

ABSTRAKT

Abstrakt česky

V této bakalářské práci najdete kapitoly jednak věnované popisu hrozeb pro informační systém podniku (vnitřní - zaměstnanci; vnější – viry, útoky hackerů atd.), ale zejména se zabývá praktickými prostředky k ochraně dat a informací jako je biometrika, šifrování, elektronický podpis, PGP, firewally, zálohování dat a hlavně tvorbou bezpečnostní politiky podniku, koncepcí ochrany informačního systému s důrazem na analýzu rizik a na závěr popisuje chyby, kterých je možné se dopustit při řešení projektu informačního systému, potažmo informačních technologií.

Abstrakt ve světovém jazyce

In this Bachelor thesis you can find chapters dedicated to the description of the threats for the company information system (internal - employees, external - viruses, hacker attacks etc.) but it is mainly concentrated in the practical solutions for the data and information protection, such as biometry, encryption, electronic signature , PGP, firewalls, data backup and the company security policy creation, conception of information system protection with emphasis on the risk analysis. In the conclusion it describes faults possibly committed during the information system or information technology projects solving.

Rád bych poděkoval vedoucímu mé bakalářské práce Mgr. Romanu Jaškovi, Ph.D, za rady a připomínky k práci.

ÚVOD.....	9
1 ZÁKLADNÍ PRINCIPY BEZPEČNOSTI PŘI POUŽITÍ IT.....	11
1.1 MOTIVACE PRO ZABEZPEČOVÁNÍ PŘI POUŽITÍ IT	11
1.2 BEZPEČNOSTNÍ MECHANISMY.....	14
1.3 ZÁSADY VÝSTAVBY BEZPEČNOSTNÍ POLITIKY IT	15
1.4 TYPY BEZPEČNOSTNÍCH POLITIK	15
2 BIOMETRICKÉ SYSTÉMY V PRAXI.....	17
2.1 JAK AUTENTIZOVAT?.....	17
2.2 AUTENTIZACE A JEJÍ METODY.....	17
2.2.1 Autentizace heslem:	18
2.2.2 Autentizace předmětem:.....	19
2.3 JAK PRACUJÍ BIOMETRICKÉ SYSTÉMY?	19
2.4 VÝHODY BIOMETRIKY:.....	20
2.5 NEVÝHODY BIOMETRIKY	20
2.6 POUŽITÍ BIOMETRIKY V PRAXI:	21
2.7 BEZPEČNOSTNÍ OPATŘENÍ.....	22
3 POČÍTAČOVÁ INFILTRACE.....	24
3.1 VIRY.....	24
3.1.1 Přehled přímých škod způsobených viry:	24
3.1.2 Přehled nepřímých škod způsobených viry:	25
3.1.3 Vzorový postup odvírování počítače:	25
3.2 TROJSKÉ KONĚ (TROJANI)	27
3.2.1 Password-stealing trojani (PWS)	27
3.2.2 Destruktivní trojani	27
3.2.3 Dropper	28
3.2.4 Backdoor	28
3.2.5 Downloader (TrojanDownloader).....	28
3.2.6 Proxy Trojan (TrojanProxy).....	29
3.3 BACKDOOR.....	29
3.3.1 IRC	29
3.4 ČERVI (WORMS)	30
3.5 SPECIÁLNÍ PŘÍPADY INFILTRACE.....	31
3.5.1 Spyware.....	31
3.5.2 Adware	31
3.5.3 Hoax	32
3.5.4 Dialer.....	32
3.5.5 rhybaření (phishing)	33
3.5.6 Pharming	34
4 ZÁKLADY ŠIFROVÁNÍ A KRYPTOANALÝZY:.....	36
4.1 ALGORITMY PRO SYMETRICKÉ ŠIFROVÁNÍ:.....	38

4.1.1	1.DES	38
4.1.2	2.IDEA	39
4.1.3	3.Blowfish	40
4.1.4	Shrnutí symetrického šifrování (systémy se soukromými klíči):.....	40
4.2	ALGORITMY PRO NESYMETRICKÉ ŠIFROVÁNÍ:	41
4.2.1	RSA	41
4.2.2	Digitální podpis:.....	42
4.3	PGP - PRETTY GOOD PRIVACY (DOCELA DOBRÉ SOUKROMÍ).....	45
5	BĚŽNÁ OHROŽENÍ ZABEZPEČENÍ V SÍTÍCH.....	48
5.1	PŘEDSTÍRÁNÍ IDENTITY (SPOOFING)	48
5.2	NEOPRÁVNĚNÉ ZMĚNY (TAMPERING).	48
5.3	ODVOLATELNOST (REPUDIATION).	48
5.4	ZVEŘEJNĚNÍ INFORMACÍ (INFORMATION DISCLOSURE).	49
5.5	ODEPŘENÍ SLUŽBY (DENIAL OF SERVICE).	49
5.6	ZVÝŠENÍ OPRAVNĚNÍ (ELEVATION OF PRIVILEGE).	49
6	FIREWALLY	51
6.1	CO JE TO FIREWALL?	51
6.2	K ČEMU JE FIREWALL ?	52
6.2.1	Možnosti firewallů:	52
6.2.2	Funkce firewallů:	52
6.3	DRUHY FIREWALLŮ:	55
6.4	JAK TO FUNGUJE?	56
6.5	TYPY FIREWALLŮ	58
6.5.1	Paketové filtry (Packet Filters)	58
6.5.2	Aplikační brány (Application Gateways or Proxies)	59
6.5.3	Stavové vícevrstvé inspekční brány SMLI (Stateful Multi-Layer Inspection Gateways)	60
6.6	VLASTNOSTI MODERNÍHO FIREWALLU:	61
7	ZÁLOHOVÁNÍ DAT JAKO SOUČÁST BEZPEČNOSTI INFORMAČNÍCH SYSTÉMŮ.....	63
7.1	POSTUPY PŘI VYTVÁŘENÍ ZÁLOHOVACÍCH STRATEGIÍ	63
7.1.1	Význam zálohování.....	63
7.2	PLÁNOVÁNÍ STRATEGIE UKLÁDÁNÍ DAT	65
7.2.1	Plné zálohování (Full Backup).....	65
7.2.2	Přírůstkové zálohování (incremental backup).....	65
7.2.3	Víceúrovňové přírůstkové zálohování	66
7.2.4	Diferenční zálohování	66
7.2.5	Zálohování na základě události	67
7.3	OBNOVENÍ DAT PO KATASTROFĚ	68
8	KONCEPCE OCHRANY INFORMAČNÍHO SYSTÉMU (RIZIKOVÁ ANALÝZA, PLÁN OPATŘENÍ, VRSTVOVÝ MODEL ATD.).....	69

8.1	BEZPEČNOSTNÍ ANALÝZA IS.....	69
8.1.1	používané pojmy:	69
8.1.2	Vztahy v bezpečnostní analýze:	69
8.1.3	obecný postup:	70
8.1.4	Typické hrozby pro IS:.....	71
8.1.5	Příznaky ohrožení systému:	71
8.2	ETAPY ZABEZPEČENÍ IS:.....	71
8.2.1	Úvodní studie	72
8.2.2	Analýza a návrh.....	72
8.2.3	Realizace	73
8.2.4	Provoz, údržba a rozvoj IS	73
8.2.5	Plán bezpečnostních opatření:	73
8.2.6	Plán bezpečnostních opatření - součástí:	73
8.2.7	Ochranné vrstvy IS:.....	74
8.2.8	Vybrané aspekty ochrany IS (prolínají se):.....	74
8.2.9	Odhad pravděpodobnosti vzniku nežádoucích situací:	75
8.2.10	Základní aspekty ochrany dat, základní požadavky:	75
8.2.11	Možné příklady rizik:	76
8.2.12	Jednoduchý vztah pro odhad rizika:.....	77
9	ANALÝZA RIZIK.....	79
9.1	METODA CRAMM	79
9.1.1	Analýza a eliminace rizik CRAMM	79
9.2	BEZPEČNOST	80
9.3	NORMY ITSEC.....	80
9.4	SYSTÉMOVÁ BEZPEČNOSTNÍ POLITIKA.....	81
9.4.1	Ochrana informačních aktiv	81
9.4.2	Definice rolí v systému bezpečnosti:	81
9.4.3	Definice cílů	82
9.4.4	Identifikace hrozeb.....	82
9.4.5	Protiopatření (dle členění hrozeb).....	83
9.4.6	Dodržování zásad bezpečnostní politiky.....	83
10	ANALÝZA CHYB PROJEKTOVÉHO TÝMU A ZADAVATELE PŘI ŘEŠENÍ PROJEKTŮ IS/IT	85
10.1	CHYBY, KTERÝCH SE DOPOUŠTÍ FIRMA ZAVÁDĚJÍCÍ IS	85
10.2	CHYBY, KTERÝCH SE DOPOUŠTÍ MANAGEMENT ZADAVATELE	85
10.2.1	Chyby při formulaci cílů	86
10.2.2	Špatně zvolená strategie firmy, ze které vychází tvorba IS	86
10.2.3	Další chyby:	87
10.3	CHYBY, KTERÝCH SE DOPOUŠTĚJÍ ŘADOVÍ PRACOVNÍCI ZADAVATELE	87
10.4	KRITICKÉ FAKTORY PROJEKTU IS	88
	ZÁVĚR.....	89
	SEZNAM POUŽITÉ LITERATURY	91
	SEZNAM OBRÁZKŮ	94

SEZNAM TABULEK.....95

ÚVOD

Nejdůležitější a nejdražší částí informačního systému jsou informace (data) v něm obsažená. Všechny ostatní prvky jsou obnovitelné, všeobecně dostupné a pouze data jsou jedinečná.

Zajištění bezpečnosti dat je součástí zajištění bezpečnosti informačního systému.

V dnešní době většina organizací uchovává důležité informace o své činnosti v elektronické podobě. Na těchto informacích jsou životně závislé a proto musí zabezpečit všem oprávněným osobám přístup k těmto informacím (to znamená zajistit dostupnost) a zajistit správnost a celistvost (to znamená zajistit integritu) informací.

Ačkoliv si mnoho organizací plně uvědomuje nutnost zabezpečení svých IT systémů a možná disponují i efektivním bezpečnostním řešením, dodržování předpisů na lidské úrovni zůstává i nadále závažným problémem. Je třeba mít na paměti, že veškerá následující opatření a doporučení jsou vytvářena lidmi a pro lidi, kteří by měli být natolik motivováni a důsledně vedeni k dodržování bezpečnostní politiky ve firmě, aby byla minimalizována příslušná rizika a management nemusel uplatňovat sankce či důraznější prostředky za nedodržování bezpečnostních předpisů.

Tato práce se zabývá popisem hrozeb pro informační systém, jako jsou viry, červi, trojské koně atd. a zmiňuje se také o „moderních“ způsobech krádeží dat jako je phishing nebo pharming. V jiných kapitolách naopak zmiňují prostředky a způsoby možného, popřípadě nutného, zabezpečení systému, například nejmodernějším způsobem ověřování totožnosti a identifikace oprávněných uživatelů (pracovníků, zaměstnanců, kontraktorů apod.) – biometrikou, či firewally jako technickými zařízeními kontrolujícími všechny provoz, který prochází mezi vnitřní chráněnou sítí a veřejným internetem. Významným způsobem ochrany dat je také šifrování. Jestliže i dojde k odcizení informací, jsou díky použití kryptografických prostředků bezcenné, jelikož náročnost jejich dešifrování je se současnými možnostmi výpočetní techniky nemožná nebo natolik náročná, že náklady vynaložené na dešifrování přesahují hodnotu dat samotných. A protože jednou z podmínek zajištění dostupnosti a integrity informací je mít jejich záložní kopie, nesmím opomenout

kapitolu věnovanou zálohování dat.

Patrně nejvýznamnější část se věnuje tvorbě, koncepci a struktuře bezpečnostní politiky, včetně možných chyb, kterých se můžeme při zpracování takto důležitého a strategického dokumentu dopustit. 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.

1 ZÁKLADNÍ PRINCIPY BEZPEČNOSTI PŘI POUŽITÍ IT

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.

Poněvadž se mnohdy 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 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 Motivace pro zabezpečování při použití IT

Narušení bezpečnosti zpracovávání informací lze provést například:

- 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.

Pojmem zabezpečování IT označujeme

proces dosažení a udržení důvěrnosti, integrity, dostupnosti, prokazatelnosti odpovědnosti, autenticity a spolehlivosti informací a služeb IT na přiměřené úrovni.

Bezpečnost IT použitých v organizaci se dosahuje především plnění manažerských funkcí, souvisejících s bezpečností IT jako integrální součástí plnění globálního plánu správy organizace.

Mezi takové manažerské funkce typicky patří:

- . určení cílů, strategií a politiky zabezpečení IT organizace
- . určení požadavků na zabezpečení IT organizace
- . identifikace a analýza hrozeb pro aktiva IT v rámci organizace
- . identifikace a analýza rizik pro organizaci plynoucích z používání IT

- specifikace přiměřených bezpečnostních opatření eliminujících nebo snižujících rizika
- sledování implementace a provozu bezpečnostních opatření použitých pro účinnou ochranu informací a služeb IT v rámci organizace
- vyvinutí a zavedení programu zvyšování bezpečnostních znalostí a vědomí nutnosti udržovat bezpečí všech, kdo IT v organizaci používají
- detekování bezpečnostních incidentů a adekvátní reakce na ně.

Bezpečnostní politika v oblasti IT 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 IT organizace (také *celková bezpečnostní politika IT*) 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 IT organizace, při respektování konkrétně použitých IT pro realizaci IS organizace, to vše je náplní *bezpečnostní politiky IS organizace* (také *systémové bezpečnostní politiky IT*).

1.2 Bezpečnostní mechanismy

Pro implementaci funkcí prosazujících bezpečnost se používají bezpečnostní mechanismy. *Bezpečnostní mechanismus* je logika nebo algoritmus, který hardwarově (technicky), softwarově (logicky), fyzicky nebo administrativně implementuje bezpečnostní funkci. Rozpoznáváme (podle publikace [ITSEC]):

-.slabé bezpečnostní mechanismy

pro ochranu před amatéry, proti náhodným útokům, lze je narušit *kvalifikovaným útokem*, tj. *útokem střední síly*

-.bezpečnostní mechanismy střední síly

pro ochranu před hackery, proti úmyslným útokům s omezenými příležitostmi a možnostmi, hovoříme o běžných útocích

-.silné bezpečnostní mechanismy

ochrana před profesionály, ochrana proti útočníkům s vysokou úrovní znalostí, s velkými příležitostmi, s velkými prostředky, používajícími *útoky vymykající se běžné praxi*.

Podle použité technologické základny rozeznáváme bezpečnostní mechanismy:

-.softwarové bezpečnostní mechanismy (mnohdy označované jako *logické bezpečnostní mechanismy*)

princip řízení přístupu v daném operačním systému, kryptografie – symetrická (s tajným klíčem), asymetrická (s veřejným a privátním klíčem), standardy pro návrh, kódování, testování, údržbu programů, ochranné nástroje v operačních systémech, např. ochrana paměti, ochrana souborů řízením přístupu, obecná ochrana objektů, tj. přístupové matice, přístupové seznamy, hesla, autentizace přístupu k terminálu, mechanismy *určené pro autentizaci zpráv*

-.hardwarové bezpečnostní mechanismy (mnohdy označované jako *technické bezpečnostní*

mechanismy)

šifrovače a autentizační a identifikační karty

-fyzické bezpečnostní mechanismy

stínění, trezory, zámky, protipožární ochrana, generátory náhradní energie, chráněná místa pro záložní kopie dat a programů

-administrativní bezpečnostní mechanismy (výběr důvěryhodných osob, hesla, právní normy, zákony, vyhlášky, předpisy).

Mezi bezpečnostní mechanismy patří i ochranné nástroje v aplikačních systémech.

1.3 Zásady výstavby bezpečnostní politiky IT

Bezpečnostní politika IT organizace obecně vymezuje:

- co vyžaduje ochranu
- proti jakým hrozbám je ochrana budovaná
- jak budeme chránit to, co vyžaduje ochranu.

1.4 Typy bezpečnostních politik

Variant postupů jak zabezpečit IS je více, některé jsou zajímavější nákladově, jiné dosaženou transparentností, další pak odolností proti útoku výjimečné síly. Doporučená varianta by měla vzejít z oponované a závazně přijaté *bezpečnostní politiky organizace*, resp. alespoň z *bezpečnostní politiky IS*, používaného organizací. Přijatá bezpečnostní politika může být podle požadované úrovně záruky za zabezpečení:

Promiskuitní politika, tj. nikoho neomezující, která každému v zásadě povoluje dělat vše, tedy i to, co by dělat neměl. Promiskuitní IS jsou obvykle provozně nenákladné, mnohdy ani nenutí povinně používat pro autentizaci alespoň hesla, a zaručují pouze minimální nebo vůbec žádnou bezpečnost. Z přesvědčení, že se dějí pouze dobré věci, se provozovatel takového informačního systému brzy vyléčí.

Liberální politika, která každému povoluje dělat vše, až na věci explicitně zakázané. Liberální bezpečnostní politika zaručuje přece jen větší bezpečí než promiskuitní politika. Z hlediska používání Internetu jsou liberální bezpečnostní politiky často uplatňovány v akademických prostředích, kde se přístup ke službám Internetu s výjimkou vyjmenovaných případů neomezuje. Typicky se opírá o zásadu *volitelného řízení přístupu*.

Opatrná politika, rozumná politika, politika zakazující dělat vše, co není explicitně povoleno. Opatrná bezpečnostní politika je nákladnější na zavedení, avšak zaručuje vyšší stupeň bezpečnosti. Při aplikaci na obecný IS vesměs požaduje provedení *klasifikace objektů a subjektů*. Opatrná politika je opřena mj. o zásadu *povinného řízení přístupu*. Z hlediska používání v Internetu je obvykle počáteční bezpečnostní politikou při zavádění firewallů.

Paranoidní politika, politika zakazující dělat vše, i to, co by nemuselo být zakazováno. Zaručuje nejvyšší stupeň bezpečnosti, ve svém důsledku však zakáže používat mj. i internetovské služby (co kdyby se daly zneužít). Vede k maximální izolaci systému. Paranoidní bezpečnostní politika stále může být pro mnoho organizací užitečná. Databázový systém zpracovávající vysoce důvěrné informace lze fyzicky a technicky izolovat na systém s konečným počtem snadno kontrolovatelných vstupů a výstupů. Paranoidní charakter bezpečnostní politiky umožní implementaci aplikace v prostředí s nízkou systémovou režii, tudíž s dosažitelnou vyšší výkonností při zachování nižší úrovně nákladů.

2 BIOMETRICKÉ SYSTÉMY V PRAXI

V dnešní době kvůli obavám z bezpečnostních rizik zvažují soukromé společnosti, banky, pojišťovny, i vládní instituce co nejkvalitnější systémy zabezpečení přístupu do svých prostor a sítí obsahujících citlivá data. Nejmodernějším způsobem ověřování totožnosti a identifikace oprávněných uživatelů (pracovníků, zaměstnanců, kontraktorů apod.) je biometrika.

2.1 Jak autentizovat?

Autentizaci, ověřování totožnosti před povolením vstupu, lze provádět třemi principiálně odlišnými způsoby, které lze účinně také kombinovat. V poslední době se hojně využívá autentizace na základě biometricky. Oproti dvěma dříve využívaným kategoriím autentizace se jedinečné charakteristiky využívané v rámci biometrické autentizace mohou jen obtížně duplikovat, ale především biometrické charakteristiky ve většině případů člověka v průběhu života neopouštějí. Síla biometricky není v utajení informací používaných pro autentizaci, ale v jedinečnosti těchto informací.

