4. Člověk, společnost a počítačové technologie

4.1 Bezpečný počítač

Bezpečný počítač pro práci je takový počítač, který neobsahuje žádný nežádoucí software a který není napadnutelný z Internetu. Část bezpečnosti zajišťují technická opatření, značný podíl mají také naše znalosti a naše opatrnost.

Aktualizace operačního systému a aplikačních programů

Dnešní operační systémy a aplikační programy jsou nesmírně složité, dlouho byly zaměřeny spíše na množství funkcí než na bezpečnost a výsledkem je stav, kdy jsou nové **bezpečnostní chyby** (díry) v systému (nebo v jiných aplikacích – typicky v prohlížeči webu) objevovány snad každý týden.

Znamená to, že skript ve webové stránce má vinou bezpečnostní chyby v prohlížeči webu přístup k souborům ve vašem počítači (a může je někam poslat nebo je smazat), vir přiložený ke zprávě se sám spustí (bez otevření přílohy), při prohlížení obrázku se může spustit program z Internetu, červ se může dostat do vašeho počítače a díky chybě (tzv. přetečení zásobníku paměti) se dostane do systémové paměti a může si dělat, co chce.

(Automatické) aktualizace systému

Jakmile je bezpečnostní chyba popsána, chvilku trvá, než se objeví vir, který ji umí využít. Výrobce operačního systému většinou mnohem dříve vydá (vystaví na Internetu) **opravu (záplatu, tzv. patch)**, která chybu odstraňuje. Systém na našem počítači ale chybu stále obsahuje, musíme do něho záplatu aplikovat – **aktualizovat systém**. Pokud to uděláme včas, případný škodlivý kód se již do počítače touto chybou nedostane.

Naštěstí však není potřeba hlídat si nové aktualizace systému (Windows i Linux), stačí správně nastavit (zapnout, povolit) **automatické aktualizace**. Pokud je počítač připojen k Internetu pevnou linkou (tj. nepřetržitě), *stahuje si operační systém sám potřebné aktualizace a pouze upozorňuje uživatele na jejich instalaci*. Totéž platí o většině aplikací, ty také často kontrolují, zda není k dispozici jejich nová verze/bezpečnostní záplata.

Firewall a další bezpečnostní nástroje

Porty – brány do počítače, hackeři, firewall. Každý počítač připojený k Internetu má svoji jednoznačnou IP adresu. Jednotlivé služby (web, pošta, sdílení souborů) pak využívají jednotlivé porty, jakési „brány“ do počítače. Např. web používá port 80, pošta odchází většinou přes port 25 a přichází přes port 110 apod. Portů je teoreticky 65 535 a přes všechny by se do počítače mohly dostat počítačové červy. Využívají je také lidé, snažící se o neoprávněný přístup do cizích systémů (**hackeři**). Program, který hlídá, co se na jednotlivých portech děje, a povoluje jen námi vyžádanou komunikaci, se nazývá **firewall** („požární zeď“, oddělující počítač od Internetu).

- **Osobní firewall** je dnes většinou součástí OS, kontroluje síťovou komunikaci z/do počítače.
- **Síťový firewall** sleduje komunikaci mezi vnitřní (lokální) sítí LAN a vnější sítí WAN (Internetem). Bývá součástí směrovače (routeru).

Další nástroje bývají dodávány jako součást kompletních (většinou komerčních) bezpečnostních balíků. Ty zahrnují **kontrolu odkazů** na webové stránky, takže na nebezpečný web se vůbec nedostaneme, **kontrolu obsahu** již navštívené webové stránky, zvýšené **zabezpečení osobních údajů** a další nástroje. O většině z nich bude zmínka dále v části o škodlivých kódech a antivirech.

Vyzkoušejte

Podle specialistů na software je v programech asi jedna bezpečnostní chyba na 1 000 řádek kódu. Zjistěte, kolik přibližně řádek kódu obsahuje OS, který používáte na svém počítači a spočítejte, kolik se v něm teoreticky skrývá bezpečnostních chyb.

Zajímavost

Service Pack – balíček záplat

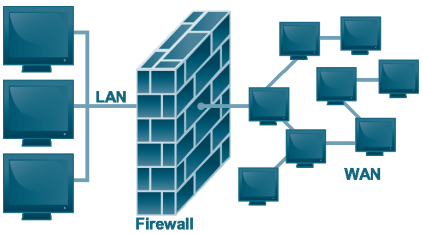
Při nákupu operačního systému je na instalačním CD často napsáno: Systém Microsoft Windows … včetně Service Pack 2. Co to znamená? Postupné přidávání záplat (od vzniku CD s instalací systému až po současnost) by bylo velmi nepohodlné. Firma Microsoft proto občas vydává pro své systémy servisní balíčky, které zahrnují veškeré v době jejich vzniku známé záplaty a často také přidávají nové funkce a vylepšují zabezpečení počítače. Novější vydání určité verze operačního systému pak již v sobě mají tento Service Pack zahrnut.

Tip

Aktualizace se někdy dělí na *bezpečnostní (kritické)*, které je nutné vždy okamžitě instalovat a na *volitelné*, které přidávají nové funkce.

Zajímavost

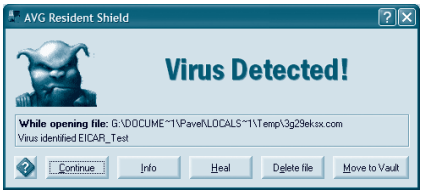
Systémy Windows v době vzniku knihy neobsahovaly centrální správu aktualizací instalovaných programů, systém zajišťoval pouze své aktualizace a dále aktualizace dalších programů firmy Microsoft. Kvůli tomu běží na počítačích množství stále spouštěných procesů, které zajišťují aktualizaci jednotlivých instalovaných programů. Některé distribuce Linuxu již měly centrální aktualizaci software implementovánu.



Zjednodušené schéma fungování firewallu (zdroj: Wikipedia.org, autor: Bruno Pedrozo)

Pracujeme

1. Potřebují aplikace využívající tzv. cloud computing neustálé aktualizace?
2. Zkontrolujte nastavení automatických aktualizací OS na svém počítači a ověřte zapnutí brány firewall.



Zajímavost

Hacker bylo původně označení pro počítačového odborníka, který je schopen analyzovat a optimalizovat činnost programů v počítači a zjišťovat a využívat jejich funkce, a to včetně jejich nedokumentovaných nebo běžně nepřístupných vlastností. Dnes se tento pojem používá pro lidi snažící se „nabourat" do cizích systémů použitím běžným uživatelům neznámých funkcí a postupů (z nichž většina je zveřejněna na Internetu). Část hackerů prolamuje (crackuje) ochrany bránící kopírovat programy, filmy nebo hudbu.

Zajímavost

Klasické viry byly na ústupu, dnes se opět šíří a to pomocí přenosných USB disků („flešek"). V systémech Windows je zahrnuta funkce, která po vložení média (disku DVD, flash disku) na něm hledá soubor Autorun.inf a pokud ho najde, spustí program v tomto souboru uvedený. Stačí tedy vložit zavirovaný flash disk do počítače a za pár desítek sekund je vir v počítači – pokud ovšem nemáme funkční antivir.

Zajímavost

V roce 2005 byl proveden následující test: K Internetu byl připojen zcela nezabezpečený server s úmyslně neaktualizovaným systémem. Již za *4 minuty* po svém připojení byl tento server atakován internetovým červem. Za *dva dny* po připojení byl nalezen hackerem, který do něho nainstaloval falešné stránky banky a pokoušel se z něho rozesílat tzv. phishing – zprávy vyžadující zadání přístupových údajů k účtu této banky. Poté byl server odpojen. Jak dlouho by napadení nezabezpečeného počítače trvalo dnes?

Důležité

V roce 2010 byl počet počítačů nakažených nějakým druhem malware odhadován optimisty na 50 %, pesimisty na více než 60 %. V absolutních číslech šlo o více než 500 milionů počítačů.

V tomtéž roce existovalo asi 40 mil. škodlivých kódů, většina z nich byla zaměřena na systémy Microsoft Windows.

(Laici používají často pojem „nakažený" nebo zavirovaný *počítač*. Počítač (hardware) nakažený není, malware běží v jeho OS, zavirovaný je tedy *operační systém*.)

Počítačové viry a červy, malware a spyware

Počítačový vir nebo červ je program, který někdo vytvořil, aby získal důvěrná data z vašeho počítače, získal kontrolu nad vaším počítačem nebo alespoň mohl využívat jeho zdroje, případně aby zničil vaši práci. Proč to lidé dělají? V současnosti není nejčastějším důvodem psychické narušení tvůrce (potřeba něco si dokázat), jako tomu bylo dříve, ale snaha *okrást majitele počítače o data, hesla, počítačové zdroje, tedy v konečném důsledku o peníze*.

