Bankovní institut vysoká škola Praha
Katedra informačních technologií a elektronického obchodování

Implementace bezpečné počítačové sítě v podmínkách vnitropodnikové komunikace

Bakalářská práce

Autor: Radek Šnejdar

Informační technologie, Manažer projektů informačních systémů

Vedoucí práce: Ing. Antonín Vogeltanz

Teplice Duben, 2007

Prohlášení:

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně a s použitím uvedené literatury.

V Teplicích dne 15. 4. 2007 ***Radek Šnejdar***

Anotace práce:

Práce pojednává o problematice bezpečnosti počítačových sítí v podmínkách vnitropodnikové komunikace. V první části je popis základů počítačových sítí, standardů pro datovou komunikaci a přehled norem, které se týkají bezpečnosti počítačových sítí. Dále následuje přehled obecných zásad v rámci bezpečnosti počítačových sítí. Detailněji jsou popsány zásady bezpečnosti z hlediska šifrování dat, přihlašování uživatelů k síti a přehled technických prostředků pro zvýšení bezpečnosti podnikových sítí.

V poslední kapitole jsou uvedeny příklady možných hrozeb a příklady protiopatření. Na závěr jsou stručně popsány nástroje pro detekci a prevenci průniku do podnikové sítě, popis nástrojů pro odhalení nezabezpečených míst a příklad zařízení pro zvýšení bezpečnosti počítačových sítí v organizaci.

Obsah:

Úvod

Cílem této práce je seznámit širokou veřejnost s problematikou bezpečnosti počítačových sítí. Každá počítačová síť, a také domácí počítač, je vystavena různým nebezpečím ze strany uživatele, poruchy zařízení a z Internetu. Internet je mocný komunikační prostředek pro získání spousty užitečných informací, ale také skrývá mnoho nebezpečí. Pomocí Internetu dnes komunikujeme s lidmi na druhém konci světa, najdeme si odjezd vlaků, přečteme noviny a získáme množství informací týkajících se prakticky čehokoliv, a to všechno z tepla domova nebo kanceláře. Být nepřipojen k Internetu si řada lidí nedovede představit a také pro některé organizace je Internet klíčová oblast podnikání a bez bezpečného připojení nejsou schopni své aktivity provozovat. Problematika bezpečnosti počítačových sítí se netýká jen Internetu, ale neméně důležitý je provoz sítě uvnitř organizace. S rozmachem informačních technologií jsou organizace odkázány právě na správné fungování podnikové sítě. Počítače dnes řídí výrobní linky, zpracovávají účetnictví a vyvíjejí nové produkty. Případný výpadek počítačové sítě může znamenat značné finanční ztráty, ale také může ohrozit zdraví a život lidí. Organizace mají také ve své síti důvěrná data a jejich zcizení může ohrozit jejich fungování. Dnes je již běžný pojem „počítačová kriminalita“ a téměř každý slyšel o nějaké události, kdy byla ukradena důležitá data z firmy, pokus o nabourání do sítě FBI nebo o bankovním podvodu v řádech milionů korun. Proto si myslím, že téma bezpečnost počítačových sítí je velmi aktuální a důležité, a věřím, že tato práce bude přínosem pro čtenáře, který se s pojmem „ Bezpečnost počítačových sítí“ ještě nesetkal.

1. Druhy a topologie sítí, síťové standardy a protokoly, normy a normy ČSN

1.1. Klasifikace sítí

Počítačové sít lze klasifikovat podle různých kritérií.

Podle rozlohy

- Lokální sítě (LAN)
- Rozlehlé sítě (WAN)
- Metropolitní sítě (MAN)
- Personální (domácí) sítě (PAN (HAN))
- Úložné sítě (SAN)

Podle topologie

- Dvoubodové sítě
- Sběrnicové sítě
- Hvězdicové sítě
- Kruhové sítě
- Stromové sítě
- Sítě Mesh

Podle technologie

- Ethernet
- Token Bus
- Token Ring
- IsoEthernet
- 100VG-AnyLAN
- ETSI:HIPERLAN
- ANSI:FDDI
- ANSI:FibreChanel

Podle vlastnictví

- Veřejné
- Privátní

1.2. Rozdělení sítí podle rozlohy

1.2.1. LAN – Local Area Network

Lokální sítě jsou komunikační sítě propojující koncové zařízení (osobní počítače, pracovní stanice, servery, terminály, tiskárny, skenery) a umožňují jejich vzájemnou spolupráci a sdílení síťových prostředků. Tyto sítě jsou omezeny svým rozsahem maximálně do několika kilometrů, nejčastěji působí v rámci jednoho patra, jedné budovy nebo skupiny budov. Propojení je realizováno různými druhy spojení a přenosové rychlosti jsou v řádech Mbitů a Gbitů.

Technologie spojení

Mezi zastaralý a málo používaný typy spojení je např. koaxiální kabel (Rychlost max. 10Mbit).

V současné době je nejvíce používaná technologie spojení strukturovanou kabeláží, optickými vlákny, bezdrátový přenos.

Přiklad rychlostí spojení strukturované kabeláže a optického vlákna (Fibre Channel)

- Ethernet – 10Mbit
- Fast Ethernet – 100MBit
- Gigabit Ethernet – 1GBit

10GB Ethernet – 10GBit

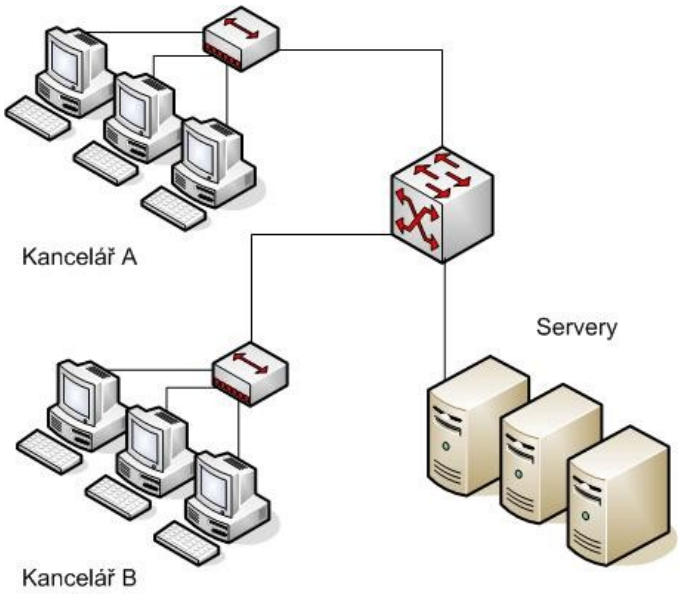
Další typy LAN

- WLAN (Bezdrátová lokální síť)

WLAN představuje velmi rychlé a jednoduché rozšíření klasické sítě LAN bez nutnosti zásahu do stávající kabeláže. Stačí připojit přístupový bod a mohou se okamžitě stanice a notebooky, vybavené bezdrátovou síťovou kartou, téměř okamžitě připojit do lokální sítě. Rychlosti tohoto připojení je dnes až 108Mbit a to na vzdálenost až 300m.

- VLAN (Virtuální lokální síť)

VLAN umožňuje vytvoření logických skupin uživatelů v lokální síti (např. podle oddělení), které jsou nezávislé na fyzickém umístění v síti.

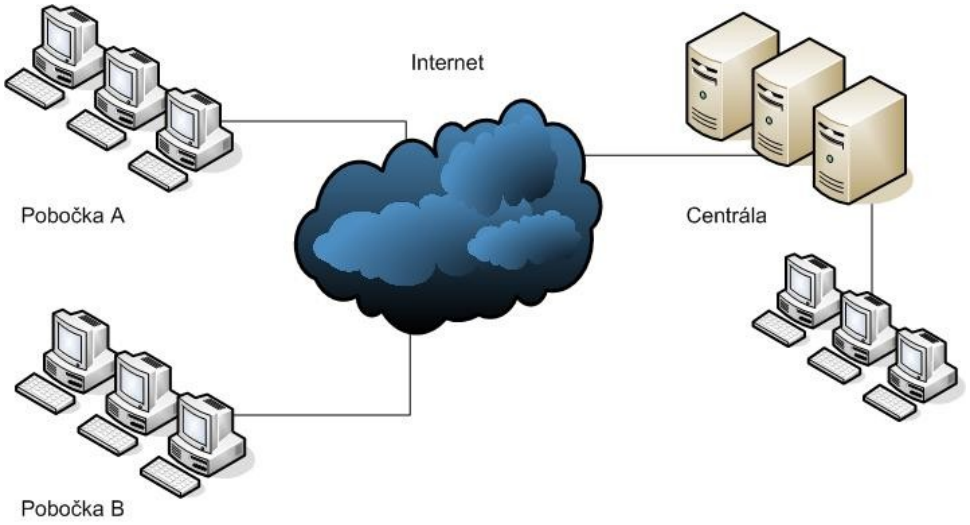


1 Příklad sítě LAN

1.2.2. WAN – Wide Area Network

Sítě WAN umožňují komunikaci mezi koncovými uzly a stanicemi zpravidla na velkou vzdálenost. Jedná se o síť, která propojuje rozsáhlé oblasti, státy, kontinenty. Propojuje jednotlivé sítě LAN, ale i jednotlivce. Přenosové rychlosti jsou Mbps až Gbps. V tomto případě se jedná převážně o sítě, které propojují velké servery, osobní počítače a další zařízení připojované prostřednictvím veřejné sítě.

Pro bezpečné propojení LAN sítí přes WAN se zpravidla používají jednoúčelová technická zařízení.[1]



2 Přiklad sítě WAN

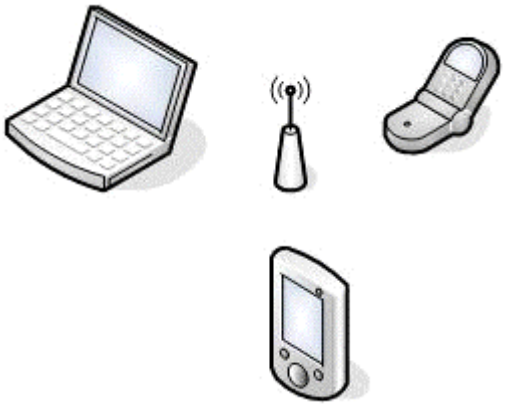
[1] Směrovač, firewall – viz. kapitola 2.

1.2.3. MAN – Metropolitan Area Network

Sítě MAN se nachází na hranici mezi sítěmi lokálními (LAN) a rozlehlými (WAN). Typicky pokrývají tyto sítě nějaké město. V těchto sítích se dosahuje v současnosti vzdáleností řádově stovek metrů až desítky kilometrů. Přenosové rychlosti se pohybují řádově v Mbps a Gbps.

1.2.4. PAN – Personal Area Network

V současné době se objevuje i toto označení sítě, která nezapadá do žádného členění podle dosahu. Dosah této sítě bývá velmi malý, maximálně několik málo metrů a slouží potřebám jednotlivce, případně velmi malé skupiny uživatelů. Nejčastěji propojuje mobilní zařízení (například různá PDA, notebooky, mobilní telefony), a umožňuje jim vzájemně komunikovat. Mezi technologie, které takovéto propojení zajišťují, patří zejména Bluetooth, Wi-Fi, IrDa, a z drátových pak USB.



3 Příklad sítě PAN

1.2.5. SAN – Storage Area Network

SAN je vysokorychlostní síť obvykle s malým dosahem a obvykle propojuje různé typy úložných zařízení (diskové pole, knihovny) a servery. SAN je propojena s podnikovou architekturou a podporuje zálohování dat, rychlý přístup k datům a zrcadlení disků a serverů. Propojení je realizováno optickým vláknem (Fibre Channel), iSCSI, mezi starší typy spojení patří např. ESCON.

1.3. Rozdělení sítí podle topologie

Topologie (prostorové uspořádání) sítě charakterizuje způsob, jakým jsou mezi sebou propojeny jednotlivé počítače.

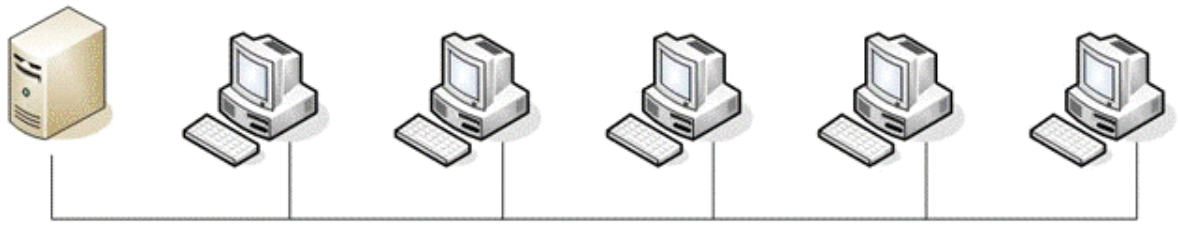
1.3.1. Dvoubodové sítě

Jde o přímou komunikaci mezi síťovými uzly (bez potřeby dalších zařízení). Toto spojení je základem všech sítí. Pro propojení lze využít libovolné přenosné médium (kabel, bezdrátový přenos). Všechno zařízení jsou si rovnocenné. Největší výhoda je v jednoduchosti. Nevýhodou je, že nelze přidat další zařízení.

