Důvěryhodnost zdroje, počítačová kriminalita

Nevěřme všemu, co slyšíme nebo čteme. Se snadnější dostupností předávání informací souvisí i jejich **důvěryhodnost**. Když je předávání informací milionům lidí tak jednoduché jako publikování na internetu, jak zařídit, aby se zde objevovaly pouze pravdivé informace?
Ke každé informaci bychom proto měli přistupovat kriticky. Ano, tohle jsem slyšel, ale je to opravdu tak? Když jsou tyto prášky na hubnutí doopravdy tak zázračné, jak je možné, že se o nich nemluví na světových lékařských konferencích o obezitě? Má tento krém skutečně tak zázračné účinky na moji pleť, abych za něj dala třikrát tolik co za jakýkoliv jiný? Není nějaké divné, že mi tato firma půjčí peníze tak rychle? Nebudu pak čirou náhodou splácet daleko víc, než kdybych si úvěr vyřídila v klasické bance? Dokážu si představit logiku mimozemšťana, který se táhne miliony let k nám, proletí se nad zeměkoulí, udělá kruh v obilí a pak si řekne, že by byla docela švanda se vypařit, a letí zase miliony let domů? Nedělá si ze mě náhodou někdo legraci?
Existují informační zdroje, kterým můžete důvěřovat více, a zdroje, které bychom měli brát bez záruky. V bulvárních plátcích se dočteme o zaručených zprávách od předního českého zahrádkáře Jožky Celera o tom, že letošní léto bude suché, protože mu to řekla mrkev.
A pak, v nějakých seriózních novinách, uveřejní rozhovor se skutečným meteorologem o tom, že žádný profesionál na světě nedokáže určit kvalifikovaně předpověď počasí na delší dobu než týden. Komu budeme věřit? „Odborníkovi", o kterém nikdo nikdy neslyšel, anebo profesionálovi v oboru, jehož náplní práce je vědecky ověřovat každou možnou i nemožnou metodu proto, aby zjistil, co nás čeká? Daleko větší pravdu bychom asi měli čekat od meteorologa, bez ohledu na to, že i Jožkovi Celerovi může shodou okolností jeho předpověď někdy vyjít.
A na internetu je to podobné. Co zveřejní na svých serverech renomované noviny, časopisy a tiskové agentury, na to se pravděpodobně bude dát spolehnout (i když ani to neplatí vždycky, tak už to ve světě chodí). Ale najít nějakou stránku a považovat ji za stoprocentně pravdivou - to je v době, kdy na internetu umí publikovat kdekdo, docela šílenství. I my už možná umíme tvořit webové stránky, budeme se to učit. Jaký bude obsah našich stránek - zda pravdivé svědectví o prázdninových zážitcích, nebo vědecký článek o tom, že jsme našli ve starém lomu mumii starou 30 000 let s návodem na obsluhu digitální kamery v ruce - to už je na vás. A taky na ostatních, tak sebou nenechte houpat.

Úkoly:

1. *Přineste do školy článek, o jehož pravdivosti by se dalo pochybovat. Úkol trvá jeden měsíc - vyhrává ten, kdo najde co největší nesmysl zabalený do co nejserióznějišího hávu.*
2. *Najděte v novinách rozhovor, ve kterém dotazovaný odpovídá na jinou otázku, než jakou dostal. Stačí si vzít kterékoliv (klidně i seriózní) noviny s trochu delším rozhovorem a začít si skutečně všímat toho, jak zněla otázka a o čem je odpověď.*
3. *Seřaďte následující články podle toho, jak moc jim věříte:*

Za co dostanete padáka

Anketa
Dostali jste výpověď? Kvůli čemu?

Princ Harry: Už má novou blondýnu!

LONDÝN – Britský princ Harry (24) má nejspíš novou lásku! Je jí blondatá kráska Astrid Harbord (27), která se nápadně podobá jeho bývalé přítelkyni Chelsy Davy (23). Je to opravdu jen náhoda, anebo je princ Harry na blondýny?

Harry a Astrid minulý týden protančil noc na večírku, odkud se po třetí hodině ranní nechali odvézt šoférem přímo do Harryho soukromého apartmánu v sídle prince Charlese v londýnské čtvrti Westminster. Na pozemek prý vjížděli zadním vchodem, který je určen výhradně pro členy britské královské rodiny.

Astrid je dobrou kamarádkou Kate Middleton (27), přítelkyně Harryho bratra – prince Williama (26). Vystudovala univerzitu v Bristolu a žije v londýnské čtvrti Chelsea. Na škole měly se svou sestrou pověst divokých, nespoutaných dračic, které nesměly chybět na žádné párty. Astrid se ráda pobaví i dnes, s oblibou u toho popíjí vodku s brusinkovým džusem, to vyvolává spekulace, jestli její vztah s princem Harrym není jen krátkodobý nezávazný románek.

