# 1 Jakými právnímy předpisy je v ČR ošetřena problematika počítačové kriminality?

**1. Právní předpisy**

Trestní zákoník: Zákon č. 40/2009 Sb.

§ 230 Neoprávněný přístup k počítačovému systému a nosiči informací

§ 231 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat

§ 232 Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti

§ 182 Porušení tajemství dopravovaných zpráv

Občanský zákoník (40/1964)
Obchodní zákoník (513/1991)
Telekomunikační zákon (513/1991)

**Doplňující legislativa:**Autorský zákon (121/2000)
Zákony na ochranu průmyslového vlastnictví (14/1993)
Zákon o ochraně osobních údajů (101/2000)
Zákon o regulaci reklamy (40/1995)
Zákon o elektronickém podpisu (227/2000)
Zákon o svobodném přístupu k informacím (106/1999)
Zákon o informačních systémech veřejné správy (365/2000)

# 2 Čeho se týká paragraf 230 zákona č. 40?

§ 230 Neoprávněný přístup k počítačovému systému a nosiči informací

# 3 Čeho se týká paragraf 231 zákona č. 40?

§ 231 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat

# 4 Čeho se týká paragraf 232 zákona č. 40?

§ 232 Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti

# 5 Čeho se týká paragraf 181 (prej to má bejt 182) zákona č. 40?

§ 182 Porušení tajemství dopravovaných zpráv

Nevim jestli je to překlep a neměl tu být § 182, ale kdyby náhodou tak:

§ 181 Poškození cizích práv

(dobrej postřech, ale asi překlep)

# 6 Uveďte příklady doplňující legislativy k zákonu č. 40.

Doplňující legislativa:

Autorský zákon (121/2000)
Zákony na ochranu průmyslového vlastnictví (14/1993)
Zákon o ochraně osobních údajů (101/2000)
Zákon o regulaci reklamy (40/1995)
Zákon o elektronickém podpisu (227/2000)
Zákon o svobodném přístupu k informacím (106/1999)
Zákon o informačních systémech veřejné správy (365/2000)

# 7 Co to je počítačový systém?

**Počítačový systém**
Jakékoli zařízení, nebo skupina vzájemně propojených nebo souvisejících zařízení, z nichž jedno nebo více provádí na základě programu automatické zpracování dat.

# 8 Co to jsou provozní data?

**Provozní data**
Jakákoli počítačová data související s přenosem dat prostřednictvím počítačového systému, generovaná počítačovým systémem, který tvořil součást komunikačního řetězce, jež vyjadřují původ, cíl, trasu, dobu, objem, dobu trvání přenosu dat, nebo druh použité služby.

# 9 Kdo to je poskytovatel služeb?

**Poskytovatel služeb**
- jakýkoli veřejný, nebo soukromý subjekt, který poskytuje uživatelům služby možnost komunikovat prostřednictvím počítačového systému
- jakýkoli jiný subjekt, který zpracovává, nebo ukládá počítačová data pro tuto komunikační službu, nebo uživatele této služby

# 10 Uveďte některé trestné činy proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů.

**I) Trestné činy proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů**

a) Neoprávněný přístup
b) Neoprávněné zachycení informací
c) Zásah do dat
d) Zásah do systému
e) Zneužití zařízení

# 11 Uveďte trestné činy související s obsahem.

**III) Trestné činy související s obsahem**

a) Trestné činy související s dětskou pornografií a uchovávání hesel k počítačům

sdílení autorsky chráněných děl

#

# 12 Uveďte příklady trestné činnosti související s informačnímy systémy.

* vydírání
* krádež
* podvod
* zneužití webserveru
* útoky související s emailem (krádeže identity, spam)
* odposlechy
* modifikace dat
* znepřístupnění nějaké služby

**Kriminalita, související s pokročilými technologiemi (high-tech crime):** Trestná činnost, zaměřená na

vyspělou techniku jako cíl, prostředí nebo nástroj pachatele trestného činu (zpravidla se jedná zároveň

aktivitu, označitelnou za „počítačovou“ či „informační“ kriminalitu).

Ve své podstatě přitom může jít ve všech výše zmíněných variantách o velmi různorodou směsici činů, kdy

konkrétní technologie může být jak předmětem zájmu, objektem (prostředím) nebo nástrojem pro jejich

uskutečnění. To v konečném důsledku může vést k přístupu, kdy je zmíněná množina aktivit chápána:

- značně široce („jakákoli trestná či jinak závadová činnost s prvky výpočetní techniky“), včetně

případu, kdy je např. počítačová sestava použita při padělání peněz nebo cenných listin;

- značně úzce tedy výhradně jako činy, spáchané proti informačním technologiím, které nemohou být

spáchány žádným jiným způsobem ani proti jinému cíli.