4 Příklad dvoubodové sítě

1.3.2. Sběrnicová topologie

Topologie sběrnice nemá centrální uzel a všechny uzly jsou připojeny ke sdílenému přenosovému prostředku, který umožňuje komunikaci každý s každým. Vyžaduje složitější řízení přístupu ke sdílenému prostředku a komplikovanější protokoly pro řízení přenosu dat po sběrnici. Informační signál nesoucí zprávu se šíří sběrnicí všemi směry a všechny stanice mají přístup ke všem zprávám na sběrnici; skutečně přijmou však jen takovou, která je jim podle cílové adresy skutečně určena.
Ke sběrnici lze snadno přidávat nebo odebírat uzly, aniž se tím poruší informační tok.[2]



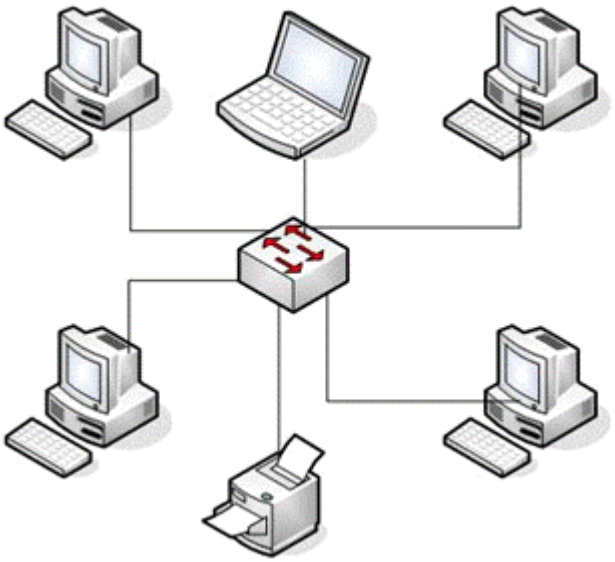
5 Sběrnicová topologie

1.3.3. Hvězdicová topologie

Topologie hvězdy je analogií starých terminálových sítí s centrálním řízením. Centrální uzel sítě řídí směrování v síti, zatímco ostatní uzly se o směrování dat nestarají, a mohou

[2] Pužmanová, Rita: Moderní komunikační sítě od A do Z; str. 37

proto být velmi jednoduché. Je vhodná v případech, kdy převažuje komunikace vedená mezi okrajovým a centrálním uzlem. Pokud vyžaduje aplikace komunikaci mezi okrajovými uzly, kladou se na centrální uzel vysoké požadavky (na výkon a spolehlivost). Tyto sítě jsou pak méně spolehlivé ve srovnání s ostatními používanými topologiemi. Přenos dat v těchto sítích lze řídit jednoduchými protokoly a lze jej snadno monitorovat.[3]



6 Hvězdicová topologie

1.3.4. Mnohahvězdicové topologie

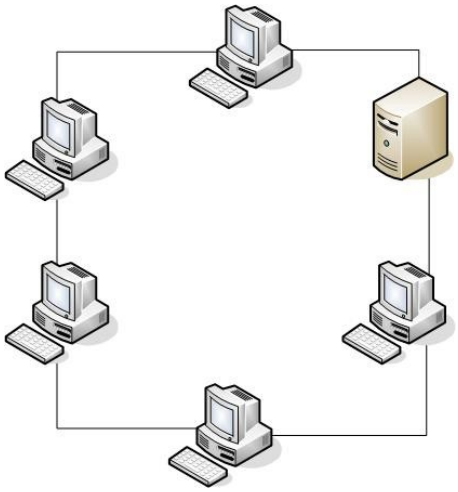
V mnohahvězdicové topologii jsou počítače spojené do jednotlivých hvězdic a ty jsou dále mezi sebou propojeny. Základem těchto sítí jsou zařízení (rozbočovač, přepínač), které jsou propojeny mezi sebou a na každé zařízení je připojeno několik počítačů. Výhodou tohoto systému je zvýšená odolnost proti případné poruše jednoho zařízení. V případě takové poruchy přestane fungovat jen jedna hvězda a další počítače na ostatních hvězdách mohou dále pracovat.

1.3.5. Kruhová topologie

Topologie kruh rovněž nemá centrální uzel. Spojuje každé zařízení pouze s předchozím a následujícím zařízením v síti, s ostatními uzly v síti probíhá komunikace nepřímo, přes jeden nebo více dalších uzlů. Zprávy obíhající uzavřenou cestou jedním směrem mezi uzly, proto není třeba řešit žádné směrování toku. Každý uzel převezme zprávu od svého předchůdce, a pokud není sám adresátem zprávy, předá ji svému následovníkovi.

[3] Pužmanová, Rita: Moderní komunikační sítě od A do Z; str. 37

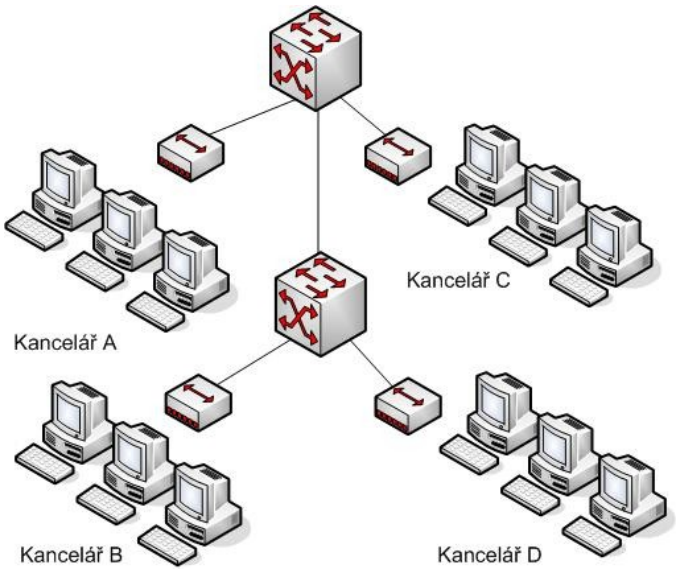
Výhodou kruhové topologie je jednoduchý způsob předávání datových zpráv bez existence kolizí mezi stanicemi, nevýhodou je, že v případě výpadku stanice dojde k přerušení činnosti sítě.[4]



7 Kruhová topologie

1.3.6. Stromová topologie

Stromová topologie je složena z několika sítí typu hvězda propojené jedním spojem. Tento druh sítě je více odolný proti poruchám jednotlivých zařízení. V případě poruchy jednotlivého zařízení je mimo provoz pouze jedna větev stromu, další zůstávají funkční. U těchto typů sítí lze jednoduše síť rozšiřovat a přidávat další uživatele. Pro větší spolehlivost lze volit topologie sítě se smyčkami.



8 Stromová topologie

[4] Pužmanová, Rita: Moderní komunikační sítě od A do Z; str. 38

1.3.7. Topologie sítě se smyčkami

Topologie sítě se smyčkami (Mesh) nabízí více možných spojů mezi uzly.

- Full Mesh (plně propojená síť)

Jedná se o plně propojenou síť, kdy všechny uzly jsou propojeny každý s každým.

- Partial Mesh (částečně propojená síť)

V síti se používá méně spojů. Uzly, které nejsou přímo propojeny s ostatními uzly, komunikují přes spojené uzly v síti.

Výhodou topologie Mesh je vysoká spolehlivost, kdy v případě výpadku některého ze spojů jej zastoupí další spoj. Nevýhodou je vysoká cena při budování tohoto typu sítě.

1.4. Síťové standardy a protokoly

Protokol je sada předdefinovaných pravidel, která určují, jak budou dva nebo více procesů vzájemně komunikovat a vyměňovat data. Procesy mohou běžet na stejném počítači nebo různých počítačích. Program transportní vrstvy na jednom počítači například používá protokol, který mu umožňuje „dohovořit se“ se svým protějškem na jiném počítači. Protokoly jsou většinou svázány s určitými službami nebo úkoly, jako je zpracování dat a směrování paketů. Protokol specifikuje pravidla pro vytváření, provádění a ukončení komunikační relace. Určuje také formát informací, které pakety musí mít, aby mohly být šířeny sítí.[5]

1.4.1. Standard IEEE 802.x

IEEE je americká organizace, která definuje standardy týkající se sítí a jiných oblastí. Jsou zde série standardů, doporučení a informačních dokumentů, které se týkají sítí a komunikací. Organizace výboru IEEE dokončila základní sadu norem pro různé typy přenosových prostředků v roce 1985. O dva roky později byly tyto normy přijaty ISO pod číslem 8802.

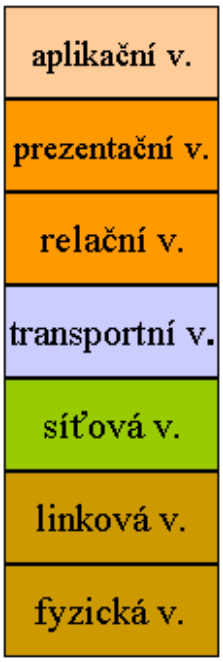
Seznam norem je dostupný na stránkách www.ieee802.org

1.4.2. Model ISO/OSI

Standard OSI představuje model se sedmi vrstvami, který zajišťuje účinnou komunikaci v rámci sítí. OSI model je referenční model ISO/OSI vypracovaný organizací ISO jako

[5] Werner Feibel: Encyklopedie počítačových síti; str.795

hlavní část snahy o standardizaci počítačových sítí nazvané OSI. V roce 1984 byl přijatý standard OSI jako mezinárodní norma pod označením ISO 7498. Komplexní text normy přijala také CCITT jako doporučení X.200.



9 Model ISO/OSI

Zdroj: http://www.earchiv.cz/l215/slide.php3?&l=2&me=4

Popis jednotlivých vrstev referenčního modelu OSI/ISO:

- Fyzická vrstva (vrstva 1)

Jedinou vrstvou, která podporuje fyzickou komunikaci dat mezi systémy, je nejnižší vrstva fyzická. Jejím účelem je aktivace, udržování v aktivním stavu a dezaktivace fyzických spojení určených pro přenos bitů nebo značek. Fyzické spojení může být vytvořené ve formě propojení datových okruhů s využitím zprostředkovacích funkcí ve fyzické vrstvě. Datový okruh představuje komunikační cestu ve fyzických médiích mezi dvěma fyzickými entitami a prostředky potřebné pro uskutečnění přenosů bitů přes tuto komunikační cestu. Fyzické spojení může dovolit přenos bitových posloupností v plném, nebo polovičním duplexu a může být dvoubodové nebo mnohabodové.

- Spojová (linková) vrstva (vrstva 2)

Spojová vrstva musí umožnit zahajování, udržování a závěr vytvořených spojení, rozvětvení spojení, formátování rámců, identifikace koncových bodů spojení, seřazování přenášených rámců, oznamování neopravitelných chyb síťové vrstvě, detekci a opravu chyb, řízení toku, identifikaci a výměnu parametrů a dodržování hodnot výkonnosti

spojových služeb. Spojová vrstva umožňuje síťové vrstvě řídit propojení datových okruhů ve fyzické vrstvě.

- Síťová vrstva (vrstva 3)

Účelem síťové vrstvy je poskytnout síťové spojení otevřeným systémům, které spolu chtějí komunikovat a přitom spolu nemusí přímo sousedit. Na základě síťové (logické) adresace je síťová vrstva zodpovědná za vlastní komunikaci v komplexní síti, směrování (výběr vhodné cesty sítí) a přenos datových jednotek označovaných jako pakety (datagramy) od zdroje k cíli. Poskytuje tak transportní vrstvě nezávislost na směrování, vytváření a využívání příslušných síťových spojení. Zprostředkovací funkce a protokoly zahrnující rozšířenou službu pro přenos po úsecích, které se využívají v rámci síťové služby uplatněné mezi koncovými otevřenými systémy, se realizují pod transportní vrstvou (v síťové vrstvě nebo pod ní).

- Transportní vrstva (vrstva 4)

Transportní vrstva poskytuje transparentní, spolehlivý a cenově dostupný přenos s požadovanou kvalitou a optimalizuje nejrůznější síťové služby.

- Relační vrstva (vrstva 5)

Smyslem relační vrstvy je organizovat a synchronizovat dialog mezi spolupracujícími prezentačními entitami a řídit výměnu dat mezi nimi. Prezentační entita může být současně připojena k více relačním spojením. Relační vrstva poskytuje služby vytváření a závěr relačního spojení, normální a spěšný přenos zpráv, pozdržený přenos zpráv (část zpráv přenesená relačním spojením se uvolňuje právo adresáta až na pokyn odesílatele), řízení interakce (jednosměrné, obousměrné střídavé).

- Prezentační vrstva (vrstva 6)

Prezentační vrstva zajišťuje transparentní přenos zpráv mezi koncovými uživateli a zabývá se jen strukturou zpráv a nikoliv jejich významem (sémantikou), který je znám pouze aplikační vrstvě.

- Aplikační vrstva (vrstva 7)

Účelem aplikační vrstvy je poskytnout aplikačním procesům přístup ke komunikačnímu systému a tím umožnit jejich vzájemnou spolupráci.

1.4.3. MAC adresa

MAC (Media Access Control) adresa je celosvětově jednoznačný identifikátor většiny síťového zařízení, který používá mnoho síťových protokolů druhé vrstvy, nejznámější je ethernet.

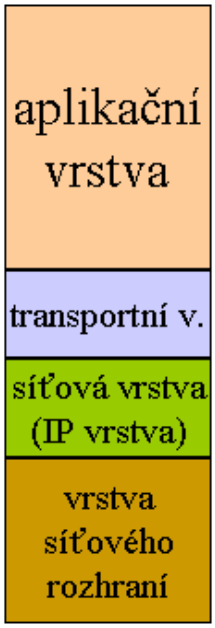
Ethernetová MAC adresa má 48 bitů a nejčastěji se zapisuje jako šestice dvou hexadecimálních čísel, tedy ve tvaru xx:xx:xx:xx:xx:xx. První tři dvojice určují výrobce zařízení. MAC adresa je uložena v ROM zařízení, někdy se označuje jako BIA (burned in address).[6]

1.4.4. Sady síťových protokolů

TCP/IP

TCP/IP je sada síťových protokolů určených pro komunikaci v počítačových sítí. Tato sada protokolů je nejvíce používána na různých platformách (Windows, UNIX, Linux).

Architektura TCP/IP je rozdělena pouze do 4 vrstev narozdíl od modelu OSI.



10 Architektura TCP/IP

Zdroj: http://www.earchiv.cz/l215/slide.php3?&l=2&me=4

Adresace v IP sítích

Adresace v počítačových sítích, nezávisle na typu protokolu, musí zajistit unikátnost adresy uzlu v rámci celé sítě. Tento problém je řešen logickým rozdělením adres na část adresy sítě a adresy uzlu (jde o jakousi analogii telefonních čísel, kde je koncový uzel jednoznačně určen dvojicí číslo předvolby a číslo koncové stanice). V IP prostředí je

[6] http://www.abclinuxu.cz/slovnik/mac-adresa;jsessionid=1wiaqolgdmiti

konkrétní vyjádření adresy ve formátu 4 jednobytových čísel oddělených tečkami. Vypadá tedy následovně – x.x.x.x (např. 192.168.1.3).[7]

Paket (Packet)

Paket je pevně definovaný blok bytů, skládající se z hlavičky, dat a koncové části. Ve vrstvených síťových architekturách je paket vytvořen na jedné úrovni (zpravidla na linkové vrstvě) a na dalších, nižších úrovních může být opatřen jinou obálkou, skládající se z hlavičky a koncové části.

Rámec (Frame)

Definice rámce je obdobná jako u paketu s tím rozdílem, že rámec je vytvořen na spojové (linkové) vrstvě a obsahuje data a řídící informace.

Příklady protokolů:

IP: základní protokol síťové vrstvy

IPv4: internet protokol (32bitové adresy)

IPv6: internet protokol (128bitové adresy)

TCP: transportní služba pro spolehlivý přenos dat

ARP: tento protokol se používá k nalezení fyzické adresy MAC podle známé IP adresy

HTTP: přenos hypertextových dokumentů (WWW)

HTTPS: nadstavba protokolu HTTP, která poskytuje zvýšenou bezpečnost

FTP: přenos souborů po síti

SMTP: zasílání elektronické pošty

POP3: získání elektronické pošty z poštovního serveru

DHCP: dynamické přidělování adres

DNS: systém doménových jmen

SNMP: protokol pro management sítí

Telnet: protokol pro přihlášení ze vzdáleného počítače do lokální sítě

AppleTalk

AppleTalk je sada protokolů firmy Apple pro síťovou komunikaci počítačů Macintosh. Používá vícevrstvou architekturu typu Peer-to-Peer, která používá služby vestavěné do operačního systému.

