Návrh řešení bezpečnostní politiky firmy z pohledu ochrany znalostí a dat

Project of security policy in light of protection knowledge and data

Pavel Polínek

Bakalářská práce
2008

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav elektrotechniky a měření
akademický rok: 2007/2008

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Pavel POLÍNEK**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Návrh bezpečnostní politiky z hlediska ochrany znalostí a dat**

Zásady pro vypracování:

Práce řeší problematiku bezpečnostní politiky konkrétní firmy z komplexního pohledu. Při práci budou využity volně dostupné internetové informační zdroje, odborná literatura a interní firemní materiály dle možností.

1. **Analyzujte dostupné informační zdroje vhodné pro řešení dané problematiky.**
2. **Stanovte postupy využitelné pro řešení bezpečnostní politiky a strategie firmy.**
3. **Navrhněte pro organizaci střední velikosti bezpečnostní politiku v souladu s normami EU.**
4. **Proveďte shrnutí svých zkušeností z pohledu přínosu, pozitiv i negativ.**

Rozsah práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **Volně dostupné internetové zdroje (portály profesních organizací, minsterstev a EU)**
2. **KRÁL, M. Bezpečnost domácího počítače. 1. vyd. Grada, 2006. 336 s. ISBn 8024714086**
3. **ENDORF, C.,SHULTZ, E., MELLANDER, J. Hacking. Detekce a prevence počítačového útoku. 1. vyd. Grada 2005. 336 s. ISBN 8024710358**
4. **JAŠEK, R. Informační a datová bezpečnost. 1. vyd. Academia centrum UTB, 2006. 140 s. ISBN 8073184567**
5. **DOSEDĚL, T. 21 základních pravidel počítačové bezpečnosti. 1. vyd. Computer press, a.s., 2005. 56 s. ISBN 8025105741**

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

Datum zadání bakalářské práce: **22. února 2008**

Termín odevzdání bakalářské práce: **3. června 2008**

Ve Zlíně dne 22. února 2008

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Ve své bakalářské práci se budu zabývat problematikou návrhu bezpečnostní politiky firmy z pohledu informační roviny. V teoretické části se pokusím objasnit pojem bezpečnost informačních systémů. Dále se budu zabývat materiály týkajících se komplexního řešení informační bezpečnosti, které zkomponuji do kroků vedoucích k jejímu zajištění. V praktické části se pokusím utvořit šablonu návrhu bezpečnostní politiky použitelnou pro firmy a organizace jakékoliv velikosti a uvedu analýzu konkrétní firmy.

Klíčová slova:

bezpečnostní politika, analýza rizik, audit

ABSTRACT

In my bachelor project I will solve problem of firm security policy in light of information level. In teoretic part I will try to explain conception security of information systems. Then I will deal with materials about complex projecting of information security, which I'll compose to steps leading to its ensure. In practical part I'll try to make template of security policy, which can be aplly for any size of organizations and I'll produce analysis of specific firm.

Keywords:

security policy, risk analysys, audit

Chtěl bych poděkovat vedoucímu mé práce doc. Mgr. Romanu Jaškovi, Ph.D., za jeho konstruktivní rady a čas, který do ně investoval. Dále taky své rodině, která mně podporuje ve studium a povzbuzuje k lepším výsledkům. A v neposlední řadě též všem autorům citované literatury, z které jsem si dovolil čerpat. Děkuji

Jako motto své práce bych rád uvedl známé rčení: „Může-li se něco pokazit, pokazí se to.“, které v průmyslu komerční bezpečnosti platí dvojnásob. Počítejme tedy s tím a připravme se na to!

Prohlašuji, že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků, je-li to uvolněno na základě licenční smlouvy, budu uveden jako spoluautor.

Ve Zlíně ……

Podpis diplomanta

OBSAH

ÚVOD

V dnešní době je práce s počítačem naprosto samozřejmá věc. K počítačům se také neodmyslitelně váže internet co by obrovské médium plné informací. S internetem je také spjata elektronická pošta hojně využívaná firmami a širokou veřejností. Můžeme říci, že elektronická komunikace značně usnadňuje přenos informací, což je velmi výhodné. Většina uživatelů si však neuvědomuje nebezpečí skryté v internetu a elektronické poště.

S nástupem informačních technologií a éry internetu přichází do hry také informační zabezpečení. Můžeme tvrdit, že v dnešní době jsou téměř všechny firmy a organizace plně nebo částečně závislé na informačních technologiích. Informace jsou mnohdy jedno z hlavních aktiv organizace, proto také vzniká potřeba je chránit. Ztráta nebo poškození choulostivých informací může organizacím či firmám způsobit nemalé škody.

Jako téma jsem si vybral návrh bezpečnostní politiky zaměřený na ochranu dat, protože datová bezpečnost je aktuální a rozvíjející se problematika. Dříve se návrhům bezpečnostních politik věnoval jen málokdo. V současnosti je situace opačná a stále více organizací a firem vynakládá prostředky na vytváření kvalitních bezpečnostních politik.

Cílem mé práce tedy je prozkoumat informační zdroje týkající se vytváření bezpečnostní politiky, zjistit co taková politika obsahuje, jak se vytváří a co všechno musí člověk znát, aby dokázal bezpečnostní politiku navrhnout a uvést k životu.

I. TEORETICKÁ ČÁST

1 BEZPEČNOST OBECNĚ

1.1 Teoretická bezpečnost

Pod pojmem bezpečnost si můžeme představit takový stav věci, při kterém chráněnému objektu nehrozí žádné nebezpečí a nemohou mu vzniknout žádné škody. Tento objekt je potom totálně zabezpečen.

1.2 Reálná bezpečnost

Z praxe ovšem víme, že dosáhnout stavu totálního zabezpečení je nemožné. Je tedy nasnadě pojem bezpečnost definovat do reálné roviny. Reálná bezpečnost tedy představuje takový stav věci, kdy míra hrozících nebezpečí, poškození, ztráty nebo zničení chráněného objektu je co nejnižší v důsledku provedených bezpečnostních opatření.

1.3 Bezpečný počítač

Z daných definic vyplývá, že bezpečný počítač může vypadat asi takto:

- není připojen k jiným počítačům a internetu
- je v něm naistalován pouze operační systém a programy nezbytné k chodu
- není používán žádným uživatelem
- je bezpečně uložen v trezoru, kam k němu nikdo nemůže

Takovýto počítač je pro potřeby informačních systému zcela nevhodný a můžeme ho bez nadsázky označit za „mrtvý“. Proto při návrhu bezpečnostní politiky vždy počítáme s tím, že nic není stoprocentní, ale snažíme se dosáhnout co možná nejvyšší míry zabezpečení za použití nejmodernějších technologií a postupů.

1.4 Informační bezpečnost (bezpečnost informačních systémů)

V dnešních dnech často slýcháme pojem informační bezpečnost nebo-li systémová bezpečnost. Co si pod těmito pojmy představit?

Již podle názvu můžeme usoudit, že tyto pojmy mají určitou spojitost s informacemi. V dnešní době rapidně stoupá počet firem, které jsou zcela či částečně závislé na práci s informacemi. Jakákoliv ztráta nebo poškození informací má pro tyto firmy katastrofální následek. Proto je velmi důležité tyto informace a všechno co se kolem nich točí chránit. Právě toto má za úkol informační bezpečnost.

Ve zkratce můžeme říci, že se zabývá ochranou:

