MUNI
MED

Uživatel počítačové sítě

Daniel Klimeš, Jan Krejčí, Roman Šmíd

Osnova

1. Pojmy, termíny
2. Připojení k počítačové síti
   - Možnosti připojení, co je zapotřebí, srovnání
3. Síťové služby
   - DHCP, DNS, HTTP, Email, vzdálený přístup
4. **Bezpečnost na síti**
   - **Hesla, viry, firewall, email, spyware, phishing**
5. Šifrování, elektronický podpis, elektronická identita a její prokazování
6. Český E-government
7. Elektronické zdravotnictví ČR
   - Pro DPS studium

MUNI MED

MUNI
MED

Bezpečnostní zásady při práci s IT

Rizika při práci v počítačové síti

Roman Šmíd , Jan Krejčí, Daniel Klimeš

Počítačová bezpečnost

- je součástí informační bezpečnosti
- zabývá se tou částí bezpečnosti, která souvisí s ICT
  - Síťová bezpečnost
  - Internetová bezpečnost
  - Bezpečnost koncových zařízení
  - Kryptografie (PKI a certifikační autority, e-podpis, e-archivace)
  - Speciální prostředky (odposlech, sledování)
- cílem je
  - předcházet počítačovým útokům
  - zajistit bezpečný provoz
  - omezit pravděpodobnost výskytu rizik

Počítačová bezpečnost

- se týká:
  - koncových zařízení, (osobní počítače, mobilní zařízení) tak
  - všech ostatních částí IT infrastruktury, zejména serverů a počítačové sítě.

- zahrnuje zhruba tyto činnosti:
  - Zabezpečení ochrany před neoprávněnou fyzickou manipulací s IT (fyzická krádež)
  - Zabezpečení přístupu k datům (autentizace a autorizace)
  - Zabezpečení ochrany před neoprávněnou manipulací s daty (narušení celistvosti, důvěrnosti a dostupnosti)
  - Zajištění zálohování dat (plán obnovy)
  - Zabezpečení ochrany software před krádeží (ochrana autorského práva)
  - Zabezpečení komunikace a přenosu dat (kryptografie)

Bezpečnost dat především

- data jsou to nejcennější elektronické aktivum jaké máme
- aby mohly být správně využité, musí být **dostupné a to jen oprávněným osobám**
- aby mohly být chráněné, musí být zajištěno
  - abychom o ně nějakým způsobem nepřišli
  - aby neskončily v nesprávných rukách
- následky ztráty jsou ale individuální, záleží na povaze dat
  - pokud o ně přijdeme nebo naše klíčové informace získá konkurence, může to také znamenat konec naše podnikání nebo fungování
  - pokud jde o osobní nebo citlivá data, mohou být využita k vydírání nebo kompromitaci uživatele

Nejčastější útoky a hrozby

- **virus** je škodlivý program, který se dokáže šířit a působit bez vědomí uživatele
- **phishing** je útok využívající metod sociálního inženýrství za účelem získání citlivých nebo přihlašovacích údajů
- **spyware** je software odesílající data z napadeného počítače bez vědomí uživatele
- **DoS a DDoS** je útok způsobující přehlcení a odstavení služby
- **spam** je nevyžádané obchodní sdělení (nejčastěji e-mailem)
- **hoax** je klamavá informace
- **ransomware** je virus způsobující zašifrování koncového zařízení, pro odšifrování chtějí útočníci vysoké výkupné v anonymní měně

Síťová bezpečnost - domácí wifi síť I.

- Základem je neponechávat bezdrátový přístupový bod či router ve výchozím nastavení od výrobce.
- Je nutné nastavit nové administrátorské heslo a zvolit vhodné zabezpečení Wi-Fi.
- Existující formy zabezpečení domácích wifi routerů:
  - Otevřená síť (nepoužívat ani omylem, komunikace není šifrována)
  - Šifrování WEP (zastaralé, dávno prolomeno)
  - Šifrování WPA-PSK (lze v případě nouze použít, ale má slabší šifrování)
  - Šifrování WPA2-PSK (pokud je navíc dostupná volba šifrování AES nebo TKIP, použít šifrování AES)
  - Šifrování WPA3 (nově zaváděno od 2018) – vylepšené šifrování, ale ne všechna zařízení jej podporují

Síťová bezpečnost - domácí wifi síť II.

