TIEKE

Tietoturvan inhimilliset riskit ja ratkaisut

Mikko Eloholma
Digiosaamisen vauhdittaja
TIEKE Tietoyhteiskunnan kehittämiskeskus ry

DiyKS – Digiosaavat yritykset ja yhteisöt Keski-Suomessa

26.04.2023

26.4. klo 15-16 | Webinaari: Tietoturvan inhimilliset riskit ja ratkaisut

Mikko Eloholma
Digiosaamisen vauhdittaja, TIEKE

Webinaarissa perehdymme tietoturvan perusteisiin ja käsittelemme mm. seuraavia aiheita.

- Tapausesimerkkejä - miksi tietoturvasta on syytä huolehtia?
- Minkälaisia ovat keskeiset tietoturvariskit yrityksille ja yhteisöille?
- Miten varautua keskeisiin inhimillisiin tietoturvariskeihin?

DiyKS-hankkeen webinaarisarja tietosuojasta ja tietoturvasta

- 18.4. Tietosuojan perusteita yrityksille ja yhteisöille
- **26.4. Tietoturvan inhimilliset riskit ja ratkaisut**

- Syksy 2023: Tietosuoja: läpinäkyvyys, informointi ja tietosuojaseloste
- Syksy 2023: Tietoturva: organisaation riskit ja ratkaisut

Keskeisiä lähteitä

- Keskuskauppakamari: Tietoturvaopas yrityksille (2016)
- Traficomin Kyberturvallisuuskeskuksen oppaat ja materiaalit
- Poliisiammattikorkeakoulun ja Jamkin CYBERDI-hankkeen materiaalit
- Webinaari: Käytännön tietoturvasuunnitelma henkilötietojen turvaamiseksi | Ismo Paananen, Agendium

Tietosuoja ja tietoturva

- **Tietosuoja** on perusoikeus, joka turvaa yksilön oikeuksien ja vapauksien toteutumisen henkilötietojen käsittelyssä.

- **Tietoturva** viittaa yleensä tietojen turvaamisen keinoihin. Voidaan ajatella, että tietoturva on myös tietosuojan toteuttamisen keino.

Tietosuoja ja tietoturva

- **Miten tietosuojasta huolehditaan?**
  - Riskien arviointi – minkälaisia riskejä yksilöihin kohdistuu henkilötietojen käsittelystä?
  - Käsittelyn tarkoitusten ja perusteiden tunnistaminen ja dokumentointi
  - Asiakkaiden ja muiden osallisten informointi esimerkiksi tietosuojaselosteella

- **Miten tietoturvasta huolehditaan?**
  - Käyttöoikeuksien hallinta yrityksen sisällä – tiedot ovat saatavilla vain niitä todella tarvitseville, ja käyttöoikeuksia myös poistetaan prosessien mukaisesti
  - Laitteiden ja palvelimien pitäminen suojattuina
  - Työntekijöiden perehdytys ohjeistusten noudattamiseen (ohjelmien päivitykset, vahvat salasanat jne.)

Tausta: Kyberturvallisuus-tilanne ja uhat

Keskeisiä tietoturvauhkia

Kyberturvallisuustilanne murroksessa?

https://helsinki.chamber.fi/suomalaisen-yrityksen-kyberturvallisuus-ukrainan-sodan-varjossa/

Dokumentointi: lähtökohta tietoturvaan ja tietosuojaan

Dokumentointi: lähtökohta tietoturvaan ja tietosuojaan

Jos organisaatio ei ole dokumentoinut sitä, *minkälaista tietoa sillä on, missä järjestelmissä tietoa on, mitä varten tietoa kerätään ja mitkä tahot (tai henkilöt) tietoa käsittelevät*, sen on hyvin vaikeaa huolehtia tietosuojasta ja tietoturvasta riittävällä tasolla.

Dokumentointi: lähtökohta tietoturvaan ja tietosuojaan

Jos organisaatio ei ole dokumentoinut sitä, *minkälaista tietoa sillä on, missä järjestelmissä tietoa on, mitä varten tietoa kerätään ja mitkä tahot (tai henkilöt) tietoa käsittelevät*, sen on hyvin vaikeaa huolehtia tietosuojasta ja tietoturvasta riittävällä tasolla.