Malware (škodlivý software): Souhrnný pojem pro jakýkoli software, který při svém spuštění zahájí

činnost ke škodě systému, ve kterém se nachází. Jeho vnější projevy mohou být časovány, nebo reagovat na

konkrétní naprogramovanou spouštěcí událost (např. na okamžik, kdy oprávněný uživatel otevře zprávu

v rámci elektronické pošty). Muže se jednat například o:

Trojské koně, keyloggery:

Přesměrovávače (re-dial, „pharming crimeware“):

# 13 Uveďte metody používané při trestné činnosti související s informačnímy systémy.

odposlech

fyzické vniknutí

ovládnutí

* sociální inženýrství
	+ spearing
	+ phishing
	+ baiting
	+ telefonický phishing

# 14 Uveďte základní zdroje informací a nástroje použitelné při testování bezpečnosti WEB serverů a aplikací.

* OWASP - zdroj informaci a postupů pro testováni WEB severu
* Webgoat - server který má úmyslné chyby a lze na něm testovat postupy pro zjištěni těchto chyb
* nmap - skener portů

# 15 Uveďte metody získávání informací o WEB serveru, aplikaci.

**1. Získávání informací o systému**

**1.1 robots.txt**

**Formát souboru:**

User-agent: \*

Allow: /searchhistory/

Disallow: /admin

**Získání souboru:**

wget <http://www.tuzkarny.cz/robots.txt>

**Více informací o struktuře a funkci:**

<http://www.robotstxt.org/>

**1.2. Google**

**Operátory:**

site:

cache:

inurl:

filetype:

**Vyhledávání informací souvisejících se zabezpečením serveru:**

“Password”, “Heslo”, “Login”, “Index of ...”

**1.3 Identifikace serveru**

a) Pole “Server:” hlavičky HTTP protokolu

Využití programu NetCat k získání hlavičky HTTP protokolu:

nc IP\_adresa\_serveru port

HEAD / HTTP/1.0

b) Pořadí polí hlavičky

c) Nekorektní dotaz

nc IP\_adresa\_serveru port

GET / HTTP/3.0

neexistující protokol:

nc IP\_adresa\_serveru port

GET / BLBOST/1.0

**Automatizované nástroje:**

Httprint

**Online:**

Netcraft ([http://www.netcraft.com](http://www.netcraft.com/))

**1.5 Aplikace**

**Detekce aplikace:**

Aplikace se mohou skrývat pod různými adresáři:

[www.tuzkarny.cz/](http://www.tuzkarny.cz/)

[www.tuzkarny.cz/apl1](http://www.tuzkarny.cz/apl1)

[www.tuzkarny.cz/apl2](http://www.tuzkarny.cz/apl2)

Jak tyto adresáře nalézt?

* procházení indexovaných adresářů
* odkazy z jiných stránek
* site:[www.tuzkarny.cz](http://www.tuzkarny.cz/)
* hrubá síla

Aplikace se mohou skrývat na jiných (nestandardních) portech:

nmap -PN -sT -sV -p0-65535

a v různých doménách na virtuálních webserverech:

[www.tuzkarny.cz](http://www.tuzkarny.cz/)

apl1.tuzkarny.cz

apl2.tuzkarny.cz

* položka “Host:” HTTP 1.1 hlavičky:
* DNS zone transfer
* reverzní DNS dotazy
* hledání jmen pomocí WEB rozhraní
* NetCraft

**1.6 Detekce paramertrů aplikace**

* lokálný Proxy server (Burp proxy, WEB Scarab)

**1.7 Analýza chybových hlášení**

* neexistující stránky
* chybné/žádné parametry
* špatné/žádné jméno heslo

# 16 Uveďte nedostatky konfigurace WEB serveru a aplikace.

**2. Nedostatky konfigurace WEB serveru a aplikace**

**2.1 SSL/TLS**

* detekce podporovaných slabých šifer

Například příkazem openssl:

openssl s\_client -no\_tls1 -no\_ssl3 -connect IP:443

* validita certifikátu
* kvalita algoritmu, kterým je certifikát podepsán

**2.2 Management serveru**

* identifikace architektury (LDAP, firewall, aplikační proxy, DMZ)
* známé chyby serveru
* administrativní rozhraní (web, ftp, WebDAV, NFS)
	+ odkud je dostupné? (vnitřní síť, Internet, je filtrované?)
	+ autentizační mechanizmus
	+ implicitní hesla

