Řízení vybraných bezpečnostních rizik v podnikových informačních systémech

Bc. Aleš Bednář

Diplomová práce
2006

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav aplikované informatiky
akademický rok: 2005/2006

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Aleš BEDNÁŘ**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Informační technologie**
Téma práce:	**Řízení vybraných bezpečnostních rizik v podnikových informačních systémech.**

Zásady pro vypracování:

1) s využitím dostupných informačních zdrojů proveďte analýzu současné situace z pohledu řešeného problému
2) vypracujte návrh řízení vybraných bezpečnostních rizik v podnikových informačních systémech
3) navrhněte vhodnou implementaci řízení vybraných bezpečnostních rizik
4) aplikujte (pokuste se o aplikaci) do reálné praxe
5) proveďte vyhodnocení

Rozsah práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná**

Seznam odborné literatury:

1) Bezpečnost informačních systémů, Petr Hanáček, Jan Staudek, 2000
2) Příručka o ochraně dat pro veřejnou správu, 2005
3) Závislost prosperity firmy na bezpečnosti informací, Roman Jašek, 2005
4) Průvodce zabezpečením pro malé organizace, Donald Wilson, 2004
5) Moderní počítačové viry, Igor Hák, 2005

Vedoucí diplomové práce: **Mgr. Roman Jašek, Ph.D.**
Ústav informatiky a statistiky

Datum zadání diplomové práce: **14. února 2006**

Termín odevzdání diplomové práce: **26. května 2006**

Ve Zlíně dne 14. února 2006

prof. Ing. Vladimír Vašek, CSc.
pověřený děkan

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
①

doc. Ing. Ivan Zelinka, Ph.D.
ředitel ústavu

ABSTRAKT

Cílem této práce, která má název Řízení vybraných bezpečnostních rizik v podnikových informačních systémech, je vytvoření postupů při řízení bezpečnosti IS a zavádění řízení bezpečnosti informačních systémů uvnitř organizace.

Teoretická část seznámí čtenáře s danou problematikou a definicemi základních pojmů z oblasti bezpečnosti a ochrany dat. Praktická část definuje jednotlivé problémy a obsahuje postupy a doporučení pro řízenou bezpečnost informačního systému a informačních technologií ve firmách a institucích. V závěrečné části je vypracována případová studie, prakticky ukazuje teoretické poznatky a navazuje na předchozí částech práce.

Klíčová slova: informační systémy, IS, bezpečnost IS, řízení bezpečnosti, informační bezpečnost, podniková bezpečnost, bezpečnostní rizika

ABSTRACT

The purpose of this work with name Managing of exquisite security risks in business information systems is to create procedures for IS security management and for implementation of IS security management in the organization.

Theoretical part informs the reader with given problems and with definitions of basics terms from area data security and data protection. Practical part defines several problems and contains procedures and advices for IS and IT security management in companies and institutions. In the closing part there is case study practically showing theoretical knowledge and concurring on previous parts of the work.

Keywords: information systems, IS/IT security , security managing, information security, business security, security risks

Na tomto místě bych rád poděkoval Mgr. Romanu Jaškovi, Ph.D. za cenné rady a připomínky, kterými přispěl ke zdárnému završení této práce.

OBSAH

ÚVOD

V době, která je v celém světe charakterizována jako „věk informace“, jsou informace důležitým předpokladem pro získání konkurenční výhody firmy a tím zajištění vysoké prosperity instituce. Proto se do popředí dostává informační systém. Jeho kvalita může být posuzována z různých hledisek. Jedním z nejdůležitějších je hledisko zabezpečení informačního systému a všech jeho informací, neboť jakákoliv bezpečností hrozba se může negativně odrazit na celkové provozuschopnosti systému podniku a způsobit nevyčíslitelné škody, které mohou vést až k bankrotu společnosti. Nepřetržitý vývoj informačních technologií, stále rostoucí množství informací z interních i externích zdrojů, které je potřebné zpracovávat, a tím i rostoucí složitost informačních systémů způsobily, že se vybudování kvalitní řízené bezpečnosti informačního systému stalo pro vedení firem nelehkým úkolem. Všechny tyto technologie však mohou přinášet očekávaný efekt pouze tehdy, jsou-li vytvořeny podmínky pro jejich účinné zavedení a využívání, a to nejen technologické, ale hlavně personální.

Za cíl mé práce, která má název Řízení vybraných bezpečnostních rizik v podnikových informačních systémech, považuji vytvoření postupů řízení bezpečnosti podnikových systémů v organizaci. Dále chci navrhnout postupy pro řízení bezpečnosti informačních systémů z pohledu budoucích uživatelů a ostatních pracovníků ve firmách a institucích, které se rozhodly řídit vnitřní bezpečnost informačních systémů. Tyto postupy lze obzvláště doporučit v podmínkách České republiky, kde je zkušenost s provozováním informačních technologií v tržním prostředí relativně krátkodobá a proto není tento trh zcela obsazen jako v zahraničí.

Práci jsem rozdělil do čtyř částí, které na sebe tématicky navazují a tvoří ucelený soubor kroků, pomocí kterých je možné efektivně řídit bezpečnost informačních systémů uvnitř organizací. Je nutné poznamenat, že není možné jednotlivé oblasti přeskočit či přeskládat. Teoretická část je věnována především vymezení dané problematiky a definici základních pojmů z oblasti bezpečnosti a ochrany dat. Dále v této části najdeme odpovědi na otázky a důvody řízení bezpečnosti v podnikových informačních systémech. Vzhledem k navazujícím částem mé diplomové práce v teoretické dále uvádím i jednotlivé kroky při implementaci řízení bezpečnosti informačních systémů v podnicích či institucích.

Praktická část definuje jednotlivé problémy a obsahuje postupy a doporučení pro řízenou bezpečnost informačního systému a informačních technologií ve firmách a institucích. Většina prezentovaných problémů se týká zabezpečení dat a informací. Postupy jsou úzce spojeny s organizací práce a pracovními postupy jak pro vedoucí pracovníky podílející se na řízení bezpečnosti tak i pro řadové zaměstnance. Závěrečnou část bychom mohli nazvat projektem či případovou studií, která nese název Řízení bezpečnostních rizik v podnikovém informačním systému. Prakticky na ní ukazuji teoretické poznatky, které jsem uvedl v předchozích částech mé práce.

Ve své diplomové práci nechci jen opisovat knihy, ale jde mi o to ukázat problematiku zabezpečování dat z pohledu problémů, ke kterým může docházet při implementaci do podnikových struktur organizací.

I. TEORETICKÁ ČÁST

1 ÚVOD DO INFORMAČNÍ BEZPEČNOSTI

Dnes je pojem systém užíván jako označení určité části reálného světa s charakteristickými vlastnosti. Takto nazírané systémy se dělí na systémy přirozené, kdy hlavní části systému nejsou vytvořeny člověkem a existují nezávisle na něm, a na systémy umělé, vytvořené člověkem. Z tohoto pohledu je informační systém umělým a člověk může výrazně ovlivňovat jeho kvalitu.

Existuje celá řada definic IS[1]. Z obsahově podobných definic informačního systému je nejvýstižnější: „Informační systém lze definovat jako soubor lidí, metoda a technických prostředků zajištujících sběr, přenos, uchování a zpracování dat s cílem tvorby a poskytování informací dle potřeb příjemců informací činných v systémech řízení“

Zahrnuje člověka jako součást informačního systému a zmiňuje se o míře potřeby příjemců informací. V současné době lze tuto definici doplnit: „Informační systém lze definovat jako soubor lidí, metod a technických prostředků zajišťujících sběr, přenos, uchovávání, zpracování a prezentaci dat s cílem tvorby a poskytování informací dle potřeb příjemců informací činných v systémech řízení.“

Další definice popisuje informační systém z jiného pohledu a zní: „Informační systém je obecně podpůrný systém pro systém řízení. Jestliže chceme projektovat systém řízení jako takový, musíme znát, jaké jsou cíle, a informační systém řešit tak, aby tyto cíle podporoval.“

Jedno mají uvedené definice společné – shodují se v tom, že informační systém je účelnou formou využití informačních technologií v sociálně-ekonomických systémech.

Informační systém se skládá z následujících komponent:

- technické prostředky – počítačové systémy různého druhu a velikosti, doplněné o potřebné periferní jednotky, které jsou v případě potřeby propojeny prostřednictvím počítačové sítě a napojeny na diskový subsystém pro práci s velkými objemy dat,

[1] IS – Informační systém

- programové prostředky – tvořené systémovými programy řídící chod počítače, efektivní práci s daty a komunikaci počítačového systému s reálným světem a programy aplikačními řešícími určité třídy úloh určitých tříd uživatelů,
- organizační prostředky – tvořené souborem nařízení a pravidel definujících provozování a využívání informačního systému a informačních technologií,
- lidská složka – řešení otázky adaptace a účinného fungování člověka v počítačovém prostředí, do kterého je vřazen,
- reálný svět – kontext informačního systému např. informační zdroje, normy, legislativa.

Má-li být informační systém firmy či instituce efektivní, nesmí být pří jeho vývoji zanedbaná žádná z jeho složek a to ani složka týkající se bezpečnosti takovéhoto systému. Při úvahách o míře aplikování zabezpečení systému je potřebné uvažovat také o velikosti konkrétní firmy či instituce, jež může být charakterizována kterýkoli z následujících ukazatelů:

- počet zaměstnanců,
- objem výroby, objem prodeje či poskytování služeb,
- velikostí trhu, resp. počtem zákazníků.

Reálný svět	Uživatel	Informační technologie
Informační zdroje, legislativa, normy	Organizační prostředky a lidská složka	Hardware, software
Informační systém		

Informační technologie zpracovávají stále více a více informací s velkou hodnotou. Pokud hovoříme v souvislosti s informačními technologiemi o zpracovávání informací, pak tím rozumíme použití těchto technologií k uchovávání, přenosu, vyhodnocování a prezentaci informací. Mnohdy se jedná o informace s nezanedbatelnou hodnotou (např. zdravotní záznamy, daňová přiznání, bankovní účty, elektronické platební nástroje, výsledky vývoje nebo výzkumu, obchodní záměry), musí být chráněny tak, aby byly splněny následující základní body:

- aby k nim měly přístup pouze oprávněné osoby,

- aby se zpracovávaly nefalšované informace,
- aby se dalo zjistit, kdo je vytvořil, změnil nebo odstranil,
- aby nebyly nekontrolovaným způsobem vyzrazeny,
- aby byly dostupné tehdy, když jsou potřebné.

1.1 Výklad základních pojmů z oblasti bezpečnosti IS

Základní pojmy, vymezující oblast bezpečnosti IS, je možné vysvětlit na následujícím modelu, který je tvořen ze čtyř následujících složek:

- hardware – procesor, paměti, terminály, telekomunikace atd.,
- software – aplikační programy, operační systém atd.,
- data – data uložená v databázi, výsledky, výstupní sestavy, vstupní data atd.,
- lidé – uživatelé, personál, osoby vstupující do informačního systému atd.

Způsob dosažení bezpečnosti a bezpečnostní vlastnosti určuje bezpečnostní politika. Pojmem bezpečnostní politika IS označujeme souhrn norem, pravidel a praktik, definující způsob správy, ochrany a distribuce citlivých dat a jiných aktiv v rámci činnosti IS. Citlivá data mají pro chod organizace zásadní význam, jejich kompromitací nebo zneužitím by vznikla organizaci škoda, případně by organizace nemohla řádně plnit svoje poslání. Bez explicitní definice a ohodnocení aktiv nelze implementovat a udržovat žádný bezpečnostní program. Je třeba si uvědomit, že každý IS je zranitelný, bezpečnostní politika IS pouze snižuje pravděpodobnost úspěchu útoku proti IS nebo nutí útočníka vynakládat více peněz nebo času. Absolutně bezpečný systém však neexistuje.

1.2 Zranitelné místo, hrozba, riziko, útok, útočník

1.2.1 Zranitelné místo

Slabina IS využitelná ke způsobení škod nebo ztrát útokem na IS se označuje jako zranitelné místo. Existence zranitelných míst je důsledek chyb, selhání v analýze, v návrhu nebo v implementaci IS, důsledek vysoké hustoty uložených informací, složitosti softwaru, existence skrytých kanálů pro přenos informace jinou než zamýšlenou cestou apod.Podstata zranitelného místa může být:

- fyzická - např. umístění IS v místě, které je snadno dostupné sabotáži nebo vandalismu, výpadek napětí,
- přírodní - objektivní faktory typu záplava, požár, zemětřesení, blesk
- hardwarová nebo softwarová,
- fyzikální - vyzařování, útoky při komunikaci na výměnu zprávy, na spoje
- lidský faktor - největší zranitelnost ze všech možných variant.

Zranitelná místa vznikají jako důsledek selhání nebo zanedbání při následujících činnostech :

- v návrhu informačního systému,
- ve specifikaci požadavků - IS může plnit všechny funkce a vykazovat všechny bezpečnostní rysy po něm požadované a přesto stále ještě obsahuje zranitelná místa, která ho činí z hlediska bezpečnosti nevhodným nebo neúčinným,
- v řešení (projektu),
- v konstrukci - IS nesplňuje svoje specifikace nebo byla do něj zavlečena zranitelná místa v důsledku špatných konstrukčních standardů nebo nesprávných rozhodnutí,
- při návrhu či implementaci,
- v provozu - IS byl sice správně zkonstruován podle správných specifikací, ale zranitelná místa do něj byla zavlečena v důsledku použití neadekvátních provozních řídicích nástrojů.

1.2.2 Hrozba

Charakteristikou hrozby je její zdroj (např. vnější nebo vnitřní), motivace potenciálního útočníka (finanční zisk, získání konkurenční převahy), frekvence a kritičnost uplatnění hrozby. Zranitelná místa jsou vlastnostmi (součástmi) informačního systému, jejichž existence způsobuje, že některé vlivy prostředí, ve kterém se informační systém provozuje, představují pro něj hrozby. Pojmem hrozba označuje možnost využitkovat zranitelné místo IS k útoku na způsobení škody na aktivech. Hrozby lze kategorizovat na objektivní nebo na subjektivní. Do kategorie objektivních hrozeb je možné zařadit nepředvídatelné události týkající se například přírodních katastrof a s nimi souvisejícím fyzickým poškozením např.

požár, povodeň, výpadek napětí, poruchy atd., u kterých je prevence obtížná a u kterých je třeba řešit spíše minimalizaci dopadů vhodným plánem obnovy. Subjektivní hrozby jsou především hrozby plynoucí z lidského faktoru. Základní další dělení může být například na kategorii neúmyslných, např. působení neškoleného uživatele/správce, a na kategorii úmyslných, kam spadají především představované potenciální existencí vnějších útočníků (špioni, teroristi, kriminální živly, konkurenti, hackeři) i vnitřních útočníků (odhaduje se, že 80 % útoků na IS je vedeno zevnitř nebo také útočníkem, kterým může být propuštěný, rozzlobený, vydíraný nebo chamtivý zaměstnanec).

Dalším typem hrozeb je neautorizované použití zdrojů (krádeže hardwarových a softwarových komponent, včetně používání jejich neoprávněných kopií), neautorizované používání informačních systémů a služeb jimi poskytovaných, znepřístupnění služeb, tj. akce a události, které brání autorizovaným subjektům využívat systém IT[2] na dohodnuté úrovni poskytovaných služeb, popírání odpovědnosti za akce citlivé z hlediska bezpečnosti, např. popírání aktu zaslání nebo přijetí zprávy, popírání autorství dané zprávy atd.

1.2.3 Útok

Útokem, který nazýváme rovněž bezpečnostní incident, rozumíme buďto úmyslné využitkování zranitelného místa, tj. využití zranitelného místa ke způsobení škod/ztrát na aktivech IS, nebo neúmyslné uskutečnění akce, jejímž výsledkem je škoda na aktivech. Při analýze možných forem útoků na IT je třeba typicky řešit problémy typu: jak se projevuje počítačová kriminalita, jaké jsou možné formy útoků, kdo útočí, kdo může páchat počítačový zločin, jaká rizika souvisí s používáním informačních technologií, jak se chránit před útoky apod. Následně řešenými problémy jsou pak rozhodnutí typu: jak detekovat útok, jak zjistit bezpečnostní incident, jak reagovat na útok, co dělat, když dojde k bezpečnostnímu incidentu. Útočit lze:

- přerušením - aktivní útok na dostupnost, např. ztráta, znepřístupnění, poškození aktiva, porucha periférie, vymazání programu, vymazání dat, porucha v operačním systému,

[2] IT – Informační technologie

- odposlechem - pasivní útok na důvěrnost, kdy neautorizovaný subjekt si neoprávněně zpřístupní aktiva, jde např. o okopírování programu nebo o okopírování dat,
- změnou - aktivní útok na integritu, neautorizovaný subjekt zasáhne do aktiva, provede se např. změna uložených a/nebo přenášených dat, přidání funkce do programu,
- přidáním hodnoty - aktivní útok na integritu nebo útok na autenticitu, tj. o případ, kdy neautorizovaná strana něco vytvoří (podvržení transakce, dodání falešných dat).

Vhodnou formou ochrany před pasivními útoky odposlechem je prevence, poněvadž detekce odposlechu je velmi obtížná. Absolutní prevence útoků ovšem zajistitelná není, proto typická ochrana (hlavně před aktivními formami útoků) je založena na detekci útoků a na následné obnově činnosti. Velmi důležité je vzít si poučení ze zjištěných skutečností a získané zkušenosti uplatnit při vylepšování ochran, ať již preventivních, nebo detekčních či aktivních, heuristických (založených na určitých hypotézách). Útok může být úmyslný nebo neúmyslný, resp. náhodný.

1.2.4 Útočník

Důležité je si uvědomit, kdo může útočit. Útočník může být vnější, ale v organizaci se často vyskytuje i vnitřní útočník. Podle znalosti a vybavenosti rozeznáváme:

- útočníky slabé síly - amatéři, náhodní útočníci, využívající náhodně objevená zranitelná místa při běžné práci; jedná se o náhodné, často neúmyslné útoky, útočníci mají omezené znalosti, příležitosti i prostředky, pro ochranu před nimi stačí přijmout relativně slabá bezpečnostní opatření, která jsou levná,
- útočníky střední síly - hackeři, jejichž častým krédem je dostat se k tomu, k čemu nejsou autorizovaní; jedná se o běžné útoky, útočníci mají mnohdy hodně znalostí, obvykle ale nemají zjevné příležitosti k útokům a mívají omezené prostředky; jako ochrana proti nim se přijímají bezpečnostní opatření střední síly,
- útočníky velké síly - profesionální zločinci, kteří mají původ obvykle mezi počítačovými profesionály, je pro ně typická vysoká úroveň znalostí, mají obvykle dostatek prostředků (peněz) a mnohdy i dost času k provedení útoku, provádějí útoky vymykající se běžné praxi, pro ochranu před nimi je nutno přijímat silná bezpečnostní opatření.

1.2.5 Riziko

Existence hrozby představuje riziko. Rizikem rozumíme pravděpodobnost využitkování zranitelného místa IS. Říkáme, že se hrozba uplatní s takovou a takovou pravděpodobností. Rizika lze charakterizovat vedle pravděpodobnosti výskytu bezpečnostního incidentu i potenciálně způsobenou škodou.

1.3 Bezpečnost IT

Pod pojmem bezpečnost IT obvykle rozumíme ochranu odpovídajících IS a informací, které jsou v nich uchovávány, zpracovávány a přenášeny. Součástí takto obecně chápané bezpečnosti IT je i komunikační bezpečnost, tj. ochrana informace přenášené mezi počítači, fyzická bezpečnost, tj. ochrana před přírodními hrozbami a fyzickými útočníky a personální bezpečnost, tj. ochrana před vnitřními útočníky. Pojem bezpečnost IT v sobě tedy zahrnuje i takové pojmy, jakými jsou bezpečnost informačních systémů, ochrana informačních systémů, bezpečnost informací, ochrana informací, ochrana informačních technologií, počítačová bezpečnost, telekomunikační bezpečnost a ochrana informačních technologií. Všechny uvedené pojmy mají jistě svůj nezanedbatelný význam při popisu a diskusi bezpečnosti a ochrany počítačových a telekomunikačních systémů a informací uložených, zpracovávaných a přenášených v takových systémech.

Pojem bezpečnost IT ale budeme používat jako obecný pojem, který může reprezentovat kterýkoli z ostatních uvedených pojmů. Mezinárodní normalizační organizace ISO ve svých normách definuje bezpečnost jako zajištěnost proti nebezpečím, minimalizaci rizik a jako komplex administrativních, logických, technických a fyzických opatření pro prevenci, detekci a opravu nesprávného použití IS. Bezpečný IS je takový IS, který je zajištěn fyzicky, administrativně, logicky i technicky. IS je třeba zabezpečovat, protože se jedná o ochranu investic, neboť informace je zboží, nutí k tomu právní nebo morální pravidla, činnost konkurence a zákonné úpravy pro ochranu dat.

V soudobém chápání bezpečnosti IT je bezpečnost dána zajištěním:

- důvěrnosti - k aktivům (k údajům) mají přístup pouze autorizované subjekty,
- integrity a autenticity - aktiva (data, software, hardware) smí modifikovat jen autorizované subjekty a původ informací je ověřitelný,

- dostupnosti - aktiva (data nebo služby) jsou autorizovaným subjektům do určité doby dostupná, nedojde tedy k odmítnutí služby, kdy subjekt nedostane to na co má právo.

K těmto dnes již klasickým hlediskům bezpečnosti se v současnosti nedělitelně druží hlediska prokazatelnosti odpovědnosti, nepopiratelnosti odpovědnosti a spolehlivosti. Pokud budeme posuzovat útoky z hlediska takto definované bezpečnosti, rozpoznáváme útok na důvěrnost (analýza odpadu, elektromagnetické vyzařování, odposlech komunikací, analýza toku zpráv, kopírování pamětí, agregace, dedukce), útok na integritu a autenticitu (modifikace softwaru na škodlivý software, viry, trojské koně, zadní vrátka, logické bomby, použití neodsouhlaseného hardwaru, obcházení bezpečnostních opatření, narušení transakcí, změna uložených dat, změna dat při jejich přenosu, vkládání falešných zpráv, replikace zpráv), útok na dostupnost (např. znemožněním poskytnutí služby zahlcením, výpadkem energie), útok na nepopiratelnost odpovědnosti a útok na spolehlivost.

1.3.1 Bezpečnostní funkce a mechanismy

Zabezpečujeme-li IS, je třeba nejprve stanovit bezpečnostní cíle a způsob jejich dosažení. Bezpečnostní cíle jsou dílčí přínosy k bezpečnosti, kterou dosahuje IS z hlediska udržení důvěrnosti, integrity a dostupnosti. Pro jejich dosažení se aplikuje používání funkcí prosazujících bezpečnost, nazývaných rovněž bezpečnostní funkce nebo bezpečnostní opatření. Bezpečnostní funkce přispívá buďto ke splnění jednoho bezpečnostního cíle, nebo ke splnění několika bezpečnostních cílů. Abychom mohli bezpečnostní cíle stanovit, je potřeba znát zranitelná místa, jak lze tato zranitelná místa využitkovávat, možné formy útoků, kdo může zranitelná místa využitkovat nebo jejich prostřednictvím způsobit neúmyslnou škodu, kdo jsou potenciální útočníci, s jakou pravděpodobností dochází k útoku, jak se lze proti útokům bránit a jaké škody mohou útoky způsobit. Prostředkem použitým pro dosažení stanovených bezpečnostních cílů IS jsou bezpečnostní funkce IS (bezpečnostní opatření), které mohou být administrativního, fyzického nebo logického typu, tj. mohou být implementovány takovými mechanismy, jakými jsou administrativní akce, hardwarová zařízení, procedury, programy.

Bezpečnostní funkce můžeme kategorizovat rovněž podle způsobu implementace. Implementující bezpečnostní mechanismus může mít charakter fyzického opatření, administra-

tivní akce, může jím být technické zařízení nebo logický nástroj (procedura, algoritmus). Podle způsobu implementace pak rozeznáváme bezpečnostní funkce:

- softwarového charakteru (mnohdy označované jako logické bezpečnostní funkce) např. softwarové řízení přístupu, funkce založené na použití kryptografie, digitální podepisování, antivirové prostředky, zřizování účtů, standardy pro návrh, kódování, testování, údržbu programů, ochranné nástroje v operačních systémech (ochrana paměti, ochrana souborů řízením přístupu, přístupové matice, přístupové seznamy, hesla, autentizace přístupu k terminálu), ochranné nástroje v aplikačních systémech pro autentizaci přístupu, pro autentizaci zpráv atd.,
- administrativního a správního charakteru ochrana proti hrozbám souvisejícím s nedokonalostí odpovědnosti a řízení systému IT; výběr a školení důvěryhodných osob, hesla, autorizační postupy, přijímací a výpovědní postupy, právní normy, zákony, vyhlášky, předpisy, etické normy, licenční politika, nástroje provozního řízení, zpravodajství o událostech a stavech významných z hlediska bezpečnosti, sběru a analýzy statistik, konfigurace systému apod. hardwarového charakteru (mnohdy označované jako technické bezpečnostní funkce) autentizace na bázi identifikačních karet, šifrovače, autentizační kalkulátory, firewally, archivní pásky – záložní kopie dat a programů,
- fyzického charakteru stínění, trezory, zámky, strážní, jmenovky, protipožární ochrana, záložní generátory energie.

1.4 Bezpečnostní monitoring informačních systémů

Vzrůstající závislost na informačních systémech a prostředcích IT nutí organizace zavádět systémy řízení informační bezpečnosti. Důležitou součástí takového systému je i požadavek zajistit monitorování přístupu k informačním systémům a jejich použití.

Implementace optimalizovaného systému bezpečnostního monitoringu IS napomáhá splnit významné bezpečnostní cíle. Zejména pak musí zajistit:

- odpovědnost jedince,
- rekonstrukci události,
- detekci narušení,

- podporu při analýze a řešení vzniklých problémů.

Významným přínosem bezpečnostního monitoringu IS je získání určité kontroly nad aktivitami tzv. privilegovaných uživatelů informačního systému (administrátoři a správci). Bezpečnostní monitoring IS tak významnou měrou přispívá k oddělení rolí "kontrolovaný" a "kontrolující" ve skupině privilegovaných uživatelů a k zajištění průkaznosti jejich odpovědnosti.

Systém bezpečnostního monitoringu IS slouží rovněž jako jeden z nástrojů pro sledování a vyhodnocování dosažené úrovně informační bezpečnosti v organizaci. Požadovaná úroveň bezpečnosti informací v organizaci je stanovena bezpečnostní politikou.

Bezpečnostní monitoring IS se běžně dělí na následující oblasti:

- real-time monitoring - zajišťuje průběžné sledování sítí a systémů s cílem detekovat útoky a analyzovat je,
- analýza souborů s auditními záznamy - zajišťuje vyhodnocování bezpečnostních událostí,
- diagnostika - zajišťuje pravidelné prověrky systémové infrastruktury s cílem odhalit specifické zranitelnosti.

1.4.1 Relevantní standardy

Některé aspekty související s otázkou bezpečnostního monitoringu jsou řešeny i uznávanými mezinárodními standardy v oblasti bezpečnosti IS. Nejdůležitější jsou tyto normy:

- ČSN ISO/IEC 17799 Informační technologie - Soubor postupů pro řízení informační bezpečnosti,
- ČSN ISO/IEC TR 13355 Informační technologie - Směrnice pro řízení bezpečnosti IT.

Standard ČSN ISO/IEC 17799 zasazuje bezpečnostní monitoring IS do širšího kontextu řízení bezpečnosti IS. Monitorování přístupu a monitorování užití systému umožňuje kontrolu událostí, která představuje významný vstup do dalších modulů systému, zejména pak do modulů řízení rizik, řízení incidentů a modulu detekce průniku.

Aby mohl být bezpečnostní monitoring IS v organizaci zaveden, je nutné splnit řadu předpokladů, zejména zajistit zaznamenávání událostí do auditních záznamů, oddělit role kont-

rolovaného a kontrolujícího, ukládat auditní záznamy a zajistit jejich bezpečnost a archivování. Je samozřejmé, že pro nezpochybnitelné zaznamenávání událostí je nutným předpokladem efektivní systém řízení přístupu. V neposlední řadě je důležité zajistit synchronizaci času na všech sledovaných prostředcích. Systém jednotného času usnadní případné sledování a vyhodnocování událostí, které mají projevy na různých prostředcích technické infrastruktury.

1.4.2 Bezpečnostní události a incidenty

Jednou z hlavních úloh bezpečnostního monitoringu IS je detekce bezpečnostních událostí, a zejména pak těch událostí, které mají povahu útoku proti informačnímu systému. Bezpečnostní událost lze charakterizovat jako určitou akci proti prostředku informačního systému. Formy akcí mohou být různé a různé mohou být i prostředky, na které je akce namířena.

Aby mohla být akce provedena, je zpravidla nutné použít vhodný nástroj, který využívá existující slabiny informačního systému. Tyto slabiny, nazývané zranitelnosti, mají svůj původ v návrhu informačního systému, ve způsobu jeho implementace nebo v nevhodné konfiguraci jeho jednotlivých komponent. Za každým útokem je potřebné vidět konkrétního útočníka, který neautorizovanou činností (výsledkem činnosti) sleduje svůj určitý cíl.