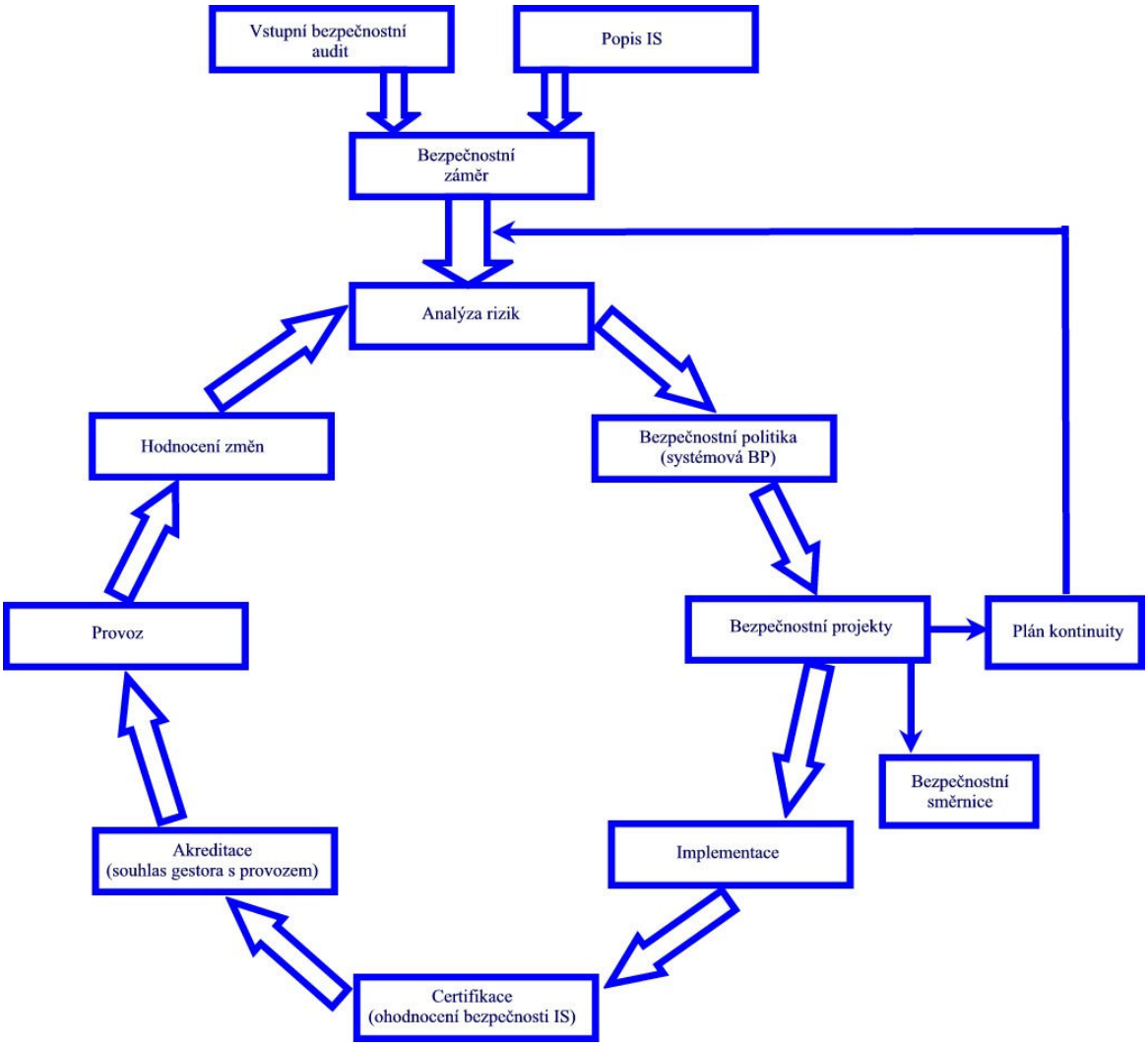
- informací
- přístupu k informacím
- informačních toků
- informačních systémů

S informacemi je bezprostředně spjata i výpočetní technika. To znamená, že při řešení informační bezpečnosti se budeme pohybovat víceméně v prostředí podnikových sítí a internetu. Internet v kombinaci se selháním lidského faktoru považujeme za jednu z největších hrozeb pro informační systémy.

2 KOMPLEXNÍ ŘEŠENÍ INFORMAČNÍ BEZPEČNOSTI

Před návrhem samotné bezpečnostní politiky si musíme ujasnit, jak vůbec budeme postupovat. Musíme vědět na jaký informační systém budeme bezpečnostní politiku aplikovat, přesně si určit bezpečnostní záměr, kterého chceme dosáhnout, provést analýzu rizik hrozících námi zabezpečovaném informačním systému. Při tom využíváme vlastních zkušeností, zavedených postupů a řídíme se příslušnými normami a legislativou.

Níže uvedené schéma zobrazuje možný postup při vytváření, komplexního řešení zabezpečení informačního systému. Obsahuje tvorbu bezpečnostní politiky, bezpečnostních projektů a plánu kontinuity a jejich zavedení do provozu, certifikaci, akreditaci a hodnocení změn.



obrázek 1 Návrh komplexního řešení informační bezpečnosti

Dosažení komplexní informační bezpečnosti je cyklický nikdy nekončící proces, což je ze schématu patrné.

V následujících kapitolách si přiblížíme jednotlivé bloky výše uvedeného schématu.

2.1 Popis informačního systému

Při popisu informačního systému sbíráme základní údaje o jeho funkcích a obsahu jeho vybavení. Zajímá nás např. topologie sítí, počet používaných počítačů a serverů, atd. Můžeme si to vysvětlit tak, že vlastně provádíme podrobnou inventarizaci. Výstupem potom bude zpráva obsahující seznam požadovaných funkcí systému a seznam použitého vybavení (jak hardware tak software). Tato zpráva nám pomáhá zjistit v jakém stavu se informační systém nachází. Podle toho pak realizujeme bezpečnostní opatření a případnou modernizaci či aktualizaci.

Zde uvedu stručný příklad nepodrobného popisu IS, jen pro představu:

Při popisu informačního systému nezávislé fiktivní firmy Independet Graphics bylo zjištěno:

- firma používá čtyři počítače
- internetové připojení je realizováno přostřednictvím kabelové televize
- počítače jsou propojeny mezi sebou do lokální sítě a každý z nich je individuálně připojen k internetu
- počítače běží na operačním systému Windows XP SP2
- jako firewall je použit Kerio Personal Firewall 4 free verze bez možnosti filtrování obsahu WWW
- jako antivirový program je použit avast!
- na všech počítačích je nainstalován prohlížeč webu Mozila Firefox
- každý počítač používá poštovního klienta Mozila Thunderbird
- atd.

„Popis IS je vhodnou součástí nebo předstupněm pro technický audit, audit informační strategie, případně analýzu rizik.“ [1]

2.2 Vstupní bezpečnostní audit

Úkolem bezpečnostního auditu je zjistit v jakém stavu se nachází bezpečnostní systém. Hlavním cílem je vyhledání slabých míst v zabezpečení a navrhnutí vhodných protiopatření, která sníží míru zranitelnosti. Dále pak zjišťuje co je třeba modernizovat a nebo úplně předělat.

„Bezpečnostní audit spočívá zejména v těchto oblastech:

- ověření bezpečnosti z hlediska vnitřních sítí (datové rozvody v budově, propojení poboček, virtuální privátní sítě atd.)
- ověření bezpečnosti z hlediska vnějších sítí (Internet, Extranet, napojení na parterské informační systémy)
- analýza přístupových práv počítačové sítě
- analýza zabezpečení přístupu autorizovaných osob
- analýza odolnosti Vašich systémů vůči počítačovým virům
- bezpečnost komunikace a přenosu dat
- zálohování dat
- ochrana uložených dat
- ochrana dat při výpadku napájení
- řešení krizových situací
- administrativní bezpečnost

Pro koho je bezpečnostní audit určen

Bezpečností audit je určen jak pro malé tak velké firmy, které pracují s informačními technologiemi. Není důležité, zda jste živnostník s několika počítači nebo velká firma s

mnoha pobočkami. Důležitá je cena Vašich dat, jenž je mnohdy nevyčíslitelná. Nemůžete čekat až se nějaký problém objeví, musíte jim předcházet a ochránit tak mnohdy nejcennější duševní vlastnictví Vaší společnosti.“ [2]

