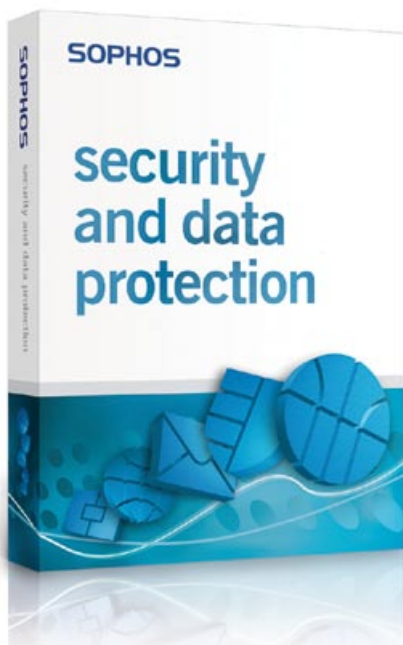




# SOPHOS Security & Data Protection

## Virusi v poslovnem okolju

„TUDI V ZADNJEM LETU JE PRISOTEN TREND NARAŠČANJA ŠKODLJIVE KODE (VIRUSI, SPYWARE, SPAM ...), NA PRVEM MESTU DISTRIBUCIJE LE-TE PA OSTAJA INTERNETNO OMREŽJE..“



Naraščanje „proizvodnje“ škodljive kode narekuje vedno večje zahteve glede učinkovitosti zaščite na vseh nivojih poslovnega omrežja. Poleg obveznega osveščanja/izobraževanja uporabnikov o tej problematiki je glavno orožje učinkovita zaščita poslovnega omrežja. Ena izmed takih rešitev je **Sophos Security & Data protection**. Vsebuje posamezne module za vse nivoje zaščite, od končnega uporabnika, strežnikov, elektronske pošte in interneta, do varovanja podatkov s

pomočjo kriptiranja in nadzora nad uporabo brezžičnih naprav ter zunanjih naprav za shranjevanje podatkov. Poleg **antivirus**, **antispyware in adware** zaščite, so na vojo še: **application control**, ki upravlja aplikacije s področja VoIP, Instant Messaging, P2P, iger, oddaljenega dostopa itd., katerih bazo posodablja SophosLabs. Naslednja pomembna funkcionalnost je **HIPS (host intrusion prevention system)**, ki preprečuje izvajanje sumljivih procesov in aplikacij ter ščiti pred buffer overflow napadi. Na ta način je sistem zaščiten tudi brez novih virusnih definicij. Novost pri varovanju pred novimi grožnjami je tudi **Sophos Live Protection** in-the-cloud tehnologija, s pomočjo katere se posamezna zaznavanja sumljivega obnašanja aplikacij takoj preverijo v Sophosovi bazi ter na ta način zagotavlja analizo v realnem času, saj se po potrebi lahko vzorec zaznane datoteke prenese v SophosLabs, ki lahko nemudoma izdela potrebno posodobitveno definicijo. Kot pomemben del zaščite je na voljo **device control** za podrobnejši nadzor nad uporabo zunanjih diskov, USB ključev, CD/DVD pogonov itd., pri katerem je možno avtorizirati uporabo točno določenih naprav ali samo kriptiranih medijev ali pa je omogočen sa-



mo dostop za branje podatkov. Kot zadnja novost je dodan še **data control**, s katerim je omogočen nadzor nad odtokanjem občutljivih podatkov preko internet in email odjemalcev (IE6,7,8..Firefox - npr. ne dovolite pošiljanja preko e-mail in webmail klientov ali kopiranja na zunanje naprave za določene vrste datotek ali datoteke z določeno vsebino.)

Ostali moduli so še Sophos Client Firewall - požarni zid; Sophos Mobile Security; SAV for NetApp Filers; NAC (Network Access Control). Za upravljanje vseh naštetih modulov pa je na voljo **enterprise console** - konzola za upravljanje, nadzor in nameščanje omenjene zaščite in izdelavo poročil o dogajanju v omrežju za Windows, Mac, Linux sisteme z možnostjo sinhronizacije z AD za samodejno namestitve anti-virus zaščite.

Glede na dejstvo, da je glavni vir škodljive kode v zadnjih letih internetno omrežje, kjer je v porastu spletni kriminal motiviran za doseganje ekonomskih, političnih in vojaških ciljev, je bilo seveda pričakovati odziv ponudnikov zaščite tudi na tem področju. Tako pri Sophosu dodajajo k prej omenjenim modulom še **Web protection** funkcionalnost, ki uporabnikom prepreči dostop do okuženih spletnih strani. Klient za vsak dostop v realnem času preveri ali se zelena spletna stran nahaja v bazi sumljivih/okuženih spletnih strani in po potrebi dostop blokira. Za tiste, ki pa želijo poleg zaščite internetnega prometa še nadzor nad uporabo interneta, pa je na voljo **Sophos Web Security & Control** programska oprema, ki je nameščena na namenski napravi **WS500/WS1100** in pregleduje prihajajoči in odhajajoči promet in aktivne vsebine po protokolih HTTP, HTTPS in FTP. Omogoča prilagajanje rabe interneta uporabnikovi varnostni politiki. Posamezne spletne strani so razdeljene v 54 kategorij, ki jih lahko omogočimo ali preprečimo z uporabo nastavitvenih politik. Politike lahko veljajo za vse uporabnike ali samo za določeno skupino. S prilagajanjem uporabe interneta omogočimo večjo prepustnost in zmanjšamo ranljivost našega omrežja. Glede na iznajdljivost uporabnikov pa rešitev omogoča tudi zaznavanje anonymizing proxy strežnikov, ki omogočajo uporabnikom, da zaobidejo nastavitve skrbnikov omrežja.

Upravljanje z namensko napravo je možno preko spletnega brskalnika in omogoča hiter dostop do nastavitve naprave in poročil o delovanju. Za miren spanec skrbnikov je poskrbljeno z več kot 50 nameščenimi monitorji, ki spremljajo tako delovanje strojne, kot tudi programske opreme in o morebitnih težavah obveščajo skrbnike oziroma Sophos podporo. V ceni licence je všteta **24/7** podpora ter vse posodobitve in nadgradnje programske opreme. Za namenske naprave pa velja še **triletna garancija**. (P.R.)

# SOPHOS

**SOPHOS d.o.o.**

Germova ulica 9, 8000 Novo mesto  
 Tel.: (07) 393 5 600, Faks: (07) 393 5 610  
 e-pošta: slovenija@sophos.si  
 spletni naslov: www.sophos.si