3M | The experts in screen privacy.

GDPR-valmius Usein kysytyt kysymykset

Enza Lannopollo, Forrester Research

Enza on analyytikko tietoturva- ja riskitiimissä, ja hänellä on eurooppalainen Certified Information Privacy Professional -tietosuojasertifikaatti (CIPP/E). Hän käsittelee Forresterilla tietosuojaa, yksityisyyttä sekä analytiikkaa ja keskittyy erityisesti niihin liittyviin määräyksiin ja teknologiaan.

GDPR on yksi tärkeimmistä tietosuojamääräysten muutoksista 20 vuoteen. Se määrittää, kuinka organisaatioiden täytyy käsitellä asiakkaiden, työntekijöiden ja liikekumppaneiden henkilötietoja. 3M keskusteli Forrester Researchin Enza Lannopollon kanssa suojaustoimenpiteistä, käytännöistä ja tietosuojamääräysten noudattamisen ohjelmista, joita monet organisaatiot ottavat käyttöön noudattaakseen GDPR:n määräyksiä. Enza jakoi tietoa työpaikkojen valmiuksista ja korosti fyysisten suojakeinojen käytön tarvetta taistelussa tietosuojauhkia vastaan.

Tässä hänen viestinsä:

Mitä on vaakalaudalla?

Organisaatioille voidaan määrätä sakkoja jopa 4 % vuosittaisesta maailmanlaajuisesta liikevaihdosta tai

20 M€ FINE

K. Onko työvoima valmiina noudattamaan GDPR:ää?

V. Lukumme osoittavat, että maailmanlaajuisesti vain yksi kolmesta yrityksestä on valmis noudattamaan Yleistä tietosuoja-asetusta (GDPR). Koska GDPR astuu voimaan 25. toukokuuta 2018, on selvää, että useiden organisaatioiden täytyy viimeistellä valmistelunsa nopeasti.

Olemme erityisesti huomanneet, että yrityksillä on ongelmia täyttää vaatimus työntekijöiden tietoturvakoulutuksen ja tiedotusohjelmien käyttöönotosta ja dokumentoinnista. EU:n sääntelijät ovat ilmaisseet, että nämä ohjelmat ovat edellytys GDPR:n noudattamiselle. Samalla olemme huomanneet, että tämän edellytyksen täyttävien organisaatioiden tietosuojakulttuuri on parantunut ja käyttöön otetut parhaat käytännöt ylittävät joskus säännösvaatimukset.

K. Ovatko tietyillä alueilla sijaitsevat yritykset valmistautuneet paremmin kuin muut?

V. 34 prosenttia USA:n yrityksistä ilmoitti olevansa valmiina, kun taas Euroopassa sama luku on 26 prosenttia.[1] GDPR:ää noudattamattomat yritykset ottavat, tietoisesti tai tiedostamatta, suuren liiketoimintariskin. Yrityksissä, joissa luullaan virheellisesti valmiuden olevan kohdallaan, riski on vielä suurempi.

On mielenkiintoista huomata, että USA:ssa suurempi osa yrityksistä uskoo valmiuteensa kuin Euroopassa. Tämä liittyy GDPR:n rajat ylittävään vaikutukseen. Määräys koskee kaikkia yrityksiä, jotka käsittelevät tai säilyttävät Euroopan unionin asukkaiden henkilötietoja, riippumatta yritysten sijainnista. Tämä merkitsee, että eurooppalaisten yritysten lisäksi useiden yritysten, joiden pääkonttori sijaitsee USA:ssa, täytyy noudattaa näitä tiukkoja tietosuojavaatimuksia.

Epäilemme, että sääntöjen pinnallinen lukeminen yhdistettynä harhaanjohtaviin ja perusteettomiin odotuksiin GDPR:n heikosta täytäntöönpanosta voivat vaikuttaa yritysten näkemyksiin omasta valmiudestaan.

A. Mitä fyysisiä tietoturvan ja yksityisyyden suojatoimenpiteitä GDPR vaatii?

V. GDPR on periaatteisiin pohjautuva määräys. Tämä merkitsee, että sääntelijät eivät määrää organisaatioille konkreettisia toimenpiteitä. Sen sijaan organisaatioiden tulee ajatella GDPR-vaatimusten olevan tietojen käsittelytoimenpiteiden "tavoitetila". Tämä merkitsee myös, että organisaatioiden tulee tunnistaa ja arvioida riskejä, joita niiden täytyy vähentää noudattaakseen GDPR-vaatimuksia.

