VI –Bezpečnost podnikové infrastruktury

3. 5. 2013 – VIKMA07 - IM

Potencionální nebezpečí

Formy ohrožení bezpečnosti: odposlech, modifikace přenášených dat, neoprávněný přístup do lokální sítě

Oblast ochrany:

- data (zajistit, aby je nemohl někdo získat, měnit či mazat)
- výpočetní kapacity jednotlivých uzlů v síti
- omezování funkčnosti či narušování provozu některých služeb

Formy útoku

Pasivní útoky

- „odposlouchávání “ dat - cílem získat nezveřejňované informace, které lze zneužít
- monitorování provozu - analýzy takto provozovaných kontaktů

Aktivní útoky

- modifikace dat
- vytváření falešných dat
- aktivním útokům nelze zcela zabránit, ale lze je na rozdíl od pasivních útoků snadněji detekovat

Rámcové oblasti zabezpečení podnikové sítě

- zajištění důvěrnosti dat - pomocí šifrování celého komunikačního kanálu nebo jen vybraných citlivých dat
- zajištění autentizace uživatelů sítě
- zajištění integrity dat
- zajištění neodmítnutelnosti zpráv - zajistit, aby odesílatel nemohl popřít odeslání zprávy a příjemce nemohl popřít přijetí zprávy
- přiřazování přístupových práv - cílem je omezit (a řídit) přístup k počítači, datům a aplikacím, součástí je identifikace a autentizace toho, kdo žádá o přístup
- zabezpečení dostupnosti síťových služeb - útokům na dostupnost služeb lze zabránit autentizací a šifrováním

HW útoky

fyzické útoky

- cílem je fyzické poškození síťového HW – přerušení kabeláže, vyřazení aktivních prvků, poškození HDD apod.
- záležitost zejména lokálních sítí LAN

rušení signálu

- pomocí silného elektromagnetického zářiče blízko síťových rozvodů
- narušení mikrovlnného spoje
- nemusí být úmyslné, o to hůře odhalitelné

HW útoky

odposlechy

- fyzické odposlechy (např. modemu nebo teoreticky i signálu v kabelu)
- SW odposlech Ethernetu – sdílené médium doručí signál každému, kdo je připojen; postačí přepnout kartu do tzv. promiskuitního režimu (přijímá všechna data, nejen ta, která jí patří); přepínače komplikují tuto možnost
- využívá se i při řešení problémů se sítí

SW útoky

pomocí chyb v programech

- **přetečení zásobníku (stack overflow)** – aplikace zapíše do paměti, kam normálně nemá přístup; vede k provedení útočníkova programu ochrana: aktualizace aplikace
- **backdoor** – přístup, který si vytvořil autor programu pro ladění aplikace; může později posloužit útočníkovi ochrana: může odhalit scanování

SW útoky

útoky proti WWW

- Rozšířená forma útoku
- Díky dostupnosti skriptovacích jazyků dnes web programuje „skoro každý“
- Často pouze orientace na funkčnost, nedostatečné zabezpečení

Podvržení identity

- IP spoofing – do odchozích paketů je vkládána falešná (cizí nebo podvržená) IP adresa
- source routing – varianta, útočník se vydává za důvěryhodný počítač, který předtím vyřadil pomocí DoS útoku

DoS (Denial of Service) útoky

- Cíl útoku je vyřazen z provozu často formou zahlcení
- Může jít pouze o součást útoku či jeho zamaskování

DoS útok pomocí nedokonalostí TCP/IP:

SYN flooding

- útočník zahájí navázání TCP spojení (pošle paket SYN)
- cíl potvrdí (SYN ACK) a alokuje pro otevírané spojení zdroje
- útočník ale nedokončí navázání spojení, místo toho zahajuje otevírání dalších a dalších spojení
- cíl postupně vyčerpá své zdroje a přestane přijímat žádosti o spojení od regulérních klientů

řešení: zkrátit dobu čekání na potvrzení navázaného spojení od klienta, alokovat pro ně zdroje až po potvrzení

DoS (Denial of Service) útoky

- **Land attack** – varianta SYN útoku, v žádosti o spojení je jako adresát i odesilatel uveden cílový stroj, ten se zahltí zasíláním potvrzení sám sobě
- **Smurf** – zahlcení cíle ICMP pakety (ping), jejich zpracování mívá někdy přednost před běžným provozem; útočník pošle žádost o ping všem (broadcast) a jako odesilatele uvede cíl útoku
- **DNS útok** – podobný předchozímu, jen místo ICMP používá DNS dotazy a odpovědi