2.2 Autentizace a její metody

Tradičně se dělí metody autentizace uživatelů podle toho:

- **co uživatel zná** – hesla v podobě alfanumerických řetězců, např. PIN ke kartě. Nebezpečí: zapomenutí/krádež (zaznamenaných hesel);
- **co uživatel má** – typickým příkladem autentizace tohoto typu jsou magnetické nebo čipové karty, které běžně nezpracovávají informace, pouze je ukládají a vyžadují na straně ověřujícího subjektu příslušné čtecí zařízení. Nebezpečí: ztráta/krádež či poškození;
- **co uživatele charakterizuje** – na základě rozpoznání vzorku trvalé fyzické nebo psychické vlastnosti jedince; mezi fyzickými charakteristikami se využívají nejčastěji otisky prstů a struktura oční duhovky nebo sítnice, zkoumá se využití vlastností jako tvar

ruky nebo obličeje; z charakteristik chování pak lze využít hlas, smích, způsob podpisu či způsob chůze. Nevýhody: komplexnost a nákladnost.

Každý systém automatizovaného přístupu je závislý hlavně na kvalitě autentizačního mechanismu. Každý mechanismus pracuje s tzv. povolenou odchylkou.

V těchto případech pak používáme následující terminologii:

autentizace heslem

autentizace předmětem

biometrická autentizace

2.2.1 Autentizace heslem:

Autentizace heslem je stále nejvíce používaným typem autentizace. Výhody tohoto typu autentizace jsou zejména v jeho lehké realizovatelnosti, a tím i levné implementaci. Nicméně, autentizační systém na heslo má řadu nevýhod, které omezují jeho použití na aplikace s minimálními bezpečnostními požadavky.

Autentizace založená na hesle často selhává z mnoha důvodů. Uživatelé si volí taková hesla, která jsou lehce uhádnutelná, nebo si je někde poznamená. Hesla mohou být také zachycena při přenosu k cílovému uzlu. To vše klade velký důraz na generaci, distribuci a užití hesel.

Charakteristikou dobrého hesla je, že:

- je distribuováno zabezpečeným způsobem, obsahuje malá i velká písmena, číslice a další znaky dostupné na klávesnici
- má dostatečnou délku - alespoň 6 znaků

- nejde o obvyklé slovo nebo známou frázi
- je nepravděpodobné - nelze jej odvodit ze znalosti osoby vlastníka
- je často obměňované - alespoň každé dva měsíce
- není nikde poznamenáno

2.2.2 Autentizace předmětem:

Autentizační předmět, se nazývá token. Token musí být jedinečný a obtížně padělatelný. Tokeny jsou vybaveny informací, která je používána při provádění autentizačního protokolu. Výhoda, ale zároveň i nevýhoda tohoto typu autentizace je, že token, který ověřuje identitu uživatele, je přenosný. Autentizační informace je tak vlastnictvím uživatele. Bezpečnost tokenů může být posílena tím, že autentizační systém požaduje nejen token, ale i heslo. Hlavní nevýhodou, stejně jako u hesel, je jejich přenositelnost umožňující komukoli vydávat se za někoho jiného.

2.3 Jak pracují biometrické systémy?

Zařazení uživatele do systému (enrollment):

- . sejmутí potřebných charakteristik a vytvoření referenčního profilu (vzorku). zpracování měření, extrakce nejdůležitějších charakteristik, vytvoření a uložení šablony (template)
- . uložení šablony v identifikační databázi (ve vazbě na určitý identifikátor)

Ověření totožnosti/identifikace:

- . aktuální měření/snímání daných charakteristik
- . zpracování výsledků
- . vyhledání šablony v databázi podle identifikátoru přiřazeného uživateli a porovnání s aktuálním měřením

zaznamenání výsledku porovnání a následná akce:

verifikace uživatele při shodě aktuálního měření s profilem, nebo odmítnutí pro nedostatečnou shodu

Menší bariérou při nasazování biometrických systémů je obava o vlastní soukromí u osob, které musí do systému uložit některé své identifikační znaky.

2.4 Výhody biometriky:

- silná metoda; jak pro autentizaci samotnou, tak z hlediska obrany proti zneužití
- možnost kombinace s hesly nebo zdvojení více biometrických metod pro zvýšení spolehlivosti (pro kritické systémy)
- odolnost vůči krádežím nebo monitorování (na rozdíl od hesel nebo karet)
- Nulové provozní náklady - žádná režie spojená s identifikačními tokeny atd.
- Rychlost - nic se nehledá (tokeny)
- Praktičnost - uživatel se nemusí obávat ztráty karty nebo zapomenutí hesla či PIN
- Zřejmost - identifikace je jednoduchá a výsledek je ihned znám
- Efektivnost - přímé datové propojení počítačových databází, automatizace
- Spolehlivost - osvědčené technologie
- Cena - příznivá cena ve vztahu k bezpečnosti a neexistujícím dodatečným nákladům

2.5 Nevýhody biometriky

- složitost a náročnost na prostředky (technické i finanční) pro snímání a porovnání snímaného údaje s mnoha uloženými údaji v databázi
- nutnost zabezpečení identifikační databáze
- různá chybovost: chybné přijetí (nesprávné ztotožnění uživatele se vzorkem někoho

jiného) nebo chybné odmítnutí (neztotožnění uživatele s jeho vlastním vzorkem)

2.6 Použití biometriky v praxi:

Přístupové systémy:

budovy

sklady

elektrárny

letišť

výpočetní střediska

trezory

Identifikace osob

náhrada průkazů

náhrada podpisů

věrnostní systémy a supermarkety

půjčovny

turistické zóny a kasína

stravovací systémy

Docházkové systémy:

státní instituce

komerční organizace

Ochrana počítačů:

přístupy k souborům a adresářům

přístupy do serverů

přístupy do sítí

aplikační software

komerční využití internetu

2.7 Bezpečnostní opatření

Správce musí v souladu s ustanoveními článku 17 Směrnice 95/46/ES přijmout veškerá vhodná technická a organizační bezpečnostní opatření na ochranu osobních údajů proti náhodnému nebo nezákonnému zničení nebo náhodné ztrátě, změně, neoprávněnému prozrazení nebo přístupu, zejména pokud zpracování zahrnuje předávání biometrických dat po síti. Bezpečnostní opatření musejí být učiněna, jestliže jsou biometrická data zpracovávána (uchovávání, předávání, výběr charakteristik a porovnávání, atd.) a zejména, když správce předává takové údaje prostřednictvím Internetu. Kromě kontroly přístupu a ochrany, která skutečně znemožní rekonstruovat původní data ze šablon, by bezpečnostní opatření mohla zahrnovat například kódování šablony a ochranu kódovacích klíčů.

V této souvislosti by měly být vzaty v úvahu některé nové technologie. Zajímavým vývojovým krokem je možnost použití biometrických dat jako kódovacích klíčů. To by vytvářelo menší riziko pro uživatele (tzv. subjekt údajů), protože dekódování může být provedeno pouze na základě nového sběru biometrických dat od uživatele samotného, a tak se lze vyhnout vytváření databází obsahujících šablony biometrických dat, u kterých existuje možnost jejich opětovného použití pro nesouvisející účely.

Nezbytná bezpečnostní opatření by měla být zavedena od počátku zpracování, a zvláště pak během fáze "zázpisu", kde jsou biometrická data převáděna na šablony nebo obrazy. Je třeba pochopit, že jakákoli ztráta rysů integrity, důvěrnosti a dostupnosti v souvislosti s určitými databázemi, by zjevně neblaze ovlivnila všechny budoucí aplikace založené na informacích obsažených v takových databázích, a zároveň by způsobila nenapravitelnou škodu subjektům údajů (uživatelům). Kdyby například otisky prstů oprávněného jednotlivce byly přiřazeny k totožnosti jednotlivce neoprávněného, mohl by posledně

jmenovaný mít přístup k službám dostupným vlastníkovu otisku prstu, aniž by k tomu byl oprávněn. To by mohlo vést ke krádeži identity, což by, bez ohledu na to, zda bude nebo nebude odhalena, učinilo otisky prstů jednotlivce nespolehlivými pro budoucí použití a tím by omezilo jeho svobodu.

Chyby, které se vyskytnou v biometrických systémech mohou mít vážné důsledky pro jednotlivce a zejména chybné odmítnutí oprávněných osob a chybné přijetí neoprávněných osob může způsobit vážné problémy na mnoha různých úrovních. A priori by použití biometrických dat mělo snížit riziko takových chyb. Avšak rovněž by mohlo vyvolat zdání, že identifikace nebo autentizace/verifikace subjektu údajů je vždy správná. Uživatel může shledat jako obtížné nebo dokonce nemožné prokázat opak. Systém může například mylně identifikovat uživatele jako někoho, komu by nemělo být povoleno použít letadlo nebo vstoupit do určité země, a ten by pak měl velmi omezené prostředky, jak čelit problému s takovým, proti němu naměřeným "nesporným" důkazem. Pro tyto případy by mělo být znovu zdůrazněno, že jakékoli rozhodnutí, které má právní dopad na jednotlivce, by mělo být učiněno až po potvrzení výsledku automatizovaného zpracování v souladu s článkem 15 Směrnice 95/46/ES.

Nakonec by mělo být zmíněno, že použití biometrie by mohlo zdokonalit kontrolní postupy například v případě přístupu k osobním údajům týkajících se třetích stran, například v případě krádeže nebo zneužití (autorizační postupy).

3 POČÍTAČOVÁ INFILTRACE

3.1 Viry

Jde o nejčastější formu infiltrace, přičemž název je odvozen díky jistým podobnostem od biologických originálů. Virus je schopen sebe-replikace, tedy množení sebe sama, ovšem za přítomnosti vykonatelného hostitele k němuž je připojen.

Hostitelem mohou být například spustitelné (executable) soubory, systémové oblasti disku, popřípadě soubory, které nelze vykonat přímo, ale za použití specifických aplikací (dokumenty Microsoft Wordu, skripty Visual Basicu apod.). Jakmile je tento hostitel spuštěn (vykonán), provede se rovněž kód viru. Během tohoto okamžiku se obvykle virus pokouší zajistit další sebe-replikaci a to připojením k dalším vhodným vykonatelným hostitelům.

3.1.1 Přehled přímých škod způsobených viry:

- náklady na odstranění viru
- náklady na kontrolu, opravu resp. dearchivaci poškozených dat a na reinstalaci software
- náklady na znovuvytvoření poškozených dat
- náklady vzniklé v důsledku výpadku výroby, organizace firmy, chybně provedených finančních operací (banky, burza, platební příkazy pro banku aj.)
- následky havárie (chemická továrny, jaderná elektrárna) jako důsledek chybného řízení technologického procesu
- poškození zdraví v důsledku používání poškozeného programu

3.1.2 Přehled nepřímých škod způsobených viry:

- náklady na nákup a provoz AV SW a HW (programy a zařízení pro ochranu dat)
- náklady z omezení provozu daná opatřeními v antivirové ochraně (obtížný přístup k HW i SW - odpojení disketových mechanik, používání kódovaných dat apod.)
- Utility pro obnovu a ochranu dat

Po zjištění napadení je nutné virus neprodleně, spolehlivě a s minimálním poškozením souborů odstranit, zamezit jeho šíření a znovuobjevení ve vlastním i cizím počítači, a napravit škody tak, aby nevratných škod bylo minimum.

Specializované prostředky pro opravu systémových částí disku poskytují vlastní antivirové balíky, utility, specializované programy firem zabývajících se antivirovou ochranou.

Je velice obtížné podat jednoznačný návod na odstranění viru a redukci způsobených škod na minimum - konkrétní postup bude závislý na druhu a době působení viru, charakteru dat na disku a dalších médiích a odborné způsobilosti uživatele.

3.1.3 Vzorový postup odvírování počítače:

Vzorový postup č. 1:

Virus byl zjištěn AV programem zpuštěným z pevného disku, podle vnějších projevů viru, prohlížením obsahu disku nebo operační paměti atd. Pevný disk je přístupný, virus neprovádí žádnou destruktivní činnost.

Uživatel uzavře běžící aplikace, neodpojuje se z počítačové sítě (možnost napadení logout.exe) a vypne počítač síťovým vypínačem (NE ctrl+alt+del), čímž se zabrání případné destruktivní činnosti viru.

Méně zkušený uživatel vyhledá zkušenějšího uživatele či antivirového odborníka, zkušenější uživatel zkontroluje výskyt viru, a pokud nešlo o planý poplach, pečlivě zváží a zapisuje si další kroky - neboť nesprávný postup může způsobit více škod nežli virus samotný.

- upozorní všechny uživatele napadeného počítače na výskyt viru
- zavede systém z čisté systémové diskety (nebo jakéhokoliv bootovatelného média) chráněné proti zápisu, změní sekvenci pro zavádění systému na pořadí a: c: (místo „a“ použijte písmeno média, ze kterého chcete zavést systém) v paměti BIOSu (např. virus EXEBUG totiž mění CMOS)
- nespouští žádné aplikace na infikovaném disku (možnost aktivace viru) a nepokouší se na disk cokoli zapisovat (došlo by k přepsání smazaných souborů)
- použije antivirový program z diskety k detekci a identifikaci infekce a k určení jejího rozsahu
- po identifikaci viru zjistí informace o viru v příslušné databázi (typy infikovaných souborů, způsobované škody, doporučený způsob odstranění viru)
- zkopíruje infikované soubory na čistou disketu a zašle ji antivirové firmě
- po skončení odvirování reinstaluje napadené programy (nejspolehlivější), nebo je obnoví ze záloh
- odstraní škody - obnoví smazané soubory pomocí programu undelete, opraví zkřížené clustery apod. Pokud byly obnoveny smazané soubory, znovu disk prověří AV programem
- vypne počítač, nabootuje z HDD a znovu použije AV k detekci infekce
- zkontroluje všechna paměťová média, která mohla být napadena
- zkontroluje všechny komprimované soubory na přítomnost viru
- jestliže počítač obsahoval vzácná data, je vhodné další postup konzultovat s antivirovou firmou
- doporučí, aby uživatel pozorně sledoval chování počítače a častěji používal AV programy

Při záchraně dat, např. po zformátování HDD se dobře uplatní např. Nortonovy utility

Vzorový postup č.2:

zjištěný virus provádí záludně destruktivní činnost (kódování disku, cílené poškozování datových souborů):

- uživatel uzavře běžící aplikace a vypne počítač síťovým vypínačem
- upozorní všechny uživatele napadeného počítače na výskyt viru
- přivolá specialistu, který po zavedení systému z čisté systémové diskety (CD, Flash disku,...) chráněné proti zápisu zkontroluje výskyt viru, ověří velikost způsobených škod a rozhodne o dalším postupu

Jestliže počítač obsahoval vzácná data, je vhodné další postup konzultovat s antivirovou firmou

3.2 Trojské koně (Trojani)

Narozdíl od virů není tento typ škodlivého kódu schopen sebe-replikace a infekce souborů. Trojský kůň nejčastěji vystupuje pod spustitelným souborem typu EXE, který neobsahuje nic jiného (užitečného), než samotné „tělo“ trojského koně. Odtud společně se skutečností, že trojan není připojen k žádnému hostiteli plyne, že jedinou formou dezinfekce je odmazání dotyčného souboru. Starší definice říkají, že trojan je program, vizuálně vypadající jako užitečný, ve skutečnosti však škodlivý. V současnosti se tak můžeme setkat nejčastěji s následující formou trojanů, nikoliv však v takové četnosti jako v případě virů:

3.2.1 Password-stealing trojani (PWS)

Skupina trojských koní, která obvykle sleduje jednotlivé stisky kláves (keyloggers) a tyto ukládá a následně i odesílá na dané e-mailové adresy. Majitelé těchto emailových adres (nejčastěji samotní autoři trojského koně) tak mohou získat i velice důležitá hesla. Tento typ infiltrace lze klasifikovat i jako spyware.

3.2.2 Destruktivní trojani

Klasická forma, pod kterou je pojem trojských koní obecně chápán. Pokud je takový trojský kůň spuštěn, pak likviduje soubory na disku, nebo ho rovnou kompletně zformátuje. Do této kategorie můžeme zařadit i většinu BAT trojanů, tj. škodlivých

dávkových souborů s příponou BAT. V tomto případě může překvapit snad jen občasné jednoduché kódování obsahu, díky čemuž není na první pohled zřejmé, co takový kód provádí.

3.2.3 Dropper

Dropper – „vypouštěč“. Nese ve svém těle jiný škodlivý kód (například virus), který je vypuštěn po aktivaci trojanu do systému.

3.2.4 Backdoor

Speciální skupina trojských koní, detailněji popsána níže.

Z výše uvedené charakteristiky je zřejmé, že setkání s trojským koněm není běžnou záležitostí. Pravděpodobnost setkání je ovšem vyšší od chvíle, kdy řada virů začala nést takové trojské koně s sebou a během svého šíření je vypouští na jednotlivé počítače. Pokud je virus úspěšný, dojde jak k masivnímu rozšíření viru, tak i k vypuštění velké spousty trojských koní. Nejčastěji jsou vypouštěni password-stealing trojani a backdoory. Potom už záleží jen na autorovi daného viru, jak dokáže získané možnosti využít.

3.2.5 Downloader (TrojanDownloader)

Obvykle jde jen o součást řetězce, který se v řadě případů proplétá s infiltrací typu spyware, adware apod. Downloader je obvykle spustitelným EXE souborem, který je během surfování uložen na disk a následně spuštěn (v některých případech je využito bezpečnostní díry, takže k tomu může dojít zcela automaticky). Downloader se postará o stažení a spuštění dalších konkrétních souborů z Internetu.

Uvedené programy mají v řadě případů problémy s českým jazykem a vedlejším efektem bývá, že například při pokusu napsat velké písmeno s háčkem dostáváme následující výsledek: chceme napsat „Č“, dostáváme: „~C“.

3.2.6 Proxy Trojan (TrojanProxy)

Některé trojské koně se postarají o to, že infikovaný počítač může být zneužit například pro odesílání spamu – nevyžádané pošty. Právě o tuto činnost se stará tento typ infiltrace. Při využití proxy je téměř nulová šance, že bude vypátrán skutečný autor nevyžádané pošty. Je to způsobeno samotným principem proxy.

3.3 Backdoor

Jde o aplikace typu klient-server, které jsou schopnostmi velice podobné komerčním produktům jako pcAnyWhere, VNC či Remote Administrator. Narozdíl od nich ovšem vystupují anonymně, uživatel není schopen jejich přítomnost běžným způsobem vypořádat a to je důvodem, proč jsou preventivně detekovány antiviry jako jeden z typů infiltrace. Mluvíme o neautorizovaném vstupu.

Backdoor je tak aplikace, sloužící pro vzdálenou správu PC a sama osobě nemusí být škodlivá. Záleží pouze na osobě, která tuto vzdálenou správu vykonává. Pokud půjde o činnost škodlivou, pak tuto osobu nazýváme vzdáleným útočníkem. Princip fungování backdooru je následující. Klientská část vysílá požadavky útočníka serverové části, ta tyto požadavky plní, popřípadě odesílá zpět klientu požadované informace. Z předchozího je zřejmé, že klientskou část aplikace by měl vlastnit útočník a serverová by měla být umístěna na počítači, kde lze očekávat kupříkladu důležitá data. Pokud je serverová část backdooru vypouštěna úspěšně se šířícím virem, má vzdálený útočník k dispozici tisíce počítačů, ke kterým může vzdáleně přistupovat. Celá komunikace probíhá ve většině případů na bázi TCP/IP, která ve spojení s celosvětovou sítí Internet umožňuje, aby útočník byl vzdálen tisíce kilometrů od serverové části backdooru.

3.3.1 IRC

Zvláštní skupinou jsou pak backdoory (nemusí jít nutně o ně), komunikující

s útočníkem skrze domluvený kanál v síti IRC. Jako příklad jmenujme virus Win32/Anarxy, který se snaží z infikovaného PC připojit ke kanálu #iworm_anarxy_channel. V něm vystupuje jako „bot“, na první pohled jeví se jako skutečná osoba, chatující na IRC. Útočník tak má teoreticky pohromadě všechny instance viru běžících ve světě a k libovolné z nich se může zalogovat a domluvenými rozkazy ji vzdáleně ovládat. Některé viry pak IRC využívají přímo pro zasílání kopií.

V praxi jsou tyto hodnoty nižší, například díky přítomnosti firewallů, popřípadě díky omezením plynoucím z použití privátních IP adres v rámci sítě LAN.

