Cisco hoiatab: ettevõtted on ohtlikus maailmas liiga optimistlikud

11 aastat tagasi - 28.01.2015 Autor: AM

Meil on kõik korras, kinnitavad turvaosakonna spetsialistid. Õppinud mehed, uued tööriistad. Kuid Cisco läbiviidud uuring kinnitab, et kohati on ettevõtted selles osas liiga optimistlikud. Pahalased võivad olla pool sammu firmadest ees. Ja sellest piisab, et märkamatult tegutseda.

Cisco küberturvalisuse aastaaruanne paljastab aina suureneva lõhe tajutava ja tegeliku olukorra vahel küberturvalisuses. 60% kaitsevõime küsitlusele vastanutest ei paigalda turvaparandusi ja vaid 10% Internet Exploreri kasutajatest kasutavad selle brauseri viimast versiooni. Samas koguni 90% vastanutest on endiselt kindlad oma küberturvalisuses.

FOTO: (CC) Stuart Miles, Freedigitalphotos.net

Värskelt avaldatud Cisco 2015. aasta küberturvalisuse aruanne, mis vaatleb nii küberohtude vastast võitlust kui küberturvalisuse trende, jõuab järeldusele, et ettevõtted peavad asuma kindlamalt võitlema küberrünnakute vastu.

Cisco Systems Eesti juht Lauri Makke kinnitabki, et ründajad on mõnikord ajast ees: “Ründajad on muutunud osavamaks uute turvaaukude ärakasutamisel veel enne, kui need avastatakse ja nende vastu midagi ette võetakse. Kaitsjad, täpsemalt ettevõtete turvameeskonnad, kes peavad pidevalt arendama organisatsiooni küberkaitsevõimet, puutuvad aina rohkem kokku kiiremate ja keerulisemate rünnakutega kui seni. Olukorrale lisavad keerukust ründajate geopoliitilised huvid ning riikide erinevad nõuded andmete suveräänsusele, lokaliseerimisele ja krüpteerimisele.”

Enimlevinud ründed

Küberkurjategijad laiendavad pidevalt oma võtteid ja tehnikat, et muuta rünnakud raskemini avastatavaks. Cisco poolt on avastatud kolm olulisemat trendi:

1. **Nn. “Lumeräätsaspämm**” on muutumas üheks levinumaks ründemeetodiks. Ründajad saadavad väga paljudelt erinevatelt IP aadressidelt välja vähesel määral spämmkirju, et vältida spämmifiltrite poolt avastamist. See, nagu räätsaga pehmel lumel jalutamine ilma läbi vajumata, eeldab paljude kasutajakontode ülevõtmist, mida saaks hajutatud spämmimiseks kasutada.
2. **Veebilehe salaja hõivamine ilma väliseid märke jätmata**: tavaliselt avastatakse enimlevinud veebihõivamisvahendid küberturvalisuse eest võitlevate firmade poolt kiiresti. Sellest tulenevalt proovivad küberkurjategijad kasutada vähemlevinud töövahendeid, mis ei jäta veebilehele jälgi ja ei tõmba tähelepanu. Koduleht hõivatakse vaikselt ja märkamatult, jättes pealtnäha kõik endiseks.
3. **Nn “Kurjad kombinatsioonid”:** Flash ja JavaScript on juba ajalooliselt olnud ebaturvalised, kuid arenenud küberkaitsevahendid aitavad neid siiski hoida piisavalt turvalistena, et sissetungi vältida. Ründajad on aga arendanud välja kombineeritud ründevahendid, mis nende nõrkusi mitme erineva turvaaugu kaudu ära kasutavad. Tekitades turvaaugu läbi mitme faili, näiteks ühe Flashi ja ühe JavaScripti faili kaudu, saab teha turvalahendustele rünnaku avastamise ja blokeerimise tunduvalt raskemaks.

Rünnakud arvutikasutajatele on kasvanud 250%

Arvutikasutajad ei ole alati vaid lõppsihtmärk, keda rünnatakse. Nad on ka enese teadmata küberrünnakutele kaasaaitamise vahendid. 2014. aastal avastas Cisco küberrünnakute uurimise töögrupp, et ründajad on aina enam nihutamas oma fookust serveritesse ja operatsioonisüsteemidesse sissemurdmise pealt kasutajate veebilehitsejate ja e-posti nakatamisele. Rünnakud läbi kasutajate, kes laevad näiteks nakatunud saidilt alla Silverlighti pahavara, on kasvanud 228% ja spämmi ning pahavarareklaamide kaudu toimunud rünnakute hulk on kasvanud 250%.

Ettevõtted hindavad enda kaitsevõimeid üle

Cisco küberturvalisuse kaitsevõime uuringust, millele vastasid 1700 ettevõtte infoturvalisuse juhti ja turvaeksperti üheksast riigist selgub, et lõhe kaitsjate arvamusest oma kaitstuse kohta ja tegeliku kaitsevõime vahel aina suureneb.

Uuring näitab, et 75% infoturvalisuse juhtidest peavad enda kaitsesüsteeme kas väga või ülimalt tõhusateks. Samas alla 50% vastanutest kasutavad tavalisi standardseid kaitsevahendeid, nagu turvalappide paigaldamine ja turvaseadete seadistamine. Heartbleedi turvaintsident oli eelmisel aastal hea indikaator, mis näitas, et tegelikult olid 56% kõigist installeeritud OpenSSL-i versioonidest vanemad kui neli aastat. See näitab selgelt, et turvatiimid ei paigalda hoolikalt uusimat tarkvara ega turvalappe.

Aruandest

Cisco küberturvalisuse kaitsevõime aastaaruanne 2015 on üks olulisemaid turvalisuse aruandeid, mis uurib Cisco turvalisuse ekspertide poolt kogutud viimaseid turvaohte, pakkudes ettevõtetele olulisi trende ja paljastusi küberturvalisusest viimase aasta jooksul. Aruanne toob välja ettevõtete seisukohad ja suhtumised turvalisusküsimustesse ja nende ettekujutuse valmisolekust end küberrünnakute eest kaitsta. Geopoliitilised trendid, ülemaailmsed arengud ja küberturvalisuse olulisus juhtkonnale leiavad aruandes samuti kajastamist.

Täispikka aruannet saab lugeda siit: www.cisco.com/go/asr2015

Vaata ka videokommentaari aruandele, inglise keeles:

- Uudised
- Turvalisus