Počítačová bezpečnost

- aktualizace operačního systému a aplikačních programů
- firewall a další bezpečnostní nástroje
- počítačové viry a červy, spyware
- metody útoků přes webové stránky a elektronickou poštu
- antivirový program
- problematika spamu a obrana proti němu
- podvody (tzv. techniky sociálního inženýrství), hoaxy
- zásady vytvoření bezpečného hesla
- zabezpečení počítače a dat před zneužitím cizí osobou
- šifrování souborů
- ochrana dat před ztrátou, zálohování dat

Počítačová bezpečnost je obor informatiky, který se zabývá zabezpečením informací v počítačích (odhalení a zmenšení rizik spojených s používáním počítače). Počítačová bezpečnost zahrnuje tyto úkoly:

- zabezpečení ochrany před neoprávněným manipulováním se zařízeními počítačového systému
- ochranu před neoprávněnou manipulací s daty
- ochranu informací před krádeží (nelegální tvorba kopií dat) nebo poškozením
- bezpečnou komunikaci a přenos dat
- bezpečné uložení dat

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 opatrnost.

Počítačová bezpečnost spočívá ve třech krocích:

- prevence – ochrana před hrozbami
- detekce – odhalení neoprávněných (skrytých, nezamýšlených) činností a slabých míst v systému
- náprava – odstranění slabého místa v systému a aplikačním programu – bezpečnostní chyby (díry)

Aktualizace OS a aplikačních programů

Výrobce OS vydá opravu (záplatu, tzv. patch), která bezpečnostní chybu odstraňuje. Opravu je nutné do našeho systému aplikovat – aktualizovat operační systém. Je možné si povolit automatické aktualizace. Pokud je počítač připojen k Internetu nepřetržitě, stahuje si OS sám potřebné aktualizace a pouze upozorňuje uživatele na jejich instalaci. Totéž platí o většině aplikací, upozorňují na novou verzi programu.

Firewall a další bezpečnostní nástroje

Každý počítač připojený k Internetu má svoji jednoznačnou IP adresu. Jednotlivé služby (web, pošta) pak využívají porty (brány do počítače). Např. web port 80, odchozí pošta port 25, příchozí pošta port 110. Portů je teoreticky 65 535 a přes všechny by se mohl dostat do počítače počítačový červ.

Využívají je také lidé, kteří se snaží o neoprávněný přístup do cizích systémů (hackeři). Program, který hlídá a povoluje komunikaci na jednotlivých portech, se nazývá firewall.
Osobní firewall – většinou součástí OS, kontroluje síťovou komunikaci z/do počítače
Síťový firewall – bývá součástí směrovače (routeru), sleduje komunikaci mezi vnitřní sítí LAN a vnější sítí WAN (Internetem).
Další nástroje bývají součástí kompletních (většinou komerčních) bezpečnostních balíků. Zahrnují kontrolu odkazů na webové stránky, kontrolu obsahu navštívených stránek, zabezpečení osobních údajů (antiviry…).

Počítačové viry a červy, spyware

Počítačový vir nebo červ je program, který někdo vytvořil, aby získal data z cizího počítače, získal kontrolu nad ním. Způsobuje poškození počítače, dat, zpomalení připojení k Internetu. Může být také využít ke sledování zvyklostí, které se týkají procházení Internetu, krádežím hesel.

Druhy škodlivých programů

- virus – počítačový kód, který sám sebe připojí k programu a s ním se šíří. Spuštěním programu uživatel nevědomky spustí i virus
- makrovirus – virus, který není součástí programu, ale dokumentu s makry (vložené programové kódy)
- červ – má vlastní soubor, šíří sám po síti (i Internetu), sám se propaguje, spustí. Využívá chyb v systému, elektronické poště. Nezachytí ho antivir. Nevyžaduje aktivitu uživatele, stačí pasivita (neprovedené aktualizace)
- rootkit – škodlivý kód, běží v jádru OS s právy administrátora počítače. Špatně se detekuje a odstraňuje, protože je součástí jádra OS. Nenajde ho antivir.
- Spyware - po instalaci (bez vědomí samotného uživatele) provádí na pozadí operačního systému nevyžádanou činnost. Touto činností může být odesílání soukromých dat na server útočníka, opakovaná změna domovské stránky prohlížeče. Šíří se nejčastěji s freewarovými programy nebo prohlížením webových stránek.
- Adware - znepříjemňuje práci reklamou. Zobrazuje "vyskakující" pop-up reklamní okna během surfování na internetu, vnucuje stránky, o které nemá uživatel zájem.
  Na odstraňování spywaru a adware jsou zaměřené speciální programy, tzv. antispyware (např. Ad-Aware)

