Organisaatioissa jokainen sähköpostia käyttävä henkilö on, halusi sitä tai ei, huomattava vastuun kantaja.

2017-01-23 15:32 EET

Mikä on tiedon hinta?

Verkkopalveluihin kohdistuneissa verkkomurroissa kansanedustajien ja poliisien salasanoja on vuotanut, tietoja kerätty sekä järjestelmiä lukittu lunnasrahavaatimuksien kera. Trendinä hyvin useassa tapauksessa on ollut hyökkäyksen kohdistaminen käyttäjään.

Oletko harjoitellut organisaatiossasi varmuuskopioiden käyttöä?
Nykypäivän uhkakuviin riittää, että yksi organisaation työntekijä avaa yksittäisen sähköpostin liitetiedoston tai linkin, jonka jälkeen ulkopuolinen taho pääsee salaamaan koko organisaation tietojenkäsittelyjärjestelmät. Jotta ne saadaan taas käyttökelpoiseksi, verkkorikolliset vaativat tuhansien bitcoinien kokoisia lunnaita. Kun organisaatiossa vielä mietitään mitä pitäisi tehdä, on sen toiminta todennäköisesti jo pysähtynyt. Yhtenä vaihtoehtona on sulkea järjestelmät ja palauttaa oikeaoppisesti tehdyt varmuuskopiot. Tämä vaihtoehto edellyttää sitä, että organisaatio on harjoitellut varmuuskopioiden käyttöönottoa, tehnyt niitä systemaattisesti sekä pitänyt niitä erillään omasta järjestelmästään. Toisena vaihtoehtona on maksaa lunnaat ja toivoa, että taho jolle rahat on siirretty, on tarpeeksi hyväntahtoinen antaakseen tarvittavan salasanan.

Organisaatioissa jokainen sähköpostia käyttävä henkilö on, halusi sitä tai ei, huomattava vastuun kantaja. Kiristysohjelmistot pakottavat organisaation miettimään kaapatun tiedon hintaa ja tiedon varastamista vastaan tehtäviä toimenpiteitä.

Teknisillä ratkaisuilla apua tietoturva-aukkoihin
Markkinoilla on saatavilla erilaisia teknisiä ratkaisuja vastaavia hyökkäyksiä vastaan. Yksi suosituimmista on sähköpostien liitetiedostoja skannaavat ohjelmistot, jotka tarkistavat esimerkiksi vanhempaa tiedostotyyppiä olevia Excel ja Word -tiedostoja makrovirusten varalta. Tämäntapaisissa hyökkäyksissä sähköpostiosoite naamioidaan tulevan organisaation sisältä tai

muulta luotettavalta taholta tulevaksi. Liitetiedosto taas sisältää ajankohtaisen raportin, työhakemuksen, sopimuksen tai muun vastaavan. Henkilöstön avatessa tiedoston, sen sisälle piilotettu makro antaa hyökkääjälle pääsyn laitteeseen. Näitä vastaan toimivat skannausohjelmistot ovat yksi ja erittäin suositeltu osaratkaisu, mutta sekä verkko, että reaalimaailma sisältävät myös muita tietoon kohdistuvia uhkia.

Tietosuoja-asetus asettaa velvollisuuksia yrityksille ja orgnisaatioille

EU:n tulevaa tietosuoja-asetuksen sisältöä on avattu aikaisemmassa artikkelissani. Tietoturvallisuuden näkökulmasta se asettaa tiettyjä velvollisuuksia yrityksille ja organisaatioille, jotka käsittelevät henkilötietoja. Nämä vaateet sisältävät niin teknisiä kuin organisaatiollisia toimenpiteitä, mukaanlukien tietoturvakoulutuksen ja tämän koulutuksen todentamisvaateen. Alertumin tietoturvakoulutuksessa todentamistarve on huomioitu työturvallisuuskortin tapaisella henkilökohtaisella kortilla.

Henkilöstön rooli merkittävä tietoturvallisuudessa

Henkilöstön osaamisen ja tietoisuuden merkitys on Aalto-Yliopistonkin tekemien tutkimuksien mukaan merkittävä, vaikka usein unohdettu osa tietoturvallisuutta. Tietosuoja-asetuksen mukana tulevat mittavat sakkorangaistukset tuovat osaltaan myös insentiiviä yrityksille, jotka käsittelevät henkilötietorekisterejä liiketoiminnassaan, huolehtia asetuksen mukaisista toimenpiteistä tietojen suojaamiseksi.

Tämän artikkelin kirjoittaja on Alertumin tietoturvallisuus- ja tietosuojakouluttaja Leo Hämäläinen.

Alertum luo osaamisella maailman turvallisinta yhteiskuntaa.

Alertum Oy on kasvava ja kehittyvä turvallisuuskoulutuksia tarjoava yksityisyritys. Toteutamme turvallisuutta edistäviä lyhytkoulutuksia valtakunnallisesti.

Palvelumme huomioivat yksilöllisesti sekä pienen että suuren yrityksen tai julkisen toimijan tarpeet henkilöstön turvallisuusosaamisen kehittämisessä. Tarjoamme osaamistamme pätevyyskoulutusten suunnittelussa, toteutuksissa ja pätevyyksien ylläpidossa.

Yhteyshenkilöt

Lari Lindén
Lehdistökontakti
kehitysjohtaja
lari.linden@alertum.fi
010 320 5773