2.3 Bezpečnostní záměr

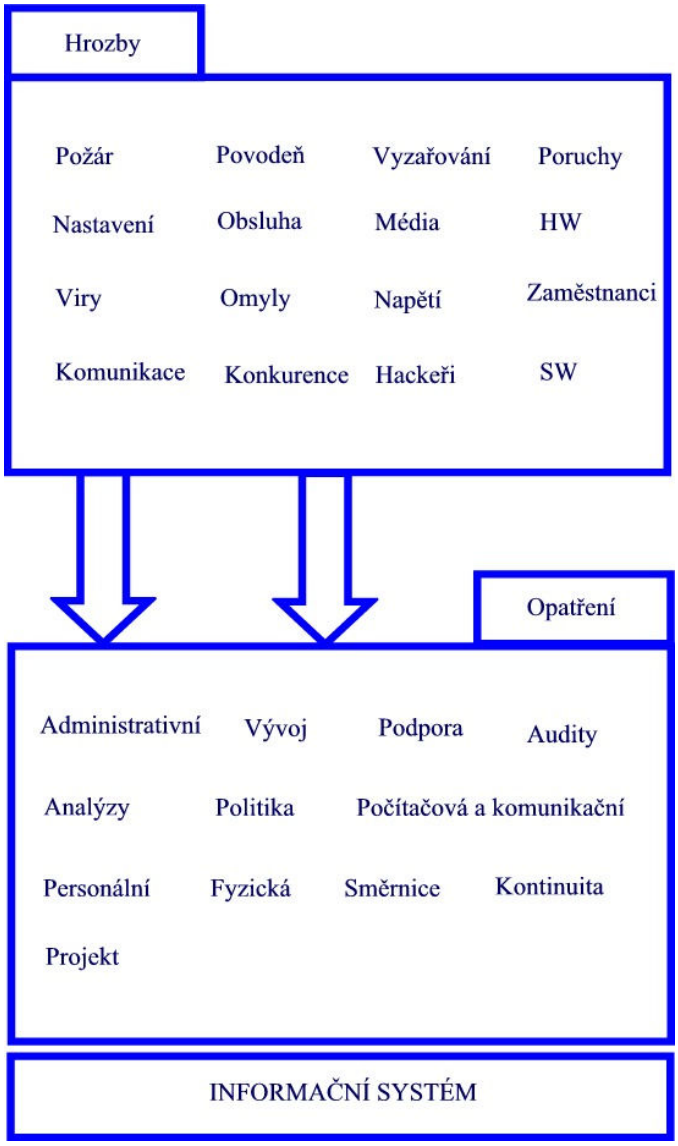
Bezpečnostní záměr definuje cíle, které chceme dosáhnout aplikací bezpečnostní politiky. Obvykle jej stanovuje nejvyšší management organizace. Při tom jako hlavní cíl považujeme ochranu aktiv organizace s čímž je bezprostředně spajt i bezproblémový chod organizace. Když to převedeme do konkrétní řeči, tak by se mohlo jednat např. o ochranu kritických procesů organizace, ochranu choulostivých informací, ochranu cenných zařízení, atd.

2.4 Analýza rizik

Žádná organizace se nenachází v bezrizikovém prostředí. Tato rizika nebo-li hrozby mohou být různého charakteru. Můžeme je rozdělit na tři základní kategorie:

- přírodní (povodně, zemětřesení, sopečné erupce, rozsáhlé požáry,…)
- způsobené člověkem (selhání lidského faktoru)
- technického charakteru nezaviněné člověkem (poruchy zařízení, únava materiálu,…)

Při návrhu komplexního řešení bezpečnosti organizace musíme s těmito riziky počítat. Jakékoliv opomenutí nebo chyba v úsudku může mít pro organizaci katastrofální dopady. Proto hraje analýza rizik v procesu zajištění bezpečnosti veledůležitou roli. Pomáhá nám totiž zjistit, která rizika organizaci bezprostředně hrozí, a která jsou naopak téměř zanedbatelná. V ČR se například sopečných erupcí obávat nemusíme. Analýza rizik musí být provedena důkladně (nejlépe specializovanou firmou) a bez chyb. Jakákoliv chyba by vedla k zavedení špatných a neúčinných bezpečnostních opatření. Toto by se v budoucnu při vzniku bezpečnostního incidentu mohlo stát organizaci osudným.



obrázek 2 Přehled rizik a opatření

„Analýza rizik zahrnuje:

- identifikaci aktiv
- identifikaci hrozeb
- ohodnocení aktiv
- určení pravděpodobnosti uplatnění hrozby
- určení zranitelnosti každého aktiva hrozbou

- výpočet hodnoty Riziko pro každou dvojici aktiva a hrozby

Riziko = Hodnota aktiva * Pravděpodobnost uplatnění hrozby * Zranitelnost

Při hodnocení rizik:

1. se zvažuje poškození aktiv, kde poškození může být způsobeno selháním bezpečnosti. Při hodnocení je nutno vzít v úvahu potenciální důsledky ze ztráty důvěryhodnosti, integrity nebo dostupnosti informací a jiných aktiv;

2. se posuzují reálné pravděpodobnosti výskytu chyb z pohledu převažujících hrozeb, zranitelnosti a aktuálně implementovaných opatření.“ **[3]**

Výsledkem analýzy rizik potom může být zpráva, která uvádí možná rizika ohrožující organizaci a jejich dopad na organizaci. Součástí tohoto dokumentu dále může být návrh bezpečnostních opatření. Výsledek analýzy rizik pomáhá vrcholovému managementu organizace stanovit priority při ochraně aktiv a určit, která bezpečnostní opatření budou zavedena.

Protože je má práce zaměřena na ochranu dat, přikládám tabulku, která vyobrazuje ohrožení datových aktivit.

Příklad ohrožení datových aktivit		
Úmyslné	**Náhodné**	**Přírodního rázu**
● odhalení/odposlech	● chyby a opomenutí	● zemětřesení
● podvod/narušení integrity	● vymazání souboru	● blesk
● narušení dostupnosti	● nesprávné směrování	● požár
● přisvojení/krádež	● fyzické nehody	● povodeň
		● elektrostatický výboj

obrázek 3 Přehled ohrožení datových aktiv[4]

2.5 Bezpečnostní politika

Pod pojmem bezpečnostní politika si představme dokument definující zásady a nařízení vedoucí k zajištění komplexní bezpečnosti organizace. Dříve se na bezpečnostní politiky tolik nedbalo, ale dnes je jejich vytváření trendem. To je zapříčiněno tím, že jak velké organizace tak i malé firmy si uvědomují důležitost ochrany proti stále se rozšiřujícímu počtu hrozících rizik. S nástupem informačních technologií a éry internetu do bezpečnostní politiky vstupuje další pojem nazvaný informační bezpečnost. V dnešní době jsou již firmy

či organizace zcela nebo částečně závisle na informačních technologiích. Bezpečnostní politika si tedy klade za cíl ochránit podniky proti ztrátám, vloupáním, rozkrádání, konkurenční špionáži, internetovým útokům, poškození dobrého jména firmy, požáry, haváriemi, povodněmi, atd. Souhrnně se tedy dá říci, že hlavním cílem bezpečnostní politiky je ochrana důležitých aktiv organizace a zajištění jejího bezproblémového chodu, tím že se snaží eliminovat či co nejvíce snížit míru hrozících rizik.

„Součástí Celkové bezpečnostní politiky je systémová bezpečnostní politika. Ta definuje, jakou architekturu používá informační systém, jaká je topologie sítě, jaké technologie (resp. Principy) by měly být využívány při provozu IS, jaká organizační pravidla je třeba dodržovat. Systémová bezpečnostní politika má za úkol zajistit aktiva, která jsou součástí IS. Jsou to technická zařízení (komunikační vrstva, výpočetní vrstva, podpůrná zařízení), logické nástroje (zpravidla SW) a v neposlední řadě data. Data bývají často jedním z nejcennějších aktiv, je třeba jim proto věnovat velkou pozornost.“ [5]

„Bezpečnostní politika pokrývá tyto oblasti informační bezpečnosti:

a) Organizaci a řízení bezpečnosti
b) Řízení aktiv
c) Personální bezpečnost
d) Fyzickou bezpečnost a bezpečnost prostředí
e) Řízení komunikací a provozu
f) Řízení přístupu
g) Pořízení, vývoj a údržba informačních systémů
h) Správa incidentů informační bezpečnosti
i) Řízení kontinuity činností organizace
j) Soulad s požadavky“ [6]

Za východiska považujeme především:

ČSN ISO/IEC 17799 Informační technologie – Soubor postupů pro řízení informační bezpečnosti,

ČSN ISO/IEC TR 13335 Informační technologie – Směrnice pro řízení bezpečnosti IT,

Information Security Management: Překlad a interpretace standardu BS 7799 pro české prostředí,

v oblasti norem, a těchto právních předpisů:

zákon č. 101/2000 Sb. O ochraně osobních údajů,

zákon č. 227/2000 Sb. O elektronickém podpise,

zákon č. 365/2000 Sb. O informačních systémech veřejné správy.

2.6 Bezpečnostní projekt

Bezpečnostní projekt konkrétně řeší realizaci navrhnuté bezpečnostní politiky. Popisuje použité bezpečnostní prvky a aplikaci informační, počítačové, komunikační, fyzické, personální a administrativní bezpečnosti. Při utváření bezpečnostního projektu vycházíme z bezpečnostních standardů a příslušných norem zabývajících se informační bezpečností. Dále také musíme dbát na to, aby bezpečnostní projekt byl v souladu se systémovou bezpečnostní politikou. Pro dosažení kýžených výsledků je velmi důležitá komunikace a spolupráce se zákazníkem.

„Při zpracování bezpečnostního projektu se řídíme těmito kroky:

1) Seznámení se s prostředím zákazníka.

2) Návrh bezpečnostních prvků podle požadavků bezpečnostní politiky.

3) Popis řešení a nastavení bezpečnostních prvků.

4) Předání díla.“ [7]

Jak vyplývá z výše uvedeného schématu musíme vzít v potaz při řešení bezpečnostního projektu bezpečnostní směrnice. Nedílnou součástí je také plán kontinuity.

