Infrastruktura podnikové sítě

Informační management VIKMA07

Mgr. Jan Matula, PhD.

jan.matula@fpf.slu.cz

VI. blok

IM a jeho role - ICT v podnikové infrastruktuře

- Řízení zdrojů ICT – pracovní náplň IM, vazba na ICT oddělení.
- Informatizace procesů v podniku s ohledem na aktuální možnosti a trendy v ICT.
- Akvizice HW & SW, implementace IS (EIZ, CRM, atd.).
- Správa dat, databází a datových toků.
- Zajištění komunikace (interní, externí).
- Webová prezentace organizace (nasazení, správa CMS)
- Optimalizace využití ICT = Konsolidace ICT (virtualizace, terminálový přístup, atd.)
- Zajištění bezpečnosti (širší problematika zahrnující el. podpisy, doménové certifikáty, vzdálené přístupy do sítě, zabezpečení dat)
- Archivace dat (v návaznosti na Spisový a skartační rejstřík)

Podniková síť

- aktivní prvky sítě & uzly
- protokoly sítě (TCP/IP, FTP, IMAP, POP3, SMTP, DHCP, DNS, WEBDAV, atd.)
- přenosová média (kabely, radiová bezdrátová komunikace, optická bezdrátová komunikace)
- platformy (OS) a jejich vzájemná kompatibilita – snaha o homogení prostředí.
- architektura sítě (klient-server), rozlehlost PAN, LAN, MAN, WAN, WLAN a topologie: sběrnicová, kruhová, hvězdicová, stromová.

Základní pojmy

- **Server** - služba nebo HW (aktuální verze SW - MS Win Server 2016, licencování zde).
- **Dedikovaný server** je fyzický server vyhrazený celý jedinému zákazníkovi a jeho webovým aplikacím, databázím a e-mailům. Na rozdíl od **tzv. virtuálního serveru** - kde sdílí jednu HW platformu s desítkami (někdy i stovkami) těchto virtualních serverů (nazývá se i "sdílený hosting").
- **Podniková doména** - podniková síť – databáze uživatelských účtů, skupin uživatelů, účty počítačů, informace o tiskárnách atd. (uzavřená síť – pro přístup se používá VPN)
- **Active Directory** - rozšiřitelná a škálovatelná adresářová služba, která umožňuje efektivně uspořádat síťové prostředky. Kromě informací o objektech v počítačové síti (uživatelské účty, počítače, tiskárny) umožňuje používat stromovou strukturu objektů, nastavovat globálně systémové politiky, instalovat programy na počítače nebo aplikovat kritické aktualizace v celé organizační struktuře.

Základní pojmy

- **Tenký klient** je počítač nebo počítačový program, který při plnění svého úkolu závisí na jiném počítači (na svém serveru). Thin client je "pouze" monitor a síťová karta (+ periferie) - veškeré výpočty probíhají na serveru.
- **Tlustý klient** v sobě obsahuje jak prezentační tak i aplikační vrstvu a připojuje se přímo k databázovému nebo jinému serveru. Zpravidla přes síť stahuje velký objem dat, která zpracuje a výsledek pak přenese zpět na server.

Základní pojmy

- **Chytrý klient** kombinuje výhody tenkého a tlustého klienta a potlačuje jejich nevýhody. Aby mohl pracovat offline, obsahuje určitou logiku a drží data, která se v okamžiku navázání spojení synchronizují.
- Využívá místní systémové zdroje jako je např. paměť, procesor a diskový prostor, ale může komunikovat a využívat i připojených zařízení. Stejně tak může využívat přítomnosti a funkcí, které nabízejí ostatní nainstalované aplikace např. MS Office.

Základní pojmy

- **Microsoft SQL Server 2016** je databázový a analytický systém, speciálně vyvinutý pro internetové obchody, datové sklady a další související byznys. SQL Server dokáže díky správě podnikových dat zvýšit efektivitu vaší firmy. Jeho vývoj započal roku 1985 firmami Microsoft a IBM. Více informací zde.

