
KANSALLISARKISTO

KANSALLISARKISTO

Tietoturva digitoinnissa

Mitä kaikkea tulee ottaa huomioon

Mikko Knutas

3.6.2025

Tietoturvan yleiset käsitteet

- Tietoturva eli tietoturvallisuus tarkoittaa tiedon saatavuuden, luottamuksellisuuden ja eheyden ylläpitämistä
- Turvattava tieto voi ilmetä useassa eri muodossa. Näitä ovat esimerkiksi digitaaliset tallenteet, fyysiset tallenteet sekä ihmisten, kuten työntekijöiden, tietämys. Tietoturva koskee tiedon suojaamista myös sen siirtämisen aikana
- Tietoturvallisuuden keskeiset tekijät ovat
    - **Eheys:** Tieto säilyy muuttumattomana ja luotettavana, eikä sitä ole muokattu luvattomasti
    - **Luottamuksellisuus**: Tiedon luottamuksellisuus tarkoittaa sitä, että vain oikeutetut käyttäjät voivat saada pääsyn tiettyyn tietoon.
    - **Saatavuus**: Tietojen saatavuus varmistaa sen, että tietoja on saatavilla oikeille käyttäjille silloin kun niitä tarvitaan.

Tietoturvan yleiset käsitteet

- Tietoturvan keskeisinä käsitteinä voidaan pitää myös seuraavia:
  - **Kiistämättömyys**: Henkilö ei voi menestyksellisesti kiistää tekoa, jonka hän on tehnyt. Kiistämättömyys riippuu viime kädessä siitä, mitä oikeudessa hyväksytään näytöksi.
  - **Tunnistus**: Henkilö (tietojärjestelmän käyttäjä) voidaan tarvittaessa liittää käyttäjätunnukseen (joka voi olla anonyymi).
  - **Todennus**: Henkilö (tietojärjestelmän käyttäjä) voidaan luottavasti tunnistaa luonnolliseksi tai oikeushenkilöksi.

Tietoturvan toteutuskeinot

- **Riskien arviointi ja hallinta**: Aloita tietoturvan toteutus riskien arvioinnilla, jossa tunnistetaan organisaation tärkeimmät tiedot ja järjestelmät sekä niihin liittyvät uhkat ja haavoittuvuudet. Sen jälkeen kehitä strategia riskien hallitsemiseksi.
- **Tietoturvapolitiikat ja -menettelyt**: Laadi selkeät tietoturvapolitiikat ja -menettelyt, jotka ohjaavat organisaation toimintaa tietoturvan suhteen. Näihin voi kuulua salasanojen hallintaohjeet, tietojen luokittelu, käyttäjätunnuksen ja salasanan käyttöoikeudet jne.
- **Koulutus ja tietoisuuden lisääminen**: Kouluta henkilöstöä tunnistamaan tietoturvaan liittyvät riskit ja noudattamaan hyviä tietoturvakäytäntöjä. Tietoisuuden lisääminen auttaa vähentämään inhimillisten virheiden aiheuttamia riskejä.
- **Vahva autentikointi**: Käytä vahvoja autentikointimenetelmiä, kuten monivaiheista tunnistautumista, varmistaaksesi käyttäjien henkilöllisyyden ja estääksesi luvattomat pääsyt.

Tietoturvan toteutuskeinot

- **Ohjelmistopäivitykset ja haavoittuvuuksien hallinta**: Päivitä ohjelmistot säännöllisesti ja seuraa tietoturvapäivityksiä, jotta mahdolliset haavoittuvuudet voidaan korjata nopeasti.
- **Tietojen salaaminen**: Salaus auttaa suojaamaan tietoa sekä siirron että tallennuksen aikana. Käytä salausta erityisesti arkaluonteisten tietojen käsittelyssä.
- **Verkon suojaus**: Käytä palomuureja, verkon valvontajärjestelmiä ja muuta verkon suojaustekniikkaa estämään luvattomat pääsyt verkkoon.
- **Varmuuskopiointi ja palautussuunnitelmat**: Tee säännöllisiä varmuuskopioita tärkeistä tiedoista ja kehitä suunnitelma tietojen palauttamiseksi hätätilanteissa, kuten tietojen menetyksen tai tietomurron tapahtuessa.