Při navrhování bezpečnostního projektu se musíme řídit zejména těmito normami:

ČSN ISO/IEC 17799:2001

Informační technologie – Soubor postupů pro řízení informační bezpečnosti.

ČSN BS 7799-2:2004

Systém managementu bezpečnosti informací - Specifikace s návodem pro použití.

ČSN ISO/IEC TR 13335-1:1999

Informační technologie - Směrnice pro řízení bezpečnosti IT - Část 1: Pojetí a modely bezpečnosti IT.

ČSN ISO/IEC TR 13335-2:2000

Informační technologie - Směrnice pro řízení bezpečnosti IT - Část 2: Řízení a plánování bezpečnosti IT.

ČSN ISO/IEC TR 13335-3:2000

Informační technologie - Směrnice pro řízení bezpečnosti IT - Část 3: Techniky pro řízení bezpečnosti IT.

ČSN ISO/IEC TR 13335-4:2002

Informační technologie - Směrnice pro řízení bezpečnosti IT - Část 4: Výběr ochranných opatření.

ČSN ISO/IEC TR 13335-5 (zatím nevydáno)

Informační technologie - Směrnice pro řízení bezpečnosti IT - Část 5: Ochranná opatření pro externí spojení.

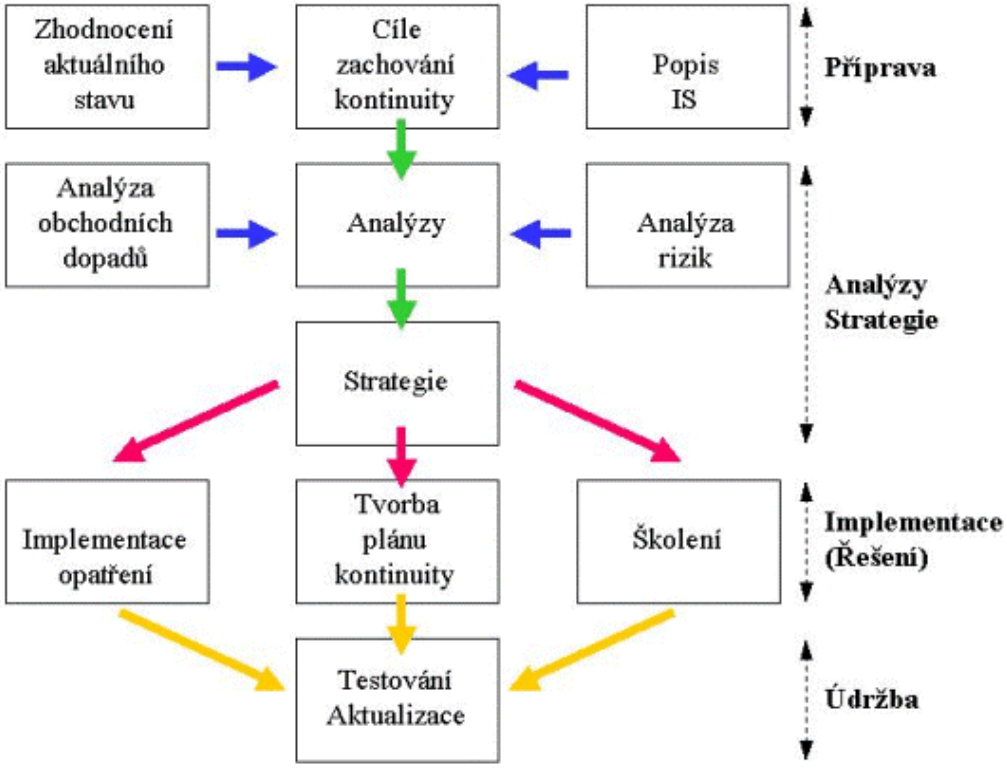
Legislativní předpisy evropské unie týkající se informačních technologií:

Směrnice 1997/66/ES *o ochraně dat v telekomunikacích.*
Směrnice 1995/46/ES *o ochraně osobních dat.*
Směrnice 2002/58/ES *o soukromí v elektronické komunikaci.*
Směrnice 1999/93/ES *o zásadách Společenství pro elektronické podpisy.*
Směrnice 2002/58/ES *o zpracování osobních údajů a ochraně soukromí.*
Nařízení 2001/45/ES *o ochraně fyzických osob při zpracování osobních údajů orgány a institucemi.*
Směrnice rady 1991/250/EHS *o právní ochraně počítačových programů.*
Směrnice rady 2001/264/EC *o ochraně utajovaných informacích.*

Plán kontinuity:

Plán kontinuity zajišťuje chod informačního sytému organizace v případech jako jsou mimořádná situace, havárie, vylepšení informačního systému nebo normálního chodu. Pokud tento plán není vypracován a nastanou výše popsané situace, tak se organizace může ocitnout na pokraji krachu informačního systému.

Postup vytváření plánu kontinuity:



obrázek 4 Návrh plánu kontinuity[8]

1. fáze: Příprava

V této fázi se provádí popis informačního systému (výše popsáno), zhodnocení aktuálního stavu a vytyčují se cíle zachování kontinuity.

Zhodnocení aktuálního stavu

Nám pomáhá vytvořit si kompletní obraz o zabezpečení informačního systému firmy. Zajímají nás hlavně provedená bezpečnostní opatření a to fyzická, režimová, informační a softwareová. Zkoumáme, jestli všechno funguje tak jak má, co by se dalo vylepšit a modernizovat popřípadě úplně změnit a to vše v zájmu prosperity a konkurence schopnosti firmy. Při hodnocení aktuálního stavu nám může pomoci výsledek provedeného bezpečnostního auditu. Na závěr hodnotíme stav zabezpečení informačního systému firmy. Všechny sesbírané informace a zjištěné skutečnosti doplněné vlastními názory, hodnocením a navrhovanými vylepšeními musíme uvést v písemné zprávě. Na základě této zprávy posléze stanovíme cíle zachování kontinuity.

Cíle zachování kontinuity:

Za hlavní cíl zachování kontinuity považujeme bezproblémový chod organizace a eliminaci nebo co největší zmírnění škod při vzniku mimořádných situací či havárií zapříčiněných živelnou pohromou, selháním lidského faktoru, poruchou zařízení, úmyslným útokem zevnitř či zvenčí a kriminální činností.

K cílům zachování kontinuity můžeme také přiřadit níže uvedené body.

Shrnuto v bodech:

1) **Prevence** – prevence znamená přípravu plánů a jejich realizační opatření, přípravu lidí i technických prostředků pro případ havárie. Na kvalitě prevence závisí četnost a kvalita výpadků a náklady na obnovu funkčnosti.
2) **Reakce na mimořádnou událost** – prvořadým zájmem každé společnosti je, aby škody vzniklé v případě havárie byly co nejmenší a co nejméně narušili chod

společnosti. Do této fáze spadá také ochrana zdraví a lidských životů. Probíhají činnosti k zastavení, omezení rozsahu či zpomalení události.

3) **Obnova kritických funkcí** – po prvotní reakci následuje obnova kritických procesů. Tato fáze má pro organizace velký význam, neboť zde se rozhoduje o velikosti následných škod, případně o samotné existenci organizace. Činnosti pracovníků se přitom řídí dle havarijních procedur. Jejich součástí je např. přesun provozu do náhradních prostor a náhradního zařízení, obnova provozu v nouzovém, havarijním stavu, atp.

4) Zotavení z mimořádné situace – další fází procesu obnovy je obnova podpůrných činností a celkové zotavení organizace z narušení. Obnovují se především takové funkce, které z hlediska časové dostupnosti a významu nejsou kritické, ale přesto se značnou měrou podílejí na kvalitě služeb, které organizace poskytuje.

5) **Obnova chodu** – v této fázi se obnovuje původní stav provozu IS, je zjištěn rozsah škod, jsou rekonstruovány budovy místnosti, zajištěna tachnika, SW prostředky a přechod provozu z havarijního do normálního stavu.

2. fáze Analýzy a strategie

Analýza obchodních dopadů

Při vytváření analýzy obchodních dopadů zjišťujeme a hodnotíme finanční dopad na organizaci při vzniku havárie a výpadku kritických procesů. Zaměřujeme se na výši ztrát a ušlých zisků, které mají dopad na postavení organizace na trhu a její konkurence schopnost.

Uveďme si malý příklad:

Internetová firma food online, zprostředkovává pomocí internetu objednávku a rozvážku různých druhů potravin a provozuje internetový obchod s potravinami. Z tohoto tvrzení plyne, že je firma zcela závislá na internetu. V důsledku zemětřesení dojde v regionu, kde

firma provádí svou činnost, k výpadku dodávky elektrického proudu a zhroucení internetového připojení. Jedná se o regionální krizovou situaci. Dodávku elektrického proudu se podařilo obnovit do dvou dnů a internetové připojení bylo opraveno po třech dnech. Po tuto dobu firma nemohla provozovat svoji činnost.

