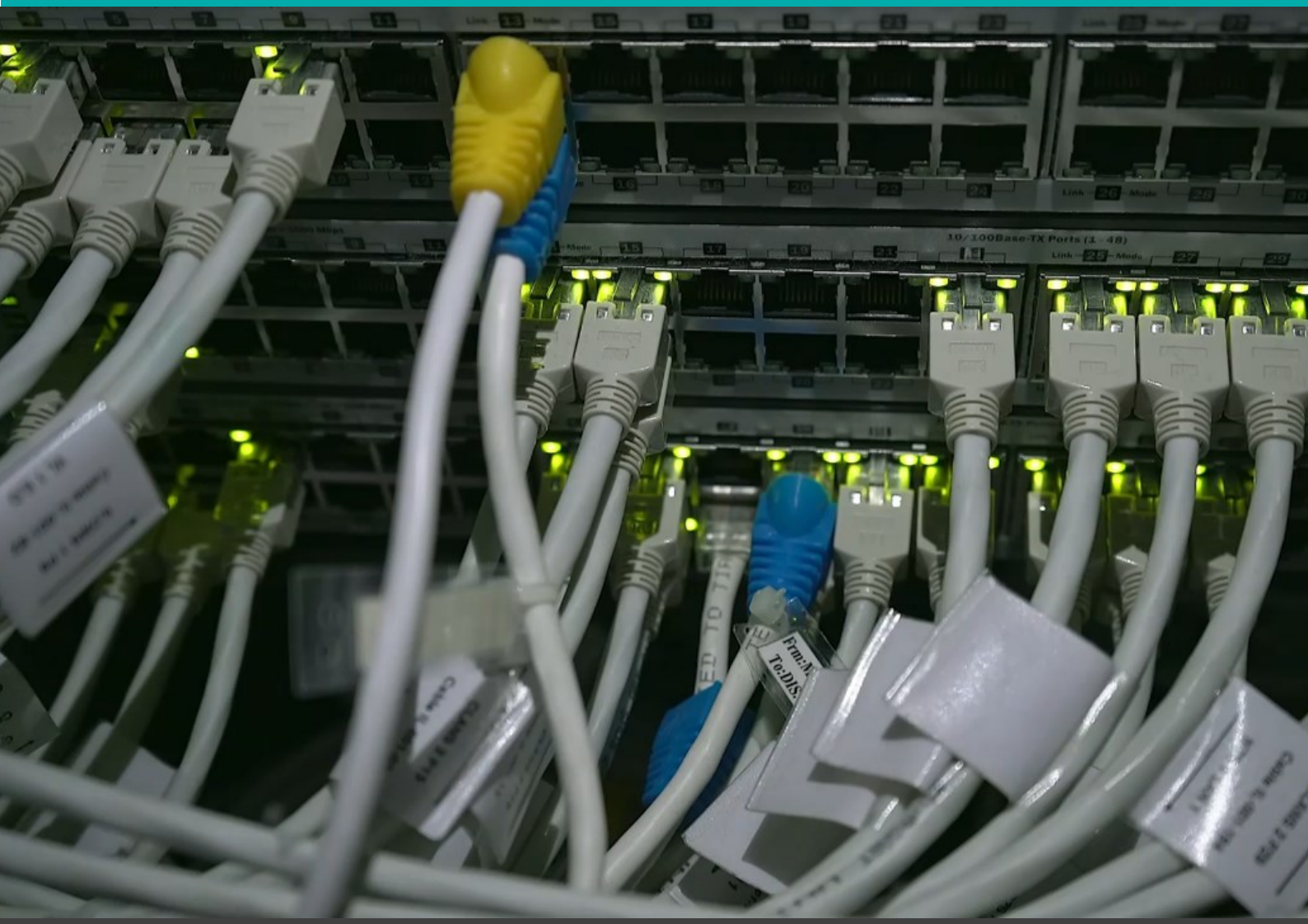


Principy a možnosti počítačových sítí

Podpora ICT koordinátorů na základních a středních školách

2023

Obsah

Úvod

Tento kurz představuje základní principy počítačových IP sítí, tak aby student uměl vyhodnotit návrh dané počítačové sítě, včetně použitých technologií pro přenos dat, jejich základních služeb a měl základní povědomí o možnostech a požadavcích na jejich správu. Kurz je sestaven tak, aby student, bez předchozích znalostí problematiky počítačových sítí pronikl do daného tématu, získal základní znalost o principech a trendech v počítačových sítích a mohl efektivně, systematicky definovat a analyzovat služby, které má daná počítačová síť poskytovat.

V první kapitole se seznámíme se základními pojmy. Pomocí druhé kapitoly budeme schopni vytvořit základní schéma sítě, logickou a fyzickou topologii. Třetí kapitola nás seznámí s principy komunikace v počítačové síti. Čtvrtá kapitola nás seznámí s možnostmi virtualizace a cloud computingu. V páté kapitole probereme základní bezpečnostní hrozby a principy bezpečnosti počítačové sítě. Šestá kapitola nám objasní, co by měla obsahovat dokumentace.

Je třeba také zmínit, že nástroj Cisco Packet Tracer je bezesporu dlouhodobě nejlepším simulátorem počítačových sítí a nejlepším pomocníkem při jejich studiu. V současné době jej můžete využívat zdarma díky výukovému webu Skills for All by Cisco: Free Online Tech Courses For All

Odkaz: Cisco Packet Tracer: A Free and Fun Course for Beginners (skillsforall.com)

V případě, že se budete chtít danou problematikou zabývat podrobněji, doporučujeme výše uvedený web a kurzy, které jsou pro veřejnost zdarma.

Proč si projít tuto kapitolu?

Nejspíše proto, že chcete úspěšně zvládnout daný modul, nicméně to bych se opakoval každou chvíli. Věřím, že chcete nejen úspěšně zvládnout Vaše studium, ale že se toužíte se dozvědět více o tom, jak počítačové sítě fungují a jak spolu zařízení komunikují. Tato první kapitola znamená první krok na cestě poznání. Tak ať se Vám líbí.

Co se v této kapitole naučím?

Naučíte se identifikovat typy sítí, popsat síťová data, znát základní pojmy jako je šířka pásma a propustnost, seznámíte se s významem klientů a serverů v síti.

Časová náročnost: 60 minut

1 Svět v síti

1.1 Internet

V dnešní době je internet a digitální technologie běžnou součástí našich životů a mnoho lidí tráví část nebo většinu svého času online. Podle statistiky z roku 2021 bylo celosvětově přes 4,9 miliardy uživatelů internetu, což představuje více než 60 % celkového světového obyvatelstva. A zvyšuje se nejen počet uživatelů ale také i čas, který lidé tráví online.

Nejspíše běžně předpokládáme, že naše „hračky“, telefony, tablety, notebooky a počítače budou vždy připojeny do sítě internetu. Díky této technologii jsou lidé schopni komunikovat navzájem a třeba i na druhé straně světa, pracovat z domova, nakupovat, pouštět si filmy a hudbu, hledat informace a učit se nové věci. Využíváme tak výhod a přínosů internetu a dalších digitálních technologií, abychom si usnadnili své každodenní činnosti a zlepšili své pracovní, osobní a společenské vztahy. Internet se stal součástí každodenního života a bereme jej jako samozřejmost.

Internet můžeme vnímat různě, v závislosti na věku, kultuře, zkušenostech a vzdělání. Pro některé lidi může být internet také zdrojem stresu, úzkosti a nebezpečí, jako jsou kyberšikana, podvody a ztráta soukromí. Někteří lidé se obávají závislosti na internetu (netolismus) a snižování schopnosti interagovat s lidmi v reálném životě. Nicméně, obecně platí, že internet je vnímán jako užitečný nástroj, který má pozitivní vliv na životy mnoha lidí a umožňuje jim rychlé a snadné připojení k informacím, službám a lidem po celém světě.

Málokdo z nás vnímá internet jako fyzické propojení skutečného světa. Propojení pomocí telefonních, optických a dalších kabelů, propojení pomocí bezdrátových médií nebo také satelitních linek. Spojení například vašeho telefonu s jiným na druhé straně světa pomocí dalších komunikačních zařízení a mnoha různých cest. Všechna tato propojení a sítě jsou udržovány nezávisle různými jednotlivci, společnostmi a poskytovateli a to většinou na jejich náklady.

Internet není vlastnictvím jediného subjektu, osoby nebo organizace. Internet je decentralizovaná sít propojených počítačů a zařízení po celém světě, které komunikují pomocí standardizovaných protokolů.

Existují však organizace a instituce, které mají vliv na internetovou infrastrukturu, jako jsou například poskytovatelé internetového připojení, technologické firmy a vlády. Tyto subjekty mohou mít vliv na regulaci a řízení určitých aspektů internetu, jako jsou například pravidla pro používání internetu, ochrana soukromí a zabezpečení sítí. Nicméně, samotný internet zůstává otevřený a přístupný pro každého, kdo má přístup k internetovému připojení a zařízení.

Vše, k čemu se online dostanete je uloženo „někde“ v internetu. Stránky sociálních médií, herní servery, centra pro správu služeb jako jsou email, úložiště, databáze, a mnoho dalšího, to vše je uloženo v jednotlivých sítích, které díky propojení s dalšími mohou odesílat a přijímat informace.

1.2 Počítačové sítě

Počítačové sítě mohou být různých velikostí, od jednoduchých, které jsou tvořeny třeba jen dvěma počítači, až po sítě, které spojují stovky tisíc zařízení. Sítě v malých kancelářích

a domácnostech jsou označovány také jako SOHO (small office/home office). Tyto sítě nám dovolují sdílet mezi uživateli tiskárny, dokumenty, obrázky, hudbu apod.

Rozsáhlejší sítě se využívají pro nejrůznější činnosti, pro reklamu, prodej produktů, objednávání zásob, komunikaci se zákazníky, poskytování informací, zábavy, vzdělání.

Počítačové sítě ve školním prostředí

- umožňují studentům a učitelům přístup k množství informací a zdrojů, jako jsou elektronické knihy, vědecké časopisy, online encyklopedie a další. Tímto způsobem mohou studenti rychleji najít informace a učitelé mohou nabízet širší spektrum materiálů
- umožňují studentům a učitelům snadno sdílet informace, jako jsou prezentace, dokumenty a další materiály. To znamená, že studenti mohou snadno získat informace z jiných zdrojů a učitelé mohou snadno sdílet materiály s celou třídou.
- umožňují školám nabízet online kurzy a vzdělávací programy. Což je užitečné pro studenty, kteří se potřebují učit z domova, a také pro ty, kteří chtějí rozšířit své znalosti a dovednosti mimo tradiční rozvrh.
- umožňují učitelům a studentům snadno komunikovat prostřednictvím e-mailu, chatu a jiných online nástrojů.
- usnadňují administrativní práci učitelům a dalším zaměstnancům.

Komunikace pomocí počítačové sítě je obvykle efektivnější a méně nákladná, než tradičnější formy předávání a sdílení informací pomocí pošty nebo telefonních hovorů.

1.3 Rozdělení sítí dle velikosti

Sítě, které komunikuji v rámci cca 1 metru můžeme označit jako **PAN (Personal Area Network)**. Do této kategorie řadíme technologie: Bluetooth, Infra, NFC, zkrátka osobní síť.

Malé domácí sítě mohou propojit navzájem mezi sebou a k internetu několik počítačů nebo dalších zařízení. SOHO sítě umožňují připojení kancelářských počítačů a zařízení k podnikové síti, většinou se zde setkáváme se serverovým řešením, které umožňuje centrální správu počítačů a uživatelů a také sdílených zdrojů, jako jsou úložiště, databázové služby, sdílené aplikace apod. Střední až rozsáhlé sítě, mezi které můžeme zařadit větší organizace a také školy, mohou mít více lokací se stovkami až tisíci zařízeními. O uvedených sítích mluvíme jako o **LAN (Local Area Network)**.

Rozsáhlé sítě, které nepřekračují hranice města, a které mohou (a nemusí) být vlastněny více organizacemi označujeme jako **MAN (Metropolitan Area Network)**.

Komunikační sítě, pokrývající rozsáhlé území státu, nebo kontinentu označujeme jako **WAN (Wide Area Network)**.

Síť, která pokrývá celou planetu, se nazývá Internet a propojuje nám stovky miliónů zařízení po celém světě. Můžeme také říci, že se jedná o neznámější WAN.

1.4 Data, informace a bity

Data, data, data, digitalizace a data. Data jsou získávána, těžena, přenášena, analyzována, ukládaná. Co to tedy data jsou? Jednoduše řečeno data jsou hodnoty, které nám něco představují. Ve fyzickém světě jsou to čísla, vzorce, znaky, obrazy. Zamyslete se nad tím, kolik dat existuje jen o vaší osobě.

Co je to bit?

Všechny počítače a všechna digitální zařízení se kterými se můžete setkat používají pouze binární čísla: jedničky a nuly. Asi je těžké si představit, že všechna data, která sdílíte, tvoříte, posíláte a čtete jsou tvořena pouze obrovskou skupinou bitů a bit může nabývat pouze dvou možných hodnot: 0 a 1. Bit je zkratka výrazu „binární číslo“ (binary digit) a představuje nám nejmenší možnou jednotku dat nebo informací.