Tietosuojan yleiset käsitteet

- **Tietosuoja** on perusoikeus, joka turvaa rekisteröidyn oikeuksien ja vapauksien toteutumisen henkilötietojen käsittelyssä. Tietosuojan tarkoituksena on osoittaa, milloin ja millä edellytyksillä henkilö tietoja voidaan käsitellä.
- Henkilötietojen käsittelyn on aina perustuttava lakiin. Riippumaton viranomainen valvoo henkilötietojen suojaa koskevien säännösten noudattamista.
- Henkilötietoja ovat kaikki tiedot, jotka liittyvät tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön.
- Henkilötietoja voi olla talletettuna esimerkiksi sähköisissä tiedostoissa, tietokannoissa, paperilla, kortistossa, mapeissa tai ääni- tai kuvatallenteella.

Tietosuojan yleiset käsitteet

- Rekisteröity on henkilö, jota henkilötieto koskee.
- Rekisterinpitäjäksi kutsutaan henkilöä, yritystä, viranomaista tai yhteisöä, joka määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot.
- Henkilötietojen käsittelijäksi kutsutaan rekisterinpitäjästä ulkopuolista tahoa, joka käsittelee henkilötietoja rekisterinpitäjän lukuun.

Tiedon tunnistaminen

- Tiedot voivat olla joko julkisia tai salassa pidettäviä. Salassapidon perusteet tulevat aina lainsäädännöstä. Yleisimmin tiedot ovat salassa pidettäviä julkisuuslain 24§ perusteella, mutta salassapitoperusteita löytyy myös sektorikohtaisesta erityislainsäädännöstä (Laki viranomaisten toiminnan julkisuudesta 621/1999).
- Jos käsittelet työtehtävissäsi henkilötietoja, sinun on hyvä tuntea niihin liittyvät periaatteet ja rajoitukset. Vuonna 2018 sovellettavaksi tullut EU:n yleinen tietosuoja-asetus 2016/679 (englanniksi General Data Protection Regulation eli GDPR) asettaa raamit henkilötietojen käsittelylle. GDPR:ssä määritellään kansalaisen oikeudet henkilötietojen käsittelyyn liittyen sekä velvoitetaan rekisterinpitäjät toimimaan niin, että nämä oikeudet toteutuvat.
- Salassa pidettävän tiedon käsittelyssä on tärkeää, että tiedot liittyvät työtehtäviin ja tunnet tietojen käsittelyä koskevat ohjeet ja rajoitukset. Tietojen käsittelyä voidaan rajoittaa ja niiden käyttöä voidaan seurata tai selvittää jälkikäteen esimerkiksi lokitiedoista.

Tiedon tunnistaminen

- Valtion viranomaisten tiedot voivat olla turvallisuusluokiteltuja, jos salassapito perustuu julkisuuslain 24 §:n 1 momentin 2, 5 tai 7–11 kohtiin ja asiakirjaan sisältyvän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa maanpuolustukselle, poikkeusoloihin varautumiselle, kansainvälisille suhteille, rikosten torjunnalle, yleiselle turvallisuudelle tai valtion- ja kansantalouden toimivuudelle taikka muulla niihin rinnastettavalla tavalla Suomen turvallisuudelle.
- Turvallisuusluokitellut tiedot jaetaan neljään luokkaan, ja niihin on tehtävä luokitusmerkintä. Turvallisuusluokat ovat TL IV Käyttö rajoitettu, TL III Luottamuksellinen, TL II Salainen ja TL I Erittäin salainen. Turvallisuusluokitellun tiedon käyttöön liittyy monenlaisia rajoitteita, joista kukin viranomainen on velvoitettu ohjeistamaan omaa henkilökuntaansa. Jos käsittelet työssäsi turvallisuusluokiteltua tietoa, tarkista oikeat toimintatavat organisaatiosi ohjeistuksesta.

