

Identifikátor materiálu: **ICT-2-01**

Předmět	Informační a komunikační technologie
Téma materiálu	Počítačová bezpečnost
Autor	Ing. Bohuslav Nepovím
Anotace	Student si procvičí / osvojí počítačovou bezpečnost.
Druh učebního materiálu	Prezentace (Výklad / Test)
Typ vzdělávání	Střední škola / SOU
Ročník	1. – 3.
Datum vytvoření	Prosinec 2012

Informační a komunikační technologie

Počítačová bezpečnost

Bezpečnost

Informatika jako taková nám pomáhá zjednodušovat, urychlovat a automatizovat práci, ať pracujeme v kterémkoliv oboru. V posledních několika letech se většina papírových formulářů digitalizuje, využívají se více informační systémy obsahující citlivé informace a v neposlední řadě narůstá i komunikace s veřejnou správou pomocí různých internetových portálů. Bohužel všechny tyto výhody, kterých využíváme nebo můžeme využívat, nesou s sebou i bezpečnostní rizika. Ať už se to týká virů, trojských koní, nevyžádaných e-mailů či přímých útoků na počítače či počítačové sítě, vždy se jedná o závažný problém, který nám může způsobit nevratné škody. Proto je zapotřebí těmto rizikům předcházet, a to nejen zabezpečením počítačové sítě, ale také dodržováním bezpečnostních pravidel od uživatelů, kteří v této síti pracují.

Počítačová bezpečnost je obor informatiky, který se zabývá zabezpečením informací v počítačích (odhalení a zmenšení rizik spojených s používáním počítače).

Počítačová bezpečnost zahrnuje tyto úkoly:

- zabezpečení ochrany před neoprávněným manipulováním se zařízeními počítačového systému,
- ochranu před neoprávněnou manipulací s daty,
- ochranu informací před krádeží (nelegální tvorba kopií dat) nebo poškozením,
- bezpečnou komunikaci a přenos dat (kryptografie),
- bezpečné uložení dat,
- celistvost a nepodvrhnutelnost dat.

Prvky pro obranu bezpečnosti

- **Firewall** je síťové zařízení, které pomocí množiny pravidel povoluje či zamítá síťový provoz. Filtrování provozu je v něm mnohem důkladnější než ve směrovači. Firewally slouží k ochraně síťových počítačů před operacemi, které by mohly vést k napadení interních počítačů, a tím pádem poškození jejich dat, nebo odepření služeb pro oprávněné uživatele.
- **IDS (systém detekce vniknutí)** funguje jako poplašný systém, který detekuje síťové narušení. Jeho úkolem je identifikování útoků a bezpečnostních incidentů, a tím může enormně zlepšit celkovou bezpečnost sítě.
- **Antivirové programy a aktualizace operačního systému a aplikačních programů**

Bezpečnostní prvky

Identifikace – neověřené prohlášení osoby o své identitě (například zadání uživatelského jména, to může být veřejně známé).

Autentizace – ověření identity uživatele (například heslem, otiskem prstu aj.). Modely autentizace:

- *důkaz znalostí* – autentizující se subjekt něco zná (například heslo)
- *důkaz vlastnictvím* – autentizující se subjekt něco má (například přístupová karta, klasický klíč)
- *důkaz vlastností* – autentizující se subjekt něco je (například biometrika).

Autorizace - ověření zda autentizovaný subjekt může využívat daný zdroj (více méně přístupový práva).

Prostředky autentizace

Heslo

Je obecný prostředek k autentizaci uživatele. Uživatel je pokládán za oprávněného, pokud prokáže znalost hesla. Oprávněný uživatel musí držet heslo v tajnosti.

Důkaz vlastnictvím

- **Magnetické karty** - paměť pro řádově stovky bitů dat: informace identifikující uživatele, číslo jeho bankovního účtu, ...
Ověření prohlašované identity – PINem. Magnetické karty lze snadno falšovat nebo neoprávněně kopírovat.
- **Čipové karty (Smart Cards)** - karty s mikropočítačem, paměťí RAM a ROM. Poskytují větší paměťovou kapacitu než magnetické karty a navíc výpočetní výkon přímo na kartě. Fyzická ochrana uložených dat. Lze je obtížně kopírovat. Lze použít pro vytváření digitálního podpisu, jako kalkulačku s displejem pro výpočet identifikační informace při autentizaci.

