňovanie nedostatkov ISMS	24
2.3 Normy v oblasti bezpečnosti IT	24
2.3.1 Normy ISO/IEC rady 27000	24
2.3.2 Norma ISO/IEC 27033	25
2.3.3 Norma ISO/IEC 18028	27
2.4 Analýza rizík	27
2.4.1 Základné pojmy analýzy rizík	28
2.4.2 Vzťahy v analýze rizík	30
2.5 Sieťová bezpečnosť	31
2.5.1 Potreba sieťovej bezpečnostnej politiky	32
2.5.2 Riziká sieťovej konektivity	33
2.5.3 Súčasti sieťovej bezpečnostnej politiky	33
2.5.4 Kroky potrebné na zostavenie sieťovej bezpečnostnej politiky	35
2.6 Referenčná architektúra pre sieťovú bezpečnosť	37
2.6.1 Bezpečnostné dimenzie	37
2.6.2 Bezpečnostné vrstvy	39
2.6.3 Bezpečnostné roviny	40
2.6.4 Bezpečnostné hrozby	41
2.7 Bezpečnosť sieťovej infraštruktúry	41
2.7.1 Kľúčovaná konektivita	42
2.7.2 Zabezpečenie siete (príslušenstvo)	43

3 Návrh riešenia	44
3.1 Správa o hodnotení rizík	44
3.1.1 Identifikácia aktív a ich hodnotenie	44
3.1.2 Identifikácia hrozieb a ich pravdepodobnosť	45
3.1.3 Vyhodnotenie miery rizík	46
3.2 Sieťová bezpečnostná politika	47
3.2.1 Prípustné užívanie	48
3.2.2 Prípustné šifrovanie	53
3.2.3 Pokyny pre antivírusovú ochranu	54
3.2.4 Práca s heslami	54
3.2.5 Bezpečnosť komunikačných zariadení	57
3.2.6 Zabezpečenie pre router a switch	59
3.2.7 Zabezpečenie serverov	60
3.2.8 Audit komunikačných zariadení a serverov	62
3.2.9 Plán zvládania katastrof	64
3.2.10 Celkové náklady sieťovej bezpečnostnej politiky	65
3.3 Návrh zabezpečenia sieťovej infraštruktúry	66
3.3.1 Zhrnutie pre vedúcich pracovníkov	67
3.3.2 Požiadavky návrhu siete	67
3.3.3 Riešenie návrhu siete	68
3.3.4 Náklady	71
Zhodnotenie a záver	73
Literatúra	74
Zoznam skratiek	76
Zoznam obrázkov	77
Zoznam tabuliek	78

Úvod

Počítačová bezpečnosť je v poslednej dobe veľmi aktuálnou témou kvôli častým výskytom bezpečnostných incidentov v rôznych oblastiach ľudskej činnosti. S rozvojom komunikačných technológií sa veľká časť obchodných aktivít podnikateľských subjektov presunula do prostredia Internetu. Spoločnosti využívajú voľne dostupné služby na podporu podnikania, ponúkajú svoje vlastné produkty on-line zákazníkom a v neposlednom rade spolupracujú s ostatnými subjektmi prostredníctvom zdieľania informácií. Práve tento nárast on-line pôsobenia firiem je dôvodom toho, že sa komunikačné technológie často stávajú terčom útokov. Nejde len o útoky na firemné aktíva z vonku, ale aj o útoky priamo z radov zamestnancov. Spoločným prvkom týchto dvoch prístupov je počítačová sieť, ktorá poskytuje prostredie pre takéto útoky.

Trend poslednej doby je chrániť spoločnosť využitím systematického prístupu riadenia bezpečnosti informácií. Najvšeobecnejší prístup má však veľmi široký záber a je takmer nemožné pokryť všetky oblasti, ktoré si vyžadujú ochranu. Úzka špecializácia umožňuje riešiť problémy do hĺbky namiesto riešenia do šírky. Práve tento spôsob riešenia bezpečnostných problémov využíva táto diplomová práca. Vy-medzuje nasadenie bezpečnosti informácií v konkrétnej spoločnosti na oblasť počítačových sietí. Poskytuje sadu bezpečnostných zásad špecifikovaných presne pre potreby analyzovanej firmy.

Práca ďalej obsahuje návrh zvýšenia bezpečnosti sieťovej infraštruktúry pomocou novej technológie od spoločnosti Panduit s názvom *Network Infrastructure Security Solution*. Pri riešení všetkých bezpečnostných problémov sa práca opiera o bezpečnostné normy rodiny ISO/IEC 27000. Keďže je hlavným zameraním práce sieťová bezpečnosť, prezentované riešenia sú založené na sade noriem ISO/IEC 18028, ktoré sa zaoberajú práve sieťovou bezpečnosťou. Sieťové bezpečnostné normy ISO/IEC 27033 nie sú v dobe písania práce plne v platnosti.

Všetky navrhované zmeny sú doplnené o finančné náklady, ktoré je potrebné vynaložiť na uskutočnenie jednotlivých zmien.

Vymedzenie problému a ciele práce

Práca sa zaoberá bezpečnosťou počítačových sietí z pohľadu spoločnosti, ktorá má záujem zaviesť management informačnej bezpečnosti vyprofilovaný na túto oblasť. Práve sieťové prostredie skrýva pomerne mnoho veľmi cenných aktív, ktoré môže spoločnosť ohroziť nedostatočným zabezpečením siete a ich vystavením verejnosti. Bezpečnostné hrozby čoraz viac súvisia s Internetom, preto by mal existovať záujem zo strany podnikateľských subjektov chrániť svoje lokálne siete pripojené priamo k tejto globálnej sieti. V dnešnej dobe ja každá firemná sieť pripojená na Internet a preto je téma bezpečnosti veľmi aktuálna.

Požiadavkou na výstup práce je sada bezpečnostných zásad z oblasti počítačových sietí, keďže tie v súčasnosti spoločnosť nemá definované a vzhľadom na rast je len otázkou času, kedy sa začnú pravidelne vyskytovať incidenty a spoločnosť nebude mať v rukách žiadny nástroj na vyvodenie zodpovednosti. V rámci tejto časti práce dôjde k definovaniu sieťových bezpečnostných zásad na základe správy o hodnotení rizík v sieťovom prostredí spoločnosti. V rámci tejto požiadavky je potrebné zohľadniť súčasný stav. Spoločnosť nemá záujem o výraznú modifikáciu sieťovej architektúry, ak to nebude vyslovene nevyhnutné. Sama nie je zodpovedná za kompletne sieťové riešenie a komunikácia o zmenách je pomerne komplikovaná. Sada bezpečnostných zásad je to, o čo má spoločnosť primárny záujem.

Spoločnosť je zároveň otvorená aj iným možnostiam vylepšiť aktuálnu bezpečnostnú situáciu v oblasti počítačových sietí. Uvedomuje si cenu dát, ktoré sa v jej firemnej sieti nachádzajú a chce sa uistiť, že z hľadiska bezpečnosti bude pripravená na možné budúce situácie.

Kapitola 1

Analýza súčasného stavu

1.1 Popis spoločnosti

Analyzovaná spoločnosť sa v rámci svojej podnikateľskej činnosti zaoberá vývojom softwaru a poradenstvom v oblasti IT všeobecne, ako aj v oblasti interných firemných hrozieb. Software tvorí konkrétnym zákazníkom priamo na mieru podľa požiadaviek. Primárne sa ale zamestnanci spoločnosti zameriavajú na vývoj bezpečnostného softwaru, ktorým sa spoločnosť prezentuje navonok. Spoločnosť podniká v oblasti tvorby softwaru od roku 2004.

Spoločnosť zamestnáva viac ako 40 odborníkov, kde väčšinu tvoria stáli zamestnanci. Ďalej využíva spoluprácu s externými konzultantmi a profesionálnymi vývojármi. Zároveň vypisuje prakticky zamerané bakalárske a diplomové práce pre študentov z oblasti IT. V poslednej dobe do spoločnosti prichádza pomerne veľa nových pracovníkov, ktorí prechádzajú z konkurenčných firiem.

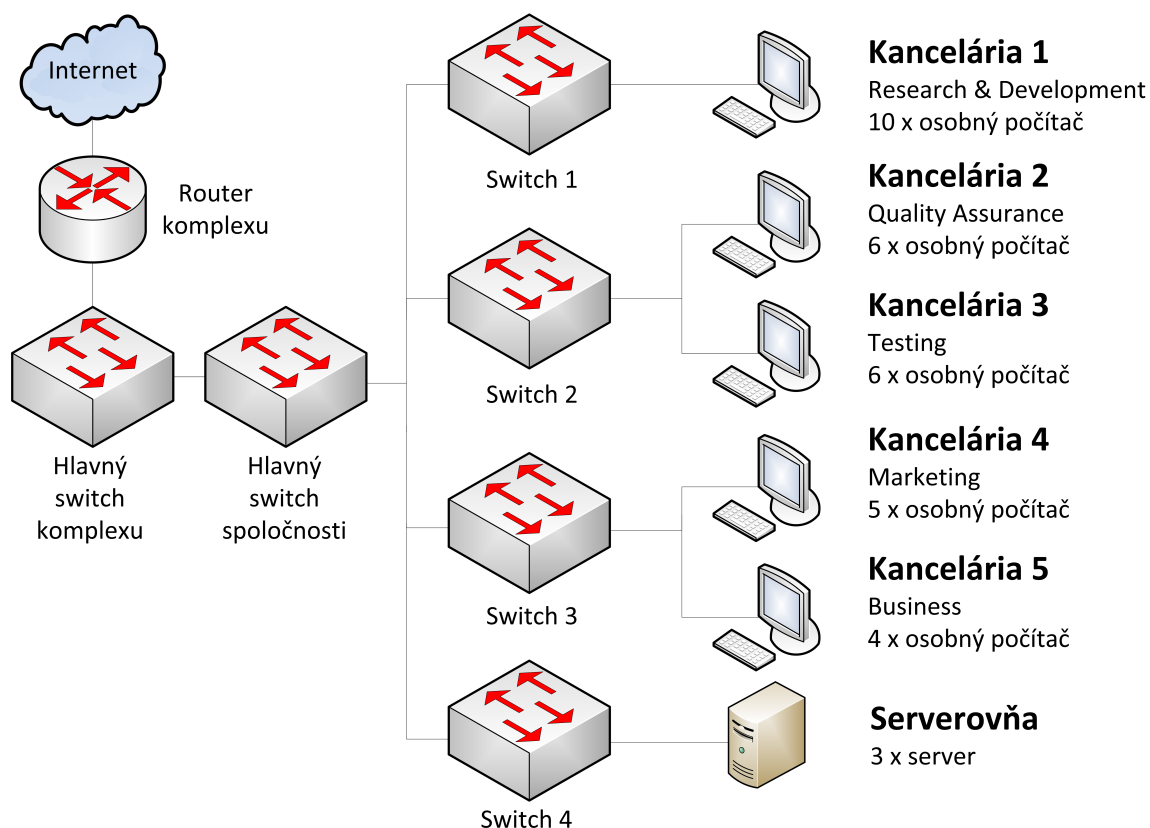
V súčasnosti má spoločnosť dve pobočky na území Českej republiky. V rámci partnerskej siete spolupracuje s distribútormi softwaru po celom svete. Zákaznícka báza je pomerne rozsiahla, medzi zákazníkov patria súkromné osoby, rovnako ako aj korporátne spoločnosti.

1.2 Zhodnotenie stavu

Spoločnosť nemá zavedený management informačnej bezpečnosti, zároveň neexistuje bezpečnostná politika ani žiadne bezpečnostné zásady. Čo odzrkadľujú aj požiadavky spoločnosti na zlepšenie súčasného stavu. Povedomie o informačnej bezpečnosti v spoločnosti je na dobrej úrovni a vedenie preukázalo záujem spolupracovať pri zlepšení stavu jasne definovanými požiadavkami.

Vzhľadom na to, že hlavnou požiadavkou je zavedenie managementu sieťovej bezpečnosti a vytvorenie vhodných bezpečnostných zásad (politik) odzrkadľujúcich súčasný stav, zameriame sa na súčasnú sieťovú situáciu. Spoločnosť sa nachádza v komplexe kancelárskych priestorov a čiastočne zdieľa sieťové prvky s ostatnými firmami. Tieto sieťové prvky spravuje spoločnosť poskytujúca kancelárske priestory.

Sieťová architektúra je zobrazená na obrázku 1.1. Hlavný switch spoločnosti je priamo pripojený na hlavný switch komplexu. Sieť je tým pádom fyzicky oddelená a spoločnosť môže spravovať lokálnu komunikáciu vo vlastnej réžii. Každý switch na



Obr. 1.1: Sieťová architektúra spoločnosti (Zdroj: Vlastná analýza)

nižšej úrovni slúži na oddelenie kancelárií. Kancelárie Quality Assurance a Testing sú pripojené na jeden switch, rovnako sú kancelárie Marketing a Business pripojené na jeden switch. Všetky servery spoločnosti sú v jednej miestnosti pripojené na samostatný switch.

Obrázok 1.1 zobrazuje aj počet osobných počítačov v jednotlivých kanceláriách. Na všetkých osobných počítačoch je nainštalovaný operačný systém Microsoft Windows 7 Pro. Všetky zariadenia typu switch sú 24-portové. Z toho vyplýva aj počet využitých a nevyužitých portov na jednotlivých zariadeniach. Zamestnanci v kanceláriách, kde prebieha vývoj, quality assurance a testing využívajú tri nasledujúce aplikačné servery (operačný systém Microsoft Windows Server 2012):

SQL a FTP server

Tento jeden server sa využíva ako SQL aj ako FTP server. Zamestnanci využívajú obe služby za účelom plnenia pracovných povinností.

SQL server slúži na ukladanie rozsiahlej databázy, ktorú využíva spoločnosť na testovanie vlastného produktu (vyvíjaný bezpečnostný software ukladá záznamy o činnosti v podobe SQL tabuliek). Na tento server sa pripájajú zamestnanci zodpovední za testing pri rutinných aj záťažových testoch. Vývojári majú na server rovnako prístup, dostupné databázy používajú pri vývoji škálovateľných softwarových riešení.

Na FTP server sa ukladajú inštalateľné balíky vyvíjaného produktu pre partnerov.

To znamená, že na FTP server sa pristupuje pravidelne z vonku. Okrem inštalačných balíčkov obsahuje FTP server súkromné zložky jednotlivých zamestnancov, ktorí ich využívajú napr. na ukladanie rôznych dokumentácií.

TFS server

Team Foundation Server 2012 využíva celá spoločnosť na podporu vývoja, či už ide o správu zdrojových kódov, zber dát, správu vývojových projektov apod.

Hyper-V server

Hyper-V server spoločnosť využíva pri testovaní jednotlivých verzií produktu a jeho kompatibilitu s garantovanými operačnými systémami.

Spoločnosť nemá vo svojej sieti vlastný e-mailový server, ale využíva jednu z aplikácií Google Apps, konkrétne Google Mail. Okrem tejto aplikácie, využíva spoločnosť na správu dokumentov aplikáciu Google Docs. Zamestnanci v prípade vzdialeného prístupu z domu nevyužívajú VPN ale na firemné stanice sa pripájajú pomocou aplikácie TeamViewer, ktorá však z bezpečnostného hľadiska plne spĺňa požiadavky normy ISO/IEC 27001 (1).

Kapitola 2

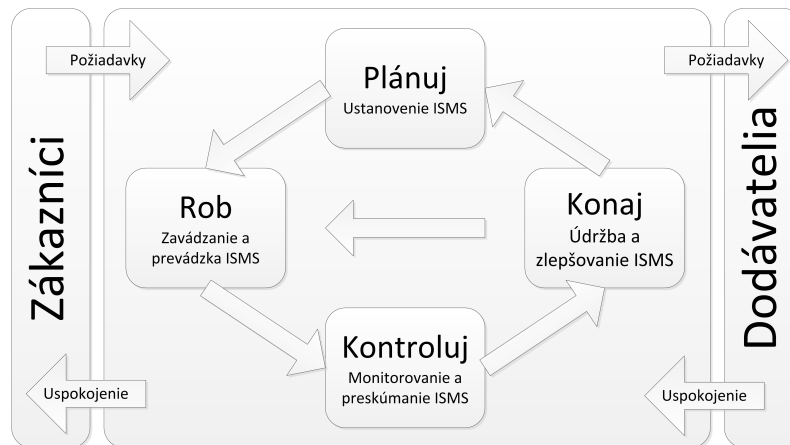
Teoretické východiská riešenia

2.1 Model PDCA

Koncept modelu PDCA (*Plan-Do-Check-Act*) poskytuje schematicke vyjadrenia životného cyklu celého integrovaného systému riadenia alebo jeho komponenty a zároveň jej zaisťuje tzv. spätnú väzbu. Koncept modelu PDCA je znázornená na obrázku 2.1. Táto časť práce vychádza z (2).

Tento prístup umožňuje používať zhodné metódy, metodiky a postupy na riadenie každej komponenty integrovaného systému riadenia a IMS (*Integrated Management System*) ako celku. Okrem riadenia komponent integrovaného systému riadenia je dôležité vedieť sledovať a vyhodnocovať ich *účinnosť* a *účelnosť*. Účelnosť komponent sa meria obvykle porovnaním s niektorým medzinárodným štandardom (normou). Tieto normy sú systémovým návodom ako vykonať správne kroky, resp. podľa najlepších skúseností (*best practices*), ktoré vznikli v rôznych častiach sveta a ktoré sa presadili v praxi. Avšak môže ísť o jedny z najlepších skúseností, aké boli svetovou praxou vymedzené, nie je možné ich preberať mechanicky a bez kreatívneho prístupu. Každá organizácia má svoje vlastné špecifiká, ktoré nútia zodpovedného tvorca integrovaného systému riadenia modifikovať odporúčenia medzinárodných noriem. Pokiaľ by chcel napríklad manažér v malej organizácii aplikovať nasadenie všetkých doporučených organizačných štruktúr tak, ako sú uvedené v medzinárodných štandardoch, vyzeralo by to veľmi nešikovne. Štandardy majú síce celosvetovú platnosť, ale špecifiká jednotlivých organizácií, firiem, krajín a kultúr musia vystihnúť lokálni odborníci. Tým platnosť medzinárodných noriem nie len potvrdia, ale myšlienky v nich uložené ešte zúročia do väčších efektov pre cieľovú organizáciu. Účinnosť potom predstavuje postupy ako vykonať kroky správne. Je meraná vo vnútri životného cyklu buď komponentu IMS alebo ako celku a to obvykle sústavou ukazovateľov. Hlavné úseky dôležité pre meranie účinnosti sú:

- v 1. etape životného cyklu - Plánuj
 - definícia cieľov komponenty IMS a stanovenie spôsobov (postupov, metódik) ich merania,
 - stanovenie ukazovateľov na meranie dosiahnutia cieľov,
 - stanovenie ukazovateľov na merania prevádzky komponenty,



Obr. 2.1: Model PDCA použitý na riadenie bezpečnosti informácií (Prevzaté z (2))

- stanovenie spôsobu zberu dát na vyhodnocovanie prevádzky komponenty a na vyhodnocovanie dosiahnutia jej cieľov,
- stanovenie zodpovedajúcich organizačných štruktúr, zodpovedných za zber dát a za vyhodnocovanie efektívnosti komponenty IMS,
- návrh právomocí a stanovenie reportovacích povinností týmto organizačným štruktúram.

- **v 2. etape životného cyklu - Rob**

- realizácia navrhnutých organizačných štruktúr v systéme riadenia organizácie vrátane presadenia ich právomocí, zodpovedností a reportovacích povinností,
- zavedenie požadovaných veličín a ukazovateľov do systému riadenia organizácie,
- nastavenie spôsobov ich sledovania a zaistenie prenosu príslušných dát zodpovedajúcim organizačným štruktúram.

- **v 3. etape životného cyklu - Kontroluj**

- stanovenie základných hodnôt sledovaných ukazovateľov, ktoré určujú štartovacie nastavenie systému merania efektívnosti komponenty,
- zaistenie práce príslušných organizačných štruktúr zodpovedných za vyhodnocovanie účinnosti komponenty IMS.

- **v 4. etape životného cyklu - Konaj**

- prevedenia nápravných opatrení a preventívnych činností, založených na základe vyhodnotení prevedených vedením organizácie,
- permanentné zlepšovanie IMS.

Súčasťou modelu PDCA je aj dokumentácia každej jeho etapy. Dokumentácia je často vnímaná ako najnáročnejšia a najneprijemnejšia súčasť zavedenia integrovaného systému riadenia. V rámci zachovania objektivity pohľadu na model PDCA a

integrovaný systém riadenia je nutné zdôrazniť, že dokumentácia je jednou z kľúčových častí celého modelu PDCA. Aby bolo možné prevádzať akýkoľvek *reengineering* ľubovoľných procesov, je nevyhnutné dodržať zásady procesného riadenia. To v praxi znamená:

- identifikovať procesy,
- procesy popísať a zdokumentovať,
- na základe dokumentácie procesy riadiť a
- následne ich priebeh optimalizovať.

2.2 Systém riadenia bezpečnosti informácií

V dnešnej dobe sa žiadna organizácia nemôže zaobiť bez riadenia bezpečnosti informácií. Bezpečnosť sa stala nedeliteľnou súčasťou každodenného riadenia vnútornej kultúry organizácie. Aby sme boli schopní riadiť bezpečnosť cielene a efektívne rozvíjať, je potrebné na tento prvok riadenia nahliadať ako na systém riadenia bezpečnosti informácií.

Systém riadenia bezpečnosti informácií - ISMS (*Information Security Management System*) je časť celkového systému riadenia organizácie, založená na prístupe (organizácie) k rizikám činností, ktorá je zameraná na ustanovenie, zavádzanie, prevádzku, monitorovanie, preskúvanie, údržbu a zlepšovanie bezpečnosti informácií.

Systém riadenia bezpečnosti informácií je podobný ako ostatné systémy riadenia založený na modeli PDCA. Využitie tohto modelu pre ISMS je zachytené na obrázku, na ktorom boli definované nasledujúce štyri etapy celého systému riadenia:

- **Ustanovenie ISMS** - cieľom tejto etapy je spresniť rozsah a hranice, ktorých sa riadenie bezpečnosti týka, stanoviť jasné manažérske zadanie a na základe ohodnotenia rizík vybrať nevyhnutné bezpečnostné opatrenia.
- **Zavádzanie a prevádzka** - cieľom tejto etapy je efektívne a systematicky presadiť vybrané bezpečnostné opatrenia.
- **Monitorovanie a preskúvanie ISMS** - hlavným cieľom tejto etapy je zaisťovanie spätnej väzby a pravidelného sledovania a hodnotenia úspešných i nedostatočných stránok riadenia bezpečnosti informácií.
- **Údržba a zlepšovanie ISMS** - cieľom poslednej etapy je realizácia možností zlepšovania systému alebo odstraňovanie zistených slabín a nedostatkov.