Bit je uložen a přenášen jako jeden ze dvou možných stavů, například pomocí dvou směrů magnetických sil, dvou různých elektrických napětí, dvou jinak intenzivních světelných paprsků nebo jakýchkoliv jiných fyzikálních způsobů vyjádření dvou stavů. Můžete si představit, že světlo u vás v pokoji může být zapnuto nebo vypnuto, respektive binárně vyjádřeno pomocí 1 nebo 0. Což už nám třeba umožní komunikaci se sousedem (sousedkou).

Každá skupina osmi bitů se označuje jako **byte** (bajt). Bit můžeme označit malým b, byte označujeme velkým B. Pomocí jednoho Byte (Bajtu) můžeme zakódovat až 256 informací.

Běžné metody přenosu dat

Poté, co jsou data převedeny do binární formy, musí být převedeny do signálů, které se do svého cíle posílají přes tzv. síťová média (měděný kabel, optický kabel, elektromagnetické vlnění).

Signál se skládá s elektrických nebo optických vzorců, které jsou přenášeny z jednoho připojeného zařízení k druhému. Tyto vzorce jsou reprezentovány digitálními bity a cestují od zdroje k cíli buď jako elektrické nebo světelné pulzování nebo jako rádiové vlny. Signály mohou být převedeny několikrát, než dosáhnou kýženého cíle.

V počítačových sítích využíváme tyto tři metody přenosu signálu

- elektrické signály

- optické signály
- bezdrátové signály

1.5 Šířka pásma a propustnost

Pokud potřebujeme přehrát film (výukový materiál) nebo přenést velké množství dat potřebujeme spolehlivé a rychlé připojení k internetu, to znamená že potřebujeme zařízení a počítačovou síť, která umožňuje velmi rychlým způsobem přenášet data, tzn. vysílat a přijímat bity.

Různá fyzická média nám umožňují různé rychlosti a v souvislosti s tím se seznámíme s pojmy šířka pásma a propustnost.

Šířka pásma je kapacita daného média. Digitální šířka pásma vyjadřuje množství dat, které může být přeneseno z jedné lokace do druhé za určitou časovou jednotku, typicky používáme bity za sekundu. Běžné hodnoty jsou

- tisíc bitů za sekundu – kilobit (1 Kbps = 1 000 bps = 10^3 bps)
- milión bitů za sekundu – megabit (1 Mbps = 1 000 000 bps = 10^6 bps)
- miliarda bitů za sekundu – gigabit (1 Gbps = 1 000 000 000 bps = 10^9 bps)

Propustnost v počítačových sítích se odkazuje na schopnost sítě přenášet data nebo informace z jednoho místa na druhé za určité období. Jedná se o měřítko, jak efektivně a rychle mohou data proudit skrz síť. Vyšší propustnost znamená schopnost přenášet větší množství dat za krátkou dobu, což je klíčový faktor pro výkon a efektivitu počítačových sítí. Faktory, které ovlivňují propustnost:

- množství dat, která se odesílají a přijímají
- typ přenášených dat
- zpoždění (latence), které je způsobeno počtem a komunikací mezi síťovými prvky, které jsou mezi zdrojovou a cílovou destinací.

Pokud data cestují přes různá média a různé síťové segmenty, pak propustnost není větší než nejpomalejší část spojení na cestě mezi zařízením, které data odesílá a zařízením, které data přijímá.

1.6 Sítě typu klient – server a P2P

Všechna zařízení v počítačové síti označujeme slovem hostitel (anglicky *host*). Každý hostitel může přijímat nebo vysílat informace. V tomto materiálu budeme občas používat místo slova hostitel, slovo počítač, i když se může jednat o libovolné zařízení v síti, jako je mobilní telefon, tablet, notebook, apod.

Z důvodu optimalizace, dostupnosti a výkonu může být na některém z počítačů instalován serverový software. Tento software dělá z daného hostitele (počítače) server, který může poskytovat ostatním zařízením v síti služby jako jsou email, webové stránky, sdílení souborů, správa uživatelů a mnoho dalších. Hostitelé s instalovaným klientským softwarem se nazývají klienti. Klientským softwarem pro poštovní (emailové) služby může být například Microsoft Outlook nebo Mozilla Thunderbird. Mezi software pro prohlížení webových stránek řadíme Chrome, Safari, Edge a další. Pro práci se soubory a sdílenými složkami využíváme například Průzkumník souborů ve Windows nebo např. Total commander (https://www.ghisler.com/).

Sítě, ve kterých všechny počítače hrají roli jak serveru, tak klienta označujeme jako sítě Peer-to-Peer (P2P). Nejjednodušší taková síť je tvořena dvěma počítači, kdy můžeme sdílet například tiskárnu, nebo soubory. V případě více počítačů (více než 2) musíme použít síťové zařízení, které označujeme jako switch (přepínač). Mezi výhody takových sítí patří jednoduché zapojení a správa a třeba i nižší cena. Za nevýhody můžeme považovat nemožnost centralizované administrace a nižší výkon v případě, že stanice slouží jako server i klient zároveň.

2 Síťová architektura

Proč si projít tuto kapitolu?

Seznámíte se s jednotlivými prvky počítačové sítě, naučíte se je graficky znázorňovat. Po absolvování této kapitoly budete schopni vytvořit plán vaší současné, nebo budoucí sítě. Což je jeden z úkolů, který vás ještě čeká. Odhalíme vám tajemství jednotlivých symbolů a jejich úlohu v procesu přenosu dat a informací.

Co se v této kapitole naučím?

Naučíte se identifikovat jednotlivá zařízení síťové infrastruktury, znát jejich funkci, používat nástroje pro tvorbu diagramů.

Časová náročnost: 30 minut

Existují jednoduchá propojení, např. kabel, který nám spojí dva počítače, anebo složitější, kdy data cestují přes celou planetu. Přenášení dat nám zprostředkovává síťová infrastruktura, což je platforma, zajišťující (v ideálním případě) stabilní a spolehlivý přenos.

Síťovou architekturu tvoří tři kategorie hardwaru:

- koncová zařízení
    - zdroje a cíle dat
    - iniciátoři komunikace
- zprostředkující nebo také přenosová zařízení (intermediary devices)
    - zabezpečují průchod dat
- síťová média
    - bezdrátová
    - metalická
    - optická

Tato zařízení a média jsou fyzické prvky, hardware počítačové sítě. Hardware, který známe: počítače, notebooky, switche (přepínače), routery (směrovače), ap (access points - přístupové body, někdy říkáme *wifiny*) a také kabeláž, která nám tyto prvky propojuje. Do této kategorie však patří i prvky, které viditelné nejsou, např. bezdrátová komunikace pomocí radiových frekvencí nebo infračervené záření (dálkové ovladače k televizi nebo dataprojektoru).

Tuto kapitolu využijete pro grafické znázornění vaší školní sítě. Proto se pojďme podívat na běžné grafické znázornění daných zařízení a software, který můžete využít.

2.1 Koncová zařízení

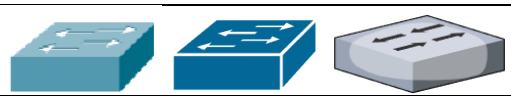
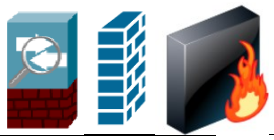
Síťové prvky, které nejspíše znáte nejlépe, jsou koncovými zařízeními, která tvoří rozhraní mezi uživateli a komunikační sítí.

Následující následující tabulka obsahuje běžné grafické symboly, které pak můžete využít pro dokumentaci. Dané symboly můžete také najít v aplikaci https://draw.io, kdy v levém menu dole zvolíte + Další tvary a v kategorii síťování zaškrtnete ☑ Cisco, případně Allied Telesis. A také můžete využít přímo Cisco Brand [5].

Symbol	Popis
	Osobní počítač
	Notebook
	Tablet
	Server
	Tiskárna
	Chytrý telefon, IP telefon

Mezi koncová zařízení také patří skenery, webkamery, dataprojektory, chytré televize, IoT zařízení a další.

2.2 Zprostředkující zařízení

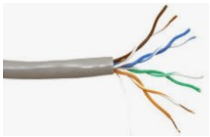
	Switch (směrovač) nám umožňuje propojit koncová zařízení v jedné počítačové síti.
	Router (přepínač) nám umožňuje projit síť s jinou sítí.
	Firewall nám umožňuje v několika úrovních filtrovat provoz mezi počítačovými sítěmi.
	Bezdrátový router v kombinaci se switchem je právě ta krabička, kterou máte s největší pravděpodobností doma.
	Access point (přístupový bod) slouží pro připojení k bezdrátové síti
	Modem je zařízení pro převod analogového signálu na digitální (modulace demodulace). Máte jej v případě používání ASDL, VDSL, internetu po telefonních kabelech.

2.3 Přenosová média

Přenosová média nám slouží k propojení jednotlivých prvků sítě a k přenosu dat mezi nimi. Komunikace probíhá pomocí modulovaného vlnění

Metalická kabeláž (elektrické signály)

- koaxiální kabel – v moderních počítačových sítích ho už neuvidíte, ale stále má uplatnění
- sériová linka – mnoho druhů, využívá se v dálkových linkách, a tam, kde je nepraktická paralelní komunikace
- ethernet UTP – kabel bez stínění, pouze kroucené páry, s tímto a níže uvedenými variantami se asi setkáte nejčastěji



- ethernet STP – stíněné kroucené páry
- ethernet FTP – zkroucené foliované páry

Optická kabeláž (světelné signály)

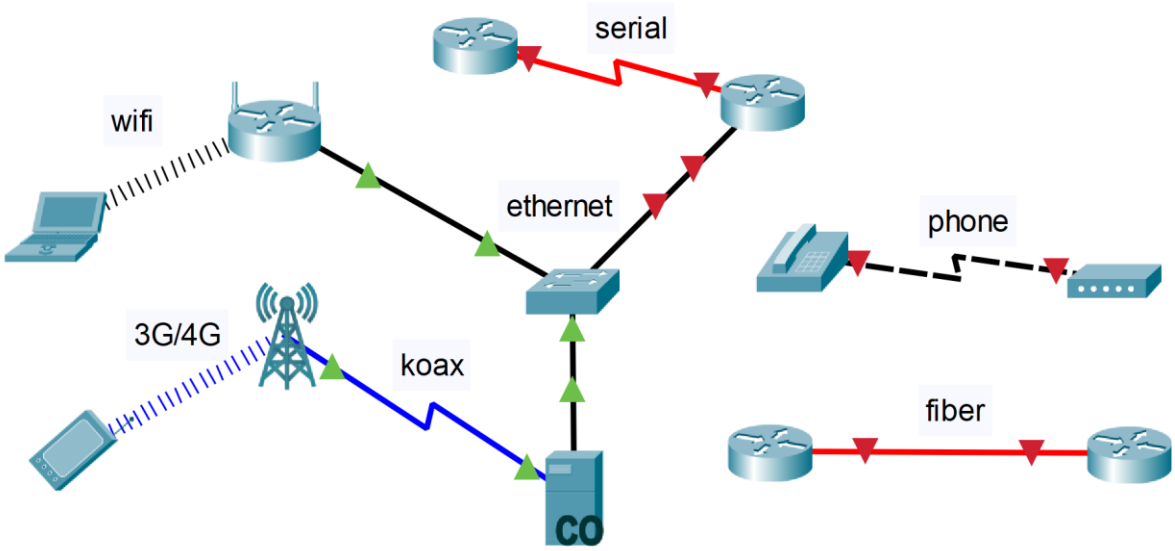
- jednovidová – malé jádro, větší úhel odrazu světla, větší vzdálenosti