Riskien tunnistamisessa yritysten täytyy ottaa huomioon tietojen käsittelijät ja erityisesti tilanteet, joissa voi tapahtua vahingollinen tai laiton siirrettyjen, varastoitujen tai muuten käsiteltyjen henkilötietojen menetys, niiden valtuuttamaton paljastus tai käyttö. Sillä ei ole väliä, johtuuko tietojen luvaton vuoto hakkerin kehittyneestä kyberhyökkäyksestä yrityksen verkkosivuja vastaan vai siitä, että ulkopuolinen ottaa työntekijän näytöltä valokuvan arkaluontoisista tiedoista. Kumpikin riski on yhtä vakava, ja molempien riskien poistamiseen tarvitaan sopivia strategioita.

K. Onko visuaalinen hakkerointi riski?

V. Totta kai. Muista: Useiden organisaatioiden tärkeät avaimet koostuvat käyttäjänimestä ja salasanasta. Nopea suojaamattoman näytön vilkaisu voi antaa valtuuttamattomalle henkilölle nämä avaimet. Riski on vielä suurempi sosiaalisen hakkeroinnin kehittymisen myötä.

Vuosi sitten eräs journalisti joutui hakkeroinnin kohteeksi työskennellessään lentokoneessa.[2] Hakkeri pystyi kuvailemaan artikkelia, jota journalisti kirjoitti, lähetettyjä sähköpostiviestejä ja tulevia kokouksia. Hakkeri kertoi kaapanneensa kaikki nämä tiedot hakkeroimalla lentokoneen Wi-Fi-verkon. Hakkeri saattoi myös vain katsoa journalistin kannettavan näyttöä. Journalisti oli vihainen, mutta ymmärsi viestin: Kun hän kirjoitti arkaluontoista artikkelia siitä, miten Apple hylkäsi FBI:n pyynnön purkaa terroristin puhelimen salaus, ja tähän mahdollisesti liittyvistä merkittävistä seurauksista tietosuojan kannalta, hän unohti suojata laitteensa yksityisyyden ja immateriaalioikeudet. Kuten tämä journalisti, myös useat organisaatiot tekevät saman virheen: He aliarvioivat kyberhakkeroinnin ja visuaalisen hakkeroinnin riskit.

K. Mitä etuja saadaan ottamalla käyttöön teknisesti yksinkertaisia fyysisiä suojaustoimia?

V. Kun uutisissa raportoidaan jatkuvasti suuren mittakaavan tietovuodoista, on helppo unohtaa, että nykyisten digitaalialan yritysten täytyy suojautua fyysisiä tietoturvauhkia vastaan. Fyysisten suojaustoimien, kuten valvontakameroiden, tietokonelaukkujen lukkojen sekä näyttöjen, kannettavien, tablettien ja älypuhelinten tietoturvasuojien käyttämisestä on paljon hyötyä. Esimerkiksi näytöissä käytettävät tietoturvasuojat ovat toimiva tapa lieventää tietosuojan ja tietoturvaloukkauksien riskejä. Haitallisen ja hyvin julkisen tietoturvaloukkauksen laukaisemiseen voi riittää, että arkaluontoiset asiakas- tai työntekijätiedot joutuvat väärien ihmisten silmien eteen.

Parhaat käytännöt voivat tukea muidenkin vaatimusten kuin GDPR:n noudattamista. Esimerkiksi muutama vuosi sitten avustaja erotettiin sairaalasta Iowan yliopistossa potilaiden tietosuojasääntöjen rikkomisen vuoksi. Häntä syytettiin työtoverin visuaalisesta hakkeroinnista, kun tämä tutki potilastietoja, mikä on HIPAA-lain rikkomus.[3]

Fyysiset suojaustoimet, kuten tietoturvasuojat, voivat muistuttaa työntekijöitä siitä, että tietoturvan ja yksityisyyden takaavat parhaat käytännöt ovat organisaatiossa tärkeitä. Lisäksi visuaalisessa tietosuojassa on aina kyse muustakin kuin vaatimustenmukaisuudesta. Kyseessä on yrityksen arvokkaan omaisuuden suojelu.