2.2.1 Ustanovenie ISMS

Prvou etapou budovania ISMS je ustanovenie systému, pri ktorom sú spresnené správne formy riešenia bezpečnosti informácií. Okrem definície obsahu ISMS a odsúhlasenia Prehlásenia o politike ISMS (záväzok vedenia podporovať informačnú

bezpečnosť) patria medzi kritické činnosti prevedenie analýzy rizík a výber vhodných bezpečnostných opatrení na zníženie vplyvu existujúcich rizík. Táto etapa presadzovania ISMS by mala byť ukončená súhlasom vedenia so zavedením ISMS podľa potreby organizácie zistených pri analýze a zvládaní rizík ISMS. Ustanovenie ISMS je možné rozdeliť na nasledujúce skupiny činností:

- definovanie rozsahu, hraníc a väzieb ISMS,
- definovanie a odsúhlasenie Prehlásenia o politike ISMS,
- analýzy a zvládanie rizík,
 - definovanie prístupu organizácie k hodnoteniu rizík,
 - identifikácia rizika vrátane určenia aktív a ich vlastníkov,
 - analýza a vyhodnotenie rizík,
 - identifikácia a ohodnotenie variant pre zvládanie rizík,
 - výber cieľov opatrení a jednotlivých opatrení na zvládanie rizík,
- súhlas vedenia organizácie s navrhovanými zvyškovými rizikami a so zavedením ISMS,
- príprava Prehlásenia o aplikovateľnosti.

Táto etapa budovania má zásadné dopady na fungovanie ISMS behom jeho celého životného cyklu.

Definícia rozsahu a hraníc ISMS

Prvou úlohou riadenia bezpečnosti je spresnenie rozsahu a hraníc, v ktorých je ISMS uplatňované. V rámci tejto časti zavádzania ISMS je dôležité si pripomenúť charakteristické činnosti a ciele organizácie, používanú organizačnú štruktúru, umiestnenie lokalít či využívané technológie na prenos a spracovanie informácií atd. Na tomto základe je možné stanoviť počiatočný rozsah a hranice ISMS, ktorý musí vždy pokryť celú organizáciu.

Z hľadiska praktického presadenia ISMS je možné sa k stanoveniu rozsahu postaviť dvoma základným spôsobmi. V prvom prípade je rozsah ISMS od začiatku identický s rozsahom celej organizácie. Základná výhoda spočíva v tom, že riadenie od začiatku rieši bezpečnosť informácií v celej organizácii. To vyžaduje pomerne významné investície z hľadiska spotreby zdrojov a financií a nie vždy sú realizované všetky plánované a očakávané prínosy riadenia bezpečnosti. V mnohých prípadoch veľkosť projektov býva pre rozvoj bezpečnosti skôr na škodu. Inou možnosťou je definovaný rozsah ISMS na začiatku obmedziť ISMS aplikovať len na jasne definovanú časť organizácie napr. vybranú pobočku, určený organizačný celok či najčastejšie ucelený informačný systém. Nemusí nutne ísť o najdôležitejšiu časť organizácie. Skôr je vhodné vybrať tú časť (úsek, organizačnú jednotku), ktorá je otvorená zavádzaniu novinek a je ochotná zavádzať zmysluplné zmeny a zlepšenia.

Významnou výhodou riešení, ktoré sa sústredia na čiastkové celky, je skutočnosť, že je možné sústrediť vyššiu mieru úsilia do zvolenej oblasti a v tomto obmedzenom

rozsahu zvládnuť dve neľahké úlohy. Prvým je obhájenie účelnosti a potrebnosti systematického riešenia bezpečnosti. To nie je vždy úplná samozrejmosť a možnosť predstavenia výhod na základe praktických skúseností je vždy výhodou.

Druhou úlohou je dôsledné zvládanie všetkých požiadaviek ISMS pri ich praktickom presadzovaní. Fungovanie a kultúra organizácií bývajú veľmi odlišné a voľba správnych a účinných spôsobov na presadenie ISMS nie je jednoduchá ani pre osoby, ktoré disponujú bohatými skúsenosťami. Osoby, ktorých skúsenosti sú menšie, si potrebujú overiť, ako teoretické pravidlá úspešne aplikovať v reálnom živote. Ten je na rozdiel od teórií plný rozličných osobných a skupinových záujmov, bežných odchýlok, drobných chýb či koncepčných nedostatkov a ďalších nepredvídateľných záľudností. A práve zúžením rozsahu ISMS obmedzujeme aj počet súvisiacich problémov, nerozumení či odmietnutí rozvoja.

Prehlásenie o politike ISMS

Druhým krokom je definícia prehlásenia o politike ISMS, ktoré vzniká na základe špecifických potrieb danej organizácie. Z praktického hľadiska je dôležité, aby politika ISMS:

- spresnila ciele ISMS a definovala základný smer a rámec na riadenie bezpečnosti informácií,
- zohľadnila ciele a požiadavky organizácie a súvisiace zákonné, regulatívne a zmluvné požiadavky,
- vytvorila potrebné väzby na vybudovanie a údržbu ISMS v danej organizácii (zohľadnila jej stratégiu, organizačnú štruktúru, používané procesy apod.),
- stanovila kritériá, podľa ktorých sú popisované a hodnotené riziká,
- bola schválená vedením organizácie.

Politika ISMS je rozsahom krátky, ale významom veľmi dôležitý dokument, pretože prezentuje záujem vedenia organizácie o riadenie bezpečnosti informácií a definuje kľúčové podmienky na ohodnotenie rizík, čo je základom pre celý ISMS. Správne definovaná politika ISMS môže veľmi uľahčiť budúce presadzovanie pravidiel a požiadaviek na bezpečnosť informácií v organizácii.

Pravidlá a postupy riadenia rizík

Riadenie rizík je kľúčovým nástrojom na systematické riadenie bezpečnosti informácií. Presná znalosť skutočných rizík rozhoduje o výbere a presadení vhodných bezpečnostných opatrení schopných znížiť negatívne dopady týchto rizík. Dobrá a presná znalosť bezpečnostných opatrení vedie k účinnému vynakladaniu úsilia pri presadzovaní bezpečnostných opatrení, ktoré tak prinášajú väčšiu efektívnosť. Riadenie rizík je preto základom pre každý systém riadenia bezpečnosti informácií a navyše podstatným spôsobom ovplyvňuje efektívnosť fungovania celého ISMS.

Súhlas vedenia so zavedením ISMS a so zvyškovými rizikami

Na základe výsledkov riadenia rizík by mali byť pripravené dva formálne kroky, v ktorých vedenie organizácia odsúhlasí zistené skutočnosti. Tu je potrebné, aby vedenie organizácie odsúhlasilo návrh bezpečnostných opatrení, ktoré sú nutné na zníženie bezpečnostných rizík. Súčasne s tým, by sa vedenie malo vyjadriť, či sú existujúce zvyškové riziká pre chod organizácie prijateľné alebo nie. V prípade, že vedenie zistí, že výsledky riadenia rizík nevedú k požadovanej úrovni bezpečnosti, je možné včas upraviť návrh bezpečnostných opatrení.

Tieto dva dokumenty predstavujú základné východiská na ďalšiu prácu v riadení bezpečnosti. Návrh bezpečnostných opatrení slúži ako základ k príprave budúcich bezpečnostných projektov (vrátane stanovenia priorít ich realizácie, uvoľnenie kapacít organizácie na ich riešenie apod.), ktoré by mali zlepšiť úroveň bezpečnosti informácií v organizácii. Súhlas so zvyškovými rizikami potom predstavuje súhlas vedenia s určitou mierou rizika pri ochrane informácií v organizácii.

Prehlásenie o aplikovanosti

Prehlásenie o aplikovanosti je povinným dokumentom pre organizácie, ktoré usilujú o zhodu svojho ISMS s normou ISO/IEC 27001. Tento dokument musí obsahovať ciele opatrení a jednotlivé bezpečnostné opatrenia, ktoré boli pre daný ISMS vybrané na pokrytie existujúcich bezpečnostných rizík.

V praxi je prehlásenie o aplikovateľnosti najdôležitejším dokumentom, ktorý posilňuje systémové väzby ISMS. Doporučené formáty dokumentu najčastejšie zobrazujú maticu vzťahov medzi zistenými rizikami a vybranými bezpečnostnými opatreniami. Z tejto matice sú potom jasné dôvody pre nasadenie bezpečnostných opatrení a vlastná realizácia môže na tieto dôvody vhodným spôsobom reagovať (napr. miera fyzickej bezpečnosti môže byť podriadená skutočným hrozbám).

2.2.2 Zavádzanie a prevádzka ISMS

Táto etapa životného cyklu sa sústreďuje na presadzovanie všetkých bezpečnostných opatrení tak, ako boli navrhnuté v predchádzajúcej etape pri ustanovení ISMS. Dôležité je predovšetkým pripraviť čiastkové plány, kde sú spresnené termíny, zodpovedné osoby apod. Všetky bezpečnostné opatrenia by mali byť zdokumentované v tzv. Príručke bezpečnosti informácií a malo by dôjsť k vysvetleniu bezpečnostných princípov všetkým užívateľom a manažérom.

Behom tejto etapy zavádzania ISMS je nevyhnutné vykonať nasledujúce činnosti:

- Formulovať dokument Plán zvládania rizík a začať s jeho zavádzaním.
- Zaviesť plánované bezpečnostné opatrenia a sformulovať príručku bezpečnosti informácií, ktorá spresní pravidlá a postupy aplikovaných opatrení v definovaných oblastiach bezpečnosti informácií.
- Definovať program budovania bezpečnostného povedomia a vykonať prípravu a zaškolenie všetkých užívateľov, manažérov a odborných pracovníkov z úseku informatiky a hlavne z oblasti riadenia bezpečnosti.

- Spresniť spôsoby merania účinnosti bezpečnostných opatrení a sledovať stanovené ukazovatele.
- Zaviesť postupy a ďalšie opatrenia na rýchlu detekciu a reakciu na bezpečnostné incidenty.
- Riadiť zdroje, dokumenty a záznamy ISMS.

Plán zvládania rizík

Plán zvládania rizík je dôležitým dokumentom, ktorý popisuje všetky činnosti ISMS, ktoré sú potrebné na riadenie bezpečnostných rizík, stanovené ciele a priority týchto činností ISMS, obmedzujúce faktory a potrebné zdroje (personálne, finančné, technologické, znalostné apod.). Jeho významným prvkom je tiež jednoznačné určenie osobnej zodpovednosti za prevádzanie jednotlivých naplánovaných činností.

Východiskom pre zostavenie plánu zvládania rizík sú predovšetkým dva základné zdroje informácií o ISMS. V počiatočných fázach ide o podklady, ktoré sú o ISMS získané pri ustanovení ISMS (predovšetkým ide o výsledky riadenia rizík zdokumentované v správe o hodnotení rizík a v prehlásení o aplikovateľnosti). Tieto dva dokumenty určujú bezpečnostné potreby a mieru ich realizácie. Na základe rozdielu medzi bezpečnostnými potrebami a skutočným stavom presadenia bezpečnostných opatrení je možné dobre definovať potrebné činnosti na zlepšenie stavu ISMS.

Druhým významným zdrojom dôležitých údajov pre tvorbu plánu zvládania rizík sú podnety získané pri pravidelných prehodnoteniach ISMS vedením organizácie, ktoré by mali byť zhromažďované v správe o stave ISMS. Tieto informácie dovoľujú do plánu zvládania rizík premietnuť skúsenosti s fungovaním ISMS.

Príručka bezpečnosti informácií

Pri posudzovaní vybraných bezpečnostných opatrení je potrebné definovať stanovené bezpečnostné pravidlá a zodpovednosti s tým súvisiace. To sa najčastejšie deje pomocou dokumentov ako sú bezpečnostné politiky či bezpečnostné smernice apod., ktoré určujú dlhodobu platné bezpečnostné princípy, pravidlá, zásady a zodpovednosti a ktoré sú často súhrnné nazývané ako príručka bezpečnosti informácií.

Pri tvorbe bezpečnostnej dokumentácie je potrebné rozlišovať rôzne úrovne pripravovaných dokumentov. Na tej najvyššej úrovni sú to predovšetkým dokumenty, ktoré si vyžaduje systém riadenia a ktoré sú s ohľadom na požiadavky ISMS povinné (napr. rozsah ISMS, politika ISMS, správa o hodnotení rizík, prehlásenie o aplikovateľnosti, plán zvládania rizík apod.). Tieto dokumenty majú svoje špecifické miesto v systéme a tomu je často podriadená aj ich forma.

V druhej úrovni je dokumentácia, ktorá slúži na podporu presadzovania ISMS a vždy by mala byť prispôbena konkrétnemu ISMS. Najčastejšie ide o príručku bezpečnosti informácií. Dôležitým prvkom pri tvorbe tejto dokumentácie je definícia čiastkových procesov a postupov, ktoré zaisťujú efektívne presadenie čiastkových bezpečnostných opatrení. A preto je dôležité definovať kto, čo, kedy, kde a ako má urobiť.

Na najnižšej úrovni bezpečnostnej dokumentácie sa nachádzajú tzv. pracovné postupy. Tieto dokumenty by mali podrobne vysvetliť úkony, ktoré sú nevyhnutné

na naplnenie čiastkových procesov. Nie vždy je táto úroveň potrebná a často môže byť riešená odkazom na príslušnú dokumentáciu použitých technických systémov.

Prehlbovanie bezpečnostného povedomia

Jedným z najdôležitejších prvkov pri presadzovaní ISMS je prehlbovanie bezpečnostného povedomia, za ktorým sa skrýva premietnutie všetkých definovaných pravidiel a postupov do skutočného chovania všetkých zodpovedných pracovníkov a užívateľov. Tento jednoduchý cieľ je veľmi zložitou úlohou, ktorá vyžaduje vysoké a systematické úsilie. Vďaka zmenám, ktoré si vyžaduje rozvoj ISMS a pravidelná obmena pracovníkov organizácie, je to trvalý a nekonečný proces, ktorý často rozhoduje o skutočnej efektívnosti ISMS.

Najmodernejšie bezpečnostné nástroje sú neúčinné, ak užívatelia nie sú ochotní a schopní ochrániť si svoje prístupové heslo. Sofistikovaný systém na riadenie prístupu takisto neúčinný, ak je oprávnený užívateľ ochotný poskytnúť citlivé informácie neznámym osobám.

Aby k podobným situáciám nedochádzalo, je nutné všetkým pracovníkom zrozumiteľne vysvetľovať bezpečnostné princípy a pravidlá, zoznamovať ich s bezpečnostnými rizikami tak, aby boli schopní správne reagovať na situácie, ktoré dokumentácie nepostihuje, a konzultovať s nimi bezpečnostné incidenty, ich príčiny a skutočné aj potenciálne následky.

Jedine takouto systematickou komunikáciou s pracovníkmi bude možné zaistiť väčšiu odolnosť najslabšieho článku v pomyselnom reťazci ISMS. Tým vždy bude ľudský faktor a jeho nepredvídateľné prejavy.

Meranie účinnosti ISMS

Ďalšou dôležitou témou, ktorá je spojená s presadzovaním efektívneho riadenia bezpečnosti, je meranie účinnosti aplikovaných bezpečnostných opatrení. Tu je potrebné definovať a pravidelne sledovať objektívne údaje o skutočnom fungovaní systému riadenia bezpečnosti, na základe ktorých je vhodné prevádzať všetky dôležité rozhodnutia.

Proces riadenia účinnosti systému riadenia bezpečnosti informácií v organizácii nie je jednoduchý a je nutné ho mať na zreteli už v okamihu návrhu celého ISMS, pretože veľmi podstatné kroky na meranie efektívnosti a jej vyhodnocovania sú už súčasťou prvej etapy životného cyklu.

O skutočnej účelnosti a účinnosti ISMS sa rozhoduje už v etape plánovania. Vtedy prebieha vstupná analýza rizík a na jej kvalite bezprostredne závisí aj kvalita navrhnutého ISMS. Významný vzťah k účinnosti celého navrhovaného ISMS má tiež prístup vrcholového vedenia organizácie a jeho kompetencie. V tejto etape je tiež nutné zohľadniť aj ďalšie zákonné, prípadne iné úpravy, ktorými sa organizácia musí riadiť a ktoré vychádzajú z jej celkovej stratégie.

Riadenie prevádzky, zdrojov, dokumentácie a záznamov ISMS

Posledným bodom etapy zavádzania ISMS je prevádzkanie všetkých činností riadeným spôsobom. Nestačí len postupovať podľa dohodnutých pravidiel, ale je nutné

aj zhromažďovať podklady pre ďalšiu fázu monitorovania. Na umožnenie kontroly správnosti fungovania ISMS je podstatné vytvoriť definované pravidlá na tvorbu, schvaľovanie, distribúciu a aktualizáciu dokumentácie riadenia bezpečnosti (vrátane odoberania a zneplatnenia a skartácie už neplatných verzií dokumentov). Súčasne je podstatné vytvárať záznamy o jednotlivých prevedených úkonoch ISMS, kde sa objavia základné informácie o prevedenej činnosti (identifikácia osoby, ktorá činnosť prevádzkala, termín a miesto realizácie činnosti, výsledky prevedenej činnosti, atd.). Vytváranie takýchto záznamov o čiastkových reálnych úkonoch musí byť vytvorené tak, aby umožňovalo relatívne jednoduché dohľadanie určitých presne definovaných skupín aktivít (vyhľadanie určitých typov činností, vyhľadanie činností realizovaných v danom období či určitou osobou alebo zariadením).

Z pohľadu riadenia ISMS zdrojov je potrebné sledovať, či sú potreby ISMS pokryté odpovedajúcim množstvom odborných zdrojov (ľudských, finančných, technických, znalostných a iných) a účinne riadiť použitie týchto zdrojov na účinné fungovanie ISMS. Podstatnou prevádzkovou požiadavkou je tiež definícia postupov a opatrení na riadenie incidentov. Tu je nutné využiť nástroje, ktoré sú schopné včas odhaľovať bezpečnostné slabiny a incidenty a na tieto udalosti upozorniť príslušných zodpovedných pracovníkov organizácie. Títo pracovníci potom zaistia prešetrenie podnetov podľa definovaných postupov a pravidiel vrátane zaznamenania priebehu a výsledkov šetrenia. Podnety z riešenia bezpečnostných incidentov by mali byť tiež využité na spresnenie hodnotenia rizík a pre optimalizáciu pravidiel ISMS.

2.2.3 Monitorovanie a preskúvanie ISMS

Hlavnou úlohou tejto etapy zavádzania ISMS je zaistiť účinné spätné väzby. V súvislosti s touto požiadavkou by preto malo dôjsť k prevereniu všetkých aplikovaných bezpečnostných opatrení a ich dôsledkov na ISMS. Vlastné overenie začína priamou kontrolou zodpovedných osôb zo strany ich nadriadených či bezpečnostným manažérom. Dôležitú rolu zohráva tiež nezávislé posúdenie fungovania a účinnosti ISMS pomocou interných auditov ISMS. Všeobecným cieľom všetkých použitých spätných väzieb je pripraviť dostatok podkladov o skutočnom fungovaní ISMS, ktoré budú predložené vedeniu za účelom preskúmania, či je realizácia ISMS v súlade s všeobecnými potrebami organizácie. Počas tejto časti zavádzania ISMS je nevyhnutné vykonať nasledujúce činnosti:

- monitorovať a overiť účinnosť presadenia bezpečnostných opatrení,
- vykonať interné audity ISMS, ktorých náplň pokryje celý rozsah ISMS,
- pripraviť správu o stave ISMS a na jej základe prehodnotiť ISMS na úrovni vedenia organizácie (vrátane revízie zvyškových a akceptovaných rizík).

Kontroly ISMS

Základná spätná väzba, ktorá je pre fungovanie ISMS nevyhnutná, je prevádzanie kontrol zo strany všetkých osôb, ktoré majú za fungovanie ISMS nejakú zodpovednosť a to na všetkých manažérskych úrovniach. Tieto osoby by sa mali aktívne starať o zverené úlohy a dohliadať na to, či dochádza k splneniu všetkých bezpečnostných

požiadaviek. Zároveň by tieto osoby mali dohliadať na to, či bezpečnostné opatrenia patriace do ich kompetencií naplňajú očakávania, ktoré boli do nich pri zavádzaní vkladané.

Súčasťou kontrol ISMS musí byť aj schopnosť včasnej detekcie chýb, úspešných aj neúspešných pokusov o narušenie bezpečnosti či schopnosť sledovania bezpečnostných udalostí a včasnej detekcie bezpečnostných incidentov.

Medzi kontrolné činnosti patrí aj vyhodnocovanie merania účinnosti ISMS a aplikovaných bezpečnostných opatrení. Výsledky merania účinnosti sú podstatným pre ďalšiu významnú kontrolnú činnosť, za ktorú je považované prehodnotenie výsledkov ohodnotenia rizík na základe skúseností z praktického fungovania ISMS. Podnety z týchto aktivít je nutné premietnuť do aktualizácie príslušných dokumentov a plánov ISMS.

Interné audity ISMS

Ďalším kritickým prvkom spätnej väzby je prevádzanie auditov ISMS, ktoré zaisťujú nezávislý pohľad na fungovanie ISMS.

Pri plánovaní auditov je potrebné pamätať na skutočnosť, aby interné audity mali svoje zameranie rovnomerne rozložiť na celý rozsah ISMS samozrejme pri zvažovaní cieľov, priorít a rizikových oblastí ISMS. Audity ISMS by mali preverovať oba aspekty ISMS. Prvým je dodržiavanie procesným pravidliem, kde je dominantným kritériom auditu naplňovanie požiadaviek ISO/IEC 27001, Druhým aspektom auditu ISMS je preverenie fungovania jednotlivých bezpečnostných opatrení, ktoré sú pre potreby ISMS zavedené. Tu sa ako kritérium auditu uplatňuje norma ISO/IEC 27002 a auditori preverujú spôsob, vhodnosť a mieru presadenia aplikovaných bezpečnostných opatrení. Je zrejmé, že oba aspekty auditu ISMS spolu úzko súvisia.

Preskúvanie ISMS vedením organizácie

Podnety a pripomienky k ISMS získané pri jeho monitorovaní sú dôležitými informáciami, ktoré slúžia na objektívne a efektívne preskúvanie ISMS vedením organizácie. Preskúvanie by malo prebiehať pravidelne a to najmenej raz za rok. Nie je ale výnimkou, že prebieha častejšie a to hlavne u novo zavedených ISMS, kde je potreba prehodnotenia častejšia.

Medzi vstupy na preskúvanie ISMS patria všetky podstatné informácie o fungovaní ISMS za hodnotené obdobie. Významná pozornosť by mala byť venovaná nasledujúcim skutočnostiam:

- výsledkom prevedených auditov ISMS,
- spätnej väzbe od zainteresovaných užívateľov a tretích strán
- existujúcim slabším a hrozbám, ktoré mohli byť pri analýze rizík podceňované,
- výsledkom meraní účinnosti ISMS,
- zmenám, ktoré ovplyvňujú ISMS,
- získaným odporúčaniami pre ďalšie zlepšovanie ISMS.