- mnohovidová – velké jádro, do 600 metrů

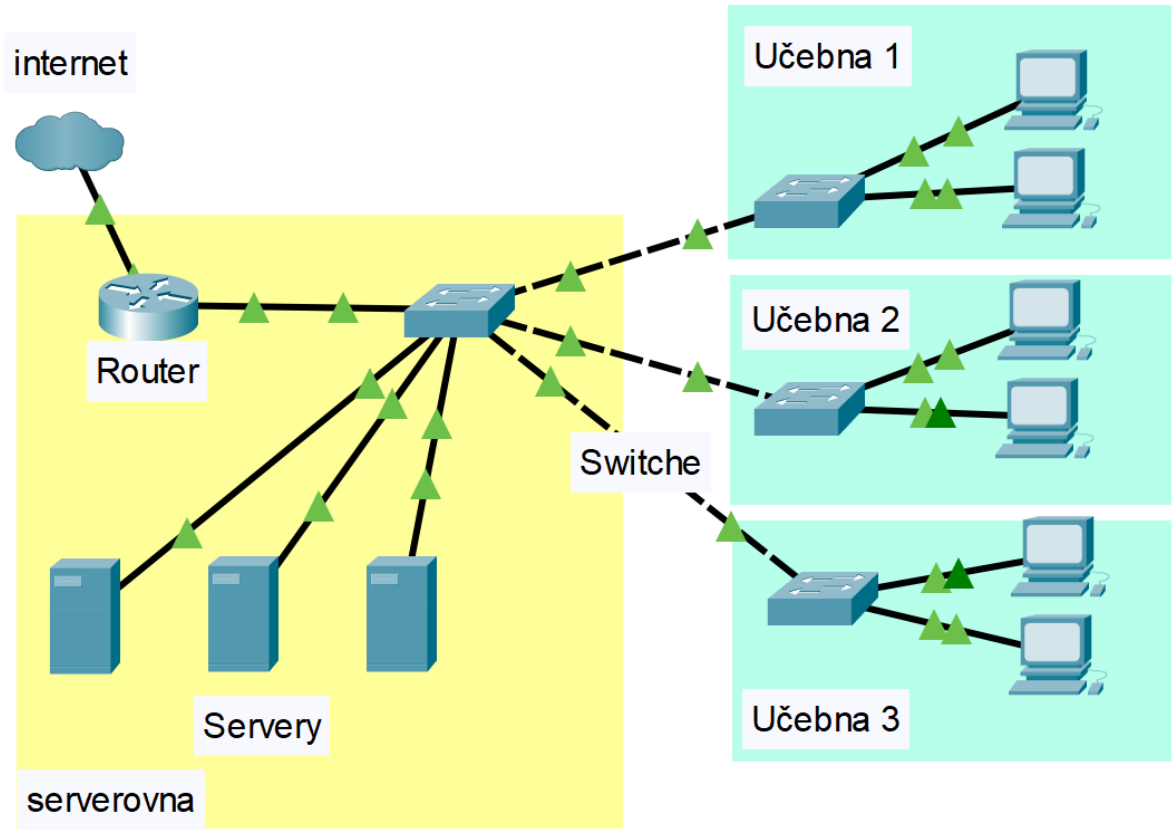
Optická kabeláž je odolná vůči elektromagnetickému rušení, má širší přenosové pásmo a kabely jsou odolnější.

Bezdrátová média (specifické frekvence elektromagnetického vlnění)

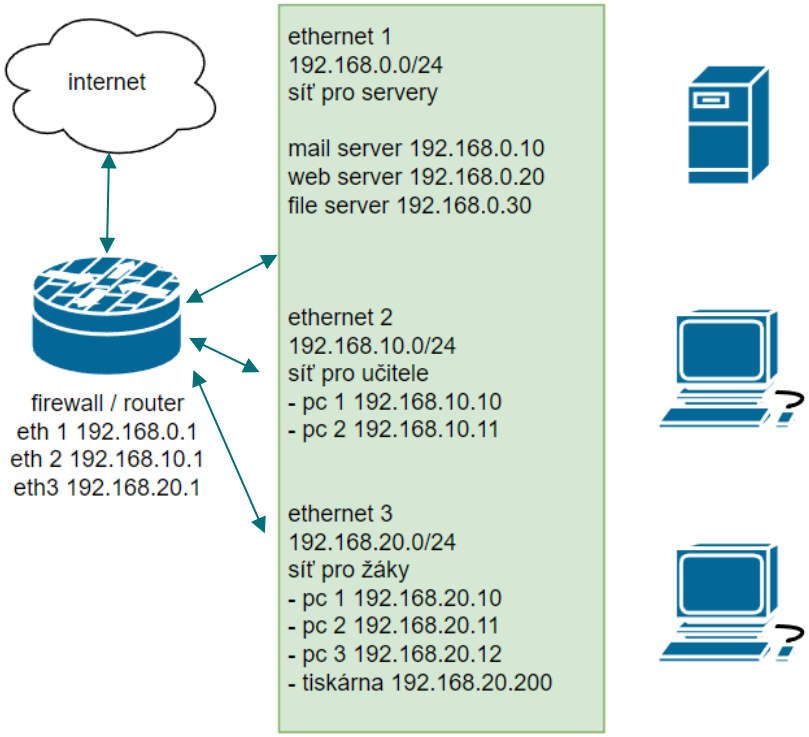
Bezdrátovou komunikaci si přiblížíme pomocí mobilního telefonu. Pokud telefonujeme, využíváme 4G/5G síť našeho operátora. Technologii Bluetooth (jiný typ sítě) využijeme pro připojení sluchátek, reproduktoru nebo chytrých hodinek. Pokud jsme v dosahu našeho AP, můžeme se k naší počítačové síti a také k internetu připojit pomocí Wi-Fi. Máme možnost také využít signál GPS pro určení naší polohy a jako poslední si uvedeme technologii NFC, kterou využíváme např. pro platby nebo připojení k jinému telefonu (dosah komunikace je do 4 cm). Je to tak, v zařízení, které denně používáme máme spojeno 5 druhů komunikačních sítí.



OBRÁZEK 1 UKÁZKA GRAFICKÉHO ZNÁZORNĚNÍ NĚKTERÝCH PŘENOSOVÝCH MÉDIÍ



2 UKÁZKA FYZICKÉ TOPOLOGIE SÍTĚ



3 LOGICKÁ TOPOLOGIE SÍTĚ

3 Komunikace nejen v počítačové síti

Proč si projít tuto kapitolu?

Pokud s někým mluvíte, komunikujete. Pokud posíláte dopis k vánocům svým rodičům, komunikujete. Určitě nepřemýšlíte o pravidlech této komunikace, nicméně ta pravidla existují, a pokud má být komunikace skutečně dobrá a na úrovni, je třeba se jimi řídit. To stejné platí v počítačových sítích. V níže uvedených odstavcích se seznámíte s komunikačními pravidly a protokoly síťové komunikace. Pokud jim porozumíte, budete vědět, jak komunikace v internetu funguje a budete schopni i řešit komunikační problémy.

Co se v této kapitole naučím?

Naučíte se jak vypadá adresa zařízení a jak si můžete otestovat dostupnost dalších zařízení v síti. Seznámíte se s modelem TCP/IP a základními protokoly síťové komunikace. A s dalšími pojmy jako je VLAN a DNS.

Časová náročnost: 90 minut

3.1 Adresace zařízení

Aby spolu mohla jednotlivá zařízení komunikovat, tedy přenášet data, odesílat a přijímat bity, musíme je jednoznačně identifikovat. Každé zařízení připojené k počítačové síti má kartu síťového rozhraní (NIC, network interface card). Každá NIC má jednoznačnou *fyzickou* MAC[1] (Media Access Control) adresu danou výrobcem, každá tato adresa by měla být na světě unikátní, a první polovina adresy většinou identifikuje výrobce. Nicméně upravovat, přepisovat adresu MAC daného rozhraní je velmi jednoduché, některá zařízení, jako jsou například mobilní telefony, umí pro každé připojení generovat novou MAC adresu a tím se dá v určitých sítích zabránit sledování.

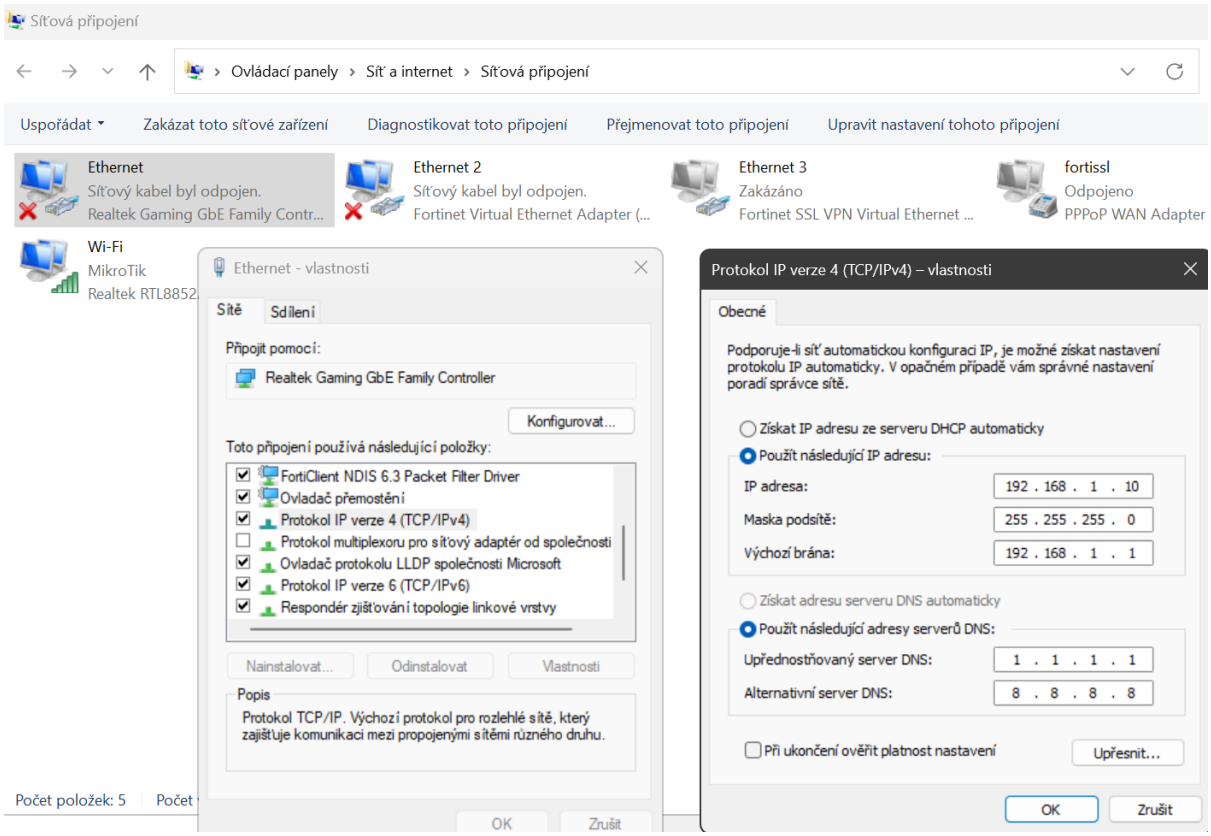
Pomocí NIC můžeme dané zařízení připojit k síti a to pomocí kabeláže, nebo bezdrátově. Krom tohoto fyzického připojení je třeba ještě nakonfigurovat operační systém zařízení tak, aby mohlo dojít k síťovému spojení. Pro *logickou* identifikaci zařízení v síti používáme IP (Internet Protocol) adresu. Každá IP adresa má tři části, které musíme správně nakonfigurovat, aby dané zařízení mohlo přijímat a odesílat data.

- **IP adresa** – jednoznačný identifikátor daného zařízení v síti
- **Maska sítě** – údaj pro dekódování sítě a prostoru pro hosty

[1] Ukázka MAC adresy (48 bitů, šestice dvojciferných hexadecimálních čísel): 01-23-45-67-89-AB

- **Defaultní brána (default gateway)** – adresa síťového zařízení pro připojení k jiné síti, všechny informace (data, packety), které nepatří do naší sítě se automaticky posílají na rozhraní routeru identifikované IP adresou defaultní brány, a router už bude vědět, kam je poslat dál.

Pro úspěšnou komunikaci v síti se využívají jak MAC, tak IP adresy. V případě používání (nejen) webových služeb identifikujeme počítače nikoli pomocí IP adresy, ale také podle doménového jména, například www.npi.cz. Aby toto mohlo fungovat, je třeba využít služby **DNS**, která nám překládá doménová jména na IP adresy.



4 UKÁZKA KONFIGURACE SÍŤOVÉHO PŘIPOJENÍ

```
Connection-specific DNS Suffix  . :
Description . . . . . . . . . . . : Realtek RTL8852AE WiFi 6 802.11ax PCIe Adapter
Physical Address. . . . . . . . . : C8-94-02-A8-ED-E7
DHCP Enabled. . . . . . . . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . . . . . . . : 2a02:f000:f80:1900:12a5:8213:a18b:3a73(Preferred)
Temporary IPv6 Address. . . . . . : 2a02:f000:f80:1900:408a:293:8774:51a7(Preferred)
Link-local IPv6 Address . . . . . : fe80::a898:3af0:4cad:c756%22(Preferred)
IPv4 Address. . . . . . . . . . . : 192.168.111.126(Preferred)
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Lease Obtained. . . . . . . . . . : sobota 6. května 2023 12:23:58
Lease Expires . . . . . . . . . . : neděle 7. května 2023 0:33:58
Default Gateway . . . . . . . . . : fe80::e68d:8cff:fe43:f10d%22
                                    192.168.111.1
DHCP Server . . . . . . . . . . . : 192.168.111.1
DHCPv6 IAID . . . . . . . . . . . : 315134978
DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-28-FC-D5-04-E0-70-EA-AE-7A-0A
DNS Servers . . . . . . . . . . . : 10.88.1.2
                                    10.89.1.2
NetBIOS over Tcpip. . . . . . . . : Enabled
```

5 ZOBRAZENÍ PODROBNÉHO NASTAVENÍ SYSTÉMU POMOCÍ PŘÍKAZU IPCONFIG /ALL

3.2 IPv4 adresa

. Pokud spolu zařízení (domy) chtějí komunikovat, musí být v jedné ulici (v jedné síti). Adresa vysílání (broadcast) je speciální adresa, která nám slouží ke komunikaci se všemi domy v ulici. Minimální hostitel je první možná síťová adresa (dům v ulici s číslem 1) Maximální hostitel je naopak poslední možná síťová adresa (dům na konci ulice). Hostitelé v síti nám udávají, kolik počítačů (zařízení) můžeme v dané síti mít. Pozor, jednu adresu si musíme vyhradit na default gateway, tedy na adresu, která nás propojuje s ostatními sítěmi. V případě, že potřebujete mít v síti více počítačů (zařízení) než 253, tak snižte počet jedniček v masce sítě (místo 24 zkuste 23) a rázem se nám všechno přepočítá. a proto máte k dispozici pouze rozsahy:2

V současné chvíli se již běžně používá také IPv6 adresace, zjednodušeně můžeme říci, že je zde podobná logika a existují i IPv6 kalkulačky.