Tiedon elinkaari

- Tiedon tunnistamisen lisäksi tulee huomioida tiedon elinkaari, joka sisältää tiedon luonnin tai vastaanoton, säilytyksen, käytön, jakamisen ja siirron sekä arkistoinnin tai tuhoamisen. On tärkeää huomata, että tiedon tyyppi ja luokitus vaikuttavat näihin kaikkiin.
  - Luonti
    - Esimerkiksi henkilötiedon keräämisellä on aina oltava laillinen peruste, kuten suostumus tai lakisääteinen velvoite
  - Tallennus
    - Tiedon luokitus vaikuttaa myös siihen miten ja missä tietoa voidaan säilyttää. Esimerkiksi henkilötietoja tulee lähtökohtaisesti säilyttää EU/ETA-alueella
  - Käyttö
    - Salassa pidettävien ja henkilötietojen osalta on huomioitava, että käsitellään ainoastaan sellaisai tieotja, joiden käsittely on tarpeen työtehtävien suorittamiseksi

Tiedon elinkaari

- Jakaminen
  - Tiedon luokitus vaikuttaa myös siihen kenelle tietoa saa jakaa
- Arkistointi
  - Tiedolla voi olla lakisääteisiä säilytysaikoja
- Tuhoaminen
  - Säilytysajan äätyttyä tieto pitää tuhota luetettavalla tavalla. Esim julkinen aineisto voidaan toimittaa normaaliin paperinkierrätykseen, mutta salassa pidettävien tai henkilötietojen osalta tulee noudattaa tietoturvallisia hävitystapoja

Tiedon käsittely

- Tiedon tyyppi vaikuttaa siihen miten ja missä tiloissa sitä voidaan käsitellä
- Julkisissa tiloissa voi käsitellä vain julkista tietoa
- Tilat, joissa käsitellään salassa pidettävää tietoa, on yleensä rajattu organisaation henkilöstölle.
- Henkilöiltä saatetaan edellyttää turvallisuusselvitystä.
- Tiloissa kulkevat tuntemattomat henkilöt pitää pystyä tunnistamaan.
- Tilat, joissa käsitellään turvaluokiteltuja tietoja, on rajattu vielä tiukemmin. Näihin tiloihin pääsee yleensä vain pieni osa henkilöstöstä.

Tietojen varmuuskopiointi

- Tietojen varmuuskopiointi on keskeinen osa tietoturvaa ja riskinhallintaa. Se tarkoittaa tietojen kopioimista ja tallentamista erilliselle säilytysvälineelle tai palvelimelle varmuuden vuoksi, jotta ne voidaan palauttaa alkuperäiseen tilaansa, jos alkuperäiset tiedot vahingoittuvat, tuhoutuvat tai muuttuvat käyttökelvottomiksi.
    - **Säännöllisyys:** Tietojen varmuuskopiot tulisi tehdä säännöllisesti, jotta varmistetaan, että mahdolliset tietojen menetykset voidaan minimoida. Useimmissa tapauksissa päivittäiset tai viikoittaiset varmuuskopiot ovat suositeltavia.
    - **Tärkeiden tietojen tunnistaminen**: On tärkeää tunnistaa ne tiedot, jotka ovat kriittisiä liiketoiminnalle tai joita ei ole helppo korvata, ja varmuuskopioida ne ensisijaisesti.
    - **Varmuuskopiointimenetelmät:** On olemassa erilaisia varmuuskopiointimenetelmiä, kuten täydelliset varmuuskopiot, differentiaalivarhaiset ja inkrementaaliset varmuuskopiot. Organisaation tulisi valita sopiva menetelmä riippuen sen tarpeista, tallennustilan saatavuudesta ja tietojen koon kasvusta.