- Ilman dokumentointia on vaikeaa määritellä esimerkiksi sitä, kenellä tulisi olla käyttöoikeudet eri tietojärjestelmiin. Näin myöskään tietoturvan riskien tunnistaminen ei onnistu.
- Kun dokumentointi tehdään huolellisesti, huolehditaan samalla myös tietosuojan **osoitusvelvollisuudesta.**

Esimerkki dokumentoinnista

Mitä ovat tietoturvan inhimilliset riskit?

Tietoturvan inhimilliset ja teknologiset riskit

Inhimilliset riskit

Huijauksiin lankeaminen,
heikot salasanat,
Puutteellinen osaaminen,
Sähköpostin huolimaton käyttö,
Laitteiden hävittäminen

Organisaation teknologiset ja hallinnolliset riskit

Ei huolehdittu työntekijöiden tunnistamisesta (esimerkiksi 2-vaiheisen tunnistaminen)
Puutteellinen ohjeistus uusien työntekijöiden perehdytykseen

Tietoturva riippuu muustakin kuin teknologiasta, **joten sitä ei voi kokonaan ulkoistaa IT hallinnolle**.

Riski 1: Tietojenkalastelu ja huijaukset

- Esimerkki: Microsoft 365 -tunnusten kalastelu
- Miten riskiin voi varautua?

Riski 2: Heikot salasanat

- Microsoft 365 -tunnusten kalastelu
- T

Riski 3: Päivitysten lykkääminen

- Microsoft 365 -tunnusten kalastelu
- T

Riski 4: Liikkuvan työn erityiset haasteet

Riski 5: Fyysisen turvallisuuden laiminlyönti

Kertaus

- Omien tietosuojan käsittelytoimien tunnistaminen ja dokumentointi on lähtökohta tietosuojasta huolehtimiselle ja **osoitusvelvollisuuden** täyttämiselle.
- Dokumentointia voi tehdä taulukkoon, ja tietovirtoja on helpointa hahmottaa visuaalisesti. Osana dokumentointia tulee pohtia **käsittelyn tarkoitukset sekä perusteet**
- **Tarkoitus** tulee määritellä itse omaan toimintaan perustuen ennen käsittelyn aloittamista. Tietoja ei saa käsitellä alkuperäisten tarkoitusten kanssa yhteensopimattomalla tavalla myöhemmin.
- Mahdolliset **käsittelyperusteita** on tietosuojalainsäädännössä määritelty 6 kpl: *rekisteröidyn suostumus, lakisääteinen velvoite, elintärkeiden etujen suojaaminen, yleistä etua koskeva tehtävä tai julkinen valta ja oikeutettu etu.*

Vinkkejä ja lukemista

- Tietosuojaapkyrityksille.fi – Kokeile itsearviointiin perustuvaa tietosuojatyökalua!
- Tietosuojaapkyrityksille.fi – Ohjesivu käsittelyperusteista
  https://www.tietosuojaapkyrityksille.fi/ohjesivut/kasittelyn-peruste/
- Suomen yrittäjät – Yrittäjän tietosuojaopas
  https://www.yrittajat.fi/oppaat/yrittajan-tietosuojaopas/
- Tietosuoja.fi – Usein kysyttyä yhdistystoiminnasta ja yhdistysopas
  https://tietosuoja.fi/usein-kysyttya-yhdistystoiminta
- Keskuskauppakamarin tietosuojaopas
  https://kauppakamari.fi/wp-content/uploads/2020/05/tietosuoja-pahkinankuoressa.-tietosuojaopas-yrityksille.verkkoversio.pdf
- Jamkin ja Poliisiammattikorkeakoulun CYBERDI-hankkeen digiturvallisuuden tietopankki:
  https://www.jamk.fi/fi/Tutkimus-ja-kehitys/projektit/CYBERDI/tietopankki/