Laki julkisen hallinnon tiedonhallinnasta Suosituskortti	B
13 § 2 mom Vikasietoisuus ja toiminnallinen käytettävyys	versio 0.9/16.4.2021

13 § Tietoaineistojen ja tietojärjestelmien tietoturvallisuus
4 luvun 13 § 2 mom

Viranomaisen tehtävien hoitamisen kannalta **olennaisten tietojärjestelmien vikasietoisuus** ja **toiminnallinen käytettävyys** on varmistettava riittävällä testauksella säännöllisesti.

Perustelumuistio
https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_284+2018.aspx

Olennaiset tietojärjestelmät kartoitetaan laatimalla tietojärjestelmille kriittisyysluokitus. Luokituksessa on huomioitava lakisääteiset tehtävät sekä riippuvuus muista järjestelmistä (oman organisaation sisällä sekä viranomaisten kesken).

Vikasietoisuuden varmistaminen tapahtuu **esimerkiksi** joillakin alla kuvatuista menetelmistä

- testaus ennen käyttöönottoa sekä merkittävien ylläpitotoimien yhteydessä,
    - testauksen laajuus ja toteutustapa valitaan järjestelmän riski-/kriittisyysluokituksen mukaisesti,
    - testataan, että tietoturvallisuus on toteutettu ennalta määritettyjen vaatimusten mukaisesti,
- järjestelmätestaus ja hyväksymistestaus; tietoturvallisuuteen liittyvät käyttötapaukset,
- kuormitustestaus,
- koodikatselmoinnit,
- haavoittuvuusskannaukset tai automatisoidut tietoturvatestaukset.

Testauksista pitää syntyä raportteja, joista selviää mitä on testattu ja millaisia tuloksia testauksessa on saatu.

Tietoturvatestausta voidaan toteuttaa esimerkiksi seuraavia standardeja vasten,

- Sovelluksen tietoturvallisuus
    - OWASP Application Security Verification Standard (ASVS)
        - Varmennustaso (1-3) valitaan sovelluksen kriittisyyden tai sensitiivisyyden perusteella
- Mobiilisovelluksen tietoturvallisuus
    - OWASP Mobile Application Security Verification Standard (MASVS)
        - Varmennustaso (L1 tai L2) ja vaatimus sovelluksen resilienssistä (-R-) valitaan sovelluksen käsittelemien tietojen sensitiivisyyden perusteella
- IoT-laitteen tietoturvallisuus
    - OWASP IoT Security Verification Standard (ISVS)
        - Varmennustaso (1-3) valitaan laitteen kriittisyyden tai sen käsittelemien tietojen sensitiivisyyden perusteella
- Alustan (Käyttöjärjestelmä ja Middleware) tietoturvallisuus
    - Center for Internet Security (CIS) benchmarkit

- Varmennustaso (1 tai 2) valitaan järjestelmän kriittisyyden tai sensitiivisyyden perusteella

Hankittaessa sovelluksia, järjestelmiä, palveluita tai sovelluskehitystyötä ulkoisilta toimittajilta, kannattaa sopimuksessa vaatia asiaankuuluvien edellä mainittujen standardien ja näihin liittyvien varmistustasojen täyttymistä.

Tietoturvatestausta kannattaa lisäksi erityisesti kohdistaa mahdollisessa uhkamallinnuksessa (esim. STRIDE-TRIM, Uhkapuu, tietovuo) tunnistettuihin merkittävimpiin uhkiin.

Tietoturvatestausta voidaan toteuttaa esimerkiksi seuraavien ohjeiden mukaisesti:
- OWASP Web Security Testing Guide
- OWASP Mobile Security Testing Guide
- The Open Source Security Testing Methodology Manual (OSSTMM)
- Secure Coding Guidelines For Java (koodikatselmointi)

Tietoturvatestausta voidaan toteuttaa esimerkiksi seuraavien osapuolten toimesta:
- Dedikoidut tietoturvatestaajat, esim.
  - Tekninen tietoturvatestaus tietoturvatestaustyökaluja hyödyntämällä (haavoittuvuustestaus)
  - Tunkeutumis-/penetraatiotestaus
  - Red teaming (tunkeutumistestaus laajalla skopella ja aikaikkunalla)
- Ohjelmistotestaajat / QA, esim.
  - Pääsynhallinnan testaaminen (Tunnistaminen, valtuutus, lokitus)
  - Käyttötapaukset ja väärinkäyttötapaukset
  - Yleisten syötteentarkistusten testaus
  - Businesslogiikan ohitusten testaus
- Automaattinen tietoturvatestaus, CI/CD, esim.
  - Dynaamiset ja staattiset koodiskannerit
  - Automatisoidut käyttö- ja väärinkäyttötapaukset (esim. Selenium, Robot Framework)
  - Automatisoidut haavoittuvuusskannaukset ja haavoittuvuustestaukset (proxyt)

Määritettäessä haavoittuvuustestauksen löydösten kriittisyyttä on syytä käyttää standardoitua menetelmää kuten CVSS:ää (Common Vulnerability Scoring System) ja määritellä sekä toimitusportteihin että toimitussopimuksiin tiukemmat vaatimukset sen perusteella onko kyseessä matalan, keskitason vai korkean luokan haavoittuvuus. Esimerkiksi korkean luokan haavoittuvuudet on syytä korjata heti ja näiden kanssa ei oletuksena kannata edetä tuotantoon kun taas alemman luokan haavoittuvuuksien osalta voidaan tapauskohtaisesti hyväksyä näihin liittyvää matalampaa riskiä (ainakin väliaikaisesti).

