Západočeská univerzita v Plzni
Centrum informatizace a výpočetní techniky

Informační Bulletin

1

Září 2006

Publikace neprošla jazykovou ani grafickou úpravou.

Redakční rada: A. Padrta, J. Sitera, P. Hanousek, R. Bodó a M. Švamberg
Autor textu: A. Padrta
Ilustrace: M. Vojtková

Sazba písmy Bitstream Charter a Concrete v systému LaTeX 2ε.

Vydání první, náklad 500 výtisků.
Vydala Západočeská univerzita v Plzni.

ISBN 80-7043-482-1

Obsah

Kapitola 1

Bezpečnost? Bezpečnost!

Počet lidí, kteří potřebují výpočetní techniku pro svou práci, neustále stoupá, neboť jde o bezesporu užitečného pomocníka. Západočeské univerzitě v Plzni se tento trend také nevyhnul. Velkým magnetem pro využívání výpočetní techniky se stalo připojení k celosvětové síti internet, která umožňuje zejména efektivní vyhledávání a získávání informací. Pro připojení zaměstnanců i studentů k internetu slouží univerzitní síť WEBnet.

Převážná většina uživatelů se spokojí s povrchní znalostí svého počítače, protože ke své práci jim postačí ovládání několika softwarových produktů (programů). Osvojování čehokoliv dalšího se na první pohled zdá být plýtváním času a energií. Pochopitelně není možné chtít po všech uživatelích, aby z nich byli specialisté na informační technologie, nicméně základní znalosti je potřeba mít a také se podle nich chovat. V poslední době se prostředí internetu stává stále agresivnějším, proto je potřeba věnovat zvýšenou pozornost zejména zabezpečení jednotlivých počítačů a hlavně bezpečnému chování uživatelů. Jak má ale běžný uživatel zjistit, co má dělat, aniž by tím strávil neúměrně mnoho času?

Pro potřeby uživatelů sítě WEBnet, kterým není lhostejná jejich bezpečnost, je určen právě tento sborník. Informace, které zde naleznete jsou primárně určeny začínajícím uživatelům, ale na své si přijdou i zkušenější uživatelé. Vzhledem ke značnému počtu netechnicky orientovaných uživatelů je důraz kladen zejména na osvojení si základních zásad bezpečného chování, bez nutnosti znát všechny technické detaily. Kromě všeobecně platných principů zde naleznete také konkrétní doporučení pro podmínky sítě WEBnet.

Kapitola 2 obsahuje informace o tom, proč se vlastně musíme bránit a o co můžeme přijít, pokud se někomu podaří získat nadvládu nad naším počítačem. Dále je zde uveden přehled potenciálních nebezpečí, kterým je vystaven každý počítač připojený do sítě internet, resp. sítě WEBnet.

V kapitole 3 je pak představeno devatero rad pro zvýšení počítačové bezpečnosti, které by měl každý uživatel sítě WEBnet ve svém vlastním zájmu znát a dodržovat. Nejprve jsou popsány základní technické prostředky a ve zkratce také princip na jakém fungují. Dále je nemalá část věnována bezpečnému chování uživatelů, které je velmi důležité – nepoučenému uživateli nepomůže sebelepší technický prostředek, pokud nebude vědět, jak jej používat.

Po přečtení tohoto sborníku byste měli mít základní povědomí o tom, co se myslí pod pojmem počítačová bezpečnost, jaké prostředky lze použít pro zvýšení Vaší bezpečnosti a jak se vyhnout kritickým aktivitám. Nemusíte být zrovna paranoidní, ale proč zbytečně riskovat?

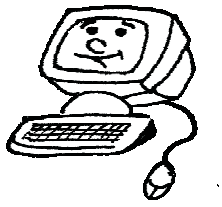
KAPITOLA 2

KDOPAK TO ZLOBÍ?

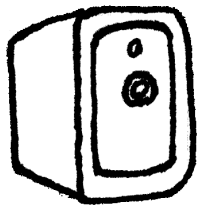
Máme-li se účinně bránit před nějakým nebezpečím, je nutné nejprve zjistit, co všechno nám reálně hrozí. Pokud budeme znát také důvody, které vedly ke vzniku zmiňovaného nebezpečí, tím lépe. V této kapitole jsou popsány nejrozšířenější pohnutky a naznačeny metody „temné strany“, kvůli kterým je bezpečnosti věnována taková pozornost.

