Síťová bezpečnost

I. Základní popis zabezpečení

1. Úvod

Pojmem bezpečnost rozumíme nikoliv stav, ale neustálý proces, kterým se snažíme dosáhnout a udržet uspokojivé zabezpečení sítě. Síťové technologie se velmi rychle vyvíjí a s nimi rovněž také znalosti a nástroje potenciálních útočníků. Potenciální hrozbou pro síť jsou lidé (nedbalost či neznalost uživatelů nebo úmyslné útoky, krádeže apod.) a přírodní faktory (blesk, požár, záplavy apod.). Dříve než začneme plánovat zabezpečení vlastní sítě, je třeba nejdříve zvážit jakou cenu mají aktiva (hardware, software, data) a jaká jsou s jejich případným zneužitím, odcizením či poškozením spojená rizika (ztráta zákazníků, poškození dobrého jména organizace apod.) tak, aby plánované prostředky vynaložené na zabezpečení byly na jednu stranu dostatečné ale nikoliv zase přemrštěné (pro příměr: aby nebyl sejf dražší než jeho obsah). V souvislosti s možným výskytem bezpečnostních incidentů (narušení bezpečnosti) je třeba mít připraven plán jejich zvládání (adekvátních reakcí na ně) včetně plánu zachování (či rychlého obnovení) chodu organizace až do jejich úplného vyřešení a návratu do původního stavu. Náplní předchozích dvou souvětí se zabývá zejména:

- řízení rizik (RM - Risk Management [1])
  - identifikace aktiv a stanovení jejich hodnoty
  - identifikace hrozeb a slabin
  - stanovení závažnosti hrozeb a míry zranitelnosti
- plán obnovy po havárii (DRP - Disaster Recovery Plan [2])
  - prevence bezpečnostních incidentů
  - detekce bezpečnostních incidentů
  - obnova po výskytu bezpečnostního incidentu
- řízení kontinuity činností organizace (BCM - Business Continuity Management [3])
  - porozumění činnosti organizace
  - návrh a implementace bezpečnostních opatření (interní předpisy, bezpečnostní politika, DRP, BCP, strategie reakcí na incidenty)
  - audit, testování, hodnocení a případná změna bezpečnostních opatření
- plán kontinuity činností organizace (BCP - Business Continuity Plan)
  - aktualizované úložiště dat a dokumentů (smlouvy, pojištění, účetnictví) v jiné lokalitě (off-site)
  - kontakty na zaměstnance, krizové vedení a obchodní partnery
  - směrnice a postupy pro aktivaci DRP
- strategie reakcí na incidenty
  - ochrana životů a zdraví
  - zamezení dalších škod
  - hodnocení škod
  - použití BCP (+ obnova běžného chodu organizace dle DRP)

Kromě toho, že útoky na bezpečnost sítě můžeme dělit dle lokace útočníka na vnitřní (neznalost, nedbalost či útok ze strany vlastních zaměstnanců) a vnější (náhodný či promyšlený útok zvenčí), bezpečnost sítě lze rozdělit na fyzickou bezpečnost, bezpečnost sítě a služeb a bezpečnost lidských zdrojů.