DoS (Denial of Service) útoky

DoS pomocí chyb v implementaci IP

- **PingOfDeath** – odeslání příliš velkého paketu pomocí ping, nekontrolující příjemce se zhroutil
- **Teardrops** – využívá chyby při skládání fragmentovaných paketů (posílá nekorektní fragmenty)

DDoS – Distributed Denial of Service

- DoS útok vedený souběžně z mnoha stanic
- na nezabezpečené počítače je distribuován útočný program (označován jako zombie), např. virem
- v určitý čas útočník vzbudí zombie a pošle je současně na cíl
- mnoho různých variant, zejména v přístupu k synchronizaci zombie
- obtížně se blokuje – zdrojů je příliš mnoho

Útoky na servery DNS a směrovače

- **otrávení informace v cache** – ukládání falešných informací do paměti serveru vede k tomu, že útočník může přesměrovat provoz na server pod správou útočníka
- **změna dat** – útočníci mohou využít slabiny některých verzí a pro uživatele DNS pozměnit některá data
- **odmítnutí služby** – tento útok může znamenat problém v rámci celého internetu (nedostupnost)
- **únos domény** – útočníci mohou neoprávněně převzít registrační proces a tak unést legitimní domény

Útoky na servery DNS a směrovače

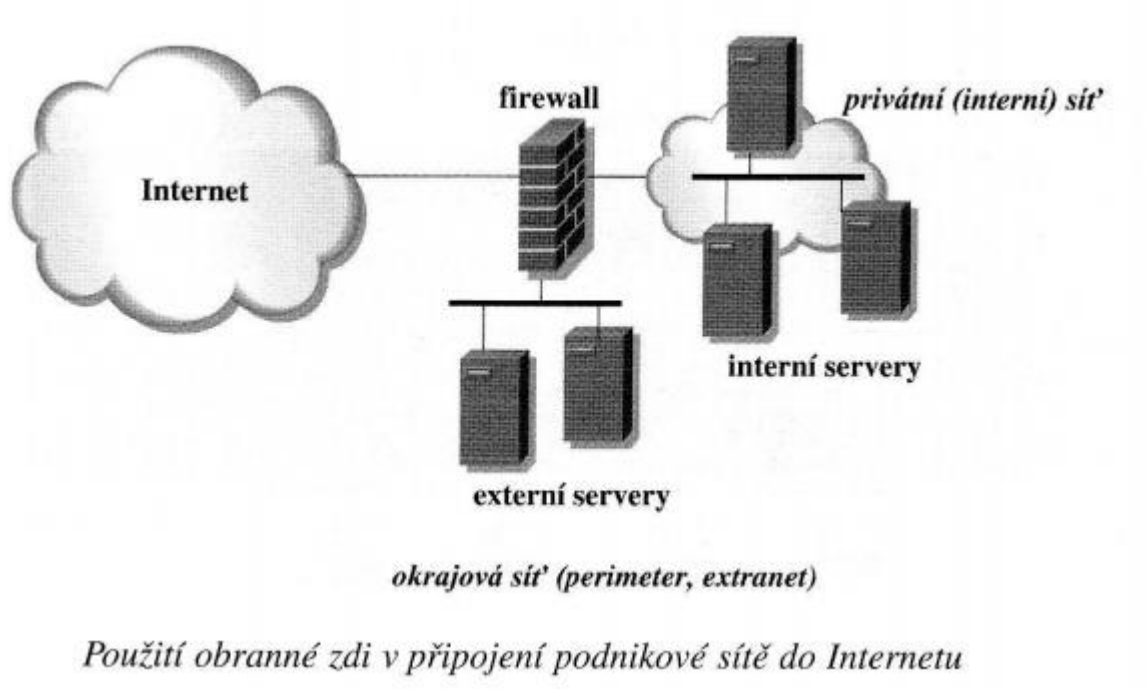
- Kromě DNS jsou častými cíly útoků směrovače. Pokud nejsou zabezpečeny proti útokům zvenčí představují pro útočníky potenciální platformu pro vedení útoku. Při realizaci směrování je nutné zvážit všechny požadavky zabezpečení jednotlivých směrovačů a použít prvky s vhodnou hardwarovou podporou zabezpečení.

