Pristop k varnosti mora biti večplasten

# Trend poskusov vdiranja in iskanja ranljivosti v omrežjih vztrajno narašča

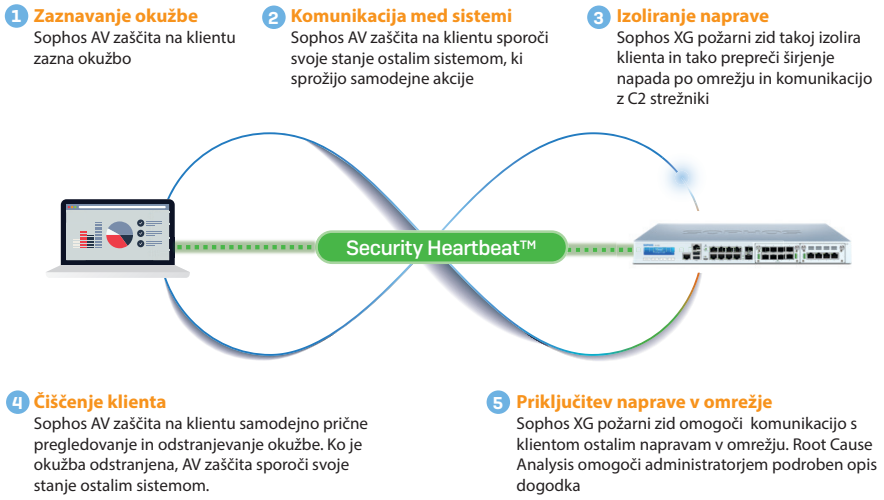
**.. V nedavno objavljenem poročilu podjetja Sophos (SophosLabs 2019 Threat Report) o pričakovanih grožnjah v letu 2019, je bilo izpostavljeno, da kibernetski kriminalci ponavadi dlje časa spremljajo svoje žrtve, preden izvedejo napad ..**

Zgoraj navedeno pomeni, da se napadalci skrivajo, spremljajo in analizirajo promet po omrežju in napadejo šele takrat, ko je pod njihovim nadzorom nameščenih dovolj kontrolnih komponent na najpomembnejših točkah v omrežju in, ko obstaja najmanjša možnost, da se napad zazna in prekine.

Razlog skrivanja je jasen: končni odjemalci v podjetjih so vedno bolje zaščiteni in kibernetski kriminalci iščejo naslednjo najšibkejšo povezavo. Zato morajo varnostni strokovnjaki v podjetju imeti orodja, ki prepoznajo take napade in so jih zmožna izolirati s pomočjo povezanih varnostnih sistemov (npr. povezanega požarnega zidu in protivirusnega programa). Povezljivost in komunikacija varnostnih orodij je za dobro obrambo omrežij v podjetjih ključna.

## Prihodnost je v povezovanju varnostnih tehnologij

Današnji poslovni uporabniki so s svojimi napravami stalno povezani do službenih omrežij in podatkov, zato ne preseneča, da so to z navdušenjem sprejeli tudi današnji podjetni kibernetski kriminalci, ki v svojih napadih prav tako uporabljajo vrsto povezanih tehnologij: e-poštno sporočilo z lažnim predstavljanjem je prva stopnja napada, tej sledi okužba z zlonamerno programsko kodo, nato sledi stopnjevanje administratorskih privilegijev ali širitev okužbe po samem omrežju med različnimi napravami. Ena




sama v omrežje povezana napadena naprava lahko pomeni grožnjo celotnemu omrežju. V preteklosti so se tehnološka varnostna podjetja posvečala ustvarjanju izdelkov, ki se osredotočajo samo na določen del problema (protivirusna zaščita, požarni zidovi …). Podjetja imajo na voljo vrsto dobrih izdelkov za varnost, a je tak pristop napačen za današnje grožnje, saj ima vsak izdelek le omejeno delovanje in zato varnost ni postala nič boljša. Večina IT strokovnjakov za varnost je enotnih, da je današnje varnostne grožnje vse težje ustaviti.

## Sophos Synchronized Security

Vlaganje denarja v individualne varnostne izdelke ni več realna dolgoročna rešitev in podjetja zato potrebujejo večplasten pristop k varnosti, kjer so varnostni izdelki med seboj povezani (sinhronizirani), si med seboj izmenjujejo informacije in delujejo kot enoten sistem. Zato je podjetje Sophos že pred časom predstavilo tehnologijo Synchronized security. Omenjeni varnostni sistem prinaša avtomatizacijo, ki izboljša obrambo, saj se samodejno odzove na varnostne incidente in s tem zmanjša tveganje, čas in denar, porabljen za upravljanje IT varnosti.

S povezovanjem vseh stebrov kibernetske varnosti podjetja ustvarijo boljši varnostni sistem, ki omogoča ustvarjanje dolgoročnih varnostnih strategij in zagotavlja večjo varnost. (P.R.)