Uživatel počítačových sítí

Intenzivní kurz IBA

Daniel Klimeš, Roman Šmíd

Organizace kurzu

- Dvoudenní kurz
  - Dnes teoreticky
  - Následně prakticky – Kamenice 3 – 6.patro
- Podmínky zápočtu
  - Registrace v is.muni.cz
  - Účast na teoretické části
  - Účast na praktické části nebo odpověď na praktický test

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Osnova

- O IBA
- Pojmy, termíny
- Počítačová síť - základní hardware a topologie
- Připojení k síti
  - Možnosti připojení
  - Co je zapotřebí
  - Srovnání
- Síťové služby
  - DHCP, DNS, HTTP, FTP
  - E-mailové
- Bezpečnost na síti
  - Hesla a průzkumník vůbec, Firewall, mail spyware phishing
- Šifrování a elektronický podpis

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

O IBA

- **Institut biostatistiky a analýz Lékařské a Přírodovědecké fakulty MU**
- je pracovištěm pro vzdělávací a vědeckovýzkumnou činnost v oblasti
  - **analýzy biologických a klinických dat**,
  - organizace a **managementu klinických studií a registrů**,
  - vývoje softwaru a aplikace ICT.
  - Výuka matematické biologie

- http://www.iba.muni.cz/

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Data a jejich objem

- Jak vyjádřit informaci
- **1 bit (b) - základní informační jednotka 1/0**
- **1 Byte (B) – 8 bitů, celé číslo od 0 do 255,**
  - **1 textový znak (ASCII)**
- 1 Kb - 1024 bitů
- 1 KB - 1024 Bytů
- 1 MB - 1024 KB = 1048576 Bytů = 8388608 bitů
  - Někdy je K = 1000 x
- KiB je vždy 1024 – norma (omezené využívání)

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Komprese dat

- Čeho a k čemu se využívá komprese?
- Datový objem x informační hodnota

- Bezeztrátová x ztrátová komprese
  (Zip, rar) x (jpg, mp3,divx)

- Dokumenty MS Office 2007 a novější (Docx, xlsx, pptx) jsou zazipované soubory – další komprese bez efektu

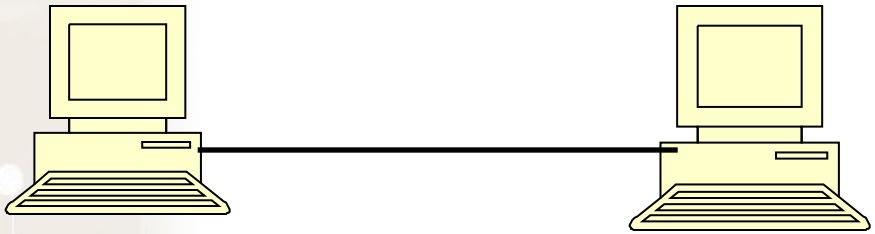
Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.

Počítačová síť

- Propojení dvou a více počítačů
- Součástí sítě jsou síťové prvky
  - PC se síťovou kartou či modemem
  - Kabeláž (metalická, optická)
  - Rozbočovače, směrovače a přepínače
  - Zařízení poskytující síťové služby, síťové tiskárny…
- Kvalitu sítě, respektive konkrétní cesty v síti, lze hodnotit podle
  - Propustnosti (rychlosti) sítě - (K/M/G)bity za sekundu
  - Rychlosti odezvy (milisekundy) - ping

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Propojení dvou počítačů



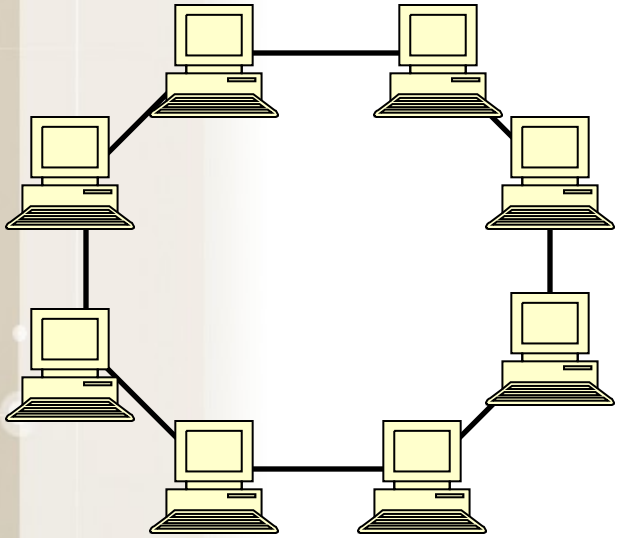
Potřebné vybavení
- 2 síťové karty
- UTP křížený kabel

Alternativy:
- bezdrátové připojení - Bluetooth
- Wi-fi
- propojení kabelem přes USB
  - (v. USB 1.1 = 1.5Mbit/s; v2.0 = 400Mbit/s; v3.0 = 5Gbit/s)
- “kabelový” přenos

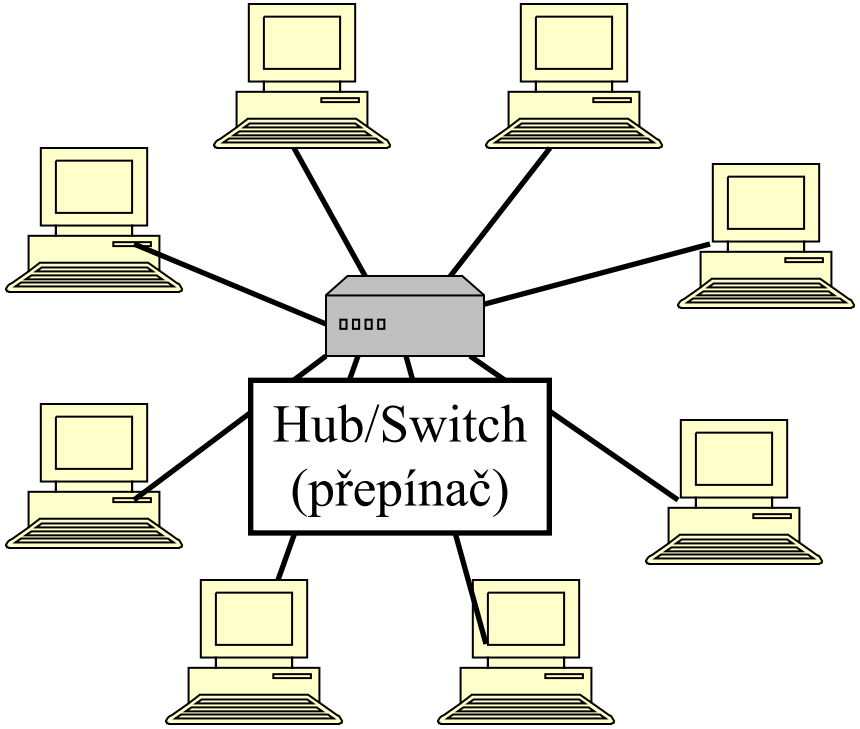
Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Propojení více PC - síť

