Pahavara tõrjumine kolmel rindel - kuidas see käib?

11 years tagasi Autor: AM

*Cisco Systems Eesti juht **Lauri Makke** selgitab uue kolmeastmelise pahavaratõrje tööpõhimõtteid.*

Pahavara loojad on tõrjepakkujatest alati mitu sammu ees ja tänased internetis hiilivad ohud on sedavõrd tegusad, et nendega võitlemine nõuab kombineeritud lahendusi. Iga päevaga tuleb võrku suur hulk seadmeid juurde, süsteemid on väga keerulised ja taustal käib pahavara loojate vilgas arendustegevus.

Teiselt poolt on palju ka turvaprobleemidega tegelejaid. Näiteks Cisco on lisanud oma praegustele turvalahendustele kolmeastmelise turvamudeli Advanced Malware Protection, mille käigus riske hinnatakse ründe eel, selle ajal ja pärast rünnet. Analüüsime ainsana katkematult kogu infrastruktuuri: pilve, arvuti- ja mobiilivõrku ühendatud, lõppkasutaja seadmeid ning virtuaalkeskkondi.

Cisco on pahavaratõrjesse lisanud ka niinimetatud "tunnetusliku ohuanalüüsi" Cognitive Threat Analytics. Ohuanalüüs on intuitiivne iseõppiv süsteem, mis kasutab käitumuslikku modelleerimist ja anomaaliatuvastust ründetegevuse kindlaksmääramiseks ning vähendab võrgus toimivate ohtude avastamise aega.

Lisaks tavapärastele pahavara avastamise meetoditele kasutatakse faili maine uuringut, faili "liivakasti" ehk Sandboxi paigutamist ja tagasiulatuvat failianalüüsi ohtude kindlaksmääramiseks ja peatamiseks ründejadas.

> **Kolmeastmelise pahavara tõrjumise tööpõhimõte**
>
> **Esmalt** analüüsitakse võrgu läbimisel faili mainet, mis pakub süsteemile vajalikke teadmisi pahavaraga nakatatud ründefailide automaatseks blokeerimiseks ning administraatori eeskirjajärgseks tegutsemiseks olemasolevas veebi- ja meiliturbe kasutajaliideses.
>
> **Teiseks** võidakse fail paigutada "liivakasti" ehk *Sandbox*i – pilves asuvasse turvalisse keskkonda võrku läbivate tundmatute failide tegeliku käitumise analüüsimiseks. See võimaldab täiustatud pahavaratõrjel koguda rohkem andmeid faili kohta ning ühendada need teadmised üksikasjalikuma inim- ja masinanalüüsiga faili ohutaseme kindlaksmääramiseks.
>
> **Kolmandaks** ehk kõige viimasemas etapis tehakse täiustatud pahavaratõrje kasutuselevõtuga lisandunud faili minevikuvaatlus, millega vaadeldakse tõrje läbinud ründefaile, mida seejärel ikkagi peetakse ohtlikuks. Faili minevikuvaatlus on selle püsianalüüs pilvepõhisest teabevõrgust pärit reaalaja andmete toel, et olla kursis muutuvate ohutasemetega.

Kui seni on ettevõtted pidanud haldama mitut turvalahendust, et tagada mitmekihilist kaitset, siis uute lahendustega käib haldamine vaid ühe kasutajaliidese kaudu ning võtab oluliselt vähem aega, kasutades iseõppivat automaatikat. Varem pidid võrguadministraatorid uued turvareeglid ise käsitsi süsteemis kirjeldama, uues süsteemis toimub kõik automaatselt ning tänu pidevale jälgimisele ka koheselt.

Arvutikasutajale, kes igapäevaselt oma tööd teeb, jääb tema tööandja või talle teenust pakkuva arvutivõrgu poolt kasutusele võetud täiustatud pahavaratõrje toimimine märkamatuks, kuid väljendub selles, et talle ei saadeta enam ohtlikke linke, spämmi ega viirusega nakatatud faile.

LAURI MAKKE

- Lahendused

- Tarkvara
- Turvalisus