- v domácích podmínkách preferujeme zabezpečení WPA2-PSK v kombinaci se šifrováním AES
  - nabízí rozumnou míru bezpečnosti
  - Je podporováno již všemi bezdrátovými zařízeními
- je nutné zvolit kvalitní PSK (rozumně dlouhé a složité heslo) a také netriviální název přístupového bodu (SSID).
  - pro heslo se doporučuje alespoň 13 znaků, kombinace písmen a číslic
  - nepoužívat známá hesla (existují seznamy nejpoužívanějších hesel)
- vypnout WPS (WiFi Protected Setup)
  - prolomeno v prosinci 2011

Internetová bezpečnost – emailové hrozby

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

Internetová bezpečnost – emailová pravidla

- 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…)

Internetová bezpečnost
vzorový spam obsahující virus

Vážená paní, vážený pane,
děkujeme za projevenou důvěru v internetové obchody obchody24.cz.

Tímto emailem potvrzujeme, že jsme v pořádku přijali vaši objednávku.

Číslo objednávky (variabilní symbol): JCBDF729B439057
Datum a čas objednávky: 11.01.15 00:45
Kontaktní údaje: Barbora Záňová,+420 604 920 148

Vaše objednávka:

SONY DSC-F828 Cyber-Shot 8 mil. obraz.bodu, bílá: 1 x 23 549,00 Kč =23 549,00 Kč
Doprava PPL: 113 Kč

Celková cena nákupu vč. DPH: 23 662,00 Kč Způsob platby: Platba předem – platební karta
Poznámka: Potvrzení platby a fakturu najdete v přiloženém souboru (ucet111D535.zip)

-

Nyní prosím vyčkejte na našeho operátora, který se s vámi spojí maximálně do 1 pracovního dne a dohodne podrobnosti ohledně Vaší objednávky.

Internetová bezpečnost – vzorový phising

Internetová bezpečnost - Instant Messaging

- Co je IM? Facebook chat, WhatsApp, Viber, Skype, Telegram…jakýkoli komunikátor v reálném čase
- Hrozby v instantních zprávách jsou podobné hrozbám emailovým
- Pravidla pro bezpečné používání jsou stejné jako emailová pravidla
- Hrozby pramenící z neaktualizovaného IM klienta
  - Neaktualizovaný klient může být zneužit k instalaci škodlivého kódu do PC bez vědomí uživatele

  - **Zabezpečit pravidelnou aktualizaci používaného klienta na poslední verzi a mít aktualizovaný antivirový program**
  - **Neklikat bez rozmyslu na každý odkaz, který mi někdo zašle**

Internetová bezpečnost – cloudové služby

- **MS OneDrive, Goggle Drive (Disk Google) atd…**
- **Hrozbou je odevzdání vašich dat cizímu subjektu.**
- U většiny cloudových služeb jejich používáním souhlasíte s tím, **že data tam nahraná může firma použít k jakýmkoli účelům**, předávat je dalším subjektům, publikovat, analyzovat atd.
- Týká se to drtivé většiny nešifrovaných cloudových poskytovatelů i poskytovatelů emailových služeb.
- **Tyto služby jsou nevhodné pro jakkoliv citlivá data** – osobní údaje, vědecké publikace….
- Možné řešení jsou **šifrované cloudové služby**, tedy takové kde poskytovatel služby do Vašich dat nevidí, protože se ukládají na jejich serverech šifrovaně a klíč má pouze uživatel.
  - Emailové služby – Protonmail, Lavabit,…
  - Služby pro ukládání dat – SpiderOak, Mega.nz,…
- Pokud nechcete odevzdat svá data cizí firmě, používejte pouze šifrované cloudové služby. Vždy je vhodné číst podmínky použití dané služby.