historický způsob
topologie kruh

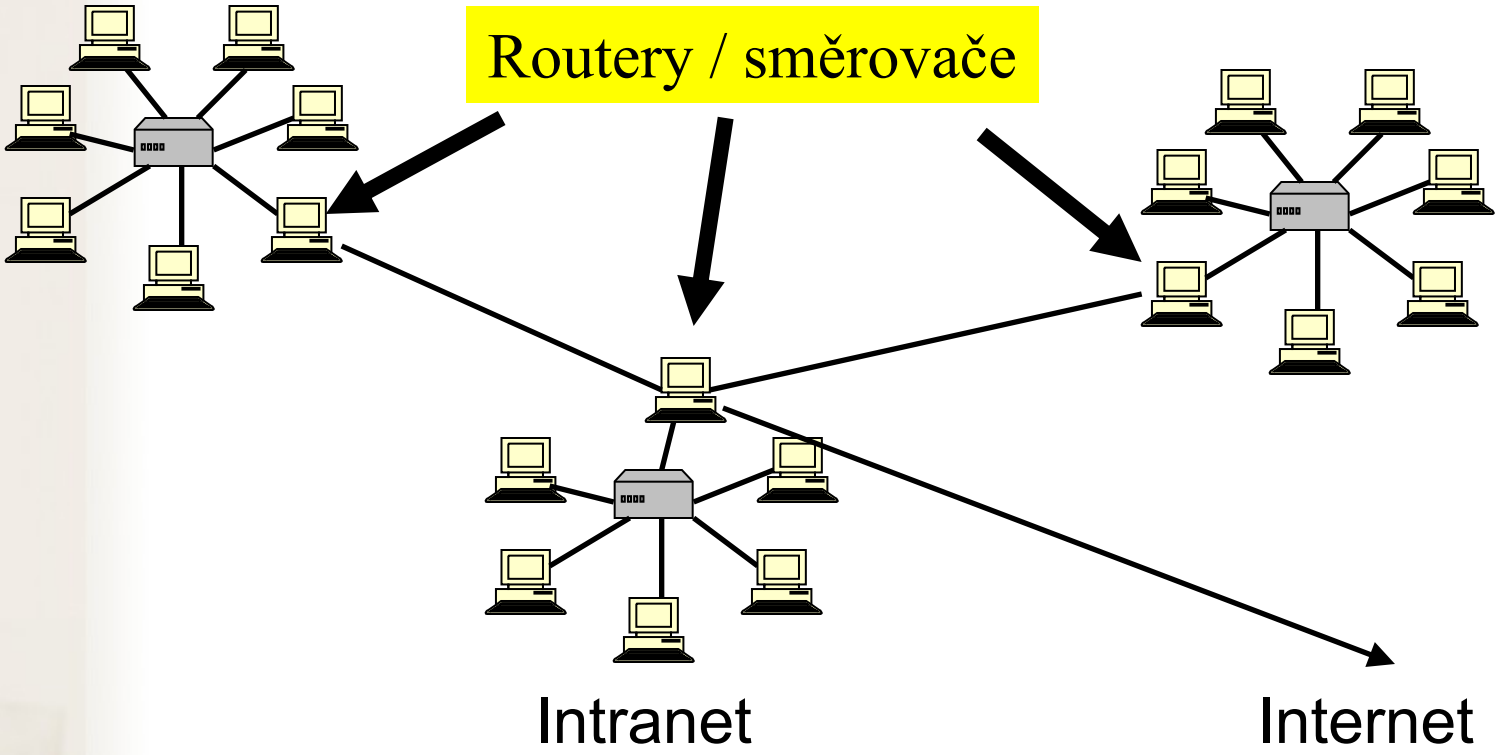


současný způsob
topologie hvězda



Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Propojení lokálních sítí



Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Identifikace PC v síti

- Identifikace síťové karty
  - Celosvětově „jedinečná“ MAC adresa (fyzická adresa)
  - 00-0A-E4-C0-36-81
- IP adresa (obdoba IČO nebo telefonu)
  - Celosvětově „jedinečné“
  - 147.251.147.76
- Internetové jméno (obdoba pošt. adresy) - URL
  - Celosvětově jedinečné
  - www.iba.muni.cz
- Windows jméno (číslo kanceláře)
  - Lokální jméno pouze v rámci místní sítě
  - Server1, kancelar1, kancelar2

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

IP adresa

IPv4 x IPv6

- IPv4: 32b = 2^{32} IP adres => cca 4 * 10^{9} adres
- IPv6: postupně zaváděna 128b => 3,4 * 10^{38} adres

- Identifikace sítě
- Identifikace počítače

```
147.251.147.76
255.255.255.0
```

ID sítě

ID počítače

Stejný počítač přenesený do jiné sítě má zpravidla jinou IP adresu!

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

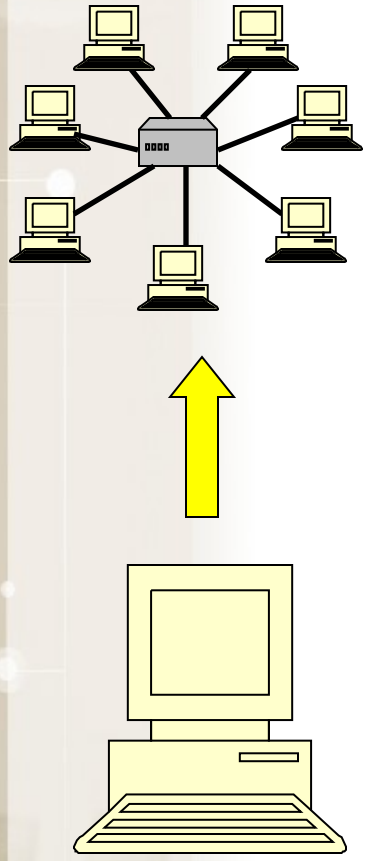
IP adresa

- Pevná x dynamická IP adresa
- Veřejná x neveřejná IP adresa
  - Neveřejná IP není celosvětově unikátní – pouze v rámci lokální podsítě
  - Neveřejné adresy nemívají přiřazené internetové jméno
  - Dynamická + neveřejná IP – typický konzument služeb
  - Pevná + veřejná IP – typický poskytovatel služeb

http://www.ip-adress.com/

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

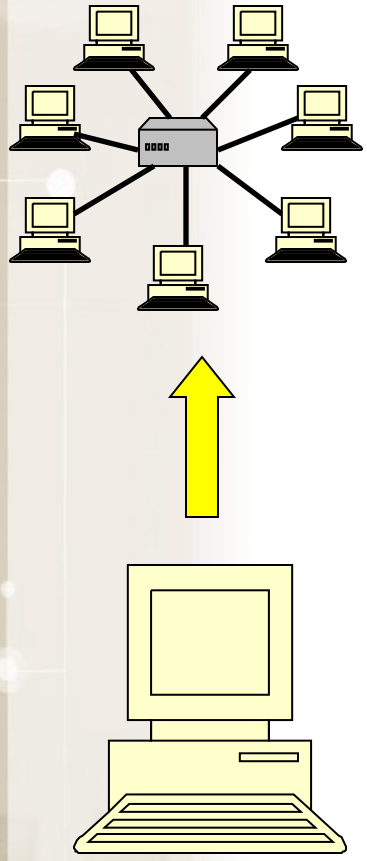
Fyzické připojení PC do sítě



- Pevné páteřní připojení
  - Síťová karta (až 1 Gb/s)
- Telefonní linka
  - ADSL modem
- Mobilní připojení
  - Modem nebo mobilní telefon
- Bezdrátové připojení – WIFI
  - Speciální zařízení/karta, anténa
- Kabelová televize
  - Modem

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Telefonní linka



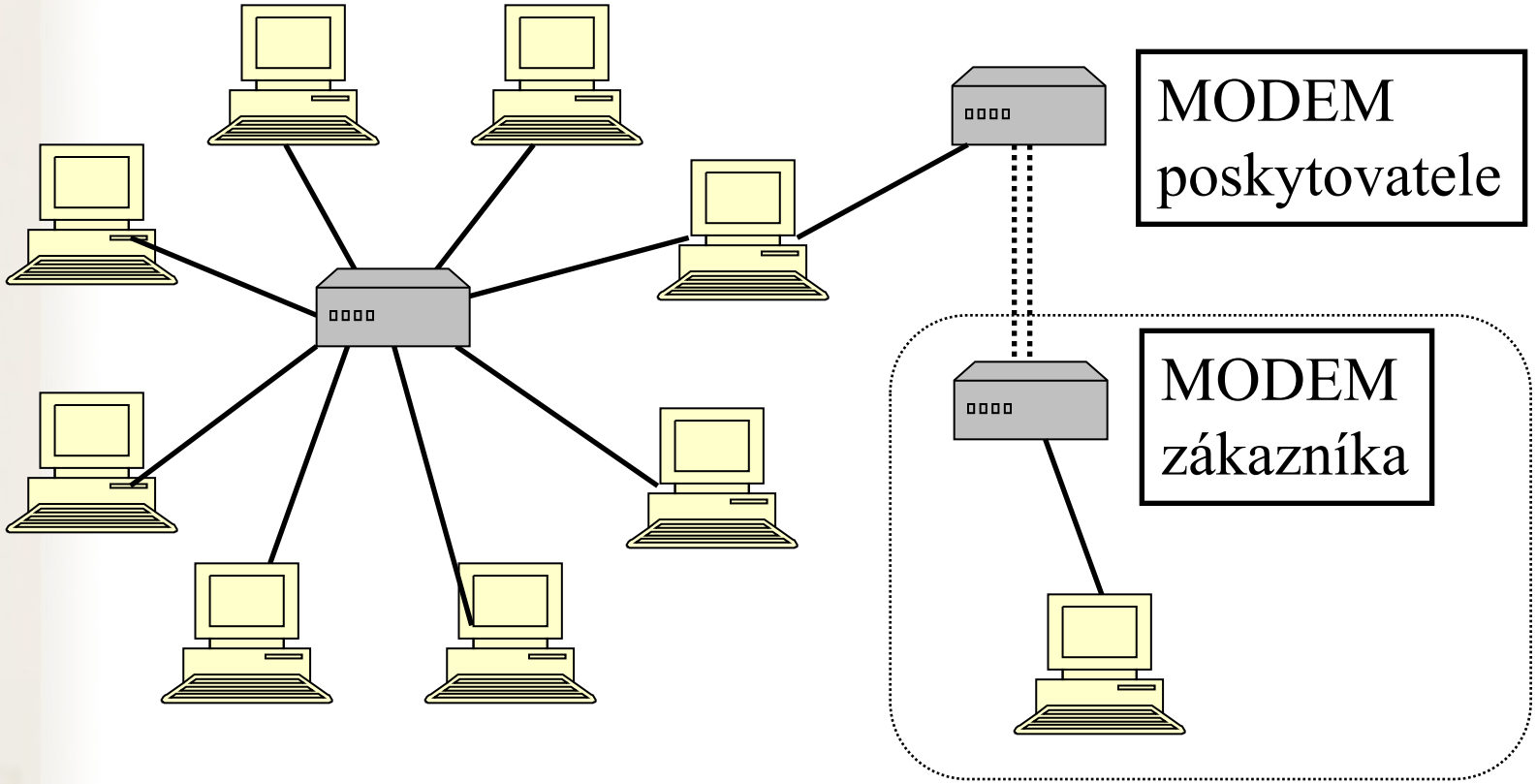
- ~~Vytáčené připojení (až 56 kb/s)~~
- ~~ISDN (až 128 kb/s)~~
- ADSL (až 16 Mb/s i více (VDSL))
  - www.dsl.cz

