



evropský
sociální
fond v ČR



EVROPSKÁ UNIE



MINISTERSTVO ŠKOLSTVÍ,
MLÁDEŽE A TĚLOVÝCHOVY



OP Vzdělávání
pro konkurenceschopnost



**Masarykova střední škola zemědělská
a Vyšší odborná škola, Opava,
příspěvková organizace**

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Číslo projektu	CZ.1.07/1.5.00/34.0565
Číslo materiálu	VY_32_INOVACE_293_Bezpečnost_v_síti
Autor	Mgr. Pavel Vojkůvka
Průřezové téma	Informační a komunikační technologie
Předmět	Informatika
Ročník	1.
Datum tvorby	5. 12. 2012
Datum ověření	11. 1. 2013
Druh učebního materiálu	Prezentace
Anotace	Prezentace seznamuje studenty s bezpečnostními požadavky a činnostmi v rámci počítačových sítí.
Klíčová slova	Počítačová síť, Bezpečnost, Password, Firewall
Metodický pokyn	Určeno k výkladu do hodiny a k praktickému procvičení
Pokud není uvedeno jinak, použitý materiál je z vlastních zdrojů autora	

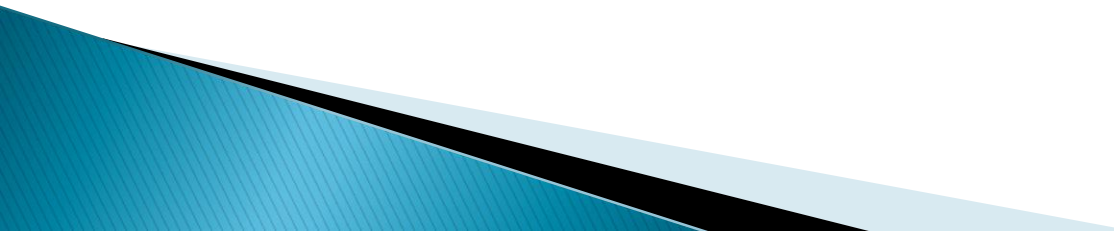
Bezpečnost v síti

Mgr. Pavel Vojkůvka

Bezpečnost v síti

- ▶ Síťovou bezpečnost je nutno rozlišovat:
 - interní bezpečnost
 - externí bezpečnost
- ▶ V případě správy více PC nás zajímá hierarchie správy sítě.

Interní bezpečnost

- ▶ Interní bezpečností sítě rozumíme kvalitu souboru pravidel, který je zaveden pro provoz počítačů v síti.
 - ▶ Zajímá nás primárně systém správy uživatelských identit a jejich oprávnění.
- 

Interní bezpečnost

- ▶ Uživatelé spravování **centrálně** nebo **lokálně**
- ▶ Uživatelům jsou přidělována práva (oprávnění k):
 - zásahům do systému (instalace SW, změny nastavení)
 - spouštění programů
 - přístupu k databázím či souborům
 - síťovým prostředkům (subsítě, proxy, servery)
 - přístupu k hardwaru (správa tisku, atp.)

Externí bezpečnost

- ▶ Externí bezpečností rozumíme zabezpečení sítě proti neoprávněným zásahům zvenčí
- ▶ Separace sítě LAN od WAN (NAT)
- ▶ Kontrola přístupových cest – autorizace přístupu
 - VPN – zprůchodnění cesty zvenčí pro oprávněné uživatele
- ▶ Zabezpečení int. služeb pro vnitřní uživatele
 - antivirová kontrola, centrální firewall
 - bezpečná e-mailová pošta – antispam, SPF record, ...

Správa zabezpečení

- ▶ Za bezpečnost je v organizaci vhodné stanovit osobní odpovědnost
 - nikdo neposkytne přihlašovací údaje třetím osobám
 - každý je zodpovědný za svá přenosná zařízení (malware)
 - osoba nevynese z organizace tajné dokumenty
 - do sítě lze připojit pouze autorizovaná zařízení
- ▶ Nutný kvalitní dohledový a sankční systém

Hierarchie správy

- ▶ Správu sítě musí mít na starost **POUZE** jeden člověk, který má přehled o aplikovaných metodách zabezpečení, ne 5 lidí, kteří neví o plánech a akcích druhých.
- ▶ Je samozřejmě možné svěřit ostatním dílčí úkoly, avšak je nutno dbát na to, aby klíčové prvky ovládal pouze správce.