Virus často hned v počítači nepoznáme. Nějakou dobu se šíří, infikuje další soubory v počítači. Po určité době provede v PC nepříjemnou činnost:

- Ovládnutí PC – program typu backdoor otevře některé porty a naslouchá na nich povelům zvenčí. Např. trojský kůň – program, který kromě své zjevné činnosti vykonává ještě jiné neuvedené akce bez souhlasu uživatele
- Odcizení obsahu PC – útočník může kopírovat soubory, sledovat stisknuté klávesy (keylogger), shromažďovat data o činnosti uživatele (dataminder)
- Mazání obsahu PC – není časté. Pro útočníka nemá finanční efekt.

Metody útoků přes webové stránky a elektronickou poštu

- Umísťování zavirovaného souboru do jinak užitečného programu na web. Obvykle na webech s nelegálním obsahem (cracky…). Uživatel stáhne program, spustí a zaviruje PC.

- Umísťování zavirovaného souboru na 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 spustí tento kód, nahraje se do OS škodlivý kód. Využívají bezpečnostních chyb – nutná aktualizace. Prohlížeče mají zabudované ochrany (zakázané skripty, spuštění pouze na dotaz)
- Vytvoření zavirovaného doplňku (plug-in) pro webový prohlížeč. Uživatel nainstaluje zavirovaný plug-in
- Využití podvržené stránky – falešná stránka banky

Elektronická pošta – dnes se šíří mailem málo virů (10 %). E-mailová zpráva s přílohou může obsahovat vir. Většina e-mailových serverů má integrován antivirový program. Zavirované zprávy jsou odstraněny, proto útočníci používají zprávy s odkazem na zavirované weby.

Antivirový program

Antivirový program chrání počítač před viry. Pomáhá zachovat bezpečnost počítače. Je nutné ho pravidelně aktualizovat.

Činnosti antiviru

- běží v paměti počítače a sleduje probíhající činnost. Antivir běží v pozadí. Upozorní, až dojde k podezřelé operaci (např. zápis do systémové oblasti disku, úpravě spustitelných souborů)
- testování - antivirový program má databázi škodlivých programů. Obsah tohoto souboru porovnává s obsahem souborů, které určíme, aby prohledával
- porovnává adresy webů se seznamem nebezpečných stránek

Problematika spamu a obrana proti němu

Spam - nevyžádané hromadně rozesílané zprávy s reklamou.
Šiřitelé spamu získávají adresy

- pomocí specializovaných programů (robotů) prohledávají web
- pomocí virů – odešlou celý adresář e-mailového klienta
- koupí databází adres od jiných spamerů
- generováním náhodné adresy podle seznamů jmen a rozšířených poštovních serverů

Obrana proti spamu

- opatrně zadávat e-mail – používat dvě adresy, jednu pro soukromé účely, druhou pro registrace
- většina spamu v angličtině – u nás rychlejší odhalení spamu než v anglicky mluvících zemích
- e-mailový klient doplnit o antispamový filtr – přesun zpráv do zvláštní složky
- blokovány stránky, ze kterých odchází hodně zpráv, poskytovateli Internetu

Za obsah webových stránek odpovídá autor, ne poskytovatel Internetu.

Podvody, hoaxy

Většina finančních podvodů není provedena dokonalými špionážními programy, ale tak, že útočník požádá majitele o heslo k jeho bankovnímu účtu a on mu jej pošle. Útoky tohoto typu, které využívají psychologii člověka, bávají označovány jako sociotechnické útoky.

Podvodné sociotechnické metody

- nabízejí zdarma tajný materiál (fotografie celebrit, dokumenty o machinacích při soutěži…)
- nabízejí velký finanční zisk při minimálním úsilí (tzv. nigerijské dopisy, které slibují 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
- hlavně: nutí jednat okamžitě, nedávají čas na rozmyšlenou („pokud okamžitě nenainstalujete tuto bezpečnostní záplatu, obsah disku bude smazán…“, „pokud ihned nezrušíte příkaz, odejde z vašeho účtu X peněz…“)

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

Ukradení (zneužití) identity

Typickým příkladem je tzv. phishing. 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 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.