Na základe týchto podnetov dochádza k posúdeniu silných a slabých stránok ISMS (SWOT analýza). Medzi dôležité výstupy SWOT analýzy patrí:

- zlepšenie účinnosti ISMS (zvyšovanie miery bezpečnosti pri znižovaní náročnosti realizácie bezpečnostných opatrení),
- aktualizácia ohodnotených rizík a súvisiacich plánov na zvládanie rizík,
- nevyhnutné úpravy procesov, pravidiel a postupov ISMS,
- plánovaná náročnosť ISMS na zdroje (finančné, ľudské, technologické apod.) v ďalšom období.

Častým prejavom prehodnotenia ISMS je príprava správy o stave ISMS, ktorá zhrnie, čo na ISMS funguje dobre a je možné sa o tieto vlastnosti v budúcnosti oprieť a zároveň zhrnie skutočnosti, ktoré zatiaľ optimálne nefungujú, a bude ich potrebné ďalej zlepšovať. Pomocou správy o stave ISMS, ktorý by mala byť orientovaná predovšetkým na budúcnosť, je možné s vedením organizácie uzavrieť dohodu o prehlbovaní bezpečnosti. Manažérom ISMS správa dovoľuje definovať ciele pre obdobie a žiadať vedenie organizácie o pridelenie príslušných zdrojov na naplnenie cieľov uvedených v správe.

2.2.4 Údržba a zlepšovanie ISMS

Poslednou etapou celého cyklu presadzovania ISMS je jeho udržovanie a zlepšovanie. Ide predovšetkým o to, že v tejto fáze by malo dochádzať k zberu podnetov na zlepšenie ISMS a k náprave všetkých nedostatkov tzv. nezhôd, ktoré sa v ISMS objavujú. V rámci tejto časti zavádzania je nevyhnutné vykonať nasledujúce činnosti:

- zavádzať identifikované možnosti zlepšenia ISMS (predovšetkým na základe prehodnotenia vedením),
- vykonať odpovedajúce opatrenia na nápravu a preventívne opatrenia na odstránenie nedostatkov.

2.2.5 Sústavné zlepšovanie ISMS

Návrh dokonalých systémov riadenia je v praxi veľmi náročný. V podstate také systémy neexistujú, preto je veľmi dôležité do každého systému zapracovať účinnú spätnú väzbu. Ta by mala fungovať tak, že na jednej strane získava podnety, ktoré môžu viesť k efektívnejšiemu fungovaniu ISMS. Na druhej strane musí táto väzba odhaľovať nedostatky a ich príčiny a vhodným spôsobom na tieto podnety reagovať.

Podstatným prvkom zlepšovania je predovšetkým využitie pozitívnej spätnej väzby. Je žiaduce, aby sa zlepšovanie IMS opieralo o skúsenosti aktívnych účastníkov. Tie by mali osoby zodpovedné za ISMS informovať o svojich podnetoch, ktoré môžu fungovanie ISMS zlepšiť. Nápady pochádzajúce z reálnej praxe sú vždy nenahraditeľné a ich dôslednému spracovaniu by mala byť venovaná veľká pozornosť.

Pre rozvoj ISMS je dôležité i prehlbovať motiváciu pracovníkov na účasti pri všetkých činnostiach spojených s ISMS v tom, aby zdieľali svoje skúsenosti a aby otvorene navrhovali, čo je vhodné a žiaduce na chode ISMS zlepšiť.

2.2.6 Odstraňovanie nedostatkov ISMS

Existujú dve formy opatrení na odstraňovanie nedostatkov:

- opatrenia k náprave a
- preventívne opatrenia

Opatrenie k náprave je reaktívnou formou riešenia nedostatku. V tomto prípade sa už nedostatok nejakým spôsobom prejavil (často označujeme túto skutočnosť nezhodou) a je potrebné na neho vhodným spôsobom reagovať.

Naproti tomu preventívne opatrenie je proaktívnou formou riešenia nedostatkov ISMS. V tomto prípade sa vychádza z toho, že sa zistený nedostatok ešte neprejavil, ale ďalší odklad jeho riešenia by mohol viesť k tomu, že sa v budúcnosti nejaká negatívna udalosť objaví a spôsoby vážnejšie problémy.

Dôležitým a nenahraditeľným prvkom odstraňovania nedostatkov oboma spôsobmi je objasnenie príčin, ktoré k týmto nedostatkom viedli. V tomto zmysle nestačí len vykonať nápravu u konkrétnej nezahody. Je dôležité sa pozrieť na súvislosti a opatrenia realizovať tak, aby sa obmedzili možnosti opakovania tohto nedostatku. Pred presadením oboch typov opatrení je tiež nevyhnutné posúdiť, či zvolené opatrenia dostatočne zamedzia nedostatku a prípadne pokryjú jeho príčiny.

Postupy na riešenie opatrení k náprave a preventívnych opatrení musia byť zdokumentované a všetky činnosti s nimi spojené musia byť zaznamenané a zahrnuté do dokumentácie. Po zavedení opatrení je tiež dôležité preskúmať, či zvolené opatrenia skutočne zaistili očakávanú zmenu účinnosti ISMS. To sa najčastejšie prevádza priamou kontrolou, v prípade vážnejších nedostatkov mimoriadnym auditom ISMS.

2.3 Normy v oblasti bezpečnosti IT

2.3.1 Normy ISO/IEC rady 27000

Táto norma položila základ pre zavádzanie implementácie managementu bezpečnosti informačných systémov bola uvedená v platnosť v roku 1995. Pôvodne norma Britského normalizačného inštitútu sa postupom času začal uplatňovať aj v ostatných krajinách s označením ISMS (*Information Security Management System*). Je zameraná na faktory dostupnosti, dôverylosti a integrity informácií a informačných systémov v podniku. Norma sa snaží komplexne riešiť obranu proti možným hrozbám, ktoré boli v podniku identifikované, ocenené a môžu mať ďalekosiahle následky, resp. dopady. V roku 2000 bola prijatá ako nadnárodná norma štandardu ISO pod označením ISO 17799. Medzinárodná organizácia pre normalizáciu v roku 2005 vydala sériu noriem ISO/IEC 27000 zahrňujúcu systém riadenia informačnej bezpečnosti, tieto normy vychádzajú z normy ISO 17799. Normy rady ISO/IEC 27000 sú tvorené nasledujúcimi časťami (2):

- **ISO 27000** - zavádza pojmy, definície a terminologický slovník pre všetky nasledujúce normy rady 27000.

- **ISO 27001** - norma bola vydaná koncom roku 2005 a ide o normu, podľa ktorej sa systémy riadenia bezpečnosti informácií certifikujú. (pôvodná norma BS7799-2)
- **ISO 27002** - aktuálna verzia normy od júla 2007 je táto norma označovaná ako ISO/IEC 27002:2005. (nahradila normu ISO/IEC 17799:2005). Obsahuje zbierku najlepších bezpečnostných praktík a môže byť využitá ako zoznam postupov, ktoré je nutné pre bezpečnosť informácií v organizácii vykonať.
- **ISO 27003** - poskytuje implementačné návody pre ostatné normy rady 27000.
- **ISO 27004** - táto norma poskytuje odporúčenia pre vývoj a používanie metrík a pre meranie účinnosti zavedeného systému riadenia bezpečnosti informácií (ISMS) a účinnosti opatrení alebo skupín opatrení, ako je uvedené v ISO/IEC 27001.
- **ISO 27005** - norma sa zameriava na riadenie bezpečnostných rizík informačných technológií.
- **ISO 27006** - obsahuje požiadavky na orgány prevádzajúce audit a certifikáciu systémov riadenia bezpečnosti informácií.
- **ISO 27033** - je to viacdielny štandard vytvorený z päťdielného štandardu pre sieťovú bezpečnosť ISO/IEC 18028. Je rozsiahlo prepracovaný, nie len premenovaný, aby spadol do série noriem rady ISO 27000.

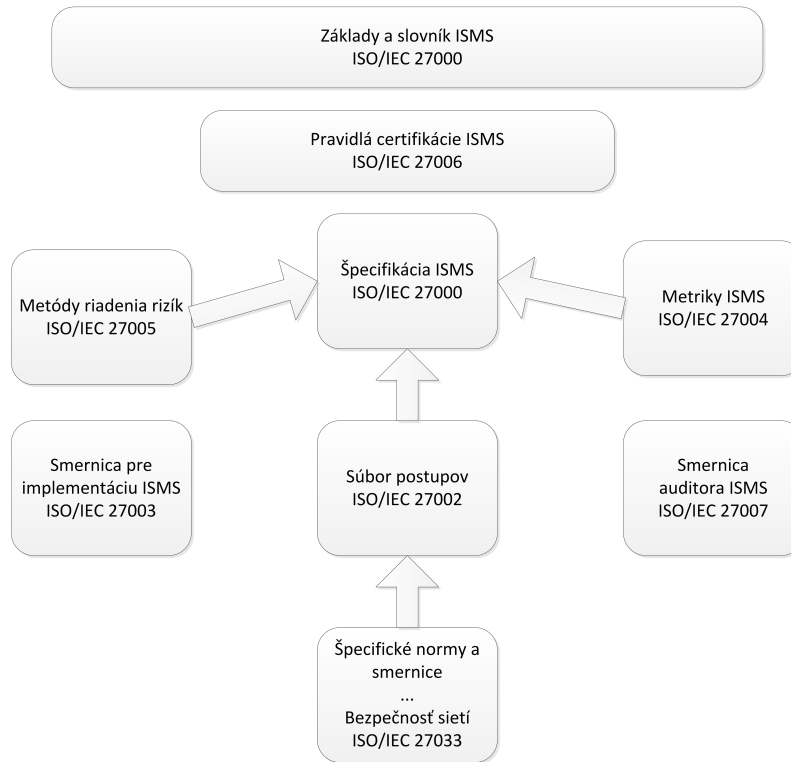
Všetky tieto rodiny noriem majú väzbu na ostatné rodiny noriem, ktoré vymedzujú integrovaný systém riadenia ISO 9000 a ISO 14000. Dôležitou skutočnosťou pre úspešný rozvoj série ISO/IEC 27000 je tiež vyjasnenie vzťahu s ostatnými bezpečnostnými normami. Nie je cieľom série zaoberať sa všetkým. Práve naopak, veľká pozornosť je venovaná tomu, aby bezpečnostné opatrenia boli naviazané na normy, ktoré hlbšie rozoberajú určité oblasti bezpečnosti. Tento koncept je zobrazený na obrázku 2.2.

Z vyššie uvedeného je zrejmé, že problematika riadenia bezpečnosti informácií a informačných technológií je riešená pomocou postupov definovaných v patričných normách (nielen v rade 27000). Normy tvoria obvyklé doporučené postupy a podnik, ktorý sa rozhodne riešiť problematiku ISMS, si môže pre zavedenie zvoliť oblasti, ktoré je schopný zvládnuť.

2.3.2 Norma ISO/IEC 27033

Zmyslom ISO/IEC 27033 je poskytnúť detailné zásady v bezpečnostných aspektoch managementu, operácii a použití počítačových sietí a ich prepojení. Zodpovedné osoby v organizáciách za informačnú bezpečnosť vo všeobecnosti a konkrétne sieťovú bezpečnosť by mali byť schopní využiť túto normu na pokrytie ich vlastných špecifických požiadaviek. ISO/IEC 27033 poskytuje detailné zásady pre zavádzanie kontrolných mechanizmov v oblasti sieťovej bezpečnosti uvedené v ISO/IEC 27002.

Rada ISO/IEC 27000 Riadenie bezpečnosti informácií



Obr. 2.2: Koncept rady ISO/IEC 27000 pre riadenia bezpečnosti informácií (Prezvané z (2))

Vzťahuje sa na sieťové zariadenia a na management ich bezpečnosti, sieťových aplikácií, resp. služieb a užívateľov siete. Súbežne s tým sa vzťahuje na bezpečnosť informácií prenášaných cez komunikačné kanály. Je určená pre sieťových architektov, návrhárov, manažérov a vedúcich pracovníkov. Množstvo častí spolu s ich rozsahom sú predmetom zmien a štandard sa neustále vyvíja súbežne s vývojom sieťovej bezpečnosti. Norma ISO/IEC 27033 sa skladá z nasledujúcich častí (6):

- **ISO/IEC 27033-1:2009:** Prehľad sieťovej bezpečnosti a konceptov
- **ISO/IEC 27033-2:2012:** Zásady v návrhu a implementácii sieťovej bezpečnosti
- **ISO/IEC 27033-3:2010:** Referenčné sieťové prípady, hrozby, návrhové techniky a zákutia kontrolných mechanizmov
- **ISO/IEC 27033-4:** Zabezpečenie komunikácie medzi sieťami využitím bezpečnostných brán (DRAFT)
- **ISO/IEC 27033-5:** (DRAFT) Zabezpečenie komunikácie cez siete využitím technológie VPN (DRAFT)

- **ISO/IEC 27033-6:** Zabezpečenie prístupu k IP sieťam cez bezdrôtové pripojenie (DRAFT)

2.3.3 Norma ISO/IEC 18028

Účelom normy ISO/IEC 18028 je poskytnúť detailné návody manažmentu bezpečnostných aspektov počítačových sietí. Je rozdelené na viacero častí, aby obsahla rôzne prístupy a pohľady na počítačové siete (?).

- **ISO/IEC 18028-1:** Definuje a popisuje koncepty súvisiace so sieťovou bezpečnosťou (a poskytuje pokyny pre jej riadenie). Zahŕňa návody ako identifikovať a analyzovať faktory súvisiace s počítačovou bezpečnosťou.
- **ISO/IEC 18028-2:** Define štandardy bezpečnej architektúry, ktorými popisuje ucelený rámec na podporu plánovania, návrhu a implementácie sieťovej bezpečnosti.
- **ISO/IEC 18028-3:** Definuje techniky na zabezpečenie informačných tokov medzi sieťami využívajúcimi bezpečnostné brány.
- **ISO/IEC 18028-4:** Definuje techniky zabezpečenia vzdialeného prístupu.
- **ISO/IEC 18028-5:** Definuje techniky na zabezpečenie komunikácie medzi sieťami využitím virtuálnych privátnych sietí (VPN).

Vzhľadom na to, že normy 27033 ešte nie sú kompletne vydané a normy ISO/IEC 18028 neboli oficiálne nahradené novým štandardom bude táto práca v nasledujúcom texte využívať práve staršiu sadu noriem pri realizácii bezpečnostných opatrení.

2.4 Analýza rizík

Analýza rizík je chápaná ako proces definovania hrozieb, pravdepodobnosti ich uskutočnenia a dopadu na aktíva, teda stanovenie rizík a ich závažností. Detailne sa touto problematikou zaoberá (9). Táto časť textu vychádza z poznatkov uvedených v spomínanej publikácii. Nadväzujúcou činnosťou je riadenie rizík. Analýza rizík spravidla zahrňuje

- **identifikácia aktív** - vymedzenie posudzovaného subjektu a popis aktív, ktoré vlastní,
- **stanovenie hodnoty aktív** - určenie hodnoty aktív a ich význam pre subjekt, ohodnotenie možného dopadu ich straty, zmeny či poškodenia na existencii či chovaní subjektu,
- **identifikácia hrozieb a slabín** - určenie druhov udalostí a akcií, ktoré môžu ovplyvniť negatívne hodnotu aktív, určenie slabých miest subjektu, ktoré môžu umožniť pôsobenie hrozieb,

- **stanovenie závažnosti hrozieb a miera zraniteľnosti** - určenie pravdepodobnosti výskytu hrozby a miery zraniteľnosti subjektu voči danej hrozbe.

Výsledky hodnotenia rizík môžu pomôcť určiť odpovedajúce kroky vedenia organizácia a priority pre zvládanie rizík pre realizáciu opatrení určených k zamedzeniu ich výskytu. Je možné, že proces hodnotenia rizík a stanovenia opatrení bude potrebné opakovať niekoľkokrát, aby boli pokryté rôzne časti subjektu (organizácie) alebo jednotlivé časti.

V každom prípade je nutné si už na začiatku stanoviť úroveň, na akú chceme analyzované riziká eliminovať. Snaha o odstránenie všetkých rizík by samozrejme viedla k neúmerným nákladom pri realizácii príslušných opatrení a v každom prípade by sa zákonite podpísala i na funkčnosti daného subjektu.

Z tohto dôvodu v rámci analýzy rizík posúdime otázky zvyškových rizík, ktoré sa snažíme vymedziť na základe ich posúdenia vo vzťahu k hrozbám, úrovni zraniteľnosti a navrhovaných protiopatrení. Na základe toho potom vyberáme konkrétny prístup a metódu analýzy rizík.

2.4.1 Základné pojmy analýzy rizík

Aktívum

Aktívum je všetko, čo má pre organizáciu hodnotu, ktorá môže byť zmenšená pôsobením hrozby. Aktíva delíme na *hmotné* (napríklad nehnuteľnosti, cenné papiere, peniaze apod.) a na *nehmotné* (napríklad informácie, predmety priemyselného a autorského práva, morálka pracovníkov, kvalita personálu apod.). Aktívom ale môže byť aj sám subjekt, pretože hrozba môže pôsobiť na celú jeho existenciu. Základnou charakteristikou aktíva je *hodnota aktíva*, ktorá je založená na objektívnom vyjadrení všeobecne vnímanej ceny alebo na subjektívnom ocenení dôležitosti (kritickosti) aktíva pre daný subjekt, poprípade na kombinácii oboch prístupov. Hodnota aktíva je relatívna v závislosti na uhle pohľadu hodnotenia.

Pri hodnotení aktíva sa berú v úvahu predovšetkým nasledujúce hľadiská:

- obstarávacie náklady či iná hodnota aktíva,
- dôležitosť aktíva pre existenciu či chovanie organizácie,
- náklady na preklopenie prípadnej škody na aktíve,
- rýchlosť odstránenia prípadnej škody na aktíve,
- iné hľadiská (môžu byť špecifické prípad od prípadu).

Ďalšou charakteristikou aktíva, ktorá vyjadruje jeho citlivosť na pôsobení hrozby, je *zraniteľnosť*, ktorá bude charakterizovaná nižšie.

Hrozba

Hrozba je sila, udalosť, aktivita alebo osoba, ktorá má nežiaduci vplyv na bezpečnosť alebo môže spôsobiť škodu. Hrozbou môže byť napríklad požiar, prírodná katastrofa, krádež zariadenia, získanie prístupu k informáciám neoprávnenou osobou, chyba obsluhy, ale i kontrola finančného úradu alebo rast kurzu českej koruny vzhľadom k európskej mene apod.

Škoda, ktorú spôsobí hrozba pri jednom pôsobení na určité aktívum, sa nazýva *dopad hrozby*. Dopad hrozby môže byť odvodený od absolútnej hodnoty strát, do ktorej sú zahrnuté náklady na znovuoobnovenie činnosti aktíva alebo náklady na odstránenie následkov škôd spôsobených organizácii hrozbou.

Základnou charakteristikou hrozby je jej úroveň. Úroveň hrozby sa hodnotí podľa nasledujúcich faktorov:

- **Nebezpečnosť:** schopnosť hrozby spôsobiť škodu.
- **Prístup:** pravdepodobnosť, že sa hrozba svojím pôsobením dostane k aktívu (získa k nemu prístup). Jednou z foriem vyjadrenia môže byť frekvencia výskytu hrozby.
- **Motivácia:** záujem iniciovať hrozbu voči aktívu. Odhad motivácie spočíva v pochopení skupinových a národných zámerov i zámerov jednotlivcov, ich cieľov a politiky - to všetko sa analyzuje s ohľadom na predchádzajúce podmienky a činnosť týchto ohrozovateľov (útočníkov). Odhad motivácie napomáha pri tvorbe expertných stanovísk a odhadov hrozieb.

Zraniteľnosť

Zraniteľnosť je nedostatok, slabina alebo stav analyzovaného aktíva (prípadne organizácie alebo jej časti), ktorý môže hrozba využiť na uplatnenie svojho nežiaduceho vplyvu. Táto veličina je vlastnosťou aktíva a vyjadruje, ako citlivé je aktívum na pôsobenie danej hrozby.

Zraniteľnosť vznikne všade tam, kde dochádza k interakcii medzi hrozbou a aktívom. Základnou charakteristikou zraniteľnosti je jej úroveň. Úroveň zraniteľnosti aktíva sa hodnotí podľa nasledujúcich faktorov:

- **Citlivosť:** náchylnosť aktíva byť poškodené danou hrozbou.
- **Kritickosť:** dôležitosť aktíva pre analyzovanú spoločnosť.

Opatrenie

Opatrenie je postup, proces, procedúra, technický prostriedok alebo čokoľvek, čo bolo špeciálne navrhnuté na zmiernenie pôsobenia hrozby (jej elimináciu), zníženie zraniteľnosti alebo dopadu hrozby. Protiopatrenia sa navrhujú s cieľom predísť vzniku škody alebo s cieľom uľahčiť zvládnuť následky vzniknutej škody.

Z hľadiska analýzy rizík je opatrenie charakterizované *efektivitou* a *nákladmi*. Efektivita protiopatrenia vyjadruje, nakoľko opatrenie zníži účinok hrozby. Používa

sa vo fáze zvládania rizík ako jeden z hlavných parametrov pri hodnotení vhodnosti použitia daného protiopatrenia.

Protiopatrenia sa zameriavajú na oblasti zníženia úrovne hrozby, zníženia úrovne zraniteľnosti, zníženia následkov pôsobenia hrozby, detekcie nežiaduceho vplyvu s cieľom včas indikovať pôsobenie hrozby a predísť možnosti jej plného uplatnenia, ďalej sa potom zameriavajú na oblasť obnovenia činnosti po pôsobení hrozby.

Do nákladov na opatrenie sa započítavajú náklady na obstaranie, zavedenie a prevádzkovanie protiopatrení. Spoločne s efektivitou protiopatrení sú tieto náklady dôležitými parametrami pri výbere protiopatrení. Výber vhodného protiopatrenia spočíva v optimalizácii, kedy sa hľadajú najúčinnšie opatrenia, ktorých realizácia prinesie čo najmenšie náklady.

Riziko

Riziko vzniká vzájomným pôsobením hrozby a aktíva. Hrozba, ktorá nepôsobí na žiadne aktívum, nemusí byť pri analýze rizík braná do úvahy. Aktívum, na ktoré nepôsobí žiadna hrozba, nie je predmetom analýzy rizík.

Úroveň rizika je určená hodnotou aktíva, zraniteľnosťou aktíva a úrovňou hrozby. Na raste úrovne rizika sa podieľa úroveň hrozby, zraniteľnosť a hodnota aktíva. Jedine opatrenie úroveň rizika znižuje.

Pri návrhu protiopatrení sa používa pravidlo, ktoré stanovuje, že náklady vynaložené na zníženie rizika musia byť primerané hodnote chránených aktív (prípadne hodnote škôd, vzniknutých dopadom hrozby). S týmto pravidlom súvisí stanovenie referenčnej úrovne rizika, pod ktorou sa riziko prehlási za zvyškové a nepodnikajú sa žiadne protiopatrenia.