Základní pojmy

- **Microsoft Exchange Server (2016)** - slouží k výměně e-mailových zpráv a sdílení zdrojů. Tvoří jeden ze základů portfolia Microsoftu v oblasti nabídky firemních systémů. Mezi jeho hlavní vlastnosti patří příjem a odesílání poštovních zpráv, správa kalendáře a kontaktů, sdílení veřejných složek, možnost přístupu do poštovních schránek přes webové rozhraní, přístup k systému pomocí mobilních zařízení a vlastnost datového úložiště. Možnosti licencování zde.
- **Alternativní služby:** IBM Lotus Notes/Domino, Novell GroupWise, Kerio Connect

Základní pojmy

- **Microsoft SharePoint 2016** - SharePoint je platforma pro webové aplikace. Tato platforma v sobě spojuje různé funkce, které jsou tradičně oddělené aplikace: intranet, extranet, správa obsahu, správa dokumentů, osobní cloud, firemní sociální síť, firemní vyhledávání, správa pracovních postupů a firemní úložiště aplikací.
- SharePoint byl původně vyvíjen pro vnitrofiremní využití ve středně velkých firmách a velkých firemních odděleních ve spolupráci s Microsoft Exchange, Skype pro firmy a Office webovými aplikacemi. Office 365 rozšířily používání SharePointu i v menších organizacích. Bližší informace zde.

Základní pojmy

- **Hyper-V** je hypervizorově stavěný serverový systém. To znamená, že má svůj vlastní hlavní operační systém (Většinou Windows Server 2018 apod.) a pomocí virtualizace se skrze něj mohou spustit další operační systémy - vše v rámci jednoho fyzického počítače.
- Hlavní systém má na starosti ostatní systémy. Tvoří se tzv. API hypercall, což je rozhraní programování a nastavování aplikací. Ostatní systémy nemají obecně přímý přístup k procesoru a hardwaru. Každá žádost o využití HW je převáděna skrz tzv. VMBus (Virtual Machine Bus) na hlavní operační systém.

Cloud computing

- Cloud computing lze vyjádřit jako: *"řadu procesů, technologií a obchodních modelů, které umožní dodat ICT (software, platformu, hardware) jako službu, a to na vyžádání a pružně."*
- Služby a programy jsou uloženy na serverech na internetu ve vzdálených datových centrech, k nimž mohou klienti přistupovat prostřednictvím webových aplikací nebo klienta dané aplikace.
- Jeden z hlavních vývojových trendů v ICT

Výhody Cloud computingu

- aplikace hostovány jinou společností (outsourcing), uživatel ušetří finanční prostředky, které by jinak připadly na údržbu a zařízení.
- odpadá starost o permanentní aktualizace SW.
- jednoduchost využívání hostovaných aplikací prakticky odkudkoli s přístupem na Internet.

Průkopníci cloud computingu: Amazon, Google, Microsoft, IBM a Yahoo!

Nevýhody Cloud computingu

- závislost na Internetovém připojení
- uživatel se může dostat do sítě, ve které jsou blokovány některé porty (nedostane se ke službě)
- obava o interní citlivá data svěřená druhé straně (cizí firmě)
- prozatím nedostatek zkušeností (a povědomí) s tímto řešením

Cloud computing - služby

Software jako služba (SaaS)

Softwarové aplikace jsou poskytované přes Internet jako služby zákazníkům. Hostované aplikace nemusí klient nijak spravovat ani instalovat. O vše se stará poskytovatel služby. Klienti potřebují pouze přístup k webu.

Pokud se SaaS (dále jen SaaS) využívá společně s dalším softwarem, označuje se jako "mashup" nebo "plugin."

Cloud computing - služby

Platforma jako služba (PaaS)

Platforma jako služba (dále jen PaaS) je založena na jazyku HTML nebo JavaScriptu. Na klientovi je postarat se o správu, instalaci a provoz aplikace*."PaaS poskytuje všechny prostředky nutné k vytváření aplikací a služeb výlučně z Internetu, aniž by bylo potřeba stahovat nebo instalovat software.“*

Cloud computing - služby

Hardware jako služba (HaaS)

Na rozdíl od předchozích služeb neposkytuje Hardware jako služba žádnou aplikaci, ale naopak hardware. Klient si může pronajmout: "místo na serveru, síťová zařízení, paměť, cykly procesoru, úložné místo.“ HaaS se označuje také jako **Infastruktura jako služba (dále jen IaaS).**