3.3 Ověření síťové komunikace

Každé zařízení, které chce zasílat data musí mít IP adresu. IP adresy jsou přiřazovány administrátorem, nebo automaticky pomocí správného nastavení DHCP serveru. Pro ověření komunikace mezi dvěma IP adresami můžeme využít nástroj **ping**. Ve svém zařízení si otevřete terminálové okno[2], případně jiné, kam můžete psát příkazy v příkazovém řádku. Nejdříve si otestujte, zda máte správně nastaven IP protokol příkazem ping s vaší adresou (např. *ping 192.168.111.126*), poté můžete vyzkoušet ping na jinou adresu ve vaší síti (192.168.111.1).

[2] Ve Windows zkuste klávesu Win + R a zadejte cmd a zmáčkněte enter.

V případě, že získáte odezvu (např. *Reply from 192.168.111.1: bytes=32 time<1ms TTL=64)* je vše v pořádku a komunikace probíhá jak má.

Pro zobrazení celé cesty mezi dvěma IP adresami můžete využít nástroj **tracert** (ve Windows) nebo **traceroute** (v linuxu). Tracert je síťový diagnostický nástroj používaný k zjištění cesty, kterou datové pakety přecházejí ze zdrojového zařízení (například počítače nebo serveru) k cílovému zařízení (také počítači nebo serveru). Traceroute funguje tak, že pošle sérii paketů s postupně se zvyšujícím "časovým životem" (TTL - Time to Live) směrem k cílovému zařízení. Každý router na trase paketu sníží TTL o jeden, než ho přepošle. Když je TTL sníženo na nulu, router paket zahodí a pošle zpět informaci o své adrese zpět na zdrojové zařízení. Tím získáte seznam routerů, které paket přechází na cestě k cíli. Traceroute zobrazuje každý router na trase, spolu s informacemi o době odezvy (ping) mezi jednotlivými routery. Tímto způsobem můžete zjistit, kolik času trvá přenos dat mezi jednotlivými body na síti a zjistit, jestli existuje nějaké místo, kde se ztrácejí nebo zpomalují pakety.

Traceroute a ping jsou užitečné nástroje pro diagnostiku problémů v sítích.

```
C:\Users\marti>nslookup seznam.cz
Server:  dns.interconnect.cz
Address:  10.88.1.2

Non-authoritative answer:
Name:    seznam.cz
Addresses:  2a02:598:a::79:222
          2a02:598:2::1222
          77.75.77.222
          77.75.79.222


C:\Users\marti>tracert 77.75.77.222

Tracing route to www.seznam.cz [77.75.77.222]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.111.1
  2     6 ms     5 ms     7 ms  10.11.5.146
  3     *        *        *     Request timed out.
  4    13 ms    12 ms    12 ms  253-199-100-185.pragmatel.cz [185.100.199.253]
  5    12 ms    13 ms    12 ms  125-49.interconnect.local [10.88.125.49]
  6    20 ms    11 ms    12 ms  bgp01.sitel.backbone.interconnect.cz [185.14.235.241]
  7    13 ms    13 ms    13 ms  nix2.seznam.cz [91.210.16.194]
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10    13 ms    12 ms    13 ms  www.seznam.cz [77.75.77.222]

Trace complete.
```

6 UKÁZKA VYHLEDÁNÍ ADRESY (NSLOOKUP) A VÝPISU IPV4 CESTY POMOCÍ PŘÍKAZU TRACERT

3.4 Pravidla komunikace a komunikační protokoly

Sítě stavíme pro komunikaci a sdílení informací. Každá komunikace začíná nějakou zprávou nebo informací, kterou posíláme z jednoho zařízení do druhého. Metody, které používáme pro zasílání, příjímání a interpretaci zprávy se mění s použitím dané technologie přenosu. Všechny komunikační metody mají ale společné tři body. Prvním bodem je zdroj zprávy, tedy její odesilatel. Zdrojem zpráv jsou lidé nebo elektronická zařízení. Druhým prvkem komunikace je cíl, tedy příjemce dané zprávy. Třetím elementem je přenosové médium, nebo komunikační kanál.

Pokud komunikujeme tváří v tvář s jiným člověkem, je vhodné si nejdříve dohodnout způsob a pravidla komunikace. Pokud budeme používat hlas, musíme se domluvit na jazyku. Potom si musíme dohodnout formát sdělení, abychom mu rozuměli a nedošlo k nedorozumění, například díky nižší slovní zásobě.

Stejným způsobem fungují komunikační protokoly v počítačové síti.

Komunikace má mnoho podob a forem. Dříve než začneme komunikovat, musíme se dohodnout:

- na způsobu, který použijeme
- jaký jazyk použijeme
- zda potřebujeme například potvrzovat přijaté zprávy

Počítače potřebují pro úspěšnou komunikaci pravidla, které nazýváme protokoly. V drátovém i bezdrátovém prostředí, v lokálních sítích musí všechna zařízení mluvit stejným jazykem, tedy používat společný protokol. Protokoly síťové komunikace definují mnoho parametrů:

- formát zprávy
- velikost zprávy
- časování
- kódování (bitové zprávy do světelných nebo elektrických impulsů)
- zapouzdření (přidávání informací jako jsou síťové adresy, kontrolní součty)
- formát komunikace (zda požadujeme potvrzení o přijetí)

3.5 Síťové protokoly

Komunikace mezi jednotlivými hosty vyžaduje interakci mnoha protokolů. Podíváme se na jednodušší soubor protokolů model TCP/IP, který je definován čtyřmi vrstvami. Reprezentace pomocí vrstev nám umožní lépe vizualizovat celý komunikační proces. Každá vrstva komunikuje pouze s vrstvou nad ní a pod ní.

Vrstva modelu TCP/IP	Popis
Aplikační (application layer)	Poskytuje data uživateli (ftp, http, dhcp, dns)

Transportní (transport layer)	Umožňuje komunikaci mezi zařízeními v síti, navazované spojení (tcp), nenavazované (udp)
Síťová (internet layer)	Určuje nám nejlepší cestu sítí. Zajišťuje adresaci a směrování. (ip, arp, icmp)
Vrstva síťového rozhranní (network interface)	Využívá hardware a síťová media pro fyzický přenos dat (např. síť ethernet)

TABULKA 1 SÍŤOVÝ MODEL TCP/IP

Ve výše uvedené tabulce uvádíme několik zkratek komunikačních protokolů:

- ftp nám zajišťuje přenos souborů mezi počítači
- http(s) umožňuje zobrazovat webové stránky
- dhcp přiděluje ip adresy a celou síťovou konfiguraci
- tcp umožňuje navázat a kontrolovat komunikaci
- udp zasílá data v síti nekontrolovaně
- ip umožňuje adresaci zařízení
- arp pracuje s fyzickými MAC adresami
- icmp odesílá diagnostické informace (ping)
- ethernet kabely už znáte z učeben nebo z domova

Oddělení služeb a funkcí do jednotlivých vrstev nám umožní nezávislý provoz. Pokud použijeme náš počítač, který máme připojený k síti pomocí ethernetového kabelu a chceme navštívit webovou stránku, můžeme ji poté navštívit znovu například pomocí bezdrátového připojení. Funkce webové komunikace (nejvyšší vrstva TCP/IP modelu) není ovlivněna změnou fyzického místa ani způsobem připojení k internetu (nejnižší vrstva TCP/IP modelu).

3.6 Uspořádání počítačových sítí

Zkuste si představit, jak by bylo obtížné komunikovat, kdybychom chtěli poslat zprávu někomu jen tak, že bychom použili jeho jméno. Kdyby nebyly ulice, města, státy. Doručit takovou zprávu by bylo nejspíše zhola nemožné. V síti je MAC adresa podobna jménu. MAC adresa je individuální identita specifického hostitele (počítače), ale nevíme, kde v síti tento hostitel je. Pokud máme všechny hostitelé na internetu, a jsou jich miliony, a každého identifkujeme pouze unikátní MAC adresou, není reálně možné je v tak velké síti najít. Krom toho, ethernetová technologie generuje docela velké množství broadcastové (všesměrové) komunikace. Všesměrové vysílání se zasílá všem zařízením v síti a tím síťovou komunikaci zpomaluje. Co by se stalo, kdyby miliony hostů byly v jedné síti? Jednoduše by nefungovala.

Z tohoto důvodu nejsou velké ethernetové sítě, které mají mnoho počítačů, tak efektivní. Proto je lepší rozdělit větší sítě do menších. Jedním ze způsobu je rozdělit sít do hierarchie.

Síťová hiearchie má 3 základní vrstvy:

- přístupová (access) vrstva – poskytuje připojení jednotlivým hostům, koncovým uživatelským zařízením, setkáme se zde se switchi a bezdrátovými AP
- distribuční vrstva – propojuje menší lokální sítě (vlan) a kontroluje tok mezi sítěmi, máme zde výkonnější switche a routery
- páteřní (core) vrstva – poskytuje vysokorychlostní propojení mezi zařízeními distribuční vrstvy a záložní propojení. Odpovídá za největší přenos dat mezi sítěmi.

Zařízení přístupové vrstvy

Přístupová (access) vrstva je nejnižší úroveň počítačové sítě. Na této úrovni uživatelé komunikují s dalšími zařízeními, využívají sdílených souborů a tiskáren. Přístupová vrstva je první linií síťových zařízení ethernetové sítě. Každý hostitel je připojen svým ethernetovým kabelem nebo bezdrátově.

Ethernet Hub

Původní ethernetová síť fungovala stejně jako ta televizní nebo telefonní. Všichni uživatelé sdíleli přenosové pásmo jednoho kabelu. To se časem stalo nepraktické a nemožné a vývojáři vymysleli zařízení pro propojení více počítačů pomocí více kabelů, tato zařízení se nazývala hub. (čti hab).

Huby měly mnoho portů pro připojení počítačů. Byla to jednoduchá zařízení, která posílala přijaté elektronické signály na všechny své porty. Cílová zařízení zprávu přijala, ostatní ji ignorovala. Nebylo možno zasílat více zpráv najednou. Při větším zatížení docházelo ke značnému zpomalování sítě. Huby jsou považovány za zastaralé a byly nahrazeny ethernetovými switchi (přepínači).

Ethernet switch

Switche jsou schopny z přijatého paketu dekódovat MAC adresu a sestavit si vlastní tabulku svých portů a MAC adres. Pokud switch přijme zprávu, ověří, zda se cílová adresa nachází v jeho tabulce, pokud ano, je vytvořeno spojení a komunikace probíhá pouze mezi dvěma porty a nejsou zatěžovány ostatní. Pokud cílovou adresu nezná, zašle informaci na všechny ostatní porty, krom vysílajícího. Každý z hostitelů porovná cílovou adresu se svou vlastní, a pokud se rovnají, hostitel odpoví odesilateli a switch si danou cílovou adresu přiřadí do své tabulky. Tak se switch naučí všechny MAC adresy připojených hostů a rázem je komunikace efektivní.

Všesměrové vysílání v síti

Občas je třeba, aby jeden host dal o sobě vědět všem ostatním. Takové zprávě se říká broadcast, tedy všesměrové vysílání. Vysílaná zpráva má ovšem pouze jednu unikátní adresu, jak je tedy možné rozeslat zprávu na všechny hosty v síti. Je to tak, že existuje unikátní MAC adresa FFFF.FFFF.FFFF, kterou rozpoznají všichni hostitelé.

Broadcastová doména

Pokud hostitel obdrží zprávu zaslanou na broadcastovou adresu, přijme ji a zpracuje. Pokud hostitel posílá broadcastovou zprávu, pak ji switche posílají na všechny připojené hosty v síti. Proto lokální sítě s jedním nebo více switchi se nazývají broadcastové domény. Pokud je v síti mnoho zařízení, pak tato brodcastová komunikace může síť zahltit a zpomalit. Z tohoto důvodu je lepší rozdělit síť do více sítí, broacastových domén. Zařízení, které to umí se nazývají routery (směrovače).