**2.3 Management aplikace**

* známé adresáře a soubory (Wikto)
* příklady, manuály
* directory traversal
* komentáře

**2.4 Soubory**

* jak server nakládá s různými typy souborů (zobrazí obsah atd.)
	+ nejprve vyhledat soubory (Google, spider, analýza kódu)
	+ [http://filext.com](http://filext.com/)
* staré soubory (zálohy, konfigurace, programy)
	+ .old, .bak, .zip, .tar, .tgz, zaloha, backup
* nápovědy
	+ viewuser.cgi: adduser.cgi, deluser.cgi, ...
	+ /app/user: /app/admin, /app/manager, ...
	+ robots.txt
* hrubá síla (Wikto)

**2.5 Administrátorská rozhraní**

* detekce URL s rozhraním (viz. 2.4 soubory)
* nápovědy ve zdrojových souborech
* dokumentace
* odhalení alternativních portů s rozhraním
* manipulace s parametry (např menu=admin, menu=1,2,3,...,495

**2.6 Podporované metody**

Jaké metody server podporuje, můžeme získat přikazem OPTIONS HTTP protokolu:

nc [www.tuzkarny.cz](http://www.tuzkarny.cz/) 80

OPTIONS / HTTP/1.1

Host: [www.tuzkarny.cz](http://www.tuzkarny.cz/)

podporované metody jsou pak zobrazeny v poli “Options:” hlavičky.

Metody a některé útoky ke kterým je možné je zneužít:

TRACE/TRACK (XST – Cross site tracing)

HEAD (obejití autentizace)

 -klasika silný klíče

 -silný hash funkce

# 17 Uveďte základní útoky na autentizační mechanizmy WEB aplikací.

Nekontrolování vstupu od uživatele

Použití neinicializovaných proměnných

• data z vnějšku mohou změnit obsah neinicializované proměnné

Ochrana session

 • útok spočívá ve špatné kontrole vstupu a v cross-site skriptování

SQL injection

 • skripty často konstruují SQL dotaz dynamicky na základě vstupů

• vstupy se musí pečlivě kontrolovat, aby chybný vstup neumožnil spuštění libovolného SQL příkazu

Když přihlašovací stránka neni šifrovaná, můžu odposlechnout

Hrubá síla

Slovníkový útok

# 18 Uveďte způsoby, kterými je možné přenášet autentizační údaje.

* šifrovaně HTTPS
* plain text
* post
* get nepoužívat je to v URL

# 19 Co to je Identifikátor relace (SessionID) a k čemu slouží.

Relace prohlížeče jsou identifikovány pomocí jednoznačných identifikátorů uložených ve vlastnosti SessionID. Identifikátor relace umožňuje aplikaci technologie ASP.NET přidružit konkrétní prohlížeč k odpovídajícím datům a informacím relace na webovém serveru. Hodnoty identifikátoru relace jsou přeneseny mezi prohlížečem a webovým serverem pomocí souboru cookie nebo pomocí adresy URL, pokud je definována relace bez souborů cookie.

# 20 Jaké vlastnosti by měl mít bezpečný Identifikátor relace?

Tokeny (Cookie, SessionID, Skrytá pole) musí být dostatečně náhodné, unikátní, odolné proti statistické a kryptografické analýze a proti únikům informací.

Cookie nesmí obsahovat pouze specifická data:

jmeno:IP:heslo

která jsou následně pouze zakódovaná (Hex,Base64,MD5).

Hybridní tokeny:

Část dat statická, část dynamická (proměnná)

# 21 Uveďte příklady útoků na autentizační mechanizmy.

* zkoušení náhodných vstupů (nepovolené znaky, name: admin heslo: admin, zkoušení errorovejch hlášek-> ta třeba může prozradit druh serveru(to se hodí možná u otázky 17 spíš, že nějaká aplikace prozradí verzi), verzi aplikace)

# 22 Uveďte příklady útoků na Identifikátor relace.

**Session fixation:**

Útočník na internetu uloží stránku s odkazem na zamýšlenou aplikaci a svou oběť/oběti – např. přes ICQ, e-mail, … – aby na tento odkaz klikly a přihlásily se do aplikace. Daný odkaz v cílové URL adrese již obsahuje (konstantní) HTTP cookie, která se použije. Útočník poté použije stejný odkaz a získá stejná oprávnění jako před tím přihlášený uživatel.