Základní typy:

- Veřejný cloud (Public cloud) – zdroje se sdílí s ostatními zákazníky,
- Soukromý cloud (Private cloud) – zdroje jsou vyhrazeny pro jednoho zákazníka,
- Komunitní cloud (Community cloud) – zdroje jsou sdíleny v rámci skupiny,
- Hybridní cloud – složený z více cloudů, např. soukromého a veřejného

Cloud computing - služby

Aplikace cloudu:

- aplikace typu peer-to-peer (Skype)
- webové aplikace (MySpace, YouTube)
- SaaS (Google Apps, Office 365)
- software plus služby (Microsoft Online Services)

Provoz datových center

- Historický vývoj od sálových počítačů k menším platformám – současný stav tzv. žiletky.
- Zmenšení ICT prostředků umožnilo serverovnám a datovým centrům konsolidovat HW prostředky.
- Při nasazení nových technologií – potřeba nových zaměstnanců spravujících systém = růst nákladů.
- S příchodem virtualizace, především té serverové, se rychlost a účinnost konsolidace ICT prostředí a služeb znásobila.
- Zatím posledním stupněm využití datových center je změna na poskytovatele cloudových služeb.

Konsolidace ICT

Probíhá až na základě komplexní analýzy podnikového prostředí ICT.

Hlavní přínosy pro organizaci:

- Zvýšení flexibility společnosti
- Snížení nákladů na provoz ICT
- Zvýšení dostupnosti a spolehlivosti služeb ICT
- Standardizace prostředí serverů
- Minimalizace ovlivňování provozních systémů ICT
- Sjednocení testovacího a provozního prostředí

Konsolidace databázových serverů a datových uložišť

- Konsolidace řeší rozložení uložišť dat v podniku.
- **Konsolidace datových serverů** = přesun databází z databázových serverů společnosti na jeden cluster databázových serverů.
- Cluster je využíván značnou částí aplikací v organizaci.
- **Konsolidace datových uložišť** = nasazení centralizovaného datového uložiště, které je dostupné přes vysokorychlostní síť pro další servery organizace.

Virtualizace

- Současný trend v optimalizaci nákladů na ICT.
- virtualizaci na úrovni hardware nebo pomocí speciálního software, virtualizují se operační systémy, ale také se virtualizují pouze aplikace.

OBECNÉ CÍLE: zjednodušení správy, lepší zhodnocení nakoupeného hardware, flexibilnější podpora businessu, snížení nákladů na provoz.

Virtualizace

- Trend - různými druhy virtualizačních technologií je nejvíce řešena virtualizace serverů na platformě Intel s operačním systémem Windows (tzv. WINTEL platforma).
- Virtualizace = infrastrukturní oblast, vliv hlavně na efektivitu a flexibilitu provozu IT
- přímý dopad na business - poskytuje tzv. zásobárnu virtuálního hardware.

Pozitivní dopady virtualizace

- Nezávislost na výběru výrobce hardware (závislost je častý problém). Některé nástroje jsou vázané na konkrétní typ hardware, jiné jsou sice univerzální ale jejich konfigurace se opět liší podle výrobce serverů.
- Pokud se organizace rozhodne vyměnit značku serverů, tak všechny používané nástroje a postupy, které se týkají virtualizovaných serverů, budou i nadále beze změny platné a funkční.
- Získání vysoké dostupnosti i pro aplikace, které samy o sobě vysokou dostupnost neřeší.
- Správně navržení = virtualizační platforma je zabezpečena proti kolapsu při výpadku jednoho či více fyzických serverů tak, že si dotčené virtuální počítače „rozebere" a znovu je spustí. Případný downtime lze tak počítat v řádu sekund (oproti hodinám v případě tradičních serverů).

Virtualizace – současný stav

- Lze virtualizovat přibližně 90 % zákaznických serverů,
- omezení - technologická, provozní, ekonomická.
- Příklady dostupných řešení: WMVARE, Microsoft (Hyper-V), ORACLE (VirtualBox), atd.
- Odkaz na případové studie, užitečné odkazy (zde).