Příklady protokolů:

ARAP: protokol spojové vrstvy

ASP: protokol transportní vstvy

---

[7] http://www.svetsiti.cz/view.asp?rubrika=Tutorialy&temaID=1&clanekID=5

AURP: směrovací protokol

Novell NetWare

Sada protokolů firmy Novell.

Příklady protokolů:

NCP: protokol tří horních vrstev (aplikační, prezentační a relační)

IPX: protokol síťové vrstvy

SPX: protokol transportní vrstvy

IBM protokoly

Sada protokolů firmy IBM

NetBIOS: protokol tří horních vrstev (aplikační, prezentační a relační)

NetBEUI: protokol původně určený pro sítě IBM Token Ring

SMB: síťový komunikační protokol aplikační vrstvy

Další známé sady protokolů jsou: DECnet Phase IV, XNS Xerox Network Systém, Banyan VINES

Specifikace protokolů je k dispozici na stránkách: http://www.rfc-editor.org/rfc.html

1.5. Zákonné normy a normy ČSN

Provozování informačního systému v každé organizaci musí být v souladu s právními předpisy a normami.

1.5.1. Přehled zákonů

- Zákon 101/2000 Sb.

Na ochranu osobních údajů

- Zákon 121 / 2000 Sb.

Autorský zákon

- Zákon 227 / 2000 Sb.

O elektronickém podpisu

- Zákon 412 / 2005 Sb.

O ochraně utajovaných skutečností

- Zákon 480/2004 Sb.

Zákon o některých službách informační společnosti

1.5.2. Normy ČSN

Uvedené normy nelze brát jako přesný návod na budování bezpečnosti podnikové sítě, ale jsou pouze návodem, jak by se správně zabezpečená podniková síť měla plánovat a implementovat.

Rozsah a struktura řízení informační bezpečnosti jsou závislé na řadě objektivních skutečností (velikost organizace, geografické umístění, rozsah a význam provozovaných informačních a komunikačních systémů, použité informační a komunikační technologie apod.). Toto je hlavní důvod, proč se aplikuje nejlepší praxe (normy, standardy a doporučení) pro zavedení informační bezpečnosti a nedá se použít univerzální šablonu. Obecně je třeba při budování informační bezpečnosti vycházet z analýzy výchozího stavu a z analýzy rizik.[8]

Norma ČSN ISO/IEC 17799:2006 obsahuje celkem 11 základních oddílů bezpečnosti, které jsou dále rozděleny do 39 kategorií bezpečnosti.

1. **Bezpečnostní politika**

- Politika bezpečnosti informací

2. **Organizace bezpečnosti informací**

- Interní organizace
- Externí subjekty

3. **Klasifikace a řízení aktiv**

- Odpovědnost za aktiva
- Klasifikace informací

4. **Bezpečnost lidských zdrojů**

- Před vznikem pracovního vztahu
- Během pracovního vztahu
- Ukončení pracovního vztahu

5. **Fyzická bezpečnost a bezpečnost prostředí**

- Zabezpečené oblasti
- Bezpečnost zařízení

6. **Řízení komunikací a řízení provozu**

- Provozní postupy a odpovědnosti
- Řízení dodávek služeb třetích stran

[8] Hanáček, Petr; Staudek, Jan, Bezpečnost informačních systémů – příloha č.2, standardy a doporučemí; str. 6

- Plánování a přejímání informačních systémů
- Ochrana proti škodlivým programům a mobilním kódům
- Zálohování
- Správa bezpečnosti sítě
- Bezpečnost při zacházení s médii
- Výměna informací
- Služby elektronického obchodu
- Monitorování

7. Řízení přístupu

- Požadavky na řízení přístupu
- Řízení přístupu uživatelů
- Odpovědnost uživatelů
- Řízení přístupu k síti
- Řízení přístupu k operačnímu systému
- Řízení přístupu k aplikacím a informacím
- Mobilní výpočetní zařízení a práce na dálku

8. Vývoj, údržba a rozšíření informačního systému

- Bezpečnostní požadavky informačních systémů
- Správné zpracování v aplikacích
- Kryptografická opatření
- Bezpečnost systémových souborů
- Bezpečnost procesů vývoje a podpory
- Řízení technických zranitelností

9. Zvládání bezpečnostní incidentů

- Hlášení bezpečnostních událostí a slabin
- Zvládání bezpečnostních incidentů a kroky k nápravě

10. Řízení kontinuity činnosti organizace

- Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací

11. Soulad s požadavky

- Soulad s právními normami
- Soulad s bezpečnostními politikami, normami a technická shoda
- Hlediska auditu informačních systémů

Přehled dalších norem vztahujících se k informační bezpečnosti a propojení otevřených systémů:

ČSN ISO/IEC TR 13335-1:

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

ČSN ISO/IEC TR 13335-2:

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

ČSN ISO/IEC TR 13335-3:

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

ČSN ISO/IEC TR 13335-4:

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

ČSN ISO/IEC 15408-1:

Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT - Část 1: Úvod a všeobecný model

ČSN ISO/IEC 15408-2:

Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT - Část 2: Bezpečnostní funkční požadavky

ČSN ISO/IEC 15408-3:

Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT - Část 3: Požadavky na záruky bezpečnosti

ČSN ISO/IEC 10181 1-7:

Informační technologie - Propojení otevřených systémů - Bezpečnostní struktury otevřených systémů:

1: Přehled, Část 2: Struktura autentizace, Část 3: Struktura řízení přístupu, Část 4: Struktura nepopiratelnosti, Část 5: Struktura důvěrnosti, Část 6: Struktura integrity a Část 7: Struktura bezpečnostního auditu a alarmů

Anotace norem je dostupná na stánkách www.cni.cz

2. Bezpečný provoz sítě LAN

Vzhledem ke standardizaci informačních technologií a nárůstu objemu přenášených dat, je problematika bezpečnosti počítačových sítí velmi aktuální téma. S rozmachem informačních technologií jsou organizace odkázány právě na správné fungování podnikové sítě. Počítače dnes řídí výrobní linky, zpracovávají účetnictví a vyvíjejí nové produkty. Organizace proto musí investovat do zajištění bezpečnosti informací velké úsilí a nemalé finanční prostředky.

2.1. Obecné zásady

2.1.1. Bezpečnostní politika

Analýza rizik[9]

Nejdůležitější etapou stanovení bezpečnostní politiky je analýza rizik. Analýza rizik předchází

vlastnímu stanovení bezpečnostní politiky. Jejím cílem je:

• identifikování, zvládnutí, odstranění nebo minimalizace událostí, které mají nežádoucí vliv na aktiva organizace

• zjištění hrozeb a rizik, kterým je IS vystaven

• určení, jaké škody mohou útokem vzniknout

• určení, která opatření rizika hrozeb odstraní nebo alespoň minimalizují, a co jednotlivá opatření stojí.

Typy bezpečnostních politik[10]

Variant přístupů k zabezpečení IT je více, některé jsou zajímavější nákladově, jiné dosaženou

transparentností, další pak odolností proti útoku výjimečné síly. Doporučená varianta bezpečnostní politiky IS by měla vždy vzejít z oponované a závazně přijaté bezpečnostní politiky organizace a bezpečnostní politiky IT organizace (při respektování výsledků analýzy rizik IS). Podle požadované úrovně zabezpečení rozpoznáváme bezpečnostní politiky čtyř obecných typů:

Promiskuitní bezpečnostní politika

---

[9] Hanáček, Petr; Staudek, Jan, Bezpečnost informačních systémů; str. 31

[10] Hanáček, Petr; Staudek, Jan, Bezpečnost informačních systémů; str. 23

je bezpečnostní politika nikoho neomezující, která každému v zásadě povoluje dělat vše, tedy i to, co by dělat neměl. IS s promiskuitní bezpečnostní politikou jsou obvykle provozně nenákladné, mnohdy ani nenutí povinně používat pro autentizaci alespoň hesla, a zaručují pouze minimální nebo vůbec žádnou bezpečnost. Důvodem používání IS s promiskuitní bezpečnostní politikou může být ekonomičnost řešení, potřebná úroveň bezpečnost může být zajišťována prostředky mimo IT.

Liberální bezpečnostní politika

je bezpečnostní politika, která každému povoluje dělat vše, až na věci explicitně zakázané. Liberální bezpečnostní politika zaručuje větší bezpečí než promiskuitní politika. Liberální bezpečnostní politika je často uplatňována v prostředích, ve kterých se hrozby považují za málo až průměrně závažné a nepominutelným požadavkem je nízká ekonomická náročnost řešení bezpečnosti. Typicky se opírá o zásadu volitelného řízení přístupu založeného na identitě subjektů.

Opatrná bezpečnostní politika, resp. racionální bezpečnostní politika

je bezpečnostní 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 podle jejich schopností a citlivosti. Je opřena mj. o zásadu povinného řízení přístupu založeného na rolích, ve kterých vystupují subjekty při styku s IS. Z hlediska používání IS v Internetu je obvykle počáteční bezpečnostní politikou při zavádění firewallů.

Paranoidní bezpečnostní politika

je bezpečnostní politika zakazující dělat vše potenciálně nebezpečné, tedy i to, co by nemuselo být explicitně zakazováno. Zaručuje nejvyšší stupeň bezpečnosti. Např. zakáže používat jakékoliv internetovské služby (co kdyby se daly zneužít), resp. předepíše používat IS bez možnosti on-line napojení na komunikace. Vede pak 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 režií, tudíž s dosažitelnou vyšší výkonností při zachování nižší úrovně nákladů.

2.1.2. 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:[11]

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.

Softwarové 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

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.

2.1.3. Fyzická bezpečnost a bezpečnost prostředí

Zajištění fyzické bezpečnosti technickými prostředky:

- Mechanické prvky (ploty, zábrany)

[11] Hanáček, Petr; Staudek, Jan, Bezpečnost informačních systémů; str. 21

- Elektrická zabezpečovací zařízení
- Elektrická protipožární signalizace
- Samočinné hasící systémy
- Systém kontroly vstupu
- Kamerové systémy
- Detekce zakázaných látek

2.1.4. Zajištění integrity a dostupnosti

Integrita dat je zajištění jejich neporušitelnosti a autenticity, to znamená, že data nebyla pozměněna (úmyslně nebo neúmyslně) během jejich uložení respektive přenosu.

Příklad možných vlivů na porušení integrity

- Technické poruchy
- Chyba údržby
- Škodlivý programový kód
- Chyba software
- Poruchy napájení
- Předstírání identity uživatele
- Chyby přenosu
- Chyba uživatele
- Použití neautorizovaných programů

Příklad ochran zajišťující integritu

- Autentikace uživatele.
- Šifrování dat
- Zařízení odolné proti poruchám
- Záložní zdroje napájení

Dostupnost dat je zajištění poskytování, autorizovaným uživatelům, požadovaných síťových služeb.

Příklad možných vlivů na porušení dostupnosti

- Technické poruchy
- Destruktivní útok
- Škodlivý programový kód
- Chyba software
- Poruchy napájení

- Přírodní katastrofy
- Zneužití zdrojů
- Přetížení provozu
- Krádež

Příklad ochran zajišťující dostupnost

- Zařízení odolné proti technickým poruchám
- Záložní zdroje napájení
- Protipožární a zabezpečovací systémy
- Prevence proti útokům

2.2. Šifrovací algoritmy (kryptografie)

Mezi základní metody zajištění provozu bezpečné počítačové sítě patří šifrování dat.

Kryptografie neboli šifrování je nauka o metodách utajování smyslu zpráv převodem do podoby, která je čitelná jen se speciální znalostí. Slovo kryptografie pochází z řečtiny – kryptós je skrytý a gráphein znamená psát. Někdy je pojem obecněji používán pro vědu o čemkoli spojeném se šiframi jako alternativa k pojmu kryptologie. Kryptologie zahrnuje kryptografii a kryptoanalýzu, neboli luštění zašifrovaných zpráv.[12]

2.2.1. Symetrické šifrování (soukromým klíčem)

Šifrování soukromým klíčem používá jediný klíč pro šifrování i dešifrování. Klíče jsou obvykle krátké, aby algoritmický výpočet prováděný pomocí nich byl dostatečně rychlý a jednoduchý. Klíč pro šifrování a dešifrování musí být tajný a musí být znám pouze určeným uživatelům. Problém je distribuce klíče všem, kteří jej potřebují, neboť je třeba zajistit bezpečnost samotného klíče při jeho přenosu sítí. Z tohoto důvodu se soukromý klíč často mění. Soukromý klíč může být bezpečně uložen na počítači nebo na čipové kartě.

Příklady:

- DES (Data Encryption Standard) je symetrická šifra vyvinutá v 70. letech. V současnosti je tato šifra považována za nespolehlivou, protože používá klíč pouze o délce 56 bitů. Možným způsobem jak zvýšit bezpečnost této šifry, je vícenásobná aplikace. Proto vznikl algoritmus 3DES, který je trojnásobnou aplikací šifry DES. Nejčastěji používaná varianta 3TDES pracuje s klíčem o celkové délce 168 bitů.

[12] http://cs.wikipedia.org/wiki/Kryptografie

- AES (Advanced Encryption Standard) je symetrická bloková šifra, která vznikla jako nástupce DES. Šifra využívá symetrického klíče pro šifrování i dešifrování. Velikost klíče může být 128, 192 nebo 256 bitů. Šifra se vyznačuje vysokou rychlostí šifrování.
- Blowfish je šifra vyvinutá v roce 1993 B. Schneierem. Tato šifra je zcela volná – nepatentovaná, nelicencovaná. Jde o blokovou šifru s délkou bloku 64 bitů a klíči dlouhými maximálně 448 bitů.

Další symetrické šifry jsou např. CAST, IDEA, RC2, RC5, SKIPJACK.

2.2.2. Asymetrické šifrování (veřejným klíčem)

Šifrování veřejným klíčem vyžaduje použití dvou klíčů – veřejný a tajný. Veřejný klíč je veřejně dostupný a tímto klíčem lze pouze zaslat zašifrovanou zprávu uživateli. K dešifrování zprávy použije uživatel jen sobě známý, tajný klíč. Tajný klíč může být uložen na čipové nebo magnetické kartě. Jedním z hlavních algoritmů asymetrického šifrování je RSA.

- RSA (iniciály autorů Rivest, Shamir, Aleman) je šifra s veřejným klíčem, která byla vyvinuta v roce 1977. Algoritmus RSA je založen na předpokladu, že rozložit číslo na součin prvočísel je velmi obtížné. Z čísla n je praktické nemožné najít prvočísla p a q, potřebné k tvorbě klíčů. RSA lze využít pro šifrování, autentizaci a má široké využití v digitálních podpisech a virtuálních privátních sítí.
- Mechanismus Diffie-Hellman

Jedná se o první algoritmus šifrování veřejným klíčem. Používá se pro bezpečnou distribuci klíčů, které se následně používají pro šifrování.