Podmínky:

- aplikace nezmění SessionID po přihlášení uživatele (nezruší SessionID vygenerované před přihlášením)

- útočník je schopen podstrčit již vygenerované SessionID uživateli, který se právě přihlašuje

- ještě snažší, pokud je SessionID přenášeno pomocí HTTP a teprve při přihlášení se přepíná na HTTPS

**CSRF:**

Jedna z metod útoku do internetových aplikací pracující na bázi neočekávaného resp. nezamýšleného požadavku pro vykonání určité akce v této aplikaci

# 23 Co to je autorizace a jak můžeme testovat její nedostatky?

* proces získávání souhlasu s provedením nějaké operace, povolení přístupu někam, k někomu nebo něčemu (nejen ve smyslu přístupu do konkrétních prostor nebo k nějaké osobě, ale také přístup k informacím, funkcím, programovým objektům a podobně).

# 24 Proč je důležitá kontrola vstupů WEB aplikace?

* Protože můžeme porušit grafiku/obsah stránky
* Vytáhnout něco z databáze
* Zasáhnout do kódu
* Spustit program
* Prej se dostanu i do kompu a pak si ho ovládam, řiká saruman Egi

# 25 Vyjmenujte útoky, ke kterým lze zneužít nedostatečnou kontrolu vstupů aplikace.

* Cross site scripting (XSS)
* SQL injection
* Interpreter injection
* Locale/Unicode útoky
* Útoky na souborový systém
* Přeplnění bufferu

# 26 Co to je XSS?

Manipulace se vstupními parametry takovým způsobem, aby aplikace generovala škodlivé výstupy. Pomocí této techniky je možné získat citlivé informace (Cookie s SessionID) z prohlížeče oběti, nebo převzetí kontroly nad prohlížečem.

# 27 Co to je SQL Injection?

Vložení SQL dotazu do vstupních dat WEB aplikace. Úspěšný útok může:

* číst data z databáze
* modifikovat data v databázi
* zadávat administrátorské příkazy (shutdown)
* vykonávat příkazy operačního systému

Tři typy SQL Injection útoků

* Inband
* Out-of-band
* Inferential

# 28 Co to je OS commanding?

Vložení kódu do formuláře, nebo parametru.

; příkaz\_operačního\_systému

může v případě formuláře, který např. vypisuje obsah zadaného adresáře způsobit vykonání zadaného příkazu (apostrof umožňuje v OS Unix řetězení příkazů).

Po zadání /etc do formuláře je interně vykonán příkaz *ls -l /etc*

Po zadání /etc ; who jsou interně vykonány příkazy *ls -l /etc ; who*

# 29 Co to je buffer overflow?

* přetečení vyrovnávací paměti (na zásobník se ukládají parametry a návratová adresa kam se vrátit, já udělám to, že škodlivým kódem to přeplním a do návratové adresy zapíšu návratovou hodnotu vlastního programu)

# 30 Proč jsou pro útočníka zajímavé odposlechy dat na síti?

* Finanční zisk
* Získání důležitých informací (důvěrných dat)
* Získání přístupu

# 31 Kde v síti je možné data odposlechnout?

* Hub
* Switch
* Koaxial
* Wi-fi

#

# 32 Jak funguje odposlech na přepínači pomocí ARP spoofingu?

ARP Spoofing

* zneužití Address Resolution Protocolu (ARP), umožňující útočníkovi vydávat se v místní síti za jiný počítač
* Princip ARP spoofingu, neboli podvržení MAC adresy, proto spočívá v neustálém zasílání „odpovědi“ se svou MAC adresou. Cíl si poté zaznamená falešnou adresu do svých vnitřních tabulek, a data bude posílat na ni.

# 33 Jaké jsou metody odposlechu dat v případě, že neputují přímo sítí útočníka?

* ARP spoofing-je technika používána pro útok v síťi Ethernet. Lze pomocí ní získat (sniff) datové rámce v [LAN](http://wiki.airdump.cz/w/index.php?title=LAN&action=edit&redlink=1) (local area network), modifikovat nebo zastavit provoz v síti nebo komunikaci (denial of service attack).