Pochopení průběhu incidentu a především pochopení rozdílnosti v pohledu útočníka a administrátora-obránce je jedním z předpokladů pro kvalitní návrh systému bezpečnostního monitoringu a jeho začlenění do systému řízení bezpečnosti IS. Je potřebné si uvědomit, že obránce zpravidla pozoruje projevy bezpečnostních událostí, aniž by měl konkrétní informace o útočníkovi a postupech, které útočník použil. V mnoha případech při detekci události není ani ihned zřejmé, zda jde skutečně o bezpečnostní událost, nebo pouze o podezření. Situace je také komplikována faktem, že není jasně zřejmý jednoznačný vztah mezi detekovanou událostí a příčinou, tedy konkrétním útokem proti IS. V mnoha případech jeden útok může generovat celou řadu událostí, jež musí obránce sledovat. Útočník k dosažení svého cíle může použít, najednou nebo postupně, celou řadu útoků. Obránce má velmi těžkou pozici v úloze přiřadit tyto útoky ke konkrétnímu incidentu.

1.4.3 Využití technologií

Vzhledem k rostoucímu významu bezpečnostního monitoringu IS se v posledních letech na tuto oblast zaměřili i přední výrobci technologií. Technologie pro bezpečnostní monitoring lze rozdělit na senzory (čidla), které detekují události významné z hlediska bezpečnosti IS a infrastrukturu (zázemí), která detekované události umožňuje analyzovat, vyhodnotit a zajistit přiměřenou reakci.

Senzory se klasicky dělí na síťové senzory sledující datové toky v síťovém prostředí (network-based) a tzv. host-based senzory, které jsou instalovány na jednotlivých hostitelských prostředcích. Dále lze senzory rozdělit na nástroje zajišťující detekci útoku a skenery prověřující prostředky IS za účelem odhalení existujících známých zranitelností.

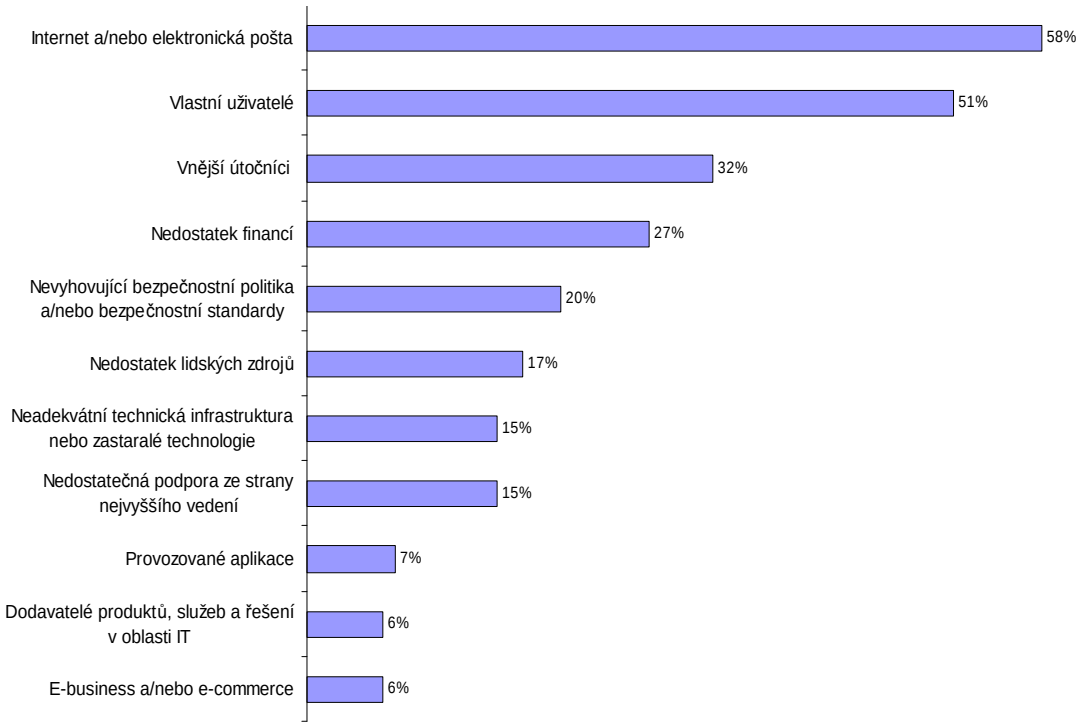
Pro detekci událostí existuje široká nabídka nástrojů. Mnohem složitější je situace v případě vhodných nástrojů zajišťujících analýzu a vyhodnocování událostí a případnou adekvátní reakci. Vhodné nástroje musí zajistit redukci dat (výběr pouze těch dat, které jsou významné) a jejich korelaci a automatizované hledání závislostí.

1.5 Motivace pro zabezpečování

Charakteristickým rysem soudobých organizací je, že svoje poslání plní pomocí propojení informačních a komunikačních systémů, a to jak uvnitř organizace tak i s ostatními organizacemi. Tím se činnosti organizace stávají silně závislé na informacích a službách IT. Důsledkem je, že ztráta důvěrnosti, integrity, dostupnosti, prokazatelnosti odpovědnosti, autenticity a spolehlivosti informací a služeb IT má na chod organizace nepříznivý dopad. Řešením je uplatnění zásad bezpečnosti IT. Pojmem zabezpečování IT označuje proces dosažení a udržení důvěrnosti, integrity, dostupnosti, prokazatelnosti odpovědnosti, autenticity a spolehlivosti informací a služeb IT na přiměřené úrovni. Vhodným metodickým průvodcem bezpečností IT je např. technická zpráva ISO/IEC TR 13335 „Information technology – Guidelines for the Management of IT Technology“. Podle tohoto materiálu se bezpečnost informačních systémů a všech prvků související s těmito systémy použitých v organizaci dosahuje především plněním manažerských funkcí, souvisejících s bezpečností IS jako součást plnění celkového plánu správy organizace. Mezi takové manažerské funkce typicky patří:

- určení cílů, strategií a politiky zabezpečení IS organizace

- určení požadavků na zabezpečení IS organizace
- identifikace a analýza hrozeb pro aktiva IS v rámci organizace
- identifikace a analýza rizik pro organizaci plynoucích z používání IS
- specifikace přiměřených bezpečnostních opatření eliminujících nebo snižujících rizika
- sledování implementace a provozu bezpečnostních opatření použitých pro účinnou ochranu informací a služeb IS v rámci organizace
- vyvinutí a zavedení programu zvyšování bezpečnostních znalostí a vědomí nutnosti udržovat bezpečí všech, kdo IS v organizaci používají detekování bezpečnostních incidentů a adekvátní reakce na ně.



Obr. 1 Největší hrozby z hlediska informační bezpečnosti

Organizace musí své informační systémy zabezpečovat stejně jako jiné investice do své činnosti. Hardwarové komponenty IS lze zničit (teroristy nebo i zaměstnanci) nebo ukrást (a levně prodat nebo používat pro vlastní potřebu). „Ukrást“ lze i software, který mnohdy představuje enormní a přitom špatně vyčíslitelné hodnoty. Neoprávněné užívání softwaru zaměstnanci pro osobní potřebu nebo pro jejich druhé zaměstnání je zdrojem jejich nele-

gálních zisků. Provozovateli kradeného softwaru mohou vzniknout škody plynoucí z trestní odpovědnosti za porušení licence.

Informační systém lze používat neautorizovaně, a tím způsobit např. zničení systému nebo porušení soukromí jiných osob („krádeží“ přístupového hesla, překonáním mechanismu řídicího přístup k IS) nebo lze využitkovávat IS i autorizovanými zaměstnanci k nepracovní činnosti, ať již osobní, nebo výdělečné. Informace jsou v podstatě zboží, pro organizaci představují mnohdy cenná aktiva. Data uložená v bázích dat lze ukrást neoprávněným okopírováním, lze ukrást i výstupy generované IS pro potřebu organizace. Data, která jsou pro organizaci citlivá, je potřeba chránit před konkurencí. Existují právní, morální a etická pravidla pro používání informací, existují zákonné úpravy pro ochranu dat, a ty je žádoucí, resp. nutné, dodržovat. Organizace se musí bránit tomu, aby funkce jejich IS nebyly ať již zlomyslně, nebo neúmyslně znepřístupněny.

Mezi hlavní důvody a motivace pro zabezpečení informačního systému organizace patří několik následujících bodů, které vyjmenovávají způsoby narušení bezpečnosti zpracovávání informací:

- narušením soukromí či utajení informací
- vydáváním se za jinou oprávněnou osobu a zneužíváním jejích privilegií
- distancováním se od odpovědnosti nebo od závazků plynoucích z manipulace s informacemi
- tvrzením, že se nějaká informace někam poslala a toto se nikdy nestalo
- tvrzením, že se informace získala od nějakého podvodníka
- neoprávněným zvýšením svých privilegií přístupu k informacím
- modifikací privilegií ostatních osob
- zatajením výskytu důvěrné informace v jiných informacích
- zjišťováním, kdo a kdy si zpřístupňuje které informace
- zařazením se jako skrytý mezičlánek v konverzaci jiných subjektů
- pokažením funkcionality softwaru doplněním skrytých funkcí
- narušením protokolu činností jiných subjektů zavedením nesprávných, nekorektních informací

- podkopáním důvěryhodnosti protokolu způsobeným zjevným, byť možná jen zdánlivými
- poruchami
- bráněním jiným uživatelům legitimně komunikovat.

Bezpečnost IS nelze řešit izolovaně. Bezpečnostní politika v oblasti IS je nedílnou součástí všeobecné bezpečnostní politiky organizace, která představuje souhrn bezpečnostních zásad a předpisů definujících způsob zabezpečení organizace od fyzické ostrahy, přes ochranu profesních zájmů až po ochranu soukromí a lidských práv.

Bezpečnostní politika organizace se v tomto kontextu zabývá výběrem bezpečnostních zásad a předpisů splňujících bezpečnostní politiku organizace a obecně definujících bezpečné používání informačních zdrojů v rámci organizace nezávisle na konkrétně použitých informačních technologiích (určuje, která data jsou pro organizaci citlivá, kdo je za ně odpovědný, předpisuje infrastrukturu zabývající se v rámci organizační struktury organizace bezpečností, vymezuje základní omezení, která se musí respektovat apod.). Určení detailních konkrétních norem, pravidel, praktik, předpisů konkrétně definujících způsob správy, ochrany, distribuce citlivých informací a jiných konkrétních informačních zdrojů v rámci organizace, specifikace bezpečnostních opatření a způsobu jejich implementace, určení způsobu jejich použití, který zaručuje přiměřenou bezpečnost odpovídající požadavkům bezpečnostní politiky organizace, při respektování konkrétně použitých IT pro realizaci IS organizace, to vše je náplní bezpečnostní politiky IS organizace.

Ani všeobecnou bezpečnostní politiku organizace nelze řešit bez návaznosti na ostatní politiky vymezující chod a poslání organizace (finanční, obchodní, sociální atd.). Je důležité si uvědomit, že zkušenosti útočníků v čase rostou, cíle jejich útoků se postupně upřesňují, informační technologie se vyvíjejí a zdokonalují, mění se případně i cíle profilu organizace. Proto se i cíle, strategie a politiky bezpečnosti musí periodicky korigovat. Vhodné jsou periodické oponentury bezpečnostních politik, které mohou vyvolat požadavek opakovaného provedení analýzy rizik, periodicky je potřebné provádět i bezpečnostní audit.

1.6 10 důvodů proč budovat systém řízení bezpečnosti IS organizace

1. Zvýší důvěryhodnost a jméno společnosti – stejně jako například certifikáty jakosti řady ISO 9000 lze jasnou bezpečnostní politiku prezentovat jako zcela zřejmou

konkurenční výhodu. V očích zákazníků pak bude firma působit důvěryhodněji, klienti budou vědět, že je zde dobře postaráno o ochranu např. obchodního tajemství...

2. Systém řízení informační bezpečnosti přinese optimální poměr mezi výší nákladů a úrovní zabezpečení informačních aktiv organizace. Budou totiž chráněna jen informační aktiva, která mají pro firmu odpovídající hodnotu a to takovými bezpečnostními mechanismy, jejichž náklady na realizování jsou zcela v souladu se stanoveným ohodnocením informačních aktiv.
3. Chrání stabilitu organizace tím, že minimalizuje nebezpečí úniku dat z IS způsobeného vnějším narušitelem, kterým může být třetí strana, hacker, bývalý zaměstnanec.
4. Definuje jasný systém organizačního zajištění bezproblémového chodu informačních a komunikačních technologií s přesně určenými prvky odpovědnosti, pravomoci a součinnosti.
5. Umožňuje strategické řízení bezpečnosti ICT[3] managementem.
6. Chrání investice organizace do výzkumu a vývoje před zneužitím konkurencí, která může využít např. nespokojených zaměstnanců, zaměstnanců na odchodu, úklidového personálu, studentů apod.
7. Chrání před počítačovými viry, trojskými koňmi, počítačovými červy, tedy před kybernetickými útoky, které paralyzují chod IS organizace.
8. Vytváří strukturu důležitosti (hierarchie priorit) jednotlivých částí IS. Víte tedy, co by se mělo chránit a hlavně jakým způsobem. To se týká jak informací, tak aplikací, ale třeba i HW[4].
9. Omezuje „absolutní moc“ administrátorů a správců nad informačním systémem.

[3] ICT - Information and Communication Technology

[4] HW - Hardware

10. Umožňuje analyzovat podezřelé situace v systému a odhalit tak nebezpečí dříve než se změní v havárii nebo bezpečnostní incident.

1.7 Bezpečnostní trendy pro letošní rok

Z informací společnosti Dimension Data jsem vybral deset největších bezpečnostních trendů pro letošní rok. Poroste jak množství nejrůznějších hrozeb, tak možnosti ochrany proti nim.

1. Očekávají se větší škody, ale méně epidemií. Množství infekcí v roce 2006 pravděpodobně vzroste a organizace se už nebudou moci spoléhat na to že, že se o problémech a masových útocích dozvědí z médií. Předpoklad, že žádné zprávy znamenají dobré zprávy, povede pouze k falešnému pocitu bezpečí.
2. Útoky už se nebudou zaměřovat pouze na operační systém Microsoft. Terčem útoků se stane více aplikací a dalších prvků infrastruktury, což povede k větším pracovním nárokům na opravování chyb zabezpečení.
3. Spyware bude nadále představovat velký problém. Z toho důvodu bude třeba více investovat do dalších technologií na boj proti spywaru.
4. Rychlé posílání zpráv a sítě peer-to-peer budou způsobovat ještě větší potíže. Široké prosazování a používání rychlého posílání zpráv může vystavit organizace novým hrozbám.
5. Zabezpečení zpráv se začne brát zodpovědně. Ohnisko zájmu se pomalu přesouvá směrem k řešením, která kromě ochrany před viry a spamem zajišťují také dodržování zásad a šifrování.
6. Představenstva firem budou bezpečnosti věnovat větší pozornost. V souladu s globálním trendem správných řídících postupů budou představenstva firem věnovat větší pozornost ochraně informačního majetku organizací před rostoucím množstvím interních a externích hrozeb.
7. Zabezpečení bezdrátové komunikace získá větší pozornost. Vzhledem k rostoucí poprávce koncových uživatelů po mobilitě potřebují organizace zajistit, aby jejich bezdrátové přístupové body byly chráněny před neoprávněným přístupem.

8. Instalace oprav začne být selektivní. Začíná být příliš pracné a nákladné implementovat všechny opravy, a proto organizace začnou selektivně instalovat opravy na základě hodnoty příslušných prvků IT a na základě konkrétních hrozeb, jimž čelí.
9. Trend směrem k bezpečné infrastruktuře bude pokračovat. Zabezpečení je čím dál častěji zabudováno přímo ve vrstvě infrastruktury, takže jsme svědky konvergence správy sítě, systémů a zabezpečení. V důsledku toho budou zákazníci čím dál častěji hledat jediného poskytovatele, který jim dodá celou infrastrukturu, bude ji spravovat a zabezpečovat.
10. Bude se klást větší důraz na zabezpečení koncových bodů. Mnohem větší pozornost se bude věnovat tomu, jak se k síti připojují nezabezpečené koncové body, například notebooky, stolní počítače a další zařízení.

2 IMPLEMENTACE ŘÍZENÍ BEZPEČNOSTNÍCH RIZIK V IS

Využívání informačních systémů a sítí a celé prostředí informačních technologií prochází neustále dramatickými proměnami. Tyto probíhající změny s sebou přinášejí výrazné výhody, ale také si vyžadují mnohem větší důraz na bezpečnost ze strany státních správ, podniků, ostatních organizací a jednotlivých uživatelů, kteří vyvíjejí, vlastní, poskytují, spravují, službami zajišťují a užívají informační systémy a sítě. Stále výkonnější osobní počítače, sbližující se technologie a široce rozšířené využívání internetu nahradily dřívější skromné, samostatné systémy v převážně uzavřených sítích. V současnosti jsou účastníci stále více propojeni a tato vzájemná propojení jdou napříč národními hranicemi. Vedle toho se o internet opírá kritická infrastruktura v odvětvích jako je energetika, doprava a finance a internet je významnou součástí obchodování mezi podniky, poskytování služeb státní správy občanům a podnikům a komunikace a výměny informací mezi jednotlivými občany. Povaha a typ technologií, z nich. je vybudována komunikační a informační infrastruktura, se rovně. výrazně změnily. Rozšířil se počet a povaha zařízení pro přístup k infrastruktuře a nyní sem patří zařízení pevná, bezdrátová a mobilní a rostoucí množství přístupů je uskutečňováno prostřednictvím stále zapnutých. připojení. Zásadně se tedy rozšířila povaha, objem a citlivost informací, které se vyměňují. Následkem zvýšené vzájemné propojitelnosti se informační systémy a sítě nyní potýkají s rostoucím počtem a širší paletou hrozeb a zranitelných míst. To vyvolává nové otázky v oblasti bezpečnosti. Z těchto důvodů se při implementaci musí počítat s tím, že se týká všech účastníků nové informační společnosti a připomíná potřebu většího porozumění bezpečnostní problematice, informovanosti o ní a potřebu vytvářet kulturu bezpečnosti.

2.1 Zásady implementace

Následujících devět zásad se navzájem doplňuje a mělo by být při implementaci řízení bezpečnosti vykládáno jako celek. Týkají se účastníků na všech úrovních, včetně úrovně koncepční a provozní. Podle této struktury se odpovědnost účastníků liší podle jejich role. Všem účastníkům pomůže informovanost, vzdělání, sdílení informací a .kolení, které může vést k lepšímu pochopení bezpečnosti a přijetí správnější praxe. Snahy prohloubit bezpečnost informačních systémů a sítí by měly být v souladu s hodnotami demokratické společnosti, zvláště s potřebou otevřeného a svobodného toku informací a se základními ohledy na ochranu soukromí.

2.1.1 Informovanost

Účastníci by měli být informováni o potřebě bezpečnosti informačních systémů a sítí a o tom, co mohou udělat, aby bezpečnost prohloubili. Informovanost o rizicích a dostupných bezpečnostních zajištěních představuje prvoliniovou obranu bezpečnosti informačních systémů a sítí. Informační systémy a sítě mohou ovlivnit jak interní, tak externí rizika. Účastníci by měli chápat, že bezpečnostní selhání mohou závažně poškodit systémy a sítě, které ovládají. Rovně. by si měli být vědomi potenciálního poškození ostatních daného vzájemnou propojitelností a závislostí. Účastníci by měli být informováni o konfiguraci svého systému a dostupných aktualizacích systému, jeho místě v rámci sítí, správné praxi, kterou mohou provádět, aby prohloubili bezpečnost a potřeby dalších účastníků.

2.1.2 Odpovědnost

Všichni účastníci jsou odpovědní za bezpečnost informačních systémů a sítí. Účastníci jsou závislí na vzájemně propojených lokálních a globálních informačních systémech a sítích a měli by rozumět své odpovědnosti za bezpečnost těchto informačních systémů a sítí. Měli by odpovídat způsobem přiměřeným jejich individuální úloze. Účastníci by měli pravidelně přehodnocovat vlastní politiku, praxi, opatření a postupy a zjišťovat, zda jsou, s ohledem na jejich prostředí, přiměřené. Ti, kteří vytvářejí, navrhují a dodávají produkty a služby, by se měli zabývat bezpečností systému a sítě a včas šířit příslušné informace včetně aktualizací, aby uživatelé lépe chápali bezpečnostní funkce produktů a služeb a svou odpovědnost v souvislosti s bezpečností.

2.1.3 Reakce

Účastníci by měli jednat včas a vzájemně spolupracovat při předcházení bezpečnostním incidentům, jejich odhalování a reagování na ně. S ohledem na vzájemnou propojitelnost informačních systémů a sítí a možnost rychlého a rozsáhlého poškození by účastníci měli jednat včas a vzájemně spolupracovat při řešení bezpečnostních incidentů. Měli by sdílet informace o hrozbách a případných zranitelných místech a zavádět postupy pro rychlou a účinnou spolupráci k zabránění bezpečnostním incidentům, jejich odhalení a reakci na ně.

2.1.4 Etika

Účastníci by měli respektovat legitimní zájmy ostatních. Vzhledem k pronikavosti informačních systémů a sítí do na.í společnosti je třeba, aby účastníci uznali, .e jejich činnost či nečinnost může poškodit ostatní. Etické chování je proto rozhodující a účastníci by se měli snažit vytvořit a přijmout nejlepší praxi a prosazovat jednání, které uznává bezpečnostní potřeby a respektuje legitimní zájmy ostatních.

2.1.5 Demokracie

Bezpečnost informačních systémů a sítí by měla být slučitelná se základními hodnotami demokratické společnosti. Bezpečnost by měla být zaváděna způsobem, který je v souladu s hodnotami uznávanými v demokratických společnostech, včetně svobody výměny myšlenek a idejí, volného toku informací, důvěrnosti informací a komunikace, příslušné ochrany osobních informací, otevřenosti a průhlednosti.

2.1.6 Odhad rizika

Účastníci by měli provádět odhady rizik. Odhad rizika poukazuje na hrozby a zranitelná místa a měl by být dostatečně široký, aby zahrnul interní i externí faktory, jako je technologie, fyzické a lidské faktory, politiky a služby třetích stran s bezpečnostními implikacemi. Odhad rizika umo.ní určit přijatelnou úroveň rizika a pomůže při výběru vhodných kontrolních mechanismů ke zvládnutí rizika potenciálního poškození informačního systému a sítě s ohledem na povahu a důležitost informací, které mají být chráněny. Vzhledem k rostoucí vzájemné propojitelnosti informačních systémů by odhad rizika měl obnášet zvážení potenciálních škod, které mohou být způsobeny ostatními nebo mohou být způsobeny ostatním.

2.1.7 Navržení a realizace bezpečnosti

Účastníci by měli bezpečnost zahrnout mezi základní prvky informačních systémů a sítí. Systémy, sítě a politiky je třeba řádně navrhovat, realizovat a koordinovat, aby bylo možné optimalizovat bezpečnost. Hlavním, ale nikoli výlučným jádrem této činnosti, je navrhovat a přijímat příslušná bezpečnostní zajištění a řešení k vyhnutí se potenciálnímu poškození ze zjištěné hrozby nebo zranitelného místa či omezení takového poškození. Je třeba jak technických, tak netechnických bezpečnostních zajištění a řešení a ta by měla být úměrná

hodnotě informací v systémech a sítích organizace. Bezpečnost by měla být základním prvkem všech produktů, služeb, systémů a sítí a integrální součástí řešení a architektury systému. Pro koncové uživatele navrhování a realizace bezpečnosti obnáší převážně výběr a konfiguraci produktů a služeb pro jejich systém.

2.1.8 Řízení bezpečnosti

Účastníci by měli k řízení bezpečnosti zaujmout komplexní přístup. Řízení bezpečnosti by mělo být založeno na odhadu rizik a mělo by být dynamické, postihovat všechny úrovně činnosti účastníků a všechny aspekty jejich provozu. Mělo by obsahovat do budoucna namířené reakce na vznikající hrozby a zabývat se prevencí a odhalováním incidentů a reakcí na ně, zotavením systému, průběžnou údržbou, revizí a auditem. Politika, praxe, opatření a postupy v oblasti bezpečnosti informačních systémů a sítí by měly být koordinovány a integrovány, aby utvářely ucelený systém bezpečnosti. Požadavky na řízení bezpečnosti závisejí na úrovni zapojení, úloze účastníka, souvisejícím riziku a požadavcích systému.

2.1.9 Přehodnocování

Účastníci by měli revidovat a přehodnocovat bezpečnost informačních systémů a sítí a provádět příslušné úpravy bezpečnostní politiky, praxe, opatření a postupů. Stále jsou odhalovány nové a proměňující se hrozby a zranitelná místa. Účastníci by měli průběžně revidovat, přehodnocovat a upravovat veškeré aspekty bezpečnosti, aby se s těmito vyvíjejícími se riziky vypořádali.

2.2 Zajištění kultury bezpečnosti

Při implementaci řízení bezpečnostních rizik se musí se prosazovat rozvoj kultury bezpečnosti tj. soustředění pozornosti na bezpečnost při vytváření informačních systémů a sítí a přijetí nových způsobů myšlení a chování při používání informačních systémů a sítí a jednání v jejich rámci. Prohlubuje se závislost účastníků na informačních systémech, sítích a souvisejících službách a je třeba, aby všechny byly spolehlivé a bezpečné. Pouze přístup, kterým se náležitě zohledňují zájmy všech účastníků a povaha systémů, sítí a souvisejících služeb, může vést k efektivnímu zajištění bezpečnosti. Každý účastník je při zajišťování bezpečnosti důležitým aktérem. Účastníci by si v souladu se svou rolí měli být vědomi příslušných bezpečnostních rizik a preventivních opatření, přebírat odpovědnost a přijímat

kroky k prohloubení bezpečnosti informačních systémů a sítí. Prosazování kultury bezpečnosti si bude vyžadovat jak vedení, tak širokou účast, a mělo by vést k přiřazení vyšší priority plánování a řízení bezpečnosti a také k pochopení potřeby bezpečnosti všemi účastníky. Bezpečnostní otázky by měly být předmětem zájmu a odpovědnosti na všech úrovních státní správy a podnikání a pro všechny účastníky. Prvky implementace představují základ pro práci směřující ke kultuře bezpečnosti jakožto způsobu přemýšlení o činnosti informačních systémů a sítí, jejím vyhodnocování a zařizování se podle ní.

Hlavním cílem při řízení bezpečnostních rizik v podnikových informačních systémech musí být prosazování kultury bezpečnosti mezi všemi účastníky jako prostředek ochrany informačních systémů a sítí. Dále také zvyšování informovanosti o riziku pro informační systémy a sítě, praxi, opatřeních a postupech, které jsou k řešení těchto rizik k dispozici, a potřebě jejich přijetí a realizace. Důležité je také vytvářet větší důvěru účastníků v informační systémy a sítě a způsob, jakým jsou poskytovány a využívány a vytváření obecných referenčních rámců, pomocí kterých budou schopni účastnici lépe porozumět bezpečnostním otázkám a ctít etické hodnoty při vytváření a realizaci promyšlené politiky, praxe, opatření a postupů k bezpečnosti informačních systémů a sítí. Důležitou složkou je takové schopnost prosazovat spolupráci a sdílení informací, jak bude vhodné, mezi všemi účastníky vytváření a realizace bezpečnostních politik, praxe, opatření a postupů a následné prosazování zohledněné bezpečnosti jako důležitý cíl všech účastníků zapojených do vytváření a realizace standardů.

2.3 Bezpečnostní zásady a reakce na události

Důvěra je ústředním motivem mnoha různých stránek věnovaných bezpečnosti a jako taková musí být naprosto prvořadá i při návrhu konkrétní bezpečnosti systémů či zásad zabezpečení. Zásady zabezpečení by se mohly postavit na myšlence, že nebude důvěra vůbec k nikomu, a to ani k zaměstnancům vlastní organizace. Takovéto zásady by však ve výsledku ale nefungovaly. Je známé, že pokud se uživatelům nějaké zásady zdají příliš svazující, tím častěji je obcházejí. V zásadách zabezpečení je proto třeba nastolit vhodnou rovnováhu mezi důvěrnou a bezpečnosti. Každá organizace má tento rovnovážný bod někde jinde podle různých faktorů, které jsou ovlivněny právě různorodostí organizací, ve kterých se daný informační systém nachází. Ale určité společné prvky zabezpečení potřebuje každý.

Při stanovování úrovně důvěry, kterou je nejvhodnější vyjádřit v písemných zásadách zabezpečení se musí brát v potaz následující otázky a během dalšího návrhu zásad a řízení bezpečnosti na těchto otázkách dále stavět:

- určit, kdo smí dostat právo přístupu do jednotlivých částí sítě,
- vymezit, k jakým prostředkům smí tito uživatelé přistupovat a jak,
- vyvážit důvěru mezi osoby a technické prostředky,
- povolit přístup podle úrovně důvěry uživatelů a prostředků,
- pomocí vhodných prostředků zajistit, že důvěra nebude narušena
- definovat odpovídající používání sítě a jejich prostředků.