Internetová bezpečnost - sociální sítě

- Základní pravidlem je neklikat na cokoli, přemýšlet. I počítače vašich přátel mohou být napadeny škodlivým kódem, který na jejich FB profilu nebo do soukromých zpráv posílá příspěvky, či odkazy.
- Vždy mějte na paměti, že to, co o sobě zveřejníte na Internetu, už obvykle nejde vzít zpět.
- Při používání sociálních sítí přemýšlejte o tom, komu a jaké informace dáváte k dispozici.
- Pozor na bezmyšlenkovité šíření nebo sdílení/lajkování poplašných zpráv (HOAXů).
- **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
- **LinkedIn** - platí obdobná pravidla jako pro Facebook, zatím méně rozšířené, zaměření na pracovní prostor
- **Twitter** – šíření adres stránek obsahujících škodlivý kód

Bezpečnost koncových zařízení

- Za koncová zařízení lze považovat:
  - Stolní počítače
  - Notebooky
  - Tablety
  - Chytré telefony
  - Chytré hodinky

- Bezpečnost koncových zařízení lze zvýšit:
  - Antivirem
  - Antispywarem
  - Zálohováním dat
  - Pravidelnou aktualizací OS a používaných programů

Bezpečnost koncových zařízení - mobilní

- hlavní problémy:
  - operační systémy a jejich aktualizace

    Ze strany výrobců zařízení je aktualizace OS v reakci na nové bezpečnostní zranitelnosti často pomalá nebo žádná. Hlavně starší modely telefonů bývají často výrobcem ponechány bez aktualizací a tedy zranitelné vůči dávno známým chybám. Vždy je vhodné sledovat, zda výrobce garantuje pro své zařízení dostupnost bezpečnostních aktualizací systému, a po jak dlouhou dobu. (Např. služba Android One apod.)
  - nepozornost uživatele

    Při instalaci nových aplikací se OS vždy ptá uživatele, zda smí aplikaci udělit oprávnění k určitým činnostem v rámci systému (např. čtení/posílání SMS, přístup na internet atd.). Uživatelé by měli dávat pozor, jaká oprávnění aplikaci udělí a jaké aplikace instalují.

- zařízení často obsahují:
  - důvěrná data uživatelů
  - přístupy k různým službám (email, bankovnictví apod.)

- často však nebývají adekvátně zabezpečena pro případ ztráty zařízení.
  - PIN ani odemčení gestem nestačí
  - Dostačující ochranou je šifrování celého zařízení včetně SD karty.
  - Vhodná je i aktivace možnosti vzdáleného vymazání zařízení v případě ztráty

- plnohodnotné pracovní nástroje – nutnost dodržovat stejné bezpečnostní zásady jako při práci s PC

Bezpečnost koncových zařízení - mobil

- Chytrý telefon (smartphone) obsahuje pokročilý operační systém, umožňuje instalaci a úpravy dalších programů, které dále rozšiřují možnosti telefonu.
- Příklady OS: Android, iOS, Firefox OS, Tizen, MeeGo, HarmonyOS, ChromeOS
- Výhody:
  - velké množství aplikací a tím i možností, co lze s telefonem dělat (kancelář, hry, čtení knih, internetové aplikace, navigace atd.)
- Nevýhody:
  - typicky kratší výdrž baterie
  - často větší rozměry
  - různá bezpečnostní rizika (viry, vyzrazení soukromých informací)
  - Cena

Bezpečnost koncových zařízení - tablet

- Dotyková zařízení, operační systém často stejný jako na smartphonech, mohou mít i telefonní funkce.
- Tvoří mezičlánek mezi smartphony a klasickými osobními počítači či notebooky.
- Některé novější tablety jsou plnohodnotnými počítači se standardním OS
- Používané OS: Android, iOS, Linux, Windows