Toiminnallisen käytettävyyden turvaamiseksi on varmistettava, että
- tietojärjestelmä on helposti opittava
- sen toimintalogiikka on helposti muistettava
- sen toiminta tukee niitä työtehtäviä, joita käyttäjän pitää tehdä tietojärjestelmällä ja
- tietojärjestelmä edistää sen käytön virheettömyyttä

Tämä toteutetaan mm. seuraavilla tavoilla

- räätälöidyissä järjestelmissä käytettävyyden määrittely ja suunnittelu tehdään organisaation hyväksytyn menetelmän mukaan. Toteutuksen käytettävyyttä on testattava jatkuvasti kehittämisen aikana.
- valmisohjelmistoissa on toteutettava käytettävyystestaus hyväksymistestauksen yhteydessä
- testaus on toteutettava eri käyttäjäryhmien näkökulmasta
- käytettävyystestausta voidaan tehdä jo hankintavaiheessa, jolloin voidaan paremmin varmistaa hankittavan järjestelmän soveltuvuus käyttötarpeeseen

Jotta tietojärjestelmän tietosuoja voidaan toteuttaa asianmukaisesti ja käyttäjälähtöisesti, on tämä suunniteltava alusta lähtien hyödyntäen oletusarvoisen tietosuojan ja yksityisyydensuojan periaatteita.

Oletusarvoisen tietosuojan periaatteiden mukaisesti tietosuoja täytyy huomioida heti tietojärjestelmän suunnittelun alkuvaiheesta, siten että henkilötietojen käsittely suojataan alusta lähtien ja näiden tietosuoja maksimoidaan esimerkiksi minimoimalla käsiteltävän tiedon määrä sekä talletusaika ja suojaamalla mahdollisuuksien mukaan tieto salauksen tai pseudonymisoinnin avulla.

Oletusarvoisen yksityisyydensuojan seitsemän perusperiaatetta ovat seuraavat:

- Se on proaktiivista, ei reaktiivista; estävää, ei korjaavaa
- Oletusasetukset takaavat yksityisyydensuojan
- Yksityisyydensuoja on sisäänrakennettu järjestelmään (designiin)
- Käyttäjälle tarjotaan täysi toiminnallisuus tinkimättä yksityisyydensuojasta – positiivista, ei nollasummapeliä
- Turvallisuus taataan päästä-päähän, tiedot on suojattu koko elinkaaren ajan
- Näkyvyys ja läpinäkyvyys - pidetään tietojen käsittely avoimena
- Kunnioitetaan käyttäjien yksityisyyttä - pidetään tietojen käsittely käyttäjäkeskeisenä

Erityisesti on varottava ettei järjestelmän suunnittelussa hyödynnetä ns. 'Dark patterneita' eli esimerkiksi käyttöliittymätoteutuksia, joilla tietoisesti pyritään saamaan käyttäjä luopumaan yksityisyydensuojastaan tai heikentämään tätä.

Suunniteltaessa ja testatessa järjestelmän toiminnallisuutta tietosuojan näkökulmasta on tärkeää huomioida erityisesti seuraavat näkökulmat:

- Hakutoiminnallisuus ei saa vuotaa valtuuttamattomille käyttäjille tietoa, josta voidaan tehdä päätelmiä tai johtaa rekisteröityjen henkilötietoja
- Liitetiedostot (kuvat, videot, toimistodokumentit, jne.) pitävät usein sisällään näkymätöntä metadataa (esim. Sijaintikoordinaatit, tunnistetietoja) - on syytä arvioida, voidaanko nämä poistaa automaattisesti tai muuten varmistaa, että nämä eivät päädy luvattomille tahoille
- Käyttäjän päätelaitteella voidaan tallettaa ei-välttämätöntä tietoa vain käyttäjän suostumuksella
- Suostumuksen keräämisen tulee olla yksiselitteinen ja aktiivinen tahdonilmaisu ja tämä tulee kerätä erikseen eri tarkoituksiin eikä yhdistää esimerkiksi käyttöehtojen hyväksymiseen
- Käyttäjää täytyy informoida läpinäkyvästi henkilötietojen käsittelystä käyttäen ymmärrettävää kielenkäyttöä

Sähköisten palveluiden toiminnallista käytettävyyttä toteutettaessa pitää huomioida myös EU:n saavutettavuusdirektiivi ((EU) 2016/2102) ja sitä seuraava kansallinen lainsäädäntö (Laki digitaalisten palveluiden tarjoamisesta 306/2019). Saavutettavuusdirektiivin soveltamisalaan kuuluvat julkisen

Laki julkisen hallinnon tiedonhallinnasta Suosituskortti	B
13 § 2 mom Vikasietoisuus ja toiminnallinen käytettävyys	versio 0.9/16.4.2021

	hallinnon ja julkista hallintotehtävää hoitavien organisaatioiden verkkosivustot ja mobiilisovellukset sekä lähes kaikki näiden sisällöt.