Princ Harry

Rooney nepomáhá manželce, na Ronalda plivou

FOTOGALERIE – Mají těžký život. Kdo? Fotbalisté Manchesteru United. Vydělávají miliony, kupují jachty a fanoušci je obdivují. Přesto se najdou jedinci, kteří klidně na Cristiana Ronalda plivnou. Waynea Rooneyho zase zatěžuje fotbal natolik, že ani není příliš ochotný pomáhat své manželce s nákupem…

Židlický s Kotalíkem rozhodli nájezdy, Brodeur vychytal rekordní výhru

18. března 2009 6:49, aktualizováno 8:29 velikost textu:

Marek Židlický a Aleš Kotalík se v úterních zápasech hokejové NHL blýskli vítěznými samostatnými nájezdy. Prvně jmenovaný obránce zařídil výhru Minnesoty nad Coloradem (3:2SN) a novic v útoku Edmontonu v osobě Kotalíka pro změnu rozhodl duel se St.Louis (2:1SN). Kanadský gólman Martin Brodeur se hned na první pokus dočkal rekordní výhry.

foto: ČTK

Marek Židlický z Minnesoty proměňuje nájezd proti Coloradu. Brankář Peter Budaj se jen ohlíží.

Počítačová kriminalita
Existuje několik základních druhů počítačové kriminality.

1. Lidé využívající nedokonalostí napsaných programů jsou:
    a. **hackeři.** Jsou to počítačoví specialisté či programátoři s detailními znalostmi fungování systému, dokážou ho výborně používat, ale především si ho i upravit podle svých potřeb. V masmédiích se tento termín používá pro počítačové zločince a narušitele počítačových sítí, kteří se ale správně označují termínem *cracker*. Dnes jsou oba pojmy bohužel často zaměňovány.
    b. **crackeři.** Cracker (též black hat) je v informatice označení pro člověka, který zneužívá své vědomosti o počítačové bezpečnosti ke svému prospěchu při průnicích do software. Cracker musí mít dobré znalosti o principech fungování počítačů (informační technologie), programování, počítačové bezpečnosti, kryptografii a podobně. Nevhodným návrhovým vzorem programů a existencí programátorských chyb vznikají v software zranitelnosti, které lze využít.

   Hacker (white hat) je tedy v podstatě opakem crackera, který využívá své znalosti ve prospěch uživatelů počítačových systémů (tj. odstraňuje programátorské chyby, diagnostikuje vadný hardware, programuje obtížné algoritmy). V médiích je často nesprávně používán termín hacker pro crackery. Původní hackeři z velké části přispěli ke zrodu počítačové sítě Internet či hnutí svobodného software, jako např. GNU.

2. Druhá varianta počítačové kriminality je daleko nebezpečnější. Patří do ní tvůrci **malwaru** (zákeřného softwaru), jako:
    a. **virů** - programů, které se dokáží šířit bez vědomí uživatele. Zatímco některé viry mohou být cíleně ničivé (např. mazat soubory na disku), mnoho jiných virů je relativně neškodných popřípadě pouze obtěžujících. U některých virů se ničivý kód spouští až se zpožděním (např. v určité datum či po nakažení určitého počtu jiných hostitelů), což se někdy označuje jako *(logická) bomba*. Nejdůležitějším negativním důsledkem šíření virů je však samotný fakt jejich reprodukce, která zatěžuje počítačové systémy a plýtvá jejich zdroji. Některé viry mohou být takzvaně polymorfní (každý jeho „potomek“ se odlišuje od svého „rodiče“). Viry se na rozdíl od červů samy šířit nemohou.
    b. **počítačových červů** - programů**,** které jsou schopny automatického rozesílání kopií sebe sama na jiné počítače. Počítačový červ je soubor obsahující výhradně škodlivý kód, který napadá hostitelské počítače a samovolně se šíří dál. Základní rozdíl mezi virem a červem spočívá v tom, že červ se dokáže šířit sám a není závislý na hostitelském souboru a boot sektoru pevného disku. Po infikování počítače provede naprogramovanou činnost. Poté, co infikuje systém, převezme kontrolu nad prostředky zodpovědnými za síťovou komunikaci a využívají je ke svému vlastnímu šíření. Kromě svého vlastního šíření, které má rozhodující vliv na úspěšnost červa, vykonává obvykle tento v počítači nějakou sekundární činnost, která je červem nesena jako „náklad“ (kód, který tvoří náklad). Typicky se jedná o:
        i. zneprovoznění počítače, nebo jeho součástí
        ii. odstraňování souborů uložených v počítači
        iii. šifrování souborů uživatele kryptovirálním útokem jako nátlak k zaplacení poplatku, po kterém je přislíbena jejich opětovná dekrypce
        iv. prohledávání počítače za účelem získání osobních dat, která mohou pro autora programu znamenat nějaký profit

v. vytváření „zadních vrátek“ do systému (tzv. backdoor), která poté mohou být využita jako přímá cesta k infikování počítače dalšími nákazami
vi. jako důsledek jiné činnosti způsobují nestandardní chování systému.