3.4 Červi (worms)

Pojmem červ (worm) byl prvně označen tzv. Morrisův červ, který v roce 1989 dokázal zahltit značnou část tehdejší sítě, ze které později vznikl Internet. Tento a další červi (z poslední doby třeba populární Code Red, SQL Slammer, Lovsan / Blaster, Sasser) pracují na nižší síťové úrovni nežli klasické viry. Nešíří se ve formě infikovaných souborů, ale síťových paketů. Jmenované pakety jsou směrovány již od úspěšně infikovaného systému na další systémy v síti Internet (ať už náhodně, nebo dle určitého klíče). Pokud takový paket dorazí k systému se specifickou bezpečností dírou, může dojít k jeho infekci a následně i k produkci dalších „červích“ paketů. Šíření červa je tedy postaveno na zneužívání konkrétních bezpečnostních děr operačního systému, úspěšnost pak od rozšířenosti daného softwaru obsahující zneužitelnou bezpečnostní díru. Z výše uvedených charakteristik plyne, že červy nelze detekovat klasickou formou antivirového softwaru. Vedlejším efektem může být kompletní zahlcení sítě, podnikové LAN nevyjímaje.

Pojem „červ“ je často spojován i s typem infiltrace šířící se elektronickou poštou. Zde tak mohou pojmy „virus“ a „červ“ splývat v jeden.

3.5 Speciální případy infiltrace

V případě falešných zpráv (hoax) nelze o infiltraci hovořit. Jde pouze o pojem, který s touto tematikou souvisí.

3.5.1 Spyware

Spyware je program, který využívá Internetu k odesílání dat z počítače bez vědomí jeho uživatele. Narozdíl od backdooru jsou odcizovány pouze „statistická“ data jako přehled navštívených stránek či nainstalovaných programů. Tato činnost bývá odůvodňována snahou zjistit potřeby nebo zájmy uživatele a tyto informace využít pro cílenou reklamu. Nikdo však nedokáže zaručit, že informace nebo tato technologie nemůže být zneužita. Proto je spousta uživatelů rozhořčena samotnou existencí a legálností spyware. Důležitým poznatkem je, že spyware se šíří společně s řadou sharewarových programů a jejich autoři o této skutečnosti vědí.

Útok typu DoS by cílový server zahltl, popřípadě zcela vyřadil z provozu.

3.5.2 Adware

Obvykle jde o produkt, který znepříjemňuje práci s PC reklamou. Typickým příznakem jsou „vyskakující“ pop-up reklamní okna během surfování, společně s vnucováním stránek (např. výchozí stránka Internet Exploreru), o které nemá uživatel zájem. Část Adware je doprovázena tzv. „EULA“ - End User License Agreement – licenčním ujednáním. Uživatel tak v řadě případů musí souhlasit s instalací.

Adware může být součástí některých produktů (např. DivX). Ačkoliv nás reklama doprovází během celé činnosti s daným programem, odměnou je větší množství funkcí, které nejsou v klasické free verzi (bez reklamy) dostupné.

3.5.3 Hoax

Slovem Hoax označujeme poplašnou zprávu, která obvykle varuje před neexistujícím nebezpečným virem. Šíření je zcela závislé na uživateli, kteří takovou zprávu e-mailem obdrží. Někteří se mohou pokusit varovat další kamarády či spolupracovníky a jednoduše jim poplašnou zprávu přeposlat (forwardovat). Tím vzniká proces šíření. Pokud budeme hovořit o poplašných zprávách týkajících se virů, pak je můžeme charakterizovat následně:

- Popis nebezpečí (viru)
Smyslené nebezpečí (virus) bývá stručně popsáno, v případě viru bývá uváděn i způsob šíření.
- Ničivé účinky viru
Zde záleží převážně na autorově fantazii. Ničivé účinky mohou být celkem obyčejné, třeba zformátování disku nebo už méně důvěryhodné - zběsilý útěk myši do ledničky, roztočení HDD opačným směrem, výbuch počítače... :-)
- Důvěryhodné zdroje varují
Ve většině případů se pisatel poplašné zprávy snaží přesvědčit, že varování přišlo od důvěryhodných zdrojů ("IBM a FBI varují" nebo "Microsoft upozorňuje" atd...)
- Výzva k dalšímu rozeslání
Tento bod HOAX vždy obsahuje! Mnoho nezkušených uživatelů se nechá zprávou napálit a bez přemýšlení výzvu uposlechnou. Díky tomu se tyto nesmysly lavinovitě šíří.

3.5.4 Dialer

Dialer je program, který změní způsob přístupu na Internet prostřednictvím modemu. Místo běžného telefonního čísla pro Internetové připojení přesměruje vytáčení na čísla se zvláštní tarifací až 60 Kč / minutu. V některých případech se tak děje zcela

nenápadně, zvláště když oběť používá špatně nastavený Internetový prohlížeč. Dialer (nejčastěji soubor typu EXE a několik pomocných souborů) je obvykle na PC vypuštěn za využití technologie ActiveX, takže problémy mohou nastat především uživatelům Internet Exploreru. Ve všech případech nemusí jít nutně o ilegální program. Můžou totiž sloužit jako způsob zpoplatnění určité služby (například přístup na porno stránky).

Dialer tak může existovat v tiché podobě, kdy přesměruje volání zcela bez vědomí uživatele, popř. v podobě „legální“, kdy je uživateli zobrazeno licenční ujednání („EULA“ -End User License Agreement) a až po odsouhlasení (tlačítkem „I Agree“ apod.) ze strany uživatele dojde k přesměrování připojení. Praxe ukázala, že taková ujednání čte minimum surfařů, takže i druhý případ se může pro postiženého uživatele jevit stejně jako první.

S tímto navíc souvisí rozdílné postoje k detekci těchto věcí ze strany antivirových společností a otázka, co vlastně detekovat a co nikoliv. Antivirový systém nedokáže rozpoznat, zda je dialer nainstalován s vědomím, či bez vědomí uživatele. Detekce všech dialerů může vést k soudním sporům mezi výrobcem dialeru, popř. provozovatelem služby využívající dialer a antivirovou společností, která tento „nevinný produkt“ detekuje jako by šlo o skutečný virus.

3.5.5 rhybaření (phishing)

Phishing čili rhybaření využívají nekalé živly k tomu, aby získaly od uživatelů citlivé údaje. Například takové, jakými jsou přihlašovací údaje k jejich účtu spravovaného prostřednictvím internetového bankovníctví.

Nejčastější scénář útoku probíhá prostřednictvím elektronické pošty. Uživatel přijme e-mail, který má zfalšovanou adresu, takže vypadá, jako by jej odeslal jeho bankovní úřad. V předmětu zprávy se pak zpravidla objevuje falešné upozornění banky, že je došlo k nějakému problému. K jeho vyřešení má pak dotyčný mimo jiné zadat přihlašovací údaje ke svému účtu či alespoň číslo kreditní karty. Tyto údaje mají být buď součástí odpovědi na tento e-mail, nebo se mají zadat na stránce, na niž vede z e-mailu odkaz. Tyto stránky pak většinou využívají chyb v neaktualizovaných prohlížečích, které jejich adresu (URL)

zobrazí, jako by to byla adresa banky. Stránka samotná pak je v podstatě zkopírovaná z webu banky, takže vypadá identicky. Na rhybaření tak většinou doplácí lidé, kteří jsou příliš důvěřiví.

Card Type:

Card Holder Full Name:

Card Number:    

Expiry Date: /

Card Verification Number:

Card PIN Number: (your 4-digit card pin) * If PIN is invalid your account will not be verified. *

Obr. 1. Příklad phishingu – část formuláře, který sbírá informace o kreditní kartě a dokonce o jejím PINu.

3.5.6 Pharming

Nový typ útoku se nazývá pharming a funguje tak, že se přihlásíte na naprosto normální stránku banky, vydáte své přístupové kódy k vašim účtům a nemáte možnost si všimnout, že jde o podvrh.

Triky, jak získat přístup k vašim bankovním účtům, většinou spočívají v získání přístupových údajů v rámci internetového bankovníctví.

Pharming však skýtá mnohem větší nebezpečí, které nemusí rozpoznat ani zkušenější uživatel. I zde dochází k podvržení falešné stránky, která vypadá, jakoby pocházela z bankovního úřadu, ale navíc se na ni můžete dostat i při správném zadání regulérní internetové adresy banky v prohlížeči. Vy jednoduše vyťukáte adresu vaší banky s tím, že prostřednictvím internetového bankovníctví budete chtít provádět nějaké operace, a nic netušíc se však dostanete na podvržené stránky. Ty navíc vypadají naprosto stejně. Jak je to možné?

Je to důsledek úspěšného napadení systému, který překládá URL adresy do formátu IP. Tento formát se v internetové komunikaci používá podobně jako telefonní čísla v telefonní síti. Každý web má totiž svou IP adresu ve formátu xxx.xxx.xxx.xxx, které může být

přiřazen lépe zapamatovatelný URL název jako je například web.utb.cz.

K tomu, aby si požadavek ve formě URL našel ten správný web, je potřeba jej nejdříve přeložit do IP formátu. K tomu slouží především tzv. DNS (Domain Name Server) servery, ale také některé služby na vašem počítači. Jestliže takový DNS server nepřidělí zadanému URL správně IP adresu, dojde k problémům. A právě toho využívají útočníci při útocích typu pharming. Pokoušejí se najít špatně zabezpečený DNS server, v němž následně přepíší IP adresu určenou například pro URL banky IP adresou falešné stránky. Tím se stanou nic netušící oběti všichni, kdo se chtějí na daný web dostat. Pharming tak dovádí rhybaření k mnohem větší účinnosti a navíc jeho prostřednictvím může být poškozeno mnohem více uživatelů najedou.

Lokální nebezpečí

Mnohem jednodušší je však pro útočníka zaútočit na uživatelské PC, kde se dá předpokládat menší míra zabezpečení. Pokud se podaří úspěšně počítač napadnout, stačí v něm již jen upravit speciální soubor Hosts. Ten v OS Windows obsahuje URL a jim přiřazené IP adresy, aby je mohl již z počítače odesílat právě v IP podobě.

O tom, že tento způsob útoku je nyní na vzestupu, svědčí již zveřejněné případy, kdy útočníci přesměrovaly návštěvníky serverů eBay, Google či weather.com na podvržené stránky, kde se jim pokoušeli nainstalovat do počítače špiónský software (spyware).

Jak se bránit

Proti úpravě IP adresy na DNS serveru se příliš bránit nemůžete, ale ten je na druhou stranu méně pravděpodobný. Proti útoku na váš počítač pak musíte použít všechny dostupné prostředky. Firewallem počínaje a aktualizovaným software konče. Při práci na internetu nesmíte přestat být obezřetní a měli byste se vždy vyvarovat klikání na odkazy a návštěvám nedůvěryhodných adres. Také mějte na paměti, že každý stažený soubor může skrývat potenciální nebezpečí.

4 ZÁKLADY ŠIFROVÁNÍ A KRYPTOANALÝZY:

Kryptologie - věda, která se zabývá šifrováním (kryptos = skrytý). Kryptologie se skládá z kryptografie - vědy o tvorbě šifer a kryptoanalýzy - vědy o jejich luštění.

Šifrování (Encryption, encoding, enciphering) - proces, při kterém je zpráva zakódována tak, že její obsah není zřejmý.

Dešifrování (decryption, decoding, deciphering) – je opakem šifrování.

Pravidla provozu šifrování:

- nevysílat stejný text zašifrovaný různými klíči
- zabránit používání velmi pravděpodobných slov a frází
- omezit používání typických kombinací písmen, interpunkčních znamének a mezer mezi slovy

Základní postupy při šifrování:

- převedení textu na čísla a následné zobrazení množiny celých čísel na množinu celých čísel
- výběr vhodné šifry (monoalfabetické nemají praktický význam) - podle příjemce, možného protivníka, podle počtu a délky vysílaných zpráv
- sdělit příjemci způsob kodování (s výjimkou systémů s veřejnými klíči nejslabší článek)
- rozdělení textu na bloky stejné délky, často se kódují jiným algoritmem
- vhodné často měnit způsob kodování

Charakteristika dobré šifry:

Šifra by neměla být prolomitelná v reálném čase a s použitím „rozumných“ výdajů (x šifrovací čipy a vlády).

Šifrování by mělo proběhnout rychle.

Množství práce vynaložené na šifrování a dešifrování by mělo být úměrné požadovanému stupni utajení.

Šifrovací algoritmus by neměl obsahovat zbytečná omezení.

Implementace algoritmu by měla být co nejjednodušší (jednorázový heslář).

Chyby při šifrování by se neměly příliš šířit.

Zprávy by se šifrováním neměly zvětšovat.

Kryptoanalytický útok - pokus o dešifrování textu. Mezi základní patří útok se znalostí otevřeného textu, útok se znalostí šifrovaného textu, útok s možností volby otevřeného textu, útok s možností volby šifrovaného textu.

základní úlohy:

dešifrování se znalostí zašifrovaného textu (základní úloha), hledání klíče nebo systému

dešifrování s částečnou znalostí přímého textu (současný šifrovací systém musí i v tomto případě vzdorovat)

dešifrování s neomezenou znalostí přímého textu

základní znalosti:

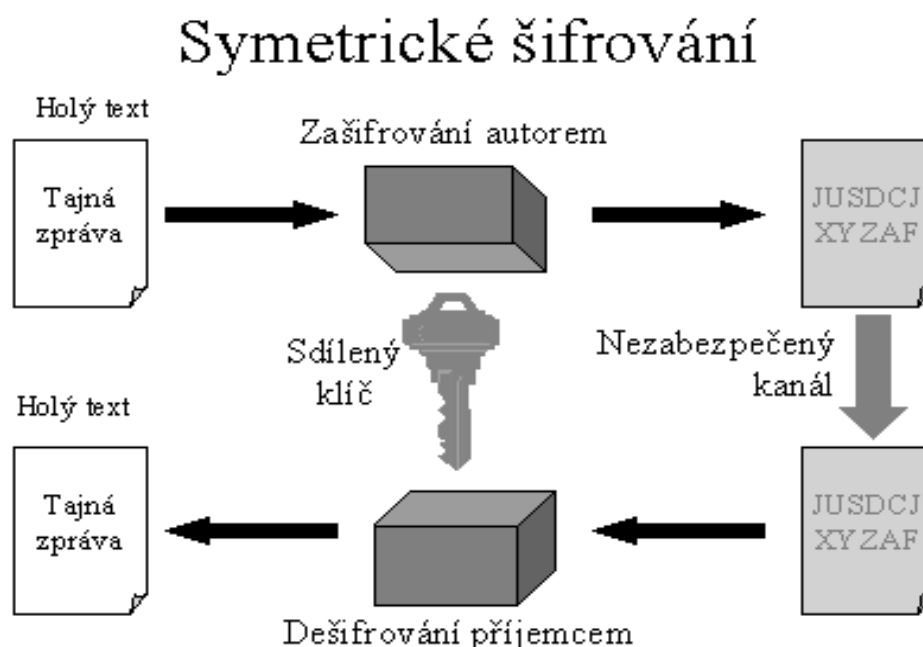
frekvence výskytu písmen je odlišná u různých jazyků

použití polyalfabetické šifry vede (v závislosti na délce klíče) ke zploštění frekvence výskytu písmen

dešifrování nemusí dát jednoznačný výsledek, např. pro Vigenérovskou šifru a šifrovaný text

Bezpečnost algoritmu - cena k prolomení vyšší než cena dat, doba k prolomení delší než aktuálnost dat, množství dat zašifrované jedním klíčem menší než množství potřebné k prolomení algoritmu

4.1 Algoritmy pro symetrické šifrování:



Obr. 2. Princip symetrického šifrování

Odesílatel svou zprávu zakóduje svým jedinečným klíčem, který zná jen on a příjemce a nikdo jiný. Pak může zprávu poslat příjemci bez toho, aby se bál, že si ji přečte někdo nepovolaný.

4.1.1 1.DES

DES znamená Data Encryption Standard a je to bloková šifra definovaná a schválená vládou USA jako oficiální šifrovací standard.

DES je symetrický šifrovací systém, tj. je-li použit ke komunikaci, pak jak odesílatel, tak i příjemce musí znát stejný tajný klíč, který je použit jak k zašifrování, tak i k dešifrování zprávy. Tato šifra využívá bloky o velikosti 64 bitů a pro šifrování používá klíč dlouhý 56 bitů (návrh původně 112 bitů).

DES může být rovněž použit pro šifrování jediným uživatelem, tj. umožňuje uživateli uložit si své soubory na pevný disk v zašifrované podobě.

Jediný vhodný způsob prolomení algoritmu DES je investovat několik milionů dolarů do výpočetní síly, která je nutná k prolomení tohoto algoritmu (útok hrubou silou, diferenciální a lineární kryptoanalýza).

Je-li DES používán ke komunikaci, je třeba měnit často klíče a věnovat speciální pozornost správě klíčů. Nejlepším způsobem, jak použít DES k šifrování souborů na pevném disku je neměnit často DES klíče, protože to by znamenalo dešifrovat a pak znovu šifrovat všechny zvolené soubory při každé takové výměně klíče. Místo toho je lepší mít nějaký master DES klíč, kterým zašifrujeme seznam DES klíčů používaných k šifrování souborů.

Triple DES je algoritmus, který se stále více dostává do povědomí odborné veřejnosti. Jeho označení indikuje, že dochází třikrát k šifrování DES algoritmem, a ne pouze jednou. Vysoká úroveň bezpečnosti je zajištěna tím, že při každém z těchto šifrování je použit jiný klíč.

4.1.2 2.IDEA

IDEA reprezentuje pravděpodobně nejlepší a nejbezpečnější blokový šifrovací algoritmus, který je v současnosti k dispozici. Zdá se, však, že jeho popularita je negativně ovlivněna skutečností, že je tento algoritmus patentován (a to jak v Evropě, tak i v USA), na rozdíl od algoritmu DES. Navíc je to algoritmus relativně nový, byl uveden na veřejnost teprve v roce 1992. Přesto se jeho popularita stále zvyšuje, a to i v souvislosti se skutečností, že tento algoritmus je částí systému PGP.

Algoritmus IDEA je při šifrování přibližně dvakrát rychlejší než algoritmus DES. Vyšší úroveň bezpečnosti algoritmu IDEA ve srovnání s algoritmem DES se vysvětluje skutečností, že IDEA využívá klíčů o délce 128 bitů. Takže IDEA je dvakrát rychlejší než DES a současně nabízí podstatně vyšší úroveň bezpečnosti.

Abychom si ilustrovali úroveň bezpečnosti algoritmu IDEA, uveďme, že útok silou by vyžadoval 2128 (1038) šifrování k nalezení klíče. Aby toto bylo možno provést, museli bychom mít k dispozici počítačový čip schopný otestovat bilion klíčů za sekundu. Trvalo by to tedy 1013 let nalézt klíč.

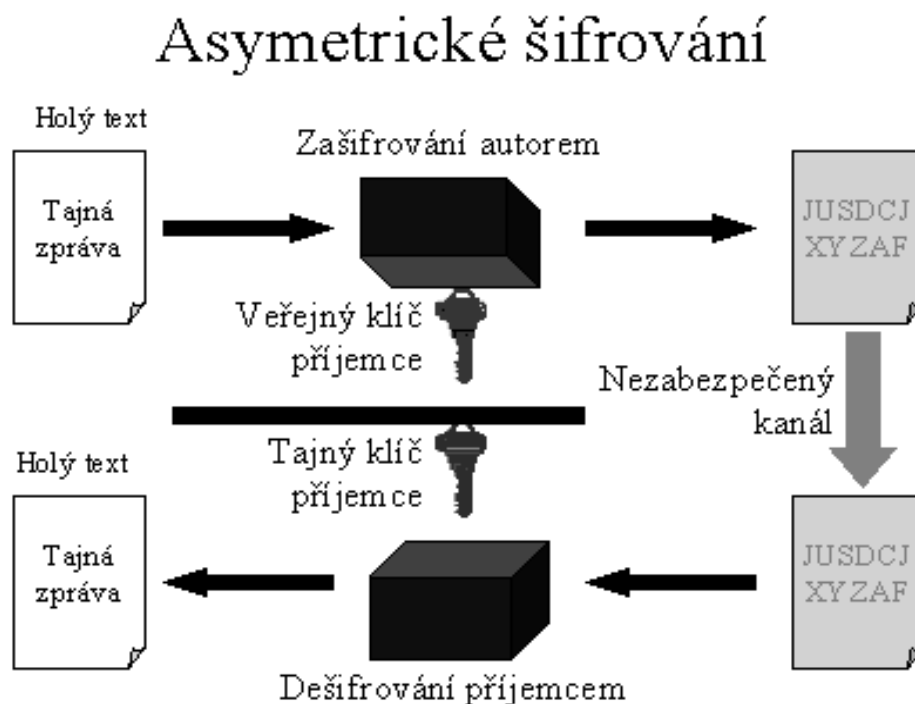
4.1.3 3.Blowfish

Blowfish je rychlý 64-bitový blokový šifrovací algoritmus s proměnnou délkou klíče. Jeho bezpečnost byla prověřena mnoha testy, které prokázaly, že se jedná o velmi silný a tedy bezpečný šifrovací algoritmus.

