Cisco: käimas on võidujooks küberründajate ja kaitsjate vahel

9. august 2015 - 22:19 Autor: AM

Cisco Midyear Security Report 2015 näitab, et üha keerukamad küberrünnakud on viinud kaitsjate ja ründajate vahelise innovatsiooni võidujooksuni. Kõige ohtlikum ründetarkvara on Angler Exploit Kit, mis on kahjustanud 40% sellega kokkupuutunud kasutajatest. Flashi turvaintsidendid on suurenenud 66%.

Juuli lõpus avaldatud Cisco Midyear Security Report 2015 analüüsib küberrünnakute keerukust ja küberturvalisuse trende. Raport soovitab organisatsioonidel tungivalt vähendada turvaohtudele reageerimise aega, et seista vastu keerukatele rünnetele kõrgelt motiveeritud ründajate poolt. Organisatsioonid peavad vastu seisma digitaalse majanduse ja asjade Interneti (IoE ehk Internet of Everything) uutele väljakutsetele ning ründevektoritele, mis pakuvad ründajatele uusi võimalusi suurte summade teenimiseks. Angler Exploit Kit on täna selleks üks enim kasutatavaid ründetarkvarasid.

Turvaraport näitab, et peamised uued riskid on seotud Flashi tarkvaraga, väljapressimistarkvara arengu (ingl. k *ransomware*) ning Dridexi muteeruva pahavara levikuga. Digitaalse äri ja asjade Interneti ajastul muutuvad turvaohud aina levinumaks, mis paneb tõsiselt proovile turvatööstuse senise hinnangu, et reageerimisaeg uuele turvaohule võib olla 100-200 päeva.

Raport leiab ka, et ettevõtted peavad rohkem looma integreeritud lahendusi, mitte vaid ühe funktsiooniga tooteid, tegema koostööd usaldusväärsete partneritega ja looma globaalseid küberkaitsevõrgustikke, et ülemaailmselt koostööd edendada.

> *Kõige ohtlikum ründetarkvara täna on Angler Exploit Kit, Adobe Flash turvaaugud on teisel kohal.*

Lauri Makke, Cisco Eesti juht: "Häkkerid hoiavad end pidevalt kursis uusimate küberlahenduste ja innovatsioonidega ning on kiired nendega kohanema. Näeme seda pidevalt, olgu siis tegemist pahavara, ründe- või väljapressimistarkvaraga. Suhtumine, et sadakond päeva on piisav aeg turvaohule reageerimiseks, on tänaseks vananenud. Organisatsioonid peavad investeerima integreeritud turvalahendustesse, mis töötavad üheskoos ja suudavad avastada ja tõrjuda uudseid küberrünnakuid tundide, mitte päevadega. Peagi võime rääkida juba minutitest."

Raporti peamised leiud:

- **Angler** on praegu kõige keerulisem ja laiemalt levinum ründetarkvara komplekt, mis kasutab osavalt ära Flashi, Java, Internet Exploreri ja Silverlighti nõrkusi. Angler kasutab tuvastamise vältimiseks ka mitmeid erinevaid tehnikaid (Domain Shadowing jne).

- **Flashi turvaohud on tagasi** – Adobe Flashi turvaaukude ärakasutamine on integreeritud Angleri ja Nucleari ründevahenditesse ja nende kasutamine on tõusuteel. See õnnestub hästi tänu Flashi automaatsete turvauuenduste puudumisele, samuti kasutatakse ära seda, et kasutajad ise ei paigalda koheselt uuendusi. 2015. aasta esimesel poolaastal oli Adobe Flash Playeri turvaintsidente 66% rohkem kui 2014. aastal. Sellega on Flash rekordigraafikus kõigi aegade suurima turvaintsidentide arvuga aasta, mis seni CVE (*Common Vulnerabilities and Exposure)* süsteemis registreeritud.

- **Väljapressimistarkvara** on saanud häkkerite jaoks tulusaks vahendiks. Pidevalt toodetakse juurde selle tarkvara uusi versioone. Väljapressimistarkvara on juba täielikult automatiseeritud ja levib n-ö tumedas veebis, kus makseid tehakse krüptorahas (näiteks bitcoinides). Välja pressitud raha saaja jääb niimoodi võimuorganite jaoks nähtamatuks.

- **Dridexi** kiiresti muutuv ründetaktika teeb antiviirustel elu keeruliseks, sest need peavad uusi modifikatsioone registreerima kui täiesti uusi turvaohte. Kiiresti muutuv on ründes kasutatavate e-kirjade sisu, lisandid ja agendid, mis ilmuvad uute ründekampaaniatena ning sunnivad traditsioonilisi antiviiruseid registreerima aina uusi ja uusi ründemeetodeid.

Kutse küberkaitsele

Võidujooks ründe- ja kaitsevahendite täiustamiseks aina kiireneb, mis paneb lõppkasutajad ja organisatsioonid suuremate riskide ette. Turvalisust tagavad partnerid peavad olema valvsad ja ehitama integreeritud turvasüsteeme, aidates organisatsioone juba ennetavalt, pakkudes õigeid inimesi, lahendusi ja tehnoloogiaid.

Integreeritud küberkaitse on oluline – organisatsioonid on silmitsi suurte väljakutsetega, kui kasutavad vaid ühe kaitsefunktsiooniga tooteid. Mõelda tuleb integreeritud kaitsearhitektuuri peale – sellise, mis kaitseb kõikjal väga erinevate rünnete eest.

Vajalik on globaalne turvavõrgustik – see on selline küberkaitsesüsteem, mis lahendab geopoliitilisi väljakutseid, tegeleb küsimustega, kuidas valitsused koguvad andmeid nii inimeste kui ettevõtete kohta, mismoodi seda jagatakse üksteisega ning kuidas valitsused teevad globaalselt koostööd selles osas. Vaja on koostöövõimelist, sidusrühmadega valitsusasutuste võrgustikku, mis suudaks maailmatasemel koostööd teha ja tagada majanduskasvu.

Usaldusväärsed partnerid on turvalisuse tagatis – organisatsioonid peavad nõudma, et nende küberkaitsepartnerid oleksid läbipaistvad, et nad suudaksid tõestada oma toodete usaldusväärsust ja seda kogu toote eluea jooksul.

- Uudised
- Turvalisus