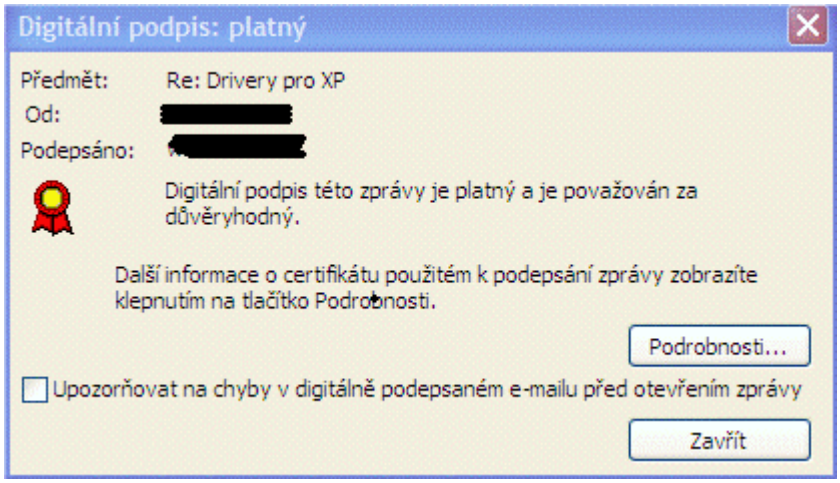
Další asymetrické šifry jsou např. Merkle-Hellman, ElGamal

2.2.3. Digitální podpis (elektronický podpis)

Digitální podpisy slouží k zajištění integrity zprávy (lze prokázat, že po podepsání nedošlo k žádné změně a že není zpráva poškozena) a k prokázání, že autorem je ten, kdo je pod zprávou podepsán.

Zaručený elektronický podpis je elektronický podpis v takové formě, která, zpravidla kryptografickými metodami, zaručuje i integritu dokumentu a autentizaci podepsaného. Pro některé účely je navíc vyžadován zaručený elektronický podpis pouze s předepsanými typy certifikace, tedy „založený na kvalifikovaném certifikátu“. Zaručený elektronický podpis zajišťuje:

- autentizaci (nepopiratelnost) – lze prokázat, že autorem je skutečně ten, kdo je pod dokumentem podepsán, autor nemůže popřít, že dokument podepsal.
- integritu dokumentu – lze prokázat, že po podepsání nedošlo k žádné změně, soubor není poškozen (ani záměrně, ani omylem),
- někdy má i funkci časového razítka, tedy prokazuje datum a čas podepsání dokumentu[13]



11 Digitální podpis

2.2.4. Hašovací funkce

Hašovací funkce je předpis pro výpočet kontrolního součtu (haše) ze zprávy či většího množství dat. Může sloužit ke kontrole integrity dat, k rychlému porovnání dvojice zpráv, indexování, vyhledávání apod. Je důležitou součástí kryptografických systémů pro digitální podpisy.[14]

2.3. Systém řízení přístupu

Pro zabezpečení počítačových sítí z hlediska přístupu se nejčastěji používá architektura AAA (Autentizace, autorizace a účtování (Authentication, Authorization and Acounting)).

2.3.1. Autentizace

Autentizace je proces ověřování a potvrzování totožnosti uživatele (komunikujících stran). Autentizace může vést k jednoznačné identifikaci (zjištění identity uživatele: Kdo je?)

[13] http://cs.wikipedia.org/wiki/Elektronický_podpis

[14] http://cs.wikipedia.org/wiki/Hašovací_funkce

nebo (častěji) k verifikaci uživatele (potvrzení identity uživatele: Je ten, kdo tvrdí, že je?) na základě zadaných údajů uživatele do autentizačního systému.

Autentizace může probíhat jednosměrně, kde se autentizuje pouze jedna strana vůči druhé, nebo obousměrně, kdy se autentizují obě strany vzájemně, a obě musí sdílet určitou tajnou informaci.

Základní metody pro zjištění identity:

- Identifikace podle uživatelského jména a hesla, PINu (něco co uživatel zná)

Jednoduchá metoda zabezpečení s minimálními náklady. Tato metoda je velmi náchylná k zapomenutí, zneužití a k uhádnutí. Někdy se vyžaduje pravidelná obměna hesel. Doporučuje se užití „silných hesel" odolných proti odhalení (kombinace malých a velkých písmen, číslic a speciálních znaků, minimální délka hesla).

Příklady odhalení hesel:

- Útok na heslo související s uživatelem (tzv. sociální inženýrství).

Útočník se pokouší použít informace, které jsou spojeny s uživatelem, např. jeho jméno, jméno partnera, rodné číslo.

- Slovníkový útok.

Útočník používá při útoku hesla, která se vyskytují v jazykových slovnících

- Útok hrubou silou (brute force)

Útočník se postupně pokouší zadat všechny možné kombinace znaků, a to tak dlouho, dokud požadované informace nenalezne.

- Využití trojského koně.

Program, který je schopen zachytit a uložit na místo přístupné útočníkovi autentizační informace.

Identifikace pomocí technického prostředku (něco co uživatel má)

Uživatel se identifikuje pomocí unikátního technického prostředku, který vlastní. Jednoduchá metoda ověření autorizace. Tato metoda je náchylná ke ztrátám, krádeži a kopiím.

Příklady technických prostředků:

- Karta SmartCard

Karta SmartCard je plastiková karta přibližně stejné velikosti jako platební karta, na kterou lze ukládat důležité informace. Lze ji použít k uchovávání certifikátů a soukromých klíčů a k provádění šifrovacích operací využívajících veřejný klíč, k nimž patří ověřování, digitální podepisování a výměna klíčů.

12 SmardCard

Zdroj: http://en.wikipedia.org/wiki/Smart_card

- Token

Token je zařízení s vlastním čipem a pamětí, kde je uložen šifrovací klíč.

Identifikace biometrickými systémy (něco čím uživatel je)

Uživatel se identifikuje podle jednoznačných ukazatelů. Tato metoda patří mezi nejbezpečnější metody identifikace a nelze téměř obelstít. Zařízení pro autentikaci jsou nákladnější.

Příklady jednoznačných ukazatelů:

- Otisk prstu, dlaně.
- Snímek oční zornice.
- Podpis.
- Hlasová analýza.

13 USB Flash Disc se čtečkou otisku prstu

http://www.pretec.com/epages/Store.storefront/?ObjectPath=/Shops/Store.Pretec/Products/UFUXXX

Dvoufaktorová autentizace

Dvoufaktorová autentizace je založena na dvou zcela nezávislých faktorech:

- něco, co uživatel zná - tajné PIN (osobní identifikační číslo)
- něco, co uživatel má - osobní autentizační předmět (např. kartu RSA SecurID)

14 RSA SecurID

Zdroj: http://www.rsa/nsf/0/61C3D928E7054C1256B76RSA%20Security

Single sign-on(SSO)

SSO řeší problém existence různých hesel pro přístup k různým aplikacím systému. Při použití aplikace SSO se uživatel autentizuje pouze jednou a autentizační údaje jsou zprostředkovány všem systémům automatizovaně.

2.3.2. Autorizace

Po úspěšné autentizaci může být uživatel autorizován pro užívání síťových prostředků a služeb. Autorizace specifikuje, jaké operace mohou uživatelé v systému provádět a jaká data jsou pro ně dostupná.

2.3.3. Účtování

Poslední složkou architektury AAA je účtování, které zodpovídá za záznam všech činností uživatele v systému. Sbírají se informace o identitě uživatele, povaze dodaných služeb a časy počátků a konců dodaných služeb.

V rámci architektury AAA pracují nejčastěji systémy TACACS a RADIUS.

TACACS (Terminal Access Controler Access Control System)

TACACS je systém řízení přístupu, který umožňuje vzdálenému přístupovému serveru komunikovat s autentizačním serverem. Ten rozhodne, zda má uživatel oprávnění přístupu k síti. Rozšířený systém TACACS+ již podporuje všechny tři složky architektury AAA. Autentizaci při přihlášení do systému, autorizaci a shromažďování údajů o využívání systému uživatelem.

RADIUS (Remote Authentication Dial-In User Service)

RADIUS je služba pro autentizaci vzdálených uživatelů, která v sobě zahrnuje všechny tři složky architektury AAA a odpovídá za ověření uživatelů před přístupem do sítě. Pracuje

na principu klient/server a přenos mezi serverem a klienty využívá transportního protokolu UDP. Transakce mezi serverem a klienty se autentizují prostřednictvím sdíleného hesla, které se nikdy nepřenáší v síti. Hesla uživatelů se posílají mezi klienty a serverem zašifrovaná.

2.3.4. Autentizace pomocí IEEE 802.1x

IEEE 802.1x je standard organizace IEEE pro řízení přístupu k síti povolující nebo zakazující jednotlivé porty na přepínači. Podle výsledku autentizace zařízení připojeného k síťovému portu, buď poskytne připojení k síti, nebo tomuto připojení zamezí, pokud autentizace selhala.

802.1x je dostupné na některých zařízeních typu přepínač, který může být nakonfigurován k autentizaci těch zařízení, které jsou vybaveny takzvaným prosebníkem (supplicant), tedy softwarem snažícím se autentizovat. Zakazuje neautorizovaný přístup k síti na datové vrstvě.

RADA

RADA je rozšířený standard 802.1x a umožňuje ověřování uživatelů přes jméno a heslo (802.1x Network Login), ověřování zařízení přes hardwarovou adresu (RADA ověřuje tiskárny, bezdrátové přístupové body – nevyžaduje software pro autentizaci) nebo kombinaci ověření přes uživatele i hardwarovou adresu.

Další vlastnosti systému RADA:

- Řešení přístupu k síti pro dočasné uživatele (např. návštěva)
- Hostitelská VLAN pro konferenční prostory
- Omezený přístup k podnikové síti k některým zdrojům (např. povolení připojení pouze k Internetu)
- Automatická konfigurace stanice ke skupině (VLAN)

Podle jména a hesla nebo hardwarové adresy

Praktické při stěhování uživatelů a zařízení

- Automatické nastavení QoS (Quality of Service) parametrů

Prioritizace kritický dat je nastavená automaticky

2.4. Bezpečné podnikové sítě

2.4.1. Filtrování paketů

Filtrování paketů je jedním z nejstarších a zároveň nejběžnějších typů dostupných technologií pro inspekci paketů. Nejprve provede kontrolu obsahu paketu, aplikuje na něj určitá pravidla a podle nich stanoví, jestli se paket může propustit (povolit mu průchod), nebo jestli se zahodí. Filtrování probíhá na základě přístupových seznamů. Existují dva základní typy přístupových seznamů:

- Standardní přístupové seznamy IP – shoda se zjišťuje jen podle zdrojové adresy
- Rozšířené přístupové seznamy IP – shoda se zjišťuje podle zdrojové i cílové adresy a pro kontrolu také podle typu protokolu a čísla portu

Filtrování paketů patří mezi základní úroveň zabezpečení sítě. Pokročilejší metoda inspekce paketů je tzv. stavová inspekce paketů (SPI).

- Stavové paketové filtry – na rozdíl od jednoduchého filtrování paketů stavové paketové filtry ukládají informace o povolených spojení, a tím se urychluje zpracování paketů.
- Stavové paketové filtry s kontrolou protokolů a IDS – kontrolují pakety na úrovni aplikací a mohou omezit nebo zakázat průchod nežádoucího spojení.

2.4.2. Překlad síťových adres (NAT)

Překlad síťových adres IP mezi podnikovou a veřejnou sítí umožňuje ochranu vnitřních uživatelů sítě, jejichž adresy zůstávají pro vnější svět neznámé, a tedy nedostupné. Veškeré pakety z podnikové chráněné sítě ji opouštějí s adresou výstupních rozhraní směrovače nebo firewallu a obráceně. V příchozích paketech jsou tyto adresy nahrazovány skutečnými adresami stanice v síti.

Pomocí překladu NAT mohou organizace také řešit nedostatek veřejných IP adres ve své podnikové síti. Překlad NAT zvyšuje úroveň zabezpečení sítě (útočník nezná skutečnou IP adresu uživatele).

Typy NAT

- Statický NAT
- Dynamický NAT
- Přetížený NAT

2.4.3. Zástupný server (Proxy server)

Proxy server ověřuje pakety z hlediska platnosti dat na aplikační úrovni před otevřením spojení. Server si udržuje všechny informace o stavu spojení a číslech paketů. Zástupné servery mohou také ověřovat uživatelská hesla a požadavky na služby. Servery nedovolují přímou komunikaci s reálnou službou, starají se o veškerá spojení mezi uživatelem a požadovanou službou a jsou z hlediska uživatele transparentní. Oproti paketovým filtrům se bezpečnost s proxy zvýšila, ale zhoršila se výkonnost sítě. Včlenění proxy mezi klienta a server totiž zpomaluje komunikaci.[15]

Typy Proxy serveru

- Standardní proxy server
- Dynamický proxy server

2.4.4. Filtrování obsahu

Tento mechanismus je schopen, podle definovaných pravidel, zamezit průchod podezřelé elektronické poště (např. infikované virem, spam, trojské koně) a znemožnit uživatelům přístup na internetové stránky s nevhodnou tématikou (např. pornografie, násilí).

2.4.5. Firewall (ochranná zeď)

Firewall tvoří zásady zabezpečení. Nejdůležitějším předpokladem správné funkčnosti firewallu je, že veškerá komunikace mezi podnikovou sítí a veřejnou sítí musí projít přes něj.

Nejběžnější pravidla činnosti firewallů a jejich funkce:[16]

- Blokování příchozího síťového provozu podle jeho zdroje nebo cíle.

Zablokování nežádoucího příchozího provozu je nejběžnější funkcí firewallu a je konec konců hlavním důvodem pro jeho instalaci – zabránit vstupu nežádoucího provozu do vnitřní sítě. Takovýto provoz obvykle pochází od útočníků, takže jej budeme chtít určitě rychle vykázat pryč.

- Blokování odchozího síťového provozu podle jeho zdroje nebo cíle.

Řada firewallů dokáže sledovat také síťový provoz ve směru z vnitřní sítě do veřejného Internetu; takto můžeme například zaměstnancům vlastní firmy zabránit v přístupu k nevhodným webovým stránkám.

---

[15] Pužmanová, Rita: Moderní komunikační sítě od A do Z; str. 373-374

[16] Thomas, M. Thomas, Zabezpečení počítačových sítí; str. 140

- Blokování síťového provozu podle obsahu.

Vyspělejší firewally sledují v síťovém provozu také nepřípustný obsah. S firewallem může být například integrován antivirový program, který zabraňuje virům ve vstupu do vnitřní sítě; jiné firewally jsou integrovány s e-mailovými službami a monitorují a blokují průchod nežádoucí elektronické pošty.