- **Virus** je malý program, který se umí *vložit do jiného programu* a s ním se šířit. Spuštěním programu tedy spustíte nevědomky i virus, který napadne další programy.
- **Makrovirus** je virus, který není součástí programu, ale *dokumentu, který může obsahovat makra*, tj. vlastně v dokumentu vložené programové kódy (dnes mnoho typů dokumentů).
- **Červ** *má vlastní soubor* a většinou se snaží přimět uživatele počítače, aby ho spustil, případně *využívá bezpečnostní chybu* (poštovního programu, prohlížeče webu apod.) a snaží se spustit sám. Některé *internetové červy využívají chyby v zabezpečení síťového připojení operačního systému* a šíří se přímo v paketech síťového protokolu. Jsou velmi nebezpečné, protože je nezachytí antivirový program a protože nevyžadují k napadení počítače aktivitu uživatele (jen jeho pasivitu, tj. opomenutí instalace bezpečnostní záplaty).
- **Rootkit** je škodlivý kód, který běží v jádru operačního systému s právy administrátora počítače. Špatně se detekuje a odstraňuje, protože je součástí jádra OS, může se skrýt před běžným antivirovým programem.
- **Malware** je shrnující označení pro škodlivé kódy (spojení malicious – zákeřný + software).
- **Spyware** jsou programy, které sledují činnost uživatele a předávají o ní někomu zprávy, nebo prohledávají obsah počítače a opět o něm někoho informují. Spyware (a adware) se často instaluje spolu s nějakým programem nebo pomocí aktivního obsahu webových stránek.
- **Adware** také sleduje aktivity uživatele počítače na Internetu a cíleně mu zobrazuje reklamu, nemusí to být vždy škodlivý kód.

Virus (červ), který přijde na váš počítač, ihned nepoznáte. Nějakou dobu se jen šíří, infikuje další soubory v počítači, rozesílá se na všechny nebo pouze na vybrané e-mailové adresy z vašeho adresáře. Teprve po určité době, v určitý den, po určitém počtu spuštění apod. provede nějakou nepříjemnou činnost:

- **Ovládnutí počítače.** Program typu *backdoor* (zadní vrátka) otevře některé porty počítače a naslouchá na nich povelům zvenčí. Podobně pracuje *trojský kůň*, program, který kromě své zjevné činnosti vykonává ještě nikde neuvedené akce bez souhlasu uživatele. Umožní tak získat útočníkovi přístup do počítače a pracovat s ním.
- **Odcizení obsahu počítače.** Vzdálený útočník si může díky získanému přístupu kopírovat soubory z napadeného počítače, případně použít program typu *keylogger* ke sledování stisknutých kláves (např. při vyplňování políček ve formulářích), nebo *dataminder*, program, který shromažďuje data o činnosti uživatele počítače.
- **Využití počítače pro nelegální činnost.** Mnoho zásahů proti rozesilatelům spamu (nevyžádané reklamní pošty) nebo serverům s nelegálním obsahem (dětská pornografie, rasistické a podobné stránky) skončí tím, že policie zasáhne u překvapeného majitele počítače, který o jeho nelegální funkci neměl ani tušení. Vzdálený útočník přeměnil nezabezpečený počítač v server rozesílající spam nebo poskytující zmíněné stránky.
- **Mazání obsahu počítače** není dnes u škodlivých kódů obvyklé. Kromě uspokojení z poškození neznámého člověka totiž nepřináší žádný (finanční) efekt.

Pracujeme

1. Udělejte si ve třídě malý průzkum, zjistěte, kdo se již setkal (nebo možná raději nesetkal) s malware, přesněji, kdo měl nakažen svůj operační systém.
2. Zjistěte aktuální statistiky rozšíření malware a počty nakažených počítačů.
3. Najděte hodnocení bezpečnosti současných OS pro osobní počítače.
4. Proč se většina malware zaměřuje na systémy Microsoft Windows?
5. Proč jsou počítačové červy nebezpečnější než viry a proč představují rootkity závažné ohrožení?

Metody útoků přes webové stránky a elektronickou poštu

Web, dnes nejpoužívanější služba Internetu, vytvořil svůj vlastní „svět“. Jako ve skutečném světě v něm působí lidé, kteří chtějí okrást nebo ovládnout jiné lidi. 60 % škodlivých kódů se dnes šíří přes nakažené webové stránky. Protože jsou autoři virů často technicky vzdělaní (nebo si najímají kvalifikované lidi), využívají širokou škálu technologií.

- **Umístění zavirovaného souboru** (programu) do jinak užitečného programu na web. Obvyklé na webech s nelegálním obsahem (cracky, warez). Uživatel si stáhne program, spustí ho a tím si zaviruje počítač.
- **Umístění zavirovaného souboru** na zcela *důvěryhodný web*, který byl předtím napaden hackery a místo původních souborů na něm byly umístěny zavirované programy.
- **Umístění skriptu (programu)** do kódu webové stránky. Pokud prohlížeč tento kód spustí, nahraje se do OS škodlivý kód. Prohlížeče však obsahují zabudované ochrany (zakázané skripty, spuštění pouze na dotaz), takže jde většinou o využití *bezpečnostní chyby v prohlížeči*, která nebyla záplatována (viz část o automatických aktualizacích). Rozšířeným útokem je nabídka *falešné antivirové kontroly počítače*. Webová stránka zobrazí upozornění na nalezení viru v počítači (fiktivní, emotivně zbarvené) a nabídne jeho odstranění, stačí pouze spustit nabízený antivir... Uživatel odmítne všechna bezpečnostní varování prohlížeče a vir spustí.
- **Vytvoření zavirovaného doplňku** (plug-inu) pro webový prohlížeč. Uživatel si s doplňkem nainstaluje i škodlivý kód.
- **Využití podvržené stránky.** Uživatel je přesměrován na falešnou stránku, napodobující originál (bankovní web apod.) kde vyplní své přihlašovací údaje a tím je poskytne útočníkům.
- **Další rafinované způsoby** „propašování“ viru do systému nebo získání důležitých (osobních) údajů. Stále se vyvíjejí a je proto potřeba sledovat odborné weby (*www.viry.cz, www.zive.cz, www.lupa.cz, www.root.cz*).

Elektronická pošta fungovala v minulosti jako hlavní přenašeč virů. Dnes se jich šíří e-mailem méně než 10 % a toto číslo stále klesá. Typickým způsobem je e-mailová zpráva *s přílohou, ve které je umístěn vir*. Při otevření přílohy dojde ke spuštění viru a nakažení počítače.

Většina e-mailových serverů má dnes integrován antivirový program. Zavirované zprávy jsou proto většinou odstraněny dříve, než si je stáhnete na svůj počítač. Proto útočníci používají *zprávy s odkazy* na zavirované webové stránky.

Antivirový program

Na antivirový program mnoho uživatelů počítače spoléhá jako na nepřekonatelnou ochranu svého počítače. Není to bohužel pravda, největším nebezpečím pro počítač bývá jeho uživatel (viz dále). Antivir však nabízí hodně a měl by být proto na každém počítači.

- **Antivir stále běží v paměti počítače** a kontroluje každý spouštěný program a každý otevíraný dokument. Nejdůležitější funkce, která by měla zabránit spustění jakéhokoliv škodlivého kódu.
- **Antivir na náš pokyn otestuje počítač,** přesněji zkonroluje, zda v paměti počítače neběží škodlivý kód a potom zkontroluje všechny (nebo určené) soubory v počítači.

Jak funguje antivirový program:

- **Porovnává programy** se svojí databází škodlivých kódů. Podobně **porovnává adresy webů** s černou listinou nebezpečných stránek.
- **Sleduje podezřelé aktivity** jako je zápis do systémových souborů a jiných programů, na webu obsah (javaskriptového) programu vloženého do stránky. Má tak šanci nalézt i dosud neznámý vir.

Aktualizace antiviru je samozřejmě zcela nutná, jinak by neznal nejnovější hrozby. Všechny antiviry se aktualizují samy, některé i několikrát denně. Zatím méně rozšířená je kontrola programů vůči antivirové *databázi umístěné na Internetu*, ta je samozřejmě neustále zcela aktuální.

Odvirování nakaženého počítače není vždy jednoduché, mnoho virů (pokud již běží v paměti) se dokáže skrýt před antivirovým programem. Řešením je *nabootovat (jiný) operační systém* z Live CD nebo z USB disku. Vir pak již není aktivní a je možné ho skenováním disku najít a odstranit. Alternativou je vyjmutí disku z nakaženého počítače, jeho umístění v čistém stroji a odvirování.

