

**ESET**

# Preventiva je najboljša zaščita

„PRI DELU Z RAČUNALNIKOM, IN ŠE POSEBNO, KO BRSKAMO PO SPLETU, SE MORAMO ZAVEDATI, DA NOBENA PROTIVIRUSNA ZAŠČITA NE MORE ZAGOTOVITI STOODSTOTNE VARNOSTI PRED VDORI IN NAPADI. TO MOŽNOST PA MOČNO ZMANJŠAMO, ČE SPROTI IZVAJAMO PREVENTIVNE UKREPE.“

Podatek, ki pravi, da povprečen uporabnik letno porabi več denarja za varnost in zaščito strojne in programske opreme, kot pa za samo opremo, vsekakor ni zanemarljiv. Vedno znova se pojavljajo nove grožnje, sorazmerno z njimi pa tudi nove rešitve za zaščito. Poleg same zaščite, pa obstaja kar nekaj načinov, s katerimi lahko tudi sami vplivamo na varnost svojih podatkov.

## REDNE POSODOBITVE

Podatki, ki jih ESET pridobi s pomočjo ThreatSense.Net tehnologije kažejo, da se vsak dan pojavi na tisoče novih škodljivih programov, ki poskušajo izkoristiti varnostne luknje. Raziskovalci v ESET-ovem virusnem laboratoriju te grožnje analizirajo vsak dan in skladno z njimi

### Nekaj uporabnih nasvetov:

- Ne obiskujte spletnih strani z veliko pojavnimi okni in vpadljivimi reklamami.
- Bodite previdni pri prenosu in nameščanju brezplačnih programov.
- Bodite previdni pri odpiranju priponk v e-pošti.
- Ne uporabljajte administratorskih računov za običajno delo z računalnikom.
- Bodite previdni pri uporabi Peer-to-Peer programov (BitTorrent ipd.).

pripravljajo nove posodobitve virusnih definicij. Na ta način so uporabniki zaščiteni pred najnovejšimi grožnjami.

Nepravilno nastavljeno posodabljanje močno zmanjša učinkovitost protivirusnega programa. Nasvete glede posodabljanja ter ostalih nastavitvev si lahko ogledate na naslovu <http://podpora.sisplet.com>

## VARNOSTNI POPRAVKI

Pisci škodljivih programov za širjenje svoje škodljive kode zelo radi izkoriščajo varnostne luknje v operacijskih sistemih. Zato podjetja, ki ponujajo operacijske sisteme, neprestano pripravljajo varnostne popravke, ki te luknje zapirajo. Zelo priporočljivo je, da te popravke naložite čimprej po izidu. Primeri takih programov sta operacijski sistem Windows in spletni brskalnik Internet Explorer.

## VARNOSTNE KOPIJE

Avtorjem škodljivih programov ni mar za vaše podatke, saj njihova koda velikokrat povsem onemogoči operacijski sistem ali poškoduje pomembne podatke. Priporočljivo je, da pomembne in občutljive podatke kopiramo na zunanje nosilce, recimo DVD medije ali zunanji trdi disk. Varnostne kopije so v primeru okvare operacijskega sistema neprecenljive in nam močno olajšajo delo.

eSet Top 10		www.eset.si
Deset najbolj razširjenih groženj v zadnjem tednu		
	število okuženih e-sporočil	
Win32/Netsky.Q worm	27829	
Win32/Zafi.B worm	16302	
različica Win32/Injector.BZ trojan	3550	
Win32/Bagle.HE worm	1746	
Win32/Netsky.AB worm	1389	
Win32/Mydoom.R worm	588	
Win32/Netsky.Z worm	452	
Win32/AutoRun.TT worm	447	
Win32/Agent.OWX trojan	273	
Win32/Agent.OXM trojan	271	

## REDNO PREISKOVANJE

Zelo priporočljivo je, da svoj računalnik redno pregledamo z antivirusnim programom vsakih štirinajst dni. Vedno namreč obstaja možnost, da se na našem trdem disku nahaja okužena datoteka, ki je protivirusni program s starimi definicijami ni prepoznal. ESET NOD32 in ESET Smart Security v nastavitvah ponujata možnost, da se takšno preiskovanje izvede samodejno, v poljubnih intervalih.

## UPOŠTEVAJTE OSNOVNA VARNOSTNA NAVODILA

Najbolj uporaben in učinkovit nasvet je: »Bodite previdni!« Veliko škodljivih programov od uporabnika zahteva interakcijo, zato bo previdnost pri odpiranju novih datotek prihranila ogromno časa in truda z brisanjem okužb. (P.R.)

## Odločite se za kvalitetne rešitve, tako doma kot na poslovnem mestu

### Varnostne rešitve:

- Antivirus: ESET NOD32 in Smart Security
- Antispam: Cloudmark Desktop
- Antispyware: Webroot Spy Sweeper

### Sistemske rešitve:

- Spletno gostovanje
- Servisne storitve
- Informacijska varnost



Uporabljate zaščito?