4.1.4 Shrnutí symetrického šifrování (systémy se soukromými klíči):

- používá stejný klíč pro šifrování i pro dešifrování
- má rychlé algoritmy
- může vykazovat problémy při správě klíčů
- využívá algoritmy DES (délka klíče 56 bitů), BlowFish (proměnná délka klíče až 256 bitů) a IDEA (délka klíče 128 bitů) jako nejběžnější průmyslové standardy (k dispozici v produktu IW Wall nebo IW Folder)
- využívá algoritmus CIPHER (délka klíče 16 bitů), což je vlastní algoritmus vyvinutý společností AEC (k dispozici v produktu IW Wall)
- používá se pro šifrování a dešifrování dat ve formě textu nebo souborů (toto je napsáno už výše v textu)

4.2 Algoritmy pro nesymetrické šifrování:



Obr. 3. Princip nesymetrického šifrování

Asymetrická kryptografie využívá jiného klíče pro šifrování a jiného pro dešifrování (narozdíl od symetrické). Asymetrická kryptografie je založena na této myšlence: Každý subjekt má svůj tajný (soukromý) klíč k dešifrování a k němu veřejný klíč k zašifrování.

4.2.1 RSA

Algoritmus RSA je bezesporu nejznámější algoritmus systémů s veřejným klíčem na světě.

Společnost RSA Data Security Inc. vyvinula asymetrický algoritmus RSA, na který má USA patent. Algoritmus RSA se bez pochyby stal nejvíce využívaným asymetrickým algoritmem. Jeho vývojáři prohlašují, že po celém světě se používá 25 milionů kopií RSA technologie. Mnohé společnosti slavných jmen používají RSA algoritmus ve svých produktech, např. IBM, Microsoft, Lotus, Apple, Novell, AT&T a Digital. Interně jej pak používají společnosti jako jsou Boeing, Shell Oil, DuPont, Raytheon a Citicorp.

Ve skutečnosti je algoritmus RSA jakýmsi šifrovacím standardem ve většině světa, i když nezískal plné ocenění a označení ISO. Jednotlivé státy (jako např. Austrálie) se rozhodly přijmout algoritmus RSA jako standard, stejně jako některá odvětví průmyslu (např. francouzský bankovní sektor).

Důležitou součástí algoritmu RSA je jeho systém ověřování pomocí digitálních podpisů.

4.2.2 Digitální podpis:

- využívá SHA hašovací algoritmus a 160 bitů dlouhý CRC soubor
- vyžaduje na uživateli, aby použil svůj soukromý klíč k zašifrování CRC souboru
- přidává zašifrovaný CRC soubor k datovému souboru
- vyžaduje na příjemci, aby použil svůj veřejný klíč k dešifrování CRC souboru - vyžaduje na příjemci, aby porovnal a zjistil soulad mezi oběma CRC soubory vytvořenými odesílatelem a příjemcem. Jestliže tyto dva CRC soubory souhlasí, pak je integrita zprávy v pořádku a digitální podpis tím byl ověřen.

Kryptografický systém - systém provádějící transformaci nechráněného textu na text chráněný (nešifrovaného na šifrovaný). Všechny transformace jsou prováděny příslušným kryptografickým algoritmem s použitím klíčů.

Tradiční kryptografické systémy jsou založeny na tom, že jak odesílatel, tak i příjemce, mají stejný tajný klíč, tj. ten samý klíč je použit k zašifrování i k dešifrování. Tato metoda je známá jako symetrická kryptografie. Problém této metody spočívá v tom, že odesílatel musí nějakým způsobem doručit tento tajný (soukromý) klíč příjemci; a odesílatel nemůže zaručit, že klíč nebude cestou zachycen neautorizovanou osobou.

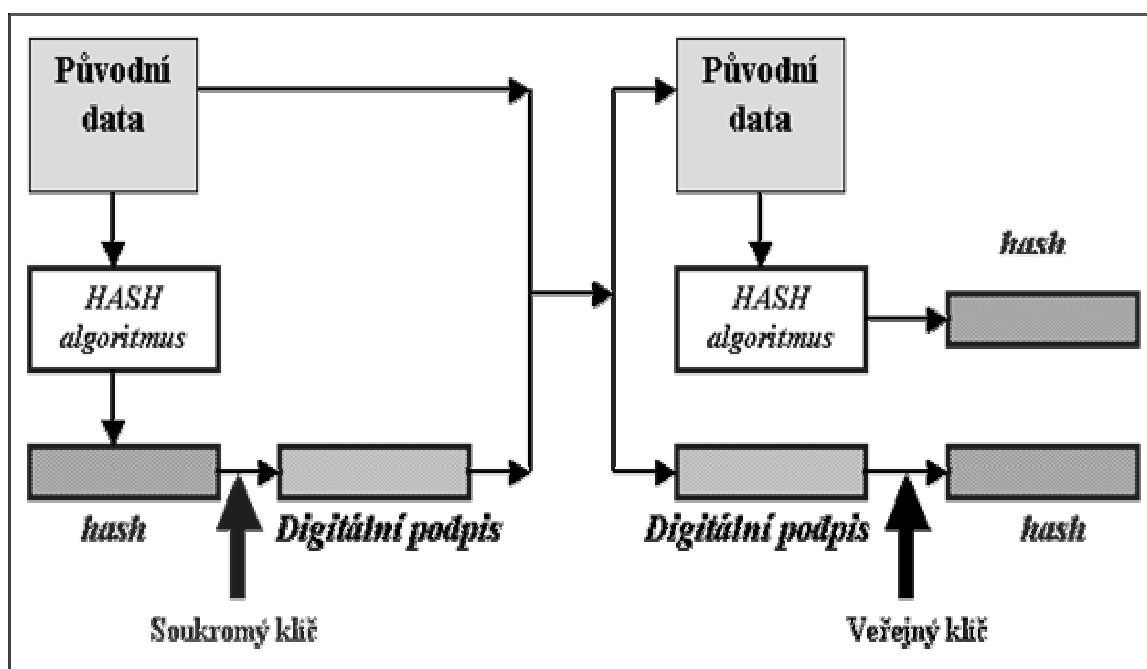
Kryptografické systémy s veřejnými klíči (nesymetrická kryptografie) - v kryptografických systémech s veřejnými klíči obdrží každá osoba pár klíčů, jeden z nich je soukromý a druhý je veřejný. Veřejné klíče jsou dostupné komukoliv, ale soukromé klíče jsou udržovány v tajnosti. Při komunikaci dochází k přenosu veřejných klíčů, zatímco soukromý klíč není nikdy nikam přenášen ani není s nikým sdílen. Zašifrované zprávy jsou

odesílány otevřeně a po přijetí jsou dešifrovány soukromými klíči. Jediným požadavkem je, aby veřejné klíče byly přiřazeny svým vlastníkům (např. v důvěryhodném adresáři). Tato metoda může být také použita pro autentizaci zpráv (pomocí digitálního podpisu).

Digitální podpis - použití soukromého klíče k šifrování, podpis je dešifrován veřejným klíčem

Zašifrování pomocí veřejných klíčů - Jestliže chce Zuzana poslat tajnou zprávu Františkovi, použije Františkův veřejný klíč k zašifrování zprávy a pak ji odešle. František pak užije svůj soukromý klíč k dešifrování zprávy, takže si ji může přečíst. Nikdo jiný nemůže dešifrovat zprávu, protože nemá Františkův soukromý klíč. Bezpečnost tohoto komunikačního systému tedy stojí na skutečnosti, že není možné získat soukromé klíče ze znalosti odpovídajících veřejných klíčů.

Digitální podpisy - Jestliže chce Zuzana podepsat svou zprávu Františkovi, provede výpočet, který použije její soukromý klíč a zprávu samotnou. Výsledek tohoto výpočtu je nazýván digitální podpis, a ten je připojen ke zprávě před jejím odesláním. Poté, co František zprávu přijme, chce prověřit její pravost. Proto provede výpočet, který využívá zprávu, podpis, který obdržel, a Zuzanin veřejný klíč. Jestliže je výsledek tohoto výpočtu kompatibilní s jednoduchým matematickým vztahem, pak František ví, že zpráva je pravá, tj. že nebyla podvržena ani pozměněna cestou.



Obr. 4. Princip digitálního podpisu

Kryptografie s veřejnými klíči má určité přednosti oproti symetrické kryptografii:

Soukromé klíče nemusí být přenášeny ani nikomu předávány

Prověřování digitálních podpisů pomocí veřejných klíčů nenarušuje odpovědnost uživatele za ochranu svého vlastního soukromého klíče. Tato skutečnost je často nazývána nepopíratelnost zodpovědnosti za zprávu.

Kryptografie s veřejnými klíči využívá algoritmus RSA (s délkou klíče až 1200 bitů) jako průmyslový standard.

Nevýhody šifrování s veřejnými klíči:

Kryptografie s veřejnými klíči je při šifrování pomalejší než symetrická kryptografie, ve skutečnosti populární metody šifrování s tajnými klíči jsou podstatně rychlejší než v současnosti používané šifrovací metody s veřejnými klíči. Proto je obvyklé kombinovat metodu šifrování s veřejnými klíči s metodou šifrování s tajnými klíči a využít tak předností obou; veřejný klíč může být použit k zašifrování tajného klíče, který se potom použije k zašifrování zprávy nebo souboru.

Kryptografie s veřejnými klíči se může stát náchylnou k falšování zpráv i tehdy, když soukromé klíče uživatelů nejsou dostupné pro útočníky. Úspěšný útok na certifikační úřad dovolí útočníkovi využít certifikát veřejného klíče zkompromitovaného úřadu a spojit tak

klíč podle volby útočníka se jménem jiného uživatele.

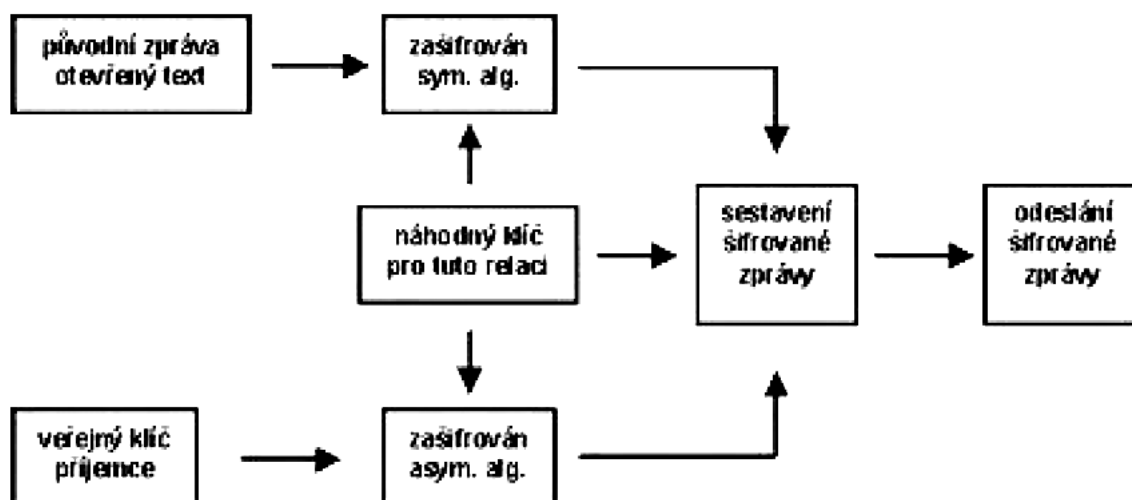
Existují situace, kdy není využití kryptografie s veřejnými klíči nutné, a samotná symetrická kryptografie s tajnými klíči je dostačující, např. v situaci, kdy se obě strany osobně setkají k výměně tajných klíčů.

Navíc využití kryptografie s veřejnými klíči není nutné ani v případě prostředí jednoho uživatele, takže, jestliže si přejete zašifrovat své vlastní osobní soubory, můžete použít jakýkoliv symetrický šifrovací algoritmus a použít, řekněme, své osobní heslo jako tajný klíč.

Obecně, využití kryptografie s veřejnými klíči je nejvhodnější pro otevřené prostředí s více uživateli, a nepředpokládá se, že by nahradilo symetrickou kryptografií. Kombinace obou metod zajišťuje nejlepší úroveň bezpečnosti.

4.3 PGP - Pretty Good Privacy (Docela dobré soukromí)

Je kryptografický balík, který je využíván především pro šifrování zpráv a souborů a vytváření/ověřování digitálních podpisů. Jeho autorem je američan Philip R. Zimmermann. První verze tohoto programu byla uvolněna v červnu 1991 jako 'free software'. Další verze (i komerční od PGP Security - Network Associates) následovaly a dnes patří program PGP bezesporu mezi jedny z nejrozšířenějších prostředků pro šifrování elektronické pošty a pro ověřování její pravosti pomocí digitálních podpisů. PGP pracuje s šifrovacími algoritmy CAST, AES, TripleDES, IDEA, Twofish, a lze tedy říci, že patří mezi kryptograficky poměrně silné prostředky. Nemalou výhodou je i dostupnost na většině platform.



Obr. 5. Šifrování pomocí PGP

PGP se navenek jeví jako systém s veřejným a soukromým klíčem. Každý uživatel si generuje jeden nebo více párů tajného (soukromého) a veřejného klíče. Veřejné klíče jsou pak zveřejněny všem ostatním uživatelům. Ve skutečnosti je však při šifrování pomocí PGP při každém použití generován náhodný symetrický klíč a zpráva nebo soubor je zašifrován symetrickou šifrou s použitím tohoto náhodného klíče. Tento klíč je pak zašifrován systémem s asymetrickou šifrou, který zde řeší pouze problém s distribucí symetrického klíče.

Kromě šifrování umožňuje PGP také opatřit přenášené zprávy digitálními podpisy (signaturami), které umožňují příjemci ujistit se o integritě a autenticitě přijatých dokumentů. V tomto případě je použito některého HASH algoritmu, který produkuje 128bitové číslo - jakýsi otisk zprávy. Toto číslo je pak zašifrováno tajným klíčem uživatele a výsledek je připojen jako digitální podpis ke zprávě. Příjemce může pomocí veřejného klíče získat původní HASH a porovnáním ověřit integritu e-mailu a pravost podpisu. Vzhledem k tomu, že tajný klíč zná jen odesílatel, nemohl zprávu nikdo podvrhnout.

Veřejné a soukromé klíče bývají obvykle uchovávány v tzv. svazcích klíčů. (Soubor pubring.pgp obsahuje obvykle veřejné klíče a je průběžně doplňován; secring.pgp je

svazek tajných klíčů, který je obvykle neměnný a je udržován v zašifrovaném tvaru.) Pokud má být použito tajného klíče, je nejprve vyžadována tzv. fráze hesla (passphrase), kterou je soubor se soukromým klíčem zašifrován. Tato fráze nemá nic společného s klíčem, může být libovolně dlouhá a má být volena tak, aby si ji uživatel snadno zapamatoval, a nebylo možné ji uhádnout (třeba i několik vět i s pravopisnými chybami apod.).

Systém PGP nabízí uživateli následující možnosti, jak publikovat svůj veřejný klíč:

- Zveřejnit klíč na veřejném serveru k tomuto účelu určenému.
- Poslat veřejný klíč e-mailem.
- Uložit ho do souboru a ten distribuovat dle uvážení.

Je důležité si povšimnout, že pokud není veřejný klíč distribuován přímo "z ruky do ruky" (například na disketě) od osoby, které klíč patří a známe ji, nemáme nikdy stoprocentní jistotu o identitě vlastníka klíče.

Systém PGP opírá svou důvěryhodnost, přesněji řečeno důvěryhodnost svých certifikátů, o vyjádření důvěry (podepsání) veřejného klíče od co největšího počtu dalších uživatelů (jejich výroky vytvářejí tzv. "pavučinu důvěry", anglicky: web of trust). To je principiálně odlišný přístup od toho, který vyžaduje platný zákon o elektronickém podpisu Zákon na rozdíl od tohoto přístupu počítá s existencí tzv. certifikačních autorit, které budou vydávat příslušné certifikáty, a tím potvrzovat spojení veřejného klíče a identity konkrétní osoby. Z tohoto principiálního důvodu nemůže být tedy systém PGP v této formě použit jako technologie pro elektronické podpisy ve smyslu platné právní úpravy. Z těchto důvodů tedy nelze ani elektronické podpisy vytvořené pomocí PGP považovat za právně relevantní.

5 BĚŽNÁ OHROŽENÍ ZABEZPEČENÍ V SÍTÍCH

Útočníci mají různé motivy – zisk, úmyslné poškození, slávu – ale pracují podobně. Existuje několik základních ohrožení, přičemž všechny mohou mít nekonečné množství variant:

5.1 Předstírání identity (spoofing)

paketů, které vypadají, že přišly z jiné adresy IP. Tato možnost se využívá zejména u jednocestných útoků (například útoky typu DoS). Pokud se paket tváří, že je odeslán z počítače ve vnitřní síti, je možné, že projde přes bránu firewall (která je navržena na ochranu proti externím útokům). Tyto útoky lze těžko detekovat. Vyžadují znalosti pro sledování a analýzu datových paketů. Předstírání identity v e-mailech znamená vytvoření e-mailu, v jehož poli Od není uvedena pravá adresa odesílatele. Například smyšlené e-maily, které se šířily v Internetu koncem roku 2003, využívaly nepravou e-mailovou adresu společnosti Microsoft, aby vypadaly jako zprávy upozorňující na oficiální aktualizace zabezpečení.

5.2 Neoprávněné změny (tampering).

Neoprávněné změny se týkají úpravy obsahu paketů při přenosu v Internetu nebo změny dat na disku počítače po průniku do sítě. Útočník může například umístit na síťový kabel odposlouchávací zařízení, které bude číst pakety opouštějící síť. Může tak zachytit či pozměnit odchozí informace.

5.3 Odvolatelnost (repudiation).

Odvolatelnost je schopnost uživatele nepravdivě popřít akci, kterou nemohou ostatní strany dokázat. Například uživatel, který odstraní určitý soubor, může úspěšně tento čin popřít, pokud neexistuje průkazní mechanismus (například auditování).

5.4 Zveřejnění informací (Information disclosure).

Zveřejnění informací je jejich poskytnutí někomu, kdo by k nim neměl mít běžně přístup.

5.5 Odepření služby (Denial of Service).

Útoky typu DoS jsou počítačové útoky prováděné útočníkem, který se pokouší přetížit či zastavit síťovou službu, jako je webový nebo souborový server. Útočník může například natolik zatížit server požadavky, na které se bude snažit odpovědět, že začne ignorovat skutečné oprávněné požadavky na připojení. V roce 2003 byl masivní útok DoS veden proti několika hlavním organizacím na webu, včetně Yahoo a Microsoft, s cílem znepřístupnit jejich servery.

5.6 Zvýšení oprávnění (Elevation of privilege).

Zvýšení práv je proces, kdy uživatel oklame systém, aby získal neoprávněnou úroveň přístupu, kterou může obvykle zneužít k jeho poškození či zničení. Útočník se může například přihlásit k síti pomocí účtu Guest a poté zneužít nedostatky v softwaru, které mu umožní získat oprávnění správce.