Zvyškové riziko je také riziko, ktoré je tak malé (nepresiahne referenčnú úroveň), že je pre organizáciu prijateľné za zvyškové a nepodnikajú sa žiadne protiopatrenia na jeho zníženie. Opatrenia proti rizikám sa nerobia prakticky nikdy zo 100

Referenčná úroveň je hranica miery rizika (stanovená hodnota veľkosti rizika), ktorá rozhoduje o tom, či je riziko zvyškové (veľkosť rizika je menšia ako referenčná úroveň) alebo nie je zvyškové (veľkosť rizika je väčšia než referenčná úroveň). Tým sa rozhodne, či proti riziku je alebo nie je nutné podniknúť ďalšie protiopatrenia na jeho zníženie. Referenčná úroveň by mala byť na takej úrovni, aby dopad hrozby bol tak malý, že je možné ho zanedbať.

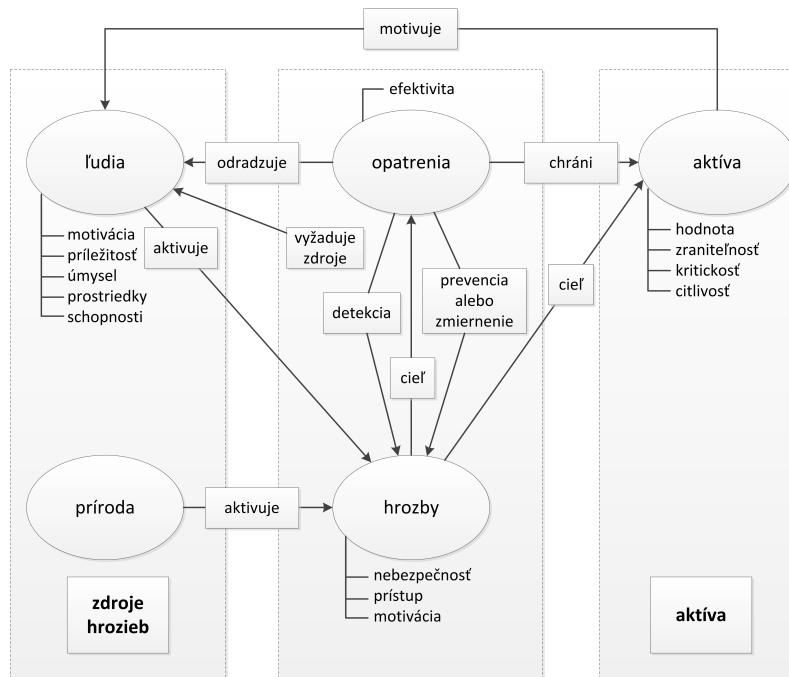
2.4.2 Vzťahy v analýze rizík

Správne pochopenie vzťahov v analýze rizík je pre úspešné analýzy kľúčové. Základné vzťahy a súvislosti sú znázornené na obrázku 2.3.

Mechanizmus uplatnenia rizika prebieha nasledujúcim spôsobom:

Mechanizmus uplatnenia rizika prebieha nasledujúcim spôsobom:

- Hrozba využije zraniteľnosti, prekoná protiopatrenia a pôsobí na aktívum, kde spôsobí škodu (dopad).
- Aktívum (svojou hodnotou) motivuje útočníka k aktivácii hrozby. Voči pôsobeniu hrozby sa aktívum vyznačuje určitou zraniteľnosťou. Aktívum je zároveň chránené protiopatrením pred hrozbami.



Obr. 2.3: Vzťahy v analýze rizík (Prevzaté z (9))

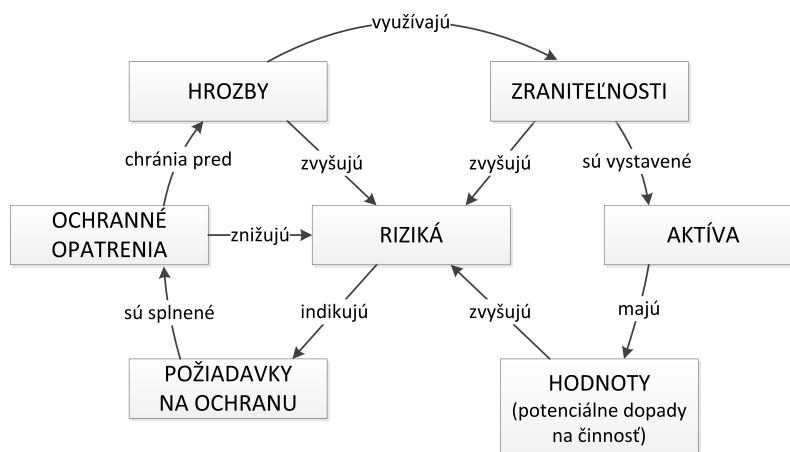
- Opatrenie chráni aktíva, detekuje hrozby a zmierňuje alebo úplne zabraňuje ich pôsobeniu na aktíva. Opatrenie zároveň odradzuje od aktivovania hrozieb
- Hrozba pôsobí priamo na aktívum alebo na opatrenie s cieľom získať prístup k aktívu. Aby mohla hrozba pôsobiť, musí byť aktivovaná. Na svoju aktiváciu vyžaduje zdroje (vytvorenie podmienok na jej pôsobenie).

Vzťahy medzi jednotlivými prvkami a riadením rizík je možné popísať napríklad modelom zobrazeným na obrázku 2.4.

2.5 Sieťová bezpečnosť

Svet počítačov sa za posledných 25 rokov dramaticky zmenil. Pred dvadsiatimi piatimi rokmi bola väčšina počítačov centralizovaná a spravovaná v dátových centrách. Počítače boli zamknuté v počítačových miestnostiach a prepojenia smerom von zo spoločnosti boli veľmi nezvyčajné. Bezpečnostné hrozby sa vyskytovali len výnimočne a vo svojej podstate súviseli s fyzickým prístupom k zariadeniam. Takéto hrozby boli dobre známe a zaobchádzalo sa s nimi štandardným spôsobom: počítače sa nachádzali za zamknutými dverami a využitie počítačových zdrojov bolo zaznamenávané. Dnes, po dvadsiatich piatich rokoch, je väčšina systémov pripojená k Internetu. Internet predstavuje obrovskú sieť bez hraníc. Skoro všetky spoločnosti sú dnes pripojené na Internet, aby boli schopné využiť nové príležitosti a výhody, ktoré z toho plynú.

Bezpečnostný rámec pre systémy pripojené do Internetu je však veľmi iný. Informácie môžu byť dostupné odšadiaľ v reálnom čase, čo predstavuje výhodu vzhľadom



Obr. 2.4: Vzťahy pri riadení rizík (Prevzaté z (9))

na ich šírenie. To ale nezabráňuje šíreniu aj zavádzajúcich, resp. klamlivých, podvodných informácií. Hackerské nástroje sú dnes bežne voľne dostupné na stiahnutie. Existujú stránky, ktoré poskytujú návody ako preniknúť do nejakého systému, obsahujú detailné informácie o zraniteľnostiach rôznych druhov systémov. Človek už v dnešnej dobe nepotrebuje byť skúseným programátorom a expertom na počítačovú bezpečnosť na to, aby sa nabúral do systému. Hocikto so zlomyseľnými úmyslami môže vyhľadať s využitím Internetu programy na vykonanie útoku na nezabezpečené počítačové systémy.

Preto je pre spoločnosti s pripojením do Internetu odporúčané zaistiť bezpečnosť sietí. To je dôležité z dôvodu snahy o minimalizáciu rizika prieniku do systému z vonku, resp. priamo zo spoločnosti (napríklad vlastnými zamestnancami). Hoci sieť nemôže byť 100% bezpečná, zabezpečená sieť odradí každého, okrem skutočne odhodlaných útočníkov. Sieť s dobrým systémom záznamov a systému auditov zaistí, že všetky aktivity budú zaznamenané, čo následne umožní rozpoznať tie škodlivé (12).

2.5.1 Potreba sieťovej bezpečnostnej politiky

Predtým ako môže byť samotná sieť zabezpečená je potrebné vytvoriť sieťovú bezpečnostnú politiku. Tá definuje očakávania organizácie vzhľadom na vhodné využitie počítačov a počítačovej siete a procedúry na zamedzenie, resp. reakcie na bezpečnostné incidenty. Sieťová bezpečnostná politika je základ bezpečnosti pretože špecifikuje hodnotu ochrany aktív a aké činnosti, resp. nečinnosti ohrozujú aktíva. Porovná možné hrozby s cenou práce zamestnancov a efektivity a identifikuje rôzne aktíva spoločnosti, ktoré potrebujú viacúrovňovú ochranu. Bez sieťovej bezpečnostnej politiky, nemôže byť vytvorený vhodný bezpečnostný rámec. Zamestnanci sa nemôžu odkázať na štandardy spoločnosti a bezpečnostné kontroly by boli obchádzané za účelom zvyšovania efektivity práce.

Politika sieťovej bezpečnosti by mala byť konzultovaná a vytvorená v spolupráci s každým, kto využíva firemnú počítačovú sieť, či už sú to zamestnanci alebo dodávatelia.

2.5.2 Riziká sieťovej konektivity

Predtým ako môže byť sieťová politika zostavená, musí byť vytvorená analýza rizík. Analýza rizík predstavuje proces identifikácie toho, čo je potrebné ochrániť, pred čím je to potrebné ochrániť, a ako to ochrániť. Je to proces analýzy všetkých rizík spoločnosti a ich ohodnotenie na základe úrovne závažnosti.

Prvým krokom pri analýze rizík sieťovej konektivity je ohodnotiť sieť, aby bolo možné určiť, ktoré aktíva je vhodné (výhodné) ochrániť a do akej úrovne. Je potrebné vytvoriť detailný zoznam všetkých aktív, ktorý zahŕňa hmotné aktíva, ako sú servery, počítačové stanice, a nehmotné aktíva, ako je software a dáta. Rovnako by mali byť identifikované zložky, ktoré obsahujú dôverné alebo kritické dokumenty. Na základe ohodnotenia je možné aktíva zoradiť podľa priority (a následne uprednostniť len niektoré).

V prípade, že sú aktíva identifikované ako tie, ktoré vyžadujú ochranu, je nevyhnutné identifikovať hrozby spojené s týmito aktívami. Medzi príklady bezpečnostných hrozieb patria:

- neautorizovaný prístup / využitie zdrojov (autentizácia)
- útok typu *Denial of Service* (dostupnosť)
- únik informácií (dôvernosť)
- poškodenie / neautorizovaná zmena dát (integrita)
- prírodné katastrofy

Dôkladné ohodnotenie rizík predstavuje najhodnotnejší pomocný nástroj pri tvorbe bezpečnostnej politiky pre firemnú počítačovú sieť. Analýzou rizík sa zistia najhodnotnejšie a zároveň najzraniteľnejšie aktíva. Bezpečnostná politika môže byť vytvorená tak, aby sa sústredila na bezpečnostné metriky, ktoré pomôžu identifikovať tieto aktíva.

2.5.3 Súčasti sieťovej bezpečnostnej politiky

Hoci sú sieťové bezpečnostné politiky subjektívne a môžu sa líšiť z dôvodu odlišností medzi rôznymi spoločnosťami, existujú isté aspekty, ktoré sú relevantné vo všetkých politikách. V tejto sekcii budú zhrnuté niektoré základné komponenty sieťovej bezpečnostnej politiky.

Fyzická bezpečnosť

Sieťová bezpečnosť priamo súvisí s fyzickou bezpečnosťou pretože veľkosť a tvar sieťového zariadenia môže svojimi rozmermi zasahovať do priestorov budovy, areálu, krajiny, resp. môže mať celosvetovú pôsobnosť z dôvodu prepojení a vzťahov dôveryhodnosti. Bez riešenia fyzickej bezpečnosti sú ostatné bezpečnostné aspekty ako dôveryhodnosť, dostupnosť a integrita ohrozené. Časť politiky zaoberajúca sa fyzickou bezpečnosťou uvádza ako majú byť priestory a hardware zabezpečené. Rovnako určuje, ktorí zamestnanci majú prístup ku kabeľáži, serverom apod.

Sieťová bezpečnosť

Časť o sieťovej bezpečnosti uvádza ako budú chránené aktíva uložené v počítačovej sieti. Táto sekcia môže obsahovať bezpečnostné metriky súvisiace s riadením prístupu, nastavením zariadení ako je firewall, ďalej informácie k sieťovému auditu, internetovým službám a súborovému systému.

Kontrola prístupu

Kontrola prístupu určuje kto môže k čomu pristupovať. Musí existovať vhodný postup na zaistenie, že len určené osoby majú prístup k určitým informáciám a službám. Správne riešené riadenie prístupu obsahuje spravovanie vzdialeného prístupu a umožnenie administrátorom pracovať efektívne. Nemalo by ísť o príliš komplexné riešenie, aby nedochádzalo k chybám.

Autentizácia

Autentizácia predstavuje postup ako užívateľ informuje sieť o svojej totožnosti. Typ autentizácie závisí na tom, odkiaľ sa užívateľ snaží autentizovať. V prípade prístupu z vlastného počítača je užívateľské meno a heslo dostačujúcim spôsobom autentizácie z dôvodu zásad vyplývajúcich z fyzickej bezpečnosti. V prípade pripojenia z prostredia Internetu je potrebná bezpečnejšia dvojfaktorová autentizácia (založená na tokenoch).

Šifrovanie

Šifrovanie zaisťuje integritu dát, resp. ochraňuje citlivé informácie pred posielením po nezabezpečených spojeniach. Takýto typ bezpečnosti je zvyčajne nevyhnutný v prípade vzdialeného prístupu k dôležitým aktívam, resp. pri zabezpečení využívania firemného intranetu.

Dodržiavanie

Sekcia o dodržiavaní bezpečnostných politík vysvetľuje ako uskutočniť vynútenie užívania sieťovej bezpečnostnej politiky. Môže obsahovať informácie o metódach ako zistiť porušenia dodržiavania politiky. Rovnako môže obsahovať sankcie za porušenie politiky.

Audity a kontroly

Po dokončení a zavedení bezpečnostnej politiky je potrebné pravidelne vykonávať kontroly či sú zahrnuté všetky komponenty siete, rovnako ako aj či sú súčasťou zásad všetci zamestnanci. Bez dostatočného auditu sa môže spoločnosť dostať do situácie, kedy nebude mať možnosti právneho postihu v prípade výskytu porušenia bezpečnosti. Audit rovnako pomôže identifikovať problémy pred tým ako vyústia do porušenia sieťovej bezpečnosti. Kontroly musia byť pravidelné, aby sa zaistilo, že politiky sú stále relevantné vzhľadom na aktuálnu situáciu v spoločnosti.

Povedomie o bezpečnosti

Nevedomí užívatelia sú často uvádzaní ako najserióznejšie hrozby sieťovej bezpečnosti. Ak si samotní užívatelia neuvedomujú silu správneho využívania počítačovej siete, môžu neúmyselne kompromitovať bezpečnosť. Zamestnanci musia spravovať svoje heslá a byť si vedomí techník ako sú útoky pomocou sociálneho inžinierstva.

Reakcia na incident a havarijný plán

Organizácia je najviac zraniteľná v prípade, keď zistí neoprávnené vniknutie do siete, prípadne keď musí čeliť nejakej katastrofe. Kroky, ktoré podnikne pár minút po udalosti, rozhodnú o tom, či sa podarí obnoviť intelektuálne vlastníctvo. Pohotovostný plán obnovy v prípade katastrofy určí ako sa organizácii podarí zotaviť z prírodnej katastrofy alebo útoku (z vonku alebo z vnútra spoločnosti od zamestnancov). Môže napríklad obsahovať bezpečnostné metriky na zálohovanie serverov, detailne určiť ako často má dochádzať k zálohám a ako majú byť zálohy uložené mimo firemné prostredie. Havarijný plán môže špecifikovať osoby zodpovedné za nápravy v prípade prírodných katastrof alebo útokov. Zároveň môže definovať metriky na zistenie toho, že každý zamestnanec firmy, vrátane zodpovedných osôb, vie, čo robiť v prípade, že ku katastrofe alebo útoku dôjde.

Prípustné užitie politiky

Časť politiky zaoberajúca sa prípustným užitím politiky uvádza ako získa užívateľ prístup k sieťovým zdrojom. Môže napríklad popisovať typy informácií, ktoré je možné šíriť pomocou e-mailovej komunikácie a uvádzať, kedy je potrebné e-mailové správy šifrovať. Môže takisto určiť či môže užívateľ hrať počítačové hry počas pracovnej doby, resp. využívať firemné zdroje ako je e-mail a prístup do internetu na súkromné účely.

Softwarová bezpečnosť

Časť sieťovej bezpečnostnej politiky zaoberajúca sa bezpečnosťou softwaru definuje ako bude spoločnosť využívať komerčný a nekomerčný software na serveroch, koncových staniciach a na sieti. Rovnako môže špecifikovať, kto môže kupovať a inštalovať software a definovať bezpečnostné metriky na sťahovanie softwaru z Internetu.

2.5.4 Kroky potrebné na zostavenie sieťovej bezpečnostnej politiky

Účel a ciele politiky

Predtým ako začne spoločnosť písať bezpečnostnú politiku, si musí jasne definovať ciele jednotlivých politik. Takto sa zabezpečí to, že sa politika nebude odchyľovať od pôvodného účelu. Cieľ politiky definuje prístup k zabezpečeniu siete. Typickým cieľom môže byť, že informácie predstavujú dôležité aktíva a že organizácia implementuje bezpečnostné metriky, aby tieto aktíva ochránila.

Rozsah a pôsobnosť dokumentu

Rozsah definuje aktíva, ktoré budú chránené danou sieťovou bezpečnostnou politikou. Sieťová bezpečnosť môže pokrývať pomerne dosť aspektov od fyzickej bezpečnosti až po osobnú, či procedurálnu bezpečnosť. Rozsah môže určiť, či sa politika vzťahuje len na sieťovú bezpečnosť alebo aj má širší bezpečnostný záber. Rozsah rovnako určuje kto má danú politiku dodržiavať, resp. či sa vzťahuje politika len na zamestnancov alebo aj na externých dodávateľov, zákazníkov, predajcov, ktorí musia politiku dodržiavať v prípade, že sa chcú pripojiť do siete organizácie.

Podpora vedenia

Predtým ako sa začne samotná práca na tvorbe politiky je potrebné zaistiť podporu vedenia spoločnosti, aby sa uľahčilo následné dodržiavanie politiky. Ak je to možné, odporúča sa medzi zainteresované osoby v oblasti informačnej bezpečnosti organizácie zahrnúť aj členov vedenia.

Odkazy na ostatné politiky

Jednotlivé politiky by sa mali na seba odkazovať a navzájom dopĺňovať. To umožní lepšie nadefinovať ciele a rozsah jednotlivých politík.

Ohodnotenie rizík

Pred samotným definovaním bezpečnostných politík je potrebné vykonať dôkladnú analýzu rizík. Tá určí na aké problémy je potrebné sa zamerať. Správa o hodnotení rizík slúži ako hodnotný nástroj pri tvorbe sieťových bezpečnostných politík.

Vytvorenie politiky

Je potrebné nadefinovať jednotlivé časti politiky. Tie sa budú odvíjať o správy hodnotenia rizík. Nie všetky časti je potrebné do výslednej politiky zahrnúť. Všetko závisí od sieťovej štruktúry, lokality a na štruktúre samotnej firmy. Politika by sa mala zamerať na všetky riziká v správe, tie riziká, ktoré nie je možné zahrnúť, by mali byť uvedené v poznámke.

Vyhodnotenie

Po vytvorení politiky by malo dôjsť k jej vyhodnoteniu, či spĺňa určené ciele. Medzi vhodné otázky patria napríklad:

- Je politika v súlade so zákonmi a povinnosťami voči tretím stranám?
- Ohrozuje politika záujmy zamestnancov, organizácie alebo tretích strán?
- Je politika praktická, funkčná a je možné vymáhať jej dodržiavanie?
- Rieši politika všetky formy komunikácie a vedenia záznamov v rámci organizácie?

- Je politika riadne prezentovaná a odsúhlasená všetkými zúčastnenými stranami?

2.6 Referenčná architektúra pre sieťovú bezpečnosť

Norma ISO/IEC 18028-2 (*Network Security Architecture*) (8) uvádza referenčnú architektúru, ktorá bola vytvorená na riešenie výziev poskytovateľov služieb, spoločností a ich zákazníkov a je použiteľná pre bezdrôtové, optické aj metalické, dátové a konvergované siete. Táto referenčná architektúra predstavuje vysokoúrovňovú bezpečnostnú architektúru, ktorá môže poslúžiť ako základ pri návrhu detailnejších bezpečnostných riešení pre rôzne typy sietí. Rieši bezpečnostné problémy správy, riadenia a využívania sieťových služieb, infraštruktúry a aplikácií. Poskytuje komplexnú *end-to-end* perspektívu zabezpečenia siete a môže byť aplikovaná na sieťové prvky, služby a aplikácie za účelom predvídania, zistenia a opravy bezpečnostných zraniteľností. Referenčná architektúra logicky delí komplexnú sadu sieťových funkcií spojených so zabezpečením do samostatných blokov. Toto rozdelenie umožňuje systematický prístup k zabezpečeniu a môže byť použité pri plánovaní nových bezpečnostných riešení, ako aj na hodnotenie bezpečnosti existujúcej siete. Referenčná architektúra rieši potreby sieťovej bezpečnosti pokrytím nasledujúcich otázok:

- Aké informácie musia byť chránené?
- Aké sú bezpečnostné riziká, a aká ochrana je potrebná na riadenie týchto rizík?
- Aké sieťové aktivity je potrebné chrániť?
- Aké typy sieťových zariadení je potrebné chrániť?

Hodnotenie rizík by malo byť vykonané podľa dôležitosti ochrany a malo by pomôcť určiť vhodné bezpečnostné opatrenia pre bezpečnostnú architektúru. Tieto otázky sú pokryté tromi prvkami: bezpečnostné dimenzie, bezpečnostné roviny a bezpečnostné vrstvy.

2.6.1 Bezpečnostné dimenzie

V rámci procesu riadenia rizík sú identifikované vhodné bezpečnostné metriky na riadenie, prípadne zmiernenie hodnotených rizík. Bezpečnostné dimenzie predstavujú zoskupenie bezpečnostných metrík, ktoré sú použité pri implementácii určitých aspektov sieťovej bezpečnosti. Koncept sieťových dimenzií nie je obmedzený len na siete, ale je rovnako použiteľný v kontexte aplikácií, resp. informácií koncových užívateľov. Navyše sa dajú tieto dimenzie aplikovať na poskytovateľov služieb alebo organizácie ponúkajúce bezpečnostné služby svojim zákazníkom. Bezpečnostné dimenzie sú: riadenie prístupu, autentizácia, nepopierateľnosť, dôvernosť dát, bezpečnosť komunikačných tokov, integrita dát, dostupnosť a súkromie.

Bezpečnostná dimenzia riadenia prístupu

Táto dimenzia poskytuje autorizáciu použitia sieťových zdrojov. Riadenie prístupu zaisťuje, že len autorizovaný personál alebo zariadenie má prístup k sieťovým prvkom, uloženým informáciám, informačným tokom, službám a aplikáciám.