Kromě tohoto výčtu několika nejzákladnějších prvků pro definování důvěry je třeba zvážit také celkovou firemní politiku a zvyklosti uživatelů společně s jejich reakcemi. Žádná bezpečností politika nemůže bohužel počítat a ošetřit naprosto vše. Přesto je ale důležité si uvědomit, že mezi lidmi vyvolává také nějakou reakci.

Proto zásady pro řízení bezpečnosti informačních systémů organizace by měly především zdůrazňovat, co je povoleno, nikoli co je zakázáno. Je-li třeba, je možné podle potřeby uvádět příklady správného a nesprávného chování. Tak nevznikají pochybnosti o významu zásad. Obecně platí, že jakékoliv chování, které není v zásadách zabezpečení výslovně povoleno, je zakázáno. Zásady zabezpečení by měly popisovat také způsoby dosažení stanových cílů. Musí také definovat prostředky, které bude organizace či firma k ochraně síti potřebovat, a opatření pro stanovenou ochranu. Jinými slovy, společně tvoří písemnou normu všech rozhodnutí, z nichž se skládají bezpečností postoje firmy. Takto vytvořené zásady je nutné zveřejnit a doručit všem zaměstnancům a jiným uživatelům systému, na které se tyto zásady a předpisy vztahují. Vedení firmy také musí zajistit, že se každý se zásadami seznámí, porozumí jim a potvrdí svou roli v jejich plnění a dodržování. Spolu se seznámením se zásadami bezpečnosti bude každý srozuměn s tresty za případné porušení.

2.3.1 Nejběžnější typy zásad zabezpečení

Přípustné šifrování - stanovuje pravidla, která omezují šifrování jen na obecně známe, prověřené a účinné algoritmy. Navíc určuje potřebné postupy, které zajišťují naplnění příslušných zákonů a nižších předpisů.

Přípustné užití - vymezuje osoby, které smí pracovat s počítačovým zařízením a sítěmi ve vlastnictví společnosti. Týká se firemních počítačů, umístěných ve firemních prostorách nebo i v domácnostech zaměstnanců.

Analogové linky - popisuje způsob přípustného využívání analogových telefonních linek a linek ISDN a nařizuje příslušné zásady a postupy pro schvalování. Pro linky, určené výhradně k faxování a příjmu hovorů, a linky zapojené do počítačů platí samostatná pravidla.

Standardy poskytovatelů - definuje kritéria minimální bezpečnosti, kterou musí aplikačních služeb splňovat každý poskytovatel aplikačních služeb.

Audit - členům oddělení informační bezpečnosti přiděluje oprávnění k výkonu bezpečnostního auditu nad libovolným systémem, který je ve vlastnictví společnosti nebo který je v jejich prostorách nainstalován.

Automatická přeposílaná pošta – zakazuje neoprávněné i neúmyslné prozrazování citlivých firemních informací.

Přístupové informace k databázím – určuje požadavky na bezpečné ukládání a načítání uživatelských jmen a hesel k databázím (neboli přístupovým informacím), která budou používat programy při přístupu k databázi provozované na firemní síti.

Extranet – určuje zásady, podle nichž se do firemní sítě smí připojit cizí organizace za účelem provádění transakcí.

Citlivost informací – napomáhá zaměstnancům určit, které informace smí sdělovat cizím osobám (mimo zaměstnanců), a také relativní citlivost informací, které se bez oprávnění sdělovat nesmí.

Bezpečnost vnitřních laboratoří – definuje požadavky informační bezpečnosti v laboratořích, které zabraňují v ohrožení důvěryhodných informací a technologií, a také ochraňují provozní služby a ostatní zájmy firmy před pokusnými laboratorními aktivitami.

Antivirová ochrana – vymezuje požadavky, jež musí splňovat všechny počítače připojené do podnikové sítě s ohledem na účinnou detekci virů a jejich prevenci.

Hesla – zavádí standardy pro vytváření silných hesel, ochranu hesel a frekvenci změn hesel.

Vzdálený přístup – definuje standardy pro připojení libovolného hostitele do firemní sítě. Tyto standardy sledují minimalizaci různých potenciálních hrozeb., jako je ztráta citlivých informací nebo důvěrných firemních dat, duševního vlastnictví, poškození image firmy na veřejnosti, poškození kriticky důležitých vnitřních systémů atd.

Posuzování rizik – zmocňuje oddělení informační bezpečnosti k provádění pravidelného posuzování rizik bezpečnosti informací, jehož účelem je zjištění zranitelných míst v síti a zahájení nápravných opatření.

Zabezpečení směšovačů a přepínačů – popisuje povinnou minimální bezpečnostní konfiguraci všech směšovačů a přepínačů, připojených do ostré provozní sítě, nebo používaných v jakémkoli ostrém provozním prostředí.

Zabezpečení serverů – vymezuje standardy pro základní konfiguraci interních serverů, které jsou ve vlastnictví anebo provozu firmy, případně které pracují ve webovém hostovaném prostoru.

Virtuální privátní sítě (VPN) – stanovuje zásady vzdáleného přístupu přes síť VPN s IPSec nebo L2TP do vnitřní firemní sítě.

Bezdrátová komunikace – určuje pravidla pro přístup do podnikové sítě prostřednictvím zabezpečených mechanismů bezdrátové komunikace.

Každý ze zaměstnanců daného oddělní či firmy musí nejenže znát obsah příslušných zásad, ale především by se jimi také měl řídit. Zásady bezpečnosti mají vliv na všechny skupiny uživatelů podnikového systému v organizaci:

Běžný uživatel – na obyčejného uživatele, který přistupuje k síťovým prostředkům mají stanové zásady největší vliv.

Týmy ve vedení firmy – tato skupina má největší zájem na ochraně podnikových prostředků a dat, přičemž je pro ni zároveň důležité, za jakou cenu budou tato opatření prováděna.

Účetní a právní oddělení, investoři – odpovědnost firmy při ochraně svých vlastních aktivit je závislá na popisovaných zásadách (bezpečností politice); každý z této skupiny si musí uvědomit, jaký pozitivní dopad mají přijaté zásady.

Týmy pro vedení bezpečnosti - hlavní rolí a úkolem této skupiny je zajišťování platnosti zásad zabezpečení.

2.3.2 Zásady přípustného užívání

Při sestavování zásad přípustného užívání by se neměla zavádět žádná omezení, která by byla v rozporu s firemní kulturou jakékoliv společnosti, na kterou se vztahuje řízení bezpečnostních rizik ve firemním informačním systému. Úkolem má být především ochrana společnosti, zaměstnanců a partnerů před nezákonnými nebo škodlivým jednáním, a to ať už vědomým nebo i nevědomým.

Veškeré systémy, související s internetem, intranetem a extranetem, včetně počítačového vybavení, softwaru, operačních systému, záznamových médií, síťových účtů s přístupem k elektronické poště, procházení sítě WWW[5] a FTP[6] jsou musí být definovány jako firemní vlastnictví. Tyto systémy pak slouží pro samotný chod firmy a slouží pro zajištění činností, které slouží zájmu společnosti, jejím klientům a zákazníkům.

Účinné zabezpečení je průřezová, týmová činnost, do níž se musí zapojit a podporovat všichni zaměstnanci, dodavatelé nebo obchodní partneři, kteří pracují s daným podnikovým informačním systémem nebo do něj jakýkoliv způsobem vstupují nebo zasahují. Každý uživatel počítače je proto povinen znát pravidla stanovená těmito zásadami zabezpečení a při své práci se jimi přiměřeně řídit.

2.3.2.1 Účel a působnost zásad

Účelem všech zásad je stanovit pravidla přístupného užívání počítačového vybavení, která jsou součástí vnitropodnikového informačního systému. Tato pravidla slouží k ochraně jak firmy samotné tak i jejích zaměstnanců. Nepřípustné užívání systémů může vystavovat společnost různým rizikům, například virovým útokům, napadení síťových systémů a služeb i právnímu postihu. Zásady proto musí platit pro každého vstupujícího do podnikového informačního systému, ať už se jedná o zaměstnance, dodavatele, konzultanta, dočasného pracovníka nebo pro ostatní osoby včetně osob spojených s příslušnými cizími subjekty. Dále by tato pravidla měla platit a měla by se také dodržovat na každém osobním zařízení, které může přijít do styku s podnikovou strukturou informačního systému.

---

[5] WWW - World Wide Web

[6] FTP - File transfer protocol

2.3.2.2 Užití bezpečnostních zásad

Snahou řízení bezpečnostních rizik je zajistit přiměřenou úroveň soukromí, uživatelé si nicméně musí být vědomi, že veškerá data, která v podnikových systémech vytvoří, zůstávají vlastnictvím podniku.

Zaměstnanci jsou odpovědní za přiměřené osobní užívaní systémů, a to podle svého nejlepšího svědomí a vědomí. Jednotlivá oddělení musí být zodpovědná za vytvoření zásad osobního užívání internetových, intranetových a extranetových systémů. Pokud takovéto zásady nejsou a chybí, musí se zaměstnanec řídit obecnými zásadami osobního užívání v daném oddělení.

Pro účely zachování bezpečnosti a údržby sítí smí oprávnění zaměstnanci kdykoli monitorovat zařízení, systémy i síťový provoz a s ohledem na zajištění platnosti zásad mají mít právo na audit veškeré sítě a s nimi spojenými systémy. Tyto poslední kroky jsou velice důležité, protože organizace takto může upozorňovat zaměstnance na možnost monitorování a auditu v síti, a to ať už pravidelného nebo namátkového.

2.3.2.3 Bezpečnost a důvěrné informace

Uživatelské rozhraní k informacím obsaženým v informačních podnikových systémech využívajících internetové, intranetové nebo extranetové připojení je vždy nutné považovat jako důvěrné nebo neutajované (bez klasifikace) a to v souladu s podnikovými zásadami klasifikace důvěrnosti. Příklady základních informací, které by měly v podnikovém informačním systému spadat do kategorie důvěrných jsou například tyto:

- Soukromé nebo důvěrné firemní informace
- Podnikové strategie a záměry
- Informace citlivé vzhledem ke konkurenci a konkurenční analýzy
- Data podléhající obchodnímu tajemství, patenty, výsledky testů
- Specifikace a provozní parametry
- Seznamy zákazníků a údaje o nich
- Výzkumné údaje

Zaměstnanci musí všemi vhodnými prostředky zabránit neoprávněnému přístupu k těmto a podobným informacím.

Dalším krokem jak zajistit ochranu před bezpečnostními riziky je uchovávání hesel v tajnosti a bezpečí. Zaměstnanci nesmí hesla nebo svůj osobní účet půjčovat nikomu jinému, kdy každý oprávněný uživatel je odpovědný za bezpečnost svého vlastního účtu i hesla. Systémová hesla je třeba měnit nejméně jednou za čtvrtletí, uživatelská hesla pak každých šest měsíců.

Veškeré osobní počítače, notebooky a pracovní stanice musí být zabezpečeny pomocí spořiče obrazovky s ochranou hesla a s automatickou aktivací nejpozději po 10 minutách nečinnosti, nebo se uživatel při vzdálení od počítače musí odhlásit. Informace umístěné na přenosných počítačích jsou obzvláštně zranitelné, a proto je nutné s nimi zacházet mimořádně opatrně.

Veškeré počítačové systémy, které zaměstnanec používá a které jsou připojeny k internetu, intranetu nebo extranetu uvnitř podnikového informačního systému, ať už jsou v majetku zaměstnance nebo firmy, musí být neustále kontrolovány schváleným antivirovým programe s aktuální databází virů. Tato zásada se musí týkat i osob, která mají ve zvyku číst e-mail z různých počítačů na různých fyzických místech. Jedná se především o zaměstnance, kteří čtou v práci poštu ze svého soukromého, bezplatného účtu přes webové rozhraní a nic netušíc stáhnou zavirovanou přílohu, soubor. Cílem předchozího pravidla je zajistit, že i takovýto virus bude zachycen ve vhodném antivirovém programu. Pokud ale zaměstnanec přistupuje ke stejnému webovému e-mailu z domácího počítače, jehož prostřednictvím se následně připojuje i do podnikové sítě, je nutné důkladně zvážit možné důsledky a ohrožení firemního systému.

Při otevírání e-mailových příloh od neznámých odesílatelů, které mohou obsahovat viry, e-mailové bomby nebo trojské koně, si uživatelé musejí počínat maximálně opatrně. V případě pochybností je uživatel povinen zkontrolovat dokument ručně před otevřením přílohy.

2.4 Vytvoření organizace bezpečnosti a bezpečnostní politiky společnosti

Proces vytvoření a schválení Bezpečnostní politiky je společný pro všechny typy organizací včetně publikování politiky vůči všem zaměstnancům. Také rozsah a obsah dokumentu je velmi podobný. Bezpečnostní politika definuje zásady a pravidla na úrovni cílů a ty jsou zpravidla shodné pro všechny organizace. Musí také obsahovat odkaz na dokument popisující rozsah řízení bezpečnosti IS, protože systém řízení nemusí být zaveden pro celý informační systém (stejně jako systém řízení kvality podle ISO řady 9000).

V dokumentu by měla být popsána mj. organizační struktura bezpečnosti. Popis bezpečnostních rolí a jejich odpovědností musí odpovídat velikosti systému a počtu uživatelů. Navíc je nutné respektovat zavedenou organizační strukturu a proto je možné pro stejně velké společnosti použít různé modely organizace bezpečnosti. Některé činnosti z oblasti bezpečnostní dokumentace mohou být v kompetenci vybraného pracovníka, který může mít na starosti také audit. Kumulace práv a pravomocí souvisejících s bezpečností informací a se správou systému je pro menší organizace rizikem, které je nutné přijmout.

Pokud má systém pouze několik desítek uživatelů, je možné jednotlivé kompetence rozdělit mezi několik stávajících pracovníků nejen z IT. Nemusí však být vždy efektivní pro 150 lidí jmenovat bezpečnostního ředitele na plný úvazek. Tímto se může stát například zástupce ředitele a ne zřídka spadnou dané kompetence na vedoucího IT oddělení. Kumulace pravomocí zejména ve výkonu bezpečnosti je rizikem i pro firmu střední velikosti. Organizace bezpečnosti v souvislosti s kumulací práva a povinností v oblasti bezpečnosti není vyřešena ani v mnoha velkých organizacích. Téměř v každé se najde jeden nebo několik „neomezených vládců systémů“, na jejichž oddanost firmě všichni spoléhají. Pro tyto situace nelze nalézt univerzální řešení a proto jsou prosazována a uplatňována různá pravidla a technologická opatření.

Tab. 1 Plán bezpečnosti a bezpečnostní politiky

Proces	Malá organizace do 15 zaměstnanců 1-2 úrovně vedení	Střední organizace do 150 zaměstnanců 3-5 úrovní vedení	Velká organizace nad 150 zaměstnanců 4 a více úrovní vedení
Plán / projekt bezpečnosti	Schválení strategie/plánu pro bezpeč-	Schválení celkové koncepce bezpečnosti	Schválení celkové koncepce bezpečnosti

	nost	Schválení projektu bezpečnosti	Vymezení rozsahu projektu + odhad zdrojů a harmonogramu Schválení projektu bezpečnosti Analýza stavu bezpečnosti
Bezpečnostní politika	Musí být napsána a schválena vedením Popisuje základní zásady bezpečnosti na úrovni cílů Definuje organizaci bezpečnosti, odpovědnosti a strukturu bezpečností dokumentace	Musí být napsána a schválena vedením Popisuje základní zásady bezpečnosti na úrovni cílů Definuje organizaci bezpečnosti, odpovědnosti a strukturu bezpečností dokumentace	Musí být napsána a schválena vedením Popisuje základní zásady bezpečnosti na úrovni cílů i strategií pro jejich dosažení včetně závazku podpory a alokace zdrojů Definuje organizaci bezpečnosti, odpovědnosti a strukturu bezpečností dokumentace
Organizace bezpečnosti	Oddělení/Odbor bezpečnosti: NE Bezp. ředitel: ředitel firmy Bezp. administrátor: administrátor IS Bezp. auditor: odpovědnost delegována na pracovníka (mimo administrátora IS)	Oddělení/Odbor bezpečnosti: ANO (pod IT) Bezp. ředitel: jmenován člen vedení Bezp. manažer: jmenováni 1-3 Bezp. auditor: pracovník interního auditu, nebo delegováno na pracovníka mimo IS Bezp. administrátoři: administrátoři částí systémů	Oddělení/Odbor bezpečnosti: ANO (v IT i mimo) Bezp. ředitel: jmenován člen vrcholového managementu Existuje oddělení bezp. s odpovědnostmi za řízení i správu všech oblastí bezpečnosti Bezp. auditor: zajišťuje oddělení interního auditu

2.5 Analýza rizik

Organizace se často obávají projektu analýzy rizik, který je nutný při zavádění Systému řízení bezpečnosti informací (ISMS – Information Security Management System). Jedním

z důvodů je i rozhodnutí, jakým způsobem (přístupem) analýzu provést. Norma ISO 17799 specifikuje dva přístupy k provedení analýzy rizik: základní, detailní, a jejich kombinaci. Tyto varianty se rozlišují podle způsobu hodnocení, použitých metrik, úrovně detailu vstupů a výstupů atd. Podle těchto kritérií lze rozdělit přístupy na:

- dodavatelský přístup – projekt analýzy rizik provádí dodavatel a nese za něj také odpovědnost,
- vlastní přístup – projekt analýzy provádí pracovníci organizace vlastními silami s pomocí zakoupené nebo vlastní metodiky, odpovědnost za provedení je na těchto pracovnících,
- partnerský přístup – projekt analýzy provádí pracovníci organizace pod metodickým i projektovým vedením dodavatelské nebo konzultační společnosti, odpovědnost je na dodavateli (konzultantovi).

Hranice mezi přístupy, které jsou dány zejména odpovědností za provedení analýzy, mohou být u dodavatelského a partnerského přístupu těžko rozeznatelné.

Základní postup jak provádět analýzu rizik lze vyjádřit výčtem následujících kroků:

1. identifikace a ocenění aktiv
2. nalezení zranitelných míst
3. odhad pravděpodobností využití zranitelných míst
4. výpočet očekávaných (ročních) ztrát
5. přehled použitelných opatření a jejich cen
6. odhad ročních úspor aplikací zvolených opatření.

U dodavatelského přístupu je spolupráce mezi organizací a dodavatelem poměrně intenzivní. Rozhodnutí, zda provést detailní či jen základní analýzu, je na vedení firmy, nicméně pouze detailní analýza provedená podle vybrané metodiky může poskytnou podklady pro efektivní výběr a implementaci bezpečnostních opatření. Detailní analýza ve středně velké organizaci trvá zpravidla 3-5 měsíců a důvodem není ani tak rozsah, který je samozřejmě větší než u malých firem, ale rychlost odezvy od respondentů či recenzentů(schvalovatelů) výstupů z analýzy. Pro malou firmu jsou závěry shrnuty v jedné zprávě o analýze rizik, po které následuje návrh implementačního plánu. Prezentace takových závěrů je velmi rychlá

a jednoduchá a odezva na ni téměř okamžitá. Ve středních firmách se projevují první známky nutné byrokracie a pro schválení závěrů je nezbytné aby výstupní dokumenty prošli minimálně 3 pracovníci. Pokud je analýza prováděna dodavatelským či partnerským přístupem, jsou v týmu dva až tři externí pracovníci a stejný počet interních. Analýza prochází vždy napříč celou organizací a tomu odpovídá i zatížení dotčených pracovníků. Počet respondentů pro hodnocení dat se pohybuje mezi 5 až 15 uživateli a hodnocení hrozeb a zranitelností včetně zavedených protiopatření je úkolem pro 3-5 administrátorů sítě či další respondenty odpovědné za různé oblasti bezpečnosti (např. pracovník s odpovědností za fyzickou bezpečnost). Obsah dokumentace, která je výstupem z projektu analýzy rizik, je velmi podobný pro všechny typy organizací. Liší se jen rozsahem podpůrných reportů, které jsou zpravidla výstupem z použité metodiky, ale manažerský styl zpráv o aktivech a dopadech či o analýze rizik je shodný. Pro malé firmy je možné vytvořit jen jednu zprávu, ale pro střední organizace je vhodné závěry separovat minimálně do dvou dokumentů.

Analýza musí zabrat celý rozsah IS a její hloubka závisí na dostupných zdrojích a požadovaných výstupech. Hlavní rozdíl je v celkovém pohledu na bezpečnost. U partnerského přístupu se organizace sama učí, jak zabezpečit svoje informace. V druhém případě spoléhá ve výhledu do budoucnosti ve všem na dodavatele a jím dodané produkty či služby. Dodavatelské a vlastní přístupy jsou známé a běžně používané. Jednotlivé přístupy mají své nesporné výhody – přínos do budoucna, vyškolení vlastních pracovníků, přenos odpovědnosti na dodavatele, ale i nevýhody – cena, nejisté výstupy, nesystémové provádění ad-hoc. V následujících odstavcích jsou všechny tři přístupy podrobně popsány.

2.5.1 Dodavatelský přístup

Management organizace stále úzce spojuje bezpečnost informací s technologiemi a není tedy nic jednoduššího, než zadat odpovědnému řediteli úkol, aby vypsal výběrové řízení na dodavatele takového projektu. Pokud je však dostatečně kompetentní dodavatel, je tento přístup optimální pro organizaci, která nemá k dispozici dostatečné know-how mezi vlastními pracovníky nebo je nechce projektem vůbec zatěžovat. Určitá spolupráce zaměstnanců s dodavatelem projektu je však nezbytná. Zejména úvodní činnosti týkající se popisu systému a tvorby modelů aktiv se neobejdou bez aktivní spolupráce. Bezpodmínečně nutná je spolupráce při hodnocení aktiv, hrozeb a zranitelností. Zde analytik klade otázky, na které znají odpověď pouze pracovníci dané společnosti. V intenzitě spolupráce mohou být

dodavatelský a partnerský přístup téměř adekvátní. Hlavní pointa je ale ve zpracování výstupů a prezentace výsledků analýzy. Výstupy by měly mít vždy dvě formy:

- pro management – stručné zprávy;
- pro konkrétní pracovníky odpovědné za bezpečnost – podrobné reporty včetně tabulek a dalších příloh.

Výhodou dodavatelského přístupu je minimální zátěž pracovníků společnosti, protože kromě rozhovorů popřípadě vyplňování dotazníků dělá vše ostatní dodavatel projektu. Společnost tedy nepotřebuje nikoho, kdo ví, jak provádět analýzu rizik. Nemusí kupovat a studovat metodiky a hlavně nikdo z jejích pracovníků nemá odpovědnost za provedení analýzy. Zároveň však na konci projektu s posledním odborníkem od dodavatele odejde i know-how a vytvořené výstupy, jak již bylo zmíněno výše, se mohou stát nesrozumitelné. Pokud je analýza rizik jedním z prvních kroků velkého bezpečnostního projektu, nezřídka se stává, že celý projekt skončí nebo se minimálně na pár měsíců zastaví právě z toho důvodu, že v konečné zprávě jsou popsána tisíce doporučení, která potřebují dodatečnou interpretaci.

2.5.2 Vlastní přístup

Mnoho společností, které disponují vlastními odborníky, řeší bezpečnost informací svými silami. Jedná se o optimální řešení, pokud je k dispozici potřebné know-how podporované metodickými postupy či nástroji. V takovém případě provádějí analýzu rizik odborníci z vlastních řad, kteří kromě toho, že rozumí problematice, také znají informační systém organizace. Navíc je ze všech tří přístupů tento nejvíce nákladově efektivní.Bez vlastních odborníků vede volba tohoto přístupu k jasné zkáze. Neexistuje horší varianta, než když se koupí metodika nebo software na provedení analýzy rizik a vyškolí se jeden z pracovníku oddělení IT. Ten dostane kromě svých každodenních povinností za úkol provést postupně detailní analýzu všech částí informačního systému včetně zpracování výstupů pro management či auditora. Takový přístup je zcela špatný.

Během provádění detailní analýzy se (ne)zkušenost analytiků projeví zejména při rozhovorech s respondenty týkajících se zjišťování hodnoty informačních aktiv. Při takovém rozhovoru musí mít analytik nejen znalosti o daném systému a bezpečnosti obecně, ale musí být také trochu psychologem. Hodnotu informací lze vždy spolehlivě určit až tehdy, pokud se s nimi doopravdy něco negativního stane. Zejména rozhovory tvoří zásadní vstupy do

analýzy, ale stejně tak hodnocení hrozeb a slabin systému či samotný návrh bezpečnostních opatření. Zkušenost je při provádění těchto činností velmi cenná a nesprávná interpretace vstupů může významně znehodnotit závěry celé analýzy.

Jistou nevýhodou vlastního přístupu je možnost „zavírání očí“ ze strany analytiků, která je u ostatních variant eliminována externím pohledem dodavatele nebo konzultační firmy. Na druhou stranu je zde plno výhod plynoucích z využití vlastních odborníků. A pokud je navíc vlastní knot-how kombinované s kvalitní metodikou pro provedení analýzy, není pro organizaci lepší volba řešení.

2.5.3 Partnerský přístup

Tento přístup není využíván příliš často, i když pro většinu organizací by byl velkým přínosem. Jestliže není k dispozici vlastní knot-how, nezbývá nic jiného než zvolit dodavatelský nebo partnerský přístup. Ten druhý však v sobě skrývá jednu zásadní výhodu: organizace postupně přechází z dodavatelského přístupu k vlastnímu řešení. Bezpečnost informací protíná celou organizaci, zasahuje do drtivé většiny činností a procesů, a proto je vhodnější takové projekty provádět více interně než dodavatelsky. Partnerský přístup je pro dotčené pracovníky prakticky školení o bezpečnosti. Konzultační firmy, které tento přístup nabízejí, přenáší na pracovníky organizace své know-how a tomu by také měla odpovídat cena za projekt. Ta může dosáhnout i 75% dodavatelské varianty a je tak významnou nevýhodou a tím i častým důvodem k odmítnutí ze strany managementu. U detailní analýzy je celkové zatížení pracovníků společnosti srovnatelné s vlastním přístupem. Na provádění veškerých činností se významně podílí interní pracovníci pod vedením externího konzultanta, který má odpovědnost za projektové a metodické vedení. Spolupráce je velmi intenzivní po celý průběh projektu, ať už při rozhovorech o hodnocení aktiv nebo při zkoumání hrozeb a zranitelností. Nejintenzivnější spolupráce je však při tvorbě výstupů, které jsou ve skutečnosti tvořeny pod hlavičkou dané společnosti nikoli jako dodavatelský materiál. Zprávy včetně doporučení tvoří pracovníci sami a rozhodují o stylu i formě, aby byly všechny výstupy srozumitelné pro všechny zainteresované včetně managementu. Prakticky to může vypadat i tak, že externí analytik dodá šablonu dokumentu, kterou pracovníci doplní vlastními závěry formulovanými na základě výsledků analýzy.

Všechny tři přístupy jsou správné a vhodné, ale ne pro každého. Může rozhodovat velikost organizace, její obchodní zaměření nebo i počet uživatelů informačního systému. V praxi

se však postupně opouští od striktně dodavatelského řešení „na klíč“ a organizace stále více využívají svých pracovníků a vlastního know-how nebo externích konzultantů na jeho získání. Přístupy nemusí být aplikovány pouze na projekt analýzy rizik, ale i na celkové řešení bezpečnosti informací – zavádění a podporu ISMS. Při rozhodování o správném přístupu je nutné zohlednit zejména očekávané přínosy pro organizaci. Pokud jsou ve vlastních řadách k dispozici odborníci na informační bezpečnost, není nutné volit dodavatelský přístup. V opačném případě závisí na zvolené strategii do budoucna. Přenést odpovědnost na dodavatele a nechat si vše externě zajistit nemusí být špatná volba. Ale organizace by měla zvážit, zda není vhodnější zvolit partnerský přístup a postupně přebírat odpovědnost za bezpečnost svých dat a vychovávat si tak vlastní odborníky.

