GAMA Electronics bitsyu.net INTERNET PROVIDER
Mišarska 11, 10000 Beograd tel: +381 11 323 94 94 fax: +381 11 322 72 81 email: prodaja@bitsyu.net http://www.bitsyu.net
Matični broj: 7489706 Šifra delatnosti: 64200 PIB: 100290617 PDV: 128976171
Računi: 160-92368-04 Banca Intesa, 180-0150660101000-90 Alpha Bank AD

Sigurnost na Internetu

Potrebno je znati da potpuna sigurnost na Internetu ne postoji, ali možete preduzeti niz osnovni radnji i pravila kako bi potencijalnu opasnost sveli na najmanju moguću meru.

S obzirom da većina korisnika na svom kompjuteru ima instaliran neki od Windows operativnih sistema, poseban osvrt ćemo napraviti na zaštitu istih.

Neka opšta pravila za prevenciju i zaštitu Vaseg kompjutera bila bi:

1. Obavezno instalirajte antivirusni program na svoj kompjuter.
Prvo i osnovno što treba da uradite jeste da instalirate pouzdan antivirusni program. Ovaj program treba da zaštiti kompjuter od zlonamernih programa (virus, trojanac, spyware itd) koji se instaliraju bez Vašeg znanja.
Virusi se lako prenose putem email poruka, kao i razmenom programa sa drugim osobama. Ovi programi mogu obrisati ili izmeniti bitne podatke na kompjuteru ali i izbrisati kompletan sadržaj hard diska. Kada instalirate antivirusni program potrebno je i da redovno ažurirate njegove baze sa opisima virusa. U suprotnom, kao i da nemate instaliran antivirusni program na kompjuteru.
Napomena: Svi nasi ADSL korisnici (privatna lica) imaju mogućnost da besplatno koriste Kaspersky AV Personal.

2. Posebnu pažnju obratite na email poruke ukoliko ne znate pošiljaoca. Ovo pravilo pogotovo važi ukoliko postoji i prilog (email-attachments). Svaki prilog u okviru email-a proverite (skenirajte) ažuriranom verzijom anti virusnog programa.

3. Instalirajte dobar firewall program na svoj kompjuter ukoliko ne posedujete hardverski firewall ili makar koristite firewall u okviru operativnog sistema.
Ovi programi su aktivni dok je kompjuter na Internetu, prate vrstu i protok podataka kroz kompjuter i u slučaju da otkriju neovlašćen pristup kompjuteru, zaustavljaju taj pokušaj i obavestavaju vas o tome.

4. Koristite Windows Update kako bi bili sigurni da su u okviru operativnog sistema instalirane poslednje sigurnosne "zakrpe" (patch).

5. Komponente Microsoft Networks i File and Printer Sharing (Control Panel - Networks) mogu omogućiti zloupotrebu podataka sa Vašeg kompjutera.
Ukoliko nemate potrebu za deljenjem fajlova u mreži, obrišite komponente Microsoft Networks i File and Printer Sharing. Korisnici koji žele da omoguće deljenje fajlova u svojoj mreži moraju da budu vrlo oprezni , pogotovo ukoliko se konektuju na Internet.

Rad sa lozinkama / šiframa
Preporučujemo da lozinke / šifre (za logovanje na sistem, za email, itd) menjate relativno šesto, na svakih nekoliko nedelja.

Primeri:

Loš primer	Dobar primer
pera	peRa14*
dunja1	xd-01cf4
miticp	goOd_One

Naravno, ove lozinke / šifre više nisu dobri primeri, zato sto su publikovane.

Neki od postupaka za uklanjanje zlonamernih programa

Autori zlonamernih programa stalno usavršavaju metode i načine širenja istih, tako da dole navedeni postupci obuhvataju samo neke od trenutno poznatih načina za uklanjanje zlonamernih programa.
Ukoliko i pored svih mera opreza dođe do instaliranja zlonamernih programa na Vašem kompjuteru, predlažemo da na svim kompjuterima u mreži uradite sledeće:
Proverite kompjuter sa antivirusnim programom koji koristite (hard disk "c:" kao i ostale diskove u kompjuteru).
Dodatnu proveru možete izvršiti preko online verzija antivirusnih programa:
http://www.kaspersky.com/kos/eng/partner/default/pages/default/check.html?n=1256923421050
i
http://security.symantec.com/sscv6/WelcomePage.asp

Sledeća provera sa odnosi na adware/trojan detektore:
a)Spybot-S&D
http://www.safer-networking.org/en/mirrors/index.html
(pre provere uraditi ažuriranje programa)
b) Malwarebytes
http://www.malwarebytes.org/, besplatna verzija i ažuriranje.
c) ComboFix
http://download.bleepingcomputer.com/sUBs/ComboFix.exe
http://www.bleepingcomputer.com/combofix/how-to-use-combofix - uputstvo

Zatim sortirati fajlove po datumu c:\windows, c:\windows\system32 i c:\windows\system32\drivers i videti ima li "dll" ili "exe" fajlova novijeg datuma i/ili čudnog imena, na www.google.com proveriti da li jos neko ima isti fajl / program i ima li komentara o trojancu ili virusu; uraditi upload preko linka http://virscan.org/ i testirati sumnjive fajlove.

Obavezno promeniti sve lozinke / šifre na online servisima koji koristite.

Povremeno proveriti preko start - run - cmd:
u konzoli kucati: netstat -o

Ova komanda daje ispis sličan navedenom primeru:

Active Connections

Proto	Local Address	Foreign Address	State	PID
TCP	127.0.0.1:1890	127.0.0.1:1891	ESTABLISHED	3160
TCP	127.0.0.1:1891	127.0.0.1:1890	ESTABLISHED	3160

....
....

Ako u koloni "Foreign Address" postoji ":25" (ili ":smtp") znači da kompjuter šalje email poruke bez Vašeg znanja.

Poslednja kolona "PID" pokazuje koji proces (program) to radi.

Komanda "tasklist /svc" daje listu procesa, tako da može da se vidi koji je "pid" odnosno program inficiran.

Ako je "pid" 0 ili 4, virus je u boot sektoru i može da se očisti samo ako se sistem podigne preko instalacionog CD-a i ručno očisti; obično se nalazi u c:\windows\system32\drivers\nestocudno.sys

Proveriti WLAN okruzenje ako postoji, mozda imate uljeza u Wireless okruzanju sa inficiranim racunarom.