Bezpečnostná dimenzia autentizácie

Bezpečnostná dimenzia autentizácie slúži na potvrdenie identity alebo iných autorizujúcich atribútov komunikujúcej entity. Autentizácia zaisťuje platnosť prehlásenej identity pri využití kontroly prístupu entít zúčastnených v komunikácii (napr. osoby, zariadenia, služby alebo aplikácie) a poskytuje uistenie, že komunikujúca entita sa nesnaží pozmeniť svoju identitu za účelom zneužitia zdrojov, prípadne sa nesnaží o neautorizované opakovanie prechádzajúcej komunikácie. Autentizačné metódy, založené na technikách ako užívateľské meno a heslo, viacfaktorová autentizácia (napr. token), biometria, sú pomerne rozšírené

Bezpečnostná dimenzia nepopierateľnosti

Táto dimenzia poskytuje technické prostriedky na zamedzenie tomu, že nejaká entita nebude schopná vykonať istú činnosť súvisiacu s dátami na sieti, tým, že budú dostupné dôkazy o vykonaní takejto činnosti (napr. dôkaz úmyslu, pôvodu dát, dôkaz vlastníctva, dôkaz využitia zdrojov). Slúži ako dostupný dôkaz tretej strane o tom, že istá udalosť, resp. činnosť reálne nastala.

Bezpečnostná dimenzia dôvernosti dát

Dimenzia dôvernosti dát chráni dáta pred neoprávnených zverejnením. Na zaistenie dôvernosti dát sa často využíva šifrovanie. Za účelom zabezpečenia dôvernosti sa používajú techniky ako *access control lists* a práva nastavené jednotlivým dokumentom.

Bezpečnostná dimenzia komunikačných tokov

Táto dimenzia zaisťuje, že informácie putujú po sieti len medzi autorizovanými koncovými zariadeniami (informácie nie sú presmerované alebo zachytené na ceste od zdroja k cieľu). Mechanizmy tejto dimenzie nechránia informácie pred modifikáciou / poškodením dát, to je úloha integrity dát. Medzi techniky používaná na zaistenie bezpečnosti komunikačných tokov patria napr. VLAN a VPN.

Bezpečnostná dimenzia integrity dát

Bezpečnostná dimenzia integrity dát zaisťuje korektnosť alebo presnosť (napr. či sú dáta spracovávané autorizovanými procesmi alebo autorizovanými osobami či zariadeniami) dát. Dáta sú chránené pred neautorizovanou zmenou, vymazaním, vytvorením a replikáciou. Existuje viacero spôsobov ako zaistiť integritu dát, napri. MD5 alebo SHA-1.

Bezpečnostná dimenzia dostupnosti

Bezpečnostná dimenzia dostupnosti zaisťuje, že sa nevyskytuje odmietnutie autorizovaného prístupu k sieťovým prvkom, uloženým informáciám, informačným tokom, službám a aplikáciám z dôvodu udalostí ovplyvňujúcich počítačovú sieť. Havarijne plány a plány obnovy sú zahrnuté do tejto kategórie.

Bezpečnostná dimenzia súkromia

Dimenzia súkromia poskytuje ochranu informácii, ktoré môžu byť získané analýzou sieťovej komunikácie. Príklady takýchto informácií tvoria navštívené webové stránky jednotlivými užívateľmi, geografická poloha užívateľov, IP adresy a DNS mená zariadení v sieti poskytovateľa služieb. NAT a aplikácie typu proxy predstavujú príklady techník použiteľných na ochranu súkromia. Táto dimenzia by mala v súlade s legislatívou poskytnúť vhodnú ochranu osobných údajov.

2.6.2 Bezpečnostné vrstvy

Aby bolo možné poskytnúť komplexné bezpečnostné riešenie je potrebné bezpečnostné dimenzie aplikovať hierarchicky podľa sieťových zariadení a zoskupení. Takéto hierarchické usporiadanie je vymedzené ako bezpečnostné vrstvy. Referenčná architektúra definuje tri bezpečnostné vrstvy: infraštruktúra, služby, aplikácie. Jednotlivé bezpečnostné vrstvy poskytujú bezpečné sieťové riešenia jedna pre druhú: bezpečnostná vrstva infraštruktúry umožňuje vytvoriť bezpečnostné riešenie pre vrstvu služieb a tá umožňuje vznik riešenia pre aplikačnú vrstvu. Referenčná architektúra sa zameriava na fakt, že každá vrstva má rozdielne bezpečnostné zraniteľnosti a poskytuje ochranu pred potenciálnymi hrozbami najvhodnejším spôsobom, pre tú ktorú vrstvu. Rozhodnutie, či vyššie vrstvy sa spoliehajú na riešenie nižších vrstiev alebo či sa ochrana na každej vrstve rieši komplexne je ponechané na samotnú implementáciu. Je potrebné zdôrazniť, že bezpečnostné vrstvy majú rozdielny význam ako vrstvy ISO/OSI sieťového modelu. Bezpečnostné vrstvy identifikujú potreby bezpečnosti v produktoch a riešeniach poskytnutím sekvenčnej perspektívy sieťovej bezpečnosti. Najprv sú identifikované zraniteľnosti pre infraštruktúru, potom pre služby a nakoniec pre aplikácie. Bezpečnostné dimenzie identifikujú oblasti, ktoré je potrebné obsiahnuť v každej bezpečnostnej vrstve.

Bezpečnostná vrstva infraštruktúry

Bezpečnostná vrstva infraštruktúry pozostáva zo sieťových zariadení a prenosových riešení ochránených pomocou bezpečnostných dimenzií. Infraštruktúra predstavuje základné stavebné bloky sietí, ich služieb a aplikácií. Príklady konkrétnych častí tejto vrstvy predstavujú zariadenia typu switch, router, server, rovnako ako aj ich vzájomné prepojenie.

Bezpečnostná vrstva služieb

Táto vrstva rieši bezpečnosť služieb, ktoré poskytovatelia garantujú svojim zákazníkom. Tieto služby majú pomerne široký záber od prenosu dát a zabezpečenia

konektivity cez služby potrebné na poskytovanie prístupu na Internet (autentizácie, autorizácia a účtovacie služby, dynamická konfigurácia staníc, DNS apod.) až po služby pridanej hodnoty ako telefonovanie po sieti, QoS, VPN, lokalizačné služby apod. Táto vrstva sa využíva na ochranu poskytovateľov služieb a ich zákazníkov, pretože obe strany predstavujú potenciálne ciele bezpečnostných hrozieb. Útočník sa môže napríklad pokúsiť zamedziť poskytovateľovi služieb ponúkať služby, resp. môže narušiť využívanie služby niektorým konkrétnym zákazníkom.

Bezpečnostná vrstva aplikácií

Aplikačná bezpečnostná vrstva sa zameriava na bezpečnosť sieťových aplikácií. Tieto aplikácie fungujú vďaka poskytovaným službám a zahŕňajú prenos dát (napr. FTP) a aplikácie ako webové prehliadače, aplikácie podporujúce hlasové služby, email, rovnako ako aj CRM systémy, on-line výukové programy, video prenos atd. Na tejto vrstve existujú štyri potenciálne ciele bezpečnostných útokov: užívateľ aplikácie, poskytovateľ aplikácie, middleware poskytovaný integrátorom (napr. webhosting) a poskytovateľ služby.

2.6.3 Bezpečnostné roviny

Bezpečnostná rovina predstavuje istý typ sieťovej aktivity chránenej mechanizmom implementovaným pre bezpečnostné dimenzie. Referenčná architektúra definuje tri bezpečnostné roviny, aby bolo možné adresovať tri typy chránených aktivít, ktoré sa vyskytujú v sieti. Bezpečnostné roviny sa delia na bezpečnostnú rovinu správy, bezpečnostnú rovinu kontroly a bezpečnostnú rovinu koncového užívateľa. Tieto roviny pokrývajú špecifické potreby súvisiace so správou sietí, kontrolou a signalizáciou aktivít a s aktivitami koncového užívateľa. Siete by mali byť navrhnuté tak, aby udalosti na jednej bezpečnostnej rovine boli izolované od udalostí na inej bezpečnostnej rovine. Napríklad záplava DNS dotazov na rovine koncového užívateľa by nemala zabrániť administrátorom siete problém odstrániť apod. Každý typ sieťovej aktivity má spoje špecifické bezpečnostné požiadavky. Koncept bezpečnostných rovín umožňuje rozlišovať medzi bezpečnostnými potrebami spojenými so skupinou aktivít a medzi možnosťou zaoberať sa aktivitami samostatne. Napríklad VoIP je súčasťou bezpečnostnej vrstvy služieb. Zabezpečenie správy VoIP musí byť nezávislé od zabezpečenia dostupnosti služby (napr. protokoly ako SIP) a rovnako musí byť nezávislé od dát prenášaných užívateľom služby (napr. hlas).

Bezpečnostná rovina správy

Bezpečnostná rovina správy je prepojená s ochranou funkcií sieťových prvkov, prenosových technológií, kancelárskych systémov a dátových centier. Je potrebné poznamenať, že sieť prenášajúca dáta súvisiace s týmito aktivitami môže byť v rámci firemnej siete a rovnako môže zasahovať aj mimo samotnú organizáciu.

Bezpečnostná rovina kontroly

Táto rovina súvisí s ochranou aktivít, ktoré umožňujú efektívne doručenie informácií a využitie služieb a aplikácií na sieti. Typicky zahrňuje komunikáciu, ktorou sieťové zariadenia (router, switch) vyberajú najvhodnejšiu cestu pre dáta v sieti. Spadajú tu tzv. kontrolné, resp. signalizačné informácie. Sieťová komunikácia obsahujúca tieto informácie môže byť v rámci firemnej siete, ale mimo organizáciu. Napr. v IP sieťach putujú kontrolné informácie lokálne, zatiaľ čo PSTN prenáša kontrolné informácie v samostatnej signalizačnej sieti (SS7 sieť). Príklady takejto komunikácie zahrňujú smerovacie protokoly, DNS, SIP, SS7 atď.

Bezpečnostná rovina koncového užívateľa

Bezpečnostná rovina koncového užívateľa rieši bezpečnosť prístupu a využitiu siete poskytovateľa služieb koncovými zákazníkmi. Rovnako sa zaoberá ochranou užívateľových dátových tokov. Užívatelia môžu využívať sieť, ktorá poskytuje konektivitu, napr. za účelom využitia služieb ako VPN alebo chcú využiť sieťové aplikácie na sieti.

2.6.4 Bezpečnostné hrozby

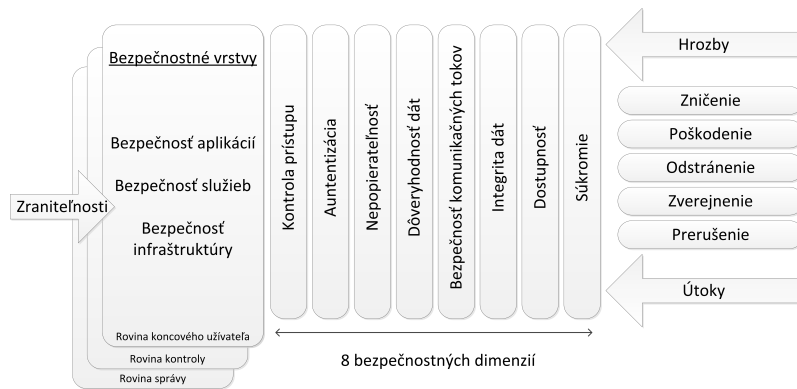
Referenčná architektúra definuje plán a sadu princípov, ktoré popisujú bezpečnostnú štruktúru pre koncové bezpečnostné riešenia. Architektúra identifikuje bezpečnostné problémy, ktoré je potrebné riešiť, aby sa predišlo úmyselným hrozbám, rovnako ako aj náhodným. V rámci referenčnej architektúry sa uvažujú nasledujúce hrozby:

- zničenie informácie a / alebo iných zdrojov, poškodenie alebo
- modifikácia informácie, krádež, odstránenie alebo strata informácie
- a / alebo iných zdrojov, zverejnenie informácie,
- prerušenie služby

Obrázok 2.5 zobrazuje referenčnú architektúru vzhľadom na bezpečnostné dimenzie, vrstvy, roviny a prezentované hrozby. Ide o koncept ochrany siete bezpečnostnými dimenziami na každej rovine všetkých bezpečnostných vrstiev za účelom poskytnúť obsiahle bezpečnostné riešenie. Je potrebné zdôrazniť, že v závislosti na požiadavky na sieťovú bezpečnosť, nemusí byť potrebné mať zahrnuté všetky prvky architektúry (tzn. mať všetky dimenzie, vrstvy a roviny).

2.7 Bezpečnosť sieťovej infraštruktúry

Rozvoj technológií je rozhodujúcim predpokladom pre zlepšovanie prevádzkového riadenia a finančnej efektivity. Tento prudký rozvoj v súvislosti so spoľahnutím sa na komunikačné technológie prináša zvýšené riziká. Širší prístup k sieťam, súborom a webovým stránkam zvyšuje hrozby predstavujúce výrazne väčšie bezpečnostné



Obr. 2.5: Referenčná architektúra (Prevzaté z (8))

riziko. Bezpečnostné predpisy by sa pritom nemali stať zásadnou prekážkou pre zlepšenie služieb a investícií do IT. Spoločnosť *Panduit* je svetový líder vo vývoji a produkcii technicky špičkových riešení optimalizácie bezpečnosti fyzickej infraštruktúry sietí. Pre siete podľa ISO 27001 vytvoril Panduit riešenie Panduit NISS (*Network Infrastructure Security Solution*). Toto riešenie bezpečnosti sieťovej infraštruktúry neumožní na fyzickej vrstve neoprávnený prístup do siete a fyzické zmeny systému neoprávneným osobám. Celý systém NISS je založený na nasledujúcich častiach (13):

- kľúčované prvky metallickej a optickej konektivity neumožňujú zasunúť kľúčovaný konektor do neklúčovaného portu a do portu s iným typom kľúča, neklúčované konektory nie je možné zasunúť do žiadneho kľúčovaného portu
- prvky pre fyzické blokovanie metalických a optických portov neumožňujú bez špeciálneho nástroja port uvoľniť
- zámky pre *Patch Cord* (metalický alebo optický) neumožňujú bez špeciálneho nástroja *Patch Cord* pripojiť do portu a ani ho vypojiť
- zabezpečené dátové zásuvky neumožňujú bez potrebných znalostí a špeciálneho vybavenia prístup k portom
- zabezpečené káblové žlaby neumožňujú bez potrebných znalostí a špeciálneho vybavenia odobrať kryty žlabov

2.7.1 Kľúčovaná konektivita

Kľúčované metalické a optické kabelážne systémy zaisťujú prevedenie bezpečnej, modulárnej, *end-to-end* konektivity pre komunikáciu z dátového centra do pracovnej stanice. Kľúčovanie prvkov konektivity výrazne zvyšuje zabezpečenie siete s využitím pozitívnych a negatívnych kľúčov prvkov, ktoré mechanicky rozlišujú pripojenie k sieti. Kľúčovaný *Plug* nie je možné fyzicky zasunúť do *Jacku* s iným typom kľúča ani do *Jacku* bez kľúča. Každý typ kľúča má pridelenú svoju farbu. Neklúčovaný *Plug* nie je možné zasunúť do žiadneho kľúčovaného *Jacku*. To isté platí pre konektory a adaptéry optických káblov. Množina farieb kľúčov vizuálne odlišuje spoje a fyzickým obmedzením bráni nechcenému pripojeniu k sieťovej infraštruktúre. Pre

zvýšenie bezpečnosti u viacerých sietí na jednej kabeláži umožňuje vylúčenie rizika zámeny prístupu a blokuje prístup do siete neautorizovaným užívateľom.

2.7.2 Zabezpečenie siete (príslušenstvo)

Prvky príslušenstva pre zabezpečenie siete blokujú neautorizovaný prístup do existujúcej sieťovej infraštruktúry. Umožňujú zablokovať porty aktívnych prvkov, konsolidačných bodov, dátových zásuviek, koncových zariadení a *Patch Panel*. Toto riešenie šetrí čas a náklady spojené s výpadkom siete, narušením zabezpečenia dát, obnovou infraštruktúry a výmenou hardwaru v dôsledku krádeží. Inovatívna konštrukcia *block-out* prvkov fyzicky zablokuje port RJ-45 a uvoľnenie je možné len pomocou špeciálneho nástroja na demontáž. Tým zaisťuje ochranu a bezpečnosť sieťovej infraštruktúry. Univerzálna konštrukcia *lock-in* prvkov je kompatibilná s väčšinou existujúcich *patch panelov*, dátových zásuviek, IP kamier, IP telefónov a ďalších IP zariadení. Tieto prvky umožňujú uzamknutie metalických *Patch Cordov*. Bez špeciálneho nástroja ich nie je možné prepojovacími káblami do portu zapojiť a ani z portu odobrať.

Kapitola 3

Návrh riešenia

V návrhu riešenia budú riešené tri oblasti. Správa o hodnotení rizík určí potrebu opatrení voči existujúcim rizikám. Praktickým nasadením opatrení vzniknú v druhej časti bezpečnostné politiky zamerané na jednotlivé problémové oblasti. V poslednej časti bude samostatne riešené posilnenie bezpečnosti sieťovej infraštruktúry spoločnosti.

3.1 Správa o hodnotení rizík

Cieľom hodnotenia rizík je identifikovať aktíva spoločnosti, posúdiť prípadné hrozby a na ich základe identifikovať riziká, ktoré musí spoločnosť odstrániť aplikáciou bezpečnostných opatrení.

3.1.1 Identifikácia aktív a ich hodnotenie

V rámci identifikácie a hodnotenia aktív z pohľadu počítačových sietí je potrebné nájsť kritické prvky, ktoré spoločnosť buď má fyzicky v sieťovej infraštruktúre, alebo sú uložené v pracovných staniciach zamestnancov a je možné k nim získať prístup cez sieť. Vzhľadom na rôznorodosť sieťových prvkov, dostupných dokumentov ovplyvňujúcich chod spoločnosti a špecifické aspekty súvisiace s prácou softwarovej firmy, budú aktíva rozdelené do dvoch kategórií: hmotné (napr. hardware) a nehmotné (napr. softwarové a elektronické dokumenty). Aktíva budeme hodnotiť na základe ich hodnoty a dopadu ich straty, zničenia, nedostupnosti apod. na fungovanie spoločnosti.

Hodnota aktíva	Označenie	Popis
Nízka	1	Žiadny dopad pre spoločnosť
Nízka	2	Mierny dopad pre spoločnosť
Stredná	3	Stredný dopad pre spoločnosť
Vysoká	4	Vysoký dopad pre spoločnosť
Vysoká	5	Kritický dopad pre spoločnosť

Tabuľka 3.1: Schéma hodnotenia dopadu (Zdroj: Vytvorené pre potreby práce)

Nasledujúca tabuľka uvádza identifikované aktíva nachádzajúce sa v počítačovej sieti analyzovanej spoločnosti.

Názov aktíva	Popis aktíva	Váha
Server	Obsahuje dôležité firemná dáta	3
Switch	Umožňuje prístup k sieti	4
Pracovná stanica	Obsahuje dôležité firemné dáta	2
Zdrojové kódy	Forma technického know-how	5
Interná dokumentácia	Forma technického know-how	5
Časový plán vývoja	Môže znamenať konkurenčnú výhodu	3
Pracovné zmluvy	Citlivé informácie o zamestancoch	3
Obchodné zmluvy	Citlivé informácie o obchodných partneroch	3
Strategický plán	Budúce smerovanie spoločnosti	4
Faktúry	Finančné zdravie spoločnosti	3

Tabuľka 3.2: Aktíva spoločnosti (Zdroj: Vytvorené pre potreby práce)

3.1.2 Identifikácia hrozieb a ich pravdepodobnosť

V súvislosti s hrozbami v prostredí počítačových sietí podľa noriem ISO/IEC 18028-1 (7) a ISO/IEC 18028-2 (8) je potrebné zamerať sa nie len na architektúru siete ale aj na aplikácie využívané na sieti, prípadne nakonfigurované protokoly. Prístupom ku koncovej stanici je možné nainštalovať sieťovú aplikáciu a aktivovať ju vo firemnom prostredí apod. Zároveň nedostatočne aktualizovaný software rovnako predstavuje pre spoločnosť hrozbu.

Každá hrozba môže nastať s istou pravdepodobnosťou. Pravdepodobnosť je možné vyjadriť za rok a na základe rozsahu určiť stupeň hrozby. Nasledujúca tabuľka zobrazuje jednu z možností ako sa dá pravdepodobnosť hrozbám priradiť.

Stupeň	% za rok	Slovné vyjadrenie
1	$\langle 0; 5 \rangle$	Prakticky nepravdepodobné
2	$\langle 5; 20 \rangle$	Málo pravdepodobné
3	$\langle 20; 50 \rangle$	Príležitostné
4	$\langle 50; 70 \rangle$	Pravdepodobné až časté
5	$\langle 70; 100 \rangle$	Veľmi časté

Tabuľka 3.3: Hodnoty pravdepodobnosti úrovne hrozby (Prevzaté z (9))

Na základe uvedených noriem z oblasti počítačovej bezpečnosti boli vybraté nasledujúce hrozby (uvedené aj s pravdepodobnosťou výskytu - P, tej ktorej konkrétnej hrozby):

Hrozba	P
Neautor. prístup k sieťovým zariadeniam	3
Server bez bezpečnostnej záplaty	2
Nízka kvalita hesiel	3
Krádež hardwaru	2
Škodlivý kód	4
Neautorizované pripojenie do LAN	4
Zlyhanie hardwaru	2
Prednastavené heslá na sieťových prvkoch	3
Nedostatočná úroveň autentizácie	3
Zahltenie siete	2
Krádež identity	3
Útoky z vonku na sieť	3

Tabuľka 3.4: Pravdepodobnosť výskytu hrozieb (Zdroj: Vytvorené pre potreby práce)

3.1.3 Vyhodnotenie miery rizík

Na celkové vyhodnotenie miery rizík bude použitá súčtová matica rizík prezentovaná v ISO/IEC 27005. Súčtová matica určuje celkové riziko na základe súčtu dopadu (hodnoty aktíva) a pravdepodobnosti výskytu hrozby v prostredí analyzovanej spoločnosti. Nasledujúca tabuľka vysvetľuje jednotlivé kategórie rizík. Dáva do vzťahu dopad a pravdepodobnosť.