Princip ARP spoofingu spočíva v odeslání falešné (fake), nebo upravené (spoofed) [ARP](http://wiki.airdump.cz/ARP) zprávy do sítě (LAN). Podstatou útoku je asociovat MAC adresu s IP adresou funkčního nodu (PC) (kupříkladu s IP brány).

Kompletní síťový provoz pro původně zamýšlenou IP adresu pak bude (chybně) odesílán na PC s podvrženou adresou. Po odchyceni (analýze, odfiltrováni dat) lze provoz forwardovat tam kam byl původně směrován, takže postižený klient nemusí nic tušit.

* DNS spoofing - zfalšování DNS odpovědi, PC nekontroluje odpověď od DNS serveru,takže musíme odpovědět dříve než skutečný DNS server(musíme zfalšovat ID dotazu a zjistit klientsky port na který odpovědět)
* DHCP spoofing - podvrhávám DHCP server PC,který je připojený do PC

podvrhnu,aby gateway byl router požadovaný a komunikace tak jde přes nás

* ICMP redirect-Jedná se o podtyp přesměrování pro hostitele. Jeho využití je prosté – pokud na gateway přijdou data určená dále a ona zjistí, že rychlejší (nebo výhodnější) by bylo, kdyby zdrojový počítač posílal data určená pro cílový počítač (nebo síť) přes jinou gateway, tak mu o tom podá zprávu právě pomocí ICMP (data ovšem nezahodí, ale pošle cílovému PC). Náš počítač tuto zprávu obdrží a pozmění si routovací tabulku.

# 34 Lze odposlechnout data zasílaná pomocí asymetrické kryptografie?

* ne (odposlechnout ano ale budete mít pouze šifrovaná data který jsou nám vlastně k ničemu)

# 35 Jaké existují metody obrany proti odposlechům na síti?

* šifrování
* tunel (jako dvojitej zásah, akorát užší) [VPN]
* silné nastavení ->jako wifi níž
* zákaz ICMP echo paketu
* dobře nastavený firewall
* dobře zabezpečit swich - zamknout nepoužité porty, zabránit proti fyzickému zneužití
* tor síť

# 36 V čem spočívá problematika bezpečnosti WiFi sítí?

* základ je nastavení SSID (zakázat)ale nelze považovat za heslo, takže dalším krokem je zaheslovat (pomocí WEP/WAP or WPA2)
* Je to sdílené médium, takže jsme všichni na jedné síti => útoky bla bla bla
* filtrace pomocí mac adres

# 37 Co to je škodlivý kód a k čemu slouží?

* Tímto kódem myslíme program, aplikaci, skript či obyčejné informace, která mají, nebo v budoucnu mohou mít, neblahý vliv na uživatelská data.

# 38 Jaké jsou základní metody ochrany proti škodlivému kódu?

* vypnout autorun(nabídka co s mediem [otevřít složku]) i autoplay (hra)
* zase nebejt admin
* antivir
* nevěřit neověřeným zdrojům (maily -> klikni vyhraješ iPhone 5)
* aktualizace
* + veškerá ochrana na servru - ošetřit vstupy atd ...

# 39 Jak můžeme škodlivý kód v síti detekovat?

* najde nám ho antivirák

# IDS (systém pro odhalení průniku)

* monitoruje síťový provoz a snaží se odhalit podezřelé aktivity
* po detekci neobvyklé aktivity vygeneruje varování (Alert), provést zápis do logu, upozornit správce sítě a případně tuto činnost zastavit
* Následky útoku mohou vyvolat i další účinky, které způsobí divné chování systému. Sledování takových účinků je ale obtížně
* u zařízení (switch/router) je třeba nastavit, aby se veškerá komunikace mirorovala na IDS, aby měla IDS co odposlouchávat, nebo je na routeru span port, kde je duplikovaná veškerá komunikace

# IPS (Intrusion prevention system)

* rozšíření IDS
* Hlavní rozdíl oproti IDS systémům je, že systém IPS je zařazen přímo do síťové cesty (in-line), a tak může aktivně předcházet, případně blokovat detekovaný nežádoucí a nebezpečný provoz na síti

# HoneyPot

* počítač na kterém jakoby běží služby (které ale nic moc neposkytují), ale ve skutečnosti tento počítač slouží k logování. Jsou tam i soubory jako etc/passwd (jména uživatelů) a etc/shadow (zašifrovaná hesla uživatelů), no a jakmile na ně někdo šáhne, tak se to zaloguje a už mám útočníka

# 40 Jaký je rozdíl mezi virem a červem?

* Rozdíl mezi virem a červem je ten, že červ se může (umí) šířit sám dál, bez závislosti na přenosu hostitele.

