Tekniset ratkaisut tietoturvan tueksi

Tietoturvan parantamiseen löytyy monia teknisiä ratkaisuja, Olli-Pekka Halonen ja Lassi Kojo kertovat.

Toukokuussa täytäntöön pantava EU:n tietosuoja-asetus mietityttää monessa yrityksessä. 25.5.2018 alkaen asetus koskettaa käytännössä kaikkia yrityksiä ja organisaatioita. Loimaalaisen JMJping Oy:n palvelut auttavat uusiin tietoturvavaatimuksiin vastaamisessa.

- Tietoturvaa voidaan parantaa esimerkiksi palomuureilla, kaksivaiheisella tunnistautumisella sekä tietojärjestelmien valvonnalla, tuotekehittäjä Olli-Pekka Halonen kertoo.

JMJping Oy on vuonna 2005 perustettu tietotekniikka-alan yritys, joka tarjoaa laadukkaita ICT-palveluja asiakaslähtöisesti ja kilpailukykyisin hinnoin.

Tietosuoja-asetuksen tarkoituksena on varmistaa, että ihmisten henkilötiedot ovat suojassa ja asiakkaan tarkastettavissa. Yritykset ovat sakon uhalla velvoitettuja käsittelemään ja säilyttämään henkilötietoja huolellisesti: teknisten suojausten ja rajoitusten tulee olla riittävällä tasolla.

- Suojaustasoa voidaan nostaa nykyaikaisella palomuurilla. Edustamamme SonicWall-palomuurit ovat markkinajohtajia, joilla voidaan reaaliaikaisesti tarkastaa ja estää jopa haittaohjelmien salattua liikennettä. Kaksivaiheisella tunnistautumisella taas voidaan huomattavasti pienentää salasanojen vuotamisesta aiheutuvaa tietoturvariskiä, Halonen sanoo.

Yritysten on siirtymäajan jälkeen muun muassa tiedettävä ja pystyttävä osoittamaan mitä, missä, miten ja kenen toimesta ne henkilötietoja käsittelevät. Jos tietomurto tai -vuoto sattuu, yrityksen on tiedotettava 72 tunnin sisällä havaitusta tietovuodosta viranomaisille.

- Yritysten voi olla vaikea huomata tietovuotoa riittävän nopeasti ilman teknisiä apuvälineitä. JMJpingin valvontajärjestelmät huomaavat, jos tietoja on käsitelty normaalista poikkeavalla tavalla tai jos järjestelmiin yritetään tunkeutua, järjestelmäasiantuntija Lassi Kojo kertoo.

- Valvontajärjestelmillä voidaan seurata, onko yrityksen tietojärjestelmissä kaikki niin kuin pitääkin. JMJ Valvonta on hajautettu valvontajärjestelmä, jolla pystytään seuraamaan suurta joukkoa eri tyyppisiä laitteistoja, palveluita ja muita järjestelmiä. Järjestelmä hälyttää, jos valvottavissa kohteissa tapahtuu jotain poikkeavaa. JMJ Analyzer -ohjelmisto puolestaan toimii suurennuslasina kaikkiin valvottaviin järjestelmiin ja kertoo, mistä hälytys johtuu, Kojo sanoo.

Tietoturvan kannalta tällaisia poikkeavia tilanteita voi olla, jos esimerkiksi väärät henkilöt tarkastelevat yrityksen rekistereitä tai verkkojaossa olevia tiedostoja, tietokannasta ladataan suuria määriä tietoja ulos tai tietoihin yritetään tunkeutua yrityksen ulkopuolelta.

- Kun mahdollisista tietoturvaloukkauksista saadaan tieto heti, niihin pystytään myös reagoimaan nopeasti ja näin minimoimaan vahingot, Kojo toteaa.

Tietoturvan lisäksi valvontajärjestelmä pyrkii ehkäisemään muitakin häiriöitä yrityksen tietojärjestelmissä. Tarkoituksena on ennakoida ja estää käytön estävien vikatilanteiden syntyminen. Valvontajärjestelmä voi esimerkiksi kertoa kiintolevyn rikkoutumisesta jo ennen kuin käyttäjä huomaa minkään olevan vialla.

jmj.fi

JMJping Oy
Käsityöläiskatu 10,
32200 Loimaa
www.jmj.fi