mr LUKAS

Kapitán Ing. Ivo L u k á š

Ochrana dat v síti intranet

Celosvětová počítačová síť Internet dnes propojuje miliony počítačů. Služeb této sítě využívají desítky milionů lidí z celého světa. Internet nabízí svým uživatelům nepřeberné množství informací ze všech možných oblastí lidského života a velké množství služeb. Svoji nezastupitelnou úlohu si tato světová síť vydobyla i v moderních armádách západních zemí, kde plní úkoly získávání nových informací a vzájemné komunikace. I v AČR je možné se na některých pracovištích s Internetem setkat a do budoucna lze doufat, že počet těchto pracovišť se bude dále zvyšovat.

* * *

Jako v každé jiné společnosti lidí, tak i v Internetu je možné nalézt osoby, jejichž cílem není přispět k vzájemné informovanosti, ale poškozovat a ničit práci někoho jiného. Přitom se může jednat buď o jakousi formu vandalismu, která není ani mnohdy cíleně zaměřena proti konkrétnímu uživateli či skupině uživatelů, nebo může jít rovněž o cílevědomou činnost s úmyslem poškodit data nebo je změnit, s cílem obohatit se, případně neoprávněně získat informace. Obohacení prostřednictvím počítačové sítě se někdy nazývá elektronickou krádeží a tato činnost je povětšinou zaměřena proti finančním institucím (např. banky, pojišťovny, investiční fondy). Armádu více zajímá druhá skupina nelegálních činností, což jsou pokusy o neoprávněné získávání jinak chráněných nebo utajovaných dat.

Příčiny možného ohrožení

V Internetu spolu komunikuje obrovské množství počítačů, které přitom pracují na zcela odlišných (jak technických, tak programových) platformách. Z hlediska Internetu je zcela lhostejné, zdali uživatel pracuje s PC, *Apple*, nebo grafickou stanicí vybavenou procesorem RISC. Není podstatné, jaký používá operační systém a jaké programy pro přístup do Internetu. U počítačů ve funkci zdrojů dat (serverů) je situace obdobná a uživatel netuší, zdali je připojen k serveru s operačním systémem Unix, Windows NT nebo jiným, a ani to vědět nemusí. Tohoto souladu mezi různými systémy je dosahováno použitím jednotných komunikačních protokolů a standardů pro výměnu dat.

Nedávno tak vznikl nápad použít stejnou techniku i pro vzájemnou komunikaci ve vnitřních datových sítích, případně na této myšlence postavit celý nebo část podnikového informačního systému. Způsob propojení počítačů s cílem vzájemné vnitropodnikové komunikace, založený na využití technologie Internetu, dostal název **intranet**.

Proč je intranet tak lákavý pro komerční organizace i pro armádu? Výhoda a současně nevýhoda soudobých informačních systémů používaných v podnicích a organizacích spočívá v tom, že většina počítačových programů pro tyto systémy nebo pro lokální zdroje informací je psána na zakázku, na míru konkrétnímu uživateli. Takové systémy většinou dobře plní svoji úlohu, ovšem mimo to, že jejich výstavba je velmi nákladná, velmi těžko se upravují a uzpůsobují měnícím se organizačním podmínkám a většinou nejsou

kompatibilní se svým okolím. Nelze tak využívat dnes tolik potřebnou výměnu dat s okolními systémy. Důvodů pro výstavbu informačního systému technologií Internetu je více, mezi nejvýznamnější patří:

- **Jednoduchá implementace.** Technologie Internetu, kdy spolu komunikuje velké množství počítačů a jejich uživatelů na obrovské vzdálenosti, je dobře zvládnutá, jednoduchá a velmi snadno dostupná.
- **Levné řešení.** Technologie je obecná a nevyžaduje vytváření speciálních a velmi nákladných projektů a programů psaných na zakázku. Ve většině případů stačí nasadit rozšířené univerzální nástroje.
- **Moderní a otevřené řešení.** Internet zaznamenává v posledních měsících rychlý vývoj. Všechny změny, nová řešení a zajímavé nové nebo zlepšené služby lze prakticky okamžitě nasadit i v intranetu. Tím lze i ve vnitřní síti držet krok se světovým vývojem. Navíc je intranet dostatečně pružný a je možné jej snadno uzpůsobovat měnící se organizaci.
- **Jednoduchá práce uživatelů.** Programy pro nejrozšířenější službu WWW (*World Wide Web*) jsou intuitivní a velmi jednoduché na ovládání, což se příznivě odráží na nákladech nutných pro školení uživatelů. Ti navíc pracují stejným způsobem v intranetu i v Internetu.
- **Různé způsoby zapojení uživatelů.** Stejně jako v Internetu, i v intranetu mohou být jednotliví uživatelé připojeni několika možnými způsoby. Jedná se především o propojení lokální počítačovou sítí, modemem nebo mobilní sítí GSM.
- **Možnost jednoduchého připojení do Internetu.** Tato jednoduchost je daná použitím stejné technologie, stejných přenosových protokolů a standardů pro výměnu dat. Jednoduchým se tak stává nejen připojení do Internetu, ale i několika vzdálených segmentů intranetu vzájemně mezi sebou.

Pro armádu je použití intranetu zajímavé kromě již zmíněných předností také možností připojení uživatelů bezdrátovými síťovými prvky nebo bezdrátovými modemy bez změny stylu práce uživatelů. Tento způsob je vhodný např. pro polní místa velení, kdy není nutné rozvinovat kabeláž. Velmi perspektivním se jeví způsob připojení prostřednictvím sítě mobilních telefonů GSM, používajících digitální přenos s modulací TDMA (*Time Division Multiple Access)* v pásmu 890 až 960 MHz. Firma Eurotel oficiálně zahájila datový provoz ve své síti GSM na podzim roku 1996, ohledně firmy Radiomobil tato služba pracuje již od počátku. V případě využití této možnosti je tak možné z kteréhokoli místa pokrytého signálem nejen telefonovat, ale i faxovat, přenášet data a být ve spojení se svým informačním systémem i na místech, kde není dosud rozvinuté žádné jiné spojení, dokonce za jízdy nebo letu uživatele. Spojení přenosného telefonu s počítačem je realizováno speciální kartou PCMCIA, což je standard pro notebooky a vlastní přenos dat probíhá rychlostí 9600 b/s. Telefon je ovládán dálkově programem z počítače a stejným způsobem lze i faxovat.

Neoprávněné průniky zvenčí do intranetu lze očekávat ze tří hlavních směrů:

- **Z Internetu.** Protože intranet i Internet je postaven na stejné technologii, je velmi jednoduché obě sítě propojit, což se také ve většině případů stává. Organizace tím získává přístup do Internetu pro své zaměstnance, možnost prezentace před celým světem, řešení propojení vzdálených segmentů intranetu a celou paletu služeb Internetu.

Vzniká však reálné nebezpečí možného neoprávněného průniku zvenčí, neboť technologie je obecně známá.

- **Použitím Internetu** pro přenos soukromých, důvěrných nebo utajovaných informací. Toto nebezpečí je charakteristické při propojení několika vzdálených segmentů intranetu Internetem. Protože mezi dvěma sítěmi intranetu je zařazeno několik (někdy i velký počet) uzlů, je možné po celou trasu procházející data v těchto uzlech číst, zadržovat a po modifikaci je zasílat dál.
- **Využitím bezdrátových prvků** a z toho vyplývajících možností odposlechu rádiových kmitočtů těchto bezdrátových zařízení nebo mobilních telefonů. Obdobný odposlech je možný i z kabelů použitých pro počítačovou síť. Tuto kategorii možného nebezpečí není třeba uvažovat, protože je „slabší" nežli předcházející, a to ze dvou důvodů: odposlechem je možné procházející data většinou pouze číst bez možnosti modifikace, navíc dosti obtížně a metody ochrany uplatněné pro předcházející kategorii plně pokryje i nebezpečí možného odposlechu.