3.7 Routing (směrování v síti a mezi sítěmi)

Jak nám roste velikost sítě, vzniká potřeba ji rozdělit do menších podsítí. Mezi hlavní důvody patří:

- velikost broadcastu (všesměrového vysílání) – pro fungování sítě je broadcast nutný (zařízení si vyměňují důležité informace), ovšem pokud je ho příliš, může dojít ke zpomalování sítě.
- požadavky na bezpečnost – router nám umožní rozdělit síť do více celků a oddělit tak komunikaci, případně skrýt adresy pro předcházení útoků a řízení přístupu
- fyzická lokace – pokud máme odloučená pracoviště, je logické, že každé pracoviště má svou síť
- logické seskupení – pomocí routerů v distribuční vrstvě umíme rozdělit síť do logických celků, např. učitelé, žáci, hosté, vedení, thp, kamery apod.

Proč potřebujeme routery?

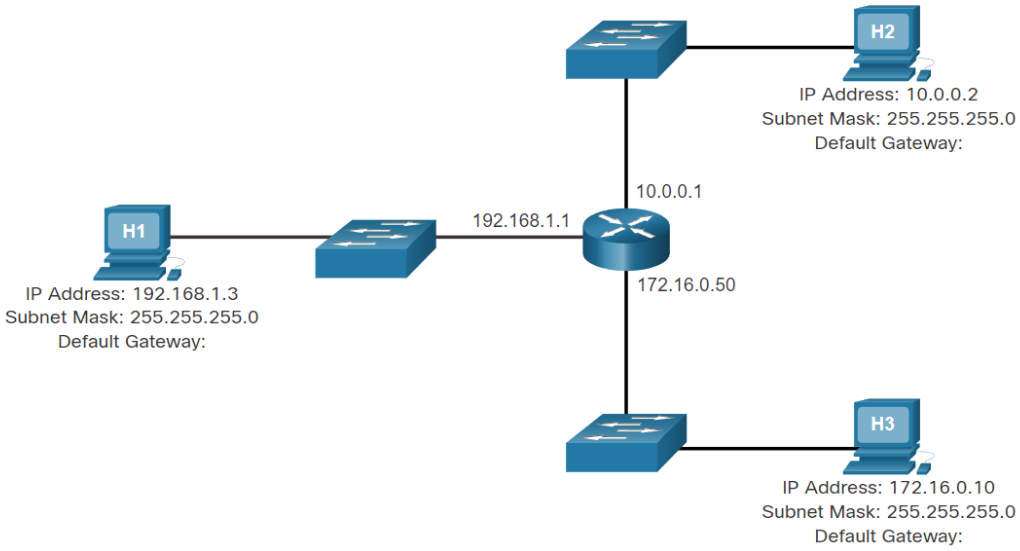
Ve většině situací chceme, aby byla naše síť propojena s ostatním světem, tedy s dalšími sítěmi. Zařízení, která jsou mimo náš síťový rozsah se označují jako vzdálení hostitelé. Pokud zasíláme pakety (data) na vzdálené hostitele, musíme využít router, tedy zařízení, která nás s dalšími sítěmi propojuje.

Každý odesílaný paket (data zabalená a posílaná přes počítačovou síť) obsahuje informaci o IP adrese odesilatele a příjemce, router umí přečíst síťovou část IP adresy, a tak určí, která z připojených sítí je nejlepší pro odeslání dané informace k cíli.

Defaultní brána

V každé IP konfiguraci síťového rozhraní můžeme nakonfigurovat defaultní bránu (default gateway). Je to IP adresa lokální sítě, kterou má rozhraní routeru. Pokud pošleme paket (data) do místní sítě, pak pomocí ARP protokolu umíme zjistit z IP adresy cílovou MAC adresu (jak jsme si

říkali výše, jedná se o unikátní jméno) a data posíláme přímo. V případě, že zasíláme data mimo naši síť, posíláme je na IP adresu defaultní brány, ale proces zjišťování MAC adresy síťového rozhraní routeru je pomocí ARP protokolu stejný.
Každopádně je třeba mít správné nastavení defaultní brány, jinak nebudeme moci s jinými sítěmi komunikovat.



OBRÁZEK 7ZVLÁDNETE URČIT SPRÁVNOU DEFAULTNÍ BRÁNU?

3.8 VLAN

Pokud máme na routeru nedostatek síťových rozhraní, můžeme použít technologii VLAN (Virtual Local Area Network). Tato technologie nám umožňuje rozdělení jedné fyzické sítě na více virtuálních sítí. Tyto virtuální sítě fungují nezávisle na sobě, jako by každá z nich byla samostatnou fyzickou sítí.

Nad jedním rozhraním router jsme schopni vytvořit klidně i 1000 virtuálních sítí. Všechny mohou fungovat na jednom ethernetovém kabelu (VLAN trunk) a jednom switchi, který technologii VLAN umí (hledejte parametr 802.1Q).

Hlavním cílem VLAN je umožnit organizaci a správu sítě podle logických skupin místo fyzických umístění. To má mnoho výhod, zejména v rozsáhlých sítích, kde je potřeba oddělit různé skupiny zařízení nebo uživatelů. Některé z těchto výhod zahrnují zlepšení výkonu sítě, zvýšenou bezpečnost a flexibilitu v konfiguraci sítě.

Při použití VLAN je možné seskupit zařízení do virtuálních skupin na základě různých kritérií, jako jsou porty na síťovém přepínači, adresy MAC nebo IP adresy. Zařízení ve stejné VLAN si

mohou vzájemně komunikovat a vyměňovat data, zatímco komunikace mezi různými VLAN musí probíhat pomocí síťových zařízení, jako jsou routery (směrovače).

Představme si příklad: V jedné budově existuje síť, která obsahuje oddělení pro správu, oddělení pro prodej a oddělení pro vývoj. Každé oddělení by mělo mít svou vlastní síťovou infrastrukturu, ale nemusí být vhodné a efektivní rozšiřovat **fyzickou síť** pro každé oddělení zvlášť. V tomto případě by mohla být použita VLAN, kde by každé oddělení bylo přiřazeno do vlastní VLAN. Tímto způsobem mohou oddělení komunikovat mezi sebou, zatímco komunikace mezi odděleními je řízena směrovačem.

3.9 Stavíme počítačovou síť

Naši síť můžeme buď postavit tak, že všechny počítače budeme mít v jednom síťovém rozsahu, nebo tak, že ji rozdělíme na více sítí připojených zařízením distribuční vrstvy (routerem).

Všechny počítače v jednom síťovém segmentu

V malé síti, může být výhodné, že se všechny počítače navzájem vidí. Pokud ovšem přibývá zařízení, pak větší množství komunikace může snižovat výkon a rychlost.

Výhody:

- lepší pro menší sítě
- jednoduší
- nižní náklady
- počítače se vidí navzájem
- rychlejší komunikace (přímá)
- jednoduší přístup k zařízením

Nevýhody

- více všesměrového vysílání může způsob zpomalení a nižší výkon
- těžko se implementují nějaké preference provozu
- těžko se implementuje nějaké zabezpečení

Více podsítí

Pokud další počítače umístíme do jiné sítě, snížíme tím dosahy požadavky na komunikaci. Ačkoliv počítače nebudou schopni komunikovat s počítači v jiné síti bez potřeby routingu. Routery zvyšují komplexnost sítové konfigurace a můžeme se zde setkávat s latencí a zpožděním.

Výhody:

- vhodné pro větší, složitější sítě,
- dělení na broadcastové domény a snížení množství komunikace
- zvýšení výkonu jednotlivých segmentů

- počítače v jiné síti budou neviditelné
- možnost nasazení bezpečnostních prvků, řízení přístupu

Nevýhody:

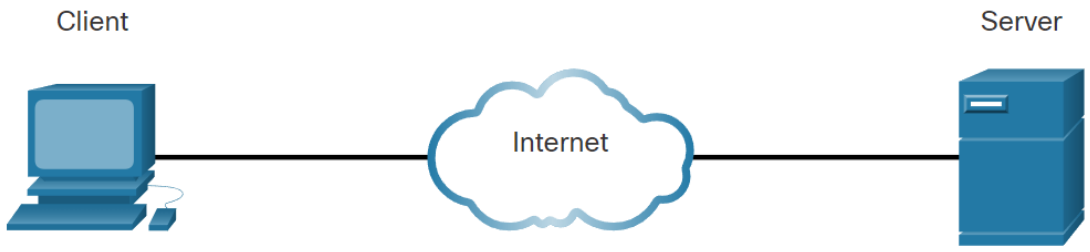
- je třeba distribuční vrstvy (routerů)
- routery mohou zpomalovat přenos zpráv mezi síťovými segmenty
- složitější pro nastavení
- dražší na pořízení

3.10 Služby transportní a aplikační vrstvy

Komunikace mezi klientem a serverem

Každý den využíváme služeb internetu a používáme služby dostupné přes počítačovou síť, komunikujeme s dalšími lidmi, prostě pracujeme. Nemyslíme na servery, klienty a síťová zařízení, která jsou nutná pro odeslání emailu, aktualizaci statusu na sociálních sítích, nebo třeba online nakupování. Většina internetových služeb závisí na interakci mezi klientem a serverem.

Označení server se týká počítače, na kterém běží aplikace poskytující informace nebo služby dalším počítačům připojeným k síti. Určitě dobře znáte webový server. Jsou miliony serverů připojených k internetu, poskytující webové služby, email, finanční informace, stahování hudby apod. Klíčovým faktorem těchto složitých interakcí je, že všechna zařízení fungují na standardech a protokolech.



Příkladem klientského softwaru je webový prohlížeč, Edge, Chrome, FireFox. Na vašem počítači může běžet mnoho typů klientského softwaru, například můžete kontrolovat email, prohlížet webové stránky, používat mesenger, poslouchat audio stream.

Webový server a webový klient využívají specifické protokoly a standardy pro výměnu informací s cílem zajistit, že zprávy jsou obdrženy a je jim rozuměno. Různé protokoly jsou nutné pro dodání webové stránky během 4 úrovních TCP/IP modelu.

Vrstva modelu TCP/IP	Popis akcí pro zobrazení webové stránky

Aplikační (application layer)	http protokol definuje formát požadavků (request) a odpovědí (response) mezi klientem a serverem
Transportní (transport layer)	protokol TCP zajišťuje, že IP pakety (data) jsou poslána kompletně beze ztráty
Síťová (internet layer)	IP protokol zasílá pakety na správnou adresu
Vrstva síťového rozhranní (network interface)	dle typu média je přenos realizován, po drátech, nebo bez

Spolehlivost TCP protokolu

Přes internet se každou chvíli přenesou miliony webových stránek. Je třeba zajistit, aby se každá zobrazila každému klientovi tak jak má. O to se nám stará protokol TCP (Transmission control Protokol)

Pokud je třeba, aby komunikace byla spolehlivá a bezztrátová, používáme právě protokol TCP. Ten rozdělí zprávu na malé kousíčky, kterým se říká segmenty, Segmenty jsou očíslovány a předány IP protokolu pro zabalení do paketů. TCP si pamatuje, jaká čísla segmentů posílá specifickému počítači a specifické aplikaci. Pokud odesilatel neobdrží oznámení během určité doby, předpokládá se, že segmenty jsou ztraceny a dojde k opětovnému odeslání. Neposílá se celá zpráva, pouze ta data, co se ztratila.

U cílového počítače je opět TCP protokol odpovědný za sestavení zprávy ze segmentů a předání aplikační vrstvě. Dalším protokolem, co využívá TCP je například FTP (přenos souborů)

Rychlost protokolu UDP

V některých případech nepotřebujeme spolehlivé doručení, které je pomalejší, protože probíhá ověřování doručení paketu, ale upřednostňujeme rychlost. Proto použijeme protokol UDP.

UDP můžeme využít u streamování audia nebo videa nebo IP telefonie. Oznamovací zprávy by jen zdržovaly komunikaci a znovu posílané pakety by nám pravděpodobně sledování filmu nebo telefonování znehodnotily.

Příkladem může být také internetové rádio. Pokud se nějaké pakety ztratí během svého putování přes internet, pak posluchač uslyší krátkou pauzu. Pokud by v tomto případě docházelo k znovu zasílání paketů, pak by poslech byl rušen o mnoho víc.

Dalším příkladem pro využití UDP protokolu služba DNS, tedy překlad doménových jmen na IP adresu. Většina požadavků se vejde do jednoho paketu a pak nějaké ověřování ztrácí smysl.

3.11 Domain Name Systém (DNS) překlad doménových jmen

Denně poskytuje své služby v internetu statisíce serverů. Každý z těch to serveru má unikátní IP adresu, která jej identifikuje v lokální síti, kde se nachází. Není možné si zapamatovat všechny IP adresy pro všechny servery na světě a proto používáme službu DNS.

Systém překladu doménových jmen (DNS) zajištuje používání doménových jmen. Na základě požadavku, poskytne správnou IP adresu. Doménová jména registrují a organizují správci TLD (Top Level Domain). Nejběžnější domény v internetu jsou .com, .edu a .net, v naší republice .cz, správce cz domény je CZ.NIC, zájmové sdružení právnických osob.