2. Fyzická bezpečnost

- ✔ vhodná lokalita pro sídlo organizace (či pro umístění jejího IT zázemí)
  - dobrá dopravní dostupnost (optimálně alespoň dvěma způsoby – auto, MHD, vlak, ...)
  - ochrana před nepříznivými přírodními vlivy
    - vyvýšený vchod (kvůli záplavám či závějím)
    - neumísťovat v záplavovém pásmu
    - neumísťovat přímo pod kopec či do svahu (riziko zavalení či sesuvu půdy)
    - neumísťovat příliš blízko stromům (nebezpečí jejich pádu atd.)
- ✔ splnění elektrotechnických předpisů
  - správné dimenzování vodičů a jističů
  - dostatečné uzemnění a izolace
  - správné krytí (IP – Ingress Protection) zařízení
  - proudové chrániče
  - ochrana před bleskem a přepětím
- ✔ splnění požárních předpisů [4]
  - žáruvzdorné materiály
  - správný hasicí systém
  - požární hlásič
  - únikový východ
- ✔ zabezpečení klíčových prostor
  - uzamykatelné prostory, bezpečnostní dveře, bezpečnostní fólie
  - Elektronický Zabezpečovací Systém (EZS [5])
  - kamerový dohled, ostraha
  - evidence vstupu povolaných osob (čipové karty, otisk prstu apod.)
  - ochrana budovy (mříže na oknech, plot, betonové zátarasy apod.)
- ✔ zajištění vhodného prostředí pro provoz informační a komunikační techniky
  - spolehlivé dodávky el. energie – nepřerušitelný zdroj napájení (UPS [6] - Uninterruptible Power Source), motorgenerátor, náhradní dodavatel elektrické energie
  - odvětrávání, chlazení, odsávání/filtrace prachu
- ✔ dostatečné označení a dokumentace
  - označení zařízení (název, inv. číslo, IP adresa, MAC adresa, kontakt na správce)
  - očíslování zásuvek a portů v panelech rozvaděčů (PP - patch panel)
  - logická a fyzická topologie sítě
- ✔ používání kvalitních komponent splňujících standardy
- ✔ nasmlouvaný servis a pojištění
- ✔ pravidelné zálohování klíčových dat (konfigurací, logů, účetnictví) a dokumentů (směrnic, smluv, obchodních kontaktů) v místě (on-site) i mimo (off-site)
- ✔ redundantní topologie
  - záložní linky

- zrcadlení (mirroring) datových úložišť
- záložní zařízení (boxy) dle stavu připravenosti (viz. níže:)
  - studená záloha
  - vlažná záloha
  - horká záloha

3. Bezpečnost sítě a služeb

- ✔ vypnutí nepotřebných služeb (každá komponenta má dělat pouze to, na co byla určena)
- ✔ zabezpečení přístupu ke zdrojům a službám
  - ověřování totožnosti, přidělování oprávnění, účtování činnosti (AAA – Authentication, Authorisation, Accounting) - lokální nebo serverové (tacacs+, radius, diameter)
    - ověření totožnosti uživatele
      - heslem (dostatečně dlouhým a složitým)
      - biometrie (otisk prstu, oční duhovka)
      - čipové karty
      - asymetrické kryptování, elektronický podpis
        - sítě důvěry – PGP (Pretty Good Privacy – aplikace na šifrování a podepisování)
        - důvěryhodná třetí strana (TTP - Trusted Third Party)
        - certifikační autorita (CA)
        - infrastruktura veřejných klíčů (PKI [7] - Public Key Infrastructure)
    - oprávnění ověřeného uživatele
    - protokolování (logování) činnosti uživatele (co a kdy dělal)
- ✔ stanovení priorit služeb [8] upřednostněním kritických systémových či real-time služeb jako směrování či hlas (voice) před např. běžným prohlížením webu
- ✔ správné rozdělení sítě
  - bezpečnostní zóny [9] jako vnější (internet), vnitřní (intranet) a mezilehlá (extranet – DMZ - DeMilitarized Zone)
  - virtuální sítě (VLAN [10]) dle skupin uživatelů s podobným oprávněním či dle jiných logických seskupení (finanční oddělení, správci sítě, ostatní zaměstnanci apod.)
- ✔ obvodová bezpečnost (PS - Perimeter Security) - ochrana na rozhraní bezpečnostních zón a/nebo virtuálních sítí
  - překlad adres (NAT – Network Address Translation, PAT – Port Address Translation, NAPT – Network Address and Port Translation [11]) – skrytí vnitřní sítě použitím privátních adres [12] s následným překladem na jednu nebo více veřejných adres
  - filtrování provozu s ohledem na bezpečnost (FW - FireWall [13])
    - omezování rychlosti (rate limiting) např. u ICMP či UDP, ochrana před útoky, které znemožňují používání služeb oprávněnými uživateli (DoS – denial of service, DDoS – distributed DoS)
    - ochrana proti podvrhování falešných dat (antispoofing) – např. zahazování zvenčí příchozích paketů se zdrojovou adresou pocházející z vnitřní sítě apod.
    - omezení přístupu pomocí přístupových seznamů (ACL – Access Control List) - např. povolení zahájit komunikaci pouze z vnitřní sítě ven
  - filtrování provozu na základě jeho obsahu (content filter) – antivirus, antispam, antimalware, omezení přístupu na některé webové stránky apod.
- ✔ ochrana koncových zařízení (endpoint security)