Nástroje pro centrální správu ICT prostředí

- **Dohledové systémy** - aplikace jsou na základě konfigurace propojeny s určenými systémy (operační systémy, hardware, aplikace, sítě) a mohou o nich na základě předem definovaných pravidel shromažďovat informace o stavu, konfiguraci, výkonu nebo zabezpečení.
- Výstupy jsou přehledně zobrazovány v jediném aplikačním rozhraní, nebo je lze doručovat například pomocí e-mailu či SMS konkrétním správcům IT služby.
- Příklady aplikací: Microsoft System Center Operations Manager, NetIQ AppManager, IBM Tivoli, HP OpenView, Nagios

Dohledové systémy

- Moderní dohledové systémy obsahují vlastní znalostní bázi, pro jednodušší práci s hlášenými událostmi nebo konfiguraci sledovaných koncových zařízení.
- Pomocí rozšíření třetích stran (např. Quest QMX pro Microsoft SCOM) lze monitorovat i produkty standardně dohledovým systémem nepodporované.

Systémy pro systémový a aplikační management

- řešení umožňuje správcům ICT centrálně instalovat, konfigurovat nebo inventarizovat koncová zařízení v ICT prostředí.
- Většinu operací lze pomocí těchto nástrojů dělat vzdáleně a lze je automatizovat.
- Samozřejmostí je možnost konfigurace spouštění úkolů mimo pracovní dobu.
- Příklady aplikací: Microsoft System Center Configuration Manager, Microsoft System Center Virtual Machine Manager, Symantec Altiris nebo CA Unicenter

Přínosy řešení pro celkovou správu ICT

- Hlavní kritérium – optimalizace provozu ICT služeb
- zefektivnění pracovních postupů,
- snížení doby odstávek,
- potřebný čas pro zjištění konkrétní události.
- Moderní management systémy jsou vytvářeny s ohledem na sadu doporučení Information Technology Infrastructure Library případně Microsoft Operations Framework.
- Potenciální úspory jsou obdobou pojištění maximální dostupnosti zdrojů a jejich minimálních prostojů. To je zajištěno okamžitou informovaností ICT specialistů o závadách, dokonce i takových, které mohou teprve nastat.
- bezodkladné řešení s možností vyhnout se vlivu na běžné uživatele.
- Akcent na další rozvoj ICT prostředí místo neustálé kontroly.

Přístupy ke zpracování dat

- Organizace sbírá řadu dat (resp. provozuje databázové systémy) – dle úrovně řízení organizace požadavky na interpretaci dat:

OLTP – online transakční zpracování

- Vytváření a modifikace záznamů

OLAP – online analytické zpracování

- Reporty a analýzy

OLAP systémy a datová uložiště

- Datové sklady (**Data Warehouse DW**) – speciální datové uložiště pro dlouhodobé ukládání dat
- DW jsou využívány tzv. systémy OLAP (**Online Analytical Processing**).
- Liší se od transakčního zpracování (OLTP)
- OLAP pracují s neměnnými daty (pouze se pravidelně přidávají) a jsou transponovány z více zdrojů.
- Nad daty se provádí statistické a analytické výpočty.

OLAP systémy a datová uložiště

- Data jsou do DW ukládána dávkově s možností redundance dat. (= datové struktury v DW nemusí odpovídat struktuře dat v provozní databázi).
- Dochází k očištění dat a k převodu tzv. **datovou pumpou.**
- Data v DW zůstávají i po provedení výpočtů.
- DW neslouží jako zálohovací médium.

OLTP systémy a datová uložiště

- Online Transaction Processing (OLTP) je označení pro tzv. transakční systémy.
- Aplikace OLTP jsou určeny pro běžné zpracování dat (finanční transakce, agenda skladu, objednávky, atd.)
- Úkoly pro OLTP jsou předem připraveny a jsou složeny z krátkých, atomických nebo izolovaných transakcí.
- OLTP vyžadují okamžité odezvy, důraz kladen na integritu a konzistenci dat