Tab. 2 Srovnání přístupů analyzování rizik

Dodavatelský přístup	
Výhody	Nevýhody
Nezatěžuje organizaci – pouze rozhovory a dotazníky Není nutné mít vlastní odborníky Odpovědnost je na straně dodavatele Není nutné kupovat metodiku či nástroje	Nesrozumitelné výstupy Vysoká cena S posledním expertem odejde i know-how
Vlastní přístup	
Výhody	Nevýhody
Všichni rozumí výstupům projektu Nejlevnější (i když se kupuje metodika nebo nástroje) Znalost interního prostředí Větší ochota vlastních zaměstnanců pracovat s kolegy než s externisty	Velmi zatěžuje organizaci Není jistota správného výsledku, pokud nejsou vlastní odborníci Neefektivní spotřeba zdrojů (pokud analýzu provádí např. správce sítě vedle svých každodenních povinností) „Vnitropodniková slepota“
Partnerský přístup	
Výhody	Nevýhody
Všichni rozumí výstupům projektu Není nutné mít vlastní odborníky Odpovědnost je na straně konzultanta Odborné vedení a dohled ze strany konzul-	Velmi zatěžuje organizaci (ale efektivně) Relativně vysoká cena Pracovník se v rámci projektu vyškolí a odejde

tanta Není nutné kupovat metodiku či nástroje Rozložení jednorázových nákladů do více projektů	

Tab. 3 Analýza rizik

Proces	Malá organizace do 15 zaměstnanců 1-2 úrovně vedení	Střední organizace do 150 zaměstnanců 3-5 úrovní vedení	Velká organizace nad 150 zaměstnanců 4 a více úrovní vedení
Analýza rizik	Nutné provést: ANO Čas: max. 1 měsíc Členové projektového týmu: jeden interní pracovník a/nebo konzultant Respondenti: max. 5 Výstupy: Zpráva o analýze rizik + Implementační plán	Nutné provést: ANO Čas: 3 - 5 měsíců Členové projektového týmu: 2-3 interní pracovníci a/nebo 2-3 konzultanti Respondenti: 5-20 Výstupy: Zpráva o aktivech a dopadech + Zpráva o analýze rizik + Implementační plán	Nutné provést: ANO Čas: 4 - 12 měsíců Členové projektového týmu: 2-n interních pracovníků a/nebo 2-3 konzultanti Respondenti: desítky Výstupy: Zpráva o aktivech a dopadech + Zpráva o analýze rizik + Implementační plán

Základní prvkem moderních metod je vybudování tzv. registru rizik, do kterého budou ukládány informace o všech bezpečnostních rizicích. Hlavním záměrem je vybudování a udržování aktuálního přehledu o známých bezpečnostních rizicích. Cílem je všechna zjištěná rizika evidovat, ohodnotit jejich významnost, určit osobu, která je odpovědná za zvládání rizika a sledovat postup zvládání rizika v čase. Tyto moderní metody řízení rizik především dovolují neustále kontrolovat aktuální situaci okolo bezpečnostních rizik a rychle zapracovávat nově zjištěná rizika. Při zvládání rizik má bezpečnostní manažer aktuální přehled o odpovědných osobách, o stavu řešení a v případě potřeby je schopen zpracovávaná rizika náležitým správným způsobem interně komunikovat. Všechny tyto informace

mohou být využity pro správné rozhodování v rámci managementu bezpečnosti, což vede ke snadnějšímu prosazování a vyšší efektivitě managementu bezpečnosti informací.

2.6 Plán implementace

Krokem logicky navazujícím na analýzu a poslední činností v části plánování je vytvoření Plánu implementace a následně Prohlášení o aplikovatelnosti. Bezpečnostní protiopatření by měla být vybrána na pokrytí zjištěných rizik a způsob jejich výběru je nezávislý na velikosti organizace. Velký rozdíl však je ve způsobu a zejména v rychlosti jejich prosazení.

Při výběru bezpečnostních opatření je vždy nutné zohlednit jejich dopad na uživatele a na procesy organizace. V malé firmě je možné jednouše a rychle změnit téměř jakýkoli proces, aby byl více bezpečný. Čím je organizace větší, tím je složitější měnit procesy a zavedené postupy. Proto je nutné při výběru protiopatření ve střední firmě více respektovat současný stav. Prohlášení o aplikovatelosti (opatření) je jedním z dokumentů nutných k certifikaci. Obsahuje informace o implementovaných opatřeních normy, případně dalších protiopatřeních navržených na pokrytí rizik. Hlavním cílem je dokumentovat rozhodnutí, proč dané protiopatření bylo či nebylo vybráno k zavedení. Pokud firma neplánuje být v budoucnosti certifikována, není nutné vytvářet samostatný dokument. Pro malou i střední firmu je plně dostačující, pokud se vhodným způsobem zaznamená rozhodnutí o výběru tak, aby i za několik měsíců bylo jasné, proč není nutné určité protiopatření implementovat.

Tab. 4 Plán implementace

Proces	Malá organizace do 15 zaměstnanců 1-2 úrovně vedení	Střední organizace do 150 zaměstnanců 3-5 úrovní vedení	Velká organizace nad 150 zaměstnanců 4 a více úrovní vedení
Výběr opatření a plán implementace	Protiopatření vyplývají z analýzy rizik Prosazuje: ředitel firmy	Protiopatření vyplývají z analýzy rizik Prosazuje: ředitel a vedoucí oddělení společně	Protiopatření vyplývají z analýzy rizik Prosazuje: podle významu protiopatření od vedení společnosti po vedoucí oddělení

2.7 Způsob implementace opatření a metody prosazení

Výběr okruhů opatření ISMS je podobný pro různě velké firmy. Velký rozdíl však je ve způsobu a zejména v rychlosti jejich prosazení. V malé firmě rozhoduje zpravidla ředitel o tom, kdo bude mít přístup k jakým datům. Ve větších společnostech je nutné vytvořit proces přidělování uživatelských oprávnění. V menších společnostech je běžné, že bezpečnostní ředitel (zpravidla ředitel firmy) rozhodne ráno o změně délky hesla z 6 na 9 znaků. Bezpečnostní administrátor (zpravidla správce sítě) protiopatření zavede ještě před obědem a všichni uživatelé si rádi změní heslo. Následující den je protiopatření v systému již zcela zavedeno a automaticky používáno a akceptováno. Taková rychlost implementace je typická pouze pro malé firmy. V ostatních organizacích je nutné vzít v úvahu akceptovatelnost protiopatření ze strany uživatelů a další souvislosti jejich realizace. Prosadit například změnu délky hesla vyžaduje revizi příslušné směrnice, zapojení několika administrátorů do práce a seznámení desítek uživatelů se změnou, například formou školení. Poté by měla následovat kontrola funkčnosti opatření.

Tab. 5 Způsob implementace

Proces	Malá organizace do 15 zaměstnanců 1-2 úrovně vedení	Střední organizace do 150 zaměstnanců 3-5 úrovní vedení	Velká organizace nad 150 zaměstnanců 4 a více úrovní vedení
Způsob implementace opatření	Okamžitě, rychle, efektivně, bez zbytečné administrativy	Podle významu protiopatření formou projektů nebo direktivním nařízením	Formou projektů

Tab. 6 Metody prosazení bezpečnosti

Proces	Malá organizace do 15 zaměstnanců 1-2 úrovně vedení	Střední organizace do 150 zaměstnanců 3-5 úrovní vedení	Velká organizace nad 150 zaměstnanců 4 a více úrovní vedení
Metody prosazení bezpečnosti	Direktivní – Osobní - Neformální Stručné pokyny (email, Intranet) a verbální působení na všechny zaměstnance	Direktivní – Neosobní - Formální Kombinace verbálních pokynů vedoucích a písemných organizačních.	Direktivní – Neosobní – Důsledně formální Písemné organizační pokyny Závazné a formální se-

		Závazné a formální seznámení s nařízeními	známení s nařízeními

2.8 Bezpečnostní dokumentace

V případě bezpečností dokumentace vznikají značné rozdíly v závislosti na velikosti společnosti, pro kterou je bezpečnostní dokumentace vytvářena a to zejména ve formě a míře detailnosti dokumentace bezpečnosti. Uvedené normy striktně nevyžadují papírovou formu dokumentace ani její pevnou strukturu, ale ponechávají na preferencích jednotlivých organizací, jakou formu a obsah zvolí. Přitom právě obava z přílišné formální administrativy nejčastěji odpuzuje organizace od zavádění doporučení těchto norem. Pracovníci menších organizací se osobně znají a velká část bezpečnosti je založena na jejich vzájemné důvěře. Není nutné proto v takovýchto organizacích vytvářet složitý systém politik, směrnic a postupů. Postačí stručné pravidlo, že bezpečnostní dokumentace je vedena ve sdílené složce elektronické pošty, definovat role a přístupy zodpovědných osob a nezbytné typy bezpečnostních dokumentů realizovat formou elektronických záznamů, obsahující stručný popis realizace daného pravidla, postupu nebo odpovědnosti. U větších organizací však již nutné zavádět podrobnější administrativní procedury, neboť existuje více oddělených rolí a odpovědností a také více definovaných pravidel. Tato administrativa je nutná, aby byly eliminovány činnosti, které se dějí při práci s daty jen tak, na „dobré slovo“. Pracovníci středně velkých firem se většinou také znají, ale jistá úroveň anonymity může být impulsem k tomu, že se někteří budou snažit bezpečnostní procedury obejít zejména, když nebudou přesněji definovány a kontrolovány. Rozsah a aktuálnost bezpečnostní dokumentace bývá často jedním z klíčových kritérií při posuzování kvality ISMS a míry dosažené shody s požadavky norem.

Tab. 7 Bezpečnostní dokumentace

Proces	Malá organizace do 15 zaměstnanců 1-2 úrovně vedení	Střední organizace do 150 zaměstnanců 3-5 úrovní vedení	Velká organizace nad 150 zaměstnanců 4 a více úrovní vedení
Bezpečnostní dokumentace	Bezpečnostní politika, některé směrnice, občas konkrétní postupy	Bezpečnostní politika a další dokumentace včetně směrnic, postupů, návodů apod.	Kompletní řízená bezpečnostní dokumentace a její průběžná (plánovaná)

			revize

2.9 Program zvyšování bezpečnostního povědomí

Další metodou jak zajistit prosazování bezpečnosti v organizacích využívajících podnikový informační systém patří program zvyšování bezpečnostního povědomí v organizacích. Tento krok je ve skutečnosti poměrně jednoduchá, levná a velice účinná metoda, která bývá bohužel mnohdy ve společnostech opomíjena. Má za cíl zvýšit u všech zaměstnanců informovanost jednak o obecných principech a souvislostech informační bezpečnosti a o konkrétních rizicích, opatřeních, odpovědnostech a pravidlech, vyplývajících ze zaváděného nebo již provozovaného ISMS. V čem vlastně spočívá „síla jednoduchosti“ tohoto opatření? Program je zaměřen na zaměstnance (a na externí spolupracující osoby apod.), kteří jsou často zdrojem bezpečnostních incidentů a kteří mohou, pokud jsou správně informováni, svým včasným jednáním šíření a škodám incidentů zabránit.

U menších společností postačí, pokud zvyšování bezpečnostního povědomí opřeme o stručné vstupní školení všech zaměstnanců a občasné projednání aktuálních bezpečnostních otázek dle potřeb organizace a vývoje nových potencionálních hrozeb (může být využito outsourcingu). U větších společností se zvyšují nároky na informovanost zaměstnanců a rozsah jejich znalostí o bezpečnostní problematice, realizovaných opatřeních, povinnostech a odpovědnostech z nich vyplývajících. Základní bezpečnostní školení se doporučuje realizovat pro všechny nové zaměstnance bez rozdílu. Zde je vhodné zaměřit se na zaměstnance déle a více také na popis a rozbor typických hrozeb a bezpečnostních incidentů. Při školení je vhodné používat odstrašujících příkladů včetně s upozorněním o případných sankcích při nedodržování definovaných pravidel. Tyto příklady mnohdy zaberou i tam, kde dobrá rada nepřesvědčí. Samozřejmě i u středně velkých organizací by nemělo být opomenuto informovat všechny zaměstnance o aktuálních hrozbách a opatřeních, např. formou zřízení centrálního informačního místa o bezpečnostních otázkách na firemním intranetu.

Tab. 8 Program zvyšování bezpečnostního povědomí

Proces	Malá organizace do 15 zaměstnanců	Střední organizace do 150 zaměstnanců	Velká organizace nad 150 zaměstnanců

	1-2 úrovně vedení	3-5 úrovní vedení	4 a více úrovní vedení
Program zvyšování bezpečnostního povědomí	Jednorázové informace dle potřeby. Bezpečnostní minimum součástí úvodního zaškolení	Nepravidelné pokyny a nařízení Bezpečnostní minimum součástí úvodního zaškolení. Specializovaná školení pro vybrané zaměstnance	Strukturovaný kontinuální vzdělávací program. Pravidelná specializovaná školení všech zaměstnanců

2.10 Informovanost zaměstnanců

Veškerá sebelepší hardwarová či softwarová opatření se ovšem zcela míjí účinkem, pokud selže nejslabší článek systému. Tím je bezesporu běžný uživatel. Nelze ale na jeho hlavu sesílat hromy a blesky, pokud mu organizace nepřipraví jasné podmínky a pokud tedy problematiku pohybu po internetu neřeší ve svých směrnicích či nařízeních. Takováto směrnice či nařízení, která má přehlednou a snadno zapamatovatelnou formu pro uživatele, dokáže řešit až 99 % mimořádných situací, do kterých se uživatel může dostat a je pro bezpečnost organizace rozhodně přínosnější než nějaká všeobjímající encyklopedie pravidle.

Nebezpečnost internetu nemusí být jako holý fakt, se kterým je nejlepší se smířit. Stačí totiž docela málo a noční můra jménem práce s internetem se může změnit v jednu z naprosto rutinních činností organice. Důležité proto je provádět školení zaměstnanců aktivní formou. Pokud je důležité, aby se zaměstnanci naučili dodržovat pravidla ochrany soukromí a bezpečnosti, pak je nutné prezentaci zpracovat tak, aby měli chuť při ní trávit čas. Pokud chceme, aby si zaměstnanci zapamatovali informace, které jim předložíme při školení je nutné experimentovat.

Jinými slovy, není vhodné spoléhat na typický přístup spočívající v tom, že na interní web budou nahrané statické informace a zaměstnanci dostanou pouze nařízení, aby uvedené stránky navštívili a s uveřejněnými informace se seznámili. Webové stránky naplněné pokyny, co mají a co nemají pracovníci dělat, nikdy zájem zaneprázdněných zaměstnanců neudrží. Proto je vhodné využívat multimediálních prvků a zahrnout je do oblasti školení a informovanosti zaměstnanců. Takovýmto přístupem je pozornost zaměstnance upoutána, seznámí se aktivní formou s informacemi týkající se bezpečnosti jejich práce

v podnikovém informačním systému, upozorní je na hrozby a způsoby jak těmto hrozbám čelit a zaměstnanci by si měli odnést základní znalosti a návyky pro následnou práci.

2.10.1 Způsoby školení

Samotný akt školení je do značné míry závislý na zvolené školicí technologii. Uvědomme si, že volba metody nemusí vždy splňovat očekávání posluchačů ve smyslu kvality předávaných informací a stylu výuky, neboť nároky na formy školení jsou často individuální. Je tedy důležité klást důraz na výběr skutečně vhodné vzdělávací techniky, případně i kombinace několika technik dohromady. V následujícím přehledu jsou shrnuty školící formy tvořící skupinu nejvíce účinných způsobů, jak zaměstnance aktivně seznámit s daným problémem.

Prezenční kurzy

Jedná se o typický způsob vzdělávání, jehož kladem je přímá interakce s přednášejícím, která umožňuje diskutovat o probírané problematice přímo. Záporem této metody jsou vyšší nároky na prostory a techniku i omezená kapacita pro počet posluchačů.

Elektronické kurzy

Představují velice moderní způsob vzdělávání, který je vázaný na výpočetní techniku. Tyto kurzy může najednou absolvovat neomezený počet studentů, kteří mají navíc možnost volby vlastního tempa školení. Výhodou jsou taktéž integrované testy, při kterých si mohou posluchači průběžně ověřovat nabyté znalosti.

Konzultace

Konzultace jsou praktickým vzděláváním spíše individuálního charakteru. Je zde kladen důraz na řešení konkrétní problematiky s odborníkem.

Coaching

Coaching je charakterizován jako dlouhodobé nabývání know-how při práci pod vedením odborníka. Výhodou je možnost zaučení se a řešení složitější problematiky. Nevýhodou je dlouhá doba, která je pro tento typ školení nutností, ale zvyšuje jeho finanční náročnost.

Bootcamp

Tento typ školení je zaměřen na intenzivní úvodní načerpání znalostí, kdy je nutné pojmout mnoho informací v relativně krátkém časovém horizontu.

2.11 Způsob zvládání rizik za provozu

Jedním z hlavních důvodů proč zavádět ISMS, je potřeba zajistit proces zvládání a řízení informačních rizik. Základem pro jejich úspěšné řízení je identifikace a analýza všech potencionálních rizik a následné rozhodnutí o způsobu jejich zvládání a sledování v čase. Účelem řízení rizik není veškerá identifikovaná rizika bezezbytku pokrýt, ale pokrýt zvolenými opatřeními pouze taková, u kterých je to efektivní. Ostatní rizika může organizace akceptovat a sledovat, některá může přenést na jinou organizaci, případně je pojistit. Pouze pokud organizace zná a sleduje všechna rizika související se zabezpečením informací a adekvátně rozhoduje o způsobu jejich zvládání, potom může prohlásit, že tyto rizika řídí a má je pod kontrolou. Tyto zásady jsou společné pro všechny velikosti a typy organizací. Otázkou je, jak se s nimi malé nebo velké organizace efektivně vypořádají. U těchto firem bude většinou velikost negativního dopadu bezpečnostního incidentu i pravděpodobnost jeho výskytu průměrně nižší než u velkých společností. Vedení těchto firem by mělo mít tendence více rizika akceptovat a přesunout svůj zájem spíše do oblasti jejich sledování a efektivního zvládání případných bezpečnostních incidentů. Pro sledování nových typů rizik a rozpoznání bezpečnostních incidentů je nutné aktivovat generování záznamů o nejdůležitějších bezpečnostních událostech (v papírové i elektronické formě) a tyto záznamy vyhodnocovat. Mezi takové záznamy patří minimálně záznamy o přístupech do budov a zabezpečených místností, přihlašování a odhlašování do počítačových systémů a citlivých aplikací, přístupy a manipulace se zvlášť citlivými informacemi apod. Řada těchto záznamů je generována automaticky po instalaci jednotlivých systémů.

Na co se však často zapomíná, je jejich systematické ukládání, zabezpečení a vyhodnocování. U menších organizací bude proces řízení a zvládání rizik realizován neformálním způsobem, bez stanovení speciálních pravomocí a oddělení rolí. Zde je vhodné a účelné dosáhnout shodné úrovně informovanosti a pravomocí u všech zaměstnanců. Pro větší společnosti je vhodné definovat postupy, oddělit pravomoci a provádět namátkové revize tohoto procesu. Pro získání přehledu o způsobu a důslednosti plnění povinností při zvládání rizik a incidentů je namístě zřídit evidenci závažných hrozeb a zranitelností a způsobů jejich pokrytí.

Tab. 9 Způsob zvládání rizik za provozu

Proces	Malá organizace	Střední organizace	Velká organizace

	do 15 zaměstnanců 1-2 úrovně vedení	do 150 zaměstnanců 3-5 úrovní vedení	nad 150 zaměstnanců 4 a více úrovní vedení
Způsob zvládání rizik za provozu	Neformální proces, bez speciálních postupů a pravomocí. Pokrytí a kontrola bezprostředně po identifikaci.	Formální proces s rámcově stanoveným postupem a odpovědnostmi. Revize zvládání rizik nepravidelná, dle potřeby.	Formálně řízený proces s předem stanovenými postupy a pravomocemi. Pravidelné analýzy a kontroly zvládání rizik.

2.12 Nároky na provoz opatření a zajištění bezpečnosti

Součástí plánu zvládání rizik je i sledování nároků na provoz jednotlivých opatření a celkového zajištění bezpečnosti. Zatímco u malých firem není potřeba plánovat ani vyhrazovat samostatný rozpočet, neboť případný nákup a provoz nezbytných opatření je operativně schválen ředitelem a hrazen dle aktuálních potřeb organizace, u středních a velkých firem je nezbytné provádět alespoň rámcové plánování potřebných finančních i lidských zdrojů. Z hlediska preferencí při výběru opatření hrají celkové nároky na jejich zavedení a provoz hlavní roli. Zatímco pro malé organizace není překážkou pružně zavádět administrativní a personální opatření i za cenu vyšších požadavků lidské zdrojů, úskalím však bývají finanční náklady na pořízení složitých technologických opatření. U velkých společností lze tyto preference vysledovat obráceně, neboť pro ně bývá snazší pružně zavést nové technologické opatření, než jej nahradit administrativními či organizačními změnami. V případě preferencí středně velkých firem je stav logicky někde uprostřed. Záleží na pružnosti řízení, technologické úrovni a znalostech pracovníků firmy, k jakým typům opatření se budou přiklánět více.

Tab. 10 Nároky na provoz opatření a zajištění bezpečnosti

Proces	Malá organizace do 15 zaměstnanců 1-2 úrovně vedení	Střední organizace do 150 zaměstnanců 3-5 úrovní vedení	Velká organizace nad 150 zaměstnanců 4 a více úrovní vedení
Nároky na provoz opatření a zajištění bezpečnosti	Krátkodobé plánování. Není separátní rozpočet.	Krátkodobé a střednědobé plánování Rozpočet v rámci IT/IS Prosazuje se outsour-	Dlouhodobé plánování Individuální rozpočet Běžné využití out-

	Externí spolupráce není obvyklá.	cing.	sourcingu

2.13 Zavedení opatření Havarijních plánů a Postupů řešení bezpečnostních incidentů

Poslední důležitou oblastí opatření při zavádění a provozu ISMS je tvorba a údržba Havarijních plánů a Postupů řešení bezpečnostních incidentů. Stejně jako v případě ostatních formálních postupů i zde platí, že pro malé organizace je neefektivní vypracovávat a udržovat podrobné formální havarijní plány. Pro obnovu systémů jim plně postačí vytvoření stručného univerzálního havarijního plánu pro všechny možné případy havárie, který bude obsahovat postup bezpečného vypnutí a restartu technického vybavení a serverů, jednoduchý záznam výsledné konfigurace technologií a aplikací, postup obnovení dat ze záložních médií a seznam kontaktů na interní a externí osoby, které mohou pomoci při výskytu havárie nebo závažného bezpečnostního incidentu. Tyto havarijní postupy by měly být alespoň jednorázově otestovány a poté postačí testy opakovat až při zásadní změně používaných technologií a služeb. U větších organizací je vhodné rozšířit zmíněný havarijní plán i o popis kroků instalace jednotlivých částí informačního systému a obnovy dat a aplikací ze záložních médií. U komplikovanějších informačních systémů je třeba rozlišit obnovu klíčových aktiv od ostatních a tomu přizpůsobit priority v havarijním plánování. Pro výběr strategie způsobu obnovy a nastavení priorit je nejlépe realizovat analýzu dopadů na činnosti organizace. Pokud byla správně realizována analýza rizik, lze informace o negativních dopadech nedostupnosti jednotlivých aktiv nalézt tam. Na základě těchto výsledků je vypracován strukturovaný havarijní plán obnovy, obsahující varianty postupu dle specifikovaných typů havarijních stavů. Takovýto plán je nezbytné pravidelně testovat a aktualizovat a na základě výsledků testů (v porovnání s cíly obnovy) vylepšovat.

Tab. 11 Havarijní plány

Proces	Malá organizace do 15 zaměstnanců 1-2 úrovně vedení	Střední organizace do 150 zaměstnanců 3-5 úrovní vedení	Velká organizace nad 150 zaměstnanců 4 a více úrovní vedení

Havarijní plány	Zpravidla řada neformálních havarijních postupů pro jednotlivá aktiva.	Formální univerzální havarijní plán Postupy zvládání bezpečnostních incidentů	Provedena analýza dopadů Strukturované havarijní plány Formální postupy zvládání bezpečnostních incidentů

2.14 Kontrola provedených opatření

Žádný proces, opatření nebo činnost sledující cíl a plnící určitou funkci v systému není možné udržet, řídit a zlepšovat v čase, pokud se neprovádí periodická kontrola jejich funkčnosti, efektivity a souladu s požadovaným stavem.

Systému řízení bezpečnosti informací (ISMS - Information Security Management System) slouží k vybudování, provozování, sledování, řízení a zlepšování bezpečnosti informací v organizacích. Jedná se o systematický a celistvý proces v čase, který má hlavní kroky a opatření plánování a provádění. Jako zpětná vazba, podávající vedení organizace a dalším odpovědným osobám informace o tom do jaké míry byly naplněny zásady a cíle bezpečnostní politiky informací slouží další fáze, kterou můžeme označit jako Kontrolování. Tato část nejen podává informace o naplnění zásad a cílů bezpečnosti ale také má za úkol informovat, zda byla zavedena všechna bezpečností opatření a zda fungují dostatečně spolehlivě a efektivně. Známé rčení „důvěřuj ale prověřuj“ je v oblasti bezpečnosti informací nanejvýš namístě a s trochou nadsázky lze dodat, že pokud „Opakování je matkou moudrosti“, pak „Prověřování je otcem bezpečnosti“ a jejich společným potomkem je právě tato etapa „Kontrolování“.

2.15 Monitoring provozu

Monitoring provozu klíčových prvků IS a ochranných opatření je základním zdrojem informací pro kontrolu jejich funkčnosti a spolehlivosti. Pokud organizace zavádějící ISMS plánuje v budoucnu i jeho certifikaci, musí vytvářet a shromažďovat záznamy o fungování alespoň těch opatření, která jsou uvedena v Prohlášení o aplikovatelnosti (ty budou předmětem auditu). Bohužel ne všechny typy opatření samy automaticky generují záznamy o činnosti a tak je nezbytné přistoupit i v prostředí malých a středních firem k nepopulárnímu ručnímu generování záznamů u takových opatření, která tuto vlastnost nemají (především

organizační a administrativní). Nemusí se přitom zdaleka jednat o únavnou administrativu, protože rozsah a složitost opatření, zvláště u malých a středních firem, nebývá nijak velký. Příkladem toho, co postačí pro audit funkčnosti opatření „bezpečnostní školení uživatelů IS“, jsou seznamy účastníků školení a datum a předmět školení. Pochopitelně pouze za jedno opatření - školení pracovníků, nicméně časová náročnost se pohybuje v rámci jednotek minut. Pro monitoring postačí u malých organizacích výchozí nastavení logování dle standardní instalace většiny produktů a jejich ruční namátková kontrola pracovníkem, pověřeným na půl úvazku základními bezpečnostními povinnostmi. U větších organizací, je již vzhledem ke komplikovanosti IS infrastruktury nedostatečné spolehnout se pouze na namátkové ruční kontroly log souborů a je třeba využít automatických nástrojů pro jejich filtrování a vyhodnocování nestandardních událostí např. pomocí skriptů nebo dodatečných produktů. Podrobnější bezpečnostní monitoring se vyplatí aktivovat pouze krátkodobě, při podezření na výskyt bezpečnostního incidentu.

2.16 Testování funkčnosti opatření

Abychom při provozu IS pomyslnému riziku předešli, je třeba uvedené pasivní metody kontroly doplnit i o aktivní a preventivní způsoby, jakými jsou např. aplikační kontroly chyb výpočtů a zpracování dat nebo testování zranitelností, případně penetrační testování systémů. Zatímco komplikovanější a časově i finančně náročnější penetračního testování má za cíl simulaci reálných útoků ze zvoleného prostředí a identifikaci možných negativních dopadů na IS, bezesporu jednodušším, rychlejším a levnějším způsobem testování odolnosti vůči útokům je vyhledání a testování zranitelností provozovaných produktů.

Oba způsoby mohou být prováděny z interní sítě, nebo častěji z externího prostředí – zpravidla Internetu nebo bezdrátových sítí, což by měly být v případě malých a středních firem hlavní oblasti prevence proti útokům na IS. Protože se v případě penetračního testování

jedná o vysoce specializovanou činnost, vyžadující detailní znalosti o technikách a nástrojích hackingu, stejně jako o bezpečnostních slabinách jednotlivých produktů a komunikačních protokolů, bývá tento úkol svěřován specializovaným externím firmám, které mají dostatečné profesní zázemí pro jejich kvalifikovanou realizaci. Naproti tomu testování zranitelností je proces, který si mnohdy mohou počítačově gramotní uživatelé udělat sami, pomocí dostupných programů nebo využít specializovaných webových služeb (např. QualysGuard®).

Pro malé organizace lze testování zranitelností doporučit, pokud využívají permanentní připojení k externím sítím nebo provozují bezdrátovou LAN v husté zástavbě. Pro střední organizace by testování zranitelností klíčových serverů a služeb IS mělo být samozřejmostí, alespoň po implementaci bezpečnostních opatření a před rutinním provozem komunikačních spojů. Pokud střední organizace provozují citlivá data a aplikace na Internetu, mohou zvážit realizaci penetračního testování nebo podrobný technický bezpečnostní audit konfigurace klíčových prvků IS a bezpečnostních opatření jako např. Firewallu, DNS[7] nebo Internetového aplikačního nebo databázového serveru či routeru na rozhraní LAN[8]/WAN[9].

[7] DNS – Domain Name Server

[8] LAN – Local Area Network

[9] WAN – Wide Area Network

Tab. 12 Monitoring IS a testovaní funkčnosti opatření

Proces	Malá organizace do 15 zaměstnanců 1-2 úrovně vedení	Střední organizace do 150 zaměstnanců 3-5 úrovní vedení	Velká organizace nad 150 zaměstnanců 4 a více úrovní vedení
Monitoring IS a testování funkčnosti opatření	Namátkový monitoring provozu IS a vyhodnocování logů a záznamů událostí (v papírové i el. podobě). Otestování zranitelností u systémů připojených k Internetu.	Pravidelný monitoring a vyhodnocování logů a záznamů událostí (v papírové i elektronické podobě). Otestování zranitelností u systémů připojeným k externím subjektům (třetím stranám).	Centralizovaný a automatizovaný monitoring provozu ICT a vyhodnocování logů a záznamů událostí. Pravidelné testování zranitelností doplněné o penetrační testování (simulaci „hacker“ útoků). Bezpečnostní analýza klíčových prvků systému.