Možná ochrana před útoky

- autentizace uživatelů sítě
- zabezpečení stanic – ochrana dat zbytku sítě (napadená stanice se stává nástrojem dalšího útoku)
- zabezpečení provozu – sledování provozu sítě, vnitřní filtrování; nejnebezpečnější útoky jsou zevnitř
- zabezpečení LAN – ochrana LAN před útoky z Internetu
- zabezpečení na úrovni poskytovatele

Firewall

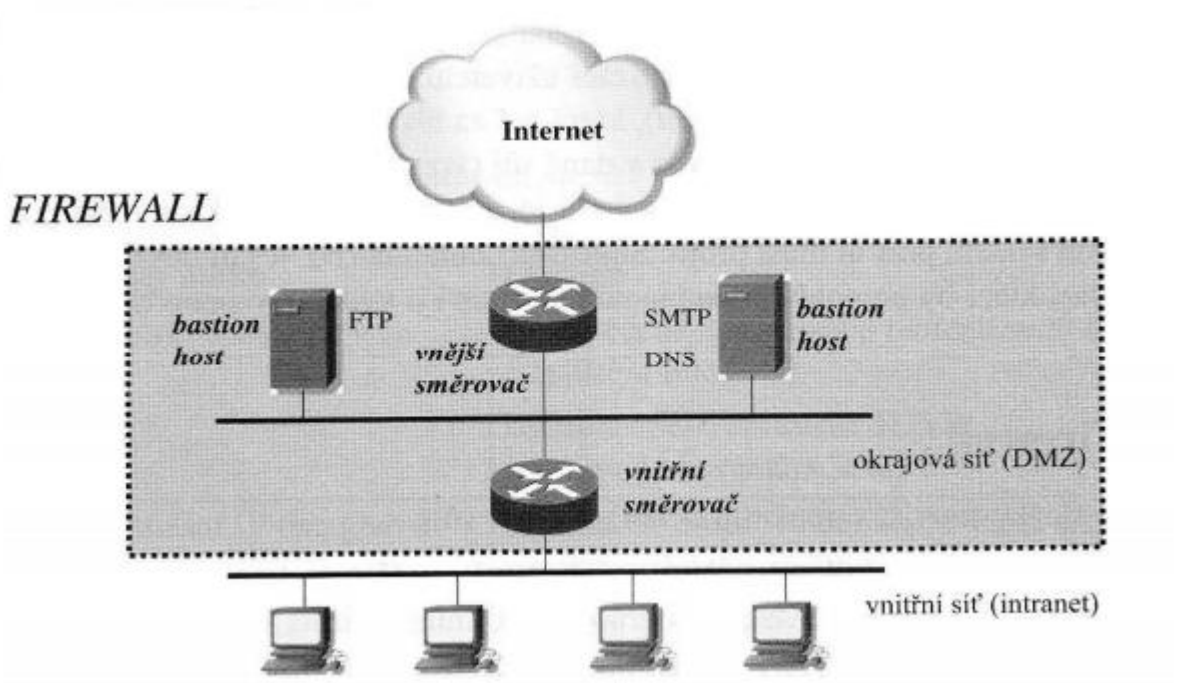
- Tvoří ho ochranné složky jak hardwarové, tak softwarové, které dohromady tvoří ochrannou zeď mezi Internetem a podnikovou sítí.



Použití obranné zdi v připojení podnikové sítě do Internetu

Firewall

- směrovače – mezi podnikovou sítí a vnějším světem filtrují provoz, minimalizují možnost vnějších útoků
- demilitarizovaná zóna – server nebo síť serverů přístupná zevnitř podnikové sítě i zvenku z Internetu – obsahuje potřebné servery WWW, SMTP, FTP a další.
- NAT – překlad síťových IP adres privátních na veřejné a opačně v závislosti na směru komunikace