Úkolem analýzy obchodních dopadů je vyčíslení škod vzniklých ušlým ziskem nebo majetkovými ztrátami.

Ušlý zisk můžeme rozdělit do dvou kategorií:

1) ušlý zisk z předem domluvených zakázek majících se uskutečnit v době havárie
2) ušlý zisk ze spontánně vzniknuvších zakázek v době havárie (nedá se přesně vyčíslit, protože nemůžeme dopředu vědět kdo si co bude chtít objednat). Vyčíslení se dá provést pomocí zpracování zisků z jednotlivých dnů a vyhodnocením jejich průměru.

Při havárii došlo též k majetkovým ztrátám a ohrožení života pracovníka firmy, a to :

- vlivem dopravní nehody k poškození dodávkového vozidla firmy a znehodnocení převážené zásilky
- lehkému zranění řidiče dodávkového vozidla

Firma vlastní rezervní dodávkové vozidlo pro případ havárií, takže dočasná ztráta jednoho vozidla po dobu jeho opravy neovlivní množství přijímaných zakázek a tím také výši ušlých zisků.

Po dobu nepřítomnosti zraněného zaměstnance budou jeho práci vykonávat kolegové, aby nedocházelo ke ztrátám zakázek.

Do celkových finančních ztrát firmy potom musíme započítat:

- ušlý zisk
- opravu dodávkového vozidla
- léčbu, bolestné, nemocenskou zaměstnance
- vyplacení přesčasů pro zástupce zraněného zaměstnance

Analýza rizik

viz. kapitola 2.4

Provedené analýzy nám poskytují výstup pro stanovení firemních strategií.

Strategie

Při vytváření strategie zachování kontinuity přímo vycházíme z provedených analýz a na jejich základě vytváříme strategický dokument pro firemní management. Vycházíme z vyčíslených ztrát a optimalizujeme investice do konkrétních opatření zabraňujících vzniku mimořádných situací. Dále také navrhujeme dílčí procesy a procedury, způsoby školení zaměstnanců v případech mimořádných situací, aktualizujeme a vylepšujeme stávající opatření. Také se věnujeme managementu rizik, který zpracovává analýzy rizik a vytváří z nich podrobné zprávy. Toto odvětví je velmi důležité, neboť nám poskytuje s nadsázkou řečeno menší náhled do budoucna. Prostřednictvím analýzy možných rizik můžeme zvýšit preventivní opatření a vyvarovat se vzniku mimořádných situací.

3. fáze: Implementace (řešení)

Tvorba plánu kontinuity

Zde již tvoříme samotný plán kontinuity zabývající se postupy, nařízeními a opatřeními v případě vzniku mimořádné situace, která může přejít v krizi. Kvalitně vytvořený plán kontinuity pomáhá firmě tyto situace zvládnout a minimalizovat vzniklé škody.

Implementace opatření

Jedná se o řešení konkrétních opatření zabezpečení informačního systému, jak v rovině softwareové tak hardwareové a režimové.

Můžeme sem zařadit:

- zálohování dat a informací
- vytváření archívů pro zálohy
- zabezpečení počítačů pomocí firewall, antivirových programů
- stanovení režimových opatření
- určení priority práce s informacemi
- mechanické a elektronické zabezpečení informačních místností (např. serverovna)
- zajištění náhradních zdrojů elektrického proudu
- zabezpečení objektu kde se nachází cenné informace (firemní know-how, informace o obchodních partnerech, atp.) proti vloupání
- zabezpečeni pro případ živelných pohrom (např.protipovodňové zátarasy)
- blokování obsahu internetu pomocí firewall
- zabezpečení podnikového intranetu
- zajištění EPS

Školení

V případě mimořádné situace nebo havárie je důležité, aby zaměstnanci firmy věděli co mají dělat. Za tímto účelem jsou prováděna bezpečnostní školení (např. požární školení). Zodpovědnost za zvládnutí těchto situací přebírá bezpečnostní manažer a jeho tým. Tito lidé musí být také řádně proškoleni a musí vědět jak reagovat v krizových situacích.

4. fáze: Údržba

Testování a aktualizace

V této fázi již máme plán kontinuity hotoví a připravený na použití v případě mimořádných a krizových situacích. Ty ale nenastávají každý den, takže plán kontinuity může dlouhou dobu zůstat nepoužitý. Organizace či firma se ovšem vyvíjí a dochází u ní k změnám hardwareového, softwareového, personálního či režimového charakteru. Je tedy nasnadě tento plán v určitých intervalech aktualizovat, modernizovat a testovat jeho funkčnost. Aktualizaci doporučuji jednou ročně a testování minimálně dvakrát do roka v závislosti na provedených změnách v organizaci či firmě.

Nyní je hotový vypracovaný bezpečností projekt předložen ke schválení zákazníkovy. Pokud zadavatel nemá žádné výhrady, můžeme bezpečnostní projekt uvést do provozu nebo-li implementovat.

2.7 Implementace

Implementací rozumíme zavedení konkrétních opatření, montáž bezpečnostních systémů a prvků, instalaci potřebného software zabývajícího se informační bezpečností.

Pohybujme se nyní v rovině zabezpečení IS a uveďme si několik příkladů:

Montáž bezpečnostních systémů:

- zajištění objektu, kde se nachází informační uzly, archiv dat, firemní know-how, ale i počítače obsahující inforamace, proti vloupání, krádeži a poškození zařízení uchovávajících informace pomocí MZS a EZS
- zabezpečení objektu proti živelným pohromám

Instalace software:

- instalace a aktualizace firewall pro server
- instalace a aktualizace firewall na jednotlivé počítače mající přístup k podnikovému intranetu a internetu
- instalace a aktualizace antivirových programů na jednotlivé počítače ve firmě
- zabezpečení bezdrátové sítě
- využití možnosti filtrování obsahu internetu pomocí firewall
- instalace a aktualizace a zabezpečení poštovních klientů na jednotlivých počítačích
- využití šifrování zpráv

Režimová opatření:

- stanovení kdy kdo smí používat počítače
- určení priority práce s informacemi
- stanovení na co smí zaměstnanci počítače používat

2.8 Certifikace (ohodnocení bezpečnosti IS)

V této fázi hodnotíme provedení zabezpečení informačního systému a zjišťujeme, jestli je v souladu s normami. Normy ovšem nejsou závazné, proto se při návrhu bezpečnostní politiky a bezpečnostních projektů řídíme hlavně přáními a požadavky zákazníka a normy bereme jako užitečné vodítko. Je ale výhodné se norem držet, protože pak máme jistotu, že námi navrhovaná bezpečnostní opatření odpovídají bezpečnostním standardům.

2.9 Akreditace (souhlas gestora s provozem)

Nyní už jsme téměř na konci koloběhu návrhu informační bezpečnosti firmy. Námi vypracované materiály předkládáme gestorovi (osoba která celé naše úsilí financuje). Gestor může s navrhovanými projekty souhlasit nebo může mít určité výhrady a připomínky. V tomto případě musíme odstranit gestorem vybrané nedokonalosti a opravit je ke spokojenosti obou zúčastněných stran. Po odsouhlasení gestorem můžeme celé naše dílo uvést do provozu.

2.10 Provoz

Námi navržená bezpečnostní politika už je aplikovaná v provozu organizace. Nyní sledujeme jestli vše funguje správně. Může se stát, že to co jsme teoreticky navrhli, se v praxi příliš neosvědčuje a je třeba to změnit. Takovýchto změn se při provozu může vyskytnout více. Proto je důležité všechny nedokonalosti monitorovat. Je obecně známo, že nelze navrhnout stoprocentní bezpečnostní systém, a tak bychom tento fakt měli respektovat.

2.11 Hodnocení změn

Zde hledáme to nejlepší řešení, jak opravit nedokonalosti bezpečnostního systému objevené při jeho uvedení do provozu. Tato část návrhu informační bezpečnosti je velmi důležitá, neboť zde dochází ke zpětné vazbě a následnému vylepšování bezpečnostního systému.

II. PRAKTICKÁ ČÁST

3 NÁVRH BEZPEČNOSTNÍ POLITIKY

V této části mé bakalářské práce se pokusím stanovit zásady a kroky obecně platné při návrhu bezpečnostní politiky jakékoliv firmy.