2.17 Audit a kontrola bezpečnostních opatření

Spolu s monitorováním provozu, testováním zranitelností a technicky zaměřeným auditem konfigurace ICT, je další metodou kontroly implementace a provozu IS / ISMS realizace Auditu a kontrol bezpečnosti IS. Obecně lze říci, že audit opatření musí být prováděn v každém typu a velikosti organizace, která provozuje systém řízení nad opatřeními, jinak by neexistovala zpětná vazba o stavu reality vůči plánu a návrhu požadovaného cílového stavu. Každý typ auditu by se měl řídit pravidly ISO 19011:2002 a měl by probíhat dle schváleného ročního i operativního plánu. Je zřejmé, že takovéto formální „harakiri“ malé a střední organizace dobrovolně nepodstoupí a že přichází v úvahu pouze v případě potřeby certifikace systému řízení.

V případě ISMS by měl audit zahrnovat kontrolu funkčních bezpečnostních i řídících opatření ISMS, která jsou deklarována v Prohlášení o aplikovatelnosti a popsána v bezpečnostní dokumentaci. Audit by měl ověřit jak jsou realizována v praxi. U malých organizací není třeba vytvářet samostatná oddělení nebo pracovní funkce interního auditora, ale je nutné i v malé organizaci funkci interního auditora dedikovat, alespoň jako přidruženou pracovní náplň

nějakému zaměstnanci. Jednou ročně je nezbytné projednání zjištěných výsledků plánovaných auditů i namátkových kontrol s majitelem / ředitelem organizace a následně se všemi zaměstnanci.

V případě středně velké organizace se již doporučuje zvážit existenci samostatné funkce interního auditora, kterému připadne i funkce bezpečnostního auditora. I v tomto případě má za úkol provádění plánovaných i namátkových kontrol dle ročního i operativního plánu auditu, který je sestavován s přihlédnutím k největším rizikům a nálezům předchozích auditů. Pro dosažení vyšší odborné úrovně a komplexnosti výsledků kontroly je doporučeno realizovat alespoň jednou ročně přehledový srovnávací audit stavu ISMS, vzhledem k požadavkům ISO 27001, s účastí jednoho externího odborného konzultanta.

Tab. 13 Audit a kontrola bezpečnostních opatření

Proces	Malá organizace do 15 zaměstnanců 1-2 úrovně vedení	Střední organizace do 150 zaměstnanců 3-5 úrovní vedení	Velká organizace nad 150 zaměstnanců 4 a více úrovní vedení
Audit a kontrola bezpečnostních opatření	Audit opatření včetně ISMS dle dokumentace a plánu auditu (v případě certifikace ISMS). Iniciuje ředitel, provádí vybraný pracovník jako rozšíření standardní pracovní náplně. Namátková interní kontrola stavu	Audit opatření včetně ISMS dle dokumentace a plánu auditu (v případě certifikace ISMS). Bezpečnostní technický audit nastavení klíčových ICT systémů. Namátková interní kontrola stavu opatření.	Pravidelná interní kontrola a audit bezpečnostních a ISMS opatření, dle interních směrnic a politik (vyhrazený interní auditor). Průběžný bezpečnostní technický audit konfigurace ICT a bezpečnostních záplat.

2.18 Revize adekvátnosti a efektivnosti ISMS

Kromě ověření funkčnosti, spolehlivosti a úplnosti funkčních i řídících opatření je třeba přibližně jednou ročně zrevidovat rozsah, adekvátnost a efektivnost celého ISMS ve vztahu k potřebám, cílům a prostředí organizace. Výsledek této celkové revize ISMS by měl být stejně jako souhrnné výsledky auditů opatření projednán s vedením organizace a pořízeny záznamy o přijatých závěrech. Jelikož se jedná o činnost vyžadující široký přehled a značné zkušenosti z oblasti bezpečnosti informací a implementace ISMS v organizacích, musejí

se malé i střední organizace spolehnout na pomoc externích specialistů, stejně jako v případě analýzy informačních rizik v etapě Plánování.

Tab. 14 Revize adekvátnosti a efektivnosti systému řízení bezpečnosti

Proces	Malá organizace do 15 zaměstnanců 1-2 úrovně vedení	Střední organizace do 150 zaměstnanců 3-5 úrovní vedení	Velká organizace nad 150 zaměstnanců 4 a více úrovní vedení
Revize adekvátnosti a efektivnosti systému řízení bezpečnosti	Rámcová revize procesu ISMS a vyhodnocení aktuálnosti, efektivnosti a adekvátnosti opatření. 1 denní workshop s využitím externího konzultanta.	Roční podrobná revize procesu ISMS a stavu opatření s využitím externího konzultanta. Porovnávání stávajících opatření s novými trendy a vývojem hrozeb a zranitelností.	Srovnávací audit stavu ISMS s normou. Průběžné přehodnocování míry zbytkových a akceptovaných rizik vůči cílům organizace. Revize podnětů na zlepšení efektivnosti.

2.19 Zlepšování a vyhodnocení

Je bezpečnost informací problematikou spíše technologickou nebo manažerskou? Jak zajistit její dlouhodobou stabilitu a konzistentnost v čase, navzdory měnícím se vnitřním i vnějším podmínkám a prostředí organizace? Co je hlavním motorem procesu zavádění, údržby a zlepšování bezpečnosti informací, kde začíná a kde vlastně končí? Lze bezpečnost informací měřit a má smysl její certifikace? Tyto otázky se pokusím zodpovědět v následujících odstavcích.

V předchozích částech byly popsány nejobsáhlejší a zdánlivě i nejdůležitější kroky procesu zavádění a využívání systému řízení bezpečnosti informací (ISMS). V každém z dílů byly postupně nastíněny hlavní činnosti jednotlivých fází Plánování, Provádění a Kontrolování, s přihlédnutím na specifické prostředí společností podle různých velikostí. Po těchto částech logicky navazuje čtvrtá část, uzavírající tento kruh řízení bezpečnosti a to fáze Jednání, představující nejdůležitější rozhodovací krok celého procesu. Součástí procesu Jednání je i celkové zhodnocení významu řízení bezpečnosti informačního systému a případná následná certifikace.

Hlavním významem čtvrté fáze Jednání je tedy vyhodnotit výsledky auditu a kontrol funkčnosti bezpečnostních opatření i procesu samotného a nastartovat další cyklus, ve kterém budou naplánovány, zavedeny, zkontrolovány a opět vyhodnoceny nápravná a preventivní opatření k zajištění požadovaného stavu bezpečnosti v čase. Provedení každé fáze následujícího cyklu je vhodné také naplánovat, zrealizovat, poté zkontrolovat a doplnit.

2.20 Vyhodnocení fáze Kontroluj

Základním předpokladem pro správné rozhodnutí „co a jak dál“ by vždy měly být co nejpřesnější a nejúplnější informace o aktuálním stavu a cílech organizace. Informace o aktuálním stavu týkající se monitoringu provozu, evidence chyb a bezpečnostních incidentů, výsledků testování funkčnosti a spolehlivosti implementovaných opatření, výsledků testování zranitelností a výsledky interních i externích auditů poskytuje předcházející fáze Kontroluj. Vyhodnocení těchto informací může provádět v menších firmách pracovník pověřený činností bezpečnostního managera na částečný úvazek, jako přidruženou činnost ke své pracovní náplni. Výsledky svého šetření by měl minimálně jednou ročně předložit majiteli, případně řediteli organizace a společně provést jejich analýzu a vyhodnocení. U středních a velkých organizací se již vyplatí přidat do tohoto kroku také revizi návrhů a možných zlepšení bezpečnosti informací i procesu řízení bezpečnosti informačních systémů, jejichž evidenci zajišťuje fórum pro bezpečnost informací, složené ze zástupců uživatelů, dodavatelů a odborných rolí delegovaných pro oblast bezpečnosti informací v organizaci. V rámci procesu řízení rizik musí být prováděno pravidelné přehodnocování úrovně zbytkových a přenesených rizik, s ohledem na změny v organizaci, technologiích, podnikatelských cílech a vnějších událostech a hrozbách.

Tab. 15 Vyhodnocování řízení bezpečnosti

Proces	Malá organizace do 15 zaměstnanců 1-2 úrovně vedení	Střední organizace do 150 zaměstnanců 3-5 úrovní vedení	Velká organizace nad 150 zaměstnanců 4 a více úrovní vedení
Vyhodnocení fáze Kontroluj	Revize zejména bezpečnostních incidentů, chyb a průběhu jejich řešení (dle potřeby).	Pravidelná revize incidentů, chyb a průběhu jejich řešení. Revize penetračních a dalších typů testů.	Proces průběžné revize výsledků monitoringu provozu, incidentů, chyb a průběhu jejich řešení.

	Revize penetračního a zkušebního testování, pokud bylo realizováno. Revize výsledků ročního auditu.	Revize výsledků auditu. Revize nápadů a podnětů ke zlepšení. Revize adekvátnosti a efektivnosti ISMS.	Revize penetračních testů a technických auditů konfigurace systémů. Revize nápadů a podnětů ke zlepšení. Revize adekvátnosti a efektivnosti ISMS.

2.21 Identifikace a analýza neshod

I když byla revize výsledků auditu zahrnuta již do předcházejícího kroku, je vhodné tuto činnost popsat podrobněji. Identifikace a analýza neshod má za úkol rozebrat výsledky interního i případného externího auditu a posoudit, které z nalezených neshod jsou skutečné, které pouze potenciální a vyřadit nesprávně identifikované neshody. Toto rozhodnutí je opět vhodné zaevidovat formou tabulky. Nakonec je pro odstranění skutečně identifikovaných neshod třeba navrhnout nápravná opatření a pro zabránění opakovaného výskytu skutečných i potencionálních neshod v budoucnu je třeba navrhnout preventivní opatření. U malých organizací provede tuto analýzu neshod majitel, případně ředitel organizace, ve spolupráci s pracovníkem pověřeným funkcí bezpečnostního managera. S výsledným rozhodnutím je vhodné seznámit všechny zaměstnance. Implementace těchto rozhodnutí bývá velmi rychlá a flexibilní. Pokud malá firma usiluje o certifikaci v řízení bezpečnosti, je vhodné obrátit se pro pomoc na externího konzultanta, případně zrealizovat srovnávací audit procesu ISMS vzhledem k ISO 27001 externí specializovanou firmou a s její pomocí navrhnout potřebná nápravná opatření pro dosažení souladu.

U středních a velkých firem bude interpretace výsledků auditů i návrh nápravných a preventivních opatření komplikovanější a formální proces, řízený pracovníky interního auditu ve spolupráci s dalšími zainteresovanými odbornými pracovníky organizace. Při přípravě na certifikaci ISMS je vhodné sáhnou pro pomoc externích odborníků, pokud takoví nejsou ve vlastních řadách.

Tab. 16 Identifikace a analýza neshod

Proces	Malá organizace do 15 zaměstnanců 1-2 úrovně vedení	Střední organizace do 150 zaměstnanců 3-5 úrovní vedení	Velká organizace nad 150 zaměstnanců 4 a více úrovní vedení
Identifikace a analýza neshod	Identifikace a evidence možností zlepšování, reálných neshod a potenciálních problémů. Interpretace a okamžitý návrh opatření ředitelem / majitelem.	Identifikace a evidence možností zlepšování, reálných neshod a potenciálních problémů. Interpretace výsledků kontrol interním auditem s využitím externích odborníků. Jednoduchý projekt pro návrh opatření.	Identifikace a řízená evidence možností zlepšování, neshod a potenciálních problémů. Vícestupňový proces analýzy neshod bezp. auditem a jejich interpretace bezp. ředitelem. Kompletní projekt pro návrh a testování opatření.

2.22 Nápravná a preventivní opatření

Nápravná opatření slouží k odstranění skutečně nalezených nedostatků a chyb, spojených s implementací a provozem ISMS a k zabránění jejich dalšímu trvání (opakování). Jedná se například o neúplnou implementaci opatření zvolených v Prohlášení o aplikovatelnosti opatření, o chybějící dokumentaci těchto opatření, o nedostatečné proškolení pracovníků zainteresovaných v procesu ISMS apod. Preventivní opatření jsou vybírána s cílem zabránit výskytu potencionálních neshod v budoucnu, tedy za účelem eliminace příčin, které by mohly vést ke vzniku reálné nežádoucí situace a reálné neshody. Příkladem takové potencionální neshody může být například nedodržení oddělení rolí u některých činností a opatření ISMS nebo nedůsledné provádění potřebných monitorovacích a kontrolních činností. Pro malé organizace je typická rychlá praktická změna bez byrokratických průtahů a příklon především k organizačním a personálním opatřením, jejichž „pořízení a zavedení“ bývá pro majitele malých firem nejpřijatelnější. Pro střední a velké organizace, není již hledisko nákladů na pořízení a zavedení opatření tak palčivé jako pro malé organizace a bude při jejich výběru více rozhodovat jeho účinnost a pokrytí nalezených nedostatků.

Tab. 17 Nápravná a preventivní opatření

Proces	Malá organizace do 15 zaměstnanců 1-2 úrovně vedení	Střední organizace do 150 zaměstnanců 3-5 úrovní vedení	Velká organizace nad 150 zaměstnanců 4 a více úrovní vedení
Nápravná a preventivní opatření	Přednostní výběr jednoduchých organizačních a personálních opatření, bez nutnosti investic. Rychlé zavedení dostupných opatření do praxe.	Výběr organizačních opatření podpořených technologiemi a nástroji. Testování opatření před uvedením do praxe. Aktualizace bezpečnostní dokumentace.	Výběr a implementace opatření formou projektu Primárně výběr robustních a automatizovaných opatření s podrobným testování a sledováním účinnosti a přizpůsobení organizaci. Řízená aktualizace bezpečnostní dokumentace.

2.23 Zavést systém řízení bezpečnosti IS?

Uvedeným přehledem byly popsány všechny hlavní kroky tvořící pilíře procesu řízení bezpečnosti informačních systémů, tak jak jsou definovány normou ISO 27001, která se v roce 2006 stane také součástí soustavy norem ČSN. Existuje jednoznačná odpověď na otázku zda zavádět systém řízení bezpečnosti proces v prostředí firem? Pokud existence, poslání nebo strategické cíle těchto firem závisejí na zajištění některého z „parametrů“ bezpečnosti informací – tj. na dostupnosti, důvěrnosti nebo integritě informací a dat, je odpověď jednoznačně Ano. Zavedení systému řízení bezpečnosti samo o sobě nezaručuje kvalitativní nárůst některého z parametrů bezpečnosti informací, ale představuje odzkoušený a celosvětově uznávaný postup, jak dosáhnout bezpečnosti informací adekvátní požadavkům a cílům organizace a jak jí udržovat a efektivně zlepšovat v čase, za pomocí ochranných opatření, odpovědností, činností a řídících a kontrolních procesů. Vzhledem ke své formalizaci tak poskytuje zdokumentovanou inventuru činností a odpovědností, které se ve velké míře stejně v organizacích provádějí, většinou ale nesystematicky a nedůsledně, což v praxi způsobuje vážná rizika a bezpečnostní incidenty.

2.24 Certifikovat systém řízení bezpečnosti IS?

Odpověď zda certifikovat systém řízení bezpečnosti IS prozatím tak jednoznačná není. Zavedení systému řízení bezpečnosti má prokazatelně pozitivní efekt. Vzhledem k narůstající závislosti firem na informačních systémech, jejich propojování a sdílení informací v rámci nejrůznějších aplikací a vzhledem k požadavkům platné národní a nadnárodní legislativy na zabezpečení informací a dat je správně zavedený a provozovaný systém řízení bezpečnosti chápán jako vysoký stupeň záruky adekvátní ochrany dat. Lze ale míru zabezpečení informací v IS organizace objektivně měřit? Celková bezpečnost informací v organizacích je zajišťována kombinací technologických opatření, fyzických, personálních a administrativních, které by měly být implementovány v rozsahu a kvalitě odpovídající prostředí a potřebám každé jednotlivé organizace. Jednou z možností jak hodnotit míru bezpečnosti informací je posouzení kvality procesu řízení bezpečnosti informací, vyhodnocením míry souladu s požadavky na tento proces dle normy ISO 27001. Pro firmy představuje proces přípravy a samotné certifikace akreditovanou certifikační autoritou nemalou investici, kterou je třeba manažersky a ekonomicky zvážit. Pokud firma podniká v sektoru, kde je důvěryhodnost vysoce ceněným faktorem a podmínkou úspěšných obchodních vztahů, může být pro takovou firmu užitečné realizovat certifikaci bezpečnosti informací jako další důkaz kvality řízení k certifikátu QMS nebo EMS (dle ISO 9001:2000 a ISO 14001:1996). Certifikace řízení bezpečnosti IS do prostředí firem, kde je již certifikován jiný systém řízení, je méně náročnou variantou. Ve světě existují již téměř dva tisíce (stav k 11/2005) certifikátů ISMS dle normy BS 7799:2000, která je předchůdcem ISO/IEC 27001:2005. Vlna certifikací ISMS je teprve před námi a jeví se velice pravděpodobné, že se prosadí ve stejné míře jako dnes certifikace QMS a EMS.

Je třeba přiznat, že zavedení a provoz systému řízení bezpečnosti IS přináší zaměstnancům i vedení firem nárůst režijních kapacit. To ale zejména proto, že donutí odpovědné osoby vykonávat činnosti, které bývají v běžné praxi opomíjeny a nebo v horších případech nejsou vůbec delegovány. Bezpečnost informací v organizacích je problematikou technologickou stejně jako manažerskou. Jedna část nemůže účinně a efektivně fungovat bez druhé. Správná konfigurace bezpečnostních produktů a bezpečnostních opatření poskytuje většinou dobrou úroveň ochrany informací. Bez zajištění systému řízení bezpečnosti IS a řídícího procesu jsou však časem znehodnoceny na úroveň zapomenuté zrezlé závory s utrženou cedulí „Zákaz vstupu“, kolem které vede vyšlapaná stezka do zakázaného prostoru.

2.25 Příklady úrovní implementace řízení bezpečnosti v organizacích

	Typická úroveň řízení ISM	Stav implementace a provozu ISM (dle dosažené úrovně řízení)	Rozsah bezpečnostní dokumentace (dle dosažené úrovně řízení ISM)*
Kvalitativní úrovně implementace a provozu řízení bezpečnosti informací (ISM) v organizacích	Re-certifikovaný ISMS (bezpečnost informací je prokazatelně dlouhodobě řízena dle BS 7799-2:2002)	Organizace opakovaně provádí re-certifikaci provozovaného ISMS dle standardu BS 7799-2:2002. Aktualizuje stav opatření a dokumentace ISMS dle změn v podnikatelských cílech, prostředí a procesech organizace a dle aktualizovaných výsledků analýzy rizik .	Aktualizace rozsahu ISMS a výsledků analýzy rizik. Pravidelná revize Bezpečnostní politiky informací. Aktualizace návrhu opatření, prohlášení o aplikovatelnosti a implementačního plánu opatření a procesů ISMS. Pravidelná revize a aktualizace bezpečnostní dokumentace opatření a procesů ISMS.
	Certifikovaný ISMS (bezpečnost informací je prokazatelně zavedena a řízena dle BS 7799-2:2002)	Organizace se rozhodla certifikovat ISMS a realizovala kontrolní pre-certifikační audit, na základě jehož výsledků zavedla chybějící opatření a dopracovala procesy a dokumentaci dle požadavků BS 7799-2. Poté přistoupila k certifikaci ISMS.	Zpráva o výsledcích pre-certifikačního auditu ISMS. Plán řízení zdrojů ISMS. Kompletní provozní dokumentace opatření ISMS. Kompletní řídící a kontrolní dokumentace ISMS. Zpráva o certifikaci ISMS. Certifikát ISMS dle BS 7799-2:2002.
	Implementovaný ISMS v souladu s normou (bezpečnost informací je systematicky řízena a zlepšována, rizika jsou řízena a zvládána)	V organizaci je implementován a provozován ISMS v souladu s normou ISO/IEC 17799:2000. Rozsah ISMS, jeho řízení, procesy a odpovědnosti jsou definovány. Jsou identifikována a zvládána všechna rizika a zavedena opatření schválená k implementaci. Bezpečnostní dokumentace pokrývá všechny oblasti ISMS, nicméně nemusí být zcela dle požadavků certifikace (revize, aktualizace)	Působnost (rozsah) ISMS. Plán zvládání rizik . Prohlášení o aplikovatelnosti opatření. Strategie BCP + DRP a IRH dokumenty a postupy. Základní provozní a řídící dokumentace opatření ISMS. Záznamy o provozu, využívání a zlepšování ISMS. Evidence bezpečnostních incidentů a následných reakcí a opatření. Výsledky auditu a evidence nalezených neshod, nápravných a preventivních opatření.
	Částečně implementovaný ISMS (koncepce bezpečnosti a plán zavedení ISMS je neúplná, nebo teprve postupně realizována)	Je přijata koncepce bezpečnosti managementem. Byla provedena analýza rizik a návrh opatření. Zavedena pouze vybraná opatření (priorita, zdroje). ISMS není řádně zdokumentován, nejsou realizovány veškeré řídící procesy (zejména kontrolní a nápravné) a řízeny zdroje ISMS. Není prováděn audit ISMS.	Zpráva o aktivech a dopadech. Zpráva o analýze rizik. Návrh opatření a implementační plán, případně Prohlášení o aplikovatelnosti opatření. Částečná provozní a řídící dokumentace procesů ISMS. Nekompletní záznamy o provozu , fungování řídících procesů ISMS a evidence bezpečnostních incidentů. Dílčí projekty/plány implementace prioritních opatření.
	Plánovaný ISMS (zavedení systému řízení bezpečnosti a zvládání rizik ve fázi přípravy a plánování)	Je přijata koncepce řízení bezpečnosti managementem na základě cíle zvládání rizik . Je vytvořen rámcový plán/projekt ISMS a případně delegován rozpočet na bezpečnost. Je vytvářeno bezpečnostní povědomí v organizaci.	Strategie bezpečnosti. Bezpečnostní politika informací. Program zvyšování bezpečnostního povědomí. Výsledky přehledové (případně detailní) analýzy rizik. Rámcový projekt bezpečnosti informací. Plán implementace ISMS a zvládání rizik.
	Ad-hoc ISM (řízení bezpečnosti informací bez znalosti a systematického zvládání bezpečnostních rizik)	Neexistuje systematická koncepce bezpečnosti, ISM „je řízena přes neznalost rizik". Částečné bezpečnostní povědomí některých pracovníků. Zavedeny vybrané dílčí opatření a procesy ISM spolu s technickými opatřeními.	Neexistuje řízená systematická bezpečnostní dokumentace. Pouze dílčí interní dokumentace pokrývající určité oblasti nebo systémy. Možný výskyt neprovázané dodavatelské dokumentace některých systémů.
	Nezavedený ISM (neprobíhá řízení bezpečnosti informací)	Neexistuje žádné bezpečnostní povědomí, řízení ani koncepce. Realizovány jsou pouze dílčí technické opatření, bez potřebných ISM procesů a dokumentace.	Interní bezpečnostní dokumentace v oblasti bezpečnosti informací neexistuje. Možný výskyt neprovázané dodavatelské dokumentace některých systémů.

Obr. 2 Příklady typických úrovní implementace řízení bezpečnosti v IS

II. PRAKTICKÁ ČÁST

3 KROKY A POSTUPY ŘÍZENÍ BEZPEČNOSTI V INFORMAČNÍCH SYSTÉMECH

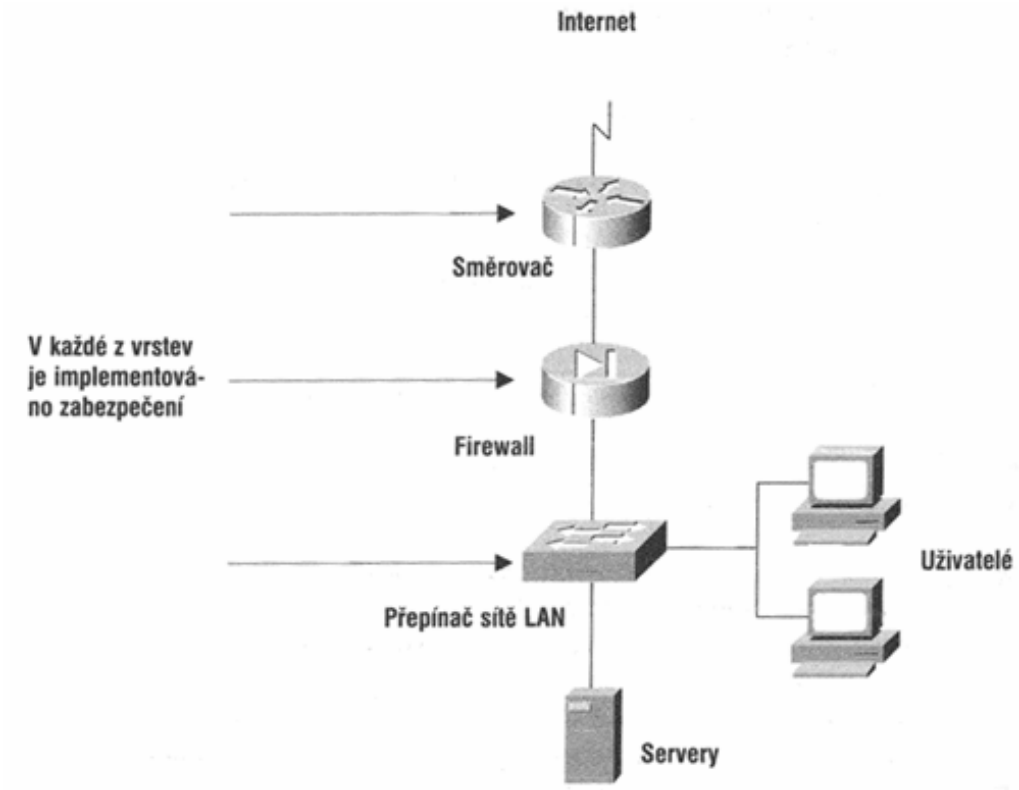
Tato část je věnována bezpečnostním opatřením, které by měly vést podnik pro zajištění vhodného řízení a ochrany před bezpečnostními riziky. Opatření zahrnují jak speciální ochranná zařízení a software, tak nutné pracovní postupy a zásady, které musí dodržovat všichni zaměstnanci daného podniku, kteří se jakýmkoliv způsobem zapojují do práce s podnikovým informačním systémem. Před samotným posouzením preventivních prostředků je třeba upřímně říci, že neexistují ideální bezpečné komunikační systémy a nemá také smysl zavádět tolik ochran, až se práce s počítači stane jednoduše neefektivní. Především je nutné vědět, že hardware a software nejsou hlavním zdrojem nebezpečí pro síť, protože nejslabším článkem je vždy tzv. lidský faktor, neboli uživatelé komunikačního systému. Z různých průzkumů vyplývá, že 75% problémů spojených s počítačovou bezpečností ve firmách nebo úřadech způsobují jejich zaměstnanci, přičemž 20% problémů je důsledkem nedostatečné loajality nebo přímo nesolidnosti zaměstnanců.

Vedoucí firemní pracovníci jsou tedy povinni provádět důslednou kontrolu svých podřízených a věnovat pozornost práci osob, které jsou odpovědné za komunikační systém. V současné době zaručují řešení dodávaná renomovanými dodavateli vyhovující úroveň bezpečnosti, problém je spíše v tom, že lidé, kteří instalují programové vybavení a konfigurují síť a jsou zároveň odpovědní za aktualizaci programů, jednoduše svoje povinnosti podceňují. Další věc je přesvědčování všech pracovníků v podniku, že bezpečnost je klíčovou záležitostí jak pro samotnou organizaci, tak pro ně osobně. Nejúčinnějším prostředkem, který umožňuje přesvědčit všechny zaměstnance o prioritě tohoto problému, jsou školení. Tyto kurzy není nutné provádět s velkými finančními a časovými náklady, nemusí se také jednat o několikadenní kurzy informatiky. Jde spíše o to, aby zaměstnanci pochopili možnosti programů, které daný podnik využívá, věděli jaká hesla mají používat a v neposlední řadě je nutné pracovníkům objasnit, které internetové stránky mohou v rámci pracovní doby prohlížet. Důležitá je také otázka jednoznačného určení postihů (včetně služebních), pro zaměstnance v případě, že tato doporučení nebudou dodržovat. Všem musí být jasné, že ani nejlepší ochrana proti vnějšímu útoku (např. útok viru staženého z internetu) bude k ničemu, pokud bude docházet k problémům v rámci organizace. Dále je nutné pracovníkům objasnit, že rozhodujícím faktorem,který může zamezit zdárnému útoku zvenčí, není brána - firewall, ale především jejich chování. Deset kroků pro vyšší bezpečnost

Při popisu jednotlivých kroků budeme vycházet z předpokladu, že v rámci bezpečnostních zásad jsou definovány požadavky, podmínky a standardy.

3.1 Základní principy návrhu zabezpečení

Bezpečnost sítě má mnoho stránek a různých úhlů pohledu, záleží vždy na tom, jakým potencionálním útokům a hrozbám je systém vystaven. Důležité je budovat zabezpečení pomocí vrstvené bezpečnosti. Tím je vytvořeno hned několik opěrných bezpečnostních bodů, které zajišťují vrstvenou bezpečnost a ochranu před možnými útoky na celý informační systém podniku.



