SANS SECURITY AWARENESS

Kuukausittainen uutiskirje tietoturvatietoisuuteen liittyvistä aiheista

GDPR

Yleiskatsaus

Olet saattanut kuulla EU:n uudesta tietosuoja-asetuksesta tai GDPR:stä joka astuu voimaan 25.5.2018. Asetus koskettaa jokaista yritystä joka käsittelee EU:n kansalaisten henkilötietoja, riippumatta missä maassa käsittely tapahtuu tai missä maassa yritys sijaitsee. Asetus vaatii yrityksiltä henkilötietojen asianmukaista suojaamista ja tietoturvallista käsittelyä. Jotta yritys pystyisi toimimaan asetuksen mukaisesti, on ymmärrettävä muutamia asioita.

Ihmisillä on oikeus yksityisyyteen ja yritysten pitää kunnioittaa tätä yksityisyyttä rajoittamalla keräämäänsä tietoa ja suojata kerättyä tietoa mahdollisimman tehokkaasti. Asetuksen vaatimukset koskevat kaikenlaista tietoa, joka suoranaista henkilötietoa, tai tietoa jota yhdistelemällä voidaan tunnistaa yksittäinen, luonnollinen henkilö. Tämä voi sisältää mm. osoitteen, passin numeron, ajokortin tiedot, taloustietoja, biometriikkaa, terveystietoja, sijaintitietoja tai tietoja poliittisesta, seksuaalisesta tai uskonnollisesta suuntautumista. Alla on listattuna joitakin asetuksen vaatimuksia jotka koskevat henkilötietojen käsittelyä:

Henkilötietoja saa käsitellä vain lainmukaisesti, asianmukaisesti ja läpinäkyvästi.

Rekisteröidyille pitää kertoa mitä tietoja kerätään ja miksi.

Henkilötietoja saa kerätä vain tiettyyn, erikseen mainittuun, lainmukaiseen tarkoitukseen. Tietoja ei saa käyttää muihin kuin mainittuihin tarkoituksiin.

Henkilötietoja saa säilyttää ja käsitellä vain sen ajan kuin mitä mainittu käyttötarkoitus edellyttää.

Säilytettävien henkilötietojen on oltava oikeita ja ajankohtaisia.

Rekisteröidyillä on oikeus nähdä itsestään tallennetut tiedot ja joissakin tapauksissa estää tietojensa käyttö tai jopa pyytää niiden poistamista.

Yritysten on ylläpidettävä asianmukaisia ja riittäviä tietoturvakontrolleja henkilötietojen käsittelyn ja säilymisen turvaamiseksi.

Edellä mainittujen lisäksi yritysten on varmistuttava, että henkilötietoja käsittelevä henkilöstö on koulutettu asianmukaisesti

Yrityksen määrittelemät suojaavat toimenpiteet ja kontrollit, joilla henkilötietoja suojataan pitää täsmäyttää yrityksen määrittelemään riskitasoon joka henkilötietojen käsittelylle yrityksessä on määritelty. Kun henkilötietojen käsittelyyn liittyvä riskitaso nousee, pitäisi henkilötietojen suojaamiseen käytetyt resurssit nousta vastaavasti. Suojaavia toimenpiteitä ja kontrolleja pitäisi arvioida ja kehittää säännöllisesti ja asetuksen vaatima dokumentaatio pitäisi olla kattavaa ja ajantasaista osoitusvelvollisuuden täyttämiseksi. Siirrettäessä henkilötietojen käsittelyä kolmannelle osapuolelle, yrityksen pitäisi varmistaa asetuksen vaatimusten täyttyminen hallinnollisin, teknisin ja sopimuksellisin keinoin. Mahdollisen tietoturvapoikkeaman sattuessa, yrityksen pitää ilmoittaa poikkeamasta oikeille tahoille 72 tunnin sisällä. Asetukseen noudattamatta jättämiseen ja rikkomuksiin liittyen on määritelty rangaistukset, jotka pahimmassa tapauksessa ovat neljä prosenttia yrityksen globaalista liikevaihdosta.

Uutiskirjeen kääntäjä Kirill Filatov (KTM) on GIAC-sertifioitu tietoturvaa rakastava, kokenut IT-ammattilainen. Kirill turvaa tällä hetkellä Nebula Oy:n asiakkaiden liiketoimintaa konsultoimalla ja kehittämällä asiakkaiden tietoturvaviitekehyksiä ja toimintamalleja.

Vierastoimittaja

Brian Honan *toimii toimitusjohtajana Irlantilaisessa BH Consulting-nimisessä yrityksessä, joka konsultoi asiakkaita kyberturvallisuuteen ja tiedon suojaamiseen liittyvissä asioissa. Brian on myös toiminut erityisasiantuntijana Europolin Kyberrikoskeskuksessa (Cybercrime Centre EC3), ollut perustamassa Irlannin ensimmäistä CERT-toimijaa ja toimii monien turvallisuusyritysten hallituksissa. Brianin löydät* www.linkedin.com/in/brianhonan *tai Twitteristä* @brianhonan.

Lähteet

GDPR Overview For Individuals and Organizations:	http://gdprandyou.ie
Tietosuoja-asetus:	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016R0679
OUCH! Käännökset ja arkistot:	https://www.sans.org/u/D88