- firewall, content filter
- systém prevence narušení (IPS – Intrusion Prevention System) při výskytu příznaků naznačujících útok zablokuje odpovídající provoz
- systém detekce narušení (IDS [14] - Intrusion Detection System) detekuje a ohlásí případný útok, na detekci je citlivější než IPS

✔ ochrana sítě před uživatelem
- sledování a kontrola přidělování dynamických IP adres (DHCP snooping [15])
- kontrola platnosti dvojic IP adresa, MAC adresa (DAI – Dynamic ARP Inspection)
- povolení pouze daných MAC adres nebo omezení jejich počtu (port security [16])
- povolení připojení do LAN pouze ověřeným uživatelům (802.1x)
- ochrana proti podvrhování falešných dat (antispoofing)

✔ ochrana vzdáleného přístupu – SSH, VPN [17] (IPSEC, SSL)

✔ používání zabezpečených služeb – HTTPS, SMTPS, IMAPS, DNSSEC

✔ ochrana paměťových médií (šifrováním při používání, důkladnou likvidací dat při jejich vyřazování)

✔ správa sítě
- management konfigurací
- používání SW pouze v souladu s jeho licencí
- aktualizace SW a OS
- logování (lokálně či šifrovaně na vzdálený syslog server)
  - přístupů a využívání služeb
  - změn stavů sítě a služeb (výpadek služby či linky, změna konfigurace, změna ve směrovací (routing) tabulce apod.)
  - statistiky provozu (NetFlow [18])

✔ dohledové centrum
- sledování funkčnosti síťových prvků (ping, Nagios [19], HPOpenView)
- vyhodnocování logů, odhalování abnormalit
- řešení problémů

✔ redundanci zajišťující protokoly (spanning tree [20], HSRP [21], VRRP [22], ...)

✔ bezpečné směrování
- stabilní - použití statických cest (v případě jednoduché sítě) nebo ručního vyjmenování vlastních sítí (zákaz automatické redistribuce z IGP v případě BGP [23])
- od důvěryhodných zdrojů (ACL, volitelná ověřování u protokolů RIP, OSPF, ISIS, BGP)
- jen nutné směrovací informace (policy routing, distribute lists, route maps)
- omezování (filtrace) na základě kontroly reverzní cesty (reverse-path filtering – dá se použít jen v případech, kdy se nepoužívá asymetrické směrování)

✔ mobilní zařízení (notebook návštěvy apod.)
- připojovat pouze do k tomu určené sítě (oddělit návštěvy od zaměstnanců)
- návštěvám přidělovat unikátní přístupové kódy jednotlivě
- mít zapnuté protokolování a aktivován firewall

4. Bezpečnost lidských zdrojů

✔ splnění předpisů BOZP (bezpečnosti a ochrany zdraví při práci)

✔ minimalizace přístupových oprávnění (každý jen tam, kam z pozice své funkce ve firmě potřebuje)

- ✔ zastupitelnost, informovanost, komunikace
- ✔ BCM – Business Continuity Management (viz. výše na první straně)
- ✔ legislativa (zákony + interní předpisy)
- ✔ přístupová oprávnění pouze na dobu nezbytně nutnou (deaktivace práv při ukončení činnosti, či ukončení pracovního poměru zaměstnanců apod.)
  - zneplatnění přístupových oprávnění (např. změna hesla)
  - zneplatnění uživatelských certifikátů
  - kontrola potenciální existence „zadních vrátek“ v systémech v minulosti spravovaných uživatelem
- ✔ Školení
  - pravidelné a s odpovídající náplní dle daných cílových skupin
  - interní předpisy, bezpečnostní politika
  - hrozby na síti, prevence a obrana, Netiketa
  - správné ovládání IT ve firmě (OS – Operační Systém, IS – Informační Systém, SW – SoftWare, HW – HardWare)