Obr. 3 Místa vrstveného zabezpečení sítě

3.2 Využívání brány firewall v internetovém připojení

Internet je mimořádně zajímavé a podnětné prostředí, která láká k objevování a zkoumání. Bývá často přirovnáván k Divokému Západu a dalším obrovským mezníkům. Díky internetu mají jednotlivý uživatelé k dispozici takové množství informací, že po letech provozu již připojení k sítí není pro osoby a firmy jen výhodou ale nezbytností. Pokud ale některé informace vystavíme do prostřední internetu, mohou se najednou kriticky důležité a důvěrné

informace ocitnou v ohrožení a zaútočit na ně může kdokoli a odkudkoli. Cílem instalace serverové brány firewall je znemožnit osobám zvenčí pronikání do sítě prostřednictvím internetu. Následně je třeba chránit jednotlivé počítače spuštěním funkce „brána - firewall“ systému Windows XP Professional. Serverová brána firewall tvoří velmi důležitou první obrannou linii, která chrání lokální sítě před útoky zvenčí tím, že odmítá nevyžádanou komunikaci. Serverovou bránu firewall je možné si představit jako telefonistku, která spojuje pouze lidi, které její šéf označil jako vhodné a ostatním říká, že „šéf je mimo“. Serverová brána firewall blokuje celý provoz, který není mezi internetem a sítí organizace dovolen. Mohou také maskovat adresy počítačů, které se nacházejí za bránou, takže díky tomu jsou počítače připojené do sítě pro osoby zvenčí neviditelné. Osobní firewall integrovaný do systému Windows XP Professional, funguje podobně jako serverová brána firewall, ale chrání pouze jediný počítač, ve kterém je osobní firewall nainstalován. Představuje vhodný doplněk serverové brány firewall, ale vzhledem k izolované činnosti není vyhovující ochranou celé sítě.

Hackeři jednající v rozporu se zákony mohou vyhledat síť organizace a případně zaměřit útok na jednotlivé počítače, aniž by věděli, na koho konkrétně útočí. Je to stejné jako náhodná volba čísel z telefonního seznamu. Pokud má organizace trvalé (stálé nebo pevné) připojení k internetu, existuje jistá pravděpodobnost, že jeho síť bude předmětem náhodných sond nebo útoků několikrát denně. Pokud útočníci mají k dispozici správnou adresu počítače, mohou využít mezer v programovém vybavení (zvláště pokud se neprovádí jeho aktualizace) nebo se mohou pokusit o překonání hesla tak, aby získali přístup. Samotný firewall nemůže zaručit bezpečnost, ale je dobrou zbraní první obranné linie. Z toho důvodu je nezbytně nutné vzít v úvahu, zda je daný počítačový systém organizace vybavený firewallem. Jestliže tedy bude mít organizace pevné připojení k internetu, ale nebude vytvořená ochranná bariéra vnitřní sítě, lze sice zdánlivě ušetřit, avšak odstranění problémů, které se brzy v nechráněné síti objeví, bude stát víc než nejdražší firewall. Proto je vhodné při výběrových řízeních na dodávku sítě nebo zavedení připojení k internetu uvést, že je nutné instalovat serverovou bránu firewall a rovněž určit úkoly, které tento firewall musí plnit. Veškerý provoz mezi sítí organizace a internetem prochází firewallem a díky tomu je chráněna celá síť. Firewall kontroluje každý příchozí a odchozí paket a buď jej přijme nebo odmítne na základě předem definovaných zásad. Firewall lze např. nastavit tak, aby přijímal daný druh provozu spojeného s elektronickou poštou a komunikací s webovou sítí, a

na druhé straně odmítal jiné typy provozu. V praxi to znamená, že díky příslušnému programovému vybavení firewall lze určit, že naši zaměstnanci nebudou moci prohlížet www stránky s pornografickým nebo zábavným obsahem, budou mít však bez problémů přístup k takovým stránkám, které jsou pro jejich práci nezbytné.

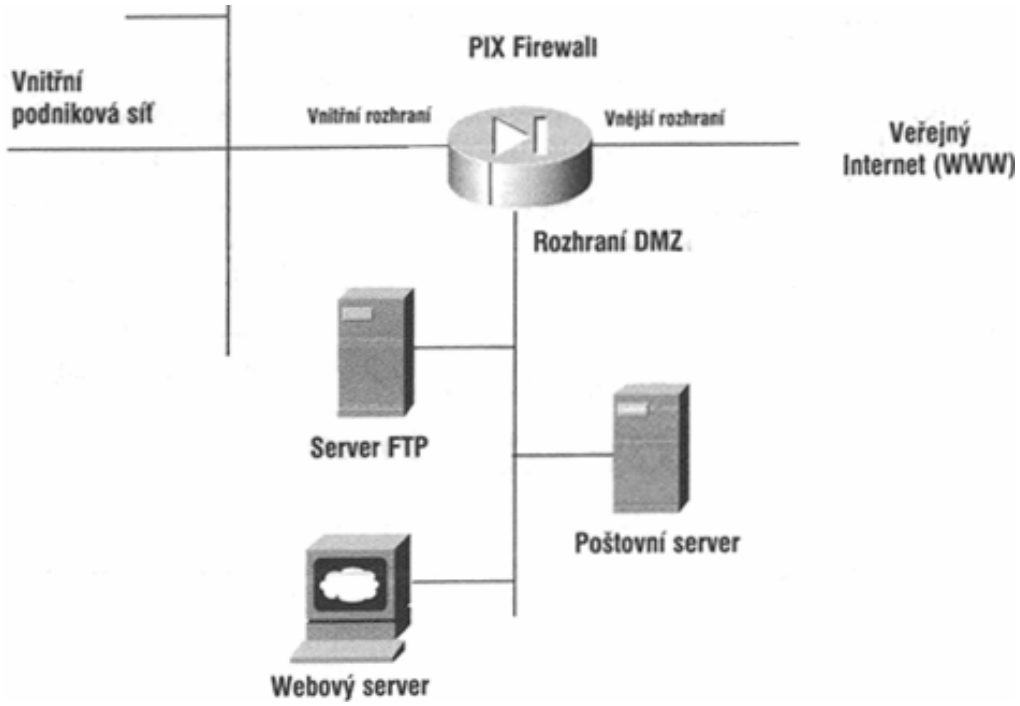
Instalace serverové brány firewall do sítě je v zásadě velmi jednoduché. Firewall se zapojuje mezi kabelový/DSL modem či jiné připojení k internetu a počítače patřící do místní sítě. Nastavení serverové brány firewall je poměrně snadné, obvykle lze nastavení provádět pomocí internetového prohlížeče. Firewally jsou obvykle nastaveny tak, aby blokovaly celý provoz přicházející z internetu; potom tedy zbývá jen určit, jaký druh provozu, pokud vůbec, bude povolen. Osobní softwarové firewally pracují na konkrétním počítači a kontrolují pouze provoz tohoto počítače, tzn. příchozí i odchozí. Pokud se k internetu připojuje jednotlivý počítač, lze využít softwarový firewall. Firewall internetového připojení instalovaný do systému Windows XP Professional je silný softwarový nástroj. Uživatelé předchozích verzí systému Windows by se však měli zaměřit na využití komerčních softwarových bran firewall například od výrobců Computer Associates, McAfee, Symantec nebo Zonelabs. Pokud jeden nebo více počítačů ve společnosti využívá telefonické připojení k internetu, musí být každý z těchto počítačů chráněný softwarovou bránou firewall.

3.2.1 Co firewall nemůže zajistit

Je třeba si uvědomit, že Firewall je pouze první obrannou linií. Nezávisle na své efektivnosti nezajišťuje ochranu před: škodlivým provozem, který neprochází přes firewall, útoky vyvolanými po narušení bezpečnosti síťového provozu (např. pokud se útočníkovi podaří využít mezeru v programovém vybavení operačního systému nebo pokud k získání přístupu do počítače došlo zevnitř společnosti), provozem probíhajícím legálními kanály, mnoha viry, včetně virů, jejichž snahou je vytvořit mezery v ochranách.

3.2.2 Využívání demilitarizované zóny

Demilitarizovaná zóna (DMZ) je rozhraní, umístěné mezi důvěryhodným segmentem sítě (firemní sítí) a nedůvěryhodným segmentem sítě (Internetem). Tím obě sítě fyzicky odděluje a izoluje, propojuje je pouze pomocní množiny jistých pravidel, definovaných ve firewallu. Toto fyzické oddělení demilitarizované zóny je velice důležité avšak v mnoha organizacích opomíjené.



Obr. 4 Umístění demilitarizované zóny a její význam

Největší výhodou této zóny je tedy izolace veškerých neznámých požadavků z Internetu do zvláštních serverů v zóně. To znamená, že tento potenciálně nebezpečný provoz se již nedostane do vnitřní sítě organizace. Provoz firewallu s rozhraním demilitarizované zóny (DMZ) má další výhody, lépe totiž je možné monitorovat, co všechno se v síti děje, a tím pádem ji dostáváme pod bezpečnější kontrol:

- audit provozu v demilitarizované zóně,
- umístění detekčního systému IDS (Intrusion Detection System) v DMZ,
- omezení aktualizací směrovaní mezi těmito rozhraními,
- umístění názvového serveru DNS v zóně DMZ.

3.3 Využívání hranových směrovačů

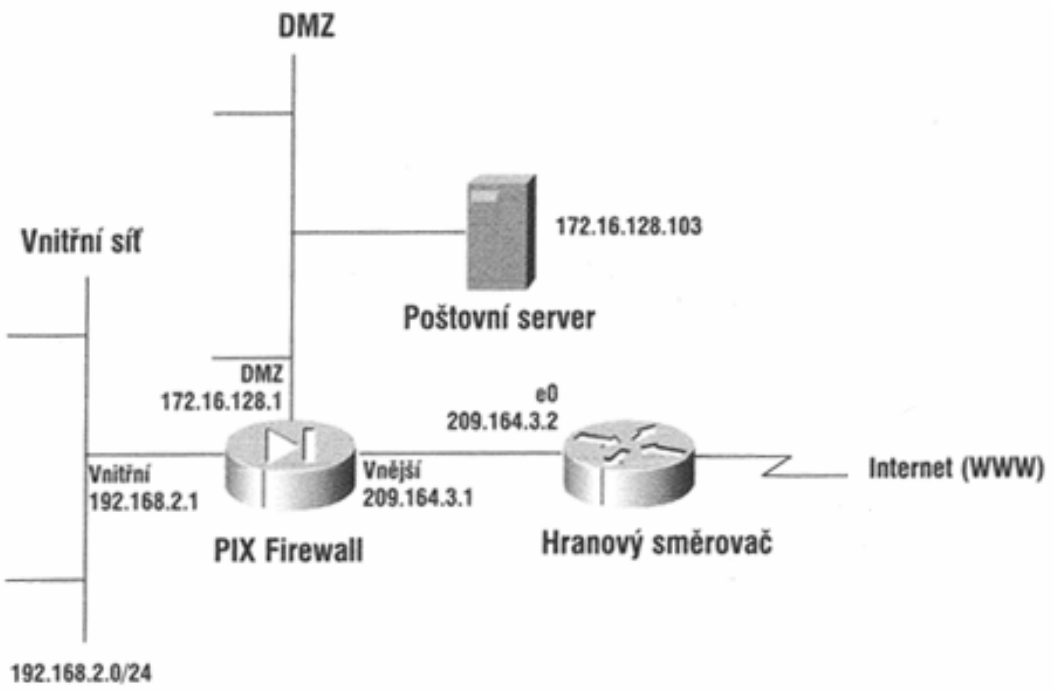
Životně důležitou součástí celkového řešení bezpečnosti je síťový firewall, který sleduje síťový provoz při průchodu obvodem sítě a uvaluje na něj omezení podle platných zásad zabezpečení. Firewall ale není všemocný nástroj v souvislosti v zavádění bezpečnosti. Další prvek vrstvené bezpečnosti je směrovač. Směrovač, který spojuje síť s Internetem, se označuje jako hranový směrovač a tvoří vnější obvod sítě. Obvodové směšovače by se mě-

ly umísťovat na každou hranici sítě, například také mezi privátní sítě, intranety, extranety a veřejným internetem. Firewally pak nejčastěji slouží k oddělení vnitřní a vnější sítě.

Hranový směrovač zajišťuje vlastní připojení firemní sítě do internetu a řada lidi na něj proto pohlíží jako na jakési nezbytné zařízení, bez něhož by v sítí nemohli být.

3.3.1 Hranový směrovač jako hrdlo sítě

Hranový směrovač v roli hrdla sítě vede ke zvýšení bezpečnosti, protože omezuje datové toky mezi vnitřní sítí a internetem. Význam hranového směšovače v roli hrdla sítě spočívá v tom, že snadno zabraňuje v přístupu ke konkrétním zařízením a aplikacím, a to bez nepříznivého vlivu na výkonnost sítě. Výkonnost sítě zůstává za normálních podmínek a okolností prakticky nezměněná proto, že směrovač musí obsah paketů IP číst tak jako tak a podle hlavičky se rozhoduje, kam má paket předat dále. Díky přístupovým seznamům je dosti velký stupeň kontroly a velké možnosti filtrování. Na obrázku je uveden příklad takovýchto pravidel a vhodně zvolené umístění směšovače v roli hrdla sítě.



Obr. 5 Hranový směrovač jako hrdlo sítě

3.4 Stahování aktualizací

Je třeba stahovat a instalovat nejnovější aktualizace programového vybavení tak, abychom byli vždy jeden krok napřed před hackery a měli jistotu, že náš počítačový systém je odolný

proti útokům, které využívají dávno identifikované a odstraněné mezery v software. Útočnici vyhledávají a využívají chyby a mezery v rozšířeném software pro zábavu, zisk a občas pouze proto, aby způsobili zmatek. Když firma Microsoft zjistí mezeru v programovém vybavení, uveřejní aktualizaci ke stažení z internetu. V průběhu doby se základní architektura počítačových systémů stává stále dokonalejší a bezpečnější. Např. systém Microsoft Windows XP Professional je bezpečnější než systém Windows 95 a Windows 98, protože tvoření nových verzí software nemá pouze komerční cíle, ale jde především o maximální zvýšení bezpečnosti uživatelů. Mnohým virovým infekcím se lze tímto způsobem úspěšně vyhnout. V některých případech zdařených útoků existovaly aktualizace, které mohly předejít vzniklým problémům, ale uživatelé je neinstalovali. Nejnovější aktualizace produktů firmy Microsoft (a mnoha jiných) je velmi snadné získat a instalovat. V případě systému Windows je třeba přejít na stránku www.windowsupdate.com, a vyhledat aktualizaci, webová stránka automaticky stáhne a instaluje všechny prvky nutné k aktualizaci počítače. Pokud má uživatel k dispozici pevné vysokorychlostní připojení, může využít funkce Automatické aktualizace, která je dostupná v mnoha novějších verzích systému Windows, včetně Windows XP Professional. Systém Windows může monitorovat dostupnost aktualizací, stahovat je a instalovat – vše automaticky na pozadí. Funkce Automatická aktualizace je součástí Centra zabezpečení, o nesprávném stavu Vás bude informovat bublina v oznamovací oblasti. V Centru zabezpečení klepněte na odkaz Spravovat nastavení zabezpečení pro: Automatické aktualizace Následně je nutné určit, jakým způsobem má být prohlížení a stahování aktualizace provedeno.

3.5 Využívání aktuálních antivirových programů

Stejně jako je nutné aktualizovat programy využívané při práci, je třeba také předcházet pronikání virů, a to především prostřednictvím instalace antivirových programů a jejich pravidelné aktualizaci. Podezřelé soubory se nedoporučuje otevírat. Viry mohou být také nasazeny na webových stránkách nebo v e-mailech připravených tak, aby vypadaly jako webové stránky (např. v e-mailových zprávách ve formátu HTML).

Je důležité dodržovat následující postupy, které mohou zásadně omezit riziko napadení virem:

- Koupit a instalovat antivirové programy a provádět jejich aktualizaci. Antivirové programy je nutné instalovat ve všech počítačích připojených k síti.

- Protože se každý měsíc objevují stovky nových virů, je nutné všechny antivirové programy pravidelně aktualizovat. Antivirové programy bez nejnovějších nejsou efektivní, proto je nutné instalovat program, který si bude automaticky stahovat definice a svoje aktualizace z internetu.
- Pokud má organizace pevné vysokorychlostní připojení, potom je možné většinu programů nastavit tak, aby program procházel a stahoval nové definice virů na pozadí.
- Pokud se používá telefonické připojení, je nutné pravidelně kontrolovat, zda proběhla aktualizace antivirového programu.
- Jako doplňkový preventivní prostředek je možné na serveru elektronické pošty instalovat program, který prochází každou část elektronické pošty, která přichází do společnosti.
- Neotevírat podezřelé soubory. Zlaté bezpečnostní pravidlo říká, že není vhodné otevírat jakékoliv soubory připojené k e-mailové zprávě odeslané z neznámého, podezřelého nebo nedůvěryhodného zdroje, a to nezávisle na tom, jak lákavě e-mailová zpráva vypadá. Stejnou opatrnost je třeba zachovávat při prohlížení webových stránek nebo při stahování souborů z internetu.
- Soubory je možné stahovat pouze z důvěryhodných stránek. Většina antivirových programů prochází soubory uložené na pevném disku nezávisle na tom, odkud pocházejí (např. z webové stránky, z elektronické pošty, z diskety nebo ze sítě). Je třeba se vždy přesvědčit, zda je v rámci antivirového programu spuštěna automatická ochrana.
- Je nutné si uvědomit, že existují také falešné poplachy, které se týkají virů a objevují se v e-mailových zprávách (podobně jako řetězové dopisy a jiné dokumenty) jsou stejně rozšířené jako samotné viry. Než takový poplach předáme dalším osobám, doporučuje se zjistit z důvěryhodného zdroje, jako je například výrobce používaného antivirového programu, zda je poplach skutečný. Jiné uživatele je vhodné vyzývat k tomu, aby zachovávali podobnou opatrnost.

3.6 Blokování spamu

Spam jsou nevyžádané komerční zprávy, jejichž počet stále roste. Asi polovinu všech e-mailových zpráv rozesílaných po celém světě tvoří spam. Některé z těchto zpráv jsou nositeli virů, jiné mají urážlivý obsah. Průměrný zaměstnanec věnuje denně asi jednu hodinu e-mailové poště, takže je jasné, že spam zjevně snižuje produktivitu jeho práce. Dalším aspektem výše popsaných rizik je znemožnění komunikace s vnějším světem. Pokud je totiž systém infikovaný virem a další je dobře chráněný, nastane situace, kdy server chráněné sítě odmítne e-mailové zprávy z napadené sítě, protože identifikuje „nakaženou adresu“. Proto je nutné využívat obranných programů proti spamu jak na straně serveru tak i na straně uživatelů. Výše uvedené preventivní prostředky umožňují minimalizaci daných typů ohrožení.

3.7 Používání silných hesel

Neexistuje žádný důvod, proč bychom měli hackerům či jiným osobám, které chtějí zaútočit na náš systém zvnějšku, usnadňovat přístup do systému. K tomu ale právě dochází, pokud si pracovníci vybírají hesla, která lze snadno odhadnout nebo překonat. Zaměstnance je nutné poučit, aby si vybírali tzv. silná hesla a pravidelně je obměňovali. Hesla jsou nejrozšířenější metodou prověřování uživatelů. Hesla se používají nejčastěji, protože jejich použití je nejjednodušší, na druhé straně však může snadno dojít k jejich zneužití. I ta nejlepší zabezpečení na světě jsou k ničemu, pokud někdo nepovolaný bude znát heslo. Především je nutné pochopit, proč jsou některá hesla tzv. slabá.

Nejčastější chyby při používání hesel:

- Nepoužívání hesel není dobrou taktikou především z toho důvodu, že každý pracovník může přijít k nezajištěnému počítači a přihlásit se.
- Hesla typu: jméno, název uživatele nebo název firmy je snadné odhadnout.
- Hesla ve formě povšechně používaných slov lze snadno odhadnout pomocí automatizovaných „slovníkových útoků“.
- Typická hesla, jako např. „heslo“ nebo „1234“ je také snadné odhadnout.
- Hesla napsaná na papírku vedle počítače lze rychle najít.

- Heslo, které se několik měsíců nemění, lze odhadnout nebo překonat bez vědomí uživatele.
- Heslo, které zná ještě někdo další, je vždy mezerou v obraně.
- Slabá hesla také často obsahují typické záměny za písmena, např. nahrazování písmena „i“ znakem „!“, písmena „s“ znakem „$“ nebo číslem „5“ nebo písmena „o“ číslem „0“ atp. Moderní metody překonávání hesel s takovým záměnami pracují, takže jejich použití samotné heslo ani trochu neposiluje. Jinak řečeno: pokud je daná substituce smysluplná pro uživatele, bude pravděpodobně stejně pochopitelná pro útočníka.

Silná hesla mají následující charakteristické vlastnosti:

- Musí obsahovat minimálně osm znaků, čím více tím lépe.
- Musí obsahovat malá a velká písmena, číslice a symboly (např. ` ~! @ # $ % ^ & *) _ + - = { } | [ ] \: "; '< >?,. / nebo znak mezery).
- Tato hesla je nutné pravidelně měnit (90 dní je vyhovující frekvence, ale doporučujeme 42 dní); nové heslo se musí zásadně lišit od předchozího hesla (Hesla s čitatelem nejsou silná, např. Heslo001, Heslo002, Heslo003).
- Podle těchto zásad by silné heslo vypadalo např. následovně: J*p2leO4>F.

Zásady týkající se hesel je vhodné předem určit s ohledem na bezpečnost a pohodlí. Příliš přísná pravidla pro tvorbu hesel pro všechny zaměstnance mohou způsobit, že si pracovníci svoje hesla zapíšou na papír. Doporučuje se tedy raději vytvořit různá pravidla pro jednotlivé typy uživatelů a systémů, např. silnější hesla vyžadovat do správců sítí nebo zaměstnanců personálního oddělení. Při zpracování pravidel je však třeba vždy počítat se sklonem lidí podlehnout různým sociotechnickým trikům a různými lidskými slabostmi. Uživatelům je proto nutné vysvětlit, že s heslem musí nakládat jako s klíčem od kanceláře, tzn. není možné jej nechat ležet všem na očích ani předávat jiným osobám. V každé organizaci bude podezřelé, pokud řadový zaměstnanec požádá o klíč od pracovny ředitele. Žádost o poskytnutí hesla kolegy či kolegyně je proto nutné považovat za stejně podezřelé. Ze stejného důvodu se doporučuje vhodné nastavení spořiče obrazovky tak, aby počítač, který se řádově několik minut nepoužívá, požadoval opětovné zadání hesla při dalším zahájení práce. Tento postup znemožní využití přihlášeného počítače, pokud se jeho uživatel vzdálí od

svého pracovního stolu. V rámci firmy je vhodné stanovit zásady pro práci s hesly, ve kterých budou uvedeny základní povinnosti související s používáním a prací s hesly.

3.8 Zajištění fyzické bezpečnosti

Ochrana stolních počítačů a omezení fyzického přístupu k pracovním stanicím a dokumentům je podstatnou součástí činnosti při zajišťování bezpečnosti dat. V těchto případech se využívají dobře známé metody: zámky, alarmy, zamykání skříněk na dokumenty, evidence návštěvníků a označování přístrojového vybavení. Ne všechny katastrofy způsobují útočníci zvenčí, kteří působí prostřednictvím internetu. Občas může být náhodné vloupání ještě horší. Ani ten nejlepší firewall není ochranou proti člověku, který pracuje se serverem nebo lokální pracovní stanicí. Níže uvádíme seznam kontrolních činností, jejichž provedení by mělo být zárukou fyzické bezpečnosti úředních informací a počítačů. Je třeba:

- Určit bezpečnostní hranice kolem chráněné zóny s využitím (podle potřeby) příček, dveří s automatickým zavírání, uzamykatelných dveří, alarmů a ochranných bariér.
- Ujistit se, že vstupy zvenčí jsou hlídané a přicházející a odcházející hosté jsou evidováni a identifikováni.
- Pokud je to možné, maximálně omezit možnost přístupu do důležitých zón (např.místnost serverů nebo místnost, kde se nacházejí osobní údaje zaměstnanců). Pravidelně kontrolovat, kdo má přístup do důležitých zón. Do těchto prostor by měli mít přístup pouze oprávněné osoby. Návštěvníci se musí pohybovat pouze v doprovodu zaměstnance. Je také nutné poučit personál, jak má reagovat v situaci, když se cizí člověk bez doprovodu zaměstnance objeví v chráněné zóně.
- Při výběru umístění serverů nebo jiných důležitých prostor je nutné vzít v úvahu rovněž taková rizika, jako je požár nebo povodeň. V případě potřeby instalovat protipožární pomůcky.
- Zajistit nepoužívaná okna a dveře.
- Pravidelně testovat poplašná zařízení.
- zásadu „prázdného stolu“, to znamená, že zaměstnanci musí zabezpečit důležité nebo hodnotné materiály, pokud s nimi právě nepracují.
- Označit počítače a jejich hlavní části identifikačními údaji o umístění a uživateli.

- Evidovat sériová čísla počítačů a jejich komponentů, aby byla možná jejich identifikace a případně vrácení v případě krádeže. Vyrýt, pokud je to možné, sériová čísla na nepříliš viditelných částech krabice počítače pomocí nože nebo jiného ostrého nástroje.
- Vysvětlit zaměstnancům, že dokumenty z tiskáren či kopírek je nutné ihned odebírat. Vyznačit tiskárny určené k tisku důvěrných informací.
- Ujistit se, že pravidla pro chování zaměstnanců určují, která zařízení mohou opustit kancelář. Hodnotná zařízení svěřit konkrétním lidem, kteří budou odpovědní za jejich vrácení.
- Je také vhodné zvážit pořízení kompletního hodnocení rizik společně s pojišťovací firmou, místním bezpečnostním oddělením a případně s nezávislým poradcem nebo konzultantem, kteří se zabývají tímto druhem zabezpečení.

3.9 Řízení bezpečnosti při pohybu na internetu

Bez větší nadsázky by se dalo říct, že každý pohyb na internetu je hned od počátku nebezpečný. Z předešlého tvrzení by mohlo vyplývat, že nejjednodušším řešením celého problému je k internetu se nepřipojovat. To je na jedné straně pravda ale na druhé je to zároveň neúčelné, i když z bezpečnostních důvodů mnoho firem a institucí k tomuto řešení občas přistupuje. Proto je nutné zčásti se s nebezpečným prostředním internetu sžít a pro své potřeby jej akceptovat. To ovšem nesmí znamenat, že se na bezpečnost rezignuje. Právě naopak, bezpečnost se musí řešit preventivně.

Je nutné zajistit, aby prohlížení webové sítě probíhalo bezpečným způsobem. To znamená, že zaměstnanci musí vědět, které www stránky mohou prohlížet a jakým způsobem mohou minimalizovat rizika s tím spojená. Webové stránky mohou obsahovat neškodné a užitečné programy (např. animace a rozbalovací menu), které někdy mohou obsahovat viry. Pokud si zaměstnanci společnosti v pracovní době prohlížejí stránky s pochybným obsahem, může to způsobit problémy s ohledem na právní důsledky takové činnosti. V neposlední řadě je především pro malé organizace často důležitá i otázka přenosové kapacity linky, takže omezení povolených internetových operací může být nápomocné při snižování zatížení linky. Existuje mnoho preventivních prostředků, které lze použít za účelem zvýšení bezpečnosti při prohlížení internetových stránek. Doporučuje se dodržovat následující zásady:

- Nenavštěvovat nedůvěryhodné internetové stránky. Jedním ze způsobů zavedení tohoto preventivního opatření je odrazovat zaměstnance od prohlížení internetových stránek na firemních počítačích ve volných chvilkách. Pracovníky je třeba požádat, aby navštěvovali pouze stránky, které jsou potřebné k jejich práci.
- Zvážit možnost instalace aplikačního firewall/proxy serveru za účelem filtrování adres z webové sítě nebo instalaci programového vybavení k filtrování obsahu webové sítě.
- Zpracovat metodický pokyn se zásadami využívání internetové sítě a rozdat jej pracovníkům.
- Určit, zda zaměstnanci mohou prohlížet internetové stránky z osobních důvodů nebo pouze za služebním účelem. Pokud mají zaměstnanci povolené prohlížení internetových stránek z osobních důvodů např. v rámci přestávky nebo po pracovní době, je to nutné v těchto zásadách uvést.
- Informovat zaměstnance, zda se využívání internetové sítě monitoruje a uvést, jestli mohou počítat se zachováním soukromí ve vztahu ke způsobu využití internetu.

Není třeba se vyhýbat doslovné specifikaci nedovoleného chování a konkrétnímu určení nepřípustných činností, jako např.: stahování dokumentů s urážlivým obsahem, výhrůžky nebo agresivní chování, nelegální činnosti, rozesílání komerční inzerce (nesouvisející z vykonávanou prací) atp. Je také nutné kontrolovat, zda zaměstnanci neobchází požadované ochrany a např. se nepřipojují k internetu pomocí soukromých telefonních modemů, instalovaných ve služebních počítačích. Instalaci takového modemu lze předejít plombováním pracovních stanic.