Mnoho útočníků využívá jako zbraň výpočetní sílu počítačů. Pomocí viru mohou do tisíců počítačů šířit program, který následně provede útok DoS. Mohou také například pracovat s

programy využívajícími slovníkových útoků na hesla. Mezi prvními zkoušenými hesly jsou samozřejmě slova jako „password“, „heslo“, „admin“ a hesla stejná jako přihlašovací jména.

Útočníci disponují programy, které vybírají náhodné adresy IP v Internetu a hledají nechráněné systémy. Pokud některý naleznou, zjistí, které porty jsou otevřené pro útok. V případě konkrétního otevřeného portu mají k dispozici knihovnu známých chyb zabezpečení, které lze zneužít k získání přístupu. V případě cílenějších útoků (například průmyslová špionáž) je nejefektivnější kombinace technologií s útoky typu social engineering. Sem patří například pokusy přimět zaměstnance k vyjádření důvěrných informací, hledání těchto informací v koši nebo také jednoduché hledání hesel napsaných mezi poznámkami v blízkosti monitorů.

6 FIREWALLY

S rozvojem počítačových sítí je neodmyslitelně spojen i trend k jejich vzájemnému propojování. Důvodem je tzv. síťový efekt, neboli skutečnost že většina služeb počítačových sítí získává svou hodnotu až teprve poté, kdy mohou fungovat v prostředí vzájemně propojených sítí o určité minimální velikosti.

Propojení intranetových sítí s internetem s sebou přináší nezbytnou nutnost ochrany počítačové sítě, aby byl povolen přístup do vnitřní sítě jen potřebným službám, a to v nezbytně nutném rozsahu, zatímco by byl umožněn potřebný provoz směrem ven. Pro tento druh ochrany se používá firewall jako technické zařízení kontrolující všechny provoz, který prochází mezi vnitřní chráněnou sítí a veřejným internetem.

Použití firewallu má svá omezení -- nejde o prostředek, který by zajistil bezpečnost počítačových systémů organizace v plném rozsahu a navždy. Jde však o poměrně spolehlivý prostředek pro zajištění základní bezpečnosti počítačové sítě. V případě, že by vnitřní síť nebyla chráněna firewallem, každý z vnitřních počítačových systémů by byl přímo vystaven nebezpečí útoku a vše by záviselo na zabezpečení každého jednotlivého systému. Tato technika ochrany hostitelských počítačů (host-based security) je však velmi náročná na správu počítačových systémů a především je závislá na používaných operačních systémech, aplikačním softwarovém vybavení a jejich verzích .

6.1 Co je to Firewall?

Firewall je tedy takový systém nebo skupina systémů, který na základě bezpečnostní politiky organizace slouží pro fyzické oddělení privátní sítě od Internetu, kontroluje provoz mezi její vnitřní chráněnou sítí a internetem, určuje, které služby poskytované vnitřní sítí mohou být dostupné z veřejného internetu a kým, které služby veřejného Internetu mohou být dostupné z vnitřní sítě. Firewall smí povolit pouze autorizovaný přístup do vnitřní sítě. Aby mohl firewall plnit svoji funkci, musí veškerý síťový provoz mezi vnitřní sítí a Internetem procházet přes něj. Firewall sám musí být samozřejmě odolný proti napadení .

Firewall je zařízení, které slouží pro fyzické oddělení privátní sítě od Internetu. Firewall pak plní funkci dohledu nad veškerou komunikací mezi vaší LAN a Internetem. Běžným příkladem použití je ochrana firemní sítě proti nepovoleným přístupům z internetu.

6.2 K čemu je firewall ?

Běžné routery (směrovače) směrují pakety na určená místa pasivně bez jakékoliv kontroly, tj. jsou směrovány i "škodlivé" pakety. Hlavním úkolem směrovače je tedy rozhodnout, kterým směrem posílat jednotlivé pakety tak, aby se dostaly až ke svým koncovým adresátům. Chceme-li kontrolovat pakety přicházející do naší sítě, můžeme mezi naší sítí a okolní svět postavít firewall, který zabrání proniknutí zlomyslných útočníků ke strojům v naší síti. Tato hradba však stojí přirozeně v cestě i paketům cestujícím ven z naší sítě. V užším smyslu lze firewall považovat za chytrý router, který se dívá dovnitř přichozích paketů a dále se rozhoduje, co se bude s paketem dít. Paket může být doručen na cílovou adresu, zahozen nebo dokonce firewall může přepsat hlavičku paketu např. za účelem překladu adres NAT (Network Address Translation). Firewall může také řešit autentizaci uživatelů nebo strojů.

6.2.1 Možnosti firewallů:

Celkem lze možnosti firewallu shrnout následovně:

Isolace vnitřní sítě - jeden bod přístupu.

Znemožnění zmapování sítě zvenčí.

Jemnější specifikace práv individuálních uživatelů.

Sledování provozu na síti.

Neutralizace případných bezpečnostních děr v softwaru síťových služeb.

6.2.2 Funkce firewallů:

Regulace přístupu vlastních uživatelů (uživatelů chráněné privátní sítě) do veřejného Internetu. Provozovatel firemní sítě může např. chtít zakázat svým zaměstnancům přístup k

některým serverům (např. erotickým), nebo naopak povolit přístup jen k některým konkrétně určeným serverům, či tyto aktivity alespoň určitým způsobem regulovat (nebo i jen evidovat, tak aby mohl následně vyhodnotit chování uživatelů). Stejně tak může chtít regulovat využívání určitých služeb (např. ICQ apod.), či může chtít vázat příslušná omezení na konkrétní časové intervaly (například na stanovenou pracovní dobu) apod.

antivirová ochrana - provozovatel připojené sítě může požadovat, aby firewall chránil tuto síť před nakažením počítačovými viry, což se může týkat jak přicházející elektronické pošty, tak například i pošty odcházející (aby nedošlo k zavirování externích uzlů), i dalšího druhu provozu (například přenosu textových souborů s makroviry)

optimalizace připojení - některé druhy firewallů mohou napomáhat efektivnějšímu využití přípojky dané sítě k vnějším sítím, typicky k Internetu. Jde o to, že v rámci firewallu může fungovat tzv. cache server, který v sobě uchovává některé objekty často požadované uživateli chráněné privátní sítě (nejčastěji: WWW stránky). Z vnějšího prostředí je pak sám stahuje (a tím zatěžuje přípojku) jen při prvním požadavku na ně, zatímco při dalších požadavcích na stejný objekt poskytne jeho kopii, kterou si uchoval. Díky tomu pak uživatelé připojené sítě mohou vystačit s pomalejší a tudíž lacinější přípojkou (k Internetu), než jakou by ke stejnému způsobu práce potřebovali bez právě popsané funkce firewallu.

řešení problému s IP adresami - jedním z nepříjemných problémů dnešního Internetu je nedostatek číselných adres (IP adres). Každý uzel, který má být připojen k Internetu, musí mít přidělenou takovou adresu, která je navíc unikátní (stejnou adresu nesmí mít žádný jiný počítač). Dnes jsou tyto adresy navíc závislé i na způsobu, jakým je připojení realizováno (jsou závislé na poskytovateli připojení). Se získáním potřebného počtu IP adres však mohou být v praxi spojeny určité problémy. Při použití firewallu (většiny druhů firewallů) však popsané pravidlo přestává platit - za firewallem mohou být použity takové IP adresy, které nejsou unikátní a ani nejsou závislé na konkrétním providerovi (poskytovateli internetového připojení), který připojení zajišťuje.

veřejné zpřístupnění zdrojů - ačkoli se provozovatelé připojených sítí především snaží chránit své zdroje (včetně nejruznějších informací) před neoprávněným přístupem zvenčí, přesto u některých konkrétních zdrojů (informací) mají zájem na jejich zpřístupnění i pro uživatele z vnějších sítí. Jde například o prezentaci firmy, její obchodní nabídky atd. -

obecně o cokoli, co si provozovatel privátní sítě sám určí za veřejné. V rámci firewallu pak bývá takovéto zveřejnění realizováno - například formou WWW serveru či FTP serveru, který je přístupný jak "zevnitř" (z chráněné sítě), tak i "z vně".

vzdálený přístup oprávněných uživatelů - provozovatelé firemních sítí (intranetů) velmi často vyžadují, aby uživatelé měli přístup ke zdrojům a službám těchto chráněných sítí i v případě, kdy se nachází mimo dosah této sítě (jsou například v terénu, u zákazníka apod.). V takovémto případě jsou oprávnění uživatelé v pozici vzdálených uživatelů, a součástí řešení firewallu bývá i umožnění jejich vzdáleného přístupu (remote access).

zabezpečená komunikace - veřejný Internet představuje nezabezpečený přenosový kanál, v tom smyslu že data která jsou přes něj přenášena nejsou žádným způsobem šifrována či jinak zabezpečena proti neoprávněnému "odposlechu". Potřebné zabezpečení je ale možné realizovat na vyšších úrovních (na úrovni transportní či aplikační vrstvy), a fakticky tak data šifrovat (kódovat) ještě před tím, než jsou předána k přenosu do veřejného Internetu. Takovéto řešení ale vyžaduje, aby "na druhé straně" byl někdo, kdo zakódovaná data vrací zpět do jejich původní podoby. V praxi mohou vše zajišťovat koncové uzly, které spolu komunikují. Stejně tak ale může potřebné šifrování (kódování) za účelem zabezpečení přenášovaných dat realizovat dvojice firewallů připojených k Internetu, která mezi sebou vytváří zabezpečený tunel. Díky němu pak mohou být propojeny například dvě chráněné privátní sítě skrze veřejný Internet, bez toho že by si jejich vnitřní uzly musely uvědomovat existenci zabezpečujících mechanismů a jakkoli se jí přizpůsobovat (bezpečný tunel mezi firewallly je pro ně koncové uzly neviditelný) . Pomocí takovýchto tunelů mezi jednotlivými firewallly lze dokonce realizovat celé privátní sítě (VPN, Virtual Private Network) vedoucí skrze veřejný Internet.

sdílení přístupu k Internetu - především u velmi malých sítí, tvořených jen několika málo počítači, je jedním z požadavků na jejich fungování to, aby vůbec umožňovaly přístup k Internetu všem uzlům připojené sítě. V zásadě jde o nahrazení funkce klasického směrovače, který je pro tuto roli jinak nezbytný.

6.3 Druhy firewallů:

Jak bylo zmíněno, firewall je v zásadě opatření plnící určitý cíl, a jako takové může být realizováno různými způsoby, pomocí různých prostředků, metod, postupů, technik apod.

V úvahu připadají firewally na bázi:

organizačního opatření - podstatou může být zavedení určitých organizačních opatření regulujících chování uživatelů připojené privátní sítě a způsob nakládání se zdroji, které se v této síti nachází. Takováto organizační opatření mohou například zakazovat uživatelům přinášet "zvenku" diskety a vkládat je do počítačů v chráněné síti (kvůli nebezpečí zavirování), instalovat jakékoli nové programy či je pouze z disket či jiných přenosných médií spouštět)opět kvůli nebezpečí virové nákazy, ale třeba také jako ochranu proti zavedení tzv. trojských koňů apod.). Nebo může být v rámci organizačních opatření uživatelům uloženo pravidelně měnit svá přístupová hesla, pravidelně zálohovat svá data, nenechávat citlivá data na počítačích zapojených do sítě (ale uchovávat je na médiích která se v době kdy nejsou používána ukládají do trezoru apod.). Míra ochrany proti neoprávněnému přístupu zvenčí i proti dalším možným ohrožením, která čistě organizační opatření poskytují, nemusí být vysoká - na druhé straně v konkrétních případech to může být plně postačující a optimální z hlediska nákladů na svou realizaci.

softwarového řešení - takovýto druh firewallu nevyžaduje žádné specifické (nové, dosud v síti neexistující) technické prostředky a je realizován výhradně programovými prostředky. Může se přitom jednat jen o vhodné nastavení existujících programových prostředků (například na existujícím směrovači jsou zakázány některé druhy přenosů, obecně provedena taková nastavení, jaká existující programové vybavení umožňuje). Možnosti nastavení, které existující programové vybavení nabízí, však nemusí postačovat pro dosažení požadovaných cílů. V takovém případě dochází k instalování dodatečných programových prostředků, například určité nadstavby nad operačním systémem směrovače, která mu dává potřebné schopnosti pro vykonávání funkce firewallu. Další možností je instalování samostatných programů (nikoli "nadstavbových" programů resp. rozšíření stávajícího programového vybavení), určených právě pro realizaci funkcí

firewallu, a to na "počítačových" uzlech sítě které zde již existují (tj. nikoli na směrovačích).

kombinované řešení - tento druh firewallů, využívající kombinaci programových a technických prostředků, je v praxi zřejmě nejčastější, protože je nejvíce univerzální a dokáže poskytnout nejvyšší úroveň ochrany připojené sítě. Možné formy realizace zahrnují řešení na principu demilitarizované zóny, či "monolitické" řešení atd.

6.4 Jak to funguje?

Firewally jsou bezpečnostní produkty, které chrání interní počítačové sítě. Instalují se na rozhraní mezi interní sítí LAN a Internet. Primární funkce firewalu je ochrana před neoprávněným průnikem do sítě, hackerskými útoky vedoucími k odepření služeb (Denial of Service, DoS) a posuzování oprávněnosti přístupu do sítě pro vzdálené uživatele (VPN). Firewall kontroluje veškerý provoz, který přes něj teče a na základě tzv. access-listů rozhoduje, jestli se spojení mezi počítači povolí nebo ne.

Oddělení potencionálních útočníků od nejdůležitějších serverů a počítačů vnitřní sítě LAN pomocí firewallu je nejjednodušším způsobem, jak zabránit napadení interní sítě společnosti. Firewall (nebo více firewallů) se udržuje mnohem jednodušeji než velké množství serverů a klientských počítačů s různými operačními systémy. Firewall navíc často chrání i proti ještě neobjeveným typům útoků na běžně používané operační systémy.

Firewall slouží jako "filtr", který určuje, jaké procesy mohou komunikovat s okolním světem, a na kterém portech se, případně, počítač okolnímu světu otevře a bude naslouchat.

Komunikace se v zásadě dělí na:

Outbound - výstupní, někdy v nastavení firewallu označovaná jako Local, Trusted Zone, či Allow Access.

Inbound - vstupní, někdy označovaná také jako Server, či Internet.

Jaký je v tom rozdíl?

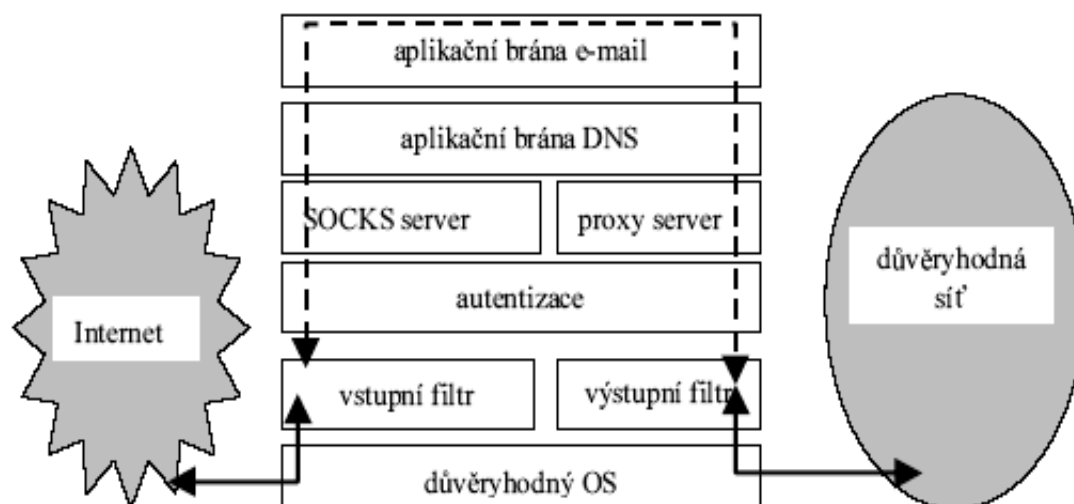
Outbound - označuje, že daný lokální proces, program, či služba může na specifikovaném portu zahájit odchozí komunikaci (iniciovat ji).

Inbound - označuje, že daný lokální proces na daném portu "naslouchá", je připraven akceptovat zahájenou komunikaci s okolním světem.

Firewall = sada pravidel pro filtrování paketů

Firewall je potom založen na sadě pravidel, která specifikují, na kterém portech bude daná aplikace naslouchat, a na kterých je oprávněna zahájit komunikaci. Pravidla pro Inbound a Outbound komunikaci se navíc liší pro tzv. Trusted Zone (komunikace na lokální síti, případně i v rámci jednoho počítače) a Internet Zone (komunikace s okolním světem).

Struktura firewallu:



Obr. 6. Struktura firewallu

6.5 Typy firewallů

Hardware

Jde o speciální zařízení se speciálním operačním systémem. Např. routery.

Výhody a nevýhody: Nízká flexibilita, vysoká cena, velká výkonnost, komplikovanější údržba a správa

Software

Jde o standardní počítače jako PC provozující běžné operační systémy jako Linux, Windows.

Výhody a nevýhody: Vysoká flexibilita, nízká cena, nižší výkonnost, jednodušší správa

Firewally se dále dělí do tří základních skupin:

Paketové filtry (Packet Filters)

Aplikační brány (Application Gateways or Proxies)

Stavové vícevrstvé inspekční brány SMLI (Stateful Multi-Layer Inspection Gateways)

6.5.1 Paketové filtry (Packet Filters)

Filtrování paketů slouží ke kontrole síťového provozu na úrovni IP paketů. Paketový filtr funguje tak, že zkoumá obsah hlavičky každého IP datagramu. Samotná hlavička obsahuje zejména IP adresu původce i adresáta, zdrojový a cílový port specifikující program, kterému je datagram určen, a další informace popisující komunikaci, ke které datagram náleží. Paketový firewall je vlastně jakýsi filtr, který na základě těchto informací rozhoduje o tom, které pakety mohou být připuštěny až k programům, nebo které naopak smějí opustit počítač. Firewall je nakonfigurován pomocí sady pravidel a pouze v případě, že paket pravidlu vyhoví, je předán dále. Pravidla jsou kombinací povolených hodnot v hlavičce IP paketu -- většinou zdrojové IP adresy, zdrojového portu, cílové IP adresy a cílového portu.

Filtrování pracuje pouze na základě uvedených vlastností paketů -- nezabývá se jejich vlastním obsahem. Dokáže tedy rozlišit pouze jednotlivé počítače, použitou službu,

případně její detaily na úrovni TCP/IP. Nedokáže již vyhodnotit nebezpečnost obsahu posílaných dat, autorizovaného uživatele apod. Dokáže však značným způsobem omezit bezpečnostní rizika. Nejčastěji se filtrování paketů kombinuje s aplikačními branami.

Jsou často implementovány na routerech.

Výhody a nevýhody:

- + není potřeba upravovat aplikace
- + vysokou rychlostí, většina operací se odehrává uvnitř jádra
- + nenáročností, lze vyrobit firewall na jedné disketě
- autentizace jen podle IP adres či čísla portů
- neumožňují logování událostí
- nejsou ani schopné upozornit administrátora na podezřelé aktivity

6.5.2 Aplikační brány (Application Gateways or Proxies)

Aplikační brána (též aplikační gateway, aplikační proxy, proxy gateway) je software běžící na firewallu, který zprostředkovává danou službu za klienta. Aplikační brána je vždy určena pouze pro jeden typ síťové služby. Její výhodou je to, že umožňuje kontrolovat provoz i na úrovni obsahu dat jednotlivých paketů, tedy na aplikační vrstvě síťového modelu OSI. Dalším důležitým faktorem je to, že často umožňuje i autentizaci uživatelů. V případě, že chce klient využít možností aplikační brány, musí se k ní nejprve přihlásit pomocí svého uživatelského jména a hesla. Toho je také možné použít k dalšímu omezení či přesnějšímu specifikování přístupových pravidel, například pro povolení práce jen vybraným uživatelům či vybraným uživatelům ve stanovený čas.