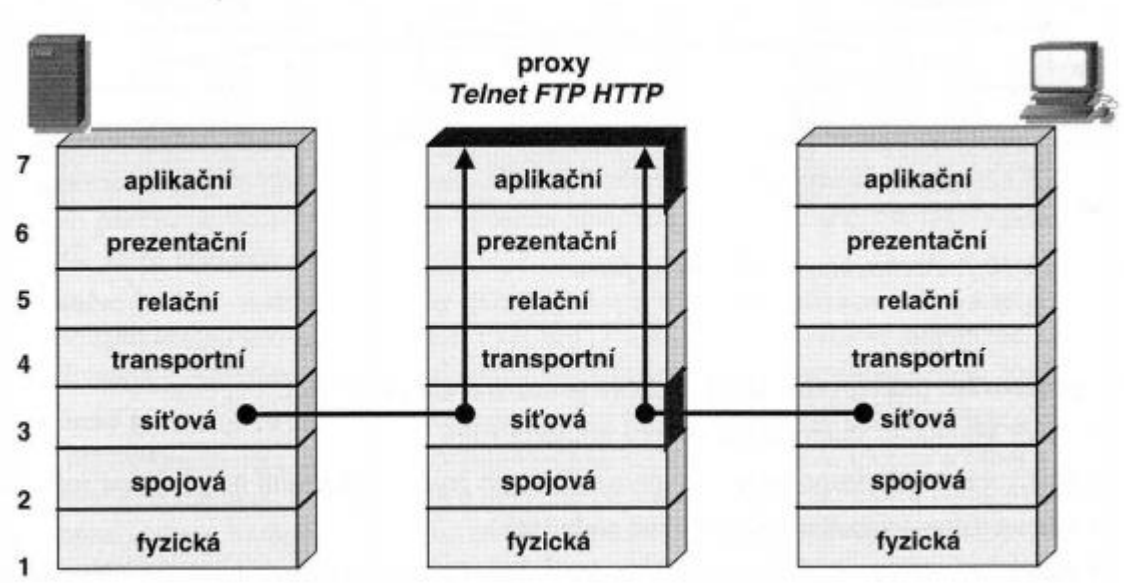


Funkce firewall

- **filtrace paketů** – na úrovni síťové vrstvy, na základě zdrojové a cílové IP adresy
- **aplikační brána** – zadržuje všechny pakety pro specifikované aplikace a chová se jako zástupný server (TELNET, FTP, SMTP…..), zjistí nejprve autentizaci zvnějšku a teprve potom povolí komunikaci se serverem v demilitarizované zóně
- **zástupný server** – (proxy), ověřuje pakety z hlediska platnosti dat na aplikační úrovni před otevřením spojení. Zástupné servery mohou také ověřovat hesla a požadavky na služby
- **řízení přístupu** – autentizační mechanismus pro ověření totožnosti uživatele na základě hesla a jeho autorizace pro užívání požadovaných služeb
- **šifrování zpráv** – zabezpečení přenosu informací (jmen, hesel, dat …)

Proxy

Druhá generace obranných zdí ve formě zástupných serverů dokáže využít filtrace na základě IP i na základě některých aplikací. Včlenění mezi klienta a server však značně zpomaluje komunikaci. Zástupný server stojí mezi klientem a reálným světem v síti. Klient vysílá požadavky směrem k cílovému serveru, ale požadavek se dostává k proxy. Ten požadavek zváží a rozhodne zda je oprávněný nebo ne a zda jej pošle k cíli.



Architektura zástupného serveru (proxy)

Řízení přístupu

Autentizace

- Je ověřování a potvrzování totožnosti uživatelů komunikujících stran. Autentizace může vést k jednoznačné identifikaci – kdo je?, nebo verifikaci – je ten, kdo tvrdí, že je? na základě zadaných údajů do autentizačního systému.

Možnosti ověření totožnosti:

- **kdo jsou** – jednoznačné ukazatel jako otisky prstů, dlaní atd., jsou sice jednoznačné ovšem velmi nákladné
- **co mají** – identifikace podle předmětů – karty, klíče atd., jednodušší možnost ověření, náchylnost ke ztrátám, krádežím …
- **co znají** – identifikace podle hesel, číselných kombinací, osobních identifikačních čísel atd.

Řízení přístupu

Autorizace

- Po úspěšné autentizaci může být udělena autorizace pro používání zdrojů a služeb. Autorizace specifikuje jaké operace se mohou prováděl a jaká data jsou dostupná

Účtování

- Zodpovídá za záznam všech činností uživatele v systému.