



Sophos Intercept X Advanced za strežnike

Kako varujete svoje strežnike?

..AVGUSTA JE PODJETJE SOPHOS, KI JE ŽE 6. LETO ZAPORED UVRŠČENO V VODILNI GARTNER KVADRANT V KATEGORIJI ENDPOINT PROTECTION PLATFORMS, PREDSTAVILO NOV PRODUKT: INTERCEPT X ADVANCED FOR SERVER..



Kot je že razvidno iz imena, je Sophos prilagodil svoj najnaprednejši protivirusni produkt Intercept X, ki je bil do tedaj na voljo le za končne uporabnike, tudi za strežnike in tako Sophos Intercept X Advanced for Server predstavlja najnaprednejšo strežniško zaščito.

ŠIROK NABOR NAPREDNIH TEHNOLOGIJ ZA STREŽNIKE

Varovanje strežnikov v oblaku ali v podjetju, na katerih tečejo najrazličnejše aplikacije in na katerih so shranjeni najpomembnejši podatki za podjetja, je ena najpomembnejših nalog za informatike podjetij. Zelo velika razlika je, če je zaradi takšnega ali drugačnega virusa ogrožen ali onemogočen končni uporabnik ali pa je ogrožen ali onemogočen eden ali več strežnikov v podjetju. Moteno delovanje strežnika, nepooblaščen dostop do strežnika, kraja podatkov ali škodljivo šifriranje podatkov ima lahko za podjetje resne posledice.

Sophos Intercept X Advanced za strežnike prinaša nove tehnologije, ki dopolnjujejo že predstavljeno in uveljavljeno zaščito za strežnike s tehnologijama, kot sta na primer Server Whitelisting, katera zaklene strežnik pred neznanimi procesi, in tehnologija Cryptoguard, ki ščiti pred škodljivimi oblikami kriptiranja podatkov. Ti dve tehnologiji sta že vključeni v produktu Central

Server Protection, ki ga lahko podjetja namestijo na manj izpostavljene strežnike.

GLAVNE NOVE TEHNOLOGIJE INTERCEPTA X ADVANCED ZA STREŽNIKE SO:

- WipeGuard (varovanje pred škodljivim prepisovanjem zagonskega sektorja trdega diska MBR);
- Active Adversary Mitigation (varovanje pred naprednimi tehnikami napadalcev, da ugotovijo svojo prisotnost na napravi, ukradejo gesla, si povečajo privilegije ali pridobijo trajnejši dostop z npr. Code Cave metodo);
- Exploit Protection (preprečuje napadalcem izvršiti različne napade, tudi zero-day napade, ki izkoriščajo že znane ranljivosti sistema);
- Root Cause Analysis (podrobna vizualna analiza na forenzičnih ravni razkriva temeljne vhodne točke napada, kar omogoča določiti smernice za pomoč pri sanaciji okužb in izboljšanje informacijske varnosti v prihodnje);
- Deep Learning (napredna oblika strojnega učenja, ki zaznava tako znano kot neznano zlonamerno programsko opremo, ne da bi se oprla na tradicionalno obliko zaščite s podpismi).

Brezplačno enomesečno testiranje produkta Intercept X Advanced for Servers je mogoče znotraj testiranja Sophos Central Free Trial produktov.

SOPHOS CENTRAL – ENOTNO UPRAVLJANJE SOPHOS PRODUKTOV

Podjetje Sophos že nekaj časa razvija skupno platformo Central, s katero lahko na pregleden in preprost način upravljamo in nadziramo Sophos produkte znotraj ene skupne platforme. Poleg večje preglednosti pa skupna platforma prinaša še eno prednost tj. Synchronized Security, s katero je podjetje Sophos doseglo, da se produkti med seboj obveščajo o odkritih grožnjah in stanju sistema. Zato se lahko Sophos produkti, ki vključujejo tehnologijo Synchronized Security samodejno odzovejo na grožnjo in izolirajo okuženo napravo in napravo zopet priključijo nazaj, ko je naprava očiščena. Vse to se zgodi brez posega administratorja in v najkrajšem možnem času, kar močno dvigne zaščito in varnost omrežja.

(P. R.)

Če vas podrobneje zanimajo nove tehnologije in produkti podjetja Sophos in bi radi sodelovali z nami, ste vabljeni na Sophos Partner Roadshow 2018, ki bo potekal 4. oktobra v hotelu Hilton v Zagrebu. Za prijavo na dogodek nas pokličite na tel. številko 07/393 56 00.

SOPHOS

Security made simple.

Distributer: Sophos d.o.o., www.sophos.si, 07/39 35 600

- | | |
|----------------------|----------------------|
| Network | Enduser&Server |
| XG Firewall | Endpoint Protection |
| SG UTM | Intercept X |
| Secure Wi-Fi | Sophos Mobile |
| Secure Web Gateway | SafeGuard Encryption |
| Secure Email Gateway | Server Protection |
| Phish Threat | Sophos Home |