Ochrana dat při použití nechráněných přenosových tras

Ačkoli intranet a Internet používají stejnou technologii, nejsou tyto sítě stejné a z bezpečnostních hledisek by ani stejné být neměly. Jedná se především o rozdíly v použitém prostředí. Nejznámější a nejdůležitější rozdíly jsou uvedeny v následující tabulce:

intranet	Internet
Počet uživatelů je známý.	Počet uživatelů je obrovský.
Všichni uživatelé jsou prověřováni při přihlášení do systému.	Uživatelé jsou ve většině přístupů neznámí (anonymní).
Správce sítě udržuje aktuální informace o uživatelích.	Nemá centrální správu pro přístup a zabezpečení.
Při výstavbě se volí model centrální správy s řízením přístupu.	Distribuovaná síť postavená na různých technických i programových platformách.
Při výstavbě se věnuje část investic na technologie zabezpečení.	Používá nové a rychle se vyvíjející technologie.

I přes tyto odlišnosti láká přímé propojení intranetu s Internetem, přístup z podnikové sítě do Internetu, umožnění přístupu z Internetu do podnikových sítí a propojení segmentů intranetu Internetem stále více.

K zabezpečení přenosových tras přes veřejnou síť Internet se nejčastěji používá šifrování pomocí veřejných klíčů a technika digitálních podpisů. Těchto technik kryptografie se užívá s cílem:

- zajištění bezpečné komunikace, neboť Internet není důvěryhodné médium,
- zašifrování důležitých souborů tak, aby se staly nesrozumitelné pro narušitele,
- zajištění integrity dat a utajení,
- ověření původu dat a zpráv.

Šifrování pomocí veřejných klíčů

Kryptografie s veřejným klíčem (na rozdíl od kryptografie se symetrickým klíčem) je založena na jednocestných funkcích, které se snadno vypočítají, ale obtížně invertují nebo reverzují bez určitých znalostí. Implementují se zde jednocestné funkce použitím dvou odlišných klíčů, které jsou ve vzájemné relaci a jsou vytvořené současně. Pro šifrování přenášených zpráv se nejprve užije veřejný klíč. Takto zakódovanou zprávu lze přenášet, k jejímu dešifrování je však zapotřebí znalosti soukromého klíče. Soukromý klíč je jedinou součástí, která musí být skutečně držena v tajnosti. Algoritmus, velikosti klíčů a formáty souborů mohou být veřejně známé bez ohrožení úrovně bezpečnosti.

Digitální podpisy

Technika digitálních podpisů se používá v případě, že příjemce potřebuje ověřit, zda zpráva, kterou obdržel:

- přichází skutečně od očekávaného odesílatele,
- nebyla cestou, poté co ji odesílatel vyslal, změněna.

Pod pojmem zpráva je nutné rozumět jakýkoliv zasílaný soubor dat. Např. při zasílání software tak lze jednoduše zjistit, že doručené programy pochází skutečně od jejich výrobce a že nebyly v průběhu svého přenosu doplněny viry. Doplněním podpisu se zpráva nemění, pouze se generuje příslušný řetězec podpisu, který lze spojit se správou, nebo jej přenést odděleně.

Digitální podpisy se rovněž šifrují technikou veřejných klíčů, ovšem ke generaci podpisu se použije soukromý klíč a k jeho ověření klíč veřejný.

Certifikáty

Certifikáty jsou v podstatě podepsané dokumenty, které zajišťují souhlas veřejných klíčů s dalšími informacemi (jméno, adresa ...). Certifikáty vydávají a podepisují certifikační autority, což je třetí strana požívající všeobecnou důvěru, která ověřuje souhlas veřejných klíčů s identitou, adresou nebo přístupovými právy.

Přínos certifikátů spočívá ve velmi snadné distribuci veřejných klíčů přímo Internetem. Pokud dva uživatelé věří stejné certifikační autoritě, mohou si zjistit vzájemně veřejné klíče. Tyto klíče pak mohou použít k šifrování vyměňovaných dat a k ověřování podpisů.