# 41 Co to je BotNet?

* Označení pro softwarové agenty nebo pro internetové roboty, kteří fungují autonomně nebo automaticky. V současné době je termín nejvíce spojován s malware, kdy botnet označuje síť počítačů infikovaných speciálním software, který je centrálně řízen z jednoho centra. Botnet pak provádí nežádoucí činnost, jako je rozesílání spamu, DDoS útoky a podobně.

#

# 42 Jaké stopy zanecháváme při práci s Internetem a kdo k nim má přístup?

* Otisk prohlížeče
* IP adresa
* Reference
* Způsob chování v síti
* E-mail
* Identita v sociální síti
* VoIP
* ID
* Přístup: poskytovatelé internetu, administrátoři PC nebo serverů
* (tahle otázka je retardovaná, kdo k nim asi tak má přístup, podle toho co z toho vyberem ne?)

# 43 Jaká jsou běžná opatření ke zvýšení soukromí na Internetu?

* anonymní remailery - systémy, které garantují anonymitu, šifrují hlavičky (v podstatě jako TOR síť)
* Použití proxy serveru
* Použití předplacené tel. karty
* Použití TOR sítě
* Nastavení web. prohlížeče aby nebyl unikátní
* nezveřejňovat svoje osobní informace - Facebook, ICQ, ...

# 44 Jak můžeme anonymně přistupovat k Internetu?

* TOR browser
* Proxy server např: HideMyAss.com
* jednorázová zařízení
* internetové kavárny, ale bacha na kamery

# 45 Jaký je rozdíl mezi anonymitou a pseudoanonymitou?

* Anonymita - Tor síť - schování za obrovskou sítí proxy serveru
* Pseudoanonymita - značí jakousi zdánlivou, nepravou anonymitu. Ač se v souvislosti s komunikací na internetu velmi často hovoří pouze o anonymitě, z větší části případů jde právě o tuto pseudoanonymitu. To z toho důvodu, že u mnoha rádoby anonymně vystupujících uživatelů jde s určitým minimem technických znalostí vypátrat jejich skutečnou identitu.

# 46 Co to je sociální inženýrství?

* Způsob manipulace lidí za účelem provedení určité akce nebo získání určité informace. Termín je běžně používán ve významu [podvodu](http://cs.wikipedia.org/wiki/Podvod) nebo podvodného jednání za účelem získání utajených informací organizace nebo přístup do informačního systému firmy. Ve většině případů útočník nepřichází do osobního kontaktu s obětí.

# 47 Co to je phishing?

* Podvodná technika používaná na Internetu k získávání citlivých údajů (hesla, čísla kreditních karet apod.) v elektronické komunikaci. K nalákání důvěřivé veřejnosti komunikace předstírá, že pochází z populárních sociálních sítí, aukčních webů, on-line platebních portálů nebo od IT administrátorů.

#

#

#

# 48 Co to je spearing?

* Spear phishing je cílený phishing, kterému se lze jen těžko bránit

|  |  |
| --- | --- |
| **Phishing** | **Spear phishing** |
| Mail je rozeslán na velký počet adres. | Mail je zaslán pouze jednomu příjemci. |
| V mailu se nachází odkaz do internetu. | Mail neobsahuje odkaz do internetu. |
| Mail přijde od osoby nebo firmy, kterou znáte. | Mail přijde od osoby nebo firmy, kterou znáte. |
| Je požadováno zadání určitých údajů. | Není požadováno zadání žádných údajů. |
| Mail obsahuje (neúmyslné) chyby. | Mail neobsahuje (neúmyslné) chyby. |
| Mail zpravidla neobsahuje žádnou přílohu. | Mail zpravidla obsahuje přílohu. |
| Cílem je získání přihlašovacích nebo osobních údajů. | Cílem je získání citlivých informací, které jsou předmětem duševního vlastnictví. |

# 49 Jaké metody používáte k zabezpečení svého osobního počítače a jak byste mohli jeho zabezpečení zvýšit?

* Nepoužívat administratorský učet
* Antivirus
* Firewall
* Používat silná hesla alespoň 9 znaků
* Aktualizace
* Vypnout nepoužívané porty

# 50 Jaká je základní metoda obrany proti sociálnímu inženýrství?

* Nebejt krypl
* Dobře nastavená bezpečnostní politika