- Zpřístupnění zdrojů vnitřní sítě.

Primárním úkolem je sice zabránit v průchodu nežádoucího síťového provozu, u většiny z nich můžeme ale také nakonfigurovat selektivní povolení přístupu ke zdrojům (prostředkům) vnitřní sítě, jako je například webový server; ostatní typy přístupu z Internetu do vnitřní sítě ponecháme zakázané. V řadě případů je možné tyto funkce zajistit pomocí takzvané demilitarizované zóny (DMZ), do níž umístíme mimo jiné i zmíněný veřejný webový server.

- Povolení některých spojení do vnitřní sítě.

Zaměstnanci se do podnikové sítě běžně připojují také prostřednictvím virtuální privátní sítě (VPN). Tyto sítě umožňují bezpečné připojení z Internetu, například pro domácí pracovníky a pro obchodní cestující v terénu, nebo také pro vzájemné spojení vzdálených poboček firmy. Některé firewally přímo obsahují funkce sítě VPN a usnadňují tak zavádění popsaných spojení.

- Oznamování průběhu síťového provozu a činnosti firewallu.

Při monitorování síťového provozu do a z Internetu je také důležité vědět, co všechno firewall dělá, kdo se pokouší „nabourat“ do vnitřní sítě, a kdo pokouší na Internetu přistupovat k nevhodnému materiálu. Většina firewallů obsahuje proto určitou formu mechanismu pro oznamování; dobrý firewall může také veškeré aktivity zaznamenávat do serveru syslog nebo do jiného záznamového zařízení. Zkoumání systémových protokolů firewallu po proběhlém útoku je jedním z důležitých a průkazních nástrojů, které máme k dispozici.

Firewally dělíme na :

- Hardwarové firewally
- Softwarové firewally

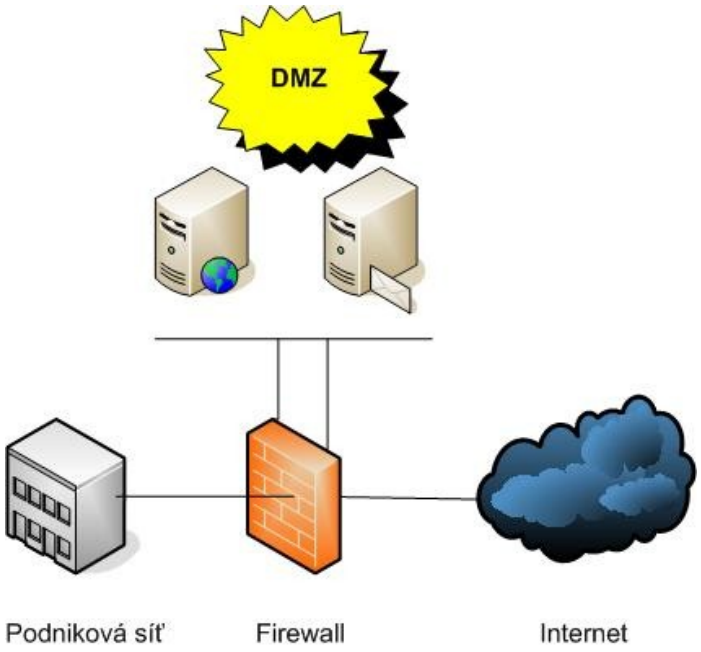
a dále na :

- Osobní firewall
- Integrovaný firewall vše v jednom (Firewall, NAT, Router)
- Firewally pro malé a střední organizace

- Firewally podnikové úrovně

Demilitarizovaná zóna

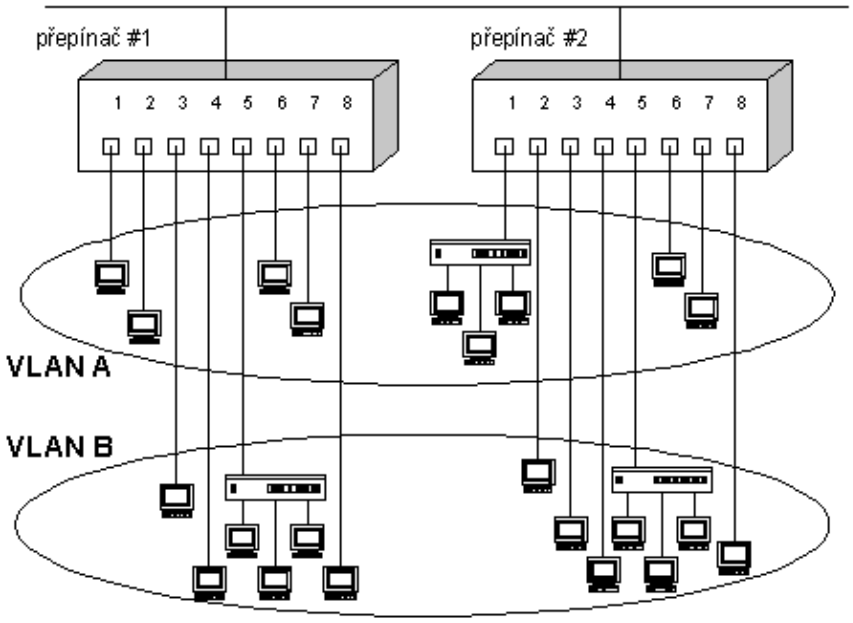
Demilitarizovaná zóna (DMZ) je rozhraní, umístěné mezi vnitřní sítí a sítí Internet. Obě sítě jsou fyzicky oddělené a komunikují pouze na základě určených pravidel, definovaných ve firewallu. V DMZ je zpravidla umístěn webový nebo server a podle určených pravidel nesmí síťový provoz z Internetu vstupovat k vnitřní síti. Další výhodou DMZ je izolace neznámých (podezřelých) požadavků z Internetu do zvláštních serverů DMZ.



15 DMZ

2.4.6. Přepínače v lokálních sítích

Přepínač (switch) je dalším základním prvkem bezpečných počítačových sítí. Přepínače pracují jako mosty s více porty na spojové vrstvě ISO/OSI a filtrují pakety pouze na základě rozhodovací tabulky MAC adresy. Přepínané sítě jsou bezpečnější než sítě bez přepínačů, protože provoz se nešíří celou sítí, ale pouze mezi komunikujícími stanicemi. Přístup k síti a přenos dat lze ovlivnit snadným nastavením přepínače. Přepínače umožňují vytvoření virtuální lokální sítě (VLAN) ve vnitřní podnikové síti. VLAN umožňuje vytvoření logických skupin uživatelů (např. podle oddělení: vedení organizace, výroba, obchodní oddělení), které jsou nezávislé na fyzickém umístění v síti. To umožňuje zjednodušit správu a management sítě.



16 Příklad VLAN

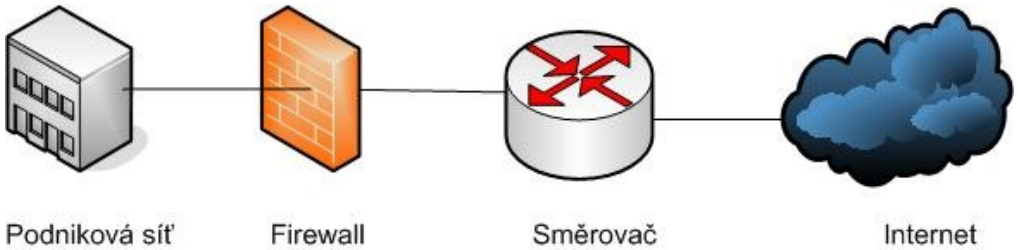
Zdroj: http://www.svetsiti.cz/view.asp?rubrika=Tutorialy&temaID=237&clanekID=239

2.4.7. Směrovač

Směrovač (router) zajišťuje vlastní připojení podnikové sítě do Internetu. Směrovač můžeme označit za „hrdlo sítě“, přes které prochází veškerá komunikace podnikové sítě s Internetem. Význam směrovače jako hrdla sítě spočívá v tom, že snadno zabraňuje v přístupu ke konkrétním aplikacím, a to bez nepříznivého vlivu na výkonnost sítě. Vyšší bezpečnost sítě zajišťují přístupové seznamy, které sledují síťový provoz na vrstvách 2, 3 a 4 referenčního modelu ISO/OSI. Přístupové seznamy umožňují vysoký stupeň kontroly a možnosti filtrování všech paketů, které procházejí směšovačem.

Základní funkce směrovače:

- Chrání vnitřní síť před průnikem z Internetu
- Zajistí bezpečnou komunikace v Internetu
- Zajistí bezpečný vzdálený přístup
- Zajistí bezpečný provoz elektronického obchodu



17 Směrovač

2.5. Bezpečnost bezdrátových sítí

Bezdrátové lokální sítě (WLAN) představují velmi rychlé a jednoduché rozšíření klasické sítě LAN bez nutnosti zásahu do stávající kabeláže. Stačí připojit přístupový bod a mohou se okamžitě stanice a notebooky, vybavené bezdrátovou síťovou kartou, téměř okamžitě připojit do lokální sítě. Rychlost tohoto připojení je srovnatelné se standardní sítí a to na vzdálenost až 300m. Přenos dat v bezdrátové síti běží otevřeným prostorem, a celá síť je tak otevřená i vůči potencionálním útočníkům.

Identifikátor SSID (Service Set Identifier)

Přístupový bod vysílá implicitně SSID a oprávněný uživatel může snadno najít správnou síť, ale zároveň se do ní dostane i neoprávněný uživatel. Hodnota parametru SSID je první úroveň zabezpečení za předpokladu, že není v základním (továrním) nastavení.

Filtrování MAC adres

Filtrování MAC adres je další úrovní zabezpečení. V přístupovém bodu lze snadno nastavit seznam oprávněných uživatelů a kohokoli jiného nepustit do sítě.

WEP (Aires Equivalnet Privacy)

WEP patří mezi slabší úroveň zabezpečení bezdrátového provozu a existují 3 obvyklé režimy:

- Bez šifrování
- 40bitové šifrování
- 128bitové šifrování

Protokol EAP

Tento protokol je založen na standardu 802.1x a představuje vyšší úroveň zabezpečení.

V rámci protokolu EAP se používají 4 metody autentizace:

- EAP-MD5
- EAP-TLS
- EAP-TTLS
- LEAP

3. Zabezpečený vzdálený přístup k síti LAN

Remote Access

Vzdálený přístup (Remote Access) k síti je technologie umožňující přístup vzdálených uživatelů k podnikové síti. Používá se pro připojení vzdálené pobočky, obchodních partnerů, domácích uživatelů nebo mobilních uživatelů pracujících v terénu. Tato technologie umožňuje vzdáleným uživatelům přistupovat k síťovým prostředkům jako je např. elektronická pošta, databáze, aplikace.

Metody vzdáleného přístupu:

- Terminal servers – přístup s emulací terminálu (např. Telnet)
- Remote node – přihlášení do sítě
- Remote control (např. MS Terminal Server, Citrix Presentation server)

3.1. Virtuální privátní síť (VPN)

Virtuální privátní sít je šifrované síťové spojení mezi dvěma koncovými body zabezpečené komunikačním tunelem. Spojení probíhá přes veřejnou infrastrukturu (veřejná síť ATM, Frame Relay nebo Internet). Za minimální cenu, tak lze připojit k firemní síti vzdálené pobočky nebo uživatele. VPN je tedy logická síť vytvořená v rámci veřejné infrastruktury, která si však zachovává charakter privátní sítě.

3.2. Typy VPN

- VPN pro připojení pobočky

Tento typ sítě rozšiřuje stávající podnikovou síť do dalších budov a pracovišť. Spojení probíhá pomocí specializovaného vybavení a vzdálený uživatel může využívat stejné síťové služby jako uživatelé v lokální síti. Tento typ sítě je většinou trvale propojený a označují se jako hardwarové VPN, intranetové VPN nebo VPN mezi sítěmi LAN (LAN-to-LAN).

- VPN pro vzdálený přístup

Tento typ VPN umožňuje bezpečné připojení jednotlivých uživatelů k centrále přes Internet. Slouží tak k připojení uživatelů z terénu nebo z domova. Na počítači uživatele je nainstalován speciální software VPN, který vytvoří bezpečnou linku do podnikové sítě

LAN. Tohoto typu připojení můžou využívat pracovníci v terénu nebo uživatelé připojující se do firemní sítě z domova.

- Extranetové VPN

Tento typ VPN umožňuje bezpečné spojení za účelem vedení elektronické komerce. Dovoluje bezpečné spojení centrály s obchodními partnery, dodavateli a zákazníky. Extranetové sítě VPN jsou rozšířením intranetových VPN a vnitřní síť je navíc chráněna pomocí firewallů.

3.3. Tunelování

Při vytváření privátní sítě v prostředí veřejného internetu se technologie VPN opírá o takzvané tunelování. V podstatě to znamená, že systém vezme celý paket dat a zapouzdří jej do jiného paketu, který následně přenese po síti; tato síť musí pouze znát protokol vnějšího paketu, jehož prostřednictvím data vstupují a vystupují ze sítě. Do celého tunelování jsou zapojeny tři různé protokoly: [17]

- Přenášený (nesený) protokol.

Původní datový protokol, obvykle IP, který se má zašifrovat pro přenos v síti VPN. Podle potřeby je možné přenášet i jiné protokoly, například IPX a NetBEUI.

- Zapouzdření – obalový protokol.

Tento protokol (GRE, IPSec, L2F, PPTP, L2TP) se „obalí“ okolo původních dat; říkáme, že data jsou v něm zapouzdřena. V současné době je de facto standardem pro zapouzdření dat IPSec; zapouzdření umožňuje šifrování a ochranu celého přenášeného paketu. Pro správnou činnost tunelu musí obě jeho rozhraní podporovat protokol IPSec.

- Nosný protokol.

Protokol, přes který v síti putují informace. Původní přenášený paket se zapouzdří v obalovém protokolu; výsledný paket se dále doplní o hlavičku nosného protokolu (je jím obvykle IP) a konečně se přenese po veřejné síti.

3.4. Protokoly pro tunelování a šifrování VPN

Tunelování umožňuje přenos dat přes veřejnou infrastrukturu, ale nezajistí soukromí. Pro zabezpečení přenosu dat proti odposlechu je nutné veškerý provoz v síti VPN šifrovat.

GRE (Generic Routing Encapsulation)

[17] Thomas, M. Thomas, Zabezpečení počítačových sítí; str. 200

GRE představuje generický mechanismus tunelování pro libovolný typ provozu. Směrovače tvořící konce tunelu zodpovídají za zapouzdření a odpouzdření paketu přenášených přes transportní síť tunelem.