5. Specifika prostředí školy

Škola kromě toho, že poskytuje internet svým zaměstnancům, tak se také stává poskytovatelem internetu pro své studenty (zpravidla formou bezdrátové sítě - Wi-Fi). Je tedy nutné zdůraznit následující:

- řádné oddělení sítí (síť pro zaměstnance, síť v počítačových učebnách, Wi-Fi síť) a s tím související přístupová práva (nejen 802.1x) a přidělení priorit jednotlivým typům služeb (QoS – Quality of Service)
- dodržování IT standardů (umožnění funkčního připojení zařízení od různých výrobců, zejména v případě Wi-Fi sítě a notebooků studentů)
- ověřování jednotlivých uživatelů samostatně (nikoliv sdílená hesla)
- přidělování oprávnění jednotlivým uživatelům individuálně (a teprve až po absolvování školení o počítačové a síťové bezpečnosti)
- protokolování (logování) aktivit uživatelů (přihlášení, odhlášení, použité služby, IP adresy apod.)
- adekvátní bezpečnostní politika - např. (dočasné) omezení přístupu k Wi-Fi (nebo jiný postih) v případě potenciálního ohrožení sítě (přítomnost viru nebo červa na notebooku apod.) či jiného porušení pravidel jejího používání, znemožnění instalování dalšího software studenty na PC v počítačových učebnách atd.
- zabezpečení bezdrátové Wi-Fi sítě (WPA2, AES, 802.1x, filtrace portu 25 – tj. používání pouze vlastního školního poštovního serveru, atd.)

II. Doporučená technická opatření

V případě používání technologie sdíleného média (10BASE-2 apod.) či jiné zastaralé technologie provést upgrade na přepínaný ethernet alespoň 100BASE-TX (nebo rovnou 1000BASE-T). Další opatření jsou následující:

- Centrální AAA server

- Centrální firewall
- IDS, IPS
- konfigurovatelný přepínač (switch) podporující QoS a zabezpečení (VLAN, DHCP snooping, DAI, port security, 802.1x, ...)
- zavedení synchronizace času, případně rovnou vlastní časový server (timeserver, NTP – Network Time Protocol, SNTP – Simple NTP)
- syslog server
- síťová monitorovací stanice (network monitoring station)
- zálohovací (backup) server
- vlastní poštovní (e-mail) server (optimálně včetně antiviru a antispamu) pokud možno podporující zabezpečené protokoly jako POP3S, IMAPS či SMTPS
- firewall, antivirus, antispam na koncových stanicích (PC)

Rovněž existují prvky, které kombinují několik výše uvedených vlastností v jednom zařízení (např. Router + FW + IDS + NTP server).

III. Základní kroky nasazení

Základní kroky nasazení bezpečnostních opatření závisejí především na výsledcích bezpečnostního auditu sítě, ze kterého je patrné, která bezpečnostní opatření jsou již zavedena a která je teprve zapotřebí zavést. Obecný postup zavádění zabezpečení krok za krokem může být např. následující:

- změnit hesla (zatím pouze na dočasná)
- aplikovat FW (centrální)
- vypnutí nepotřebných služeb
- aplikovat synchronizaci času (timeserver)
- aplikovat logování (syslog server)
- sledování sítě (network monitoring)
- aplikovat zálohování (backup server)
- zabezpečení směrování (pokud je potřeba)
- v případě nutnosti aktualizace (update či upgrade) OS kde je potřeba
- aplikovat FW a antivirus (anti-malware) na ostatních (koncových) stanicích
- zavedení bezpečnějších služeb (SMTPS, IMAPS, antispam na mailserveru atd.)
- update (či upgrade) používaného aplikačního SW
- v případě používání zastaralé technologie zavést přepínaný Ethernet
- port security, DAI, DHCP snooping
- změna hesel na hesla trvalejšího rázu
- kontrola zpětné cesty (RPF - reverse-path filtering) jen pokud se nepoužívá asymetrické směrování
- centrální AAA server
- 802.1x
- klíče, certifikáty (případně vlastní CA) , DNSSEC
- EZS - evidence vstupu (čipové karty), kamerový systém

IV. Cenové odhady

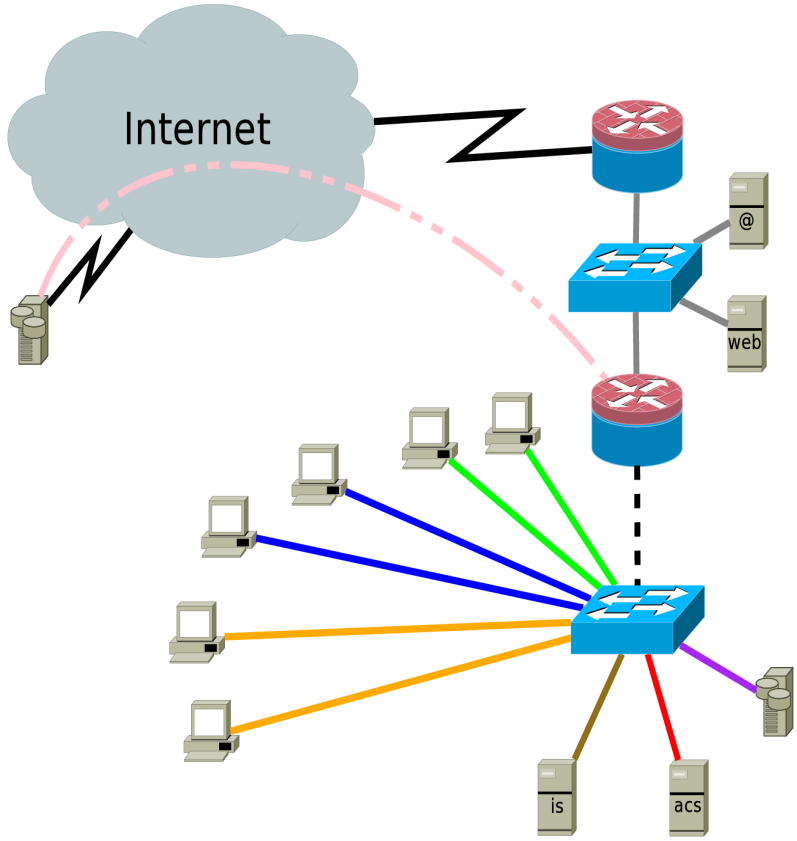
Co se cenových odhadů týká, tak zde mohou nastat výrazné cenové rozdíly v závislosti na dané implementaci (záleží na tom, zda např. zvolíme převážně PC řešení založené na Linuxu, zda budeme kombinovat několik služeb na jednom boxu či nikoliv apod.). Řešení založené na Linuxu bývá sice méně uživatelsky přívětivé (user-friendly) a vyžaduje znalého administrátora, ale zato jde o řešení poměrně univerzální s velkou možností přizpůsobení (konfigurace) na míru daným podmínkám provozu (s nízkou pořizovací cenou – většinou pouze cena HW). Co se týká sdílení více služeb na jednom boxu, je to sice řešení technicky možné (a v případě omezeného množství finančních prostředků dokonce nevyhnutelné), ale z pohledu bezpečnosti nelze doporučit, neboť v bezpečnější síti by měla mít každá služba svoje vlastní železo (+ případně jedno záložní). Zpravidla se však jedná o nějaký lepší či horší kompromis. Modelový příklad by mohl být např. následující:

Předpokládáme stávající nezabezpečenou síť:

- připojení k Internetu (poslední míle včetně směrovače)
- stávající služby (E-mail, WWW, DNS, IS)
- LAN, Wi-Fi, koncová zařízení

Nová bezpečnostní opatření (relativně jednoduchá varianta bez záložních prvků)

- upgrade na přepínaný Ethernet (pokud ještě není)
  - rozvaděč ... 14000,-Kč vč. DPH (45U 600x1000)
  - UTP kabeláž ... 1800,-Kč vč. DPH (305m kat. 5e)
  - přepínač1 ... 28000,-Kč vč. DPH (48portový Linksys SGE2010)
  - přepínač2 ... 38000,-Kč vč. DPH (48portový Linksys SGE2010P with PoE)
  - cena ostatního materiálu (jako zásuvky, konektory apod.)
  - plus cena za práci ... ?
- firewall
  - varianta1 ... 53000,-Kč vč. DPH (např. ASA5510-SEC-BUN-K9)
  - varianta2 ... 20000,-Kč vč. DPH (PC s Linuxem)
- AAA server
  - varianta1 ... 200000,-Kč vč. DPH (např. HW+SW CSACS-1121-K9)
  - varianta2 ... 100000,-Kč vč. DPH (např. Radiator, Radar, RAdmin + PC s Linuxem)
  - varianta3 ... 65000,-Kč vč. DPH (např. HW+SW CSACS-5.0-EXP-K9 do 350 uživatelů)
  - varianta4 ... 20000,-Kč vč. DPH (PC s Linuxem/Freeradius)
- syslog + zálohovací server ... 16000,-Kč vč. DPH (např. Synology DiskStation DS710+ +2x2GBHDD)
- případná výměna přepínače za konfigurovatelný se zabezpečením (cena viz. výše)
- případná výměna přístupového bodu (AP – Access Point) Wi-Fi kvůli zabezpečení (podpora WPA2, AES, 802.1x apod.)
  - varianta1 ... 4000,-Kč vč. DPH (např. Cisco WAP4410N – jen pro malé sítě)
  - varianta2 ... 12000,-Kč vč. DPH (např. Cisco Aironet 1140)
  - doplnění varianty2 o WLC ... 160000,-Kč (např. AIR WLC4402-25-K9 pro 25 AP)
- zabezpečení koncových PC
  - varianta pro Windows ... 0,-Kč vč. DPH (např. Comodo Internet Security, Thunderbird, Ossec)
  - varianta pro Linux ... 0,-Kč vč. DPH (např. Clamav, ClamTk, Iptables, Thunderbird, Ossec)



router s firewallem

DMZ (extranet)

Intranet VPN

IEEE 802.1Q Trunk

Zabezp. PC (FW, ANTI*, ...)