2.1 PROČ TO DĚLAJÍ?

Zkusme si tedy nejprve zodpovědět klíčovou otázku *„Proč je zrovna můj počítač pro někoho tak zajímavý, že hodlá vyvinout nějaké úsilí, aby se jej snažil získat pod vlastní kontrolu?“*. Samozřejmě, že se nekalé aktivity v drtivé většině případů provádějí pro zisk, ať už přímý nebo nepřímý. Způsobů jak toho dosáhnout, existuje několik.



Prvním velkým lákadlem pro všechny potenciální útočníky je počítač jako takový – může být využíván k řadě účelů, některé z nich uživatele počítače přímo neohrožují, nicméně dokáží řádně znepříjemnit práci. Do této kategorie patří například zneužívání počítačů jako datových úložišť pro distribuci nelegálních dat a zneužívání výpočetního výkonu daného počítače. Výkon počítače potřebný pro práci uživatele je tak věnován něčemu úplně jinému. Další možností, tentokrát s vážnějšími dopady, je zneužití počítače k dalším útokům. Majitelé cílových počítačů si pak na takovéto incidenty stěžují a dokud není útočící počítač „vyléčen“, nemůže být připojen do sítě WEBnet.



Dále se na každém počítači nacházejí zajímavé údaje, které mohou v nepravých rukou způsobit velké nepříjemnosti. Pachatel může získaná data zneužít buď sám nebo je za úplatu poskytnout třetí straně. Odhlédneme-li od vědecko-technické špionáže, jsou cennou kořistí například osobní informace zaměstnanců, jejich kontaktní adresy, telefonní čísla, čísla kreditních karet, hesla a řada dalších citlivých údajů. Někteří nemorální jedinci se pouští také do počítačového vydírání. Po získání přístupu na počítač zašifrují celý jeho obsah a do původního stavu jej vrátí až po poskytnutí příslušné úplaty. Pro motivaci včasné platby se vždy za určitou dobu nějaký ten soubor smaže.

Každý uživatel má jednu či více elektronických identit, pod kterými vystupuje. Pokud mu je někdo odcizí, může se za něj vydávat a napáchat závažné škody – podobně jako lze zneužít ukradený občanský průkaz. Na rozdíl od ztráty občanského průkazu Vám i po odcizení nebo prozrazení elektronické identity tato zůstává a Vy ji sdílíte s jedním nebo v horším případě s mnoha dalšími jedinci. Špatné činy někoho jiného tak padnou na hlavu nevinného uživatele – Vás, který za ně nese odpovědnost. Vzhledem k tomu, že elektronická identita je používána k přístupu ke stále se zvětšujícímu počtu služeb, jde o velmi lákavý cíl.

Výše uvedené hrozby jsou zpravidla různě kombinovány, tj. například po získání zajímavých dat je počítač zneužíván pro sdílení nelegálních dat. Počítač, který byl ovládnut jedním útočníkem, je pak také snadnou kořistí pro další podobné jedince.

Počítače v síti WEBnet jsou potenciálně zajímavé ze všech zmíněných důvodů, nejlákavější je dobré připojení k síti internet, umožňující rychlé přenosy velkého množství dat a potřebný prostor pro rozsáhlé útoky na další počítače. Hodnotných údajů se zde nachází také dost, neboť řada pracovišť provádí výzkum ve spolupráci s průmyslem a v rámci studijní a ekonomické agendy jsou zpracovávány údaje o mnoha tisících osob.

2.2 JAKÝM ZPŮSOBEM?

Zamysleme se v krátkosti nad tím, jak „temná strana“ provádí výše uvedené činnosti. V podstatě existují tři možnosti jak se na vyhlédnutý počítač dostat.

První možností je situace, kdy pachatel nějakým způsobem zjistí přístupové údaje, tj. uživatelské jméno a heslo. Počítač identifikuje osoby pouze podle těchto přístupových údajů, takže nezjistí, že slouží někomu jinému.