L2TP (Layer 2 Tunneling Protocol)

L2TP poskytuje mechanismus logického PPP (Point-to-Point) propojení vzdáleného uživatele z jeho konkrétního fyzického přístupového místa dynamicky vytvořeným tunelem do jiného předem zkonfigurovaného fyzického místa sítě. L2TP se zpravidla používá pro připojení jednotlivce k podnikové síti prostřednictvím VPN.

Protokol IPSec

Protokol IPSec chrání citlivá data při přenosu v nechráněných sítí. Bezpečnostní služby pracují na síťové vrstvě, přičemž zajišťuje ochranu a autentizaci paketů mezi dvěma koncovými zařízeními jako jsou firewally a směrovače. Protokol IPSec zajišťuje tyto bezpečnostní funkce:

- Důvěrnost dat

Odesílatel IPSec může data před přenosem po síti zašifrovat.

- Integrita dat.

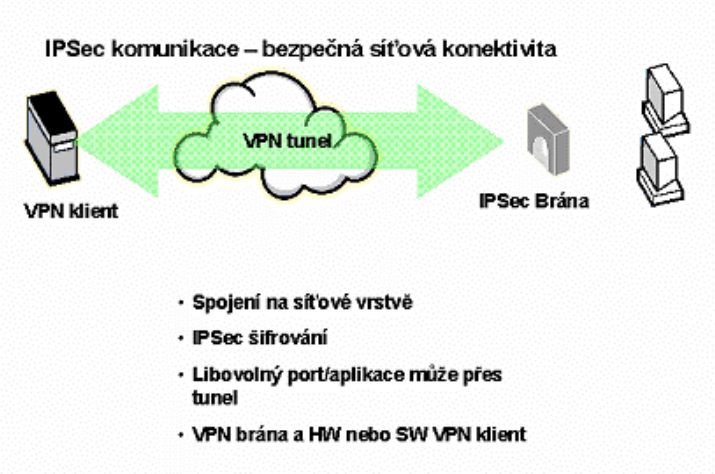
Přijímací koncový bod IPSec autentizuje veškeré pakety od odesílatele a kontroluje tak, jestli nebyla data při přenosu pozměněna.

- Autentizace původu dat.

Příjemce IPSec může dále autentizovat zdroj odeslaných paketů IPSec (toto je závislé na funkci integrity dat)

- Ochrana proti opakování relace

Příjemce IPSec může detekovat opakované pakety a zamítnout je.



18 IPSec komunikace

Zdroj: http://www.svetsiti.cz/view.asp?rubrika=Tutorialy&temaID=295&clanekID=297

Doplňující protokoly IPSec.

- ISAKMP (Internet Security Association and Key Management Protocol)

Popisuje fázi dohody o spojení v IPSec, ve které se navazuje spojení sítě VPN.

- ESP (Encapsulating Secure Payload)

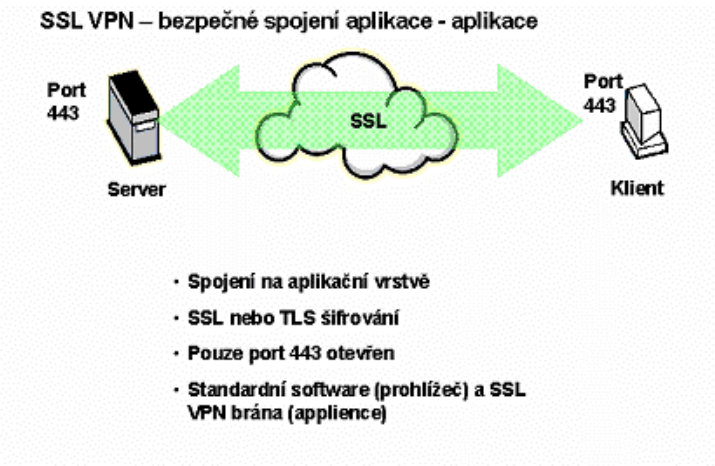
Zajišťuje důvěrnost a ochranu dat s volitelnými službami autentizace a detekce opakování relace.

- AH (Authentication Leader)

Poskytuje autentizaci a volitelně také ochranu proti opakování relace.

Protokol VPN SSL

SSL působí na vyšších vrstvách než IPSec. Používá aplikační vrstvu a nezabezpečuje veškerou komunikaci, ale pouze některé aplikace. SSL zajišťuje autenticitu odesílatele, integritu a šifrování dat při jejich přenosu přes veřejnou síť. SSL vyžaduje transportní protokol TCP a používá kombinaci šifrování veřejným a soukromým klíčem. Veřejný klíč se používá pro autentizaci a soukromý klíč pro šifrování zpráv. SSL podporuje obousměrnou autentizaci, ale většinou se používá pouze jednosměrně. Jako vyšší úroveň zabezpečení se doporučuje dvoufaktorová autentizace. Na rozdíl od IPSec není nutné použít specializovaný zařízení (firewall, směrovač) a lze se připojit prakticky z jakékoliv stanice s webovým prohlížečem. Nevýhodou je, že SSL je v praxi podporováno pro omezenou sadu aplikací typu mail, webový přístup a přenos souborů. Další verze SSL se stala základem otevřené specifikace řešení pod označením TLS.



19 SSL VPN

Zdroj: http://www.svetsiti.cz/view.asp?rubrika=Tutorialy&temaID=295&clanekID=297

4. Potencionální hrozby a protiopatření

4.1. Plány v rámci bezpečnosti IS

V rámci bezpečnosti by měly být vytvořeny následující plány:[18]

Plán zvládání rizik

Plán zvládání rizik popisuje plán a postup redukce zjištěných rizik na potřebnou úroveň. Obsahuje popis způsobu realizace jednotlivých opatření a bezpečnostních projektů vedoucích k dosažení cílových stavů definovaných v bezpečnostní politice. Ke každému projektu, opatření jsou definovány minimálně následující atributy: kritičnost, doba realizace, odpovědnost, předpokládané náklady, výstup a případné následné kroky

Plán zachování kontinuity (hlavních činností)

Jedná se o plán, který má zajistit funkceschopnost hlavních činností (například bez podpory informačních a komunikačních technologií).

Plán zálohování a obnovy

Plán popisující procesy běžného provozního zálohování (dat, programů a nastavení) včetně popisu obnovy z této zálohy (například návratové procedury po chybné implementaci servisní opravy operačního systému).

Havarijní plán (pro jednotlivé IS) + mapa všech havarijních plánů

Plány, které řeší různé typy havárií jednotlivých IS. Celková mapa těchto plánů je důležitá pro stanovení, které části informačního a komunikačního systému je nezbytné zprovoznit jako první, jelikož mají vliv na ostatní (například aby bylo možné používat elektronickou poštu, musí být nejprve zprovozněno připojení na internet, potom lokální síť, všechny potřebné síťové služby a potom má smysl se zabývat poštovním serverem a koncovým uživatelským programem). Tato mapa rovněž stanovuje priority pro postupnou obnovu IS jako celku.

Plán testování havarijních plánů

Havarijní plány je nutné pravidelně testovat a na základě výsledků testů tyto plány přehodnocovat.

Plán bezpečnostní výchovy a školení

Aby vzdělávání bylo prováděno systematicky doporučuje se sestavit plán výchovy a školení informační bezpečnosti (pro jednotlivé role v IS).

---

[18] Hanáček,Petr; Staudek, Jan,Bezpečnost informačních systémů – příloha č.2,standardy a doporučemí;str. 13

Plán auditů IS

Do plánů mají být zahrnuty různé typy kontrol například běžné provozní kontroly, interní a externí audity a penetrační testy.

4.2. Bezpečnostní audit[19]

Mezi bezpečnostní zásady usnadňující prevenci útoků patří prokazatelná (individuální) odpovědnost za akce, prováděné jednotlivými uživateli IS – účtování jejich činnosti. Je zaznamenávána relevantní informace o činnostech a procesech, vykonaných uživatelem nebo jeho jménem, takže následky takových činností mohou být s dotyčným uživatelem později prokazatelně propojeny a ten může být učiněn odpovědným za svou činnost. Relevantní události musí být zaznamenávány tak, aby zaznamenávací mechanismy nemohly být zničeny a aby údaje sloužící k autentizaci a autorizaci uživatele byly bezpečně uchovány.

Důležitou zásadou je oddělení povinností výkonných a kontrolních. Audit musí být nezávislý na prosazování provozní bezpečnosti a hlavně musí být zajištěno, že se audit skutečně provádí.

Auditní postup můžeme charakterizovat následujícími kroky:

- fáze detekce – je zjištěna událost, která má vztah k bezpečnosti
- fáze rozlišovací – určuje, zda je nutné zaznamenat událost do bezpečnostního sufitního záznamu nebo spustit bezpečnostní poplach
- fáze zpracování bezpečnostního poplachu – je spuštěn bezpečnostní poplach nebo je vydána bezpečnostní auditní zpráva
- fáze analýzy – událost, vztahující se k bezpečnosti je posouzena v kontextu dříve zjištěných zpráv, zaznamenaných v bezpečnostním záznamu a je určen průběh činnosti
- fáze agregační – distribuované záznamy dílčích bezpečnostních auditních záznamů jsou spojeny do jednoho bezpečnostního auditního záznamu
- fáze generování zprávy – z bezpečnostních auditních záznamů jsou vytvořeny sufitní zprávy
- fáze archivace – dílčí části bezpečnostního auditního záznamu jsou uloženy do archivu bezpečnostních auditních záznamů.

[19] Hanáček, Petr; Staudek, Jan, Bezpečnost informačních systémů; str. 38

Politika bezpečnostního auditu definuje, co jsou události, které mají vztah k bezpečnosti a pravidla, která mají být použita pro sběr, zaznamenání a analýzu různých událostí, které mají vztah k bezpečnosti. Pokud mají být bezpečnostní auditní záznamy používány jako právně přípustné důkazy, klade to specifické požadavky na jejich uložení a ochranu, především před jejich neoprávněnou změnou. Auditní záznamy je vhodné ukládat na médium, na které je možný zápis pouze jednou, protože pak není možné záznam vymazat nebo měnit přepsáním média. Ochrana bezpečnostního auditu je zaměřena především na dostupnost této služby. Informace určená pro bezpečnostního auditora ztrácí po určité době svoji hodnotu. Událostí relevantních pro bezpečnost může být mnoho, a proto je důležitá účinná analýza událostí. Obvykle se používá nějaký filtrovací mechanismus, který se řídí předem stanovenými kritérii. Kritéria typicky definují čas, typ události a entitu, která událost způsobila.

4.3. Potencionální hrozby

Hrozby klasifikujeme do následujících skupin:

- Přírodní (živelné pohromy – požáry, povodně)
- Fyzické (poruchy napájení)
- Technické (poruchy zařízení, poruchy sítí)
- Technologické (poruchy způsobené škodlivým kódem)
- Lidské

Neúmyslné (poruchy způsobené neznalostí nebo omylu uživatele)
úmyslné (zvenku – hacker, špionáž, terorista, zevnitř – zaměstnanec, návštěvník)

4.4. Škodlivý kód (malware)

Škodlivý kód je speciální program útočníků, jejichž cílem je poškodit programy a data, poškodit zařízení, vyčerpat systémové zdroje nebo zcizit citlivé informace. Malware patří mezi velké hrozby současného Internetu a způsobuje i velké finanční ztráty organizacím a jednotlivcům.

Viry

Název virus je odvozen z podobnosti chování s biologickými originály. Počítačový vir má schopnost vlastního množení (sebereplikace) a infikování počítačových systémů bez vědomí uživatele. Virus je program, který je navázán na jiný program jako jeho část a provádí nevyžádanou činnost. Tyto činnosti mohou být různé: neškodné (reklama, vtip),

škodné (může mazat data nebo je modifikovat). Virus má část výkonnou (provádí vlastní činnost) a část sebereplikující (zajišťuje další šíření po síti). Některé viry mají pouze část výkonnou a šíření probíhá lidským přičiněním (např. v elektronické poště).

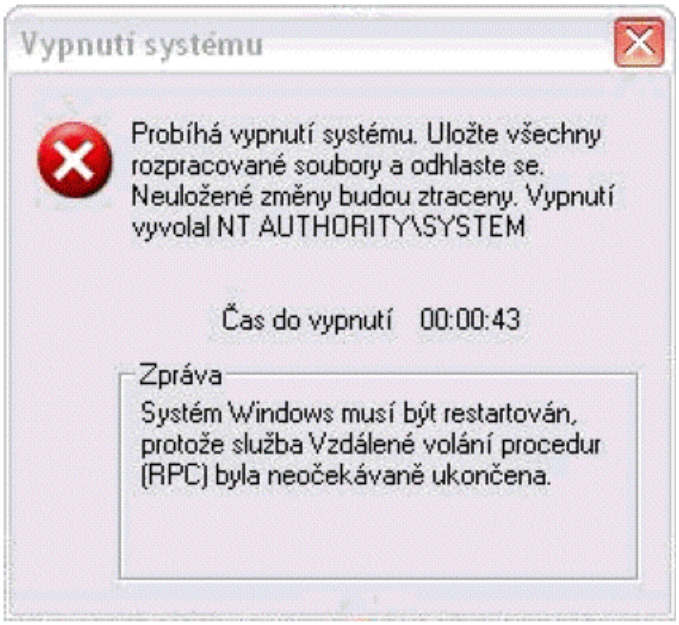
První virus se objevil v roce 1986 a vytvořili jej bratři Asit a Amjat Farooq Alviovi z Pakistánu.

Červi (worms)

Červi pracují na nižší síťové úrovni než klasické viry. Nešíří se ve formě infikovaných souborů, ale síťových paketů. Programy typu červ sám vytváří své kopie a způsobuje, že jsou spuštěny. Není tedy zapotřebí žádná činnost uživatele a červi se sami šíří sítí a můžou např. způsobit kompletní zahlcení podnikové sítě. Šíření červa je postaveno na zneužívání bezpečnostních děr v operačních systémech.

První červ byl označen jako Morrisův červ, který v roce 1988 zahltil tehdejší síť Internet.

Jako nejznámější červ se „proslavil“ např. Lovsan/Blaster.



20 Typická situace pod MS Windows XP bez příslušné bezpečnostní záplaty po napadení červem Lovsan / Blaster.

Zdroj: Bc. Igor Hák, Moderní počítačové viry

Trojské koně (trojan horses) – Trojan

Trojský kůň není schopen sebereplikace a šíří se většinou lidským přičiněním. Obvykle se jedná o typ souboru typu „EXE“ s přitažlivou nebo užitečnou tématikou. Po spuštění se obvykle aktivuje nějaký, uživateli neznámý, impuls a čeká na aktivaci. Trojani můžou mít

destruktivní účinek (např. smaže data na pevném disku) nebo sledují jednotlivé stisky kláves (např. za účelem získání hesla), tyto ukládá a posílá na dané e-mailové adresy.

Backdoor (zadní vrátka)

Backdoor je typ aplikace, sloužící pro vzdálenou správu počítače (typu klient/server) a sama o sobě nemusí být škodlivá. Vzdálený útočník tak může mít plnou kontrolu nad infikovaným počítačem.