Certifikáty mají omezenou dobu platnosti, což je jejich velmi důležitá vlastnost, neboť existuje možnost objevení mezer v algoritmech nebo protokolech. Certifikáty je také možné zrušit, což je důležité např. v případě zneužití soukromého klíče. Certifikát, jemuž prošla doba platnosti nebo byl zrušen, se vloží do seznamu zrušených certifikátů. Každý uživatel, který používá certifikát, může zkontrolovat pomocí tohoto seznamu platnost certifikátu.

Ochrana proti průnikům z Internetu

V souvislosti s ochranou intranetu proti průnikům z Internetu je možné se nejčastěji setkat s pojmem *firewall*. Firewall je počítačový systém, který realizuje administrátorem definovaná bezpečnostní pravidla při propojení sítí a představuje hraniční kontrolu dvou sítí (intranetu a Internetu). Firewall může určit, zda provoz na hranici dvou sítí je přípustný, zda splňuje bezpečnostní pravidla. Je koncipován tak, aby chránil sebe i celou interní síť

proti neautorizované interaktivní práci. Firewall je však účinný pouze tehdy, je-li součástí ucelené bezpečnostní architektury.

Firewall, jenž pracuje na nízké úrovni, kontroluje každý procházející datový paket a rozhoduje, který propustí na základě administrátorem systému stanovené tabulky přípustných adres.

Firewall, pracující na aplikační úrovni, nepřipouští žádný přímý provoz mezi sítěmi, které propojuje, ale vede záznamy o komunikaci, jež zprostředkoval. Tuto komunikaci zajišťují **proxy servery**, což jsou programové součásti firewallu, „rozumějící" použitému aplikačnímu protokolu. S využitím tohoto přístupu lze definovat možná oprávnění mnohem podrobněji. Proxy servery jsou navíc doplněny o uživatelskou identifikaci, a proto lze jednotlivým uživatelům přesně definovat, které služby sítě mohou využívat a které jim zůstanou nepřístupné. Mohou také obsahovat kontrolu na aplikační úrovni, a tak zabránit přenosu dat, jenž by mohl být nebezpečný.

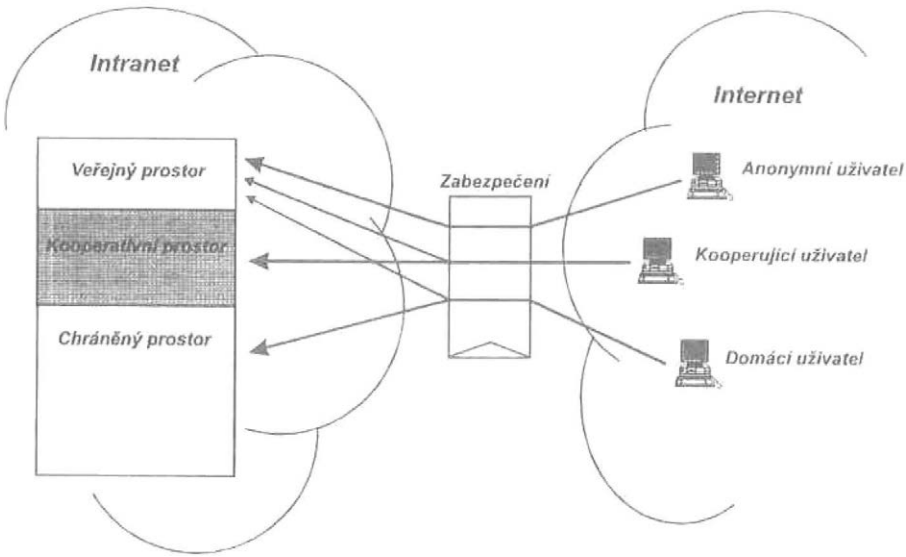
Prakticky je možné firewall provozovat na výkonnějším počítači vybaveném dvěma síťovými kartami a příslušným programovým vybavením. Jedna ze síťových karet je připojena do vnitřní sítě a je považována za „bezpečnou". Druhá je připojena do Internetu a je jí přidělena řádná adresa podle konvencí Internetu. Mnohé programy realizující tuto ochranu lze nastavit tak, aby veškerá komunikace směrem ven probíhala šifrovaně, a tím lze stavět virtuální bezpečné sítě, kde jsou eliminovány problémy při přenosu citlivých nebo utajovaných dat.