	1	2	3	4	5
5	6	7	8	9	10
4	5	6	7	8	9
3	4	5	6	7	8
2	3	4	5	6	7
1	2	3	4	5	6

Tabuľka 3.5: Súčtová matica rizík (Prevzaté z (9))

		A1	A2	A3	A4	A5	A6	A7	A8	A9	A10
	A	3	4	2	5	5	3	3	3	4	3
Hrozby	T										
Neautor.	3	6	7	5	8	8	6	6	6	7	6
Server bez záplat	2	5	6	4	7	7	5	5	5	6	5
Nízka kvalita hesiel	3	6	7	5	8	8	6	6	6	7	6
Krádež hardwaru	2	5	6	4	7	7	5	5	5	6	5
Škodlivý kód	4	7	8	6	9	9	7	7	7	8	7
Neautor. pripojenie	4	7	8	6	9	9	7	7	7	8	7
Zlyhanie hardwaru	2	5	6	4	7	7	5	5	5	6	5
Prednastavené heslá	3	6	7	5	8	8	6	6	6	7	6
Nedost. autentizácia	3	6	7	5	8	8	6	6	6	7	6
Zahľtenie siete	2	5	6	4	7	7	5	5	5	6	5
Krádež identity	3	6	7	5	8	8	6	6	6	7	6
Útoky na sieť	3	6	7	5	8	8	6	6	6	7	6

Tabuľka 3.6: Súčtová matica rizík (Zdroj: Vytvorené pre potreby práce)

3.2 Sieťová bezpečnostná politika

Na základe správy o hodnotení rizík je potrebné vykonať kroky na zmiernenie identifikovaných rizík vhodnými opatreniami a ich zavedením do každodennej praxe analyzovanej spoločnosti. Práve za týmto účelom je pre spoločnosť navrhnutá Sieťová bezpečnostná politika pozostávajúca zo sady zásad zabezpečení. Jednotlivé zásady sa zameriavajú na odstránenie problémov s rizikami a riešia bezpečnosť so zámerom pokryť čo najväčší záber bezpečnostných dimenzií, vrstiev a rovín tak, ako boli opísané v teoretickej časti tejto práce. V tejto časti vyčleníme, definujeme Tím pre kontrolu zásad zabezpečenia tak, ako je to navrhované v (10). Nasledujúca tabuľka popisuje povinnosti jednotlivých členov.

Zástupca skupiny	Povinnosti	zo spoločnosti
Vedenie firmy	Ich úlohou je uskutočňovanie (vynucovanie) prijatých zásad. Príslušným členom býva často vyšší pracovník oddelenia ľudských zdrojov.	HR pracovník
Tím podnikovej bezpečnosti	Do tímu je potrebné menovať niekoho, kto má veľmi dobré odborné znalosti a prehľad problematiky	CTO
Užívateľská sféra	Zástupca užívateľov preverí zásady z pohľadu bežného užívateľa	SW vývojár
Právne oddelenie	Právnik sa nemusí zásadám zabezpečenia venovať naplno, ale niekto by mal ich obsah revidovať s ohľadom na platné zákonné normy.	CEO
Publikačná skupina	Tento člen tímu prináša návrhy ohľadne spôsobu tvorby výsledných zásad členom organizácie, ktorí by ich mali prijať.	Riešiteľ DP

Tabuľka 3.7: Členovia tímu pre kontrolu zásad zabezpečenia (Zdroj: Vytvorené pre potreby práce)

Na základe uvedených skutočností sú vytvorené bezpečnostné zásady Publikačnou skupinou. Pre potreby zásad je potrebné rozlišovať tri zástupné označenia: XXX - analyzovaná spoločnosť; YYY - externý alebo interný auditor; ZZZ - auditorská spoločnosť. Všetky bezpečnostné zásady obsahujú v poslednom bode aj náklady vynaložené na ich tvorbu. Navrhnuté zásady vychádzajú z dostupných šablón pre rôzne oblasti od organizácie SANS (11).

3.2.1 Prípustné užívanie

Celkový prehľad

Tím podnikovej bezpečnosti je pri zostavovaní zásad prípustného užívania vedený snahou nezavádzať žiadne obmedzenia, ktoré by boli v rozpore s firemnou kultúrou spoločnosti XXX, ktorá je postavená na otvorenosti, dôvere a integrite. Úlohou tímu podnikovej bezpečnosti je neustále chrániť zamestnanca, partnerov, ale aj samotnú firmu XXX pred nezákonným alebo škodlivým jednaním jednotlivcov, a to vedomým i nevedomým.

Všetky systémy, súvisiace s Internetom, intranetom a extranetom, vrátane počítačového vybavenia, softwaru, operačných systémov, záznamových médií, sieťových účtov s prístupom k elektronickej pošte, prechádzaniu WWW a FTP (ako aj ďalšie prostriedky) sú vlastníctvom firmy XXX. Tieto systémy sú určené na zaistenie chodu firmy XXX a pre činnosti, ktoré slúžia záujmom spoločnosti XXX, jej klientom a zákazníkmi.

Účinné zabezpečenie je prierezová, tímová činnosť, do ktorej sa musia zapojiť a podporovať všetci zamestnanci, dodávatelia, obchodní partneri a ďalšie subjekty,

ktoré pracujú s informáciami a informačnými systémami. Každý užívateľ počítača je povinný poznať pravidlá stanovené týmito zásadami zabezpečenia a pri svojej práci sa nimi primerane riadiť.

Účel dokumentu

Účelom týchto zásad zabezpečenia je stanoviť pravidlá prípustného užívania počítačového vybavenia vo firme XXX. Tieto pravidlá slúžia k ochrane firmy XXX a jej zamestnancov; neprípustné užívanie môže vystavovať spoločnosť XXX rôznym rizikám, napríklad vírovým útokom, napadnutiu sieťových systémov a služieb i právnomu postihu.

Pôsobnosť dokumentu

Tieto zásady zabezpečenia platia pre každého zamestnanca, dodávateľa, konzultanta, dočasného pracovníka a pre ostatné osoby vo firme XXX, vrátane osôb spojených s príslušnými cudzími subjektami. Ďalej platí pre všetky zariadenia, ktoré sú vo vlastníctve firmy XXX alebo sú ňou prenajaté, a tiež pre každé osobné zariadenie, ktoré môže prísť do styku s podnikovou infraštruktúrou.

Užitie dokumentu a jeho vlastníctvo

1. Snahou tímu podnikovej bezpečnosti firmy XXX je zaistiť primeranú úroveň súkromia, užívateľia si ale musia byť vedomí, že všetky dáta, ktoré v podnikových systémoch vytvoria, zostávajú vlastníctvom spoločnosti XXX. Vzhľadom na nutnosť ochrany siete nemôže vedenie firmy XXX zaručiť dôvernosť žiadnych informácií, uložených na sieťovom zariadení, ktoré je majetkom firmy XXX.
2. Zamestnanci sú zodpovední za prípadné osobné užívanie systémov, a to podľa svojho najlepšieho vedomia a svedomia. Jednotlivé oddelenia sú zodpovedné za vytvorenie zásad osobného užívania internetových, intranetových a extranetových systémov. Pokiaľ takého zásady neexistujú, bude sa zamestnanec riadiť všeobecnými zásadami osobného užívania v danom oddelení; v prípade akýchkoľvek pochybností sa obráti na svojho nadriadeného.
3. Tím podnikovej bezpečnosti odporúča užívateľom šifrovať všetky informácie, ktoré sami považujú za citlivé alebo zraniteľné.
4. Pre účely zachovania bezpečnosti a údržby siete môžu oprávnení zamestnanci kedykoľvek monitorovať zariadenia, systémy a sieťovú komunikáciu, a to v súlade so Zásadami pre audit.
5. S ohľadom zaistenia platnosti týchto Zásad si spoločnosť XXX vyhradzuje právo auditovať všetky siete a s nimi prepojené systémy, a to pravidelne a náhodným spôsobom

Bezpečnosť a dôverné informácie

1. Užívateľské rozhranie k informáciám obsiahnutým v internetových, intranetových a extranetových systémoch je potrebné klasifikovať ako dôverné alebo neutajované (bez klasifikácie), a to v súlade s podnikovými zásadami klasifikácie dôvernosti. Príklady dôverných informácií sú okrem iného:
 - Súkromné alebo dôverné firemné informácie
 - Podnikové stratégie a zámery
 - Informácie citlivé vzhľadom ku konkurencii a konkurenčnej analýzy
 - dáta podliehajú obchodnému tajomstvu, patenty, výsledky testov
 - Špecifikácie a prevádzkové parametre
 - Zoznamy zákazníkov a údaje o nich
 - Výskumné údaje
2. Zamestnanci musia všetkými vhodnými prostriedkami zabrániť neoprávnenému prístupu k týmto a podobným informáciám. Ak má zamestnanec podozrenie z úniku týchto informácií mimo spoločnosť XXX, musí bezprostredne upozorniť tím podnikovej bezpečnosti.
3. Heslá je potrebné uchovávať v tajnosti a bezpečí; zamestnanci nesmú účet požičať nikomu inému. Každý oprávnený užívateľ je zodpovedný za bezpečnosť svojho vlastného účtu a hesla. Systémové heslá je potrebné meniť najmenej raz za štvrtrok, užívateľské raz za 6 mesiacov.
4. Všetky osobné počítače, notebooky a pracovné stanice musia byť zabezpečené pomocou šetriča obrazovky s ochranou heslom a s automatickou aktiváciou najneskôr po 10 minútach nečinnosti alebo sa užívateľ pri vzdialení sa od počítača musí odhlásiť.
5. Príslušné údaje je nutné v súlade so Zásadami prípustného šifrovania, vydanými tímom podnikovej bezpečnosti, šifrovať.
6. Informácie umiestnené na prenosných počítačoch sú obzvlášť zraniteľné, a preto je nutné s nimi zachádzať mimoriadne opatrne.
7. V príspevkoch do diskusných skupín, kde zamestnanec uvádza firemnú e-mailovú adresu, musí byť uvedené upozornenie, podľa ktorého sú názory v príspevkoch len osobným názorom zamestnanca a nie nutne názorom firmy XXX, výnimkou sú príspevky súvisiace s plnením pracovných povinností.
8. Všetky počítačové systémy, ktoré zamestnanec používa a ktoré sú pripojené na Internet, intranet alebo extranet vo firme XXX, či už sú majetkom zamestnanca alebo firmy XXX, musia byť neustále kontrolované schváleným antivírusovým softwarom s aktuálnou databázou vírusov.

9. Pri otváraní e-mailových príloh od neznámych odosielateľov, ktoré môžu obsahovať vírusy, e-mailové bomby alebo trojské kone, si užívatelia musia počínať maximálne opatrne. V prípade pochybností je užívateľ povinný skontrolovať dokument ručne a pred otvorením prílohy sa spojiť s tímom podnikovej bezpečnosti.

Nepripustné užívanie

Nasledujúce aktivity sú všeobecne vzaté zakázané. Zamestnancom však môže byť tento zákaz zrušený pri plnení svojich pracovných povinností (napríklad podriadený systémového administrátora môže zablokovať prístup k sieti určitého hostiteľského počítača, ktorý narušuje chod prevádzkových služieb).

Za žiadnych okolností nie sú zamestnanci spoločnosti XXX pri práci s firemnými prostriedkami oprávnení na vykonávanie akýchkoľvek aktivít, ktoré sú v rozpore s platným vnútroštátnym a medzinárodným právom a nižšími zákonnými normami. Nižšie uvedený zoznam zakázaných aktivít nie je v žiadnom prípade vyčerpávajúci, predstavuje ale istý základný prehľad neprípustného užívania systémov.

Tieto aktivity v systéme a v sieti sú bez akýchkoľvek výnimiek prísne zakázané:

1. Porušovanie práv ľubovoľnej osoby či spoločnosti, chránených autorskými zákonmi, obchodným tajomstvom, patentovým alebo iným duševným vlastníctvom, prípadne podobnými zákonmi a nariadeniami, vrátane inštalácie a distribúcie odcudzeného či pirátskeho softwaru, ktorého užívanie nie je kryté odpovedajúcou licenciou, zakúpenou pre firmu XXX.
2. Neoprávnené kopírovanie materiálu podliehajúceho autorským právam, ako je mimo iné aj digitalizácia a distribúcia fotografií z časopisov, kníh a iných zdrojov krytých autorským právom, hudby chránenej autorským zákonom, a tiež inštalácia softwaru krytého autorským právom, pre ktorý nemá spoločnosť XXX ani koncový užívateľ potrebnú aktívnu licenciou, je prísne zakázaná.
3. Taký vývoz softwaru, odborných informácií, šifrovacieho softwaru a technológií, ktorý narušuje medzinárodné či miestne predpisy pre kontrolu exportu, je nelegálny. Pred prípadným exportom diskutabilného materiálu si zamestnanec musí vyžiadať súhlas nadriadeného.
4. Zavádzanie škodlivých či zlomyseľných programov do sietí a serverov (napríklad vírusov, červov, trojských koňov, e-mailových bômb atd.).
5. Prezradenie hesla k užívateľskému účtu iným osobám alebo povolenie na využívanie účtu inou osobou. Ak vykoná zamestnanec svoju prácu doma, spadajú medzi tieto osoby aj ostatní členovia rodiny a spoločnej domácnosti.
6. Aktívne využívanie počítačových systémov vo vlastníctve firmy XXX za účelom získavania alebo odosielania materiálu, ktorý narušuje platné zákony týkajúce sa sexuálneho obťažovania či nepriateľského správania sa na pracovisku, a to podľa zákonných noriem platných v mieste pracoviska užívateľa.
7. Odosielanie falošných ponúk výrobkov, tovaru alebo služieb z akéhokoľvek užívateľského účtu v spoločnosti XXX.

8. Jednanie, ktoré má za následok prelomenie bezpečnosti alebo narušenie sieťovej komunikácie. Medzi prelomenie bezpečnosti patrí okrem iného prístup k dátam, ktoré nie sú určené danému zamestnancovi alebo prihlásenie k serveru či na účet, ku ktorému nie je zamestnanec oprávnený pristupovať, iba ak ide o úlohy spojené s plnením pracovných povinností. Za narušenie považujeme v tejto časti dokumentu odpočúvanie v sieti, záplavy dotazov ping, falšovanie paketov, odoprenie služieb a falšovanie smerovacích informácií s nekalými úmyslami.
9. Prehľadávanie portov a skúmanie bezpečnosti je výslovne zakázané, ak to nie je dopredu informovaný tím podnikovej bezpečnosti.
10. Akákoľvek forma monitorovania siete, pri ktorej zamestnanec zadržuje či odpočúva dáta, ktoré pre neho nie sú určené, iba ak toto monitorovanie spadá pod normálne pracovné povinnosti zamestnanca.
11. Obchádzanie mechanizmov autentizácie či bezpečnosti ľubovoľného hostiteľského systému, siete alebo účtu.
12. Narušovanie alebo odoprenie služby ľubovoľnému inému užívateľovi.
13. Spúšťanie akýchkoľvek programov, skriptov a príkazov, alebo odosielanie akýchkoľvek správ, ktorých cieľom je narušovanie alebo zablokovanie terminálovej relácie iného užívateľa, a to lokálne, na Internete, intranete i extranete.
14. Poskytovanie informácií o zamestnancoch firmy XXX alebo zoznamu zamestnancov vonkajším subjektom.

Tieto aktivity v elektronickej pošte a pri komunikácii sú bez akýchkoľvek výnimiek prísne zakázané:

1. Odosielanie nevyžiadaných správ elektronickej pošty, hromadných správ alebo iného reklamného materiálu jednotlivcom, ktorí ich výslovne nepožadovali (e-mailový spam).
2. Akákoľvek forma obťažovania, a to elektronicou, telefónom a inými prostriedkami, a to v ľubovoľnom jazyku, s akoukoľvek frekvenciou a pri akejkoľvek veľkosti správ.
3. Neoprávnené používanie alebo falšovanie informácií v záhlaví elektronickej pošty.
4. Vyžadovanie e-mailových správ, určených pre ktoréhokoľvek iného užívateľa či adresu so zámerom obťažovania či zhromažďovania odpovedí.
5. Vytváranie a rozosielanie elektronickej pošty zo siete spoločnosti XXX či iných poskytovateľov internetových, intranetových a extranetových služieb v mene firmy XXX, prostredníctvom služby poskytovanou firmou XXX alebo pripojenou cez sieť firmy XXX.
6. Zasielanie rovnakých či podobných správ nepracovného charakteru do veľkého množstva diskusných skupín Usenet (spam v diskusných skupinách).

Uskutočňovanie zásad

Ľubovoľný zamestnanec, ktorý bude pristihnutý pri porušovaní uvedených zásad, bude vystavený disciplinárnemu konaniu a v prípade závažného porušenia pracovnej disciplíny môže byť aj prepustený zo zamestnania.

Finančné náklady

Činnosť	Počet hodín	Hodinová mzda	Celkom
Tvorba bezpečnostných zásad prípustného užívania	24	300 Kč	7 200 Kč

Tabuľka 3.8: Náklady na tvorbu bezpečnostných zásad prípustného užívania

3.2.2 Prípustné šifrovanie

Celkový prehľad

Stanovuje pravidlá, ktoré obmedzujú šifrovanie len na všeobecne známe, preverené a účinné algoritmy. Navyše určuje potrebné postupy, ktoré zaisťujú naplnenie príslušných zákonov a nižších predpisov.

Účel dokumentu

Účel týchto zásad je poskytnúť rady ako využívať len tie šifrovacie algoritmy, ktoré boli praxou overené a bola dokázaná ich efektívnosť.

Pôsobnosť dokumentu

Tieto zásady sa vzťahujú na všetkých zamestnancov spoločnosti XXX.

Všeobecné zásady

Symetrické kryptografické kľúče musia mať minimálnu dĺžku 80 bitov, odporúčaná dĺžka je však 128 bitov. Kľúče asymetrických kryptografických systémov musia mať dĺžku, ktorá zabezpečuje ekvivalentnú bezpečnosť. Požiadavky na dĺžku kľúčov budú každoročne revidované a upravené podľa aktuálnych možností technológií.

Uskutočňovanie zásad

Ľubovoľný zamestnanec, ktorý bude pristihnutý pri porušovaní uvedených zásad, bude vystavený disciplinárnemu konaniu a v prípade závažného porušenia pracovnej disciplíny môže byť aj prepustený zo zamestnania.

Finančné náklady

Činnosť	Počet hodín	Hodinová mzda	Celkom
Tvorba bezpečnostných zásad prípustného šifrovania	8	300 Kč	2 400 Kč

Tabuľka 3.9: Náklady na tvorbu bezpečnostných zásad prípustného šifrovania

3.2.3 Pokyny pre antivírovú ochranu

Spoločnosť XXX odporúča svojim zamestnancom dodržiavať nasledujúce pokyny za účelom predchádzania problémom s vírusmi:

- Používať antivírový software schválený spoločnosťou XXX. Stiahnite a nainštalujte aktuálnu verziu. Stahujte aktualizácie antivírového software hneď ako sú dostupné.
- Nikdy neotvárajte žiadne súbory ani makrá priložené k e-mailu od neznámeho, podozrivého alebo nedôveryhodného odosielateľa. Okamžite vymažte prílohy.
- Vymažte spam, reťazové a reklamné e-maily bez toho, aby ste ich posielali ďalej, v súlade so Zásadami prípustného užívania spoločnosti XXX.
- Nikdy nesťahujte súbory z neznámych alebo podozrivých zdrojov.
- Vyvarujte sa priamemu zdieľaniu disku s právami na čítanie a zápis pokiaľ to nie je nevyhnutne nutné za účelom plnenia pracovných povinností.
- Pravidelne zálohujte kritické dáta a systémové konfigurácie a bezpečne ich uložte.

Finančné náklady

Činnosť	Počet hodín	Hodinová mzda	Celkom
Tvorba pokynov pre antivírovú ochranu	4	300 Kč	1 200 Kč

Tabuľka 3.10: Náklady na tvorbu pokynov pre antivírovú ochranu

3.2.4 Práca s heslami

Celkový prehľad

Heslá sú veľmi dôležitou stránkou zabezpečenia počítačov a tvoria prvú obrannú líniu užívateľských účtov. Nevhodne zvolené heslo môže nakoniec viesť aj k narušeniu bezpečnosti celej podnikovej siete firmy XXX. Vzhľadom na to je každý zamestnanec firmy XXX (aj každý z užívateľov medzi dodávateľmi a odberateľmi firmy XXX, ktorí majú do firmy XXX prístup) zodpovedný za správny výber hesla a jeho zabezpečenie, ako popisujú nasledujúce časti dokumentu.

Účel dokumentu

Úlohou týchto zásad je zaviesť štandard na vytváranie silných hesiel, mechanizmy ochrany hesiel, a definovať spôsob ich merania.

Pôsobnosť dokumentu

Tieto zásady zabezpečenia platia pre každú osobu, ktorá je zodpovedná za určitý účet (alebo za ľubovoľný iný typ prístupu, ktorý podporuje alebo vyžaduje zadanie hesla), a to na ľubovoľnom systéme, ktorý je umiestnený v priestoroch firmy XXX, ktorý má prístup k firemnej sieti alebo na ktorom sú uložené neverejné informácie spoločnosti.

Všeobecné zásady

- Všetky systémové heslá sa musia zmeniť aspoň raz za štvrtrok .
- Všetky užívateľské heslá musia byť zmenené najmenej raz za 6 mesiacov; doporučený interval zmien je raz za 4 mesiace.
- Užívateľské účty s oprávneniami systémovej úrovne, pridelovanými pomocou členstva užívateľa v skupinách či pomocou iných programov musí mať jedinečné heslo, rôzne od hesiel všetkých ostatných účtov danej osoby.
- Heslá nesmú byť zapisované do správ elektronickej pošty ani do inej elektronickej komunikácie.
- Heslo nesmie žiadny užívateľ prezradiť nikomu inému, bez ohľadu na pozíciu prípadného žiadateľa v organizácii. Ak niekto požiada užívateľa o heslo, ten sa musí najprv spojiť s tímom podnikovej bezpečnosti.
- Všetky užívateľské aj systémové heslá musia ďalej odpovedať zásadám, ktoré sú popísané v ďalšej časti dokumentu

Všeobecné pravidlá pre zadávanie hesiel

Heslá sa v systémoch firmy XXX používajú na rôzne účely, napríklad heslá k užívateľským účtom, k webovým účtom, k e-mailovým účtom, k šporičom obrazovky, k hlasovej pošte apod. Len máloktorý systém podporuje pritom jednorázové tokeny (alebo dynamické heslá s jednorázovou platnosťou), a preto si každý užívateľ musí zvoliť dostatočne silné heslo.

Takto vyzerá typické slabé, nevhodné heslo:

- Heslo je kratšie ako 8 znakov.
- Heslo sa dá priamo nájsť v jazykovom slovníku (českom, anglickom alebo inom).
- Heslo je bežným výrazom ako napríklad:

- Meno člena rodiny, domáceho zvierata, priateľa, spolupracovníka, filmovej postavy apod.
- Výrazy a názvy z oblasti počítačov, príkazy, servery, firmy XXX, hardware, software.
- Slová obsahujúce názov spoločnosti.
- Jednoducho uhádnuteľné vzorky písmen a číslíc, ako napríklad aaabbb, qwerty, zyxwvuts, 123321 apod.
- Ľubovoľný z vyššie uvedených výrazov napísaný obrátene.
- Ľubovoľný z vyššie uvedených výrazov, pred alebo za ktorým je jedná číslica (napríklad heslo1, 4heslo).
- Mená športových klubov a hráčov.