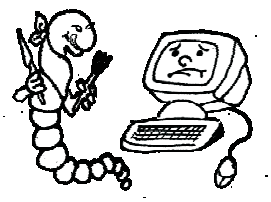
Dále se pachateli může povést na Váš počítač propašovat škodlivý program, který má v popisu práce záškodnické aktivity ve prospěch majitele a pochopitelně ve Váš neprospěch. Možností, jak to provést, je celá řada například pomocí přílohy e-mailu.

Poslední možností, jak infiltrovat Váš počítač, je zneužít nějaký užitečný program, tj. donutit jej aby prováděl akce, které vyhovují potřebám útočníka.

Všechny uvedené způsoby infiltrace však vyžadují určitou (ne)činnost uživatele počítače. V následující kapitole se podíváme detailněji na to, co je potřeba (ne)dělat, aby počítač nebyl infiltrován a zneužíván.

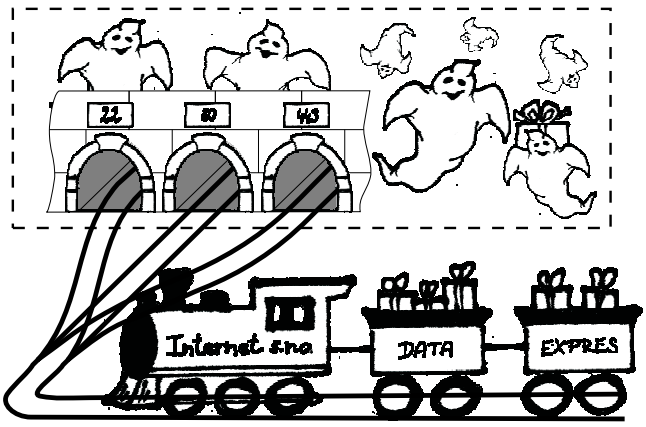
Kapitola 3

Braňme se



Pokud jste po přečtení předchozí kapitoly dospěli k závěru, že je všechno ztraceno a Váš počítač, společně s jeho obsahem, je v podstatě veřejná záležitost, nezoufejte. Relativně jednoduše se dá riziko zneužití Vašeho počítače dramaticky snížit. Ano snížit, nikoliv eliminovat, ke stejnému závěru také sami dospějete po dočtení tohoto sborníku. Stoprocentní jistotu bezpečí dává pouze vypnutý počítač. Aby bylo Vaše používání výpočetní techniky bezpečnější, stačí dodržovat devatero níže uvedených zásad.

Ještě než se pustíme do zmiňovaných pravidel bezpečného používání sítě WEBnet, vysvětleme si na velmi zjednodušeném modelu co se v počítači děje, aby i netechnicky zaměření uživatelé mohli lépe proniknout do tajů jednotlivých prvků bezpečnosti. Znalci jistě prominou drobné nepřesnosti v příkladu.



Pro potřeby sborníku vystačíme se zjednodušeným schématem počítače naznačeném na obrázku. Počítač je zde představován přerušovanou čarou, uvnitř se pak nachází řada běžících programů, které vykonávají různé činnosti potřebné pro správné fungování počítače, na obrázku jsou tyto programy zobrazeny jako duchové. Pokud je počítač připojen do sítě, ať už kabelem nebo bezdrátově, je možné si komunikaci s okolním světem představit jako příjezdy a odjezdy vlaků naložených informacemi. Jednotlivé informace přijíždějí k různým brankám, které se nazývají porty. Každý program, který se účastní výměny informací, má přidělen jeden či více portů, u kterých přebírá nebo expeduje informace.

3.1 ZÁSADA PRVNÍ – AKTUALIZACE OPERAČNÍHO SYSTÉMU A PROGRAMŮ

Při návrhu a tvorbě programů vznikají chyby, na které se přichází až s postupem času. Některé chyby jsou velmi zákeřné a umožňují daný program zneužít k činnostem, které by neměl dělat.

Každý slušný výrobce softwaru (programů) vydává opravy chyb, které jsou objeveny. Tyto opravy se nazývají záplaty (anglicky patch). Je potřeba je dostat do počítače procesem, který se nazývá aktualizace (anglicky update). Vrátíme-li se k přirovnání programu k duchovi, pak si aktualizaci můžete představit jako školení o bezpečnosti. Duchové sedí v lavicích a Dr. Patch, CSc. jim vysvětluje, co dělají špatně a jak se mají správně chovat.