3.10 Bezpečné používání elektronické pošty

Elektronická pošta je velmi důležitým komunikačním nástrojem a nejčastěji využívaná internetová služba, a proto se také velmi často stává předmětem útoků. Při využívání jejích výhod je třeba dodržovat jistá bezpečnostní omezení směřující k minimalizaci existujících rizik. Viry, spam a falešné poplachy mohou způsobit, že se používání elektronické pošty se stane velice frustrující. Existuje však několik jednoduchých preventivních prostředků, které mohou značně zvýšit uživatelskou bezpečnost. Některé z nich jsou spojeny s vhodným nastavením ovládacího programového vybavení elektronické pošty, některé vyžadují použi-

tí programů jiných firem a další záleží spíše na sebevzdělávání a školení zaměstnanců v oblasti zjišťování potenciálních problémů. Nové programové vybavení k ovládání elektronické pošty se z hlediska bezpečnosti nepřetržitě zdokonaluje, protože programátoři vzali v úvahu rostoucí počet rizik spojených s emailovými zprávami. Stále je však vhodné dodržovat některé základní bezpečnostní zásady:

Aktualizovat programy elektronické pošty (a jiné programové vybavení). Aktualizace programů často obsahují zásadní opravy problémů bezpečnostního typu. V případě použití programu Microsoft Outlook je nutné pravidelně navštěvovat stránku společnosti Microsoft.Pomocí nejnovějších aktualizací ochran je nutné také aktualizovat systém Windows. V případě využití jiného programového vybavení je třeba navštěvovat stránku výrobce tohoto programu a kontrolovat, zda jsou aktualizace k dispozici.

Instalovat antivirové programy a provádět jejich aktualizace. Antivirové programy by měly pocházet od renomovaných firem. Musí také spolupracovat s používaným programovým vybavením elektronické pošty. Je třeba také pamatovat na pravidelné stahování definic nových virů.

- Filtrování nevyžádaných zpráv. Pokud používáte program Outlook 2003 je vhodné spustit funkci filtrování nevyžádaných zpráv. U dřívějších verzí programu Outlook (nebo jiného programového vybavení) je třeba zvážit možnost aktualizace na úroveň programu Outlook 2003 nebo použití doplňku jiné firmy zaměřeného na filtrování spamu.
- Neotvírat podezřelé přílohy. Neotvírat nevyžádané přílohy e-mailových zpráv bez potvrzení obsahu přílohy u odesílatele.
- Nereagovat na spam. V rámci nevyžádaných zpráv jsou často umístěny odkazy nebo adresy umožňující odstranění z distribučního seznamu rozesílatele spamu. Odpověď na spam však nejčastěji pro jeho odesílatele znamená, že získal aktivní a správnou e-mailovou adresu. Spam je nejlépe ignorovat a odstranit.
- Nikdy neuvádět hesla, čísla kreditních karet nebo jiné osobní informace v odpovědích na e-mailovou zprávu.
- Pokud bude legální firma skutečně potřebovat takové informace, nebude žádat o jejich poskytnutí prostřednictvím e-mailu.Místo toho může navrhnout uvedení údajů na bezpečné webové stránce. Pokud si nejste jistí, že e-mailová zpráva pochází z

důvěryhodného zdroje, doporučuje se nejdříve otevřít program Microsoft Internet Explorer a uvést adresu firmy (nikdy neklikat na odkazy v e-mailové zprávě). Pokud se zobrazí skutečná stránka firmy nebo organizace, je možné prověřit, zda požadované informace může skutečně potřebovat.

3.11 Využívání sítí VPN a bezpečné připojování vzdálených uživatelů pomocí VPN s protokolem IPSec

Při přihlašování do sítě prostřednictvím internetu je vhodné plně využívat všechny možnosti šifrování a ověřování. Připojení VPN je potřebné pro zaměstnance, kteří se nacházejí mimo podnik (např. osoby pracující doma nebo v průběhu služební cesty, tak jako starosta v příkladu uvedeném na začátku Příručky, kterému ukradli notebook), za účelem přístupu do podnikové sítě. Připojování vzdálených uživatelů do sítě prostřednictvím internetu je metodou velice efektivní, protože není nutné pronajímat nekomutované (a drahé) linky. Uživatelé, kteří využívají telefonické připojení, se mohou spojit s libovolným místním poskytovatelem služeb, místo vytáčení meziměstského spojení pomocí služby zpětného volání na domácí pracoviště. Existuje několik možností dálkových připojení, ale jedním z nejbezpečnějších je využití virtuální soukromé sítě, také označované jako VPN (Virtual Private Network). Šifrování dat přenášených pomocí internetu znemožňuje dalším osobám jejich přečtení a prověřování uživatelů zaručuje připojení pouze pro oprávněné uživatele. Dálkový přístup k síti včetně elektronické pošty je důležitou součástí činnosti každé organizace. Aktuálně jde o řešení využívané pouze některými z nich, ale s postupem času lze předpokládat, že stále více administrativních pracovníků bude využívat přenosné počítače a řešit pracovní úkoly mimo pracoviště, aniž by existoval problém s využíváním dat, která jsou zde uložena. Vytvoření sítě VPN zahrnuje vyřešení tří problémů. Jednak je v rámci úřední sítě nutné provést nastavení serveru VPN (již instalovaný stolní počítač např. starosty může fungovat jako server VPN). Za druhé je nutné nastavit firewall tak, aby umožňoval provoz VPN. A konečně za třetí je třeba nastavit počítače vzdálených uživatelů, aby se mohly připojovat prostřednictvím internetu k serveru VPN.

3.11.1 Přehled sítí VPN s protokolem IPSec

Standardem pro vytváření virtuálních sítí VPN se stal protokol IPSec. Tento protokol nabízí standardní prostředky pro navázání autentizačních a šifrovacích služeb mezi komuniku-

jícími partnery a tak zajišťovat dostatečnou bezpečnost při tomto druhu komunikace. Protokol IPSec zajišťuje následující bezpečností funkce:

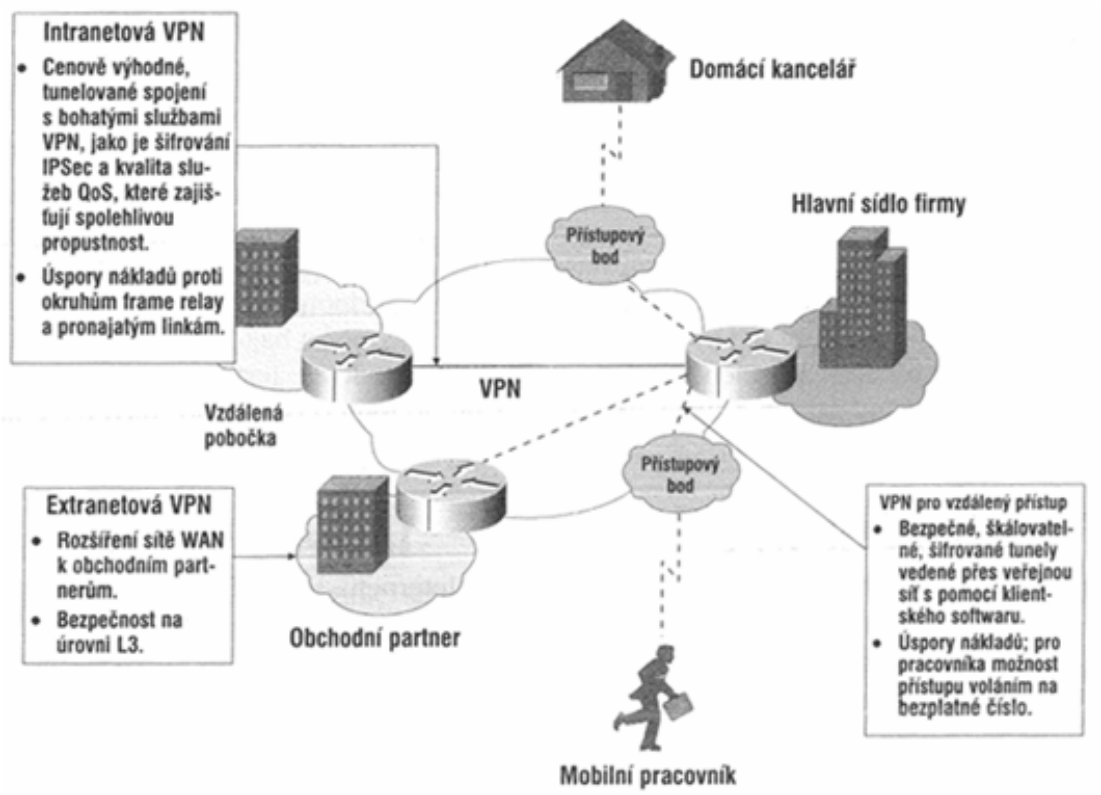
- důvěrnost dat – odesílatel IPSec může data před přenosem po síti zašifrovat,
- integrita dat – přijímající koncový bod IPSec autentizuje veškeré pakety od odesílatele a kontroluje tak, jestli nebyla data při přenosu pozměněna,
- autentizace původu dat – příjemce IPSec může dále autentizovat zdroj odesílaných paketů IPSec. Tato služba je závislá na službě integrity dat,
- ochrana proti opakování relace – příjemce IPSec může detekovat opakované pakety a zamítnout je.

Protokol IPSec tak chrání citlivá data při přenosu v nechráněných sítích, přičemž jeho bezpečnostní služby pracují na síťové vrstvě. Jednotlivé pracovní stanice, osobní počítače a či aplikace tak není třeba zvlášť konfigurovat. Tato veliký výhoda znamená současně i velkou úsporu nákladů. Nemusí se zajišťovat množství bezpečnostních služeb, které fakticky nejsou třeba, koordinovat zabezpečení zvlášť pro každou aplikaci a pro každý počítače, ale namísto toho se změní přímo síťová infrastruktura, která bude nově zajišťovat všechny potřebné bezpečností služby. Díky tomu je možné řešení IPSec snadno škálovat do středních až velkých sítí, ke je často nutné bezpečně propojit mnoho různých zařízení.

Součástí IPSec jsou zdokonalené bezpečností funkce, jako například vylepšené šifrovací algoritmy a obecnější autentizace. Podnikové sítě připojené k internetu tak mohou s protokolem IPSec snadno postavit bezpečný přístup k síti VPN. Technologie IPSec dovoluje vybudovat síť VPN s bezpečným šifrováním a ochranou proti odčerpání dat z kabelů, proti odposlechu a jiným útokům vedeným vůči privátní komunikaci. Protokol IPSec může šifrovat data mezi dvojicemi nejrůznějších zařízení, například:

- směrovač a směrovač,
- firewall a směrovač,
- firewall a firewall,
- uživatel a směrovač,
- uživatel a firewall,
- uživatel a koncentrátor VPN,

- uživatel a server.



Obr. 6 Účastníci sítě VPN

Technologie sítí VPN se velice rychle vyvíjí. I počet firem, které sítě VPN provozují nestále roste. Proto je důležité stanovit zásady pro používání VPN. Případné chyby mohou mít velmi vážné následky a to jak v bezpečnostní tak i finanční oblasti.

3.12 Bezpečnost bezdrátových sítí

V případě využití bezdrátových sítí je nutné instalovat alespoň základní bezpečnostní prvky, aby bezdrátové sítě nebyly tak snadno přístupné pro útoky zvenčí a dále pro využívání linky neoprávněnými osobami. Bezdrátové sítě, někdy označované jako sítě Wi-Fi, využívají rádiové spojení za účelem propojení počítačů bez nutnosti použití fyzických kabelů (podobně jako linky u bezdrátových telefonů). Tyto sítě umožňují rychlou a pružnou instalaci a nastavení a lze je využít k propojení osobních počítačů, notebooků a zařízení PDA s přístupovým bodem, který funguje jako koncentrátor pro všechny propojené počítače. Bezdrátové sítě jsou snadnějším cílem pro útoky než klasické kabelové sítě. Teoreticky každá osoba, která se nachází v rádiovém dosahu organizace, může odposlouchávat údaje ze sítě

nebo je může prostřednictvím této sítě přenášet. Problém spočívá v tom, že útočník nepotřebuje vůbec fyzický přístup k zařízením, aby mohl takové činnosti provádět. Může jít o osoby provozující „war driving“, které sedí v autě na parkovišti a hledají cizí tajemství nebo o lidi bydlící v sousedství, kteří se snaží tímto způsobem získat bezplatný přístup do internetové sítě. Snadno dostupné nástroje napomáhají útočníkům „vyčenichat“ nezabezpečené sítě. Většina výrobců bezdrátových produktů s pochopením pro vnější útočníky záměrně blokuje bezpečnostní funkce, aby bylo nastavení sítě snadnější, ale v důsledku toho nejsou tyto sítě vůbec chráněné. Proto lze naopak doporučit maximální ochranu bezdrátových sítí. Standard Wi-Fi sice definuje takové funkce jako šifrování a kontrola přístupu, ale způsob nastavení těchto funkcí závisí na výrobci. K získání podrobných informací z této oblasti je nutné důkladné prostudování dokumentace připojené k jednotlivým zařízením, kde je také možné zjistit, jak nastavit níže uvedené ochrany.

- Spustit šifrování Wi-Fi Protected Access (WPA) a používat jej k zamezení odposlechu. V bezdrátových sítích existuje několik technologií šifrování. Starší hardware může nabídnout pouze technologii Wired Equivalent Privacy (WEP) – méně efektivní šifrovací technologii. Pokud používané přístrojové vybavení umožňuje pouze šifrování WEP, je třeba zvážit možnost jeho výměny za hardware nabízející možnost šifrování WPA nebo, šifrování WEP zabezpečit použitím technologie Active Directory a Radius. Při nastavování šifrování je nutné používat silná hesla.
- Využívat přístupový bod (Acces Point), nikoliv sítě typu peer -to -peer. Hardware Acces Point (AP) zaručuje vyšší kontrolu nad osobami, které mají přístup do sítě.
- Omezit bezdrátový přístup. Je vhodné omezit bezdrátový přístup na obvyklou pracovní dobu v organizaci nebo na dobu, kdy se předpokládá využívání sítě.
- Používat filtrování Media Access Control (MAC).
- Každá síťová karta má přidělený individuální kód označovaný jako adresa MAC. AP je možné nastavit tak, aby přístup získaly pouze karty s důvěryhodnými adresami MAC, což znamená, že lze určit konkrétní počítače (nebo jiná zařízení), která mohou mít přístup do sítě. Zběhlý uživatel samozřejmě může toto omezení překonat nebo adresu MAC odhadnout, ale přesto tento jednoduchý postup umožňuje eliminaci útoků náhodných vetřelců.

- Omezit možnost zakládání bezdrátových sítí pro uživatele (a správce sítí). Bezdrátovou síť je nutné provozovat s velkou opatrností, protože jeden zanedbaný přístupový bod (AP) může zničit celou poctivou práci na zabezpečení dalších přístupových bodů (AP).
- Dbát na využívání bezpečnostních prvků. Je nutné se přesvědčit, že všechny bezpečnostní prvky (např. silná hesla) se používají, protože jen tak je možné vytvořit dobrou komplexní obranu proti vetřelcům.

4 PŘÍPADOVÁ STUDIE: ŘÍZENÍ BEZPEČNOSTNÍCH RIZIK V PODNIKOVÉM INFORMAČNÍM SYSTÉMU

Situace

Společnost XY a.s. je významným vývojovým dodavatelem slévárenských odlitků, zejména pro automobilový průmysl. Společnost má několik poboček v celé republice s několika zahraničními zastoupeními.

Lokality na území České republiky jsou propojeny pomocí WAN technologie. Přístup do Internetu je řešen centrálně v lokalitě sídla společnosti kombinací proxy serveru Microsoft ISA 2000 Server na Microsoft Windows 2000 Server. Ve společnosti je také aplikován poštovní server Microsoft Exchange Server 2003. Z celkového počtu asi 350 Windows stanic převážná část využívá proxy server. Ten zároveň plní funkci VPN serveru, ověřování klientů je zajištěno službami Microsoft Windows 2000 Server - IAS (Internet Authentication Service) a Active Directory. V této situaci společnost trápí časté napadení klientských stanic viry, trojskými koni, spyware a dalším škodlivým kódem staženým z Internetu. Nově také vznikla potřeba zajistit VPN spojení zahraničními pobočkami společnosti a celou podnikovou sítí a zajištění potřeby inovovat systém řízení bezpečnostních rizik v organizaci.

Obchodní cíle

Hlavním cílem projektu implementace bezpečnosti je nahradit neuspokojivé a nevyhovující řešení. Celkové řešení musí odpovídat řadě podmínek jako je vysoká míra zabezpečení a kontroly na jedné straně a přijatelné náklady organizace na dosažení takového stavu.

Podle základního popisu tedy mezi prioritní cíle celého projektu především patří:

- zlepšit zabezpečení VPN klientů a zajistit jednotnou a přehlednou správu řízení přístupu do Internetu s ohledem na co nejvyšší ochranu investic,
- připojit dceřiné společnosti v zahraničí a umožnit jejím zaměstnancům bezpečný přístup k vnitropodnikovým aplikacím,
- využít stávající hardwarové prostředky - server IBM xSeries 206 PIII

Úkol

- zajistit jednoduchou, přehlednou a centralizovanou správu zabezpečení,

- zajištění celkového zabezpečení interních serverů s přijatelnými náklady na správu,
- nezatěžování jednotlivých lokálních správců IT na pobočkách společnosti,
- snížení zatížení interních komunikačních linek mezi pobočkami a centrálou,
- integrovat do řešení systém monitoringu a systém pro detekci útoků a možnost detailního monitoringu připojení, snadného sledování a zpracování detailních výstupů,
- zajistit pokročilou ochranu sítě před útoky z internetu,
- přístup do internetu i ze vzdálených lokalit přes jediný chráněný centrálně spravovaný bod,
- zajistit zjednodušenou centralizovanou správu,
- umožnit snadné a zabezpečené poskytování interních informací přes internet,
- zabezpečený přístup partnerů k potřebným informacím v podnikové síti,
- implementace takového řešení, které bude splňovat veškeré nároky na funkci, výkon a úroveň zabezpečení při akceptovatelných nákladech,
- zajistit řízenou bezpečnost v celé organizaci v návaznosti na zaměstnance.

4.1 Celková bezpečnost sítě, řešení navržené s přihlédnutím na požadavky a možnosti společnosti

Zabezpečení sítě organizace s implementací Microsoft ISA Server 2004 v roli proxy, firewall a VPN serveru. Další prvky podílející se na zajištění bezpečnosti tvoří produkty GFi. Převážná část požadavků na provoz a údržbu celé infrastruktury postavené na platformě Microsoft, tedy i části firewallů, bude řešena interně v rámci možností centrálních správců. Při požadavcích nad rámec běžně dostupných informací bude moci využít dodavatele IT služeb.

Navržené řešení umožní:

- zabezpečení uživatelských Windows stanic před útoky z Internetu, odstranit problémy s výskytem škodlivého programového kódu,
- bezpečně připojit síť dceřiné společnosti v zahraničí,
- zjednoduší a zpřehlednit správu přístupu,

- přesně vymezí VPN přístupy pracovníkům dohledu a správy třetích firem.

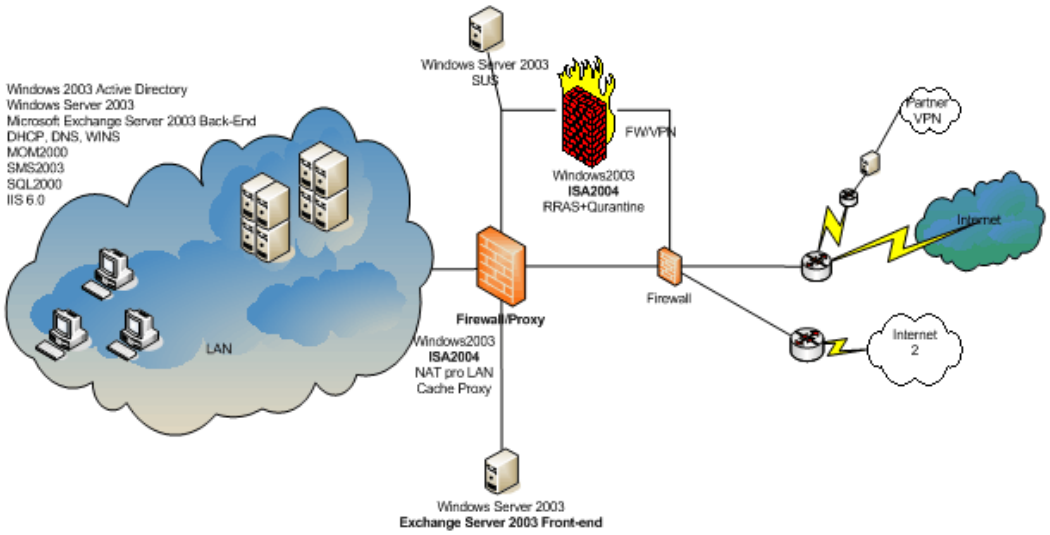
Popis řešení po funkční a technické stránce

Po zvážení situace vyšlo najevo, že řešení, které splňuje všechny nároky zákazníka, je řešení postavené na technologiích společnosti Microsoft. Především použití nového firewallu a proxy serveru Microsoft Internet Security and Acceleration Server 2004 (ISA Server 2004), který nabízí veškeré požadované funkce a technologie a navíc je výrazně levnější investicí než pouhé pořízení firewallu. Evolucí v oblasti zabezpečení interních zdrojů došlo také ke změně uspořádání v DMZ.

Součástí návrhu je také přidání Exchange Front-end server, který bude zabezpečen pomocí Form-based autentizace a SSL-Bridgingu produktu ISA Server 2004. Touto technologií dojde k ověření uživatele před tím, než jeho požadavek vůbec dorazí na Exchange Front-end.

Pro VPN server bylo navrženo řešení vycházející rovněž z Microsoft ISA Server 2004, který přináší výhodu pokročilé kontroly pomocí technologie Quarantine. Tento produkt splňuje veškeré požadavky, snadným způsobem zapadne do stávající infrastruktury a navíc byl certifikován podle mezinárodních standardů bezpečnosti (Common Criteria, NCSA Labs).

Přesto že nasazení takového řešení není jednoduchou záležitostí, k jeho nasazení výrazně přispěje a napomůže skutečnost, že tento produkt umožňuje poměrně snadné nastavení komplikovaných požadavků. Při implementaci je nutné se zabývat tím, co chceme řešit a ne jak složitě to nastavit. Do budoucna řešení navíc pokryje i řešení pro vzdálený přístup (VPN) s pokročilým ověřením uživatelů formou čipových karet a certifikátů.



Obr. 7 Rozvržení a struktura sítě

Odhadovaný rozsah využitelnosti a počet PC a využití služeb:

Odchozí komunikace: Cca 1000 uživatelů.

Vzdálený přístup: (Outlook Web Access, VPN) Cca 10% uživatelů.

Hlavní přínosy navrženého řešení

- podstatné zlepšení ochrany sítě před možnými útoky z Internetu,
- výrazné zlepšení antivirové kontroly a možností zadržení nebezpečného programového kódu,
- jednotný chráněný přístup z vnitřní sítě do Internetu, přehledné a bezpečné řešení přístupu vzdálených uživatelů do vnitřní sítě společnosti,
- optimalizace systému řízení a zpřístupnění provozních aplikací divizí a jejich zaměstnancům,
- zjednodušená a přehledná komplexní centralizovaná správa zabezpečení sítě,
- součástí návrhu byla i změna uspořádání demilitarizované zóny, která jednoznačně přinese zvýšení zabezpečení interních serverů a přístupu k jejich zdrojům: mobilní a vzdálení uživatelé budou schopni mít webový přístup k elektronické poště (OWA), bezproblémové a jednoduché připojení samotným programem Outlook k

firemnímu mailboxu, sdíleným složkám, společným kalendářům a podobně (RPC/HTPP) a konečně velmi bezpečné plnohodnotné vzdálené připojení (VPN, Quarantine),

- po celou dobu připojení existuje možnost pokročilé kontroly, snadného sledování a nakonec zpracování detailních výstupů,
- celkové řešení tedy splňuje náročné požadavky zákazníka na funkci, výkon a úroveň zabezpečení při akceptovatelných nákladech.

Interní IT administrátoři, mající znalosti s prací na produktech Microsoft, získají informace a znalosti nutné k implementaci jen z dostupné dokumentace a účasti na přehledovém semináři školení. Celou implementaci poté budou schopni provést sami bez nutnosti využít externí konzultanty. K tomu přispěje dobrá znalost prostředí produktů Microsoft a dobrá znalost technologií, které v celém scénáři zabezpečení hraje hlavní roli a přehledná konfigurace produktu Microsoft ISA Server 2004. Další výhodou je stálá možnost dalšího rozvoje a to díky otevřené architektuře použitých moderních technologií. V případě použití jiných produktů by zákazník musel využívat externí konzultanty a investovat do školení IT administrátorů, což by mělo velmi negativní dopad na celkovou návratnost a efektivitu řešení.

Podpora

Převážná část požadavků na provoz a údržbu celé infrastruktury postavené na platformě Microsoft, tedy i části firewallů, je řešena interně v rámci možností centrálních správců. Při požadavcích nad rámec běžně dostupných informací na internetu se využívá podpora dodavatele IT služeb.

Možnosti budoucího vývoje

V případě budoucího nárůstu vzdáleného připojení se uvažuje o implementaci VPN serveru s pokročilou kontrolou uživatelů. Jako vhodná varianta se nabízí technologie Qurantine, která je součástí Microsoft Windows Server 2003 v kombinaci s novými možnostmi již navrženého firewallu Microsoft ISA Server 2004. Zároveň do budoucna může být řešena také možnost nového moderního způsobu synchronizace elektronické pošty z Internetu. Klienti Microsoft Outlook 2003 tak budou bez nutnosti VPN připojení, přistupovat k elektronické poště, kalendářům a veřejným složkám na Microsoft Exchange Server 2003. Toho dosáhnout, prakticky vždy jen s připojením do Internetu.

4.2 Bezpečnost uživatelských stanic, řízení bezpečnosti v úrovni lidských zdrojů, školení

4.2.1 Hlavní rizikové oblasti

Útočníci (viry, wormy, zneužití prostředků počítačů nebo připojení k internetu a náhodné škodlivé použití). Jedná se o rizika, kterým čelí všichni, jejichž počítače jsou připojeny k Internetu. Vysoké riziko, vysoká priorita.

Ohrožení zvenku (konkurence, nespokojení bývalí zaměstnanci, zloději). Tito uživatelé používají pravděpodobně stejné nástroje jako útočníci, ale při svém záměrném útoku mohou přesvědčit zaměstnance k předání důvěrných informací nebo dokonce ukradených materiálů, které později použijí k vydírání nebo k poškození společnosti. Společnost potřebujeme své prostředky chránit fyzickou a elektronickou formou zabezpečení. Vysoké riziko, vysoká priorita.

Interní ohrožení. Ať úmyslně nebo neúmyslně, mohou zaměstnanci chybně použít svých oprávnění k vyzrazení důvěrných informací. Vysoké riziko, vysoká priorita.

Nehody a katastrofy. Požár, záplava, náhodné odstranění, porucha hardwaru a havárie počítačů. Nízké riziko.

4.2.2 Další rizikové oblasti:

Kromě fyzické vlastnictví mezi aktiva patří:

- návrhy produktů a marketingové materiály,
- záznamy o smlouvách s dodavateli a objednávky,
- e-mailová databáze a archiv,
- prodejní objednávky a databáze zákazníků,
- finanční informace,
- záznamy oddělení lidských zdrojů a právní záznamy v různých šanonech.

4.2.3 Audit zabezpečení

Antivirová ochrana: na několika uživatelských PC chybí antivirová ochrana; velká část není aktualizována; jen část uživatelů obecně zná problematiku virů, ale nejsou si zcela jisti, co mohou udělat pro ochranu proti nim.

Software pro filtrování nevyžádané pošty: Mnoho uživatelů je zatěžováno nevyžádanou poštu, přičemž nemáme žádnou ochranu.

Brána firewall: Chybí v několika uživatelských PC.

Aktualizace: Všechny počítače se systémem Windows XP Professional jsou aktualizované, neboť automaticky vyhledávají a instalují aktualizace. Některé instalace aplikací sady Office však potřebují aktualizovat a počítače se systémy Windows 98 nejsou aktualizované vůbec.

Hesla: Někteří uživatelé hesla vůbec nepoužívají nebo že si je zapsali na lístek s poznámkami. Žádný z přenosných počítačů není chráněn heslem.

Fyzické zabezpečení: Zámky dveří, oken a poplašná zařízení jsou v pořádku. Žádný počítač však nemá vyryto výrobní číslo ani neexistuje seznam výrobních čísel.

Bezdrátová síť: Zde nejsme vůbec zabezpečeni. K bezdrátové síti mají přístup osoby vybavené příslušným síťovým adaptérem, které tak mohou procházet síť a využít naše připojení k Internetu.

Přenosné počítače: Všechny přenosné počítače se přenášejí v brašnách s logem výrobce, které nemají žádné zámky.

Procházení webu: Nejsou dostatečně vytvořeny zásady přijatelného použití a nikdo se nevěnoval žádným doporučením zabezpečení.

4.2.4 Priority řízení bezpečnosti IS v organizaci

Ochrana před útoky:

- zkontrolovat, zda je firewall na každé PC, případně doinstalovat,
- zajistit ochranu proti virům,
- zesílení zabezpečení bezdrátových sítí,
- instalace systémů Windows XP Professional na počítače se systémem Windows 98,

- zajištění pravidelné aktualizace všech počítačů,
- školení uživatelů a seznámení uživatelů se zásadami podnikové bezpečnosti.