Hoax

Hoax se nazývá šíření poplašných a nebezpečných zpráv a zbytečných řetězcových zpráv. Často nabádá ke smazání „zcela nezjistitelného viru“ nebo k poslání zpráv pro záchranu nemocného člověka apod. Pokud hoax uposlechnete, smažete si sami systémové soubory, nebo zahltíte poštovní schránky jiným uživatelům. Dříve, než na podobné výzvy zareagujete, navštivte databázi hoaxů a ujistěte se, že nerozesíláte zbytečnou poplašnou zprávu.

Komplexní přístup k bezpečnosti IT

Bezpečnost počítače spočívá v technických a organizačních opatřeních

- technická opatření – základem je udržovat operační systém aktuální, zapnutý a správně nastavený firewall, funkční automaticky aktualizovaný antivirový program
- organizační opatření – opatrnost a znalost bezpečnostních hrozeb
- znalosti a opatrnost – to dnes většině uživatelů PC chybí, velké množství počítačů je součástí sítí tzv. botů rozesílajících spam a útočících na jiné systémy (DoS – Denial of Service útoky)

Bezpečnostní zásady, ochrana dat

Zásady vytvoření bezpečného hesla

Bezpečné heslo se označuje jako tzv. silné heslo.
Musí splňovat parametry:

- obsahuje minimálně 8 znaků, s počtem znaků výrazně roste počet možných kombinací a tedy i čas potřebný k útoku, za pár let bude nejspíš minimální počet znaků větší
- nedává smysl v žádném běžném jazyku

- obsahuje co nejvíce různých znaků, velká a malá písmena, číslice a další speciální znaky (? ! / (_ % > apod.)
- dá se dobře zapamatovat, abychom nemuseli nikam zapisovat
- heslo by nemělo obsahovat písmena s diakritikou a většinou ani mezery

Příklad
- silné heslo vytvoříte tak, že si pro sebe řeknete dobře zapamatovatelnou frázi, např. Moje Mladší Sestra Se Jmenuje Veronika
- mezi první (nebo poslední) písmena slov vložte číslice (třeba poslední dvojčíslí roku vašeho narození)
- na začátek (nebo kamkoli jinam) vložte speciální znak
- heslo potom je: !M8m5SsJ?V

Heslo může být odcizeno:
- sociotechnickými prostředky, tj. podvodem zjištěno od uživatele
- využitím neopatrnosti uživatele – heslo je napsané na lístečku nalepeném na monitoru, na spodní straně podložky pod myš…
- pomocí keyloggeru – malware běžící na počítači, který zjišťuje zápisy znaků do políček heslo a odesílá je uživateli
- stejná hesla – uživatelé často používají stejná hesla na důležité i méně důležité operace, např. heslo na e-mail jde přes Internet v případě protokolu POP3 zcela nezašifrováno, útočník toto heslo zjistí a použije jej na účtech uživatele

Zjištění (prolomení) hesla
K informacím chráněným heslem se útočníci pokoušejí dostat i pomocí programovacích prostředků:
- útok hrubou silou (brute force attack) – výkonný počítač zkouší všechny možné kombinace znaků, přičemž začíná omezenou skupinou možností (zvládne miliony hesel za vteřinu). Kombinací je možné vytvořit P^N, kde N je počet znaků hesla a P je počet znaků, ze kterých vybíráme, např. ze 4 číslic (0-9, tj. 10 znaků) je možné vytvořit 10^4 hesel
- slovníkový útok – útočník zjistí jazyk uživatele kterého chce napadnout, použije kompletní slovník daného jazyka a začne zkoušet slovo po slovu, nejlépe podle jejich četnosti používání. Běžné jazyky používají cca 200 000 slov, často používaných je cca 10 000. Slova se zkoušejí i pozpátku nebo se za ně přidávají číslice.

Problematiku ochrany dat rozdělíme na dvě oblasti
- Příklad 1: 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 a možná až zánik firmy.