Důkaz vlastností - biometrika

- **ověření podpisu** (nelze snadno zfalšovat). Někteří lidé se 2-krát stejně nepodepíší.
- **otisk prstu** – každý prst je unikátní, má jeden hlavní unikátní rys a 50-200 minoritních rysů. Problém při poranění. Nevýhody: lze používat kradené otisky, kulturní zábrany (lidé si mohou připadat jako zločinci).
- **ověření hlasu** – lidem nevadí, musí se nashromáždit vzorky konkrétních subjektů – standardní věty, hodně faktorů má negativní vliv, snadno se použije kopie vzorku.
- **vzorek oční sítnice** – může být pro někoho nepříjemné
- **další:** duhovka, stavba ruky, rysy obličeje, rytmus psaní na klávesnici,...

Heslo

Heslo je obecný prostředek k autentizaci uživatele. Hesla se nejčastěji používají při práci s počítačem. Uživatel je obvykle odlišen od ostatním uživatelů *uživatelským jménem* (login) a heslem.

Jak manipulovat s heslem:

- ochránit proti odpozorování při zadávání
- omezit počet pokusů pro autentizaci
- uvnitř systému uchovávat šifrovaně

Útoky na hesla

- *Sociální inženýrství* - je způsob získávání důležitých informací od uživatelů bez jejich vědomí, že důležité informace poskytují. Druhá varianta je zjistit si základní informace o daném člověku a potom zkusit zmiňované jméno partnera, dětí, dalších rodinných příslušníků, nebo domácích zvířat.
- *Slovníkový útok* - útočník má slovník slov daného jazyka a zkouší zadat jako heslo jednotlivá slova z tohoto slovníku. Samozřejmě je nezadává ručně, ale automaticky pomocí počítačového programu. Na Internetu se nachází obrovské množství nejrůznějších slovníků týkajících se různých oborů lidské činnosti v různých jazycích. Stačí pouze vybrat ty správné na základě našeho odhadu nebo vědomostí a nechat program pracovat.

- *Odchycení hesla* - k tomu se používají například tzv. keyloggery (programy pro snímání stisknutých kláves na klávesnici) a podobné.
- *Útok hrubou silou* - útočník zkouší postupně zadávat všechny kombinace, například: aaa, aab, aac, aad,...
- *Použití defaultních hesel* - vpád do systému bývá útočníkovi často usnadněn také faktem, že správci systému si nedali tu práci a nezměnili defaultní (původně nastavená) hesla operačních systémů, routerů či pobočkových ústředí. Jejich seznam je pro všechny přístupný na Internetu
- *Nepřímý útok* - prolomení hesla do nějaké špatně zabezpečené aplikace a sázka na to, že uživatel použije stejné heslo i jinde.

Pravidla volby hesla

Požadavky na hesla:

- snadno zapamatovatelné, ale těžko uhodnutelné
- délka minimálně sedm a více znaků
- velká i malá písmena, alespoň jednu číslici nebo nepísmenový znak
- ne slova přirozeného jazyka (při délce 6 znaků je jen 150 000 běžných slov)
- jednou za 2 – 3 měsíce měnit – omezení aplikovatelnosti replikace odposlechnutého hesla
- nikomu nesdělovat, nikam nepsat
- nepoužívat jména manželů/manželek, dětí, miláčků, ...
- nepoužívat telefonní čísla, datum narození, rodné čísla, ..
- nepoužívat jména organizace, operačního systému, počítače,
- nepoužívat snadno zadatelné posloupnosti (QWERTY, 1234567890,...)

Otázky:

- Co je to počítačová bezpečnost?
- Co je to firewall?
- Co je to IDS?
- Co je to identifikace?
- Co je to autentizace?
- Jaké jsou modely autentizace?
- Co je to autorizace?
- Jaké jsou možné útoky na hesla?
- Jaká jsou pravidla volby hesel?

- **Použité zdroje:**

NORTHCUTT, Stephen a kol. *Bezpečnost počítačových sítí*. 1. vyd. Brno: Computer Press, 2005. 592 s. ISBN 80-251-0697-7.

THOMAS, Thomas M. *Zabezpečení počítačových sítí bez předchozích znalostí*. 1. vyd. Brno: Computer Press, 2005. 344 s. ISBN 80-251-0417-6.

STREBE, Matthew; PERKINS, Charles. *Firewally a proxy-servery: Praktický průvodce*. 1. vyd. Brno: Computer Press, 2003. 472 s. ISBN 80-7226-983-6.

http://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%A1_bezpe%C4%8Dnost, [1.12.2012]

<http://cs.wikipedia.org/wiki/Autentizace>, [8.12.2012]

<http://cs.wikipedia.org/wiki/Heslo>, [9.12.2012]