Dialer (přesměrování telefonního připojení)

Dilaer je program, který změní číslo vytáčeného spojení k Internetu. Místo běžného čísla dialer přesměruje vytáčení na speciální čísla se zvláštním tarifem (desítky Kč za minutu spojení). Toto přesměrování většinou probíhá zcela automaticky bez vědomí uživatele. Dialer může být soubor „EXE“ nebo součást webové stránky s technologií ActiveX.

Spyware

Spyware je program zaměřený na sledování činnosti uživatele a počítače. Bez vědomí uživatele se tak odesílají statistické data jako je např. přehled navštívených stránek. Program se obvykle šíří společně s sharewarovými programy.

Adware

Adware je většinou program, který se šíří jako součást některých programů typu freeware. Typickým příznakem je zobrazování reklam nebo vnucování internetových stránek během spuštění programu.

Browser hijackers (Piráti prohlížeče)

Tento typ programu má schopnost měnit nastavení webového prohlížeče, změnit nastavení výchozí stránky, přesměrovat vyhledávání na webu na placené stránky vyhledávače.

Hoax (poplašné zprávy)

Hoax je typ poplašné zprávy, která upozorňuje na neexistující nebezpečí. Tyto zprávy se většinou šíří elektronickou poštou a odkazují se na důvěryhodné zdroje typu: Symantec, FBI varuje, Microsoft upozorňuje atd. Zpráva typu Hoax obvykle obsahuje výzvu k hromadnému odesílání na další adresy.

Nejčastější typy hoaxu:[20]

- Varování před smyšlenými viry a různými útoky na počítač
- Popis jiného nereálného nebezpečí
- Falešné prosby o pomoc
- Fámy o mobilních telefonech

[20] http://www.hoax.cz/cze/index.php?action=hoax_description

- Pyramidové hry a různé nabídky na snadné výdělky
- Řetězové dopisy štěstí
- Žertovné zprávy

Phishing

Jedná se o podvodné e-maily, které na první pohled vypadají jako informace např. z banky. Příjemce je požádán o vyplnění údajů (zpravidla číslo účtu a PIN) na formuláři. Odkaz na formulář zpravidla vypadá jako oficiální stránky banky, ale ve skutečnosti je uživatel přesměrován na cizí server.

Spam (nevyžádaná pošta)

Spam nepatří do kategorie škodlivých programů, ale trápí většinu správců počítačové sítě. Spam je elektronické zpráva reklamního charakteru nabízející zboží, služby, snadné výhry atd. Spam je rozesílán podle seznamů existujících adres nebo podle náhodně generovaných emailových adres, které se tvoří z obvyklých jmen, příjmení a přezdívek. Emailové adresy se mohou také sbírat pomocí robotů, kteří prohledávají stránky na internetu a sbírají vše, co vypadá jako emailová adresa. V případě obdržení spamu se nedoporučuje reagovat na odkazy typu „V případě, že nechcete dostávat tyto nabídky, klikněte sem“, v tomto případě se pošle potvrzení, že adresa je funkční a budou odesílány další nevyžádané zprávy. Spam je dnes veliký problém a zahlcuje poštovní servery organizacím.

Další informace o virech a dalších škodlivých programech jsou na stránkách:

www.viry.cz

www.virovyradar.cz

www.spyware.cz

www.spammer.cz

www.symantec.com

www.hoax.cz

4.5. Ochrana před škodlivým kódem

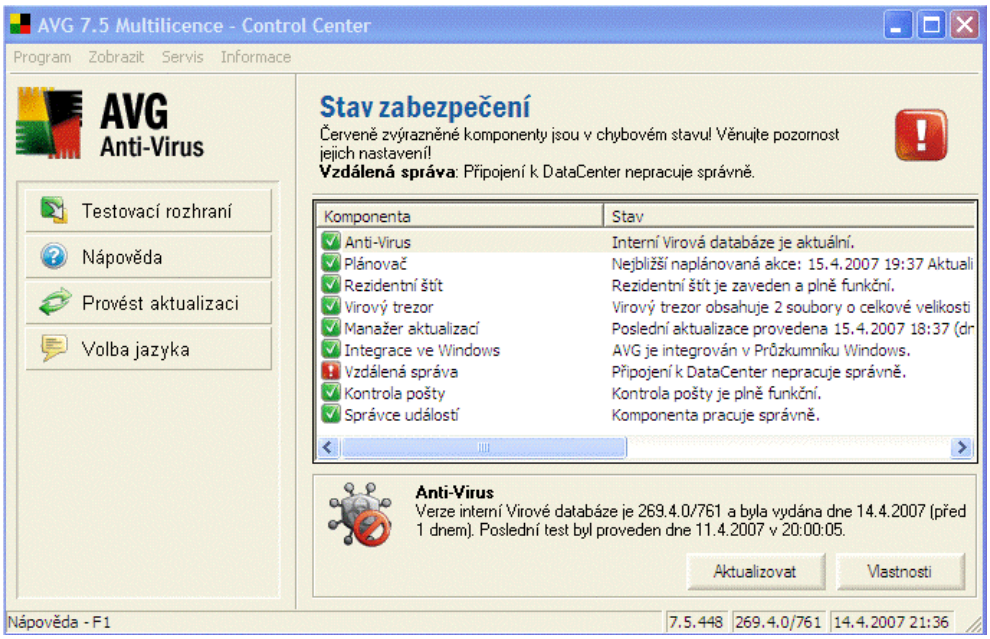
Základem ochrany před škodlivými programy je disciplína uživatele: Neotvírat poštu od neznámého uživatele, neotvírat podezřelou přílohu, návštěva podezřelých stránek. Dále záleží na konkrétní bezpečnostní politice organizace. Mohou být např. zakázány veškeré přílohy ve zprávách mimo specifikovaných typů souborů (obvykle Word, PDF…).

Ochrana softwarovými prostředky:

- Udržovat počítač aktualizovaný – pravidelně počítač aktualizovat bezpečnostními záplatami
- Použití antiviru, antispamu atd. a zajistit aktualizaci těchto programů
- Použití firewallu

Příklady programů pro osobní počítače, servery a podnikové sítě

- Ad-Aware
- Avast Antivirus
- AVG Anti-Virus
- AVG Internet Security SBS Edition – Centrálně řízená kompletní ochrana počítačových sítí a poštovních serverů
- Anti-Virus Kaspersky
- BitDefender Internet Security
- GFI MailSecurity for Exchange/SMTP - Kontrola obsahu e-mailů, detekce průniků a antiviru
- InoculanIT
- KerioWinRouteFirewall
- NOD32
- Norton AntiVirus 2007
- Norton Internet Security 2007 – osobní firewall, ochrana před viry, červi, spyware
- Norton360 – ochrana před nebezpečným softwarem a krádeží identity
- TrojanHelp Tools
- VirusScan
- A celá řada dalších



21 Příklad antivirového programu

Ochrana hardwarovými prostředky

Chránit osobní počítače, servery a sítě lze pomocí jednoúčelových nebo víceúčelových zařízení.

Příklady zařízení:

- 3COM Officeconnect Firewall
- 3COM Officeconnect Internet Access Gateways
- Cisco PIX Firewall
- Symantec MAIL SECURITY APPLIANCES Antivirus,Antispam
- Zyxel ZyWALL Firewall

4.6. Útoky na podnikové sítě

Útok na podnikovou síť může být veden z několika důvodů: snaha o získání důvěrných informací, poškození funkčnosti sítě, pomsta bývalého zaměstnance nebo „pouhé“ testování útočníkovo znalostí. Útočník tak může snadno zneužít např. slabou autentizaci a autorizaci, nedostatečně implementované zabezpečení nebo nesprávné přidělení prostředků.

4.6.1. Základní typy útoků:

Odposlech paketů (sniffers)

Tyto nástroje zachycují pakety procházející sítí v místě jejich připojení. Pro odposlech musí útočník zpravidla překonat fyzické zabezpečení sítě a „napíchnout“ zařízení (PDA, notebook) do podnikové sítě. Dokonalejší typy odposlechů umí dekódovat data z paketů všech sedmi vrstev modelu OSI/ISO. Pomocí odposlechu získá útočník cenná data, která mohou obsahovat např. uživatelská jména a hesla. Tím se útočník může dostat na různá místa v síti. Obvykle uživatelé používají stejná hesla pro různé platformy a aplikace, to následně usnadní útočníkovi dostat se i k dalším síťovým prostředkům a narušit jejich důvěrnost.

Dnes, stále oblíbenější, bezdrátové sítě umožňují útočníkovi jednoduché napíchnutí sítě bez nutnosti překonání fyzických zábran. Stačí, aby si sednul do auta s notebookem, vybaveným bezdrátovou síťovou kartou, a může tiše odposlouchávat pakety.

Základní obranou proti odposlechu je účinná fyzická bezpečnost, zabezpečení bezdrátových sítí, používání vícefaktorové autentizace a šifrování dat pro přenos v síti.

Falšování IP adres a únosy relace

Útočník vytvoří paket s jinou IP adresou a podaří se mu tak vstoupit do systému. Tento útok zneužívá vztah důvěry, protože na sebe vezme totožnost důvěryhodného hostitele. Jestliže útočník zjistí např. interval IP adres, kterým daný cílový hostitel důvěřuje, je jeho útok úspěšný a může pokračovat v činnosti. Tento typ útok se převážně používá jako první krok v dalších útočných operacích.

Příklady nástrojů:

Dsniff, Hunt, Ettercap

Jako prevence proti falšování adres je použití virtuální privátní sítě, která původní IP adresy při přenosu v síti šifrují a pakety s pozměněnou zdrojovou či cílovou adresou se okamžitě odstraní.

Útoky s odepřením služeb (DoS, Denial of Services)

Tento typ útoku bývá také označován jako distribuovaný útok odepření služeb (DDoS, Distributed Denial of Service). Základním principem je vždy přetížená sítě takovým množstvím požadavků, že dojde k zahlcení (zpomalení nebo úplné zastavení) síťového provozu. Cílem tohoto útoku není zcizení informací, ale pouze přetížení sítě, a jakmile cíl útoku přestává zvládat provoz, nemohou se k němu připojit právoplatní uživatelé a dochází tak k odepření služeb. Další typ útoku není směrován na přetížení síťového provozu, ale cílem je spotřebovat limitované zdroje oběti (zpravidla serveru). Útočník tak spotřebuje podstatnou část systémových zdrojů (paměť nebo vytížení procesoru serveru) a dojde k odmítnutí služeb pro právoplatné uživatele nebo dokonce k pádu serveru.

Zatímco útoky typu DoS se spouští z jednoho útočného místa, DDoS se spouští z více míst najednou (stovky až tisíce míst). Takový útok je mnohem účinnější a také mnohem náročnější na obranu.

Jako prevenci lze použít např. filtrování paketů na základě typu protokolu, omezení délky spojení, prevence před zahlcením segmenty TCP pro navázání spojení nebo systém zničení dlouhých paketů na hranici sítě.

Falšování protokolu ARP (spoofing)

Falšování protokolu ARP je jednou z metod úspěšného vedení útoků, kdy útočník vstoupí někde doprostřed komunikace mezi dvěma stranami – obvykle mezi klientem a serverem – a zde zachycuje přenášené zprávy. Útočník při této metodě vytvoří falešné pakety s požadavky a odpověďmi ARP a změní adresu MAC v ethernetové vrstvě 2 na libovolnou zvolenou. To umožňuje útočníkovi vydávat se v místní síti za jiný počítač (právoplatný).

Obranou proti falšování protokolu je použití statických ARP tabulek nebo zabezpečením jednotlivých portů přepínače pomocí protokolu 802.1x.

Útoky na úrovni aplikací

Tyto útoky využívají metody Trojan nebo využívají slabosti konkrétních aplikací. Útoky jsou směrovány na některé typy serverů a můžou vést k odposlechu, zničení nebo zneužití informací posílaných po podnikové síti. Jako nejnovější útoky tohoto typu jsou útoky využívající otevřenost technologií spojených se specifikací HTML, internetového prohlížeče nebo protokolu HTTP. Útoky jsou skryté v konkrétních stránkách (jako podprogram) a bez vědomí uživatele se sami šíří sítí až k internetovému prohlížeči uživatele.

Jako prevenci lze použít např. blokování některých typů příkazů, kontrola HTTP a programy proti škodlivým programům.

Existuje celá řada známých útoků a mezi další patří např.: Útok se záplavou paketů, Zadní vrátka atd.

4.6.2. Detekce a prevence průniku

Důležitým parametrem pro provoz bezpečné podnikové sítě je detekce a prevence proti neoprávněným přístupům. Existuje řada nástrojů jak tyto pokusy o průnik minimalizovat.

Systém pro detekci vniknutí (IDS, Intrusion Detection Systém)

Tento systém monitoruje veškerý síťový provoz v podnikové sítí a jeho cílem je detekovat neobvyklé chování, nevhodné aktivity a pokusy o průnik. Funguje jako „síťové poplašné zařízení“ a po rozpoznání útoků informuje správce sítě a aktivuje obranu. Obecně

rozlišujeme dva typy systémů IDS, a sice síťové a hostitelské. Pro účinnou obranu sítě se doporučuje provozovat oba systémy.

Síťový detekční systém (NIDS, Network-based Intrusion Detection System)

NIDS je umístěn přímo v chráněné síti a sleduje veškerý provoz, který v ní prochází. Tyto síťové systémy dokáží účinně sledovat nejen příchozí a odchozí provozní toky, ale také vnitřní provoz mezi jednotlivými hostitelskými systémy a mezi lokálními segmenty sítě. Systémy NIDS bývají zpravidla provozovány před a za firewallem či bránou sítě VPN, kde měří účinnost těchto bezpečnostních zařízení a dále s nimi komunikují s cílem hlubšího zabezpečení sítě.[21]

Hostitelský detekční systém (HIDS, Host-based Intrusion Detection System)

HIDS je speciální softwarová aplikace, která se nainstaluje na určitý počítač (zpravidla jsou to servery) a zde sleduje veškerý příchozí i odchozí provoz a také změny souborového systému. Systémy HIDS jsou mimořádně účinné zejména u kriticky důležitých aplikačních serverů, dostupných z veřejného Internetu, jako jsou webové a poštovní servery, protože sledují chráněnou aplikaci přímo u zdroje. [22]

Systém prevence vniknutí (IPS, Intrusion Prevention System)

IPS spolupracuje s detekčním systémem IDS a od prvního možného okamžiku aktivně reaguje a brání v úspěšném dokončení útoku. Obranu zajišťují dvě techniky:

- Odpálení komunikace (snipping)

IPS resetuje spojení TCP

- Odříkání komunikace (shunning)

IPS automaticky změní konfiguraci vstupního směrovače (firewallu), IPS se spojí s příslušným směrovačem a nařídí mu odmítat další provoz daného spojení. Dále může dojít k blokování útočníka vytvořením přístupového seznamu IP adresy.