Většina operačních systémů a nových programů umožňuje automatické stahování aktualizací z internetu. Nejjednodušší je tedy ponechat zapnutou tuto volbu a první zásadu splníte bez vynaložení dalšího úsilí. Pokud Váš operační systém nepodporuje automatické aktualizace, doporučujeme spustit aktualizaci alespoň jednou týdně.

V síti WEBnet se nacházejí v podstatě dva typy počítačů – stroje zařazené do projektu ORION a ostatní. O aktualizaci počítačů ORION se stará CIV, zatímco o ostatní počítače se musí postarat jejich administrátor. Na adrese `http://support.zcu.cz/aktualizace` lze nalézt další informace týkající se aktualizací.

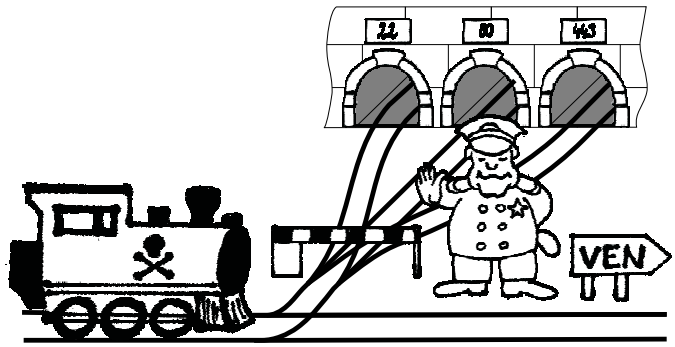
3.2 ZÁSADA DRUHÁ – ANTIVIROVÝ ŠTÍT

Předpokládejme, že nějaký neproškolený nebo vysloveně zlý program se ve Vašem počítači pokusí provést akci, kterou by rozhodně dělat neměl. Bez antivirového programu mu v této činnosti nikdo nezabrání. Antivirový program je ve své podstatě policejní hlídka, s pendrekem v rukou se prochází v počítači a hlídá, co který program dělá. Pokud se mu jeho činnost nezdá, přetáhne ho pendrekem a zabrání mu v jeho nekalé aktivitě.

Stáhněte si a nainstalujte antivirový program a nechte jej běžet v rezidentním módu. Někdy se tatáž služba označuje jako antivirový štít. Nezapomeňte, že antivirový program je potřeba také neustále aktualizovat, aby „rejstřík podezřelých aktivit“ zahrnoval nejnovější „počítačové zločiny“.

Pro všechny zaměstnance a studenty Západočeské univerzity v Plzni je zakoupena multilicence na antivirový program AVAST. Pokud nepoužíváte žádný antivirový program, navštivte co nejdříve stránky `http://support.zcu.cz/antivir`, při instalaci postupujte podle uvedených pokynů.

3.3 ZÁSADA TŘETÍ – FIREWALL



Vraťme se ke komunikaci programů s okolím. Jednotliví duchové sledují svoje svěřené porty a pokud přijedou informace, vrhnou se na jejich zpracování - bez ohledu na původ těchto informací. Firewall se chová podobně jako celnice, zásilky z nežádoucích adres nebo k nežádoucím portům jednoduše neprojdou a jsou vyhoštěny. Snižuje se tak riziko infiltrace zlých programů.

Potřebujete-li například jenom prohlížet webové stránky, pak stačí propouštět informace pouze portem s číslem 80 nebo 443. Některé firewally jsou ještě chytřejší a kontrolují také, který program u daného portu čeká, a pokud tam nemá co dělat, informace nedostane. Pokud jsou tedy „závadné informace“ zasílány z „důvěryhodné adresy“ a příslušný program je neaktualizovaný, pak nám firewall nepomůže. Je tedy mylné se domnívat, že firewall vyřeší všechny problémy.