DNS servery

Každý DNS server má tabulku, kde jsou v jednom sloupci jména počítačů a v druhém korespondující IP adresy. Pokud se klient zeptá na jméno serveru, třeba webového, pak potřebuje najít IP adresu, pošle tedy požadavek na DNS server přes port 53. Klient pro odeslání takového požadavku použije IP adresu DNS serveru, kterou má nakonfigurovánu v DNS nastavení v IP konfiguraci počítače.

Jakmile DNS server obdrží požadavek, zkontroluje svou tabulku. Pokud lokální server nemá požadovaný záznam, zeptá se jiného DNS serveru v doméně. Pokud DNS server se adresu naučí, pošle informaci klientovi. Pokud DNS server nezná IP adresu, požadavek vyprší a klient nebude schopen komunikovat s požadovaným serverem. Chybně fungující, nebo chybně nastavený DNS server způsobuje nejběžnější chyby v síti.

4 Virtualizace a cloud

Proč si projít tuto kapitolu?

Už jste použiti virtuální počítač nebo virtuální server? Pokud ne, tak jistě běžně využíváte cloudových služeb, které jsou na virtualizaci založené. Seznámíte se s nástroji, které můžete využit pro virtualizaci na vaší škole.

Co se v této kapitole naučím?

Naučíte se nové pojmy týkající se virtualizace, získáte přehled proč je výhodné virtualizace používat.

Časová náročnost: 30 minut

Virtualizace a cloud jsou dvě vzájemně propojené technologie, které přinášejí mnoho výhod pro podniky a organizace v oblasti správy infrastruktury a poskytování služeb.

Virtualizace zahrnuje vytváření virtuálních instancí hardwaru, operačních systémů, aplikací a dalších zdrojů, které umožňují běh více virtuálních strojů na jednom fyzickém stroji. Tím se dosahuje lepšího využití hardwarových prostředků, snižují se náklady na provoz a správu infrastruktury a zvyšuje se flexibilita a škálovatelnost prostřednictvím dynamického přidělování zdrojů.

Cloudové služby se pak opírají o principy virtualizace a poskytují škálovatelné a elastické prostředí pro ukládání dat, výpočty a poskytování služeb. V cloudu se infrastruktura, jako jsou servery, úložiště a sítě, virtualizuje a je poskytována jako služba. Uživatelé mohou přistupovat ke svým datům a aplikacím prostřednictvím internetu a platí pouze za využívané zdroje.

4.1 Typy cloudových služeb

SAAS Software as a Service (software jako služba) umožňuje uživateli pracovat s aplikacemi, které jsou dostupné zdarma nebo za úplatu (Office365, Google Workspace, SQL databáze apod.)

PAAS Platform as a Service (platforma jako služba) je určena zejména pro vývojáře softwaru a poskytuje prostředí pro nasazení, tvorbu, testování a provozování aplikací.

IAAS Infrastrukture as a Service (infrastruktura jako služba) nabízí virtuální prostředí, které zahrnuje virtuální servery, úložiště dat, virtuální síťové prvky, firewally, switche, routery.

Výhody spojené s kombinací virtualizace a cloudu zahrnují:

- Přístup k informacím odkudkoliv: Cloud computing umožňuje přístup k datům a aplikacím z jakéhokoli zařízení s připojením k internetu. To usnadňuje studentům, učitelům a administrátorům práci mimo školní prostředí a podporuje vzdálené vzdělávání.
- Flexibilita a škálovatelnost: Virtuální prostředí a cloudové služby umožňují školám rychle přizpůsobit svou IT infrastrukturu podle aktuálních potřeb. To znamená, že mohou lépe reagovat na změny v počtu studentů, požadavky na výpočetní výkon a další proměnné.
- Sdílení a spolupráce: Cloudové platformy a nástroje pro spolupráci umožňují studentům a učitelům snadno sdílet dokumenty, projekty a další materiály. To podporuje lepší spolupráci a interaktivitu mezi účastníky vzdělávacího procesu.
- Zálohování a obnova dat: Cloudové služby obvykle poskytují automatické zálohování dat a možnost rychlé obnovy v případě havárie. To pomáhá chránit důležitá data, jako jsou vzdělávací materiály, hodnocení a další informace.
- Snížení nákladů na infrastrukturu: Virtualizace umožňuje efektivnější využívání hardware, což může vést ke snížení nákladů na počítačovou infrastrukturu. Navíc, cloudové služby umožňují školám platit pouze za to, co skutečně používají, což může vést k úspoře finančních prostředků.
- Aktualizace a údržba: Virtualizace a cloud computing umožňují centralizovanou správu softwaru a hardware. To usnadňuje aktualizace, údržbu a správu různých systémů v rámci školní sítě.
- Přizpůsobení vzdělávacích metod: Cloudové nástroje a virtuální učebny umožňují školám a učitelům experimentovat s moderními vzdělávacími metodami, jako jsou virtuální třídy, adaptivní výukové programy a interaktivní technologie.
- Širší dostupnost vzdělávacích zdrojů: Cloudový přístup k digitálním učebním materiálům a online zdrojům může pomoci školám poskytovat širší a aktuální vzdělávací obsah.
- Celkově lze říci, že virtualizace a cloud computing přinášejí do školství moderní a efektivní přístup k IT, což může zlepšit vzdělávací procesy, usnadnit administrativu a zvýšit flexibilitu pro všechny zúčastněné strany.

Virtualizace sítě v cloudu je technologie, která umožňuje vytvářet a spravovat virtuální sítě v rámci cloudového prostředí. Tato virtualizace umožňuje organizacím vytvářet komplexní sítě, které jsou oddělené od fyzické infrastruktury a poskytují flexibilitu, škálovatelnost a efektivitu.

Virtualizační nástroje pro použití ve vlastní síti jsou například:

- VMware vSphere/ESXi: VMware je jedním z předních poskytovatelů virtualizačních technologií. VMware vSphere nabízí širokou škálu funkcí pro správu virtualizovaných prostředí a ESXi je hypervizor, který umožňuje běh virtuálních strojů.
- Microsoft Hyper-V: Hyper-V je virtualizační platforma od společnosti Microsoft. Je integrován do operačního systému Windows Server a umožňuje vytvářet a spravovat virtuální stroje.
- Proxmox Virtual Environment (Proxmox VE): Proxmox VE je otevřený software pro virtualizaci, který kombinuje dvě populární virtualizační technologie: KVM pro virtuální stroje a LXC pro kontejnery.
-

Poskytovatelé cloud computingu v ČR:

Poskytovatelé cloud computingu zapsaní dle ZoISVS platného od 1/9/2021 - Digitální a informační agentura (gov.cz)

Poskytovatelé cloud computingu ve světě:

Amazon Web Services (AWS):

AWS je jedním z největších poskytovatelů cloudových služeb, nabízí širokou škálu služeb, včetně výpočetních instancí, úložišť dat, databází, nástrojů pro umělou inteligenci a strojové učení, analytických nástrojů a dalších.

Microsoft Azure:

Azure je cloudová platforma od společnosti Microsoft, která poskytuje služby pro vývoj, nasazení a správu aplikací a služeb v cloudu. Nabízí výpočetní zdroje, databáze, úložiště, umělou inteligenci, analýzy dat a mnoho dalšího.

Google Cloud Platform (GCP):

GCP je cloudová platforma od společnosti Google, která nabízí infrastrukturu, nástroje a služby pro vývoj a provozování aplikací v cloudu. Obsahuje výpočetní zdroje, úložiště, databáze, umělou inteligenci, strojové učení, analýzy dat a další.

IBM Cloud:

IBM Cloud je cloudová platforma od společnosti IBM, která poskytuje škálu služeb, včetně výpočetních zdrojů, úložišť, databází, umělé inteligence, analýz dat, blockchainu a dalších.

Oracle Cloud:

Oracle Cloud je cloudová platforma od společnosti Oracle, která poskytuje širokou škálu služeb včetně výpočetních zdrojů, úložišť dat, databází, umělé inteligence, blockchainu, analytických nástrojů a dalších.

Alibaba Cloud:

Alibaba Cloud je cloudová platforma od čínské společnosti Alibaba Group, která poskytuje služby včetně výpočetních zdrojů, úložišť dat, databází, umělé inteligence, analýz dat, bezpečnosti a dalších.

DigitalOcean:

DigitalOcean je poskytovatel cloudových služeb, který se specializuje na jednoduché a snadno použitelné výpočetní instance a úložiště dat pro vývojáře a menší týmy.

Toto je jen několik příkladů z mnoha existujících poskytovatelů cloudových služeb. Každý poskytovatel má své vlastní specifické nabídky, ceny a vlastnosti, které je vhodné zvážit při výběru poskytovatele pro konkrétní potřeby.

5 Bezpečnostní minimum

Proč si projít tuto kapitolu?

Bezpečnostní opatření a znalosti v oblasti bezpečnosti vám pomohou chránit vaše zařízení, sítě a data před různými hrozbami, jako jsou malware, phishing, útoky hackerských skupin a další, minimalizovat riziko finančních ztrát a efektivně reagovat na různé bezpečnostní situace.

Co se v této kapitole naučím?

Naučíte se identifikovat jednotlivé hrozby a principy zajištění bezpečnosti v počítačové síti.

Časová náročnost: 60 minut

V dnešní digitální éře, kdy se stále více spoléháme na počítačové sítě a internet pro všechny druhy činností, je bezpečnost naší online přítomnosti nezbytností. Vzhledem k rostoucímu množství hrozeb a útoků, které cílí na počítačové sítě, je ochrana našich systémů, dat a soukromí stále naléhavější.

V následujících odstavcích se zaměříme na důležité aspekty počítačové bezpečnosti a opatření, která můžeme přijmout k ochraně našich systémů a dat.

Pokud se útočník dostane do naší sítě, mohou nastat tyto situace:

- únik informací
- ztráta dat nebo jejich úprava
- krádež identity
- nedostupnost služeb

Únik informací a dat

Pokud se nám někdo dostane do počítače, získává přístup k našim datům. Taková data může útočník využít k vlastní potřebě, prodat, nebo může po nás požadovat výkupné pod hrozbou zveřejnění.

Ztráta dat nebo jejich úprava

Destrukce dat může nastat například zavirováním počítače a formátováním pevného disku. Úpravou dat může útočník měnit například ceník organizace či jiné údaje.

Krádež identity často vede k finančním ztrátám, poškození pověsti oběti, právním problémům a emocionálnímu stresu. Útočník může představovat také riziko pro kontakty oběti, které může oslovit s různými požadavky.

Nedostupnost služeb představuje útok, při kterém útočník přetíží cílový systém nebo síť velkým množstvím legitimního provozu, čímž znemožňuje přístup k požadovaným službám. Jedná se do DoS (denial of service) útoky na servery, síťová zařízení nebo komunikační spojení.

5.1 Externí a interní bezpečnostní hrozby

Externí bezpečnostní hrozby přicházejí z vnějšku organizace, z internetu. Útočníci nemají fyzický přístup do počítačových systému organizace ani do její sítě a snaží se využít zranitelností, bezpečnostních chyb, nebo chyb uživatelů.

Interní bezpečnostní hrozby vycházejí zevnitř organizace. Útočník má fyzický přístup k síti a jejím službám. Také má povědomí o fungování a nastavení sítě a o lidech v organizaci. Často ví kde jsou cenné informace a jak je získat. Né všechny interní hrozby jsou záměrné, může se stát, že uživatel nedopatřením spustí nějaký malware, nebo si přinese virus z domu, aniž by to tom věděl.

Většina organizací je dobře chráněna proti externím útokům, ačkoliv nejdestruktivnější incidenty mohou být výsledkem interního zaměstnance ať už současného nebo bývalého. Pokud zaměstnanec ztratí nebo mu bude odcizen počítač, notebook nebo jiné zařízení obsahující citlivé informace, může to také vést k úniku dat.

5.2 Sociální inženýrství

Organizace může vynaložit obrovské prostředky na technické zabezpečení sítě. Bohužel za 90% kybernetických incidentů může lidský faktor tedy uživatel. Uživatel bude vždy ten nejslabší článek jakéhokoliv zabezpečení. Manipulaci s uživateli a využití jejich slabin nazýváme sociální inženýrství.

Sociální inženýrství je technika používaná útočníky s cílem manipulovat s uživateli a získat neoprávněný přístup k informacím, systémům nebo zařízením. Namísto toho, aby se útočníci zaměřovali na technické slabiny, využívají psychologické a sociální metody k přesvědčování lidí, aby odhalili citlivé informace, provedli nebezpečnou akci nebo umožnili útočníkovi fyzický přístup k danému zařízení.

Pretexting je technika, která zahrnuje vytváření falešných příběhů nebo scénářů s cílem získat důvěru oběti a získat přístup k citlivým informacím. Útočník se vydává za někoho jiného, jako je zaměstnanec společnosti, technik z technické podpory, dodavatel nebo jiná důvěryhodná osoba.

Během pretextingu útočník vytváří přesvědčivý příběh nebo důvod, proč potřebuje od oběti určité informace nebo aby provedla určitou akci. Může se jednat o žádost o ověření hesla, citlivých údajů nebo přihlašovacích informací, žádost o poskytnutí přístupu do budovy nebo k systémům, nebo dokonce o žádost o přenos peněz.