Zařízení typu IPS, tak slouží k prevenci proti útokům, ochranu proti virům, červům nebo útokům typu DoS. Dále umožňuje kontrolovat a případně i blokovat používání nežádoucích aplikací (např. komunikační programy, stahování dat z podezřelých zdrojů) a blokovat přístup na nevhodné webové stránky.

---

[21] Thomas, M. Thomas, Zabezpečení počítačových sítí; str. 255

[22] Thomas, M. Thomas, Zabezpečení počítačových sítí; str.255

4.6.3. Bezpečností situace

Průzkum[23] společnosti Van Dyke Software mezi společnostmi, jejichž systémy byly nějakým způsobem narušeny, ukázal, že největším zdrojem narušení byly viry (78%), vnější nepřátelské průniky do systémů (50%), DoS útoky (40%), vnitřní narušení (29%), spoofing (28%), datová nebo síťová sabotáž (20%) a neoprávněné průniky zevnitř sítě (16%). A to přesto, že drtivá většina společností používala vstupní firewall v perimetru sítě. Problémem je, že mnoho útoků dokáže využít nedostatky v protokolech, které mají prostupovat vstupním firewallem a maskovat útok do užitečného provozu. Často jsou rovněž zneužívány „vystavené“ webové servery, na kterých si útočník připraví základnu pro další útoky. Navíc firewall v perimetru nedokáže zabránit útokům z vnitřní části sítě a zavlečeným virům, jak ukazují nedávná hromadná rozšíření červů Slammer nebo Blaster ve velkých organizacích.

4.6.4. UnityOne jako komplexní bezpečnostní řešení podnikové sítě

TippingPoint UnityOne je unikátní bezpečnostní produkt, schopný blokovat kybernetické narušení podnikové sítě ještě před tím, než útok nakazí, poškodí nebo zničí páteřní IT infrastrukturu. V současné době systémy UnityOne filtruje přes 2000 druhů virů, červů, trojských koní, hybridních útoků, datových a statistických anomálií, DoS a DDoS útoků a chrání jednotlivé části podnikové infrastruktury. Navíc umožňuje chránit výkon sítě řízením aplikací typu Peer to Peer nebo omezením Spyware.

UnityOne patří k síťovým IPS systémům (Systém prevence vniknutí, Intrusion Prevention System), který se vřazuje do datové cesty (In-Line), aby odfiltroval škodlivý provoz. Jakmile IPS systém detekuje škodlivý paket, zapíše jej do logu a zahodí tento paket a všechny následující pakety datového toku, náležející k škodlivému paketu. Díky tomu UnityOne odstraní z datového toku například všechny součásti probíhajícího Denial Of Service útoku, aniž by měl jakýkoliv vliv na probíhající užitečnou datovou komunikaci.

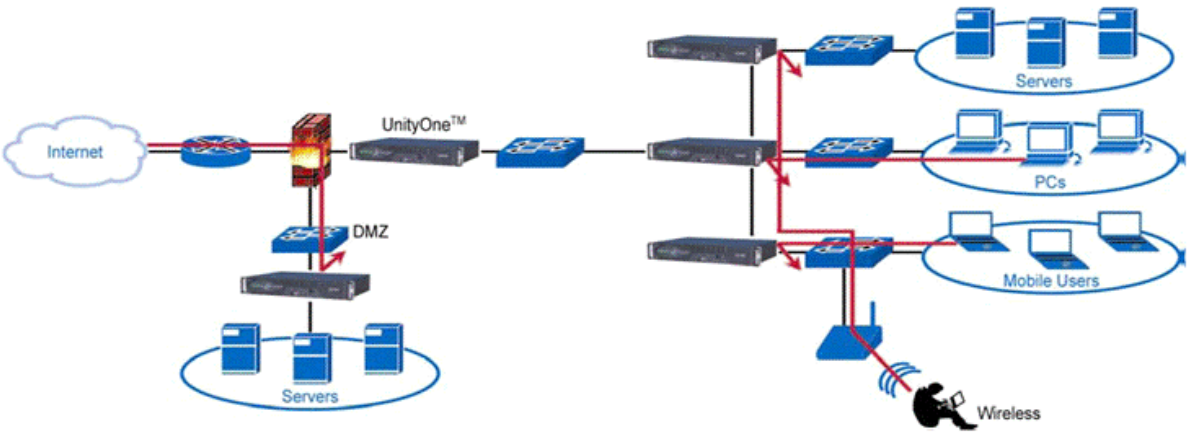
Zde je významný rozdíl oproti IDS systémům (Systém pro detekci vniknutí, Intrusion Detection System), které nebezpečný provoz pouze detekují, ale neodstraní jej z datového toku. UnityOne provádí kompletní inspekci paketů až po sedmou (aplikační) vrstvu a čistí internetový nebo intranetový provoz od virů, červů, trojských koní, chrání vnitřní sít před

[23] Z roku 2005

útoky typu DoS (Denial of Service), DDoS (Distributed Denial of Service), před útoky využívajícími otevřených zadních vrátek, škodlivými aplikacemi kradoucími pásmo i před různými smíšenými útoky. UnityOne lze nasadit jako univerzální síťovou záplatu, která umožní oddálit nebo úplně nahradit instalaci záplat na jednotlivé stanice a servery s náročným testováním kompatibility aplikací, protože UnityOne probíhající útok na servery či stanice z datového toku odstraní. UnityOne chrání síťovou infrastrukturu blokováním útoků proti směrovačům, přepínačům, DNS serverům a dalším.

UnityOne IPS s unikátním paralelním zpracováním filtrů disponuje vynikajícími výkonovými parametry s minimálním zpožděním, které umožňuje in-line nasazení. Díky tomu je možné jej použít nejen v perimetru sítě, ale je vhodný k ochraně serverů a síťových zdrojů na výkonných linkách, k oddělení skupin uživatelů, WAN, vzdálených uživatelů nebo bezdrátových uživatelů.

UnityOne kromě IPS funkcí slouží k ochraně aplikací a operačních systémů, síťové infrastruktury a výkonu. [24]



22 Příklad zapojení IPS

Zdroj: Jaroslav Babický, prezentace Bezpečné konvergované sítě

4.7. Penetrační test

Penetrační test je reálný útok prováděný téměř vždy externí firmou, jako zhodnocení bezpečnosti daného prostředí. Důrazně se doporučuje využít služeb externí firmy z důvodu snahy o maximální přiblížení reálnému útoku bez znalosti prostředí. Penetrační

[24] Babický, Jaroslav, přednáška Bezpečné konvergované sítě

test obvykle probíhá ve dvou fázích, testování možnosti průniku zevnitř a testování možnosti průniku zvenčí.

4.7.1. Posouzení zranitelných míst a možností průniku zevnitř

Podle nedávné studie americké FBI stojí uživatelé a procesy vevnitř vlastní sítě dnešních podniků za více než 60 procenty bezpečnostních hrozeb. Tyto hrozby jsou důsledkem nesprávné konfigurace síťových zařízení, chybějících účinných bezpečnostních postupů, a také provozu neaktualizovaného (nezáplatovaného, neopraveného) a zastaralého softwaru. Každý bezpečnostní konzultant musí být schopen uvedené hrozby rozpoznat a stanovit tak míru rizika úmyslných i náhodných hrozeb, jimž je síť vystavena.[25]

Metodologie posuzování

- Zjistit základní informace o testovaném prostředí
- Zmapování prostředí sítě (topologie sítě, fyzické rozložení sítě)
- Zjistit veškeré veřejně dostupné informace o podnikové síti
- Provést zkoumání a prohledání síťových aplikací
- Provést detekci otisku operačních systémů a zranitelných míst
- Charakterizovat vzorky síťového provozu a datových toků
- Detekovat veškeré potencionální slabé systémy zabezpečení (např. slabá hesla)
- Detekovat nezabezpečené bezdrátové sítě
- Analýza zranitelných míst pomocí vlastních a veřejných nástrojů
- Vyloučení falešných poplachů
- Ruční kontrola zranitelných míst
- Posouzení vnitřních bezpečnostních postupů
- Analýza zjištěných skutečností, jejich zpracování a doporučení pro zvýšení bezpečnosti

4.7.2. Posouzení zranitelných míst a možností průniku zvenčí

V organizacích stále roste potřeba využití veřejného Internetu pro komunikaci s obchodními partnery, připojení vzdálených poboček nebo připojení vzdálených uživatelů k podnikové síti. Proto se zvyšuje riziko útoku zvenčí (z Internetu). Rizika se dále zvyšují

[25] Thomas, M. Thomas, Zabezpečení počítačových sítí; str. 284

při nevhodné konfiguraci směrovačů a firewallů, nebo provozování neaktuálních a nezabezpečených aplikací.

Metodologie posuzování je obdobná jako u testování průniku zevnitř, ale s tím rozdílem, že při testu monitorujeme, zkoumáme a testujeme síťový provoz jako útočník bez znalosti prostředí testované počítačové sítě. K tomu využijeme nástroje, které jsou snadno dostupné na internetu.

Závěr a doporučení

Názory na zabezpečení podnikových počítačových sítí se liší podle úhlu pohledu. Správce sítě by nejraději prosadil paranoidní bezpečnostní politiku, uživatel se diví, proč dostal e-mail od kamaráda bez přílohy a finanční manažeři požadují „aby to stálo co nejméně“. Reálné prostředí většiny organizací je kompromis všech třech pohledů.

Implementace bezpečné počítačové sítě je náročný proces, který vyžaduje maximální koordinaci správců sítí, vedení společnosti, ale i uživatelů. Na trhu je mnoho publikací zabývajících se touto problematikou. Český normalizační institut vydává soubory norem, různá nakladatelství nabízí knihy s touto tématikou a záleží na konkrétní organizaci, jaká opatření zavede pro zvýšení bezpečnosti podnikové sítě. Např. některé státní instituce provozují vnitřní síť, která je naprosto oddělena (fyzicky) od okolního světa. Provozují pouze lokální síť bez připojení k Internetu, přístup osob je přísně kontrolován a je prakticky nemožné odnést citlivá data. Takové zajištění je pro většinu organizací nemyslitelné. Potřebují komunikovat s obchodními partnery, po jejich budovách je volný pohyb osob a jejich zaměstnanci se připojují do podnikové sítě přes veřejnou síť.

Dnešní počítačové sítě jsou převážně provozovány na sítích typu Ethernet a protokolu IP. Proto jsem se i já zaměřil na bezpečnost sítí provozovaných převážně na IP.

V práci jsem podrobně popsal zásady bezpečného přihlašování do sítě, práce s hesly a zabezpečení sítě proti útokům z Internetu. Zásady používání hesel je stálé téma a mnoho uživatelů se dopouští zásadních chyb. Jsou známy případy, kdy uživatel si heslo napíše na kousek papíru a ten schová pod klávesnici. Řízení přístupu k síti je stále dokonalejší a pomocí moderních nástrojů, jako je např. dvoufaktorová autentikace a použití biometrických prvků, se snižuje nebezpečí neoprávněného přístupu.

Další tématikou, kterou se v práci zabývám, je ochrana před útokem z Internetu a škodlivost programového kódu. Tyto potencionální hrozby spolu úzce souvisí a záleží na bezpečnostní politice dané organizace, jaké implementuje opatření. V současnosti existuje několik tisíc různých virů, červů, trojanů a také jsou na Internetu velmi snadno dostupné řady nástrojů pro potencionální útočníky (stačí zadat do vyhledávače správná klíčová slova). Bránit se proti nim může být velice obtížně, ale na trhu je množství nástrojů, které tyto hrozby minimalizují. Pro podnikové sítě to jsou např. hardwarové zařízení, která zajišťují ochranu proti škodlivým programům a útočníkům.

V poslední kapitole jsem se věnoval pojmům „Bezpečnostní audit“ a „Penetrační test“. Názory na tyto dva pojmy se rozcházejí, někdo považuje oba pojmy za stejnou činnost, jiný tvrdí opak. Zcela úmyslně jsem popis bezpečnostního auditu dal na začátek kapitoly a penetrační test na konec. Obě metody spolu souvisí a je důležité, aby organizace pravidelně prováděly obě metody. To co neodhalí bezpečnostní audit, odhalí penetrační test a naopak.

V této práci jsem se nezabýval problematikou zálohování dat, řešení poruch zařízení, fyzická kontrola osob, ochrana proti živelným pohromám, oddělení vývoje, management sítě a další činnosti, které souvisí s provozem bezpečné počítačové sítě.

Seznam použité literatury

1. Babický, Jaroslav, přednáška Bezpečné konvergované sítě, 2006
2. Beneš, Vladimír, Technická infrastruktura a síťové technologie, skripta BIVS, ISBN-80-7265-063-7, 2005
3. Feibel, Werner, Encyklopedie počítačových sítí, Computer Press, ISBN-80-85896-67-2, 1996
4. Gála, Libor; Pour, Jan; Toman, Prokop, Podniková informatika, Grada, ISBN-80-247-1278-4, 2006
5. Gert, De Laet; Gert, Schauwers, Network Security Fundamentals, Cisco press, ISBN-1-58705-167-2, 2004
6. Hák, Igor, Moderní počítačové viry, 2005. Dostupné na www.viry.cz
7. Vogeltanz, Antonín, přednášky k předmětu Bezpečnost podnikání a ochrana dat, 2007
8. Hanáček, Petr; Staudek, Jan, Bezpečnost informačních systémů, 2000, dostupné na www.micr,cz
9. Hanáček, Petr; Staudek, Jan, Bezpečnost informačních systémů – příloha č.2, standardy a doporučemí, v.08-2005, , dostupné na www.micr,cz
10. Nader, F. Mir, Computer and Communication Network, Prentice Hall, ISBN-0-13-174799-1, 2006
11. Pužmanová, Rita: Moderní komunikační sítě od A do Z, Computer Press, ISBN-80-251-1278-0, 2006.
12. Schatt, Stan, Počítačové sítě LAN od A do Z, Grada, ISBN-80-85623-76-5, 1994
13. Wendell, Odom, Computer Networking first-step, Cisco Press, ISBN-1-58720-101-1, 2004
14. Thomas, M. Thomas, Zabezpečení počítačových sítí, Computer Press, ISBN-80-251-0417-6, 2005

Internetové zdroje:

15. www.3COM.com
16. www.abclinuxu.cz
17. www.cisco.com
18. www.cni.cz
19. www.cs.wikipedia.org

20. www.earchiv.cz
21. www.en.wikipedia.org
22. www.hoax.cz
23. www.ieee802.org
24. www.micr.cz
25. www.pretec.com
26. www.rfc-editor.org
27. www.rsa.com
28. www.spammer.cz
29. www.spyware.cz
30. www.svetsiti.cz
31. www.symantec.com
32. www.viry.cz
33. www.virovyradar.cz

Seznam obrázků