- Každý typ vyžaduje specifický modem

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Telefonní linka 1



Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

ADSL připojení - rychlost

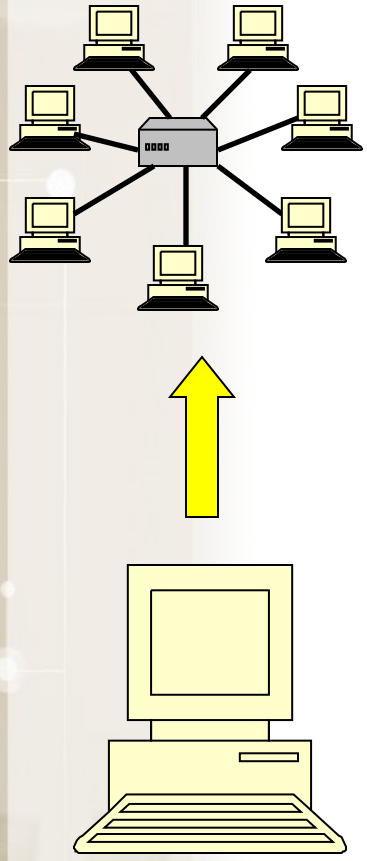
Průměrné rychlosti DSL v síti O2 II.13	ADSL		VDSL	
	8 Mbit/s	16 Mbit/s	20 Mbit/s	40 Mbit/s
O2 Internet	4 620	7 850	14 173	20 837
T-Mobile	5 027	5 133	13 626	-
Průměr všech měření	4 761	7 689	14 114	20 161
% z objednané rychlosti	*60%*	*48%*	*71%*	*50%*

Průměrné rychlosti DSL v síti O2 IV.12	ADSL		VDSL	
	8 Mbit/s	16 Mbit/s	16 Mbit/s	25 Mbit/s
O2 Internet	4 909	6 418	9 878	12 748
T-Mobile	5 505	6 359	8 770	-
Průměr všech měření	5 085	6 493	9 792	12 567
% z objednané rychlosti	*64%*	*41%*	*61%*	*50%*

zdroj: www.dsl.cz

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Kabelová televize



- V místech dostupnosti kabelové televize
- Rychlost až 100 Mb/s
- Metalické x optické připojení
- Speciální modem
- www.upc.cz
- www.netbox.cz
- http://internet.moravianet.cz/
- http://www.internetprovsechny.cz/catv.php

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

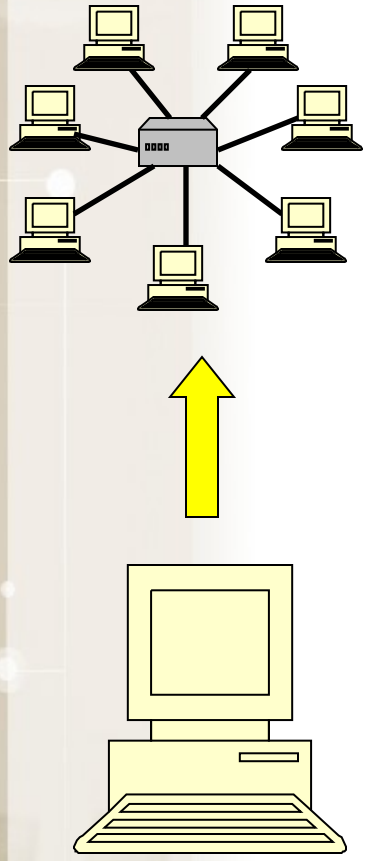
Kabelová televize

Poskytovatel	Počet měření	Download [kbps]	Upload [kbps]	Ping [ms]
RIO Media	492	19 778,29	10 207,09	34,78
UPC Česká Republika	3602	15 818,36	3 028,37	22,12
UPC-Slovensko	267	13 830,79	2 987,34	29,84
NETBOX	198	13 278,92	5 909,06	10,85

Zdroj: http://www.internetprovsechny.cz/ - duben 2012

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

WiFi-připojení



- Komerční/komunitní sítě
- Lokální domácí síť
- Rychlost typicky až 11Mb/s (54 Mb/s)
- Speciální cenově dostupné vybavení
- Zabudované v notebooku - indoor
- Riziko rušení, odposlouchávání, neoprávněného připojení
- Přístupový bod /Access point/ hot spot
- www.internetprovsechny.cz
- http://www.muni.cz/ics/services/wifi
  - Eduroam

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

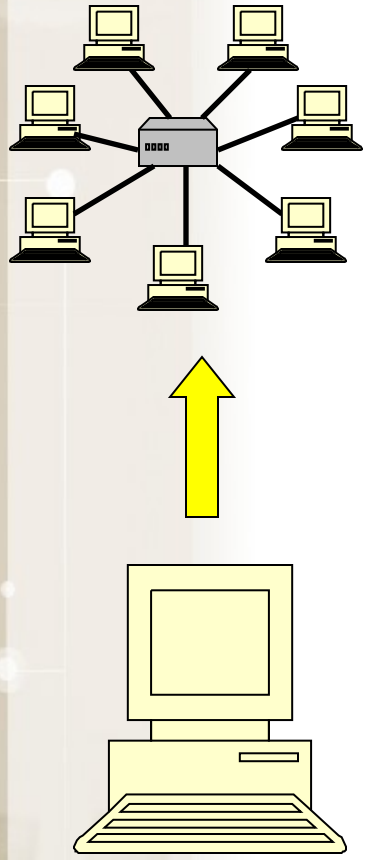
Wi-Fi připojení - rychlost

Přehled průměrných rychlostí vybraných WiFi sítí II.13			
síť	rychlost v kbit/s	síť	rychlost v kbit/s
AB-NET	5 849	Nitex	5 149
Airwaynet	5 106	Nová Morava	11 892
a-net Liberec	5 629	N-SYS	10 788
AP Sobol	3 811	NWT	4 898
B-Net Brumovice	6 094	OK-NET	4 011
Cerberos	8 523	OrbisNet	4 093
Cyrilek.net	13 643	PilsFree	10 200
Eurosignal	7 782	Praha12.Net	13 660
Fialanet	7 644	PVfree.net	7 793
Fifejdy	7 952	Rapidnet	8 984
Fortech	5 462	RIO Media	7 657
GEMNET	6 426	RPSNet	4 085
GRAPE SC	5 759	SatNET	3 977
GREMnet	9 679	Sauron	7 206
HKFree	10 888	SELECT SYTEM	5 428
HnojnikNet	8 727	SilesNet	8 090
HorkaNet	4 146	Skvely.net	7 874
Infos	3 362	Sprintel	4 329
Internethome	5 527	Starnet	12 268
JON.cz	6 504	Tkom CZ	7 272
LEVNET	3 440	Tlapnet	8 008
Ludík	8 108	TTNET	10 147
M.NET	5 160	Újezd.Net	8 812
MAXXNET	6 081	UNET	4 412
Metronet	5 416	vasesit.cz	4 864
MOVSET	7 679	Vejnet	8 748
Náš-Net	6 987	Warnet.cz	7 198
Náchodnet	2 082	Wifcom	8 866
NET On Line	7 287	za200.cz	8 283
NetFree	8 863	Ostatní	6 734
WiFi celkem		7 073	

zdroj: www.dsl.cz

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Mobilní připojení



- GPRS (až 128 kb/s)
  - Mobilní telefon s podporou GPRS
- EDGE (až 512 kb/s)
  - Mobilní telefon s podporou EDGE
- CDMA (až 800 kb/s)
  - www.cdma.cz
  - CDMA modem
- 3G-UMTS/HSDPA/4G (1024 kb/s a více)
  - Speciální modem
  - Novější mobilní telefon nebo notebook
  - Omezené pokrytí ČR

http://www.cdma.cz/pic/pokryti_cdma.gif
http://www.cz.o2.com/osobni/cz/pece_a_podpora/podpora_a_servis/mapy_pokryti.html
http://t-mobile.cz/Web/Residential/TarifySluzby/MapaPokrytiCR.aspx

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Mobilní připojení - rychlost

Průměrné rychlosti internetu v mobilních sítích II.13			
síť	rychlost v kbit/s	měsíční změna	meziroční změna
T/O2 GPRS/EDGE	134	0%	14%
T-Mobile GPRS/EDGE	120	1%	-4%
Vodafone GPRS/EDGE	106	-1%	9%
T/O2 CDMA	932	18%	6%
U:fonův internet CDMA	558	-10%	-8%
T/O2 3G	3 117	3%	50%
T-Mobile 3G	5 260	-3%	71%
Vodafone 3G	4 600	-5%	56%
Mobilní internet celkem	2 631	-11%	168%

Průměrné rychlosti internetu v mobilních sítích IV.12			
síť	rychlost v kbit/s	měsíční změna	meziroční změna
T/O2 GPRS/EDGE	99	-20%	-29%
T-Mobile GPRS/EDGE	128	-3%	3%
Vodafone GPRS/EDGE	94	-3%	-22%
T/O2 CDMA	717	-8%	-18%
U:fonův internet CDMA	585	4%	-1%
T/O2 3G	2 328	3%	22%
T-Mobile 3G	3 960	15%	42%
Vodafone 3G	3 268	6%	74%
Mobilní internet celkem	1 812	5%	145%

zdroj: www.dsl.cz

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Typy připojení – srovnání

	Výhody	Nevýhody
Kabelová televize	rychlost, spolehlivost	dostupnost
Telefonní linka	dostupnost	cena
WI-FI	cena, dostupnost	spolehlivost
Mobilní připojení	dostupnost	rychlost spolehlivost cena

Aktuální rychlost mezi dvěma počítači lze orientačně změřit pomocí speedmetrů
Např.: http://nastroje.lupa.cz/mereni-rychlosti/, www.dsl.cz

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Výběr připojení k internetu

- Způsob použití – pevné PC x notebook
- Dostupnost v daných lokalitách, pokrytí
- Rychlost, většinou v Kb/s
  - symetrické x **asymetrické** (download, upload)
  - (např.: 2048/128)
- Agregace (např.: 1:32) – (ADSL, bezdrátové připojení)
- Fair user policy (FUP) – omezení rychlosti po přenesení určitého množství dat

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Vzájemná komunikace počítačů v síti

Model Klient – Server

Kdo, po kom, co chce

UŽIVATEL

KLIENT

SERVER

Požadavek

Odpověď

- Počítač
- Program

- Počítač
- Program = SLUŽBA

Pro koho, od koho

Jakého používáte klienta pro danou službu?