Mnozí správci informačních systémů pociťují tlaky ohledně umožnění několika úrovňového přístupu do vnitřní sítě z Internetu pro různé skupiny uživatelů - s jinými právy pro domácí uživatele přistupující zvenčí ke svým datům, s jinými právy pro uživatele spolupracujících organizací pro vytvoření společné platformy a s omezenými právy ostatních (anonymních) uživatelů. **V rámci datového prostoru intranetu lze vyhradit tzv. kooperativní prostor, kam mají přístup spolupracující složky,** a to nejen pro čtení dat, ale i pro zapisování, popř. jejich modifikaci. **V případě armády by to mohla být státní správa, policie, CO, záchranná služba** apod. Přínos spočívá v možnostech širší a pružnější spolupráce s těmito složkami a poskytování rychlejších a adresnějších služeb. V případě komerčního nasazení přibývají výhody nižších nákladů, zlepšení distribuce, lepší služby zákazníkům apod. Při spojování intranetu s Internetem se obvykle vytváří několik samostatných skupin, kterým se přidělují příslušná práva.

Systém zabezpečení by měl vést k takovému cílovému stavu, aby každá skupina uživatelů měla přístup k datovému prostoru, který je pro ni určen, a k veřejnému datovému prostoru, ke kterému mají přístup všichni uživatelé, včetně neregistrovaných, tak jak je znázorněno **na schématu.**

Při takovém propojení však mohou vzniknout v současné době problémy, neboť nástroje zabezpečení nejsou dosud zcela zralé a je velmi obtížné vytvořit úplné řešení pokrývající komplexně celou problematiku. Výsledkem jsou různé zabezpečovací systémy založené na:

- firewall,
- proxy serverech,
- vyžadování hesel,
- upravenému řízení přístupu.



Schéma

V případě přístupu do vnitřní sítě z Internetu je z bezpečnostních důvodů třeba zabezpečit:

* **udržení přehledu** o tom, kteří uživatelé zevnitř (tj. vlastní organizace) a kteří uživatelé zvenčí (z Internetu) mají přístup k vnitřním zdrojům, k jakým a s jakými právy;
* **ověření uživatele** ke zjištění jeho identity; znamená to, že při každém přihlášení uživatele jej může přístupový server identifikovat, což se děje většinou na základě zadání jména a hesla v kombinaci s kontrolou přípustného rozsahu síťových adres, odkud je vznesen požadavek;
* **řízení přístupu** v rozsahu běžném pro přístupové servery lokálních sítí, kdy se určuje, do jaké části intranetu má uživatel přístup a s jakými právy;
* **certifikáty** potřebné k autentizaci uživatele a k řízení přístupu;
* **podepisování programového kódu** - toto podepisování se používá při kooperaci ve vývoji software nebo aktualizaci programového vybavení od spolupracujícího dodavatele; zjišťuje se, zda programový kód skutečně pochází od konkrétního dodavatele a neporušenost tohoto kódu;
* **bezpečný přenos dat**, pro který se používá šifrování, tedy k zajištění důvěryhodnosti citlivých dat a k bezpečnému přenosu plateb.

Cílem všech přijímaných opatření by mělo být prostředí vytvořené souběhem veřejných a vnitřních sítí. Toto prostředí by mělo být místem, kde mohou být systémy rozšiřovány k využívání nových přístupů při současné ochraně investic do stávajících systémů.

Prostředí se musí chovat jako inteligentní, bezpečná síť k šíření aplikací mezi podniky. Taková síť pak musí zajišťovat:

- bezpečnou výměnu informací,
- bezpečné provádění transakcí,
- způsob řízení přístupu k obsahu,
- distribuovanou technologii ověřování, založenou na heslech.