Upozornění

V dalším textu budou výrazy „zavirovaný“ nebo „napadený“ používány v obecném smyslu – *obsahující nějaký malware*, ne pouze počítačový vir podle specifikace na předchozí stránce.

Zajímavost

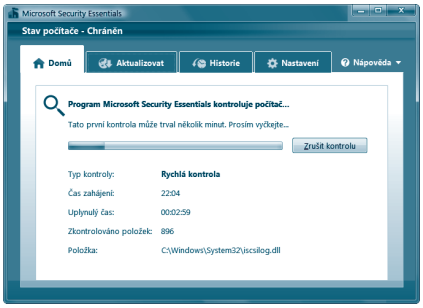
Webový prohlížeč nejen zobrazuje webové stránky, ale vykonává skripty v nich obsažené, načítá dynamicky nový obsah, přehrává animace atd. Jde vlastně o jakýsi operační systém pro webové aplikace. Ty by se neměly dostat k prostředkům hlavního OS, kvůli chybám se jim to ale občas podaří. Proto se také webový prohlížeč neustále aktualizuje.

Zajímavost

Hodně jednoduchým způsobem útoku přes e-mail je žádost o zaslání přihlašovacích údajů k nějakému účtu či službě. Ovšem i do takové zprávy někdo napíše své jméno, heslo, datum narození, číslo účtu, PIN platební karty apod.

Tip

Antivirů jsou desítky a mnohé dobře využitelné jsou dostupné zcela zdarma. Jiné jsou zadarmo pouze pro domácí (nekomerční) použití.



Pracujeme

Jaký používáte na svém počítači antivirový program? Je pravidelně aktualizovaný?

Zajímavost

Důvody a způsoby šíření spamu. Spam je pro své šiřitele výnosný, jinak by neexistoval. Firmy využívající spam dokáží tímto způsobem vnucovat obrovskému množství lidí své často nekvalitní nebo přímo nelegální zboží, a to za minimální náklady. Rozeslání spamu jeho šiřitele téměř nic nestojí – využívá volně dostupné poštovní servery a zcela obvyklé je i to, že spam je posílán z nakažených počítačů lidí, kteří vůbec nevědí, že jejich počítač byl k takovému účelu zneužit.

Podle odhadů tvořil spam v roce 2010 přes 80 % všech e-mailových zpráv.

Důležité

Na spam neodpovídejte ani nepoužívejte někdy uvedenou (fiktivní) možnost se z databáze pro zasílání odhlásit (remove address, unsubscribe apod.). Většinou to způsobí další nárůst spamu ve vaší schránce, protože tím potvrdíte, že adresa funguje a že spam čtete. (Něco jiného je, pokud se sami přihlásíte k odběru zpráv od nějakého seriózního informačního zdroje – zde odhlášení nebývá problém.)

Od	Předmět
無修正DVDを格安販売！	★★実録のDVD販売★★ 激安【代引き・局留...
Sanjuana Shawanna	axl 2u4
The Movie Downloads 2	Over 100 Million Movies & TV Shows - Unlimit...
Mr. Arjen Van Dirk	Dear friend
WordPress	[EDUIT - podpora výuky IT] Moderujte: „Co při...
Devin Sawyer	Gamblers advise Elite World Casino.
Tanaka Mayumi	★どうでもいいけど__★
礼子さん	奥さん、生でこんな事していいんですか？
san	WAITING FOR YOUR URGENT REPLY
Roscoe Tapia	Antibiotics will not cure viral illnesses, such as...
Tomoko Tabetha	guat 2o4
Marvin Oakley	Choose Canadian Pharmacy!

Zprávy zachycené spam filtrem

Tip

Spam filr mají zabudovány schránky všech velkých freemailových serverů, díky tomu se v doručené poště objeví skutečný spam jen výjimečně, ale kvůli tomu můžete přijít o důležitou zprávu. Je proto vhodné občas spam koš prohlédnout a zcela smazat.

Pracujeme

Jak řešíte problematiku spamu ve svém poštovním účtu? S jakým úspěchem?

Důležité

Pozor, myslet si, že zde uvedená fakta se *„mne netýkají, přeci nejsem tak …, abych někomu poslal(a) hesla nebo si zaviroval(a) počítač“* je naivní a nebezpečné. Podvodníci využívají lidskou psychiku (tedy i vaši), dokáží si dobře připravit terén, působit důvěryhodněji než ředitel(ka) školy a bez zdravé nedůvěry oklamou každého.

Problematika spamu a obrana proti němu

Nevyžádané, hromadně rozesílané zprávy (typicky s reklamou) se označují jako **spam**. Problematika spamu je v současnosti velmi závažná. Běžný uživatel e-mailu obdrží denně několik nevyžádaných zpráv, které musí mazat. Mnoha lidem se již stalo, že omylem spolu se spamem smazali důležitou zprávu nebo že takovou zprávu zadržel antispamový filtr. Rozesílání spamu je považováno za neetické a dnes je postižitelné i podle zákona.

Šiřitelé spamu (tzv. spameři) získávají adresy pro spam mnoha způsoby:

- Pomocí specializovaných programů (robotů podobných indexačním programům vyhledávacích serverů) **procházejí webové stránky**, diskuzní fóra a konference a sbírají z nich adresy.
- **Využívají viry**, které odešlou celý adresář poštovního programu na určitou adresu.
- **Kupují databáze** adres od jiných spamerů.
- **Generují náhodné adresy** podle seznamů jmen a rozšířených poštovních serverů.

Obrana proti spamu

Zabránit příjmu nevyžádané pošty je obtížné, spíše nemožné. Bránit se lze mnoha způsoby, žádný z nich však není stoprocentně účinný:

- Je potřeba být opatrný při zadávání své e-mailové adresy na různých webových serverech. Jednou z možností je mít dvě adresy (poštovní schránky), jednu používat pouze pro soukromé účely a druhou právě pro různé registrace. Tu pak stačí jen občas zkontrolovat a promazat.
- Zatím máme tu výhodu, že většina spamu je v angličtině, takže je podezřelá zpráva patrná na první pohled. Její rozlišení a mazání nám proto trvá kratší dobu než lidem v anglicky mluvících zemích.
- Vyspělé země přijímají zákony, umožňující postih nevyžádaných reklamních sdělení. Spameři však často využívají servery ze zemí, ve kterých podobná legislativní ochrana neexistuje.
- Poskytovatelé Internetu blokují počítače, ze kterých odchází množství zpráv (tzv. black list). Často na to ovšem doplatí nevinní lidé, protože spam server z jejich počítače vytvořil vir.
- **Poštovní program je nutné doplnit o antispamový filtr.** Ten sleduje výskyt slov indikujících spam (sex, viagra, porno atd.) a přesunuje takové zprávy do zvláštní složky. Navíc se většinou umí učit – sleduje, jaké zprávy sami označíte za spam, a podobné zprávy pak přesunuje automaticky. Občas je ale nutné složku se spamem zkontrolovat, zda v ní omylem nejsou důležité zprávy. Tato poslední možnost je nejúčinnější

Odpovědnost za obsah Internetu

Internet (web) nemá žádnou centrálu, žádného správce, proto také *za jeho obsah (jako celek) nikdo neodpovídá*. Je vždy na uživateli, aby posoudil informační hodnotu předkládaných informací a rozlišil pravdivé, nepřesné, neúplné, zavádějící a úmyslně nepravdivé informace.

Další komplikací je obtížnost aplikace zákonů na podnikání nebo zločinnou činnost pomocí Internetu. V běžném právním řádu platí, že k posouzení trestnosti se používají zákony země, ve které ke zločinu došlo. Jak ale posoudit trestné činy, které postihly občany naší vlasti provedené občany jiné země s využitím počítačů (domén, adres) registrovaných ve třetí zemi?

Co se týká obsahu, prosazuje se názor, že za obsah stránek *odpovídá jejich autor a nikoliv poskytovatel připojení a datového prostoru*, který o nelegálním obsahu nemusí vůbec vědět. Ovšem pokud je tento poskytovatel na nelegální stránky *upozorněn*, je povinen je *odstranit*.

Podvody (tzv. techniky sociálního inženýrství), hoaxy

Naprostá většina výše uvedených nebezpečných kódů vyžaduje součinnost uživatele počítače, zbytek jeho neopatrnost nebo nedbalost. *Většina červů se nešíří díky svému geniálnímu kódu, ale nesmírně jednoduše: uživatelé si je sami spustí a ještě potvrdí jejich instalaci.* Většina finančních podvodů není provedena dokonalými špionážními programy, ale tak, že útočník požádá majitele počítače o heslo k jeho bankovnímu účtu a on mu ho pošle! Útoky tohoto typu, které využívají psychologii člověka, bývají označovány jako *sociotechnické útoky*.