Nevýhodou aplikační brány je její svázanost s poskytovanou službou. Změní-li se například protokol služby, ať už kvůli rozšíření možností či bezpečnostním rizikům, je nutné použít novou verzi aplikační brány, která tyto vlastnosti podporuje. Některé služby také vyžadují použití nestandardního klienta, nebo jeho nestandardní nastavení. Pro některé síťové služby aplikační brány neexistují, případně vylučují smysluplné použití této služby.

Výhodou je nezávislost jednotlivých služeb. V případě problémů (ať již bezpečnostních či

technických) s jednou službou, je možné příslušnou aplikaci zastavit bez narušení ostatních poskytovaných služeb nebo dalších pravidel.

Jsou podstatně bezpečnější než paketové filtry, ale na druhou stranu jsou pomalejší a omezují uživatele na úzce vymezený okruh služeb (běžně 3 až 7), které jsou podporovány.

- + možnost autentizace na úrovni uživatelů
- + není potřeba zasahovat do jádra
- + nezávislost jednotlivých služeb
- nutnost úpravy aplikací
- svázanost s poskytovanou službou
- nutnost zvláštního programu pro každou aplikaci

Aplikační brána musí být vždy aplikována současně s použitím pravidel pro filtrování paketů, aby se zabránilo uživatelům v jejím obcházení.

6.5.3 Stavové vícevrstvé inspekční brány SMLI (Stateful Multi-Layer Inspection Gateways)

Zahrnují v sobě to nejlepší z obou předchozích skupin: rychlost paketových filtrů a zároveň zabezpečení na stejné (nebo lepší) úrovni, jako aplikační brány. Vzhledem k tomu, že kontrolu provádí na nejnižší možné softwarové úrovni (před síťovou vrstvou OSI modelu), chrání dokonale nejen vnitřní síť, ale i sám sebe.

Většinou jde o nadstavbu paketového filtru. Hlídá všechny platné tcp spojení a jejich porty, které ukládá do tabulky. V případě, že dorazí paket, který neodpovídá žádnému platnému spojení uplatní se na něj činnost definovaná politikou (zahození, předání ...).

Výhody stavového filtru:

Stavový firewall přináší značné zjednodušení filtrovacích pravidel. Nyní tedy můžeme, díky klasifikaci paketů, implicitně povolit, aby firewallem protékaly pakety patřící k již navázaným spojením (ESTABLISHED), a omezení stanovujeme na úrovni navázání spojení.

Nevýhody:

Jedinou větší nevýhodou jsou vyšší nároky na hardware firewallu. V paměti se musí totiž udržovat stavové informace o všech spojeních.

6.6 Vlastnosti moderního firewallu:

NAT (Network Address Translation)

Technika překladu adres může schovat interní IP adresu hosta před externím hostem. Nezvaný host má mnohem větší problémy s atakováním systému, který nemá registrovanou IP adresu.

Strong authentication

Technika silné autentikace se postará o povolení přístupu do sítě pouze autorizovaným osobám.

Rozšířené systémové logování

Rozšířené logování přístupů vede k zajištění zpětné kontroly

Použití šifrovaného přenosu dat

Tato vlastnost mnohem zvýší bezpečnost komunikace.

Firewally patří mezi nejúčinnější způsoby ochrání intranetové sítě před neoprávněným průnikem zvenčí. Firewall je takové zařízení, přes které prochází veškerý síťový provoz mezi intranetem a internetem, a kde je také tento provoz kontrolován na základě předem definovaných pravidel. Dva základní druhy firewallů fungují na principu filtrování paketů přímo na úrovni TCP/IP spojení nebo na vyšší úrovni aplikací pomocí tzv. aplikačních bran.

Programy firewallů generují rozsáhlé systémové záznamy o průběhu své činnosti. Správce sítě má tudíž k dispozici dostatek záznamů, které umožní odhalit veškeré pokusy o napadení sítě a usvědčit eventuálního útočníka. Přestože ani firewally nezaručí absolutní ochranu lokálních sítí, pravděpodobnost úspěšných útoků se značně sníží. Investice do

zřízení firewallu, i když jsou nemalé, se jistě vyplatí, neboť úspěšně vedený útok proti strategicky důležitým datům podniku, uloženým v souborových systémech serverů, může vážně podnik poškodit ekonomicky i morálně.

7 ZÁLOHOVÁNÍ DAT JAKO SOUČÁST BEZPEČNOSTI INFORMAČNÍCH SYSTÉMŮ

7.1 Postupy při vytváření zálohovacích strategií

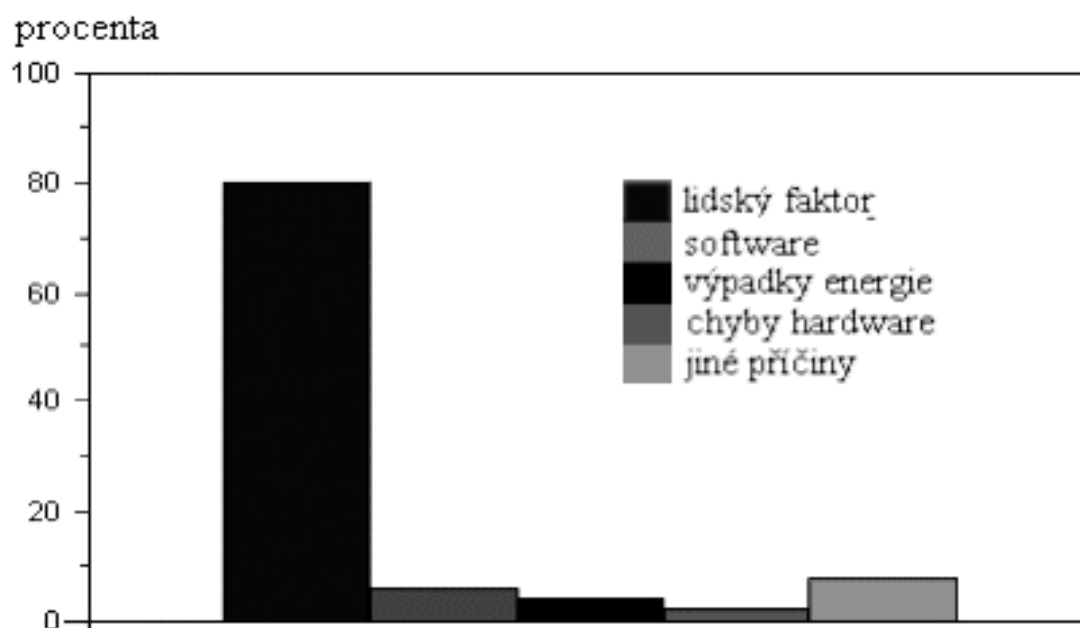
7.1.1 Význam zálohování

Nejdůležitější a nejdražší částí informačního systému jsou informace (data) v něm obsažená. Všechny ostatní prvky jsou obnovitelné, všeobecně dostupné a pouze data jsou jedinečná.

Zajištění bezpečnosti dat je součástí zajištění bezpečnosti informačního systému.

V dnešní době většina organizací uchovává důležité informace o své činnosti v elektronické podobě. Na těchto informacích jsou životně závislé a proto musí zabezpečit všem oprávněným osobám přístup k těmto informacím (to znamená zajistit dostupnost) a zajistit správnost a celistvost (to znamená zajistit integritu) informací. Jednou z podmínek zajištění dostupnosti a integrity informací je mít jejich záložní kopie. Záložní kopie slouží pro obnovení dat v případě jejich ztráty nebo znehodnocení.

Důležitost provádění zálohování dat vyplývá z následujícího grafu. Na ztrátě dat se v největší míře podílí lidský faktor (operátoři, uživatelé).



Obr. 7. Faktory ovlivňující ztrátu dat.

V tomto grafu jsou příčiny havárií zobrazeny dle statistik v procentech (zdrojem je dokumentace IBM). Proti technickým poruchám je možné stavět systémy odolné proti poruše. Pokud však uživatel omylem data vymaže nebo přepíše, je jediným zdrojem jejich obnovení záložní kopie.

Zálohovat data je možné mnoha způsoby. Správný postup stanovení metod, postupů a prostředků pro zálohování dat musí vyjít z analýzy požadavků na informační systém.

Prvním úkolem je stanovit cenu dat. Cena dat je dána odpovědí na otázku: "Kolik by nás stálo nové pořízení dat?" Mnohdy se cena dat rovná ceně organizace, protože ta není bez těchto dat schopna provozu. Další otázkou je: "Kolik nás bude stát, když nebudeme mít data k dispozici hodinu (minutu, den,...)?" Na základě odpovědí můžeme stanovit přijatelné náklady na zálohový systém v závislosti na čase obnovení. Uvedené dvě otázky jsou pouze základní. V praxi je třeba položit ještě celou další řadu otázek. Ne všechna data jsou stejně důležitá, data nejsou často uložena na jednom místě a podobně. Analýza požadavků na informační systém je pro každý informační systém jedinečná. Na základě provedené analýzy je nutné zvolit vhodnou strategii zálohování dat.

Prováděná analýza musí rovněž respektovat technické prostředí, v kterém se informační systém nachází. Při větších objemech dat může být prostředí (rychlosti přenosu po sítích,

způsoby uložení dat, druh technického vybavení) značně limitující. Dobrá analýza se snaží nekomplikovat existující systém zaváděním mnoha nových prvků, které tvoří systém komplikovanější a prodražující jeho správu.

7.2 Plánování strategie ukládání dat

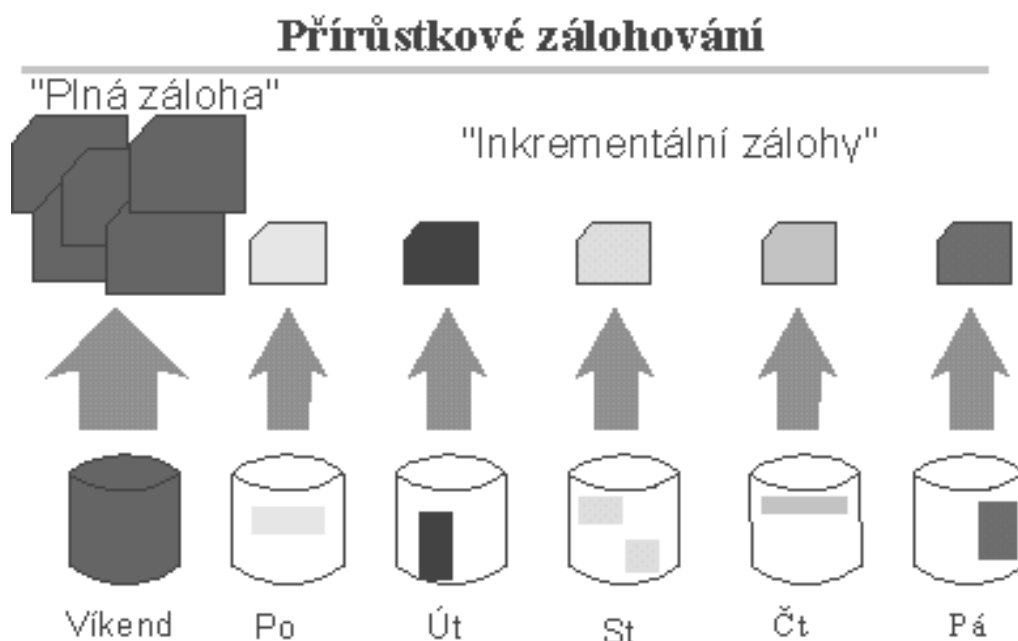
Existuje celá řada strategií zálohování dat. V následujících odstavcích popíšeme základní a nejpoužívanější typy.

7.2.1 Plné zálohování (Full Backup)

Všechna kritická data pro specifikovaný objekt jsou zálohována. Nevýhodou je časová náročnost a potřeba velkého množství úložného prostoru. Výhodou je nejrychlejší možné obnovení dat při jejich ztrátě nebo znehodnocení. Všechny poslední verze datových souborů jsou pohotově uloženy v jediném, společném balíku. Provádění plné zálohy, alespoň občas, je součástí všech užívaných zálohových strategií.

7.2.2 Přírůstkové zálohování (incremental backup)

Zálohovací systém čte atributy souborů a určí tak, které soubory byly přidány nebo modifikovány od poslední zálohy. Pouze modifikované soubory jsou zálohovány. Je to nejrychlejší způsob vytváření zálohy a je také nejúspornější z hlediska požadavků na úložný prostor. Nevýhodou je komplikovanější obnova dat. Na obrázku (Obr. 8.) je uveden příklad přírůstkové strategie. Jedná se o nejčastěji užívané schéma s jednou plnou zálohou týdně a denním přírůstkovým zálohováním. Při opravě zhavarovaného systému je nutné obnovit poslední plnou zálohu, a dále každou následující přírůstkovou zálohu.



Obr. 8. Příklad přírůstkového zálohování dat.

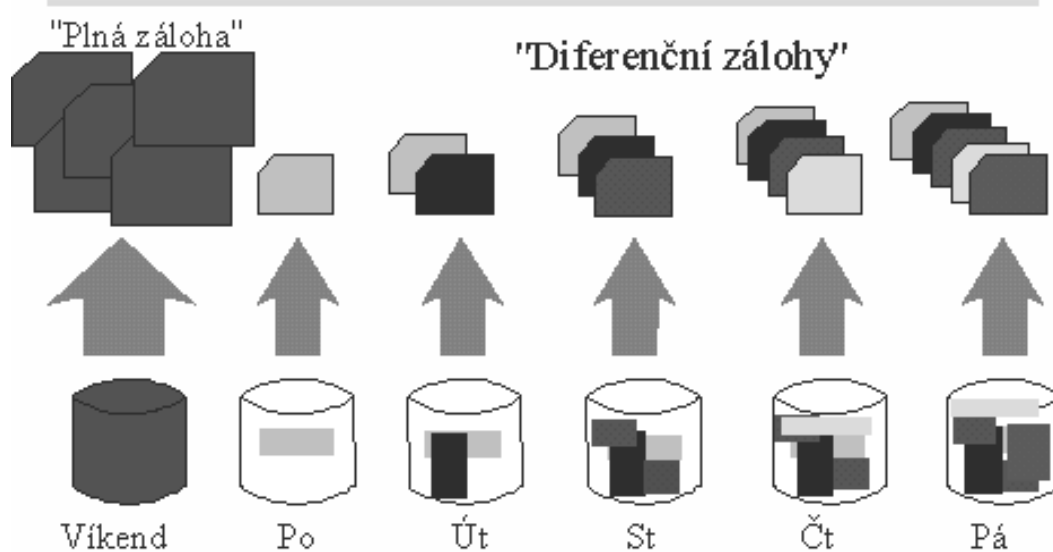
7.2.3 Víceúrovňové přírůstkové zálohování

Jedná se o stejný princip jako v předcházejícím případě. Provádíme však zálohování přírůstků z rozdílných časových intervalů. Uvedeme následující příklad: Jednou měsíčně provádíme plnou zálohu. Každý den provádíme zálohování přírůtku za daný den. Jednou týdně provedeme zálohu přírůstků za týden. Výhodou tohoto systému je jednodušší obnova dat. Vytváření záloh je oproti tomu mírně složitější.

7.2.4 Diferenční zálohování

Strategie je založena na vytváření "rozdílových" záloh. Čte atributy datových souborů a zálohuje pouze ty soubory, které byly přidány nebo změněny od poslední plné zálohy. Vytvoření zálohy potřebuje více času a úložného prostoru než přírůstkové zálohování. Proces obnovy je však mnohem jednodušší. Při obnově dat je nutné použít pouze poslední plnou zálohu a dále poslední diferenční zálohu. Příklad diferenčního zálohování je uveden na (Obr. 9.)

Diferenční zálohování



Obr. 9. Příklad diferenčního zálohování dat.

7.2.5 Zálohování na základě události

K zahájení zálohování dojde na základě předem stanovených podmínek. Např. se odpojí všichni uživatelé systému nebo dojde k replikaci dat z centrální databáze. Tato strategie neříká, zda provedené zálohování je plné nebo jiné. Tuto strategii je nutné kombinovat s některou z výše uvedených strategií.

Výše uvedené strategie jsou v podstatě nejpoužívanější strategie automatizovaného zálohování. Tyto strategie lze libovolným způsobem kombinovat dle vašich potřeb a technických či ekonomických možností.

U každé strategie je nutné ji důsledně dodržovat. Je doporučeno vést záznamy o způsobu provedení zálohování nebo si nechat tisknout seznamy zálohovaných souborů, které poté usnadňují obnovu systému. Důležitost provádění pravidelného a spolehlivého zálohování není možné podceňovat. Zvolenou zálohovací proceduru je třeba čas od času prověřit a přesvědčit se, zda jsou zálohy kompletní a spolehlivé. To znamená provést čas od času cvičnou obnovu dat (audit systému). Mnoho organizací provádí pouze zálohování a o problémech se strategií nebo postupy ukládání dat se dozví až když je pozdě.

7.3 Obnovení dat po katastrofě

Z důvodu předcházení ztrátě dat při katastrofách (požáry, povodně, teroristické útoky, atd.) je nutné vytvořit plán na ukládání a obnovu kritických dat v případě těchto událostí. Důležitým rozdílem proti běžnému zálohování je zajistit umístění záložní kopie mimo budovu, v nichž jsou data běžně uložena. Zálohovací systémy umožňují vytváření identických kopií zálohovaných dat. Takto vytvořená kopie je obvykle umístěna mimo oblast zálohovacího systému na bezpečném místě, nejlépe v protipožárním trezoru. Druhou možností je provádění zálohy kritických dat na jiný vzdálený server.

Na základě provedené analýzy a zvolené strategie je třeba zvolit vhodné prostředky pro zálohování a vytvořit postupy pro zálohování. Prostředky pro zálohování se skládají z programového vybavení, technického vybavení a komunikačních prostředků. Specializované řešení zálohování umožňují provádět ukládání dat a správu záložních dat plně automatizovaně, čímž je v podstatě možno minimalizovat lidské zásahy do tohoto systému. Kromě řešení zálohování dat umožňují i řešení dalších úzce souvisejících úloh při práci s daty, jako je archivace nebo migrace souborů. Tyto prostředky také pomáhají udržet pořádek v uložení médií se záložními kopiemi.

8 KONCEPCE OCHRANY INFORMAČNÍHO SYSTÉMU (RIZIKOVÁ ANALÝZA, PLÁN OPATŘENÍ, VRSTVOVÝ MODEL ATD.)

8.1 Bezpečnostní analýza IS

souhrn metod pro zjišťování míry bezpečnosti IS, analýza (speciální SW) a zvládání rizik

8.1.1 používané pojmy:

aktivum (vše s hodnotou),

hrozba (nebezpečnost, přístup, motivace),

zranitelnost (interakce mezi hrozbou a aktivem),

protiopatření (efektivita a náklady na pořízení, zavedení, provozování),

hranice bezpečnostní analýzy (např. složky IS, budovy, zdroje pro IS)

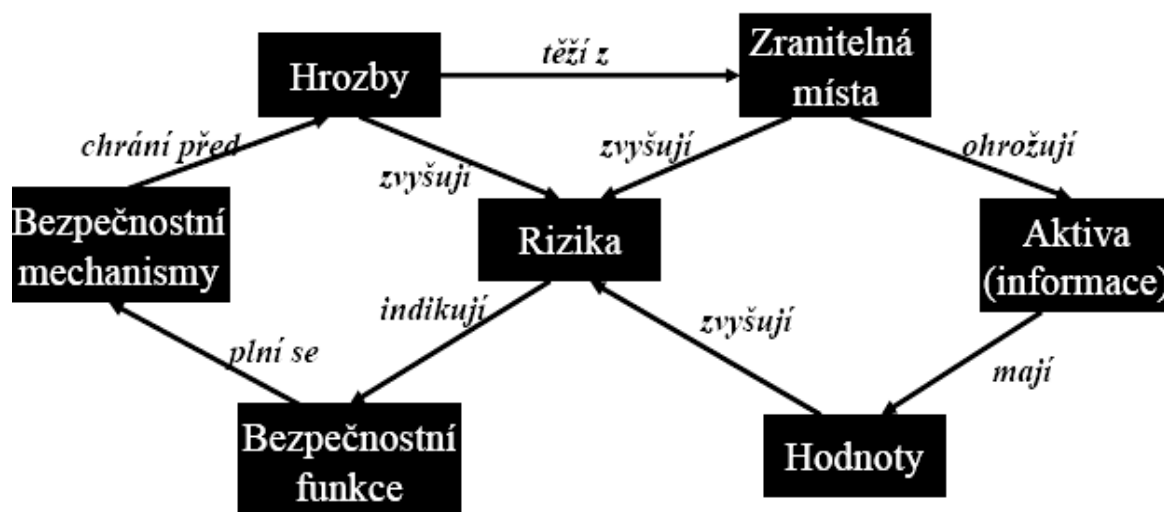
8.1.2 Vztahy v bezpečnostní analýze:

Mechanismus uplatnění rizika probíhá tak, že hrozba využije zranitelnosti, překoná protiopatření a působí na aktivum, kde způsobí škodu (důsledek).