Nainstalujte si firewall a vhodně jej nastavte. Pro uživatele sítě WEBnet jsme na stránkách `http://support.zcu.cz/firewall` připravili návody pro instalaci a vzorové konfigurace běžně používaných firewallů, které jsou k dispozici zadarmo. V systémech Linux se jedná o konfiguraci firewalu *iptables*, pro Windows 2000 a Windows XP pak o firewall nazvaný *WIPFW*. Pokud využíváte nějaké specializované programy nebo síťová zařízení, obraťte se na svého lokálního správce, aby konfiguraci vhodně upravil.

3.4 ZÁSADA ČTVRTÁ – ADMINISTRÁTORSKÝ VS. UŽIVATELSKÝ ÚČET

Na každém počítači existuje jeden speciální uživatel, nazývaný *administrátor* (v systémech Windows) nebo *root* (v systémech Unix). Jak už název napovídá, jde o uživatele, který spravuje celý počítač a není ve své činnosti ničím omezován, může spouštět všechny programy a přistupovat ke všem souborům. Ostatní uživatelé mají omezené pravomoci, nemohou ke všem souborům, nemohou ani instalovat nové programy, zkrátka mají přístup pouze k části počítače.

Výše uvedený fakt má jeden pozitivní bezpečnostní dopad. Pokud jste přihlášení jako běžný uživatel a dojde k nejhoršímu, kdy je aktivován zlý program, má tento program omezený přístup k počítači stejně jako Vy a nemůže tak napáchat tolik škody. Používání uživatelského účtu má i další pozitivní stránky, které přímo nesouvisejí s bezpečností. Pokud budete používat uživatelský účet, výrazně snižujete riziko, že si omylem něco chybně nastavíte a ohrozíte tak funkčnost Vašeho počítače. I když na konkrétním počítači pracujete pouze Vy, zřiďte si kromě administrátorského účtu také účet běžného uživatele a používejte jej pro běžnou práci.

3.5 ZÁSADA PÁTÁ – BEZPEČNÁ KOMUNIKACE

Informace přenášené mezi počítači putují přes několik síťových prvků (lze si je představit jako výhybky) než dorazí k cíli. Během cesty se může téměř kdokoliv podívat co je přenášeno. Dokud se jedná o běžně dostupné informace, jako je předpověď počasí, není důvod se znepokojovat. Jenže přenášeny jsou často i informace o přihlašovacím jméně a heslu, obsahy e-mailů, pokyny k bankovním operacím, apod. - to jsou údaje, které by každého odezírajícího piráta potěšily. Protože odezírání nejde zabránit, je nutné nějak zařídit, aby útočník nemohl získané údaje přečíst. K tomuto účelu se využívá šifrování. Všechny informace jsou zašifrovány, a i když je někdo během přenosu získá, bez patřičného dešifrovacího klíče jsou mu k ničemu.

Blíže se na problematiku zmiňovaných klíčů podíváme později. Oba dva komunikující protějšky mají dohodnutý způsob komunikace, který je označován jako *protokol*. Pokud protokol využívá šifrování, je mu dovoleno používat přívlastek *zabezpečený*.

V síti WEBnet nejsou nezabezpečené protokoly podporovány, takže jste v podstatě nuceni se chovat bezpečně, jinak Vám daná služba nebude fungovat. Protokoly a služby, kterých se to týká, jsou následující:

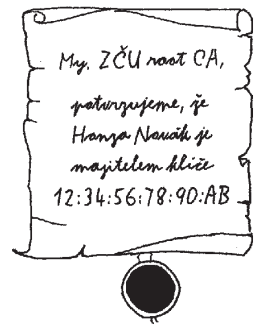
- *terminálový přístup* funguje přes protokol SSH,
- k *elektronické poště* je přistupováno protokoly IMAP nebo POP se zabezpečením SSL

Návody pro správné nastavení výše uvedených programů jsou pro Vás připraveny na adrese `http://support.zcu.cz/protokoly`. Pokud využíváte i další služby komunikující po síti, ověřte si, zda používají zabezpečené protokoly.