Odborníci na bezpečnost často konstatují, že „největší bezpečnostní problém je mezi klávesnicí a židlí“, tedy v člověku, který počítač obsluhuje. Útoky vede-

né tímto způsobem vycházejí ze znalostí psychologie a člověk, který nemá v této oblasti potřebné znalosti, jim může podlehnout bez ohledu na své vzdělání.

Jaké podvodné sociotechnické metody nejčastěji útočníci používají:

- **Nabízejí zdarma** erotický, pornografický nebo tajný obsah (fotografie celebrity XY, dokumenty o machinacích při soutěži YX apod.).
- **Nabízejí velký finanční zisk** při minimálním úsilí (např. tzv. nigerijské dopisy, slibující miliony po zaplacení pár desítek tisíc „poplatků").
- **Hrají na city uživatele** („můžete zachránit nemocného člověka...").
- **Vzbuzují strach** („pokud okamžitě neučiníte opatření – kontrolu svého účtu – může dojít k vážným důsledkům...").
- **Tváří se důvěrně** („přítel Ti věnoval píseň, klikni sem a stáhni si ji...").
- **Vydávají se za někoho jiného** (musím přenastavit server, zašlete heslo, píše správce školní sítě)
- **Mnoho dalších metod**, které většinou kombinují výše uvedené.
- **A hlavně: nutí jednat okamžitě**, nedávají čas na rozmyšlenou („pokud *okamžitě* nenainstalujete tuto bezpečnostní záplatu, obsah disku počítače bude vymazán...", pokud *ihned* nezrušíte příkaz, odejde z vašeho účtu...).

Základní obranou proti těmto útokům je vědět o jejich existenci a uvědomovat si fakt, že *Internet je potenciálně nebezpečné prostředí, které může přivést útočníka kdykoliv a kdekoliv.* Není třeba být paranoidní (chorobně podezřívavý), ale nebezpečí reálně existuje a stále roste, je proto nutné o něm vědět.

Ukradení (zneužití) identity. Typickým příkladem je tzv. *phishing* (odvozeno od *fishing* – rybaření). Útočník rozešle podvodné e-maily napodobující styl známé banky a vyzývající příjemce z nejrůznějších důvodů ke kontrole účtu. Po klepnutí na odkaz se zobrazí stránky vypadající přesně jako originální web banky. Po zadání přihlašovacího jména – čísla platební karty a hesla dojde zdánlivě ke slibované akci. Ve skutečnosti jste však zadali své přihlašovací údaje do formuláře, který je odeslal útočníkovi. Výše škody pak závisí na stavu vašeho účtu a případném limitu pro operace přes Internet...

Příklad phishingu: adresa se tváří jako odkaz na Ebay.com, ale vede jinam (viz IP adresu na stavovém řádku dole)

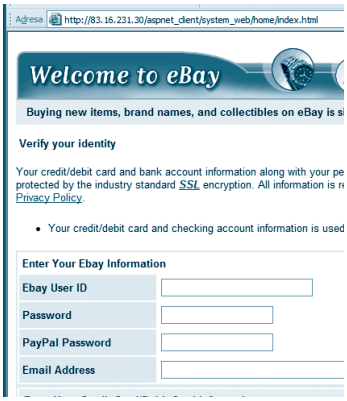
Hoax

Hoax není žádný program, je to falešná zpráva, která vás (často velmi emotivně) nabádá ke smazání „zcela nezjistitelného viru" nebo k posílání zpráv pro záchranu nemocného člověka apod. a k dalšímu rozesílání této zprávy. Pokud hoax uposlechnete, smažete si sami systémový soubor nebo alespoň zahltíte poštovní schránky jiným uživatelům. (Více na *www.hoax.cz*.)

Komplexní přístup k bezpečnosti IT

Bezpečnost počítače tedy spočívá v technických a organizačních opatřeních.

- **Technická opatření.** Základem je *udržování operačního systému v aktuálním stavu* okamžitou (nejlépe automatickou) instalací bezpečnostních záplat, dále zapnutý a správně nastavený *firewall,* dále funkční automaticky *aktualizovaný antivirový program*.
- **Organizační opatření** stojí na *znalostech* bezpečnostních hrozeb a na *opatrnosti*. Ve firmách a jiných institucích jsou určena přístupová práva uživatelů a stanoveny *směrnice*, kterými se musí řídit – komu mohou či nemohou poskytovat informace a jaké, jak se nakládá s písemnostmi (včetně způsobu jejich skartování, útočníci s oblibou vybírají popelnice s papíry a někdy v nich nalézají důležité informace).
- **Znalosti a opatrnost.** Tyto dvě věci dnes bohužel chybí většině uživatelů počítačů připojených do Internetu. Proč je tolik počítačů součástí sítí tzv. **botů** rozesílajících spam a útočících (tzv. DoS – Denial of Service útoky) na jiné systémy? Proč ztráty způsobené ukradením identity dosahují stamiliard dolarů? **Máte znalosti – používejte je a buďte opatrní.**



Podvržená stránka – kdo na ní vyplní všechny své osobní údaje?

Zajímavost

Příklady virů: Skupina hackerů založila lákavou skupinu na Facebooku. Všem příznivcům po čase zaslala odkaz na „supervideo". Ovšem při snaze o jeho spuštění vyskočilo okno se žádostí o instalaci potřebného kodeku. Kdo ho potvrdil, uviděl video, ale také si současně nasadil do systému trojského koně. (Žádosti od přátel neposuzujeme tak opatrně, jako od cizích lidí.)

Webová stránka hlásila nalezení škodlivého kódu a nabídla jeho odstranění. Uživatel potvrdí všechna hlášení OS. Po chvíli činnosti „antiviru" se objeví hlášení o úspěšnosti léčení. Systém je kompletně ovládnut virem.

Viry často skutečně udělají avizovanou činnost (zobrazení „zajímavých obrázků" apod.), ale přitom současně nakazí a ovládnou počítač – dnes je to otázka okamžiku.

Zajímavost

Klasickým případem odcizení identity je krádež osobních dokladů. Vaší identitou jsou i vaše jméno, adresa, telefon, rodné číslo a další osobní údaje. Buďte proto opatrní při jejich zadávání do různých webových formulářů.

Pracujeme

1. Najděte způsob fungování nějakého konkrétního viru a zpracujte o něm (a o možné ochraně proti němu) prezentaci.
2. Najděte způsob provedení nějakého konkrétního (sociotechnického) počítačového podvodu a zpracujte o něm (a o možné ochraně proti němu) prezentaci.
3. Laici se často ptají: „Proč by měli útočníci zaútočit zrovna na můj počítač?" Zkuste to vysvětlit.

4.2 Obecné bezpečnostní zásady a ochrana dat

Zásady vytvoření bezpečného hesla

Bezpečné heslo se často označuje jako tzv. **silné heslo**. To musí splňovat poměrně přísné parametry:

- **Obsahuje minimálně 8 znaků.** S počtem znaků výrazně roste počet možných kombinací a tedy potřebný čas pro útok hrubou silou (viz dále). Počet se může měnit, za pár let to možná bude 14 znaků.
- **Nedává smysl** v žádném běžném jazyku.
- **Obsahuje co nejvíce různých znaků**, tedy velká a malá písmena, číslice a nejlépe i další speciální znaky (? ! / (_ % / apod.).
- **Dá se dobře zapamatovat**, abychom si ho nemuseli nikam (třeba na monitor :-) zapisovat. (Viz Tip vlevo.).

Heslo může být odcizeno:

- **Sociotechnickými prostředky**, tj. podvodem zjištěno od uživatele (viz předchozí stránky), jedná se o nejčastější způsob.
- **Využitím neopatrnosti uživatele** (heslo napsané na lístečku nalepeném na monitoru, na spodní straně podložky pod myš, případně PIN napsaný na platební kartě).
- **Pomocí keyloggeru**. Malware běžící na počítači zjišťuje zápisy znaků do políček heslo (password) a odesílá je útočníkovi.
- **Stejná hesla.** Uživatelé často používají stejná hesla na důležité i relativně méně důležité operace. Např. heslo pro výběr e-mailové schránky jde přes Internet v případě protokolu POP3 zcela nezašifrováno. Útočník zjistí toto lehce odcizitelné heslo a pokusí se použít stejné heslo např. k přístupu do firemní sítě uživatele, kde se heslo přenáší šifrovaně. Tato metoda bývá bohužel často úspěšná.