Ať už je činnost, kterou takový program vykonává v síti, jakákoli, vždy s sebou nese vedlejší efekty, které jsou důsledkem této činnosti. Téměř vždy je, v případě většího rozšíření červa, těmito infekcemi snižována rychlost průtoku dat mezi jednotlivými počítači (a tím i celý internet) a způsobují menší či větší finanční škody majitelům postižených počítačů – ať už se jedná o soukromé vlastníky, nebo celé firmy.

c. **trojan –** název tohoto malwaru má v báji o trojském koni, protože se do počítače dostává pod záminkou jiné, legitimní aplikace. Jeho autoři využívají faktu, že Průzkumník souborů ve výchozím nastavení Microsoft Windows automaticky skrývá koncovky známých typů souborů. Škodlivý soubor vypadá na první pohled jako obrázek, audio soubor nebo archiv. Ve skutečnosti se jedná o kodlivý soubor s příponou .exe. Po jeho spuštění se na pozadí počítače nepozorovaně rozeběhne některá ze škodlivých činností: sběr informací, instalace dalších škodlivých aplikací, zapojení počítače do sítě botnetu apod.
d. **rootkit -** je speciální škodlivý kód, který využívá k infiltraci bezpečnostní díry v operačním systému a nainstalovaných aplikacích. Autoři rootkitů zároveň využívají nástroje na kompromaci spustitelných souborů a modifikaci zdrojového kódu, aby se vyhnuli detekci ze strany antivirových programů. Běžící rootkit se tedy vydává za běžící systémové procesy, soubory a složky, nebo data v registru a pro antivir bez pokročilé analýzy běžících procesů se jeho činnost jeví jako legitimní systémová akce. Pravidelně aktualizujte používané aplikace a operační systém.
e. **spyware –** špehovací software vytvořený za účelem sběru dat o uživateli. V hledáčku spywaru jsou především různé statistické informace jako například seznamy navštěvovaných internetových stránek a e-mailových adres v adresáři nebo informace o stisknutých klávesách. V některých případech se může jednat o zcela legitimní aplikaci, která však o aktivitách prováděných na pozadí uživatele neinformuje. Spyware se nešíří způsobem obdobným počítačovým virům, obvykle se instaluje zneužitím bezpečnostních chyb prohlížeče nebo jako trojské koně při instalaci jiného softwaru.
f. **adware –** na rozdíl od spyware neshromažďují tajně informace a neodesílají je přes internet bez souhlasu uživatele. Do počítače dostane zpravidla společně s jinou, legitimně získanou bezplatnou aplikací. Po jejím nainstalování se vám začne při používání počítače zobrazovat nevyžádaná reklama. Zároveň může docházet ke sledování vaší aktivity na počítači a internetu za účelem cíleného zobrazování reklamních oken. V průběhu instalace bezplatných programů věnujte zvýšenou pozornost tomu, zda součástí instalace není adware, případně jiný nechtěný software. Instalaci takové aplikace je možné ve většině případů odmítnout.
g. **phishing** - pojem phishing definuje kriminální činnost využívající sociální inženýrství - techniky manipulace s uživateli za účelem získání důvěrných informací, jako jsou přihlašovací údaje, čísla bankovních účtů nebo podrobnosti o kreditní kartě. Phishingové e-maily a stránky často vypadají k nerozeznání od prezentací respektovaných finančních institucí. Ignorujte výzvy k autorizaci nebo prodloužení platnosti účtů prostřednictvím vložení vašich přihlašovacích údajů (jméno, heslo) - jsou bezpochyby podvodné. Vaše banka po vás nikdy nic podobného vyžadovat nebude.