Silné, správne vytvorené heslá môžeme napríklad charakterizovať takto:

- Obsahujú veľké aj malé písmená
- Obsahujú číslice a interpunkčné znamienka
- Majú dĺžku aspoň 8 znakov
- Nie sú tvorené žiadnym slovom z bežného slovníka, slangu, dialektu apod.
- Nie sú odvodené od žiadnych osobných údajov, mien členov rodiny atp.

Vytvorené heslá sa nesmú zapisovať na papier ani ukladať v elektronickej podobe. Preto je potrebné vytvárať také heslá, ktoré sa ľahko zapamätajú.

Štandardy na ochranu hesiel

Pre účty v systémoch firmy XXX si nevolte rovnaké heslo ako pre iný, cudzí systém (napr. pre osobný účet u poskytovateľa Internetu, pre vstup do bankového účtu, obchodovania s cennými papiermi atd.). Pokiaľ to je možné, tak nepoužívajte rovnaké heslo u niekoľkých rôznych systémov XXX, iné heslo si napríklad definujte pre vývojové oddelenie a iné pre bežnú podnikovú sieť.

Heslá k systémom XXX nedávajte k dispozícii ani administratívnym pracovníkom. Všetky heslá sa považujú za citlivé a dôverné údaje firmy XXX a je potrebné s nimi tak aj zachádzať.

Nasledujúce činnosti sú zakázané:

- Nikomu nehovorte heslo po telefóne.
- Nezapisujte heslo do e-mailovej správy.
- Nehovorte heslo svojmu nadriadenému.
- Nehovorte o svojich heslách pred druhými.
- Nenapovedajte nikomu ani formát hesla.

- Nepíšte heslo na dotazníky či bezpečnostné formuláre.
- Neinformujte o svojom hesle členov rodiny.
- Neinformujte o svojom hesle spolupracovníkov, a to ani pri odchode na dovolenku.

A ďalšie pravidlá:

- Pokiaľ vás niekto o heslo požiada, odvolajte sa na tento dokument, prípadne ho pošlite k niekomu z tímu podnikovej bezpečnosti.
- V aplikáciách nepoužívajte funkciu "Zapamätať si heslo".
- Znova, heslá nikde nezapisujte a neukladajte ich v kancelárii. Neukladajte ich ani do súborov, a to na žiadnom počítačovom systéme (vrátane prenosných počítačov apod.), ktorý nemá šifrovanie schválené tímom podnikovej bezpečnosti.
- Heslo si najmenej raz za šesť mesiacov zmeňte (výnimkou sú systémové heslá, ktoré sa musia meniť raz za tri mesiace). Doporučený interval zmeny je však štyri mesiace.
- Ak máte podozrenie, že váš účet bol napadnutý, oznámte bez odkladu incident tímu podnikovej bezpečnosti a okamžite zmeňte všetky heslá.
- Tím podnikovej bezpečnosti alebo ním poverení pracovníci môžu pravidelne či náhodne prevádzať pokusy o uhádnutie alebo prelomenie hesla. Pokiaľ takémuto testu heslo nevyhoví (podarí sa ho prelomiť alebo uhádnuť), musí si ho užívateľ okamžite zmeniť.

Uskutočňovanie zásad

Ľubovoľný zamestnanec, ktorý bude pristihnutý pri porušovaní tu uvedených zásad, bude vystavený disciplinárnemu konaniu a v prípade závažného porušenia pracovnej disciplíny môže byť aj prepustený zo zamestnania.

Finančné náklady

Činnosť	Počet hodín	Hodinová mzda	Celkom
Tvorba bezpečnostných zásad pre prácu s heslami	24	300 Kč	7 200 Kč

Tabuľka 3.11: Náklady na tvorbu bezpečnostných zásad pre prácu s heslami

3.2.5 Bezpečnosť komunikačných zariadení

Celkový prehľad

Vymedzuje štandardy pre základnú konfiguráciu interných serverov, ktoré sú vo vlastníctve a/alebo prevádzke spoločnosti, prípadne ktoré pracujú vo webovom hostovanom priestore.

Účel dokumentu

Tento dokument popisuje požiadavky na bezpečnostnú konfiguráciu komunikačných zariadení spoločnosti XXX.

Pôsobnosť dokumentu

Tieto zásady sa vzťahujú na všetky komunikačné zariadenia, ktoré sú súčasťou dátovej siete spoločnosti XXX.

Všeobecné zásady

Bezpečnostné funkcie nevyhnutné na minimalizáciu rizík súvisiacich s komunikačnými zariadeniami musia byť nakonfigurované v zariadeniach pred tým ako sú samotné zariadenia zapojené do počítačovej siete. Existujú dve možné role pre pracovníkov zodpovedných za správu komunikačných zariadení: monitorovanie a administrácia. V rámci role monitorovania má pracovník práva len na kontrolu konfigurácií. Administrátorská rola oprávňuje pracovníka k zmene konfiguračných parametrov. Všetky použité príkazy musia byť zaznamenané, rovnako ako aj ostatné bezpečnostné udalosti, ktoré môžu predstavovať hrozbu pre zariadenie.

Autentizácia a autorizácia

Lokálne užívateľské účty nie sú povolené na komunikačných zariadeniach. Každý sa musí autentizovať pomocou centálneho úložiska užívateľov a využívať protokol, ktorý redukuje riziko krádeže identity.

Šifrovaná komunikácia

Všetka komunikácia smerom od zariadenia musí byť šifrovaná silným kryptografickým algoritmom, aby sa znížilo riziko odpočúvania komunikácie a útokom typu *man-in-the-middle*.

Účtovanie

Udalosti zaznamenané komunikačnými zariadeniami musia byť uchované na médiu, ktoré je predmetom pravidelných záloh. Proces spravovania týchto záloh musí zaistiť, že obsiahnuté informácie neboli pozmenené.

Prístup k heslu administrátorského účtu komunikačného zariadenia

Heslo k administrátorskému účtu komunikačného zariadenia nemôže byť známe nikomu, kto spravuje zariadenie. Ak z akýchkoľvek dôvodov je potrebné využiť heslo inou ako dopredu určenou osobou (hlavný administrátor), je potrebné po dokončení úprav zmeniť heslo hlavným administrátorom, aby sa zachovala rovnaká úroveň bezpečnosti.

Uskutočňovanie zásad

Je požadované vykonávať pravidelný audit konfigurácie komunikačných zariadení. V prípade, že je identifikovaná nejaká anomália na zariadení, správca zariadenia vykoná potrebné kroky na zistenie zodpovednej osoby za zmeny v konfigurácii. Za porušenie týchto zásad je možné vyvodiť dôsledky v znení aktuálne platných bezpečnostných zásad spoločnosti XXX.

Finančné náklady

Činnosť	Počet hodín	Hodinová mzda	Celkom
Tvorba bezpečnostných zásad pre komunikačné zariadenia	6	300 Kč	1 800 Kč

Tabuľka 3.12: Náklady na tvorbu bezpečnostných zásad pre komunikačné zariadenia

3.2.6 Zabezpečenie pre router a switch

Celkový prehľad

Vymedzuje štandardy pre základnú konfiguráciu interných sieťových zariadení typu router a switch spoločnosti XXX.

Účel dokumentu

Popisuje povinnú minimálnu bezpečnostnú konfiguráciu všetkých zariadení typu router a switch, pripojených do ostrej prevádzkovej siete alebo používaných v akomkoľvek prevádzkovom prostredí spoločnosti XXX.

Pôsobnosť dokumentu

Všetky zariadenia typu router a switch pripojené do produkčnej siete spoločnosti XXX.

Všeobecné zásady

Každý router a switch musí spĺňať nasledujúce konfiguračné štandardy:

1. Neexistujú žiadne lokálne užívateľské účty. Všetky zariadenia musia využívať TACACS+ protokol na riadenie prístupu.
2. Heslá musia byť uložené v šifrovanej podobe. Žiadne zariadenie nemôže využívať prednastavené heslo.
3. Nasledujúce služby musia byť vypnuté:
4. (a) Malé TCP služby
(b) Malé UDP služby
(c) Webové služby

5. Nové prístupové pravidlá budú pridané podľa potrieb spoločnosti XXX
6. Telnet nie je možné použiť na správu zariadení, pokiaľ nie je komunikácia ochránená protokolom SSH.

Uskutočňovanie zásad

Ľubovoľný zamestnanec, ktorý bude pristihnutý pri porušovaní tu uvedených zásad, bude vystavený disciplinárnemu konaniu a v prípade závažného porušenia pracovnej disciplíny môže byť aj prepustený zo zamestnania.

Finančné náklady

Činnosť	Počet hodín	Hodinová mzda	Celkom
Tvorba bezpečnostných zásad pre zabezpečenie zariadení typu router a switch	6	300 Kč	1 800 Kč

Tabuľka 3.13: Náklady na tvorbu bezpečnostných zásad pre zabezpečenie zariadení typu router a switch

3.2.7 Zabezpečenie serverov

Celkový prehľad

Vymedzuje štandardy pre základnú konfiguráciu interných serverov, ktoré sú vo vlastníctve a/alebo prevádzke spoločnosti, prípadne ktoré pracujú vo webovom hostovanom priestore.

Účel dokumentu

Účelom týchto zásad je vytvoriť sadu štandardov pre základnú konfiguráciu interných serverov, ktoré sú vlastnené a / alebo spravované spoločnosťou XXX. Efektívna implementácia týchto zásad minimalizuje neautorizovaný prístup k informáciám a technológiám spoločnosti XXX.

Pôsobnosť dokumentu

Tieto zásady sa vzťahujú na servery vlastnené a spravované spoločnosťou XXX, ktoré sa nachádzajú priamo v sieti spoločnosti XXX.

Všeobecné zásady

Nasledujúce informácie o serveroch musia byť zaznamenané:

- Umiestnenie serveru a informácie ohľadom zálohovania
- Hardware a operačný systém/verzia.

- Hlavné funkcie serveru a nainštalované aplikácie (ak sa to na daný server vzťahuje).

Všetky konfiguračné zmeny musia byť zaznamenané a informácie o serveroch musia byť aktualizované po prevedení každej zmeny.

Konfiguračné pokyny

- Služby a aplikácie, ktoré nebudú využívané musia byť vypnuté.
- Prístup k službám musí byť zaznamenaný a/alebo zabezpečený.
- Najnovšie bezpečnostné záplaty musia byť nainštalované hneď ako sú dostupné. Jedinou výnimkou je situácia, kedy by ich okamžité nasadenie bolo v rozpore s aktuálnymi potrebami spoločnosti XXX pri poskytovaní služieb vyplývajúcich z predmetu podnikania.
- Nikdy nevyužívať administrátorský účet v prípadoch, kedy je možné využiť nepriviligovaný účet na vykonanie požadovaných úkonov.
- Servery by mali byť fyzicky lokalizované v kontrolovaných priestoroch.

Monitorovanie

- Všetky bezpečnostné udalosti na kritických systémoch musia byť zaznamenané a uložené za účelom budúceho auditu nasledujúcim spôsobom:
 - Všetky bezpečnostné záznamy musia byť dostupné on-line minimálne 1 týždeň.
 - Denné inkrementálne zálohy musia byť zachované minimálne 1 mesiac.
 - Kompletné týždenné zálohy musia byť zachované minimálne 1 mesiac.
 - Kompletné mesačné zálohy musia byť zachované minimálne 2 roky.
- Bezpečnostné udalosti musia byť vždy reportované tímu podnikovej bezpečnosti spoločnosti XXX.

Zhoda s ostatnými zásadami

- Pravidelné audity v spoločnosti XXX budú vykonané autorizovanou auditorskou spoločnosťou.
- Audity budú vykonané v súlade so Zásadami o auditoch.
- Bude vykonané maximálne úsilie, aby sa zabránilo tomu, aby audity spôsobili nemožnosť spoločnosti vykonávať svoj podnikateľský zámer.

Uskutočňovanie zásad

Ľubovoľný zamestnanec, ktorý bude pristihnutý pri porušovaní tu uvedených zásad, bude vystavený disciplinárnemu konaniu a v prípade závažného porušenia pracovnej disciplíny môže byť aj prepustený zo zamestnania.

Finančné náklady

Činnosť	Počet hodín	Hodinová mzda	Celkom
Tvorba bezpečnostných zásad pre zabezpečenie serverov	8	300 Kč	2 400 Kč

Tabuľka 3.14: Náklady na tvorbu bezpečnostných zásad pre zabezpečenie serverov

3.2.8 Audit komunikačných zariadení a serverov

Celkový prehľad

Tímu podnikovej bezpečnosti prideluje oprávnenie na vykonávanie bezpečnostného auditu nad ľubovoľným komunikačným zariadením, ktoré je vo vlastníctve spoločnosti alebo ktoré je v jej priestoroch nainštalované.

Účel dokumentu

Účelom týchto zásad je zaistiť, že všetky komunikačné zariadenia a servery nasaďené v spoločnosti XXX sú nakonfigurované podľa ostatných bezpečnostných zásad spoločnosti XXX. Komunikačné zariadenia a servery by mali byť podrobené auditu minimálne raz ročne.

Audity môžu byť vykonávané za účelom:

- zaistiť integritu, dôvernosť a dostupnosť informácií a zdrojov,
- zaistiť zhodu s ostatnými bezpečnostnými zásadami spoločnosti XXX.

Pôsobnosť dokumentu

Tieto zásady sa vzťahujú na všetky komunikačné zariadenia a servery vlastnené a spravované spoločnosťou XXX. Tieto zásady tiež zastrešujú komunikačné zariadenia a servery v priestoroch spoločnosti XXX, ale ktoré nie sú vlastníctvom spoločnosti XXX.

Všeobecné zásady

Spoločnosť XXX poskytuje svoj súhlas, ktorý umožňuje YYY prístup k svojim komunikačným zariadeniam a serverom, za účelom, aby spoločnosť ZZZ mohla vykonať pravidelný, resp. náhodný audit všetkých komunikačných zariadení a serverov spoločnosti XXX.

Pre servery, ktoré využíva spoločnosť XXX na podporu kritických obchodných činností a uloženie citlivých dát spoločnosti je obzvlášť dôležité, aby ich konfigurácia spĺňala ostatné bezpečnostné politiky spoločnosti XXX. Nevhodná konfigurácia môže viesť k strate dôvernosti, dostupnosti alebo integrity týchto systémov.

Postupy

Schválené a štandardizované konfiguračné šablóny by mali byť použité pri nasadzovaní komunikačných zariadení a serverov tak, aby zahrňovali:

- Všetky systémové záznamy musia byť posielané do centrálného systému.
- Všetky administrátorské úkony musia byť zaznamenané.
- Je požadované využívať centrálny systém nasadzovania záplat.
- Antivírusové riešenie musí byť nainštalované a aktualizované (v prípade serverov).
- Monitorovaním siete zistiť či sú otvorené len povolené porty.
- Kontrolovať členstvo v administrátorských skupinách.

Určenie zodpovedností

YYY môže vykonať audity všetkých serverov a komunikačných zariadení vlastných a spravovaných spoločnosťou XXX. Vlastník serverov a komunikačných zariadení je vyzývaný na to, aby takéto kontroly sám podľa potreby vykonával.

Relevantné zistenia

Všetky relevantné zistenia objavené ako výsledok auditu by mali byť sprístupnené v informačnom systéme spoločnosti alebo iným dohodnutým spôsobom, aby bola zaistená rýchla náprava zistených problémov, alebo aby boli vykonané potrebné kroky na zmiernenie negatívnej situácie.

Vlastníctvo správy o audite

Všetky výsledky a nájdenia vytvorené tímom spoločnosti ZZZ musia byť poskytnuté zodpovedným osobám spoločnosti XXX najneskôr týždeň od ukončenia auditu. Táto správa sa stane vlastníctvom spoločnosti XXX a musí spadať medzi dôverné informácie.

Uskutočňovanie zásad

YYY nesmie nikdy využiť prístupové údaje potrebné na vykonanie auditov na iné účely. Zamestnanec, ktorý bude pristihnutý pri porušovaní uvedených zásad, bude vystavený disciplinárnemu konaniu a v prípade závažného porušenia pracovnej disciplíny môže byť aj prepustený zo zamestnania.

Finančné náklady

Činnosť	Počet hodín	Hodinová mzda	Celkom
Tvorba bezpečnostných zásad pre audit	10	300 Kč	3 000 Kč

Tabuľka 3.15: Náklady na tvorbu bezpečnostných zásad pre audit

3.2.9 Plán zvládania katastrof

Celkový prehľad

Vzhľadom na to, že sa katastrofy stávajú len veľmi zriedka, management často ignoruje potrebu vytvoriť plán obnovy. Je dôležité si uvedomiť, že plán zvládania nepredvídaných udalostí dáva spoločnosti XXX konkurenčnú výhodu. Tieto zásady si vyžadujú finančnú podporu od managementu spoločnosti XXX a zároveň vyžadujú jeho aktívnu účasť pri tvorbe výsledného plánu. Katastrofy nie sú limitované len na počasie. Akákoľvek udalosť, ktorá môže predĺžiť dodanie služieb, by mala byť braná do úvahy.

Účel dokumentu

Tieto zásady definujú potrebu managementu podporovať prebiehajúce plánovanie zvládania katastrof v spoločnosti XXX.

Pôsobnosť dokumentu

Tieto zásady sa vzťahujú na management a na technických pracovníkov spoločnosti XXX.

Všeobecné zásady

Plán zvládania nepredvídaných udalostí

Musia byť vytvorené nasledujúce plány:

- **Havarijný plán:** Kto má byť kontaktovaný, kedy a ako? Aké okamžité kroky je potrebné vykonať, ak nastane istý typ udalosti.
- **Zástupný plán:** Popisuje prevzatie zodpovednosti v prípade, že zodpovední pracovníci nie sú dostupní, aby si plnili svoje povinnosti.
- **Štúdia dát:** Detailne popisuje dáta uložené v jednotlivých systémoch, ich kritickosť a dôvernosť.
- **Zoznam kritických služieb:** Zoznam všetkých využívaných služieb, zoradených podľa ich dôležitosti. Zároveň určuje poradie obnovy z krátkodobého a dlhodobého hľadiska.

- **Plán zálohy a obnovy:** Detailne určuje ktoré dáta majú byť zálohované, na aké médium a kde má byť dané médium uložené, zároveň určuje ako často má byť záloha vykonaná. Rovnako popisuje ako majú byť dáta následne obnovené.
- **Plán výmeny zariadení:** Popisuje aké zariadenia sú nevyhnutné na poskytovanie aktuálne ponúkaných služieb, určuje poradie v akom je potrebné ich opätovne zaviesť. Rovnako definuje kde majú byť jednotlivé zariadenia zakúpené.
- **Plán styku s médiami:** Kto je zodpovedný za podávanie informácií médiám. Informuje o tom, aké informácie je vhodné podávať verejnosti.

Plány musia byť overené

Po vytvorení plánov je potrebné otestovať ich účelnosť. Management by si mal vyhraďiť čas na otestovanie a implementáciu plánu zvládania katastrof. Počas testovania je možné odhaliť a odstrániť slabé miesta plánu, ktoré by mohli spôsobiť zlyhanie plánu.

Plány musia byť aktualizované

Plány by mali byť aktualizované každý rok tak, aby odzrkadľovali aktuálnu situáciu spoločnosti XXX.

Uskutočňovanie zásad

Ľubovoľný zamestnanec, ktorý bude pristihnutý pri porušovaní tu uvedených zásad, bude vystavený disciplinárnemu konaniu a v prípade závažného porušenia pracovnej disciplíny môže byť aj prepustený zo zamestnania.

Finančné náklady

Činnosť	Počet hodín	Hodinová mzda	Celkom
Tvorba plánu zvládania katastrof	16	300 Kč	4 800 Kč

Tabuľka 3.16: Náklady na tvorbu plánu zvládania katastrof

3.2.10 Celkové náklady sieťovej bezpečnostnej politiky

V rámci celkových nákladov sú opätovne uvedené všetky čiastkové sumy za jednotlivé zásady. Navyše sú zahrnuté aj náklady na kontrolu zásad ostatnými členmi Tímu pre kontrolu zásad zabezpečenia. V tejto fáze uvažujeme užívateľskú a právnu kontrolu.

Finančné náklady

Činnosť	Počet hodín	Hodinová mzda	Celkom
Tvorba bezpečnostných zásad prípustného užívania	24	300 Kč	7 200 Kč
Tvorba bezpečnostných zásad prípustného šifrovania	8	300 Kč	2 400 Kč
Tvorba pokynov pre antivírovú ochranu	4	300 Kč	1 200 Kč
Tvorba bezpečnostných zásad pre prácu s heslami	24	300 Kč	7 200 Kč
Tvorba bezpečnostných zásad pre komunikačné zariadenia	6	300 Kč	1 800 Kč
Tvorba bezpečnostných zásad pre zabezpečenie zariadení typu router a switch	6	300 Kč	1 800 Kč
Tvorba bezpečnostných zásad pre zabezpečenie serverov	8	300 Kč	2 400 Kč
Tvorba bezpečnostných zásad pre audit	10	300 Kč	3 000 Kč
Tvorba plánu zvládania katastrof	16	300 Kč	4 800 Kč
Užívateľská kontrola	8	300 Kč	2 400 Kč
Právna kontrola	24	600 Kč	14 400 Kč
Celkom	138		48 600 Kč

Tabuľka 3.17: Náklady na tvorbu bezpečnostných zásad (Zdroj: Interné firemné informácie)

3.3 Návrh zabezpečenia sieťovej infraštruktúry

Táto časť obsahuje návrh zvýšenia bezpečnosti sieťovej infraštruktúry analyzovanej spoločnosti. Ide o zvýšenie fyzickej bezpečnosti pomocou riešenia Panduit NISS (*Network Infrastructure Security Solution*). Teoretické základy tohto riešenia sú zhrnuté v teoretických východiskách práce. Zvýšenie bezpečnosti sieťovej infraštruktúry zníži riziká súvisiace s neautorizovaným prístupom. Návrh nasadenia riešenia Panduit NISS bude zadávateľovi tejto práce predložené v podobe písomného dokumentu s nasledujúcou štruktúrou.

- Zhrnutie pre vedúcich pracovníkov
- Riešenie návrhu
- Náklady na navrhované riešenie
- Prílohy

3.3.1 Zhrnutie pre vedúcich pracovníkov

V tomto krátkom úseku bude zhrnutý základný zámer spolupráce na úrovni tohto písomného dokumentu medzi zadávateľom a riešiteľom tejto práce.

Účel projektu

Účelom projektu je zvýšiť bezpečnosť sieťovej infraštruktúry súčasnej architektúry počítačovej siete spoločnosti.

Základná myšlienka implementácie

Základnou myšlienkou implementácie je nasadenie riešenia Panduit NISS (*Network Infrastructure Security Solution*), ktoré rieši sieťovú bezpečnosť na troch stupňoch (0, 1 a 2). So zvyšujúcim stupňom sa zvyšuje bezpečnosť. Navrhované riešenie vhodne kombinuje všetky tri stupne za účelom čo najrobustnejšieho návrhu pre spoločnosť.