Budu se zabývat pojmy:

- analýza hrozeb
- specifikace bezpečnostní politiky
- zavedení (implementace) a správa bezpečnostní politiky
- testování a audit
- krizové plány
- dokumentace

3.1 Analýza hrozeb

Při návrhu bezpečnostní politiky se bez kvalitní analýzy hrozeb neobejdeme. Špatně či nedůkladně provedená analýza rizik má téměř vždy za následek také špatně fungující bezpečnostní politiku. Při provádění této analýzy se zabýváme následujícími body:

- vymezení chráněných aktiv a jejich ohodnocení
- identifikace slabých míst aktiv
- identifikace rizik hrozících aktivům
- odhad pravděpodobnosti útoku na aktiva
- předpokládaný dopad útoku na aktiva
- zpracování opatření zabraňujících útokům
- odhad přínosu zavedených opatření

3.1.1 Vymezení chráněných aktiv a jejich ohodnocení

Každá firma, společnost či organizace disponuje svými určitými aktivy, tzn. substancemi, které mají specifickou hodnotu a v případě jejich poškození, odcizení, ztrátě nebo zničení by došlo ke škodám. Zajímá nás tedy:

- jak jsou aktiva mezi sebou provázána
- jaká je vazba mezi aktivy a okolním světem
- hodnota aktiv

Hodnota aktiv určuje míru jejich zabezpečení. Např. detailní plány vojenských operací mají jako aktivum nevyčíslitelnou hodnotu. Při jejich vyzrazení může dojít ke ztrátám na lidských životech. Tento fakt vyžaduje, aby byla co nejvíce zabezpečena.

Dá se tedy říci, že hodnotu aktiv nám určuje míra způsobené škody při jejich poškození.

3.1.2 Identifikace slabých míst aktiv

Slabé místo aktiva představuje jeho nejzranitelnější část. Tedy tu systému část na kterou bude s největší pravděpodobností veden útok. Při identifikaci těchto míst musíme dbát na běžené použití systému a zcela nahodilé použití systému.

„Zranitelná místa lze rozdělit podle obtížnosti jejich využití na:
· obtížně využitelná (malá pravděpodobnost zranitelnosti)
· využitelná (zranitelnost je možná)
· snadno využitelná (velká pravděpodobnost zranitelnosti)“ [9]

Nyní si uvedeme několik typických slabých míst:

- používaní slabých hesel
- nechráněná paměť hesel
- absence obměny hesel

3.1.3 Identifikace hrozeb

Zde si klademe za cíl, identifikovat hrozby a s nimi spojené možné útoky.

Útoky můžeme rozdělit do třech kategorií podle četnosti jejich výskytu:

- ojedinělé útoky (s malým výskytem)
- středně časté útoky
- velmi časté útoky (s vysokou pravděpodobností)

Dále můžem útoky dělit na:

- vnější (útok je vedený na systém z vnějšku, nejčastěji pomocí internetu)
- vnitřní (útok je veden zevnitř systému, pravděpodobně zaměstnancem)

Nejčastější příklady útoků:

- napadení hackery
- rozesílání škodlivého software (viry, červi, spamm, spyware, hoax, apd.)

3.1.4 Předpokládaný dopad útoku

Zde se zabýváme dopady úspěšných útoků na aktiva. Je nutno říci, že při každém úspěšném útoku vzniká organizaci škoda. Míru těchto škod určuje hodnota poškozeného aktiva. Pod pojmem vzniklá škoda si můžeme představit např. finanční ztráty (většinou udávané za rok), poškození dobrého jména a pověsti organizace, vyzrazení citlivých informací, znehodnocení důležitých dat apod.

3.2 Specifikace bezpečnostní politiky

Provedená analýza hrozeb slouží jako podklad pro vytvoření bezpečnostní politiky. Specifikací potom rozumíme objasnění funkcí, které od systému požadujeme. Tato může být formulována neformálně, čili běžným hovorovým jazykem (čeština nebo angličtina) nebo matematicky pomocí jazyků k tomu určených. Z toho plyne, že výstupem bude dokument obsahující směrnice a nařízení.

Na základě analýzy rizik, kde jsme identifikovali a ohodnotili aktiva, můžeme nyní definovat bezpečnostní požadavky. Jejich cílem je co nejvíce snížit míru hrozících rizik.

K dosažení těchto cílů slouží bezpečnostní opatření. Jsou to vlastně obranné mechanizmy proti hrozbám. Nejdříve ale musíme globální hrozby rozdělit na jednotlivé dílčí hrozby. Po té na každou hrozbu aplikujeme bezpečnostní opatření. Podle charakteru hrozby může jít o softwareové aplikace, služby, režimová opatření, personální opatření či fyzická opatření.

Bezpečnostní opatření plní bezpečnostní procedury, které popisují zavedení požadovaných bezpečnostních funkcí. Tyto musí být v souladu s bezpečnostní politikou a musí odpovídat míře hrozících rizik.

3.3 Implementace a správa bezpečnostní politiky

Bezpečnostní politika představuje dokument obsahující směrnice, nařízení a doporučení. Procesem implementace tedy rozumíme její oživení a zavedení do praxe. Můžeme jej tedy chápat jako zavedení navrhnutých bezpečnostních opatření.

Tyto buď realizujeme sami, pakliže organizace obsahuje odbor security nebo využijeme služeb specializovaných externích firem.

Aby bezpečnostní politika fungovala správně, musí být srozumitelná, závazná, vynutitelná a vztahovat se bez výjimky na celou organizaci.

Protože se mění prostředí, ve kterém se organizace nachází a technologie jde dopředu, je nutné bezpečnostní politiku spravovat, aby i nadále vyhovovala požadavkům organizace. Rozumějme tomu tak, že jde o modernizaci, aktualizaci a přidávání nových funkcí. Je proto výhodné, vytvořit si tzv. útvar pro správu bezpečnostní politiky.

Jeho součástí by měly být:

- správa závad a chyb
- správa nastavení
- správa auditu
- správa bezpečnostních programů

3.4 Testování a audit

Když už je bezpečnostní politika implementována, je nasnadě ověřit její bezchybné fungování. K tomuto účelu slouží testování. Dříve než začneme s testováním, musíme mít vypracovaný a definovaný plán testů. Náhodné testování není průkazné. Jestliže se na

tvorbě bezpečností politiky podílela i externí specializovaná firma, měla by provést testy dodaných produktů a předložit výsledky.

Další možností ověření bezchybné funkce systému je audit.

3.4.1 Audit

Audit hraje důležitou roli při zjišťování narušení bezpečnosti. Také ho využívám v tzv. „posmrtné“ analýze. Kde nám pomáhá zjistit proč vznikl bezpečnostní incident.

Audit může být buďto interní nebo externí.

Pokud se jedná o interní audit, pak žádný z auditorů nesmí členem odboru security. A to proto abychom zabránili střetu zájmů. V případě rozsáhlé bezpečnostní politiky bych raději doporučil provést externí audit firmou, která se zabývá přímo touto problematikou. Je to sice finančně nákladnější řešení, ale za to kvalitnější.

Výstupem auditu je auditní zpráva. Zdali byl audit úspěšný můžeme vyjádřit tímto ohodnocením:

A+ - vyhovuje bez výhrad

A - vyhovuje podníněně

B - nevyhovuje

Při provádění bezpečnostního auditu se řídíme těmito vzory:

- auditní osnova
- auditní model
- auditní matrice

3.5 Krizové plány

Organizace bez zpracovaných krizových plánů riskují svou existenci. Je dosti naivní myslet si, že díky zavedeným bezpečnostním opatřením nám už žádné riziko nehrozí. V otázce bezpečnosti totiž není nic stoprocentní. Krizové plány určují postupy v případech útoků, mimořádných situací a havárií. Jejich úkolem je zajistit plynulý chod organizace a co nejvíce zmírnit škody v průběhu mimořádných situací.

V plánu by mělo být stanoveno, jak reagovat při vzniku havárie s ohledem na ochranu lidských životů a co největší snížení škod na životním prostředí a majetku organizace. Plán musí počítat s ohrožením života a zdraví zaměstnanců, vyřazením určitých funkcí systému a poškozením či zničením zařízení nebo procesů. Můžeme ho rozdělit do čtyř fází.

3.5.1 1. fáze: Okamžitá reakce

V první fázi se jedná o zjištění okamžitého stavu systému v době havárie a její likvidaci.

Klademe důraz na zamezení šíření havárie a odstranění nejtěžších škod.

3.5.2 2. fáze: Obnova kritických procesů

V druhé fázi řešíme obnovu kritických procesů organizace. Jsou to takové procesy, které při svém přerušení způsobují největší ztráty organizaci.