Heslo může být zjištěno (prolomeno):

K informacím zabezpečeným heslem se útočníci pokoušejí dostat i pomocí klasických programových prostředků:

- **Útok hrubou silou (brute force attack).** Dostatečně výkonný počítač zkouší všechny kombinace do úvahy přicházejících znaků, přičemž začíná omezenou skupinou možností (jen písmena, jen malá písmena a číslice atd.). Kombinací, které je možné vytvořit z N znaků dlouhého řetězce, kdy jednotlivé znaky vybíráte z P možností, je P^N. Tedy např. ze 4 číslic (0–9, tj. 10 znaků) je možné vytvořit 10^4 kombinací, tj. 10 000 možností (0 0 0 0), (0 0 0 1) až (9 9 9 9). To zvládne současný počítač během krátké chvilky. U hesla dlouhého 6 znaků vytvořeného z cca 200 znaků (tabulka ASCII jich obsahuje 256, ale všechny nejsou do hesla vhodné) je kombinací 200^6, tj. 64 000 000 000 000, což již většinu útoků odrazí.
- **Slovníkový útok.** Útočník zjistí jazyk uživatele zabezpečeného systému. Použije kompletní slovník daného jazyka a začne zkoušet jednotlivá slova, nejlépe podle jejich četnosti používání. Běžné jazyky používají cca 200 000 slov, často používaných je cca 10 000, takže tento útok na slovní hesla bývá velmi často úspěšný.

Problematiku ochrany dat rozdělíme na dvě oblasti:

- **Příklad 1:** Úspěšný obchodník má na svém počítači adresy všech svých zákazníků i dodavatelů. Kdyby tyto informace *získala konkurence*, mohlo by to jeho obchody vážně ohrozit.
- **Příklad 2:** Firma vede účetní knihy pouze v elektronické podobě na počítači. Jeho porucha a *ztráta veškerého účetnictví* by způsobila vážné problémy, statisícové ztráty a případně i zánik firmy.

Pokud jste četli pozorně oba příklady, všimli jste si asi rozdílu, čím je majitel počítače ohrožen:

- V prvním případě **zneužitím dat cizí osobou**. Tomu můžete zabránit *zabezpečením* počítače a dat.
- Ve druhém je ohrožen **ztrátou dat** (ať technickým selháním počítače, působením počítačových virů nebo chybou obsluhy). Základní ochranou je *zálohování* (*archivace*) dat.

Tip

Silné heslo vytvoříte tak, že si řeknete pro sebe dobře zapamatovatelnou frázi (např. *Můj Mladší Bratr Se Jmenuje Petr*) a mezi první (nebo poslední) písmena slov vložíte číslice (třeba poslední dvojčíslí roku narození vaší matky) a někam ještě speciální znak (? ! / % " apod.). Heslo *!m3m7bsjp* je silné a umíte ho odvodit.

Heslo by nemělo obsahovat písmena s diakritikou (ěščřžý…) a většinou v něm nesmějí být mezery.

Zajímavost

Většina solidních systémů neukládá hesla svých uživatelů, ale pouze jejich otisk (hash, čtěte heš). Hash je vypočtený řetězec vždy stejné délky, který se vypočítá ze zadaného textu, ale text se zpětně z hashe zjistit nedá Systém při zadání vašeho hesla z něho vypočte hash a ten porovná se svým dříve uloženým hashem. Proto většina systémů při požadavku na změnu hesla vygeneruje dočasné heslo a požaduje po uživateli jeho změnu, původní heslo vůbec nemají k dispozici. Ovšem i na hesla ukládaná pomocí hash funkcí existují promyšlené útoky.

Zajímavost

Programy na útok hrubou silou zvládají vyzkoušet až milion hesel za vteřinu, programy pro slovníkový útok zkoušejí i slova pozpátku a přidávají za slova číslice. Smart brute force attack vychází z často používaných písmen a také třeba z toho, že jen málokdo dá speciální znak na začátek slova, zato velké písmeno spíše ano.

Pracujeme

1. Zkuste spočítat, za jak dlouho najde útok hrubou silou heslo, které je dlouhé 5 znaků a obsahuje pouze malá písmena bez diakritiky (kterých je cca 26).
2. Projděte si v duchu svá hesla. Jsou bezpečná? Obstála by před slovníkovým útokem? Liší se podle důležitosti využívané služby?

Zabezpečení počítače a dat před zneužitím cizí osobou

Zabezpečení počítače

Možností, jak znemožnit práci s počítačem cizí osobě, je několik:

- **Místnost s počítačem ochránit proti vniknutí** cizí osoby bezpečnostními prvky, jako jsou kvalitní dveře a zámky, fólie nebo mříže na okna. Tento způsob je snad poněkud primitivní, je však velmi účinný a bezpečný, používá se zejména u serverů sítí. Jeho výrazně méně bezpečnou variantou je uzamčení počítače ve stole. **Kensington lock** je kovový konektor běžně používaný u notebooků, ke kterému se připojuje silné ocelové lanko. To se pak uchytí ke stolu nebo k topení apod. Notebook pak není možné jednoduše vzít a odnést.
- **Vázat spuštění počítače** (přesněji start operačního systému) **na heslo** (lze nastavit v tzv. BIOSu počítače). Jde o poměrně účinnou ochranu, špatné heslo se však dá uhodnout nebo „odkoukat" při zadávání. Heslo navíc *nechrání data při krádeži celého počítače* – heslo lze (po otevření skříně počítače) vymazat a k datům se dostat.
- **Operační systémy** a podnikové informační systémy většinou při svém spuštění vyžadují zadání *jména uživatele a heslo*. Při využití architektury klient–server jsou data fyzicky pouze na centrálním serveru, ochrana dat na stanicích pak nemusí být řešena, pouze je třeba dobře zabezpečit přístup (i dálkový) k serveru.
- **Použít speciální přídavné zařízení** k počítači, do kterého je nutné pro spuštění systému vložit *identifikační kartu nebo flash disk* (obecně tzv. **token** – zařízení nesoucí kód), podobnou kartě do bankomatu. Odpadá nutnost pamatovat si heslo. Jde o velmi dobré zabezpečení počítače.
- **Biometrické metody** spočívají ve čtení fyzických parametrů uživatele, nejčastěji otisku jeho prstu nebo oční duhovky. Své prsty a oči máme stále při sobě a identifikace otiskem prstu je téměř dokonalá. Používá se dnes proto často u manažerských notebooků.

Zabezpečení důvěrnosti dat

Probrali jsme nyní možnosti, jak zabránit někomu nepovolanému pracovat na vašem počítači. Může se však stát, že přes všechna opatření se k počítači někdo dostane, v nejhorším případě počítač bude *odcizen*. Dá se nějak zabránit zneužití dat i v těchto případech?

Důvěrnost dat v počítači zajistíme pouze jejich **zašifrováním**.

- **Softwarová ochrana počítače.** Existují speciální programy, které se stanou téměř součástí operačního systému a *šifrují veškeré zápisy na disk a samozřejmě čtení z něho dešifrují*. Oprávněný uživatel se opět musí prokázat heslem, bez kterého je obsah disku nečitelný. Heslo (kód na dešifrování) může být uloženo na externím zařízení (tokenu, např. USB disku) a v takovém případě může být i velmi dlouhé (např. 128 znaků).
- **Hardwarová ochrana počítače.** Podobně fungují i *bezpečnostní karty* do počítače, které jsou snad ještě spolehlivější. Převezmou funkci řadiče disku s tím, že opět veškeré přístupy k němu šifrují a dešifrují. Bez znalosti hesla se s diskem nedá pracovat a jeho obsah je jen změtí nul a jedniček.

Tip

Zabezpečení rozdělíme na dvě oblasti:

1. Zabezpečení přístupu k počítači a k datům v něm.
2. Zabezpečení důvěrnosti dat, ke kterým se přeci jen někdo dostal.

Snímač otisků prstů se štěrbinou pro čipovou kartu

Pracujeme 1

1. Seřaďte zde uvedené způsoby zabezpečení počítače podle stupně zabezpečení.
2. Máte k dispozici a používáte na svém počítači nějaký způsob jeho zabezpečení?

Tip

Šifrování dat na disku nabízí podnikové edice běžných operačních systémů a k dispozici jsou komerční i volně šiřitelné programy. Protože hrozí určité riziko ztráty tokenu nebo hesla k přístupu, doporučuje se mít bezpečně (v trezoru) uloženou nešifrovanou zálohu svých dat.