K. Kuinka yritykset voivat hyödyntää yksityisyyttä paremman asiakaskokemuksen takaamiseksi?

V. Vahvoja GDPR- ja tietosuojaohjelmia käyttävät yritykset saavat muitakin etuja kuin vaatimustenmukaisuuden. Paremman asiakaskokemuksen tarjoaminen on yksi näistä. Organisaatiosi toiminta asiakkaiden tietojen suojaamiseksi voi suoraan vaikuttaa asiakkaan luottamuksen voittamiseen tai sen menetykseen.

Tietojemme mukaan asiakkaat esimerkiksi vaihtavat kilpailevaan palveluntarjoajaan tietovuotojen seurauksena.[4] Lisäksi kuluttajien tietosuoja-asenteita käsittelevässä tutkimuksessamme korostui, että 30 prosenttia ihmisistä kieltäytyi suorittamasta tilitapahtumaa verkossa, jos he lukivat yrityksen tietosuojakäytännöstä jotain epämieluisaa.[5]

Jos sitoudut suojaamaan asiakkaiden tiedot ja työntekijät täyttävät tämän lupauksen asiakastyössä, yrityksesi voi erottua kilpailijoista edukseen.

K. Onko yrityksiä, jotka erottuvat tietosuoja- ja tietoturvasitoumuksillaan edukseen?

V. Tietosuojan painotus on muuttunut: Lakiosastojen erityisaiheesta on tullut monissa organisaatioissa ydinarvo. Nykyään muiden muassa tietohallinto- ja markkinointijohtajat uskovat tietojen hyökkäyksiltä ja väärinkäytöltä suojaamisen olevan yksi tärkeimmistä tavoitteistaan. Tutkimuksemme mukaan 23 prosenttia Fortune 100 -yrityksistä on ottanut tietosuojan osaksi yrityksen yhteisvastuuponnistuksia.[6] Noin 70 prosenttia on ottanut tietoturvan osaksi yhteisvastuuraportointiaan.

Huomasimme myös, että tietosuojaan ja tietoturvaan sitoutuneet yritykset hyötyvät, jos ne kertovat avoimesti henkilötietojen käsittelymenettelyistään. Tämä voi olla erittäin arvokas tapa lisätä asiakkaiden, työntekijöiden ja liikekumppaneiden mielenrauhaa. Mutta tämän sitoumuksen mukaisesti toimiminen ei ole yksinkertaista. Organisaatioiden täytyy usein muuttaa toimintaansa näiden sitoumusten toteuttamiseksi ja kannustaa yrityskulttuuriin, jossa tietosuoja ja tietoturva ovat ydinarvoja.

K. Onko muita GDPR:n kaltaisia määräyksiä odotettavissa?

V. Epäilemättä: GDPR on osa trendiä. Suoritimme hiljattain uuden tutkimuksen, jossa analysoitiin 54 maan tietosuojamääräyksiä ja -käytäntöjä.[7] On selvää, että esimerkiksi Aasian ja Tyynenmeren alueella GDPR:ää tarkastellaan harkittaessa paikallisten tietosuojamääräysten parantamista. Jotkin GDPR:n osat, kuten tietojen lokalisointi, ovat käytössä myös Latinalaisen Amerikan ja Venäjän tietosuojasäännöissä. Lisäksi Euroopan parlamentti on päivittämässä nykyisen sähköisen viestinnän tietosuojadirektiivin vaatimuksia. Yksityiskohtia ei ole vielä lyöty lukkoon, mutta suunnitelmana on yhdenmukaistaa sähköisen viestinnän tietosuojadirektiivin vaatimukset GDPR:n kanssa.

[1]Forrester Business Technographicsin tietoturvaselvitys, 2017
2Digital Trends, "Apple vs FBI shown in different light as journalist hacked mid-flight", 25. tammikuuta 2016
[3]Veriphyr, "Medical Assistant Fired for “Shoulder Surfing” and Breaching Patient Data Privacy", 2011
[4]Ponemon Institute, "The Impact of Data Breaches on Reputation and Share Value", toukokuu 2017
[5]Forrester Research Consumer Technographics European Online Benchmark Survey -kysely (osa 2), 2016
[6]Forrester-raportti "The Future of Data Security and Privacy: Growth And Competitive Differentiation", 2017
[7]Forrester, "Interactive Data Privacy Heat Map" -kartta, 2017

FORRESTER®