Aktivum (svou hodnotou) motivuje člověka k aktivaci hrozby. Vůči působení hrozby se aktivum vyznačuje určitou zranitelností. Aktivum je zároveň chráněno protiopatřeními před hrozbami.

Protiopatření chrání aktiva, detekuje hrozby a zmírňuje nebo zcela zabraňuje jejich působení na aktiva. Protiopatření zároveň odrazují od aktivování hrozeb.

Hrozba působí jednak přímo na aktivum, nebo na protiopatření, s cílem získat přístup k aktivu. Aby mohla hrozba působit, musí být aktivována. Pro svou aktivaci vyžaduje zdroje (vytvoření podmínek pro její působení).



Obr. 10. Vzájemné vztahy v informačním bezpečnostním systému.

8.1.3 obecný postup:

- stanovení hranice
- identifikace aktiv
- služby - informační, technické a komunikační
- informační aktiva . databáze, datové soubory, dokumentace a manuály, plány při haváriích
- SW aktiva
- fyzická aktiva
- stanovení hodnoty (pořizovací, závislost IS na aktivu, cena informace atd) a seskupování aktiv
- identifikace hrozeb - zkušenost, seznam podle funkcí IS
- analýza hrozeb a zranitelností
- stanovení úrovně rizika (míra nejistoty stanovení)
- zvládání rizik - vybírání protiopatření

8.1.4 Typické hrozby pro IS:

- neoprávněné čtení - z obrazovky, z klávesnice, z paměťových médií
- zneužití zdrojů systému - zneužití služeb, vyřazení systému, viry, trojské koně, nedbalost
- průniky - záměrné překonávání zabezpečení IS - nedostatek v návrhu
- selhání komponenty - zařízení, nepředpokládané stavy IS, prostředí ovlivňování - - modifikace prvků IS
- odposlouchávání
- modifikace přenášených zpráv
- odepření komunikačních služeb

8.1.5 Příznaky ohrožení systému:

1. neexistující plán celkové ochrany
2. nedostatek vyváženosti celkových opatření (např. přehlížení osob pro manipulaci s daty)
3. provozní nepořádek
4. nedostatečná dokumentace programů
5. nízká pracovní morálka
6. neadekvátní rozdělení odpovědností
7. nedostatek vnitřní kontroly bezpečnostních aspektů

8.2 Etapy zabezpečení IS:

- řešení bezpečnosti IS se prolíná všemi fázemi jeho životního cyklu
- pro každou fázi jsou podrobně předepsány vstupní a výstupní dokumenty, např. pro úvodní studii vstupními dokumenty jsou právní předpisy, záměr vytvoření IS, bezpečnostní politika, výstupními dokumenty jsou úvodní bezpečnostní studie, koncepce testování



Obr. 11. Základní fáze řešení bezpečnosti IS.

- je nutné dodržet všechny níže rozepsané etapy:

8.2.1 Úvodní studie

Záměr vytvoření IS a vlastní úvodní studie (právní požadavky, bezpečnostní politika, charakteristika současného stavu, cílů, vztahu k okolí, všeobecná charakteristika IS, koncepce bezpečnosti a podmínky pro bezpečnost)

8.2.2 Analýza a návrh

Globální a detailní (rozpracování požadavků do konkrétních opatření, bezpečnostní model a architektura, návrhy rozhraní, ověření úplnosti návrhu, dotažení na úroveň SW, HW, organizace)

8.2.3 Realizace

Implementace a zavádění (provozní dokumentace, realizace testů, získání akreditace, zaškolení obsluhy a uživatelů)

8.2.4 Provoz, údržba a rozvoj IS

Průběžné školení, vedení záznamů, kontrola dodržování, analýza rizik, reakce na změny prostředí a změny požadavků.

8.2.5 Plán bezpečnostních opatření:

Popisuje, jak daná organizace přistupuje k otázkám bezpečnosti

- musí být dostatečně často revidován a musí být zkoumáno jeho dodržování
- vypracováním plánu bývá pověřena skupina odborníků pokud možno ze všech důležitých organizačních struktur firmy, velikost a struktura tohoto týmu závisí na velikosti firmy

8.2.6 Plán bezpečnostních opatření - součásti:

- politika - vyhlášení bezpečnostních cílů (např. ochrana dat před katastrofami, před úniky mimo organizaci apod.), participace personálu, zodpovědnosti, závazky organizace na udržení bezpečnosti (počet vyčleněných pracovníků, minimální vyčleněné výdaje)
- popis současného stavu
- doporučení ke splnění bezpečnostních cílů
- kompetence osob ke splnění bezpečnostních cílů (uživatelé PC ručí za svůj počítač, administrátor databázového systému zodpovídá za přístup k datům a jejich integritu, firma může pověřit zvláštního pracovníka zodpovědného za vytvoření obecných pravidel práce s daty a jejich uvolňování či rušení, pracovníci osobního oddělení zodpovídají za přijetí důvěryhodných a spolehlivých pracovníků atd.)
- časový harmonogram
- trvalé sledování - záznamy, plán prověrek, inovací

- dodržování - seznámení všech pracovníků, dostatečná podpora vedení organizace

8.2.7 Ochranné vrstvy IS:

1. kontroly bezpečnosti a přesnosti zabudované v systému
2. fyzická obrana
3. administrativní kontroly
4. legislativní a společenské prostředí

8.2.8 Vybrané aspekty ochrany IS (prolínají se):

- personální - přihlídnutí při přijímání, působení na bezpečnostní povědomí zaměstnanců, dohoda o zachování mlčenlivosti
- organizační - kontrola, disciplinární opatření, hlášení bezpečnostních incidentů, správa oprávnění, práce s hesly, ochrana před viry a jinými nežádoucími programy včetně nelegálního software, zálohování, postupy v případě havárií

Riziková analýza:

Tab. 1. Riziková analýza hodnot IS.

Hodnota	Utajení	Integrita	Dostupnost
Hardware		přetížení, zničení, narušení	krádež ztracení, nedostupnost
Software	zcizení, kopírování, ,zneužití	viry, trojské koně, modifikace	vymazání, ukončení práva užívání
Personál	zneužití přístupových práv		výpověď, odchod na dovolenou
Data	odhalení, vnější narušitel, dedukce	poškození chybou SW, Hw nebo uživatele	vymazání, záměna, zničení
Dokument.		neautorizovaná úprava	ztráta, zcizení, poškození
Materiál			ztráta, zcizení, poškození

8.2.9 Odhad pravděpodobnosti vzniku nežádoucích situací:

dlouhodobé sledování výskytu jevů (pojišťovny - počet požárů, počet obytných domů a výše škody, trestné činy, frekvence lidských chyb)

sledování a charakteristika konkrétního systému (počet HW a SW chyb, objem dat apod.)

odhad daného odborníka

Delfský přístup - pravděpodobnost výskytu jevu odhadována nezávislými odborníky, korekce mínění odborníků po srovnání jejich názorů, snaha po konsenzu

8.2.10 Základní aspekty ochrany dat, základní požadavky:

bezpečnost a správnost dat

oprávněnost přístupu k datům

právo na soukromí

poznatky:

udržovat dostatečnou míru bezpečnosti (absolutní bezpečnost nedosažitelná)

náklady na zabezpečení by měli odpovídat stupni zranitelnosti systému a hodnotě dat

celkové riziko je součtem dílčích rizik - cílem je jeho minimalizace

při odhadu rizika se často pracuje s pojmy: pravděp. výskytu chyby, kategorie velikosti ztrát, pravděp. zabránění chybě, náklady na zabránění chybě

tři zásady:

prevence (minimalizace pravděpodobnosti vzniku)

minimalizace vzniklých škod

návrh rychlé a spolehlivé metody obnovy

8.2.11 Možné příklady rizik:

- katastrofy a živelné pohromy
- chyby technického a programového vybavení:
- výpadek počítače
- poškození stopy disku
- disk (disketa) nečitelný
- chyba v aplikačním programu poškozuje záznam
- lidská nepozornost:
- chyba zavádění vstupních dat
- zavedení a aktualizace nesprávných dat
- fyzické poškození nosného média
- úmyslné poškození:

- sabotáž
- zlomyslnost uživatele
- kriminalita, zpronevěra, korupce, špionáž aj.
- narušení soukromí:
- zvědavost
- neúmyslné prozrazení soukromých informací

8.2.12 Jednoduchý vztah pro odhad rizika:

Z - kategorie velikosti ztrát, Z=0 až 7 (od 10^1 do 10^8 USD)

P - kategorie pravděpodobnosti výskytu jevu (viz. tab.), od praktické nemožnosti po výskyt 10 x denně.

používají se vztahy

$$R = \frac{10^{(P+Z-2)}}{4} \quad (1)$$

resp. R = ztráta způsobená jevem / střední doba mezi jevy

pravděp. výskytu jevu (P):

- | | |
|---|-----------------------------|
| 1 | jednou za 400 let |
| 2 | jednou za 40 let |
| 3 | jednou za 4 roky (1000 dní) |
| 4 | jednou za 100 dní |
| 5 | jednou za 10 dní |
| 6 | jednou denně |

7 desetkrát za den

Uložení kopií na více různých místech, platí vztah součin pravděpodobností, je-li pravděpodobnost zničení dat na jednom místě postupně P_1 , P_2 , P_3 rovna 10^{-3} , je pro dvě místa pravděpodobnost ztráty $P_{1,2} = 10^{-6}$, pro tři místa již jen $P_{1,2,3} = 10^{-9}$

9 ANALÝZA RIZIK

Pro analýzu rizik bývá většinou použita britská metoda CRAMM (CCTA RISC Analysis and Management method), která je uváděna i v doporučení evropské normy ITSEM

9.1 Metoda CRAMM

CRAMM je formalizovaná a strukturovaná metoda analýzy a optimalizované eliminace bezpečnostních rizik, která byla původně vyvinutá pro implementaci a začlenění všech ochranných opatření zabezpečujících IS, která obsahují cenná nebo jinak citlivá data.

Hlavním cílem je poskytnutí úplné množiny protiopatření zabezpečujících IS jak již existující, tak vyvíjené na úrovni, jež může být dle možností a přání postupně dále zvyšována.

CRAMM definuje IS jako soubor provázaných aktiv následujících typů.

fyzická aktiva (HW tvořící počítače a komunikační S)

programová aktiva obsahující aplikační programové vybavení

datová aktiva zahrnující aplikační data

jednotlivá aktiva jsou přitom provázána řetězem závislostí (např. efektní užití dat z aplikace je vázáno na ASW, který závisí na HW

9.1.1 Analýza a eliminace rizik CRAMM

Analýza a eliminace rizik CRAMM má 3 stupně:

- 1) jsou zjištěna systémová aktiva – data, aplikační programy a technické vybavení. Tato aktiva jsou ohodnocena. Ohodnocení dat. aktiv podle předdefinovaných stupnic reprezentujících vliv na činnost S ztrátou, zničením, neoprávněným zveřejněním dat. (ohodnocení prostřednictvím interview s odpovědnými osobami, které nám řeknou co se stane, co by znamenala pro IS ztráta těchto dat). Ostatní aktiva jsou ohodnocena podle ceny.
- 2) jsou vyšetřovány míry hrozeb a zranitelnosti útočících na jednotlivá aktiva. Formou interview jsou zjišťovány odpovědi na dotazy týkající se hrozeb a zranitelnosti.

Výsledkem je stanovení míry hrozeb a zranitelnosti ve škále: malá, střední, velká. Závěrem je zjištěna míra rizika pro jednotlivé kombinace aktiv s přiřazenou hrozbou. Velikost míry rizika závisí na hodnotě aktiva, na měře hrozby a zranitelnosti. Je to číslo vypovídající jasně o potřebné míře ochrany.

- 3) pro vybraná ohrožení jsou stanovena bezpečnostní opatření, která jsou adekvátní bezpečnostním požadavkům. Bezpečnostní protipatření zahrnují následující aspekty bezpečnosti IS:
- technický protipatření – tvořící funkce a mechanismy prosazující bezpečnost,
 - netechnický protipatření fyzická, personální a procedurální.

9.2 Bezpečnost

Smyslem řešení bezpečnosti je zajistit, aby všechny fáze životního cyklu IS byly bezpečné nejen z hlediska datového obsahu ale i zajištění:

- bezpečného vývoje celého IS (používání správných vývojových prostředků a správných personálních postupů)
- bezpečného provozu IS (používání správných personálních postupů, postupů v oblasti údržby a bezpečné provádění jakýchkoli změn)

9.3 Normy ITSEC

V rámci řešení bezpečnosti IS bývají do bezpečnostní politiky zahrnuty body, týkající se oblasti bezpečnosti fyzické a personální. Teoretickým základem pro tuto činnost jsou evropské normy z oblasti bezpečnosti informačních technologií ITSEC. Specifikace bezpečnosti IS se podle ITSEC skládají z pěti částí: (dokument ITSEC)

- 1) Systémová bezpečnostní politika – dokument, který je veřejně dostupný a který uvádí hlavní bezpečnostní zásady IS.
- 2) Specifikace funkcí prosazujících bezpečnost – souhrn funkcí IS, které nějakým způsobem řeší některou oblast bezpečnosti, nebo-li lze tuto část označit jako požadavky na funkčnost IS v oblasti bezpečnosti
- 3) Požadované bezpečnostní mechanismy – nepovinná část, která se uvádí v případě, kdy je třeba zdůvodnit nutnost existence některých bezpečnostních mechanismů. Tato situace nastává v případě nutnosti akceptovat určitá technická řešení

- 4) Minimální síla mechanismů – norma ITSEC vyžaduje vedení této pasáže a volbu 1 ze 3 variant
- 5) Požadovaná úroveň hodnocení – zde se uvede ze 7 tříd požadavků na míru záruky – zvolíme si ji

9.4 Systémová bezpečnostní politika

9.4.1 Ochrana informačních aktiv

V první fázi a části se *stanovíme funkce vykonávané IS, definujeme si jednotlivá aktiva* a to jak fyzická (HW+DB server, služební server, prezentační server, firewall, síťová distribuční zařízení, komunikační linky...), programová a datová (nejdůležitější, protože počítače i programové vybavení lze získat za peníze, ale data mohou být unikátní a získatelná jsou jen velmi těžce)

Ochranou informačních aktiv rozumíme:

- fyzickou ochranu zařízení,
- udržování integrity programového vybavení a dat
- ochrana proti neoprávněnému vyzrazení informace,
- zajištění neustálé dostupnosti důležitých služeb,
- zajištění správné funkce IS,
- personální zabezpečení pro podporu předcházejících bodů.

9.4.2 Definice rolí v systému bezpečnosti:

manažer bezpečnosti – nejvyšší bezpečnostní funkce v podniku, řídí činnost nižších složek, navrhuje implementace protiopatření stanovených na základě analýzy rizik, kontroluje vedoucí projektů zda implementovali daná protiopatření.

personalista – hlídá dodržování opatření v oblasti personální bezpečnosti

správce bezpečnosti IT – prosazuje zásady bezp. IT, řídí jednotlivé správce bezp. systémů

správce budov – zodpovídá za provádění fyzických protiopatření

finanční manager – prosazuje návrhy manažera bezpečnosti z hlediska finančního

správce bezp. systému – dohlíží na bezpečný chod konkrétního S

správce OS – zodpovídá za správný chod OS, integritu vybavení, dohlíží na kapacitní využití, sleduje novinky a navrhuje přechod na novou verzi, provádí zálohování dat

správce sítě – zodpovídá za správný chod sítě a sleduje kapacitní využití

administrátor databází – dohlíží na správný chod DBS, sleduje kapacitní využití, provádí zálohování nástrojů DBS

vedoucí projektu – odpovídá za implementaci protipatření do IS (návrh na základě analýzy rizik)

9.4.3 Definice cílů

Cílem je poskytnout IS jako celku ochranu odpovídající výsledkům provedené analýzy rizik v daných oblastech:

- a) zajištění identifikace a autentizace uživatelů
- b) pravidla přístupu – rozlišit uživatele a zajistit tak diferencovaný přístup k informacím
- c) zajistit dostatečnou důvěrnost zpráv a dat ukládaných a přenášených systémem
- d) zajistit neodmítnutelnost
- e) zajistit dostatečnou dostupnost S
- f) evidence přístupu k datům – k určení osoby, která daný příkaz provedla

9.4.4 Identifikace hrozeb

Možné hrozby:

- a) předstírání identity – vydávání se za někoho jiného a vůle získat přístup k S
- b) získání nepovolených privilegií – chci získat přístup k informacím, ke kterým nemohu
- c) anonymita prováděných akcí – nelze zpět zjistit původce daných akcí
- d) prozrazení – s obsahem dat či el. zprávy se seznámí nepovolaná osoba (s uloženými daty či přímo při přenosu)
- e) modifikace – pozměnění dat (při přenosu, před promítnutím do databáze, uložených v databázi)
- f) odmítnutí zodpovědnosti – popření zaslání či odeslání dat či zprávy

- g) zneužití privilegií – důvěryhodná osoba provede akci, o které se předpokládá, že by je nikdy neprovedla (špatně určená privilegia, zařazení do vyšší kategorie)
- h) technická závada některé komponenty
- i) vnější vlivy – požár, potopa...
- j) úmyslné poškození – zastavení provozu v důsledku úmyslného poškození, krádeže či teroristického činu

Proti těmto událostem či akcím (aby byl případně minimalizován jejich dopad) jsou do IS implementován a protiopatření.

Potřeba implementace těchto protiopatření vyplynula ze závěrů provedené analýzy rizik, na základě ocenění všech aktiv, ze kterých se S skládá a ohodnocení prostředí, ve kterém je provozován.

9.4.5 Protiopatření (dle členění hrozeb)

- a) délka hesla, frekvence, změny hesla, způsob tvorby hesel...
- b) bezpečnostní účtování veškerých akcí, audit, pravidelné přezkoumávání přístup. práv
- c) přiřazení unikátního identifikátoru každému uživateli (1 uživatel – 1 účet)
- d) šifrování přenášených dat, ochrana před předstíráním identity, prostředky pro úplné rušení dat na paměťových médiích, fyzická ochrana zařízení
- e) šifrování přenášených dat, ochrana před předstíráním identity, prostředky pro úplné rušení dat na paměťových médiích, fyzická ochrana zařízení
- f) elektronické podepisování pro zabránění odmítnutí původu a přijetí založeno na asymetrické kryptografii
- g) protiopatření ze skupiny řízení správy S, personální protiopatření
- h) ochrana proti chybám zařízení, postupy havarijního plánování
- i) zajištění fyzické bezpečnosti – proti poškození vodou a ohněm, krádežím, detekce bomb, reakce na varování o uložení bomb

9.4.6 Dodržování zásad bezpečnostní politiky

Míra ochrany S i informací musí být úměrná hodnotě a předpokládaným hrozbám.

Protiopatření musí trvale pokrývat všechny významné hrozby.

Informace je nutné chránit ve všech formách a na všech médiích.

Bezpečnost S musí být řízena, provozována všemi vedoucími pracovníky a musí být všeobecně respektována.