Prevence proti krádeži

- zabezpečení přenosných počítačů,
- bezpečnostní zámky pro běžné a přenosné počítače,
- označování všech počítačů z bezpečnostních důvodů a pro inventarizaci.

Ochrana proti haváriím

- častější zálohování a uložení médií mimo organizaci,
- zálohování místních dat uživatelů,
- uložení kritických papírových dokumentů mimo organizaci,
- pravidelné testování záloh pomocí obnovení.

Interní zabezpečení

- zásady silných hesel a školení uživatelů,
- zabezpečení tiskáren pro jednotlivá oddělení a vedení společnosti,
- revize zabezpečení šanonů a důvěrných dokumentů.

Změna zásad

Nutné zhotovení příručky pro zaměstnance tak, aby především obsahovala nové zásady pro:

- přijatelné používání e-mailu a internetu,
- používání silných hesel,
- ochrana vlastnictví společnosti.

Školení uživatelů

Školení uživatelů by mělo být prováděno v malých skupinkách a současně pomocí elektronické příručky, kterou obdrží všichni zaměstnanci, jejichž práce obnáší práci na počítačovém vybavení společnosti.

Obr. 8 Příručka pro uživatele

Společně s elektronickou příručkou je k dispozici i hra v podobě „osmisměrky“ obsahující základní pojmy z oblasti bezpečnosti. Cílem takovéto hry je nenucené seznámení školených uživatelů se základními pojmy, se kterými se mohou setkat v souvislosti s řešením bezpečnostních situací při práci v podnikovém informačním systému.

Obr. 9 Osmisměrka

Hlavní body školení pro zaměstnance by měly být tvořeny těmito okruhy:

- důležitost opatření,
- hesla,
- zabezpečení přenosných PC,
- ochrana proti virům,
- bezpečné procházení internetu,
- představení zásad pro zaměstnance.

4.2.5 Software a služby

Microsoft Windows Server 2003 Standard Edition

Microsoft Internet Security and Acceleration Server 2004 Standard Edition

GFi Mail Security for Exchange/SMTP, GFi Web Monitor for ISA Server 3, GFI LANguard Security Event Log Monitor, WebMonitor for ISA Server

4.3 Dokumenty podnikových zásad zabezpečení

Dokumenty popisují zásady přípustného užívání a klade si za cíl nezavádět žádná omezení, která by byla v rozporu s firemní kulturou dané společnosti, která je postavena na otevřenosti, důvěře a integritě. Cílem je chránit zaměstnance, partnery dané organizace i organizaci samotnou a to před nezákonným nebo škodlivým jednáním jednotlivců, a to vědomým i nevědomým.

Účelem vyjmenovaných zásad v tomto dokumentu je stanovit pravidla přípustného užívání počítačového vybavení v dané společnosti. Tato pravidla mají sloužit k ochraně firmy před různými riziky, jako například virovými útoky, napadením síťových systémů a služeb. Tyto zásady musí platit pro každého zaměstnance, dodavatele, konzultanta nebo i dočasného pracovníka a pro ostatní osoby ve firmě, včetně osob spojených s příslušnými cizími subjekty. Dále platí pro veškerá zařízení, která jsou ve vlastnictví dané společnosti nebo jsou jí pronajatá, a také pro každé osobní zařízení, které může přijít do styku s podnikovou infrastrukturou informačního systému.

4.3.1 Bezpečnost a důvěrné informace

1. Uživatelské rozhraní k informacím obsaženým v informačních podnikových systémech využívajících internetové, intranetové nebo extranetové připojení je vždy nutné považovat jako důvěrné nebo neutajované (bez klasifikace) a to v souladu s podnikovými zásadami klasifikace důvěrnosti. Příklady základních informací, které by měly v podnikovém informačním systému spadat do kategorie důvěrných jsou například tyto:

- soukromé nebo důvěrné firemní informace,
- podnikové strategie a záměry,
- informace citlivé vzhledem ke konkurenci a konkurenční analýzy,
- data podléhající obchodnímu tajemství, patenty, výsledky testů,
- specifikace a provozní parametry,
- seznamy zákazníků a údaje o nich,
- výzkumné údaje,

Zaměstnanci musí všemi vhodnými prostředky zabránit neoprávněnému přístupu k těmto a podobným informacím.

2. Uchovávání hesel v tajnosti a bezpečí. Zaměstnanci nesmí hesla nebo svůj osobní účet půjčovat nikomu jinému, kdy každý oprávněný uživatel je odpovědný za bezpečnost svého vlastního účtu i hesla. Systémová hesla je třeba měnit nejméně jednou za čtvrtletí, uživatelská hesla pak každých šest měsíců.

3. Veškeré osobní počítače, notebooky a pracovní stanice musí být zabezpečeny pomocí spořiče obrazovky s ochranou hesla a s automatickou aktivací nejpozději po 10 minutách nečinnosti, nebo se uživatel při vzdálení od počítače musí odhlásit. Informace umístěné na přenosných počítačích jsou obzvláštně zranitelné, a proto je nutné s nimi zacházet mimořádně opatrně.

4. Veškeré počítačové systémy, které zaměstnanec používá a které jsou připojeny k internetu, intranetu nebo extranetu uvnitř podnikového informačního systému, ať už jsou v majetku zaměstnance nebo firmy, musí být neustále kontrolovány schváleným antivirovým programe s aktuální databází virů. Tato zásada se musí týkat i

osob, která mají ve zvyku číst e-mail z různých počítačů na různých fyzických místech. Jedná se především o zaměstnance, kteří čtou v práci poštu ze svého soukromého, bezplatného účtu přes webové rozhraní a nic netušíc stáhnou zavirovanou přílohu, soubor. Cílem předchozího pravidla je zajistit, že i takovýto virus bude zachycen ve vhodném antivirovém programu. Pokud ale zaměstnanec přistupuje ke stejnému webovému e-mailu z domácího počítače, jehož prostřednictvím se následně připojuje i do podnikové sítě, je nutné důkladně zvážit možné důsledky a ohrožení firemního systému.

5. Při otevírání e-mailových příloh od neznámých odesílatelů, které mohou obsahovat viry, e-mailové bomby nebo trojské koně, si uživatelé musejí počínat maximálně opatrně. V případě pochybností je uživatel povinen zkontrolovat dokument ručně před otevřením přílohy.

4.3.2 Nepřípustné užívání

Následující aktivity jsou obecně zakázány. Zaměstnanci mohou nicméně být uvedených zákazů zproštěni při plnění svých pracovních povinností.

Za žádných okolností nejsou zaměstnanci společnosti při práci s firemními prostředky oprávněni k provádění jakýchkoli aktivit, jež jsou v rozporu s platnými vnitrostátním i mezinárodním právem a nižšími zákonnými normami.

Níže uvedený seznam zakázaných aktivit nedokáže obsáhnout všechny možné aktivity a situace v daném podnikovém systému. Představuje však jistý základ a přehled nepřípustného užívání systému. Bude-li mít kterýkoliv zaměstnance pochybnosti a nejasnosti ohledně určité aktivity, ať se obrátí na odpovědného pracovníka zajišťující řízení bezpečnostních rizik uvnitř společnosti.

4.3.3 Aktivity v systému a v síti

Tyto aktivity jsou bez jakýchkoli výjimek přísně zakázány:

1. Porušování práv libovolné osoby či společnosti, chráněných autorskými zákony, obchodním tajemstvím, patentovým nebo jiným duševním vlastnictvím, případně podobnými zákony a nařízeními, včetně instalace a distribuce odcizeného či „pirátského“ softwaru, jehož užívání není kryto odpovídající licencí.

2. Neoprávněné kopírování materiálu podléhajícího autorským právům, jako je mimo jiní i digitalizace a distribuce fotografií z časopisů, knih a jiných zdrojů krytých autorským právem, hudby chráněné autorským právem, také instalace softwaru krytého autorským právem, pro který nemá společnost ani koncový uživatel aktivní licenci, je přísně zakázáno.
3. Takový vývoz softwaru, odborných informací, šifrovacího softwaru a technologií, který narušuje mezinárodní či místní předpisy pro kontrolu exportu, je nelegální. Před případným exportem diskutabilního materiálu si zaměstnance musí vyžádat souhlas nadřízeného.
4. Zavádění škodlivých nebo zlomyslných programů do sítí a serverů (například virů, červů, trojských koňů, e-mailových bomb atd.)
5. Prozrazení hesla k uživatelskému účtu jiným osobám nebo svolení k využívání účtu jinou osobou. Vykonává-li zaměstnance svou práci doma, spadají mezi tyto osoby i členové rodiny a společné domácnosti.
6. Aktivní využívání počítačových systémů ve vlastnictví společnosti k získávání nebo odesílání materiálů, který narušuje platné zákony týkající se nepřátelství nebo obtěžování na pracovišti, a to podle zákonných norem platných v místě pracoviště uživatele.
7. Odesílání falešných nabídek výrobků, zboží nebo služeb z jakéhokoli uživatelského účtu ve společnosti.
8. Veškeré jednání, které má za následek prolomení bezpečnosti nebo narušení síťové komunikace. Mezi prolomení bezpečnosti patří mimo jiné přístup k datům, která nejsou určena danému zaměstnanci, nebo při přihlášení k serveru či pod účet, k němuž není zaměstnanec oprávněn přistupovat. Výjimka může být udělena pouze v případě, že se jedná o úkoly spojené s plněním pracovních povinností. Za narušení bezpečnosti se považuje také odposlech v síti, záplavy dotazů ping, falšování paketů, odepření služeb a falšování směrovacích informací za nekalými úmysly.
9. Prohledávání portu a zkoumání bezpečnosti je výslovně zakázáno.

10. Jakákoli forma monitorování sítě, při němž zaměstnanec zadržuje či odposlouchává data, která pro něj nejsou určena, ledaže toto monitorování spadá pod normální pracovní povinnosti zaměstnance.
11. Obcházení mechanismů autentizace uživatelů či bezpečnosti libovolného hostitelského systému, sítě nebo účtu.
12. Narušování nebo odepírání služby libovolnému jinému uživateli.
13. Spouštění jakýchkoli programů, skriptů a příkazů, nebo odesílání jakýchkoli zpráv, jejichž cílem je narušování nebo zablokování terminálové relace jiného uživatele. Tento zákaz platí jak lokálně, tak i v internetu, intranetu nebo extranetu.
14. Poskytování informací o zaměstnancích společnosti nebo seznamu zaměstnanců vnějším subjektům.

4.3.4 Aktivity v elektronické poště a pří komunikaci

Je přísně zakázáno:

1. Odesílání nevyžádaných zpráv elektronické pošty, hromadné pošty nebo jiného reklamního materiálu jednotlivcům, kteří je výslovně nepožadovali.
2. Jakákoli forma obtěžování, a to elektronickou poštou, telefonem, pagerem a jinými prostředky, a to v libovolném jazyce, s jakoukoli frekvencí a při jakékoli velikosti zpráv.
3. Neoprávněné používání nebo falšování informací v záhlaví elektronické pošty.
4. Vyžadování e-mailových zpráv, určených pro kteréhokoli jiného uživatele nebo adresu, se záměrem obtěžování či shromažďování odpovědí.
5. Vytváření a rozesílání řetězových dopisů, pyramidových her např. „letadlo“ a podobných.
6. Zasílání nevyžádané elektronické pošty ze sítí společnosti či jiných poskytovatelů internetových, intranetových a extranetových služeb jménem společnosti.
7. Podávání stejných či podobných zpráv nepracovního charakteru do velkého množství diskusních skupin.

Libovolný zaměstnanec , který bude přistižen při porušování zde uvedených zásad, bude vystaven disciplinárnímu řízení a v případě závažného porušení pracovní kázně může být i propuštěn ze zaměstnání.

4.3.5 Zásady pro práci s hesly

Hesla jsou velice důležitou stránkou zabezpečení počítačů a tvoří první „obrannou linii“ uživatelských účtů. Nevhodně zvolené heslo může nakonec vést i k narušení bezpečnosti celé podnikové sítě a následně narušení funkčnosti vnitropodnikového informačního systému. Vzhledem k tomu je každý zaměstnanec společnosti odpovědný za správný výběr hesla a jeho zabezpečení, jak popisují následující body dokumentu. Těmito pravidly je povinen se řídit také z uživatelů mezi dodavateli a odběrateli firmy, kteří mají do firemních systému přístup. Úkolem následujících zásad je stanovit standard pro vytváření silných hesel, mechanismy ochrany hesel a definice způsoby jejich měření.

4.3.6 Obecné zásady

1. Veškerá systémová hesla se musí změnit alespoň jednou za čtvrtletí.
2. Veškerá provozní systémová hesla musí spadat pod globální databázi hesel, kterou spravuje odpovědný pracovník určený k zajišťování řízení bezpečnosti uvnitř organizace.
3. Veškerá uživatelská hesla musí být změněna nejméně jednou za šest měsíců; doporučený časový interval je jednou za čtyři měsíce.
4. Uživatelské účty s oprávněními systémové úrovně, přidělovanými pomocí členství uživatele ve skupinách či pomocí jiných programů musí mít jedinečné heslo, různé od hesel všech ostatních účtů dané osoby.
5. Hesla nesmí být zapisována do zpráv elektronické pošty ani do jiné elektronické komunikace.
6. Heslo nesmí žádný uživatel prozradit nikomu jinému, bez ohledu na pozici případného žadatele v organizaci. Požádá-li někdo o sdělení hesla, musí se uživatel nejdříve spojit s osobou zajišťující řízení bezpečnosti podnikového systému uvnitř společnosti.
7. Skupinová hesla nesmí mít standardní výchozí hodnoty.

8. Všechna uživatelská i systémová hesla musí odpovídat zásadám, které jsou popsány v následující části dokumentu.

4.3.7 Obecná pravidla pro zadávání hesel

Hesla se v systémech společnosti používají k nejrůznějším účelům. Mohou to být hesla k uživatelským účtům, k webovým účtům, k e-mailovým účtům, ke spořičům obrazovky nebo i k hlasové poště. Jen málokterý systém podporuje přitom jednorázové tokeny, dynamická hesla s jednorázovou platností, a proto si každý uživatel musí umět zvolit dostatečně silné heslo.

Slabé heslo:

1. Heslo je kratší než osm znaků.
2. Heslo se dá přímo najít v jazykovém slovníku (českém, anglickém nebo jiném).
3. Heslo je běžným výrazem, jako například:

- jméno člena rodinky, domácího zvířete, přítele, spolupracovníka, filmové postavy apod.,
- výrazy a názvy z oblasti počítačů, příkazy, servery, firmy, hardware, software,
- slova související se společností, jako je vlastní název společnosti a obecná pojmenování související se společností,
- jména sportovních klubů a hráčů,
- snadno uhodnutelné skupiny písmen a číslic, jako je například skupina aaabbb, qwertz, yxccv, 123321 apod.,
- libovolný z výše uvedených výrazů, zapsaných pozpátku,
- libovolný z výše uvedených výrazů, před nebo za kterým je jediná číslice, např. heslo1 nebo 2heslo apod.,

Silná, správně vytvořená hesla můžeme definovat takto:

1. Obsahují malá a velká písmena.
2. Obsahují číslice a interpunkční znaménka.
3. Mají délku nejméně osm alfanumerických znaků.

4. Nejsou tvořena žádným slovem z běžného slovníku, slangu, dialektu, odborných výrazů.
5. Nejsou odvozena ze žádných osobní údajů, jmen členů rodiny apod.

Takto vytvořená hesla se nesmí zapisovat na papír ani ukládat v elektronické podobě. Je třeba vytvářet proto taková hesla, která je možné si snadno zapamatovat. Vhodné je například vycházet z určité fráze, názvu hudební skladby nebo jiného slovního spojení a vhodně je přetvořit, např. „vyjmout“ z fráze první počáteční písmena u jednotlivých slov a dalšími úpravami, které jsou definovány v předešlém odstavci o silných heslech dokončit tvorbu silného hesla.

4.3.8 Standardy pro ochranu hesel

Pro účty v podnikových systémech je třeba si nevolit stejná hesla jako pro jiný, cizí systém např. pro osobní účet u poskytovatele internetu, pro vstup do bankovního účtu apod. Pokud možno je vhodné nepoužívat také stejné heslo u několika různých systémů ve společnosti. Všechna hesla se považují za citlivé a důvěrné údaje společnosti a je třeba s nimi takto i zacházet.

Následující věci jsou zakázány:

1. Nikomu neříkejte heslo po telefonu.
2. Nezapisujte hesla do e-mailové zprávy.
3. Neříkejte heslo svému nadřízenému.
4. Nemluvte o svých heslech před druhými.
5. Nenapovídejte nikomu ani formát hesla.
6. Nepište heslo na dotazníky či bezpečnostní formuláře.
7. Nesdělujte heslo členům rodiny.
8. Nesdělujte heslo spolupracovníkům, a to ani při odjezdu na dovolenou.

Další pravidla:

1. Pokud vás někdo o heslo přesto požádá, odvolejte se na tento dokument a v případě potřeby dotyčnou osobu pošlete za pracovníkem odpovědným za řízení bezpečnosti v podnikovém systému.

2. V aplikacích nepoužívejte funkci „Zapamatovat si heslo“.
3. Hesla neukládejte do žádných souborů, a to na žádném počítačovém systému, včetně přenosných počítačů.
4. Heslo si nejméně jednou za šest měsíců změňte (výjimkou jsou systémová hesla, která se musí měnit jednou za tři měsíce). Doporučený interval změny je nicméně čtyři měsíce.
5. Máte-li potíže s napadením účtu nebo hesla, oznamte bez prodlení tento problém pracovníkovi odpovědnému za řízení bezpečnosti podnikového systému a neprodleně si změňte všechna hesla.
6. Pracovník nebo pracovníci určení k řízení bezpečnosti v podnikovém systému mohou pravidelně či namátkově provádět pokusy o uhodnutí nebo prolomení hesla. Pokud takovémuto testu heslo nevyhoví, musí si je uživatel okamžitě změnit.

Libovolný zaměstnanec, který bude přistižen při porušování zde uvedených zásad, bude vystaven disciplinárnímu řízení a v případě závažného porušení pracovní kázně může být i vystaven disciplinárnímu řízení a v případě závažného porušení pracovní kázně může být i propuštěn ze zaměstnání.

4.3.9 Zásady zabezpečení sítí VPN (Virtual Private Network)

Virtuální privátní sítě VPN smí používat schválení zaměstnanci společnosti a oprávněné cizí osoby (zákazníci, dodavatelé atd.). Jedná se přitom o službu řízenou uživatelem. To znamená, že za výběr vhodného poskytovatele internetových služeb, instalaci hardwaru i softwaru a placení veškerých je zodpovědný sám uživatel.

Další pravidla:

1. Uživatel s oprávněním přístupu přes VPN má povinnost zajistit, že do interní sítě společnosti nebude míst přístup žádná neoprávněná osoba.
2. Práce v síti VPN bude řízena buďto pomocí autentizace jednorázovým heslem nebo systémem veřejného a privátního klíče se silnou přístupovou frází.
3. Během aktivního připojení do podnikové sítě musí síť VPN směrovat tunelem VPN veškerý provoz od osobního počítače uživatele a zpět. Ostatní provoz musí být zakázán.

4. Duální neboli oddělené tunelování není povoleno. Vždy smí být vedeno jen jedno síťové spojení.
5. Na všech počítačích, které jsou přes sít VPN či přes jinou technologii připojeny do interních sítí společnosti, musí pracovat aktuální antivirový software. Tomuto pravidlu podléhají i osobní počítače.
6. Po třiceti minutách nečinnosti je uživatel sítě VPN automaticky odpojen ze sítě společnosti. Poté se uživatel musí do sítě přihlásit znovu. Dotazy ping či jiné umělé síťové procesy se nepovažují za aktivitu a spojení se při nich nezachová.
7. Uživatelé počítačů, které nejsou ve vlastnictví společnosti, musí svá zařízení konfigurovat v souladu se zásadami společnosti pro zabezpečení sítě i se zásadami VPN.
8. Uživatel, který se pomocí technologie VPN připojuje ze svého osobního počítače, si musí být vědom, že se jeho počítač stává součástí rozšířené sítě společnosti a že tedy pro něj platí stejná pravidla a stejná omezení jako pro zařízení ve vlastnictví firmy, konfigurace tohoto počítače musí tedy být v souladu se všemi zásadami zabezpečení.

4.3.10 Zajištění fyzické bezpečnosti

Ochrana stolních počítačů a omezení fyzického přístupu k pracovním stanicím a dokumentům je podstatnou součástí činnosti při zajišťování bezpečnosti dat. V těchto případech se využívají dobře známé metody: zámky, alarmy, zamykání skříněk na dokumenty, evidence návštěvníků a označování přístrojového vybavení. Ne všechny katastrofy způsobují útočníci zvenčí, kteří působí prostřednictvím internetu. Občas může být náhodné vloupání ještě horší. Níže uvádíme seznam kontrolních činností, jejichž provedení by mělo být zárukou fyzické bezpečnosti úředních informací a počítačů. Je třeba:

1. Určit bezpečnostní hranice kolem chráněné zóny s využitím (podle potřeby) příček, dveří s automatickým zavírání, uzamykatelných dveří, alarmů a ochranných bariér.
2. Ujistit se, že vstupy zvenčí jsou hlídané a přicházející a odcházející hosté jsou evidováni a identifikováni.
3. Pokud je to možné, maximálně omezit možnost přístupu do důležitých zón (např.místnost serverů nebo místnost, kde se nacházejí osobní údaje zaměstnanců).

4. Pravidelně kontrolovat, kdo má přístup do důležitých zón. Do těchto prostor by měli mít přístup pouze oprávněné osoby. Návštěvníci se musí pohybovat pouze v doprovodu zaměstnance. Je také nutné poučit personál, jak má reagovat v situaci, když se cizí člověk bez doprovodu zaměstnance objeví v chráněné zóně.
5. Při výběru umístění serverů nebo jiných důležitých prostor je nutné vzít v úvahu rovněž taková rizika, jako je požár nebo povodeň. V případě potřeby instalovat protipožární pomůcky.
6. Zajistit nepoužívaná okna a dveře.
7. Pravidelně testovat poplašná zařízení.
8. zásadu „prázdného stolu“, to znamená, že zaměstnanci musí zabezpečit důležité nebo hodnotné materiály, pokud s nimi právě nepracují.
9. Označit počítače a jejich hlavní části identifikačními údaji o firmě, umístění a uživateli.
10. Evidovat sériová čísla počítačů a jejich komponentů, aby byla možná jejich identifikace a případně vrácení v případě krádeže. Vyrýt, pokud je to možné, sériová čísla na nepříliš viditelných částech krabice počítače pomocí nože nebo jiného ostrého nástroje.
11. Vysvětlit zaměstnancům, že dokumenty z tiskáren či kopírek je nutné ihned odebírat. Vyznačit tiskárny určené k tisku důvěrných informací.
12. Ujistit se, že pravidla pro chování zaměstnanců určují, která zařízení mohou opustit kancelář. Hodnotná zařízení svěřit konkrétním lidem, kteří budou odpovědní za jejich vrácení.
13. Je také vhodné zvážit pořízení kompletního hodnocení rizik společně s pojišťovací firmou, místním bezpečnostním oddělením a případně s nezávislým poradcem nebo konzultantem, kteří se zabývají tímto druhem zabezpečení.

ZÁVĚR

Dnes už prakticky neexistuje organizace či úřad, v němž by nevyužívali výpočetní techniky. Stále častěji se společnosti kontaktují s okolím pomocí internetu a využívají možnosti elektronického oběhu informací. Zajištění ochrany dat a správného fungování informačních systémů v se v takové situaci stává klíčovou záležitostí. Proto je důležité vědět, na čem je založeno řízení bezpečnosti a jaké nebezpečí může hrozit. Bezpečnost informací je velmi široké téma, avšak v mé práci se je snažím popsat jednoduchým a hlavně přístupným způsobem pro co nejširší okruh osob.

Zpracoval jsem diplomovou práci na téma: Řízení vybraných bezpečnostních rizik v podnikových informačních systémech a její cíl považuji za splněný. Zabýval jsem se návrhem tvorbou postupů řízení bezpečnosti podnikových systémů v organizaci. Dále návrhem jednotlivých kroků pro řízení bezpečnosti informačních systémů z pohledu budoucích uživatelů a ostatních pracovníků ve firmách a institucích, které se rozhodly řídit vnitřní bezpečnost informačních systémů a praktickým popisem hlavních kroků procesu implementace a využívání systému řízené bezpečnosti IS.

Má diplomová práce si klade především za cíl poskytnout informace a praktické ukázky, čemu je dobré věnovat pozornost a jaká praktická opatření podniknout za účelem zajištění bezpečnosti IS v organizaci, s přihlédnutím ke každodenní práci s počítačem. Dokonce i ten nejlepší systém, software nebo správce počítačů nemohou zajistit bezpečnost dat, pokud v organizaci dochází k zanedbávání základních organizačních otázek bezpečnosti.Tato diplomová práce obsahuje odpovědi na otázky, které je třeba pokládat při provádění analýzy skutečného stavu bezpečnosti a zavádění opatření směřujících k minimalizaci rizik.

Podat všeobecně platný návod pro tvorbu zabezpečeného kvalitního informačního systému samozřejmě nelze. Každá firma má svá specifika, která ji odlišují od ostatních, každá instituce je svým způsobem jedinečná je také její informační systém. Práce nabízí řadu doporučení pro všechny pracovníky, kteří si uvědomují význam kvalitního řízení informačního zabezpečení a procesů probíhajících v jejich firmě a usilují o vytvoření efektivní řízené bezpečnosti informačního systému.

.

SEZNAM POUŽITÉ LITERATURY

Monografie:

[1] THOMAS M, T. *Zabezpečení počítačových sítí bez předchozích znalostí.* 1. vyd. Brno: CP Books, a. s., 2005. 344 s. ISBN 80-251-0417-6.

[2] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat.* 1. vyd. Brno: CP Books, a. s., 2004. 200 s. ISBN: 80-251-0106-1.

[3] NORTHCUTT, S. *Bezpečnost počítačových sítí.* 1.vyd. Brno: CP Books, a. s., 2005. 592 s. ISBN: 80-251-0697-7.

[4] LOCKHART, A. *Bezpečnost sítí na maximum.* 1. vyd. Brno: CP Books, a. s., 2005. 280 s. ISBN: 80-251-0805-8.

[5] TVRDÍKOVÁ, M. *Zavádění a inovace informačních systémů ve firmách.* 1. vyd. Praha: GRADA Publishing, a. s., 2000. 116 s. ISBN: 80-7169-703-6.

[6] VRANA, I., RICHTA, K. *Zásady a postupy závádění podnikových informačních systémů*. 1. vyd., Praha: GRADA Publishing, a. s., 2005. 188 s. ISBN: 80-247-1103-6.

Seriálová literatura:

[7] MIKULECKÝ J., SKALICKÝ M., *Data Security Management,* Čtvrtletník 03/2004 – 06/2004.

Internetové zdroje:

[8] *Microsoft Security* [online]. [cit. 2006-03-15]. Dostupné na WWW: <http://www.microsoft.com/cze/security/default.mspx>.

[9] *Internet ve státní správě a samosprávě* [online]. [cit. 2006-04-08]. Dostupné na WWW: <http://www.isss.cz>.

[10] *Národní bezpečnostní úřad* [online]. [cit. 2006-04-17]. Dostupné na WWW: <http://www.nbu.cz>.

[11] *SANS Security Policy Project* [online]. [cit. 2006-04-21]. Dostupné na WWW: <http://www.sans.org/resource/policies >.

[12] *CERT Software Engineering Institute* [online]. [cit. 2006-04-12]. Dostupné na WWW: <http://www.cert.org>.

[13] *Federal Office for Information Security* [online]. [cit. 2006-03-29]. Dostupné na WWW: <http://www.bsi.bund.de/english/index.htm>.

[14] *Boran Consulting* [online]. [cit. 2006-04-26]. Dostupné na WWW: <http:// www.boran.com >.

[15] *ISA server* [online]. [cit. 2006-04-28]. Dostupné na WWW: <http:// www.isaserver.org >.

Interní zdroje:

[16] JAŠEK R., *Závislost prosperity firmy na bezpečnosti informací*, 2005. 62 s.

[17] HANÁČEK P., STAUDEK J., *Bezpečnost informačních systémů*. Praha: Úřad pro státní informační systém, 2000. 127 s.

[18] *Průvodce zabezpečením pro malé organizace*. Microsoft Corporation, 2004. 51 s.

[19] *Příručka o ochraně dat pro veřejnou správu.* Microsoft Corporation, 2005. 47 s.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

IS	Informační Systém
IT	Informační Technologie
ICT	Information and Communication Technology
HW	Hardware
SW	Software
VPN	Virtual Private Network
FTP	File Transfer Protocol
WW W	World Wide Web
ISMS	Information Security Management System
LAN	Local Area Network
WAN	Wide Area Network
DNS	Domain Name Server
DMZ	Demilitarizovaná zóna
IDS	Intrusion Detection System
WPA	Wi-Fi Protected Access
WEP	Wired Equivalent Privacy
AP	Acces Point
MAC	Media Access Control

SEZNAM OBRÁZKŮ

SEZNAM TABULEK