   h. **botnet** - je centrálně ovládaná síť počítačů infikovaných speciálním škodlivým kódem. Pro vytvoření botnetu musí útočník nejprve infikovat velké množství počítačů, například trojským koněm. Následně je počítač připojen k řídícím serverům útočníka a stane se z něj tzv. **zombie**. Infikované počítače jsou od té chvíle pod úplnou kontrolou útočníka, který je může zneužít k různé kriminální činnosti - od DDoS útoků přes krádeže identit uživatelů až po rozesílání spamu.
   i. **ransomware** - je druh škodlivého kódu, který zablokuje přístup do infikovaného zařízení nebo zašifruje data v něm uložená a za obnovení přístupu k nim vyžaduje značný finanční obnos. Platbu útočníci chtějí v bitcoinech nebo jiné digitální měně, u níž lze jen složitě vystopovat vlastníka účtu. Autoři ransomwaru využívají asymetrické RSA šifrování, proto není možné data bez znalosti dešifrovacího klíče obnovit. Obětem útoku ransomwaru doporučujeme výkupné neplatit; zaplacením jen podporujete kyberkriminálníky v další činnosti. Svá data pečlivě zálohujte.

3. Posledním a velmi závažným typem je **počítačové pirátství**. I my jsme se možná už setkali s někým, kdo si od kamaráda přepálil hru. Je třeba si uvědomit, že v danou chvíli porušuje zákon. A ještě horším přestupkem je, pokud na tom někdo začne vydělávat peníze. Jde o to, že někdo vyrobí nějaký program, věnuje tomu spoustu času, energie a peněz, podle toho odhadne jeho cenu a začne ho prodávat. A někdo jiný tento program vezme, přepálí ho na CD a pak ho prodá za desetinovou cenu.
   Aby bylo jasno - když si koupíme počítačovou hru nebo CD s hudbou, nikdo nám nezakazuje si toto CD přepálit. Nekupujeme si totiž CD, ale to, co je na něm vypálené. A to si klidně můžeme pro sebe zkopírovat, vyrobit si rezervní CD (třeba hodně cestujeme a nechceme riskovat, že si originál poškrábeme). Můžeme si ze zakoupených audio –CD vyrobit MP3. Můžeme si na jedno CD udělat mix písniček, které máme na třech různých cédéčkách. Ale všechny musíme mít zakoupené a výsledek musí opět sloužit pouze pro vaši vlastní potřebu. Jakmile ho někomu předáme nebo prodáme, porušujeme zákon!
   Většina počítačových programů je také vázána na počet počítačů, na kterých program spouštíme. Pokud budeme vlastnit firmu s deseti počítači, ale koupíme si jen jednu verzi operačního systému a tu nainstalujete na všechny počítače, je to nezákonné. V tom případě je moudřejší využít multilicencí - více licencí dohromady vyjde levněji než kupovat každou licenci zvlášť.
   Jak poznáme, zda program používáme legálně? Jednoduše. Při každé instalaci programu se vás program ptá, zda souhlasíte s licenčními podmínkami. Zkuste si je někdy přečíst. Je to dřina, ale informace jsou celkem zajímavé.
   Počítačové pirátství existuje všude na světě. Je potřeba si uvědomit, že počítačovou kriminalitou se policie začíná zabývat s daleko větší intenzitou a už teď existuje celá řada lidí čekajících na soud.

Poznámka: Licence je povolení používat program na počítači. U některých programů nekupujeme CD, protože bychom jich měli ve firmě příliš hodně, ale koupíme jenom licence - povolení.

Bezpečnost při práci na internetu

Chatování je forma komunikace. Existují veřejně přístupné servery, na kterých stačí zadat svou přezdívku a už se můžete bavit s jinými, stejně „postiženými" lidmi. Existují chatové servery na určité téma, třeba se můžeme bavit s lidmi o muzice, v jiném „pokoji" o výhodách vstupu do Evropské unie a podobně. Výhodou je, že na rozdíl od elektronické pošty mluvíme přímo s člověkem, který ve stejnou dobu sedí u počítače.