3.6 ZÁSADA ŠESTÁ – OVĚŘENÍ, S KÝM KOMUNIKUJEME

Dodržováním páté zásady jsme před piráty data zabezpečili během jejich putování k cíli, ale co když data doputují sice bezpečně, ale do nesprávných rukou? Na této myšlence je založeno tzv. *rhybaření* (slovní hříčka z anglického phishing). Nekalý živel si udělá vlastní kopii zajímavé stránky (např. banky či internetového obchodu) a nějakým způsobem na ni naláká uživatele – e-mailem, podvržením odkazů na jiných stránkách a podobně. Stránky jsou obvykle vizuálně k nerozeznání včetně URL (adresa stránky), kde je využíváno podobnosti některých znaků, např. `1` vs. `l`, `w` vs. `vv` a další. Příklady jsou uvedeny na stránkách `http://support.zcu.cz/phishing`. Zadané přístupové údaje, čísla kreditních karet a e-mailové adresy pak putují přímo k pachateli. U terminálového spojení je technika obdobná.

Vzpomeňme si na šifrovací klíče z předchozí kapitoly. V podstatě jde o matematickou magii (matemagiku), která umožňuje za pomoci *veřejného klíče* vytvořit kódovanou zprávu a *privátním klíčem* tuto zprávu zase dekódovat. Jak už názvy klíčů napovídají, privátní vlastní pouze majitel a nikdo jiný jej nezná, zatímco veřejný je volně k dispozici. Pokud chceme zajistit, aby naši odeslanou zprávu mohl přečíst pouze příjemce, zašifrujeme ji jeho veřejným klíčem. Protože nikdo jiný než on nemá potřebný soukromý klíč, nemůže si nikdo nepovolaný přečíst obsah zprávy.

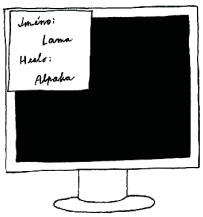


Teď jistě přemýšlíte, jak zajistit, že Vám někdo nepodstrčí svůj falešný veřejný klíč a bude se vydávat za toho, s kým chcete komunikovat. Tento problém už naštěstí vyřešili chytří pánové zavedením tzv. *certifikátů*. Takový certifikát je vlastně průkaz spojující informace o veřejném klíči s identitou konkrétního člověka nebo počítače. Každý certifikát je vydáván nějakou *certifikační autoritou*, což je instituce, která doklady vydává a která zaručuje, že údaje v certifikátu odpovídají skutečnosti, tj. zkontroluje identitu deklarované osoby či počítače a přesvědčí se, že vlastní odpovídající privátní klíč. Stejně jako na běžných dokladech je také na certifikátu „razítko“ certifikační autority ve formě *elektronického podpisu*. Pochopitelně ne všem certifikačním autoritám lze věřit, takže je nutné být lehce paranoidní a vždy prozkoumat věrohodnost certifikační autority. Uživatelé sítě WEBnet mohou důvěřovat certifikační autoritě *ZCU root CA*.

Kořenové certifikáty (to jsou ona matemagická razítka) všech certifikačních autorit, kterým důvěřujete, je potřeba dostat bezpečnou cestou do Vašeho prohlížeče, aby bylo možné ověřit, zda se nejedná o podvrženou certifikační autoritu. Návod pro bezpečný import kořenového certifikátu *ZCU root CA* je na adrese `http://support.zcu.cz/pki`. Všechny certifikáty podepsané certifikačními autoritami, které máte importované ve Vašem prohlížeči, pak budou automaticky považovány za důvěryhodné. Vyhnete se také nutnosti stále kontrolovat certifikáty stránek, které běžně navštěvujete. Výrazně se tím sníží pravděpodobnost přehlédnutí nějaké nekalosti nastražené rhybáři.

3.7 ZÁSADA SEDMÁ – ZACHÁZENÍ S HESLEM

Každý uživatel počítače ví, že při využívání poskytovaných služeb (e-mail, studijní agenda) je potřeba se přihlásit. Jednak zadáte své uživatelské jméno, aby systém věděl, s kým má tu čest, a pak musíte zadat heslo, kterým prokážete, že jste to opravdu Vy. Vaše jméno a heslo tedy tvoří Vaši identitu v rámci dané služby. Počítač nemá jiné možnosti jak zjistit, že jste to opravdu Vy. Pokud tedy někdo zná Vaše jméno i heslo, může se za Vás vydávat a Vaším jménem provádět různé nekalé činnosti, které by si pod svojí identitou nedovolil. Navenek to však bude vypadat, že pachatelem jste Vy!