Pasivní útoky

- ▶ „odposlouchávání“ dat – cílem získat nezveřejňované informace, které lze zneužít
- ▶ monitorování provozu – analýzy takto provozovaných kontaktů

Aktivní útoky

- ▶ modifikace dat
- ▶ vytváření falešných dat

- ▶ aktivním útokům nelze 100% zabránit, ale lze je na rozdíl od pasivních útoků snadněji detekovat

Firewall

- ▶ Soubor opatření (realizovaný určitým HW a SW), která zabezpečují síť proti neoprávněnému přístupu zvenčí a proti úniku informací
 - umožňuje řízení přístupu uživatele z vnější i vnitřní sítě
 - nastavení přístupových práv
 - odfiltrování nebezpečných služeb
 - zablokování nepřátelského mapování vnitřní sítě
 - audit legálních a nelegálních operací
- ▶ Zajišťuje bezpečnost při vstupu nebo výstupu do i ze sítě
- ▶ Plní funkci filtru – rozhoduje o tom, co a kam bude přes něj propuštěno

Šifrování

- ▶ Počítačový nástroj pro zajištění bezpečnosti na počítačové síti
- ▶ Klíč – doplňková informace, pomocí které odesílatel zprávu šifruje a příjemce dešifruje
- ▶ **konvenční šifrování** (se symetrickým klíčem)
 - odesílatel i příjemce používají stejný klíč, problém – distribuce sdíleného klíče
- ▶ **šifrování s veřejným klíčem**
 - snaží se řešit problematiku distribuce klíčů
 - na straně odesílatele a příjemce se používají odlišné klíče (veřejný a soukromý)
 - veřejný klíč je volně k dispozici všem zájemcům (odesílatelům)
 - zpráva zůstane čitelná pouze pro majitele soukromého klíče

Příklad bezpečnostního SW

▶ Total Network Inventory

The screenshot displays the Total Network Inventory 2.0 application window. The interface is divided into several sections:

- Left Panel (Asset Tree):** Shows a hierarchical view of assets. Under "1. Sphenisidae (6)", assets include Aptenodytes (10.0.0.154), Eudypytes (10.0.0.159), Eudyptula (10.0.0.156), Megadyptes (10.0.0.223), Pygoscelis (10.0.0.200), and Spheniscus (10.0.0.202). Under "2. The Solar System (7)", assets include Earth (10.0.0.13), Jupiter (10.0.0.12), Mars (10.0.0.8), Mercury (10.0.0.11), Neptune (10.0.0.3), Uranus (10.0.0.9), and Venus (10.0.0.7). Under "3. Olympians (7)", assets include Aphrodite (10.0.0.14), Apollo (172.16.0.2), Artemis (10.0.0.4), Dionysus (172.16.0.3), Hera (192.168.1.2), Poseidon (10.0.0.104), and Zeus (10.0.0.3). Under "The Matrix (6)", assets include Agent Smith (10.0.0.114), Morpheus (10.0.0.199), and Neo (10.211.55.5).
- Quick Add Panel:** A dropdown menu is open, showing a list of tasks and their statuses. The tasks are organized into a tree structure: Panopticon (55% Scanning... (7 / 22)), HQ (55% Scanning... (7 / 22)), and Developers (55% Scanning... (7 / 22)). Under Developers, 22 computers are listed with various scan progress bars and labels like "Ping failed", "Scanning software...", "Scanning registry...", and "Scanning hardware...".
- Right Panel (Summary and Actions):** Shows a "Scanning 66%" progress indicator and a "Stop scan" button. Below this, there are sections for "Add scan task:" (This PC, All assets, Selected assets), "IP networks:" (listing several IP ranges), "Windows network:" (WORKGROUP), "Active Directory:" (No domains found), and "Saved tasks:" (Developers, Main office).
- Bottom Panel:** A "Scanner log" section with "Messages: 0" and a "Clear" button.

Zdroje

- ▶ IRIGTEEWS. *Bezpečnosti sítí* [online]. [cit. 2012–12–05]. Dostupný z WWW:
http://informatika.topsid.com/index.php?war=zaznamova_media
- ▶ *Wikipedie: Otevřená encyklopedie: Počítačová bezpečnost* [online]. [cit. 2012–12–05]. Dostupný z WWW:
http://cs.wikipedia.org/wiki/Počítačová_bezpečnost