Vyšší úroveň

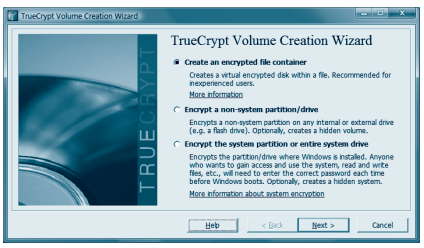
Šifrování souborů prakticky

Při šifrování souborů máme k dispozici dvě možnosti:

- Zašifrování celého disku nebo jeho oddílu (partition).
- Zašifrování vybrané složky.

V prvním případě, pokud nepoužijeme nástroje OS, se v systému tento oddíl bude jevit jako nenaformátovaný a nesmíme ho systémovými nástroji formátovat. Vždy musíme použít šifrovací program.

TrueCrypt je zdarma pod licencí GNU GPL (viz dále) šířený šifrovací program pro šifrování složek i celých disků. Umožňuje nově zformátovat diskový oddíl s jeho současným šifrování. Používá *kvalitní šifrovací algoritmy, heslo* se vytváří pohyby myší a je velmi bezpečné.



Pracujeme 2

Vytvořte zašifrovaný (nový, čistý) USB disk pomocí nějakého volně dostupného šifrovacího programu.

Zajímavost

Odborníci vedou spory o trvanlivosti záznamu na „vypalovaných" CD a DVD discích. Záloha na CD je nyní považována za výrazně trvanlivější (desítky let) než na DVD (jednotky let). USB disk se může vymazat elektrickým polem i teplotním šokem.

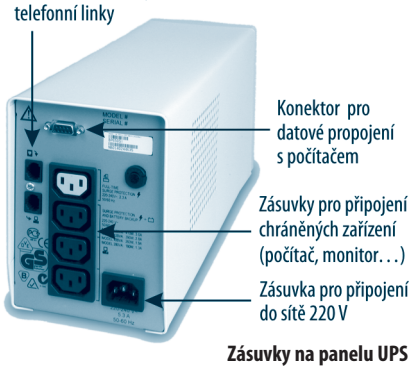
Provozní zálohování se provádí na pevný disk nebo lépe na USB disk, dlouhodobá záloha na CD (DVD) disk, obraz celého disku na externí disk

Externí pevný disk

Zajímavost

Účetní firmy vede účetnictví na počítači. Každý den před odchodem z práce archivuje (nahraje na USB disk nebo jiné médium) celé účetnictví a archiv uloží do trezoru. Před uzavřením roku vypálí kompletní stav účetnictví na dva CD/R disky včetně aktuální verze v té době používaného účetního programu.

Jednoho dne odpoledne dojde (je jedno jakým způsobem) k fyzickému zničení všech dat v počítači. Správce počítač opraví a uvede do plného provozu. Pak znovu nainstaluje účetní program a obnoví z USB disku účetnictví do stavu v okamžiku archivace, tj. předchozího dne odpoledne. Ztracena je práce jen od archivace do poruchy, tedy jedno dopoledne.



Zásuvky na panelu UPS

Ochrana dat před ztrátou, zálohování dat

Porucha počítače, chyba obsluhy, infekce počítačovými viry – všechny tyto události mají společný účinek, a tím je *poškození* nebo úplné *zničení* důležitých dat, která jsou uložena na pevném disku. Protože mají stejný účinek, je společný i základní způsob ochrany, a tím je *zálohování dat*.

Zálohování (archivace) dat je zkopírování dat z pevného disku na nějaké *jiné záznamové médium*. Nejčastěji se k tomu používají:

- **Pevný disk počítače.** Výhodnější než prostá kopie složek (disků) s důležitými daty je jejich *komprimace*, např. do ZIP souboru. Použití ZIP formátu má dvě výhody: záloha je odlišená i formátem a komprese dat šetří místo na pevném disku. **Pozor:** záloha umístěná *na stejném disku* jako jsou původní data chrání před vaší chybou (smazáním dat), *nechrání samozřejmě před zničením dat* při fyzické závadě celého disku.
- **Zapisovatelné optické disky** CD (700 MB), DVD (4,5 GB) a Blu-Ray (25 GB). Při použití jednorázově zapisovatelných médií jde o dlouhodobou zálohu, kterou je vhodné udělat po dokončení práce.
- **USB disky** (několik desítek GB). Velmi rychle provedená záloha, vhodná pro okamžité zálohování před uzavřením práce (zakázky apod.).
- **Páskové jednotky** využívají servery sítí, kapacita pásky je až stovky GB.
- **Externí pevné disky** se připojují přes USB rozhraní a jsou to vlastně běžné, kapacitou obvykle menší disky, doplněné o řídicí elektroniku. Jsou vhodné pro zálohování *celých disků nebo diskových oddílů*. Záloze disku se říká *obraz (image) disku*.
- **On-line úložiště** mají budoucnost, zvláště v placených verzích, kdy poskytovatel služby nese zodpovědnost za uložená data. Zdarma dostupné služby nabízejí zatím poměrně malé kapacity a vlastně žádné záruky trvalosti i důvěrnosti dat.

Pravidla zálohování

Zálohy je třeba provádět často, pravidelně, pečlivě a na kvalitní záznamová média:

- **Často:** Při poruše je práce od archivace do poruchy ztracena. Podle množství a důležitosti dat se určí potřebný interval jejich zálohování.
- **Pravidelně:** Co člověk nedělá pravidelně, na to zapomíná a má to pro něho malý přínos. Podle zákona schválnosti se něco pokazí v okamžiku, kdy archivaci neuděláte.
- **Pečlivě:** Vždy je třeba zálohovat všechna nová data a veškerou hotovou práci. Pomáhají s tím *specializované programy*, které kromě dokumentů umí zálohovat i zprávy elektronické pošty, adresář, oblíbené položky, nastavení systému apod.
- **Kvalitní záznamová média:** Značkoví výrobci uvádějí studie trvanlivosti dat a poskytují vyšší záruku obnovení dat než neznačková média. (Trvanlivost CD a disků DVD závisí na použitém barvivu.)

Možné způsoby zničení dat a ochrana proti nim, UPS

- **Technická porucha pevného disku.** Je poměrně nepravděpodobná, moderní disky jsou velmi spolehlivé, ale přesto k poruchám dochází.
- Porušení dat na disku **výpadkem napájení počítače**. K porušení dat nedochází při každém výpadku, ale pouze tehdy, když v okamžiku výpadku počítač zapisuje na disk. Pak může dojít k porušení struktury datových souborů a k nutnosti jejich obnovy z archivu.

Výpadku napájení i přepětí v síti lze předejít použitím *UPS – zdroje nepřetržitého napájení*. Je to přístroj, který se zapojí mezi zásuvku 230 V a napájecí kabel počítače. V případě vypnutí sítě 230 V začne bez přerušení napájet počítač ze zabudované baterie, jejíž napětí je převedeno na potřebných 230 V střídavých, a zvukovým signálem upozorňuje na tuto skutečnost. Běžné UPS umí napájet počítač jen cca 5–15 minut, tato doba však bohatě stačí na normální ukončení všech programů a vypnutí počítače. Většina UPS kromě této základní funkce také *odstraňuje kolísání síťového napětí a filtruje případná krátkodobá přepětí* včetně přepětí na telefonní lince, čímž chrání počítač.

Pracujeme

1. Jak často a jakým způsobem archivujete svá data?
2. Vytvořte směrnici pro zálohování dat malé realitní kanceláře, která má LAN s 5-ti stanicemi.

Integrita dat, hash, autenticita, šifrovací algoritmus a klíč

Internet představuje nesmírně výkonné, ale potenciálně nebezpečné prostředí pro přenos zpráv. Původní protokol TCP/IP neobsahoval žádné bezpečnostní prvky. Prioritou bylo *doručení paketu* jakýmkoliv způsobem k cílovému počítači. Brzy se proto objevila nutnost řešit bezpečnost přenosu dat nad úrovní tohoto protokolu. K čemu by bylo dokonalé zabezpečení počítače, který by hesla do banky předával ve volně čitelných balíčcích IP protokolu? Pakety s daty procházejí přes desítky směrovačů a téměř kdokoliv je může po cestě prohlížet.

Klasický, „obyčejný" přenos dat přes Internet je lehce odposlouchatelný, *nemůžete mít jistotu, že data došla v pořádku, že je nikdo nečetl a jisté není ani to, že skutečně komunikujete s tím, komu jsou data určena*. Proto byly pro komunikaci vyvinuty nejrůznější bezpečnostní prvky, které se soustřeďují na tyto oblasti:

- **Integrita dat.** Zaručuje, že se data během přenosu nezměnila.
- **Důvěrnost dat.** Požaduje, aby data nemohl nikdo cizí přečíst.
- **Autenticita.** Zaručuje identifikaci komunikujících, dává jistotu, že strany, se kterými komunikujete, jsou ty, za které se vydávají.
- **Nepopiratelnost.** Odesilatel nemůže popřít, že uvedenou zprávu (smlouvu, objednávku) poslal.
- **Datování a časování.** Umožňuje určit přesný okamžik vzniku nebo doručení zprávy.