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.

EVROPSKÁ UNIE

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Konfigurace připojení

- Automatické x manuální

▪ IP adresa	např.: 147.251.147.250
▪ masku sítě	např.: 255.255.255.0
▪ IP adresa brány (gateway)	např.: 147.251.147.1
▪ IP adresy DNS serverů	např.: 147.251.26.1

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.

EVROPSKÁ UNIE

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Služba DHCP

- Automatická konfigurace síťového připojení vašeho počítače v lokální síti
-
- DHCP protokol nastavuje veškeré parametry nutné pro připojení PC do sítě, zejména
  - IP adresa PC
  - masku sítě
  - IP adresa brány (gateway)
  - IP adresy DNS serverů
- Připojení počítače (síťové karty) může povolit/zakázat administrátor sítě

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.

EVROPSKÁ UNIE

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

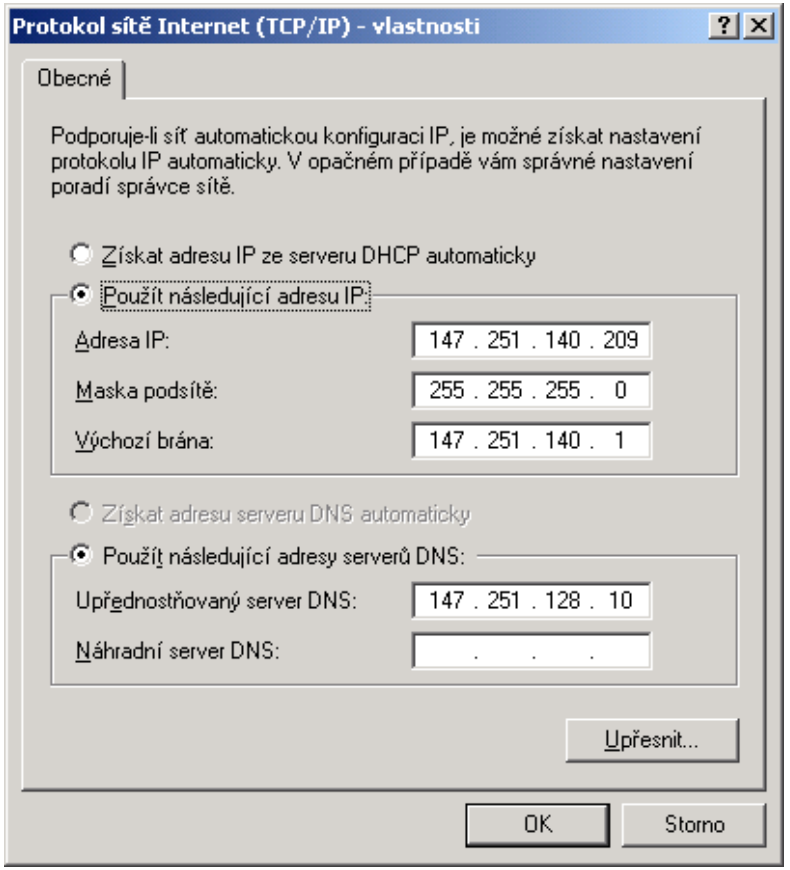
DNS služba

- Překlad internetových jmen na IP adresy
- Ne každá IP adresa má definováno internetové jméno
- Překlad realizují DNS servery, které udržují seznam známých internetových jmen a případně se dotazují dalších DNS serverů na neznámá jména
- Bez dostupnosti této služby nelze využívat internetová jména, pouze IP adresy

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Ukázka konfigurace sítě ve Windows

- Konfigurace – podle sítě
  - Manuální
    - Statické IP adresy
  - Automatická
    - DHCP server
    - Dynamické IP adresy
- cmd + ipconfig /all – aktuální síťové nastavení



Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Další síťové služby

- HTTP, FTP, SSH, POP3, IMAP, SMTP
- Typicky jeden server poskytuje více služeb
- Server je identifikován IP adresou (tel. číslo), služba svým číslem zvaným port (klapka)
- Kompletní adresa služby je IP adresa serveru + číslo portu
- Každá služba má definovaný standardní port, např. HTTP port č. 80

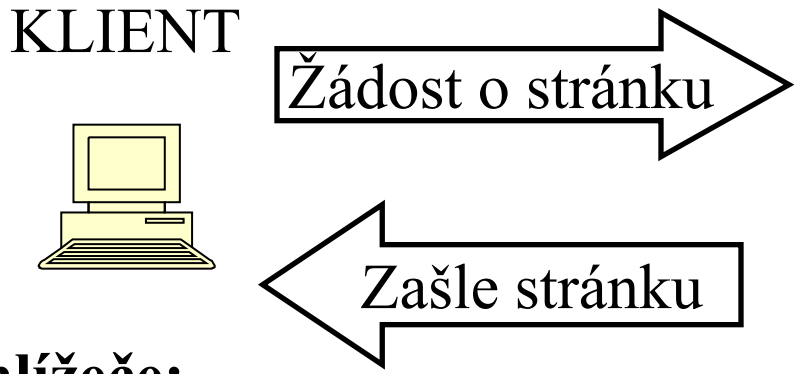
Zobrazení aktuálně využívaných služeb – cmd + netstat

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.

EVROPSKÁ UNIE

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Webové stránky HTTP(S)



Prohlížeče:
Internet Explorer
Mozilla Firefox
Chrome
Opera

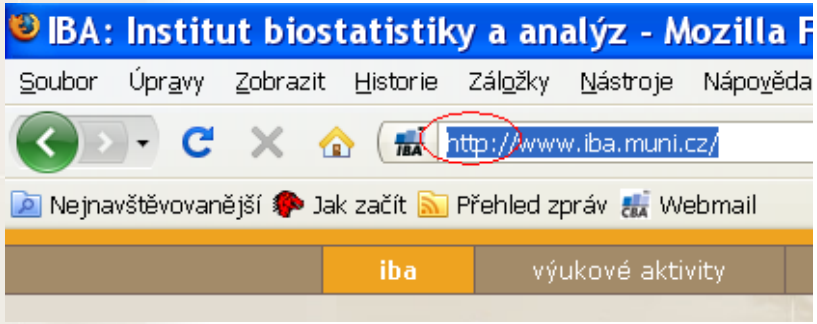
Servery:
IIS
Apache

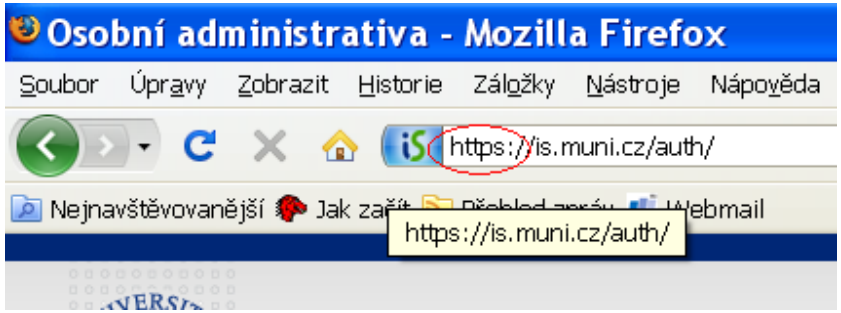
Porty:
HTTP – 80
HTTPS - 443

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

HTTP x HTTPS

- Veškerá komunikace klienta se serverem je šifrována – data jsou během přenosu nečitelná
- HTTPS má vlastní port 443
- Server musí podporovat službu HTTPS



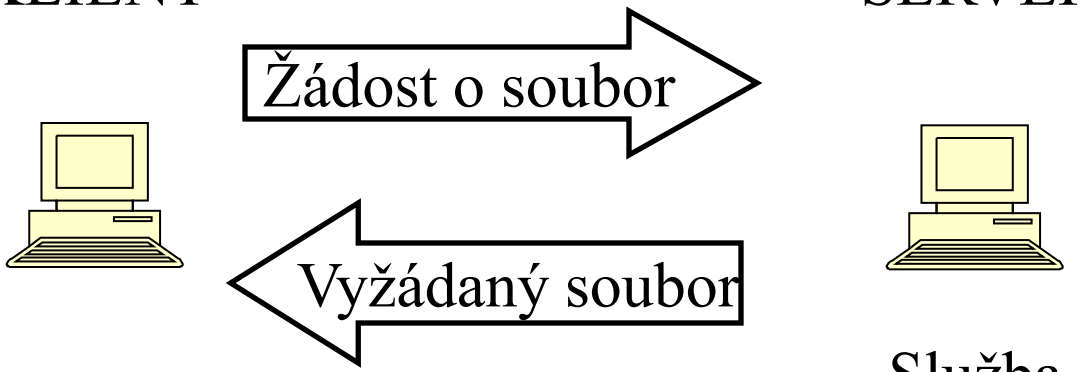


Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Služba FTP

KLIENT

SERVER



FTP klient
Total Commander
Internet explorer

Služba
FTP

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Služba FTP 1

- Anonymní
- Pouze pro čtení

- Login , heslo
- Čtení i ukládání

Přenos souborů

Textově

.txt, .htm, …

Binárně

.exe, .zip, …

- Implicitně nešifrovaný přenos
- Aktivní x pasivní přenos, firewall
- **Alternativa pro sdílení souborů jsou webové úschovny**

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.