3.5.3 3. fáze: Zotavení

Třetí fáze je pak fáze zotavení z havárie. Zde se snažíme dostat systém organizace opět do normálního chodu. Odstraňujeme závady lehčího charakteru a škody dlouhodobého charakteru, které nebylo možno odstranit v 1. fázi. Tato fáze je ze všech nejdelší.

3.5.4 4. fáze: Analýza havárie

Analýzu provádíme proto, abychom zjistili odpovědi na tyto otázky:

- Co se stalo?
- Proč se to stalo?
- Jak se to stalo?
- Kdo je za to zodpovědný?
- Dalo se tomu zabránit?
- Které z opatřeních selhalo a proč?
- Jak se tomu dalo zabránit?
- Jak se takovýmto situacím v budoucnu vyhnout?
- Jaká zavést protiopatření, aby se situace neopakovala?

3.6 Dokumentace

Není- li bezpečnostní politika řádně zdokumentována, nelze ji brát vážně. Jak jsem uvedl výše ve své práci, bezpečnostní politika musí být závazná a vynutitelná, jinak nebude správně fungovat. Proto jejím výstupem musí být srozumitelný dokument. Doporučuji, aby tento dokument obsahoval:

- specifikaci systému
- seznam bezpečnostních opatření a procedur a informace o jejich nastavení

4 ANALÝZA KONKRÉTNÍ FIRMY

V této části uvedu analýzu konkrétní firmy mého známého, který si nepřeje aby jeho jméno i jméno firmy bylo zveřejněno

4.1 Několik slov o firmě

Firma se zabývá výrobou, distribucí a servisem celoodpružených rámů horských kol určených především pro sjezdové disciplíny. Firma obsahuje 18 lidí. Nacházejí se zde konstruktéři, designéři, svářeči, dva firemní jezdci, obchodní ředitel a finanční ředitel. Kolektiv je víceméně mladý a komunikace probíhá na přátelské úrovni.

4.2 Cíl plánu zabezpečení

Firma si je vědoma možných rizik, které jí hrozí, ale také připouští, že její zabezpečení není zrovna ideální. To je hlavní důvod proč chtějí vytvořit plán zabezpečení. Při vytváření tohoto plán jsme, ale limitováni hlavně finančními možnostmi firmy. Nemůžeme si dovolit dokonalé zabezpečení na armádní úrovni. Cílem potom bude dosáhnout relativně kvalitního zabezpečení, aniž bychom vynaložili horentní sumy na jeho realizaci.

Jako hlavní cíle tedy můžeme uvést:

- identifikaci rizik
- zlepšení prevence
- návrhy krizových plánů a postupů

4.3 Vstupní bezpečnostní audit

Provedl jsem vstupní bezpečnostní audit, abych zjistil jaké úrovně dosahuje informační bezpečnost firmy, ale také i zabezpečení z hlediska fyzické roviny.

4.3.1 Síť, systém a počítače

Klientské počítače: 10

Přenosné počítače: 2 (oba ředitelé)

Server: Microsoft Windows 2003

Připojení k internetu: pomocí kabelového modenu o rychlosti 2Mb/s

Tiskárny: 2 + plotr používaný k tisku velkoformátových výkresů

Výsledek informačního auditu

	počítač 1	počítač 2	počítač 3	počítač 4	počítač 5	počítač 6	počítač 7	počítač 8	počítač 9	počítač 10	přenosný 1	přenosný 2
antivir	ne	ano	ano	ano	ne	ano	ano	ano	ano	ano	ano	ano
personální firewall	ne	ne	ne	ne	ne	ne	ne	ne	ne	ne	ano	ano
aktualizace OS	ano	ano	ano	ano	ano	ano	ano	ano	ano	ano	ano	ano
aktualizace virové databáze	ne	ne	ne	ne	ne	ne	ne	ne	ne	ne	ne	ne
filtr nevyžádané pošty	ne	ne	ne	ne	ne	ne	ne	ne	ne	ne	ne	ne
antispyware	ne	ne	ano	ano	ne	ne	ano	ano	ano	ne	ano	ano
internetový prohlížeč	IE	MF	MF	MF	IE	IE	MF	MF	IE	MF	MF	MF
aktualizace int. Prohlížeče	ne	ano	ano	ano	ne	ne	ano	ano	ne	ano	ano	ano
poštovní klient	MO	MO	MO	MO	MO	MO	MO	MO	MO	MO	MO	MO

tabulka 1 Výsledek informačního auditu

Vysvětlivky:

IE – Internet Explorer

MF – Mozilla Firefox

MO – Microsoft Outlook

Použitý antivir: Avast!

Použitý personální firewall: Kerio Personal Firewall 4 free verze

4.3.2 Informační zabezpečení

Při stanovení úrovně zabezpečení jsem použil bezplatný nástroj Microsoft Baseline Security Analyzer (MBSA), který kontroluje samostatné systémy nebo více systémů v síti a hledá chybné konfigurace a chybějící aktualizace zabezpečení. Dospěl jsem k těmto výsledkům:

***Brána firewall*:** realizována je pouze serverová brána firewall, personální firewall na klientských počítačích chybí. Na přenosných je nainstalován.

Antivirová ochrana: chybí na dvou počítačích, na ostatních není aktualizovaná.

Software pro filtrování nevyžádané pošty: celá firma využívá poštovní klient Microsoft Outlook, který má omezenou funkci filtrování ne vyžádané pošty, ale tato funkce je aktivována pouze na dvou počítačích.

Hesla: firma používá slabá hesla a navíc bylo zjištěno, že je někteří zaměstnanci mají napsaná na papírku pod klávesnicí.

Aktualizace: všechny počítače běží na systému Microsoft Windows XP Professional SP2, které si sami vyhledávají a stahují aktualizace přes internet.

Používání internetu: firma nepoužívá nástroje k filtrování obsahu webu, bezpečné použití internetu je tedy na každém zaměstnanci. Všem zaměstnancům byly sděleny zásady bezpečného použití internetu, dodržování těchto zásad však není vynutitelné.

Fyzické zabezpečení: z hlediska MZS je firma zabezpečena uspokojivě.

Přenosné počítače: nejsou vybaveny sériovými čísly ani evidenčními identifikačními prvky.

Zálohování dat: provádí se jednou měsíčně, a to pouze data na serveru. Je tedy nutné, aby zaměstnanci důležitá data kopírovali na server.

4.3.3 Identifikace aktiv

Hlavními aktivy firmy jsou:

- know – how
- konstrukční návrhy nových produktů
- uzavřené smlouvy s dodavateli a odběrateli a informace o nich
- finanční informace
- informace personálního charakteru
- e-mailová databáze

Všechna tyto aktiva jsou považována za tajná, měla by být použita pouze v případě nouze.

4.3.4 Identifikace rizik

Rizika můžeme rozdělit do čtyř kategorií:

1. Útočníci: jedná se o nebezpečí spojené s používáním internetu, každý kdo je připojený se stává potenciálním terčem útoku (viry, wormy, trojské koně, neautorizovaný přístup, zneužití nebo škodlivé použití software, atd.). Vysoké riziko, vysoká priorita.

2. Externí ohrožení (zloději, konkurence, nespojení bývalý zaměstnanci). Tyto osoby mohou využívat stejné nástroje jako útočníci, jejich útoky jsou cílené se záměrem poškodit nebo odcizit informace nebo vybavení. Můžeme sem zařadit i sociální inženýrství, což je vlastně vyzvídání informací. Nabytých informací mohou potom tito útočníci využít k vydírání nebo úplné destrukci firmy. Vysoké riziko, vysoká priorita.

3. Interní ohrožení: útok vedený zevnitř firmy, může být úmyslný nebo se může jednat o neúmyslné vyzrazení důvěrných informací. Nízké riziko, nízká priorita

4. Katastrofy a nehody (požár, záplava, sopečné erupce, zemětřesení, porucha hardware, kolaps počítače, atd.). Nízké riziko, středně vysoká priorita.

