Reg. č. projektu: CZ 1.04/ 4.1.00/A3.00004

# Zabezpečení přístupu k datům

## Pracovní sešit

Materiál vznikl v rámci řešení projektu **„Vzdělávání v oblasti registrů a dalších kmenových projektů eGovernmentu“,** registrační číslo projektu: CZ 1.04/ 4.1.00/A3.00004, který je financován z prostředků Evropského sociálního fondu ČR, Operačního programu Lidské zdroje a zaměstnanost

Zpracovatel – Institut pro veřejnou správu Praha

Praha, červen 2014

# OBSAH PRACOVNÍHO SEŠITU

# ÚKOLY

## Úvodní příklad

Jede pán autem, které se najednou zastaví. Naštvaný řidič nechá vůz odtáhnout do servisu. Mechanik zvedne kapotu, pokývá hlavou, vezme kladivo a jednou do motoru třískne. Ten hned naskočí.
„Co jsem dlužen," ptá se řidič.
„125 dolarů," odpovídá mechanik.
„Cože? Za jednu ránu kladivem 125 dolarů!?!"
„Ta rána je za pět dolarů. Sto dvacet je za ´vědět kam´."

**Napište, co podle Vás může mít tento příklad společného s bezpečností přístupu k datům a informační bezpečností (klíčová je poslední věta:-).**

_____

_____

_____

_____

## Definice pojmů

**Napište, co si pod následujícími pojmy představujete (jejich význam z hlediska informačních technologií). Následně pak můžete doplnit správnou variantu sdělenou lektorem.**

**Aktualizace** (anglicky update)

_____

_____

_____

**Backdoor**

_____

_____

_____

**Blacklist**

_____

_____

_____

**Cracker**

_____

_____

_____

**Červ**

_____

_____

_____

**Falešný poplach**

_____

_____

_____

**Firewall**

_____

_____

_____

**Greyware**

_____

_____

_____

**Hacker**

_____

_____

_____

**Hoax**

_____

_____

_____

**Malware**

_____

_____

_____

**Phishing**

_____

_____

_____

**Spam**

_____

_____

_____

**Spyware**

_____

_____

_____

**Trojský kůň** (někdy též trojan)

_____

_____

_____

**Záplata (patch)**

_____

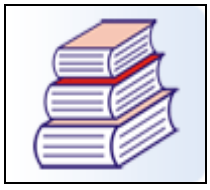
_____

_____

# LEGISLATIVNÍ ZDROJE A DOPORUČENÁ ODBORNÁ LITERATURA

## Legislativa oblasti informační bezpečnosti v ČR

- Zákon č. 101/2000 Sb., o ochraně osobních údajů
- Zákon č. 151/2000 Sb., o telekomunikacích
- Zákon č. 127/2005 Sb., o elektronických komunikacích
- Zákon č. 227/2000 Sb., o elektronickém podpisu
- Zákon č. 480/2004 Sb., o některých službách informační společnosti
- Zákon č. 563/1991 Sb., o účetnictví
- Zákon č. 499/2004 Sb., o archivnictví a spisové službě
- Zákon č. 89/2012 Sb., občanský zákoník
- další legislativa (vyhlášky, standardy atd.) MI ČR, MV ČR, ÚOOÚ a NBÚ
- Mezinárodní normy a standardy (např. ISO)



## Doporučená odborná literatura

- Kevin Mitnick: Umění klamu (Helion, 2003). Nadčasová publikace věnovaná technikám sociálního inženýrství. Její autor se stal prvním hackerem, který se dostal na seznam deseti nejhledanějších osob americkou FBI.
- Daniel Dočekal a Lenka Eckertová: Bezpečnost dětí na internetu (Computer Press, 2013). Informační bezpečnost týkající se dětí, ale poučí se i dospělí.
- Johnny Long: Google Hacking (Zoner Press, 2005). Úžasná kniha, která přináší návod, jak na internetu najít prakticky cokoliv. Vynikající materiál především z hlediska bezpečnosti: jak skrýt informace, co o mě mohou vidět ostatní apod.

- Richard Clarke: Cyber War (Ecco, 2010). Anglicky. Vynikající publikace upozorňující na rizika spojená s využíváním kybernetického prostoru.

# UŽITEČNÉ WEBOVÉ STRÁNKY

Internet může být zdrojem užitečných informací, a to také pro výkon státní správy. Proto přinášíme **několik dobrých tipů, co a kde lze na internetu najít (ve vztahu k obsahu kurzu):**

## STRÁNKY SystemOnLine

http://www.systemonline.cz/clanky/bezpecnost-dat-v-praxi.htm

- vysvětlení pojmů jako důvěryhodnost, integrita, dostupnost
- odkazy na další užitečné stránky

## STRÁNKY kyberbezpečnost

http://www.kyberbezpecnost.cz/

- aktuální články o problematice kyberbezpečnosti
- upozornění na případy počítačové kriminality

## STRÁNKY NBÚ

http://www.nbu.cz/

- **Národní bezpečnostní úřad** je gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast v ČR

http://www.govcert.cz/cs/

- **Národní centrum kybernetické bezpečnosti**, je součástí NBÚ. Jeho stránky obsahují i informační servis a aktuality z dané oblasti

**STRÁNKY magazínu ICT Security**

http://www.ictsecurity.cz/

- **ICT Security je nezávislý odborný on-line magazín**, který informuje o novinkách v dané oblasti. Přináší odborné články o možnostech zabezpečení z různých úhlů a nabízí informace a rady, které mohou pomoci při rozhodování jak řešit různé typy hrozeb v oblasti informačních technologií.

