Bezpečnosť na internete

Ochrana počítača

Súčasné aplikácie a operačné systémy obsahujú tisíce až milióny riadkov programového kódu a vytvárajú ich tímy ľudí. Spoliehať sa na to, že programátori nespravili chybu, že mysleli na všetky situácie a že naše aplikácie sú bezpečné, je naivné.
Aj keď sme vlastníkmi najnovšieho operačného systému, ktorý sa chváli prívlastkom bezpečný, nemôžeme sa na to spoliehať. Je len otázkou krátkeho času, kedy sa niekomu podarí nájsť slabé miesto. Toho sú si vedomí aj samotní autori operačných systémov. Snažia sa čo najskôr problém vyriešiť. Riešením sú **bezpečnostné záplaty** (security patch) alebo **bezpečnostné aktualizácie** (security update). Moderné operačné systémy sú navrhnuté tak, že dokážu pravidelne kontrolovať webové stránky svojho výrobcu a automaticky stiahnu najnovšie bezpečnostné aktualizácie. Aj pri inštalácii najnovšieho operačného systému sú už k dispozícii bezpečnostné aktualizácie. Prvý krok po inštalácii operačného systému na počítač je jeho aktualizácia a na stavenie automatickej aktuálizácie v budúcnosti. Pravidelne by sme mali aktualizovať aj ostatné používateľské aktualizácie.
Úloha: Pomocou systémových nástrojov počítača overte, či je váš operačný systém aktualizovaný. Ak nie, aktualizujte ho.

Kontrola sieťovej komunikácie – firewall

Firewall – je špeciálny program, ktorého úlohou je zabezpečiť počítač pred prípadným útokom a zároveň filtrovať sieťovú komunikáciu. Firewall vyhodnocuje, či dáta z internetu sú bezpečné a povolené. Len v tom prípade ich prepustí ďalej. Rovnako pri prenose dát do internetu firewall skontroluje, či daná aplikácia má právo posielať dáta smerom von z počítača. Firewall teda kontroluje, či sieťová prevádzka dodržiava isté, vopred definované pravidlá. Komunikácia, ktorá tieto pravidlá porušuje, je zablokovaná.
Firewall je súčasťou moderných operačných systémov. Napriek tomu existuje množstvo firewallov od iných výrobcov. Nech sa už rozhodneme akokoľvek, hocijaký firewall je lepší ako žiadny alebo vypnutý. Firewall býva aktívny aj na iných sieťových zariadeniach (server, smerovač,...). Podstatná časť útokov je tak odfiltrovaná ešte skôr, ako sa dostane na náš počítač.

Ochrana pred malware

Skupinu všetkých škodlivých alebo nechcených aplikácií označujeme súhrnným pojmom **malware**.
Do tejto skupiny patria najmä:

- **Vírus –** škodlivý (alebo inak nechcený) program, ktorý je schopný vytvárať svoje kópie a zabezpečiť ich aktiváciu
- **Spyware –** programy využívajúce internet na odosielanie dát z počítača bez vedomia používateľa
- **Rootkit** – špecifický typ infekcie. Vyniká schopnosťou schovať sa nielen pred zrakom používateľa, ale aj pred antivírusovým alebo iným bezpečnostným programom. Vyvolá tak falošný pocit bezpečia.

História vírusov
Prvý vírus vznikol v roku 1983 na základe pokusov F. Cohena z Pensylvánskej univerzity, ktorému sa podarilo vytvoriť samorozmnožovací kód. Tento pokus inšpiroval dvojicu Pakistancov, ktorí v roku 1986 vytvorili prvý skutočný vírus, ktorý sa šíril naozaj masovo. Do roka bolo na svete 20 vírusov, v súčasnosti ich existuje niekoľko desiatok tisíc. V roku 1988 vznikla prvá antivírusová ochrana McAfee, ktorá vydala prvý antivírusový program – VirusScan. V tom istom roku bol odsúdený aj prvý človek za výrobu a rozširovanie vírusu. Roku 1995 znamenal ďalší zásadný zlom – vírusy si za hlavnú oblasť pôsobenia vybrali operačné systémy od Microsoftu, pre ktoré je mohutná väčšina vírusov písaná i v súčasnosti.
Rozdelenie vírusov
Vzhľadom na to, že počítačový vírus silne pripomína vírus biologický, je terminológia preň veľmi podobná:

- proces šírenia vírusu – nákaza alebo **infekcia**
- napadnutý súbor sa označuje ako hostiteľ a jeho stav – **infikovaný**
- uchovanie napadnutého súboru bez odstránenia vírusu – **karanténa**
- odstraňovanie vírusu – **liečenie** a po úspešnom odstránení je súbor **vyliečený**

Vírusy možno rozdeliť podľa viacerých kritérií. Prvým kritériom môže byť **miesto, kam sa ukladajú** a využívajú ho na svoje šírenie:

- **Spustiteľné vírusy** – vírus sa obyčajne pripojí za program a na jeho začiatok vloží inštrukcii, ktorá zabezpečí, že ako prvý sa spustí vírus a až potom samotný program, prípadne prepíše začiatok súboru, čím ho znehodnotí, no počas niekoľkých pokusov o spustenie stihne nainfikovať ďalšie súbory
- **Systémové oblasti** – vírus sa umiestni do pevného disku a zabezpečí si tak spustenie ešte pred zavedením operačného systému
- **Dokumenty, ktoré obsahujú makrá** – vírus využíva samospustiteľné makrá a vloží do nich svoj kód

Podľa spôsobu **umiestnenia v pamäti** delíme vírusy na:

- **Nerezidentné –** spúšťajú sa pomocou spustiteľného programu, porozhliadajú sa po ďalších spustiteľných súboroch, nakazia ich a skončia
- **Rezidentné –** po spustení napadnutého súboru sa natrvalo usadia v pamäti a sledujú používateľa. Môžu napádať len spúšťané súbory alebo prehľadávajú disk a nenápadne sa čo najviac šíria.

Podľa spôsobu **deštruktívnosti**:

- **Nedeštruktívne vírusy** obmedzujú svoju činnosť na vizuálne a akustické prejavy (zobrazovanie textových správ, padanie písmen z obrazovky, nahrádzanie znakov znakmi, ktoré sú na klávesnici umiestnené v ich susedstve...)
- **Vírusy napádajúce programy** – prepíšu program, je pravda, že takto postihnutý súbor buď nespustíme, alebo je zdrojom nákazy pre ďalšie spustiteľné súbory, no väčšinou stačí súbor vymazať a napadnutý program nanovo nainštalovať
- **Vírusy ničiace dáta** – môžu vymazať časť disku, alebo vymazať všetky súbory
- **Vírusy modifikujúce údaje** – zvyčajne „sedia“ v počítači a občas, kde – tu, zmenia údaj. Pri niektorých nie je možné zistiť, ktoré súbory boli napadnuté a ktoré údaje sa modifikovali – nemôžeme si byť istí ani tým, či zálohy sú správne alebo údaje v nich boli tiež modifikované
- **Vírusy odosielajúce z počítača údaje** – buď prostredníctvom e-mailov na adresy z adresára používateľa, alebo prostredníctvom siete na lokality definované tvorcom vírusu

Okrem vírusov existuje aj niekoľko ďalších typov programov, ktorých primárnym cieľom je škodenie používateľom. Od vírusov sa najčastejšie odlišujú tým, že pre svoju existenciu a množenie nepotrebujú hostiteľa. Do tejto kategórie patria:

- **Trójske kone** – po infikovaní sa nemusia ďalej šíriť, ale len pozorujú systém a čakajú na svoju chvíľku. Cieľom ich činnosti môže byť ohrozenie počítača v určitom momente, sledovanie činnosti používateľa a odosielanie údajov, alebo zabezpečenie prístupu neoprávnenému používateľovi
- **Počítačové červy** – za svoju existenciu vďačia počítačovým sieťam:
  - **Sieťový červ** – sa v počítačovej sieti šíri vďaka chybám v serverových častiach programov, pričom sám aktívne vyhľadáva ďalšie počítače vhodné na napadnutie
  - **E-mailový červ** – sa šíri prostredníctvom e-mailov – po otvorení prílohy sa červ aktivuje a rozošle všetkým používateľom z adresára