EVROPSKÁ UNIE

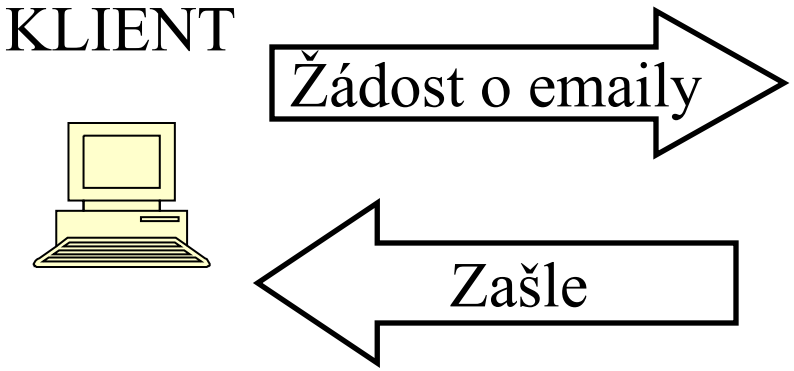
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Emailové služby

- E-mailová schránka = soubor(y) primárně ležící na poštovním serveru
- Poštovní servery spolu komunikují – přeposílají maily
- E-mailové programy x e-mail přes webové rozhraní
- Služby pro čtení pošty
- Služba pro odesílání pošty

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Čtení pošty



Outlook
Eudora
Thunderbird

Služby:
POP3
IMAP

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Služby POP3 a IMAP

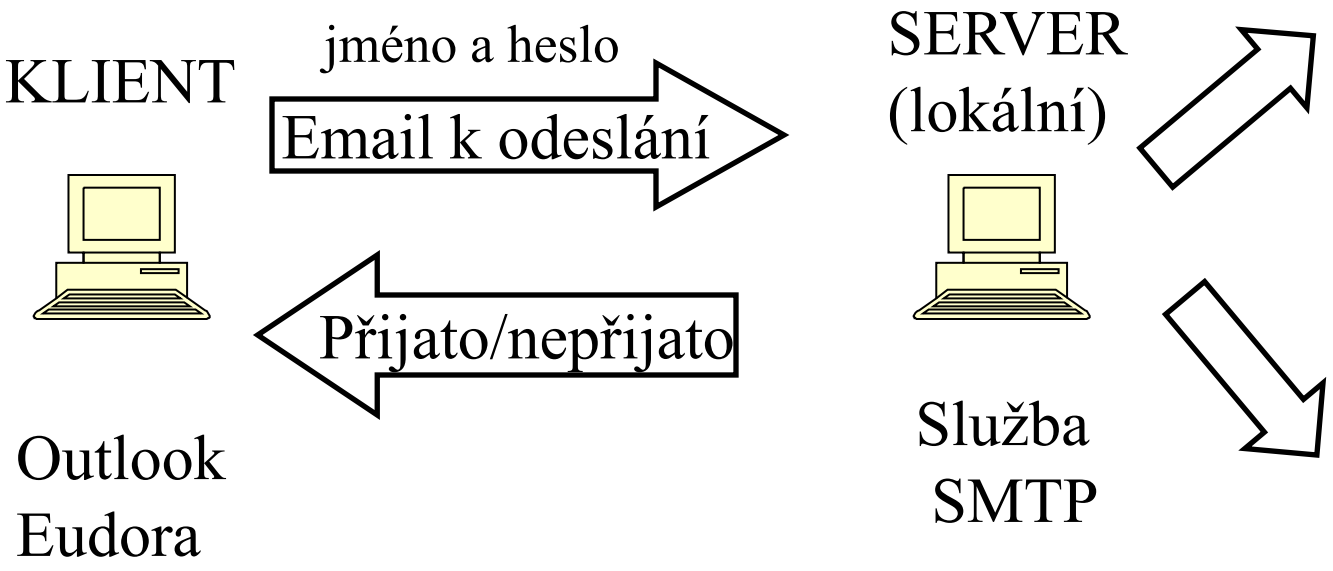
POP3	IMAP
Zašle všechny nové emaily – celé Odstraní je ze serveru	Zašle pouze hlavičky emailů Obsah emailu zašle až na vyžádání
Třídění emailů do složek na lokálním počítači	Všechny emailové složky na serveru
Vhodné pro off-line čtení	Vhodné při čtení pošty z více počítačů

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.

EVROPSKÁ UNIE

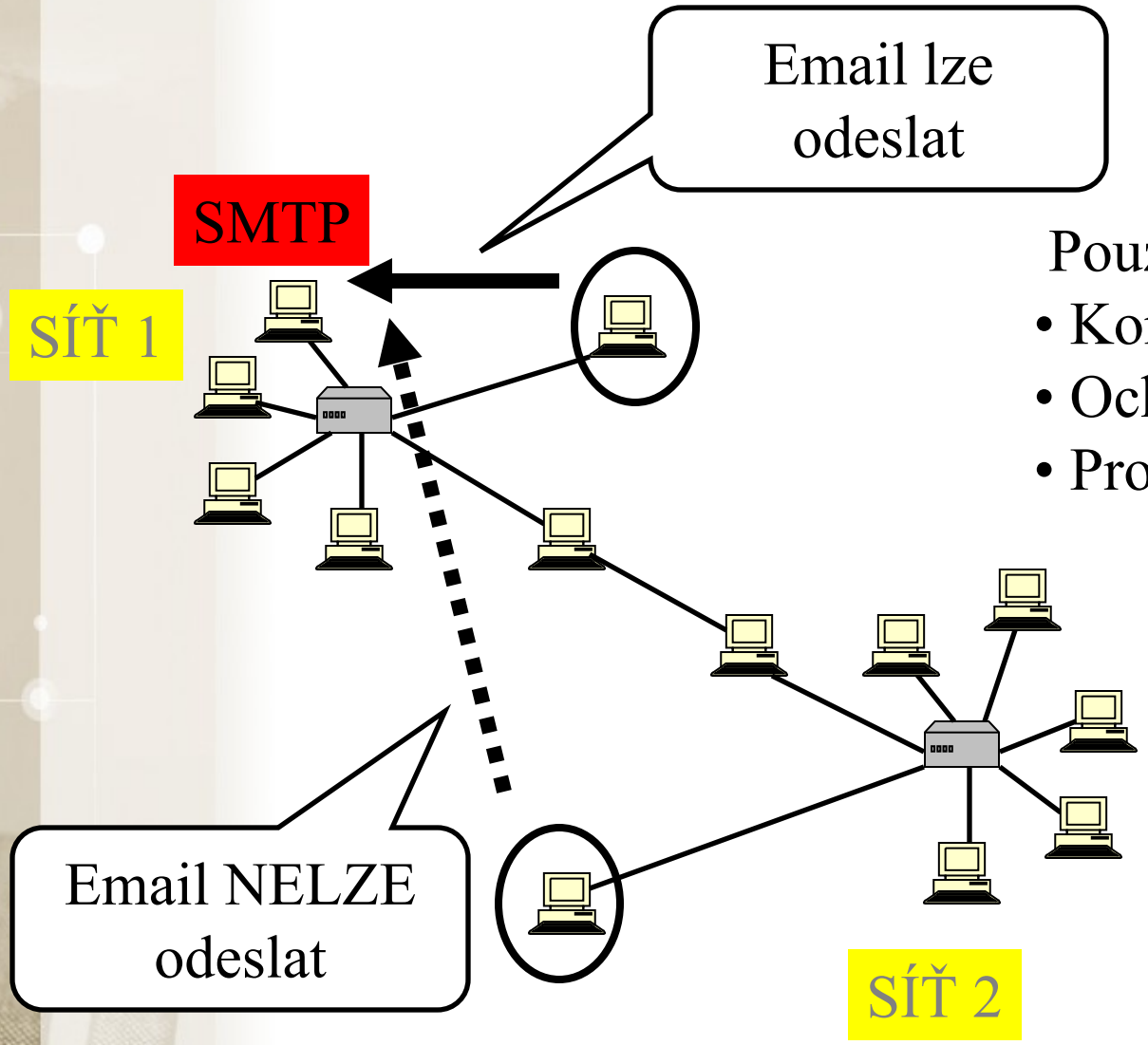
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Odesílání pošty služba SMTP



Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Omezení při migraci PC



Pouze počítače v lokální síti

- Kontrola IP adresy
- Ochrana zdrojů proti spamu
- Problém s notebookem

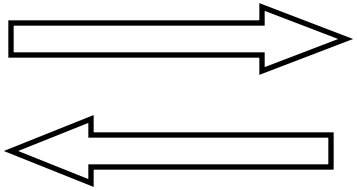
Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Email přes webové rozhraní

Seznam.cz, centrum.cz, email.cz, hotmail, …

KLIENT

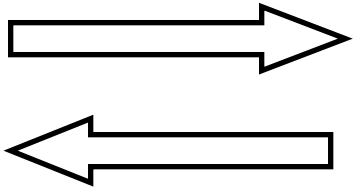
Outlook
Eudora
…



SERVER - místní

Služby:
POP3
IMAP
SMTP

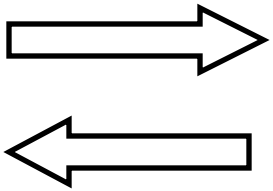
Internet
Explorer



SERVER - cizí

Služba
HTTP

KLIENT
POP3/ IMAP
SMTP



SERVER - cizí

Služby:
POP3
IMAP
SMTP

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Další služby

- Telnet, ssh, vzdálená plocha
  - Přímý přístup na vzdálený server
- SFTP, FTPS
  - Zabezpečený (šifrovaný) přenos souborů
  - Klient – WINSCP
- RSS služba
  - Čtení novinek z publikačních serverů
  - (*RSS feed*, též RSS kanál, *RSS channel*)
  - RSS čtečka
    - modul pro Thunderbird, Firefox
    - Aplikace Ziepod
  - Podcasting – multimediální obsah
    - Český rozhlas – rádio na přání www.rozhlas.cz/naprani
    - www.eslpod.com