S heslem je tedy potřeba zacházet velmi obezřetně, podobně jako s PINem bankovní karty. Heslo je Vaše tajemství a musí to tak zůstat. Nikdo jiný (ani administrátor) nemá žádný legální důvod jej znát. Aby mohlo heslo zůstat utajeno, nemělo by být nikde napsáno a už vůbec ne na lehce dostupném místě. Nejbezpečněji je heslo uloženo ve Vaší paměti. Existují však i další možnosti, jak Vaše heslo zjistit – hrubou silou, kdy si útočník postupně zkouší různá hesla, dokud se mu nepodaří zjistit to správné.

Jak si ale zvolit heslo, které nejde snadno uhodnout a zároveň je snadno zapamatovatelné? Podle posledních výzkumů chytrých pánů v bílých pláštích je vhodné zapamatovat si jakousi krátkou říkanku, frázi, citát nebo větu z oblíbené knihy a na jejím základě pak vytvořit heslo z prvních písmen jednotlivých slov. Například z větičky *„Kdo problém nepomáhá řešit, ten ho pomáhá vytvářet.“* vezmeme první písmena a diakritická znaménka, tj. *Kpnř,thpv.*, protože písmenka s diakritikou nejsou příliš vhodná, tak je nahradíme číslem klávesy, na které se nacházejí – pro *ř* je to 5 – a dostaneme pěkné heslo *Kpn5,thpv.*.

Z preventivních důvodů je heslo nutné čas od času změnit, protože někdo mohl vidět, jaké heslo zadáváte a časem je stále pravděpodobnější, že heslo může být zjištěno hrubou silou. V síti WEBnet jste nuceni změnit heslo každých 6 měsíců, což je rozumný kompromis mezi pohodlím uživatelů a bezpečností.

Pokud máte více uživatelských účtů (identit), např. konto v prostředí ORION, soukromý e-mail a přístup do banky, mějte pro každý vždy jiné heslo! V případě, že by někdo získal heslo k jedné identitě, nebude mít pak přístup i ke všem ostatním. Většina služeb v síti WEBnet využívá jednotného přihlašovacího systému, kdy na základě jednoho konta ORION můžete využívat více služeb, proto je třeba se k této Vaší identitě chovat obzvlášť obezřetně.

3.8 ZÁSADA OSMÁ – BEZPEČNÉ ZACHÁZENÍ S E-MAILEM

E-mailovou schránku čte snad každý uživatel připojený k internetu, proto jsou e-maily často využívány pro potřeby tzv. sociálního inženýrství prováděného nekalými živly. Všechny postupy využívají znalostí psychologie a snaží se čtenáře přimět k nerozumnému jednání. E-mail s takovýmto obsahem rozhodně patří mezi nevyžádané a tvoří nezanedbatelnou část nevyžádané pošty (*spam*). Podívejme se blíže na typické zástupce spamu, kteří mohou ohrozit bezpečnost Vašeho počítače nebo Vašich dat či jiných prostředků.

Nejrozšířenějším způsobem jak uživatele donutit ke spuštění škodlivého programu jsou *zlé přílohy maskované lákavým názvem*, například se jedná kamufláž za obrázek názvem *„úžasný_obrázek_co_musíte_vidět.jpg.exe“*. Převážná většina uživatelů systému Windows má zapnutou volbu „Skrývat přípony známých typů“, takže koncovka `exe` indikující spustitelný program není vidět. Po spuštění takové přílohy je počítač ihned kompromitován. Vypněte volbu skrývání přípon známých typů a spustitelné soubory (`exe`, `com`, `bat`, `pif`, `scr`) v žádném případě neotevírejte. Návod, jak nastavit systém Windows, je na adrese `http://support.zcu.cz/pripony`.

Velmi časté je *vyzvídání* hesel nebo jiných přístupových kódů. Obvykle se v takovéto zprávě dozvíte, že pokud ihned nezašlete své přístupové kódy k internetovému bankovnictví, bude Vám zablokován Váš účet. Původce zprávy očekává, že v návalu rozrušení se uživatel nebude zabývat věrohodností zprávy a požadované údaje zašle. Jak už bylo řečeno v kapitole zabývající se hesly, Vaše přístupové údaje nesmí nikdo znát! Takovýto e-mail ihned smažte. Obecně je dobré se vždy zamyslet, jestli odesílatel zprávy má právo znát požadované údaje, a jestli není divné, že důležitá zpráva putuje e-mailem místo doporučeným dopisem jako obvykle.