Antivírusové programy

napriek svojmu názvu, často integrujú nielen ochranu pred vírusmi. Ich súčasťou býva aj ochrana pred spyware a roottkitmi, Výrobcovia antivírusových softvérov čoraz častejšie ponúkajú komplexné bezpečnostné balíky. Tie okrem uvedeného zahŕňajú aj ďalšie služby (firewall, filtrovanie nevyžiadanej pošty). Najstaršou funkciou antivírusových programov je **skenovanie** spočívajúce v porovnávaní obsahu pamäte, programov a ostatných objektov na pamäťových médiách so vzorkami vírusov, ktoré má program uložené v databáze. Pokiaľ sa v kontrolovanom súbore nachádza časť, ktorá sa zhoduje s niektorou zo vzoriek, je tento označený za nakazený. Systém týmto spôsobom dokáže odhaliť len známe vírusy, preto sa datbázy v súčasnosti aktualizujú veľmi často – niekedy i viac ráz v priebehu dňa, štandartne prostredníctvom Internetu.
Medzi štandardné funkcie patrí i **heuristická analýza**, ktorá na základe analýzy neznámeho kódu dokáže s určitou pravdepodobnosťou povedať, či daná aktivita je typická pre vírusy. Silným

nástrojom odhaľujúcim vírusy je **porovnávací test**, ktorý sa realizuje na základe sledovania obsahu pevného disku. Antivírusový systém si v prvom kroku vytvorí databázu, ktorá obsahuje zoznam súborov na disku, ich veľkosť, dátum poslednej zmeny. Pri každom ďalšom spustení porovnáva uložené informácie s aktuálnymi. Pokiaľ došlo k rozsiahlejším zmenám, je pravdepodobné, že počítač bol napadnutý vírusom. Zaujímavou technikou je **pasca na súborové vírusy**, pri ktorej antivírusový program vygeneruje a na disk uloží spustiteľné súbory. Tieto potom kopíruje, spúšťa a vykonáva s nimi ďalšie operácie, pričom sleduje činnosť systému i obsah používaných súborov. V prípade neočakávaných zmien je pravdepodobné, že vírus sa chytil na návnadu.
Každý mesiac sa objavuje niekoľko desiatok až stoviek nových typov malware. Preto je dôležité mať aktualizovaný a dobre nastavený antivírusový systém.
Medzi najpopulárnejšie antivírusové programy v SR patria NOD, AVG

Nevyžiadaná pošta SAPM

SPAM – nevyžiadaná správa, často s komerčným obsahom – výhodná ponuka nejakého produktu (najčastejšie sú to lieky alebo softvér). Spam môže obsahovať aj vymyslenú, poplašnú správu, napr. varovanie pred neexistujúcim rizikom a žiadosť o rozposlanie tohto varovania čo najväčšiemu počtu ľudí – takýto druh správ označujeme pojmom **HOAX** – poplašná správa.
Podvodné e-maily informujúce o výhre v lotérii alebo možnosti získať veľké množstvo financií sa označujú **SCAM**. Často žiadajú zaslanie osobných údajov alebo uhradenie poplatkov súvisiacich s prevodom peňazí.
Správy budiace dojem, že ich autorom je naša banka a zvyčajne informujúce o nejakom probléme s naším účtom, sa označujú ako **PHISHING**. Často žiadajú, aby sme vyplnili formulár, alebo sa prihlásili do služby internet banking, prostredníctvom podstrčenej webovej stránky. Táto stránka je veľmi podobná oficiálnej stránky banky.
Správy nabádajúce k tomu, aby sme ich kópiu poslali našim najlepším priateľom, pretože v opačnom prípade nás môže postihnúť nejaká nepríjemnosť, sa nazývajú **reťazový e-mail**. Ich prílohou môže byť prezentácia obsahujúca milé obrázky a myšlienky pre priateľov.

Ochrana osobných údajov

- nezverejňujme svoje osobné údaje, ani keď nás o to na internete požiadajú
- neposkytujme žiadne informácie o svojich blízkych a známych
- vždy sa uistíme, že vieme, komu poskytujeme informácie, načo a ako ich použije
- ak registrácia na používanie nejakej služby vyžaduje zadanie osobných údajov, poraďme sa najskôr so svojimi rodičmi alebo učiteľmi
- ak použitie nejakej služby vyžaduje našu e-mailovú adresu, vytvorme si na tento účel nový e-mailový účet
- z prihlasovacieho mena alebo prezývky, ktorú používame vo verejných diskusiách, by sa nemali dať určiť naše pohlavie, adresa, veka a pod.