# KONTROLNÍ OTÁZKY

**1. Je napadání webových kamer (tedy jejich zneužití k nahlížení do našeho soukromí) činností vyloučenou, vzácnou nebo obvyklou?**

_____

_____

_____

**2. Co všechno může útočník získat tím, že získá přístup do našeho počítače?**

_____

_____

_____

**3. Co byste řekli tomu, kdo bude tvrdit, že počítačová bezpečnost je chiméra a že u něho by útočníci stejně nikdy nic nehledali?**

_____

_____

_____

**4. Proč je nutné dbát nejen na bezpečnost počítačů, ale také mobilních telefonů?**

_____

_____

_____

**5. Jak vytvořit kvalitní heslo?**

_____

_____

_____

**6. Jaké jsou výhody legálního software (z hlediska počítačové bezpečnosti)?**

_____

_____

_____

**7. Používat nebo nepoužívat bezpečnostní program a proč?**

_____

_____

_____

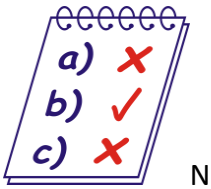
**8. Jaké jsou výhody nebo nevýhody využívání administrátorských práv (z pohledu bezpečnosti)?**

_____

_____

_____

# 3. TEST




Následující test obsahuje uzavřené otázky. Ke každé testové otázce Vám nabízíme tři varianty odpovědi, z nichž je vždy pouze jedna správná. Ta je součástí nabídky vždy. K žádné otázce v tomto testu nejsou přiřazeny dvě nebo dokonce tři správné odpovědi.

**1. Administrátorská práva**

A) jsou z hlediska bezpečnosti stejná jako práva uživatelská. Je lepší, když je mají přidělena všichni uživatelé, protože to zjednodušuje práci s počítačem.
B) jsou z hlediska bezpečnosti stejná jako práva uživatelská pouze v případě domácích počítačů. Ve firmách je důležité kvůli odpovědnosti striktně oddělit administrátory od uživatelů.
C) jsou silně nebezpečná a neměla by být přidělována běžným uživatelům. Drtivá většina útoků je totiž potřebuje pro instalaci škodlivých kódů apod.

**2. Hoax je**

A) smyšlená a nesmyslná zpráva, která se snaží tvářit důvěryhodně a které přímo či nepřímo vyzývá uživatele k dalšímu šíření.
B) speciální typ bezpečnostního programu, který blokuje viry při vstupu do počítače.
C) situace, kdy počítač „zatuhne“ a nedá se s ním déle pracovat. Problém pak řeší jen tvrdý restart (např. vyhození a nahození pojistek na celém patře).

**3. Které přílohy v e-mailech (z hlediska odesílatele i typu souboru) jsou nebezpečné?**

A) Pouze ty od neznámých osob nebo z neznámých e-mailových adres.
B) Pouze spustitelné programy. Dokumenty a další typy souborů mohu otevírat bez obav.
C) Všechny; počítač si může zavirovat (a tudíž se stát zdrojem nákazy) kdokoliv.

**4. Počítačové útoky se mobilních telefonů**

A) netýkají. Mobily mají jiný princip fungování, než počítače a nelze je napadnout.

B) týkají. Třeba počítačový virus je program jako každý jiný – pokud dokážeme do mobilu instalovat program, můžeme mít nainstalovaný i virus.
C) netýkají. Veškerý provoz v případě mobilů jde skrze operátory, kteří útoky spolehlivě filtrují.

**5. Počítačové útoky se...**

- ...nedají se zastavit, útočník se vždy prosadí. Nemá smysl používat bezpečnostní programy, jsou to jen vyhozené peníze.
- ...dají bez problémů zastavit bezpečnostními programy; pokud je máme, můžeme být v pohodě.
- ...nedají se zastavit všechny, ale bezpečnostní program a jednoduchá bezpečnostní opatření mají smysl. Bez nejmenších problémů zastaví devatenáct z dvaceti útoků.

**6. Pokud nepoužívám Windows, pak bezpečností program (antivir, firewall aj.)**

A) nepotřebuji. Windows jsou nebezpečný systém, viry pro ostatní aplikace neexistují.
B) potřebuji, ale pouze v případě, že se chovám rizikově (instaluji nelegální software, navštěvuji pochybné stránky apod.).
C) potřebuji. Existují různé viry, které nejsou závislé na použitém systému, stejně jako existují tisíce virů třeba pro Android, Linux apod.

# POZNÁMKY