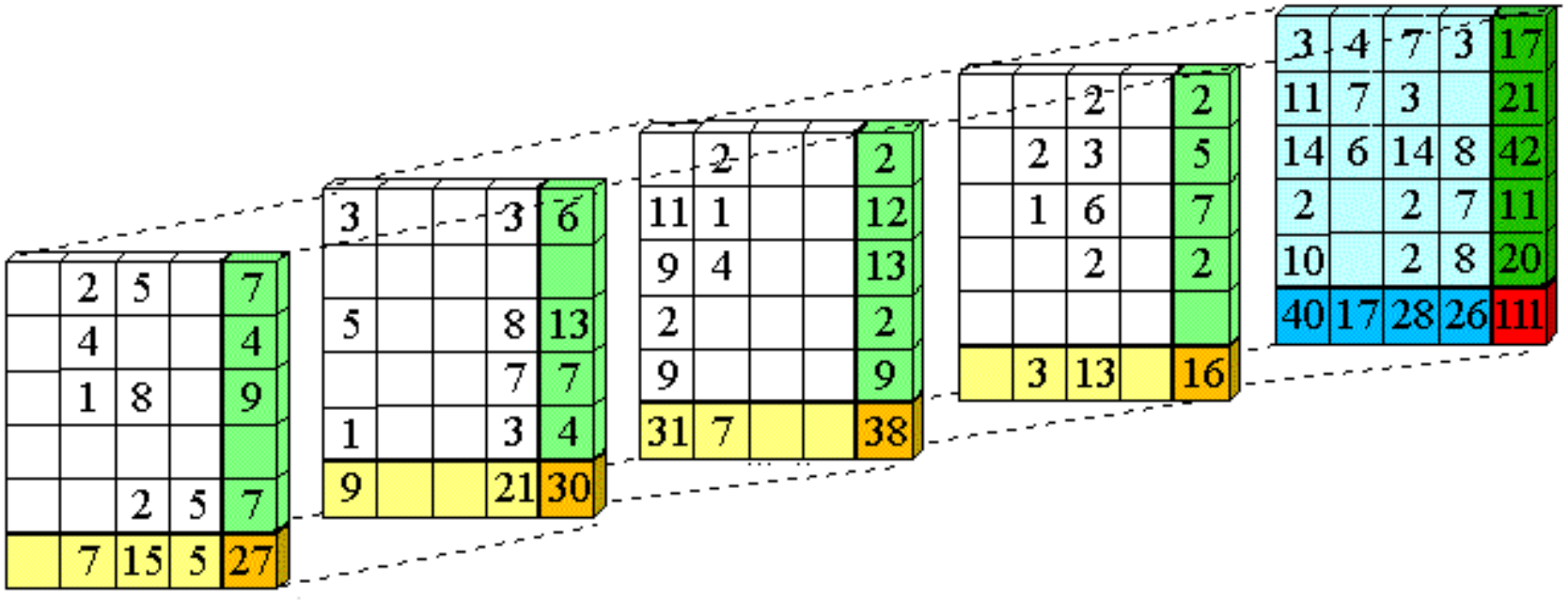
Porovnání OLTP a OLAP

- Detailní data
- Význam ve chvíli zpracování
- Častá změna dat
- Transakční orientace
- Výkonnost je důležitá
- Vysoká dostupnost je důležitá
- Redundance dat je nežádoucí
- Slouží technicko-hospodářským pracovníkům
- Předem známy požadavky na zpracování

- Agregovaná data
- Zpracování za období
- Data téměř neměnná
- Orientace na analýzu
- Výkonnost není tak důležitá
- Na vysoké dostupnosti příliš nezáleží
- Redundance dat je běžná
- Slouží především analytikům a manažerům
- Většina požadavků není předem známa

Datová kostka

- OLAP krychle (online analytical processing) je způsob organizace dat, který rozšiřuje dvojrozměrně tabulkové uspořádání tak, že každá datová dimenze je uložena v jedné ose kostky. Tím překonává některá omezení relačních databází.