Často do Vaší e-mailové schránky zavítá také *hoax*, což je poplašná zpráva, novinářská kachna nebo jinak nazvaná mystifikace. Obvykle varuje před nějakým ohromným nebezpečím, které se dá odvrátit jenom tím, že o něm budou všichni vědět. Zpravidla se odvolávají na různé oficiální zdroje jako Microsoft, FBI, ministerstva a podobně. Většinou jde o zprávy, které nenadělají mnoho škody, ale v případě různých petic nebo smyšlených podpisových akcí se požaduje vyplnění různých osobních údajů včetně adresy a rodného čísla. Takovéto e-maily rovnou mažte, v případě nejasnosti můžete navštívit server `http://www.hoax.cz`, kde je uveden přehled nejčastěji šířených hoaxů.

Ještě je potřeba zmínit, že odesílatel zprávy uvedený v hlavičce e-mailu nemusí být skutečný autor zprávy! Stejně jako lze vyměnit obálku u klasického dopisu, lze přepsat informace o odesílateli. Jistotu nám dá pouze *digitální podpis*, který na pomyslnou obálku přidá matemagickou pečeť za pomoci certifikátu patřícího odesílateli. V síti WEBnet jsou podpisové certifikáty zatím poskytovány pouze vybrané skupině uživatelů, kteří pracují s důležitými dokumenty.

Každý uživatel sítě WEBnet si na adrese `http://mail.zcu.cz/` může zapnout antivirovou a antispamovou kontrolu příchozí pošty, čímž se výrazně zredukuje počet nevyžádaných e-mailů a závadných příloh, které dojdou do Vaší e-mailové schránky. Jde o velmi užitečné pomocníky, kteří Vám pomohou bezpečněji zacházet s e-mailem.

3.9 ZÁSADA DEVÁTÁ – INSTALACE A POUŽÍVÁNÍ VHODNÝCH PROGRAMŮ

Ne všichni autoři software jej vytvářejí s úplně čistými úmysly a některé programy pak mohou mít v popisu práce provádění škodlivé činnosti. Pokud takový program nainstalujete a spustíte, můžete se rovnou rozloučit s bezpečím, protože zpravidla škodí způsobem, který antivirový policista nedokáže odhalit.

Jak takový nebezpečný program odhalit? Jako běžný uživatel sítě WEBnet nemáte, v rámci pracovní činnosti, mnoho šancí používat nevhodné programy, protože Váš zaměstnavatel Vám prostřednictvím příslušného správce připraví vhodné „hodné“ programy.

Škodlivé programy se vyskytují zejména tam, kde se pohybujeme na hraně zákona. Zejména jde o software pro P2P sítě – někteří klienti DC++, BitTorrentu, Kazaa prokazatelně provádějí i jiné věci než ke kterým byly určeny. Stejně tak tzv. *crack* – pokud máte nelegální software, a přesto jej chcete používat, je potřeba nějak překonat ochranu (kontrola CD, registrace a podobně), což dělá právě program nazývaný crack. Jenže kromě této „žádané“ činnosti může provést cokoliv jiného!

Neinstalujte programy od nedůvěryhodných výrobců, nejlépe neinstalujte vůbec žádné programy, které nutně nepotřebujete k práci.

Kapitola 4

Slovo závěrem

Po přečtení tohoto sborníku byste měli mít základní přehled o problematice počítačové bezpečnosti. Vědět, že stejně jako všude jinde i ve výpočetní technice se nacházejí kriminální živly, které zajímá pouze vlastní zisk. Bylo Vám zde představeno devět základních rad, které Vám mají pomoci s ochranou před těmito zlými hochy a děvčaty. Budete-li se těmito radami řídit, máte šanci vyhnout se drtivé většině bezpečnostních problémů. Pamatujte si, že bezpečné chování je zejména ve Vašem vlastním zájmu.

Bezpečný pobyt v síti WEBnet Vám přeje

Váš CIV