4.4 Stanovení priorit

1. Ochrana proti útokům:

- použití a správná konfigurace brány firewall
- použití antivirových programů a aktualizace virových databází
- pravidelné aktualizace operačního systému
- použití silných hesel
- školení uživatelů a zásady bezpečného užívání

2. Ochrana proti krádežím a sociálnímu inženýrství:

- zabezpečení přenosných počítačů
- umístění serveru a databází v chráněných prostorech
- evidenční čísla přenosných počítačů
- pravidelná inventura majetku
- důsledná skartace důvěrných dokumentů
- školení zaměstnanců týkající se sociálního inženýrství

3. Ochrana proti haváriím:

- častější zálohování dat
- testování záloh
- umístění zálohovacích databází mimo firmu
- umístění důvěrných dokumentů mimo firmu a s tím spojené zabezpečení

4. Ochrana proti interním útokům:

- použití silných hesel
- školení zaměstnanců
- zabezpečení tiskáren pro obchodní zástupce
- udržování přátelské atmosféry na pracovišti

4.5 Plán zabezpečení

Stručné shrnutí v bodech:

1. Zakoupení, instalace a správná konfigurace personálního firewall na všechny firemní počítače.
2. Zakoupení, instalace, správná konfigurace a pravidelná aktualizace antivirového programu na všechny firemní počítače.
3. Nastavit v poštovním klientu funkci filtrování nevyžádané pošty.
4. Ujistit se, že operační systém všech počítačů je aktualizovaný a správně nakonfigurovaný.
5. Zajistit používání silných hesel a uvědomit zaměstnance jak s nimi zacházet.
6. Provádět častěji zálohování dat (jednou týdně) a testování záloh.
7. Umístit server do chráněného prostoru.
8. Vyhradit jednu tiskárnu pouze obchodnímu oddělení, aby mohli bezpečně tisknout důvěrné dokumenty.
9. Označit přenosné počítače evidenčními čísly.
10. Proškolit zaměstnance ohledně informační bezpečnosti.

Tento projekt slouží pouze jako informační materiál. Žádná z navrhovaných rad zatím nebyla aplikována.

ZÁVĚR

Cílem bakalářské práce bylo objasnění pojmu bezpečnostní politika. Zaměřil jsem se na důvody vytváření bezpečnostních politik a jejich praktickou aplikaci. Než jsem se ale dostal do této fáze, musel jsem prostudovat spoustu materiálu týkajících se informační bezpečnosti.

Při vytváření bezpečnostní politiky musí mít projektanti komplexní přehled o organizaci, pro kterou bezpečnostní politiku navrhuje. Dále si musí stanovit jasné cíle čeho chce aplikace bezpečnostní politiky dosáhnout. Aby tato byla účinná, je nutno provést detailní analýzu rizik. Odvažuji se říci, že to je stěžejní krok při vytváření bezpečnostní politiky. Chybná analýza se může lehce stát cestou do pekel.

Jak jsem také zjistil, bezpečnostní politiku nemůže navrhnout sám jeden člověk. Jedná se o kolektivní dílo, kde všechny zúčastněné strany musí mezi sebou komunikovat. Jen tak se dá dosáhnout kýženého výsledku.

Je tedy zřejmé, že vytvoření bezpečnostní politiky je náročný a dlouhodobý projekt. Můžeme říci, že tento projekt nikdy nekončí, protože je třeba již fungující bezpečnostní politiku aktualizovat a přizpůsobovat požadavkům organizace, tak aby plně vyhovovala aktuálnímu stavu v organizaci.

Ve své práci jsem se snažil proniknout do všech oblastí návrhu bezpečnostní politiky a řešil jsem postup jak dosáhnout informační bezpečností ve firmě, objasnil jsem pojem informační bezpečnost, navrhl jsem šablonu řešení bezpečnostní politiky organizací a firem jakékoliv velikosti. Dospěl jsem k těmto závěrům:

Při návrhu bezpečnostní politiky se musíme zabývat těmito pojmy.

Analýza hrozeb: pojmenovává rizika a určuje jejich dopady na chráněná aktiva organizace.

Specifikace bezpečnostní politiky: určuje požadované funkce bezpečnostní politiky.

Zavedení (implementace) a správa bezpečnostní politiky: zabývá se oživením bezpečnostní politiky a spravuje ji, aby dokonale plnila svoji funkci.

Testování a audit: prověřuje správné funkce bezpečnostní politiky.

Krizové plány: stanovují postupy v krizových situacích.

Dokumentace: dává bezpečnostní politice hmotnou podobu.

ZÁVĚR V ANGLIČTINĚ

The goal fo my bachelor project was expalin conception of security policy. I focused on reasons to creating security policys and their practical aplication. Before I have reached to this phase, I must read through lot of materials about information security.

Projectors must have a complex survey about organization, when they creating security policy. Also they have to state clear goals of aplication security policy. We must do the risk analysys for the right effect of security policy. I think this is the pivotal step of creating security policy. Wrong analysys can be a road to hell.

I also realized that no one can project security policy alone. It's a collective work, where all parties concerned must communicate with each other. Taht is a true way to reach the right result.

Is evident, that the creating of security policy is difficult and long-time project. we can say, that this project never ends, because already functional security policy needs to update and adapt to organization requirements, so as to fully agrees with actual state in organization.

In my project I tryed to penetrate to all parts of projecting security policy and I solved a proces to achieve informatic security in organization, I cleared up conception of informatic security, I projected model of security policy of any size organizations and firms. I arrive to these conclosions:

When we project security policy we must deal with these conceptions

Risk analysys: it names risks and specifys their falls on protected active capital of organization.

Specification of security policy: specifys required fuctions of security policy.

Installing and repairing srcurity policy: deals with resurengence of security policy and manages it, so as to performs its functions totally.

Testing and auditing: checka right functions of security policy.

Krisis plans: determines advancements in critical situations.

Documentation: gives material shape to security policy.

SEZNAM POUŽITÉ LITERATURY

[1] Popis IS, *Www.tsoft.cz/files/yrchive/21.pdf* [online]. 1991-2002 [cit. 2008-05-06]. Dostupný z WWW: <http://www.tsoft.cz/files/archive>.

[2] Bezpečnostní audit (v čem spočívá, pro koho je určen) *Www.westcom.cz : Bezpečnostní audit - Informačních systémů a sítí* [online]. 1998-2008 [cit. 2008-04-27]. Dostupný z WWW: <http://westcom.cz/bezpecnostni_audit.php>.

[3] Analýza rizik, *Www.tsoft.cz : Analýza rizik* [online]. 1998 [cit. 2008-05-07]. Dostupný z WWW: <http://www.tsoft.cz/index.php?q=cz/analyza-rizik>.

[4] Přehled ohrožení datových aktiv, MARťÁK, Pavel. Bezpečnost dat v praxi. *IT Systems* [online]. 2005 [cit. 2008-05-07]. Dostupný z WWW: <http://www.systemonline.cz/clanky/bezpecnost-dat-v-praxi.htm>.

[5] Celková bezpečnostní politka, *Www.gity.cz : BEZPEČNOSTNÍ POLITIKA (CBP, SBP)* [online]. 2008 [cit. 2008-05-07]. Dostupný z WWW: <http://www.gity.cz/cz/zakaznicka-reseni/bezpecnost-it/bezpecnostni-politka-cbp-sbp/>.

[6] Pokrytí oblastí informační bezpečnosti, *Standardy a doporučení_06_NSIB_CR_Priloha_2*. [s.l.] : [s.n.], 2005. s. 0-14.

[7] Zpracování bezpečnostního projektu, *Www.tsoft.cz : Bezpečnostní projekt (příručky)* [online]. 2008 [cit. 2008-05-07]. Dostupný z WWW: <http://www.tsoft.cz/index.php?q=cz/bezpecnostni-projekt>.

[8] Návrh plánu kontinuity, *Www.tsoft.cz : Plán kontinuity IS* [online]. 2008 [cit. 2008-05-07]. Dostupný z WWW: <http://www.tsoft.cz/index.php?q=cz/plan-kontinuity-is>.

[9] Zranitelná místa aktiv, TUČEK, Pavel. *Bezpečnostní politika rozsáhlé uživatelské počítačové infrastruktury*. [s.l.], 2007. 60 s. Vedoucí diplomové práce Ondřej Krajíček.

KRÁL, M. Bezpečnost domácího počítače. 1. vyd. Grada, 2006. 336 s. ISBn 8024714086

ENDORF, C.,SHULTZ, E., MELLANDER, J. Hacking. Detekce a prevence počítačového útoku. 1. vyd. Grada 2005. 336 s. ISBN 8024710358

JAŠEK, R. Informační a datová bezpečnost. 1. vyd. Academia centrum UTB, 2006. 140 s. ISBN 8073184567

DOSEDĚL, T. 21 základních pravidel počítačové bezpečnosti. 1. vyd. Computer press, a.s., 2005. 56 s. ISBN 8025105741

LAUCKÝ, V. Technologie komerční bezpečnosti II. 2. vyd. Academia centrum UTB, 2007. 123 s. ISBN 978-80-7318-631-9

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

IS	Informační systém
BP	Bezpečnostní politika
ČR	Česká Republika
MZS	Mechanický zábranný systém
MBSA	Microsoft Baseline Security Analyzer
MF	Mozilla Firefox
OS	Operační systém
MO	Microsoft Outlook
IE	Internet Explorer

SEZNAM OBRÁZKŮ

SEZNAM TABULEK