Jaké standardní techniky budou přijaty pro ochranu intranetových sítí? Velmi záleží na tom, jak se k tomuto problému postaví velcí výrobci software. Gigant mezi těmito firmami, Microsoft, hodlá zabezpečení vnitřních sítí podporovat svým produktem *Internet Security Framework*. Filozofií tohoto produktu je dosáhnout výše uvedených cílů použitím nejlepších existujících technologií jako platformy s možností jejich rozšiřování, umožňující zahrnout i nově vznikající technologie. Poskytuje tak základní kostru pro bezpečné on-line komunikace. Zjišťování identity, ověřování a autorizace se provádí technikou veřejných klíčů a technologií založených na heslech. Tyto technologie mohou být za určitých okolností integrovány do operačních systémů Windows a Windows NT.

Základem produktu je rozhraní, které poskytuje funkce kryptografie a certifikace pro:

- ▲ výběr a využívání poskytovatelů kryptografických služeb,
- ▲ generaci a výměnu klíčů,
- ▲ šifrování a dešifrování dat,
- ▲ vzorkování, tvorbu a ověřování digitálních podpisů,
- ▲ generaci požadavků na vytvoření certifikátů,
- ▲ ukládání a načítání certifikátů,
- ▲ syntaktickou analýzu a ověřování certifikátů,
- ▲ kódování a dekódování certifikátů pro formáty „wire", jako je DER,
- ▲ abstrahování certifikátů do kryptografických zpráv, jako je formát PKCS #7.

Vrcholovou úrovní rozhraní je široká sada zabezpečovacích služeb a mechanismů vyšší úrovně. Patří mezi ně:

- ✦ zabezpečené komunikační kanály,
- ✦ prověřování totožnosti na základě certifikátů,
- ✦ prověřování totožnosti na základě hesel,
- ✦ podepisování programového kódu,
- ✦ protokol SET pro bezpečné transakce s kreditními kartami,
- ✦ Certificate Server k vydávání a rušení certifikátů,
- ✦ MS Wallet k ukládání osobních bezpečnostních informací, jako jsou klíče, certifikáty a informace o kreditních kartách,
- ✦ řízení přístupu,
- ✦ distribuovaná technologie prověřování totožnosti, založená na heslech, včetně integrace s protokoly Internetu.

Uvedené funkce budou dostupné přes prohlížecí program služby WWW - Internet Explorer na platformách Windows 95, Windows NT, Windows 3.1, počítačích Macintosh a UNIXu.

Z praktického uživatelského hlediska je možné s tímto produktem zajistit jediné přihlášení, kdy uživatelé potřebují jednu sadu dokladů pro získání přístupu ke klíčům a certifikátům. Dále se intranet a Internet jeví jako jediná síť, více systémů se jeví jako jediný systém a různé počítače se jeví jako jediný počítač.

* * *

Celosvětová počítačová síť Internet i vnitřní sítě intranet prožívají v posledních měsících obrovský rozvoj. Mimo jiné se tento vývoj týká i zabezpečujících prvků ochrany dat intranetu v případě jeho propojení do Internetu. Výše uvedený příklad produktu *Microsoft - Internet Security Framework* - naznačuje, jaké funkce pro zabezpečení lze očekávat v nejbližší budoucnosti a jeho možné využití v AČR při budování intranetu nebo při propojení existujících vnitřních sítí s Internetem pro bezpečnou výměnu informací v rámci rezortu nebo se spolupracujícími složkami.

Použito informací firmy Microsoft uveřejněných v Internetu.

Poslání NATO se podle mne často zužuje na domněnku, že je to vojenský pakt. Je to však vojensko-politické uskupení států, do něhož nevstupuje pouze Armáda ČR, ale celý stát. Musíme se proto ptát, co naše země nabízí tomuto společenství demokratických států. Domnívám se, že stabilizovanou demokracii, stabilizovanou politickou i sociální situaci. Můžeme prostě nabídnout hodnoty, které sdílejí členové Aliance.

Z rozhovoru s ministrem obrany ČR Miloslavem Výborným, Respekt 42/1996.