Lehdistötiedote 9.4.2014

Mitä tapahtuu kyberhyökkäyksen jälkeen?

Yritysverkkoihin tunkeudutaan edelleen luvattomasti, vaikka palomuurit ja virustorjuntaohjelmat ovat paikoillaan. Nyt onkin syytä miettiä, mitä pitää tehdä, jotta tietomurron tai muun kyberuhan aiheuttamat vauriot jäävät mahdollisimman pieniksi. Exclusive Networks Groupin vastaus ongelmaan on joustava ja kattava CARM-konsepti, joka yhdistää useiden toimijoiden tarjonnan parhaat palat.

Mitä tapahtuu, jos kyberrikollinen onnistuu ohittamaan yrityksen palomuurit, virusohjelmat ja muut suojaukset? Miten pahasti ja miten pitkäksi ajaksi organisaatio vahingoittuu? Kuinka kalliiksi se tulee? Kuinka paljon henkilökuntaa kriisitilanne sitoo? Siinä kysymyksiä, jota yrityksissä pohditaan ja pitääkin pohtia. Tietomurtoja tehdään niin paljon, että on vain ajan kysymys, milloin pitkäkyntinen ehtii omalle ovelle.

Miksi kyberuhat ovat vaikeita torjua?

Jotta kyberhyökkäyksiltä voidaan suojautua, on tunnettava vihollinen. Kyberuhkien täydellinen torjunta on vaikeaa, koska:

- Yritysverkkoon liitettyjen laitteiden määrä kasvaa jatkuvasti. Monet käyttävät yrityksen dataa jo kahdella tai kolmella eri laitteella.
- Kun henkilöstö käyttää omia laitteitaan (BYOD), IT-osaston on vaikeaa varmistaa kaikkien laitteiden tietoturvan tasoa.
- Pilvipalvelut tarjoavat kyberrikollisille laskentaresursseja sekä uusia ovia koputeltaviksi.
- Android-käyttöjärjestelmän yleistyttyä kyberrikolliset ovat innostuneet kehittämään runsaasti uusia haittaohjelmia juuri Android-laitteille.
- Henkilöstö lataa koneilleen sovelluksia välittämättä työnantajan tietoturvaohjeista.
- Kyberhyökkäykset ovat entistä järeämpiä. Ponemon Instituten kansainväliseen tutkimukseen vastanneista IT-asiantuntijoista yli puolet raportoi hyökkäysten esiintymistiheyden ja voiman kasvaneen entisestä.
- Tietomurroista 75 % tehdään tällä hetkellä yritysverkon ulkopuolelta. Yritysverkon sisältä vuodetaan tietoja suhteessa entistä harvemmin, vain alle 10 % tapauksista.
- Kyberuhat ovat entistä monimutkaisempia ja hienostuneempia ja siksi vaikeampia havaita ja torjua. Tunnettuja tekniikoita eri tavoin yhdistelevät APT:t (Advanced Persistent Threat) ovat yleistyneet. On tärkeää, että tietoturvaratkaisu tunnistaa myös uudet haittaohjelmat eli Zero day -hyökkäykset. Uusimmat kyberuhat osaavat muuntautua ja ottaa useita valepukuja.

Exclusive Networks Groupin ratkaisu on CARM

Nykyiset tietoturvajärjestelmät keskittyvät pitkälti pitämään kyberuhat yritysverkon ulkopuolella. Pelkkä torjuntastrategia ei kuitenkaan enää riitä, vaan yrityksen pitää varautua myös tietomurron jälkeiseen aikaan. Tarvitaan strategia vahinkojen minimoimiseksi.

Exclusive Networks Groupin ratkaisu tietoturvan kriisitilanteisiin on CARM (Cyber Attack Remediation & Mitigation). Kun tietoverkkoon tunkeudutaan, CARM antaa organisaatiolle nopeasti kaikki sen tarvitsemat tiedot: mitä on tapahtunut, missä, milloin, miksi ja miten. Aktiivinen puolustautuminen ja uhan vaikutusten minimointi alkavat automaattisesti ja välittömästi.

CARMin prosessi sisältää uhkien torjunnan lisäksi tietoverkon reaaliaikaisen seurannan, poikkeavuuksien havaitsemisen, tunnistamisen ja luokittelun, nopean reagoimisen ja kriisinhallintaominaisuudet. Siksi hyökkääjä ei onnistu tavoitteessaan. Lopputuloksena on liiketoiminnan lamaantumisen sijasta tunnistettu uhka, jolta osataan jatkossa suojautua.

Kattava järjestelmä on koottu Arbor Networksin, LogRhythmin, FireEyen, Palo Alto Networksin, Infobloxin, Bit9:n, Impervan, Mandiantin ja Fortinetin tarjonnasta. CARM yhdistää näiden teknologioiden avaintoiminnot siten, että niiden yhteinen tehokkuus maksimoituu, mutta samalla kustannukset pysyvät kurissa. Automatisoitu järjestelmä säästää myös yrityksen henkilöstön työaikaa.

CARM on integroitavissa yrityksen olemassaolevaan tietoturvaan. Aiemmat investoinnit esimerkiksi palomuureihin, IPS:ään tai virustorjuntaan eivät mene hukkaan. CARMin avulla yrityksen vanha, uhkien torjumiseen keskittyvä tietoturvaratkaisu on nostettavissa uudelle, nykytilanteen vaatimalle tasolle.

CARM tarjoaa:

- Nopeamman reagoinnin, jolloin hyökkäyksen vaikutukset jäävät vähäisemmiksi
- Paremman ja nopeamman reagoinnin tietovuotojen eristykseen ja paikkaukseen
- Nopean vasteajan datamääristä riippumatta
- Vähemmän IT-työtunteja automaation ansiosta
- Oppivan järjestelmän, joka tunnistaa uhan jatkossa
- Kustannustehokkaan ratkaisun

###

Exclusive Networks Group
Exclusive Networks Group tuo vakiintuneet ja kasvuvaiheessa olevat globaalit teknologiayritykset EMEA-alueen markkinoille hyödyntäen SuperVAD-jakelumalliaan. Se on erikoistunut yritysten turvallisuus-, verkko-, infrastruktuuri- ja tallennusratkaisuihin ja sen yhteistyökumppaneina on tuhansia jälleenmyyjiä.

Yhtiö koostuu yhtenäisesti ohjatusta ryhmästä kansallisesti toimivia, riippumattomia ja yrittäjävetoisia bisnesyksiöitä. Se tunnetaan innovatiivisten ja epätavanomaisten teknologioiden tuomisesta EMEA-alueen markkinoille sekä näiden teknologioiden kasvun pitkäjänteisestä tukemisesta. Vuonna 2003 perustettu yhtiö on kasvanut itse ja tukenut jälleenmyyjä-, integraattori-, VAR- ja palveluntarjoajapartnereidensa kasvua merkittävästi vauhdittamalla niiden markkinoille tuloa konsultointi-, suunnittelu-, markkinointi-, myynti- ja koulutuspalveluiden sekä teknisen tuen avulla.

Exclusive Networks Groupin pääkonttori on Ranskassa, ja se toimii yli 20 Euroopan, Lähi-idän ja Pohjois-Afrikan maassa.

Lehdistökontakti:

Jussi Mero
Head of Sales
Exclusive Networks
P. 020 7551 640
jmero@exclusive-networks.com