Integrita dat, hash

Integrita dat je jejich zcela zásadní vlastnost, nikdo nechce dostat jiná data, než mu byla odeslána. Na úrovni komunikace zařízení se zajišťuje kontrolními součty a samoopravnými kódy (viz první kapitola). Na úrovni ověření přenosu zpráv se často používá tzv. hash (čtěte heš).

Hash je jakýsi otisk dokumentu, kontrolní součet, který umožňuje *digitální podpis* dokumentu. Speciálním algoritmem (např. MD5) se provede *jednosměrná transformace*, která z obsahu dokumentu vrátí *jednoznačnou hodnotu* (textový řetězec) *pevné délky* (cca 40 až 200 znaků), který je mnohem kratší než původní dokument. Jestliže se v původním dokumentu změní byť jediné písmenko, změní se výrazně generovaný hash. **Hash má tedy tyto vlastnosti:**

- **Vždy stejnou** předem určenou délku.
- Z hashe se nedá nijak **odvodit původní obsah**.
- **Malá změna originálu** způsobí **velké změny hashe**.

Řetězec Hash se zašifruje a pošle se šifrovaný spolu se zprávou. U příjemce zprávy se pak z celé došlé zprávy vypočte opět hash. Zašifrovaný hash se dešifruje a porovná s nově vypočteným. Pokud si oba hash řetězce odpovídají, nebyla zpráva při přenosu změněna. Zpráva tedy nešla přes síť šifrovaná, zašifrovaný byl jen její krátký otisk – hash, máte ale jistotu, že *nebyla změněna*.

Autenticita komunikujících stran

Spameři často využívají podvrženou adresu odesilatele e-mailové zprávy, také phishing využívá podvržené stránky banky apod. Autencitita přístupu k počítači byla probrána na předchozích stránkách, nyní se zaměříme na autenticitu komunikace přes Internet.

Certifikáty počítačů a uživatelů ověřující identitu vůči certifikační autoritě představují základní prostředek ověřování identity. Protože souvisí s metodami šifrování dat, vrátíme se k nim po vysvětlení této problematiky.

Šifrování dat, šifrovací algoritmus a klíč

Bezpečnost šifry závisí na použitém algoritmu a na délce klíče.

- **Algoritmus je předpis,** který šifrovací prostředek (člověk, program, technické zařízení) používá na šifrování dat. Například můžeme zašifrovat text tak, že k ASCII kódu každého znaku připočteme určité číslo a opět ho převedeme na text, vlastně posuneme písmena v abecedě.
- **Klíč** si vytváří uživatel sám, případně je generován pro určitého uživatele. Množství lidí tedy používá pro šifrování *stejný algoritmus, ale různé klíče*. V triviálním příkladu kódování pomocí posunu znaků by klíč tvořilo číslo udávající, o kolik znaků je kód posunut.

Zajímavost

Potřeba bezpečného přenosu informací není nijak nová, již starověké národy používaly různé šifry a kódy. O strategické důležitosti šifrování svědčí i to, že americká vláda určitou dobu nepovolovala vývoz šifer o délce klíče delší než 40 bitů. Tzv. *slabé šifry* se dají prolomit nasazením speciálních systémů, tzv. *silné šifry* by měly odolat jakýmkoliv snahám o dešifrování.

Zajímavost

Nová verze protokolu IPv6 (IPsec) umožňuje jak ověřování autora paketů, tak jejich šifrování, dává tak další silný nástroj ke zvýšení bezpečnosti přenosu dat.

Vyzkoušejte

Co to byla Enigma a jak ovlivnila průběh druhé světové války?

Zajímavost

Referenční integrita (databázových) dat je vysvětlena v praktické učebnici. Zjednodušeně řečeno: údaje v databázi musí být stále kompletní. Není například možné vymazat z *evidence žáků* studenta, který má v *evidenci známek* uvedeny záznamy, protože tyto záznamy by byly svázány s neexistujícím záznamem v evidenci žáků.

Pracujeme

Najděte program na vytváření hash řetězců a vytvořte hash nějakého souboru. Pak v souboru změňte jediné písmeno a vytvořte nový hash. Oba hashe porovnejte a zjistěte splnění zde uvedených vlastností.

Tip

Je zřejmé, že algoritmus musí být hodně složitý a klíč hodně dlouhý, jinak bude prolomení šifry velmi jednoduché.

Důležité

Kryptografie je vědecká disciplína zabývající se šifrováním. Díky počítačům je možné obrovskou rychlostí luštit jednoduché, dříve používané šifry, díky nim je naštěstí také možné vytvářet tak složité šifry, které se běžnými prostředky dnes nedají prolomit.

Zajímavost

Předání klíče je u symetrické šifry zásadní, musí jít vždy přes zabezpečený kanál, tedy osobně, v horším případě telefonicky nebo při komunikaci s úřady písemnou zásilkou (doručenou do vlastních rukou).

Zajímavost

Pokud by tedy případný útočník zachytil veřejný klíč, může příjemci posílat zašifrované zprávy, ale nemůže číst zprávy, které zašifrují jiní odesilatelé.

Zajímavost

V praxi se používá kombinace obou způsobů. Asymetrická kryptografie je totiž pomalá, symetrická rychlá, ale vyžaduje jeden stejný klíč na obou stranách. Asymetrická metoda však umí poslat šifrovanou zprávu, i když se účastníci komunikace nikdy osobně nepotkali. Touto zprávou může být klidně i jednotný klíč pro symetrickou šifru.

Bezpečná komunikace pak probíhá tak, že komunikující strany si s *pomocí asymetrické kryptografie vymění klíče pro symetrické šifrování* a pak již šifrují symetricky. Šifrovací klíč je pro každou komunikaci vždy nově generován.

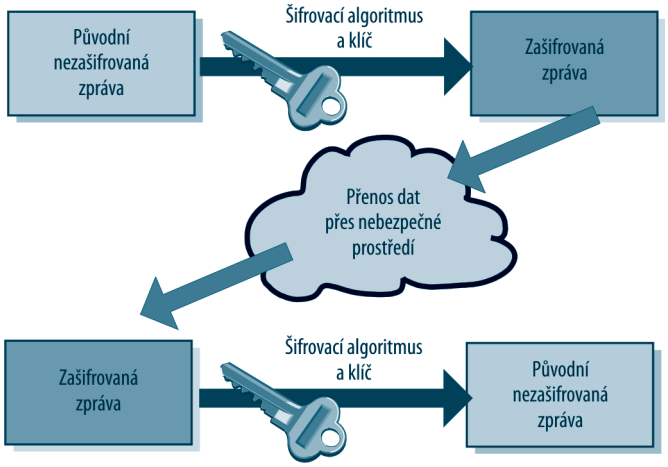
Zajímavost

Používání bezpečnostních kryptografických metod je zcela běžné a u zabezpečeného připojení pomocí protokolu *HTTPS* o něm uživatel většinou ani neví. Využívání *osobních* certifikátů bude brzy také obvyklé, možná se s ním setkáte např. i při přihlašování na vysokou školu.

Více např. na *www.ica.cz* nebo *www.caczechia.cz*.

Symetrická kryptografie a oblasti jejího nasazení

Symetrická kryptografie je v principu velmi jednoduchá. Existuje *algoritmus* a *klíč*, kterými se zpráva zašifruje, a *stejným* algoritmem a klíčem se zase dešifruje. Používá se pro *lokální šifrování*, např. obsahu disku počítače, kdy šifrování i dešifrování probíhá na stejném místě. Dnes používané algoritmy (např. DES) umožňují i silné symetrické šifrování téměř v reálném čase. Pro přenos dat se symetrické šifrování hodí méně, vyžaduje totiž *bezpečné předání stejného klíče* mezi oběma komunikujícími stranami.