Útočníci při pretextingu často využívají různé taktiky, jako jsou:

- Vytváření důvěry: Útočník se snaží vytvořit důvěru oběti tím, že se představí jako důvěryhodná osoba nebo poskytne detaily, které jsou známé pouze oprávněným osobám.
- Pocit naléhavosti: Útočník vytváří situaci, která vyvolává pocit naléhavosti, aby oběť pod tlakem rychle jednala a poskytla požadované informace.

- Postupné získávání informací: Útočník začíná se získáváním neškodných a necitlivých informací a postupně se posouvá k získávání citlivějších údajů.

Phishing je jednou z nejrozšířenějších technik sociálního inženýrství, která se používá k získání citlivých informací od uživatelů. Útočníci vytvářejí falešné e-maily, zprávy nebo webové stránky, které se zdají být nerozeznatelné od důvěryhodných zdrojů, jako jsou banky, společnosti nebo vládní instituce. Cílem je nalákat oběť, aby poskytla své citlivé informace, jako jsou přihlašovací údaje, hesla, čísla kreditních karet nebo osobní identifikační údaje.

Phishingový útoku může mít následující znaky:

Vytvoření falešného podnětu: Útočník vytvoří e-mail nebo zprávu, která vypadá autenticky a zdá se být od důvěryhodného zdroje, jako je banka, online obchod nebo sociální média. Může to být například varování o neobvyklé aktivitě na účtu, žádost o ověření účtu nebo informace o výhodné nabídce.

Vytvoření pocitu naléhavosti: Útočník vytváří pocit naléhavosti nebo strachu u oběti, aby ji donutil jednat rychle a bez rozmyslu. Může to být například tvrzení, že účet je v ohrožení, že dojde k omezení přístupu nebo že oběť přijde o výhodnou nabídku.

Odkaz na falešnou webovou stránku: V e-mailu je zařazen odkaz, který vede na falešnou webovou stránku, která se velmi podobá skutečnému webu důvěryhodné organizace. Útočníci se snaží, aby tato stránka vypadala co nejautentičtěji a vyzývají oběť k zadání svých citlivých údajů.

Sběr citlivých informací: Pokud oběť podlehne a zadá své citlivé údaje na falešné webové stránce, útočníci je získají a mohou je následně zneužít k nelegálním účelům, jako je krádež identity nebo finanční podvody.

Vishing a smishing jsou další techniky sociálního inženýrství, které se podobají phishingu, ale jsou prováděny prostřednictvím jiných komunikačních kanálů.

Vishing (hlasový phishing) je technika, při které útočníci využívají telefonních hovorů k získání citlivých informací od oběti. Útočníci se vydávají za zaměstnance bank, poskytovatelů kreditních karet, telefonních operátorů nebo jiných důvěryhodných organizací a přesvědčují oběť, aby poskytla své osobní údaje, hesla nebo informace o účtech. Mohou také používat techniky, jako je hraní na emoce, vytváření strachu nebo naléhavosti, aby donutili oběť jednat rychle a bez rozmyslu.

Smishing (SMS phishing) je technika, při které útočníci využívají textových zpráv (SMS) k provádění phishingových útoků. Útočníci pošlou oběti falešné textové zprávy, které se tváří jako oznámení od banky, mobilního operátora nebo jiného důvěryhodného subjektu. Zpráva může obsahovat odkaz na falešnou webovou stránku nebo požadavek na odpověď s citlivými informacemi. Cílem je získat citlivé údaje od oběti, stejně jako při phishingových útocích.

5.3 Malware

Kategorií softwaru, který v počítači nechcete je malware. Mezi malware můžeme zařadit viry, počítačové červy a trojské koně. Malware může poškodit operační systém, ničit data, zablokovat přístup k síti či službám. Může také odesílat data a osobní informace (hesla, karty, fotografie), záznam z webové kamery nebo mikrofonu, a v neposlední řadě stisknuté klávesy.

Virus je programový kód, který se šíří tím, že infikuje a napadá jiné soubory nebo programy. Viry se obvykle připojují k existujícím souborům a šíří se tím, že se spouštějí nebo kopírují do dalších souborů nebo zařízení. Viry mohou způsobit poškození dat, zpomalit systém, vymazat soubory nebo dokonce zneužít systém k nelegálním účelům. Viry se mohou šířit emailem, staženými soubory, pomocí instant messengeru, nebo před usb zařízení.

Červ je škodlivý program, který se šíří bez nutnosti připojení k existujícím souborům. Červové programy se šíří počítačovou sítí a samostatně se replikují na dalších systémech. Červové infekce mohou zatížit síťový provoz, způsobit výpadek systému, ovládnout zranitelné počítače nebo krást citlivé informace.

Trojský kůň (zkráceně trojan) je škodlivý program, který se představuje jako neškodný a užitečný software, ale ve skutečnosti obsahuje skryté škodlivé funkce. Trojské koně mohou sloužit různým účelům, jako je otevírání zadních dveří pro útočníka, sběr citlivých informací, ovládání systému nebo instalace dalšího škodlivého softwaru.

5.4 Spyware a Adware

Spyware je typ škodlivého softwaru, který se tajně instaluje na počítači nebo jiném zařízení a sleduje aktivity uživatele bez jeho vědomí nebo souhlasu. Jeho hlavním cílem je shromažďovat citlivé informace o uživateli, jako jsou přihlašovací údaje, bankovní informace, osobní údaje nebo prohlížené webové stránky.

Spyware může být distribuován prostřednictvím nebezpečných e-mailových příloh, stahování nelegálního softwaru, klikání na podezřelé odkazy nebo prostřednictvím zranitelností systému. Po infekci se spyware skrývá a pokouší se být co nejméně detekovatelný.

Sledovací cookie jsou malé textové soubory uložené na počítači uživatele, které jsou vytvářeny webovými stránkami, které navštěvujete. Tyto soubory obsahují informace o vašem prohlížení webových stránek a jsou používány k sledování vaší aktivity online.

Cookie mohou uchovávat informace o vašich volbách na webových stránkách, například jazykové preference nebo nastavení rozložení stránek. Webové stránky mohou používat cookie k uchování informací o stránkách, které jste navštívili. To jim umožňuje personalizovat obsah a nabízet relevantní reklamy. Cookie mohou obsahovat identifikátory, které jsou používány k rozpoznání uživatele při opakovaných návštěvách webových stránek. Mnoho webových stránek používá cookie k sledování vaší aktivity a zobrazování cílené reklamy. Informace o vašich zájmech a preferencích se mohou sdílet s reklamními sítěmi a třetími stranami za účelem personalizovaného zobrazení reklam.

Ne všechna cookie je třeba zakázat, záleží na našich preferencích.

Adware je zkratka z anglického výrazu "advertising software" a označuje druh softwaru, který je navržen tak, aby zobrazoval reklamy uživateli během jeho interakce s programem nebo webovou stránkou.

Adware může být nainstalován na počítači uživatele spolu s jiným softwarem, často zdarma dostupným na internetu. Jeho hlavním cílem je generovat příjmy pro tvůrce nebo vlastníka softwaru prostřednictvím zobrazování reklam, často ve formě vyskakovacích oken, bannerů nebo textových odkazů.

Pop-up reklamy se zobrazují ve vyskakovacích oknech nad aktuálním oknem prohlížeče. Mohou obsahovat různé typy obsahu, jako jsou reklamy, oznámení, nabídky nebo okna s dotazem na vstup uživatele.

Pop-under reklamy jsou podobné pop-up reklamám, ale zobrazují se pod aktuálním oknem prohlížeče, takže uživatel je nejprve nevidí. Po zavření okna nebo opuštění webové stránky se pop-under reklama objeví na pozadí nebo na nově otevřené kartě prohlížeče.

Oba typy reklam jsou často používány k propagaci produktů, služeb nebo obsahu, a mohou být buďto součástí webových stránek, které navštěvujete, nebo generovány externími reklamními sítěmi.

Zatímco některé pop-up a pop-under reklamy mohou být legitimní a neškodné, jiné mohou být obtěžující nebo dokonce obsahovat škodlivý obsah, jako jsou phishingové útoky, malware nebo nelegitimní nabídky.

5.5 Botnet a zombie

Botnet je síť počítačů, které jsou infikovány malwarovým programem nazývaným bot (zkratka z anglického slova "robot"). Tyto infikované počítače, nazývané také zombie počítače, jsou pod kontrolou kyberkriminálníka a mohou být využity k provádění různých útoků.

Zombie počítače, které jsou součástí botnetu, mohou být napadeny a ovládnuty různými způsoby, jako je infekce malwarem, pomocí phishingu nebo zranitelnosti v softwaru. Jakmile jsou počítače infikovány, jsou propojeny s řídícím serverem útočníka, který může vydávat příkazy a řídit jejich chování.

Botnet může být využit k různým účelům, například:

- k masovému odesílání spamových e-mailů. Zombie počítače slouží jako prostředníci pro rozesílání spamových zpráv, čímž ztěžují identifikaci skutečného zdroje.
- k šíření malware, jako jsou viry, červi nebo trojské koně. Zombie počítače mohou být využity k infikování dalších počítačů a rozšíření škodlivého softwaru.
- k provedení distribuovaného DoS útoku. Tímto způsobem mohou zahlcovat cílové servery nebo sítě velkým množstvím žádostí, což vede k jejich přetížení a nedostupnosti pro legitimní uživatele.

5.6 Bezpečnostní praktiky a procedury

Je nebezpečné předpokládat, že se nemůžeme stát předmětem kybernetického útoku. Je třeba aplikovat základní bezpečnostní opatření jako je přístup pomocí uživatelského jména a hesla do do BIOSU počítače, do operačního systému, do počítačové sítě a také do jednotlivých aplikací.

V rámci bezpečnosti počítačové sítě nesmí existovat žádný anonymní přístup.

Následující odstavce zahrnují základní nástroje pro zajištění bezpečnosti počítačové sítě.

Firewall je zabezpečovací systém, který monitoruje a kontroluje příchozí a odchozí síťový provoz mezi počítačem nebo sítí a vnějším prostředím (například internetem). Jeho hlavním úkolem je chránit počítačovou síť před neoprávněným přístupem, škodlivým provozem a útoky.

Tradiční firewall pracuje na základě pravidel, která určují, jaký provoz je povolen nebo blokován na základě zdroje, cíle, typu služby nebo dalších parametrů.

Firewally, ať už jde o hardware nebo software, jsou klíčovými prvkami zabezpečení sítě. Zde jsou některé obecné výhody a nevýhody obou typů firewallů:

Hardware Firewall:

Výhody:

Fyzická izolace: Hardware firewall je samostatné zařízení, což znamená, že je fyzicky odděleno od ostatních síťových komponent, což může ztížit neoprávněným osobám přístup k němu.

Výkon: Hardware firewally jsou často optimalizovány pro výkon a mohou poskytovat lepší škálovatelnost a výkon než software firewally, zejména v případě velkých sítí.

Jednoduchost správy: Hardware firewall poskytuje centrální bod pro správu bezpečnosti sítě. To může usnadnit správu a sledování síťových aktivit.

Nevýhody:

Náklady: Hardware firewally jsou obvykle dražší než software firewally, a jejich pořízení a údržba může být finančně náročná.

Omezená flexibilita: Některé hardware firewally mohou být méně flexibilní ve srovnání se software firewally, co se týče možnosti konfigurace a aktualizací.

Software Firewall:

Výhody:

Flexibilita: Software firewall je mnohem flexibilnější, umožňuje konfiguraci podle potřeby a často nabízí širokou škálu možností nastavení.

Náklady: Software firewall obvykle vyžaduje nižší investice než hardware firewall, zejména pro domácí uživatele a malé firmy.

Snazší aktualizace: Aktualizace a vylepšení mohou být snazší provádět, protože lze jednoduše nainstalovat nový software nebo aktualizace.

Nevýhody:

Výpočetní zátěž: Software firewall běžící na počítači může zabrat část výpočetního výkonu tohoto počítače, což může ovlivnit celkový výkon.

Omezená fyzická izolace: Software firewall běžící na obecném počítači nemá stejnou fyzickou izolaci jako hardware firewall, což může znamenat větší riziko při fyzickém přístupu k zařízení.

Obecně platí, že optimální volba závisí na konkrétních potřebách a prostředí uživatele. Často se kombinuje použití obou typů firewallů pro dosažení vyvážené úrovně bezpečnosti.

Aktualizace operačního systému a softwaru jsou důležité pro udržení bezpečnosti, stability a výkonu počítače. Zahrnují aktualizace operačního systému (např. Windows, macOS, Linux) a dalšího softwaru, jako jsou webové prohlížeče, antivirové programy, produktivní aplikace a další.

Aktualizace často zahrnují opravy bezpečnostních chyb, které byly v softwaru objeveny. Tím se minimalizuje riziko zneužití těchto zranitelností útočníky. Aktualizace mohou obsahovat opravy chyb, které mohou ovlivňovat stabilitu systému nebo softwaru. Některé aktualizace mohou zlepšovat výkon systému nebo softwaru. Aktualizace také přinášejí nové funkce, rozšíření a vylepšení softwaru.