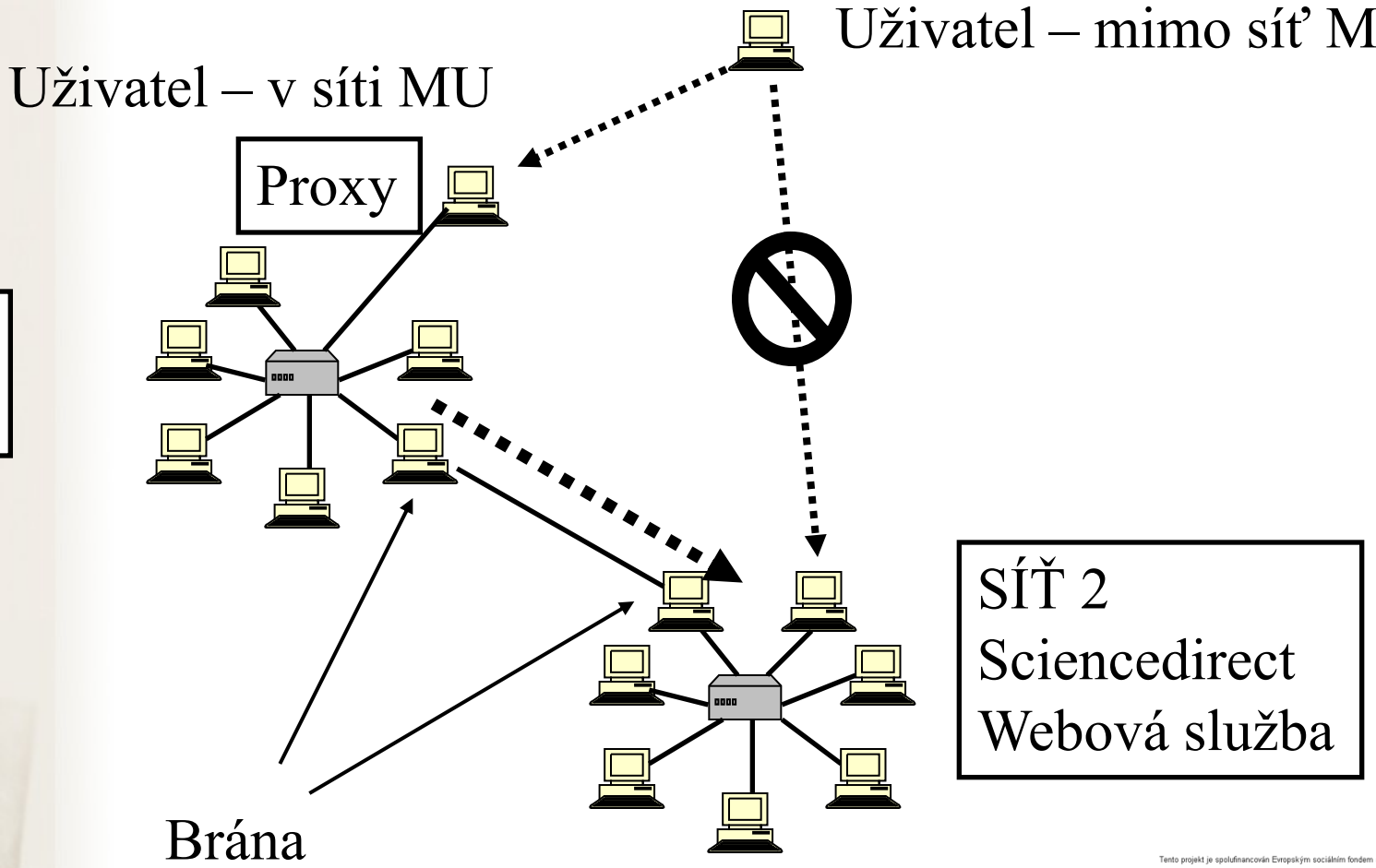
Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Proxy server

- Zprostředkovatel komunikace mezi klientem a serverem
- Ochrana lokální sítě
- Vyrovnávací paměť – zlepšení rychlosti odezvy

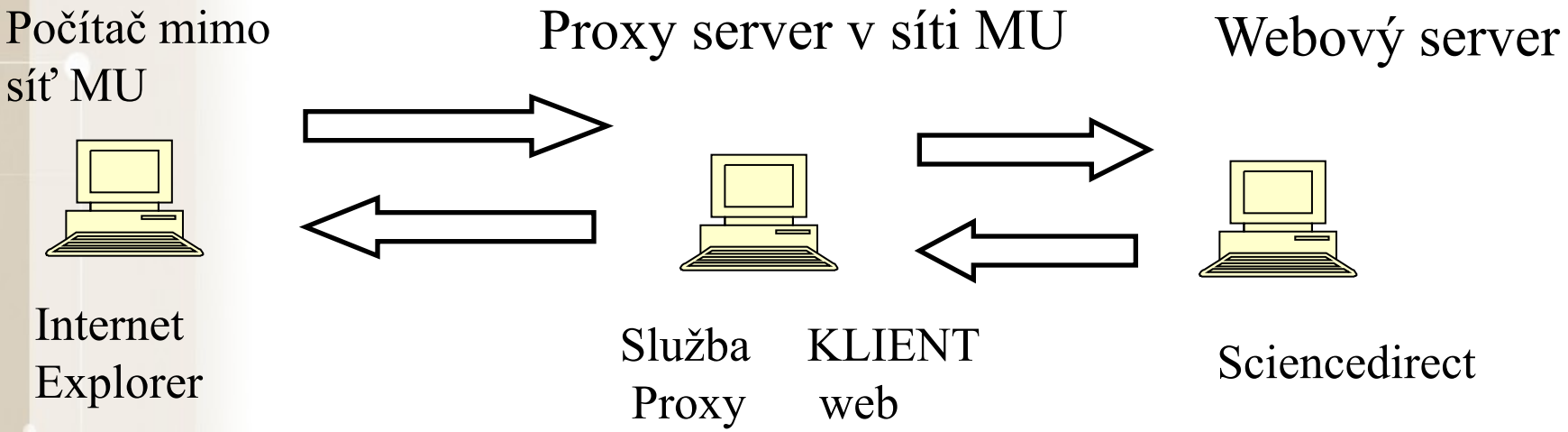
Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.

Proxy server 1



Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Proxy server 2



Podrobný popis služby proxy MU
http://library.muni.cz/ezdroje/proxy.php

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

VPN

- Služba simuluje připojení vzdáleného počítače do lokální sítě
- „Tunel“ do vzdálené sítě
- Vzdálenému počítači je přidělena lokální IP adresa
- Vzdálené PC se pak stává „téměř“ plnohodnotnou součástí vnitřní sítě
- https://vpn.muni.cz/

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Bezpečnostní zásady při práci s PC

Rizika při práci v počítačové síti

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.

Úvod – co nám hrozí?

- Útok hackera
  - Automatizovaný a plošný (e-mail, www, IM, sociální sítě)
    - Cílem hackera je ovládnout váš PC, získat z něj citlivé údaje (čísla kreditních karet, hesla…), odcizit hotovost z účtu nebo jej použít k dalším útokům
  - Cílený přímo na Vás
    - Cílem může být získání citlivých firemních dat (konkurenční boj, diskreditace)

Možné následky útoku:

  - Přímá finanční ztráta (odcizení peněz z účtu přes kreditní kartu)
    - Správné nastavení limitů na kartě
  - Policejní stíhání (obvinění z použití PC k nelegálním aktivitám)
  - Problémy v zaměstnání
  - Vydírání a diskreditace (zveřejnění citlivých informací, fotografií, e-mailů…)
  - Odcizení výpočetního výkonu (zpomalení PC) za účelem výdělku (Bitcoin)

- Ztráta dat
  - V případě selhání hardware, ztráty nebo odcizení PC, zavirování

Následky ztráty dat jsou individuální, záleží na povaze dat.

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Úvod – jak se bránit?