Rozdíl v ohrožení
- V prvním případě hrozí zneužití dat cizí osobou, tomu se dá zabránit zabezpečením počítače.
- V druhém případě je ohrožení ztráty dat, základní ochranou je zálohování dat.

Zabezpečení počítače a dat před zneužitím cizí osobou

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

- místnost s počítačem ochránit proti vniknutí – tento způsob je snad poněkud primitivní ale velmi účinný a bezpečný
- vázat spuštění počítače na heslo – lze nastavit v BIOSu, špatné heslo se však dá snadno uhodnout nebo „okoukat“, heslo nechrání data při krádeži počítače – po otevření skříně lze heslo vymazat a k datům se dostat
- operační systémy a podnikové informační systémy většinou při spuštění vyžadují jméno uživatele a heslo. Při síti klient-server jsou data fyzicky jen na serveru, ochrana dat na stanicích tedy nemusí být řešena, musí se zabezpečit pouze přístup k serveru
- použití speciálního přídavného zařízení k počítači, do kterého je nutné pro spuštění systému vložit identifikační kartu nebo flash disk (obecně tzv. token – zařízení nesoucí kód), odpadá nutnost pamatovat si heslo. Jde o velmi dobré zabezpečení počítače
- biometrické metody spočívají ve čtení fyzických parametrů uživatele – nejčastěji otisk prstu, často používané u manažerských notebooků

Zabezpečení důvěrnosti dat

V případě, že i přes výše popsaná opatření se k počítači někdo dostane nebo ho odcizí, dá se nějak zabránit zneužití dat? Důvěrnost dat v počítači zajistíme jejich šifrováním.

- softwarová ochrana počítače – existují speciální programy, které se stanou téměř součástí operačního systému a šifrují veškeré zápisy na disk a čtení z disku dešifrují. Oprávněný uživatel se musí prokázat heslem, bez kterého je obsah disku nečitelný. Heslo může být uloženo na externím zařízení a v tom případě může být i velmi dlouhé (např. 128 znaků)
- hardwarová ochrana počítače – bezpečnostní karty do počítače, převezmou funkcí řadiče disku s tím, že opět veškeré přístupy k němu šifrují a dešifrují. Bez znalosti hesla se s diskem nedá pracovat, obsah disku je jen změť nul a jedniček

Ochrana dat před ztrátou, zálohování dat

Porucha počítače, chyba obsluhy, infekce počítačovými vity – všechny tyto události mají společný účinek, a tím je poškození nebo úplné zničení důležitých dat, která jsou uložena na pevném disku. Ochrana – zálohování (archivace) dat – zkopírování dat z pevného disku na nějaké jiné záznamové médium.

Nejčastěji se k tomu používají

- pevný disk počítače – výhodnější než prostá kopie je komprimace (př. do ZIP souboru). Pozor: záloha umístěná na stejném disku jako jsou původní data chrání před vaší chybou (smazáním), ne před zničením dat při fyzické závadě celého disku
- zapisovatelné optické disky CD, DVD, Blue-ray
- USB disky – vhodná pro okamžité zálohování
- Páskové jednotky – servery sítí, kapacita pásky až stovky GB
- Externí pevné disky – záloze disku se říká obraz (image) disku
- On-line úložiště – hlavně placené verze, kdy poskytovatel nese odpovědnost za uložená data

Pravidla zálohování

Zálohy je třeba provádět

- často
- pravidelně
- pečlivě – pomáhají i specializované programy, umí i zálohovat zprávy elektronické pošty, adresář, nastavení systému
- kvalitní záznamová média – značkoví výrobci uvádějí trvanlivost dat (trvanlivost CD a DVD závisí na použitém barvivu

Možné způsoby zničení dat a ochrana proti nim, UPS

- technická porucha pevného disku
- porušení dat na disku výpadkem napájení počítače – pouze v případě, že k výpadku došlo při zápisu na disk

Výpadku napájení 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. Běžně umí napájet cca 15 min, tato doba stačí na normální ukončení všech programů a vypnutí počítače.

Použitý zdroj

ROUBAL, Pavel. *Informatika a výpočetní technika pro střední školy*: Teoretická *učebnice*. 1. vyd. Brno, Computer Press, 2012. 103 s. ISBN 978-80-251-3228-9.