Další výhodou internetového chatování je anonymita. Zvolíme si přezdívku a můžeme začít. Můžeme se vydávat, za koho chceme, předstírat, že jsme někdo lepší, a nikdo to nemůže kontrolovat. Můžeme ze sebe udělat krásnou osmnáctiletou dlouhonohou blondýnu s autem.
Nevýhodou internetového chatování je opět anonymita. Někdo jiný si zvolí přezdívku a může se vydávat, za koho chce, předstírat, že je někdo lepší, než ve skutečnosti je, a my si to nemůžete zkontrolovat. Kdokoliv ze sebe může udělat světaznalého atraktivního mladíka, který si prostě jenom chce poklábosit. Bez ohledu na to, že je mu padesát, je dvakrát rozvedený a stejně jako s námi si píše ještě s dalšími deseti lidmi. Z našich náznaků už si poskládal místo vašeho bydliště, takže vás nenápadně každé ráno sleduje, jak jdeme do školy.
Je to samozřejmě silná nadsázka, nebezpečným vrahem ani zdaleka není každý, s kým se bavíme. Ale i tak bychom měli dodržovat určitá bezpečnostní opatření, a hlavně bychom skutečně měli být připraveni na to, že ne každý mluví pravdu. Když už nic, aspoň nás to uchrání od zklamání. Vždyť lhát na chatu je tak jednoduché!
Obdobné to samozřejmě bude fungovat u dalších způsobů komunikace v internetu, jako např. v sociálních sítích.
První a nejdůležitější zásada anonymního chatování je, aby zůstalo skutečně anonymní. **Nesdělujme** své jméno ani město, ve kterém bydlíme, **nesdělujme**, že každý večer chodíme kolem parku z florbalu, **nesdělujme** ani svoje telefonní číslo, **nesdělujme** žádné osobní informace.
Poměrně často na internetu narazíme na požadavek vyplňovat osobní údaje, třeba když si stahujeme nějaký program. Vždy si pečlivě rozmysleme, jestli je to opravdu nutné, a i potom radši nevyplňujme údaje, které nejsou bezpodmínečně nutné. Tady nám nehrozí ani tak útok na naši bezpečnost, jako spíš na naše nervy. Neseriózní firma může využít naši emailovou adresu k tomu, aby vám zasílala nejrůznější reklamní prospekty a další nevyžádané dopisy, které nám budou znepříjemňovat život a můžou zahltit nši mailovou schránku.

Spam
Spam je nevyžádané sdělení (nejčastěji reklamní) masově šířené internetem. Původně se používalo především pro nevyžádané reklamní e-maily, postupem času tento fenomén postihl i ostatní druhy internetové komunikace – např. diskuzní fóra, komentáře apod. Pro opak spamu, tj. poštu, která je zaslána konkrétní osobou se specifickým jednorázovým účelem a adresát ji považuje za žádoucí, se řidčeji používá termín ham (anglicky šunka).

Stalking
Stalker je člověk patologicky posedlý zájmem o jinou osobu, často veřejně známou, nebo jemu blízkou. Projevuje se zejména opakovaným fyzickým sledováním, nechtěnými kontakty (dopisy atp.), dlouhodobým sledováním aktivit dotyčné osoby a sbíráním informací o ní, případně nemístným oslovováním jejích příbuzných, přátel atp. Takový zájem cílenou osobu obtěžuje, narušuje její soukromí a může vzbuzovat strach; někdy ústí až v trestní stíhání stalkera.

Nakupování po internetu, stejně jako placení po internetu už je samozřejmostí. V podstatě to funguje tak, že pokud máme kreditní kartu, která to umožňuje, stačí v internetovém obchodě zadat její číslo a peníze se samy stáhnou z našeho účtu. I když se nedá platba po internetu zavrhnout, je potřeba být více než opatrný na to, co a komu sdělujete.
Příklad: Existoval kdysi hacker. A ten si vytipoval lidi, a napsal jim po internetu dopis typu: „Dobrý den, já jsem z Vaší banky a ještě předtím, než budeme pokračovat dál, potřebuji, abyste mi pro ověření sdělil číslo Vaší kreditní karty a svůj PIN. Děkuji." Lidé mu napsali všechno, co potřeboval, a on pomocí těchto čísel po internetu nakupoval. A lidé se dušovali, že číslo přece nikomu nepovolanému nedávali, psali to přece své bance!

Takže po internetu nesdělujte **NIKDY** číslo kreditní karty, pokud si nejste jistí, že se to nedá zneužít. A už určitě **NIKDY** nikomu nepište svůj PIN karty.

Pozorně si prostuduj předchozí text a zkus zodpovědět následující otázky k zopakování a pochopení textu:

1. *Jakým informacím publikovaným v médiích (a tedy i na internetu) je radno věřit?*
2. *Na jaké vlastnosti informace se při jejím přijímání zaměříme?*
3. *Která konkrétní média byste označili za bulvár?*
4. *Jaké druhy počítačové kriminality rozlišujeme?*
5. *Jak se liší hacker a cracker?*
6. *Co je to malware, které jeho druhy znáš?*
7. *Jak se liší počítačový vir a červ?*
8. *Jaký je rozdíl mezi adwarem a spywarem?*
9. *Co je počítačové pirátství? Které aktivity se dají takto posuzovat?*
10. *Jaké jsou základní prvky bezpečnosti při práci na internetu?*
11. *Vysvětli pojmy spam a stalking*

Použité zdroje:
Obrázky: Denní tisk
Texty: wikipedia.cz