Medzi údaje, ktoré by sme nemali zverejňovať, patria: meno, adresa, telefónne číslo, vek, pohlavie, rodné číslo, čísla účtov a platobných kariet, heslá, fotografie z dovolenky, fotografie v plavkách, s kým a kde žijeme, vybavenie našej domácnosti

Bezpečné správanie v sieti internet

Okrem toho by sme mali dodržiavať aj ďalšie pravidlá:
- na podozrivú alebo nevyžiadanú e-mailovú správu nikdy nereagujme, neotvárajme prílohu v nej, neklikajme na žiadne odkazy v tejto správe, neposielajme ju ďalej
- ak partnera v diskusii poznáme len z internetu, nemôžeme si byť istí, s kým v skutočnosti diskutujeme, preto:
  - ak je komunikácia pre nás nepríjemná, ukončime ju
  - ak nás partner požiada, aby sme zapli webovú kameru alebo sa odfotili, takisto ukončíme diskusiu
  - zvýšme opatrnosť, ak náš partner na internete nechce, aby sme o našom vzťahu informovali niekoho ďalšieho, v žiadnom prípade si sním nedohodnime schôdzku
  - zvýšme opatrnosť, ak sa nám zdá, že náš partner má veľa rovnakých záľub a názorov ako my

- buďme opatrní pri zverejňovaní informácii – každá zverejnená informácia je verejná a je prakticky nemožné ju z internetu odstrániť
- nenechajme sa zatiahnuť do urážlivých diskusií
- buďme opatrní pri sťahovaní dát z internetu
- voľme bezpečné heslá
- správajme sa zodpovedne – o svojich internetových kontaktoch hovorme so svojimi rodičmi, priateľmi, učiteľmi

Domáca úloha – písomne vypracovať

a) Elektronickou poštou dostanete mail s prílohou od neznámeho odosielateľa. Aké riziko je spojené s otvorením tohto mailu? Čo je počítačový vírus a aké druhy vírusov poznáte? Ako môžeme chrániť počítač pred vírusmi? (IS – informačná spoločnosť)

a) Pri surfovaní po Internete ste narazili na zaujímavú stránku ponúkajúcu Vám množstvo zaujímavých obrázkov a hier, ktoré si môžete stiahnuť po zaregistrovaní. Aké sú riziká spojené so zverejnením svojich osobných údajov? So zverejnením svojej emailovej adresy? Aké druhy počítačovej kriminality poznáte? (IS – informačná spoločnosť)

b) Ako nastavíte, aby každý odoslaný e-mail mal rovnaký podpis? Čo je to elektronický podpis (súkromný a verejný kľúč)? (IS – informačná spoločnosť)

c) Definujte pojem počítačovej kriminality a popíšte jej formy. Prečo je „domáce napaľovanie“ napr. hier distribuovaných na CD/DVD trestné? Kto je tým poškodený? (IS – informačná spoločnosť)

d) Pri surfovaní po Internete ste narazili na zaujímavú stránku ponúkajúcu Vám množstvo zaujímavých obrázkov a hier, ktoré si môžete stiahnuť po zaregistrovaní. Aké sú riziká spojené so zverejnením svojich osobných údajov? (IS – informačná spoločnosť)

e) Vysvetlite pojmy počítačový vírus, trójsky kôň, počítačový červ a popíšte ich činnosť. Popíšte ako môžeme chrániť počítač pred rôznym škodlivým softvérom, ako aj princíp práce a použitie antivírusových programov. (IS – informačná spoločnosť)

f) Zistite, aký antivírový program je nainštalovaný na počítači, ktorý používate, či je činný a či je aktuálny. Prezentujte pomocou tohto softvéru ako sa chránite proti vírusom. Vysvetlite čo je vírus a ako sa môžete pred ním chrániť a aké metódy detekcie používajú antivírusové programy. (IS – informačná spoločnosť)

g) Predpokladajte, že ste autorom reťazovej správy. Poslali ste ju šiestim priateľom s prosbou, aby ju poslali ďalším šiestim priateľom. Koľko ľudí dostane danú správu v deviatej vlne? Popíšte riziká e-mailových správ (spamy, hoax) (IS – informačná spoločnosť)