on-site a off-site backup server

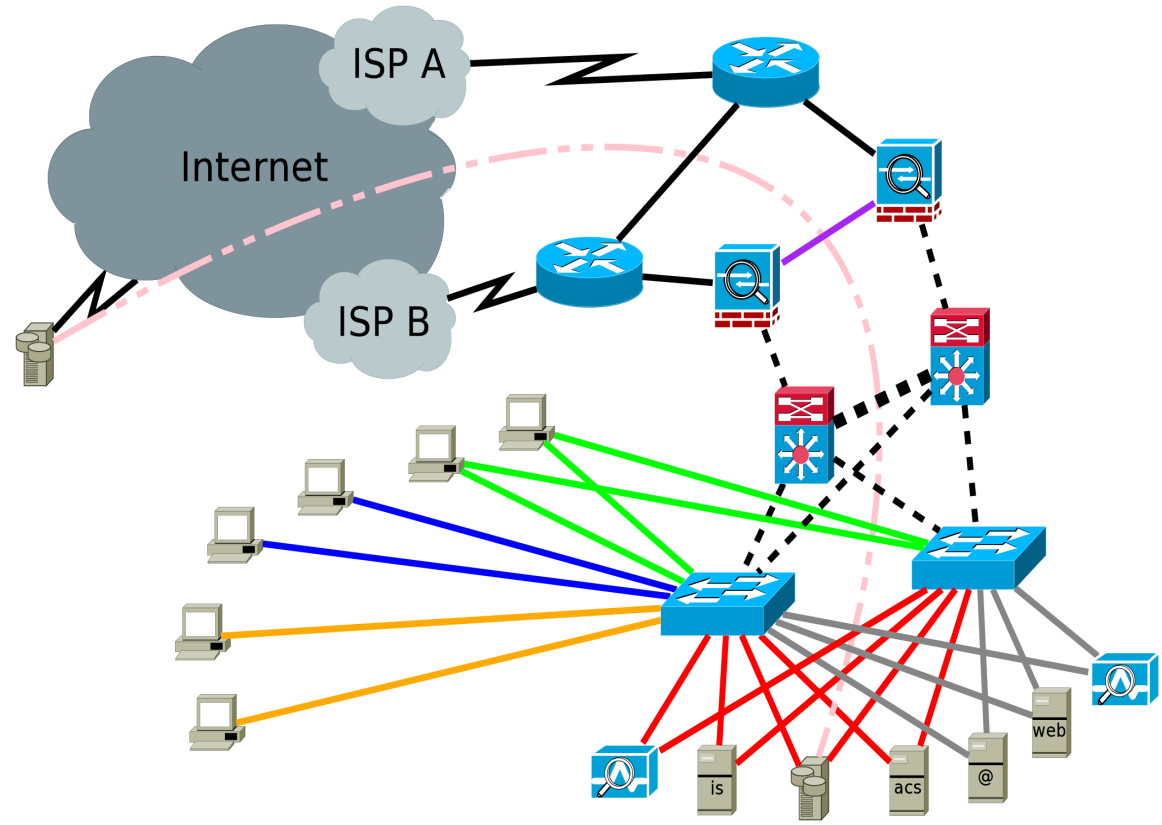
VLAN správy sítě

VLAN vedení (řed., fin. a pr.)

VLAN ostatních zaměstnanců

VLANy vnitřních serverů

Intranet



DMZ

VPN pro účely zálohování

IEEE 802.1Q Trunk

LACP 802.1Q Trunk

Zabezpečená PC (FW, ANTI*, ...)

on-site a off-site backup server

VLAN správy sítě

VLAN vedení (řed., fin. a pr.)

VLAN ostatních zaměstnanců

VLAN vnitřních serverů

Intranet

Firewall failover

1 *** ISO 16085; **Risk Management: Concepts and Guidance**, Carl L. Pritchard, ESI International, USA, 2001, ISBN: 1890367303; http://riskm-aka.blogspot.com/

2 *** ISO/IEC 24762:2008; Disaster Recovery Planning: For Computers and Communication Resouces, Jon William Toigo, Wiley, 1995, ISBN-10: 0471121754, ISBN-13: 978-0471121756

3 *** BS 25999

4 *** Zákon č. 133/1985 Sb.

5 *** ČSN EN 50131-1

6 *** IEC 62040-3:1999, ČSN EN 50091

7 *** X.509

8 *** IEEE 802.1P

9 *** RFC 2647

10 *** IEEE 802.1Q

11 *** RFC 2663

12 *** RFC 1918

13 *** RFC 2979

14 *** http://csrc.ncsl.nist.gov/publications/nistpubs/800-94/SP800-94.pdf; http://www.dmoz.org/Computers/Security/Intrusion_Detection_Systems/

15 *** http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.1/13ew/configuration/guide/dhcp.html

16 *** http://www.enterprisenetworkingplanet.com/netsecur/print.php/3462211

17 *** http://home.zcu.cz/~ondrous/

18 *** http://www.cisco.com/go/netflow

19 *** http://www.nagios.org/

20 *** IEEE 802.1D; IEEE 802.1w; IEEE 802.1s (nyní IEEE 802.1Q)

21 *** RFC 2281

22 *** RFC 3768; RFC 5798

23 *** RFC 1771