Shrnutí:

Pro **analýzu rizik** bývá většinou použita britská metoda **CRAMM** (CCTA RISC Analysis and Management method), která je uváděna i v doporučení evropské normy ITSEM

CRAMM je formalizovaná a strukturovaná metoda analýzy a optimalizované eliminace bezpečnostních rizik, která byla původně vyvinutá pro implementaci a začlenění všech ochranných opatření zabezpečujících IS, která obsahují cenná nebo jinak citlivá data.

Analýza a eliminace rizik CRAMM má 3 stupně:

- jsou zjištěna systémová aktiva,
- jsou vyšetřovány míry hrozeb a zranitelnosti útočících na jednotlivá aktiva,
- pro vybraná ohrožení jsou stanovena bezpečnostní opatření.

Smyslem **řešení bezpečnosti** je zajistit, aby všechny fáze životního cyklu IS byly bezpečné nejen z hlediska datového obsahu ale i zajištění:

- bezpečného vývoje celého IS,
- bezpečného provozu IS.

V rámci řešení bezpečnosti IS bývají do bezpečnostní politiky zahrnuty body, týkající se oblasti bezpečnosti fyzické a personální. Teoretickým základem pro tuto činnost jsou evropské normy z oblasti bezpečnosti informačních technologií ITSEC.

Systémová bezpečnostní politika zhrnuje tyto části:

- ochrana informačních aktiv,
- definice rolí v systému bezpečnosti
- definice cílů,
- identifikace hrozeb,
- protiopatření,
- dodržování zásad bezpečnostní politiky.

10 ANALÝZA CHYB PROJEKTOVÉHO TÝMU A ZADAVATELE PŘI ŘEŠENÍ PROJEKTŮ IS/IT

10.1 Chyby, kterých se dopouští firma zavádějící IS

-jde o tzv. **bariéry na straně dodavatelské firmy**

- 1. poruchy v komunikaci**
- 2. nejsou zjištěny všechny informace o firmě (strategie firmy, informační strategie firmy, požadavky na systém, funkce systému apod.)**
- 3. chybné sestavení časového harmonogramu a koordinace jednotlivých činností, chybné odhady finanční náročnosti**
- 4. nenaplněná očekávání**
- 5. technické problémy**
- 6. potíže při spolupráci s jinými IS**
- 7. konverze dat**
- 8. vlivy konkurence**
- 9. určení zodpovědných pracovníků za jednotlivé činnosti etapy zavádění**
- 10. nedostatečná kvalifikace pracovníků a neustálé zdokonalování (kurzy)**
- 11. neúplná či nesrozumitelná dokumentace**

10.2 Chyby, kterých se dopouští management zadavatele

- jde o tzv. **bariéry na straně managementu**

IS má managementu sloužit jako podpora jeho strategického, taktického a operativního řízení.

Chyby:

10.2.1 Chyby při formulaci cílů

Špatný cíl - spočívá v rozsahu, obsahu a načasování, špatná strategie.

Nízký cíl - důsledek povrchní analýzy jak vlastní firmy, tak okolí, nevyužití zdroje, averze k riziku.

Nejasný cíl, plané řeči, na stanovení cíle se nepodílely výkonné složky, a tak ho nesdílejí, nejistota personálu firmy.

Příliš vysoký cíl - špatné odhady, podcenění rizika, stresování a konflikty. Z uvedeného vyplývá, že před konečnou formulací cílů je nutné provést tzv. manažerský audit – odhalení rizikových faktorů, jedná se o posouzení fungování řídicích procedur, posouzení ekonomie a efektivnosti a úsilí, s jakým firma dosahuje svých cílů.

10.2.2 Špatně zvolená strategie firmy, ze které vychází tvorba IS

při tvorbě strategie je možné se dopustit chyb v různých fázích procesu tvorby:

a) chyby, kterých se tým navrhující systém dopouští v práci s informacemi v průběhu organizování prací: selektivní slepota, bariéry komunikace, nejasné kompetence, anonymita, neschopnost formulace, anonymita rozhodnutí, podcenění detailů

b) chyby v procesu rozhodování - přílišná kvantifikace, vynechání důležitých závislostí, nesoulad a neúčinnost prostředků, nevhodný způsob realizace, princip satisfakce, snaha dosáhnout požadovaný výsledek, zásada ekonomie rozhodování, neschopnost analyzovat riziko a vyjádřit protiriziková opatření, přeceňování příznivých jevů, podceňování nepříznivých jevů

c) chyby, kterých se lze dopustit v návrhové části tvorby strategie

špatně stanovený cíl, odtržení od reality, jazyk strategie, časté revize strategie, přílišná orientace na přítomnost, orientace na nepřiměřený růst firmy, problém metod, neschopnost plánovat

Závažnou chybou je také nesoulad mezi funkcionálními strategiemi – stanovení priorit mezi jednotlivými strategiemi.

10.2.3 Další chyby:

Problémy s organizačními změnami (nutná příprava změn + zainteresovanost na řízení a účasti celého projektu)

Komunikace uvnitř firmy, komunikace s dodavatelem IS

Negativní postoj k IS/IT, neznalost IS (psychologický faktor)

Přijímání nových pracovníků (pro provoz nového systému)

Nedostatečná motivace svých řadových pracovníků (příprava na změny)

Nejsou stanoveny osoby, odpovědné za případné prováděné změny apod.

Dozorčí komise neprovádí dohled nad průběhem instalace

10.3 Chyby, kterých se dopouštějí řadoví pracovníci zadavatele

-jde o tzv. bariéry na straně zaměstnanců uživatele IS

1. **podcenění změn** - uživatel musí dělat jednak svoji běžnou práci a často ještě pracovat se dvěma systémy najednou (časová náročnost)
2. **neumí popsat svou práci**
3. **necítí se být zlepšovatelem a organizátorem své práce**
4. **malá informovanost řadových pracovníků o možnostech IS**
5. **psychologický faktor** (neví, co by měli od PC požadovat, odmítají používat PC, nechutí k změnám)

Většině chyb se dá předcházet, protože problémy, které se vyskytnou, se objevují při každém projektu. Chyby vyplývají mimo jiné také z podceňování tzv. **kritických faktorů**.

10.4 Kritické faktory projektu IS

Pevně stanovený čas – u velkých projektů nelze ihned na začátku odhadnout trvání celého projektu. Je nutné plán rozdělit podle etap. Na začátku vývoje se vytvoří pouze rámcový odhad času a pro každou etapu se upřesňuje.

Pevně stanovená cena – opět u velkých projektů nelze cenu stanovit dříve, než po úvodní studii (kdy lze podle rozsahu plánovaných prací a změny technologické infrastruktury a na základě předchozích projektů udělat přesnější odhad).

Omezené zdroje – lidé pracující na projektu musí plnit i své běžné úkoly (hlavně delegování uživatelé do projekčního týmu a GIT. Je nutné předem určit podíl těchto pracovníků na projektu, komu budou podřízeni, kdo jim bude podepisovat plat, apod.)

Různé profese pracující v jednom týmu – způsobují problémy při komunikaci. Lze tomu předcházet zavedením jednotné metodologie (základ komunikace).

Neustálé změny požadavků ze strany uživatele/zadavatele – je třeba formálně definovat změnové řízení (k tomu je třeba mít formální specifikaci požadavků), písemnou dokumentaci (včetně dokumentace všech rozhodnutí). Navíc používat takové techniky a nástroje, které umožní snadné promítání změn do specifikace a návrhu.

Zralost organizace, potřebná k akceptování informačního systému a změn, které z jeho zavedení vyplývají. Organizace zpravidla není schopna přeskočit několik stupňů „vyspělosti“. Stupeň zralosti organizace k zavedení systému je dán současnou úrovní informační technologie. Tento faktor musí být zohledněn již v etapě informační strategie a rozpracování v úvodní studii.

Každý projekt má určitou **míru rizika výskytu chyb**. Tato míra je daná:

- velikostí projektu (velké projekty jsou rizikovější než malé)
- zkušeností týmu s používanou technologií (vývoje a realizace) – riziko se snižuje, jestliže má vývojový tým zkušenosti s používanou technologií (tj. zná metody a techniky používané při vývoji, umí pracovat s používaným CASE prostředím, zná implementační prostředí) a zároveň pokud vývojový tým a uživatelé znají oblast, pro kterou se informační systém vytváří
- strukturou projektu (riziko se sníží, pokud navrhovaná aplikace odpovídá existující struktuře práce a pokud v organizaci souhlasí a podporují změny).

ZÁVĚR

Bezpečnost informací je velmi složitá sféra zásadní důležitosti v oblasti komunikace. Bezpečnostní opatření musí chránit informace v sítích před různými typy ohrožení.

Na začátku byly řečeny základní principy bezpečnosti – jaké vlastnosti má mít systém a jakým způsobem lze narušit bezpečnost zpracovávání informací. Protože bezpečnost IT použitých v organizaci se dosahuje především plněním manažerských funkcí, byly vyjmenovány.

Kvůli obavám z bezpečnostních rizik zvažují soukromé společnosti, banky, pojišťovny, i vládní instituce co nejkvalitnější systémy zabezpečení přístupu do svých prostor a sítí obsahujících citlivá data. K těmto účelům si vybírají systémy s biometrikou, proto jí byla věnována jedna kapitola alespoň pro základní orientaci - jak fungují, kde se používají, jaké mají výhody a nevýhody. Použití biometrie by mohlo zdokonalit kontrolní postupy například v případě přístupu k osobním údajům týkajících se třetích stran, například v případě krádeže nebo zneužití (autorizační postupy).

Část věnovaná infiltracím prozradila jaké bezpečnostní nástrahy číhají na naše informace, jaké škody mohou nastat a také byly uvedeny dva vzorové příklady k odvirování počítače. Základy kryptografie byly vybrány proto, že tato problematika je velmi skloňována zejména z toho důvodu, že běžný provoz v sítích a internetu šifrován není a pro útočníka není problém odchyťovat (odposlouchávat) komunikaci a tím buď přímo zjistit např. obsah e-mailové zprávy nebo získat důležitá hesla. Šifrování je silný prostředek jak tomu čelit a díky kryptografickému balíku PGP je tato metoda dostupná široké veřejnosti, zejména kvůli integraci do programu MS Outlook a není problém s ním vytvořit třeba celý šifrovaný disk, ovšem v placené verzi. Využívá zejména nesymetrické šifrování, jehož princip byl vysvětlen a pro lepší představu doplněn grafickým znázorněním. Patří sem i elektronický podpis, popřípadě zaručený elektronický podpis, který se snad začne hojněji používat při styku s našimi úřady.

Útočníci mají různé motivy – zisk, úmyslné poškození, slávu – ale pracují podobně. Existuje několik základních ohrožení zabezpečení v sítích popsanych v 5. kapitole. Propojení intranetových sítí s internetem s sebou přináší nezbytnou nutnost ochrany počítačové sítě, aby byl povolen přístup do vnitřní sítě jen potřebným službám, a to v nezbytně nutném rozsahu, zatímco by byl umožněn potřebný provoz směrem ven. Pro

tento druh ochrany se používá firewall. Co to je, k čemu slouží, jaké jsou jeho funkce, druhy, typy, jak funguje a jaké má mít moderní firewall vlastnosti, k tomu posloužila kapitola jím věnovaná. Investice do zřízení firewallu, i když jsou nemalé, se jistě vyplatí, neboť úspěšně vedený útok proti strategicky důležitým datům podniku, uloženým v souborových systémech serverů, může vážně podnik poškodit ekonomicky i morálně.

Jednou z podmínek zajištění dostupnosti a integrity informací je mít jejich záložní kopie. Záložní kopie slouží pro obnovení dat v případě jejich ztráty nebo znehodnocení. Je dobré vědět, jaké máme plánovací strategie ukládání dat, jaké jsou jejich výhody a nevýhody. Vyplynulo, že u každé strategie je nutné ji důsledně dodržovat, že důležitost provádění pravidelného a spolehlivého zálohování není možné podceňovat a zvolenou zálohovací proceduru je třeba čas od času prověřit a přesvědčit se, zda jsou zálohy kompletní a spolehlivé. To znamená provést čas od času cvičnou obnovu dat (audit systému).

Z dalších kapitol jsou důležité základní požadavky ochrany dat, tedy konkrétně: bezpečnost a správnost dat, oprávněnost přístupu k datům a právo na soukromí. Shrnující poznatky říkají, že je potřeba udržovat dostatečnou míru bezpečnosti, náklady na zabezpečení by měly odpovídat stupni zranitelnosti systému a hodnotě dat a že celkové riziko je součtem dílčích rizik - cílem je jeho minimalizace, což se dá naplnit třemi zásadami: prevencí (minimalizace pravděpodobnosti vzniku), minimalizací vzniklých škod a nakonec návrhem rychlé a spolehlivé metody obnovy. Na konec byla ponechána analýza chyb projektového týmu a zadavatele při řešení projektů IS/IT. Většině chyb se dá předcházet, protože problémy, které se vyskytnou, se objevují při každém projektu. Chyby vyplývají mimo jiné také z podceňování tzv. kritických faktorů, viz. posední kapitola této práce. Na závěr je třeba poznamenat věc nejdůležitější, a to, že absolutní bezpečnost je nedosažitelná, není ani stálá, a proto si musíme pamatovat, že : **BEZPEČNOST JE TRVALÝ PROCES!**

SEZNAM POUŽITÉ LITERATURY

- [1] Ing. Rita Pužmanová, CSc., MBA. Biometrické systémy v praxi. *IT SYSTEM 3/2004 - Bezpečnost* [online]. 2004, [cit. 2005-28-05]. Dostupný z WWW: <http://www.systemonline.cz/site/bezpecnost/04_02puzman.htm>.
- [2] Milan Ďásek. Biometrika. *referát do BIS* [online]. 26.02.2003, [cit. 2005-28-05]. Dostupný z WWW: <<http://www.volny.cz/pretorian/biometrika.html>>.
- [3] Úřadu pro ochranu osobních údajů : *Pracovní dokument o biometrii* [online]. [cit. 2005-28-05]. Dostupný z WWW: <http://www.uoou.cz/zahr_EK_WP29_3.php3>.
- [4] Igor Hák. Moderní počítačové viry. Bakalářská práce [online]. 07.12.2003, [cit. 2005-28-05]. Dostupný z WWW: <<http://www.viry.cz/kniha/kniha.pdf>>.
- [5] Ing. Lukáš Grásgruber, Petr Nádeníček. Elektronický podpis v ohrožení?. *IT SYSTÉM Příloha 7-8/2001, str. 56 Bezpečnost* [online]. 2001, [cit. 2005-28-05]. Dostupný z WWW: <<http://www.systemonline.cz/site/bezpecnost/aec.htm>>.
- [6] Ing. Jindřich Kodl. ELEKTRONICKÝ PODPIS. *Data security management* [online]. 2001, [cit. 2005-28-05]. Dostupný z WWW: <http://www.fzu.cz/texty/ruzne/el_podpis.html>.
- [7] Dušan Kožušník. Elektronický podpis a čipové karty. *Živě* [online]. 27. 12. 2001, [cit. 2005-28-05]. Dostupný z WWW: <<http://www.zive.cz/h/Uzivatek/AR.asp?ARI=103429>>.
- [8] Martin Kot. Bezpečnost elektronické pošty. *Projekt do BIT* [online]. [cit. 2005-28-05]. Dostupný z WWW: <<http://www.cs.vsb.cz/kot/Reports/Bit/index.htm>>.
- [9] Věra Šumová. Elektronický podpis. [online]. 2001, [cit. 2005-28-05]. Dostupný z WWW: <http://www-troja.fjfi.cvut.cz/~sumova/El_podpis/>.
- [10] *REKONix : Firewally* [online]. [cit. 2005-28-05]. Dostupný z WWW: <<http://www.rekonix.cz/rekonix/cs/page.php?n=firewally.html>>.
- [11] *DIX – Digital Information Exchange : Zabezpečení sítě, dat a komunikace* [online]. [cit. 2005-28-05]. Dostupný z WWW:

http://www.dix.st/bezpecnost_detail.html#firewall>.

- [12] Pavel Tuček. Filtrování paketů. [online]. 2003, [cit. 2005-28-05]. Dostupný z WWW: <<http://home.zcu.cz/~tuca/projekty/pd/obsah.html>>.
- [13] David Šafránek. Firewall - paketový filtr. [online]. [cit. 2005-28-05]. Dostupný z WWW: <<http://www.fi.muni.cz/~xsafran1/linux/netfilter.html#cast1>>.
- [14] Petr Lasek – Actinet. Současnost a trendy řešení firewallů. [online]. 11. 10. 2004 [cit. 2005-28-05]. Dostupný z WWW: <http://www.actinet.cz/bezpecnost_informacnich_tehnologii/119/cl44/j1/Soucasnost_a_trendy_reseni_firewallu.html>.
- [15] Jakub Souček. Systémová opatření bezpečnosti v intranetových sítích. Diplomová práce [online]. 2001, [cit. 2005-28-05]. Dostupný z WWW: <<http://kuba.spika.cz/diplomka/index.htmf>>.
- [16] Jiří Peterka. Principy firewallů. [online]. [cit. 2005-28-05]. Dostupný z WWW: <<http://archiv.isdn.cz//b01/b0100020.php3>>.
- [17] Ing. Ludmila Kunderová, Ing. Ivo Liška. Datová komunikace a informační zdroje. [online]. [cit. 2005-28-05]. Dostupný z WWW: <<http://old.mendelu.cz/~lidak/site3/index1.htm>>.
- [18] Miroslav Novotný. Nebezpečí zvané internet. *Stapro 1/2004* [online]. [cit. 2005-28-05]. Dostupný z WWW: <http://www.stapro.cz/zpravodaj/nebezpeci_zvane_internet.htm>.
- [19] Petr Paukner. Bezpečnostní kritéria a ohodnocení IT produktů. Databázový svět [online]. 21. 12. 2004 [cit. 2005-28-05]. Dostupný z WWW: <<http://www.dbsvet.cz/view.php?cisloclanku=2004122101>>.
- [20] I.C.C.C. Group, a.s. : *Zálohování dat jako součást bezpečnosti informačních systémů* [online]. 2005 [cit. 2005-28-05]. Dostupný z WWW: <<http://www.iccc-group.com/cze/zaladat.php>>.

- [22] Hanáček, Petr; Staudek, Jan. *Bezpečnost informačních systémů : Metodická příručka zabezpečování produktů a systémů budovaných na bázi informačních technologií*. 1. vyd. Praha : Úřad pro státní informační systém, 2000. 127 s. ISBN 80-238-5400-3.
- [22] Příbyl J. *Ochrana dat v informatice*. skriptu ČVUT Praha 1997. ISBN 80-01-01664-1.
- [23] Staša, P., Rodyryčová, D. *Bezpečnost informací jako prosperita firmy*. Grada, 2000, 144 str. ISBN 80-7169-144-5.
- [24] Kovacich, G. *Průvodce bezpečnostního pracovníka informačních systémů*. UNIS, 2000, 200 str. ISBN 80-86097-42-0.
- [25] Dobda, Luboš. *Ochrana dat v informačních systémech*. Grada Publishing, 1998 - 286 s. ISBN 80-7169-479-7.
- [26] Jašek, Roman. *Ochrana znalostí a dat v podnikových informačních systémech*. Vyd. 1.. - Zlín : Univerzita Tomáše Bati, Fakulta managementu a ekonomiky, 2002, 115 str. ISBN 80-7318-095-2.

SEZNAM OBRÁZKŮ

Obr. 1. Příklad phishingu – část formuláře, který sbírá informace o kreditní kartě a dokonce o jejím PINu.....	34
Obr. 2. Princip symetrického šifrování.....	38
Obr. 3. Princip nesymetrického šifrování.....	41
Obr. 4. Princip digitálního podpisu.....	44
Obr. 5. Šifrování pomocí PGP.....	46
Obr. 6. Struktura firewallu.....	57
Obr. 7. Faktory ovlivňující ztrátu dat.	64
Obr. 8. Příklad přírůstkového zálohování dat.	66
Obr. 9. Příklad diferenčního zálohování dat.	67
Obr. 10. Vzájemné vztahy v informačním bezpečnostním systému.....	70
Obr. 11. Základní fáze řešení bezpečnosti IS.	72

SEZNAM TABULEK

Tab. 1. Riziková analýza hodnot IS.....	75
---	----