- PC jako pracovní nástroj: je nutné dodržovat bezpečnostní pravidla jako s každým jiným nástrojem, zejména v těchto oblastech:
  - Práce s emailem a přílohami
  - Instant messaging (Skype, ICQ, Jabber…)
  - Sociální sítě (Facebook, Google+, LinkedIn, Twitter…)
- Je třeba **rozumět hlášením operačního systému** a dalších programů, které vyžadují uživatelskou akci a adekvátně reagovat
- Je třeba udržovat OS, antivir a všechny používané aplikace aktualizované
- Data jsou často důležitější než samotný hardware – je důležité **zálohovat**:
  - Vím, co se z mého PC zálohuje, kam a v jakých intervalech?
  - Umím si zkontrolovat, zda zálohování funguje?
  - Umím si zálohovaná data v případě potřeby obnovit?
- Přístupové údaje k různým službám – jaká mám kde hesla? Kam je ukládám?
- Správně zabezpečená WiFi síť

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Bezpečnost E-mailu

- Hrozby:
  - SPAM – nevyžádané zprávy posílané za účelem:
    - Rozesílání reklamy
    - Sběru aktivních emailových adres
    - Distribuce škodlivého kódu
    - Vylákání peněz
  - Phishing – nevyžádaná zpráva, hromadně rozesílaná za účelem:
    - Vylákání přístupových údajů k různým službám
    - Vylákání soukromých informací
  - Spear Phishing – nevyžádaná zpráva cílená a upravená pro konkrétního uživatele
    - Převážně na objednávku
    - Cílem bývá zavlečení škodlivého kódu do vnitřní sítě organizace za účelem získání přístupu k citlivým firemním datům
    - Jde o velmi zákeřný útok, na který se mohou nachytat i zkušení uživatelé

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Bezpečnost E-mailu

- Pravidla:
  - Neklikat na odkazy v neznámých zprávách (nebezpečí podvržení adresy, nasměrování na stránku se škodlivým kódem)
  - Neotvírat přílohy v neznámých a podezřelých zprávách
  - Nikam neposílat loginy a hesla, čísla kreditních karet
  - Všímat si podezřelých rysů ve zprávách (strojově přeložený text, odkazy vedou jinam než jejich popis, zprávy předstírající že pocházejí od masově používaných služeb (Facebook, banky atd…), podezřelá adresa odesílatele
  - Neignorovat případná varování antivirových programů
  - Nenechat se zastrašit (Pokud nenainstalujete software X.Y., váš počítač bude ohrožen…)

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Instant Messaging (Skype, Jabber, ICQ)

- Hrozby ve zprávách: jsou podobné hrozbám E-mailovým
  - IM SPAM – nevyžádané zprávy posílané za účelem:
    - Rozesílání reklamy
    - Sběru aktivních emailových adres
    - Distribuce škodlivého kódu
    - Vylákání peněz
  - Phishing – nevyžádaná zpráva, hromadně rozesílaná za účelem:
    - Vylákání přístupových údajů k různým službám
    - Vylákání soukromých informací
  - Spear Phishing – nevyžádaná zpráva cílená na konkrétního uživatele
    - Převážně na objednávku
    - Cílem bývá zavlečení škodlivého kódu do vnitřní sítě organizace za účelem získání přístupu k citlivým firemním datům
- Hrozby pramenící z neaktualizovaného IM klienta
  - Neaktualizovaný IM klient může být zneužit k instalaci škodlivého kódu do PC bez vědomí uživatele
- Pravidla:
  - Neklikat na odkazy ve zprávách od neznámých osob (nebezpečí nasměrování na stránku se škodlivým kódem
  - Neotvírat soubory od neznámých osob
  - Nikam nezadávat ani neposílat loginy a hesla, čísla kreditních karet
  - Všímat si podezřelých zpráv od známých osob v kontaktech – mohou mít zavirovaný počítač a zprávu odesílá virus
  - Neignorovat případná varování antivirových programů
  - Nenechat se zastrašit (Pokud nenainstalujete software X.Y., váš počítač bude ohrožen…)
  - **Zabezpečit pravidelnou aktualizaci používaného klienta na poslední verzi**

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Sociální sítě

- **Facebook** – zneužíván pro šíření spamu, hoaxů, škodlivého kódu
  - Nebezpečná je důvěra v přátele: kliknu na cokoli, co postne někdo z mých přátel
  - Obtížná orientace v prostředí, které se často mění – pasti na neznalé uživatele
  - Clickjacking – kombinace sociálního inženýrství a tlačítek To se mi líbí
    - Příklad: Klikněte postupně na všechna tlačítka To se mi líbí pro zobrazení videa apod.
    - Na konci často pouze webová stránka se škodlivým kódem, stránka tahající z lidí peníze nebo zvyšující si uměle návštěvnost
- **Google+** - platí obdobná pravidla jako pro Facebook, zatím méně rozšířené
- **Twitter** – šíření adres stránek obsahujících škodlivý kód

Základní pravidlo – neklikat na cokoli, přemýšlet. I počítače vašich přátel mohou být napadeny škodlivým kódem, který na jejich FB profilu posílá příspěvky…

Na sociální sítě přistupujeme většinou přes internetový prohlížeč – tedy platí zásady zabezpečení prohlížeče (viz. dále)

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Antivirus a antispyware

Pokud nepoužíváme nějaký **placený antivirový program**, je vhodné použít **zdarma dostupné antivirové produkty.**

Pro domácí nekomerční použití jsou to například

- **Microsoft Security Essentials** – produkt Microsoftu, distribuovaný přes Microsoft Update. Nenáročný, dostačující, v češtině
- **Avast Free Antivirus** – produkt české firmy AVAST Software, velmi oblíbený, automatické aktualizace, mírně náročnější na systémové zdroje, nutná obnova bezplatné registrace po 1 roce
- **AVG Antivirus FREE** – další český produkt, také vhodný pro běžné použití
- **Panda Cloud Antivirus FREE** – antivir pracující na cloudové bázi, menší zátěž PC
- **Comodo Antivirus** – základní ochrana od firmy Comodo

Antiviry si většinou automaticky aktualizují své virové databáze, je třeba nechat tuto funkci povolenou!

Antispyware – software na odstranění a blokování spyware (programy, které odesílají data o uživateli třetí straně bez jeho vědomí)

- **Spybot Search & Destroy** – zdarma pro nekomerční účely, český překlad
- **Spyware Terminator** – zdarma i pro komerční účely, český překlad
- **Ad Aware SE Personal Edition** – zdarma pro nekomerční účely
- **Windows Defender** – standardní součást Windows Vista a vyšších verzí

Antispyware není většinou nutné používat stále, ale je vhodné občas nějaký nainstalovat a nechat proskenovat počítač.

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Přístupová hesla

Běžně využíváme mnoho různých internetových služeb – máme mnoho přístupových údajů

- Nebezpečné tendence – všude používat stejné a jednoduché heslo
- Známé služby čelí častým útokům hackerů s cílem ukrást přístupové údaje uživatelů (často úspěšně)
- Pokud mám všude stejný login a heslo, hacker najednou získá přístup do všech mých účtů!
- Zásady:
  - do důležitých služeb (přístupy do banky atd.) používat **unikátní přístupové údaje**
  - Jako přístupové údaje jsou často vyžadovány e-mail a heslo. **Nikdy nezadávat stejné heslo, jako máme do emailu!!** Při vyzrazení těchto údajů hackeři začnou využívat váš e-mail k šíření spamu a virů, hrozí zablokování účtu.
  - Pokud máme hesel mnoho, zvážit použití **softwarového správce hesel**

Správce hesel – užitečný pomocník pro bezpečnou práci s hesly

Je třeba si pamatovat pouze jedno hlavní heslo, ostatní hesla jsou bezpečně a přehledně uloženy v programu.

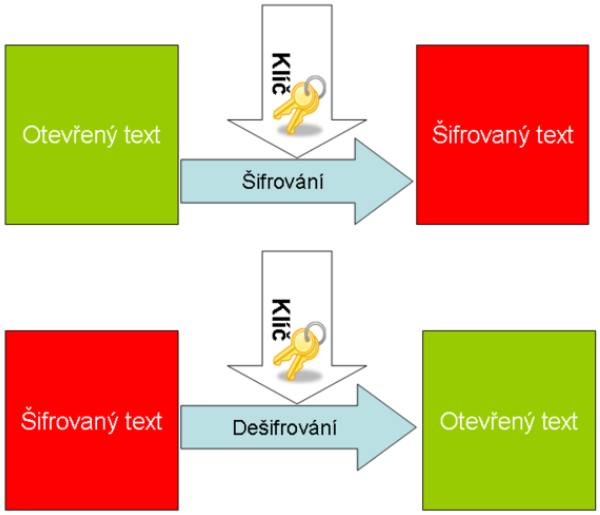
Mezi nejznámější software této kategorie patří:

- **KeePass Password Safe** – přehledný správce hesel, zdarma i pro komerční použití, existuje i verze pro mobilní telefony
- **LastPass** – doplněk pro internetové prohlížeče, předvyplní internetové formuláře, generuje hesla
- **Password Agent** – umí uchovat hesla a další informace, možnost instalace na USB klíčenku

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Šifrování

- Změna podoby (zakódování) textu a dat do formy, která je bez znalosti dešifrovacího klíče (hesla) nečitelná



- Lze šifrovat např.
  - Dokumenty (7zip, winrar - symetricky)
  - Emaily (podpora emailových klientů, veřejný klíč adresáta)
  - Síťovou komunikaci (https, sftp, imaps, ssh)
  - Disky (truecrypt, realcrypt)
- Utajení obsahu komunikace a dokumentů
- S/MIME, Pretty Good Privacy (http://home.eunet.cz/furt/pgp/)
- Výpočetně náročné

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Typy šifrování

- Symetrické šifrování
  - Jednodušší podoba, pro šifrování i dešifrování je použit jediný klíč - heslo
- Asymetrické šifrování
  - Klíč má dvě části, **soukromou** a **veřejnou**
    - Pokud mi chce někdo zaslat šifrované informace, zašifruje je pomocí mé známé veřejné části klíče.
    - Jediný, kdo dokáže tato data dešifrovat je vlastník privátní části klíče, tedy já

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Elektronický podpis

- **Jedná se o asymetrický klíč, má tedy privátní a veřejnou část**
- Pokud chci nějaký text digitálně podepsat, stačí pro podepsání použít privátní část klíče (provede emailový klient)
- Každý, kdo zná veřejnou část mého klíče (je odesílána automaticky s podepsaným emailem) pak může mnou digitálně podepsaný text
  - Přečíst
  - Ověřit, zda jsem odesílatelem
  - Ověřit, zda nebyl text někým neoprávněně pozměněn
- Podepsaný email není šifrovaný!!
- Pokud chceme někomu poslat zašifrovaný email, musíme jej zašifrovat **jeho** veřejným klíčem, který musíme mít předem k dispozici (uložený v emailovém klientovi)
  - Nemusíte nic „počítat“ nebo si pamatovat, provede emailový klient nebo jiná aplikace (pdf reader)