Bezpečnost koncových zařízení - konektivita

- připojení je bezdrátové (WiFi nebo LTE)
- mohou obsahovat
  - plnohodnotný internetový prohlížeč
  - emailový klient
  - Komunikátory
  - VoIP klienty
  - VPN
  - terminálové klienty
  - vzdálenou plochu
- při připojení přes GSM může být limitujícím faktorem datový tarif. Po vyčerpání datového limitu se připojení zpomalí a práce s internetem se stává nepohodlná nebo nefunguje prakticky vůbec. Důležitý je správný výběr datového tarifu.
- Plnohodnotný pracovní nástroj – nutnost dodržovat stejné bezpečnostní zásady jako při práci s PC

Zajištění ochrany

- Zásady při práci s internetem, emailem a sociálními sítěmi
- Pravidelné aktualizace
- Antivirus a antispyware
- Ukládání přístupových hesel
- Správné zabezpečení domácí sítě
- **Základem je vždy prevence!**

Zajištění ochrany – pravidelné aktualizace

- je třeba rozumět hlášením operačního systému a dalších programů
- umět adekvátně reagovat na události vyžadující reakci uživatele
- pravidelně aktualizovat:
  - operační systém
  - antivirovou databázi
  - antispyware databázi
  - veškeré programové vybavení

Zajištění ochrany – pravidelné zálohování

- Data jsou často důležitější než samotný hardware

- Je důležité zálohovat:
  - Vím, co se z mého zařízení zálohuje, kam a v jakých intervalech?
  - Umím si zkontrolovat, zda zálohování funguje?
  - Umím si zálohovaná data v případě potřeby obnovit?
  - Mám zálohy na více místech?
  - Mám zálohy zabezpečené?

  - Zálohujeme v pravidelných intervalech, nejlépe automaticky

Zajištění ochrany – možnosti zálohování

Možnosti zálohování:

- Fyzické médium
  - CD/DVD
  - Jiný počítač
  - USB disk
- NAS
  - (Network Attached Storage – „datové úložiště na síti“, například externí disk přípojený do sítě)
- Cloudové úložiště
  - OneDrive
  - GoogleDrive
- Aplikační zálohování
  - Windows Backup (ve Windows 7 a Windows 10)
  - Duplicati (pro Windows i Linux)
  - Cobian Backup (pro Windows)
  - SyncThing - synchronizace

Zajištění ochrany - antivirus

- Je vhodné používat některé z komerčních řešení, ale doporučuje se použít minimálně nějaký zdarma dostupný antivirový produkt.

- Pro domácí nekomerční použití jsou to například:
  - Microsoft Antivirus - produkt Microsoftu, od Windows 10 součástí systému jako Ochrana před viry a hrozbami. Dostačující, v češtině.
  - Avast Free Antivirus - produkt české firmy AVAST Software, 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

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

Zajištění ochrany - antispyware

- Antispyware je software na odstranění a blokování spyware.

- Existuje dostatek bezplatných programů pro domácí použití:
  - 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, aktualizovat a nechat proskenovat počítač.

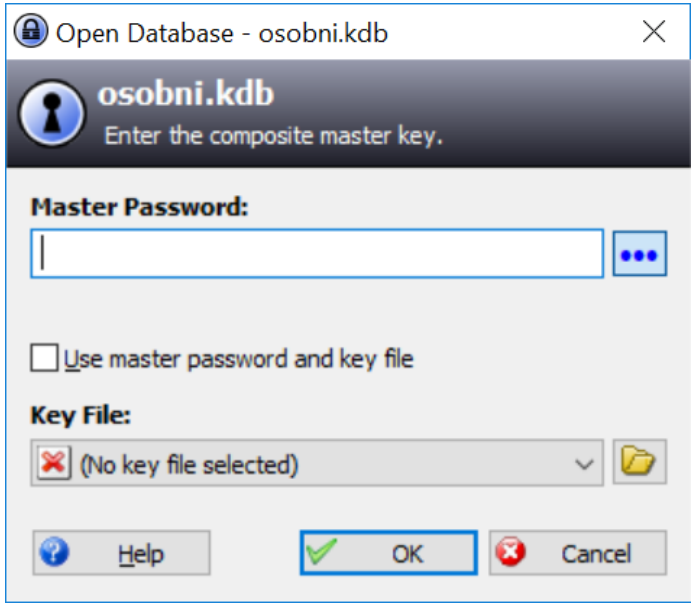
Zajištění ochrany - přístupová hesla

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**
  - **U důležitých služeb (bankovnictví aj.) používat dvoufaktorovou autentizaci (např. potvrzení přes SMS kód aj.)**