Tietojen varmuuskopiointi

- **Säilytyspaikka**: Varmuuskopiot tulisi tallentaa erilliselle säilytysvälineelle tai -paikalle, joka on suojattu fyysisiltä ja digitaalisilta uhkilta. Tämä voi sisältää ulkoisia kiintolevyjä, pilvipalveluja tai offsite-varastointipaikkoja.
- **Testaus ja varmuuden tarkistaminen**: Varmista, että varmuuskopioita voidaan palauttaa onnistuneesti tarvittaessa. Säännölliset testit auttavat varmistamaan, että varmuuskopioprosessi toimii ja että tiedot voidaan palauttaa asianmukaisesti.
- **Automaatio:** Automaattiset varmuuskopiointityökalut ja -ohjelmistot voivat helpottaa varmuuskopiointiprosessin hallintaa ja varmistaa, että varmuuskopiot suoritetaan säännöllisesti ilman manuaalista interventiota.
- **Tietojen elinkaaren hallinta**: Tietojen varmuuskopiointi tulisi ottaa huomioon osana tietojen elinkaaren hallintaa, joka sisältää tietojen tallentamisen, käytön, arkistoinnin ja hävittämisen.

Tietoturvan tekniset toimet

- **Palomuurit**: Palomuurit ovat tietoturvalaitteistoja tai -ohjelmistoja, jotka valvovat ja rajoittavat tietoliikennettä verkossa. Ne voivat estää luvattomat pääsyt ja suojata järjestelmiä haittaohjelmilta.
- **Virustorjuntaohjelmistot**: Virustorjuntaohjelmistot suojaavat tietokoneita ja järjestelmiä haittaohjelmilta, kuten viruksilta, madoilta ja troijalaisilta, skannaamalla ja tunnistamalla uhkia ja poistamalla ne.
- **Salaus**: Salaus on prosessi, jolla tieto muunnetaan muotoon, joka on vaikea ymmärtää ilman oikeaa purkavaintoa
- **Pääsynvalvonta:** Pääsynvalvonta rajoittaa käyttäjien pääsyä tietoihin ja järjestelmiin tarpeen mukaan. Tämä voi sisältää käyttäjätunnuksen ja salasanan käytön, kaksivaiheisen todennuksen, roolipohjaisen pääsynhallinnan ja auditointipolitiikkojen määrittämisen.

Tietoturvan tekniset toimet

- **Sovellusten turvallisuus:** Käytä luotettavia ohjelmistoja ja sovelluksia, ja varmista, että ne päivitetään säännöllisesti. Haavoittuvuudet ohjelmistoissa ovat yleisiä, ja päivitykset sisältävät usein korjauksia tunnetuille haavoittuvuuksille.
- **Koulutus ja tietoisuus**: Kouluta henkilöitä tunnistamaan tietoturvauhat ja -riskit sekä noudattamaan hyviä tietoturvakäytäntöjä. Tietoturvavaroitukset, kuten kalasteluviestit, voivat olla merkittävä riski organisaatiolle.
- **Jatkuva seuranta ja arviointi**: Seuraa jatkuvasti järjestelmien ja verkon toimintaa sekä suorita säännöllisiä tietoturvatestauksia ja auditointeja tunnistamalla mahdollisia haavoittuvuuksia ja suojaustoimenpiteiden tehokkuutta.
- **Kumppanien ja toimittajien tietoturva:** Arvioi myös kumppaneiden ja toimittajien tietoturvakäytäntöjä varmistaaksesi, että heidän järjestelmiensä ja palveluidensa tietoturva täyttää tarpeesi ja vaatimuksesi.

Esitys on toteutettu osana Kaakkois-Suomen ammattikorkeakoulu Xamk:n, Ammattiopisto Samiedun ja Kansallisarkiston yhteishanketta JoDi-Joustavat koulutus ja työelämäpolut tulevaisuuden digitointiosaajille (ESR+ 2023-2025).

SAMiEDU
KANSALLISARKISTO
Elinkeino-, liikenne- ja ympäristökeskus
Euroopan unionin osarahoittama
XAMK

KANSALLISARKISTO

www.kansallisarkisto.fi

@kansallisarkisto

@kansallisarkist