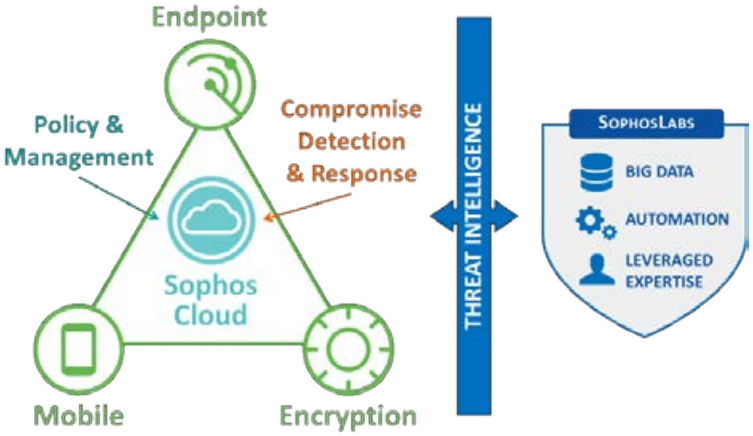
Sophos Next-Generation Endpoint Protection

Protivirusna zaščita ni mrtva

..Napredna zaščita naprav in podatkov z integracijo in inovativnostjo gradnikov zaščite..

Varovanje sistemov v poslovnem omrežju že dolgo ni več omejeno na delovne postaje in strežnike v okolju Windows, ki so povezani znotraj omrežja. Poslovna omrežja prehajajo meje zaprtega omrežja, zato se skrbniki sistemov spopadajo s čedalje večjim naborom naprav, ki se v poslovno omrežje povezujejo od koderkoli in dostopajo do poslovnih podatkov. S tem načinom delovanja pa se je povečala tudi možnost napadov in vdorov v omrežja oziroma odtekanje informacij s škodljivo kodo, ki se dnevno prilagaja varnostnim mehanizmom in omogoča izvajanje naprednih napadov na sisteme.



Sophos predstavlja nov, svež pristop pri gradnji varnostnih mehanizmov za zaščito poslovnih omrežij, ki bazira na treh glavnih načelih.

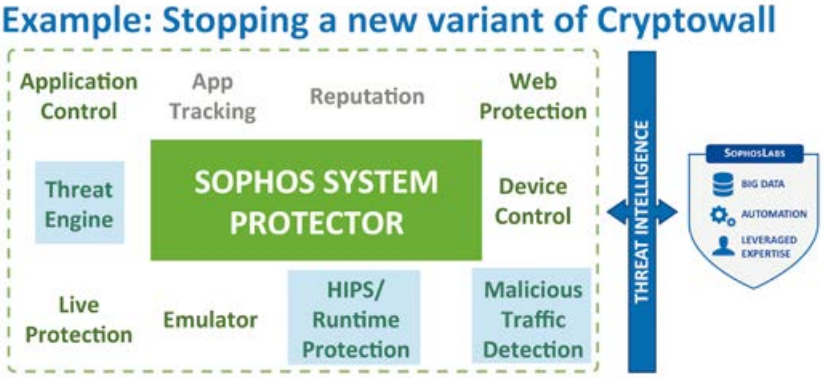
1. Zaščita omrežja mora pokrivati krovne zahteve uporabnika in vsebovati vse funkcionalnosti za enostavno in učinkovito delovanje sistema.

2. Zaščita omrežja mora zagotavljati enostavno uporabniško izkušnjo za upravljanje, nameščanje in poročanje o stanju omrežja.

3. Zadnje načelo pa pravi, da mora zaščita delovati kot sistem. Posamezne tehnološke rešitve in komponente morajo medsebojno komunicirati in sodelovati pri zagotavljanju varnosti v omrežju.

Next-Generation Endpoint Protection predstavlja vizijo zgoraj omenjenih načel in omogoča večjo varnost računalnikov, mobilnih naprav in podatkov, shranjenih v poslovnem omrežju. Rešitev najprej identificira okužen sistem v omrežju, obvesti skrbnika, prepreči dostop okuženega sistema do omrežja in poslovnih podatkov ter na koncu poskrbi za odstranjevanje okužbe same. Pri tradicionalni protivirusni rešitvi se vse skupaj začne in konča s preprečevanjem okužbe. Če se škodljiva koda vseeno izvede, ima napadalec možnost dostopanja do podatkov ali izvrševanja nadaljnjih napadov. NGEP pa poleg identifikacije okužbe preverja tudi dogajanje v sistemu, kaj določeni procesi počnejo, kam se povezujejo v omrežju in izven njega. Prvi tak dodatni gradnik je Malicious Traffic Detection, ki prestreza komunikacijo med sistemom in nadzornimi strežniki hekerjev – Command & Control servers (C&C). Podobno tehnologijo poznamo že pri požarnih zidovih naslednje generacije (na primer Sophos UTM), kjer nas na okužen sistem opozori požarni zid. Z rešitvijo NGEP pa zagotovimo, da takšne povezave zazna že sam okuženi sistem, ki lahko na ta način identificira škodljivo datoteko/proces in ga odstrani. Pri tem mu pomaga Sophos System Protector, ki predstavlja možgane rešitve NGEP in omogoča boljšo zaščito in komunikacijo med posameznimi komponentami rešitve NGEP. Primer delovanja v nekaj korakih je naslednji. Uporabnik zažene škodljivo kodo (na primer priponko v elektronski pošti), aplikacija se uvrsti med zagonske procese, kar takoj zazna Sophos System Protector, ki postane pozoren na nadaljnje delovanje sumljive aplikacije. Aplikacija se injicira v explorer.exe. To predstavlja že dodatni alarm za Sophos System Protector. Explorer.exe poskuša s komunikacijo do strežnika C&C. Sophos System Protector dobi opozorilo s strani detektorja Malicious Traffic Detector in aplikacijo blokira oziroma ustavi. Na SophosLabs pošlje tudi informacijo o sami škodljivi aplikaciji, tako da so morebitne nove okužbe blokirane že ob zagonu škodljive aplikacije.

V prihodnosti bo Sophos dodal še dodatne nivoje varnosti v NGEP, in sicer z enkripcijo ter na ta način zagotovil še boljšo zaščito, zaznavanje in odpravljanje škodljive kode v poslovnih omrežjih in izven njih. Pri tem pa je pomembno tudi dejstvo, da Sophos v svoji rešitvi ohranja vse svoje dosedanje funkcionalnosti (Application control, Device control, Data control, Client firewall in drugo), kar predstavlja prednost pred konkurenco. (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