Fișa informațională nr.16

Securitatea

Introducere

- Securitatea dvs. online poate fi comparată cu securitatea la domiciliu. Protecţia este asigurată prin închiderea şi zăvorârea ferestrelor şi a uşilor.
- Malware (http://en.wikipedia.org/wiki/Malware) este un termen generic pentru programele contagioase, de exemplu, viruşii (http://en.wikipedia.org/wiki/Computer_virus), care pot infecta un computer. Malware-urile pot avea mai multe efecte, cum ar fi afectarea programelor din computerul dvs., accesul neautorizat la datele dvs. sau suprimarea datelor.
- Cele mai comune forme de malware sunt viruşii (http://en.wikipedia.org/wiki/Computer_virus) şi viermii (http://en.wikipedia.org/wiki/Computer_worm), programe ce se autoreplică.
- În pofida numelui, nu toţi viruşii şi alte forme de malware sunt create cu rea intenţie.
- În medie, zilnic sunt identificaţi 10 viruşi noi.
- Mulţi factori relevanţi pentru securitate pot fi aplicaţi şi pentru protejarea vieţii private (vedeţi Fişa informaţională nr.15).

Aplicații pedagogice

- Discutaţi cu studenţii problemele de autoprotecţie şi responsabilitate. Deoarece mulţi tineri sunt mai bine informaţi decât adulţii, încurajaţi-i să împărtăşească cunoştinţele şi propria experienţă colegilor şi familiilor lor.
- Mulţi hackeri şi creatori de viruşi sunt foarte tineri. Dezbateţi acest subiect în cadrul orelor.

Probleme etice şi de securitate

- Insecuritatea computerului dvs. se poate răsfrânge asupra altor computere. Viruşii care afectează computerul dvs. pot fi transmişi altor ordinatoare.
- Oricine depozitează date personale ale clienţilor este responsabil de protejarea acestora.

- Pirateria (hacking) (http://en.wikipedia.org/wiki/Hack_%28technology_slang%29) sau alt acces neautorizat la informaţia ce vizează alte persoane constituie o violare a dreptului la viaţa privată.
- E important să fiţi precaut, dar nu exageraţi în ceea ce priveşte măsurile de securitate! Una din calităţile minunate ale Internetului este accesibilitatea acestuia. Restrângerea drepturilor sau filtrajul excesiv pot fi calificate drept cenzură şi reduc accesul la Internet.
- Programele de spionaj (spyware) reprezintă software-uri infiltrate în computere, de obicei în scopuri comerciale. Acestea pot încerca să difuzeze informaţie publicitară sau să sustragă informaţiile bancare. Un dialer este o formă de spyware, prin care modemele culeg numerele fără consimţământul utilizatorului. În general, e vorba de numere de telefon premium.
- Cookie-urile presupun depozitarea informaţiei personale. Pentru mai multă informaţie, citiţi Fişa informaţională nr.15 despre viaţa privată.

Sugestii practice

- Instalaţi programe antivirus (http://en.wikipedia.org/wiki/Anti-virus_software) şi actualizaţi-le în permanenţă.
- Instalaţi fără întârziere corective de securitate. Unele sisteme operaţionale şi programe se actualizează automat sau vă informează imediat ce un corectiv este disponibil pentru preluare (activare).
- Instalaţi un program de protecţie „parafoc" (firewall) (http://en.wikipedia.org/wiki/Firewall_%28networking%29) pentru a controla traficul informaţional.
- Nu lăsaţi ordinatorul dvs. conectat la Internet, dacă nu e necesar. Abonamentele la debit înalt permit conexiuni nelimitate, dar pot compromite securitatea datelor dvs.
- Evitaţi să folosiţi parole (http://en.wikipedia.org/wiki/Password#Factors_ in_the_security_of_an_individual_password) asociate evident cu dvs. Folosiţi o combinaţie din litere şi cifre.
- Dezactivaţi script-urile în browserul dvs. (http://en.wikipedia.org/wiki/Web_browser). Activaţi script-urile doar în cazurile site-urilor în care aveţi încredere.
- Nu deschideţi mesajele electronice care vă par dubioase (vedeţi Fişa informaţională nr.5 despre e-mail).
- Verificaţi credibilitatea sursei înainte de a activa un fişier în computerul dvs. Trebuie să fiţi conştient că programele P2P (http://en.wikipedia.org/wiki/Peer_to_peer) au reputaţia de a fi distribuitoare de programe de spionaj (spyware) (citiţi Fişa informaţională 10 despre muzică şi imagini).

- Copiaţi cu regularitate fişierele importante pe un suport extern, CD-romuri, de exemplu.
- Dacă gestionaţi mai mulţi utilizatori sau o reţea, nu uitaţi că fiecare utilizator are anumite drepturi. Restrângerea drepturilor ce nu sunt absolut necesare vă poate ajuta să evitaţi probleme de securitate accidentale sau intenţionate.
- Administratorii de reţea trebuie să creeze o politică acceptabilă de utilizare (PAU) (http://en.wikipedia.org/wiki/AUP) pentru ca beneficiarii să nu pună în pericol securitatea sistemului.
- Cele mai comune ţinte ale malware-ului sunt sistemul operaţional Windows şi browserul Internet Explorer. Luaţi în calcul şi programele numite "surse deschise" (http://en.wikipedia.org/wiki/Open_source) sau Mozilla Firefox: <http://www.mozilla. org/>.

Informații complementare

- http://www.microsoft.com/security/default.mspx: pagina de securitate a Microsoft-ului.
- http://www.apple.com/support/security: pagina de securitate a Apple.
- http://www.searchsecurity.com: informaţii detaliate pentru profesioniştii din domeniul tehnologiilor informaţionale.
- http://www.enisa.eu.int/: Agenţia europeană pentru securitatea reţelelor şi a informaţiei.
- http://www.oecd.org/document/42/0,2340,en_2649_34255_15582250_1_1_1_1,00.html: directivele OCDE pentru securizarea sistemelor informaţionale şi a reţelelor.
- http://informationsecurity.techtarget.com/: revista de securitate informaţională.
- http://www.2privacy.com/: pagina web 2privacy.com poate evalua online dacă ordinatorul dvs. a fost obiectul intruziunilor externe.
- Sfaturi acordate de guvernul Marii Britanii <http://www. itsafe.gov.uk/> şi cel al Statelor Unite http://www.uscert.gov/ în materie de securitate online.
- http://www.the-dma.org/guidelines/informationsecurity. shtml: directive privind securitatea informaţiei în cazul comerţului online.