Výhody predkladaného riešenia

Medzi výhody riešenia patria adekvátne vysoké náklady voči zvýšeniu bezpečnosti. Ďalšou výhodou je zvýšenie prehľadnosti a spoľahlivosti infraštruktúry na úrovni kabeláže. Zavedením sa spoločnosť zároveň priblíži k splneniu požiadaviek na udelenie ISO certifikátu z oblasti informačnej bezpečnosti, aj keď v súčasnosti neexistuje priame napojenie na ISO normy z oblasti bezpečnosti počítačových sietí, je vysoko pravdepodobné, že nová sada noriem ISO 27033 bude plne podporovať riešenie Panduit NISS pre zabezpečenie fyzickej vrstvy.

3.3.2 Požiadavky návrhu siete

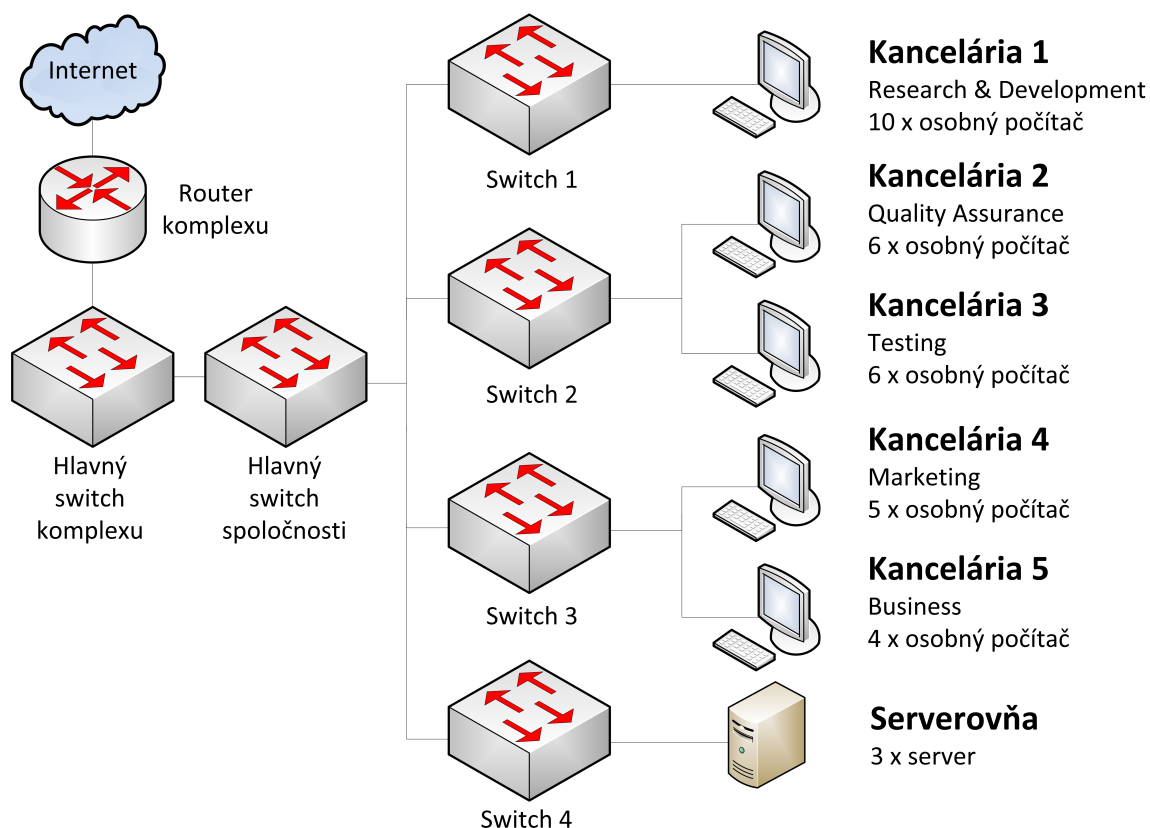
V tejto časti dokument uvedie do súvislosti súčasný a očakávaný budúci stav počítačovej siete zákazníka. Na základe tejto časti je možné návrh prijať, resp. dodatočne upraviť podľa bezpečnostných a finančných požiadaviek spoločnosti.

Charakteristika súčasnej siete

Súčasnú situáciu je možné opísať pomocou diagramu, ktorý zobrazuje sieťovú architektúru. Požadované riešenie nesiahá do vyšších vrstiev ISO/OSI modelu ako je vrstva prvá, preto nie je potrebné uvádzať ďalšie detaily.

Požiadavky zákazníka

Požiadavky zákazníka sú vo všeobecnosti zvýšiť zabezpečenie počítačovej siete. Z tohto pohľadu dôjde zároveň k sprehľadneniu kabeláže v jednotlivých kanceláriách a v ostatných priestoroch, ktoré si spoločnosť prenajíma za účelom vykonávania podnikateľskej činnosti.



Obr. 3.1: Sieťová architektúra spoločnosti

3.3.3 Riešenie návrhu siete

Návrh bude rozdelený podľa jednotlivých logických celkov ako je napojenie sa na sieť komplexu kancelárskych priestorov, prepojenie hlavného zariadenia typu switch a jednotlivých podporných zariadení typu switch, využitých za účelom hierarchickej architektúry počítačovej siete, ďalším logickým celkom sú kancelárie a ostatné prenajaté priestory zadávateľa.

Všetky kancelárie spoločnosti majú privedenú sieťovú kabeľnú pomocou žlabov do sieťových zásuviek. Z dôvodu snahy o zvýšenie bezpečnosti navrhujeme nahradiť existujúce zásuvky sieťovými zásuvkami s obmedzením prístupu a zaviesť kľúčovanú konektivitu do všetkých kancelárií spoločnosti. Prepojenie medzi sieťovými prvkami spoločnosti navrhujeme riešiť pomocou uzamykacích prvkov, aby sa zamedzilo neoprávnenému odpojeniu. Všetky nevyužité porty navrhujeme zablokovať modulom na blokovanie RJ-45.

Nasledujúca sada tabuliek zhrňa súčasný stav a navrhované riešenie pre jednotlivé kancelárie spoločnosti, serverovňu a ostatné spojenia sieťových prvkov. Ceny jednotlivých prvkov vychádzajú z cenníka uvedeného na stránke spoločnosti Cable-Organizer.com (14).

R&D - switch 1	Počet	
Porty	24	
Porty/kanc. R&D	22	
Vyvedené zásuvky	12	
Počítače	10	
Neobsadené zásuvky	2	
Porty prepojenia	2	
Počet prepojení	1	
Neobsadené porty prepojenia	1	
Riešenie NISS	Počet	Cena
Počet chránených zásuviek (PAN-UICFPRTR4IW)	3	183 Kč
Moduly na blokovanie RJ-45 (PAN-PSL-DJBC-RD) (10 ks)	1	508 Kč
Kľúčovaný UTP kábel (blue) (PAN-UTPKSP1MBU)	12	206 Kč
Kľúčovaný modul UTP (blue) (PAN-CJK688TGBU)	12	237 Kč
Celkom	6 373 Kč	

Tabuľka 3.18: Nasadenie NISS pre kanceláriu vývoja (Zdroj: Vytvorené pre potrebu práce)

QA & Testing - switch 2	Počet	
Porty	24	
Porty/kanc. QA	10	
Porty/kanc. Testing	10	
Vyvedené zásuvky / kanc. QA	8	
Vyvedené zásuvky / kanc. Testing	8	
Počítače / kanc. QA	6	
Počítače / kanc. Testing	6	
Neobsadené zásuvky / kanc. QA	2	
Neobsadené zásuvky / kanc. Testing	2	
Porty prepojenia	4	
Počet prepojení	1	
Neobsadené porty prepojenia	3	
Riešenie NISS	Počet	Cena
Počet chránených zásuviek (PAN-UICFPRTR4IW)	4	183 Kč
Moduly na blokovanie RJ-45 (PAN-PSL-DJBC-RD) (10 ks)	1	508 Kč
Kľúčovaný UTP kábel (green) (PAN-UTPKSP1MBU)	8	206 Kč
Kľúčovaný modul UTP (green) (PAN-CJK688TGBU)	8	237 Kč
Kľúčovaný UTP kábel (yellow) (PAN-UTPKSP1MBU)	8	206 Kč
Kľúčovaný modul UTP (yellow) (PAN-CJK688TGBU)	8	237 Kč
Celkom	8 328 Kč	

Tabuľka 3.19: Nasadenie NISS pre kancelárie Quality Assurance a Testing (Zdroj: Vytvorené pre potrebu práce)

Marketing & Business - switch 3	Počet	
Porty	24	
Porty/kanc. Marketing	10	
Porty/kanc. Business	10	
Vyvedené zásuvky / kanc. Marketing	8	
Vyvedené zásuvky / kanc. Business	8	
Počítače / kanc. Marketing	6	
Počítače / kanc. Business	6	
Neobsadené zásuvky / kanc. Marketing	2	
Neobsadené zásuvky / kanc. Business	2	
Porty prepojenia	4	
Počet prepojení	1	
Neobsadené porty prepojenia	3	
Riešenie NISS	Počet	Cena
Počet chránených zásuviek (PAN-UICFPRTR4IW)	4	183 Kč
Moduly na blokovanie RJ-45 (PAN-PSL-DJBC-RD) (10 ks)	1	508 Kč
Kľúčovaný UTP kábel (black) (PAN-UTPKSP1MBU)	8	206 Kč
Kľúčovaný modul UTP (black) (PAN-CJK688TGBU)	8	237 Kč
Kľúčovaný UTP kábel (orange) (PAN-UTPKSP1MBU)	8	206 Kč
Kľúčovaný modul UTP (orange) (PAN-CJK688TGBU)	8	237 Kč
Celkom		8 328 Kč

Tabuľka 3.20: Nasadenie NISS pre kancelárie Marketing a Business (Zdroj: Vytvorené pre potrebu práce)

Serverovňa - switch 4	Počet	
Porty	24	
Porty vyhradené pre servery	10	
Vyvedené zásuvky	4	
Servery	3	
Neobsadené zásuvky	1	
Porty prepojenia	2	
Počet prepojení	1	
Neobsadené porty prepojenia	1	
Riešenie NISS	Počet	Cena
Počet chránených zásuviek (PAN-UICFPRTR4IW)	1	183 Kč
Moduly na blokovanie RJ-45 (PAN-PSL-DJBC-RD) (10 ks)	2	508 Kč
Kľúčovaný UTP kábel (gray) (PAN-UTPKSP1MBU)	3	206 Kč
Kľúčovaný modul UTP (gray) (PAN-CJK688TGBU)	3	237 Kč
Celkom		2 528 Kč

Tabuľka 3.21: Nasadenie NISS pre serverovú miestnosť spoločnosti (Zdroj: Vytvorené pre potrebu práce)



Obr. 3.2: Modul na blokovanie RJ-45 (PAN-PSL-DJBC-RD) (Prevzaté z (14))



Obr. 3.3: Uzamykací prvok RJ-45 (red) (PAN-PSL-DCPL-C) (Prevzaté z (14))

Riešenie NISS pre ostatné prepojenia (switch)	Počet	Cena
Uzamykací prvok RJ-45 (red) (PAN-PSL-DCPL-C) (10 ks)	1	839 Kč
Moduly na blokovanie RJ-45 (PAN-PSL-DJBC-RD) (10 ks)	2	508 Kč
Celkom		1 855 Kč

Tabuľka 3.22: Nasadenie NISS pre ostatné sieťové spojenia (Zdroj: Vytvorené pre potrebu práce)

Na obrázkoch 3.2, 3.3, 3.4, 3.5 a 3.6 je možné vidieť jednotlivé prvky, ktoré sú použité v návrhu zmien.

3.3.4 Náklady

Celkové náklady na riešenie bezpečnosti sieťovej infraštruktúry sú 27 412 Kč. Navrhované zmeny odporúčame prijať aj napriek pomerne vysokým nákladom na tento typ bezpečnosti. Prínosy predstavujú hlavne zníženie rizík súvisiacich s neautorizovaným prístupom.



Obr. 3.4: Zásuvka s chráneným prístupom (PAN-UICFPRT4IW) (Prevzaté z (14))



Obr. 3.5: Klúčovaný UTP kábel (blue) (PAN-UTPKSP1MBU) (Prevzaté z (14))



Obr. 3.6: Klúčovaný modul UTP (blue) (PAN-CJK688TGBU) (Prevzaté z (14))

Zhodnotenie a záver

Táto diplomová práca predstavila možnosti riadenia informačnej bezpečnosti v súlade s normou ISO/IEC 27001 so špeciálnym vymedzením na sieťovú bezpečnosť podľa ISO/IEC 18028 (ISO/IEC 27033 ešte nie je v dobe písania diplomovej práce kompletne v platnosti). Všetky bezpečnostné riešenia práce sú úzko špecializované na oblasť počítačových sietí, čo umožnilo detailné riešenie bezpečnostných aspektov. Práca v úvode definuje proces nasadzovania ISMS, spôsoby analýzy rizík a smeruje postupne k tvorbe bezpečnostnej politiky so zameraním na siete. Uvádza spôsoby prístupu k bezpečnosti počítačových sietí a na základne všetkých teoretických poznatkov navrhuje výslednú podobu bezpečnostnej politiky pozostávajúcej z bezpečnostných zásad. Táto politika vychádza z analýzy súčasného stavu spoločnosti a zároveň spĺňa požiadavky zadávateľa na zvýšenie bezpečnosti firemnej počítačovej siete.

Výsledkom práce je teda sieťová bezpečnostná politika s komplexným záberom. Aplikovaním definovaných bezpečnostných zásad spoločnosť pokryje riziká súvisiace s aktivitami identifikovanými v počítačovej sieti, čo predstavuje pre spoločnosť veľký prínos. Ďalším prínosom diplomovej práce je to, že zásady zabezpečenia predstavujú pre firmu prostriedok na vymáhanie zodpovednosti v prípade nevhodného správania sa zamestnancov na pracovisku (z hľadiska informačnej bezpečnosti spoločnosti).

Ďalej bol vytvorený návrh zabezpečenia sieťovej infraštruktúry pomocou technológie NISS (*Network Infrastructure Security Solution*) spoločnosti Panduit. V súčasnosti neexistujú návody ani pokyny ako správne nasadiť uvedené riešenie v súlade s normou ISO/IEC 27001. V tejto práci je riešená bezpečnosť sieťovej infraštruktúry za účelom zníženie dopadu identifikovaných rizík.

Príprava sieťovej bezpečnostnej politiky bola ohodnotená na 48 600 Kč (celková suma odzrkadľuje potrebu účasti viacerých pracovníkov spoločnosti). Náklady na zvýšenie bezpečnosti sieťovej infraštruktúry boli vyčíslené na 27 412 Kč. V oboch prípadoch ide o adekvátne náklady vzhľadom na získané zvýšenie bezpečnosti.

Literatúra

- (1) TeamViewer GmbH. *TeamViewer Security Information*. [online]. 2012. [cit. 2013-05-20]. Dostupné z: http://www.teamviewer.com/images/pdf/TeamViewer_SecurityStatement.pdf.
- (2) DOUCEK, P., NOVÁK, L., SVATÁ, V. *Řízení bezpečnosti informací*. 1. vyd. Praha: Professional Publishing, 2008, 239 s. ISBN 978-80-86946-88-7.
- (3) ČESKÝ NORMALIZAČNÍ INSTITUT. ČSN ISO/IEC 17799. *Informační technologie - Bezpečnostní techniky - Soubor postupů pro management bezpečnosti informací*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2006. 94 s. Třídící znak 36 9790.
- (4) ČESKÝ NORMALIZAČNÍ INSTITUT. ČSN ISO/IEC 27000:2009. *Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Přehled a slovník*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2010. 24 s. Třídící znak 36 9790.
- (5) ČESKÝ NORMALIZAČNÍ INSTITUT. ČSN ISO/IEC 27001:2006. *Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2006. 35 s. Třídící znak 36 9790.
- (6) IsecT. *ISO/IEC 27033*. [online]. 2013. [cit. 2013-04-20]. Dostupné z: <http://www.iso27001security.com/html/27033.html>.
- (7) International Organization for Standardization. ISO/IEC 18028-1:2006. *Information technology - security techniques - IT network security - part 1: Network security management*. ISO, 2006. 66 s.
- (8) International Organization for Standardization. ISO/IEC 18028-1:2006. *Information technology - Security techniques - IT network security - part 2: Network security architecture*. ISO, 2006. 27 s.
- (9) SMEJKAL, V. a RAIS, K. *Řízení rizik ve firmách a jiných organizacích*. 3., rozš. a aktualiz. vyd. Praha: Grada, 2010, 354 s. Expert (Grada). ISBN 978-80-247-3051-6.
- (10) THOMAS, T. *Zabezpečení počítačových sítí bez předchozích znalostí*. 1. vyd. Brno: CP Books, a.s., 2005, 338 s. ISBN 80-251-0417-6.

- (11) SANS. *Information Security Policy Templates*. [online]. 2013. [cit. 2013-05-07]. Dostupné z: <<http://www.sans.org/security-resources/policies/>>.
- (12) Singapore IT Security Techno Portal. *How to develop a Network Security Policy*. [online]. 2002. [cit. 2013-05-02]. Dostupné z: <http://www.windowsecurity.com/whitepapers/policy_and_standards/How_to_develop_a_Network_Security_Policy_.html>.
- (13) PANDUIT. *Network Infrastructure Security Solution*. [online]. 2012. [cit. 2013-03-29]. Dostupné z: <http://www.panduit.com/ccurl/214/313/InfrastructureSecurity_BR_SA-CPCB83_ENG.pdf>.
- (14) CableOrganizer.com. *Panduit Products*. [online]. 2013. [cit. 2013-05-19]. Dostupné z: <<http://www.cableorganizer.com/panduit/>>.

Zoznam skratiek

CRM	<i>Customer Relationship Management</i> (Riadenie vzťahov so zákazníkmi)
DNS	<i>Domain Name System</i> (Hierarchický systém doménových mien)
FTP	File Transfer Protocol (Protokol na prenos súborov)
IEC	International Electrotechnical Commission (Medzinárodný úrad pre elektrotechniku)
IMS	Integrated Management System (Integrovaný systém riadenia)
IP	Internet Protocol (Základný internetový protokol)
ISMS	Information Security Management System (Systém riadenia bezpečnosti informácií)
ISO	International Organization for Standardization (Medzinárodná organizácia pre štandardizáciu)
LAN	Local Area Network (Lokálna sieť)
MD5	Message-Digest Algorithm (Rodina hašovacích funkcií)
NAT	Network Address Translation (Preklad sieťových adries)
NISS	Network Infrastructure Security Solution (Bezpečnostné riešenie sieťovej infraštruktúry)
PDCA	Plan-Do-Check-Act (Demingov cyklus)
PSTN	Public Switched Telephone Network (Verejná telefónna sieť)
QoS	Quality of Service (Kvalita služieb)
SHA	Secure Hash Algorithm (Rozšírená hašovacia funkcia)
SQL	Structured Query Language (Štruktúrovaný dotazovací jazyk)
SS7	Signalling System 7 (Sada signalizačných protokolov)
SSH	Secure Shell (Zabezpečený komunikačný protokol)
TACACS+	Terminal Access Controller Access-Control System Plus (Protokol riadenia prístupu)
TCP	Transmission Control Protocol (Spoľahlivý protokol prenosu dát)
TFS	Team Foundation Server (Riešenie od spoločnosti Microsoft na podporu vývoja)
UDP	User Data Protocol (Nespoľahlivý protokol prenosu dát)
VLAN	Virtual LAN (Virtuálna LAN)
VPN	Virtual Private Network (Virtuálna privátna sieť)
WWW	World Wide Web (Celosvetová komunikačná sieť)

Zoznam obrázkov

1.1	Sieťová architektúra spoločnosti (Zdroj: Vlastná analýza)	11
2.1	Model PDCA použitý na riadenie bezpečnosti informácií (Prevzaté z (2))	14
2.2	Koncept rady ISO/IEC 27000 pre riadenia bezpečnosti informácií (Prevzaté z (2))	26
2.3	Vzťahy v analýze rizík (Prevzaté z (9))	31
2.4	Vzťahy pri riadení rizík (Prevzaté z (9))	32
2.5	Referenčná architektúra (Prevzaté z (8))	42
3.1	Sieťová architektúra spoločnosti	68
3.2	Modul na blokovanie RJ-45 (PAN-PSL-DJBC-RD) (Prevzaté z (14))	71
3.3	Uzamykací prvok RJ-45 (red) (PAN-PSL-DCPL-C) (Prevzaté z (14))	71
3.4	Zásuvka s chráneným prístupom (PAN-UICFPRTR4IW) (Prevzaté z (14))	72
3.5	Kľúčovaný UTP kábel (blue) (PAN-UTPKSP1MBU) (Prevzaté z (14))	72
3.6	Kľúčovaný modul UTP (blue) (PAN-CJK688TGBU) (Prevzaté z (14))	72

Zoznam tabuliek

3.1	Schéma hodnotenia dopadu (Zdroj: Vytvorené pre potreby práce)	44
3.2	Aktíva spoločnosti (Zdroj: Vytvorené pre potreby práce)	45
3.3	Hodnoty pravdepodobnosti úrovne hrozby (Prevzaté z (9))	45
3.4	Pravdepodobnosť výskytu hrozieb (Zdroj: Vytvorené pre potreby práce)	46
3.5	Súčtová matica rizík (Prevzaté z (9))	46
3.6	Súčtová matica rizík (Zdroj: Vytvorené pre potreby práce)	47
3.7	Členovia tímu pre kontrolu zásad zabezpečenia (Zdroj: Vytvorené pre potreby práce)	48
3.8	Náklady na tvorbu bezpečnostných zásad prípustného užívania	53
3.9	Náklady na tvorbu bezpečnostných zásad prípustného šifrovania	54
3.10	Náklady na tvorbu pokynov pre antivírusovú ochranu	54
3.11	Náklady na tvorbu bezpečnostných zásad pre prácu s heslami	57
3.12	Náklady na tvorbu bezpečnostných zásad pre komunikačné zariadenia	59
3.13	Náklady na tvorbu bezpečnostných zásad pre zabezpečenie zariadení typu router a switch	60
3.14	Náklady na tvorbu bezpečnostných zásad pre zabezpečenie serverov	62
3.15	Náklady na tvorbu bezpečnostných zásad pre audit	64
3.16	Náklady na tvorbu plánu zvládania katastrof	65
3.17	Náklady na tvorbu bezpečnostných zásad (Zdroj: Interné firemné informácie)	66
3.18	Nasadenie NISS pre kanceláriu vývoja (Zdroj: Vytvorené pre potrebu práce)	69
3.19	Nasadenie NISS pre kancelárie Quality Assurance a Testing (Zdroj: Vytvorené pre potrebu práce)	69
3.20	Nasadenie NISS pre kancelárie Marketing a Business (Zdroj: Vytvorené pre potrebu práce)	70
3.21	Nasadenie NISS pre serverovú miestnosť spoločnosti (Zdroj: Vytvorené pre potrebu práce)	70
3.22	Nasadenie NISS pre ostatné sieťové spojenia (Zdroj: Vytvorené pre potrebu práce)	71