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Digitální certifikát

- Fyzicky = počítačový soubor , který obdržíte spolu s elektronickým podpisem a můžete importovat do počítačových programů (emailový klient, internetový prohlížeč)
- Elektronická vizitka uživatele nebo počítače – slouží k ověření totožnosti, k šifrovanému přenosu dat – pro bezpečnou komunikaci
- Vydává certifikační autorita (případně i místní řešení)
- Omezená platnost certifikátu
- Obsahuje
  - Hlavička
  - Údaje o subjektu (uživatel, server)
    - Jméno
    - E-mailová adresa
    - Další identifikační údaje
    - Veřejný šifrovací klíč (serveru, uživatele)
  - Veřejný klíč certifikační autority
  - Podpis certifikační autority (hash veřejného klíče subjektu)
  - Veřejný klíč subjektu

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Digitální certifikát – jak získat prakticky

- Vydávají tzv. certifikační autority (např. Česká pošta)
  - Přihlášení do webové (případně stažení off-line) aplikace
  - Vlastnoruční vygenerování a uložení páru klíčů s heslem
  - Vyplnění žádosti
  - Návštěva pobočky s žádostí, ověření údajů
  - Zařazení veřejné části klíče certifikační autoritou do seznamu ověřených klíčů
  - Obdržení podepsaného certifikátu s veřejným klíčem a identifikací
  - http://www.linuxexpres.cz/praxe/elektronicky-podpis-za-par-minut
- Lze snadno integrovat do používaných emailových aplikací ve formě certifikátu = zaručený digitální (elektronický) podpis

- Na MU lze získat osobní digitální certifikát pro uživatele zdarma na adrese http://pki.cesnet.cz/cs/tcs-personal.html

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Kde lze použít elektronický podpis

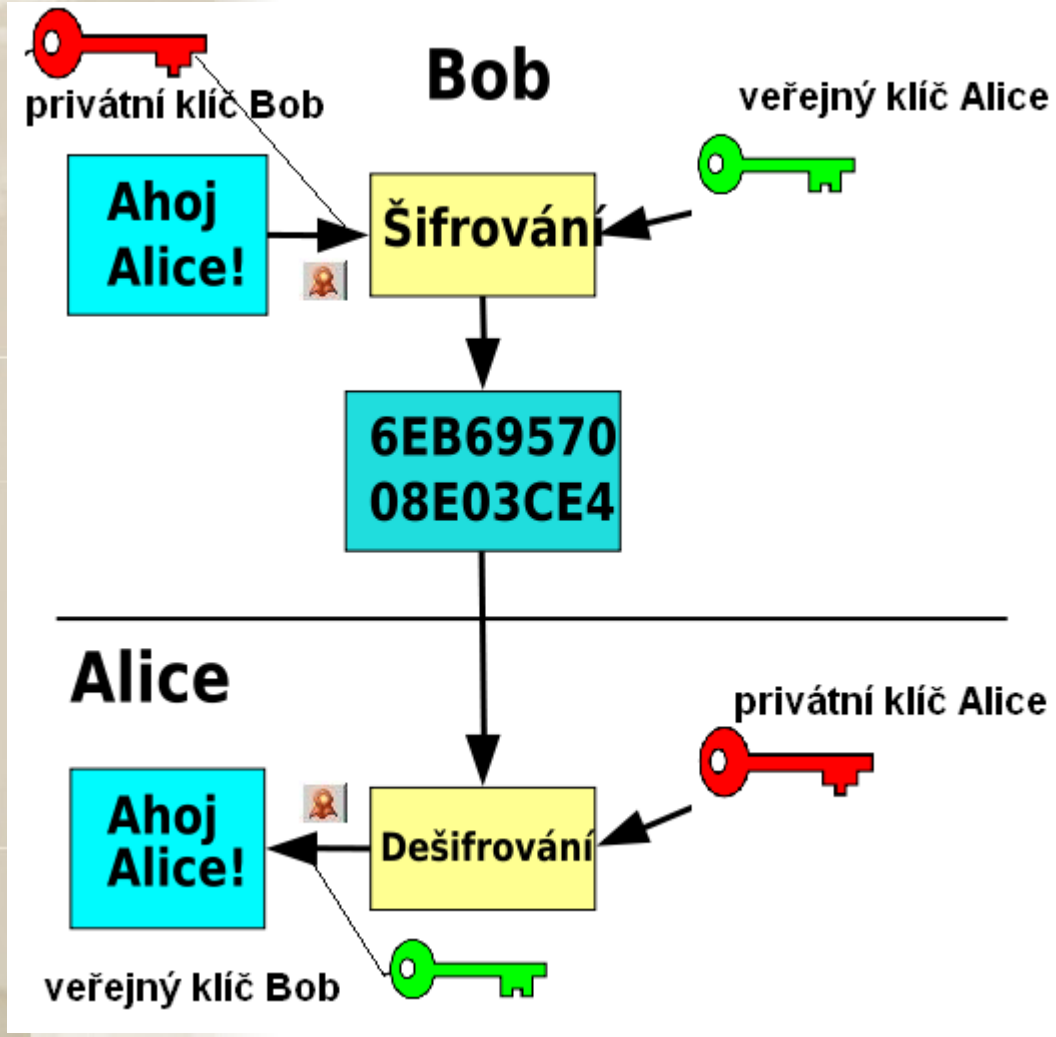
- při podání přehledu o příjmech a výdajích OSVČ
- u přihlášky a odhlášky k nemocenskému pojištění
- u přiznání k DPH
- při elektronické komunikaci se státní správou
- při elektronické komunikaci s krajskými a městskými úřady
- při elektronické komunikaci se zdravotními pojišťovnami
- při žádosti o sociální dávky
- při podávání žádostí o dotace EU
- při použití datové schránky
- při podepisování faktur
- jako elektronický podpis PDF dokumentů

Při komunikaci se státními institucemi je nutné používat certifikáty vydané Českou poštou (tzv. zaručený elektronický podpis)

Zdroj: cs.wikipedia.org

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Šifrovaný email



- Bob **podepíše** zprávu Alici svým elektronickým podpisem
- E-mail **zašifruje** veřejným klíčem Alice
- Alice **dešifruje** zprávu svým privátním klíčem
- **Ověří** Bobův podpis pomocí jeho veřejného klíče

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Další odkazy

- Kniha **Báječný svět elektronického podpisu (zdarma)** http://knihy.nic.cz/ (pdf)
- http://www.businessinfo.cz/cz/clanek/it-telekomunikace/elektronicky-podpis-a-jeho-vyuziti/1000473/2984/
- http://www.linuxexpres.cz/praxe/elektronicky-podpis-za-par-minut

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Zabezpečení domácí Wi-Fi sítě

Neponechávat AP ve výchozím nastavení od výrobce!! Nastavit admin. heslo a zvolit vhodné zabezpečení:

Existující formy zabezpečení domácích AP (Access point, bezdrátový router):

- Otevřená síť (bez zabezpečení) (nepoužívat ani omylem, kom. není šifrována)
- Šifrování WEP (zastaralé, dávno prolomeno)
- **Šifrování WPA-PSK nebo WPA2-PSK**
- Šifrování WPA(2) – Enterprise (Eduroam, podnikové)

V domácích podmínkách preferujeme zabezpečení **WPA2-PSK** v kombinaci se šifrováním **AES** (někdy označováno jako CCMP)

- nabízí rozumnou míru bezpečnosti
- je nutné zvolit **kvalitní PSK** (rozumně dlouhé a složité heslo)
  - doporučuje se **alespoň 13 znaků**
  - kombinace písmen a číslic
  - nepoužívat známá hesla (existují seznamy nejpoužívanějších hesel)
- **vypnout WPS (QSS)** (WiFi Protected Setup) na AP (prolomeno v prosinci 2011)

Nekvalitně zabezpečený AP vystavuje nebezpečí vás!!

zdroj: www.dsl.cz

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
Institut biostatistiky a analýz,
Lékařská a Přírodovědecká fakulta,
Masarykova univerzita, Brno
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Co příště

- Praktická část
- login/heslo do is.muni.cz

- Podmínka zápočtu
  - Registrace v IS.muni.cz
  - Účast na teoretické části
  - Účast na praktické části nebo odpověď na praktický test

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.

Druhý den

- Testové úkoly
- Netstat
- Nastavení přesměrování emailu v IS
- http://www.lupa.cz/clanky/pouzivate-internetove-uschovny/
- Nastavení sítě ve Windows
- Nastavení updates, firewall Windows
- Nastavení proxy serveru
- Nastavení VPN – stránka informatiků analogie proxy
- Práce s Ad-aware, způsoby detekce viru

http://www.cdma.cz/pic/pokryti_cdma.gif
http://www.cz.o2.com/osobni/cz/pece_a_podpora/podpora_a_servis/mapy_pokryti.html
http://t-mobile.cz/Web/Residential/TarifySluzby/MapaPokrytiCR.aspx

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Test

- IP adresa vašeho počítače
- Fyzická adresa (MAC) vašeho síťového zařízení
- IP adresa vámi používaného DNS
- Změřit aktuální skutečnou rychlost připojení pomocí vybrané služby
- Rychlost odezvy serveru www.seznam.cz
- Obsah readme souboru z ftp serveru ftp://ftp.muni.cz/pub/tex/local/cstex/chyby.txt
- Odeslání na adresu klimes@iba.muni.cz, předmět UPS TEST

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.

Přihlášení

- Účet Student
- Heslo student123

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.

EVROPSKÁ UNIE

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