Bezpečnost podnikové infrastruktury

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

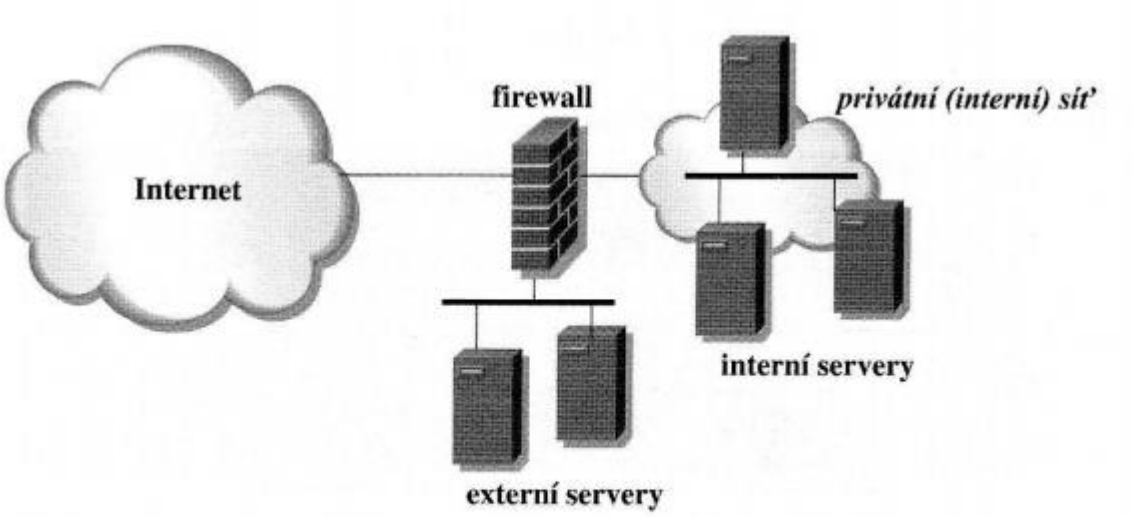
- Kromě DNS jsou častými cíly útoků směrovače. Pokud nejsou zabezpečeny proti útokům zvenčí představují pro útočníky potenciální platformu pro vedení útoku. Při realizaci směrování je nutné zvážit všechny požadavky zabezpečení jednotlivých směrovačů a použít prvky s vhodnou hardwarovou podporou zabezpečení.

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

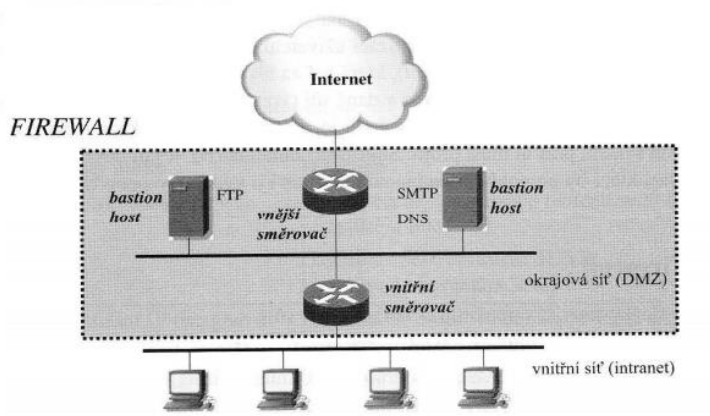
- Tvoří ho ochranné složky jak hardwarové, tak softwarové, které dohromady tvoří ochrannou zeď mezi Internetem a podnikovou sítí.



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

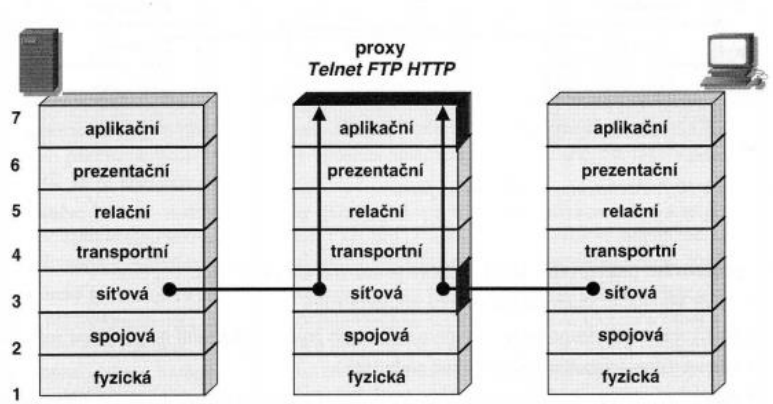


Funkce firewall

- **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.