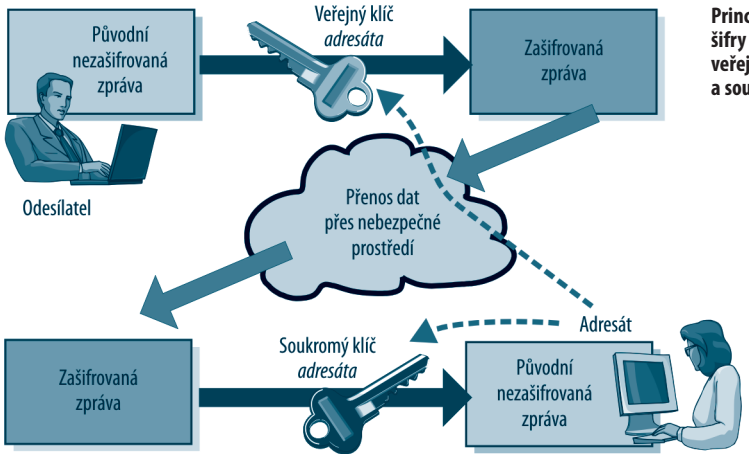
Princip symetrické šifry

Asymetrická kryptografie, privátní a veřejný klíč

Asymetrická kryptografie již tak jednoduchá není, umožňuje však bezpečnou komunikaci *bez* předchozí osobní *výměny* klíče. Používá k tomu *dva klíče*: *veřejný a soukromý*.

Každý uživatel bezpečného spojení vlastní dvojici klíčů: *veřejný* klíč, který zveřejní (pošle lidem, se kterými komunikuje), a *soukromý* (*privátní*) klíč, který pečlivě tají. Tyto klíče jsou šifrovacím algoritmem neoddělitelně svázány, tj. *zprávu zašifrovanou veřejným klíčem je možné dešifrovat pouze k němu náležejícím klíčem soukromým* a naopak (není tedy možné ji dešifrovat veřejným klíčem, kterým byla zašifrována). Nevýhodou této metody je pomalé zpracování dat.

Pokud tedy adresát od odesílatele potřebuje získat bezpečně přenesená šifrovaná data, postupuje takto:



Princip asymetrické šifry s využitím veřejného a soukromého klíče

- Pomocí šifrovacího programu si *vytvoří (vygeneruje) oba klíče*, *veřejný i soukromý*.
- **Soukromý (privátní) klíč** si pečlivě *schová* (např. na USB disk) a přístup k němu chrání silným heslem.
- **Veřejný klíč** naopak *pošle* všem odesílatelům, od kterých předpokládá šifrované dokumenty.
- Odesílatelé mohou posílat veřejným klíčem adresáta zašifrované dokumenty, které on svým privátním klíčem dešifruje.

V případě obousměrné komunikace samozřejmě musí stejný postup absolvovat obě strany.

Bezpečnostní certifikáty, certifikační autorita

Výše uvedená asymetrická šifrovaná komunikace má jedno slabé místo: předání veřejného certifikátu. Budoucí odesilatel si nemůže být zcela jist, zda ho dostal od uvedeného budoucího adresáta, protože jeho předání není ničím autentizováno. Proto vznikl institut *certifikační (registrační) autority*, která vydává tzv. *bezpečnostní certifikáty* a ověřuje je. Důvěra mezi mnoha šifrujícími stranami se potom omezuje na důvěru všech stran v určitou certifikační autoritu.

Certifikát je vlastně soubor s údaji o určité osobě (firmě), který je *elektronicky podepsán pomocí certifikátu registrační autority*. K certifikátu se ještě uloží výše uvedené soukromé a veřejné klíče, doplněné o osobní údaje o osobě, která je vlastní, a o době platnosti certifikátu.

Elektronický podpis

Jak potom funguje zaručený elektronický podpis, použitelný pro úřední komunikaci (a samozřejmě i jakoukoliv jinou, soukromou nebo obchodní)? Ukážeme si to na příkladu komunikace *Adama* a *Evy*, přičemž na místě Adama nebo Evy může být klidně úřad, banka apod. Adam chce Evě poslat elektronicky podepsanou zprávu.

1. Adam musí nejdříve získat svůj elektronický podpis, který obsahuje jeho **osobní certifikát (digitální ID)** a jeho *soukromý i veřejný klíč*. Navštíví proto osobně (nebo zašle úředně ověřené doklady) *certifikační* (*registrační*) *autoritu*, předloží své doklady totožnosti a získá nosič (USB disk, obecně tzv. *token* – nosič certifikátů nebo šifrovacích klíčů), na kterém budou jeho soubory. Ty jsou elektronicky podepsány certifikační autoritou, přístup k osobnímu klíči je chráněn heslem.
2. Adam na svém osobním počítači nejdříve *nainstaluje kořenový certifikát certifikační autority* mezi důvěryhodné cerifikační autority a potom importuje svůj elektronický podpis do e-mailového a webového klienta.
3. Nyní může Adam *podepsat* svým elektronickým podpisem zprávu a poslat ji Evě. *Elektronický podpis zprávy* je pomocí soukromého klíče vytvořený kontrolní součet (otisk, hash) zprávy, dále *Adamův certifikát* a jeho *veřejný klíč*. To vše se předává spolu se zprávou.
4. Eva obdrží podepsanou zprávu (tj. vše výše uvedené). Aby Eva mohla ověřit Adamův certifikát (který je podepsán certifikační autoritou), musí mít *předem na svém počítači instalován jako důvěryhodný kořenový certifikát registrační autority*, která ověřuje Adamův podpis. Ten si většinou stáhne z webu certifikační autority. Oba musí tedy důvěřovat jedné certifikační autoritě.
5. Komunikační program pomocí veřejného klíče vypočte hash a ověří správný obsah zprávy a dále jím ověří, že Adamův certifikát nebyl při přenosu změněn. Adamovu certifikátu věří, protože je ověřen (podepsán) nezávislou certifikační autoritou. *Eva ví nyní jistě, kdo zprávu poslal a že nedošlo k její změně* (samotný podpis neřeší časové razítko a šifrování).

Pokud je vyžadováno určení času (okamžiku) odeslání zprávy, může k ní být připojeno tzv. *časové razítko*, které si vyžádá přesný čas od serveru Internetu poskytujícího tuto službu.

Datová schránka

Datová schránka je pro úřední potřeby zřízená speciální (poštovní) schránka. Její zřízení podléhá podobnému režimu jako elektronický podpis, tedy osoba, úřad nebo organizace musí předložit své zřizovací listiny a *datová schránka je napevno svázána s určitým subjektem*.

Vlastníci datových schránek si do nich mohou *navzájem* posílat zprávy. Systém datových schránek zaručuje autenticitu, integritu i důvěrnost dat, tedy příjemce má jistotu, od koho zpráva přišla, že její obsah nebyl změněn a že ho nikdo jiný nečetl. Speciálním ustanovením je, že obsah datové zprávy je po určité době (nyní 14 dní) *považován za přečtený, i kdyby ho příjemce nečetl*. To zajišťuje *doručitelnost* úředních (soudních) rozhodnutí.

Pracujeme

1. Zkuste najít poskytovatele cvičného kořenového certifikátu a cvičného elektronického podpisu. Pokud ho naleznete, vyzkoušejte si prakticky instalaci certifikátu i podpisu a poté bezpečnou komunikaci.
2. Vytvořte prezentaci shrnující výhody a rizika stávajícího systému datových schránek.

Zajímavost

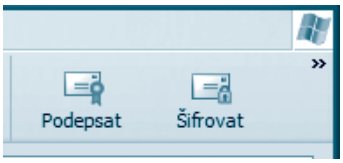
Certifikační autoritou pro úředně (státními orgány) uznávané elektronické podpisy se může stát pouze firma akreditovaná Ministerstvem vnitra ČR, tzv. *registrační autorita*. Za vydání certifikátu a jeho správu se většinou platí. Více na *www.mvrc.cz*.

Vyzkoušejte

Na webu Ministerstva vnitra ČR zjistěte, které české firmy jsou v současnosti akreditovanými poskytovateli certifikačních služeb a kolik stojí vydání a roční poplatek elektronického podpisu.

Zajímavost

V uvedeném postupu je vysvětlen princip elektronického podpisu. Jeho praktická realizace je *pro uživatele* mnohem jednodušší, všechny operace vykonává e-mailový klient. Správce počítače musí správně nainstalovat kořenové certifikáty registrační (certifikační) autority a potom uživatelovi certifikáty. Potom je elektronický podpis zprávy věcí jednoho klepnutí na tlačítko *Podepsat* a zadání přístupového hesla k podpisu.



Zprávu je možné digitálně podepsat, zašifrovat, nebo obojí

Tip

Pro šifrování zpráv si musí zřídit elektronický podpis (a tedy i soukromý a veřejný klíč) obě strany komunikace a předem si své veřejné certifikáty (klíče) předat, tj. poslat si nezašifrované, ale podepsané zprávy. (S první elektronicky podepsanou zprávou od Adama dostane Eva také jeho veřejný klíč. Poté už mu může poslat zašifrovanou zprávu.)