Je důležité pravidelně sledovat a instalovat dostupné aktualizace operačního systému a softwaru, který používáte. Většina operačních systémů a softwarových aplikací nabízí automatické aktualizace, které umožňují snadnou instalaci nejnovějších verzí.

Antivirové a antimalwarové programy jsou software navržený k detekci, prevenci a odstraňování škodlivého softwaru, jako jsou viry, spyware, ransomware, trojské koně a další formy malwaru.

Antivirové programy se zaměřují především na detekci a eliminaci virů, což jsou škodlivé programy, které se šíří a infikují soubory nebo systémy. Tyto programy monitorují aktivitu systému a hledají známé vzory a chování, které naznačují přítomnost virů. Pokud je detekován vir, antivirový program ho buď odstraní nebo umožní uživateli rozhodnout, jak se s infikovaným souborem zacházet.

Antimalwarové programy mají širší záběr a zaměřují se na detekci a odstranění různých forem malwaru, včetně virů, spyware, ransomware, trojských koní, adware a dalších. Tyto programy používají různé metody detekce, jako jsou heuristické analýzy, sandboxing, chování monitorování

a další techniky, aby identifikovaly potenciálně nebezpečný software a zabránily jeho škodlivým účinkům.

Antivirové a antimalwarové programy obvykle poskytují několik funkcí a vlastností, včetně:

1. Provádění pravidelných skenů systému a souborů s cílem identifikovat potenciálně nebezpečný software.

2. Rozpoznání a odstranění virů, malware a dalších škodlivých programů.

3. Prevence: Monitorování a blokování podezřelých aktivit, snažících se infikovat systém.

4. Aktualizace: Pravidelné aktualizace databází a softwaru, aby byla zajištěna ochrana proti novým hrozbám.

5. Firewall: Některé antivirové programy obsahují také integrovaný firewall, který chrání před neautorizovaným přístupem k počítači nebo síti.

Doporučuje se pravidelně skenovat systém a získávat programy pouze z důvěryhodných zdrojů, abyste minimalizovali riziko infekce malwarem.

Příznaky infekce malwarem se mohou lišit v závislosti na konkrétním druhu malwaru a jeho účelu. Nicméně, některé obecné příznaky infekce malwarem zahrnují:

- zpomalení počítače nebo jiných zařízení. Systém může být pomalejší při spouštění programů, načítání webových stránek nebo provádění běžných úkolů.
- neočekávané chyby, pády programů nebo restarty systému. To může být způsobeno konflikty s existujícím softwarem nebo přímým ovlivněním systémových souborů.
- neautorizované změny v nastavení systému, jako je změna domovské stránky webového prohlížeče, přesměrování vyhledávačů nebo vytváření nových ikon na ploše.
- neobvyklá síťová aktivita, jako je odesílání nebo příjem dat bez povolení uživatele. To může být indikací, že malware komunikuje se vzdáleným serverem nebo se snaží rozšířit na další systémy.
- změny ve webovém prohlížeči: Malware může ovlivnit webový prohlížeč tím, že zobrazuje nechtěné reklamy, přesměrovává na podezřelé stránky, nebo ukládá sledovací cookies.

Firewall sandboxing je technika používaná k izolaci a testování neznámého nebo potenciálně nebezpečného softwaru. Tato technika využívá izolovaného prostředí, nazývaného "sandbox", ve kterém se spouštějí nebo analyzují neznámé aplikace nebo soubory.

Základní myšlenka spočívá v tom, že sandbox vytváří virtuální prostředí, ve kterém může být neznámý software spuštěn, aniž by měl přístup k ostatním částem systému. To umožňuje bezpečný výzkum a testování potenciálně škodlivého kódu bez rizika, že by ovlivnil normální provoz počítače nebo sítě.

Firewall sandboxing se často používá k analýze neznámých hrozeb, například škodlivého softwaru (malware), a pomáhá identifikovat jejich chování a metody šíření. Tímto způsobem může pomoci chránit systém nebo síť před potenciálně škodlivým kódem a přispět k zlepšení kybernetické bezpečnosti.

-

5.7 Shrnutí základních principů bezpečnosti počítačové sítě

- Firewall: Firewall je základní prvek bezpečnosti sítě. Pomáhá kontrolovat přístup do sítě a filtrovat nežádoucí síťový provoz. Správně nakonfigurovaný firewall může zabránit mnoha útokům.
- Antivirový software: Používání antivirového softwaru je důležité pro ochranu před škodlivým softwarem, jako jsou viry, trojské koně a spyware. Aktualizace antivirového softwaru a pravidelné skenování systému jsou nezbytné pro účinnou ochranu.
- Aktualizace a záplatování: Důležitým aspektem bezpečnosti je pravidelné aktualizování operačních systémů a softwaru na nejnovější verze. Vývojáři často vydávají opravy a záplaty, které řeší nalezené bezpečnostní chyby. Aktualizace zabraňuje využívání známých zranitelností útočníky.
- Silná autentizace představuje metodu ověřování identit, která využívá alespoň dvou faktorů s cílem zvýšit bezpečnost. Těmito faktory mohou být informace, které uživatel zná (například heslo), něco, co uživatel vlastní (jako mobilní telefon nebo klíčovou kartu), nebo charakteristika samotného uživatele (jako otisk prstu nebo sken oční sítnice).

V kontextu autentikátoru lze uvést následující tři hlavní kategorie faktorů pro silnou autentizaci:

Něco, co znáte (znalostní faktor):

Heslo nebo PIN kód je běžným zástupcem tohoto faktoru. Uživatel je ověřován na základě znalosti tajného hesla nebo kódu.

Něco, co máte (vlastnický faktor):

Sem patří fyzické objekty vlastněné uživatelem, jako je chytrý telefon, bezpečnostní klíč nebo smart karta. Příkladem může být příjem jednorázového kódu zaslaného na mobilní telefon, který je potřeba zadat k dokončení přihlášení.

Něco, co jste (biometrický faktor):

Tato kategorie zahrnuje biometrické charakteristiky, například otisky prstů, rozpoznávání obličeje, hlas nebo sken oční sítnice. Systém porovnává živý biometrický vzor s uloženým vzorem v databázi.

Využití autentikátoru představuje konkrétní implementaci silné autentizace, kde se často kombinují různé faktory pro dosažení vyšší úrovně zabezpečení. Použití autentikátoru je zvláště běžné v online prostředí, kde poskytuje účinnou ochranu před kybernetickými hrozbami a neoprávněným přístupem.

- Šifrování: Používání šifrování při přenosu dat přes sítě je důležité pro ochranu citlivých informací.
- Zálohování dat: Pravidelné zálohování dat je klíčové pro obnovu v případě úspěšného útoku nebo jiného výpadku. Zálohy by měly být uchovávány na bezpečném místě mimo provozní síť.
- Školení zaměstnanců: Bezpečnost sítě není pouze o technologii, ale také o povědomí a školení zaměstnanců. Je nutné informování zaměstnanců o bezpečnostních postupech, jako jsou silná hesla, rozpoznávání phishingových e-mailů a správné zacházení s citlivými údaji.

- Monitorování a detekce hrozeb: Síťový provoz by měl být průběžně monitorován a analyzován, aby bylo možné detekovat podezřelou činnost a hrozby. Použití bezpečnostních informačních a událostních řízení (SIEM) nebo systémů detekce a prevence útoků (IDS/IPS) může pomoci identifikovat a reagovat na potenciální útoky.

6 Dokumentace

Proč si projít tuto kapitolu?

Dobrá dokumentace počítačové sítě je základ pro řízení IT procesů, pro řešení problémů, pro získávání financí a pro rozvoj. Dobrá dokumentace se vždy vyplatí.

Co se naučím?

Naučíte se, co by měla dokumentace obsahovat..

Časová náročnost: 30 minut

Dokumentace počítačové sítě je důležitou součástí správy počítačové infrastruktury. Zahrnuje informace o topologii sítě, hardware a software, konfiguraci zařízení, připojení k síti a další údaje potřebné pro úspěšnou správu, údržbu sítě a řešení problémů.

Pokud sepisujeme prvky počítačové síti, mluvíme o aktivech, která děláme na primární a podpůrná.

Primární aktiva – jednotlivé informační systémy, nebo celky, které mají pro školu zásadní význam. Dovolil bych si sem zařadit i vzdělávání v počítačových učebnách a prostředky pro výuku v učebnách vybavených audiovizuální technikou.

Podpůrná aktiva – infrastruktura, servery, switche, firewally

Máte-li evidenci aktiv, je dobré zpracovat i registr hrozeb a zranitelností. Poté můžete stanovit rizika, které vašim aktivum hrozí a soubor opatření, jak tato rizika zmírnit.

Takový dokument bývá většinou to jediné, na co management organizace slyší a je pak ochoten dávat peníze do IT infrastruktury.

Dokumentace sítě by měla být pravidelně aktualizována a udržována v aktuálním stavu, aby správci sítě měli k dispozici co nejaktuálnější informace pro úspěšnou správu sítě.

Dokumentace by měla být uložena v bezpečném a přístupném místě. Důležité informace by měly být chráněny heslem nebo jiným zabezpečením tak, aby byly přístupné pouze oprávněným osobám.

6.1 Provozní IT dokumentace

- seznam aktiv (primární i podpůrná)
    - veškerý hardware a software
    - typ podpory – ideální stav je **podporovaný** hw i software (aktualizace, nové verze)
    - definice životního cyklu – vodítko do budoucna, co bude třeba časem vyměnit, podpora plánování
    - popis verze
    - konfigurace (uložená například na githubu, i historie)
    - umístění a inventarizace
    - odpovědnost – kdo má přehled, přístup, kdo se o to stará
    - riziko – co se může stát nebo stupeň rizikovosti
    - vyznačení dílčích celků (učebny, projekty, lokality)
- topologie sítě
    - schéma sítě (HW prvky, co je s čím fyzicky spojené a jak) a seznam IP adres přiřazených jednotlivým zařízením v síti
    - funkční schéma aplikačních vazeb – jakým způsobem si povídají aplikace mezi sebou, propojení databází, provázání aplikací,
    - komunikační schéma sítě – způsoby komunikace, porty, služby
    - schéma bezpečnosti infrastruktury – je dobré, pokud jsou firewally a jejich nastavení popsány ještě odděleně
    - další schémata k popisu funkce specifických částí (energie, kamery, čipy, meteostanice a další IoT)
- uživatelé – řízení přístupu ideálně identity management software
    - architektura LDAP / AD
    - proces přidávání a schvalování uživatelů
    - revize přístupů a evidence změn
    - evidence a řízení speciálních účtů (root, administrator adt)
    - rozdělení práv a postupy pro případ nepřítomnosti majitele admin účtu
    - evidence vzdálených přístupů
    - retence hesel – password management
    - popis kontrol – jak kontrolujete uživatele a pohyb po systémech
- zálohování a obnova / krizový scénář
    - definice potřeb záloh dat/systémů – jak budeme řešit obnovu

        - pravidlo 3-2-1+1
            - veškerá data 3x
            - na 2 různých technologiích
            - 1x mimo lokaci
            - 1x offline
    - definice akceptovatelnosti stáří dat při obnově
    - čas obnovy – je třeba testovat, jak dlouho obnova bude trvat
    - postup obnovy
    - krizové scénáře (více verzí např. v případě ztráty více systémů či celé lokality – tvorba disaster recovery scénáře ve spolupráci s vedením společnosti)
- procesy a odpovědnosti (ITIL)
    - jak přidávám uživatele
    - jak zakládám nový server
    - jak dělám pravidla na firewallu
    - popíšu jednotlivé běžné činnosti, změny, reakci na problémy
    - je dobré vycházet z ITIL[3] (soubor nejlepších praktik pro řízení IT)
- plán rozvoje sítě
- historie změn

[3] ITIL tajemství zbavený - CleverAndSmart Management Consulting

Další zdroje a inspirace

[1] SAMURAJ-cz.com - administrace, počítačové sítě, Cisco, Microsoft, Fortinet, NetApp, Veeam, VMware [online]. Petr Bouška, 2023 [cit. 2023-05-03].
[2] Skills for All by Cisco: Free Online Tech Courses For All [online]. Cisco, 2023 [cit. 2023-05-03].
[3] itnetwork.cz - Učíme národ IT [online]. David Čápka, 2023 [cit. 2023-05-03].
[4] https://www.drawio.com/ (https://draw.io) [online] Aplikace pro tvorbu diagramů [cit. 2023-05-03].
[5] Network Topology Icons - Doing Business With Cisco - Cisco [online]. Cisco, 2023 [cit. 2023-05-03].
[6] Standard konektivity a bezpečnosti škol - edu.cz [online]. MŠMT, 2023 [cit. 2023-05-03].
[7] ITIL tajemství zbavený - CleverAndSmart Management Consulting [online]. Miroslav Čermák, 2023 [cit. 2023-05-03].