Přístupová hesla – správce hesel

- Správce hesel je 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



Služby poskytující autentizaci

- Vhodným způsobem pro autentizaci uživatelů jsou také služby třetích stran poskytujících autentizaci.
- U poskytovatele si založíme účet a předávání autentizačních informací pak necháme na poskytovateli.
- Výhodou je, že si musíme pamatovat pouze jedno jméno a heslo, a u všech dalších služeb, které to podporují, použijeme přihlášení přes tohoto poskytovatele.
- Máme také kontrolu nad tím, jaké údaje a komu předáváme.

- V ČR je rozšířeným a důvěryhodným poskytovatelem mojeID (www.mojeid.cz), pomocí kterého se lze přihlašovat i na weby státní správy, Portál občana apod.

Porušení ochrany – co nám hrozí

Při porušení ochrany může dojít ke ztrátě nebo nedostupnosti dat:

- způsobené nepozorností či nedbalostí (lze jim předcházet):
  - ztráta informací
  - nedostupnost informací
- způsobené třetí stranou (útočník, zloděj):
  - odcizení dat
  - zneužití dat

Problémové situace - únik dat omylem

Způsobené nepozorností či nedbalostí (lze jim předcházet):

- ztráta informací
  - nastane při selhání techniky (například vada disku), či smazání či skartace uživatelem (omylem)
  - informaci nemáte vy ani nikdo jiný –> přestávají existovat
  - jediná ochrana jsou pravidelné zálohy
  - následky ztráty dat jsou individuální, záleží na povaze dat.

- nedostupnost informací
  - nemáme přístup na místo uložení (jsme offline), či jsme ztratili přístupové údaje (heslo, klíč)
  - hlavní ochrana jsou pravidelné zálohy
  - sekundární ochrana v některých případech může být záložní přístupová cesta (nebo záloha přístupů)

Problémové situace – únik dat útokem

Způsobené třetí stranou (útočník, zloděj):

- odcizení dat
  - nastane při krádeži dat, nebo útoku typu ransomware
  - ochrana dostupnosti jsou pravidelné zálohy
  - ochrana proti zneužití je zabezpečení nosičů dat (šifrování či heslo - externí disk, flash disk, telefon, …)
  - hrozí možnost zneužití dat

- zneužití dat
  - nastane při odcizení dat nebo aktivního napadení útočníkem
  - o data jako taková fyzicky nepřicházíme
  - v případě zneužití dat jejich hodnota klesá a informace může být použita proti nám

Problémové situace – co nám hrozí

- Přímá finanční ztráta (odcizení peněz z účtu přes kreditní kartu)
  - Správné nastavení limitů na kartě
  - Autorizace všech operací přes druhý faktor
- Policejní stíhání (obvinění z použití PC k nelegálním aktivitám)
- Problémy v zaměstnání (zablokovaný email, VPN, …)
- Vydírání a diskreditace (zveřejnění citlivých informací, fotografií, e-mailů…)
- Ztráta dat (RansomWare)
  - WannaCry (květen 2017)
  - Benešovská nemocnice (prosinec 2019)

    Při ransomwarovém útoku na nemocnici v Benešově na konci roku 2019 byly zašifrovány síťové disky všech zařízení v síti a nemocnice byla vyřazena z chodu na více než 3 týdny.
  - FN Brno – v roce 2020 zažila FN Brno podobný útok, byly odstaveny životně důležité nemocniční systémy, odkládaly se operace, byly velké finanční ztráty.