DIGI- JA VÄESTÖTIETO-VIRASTO

Opas teknologiatuotteiden turvallisuuden arviointiin

VAHTI hyvät käytännöt tukimateriaali

30.10.2023

Puh. **0295 536 000** (vaihde) | Yhteystiedot, katso **www.dvv.fi**

Sisällysluettelo

Opas teknologiatuotteiden turvallisuuden arviointiin

1 Yleistä

Tämä opas on tarkoitettu vapaasti hyödynnettäväksi ja sovellettavaksi tukimateriaalina. Sen tarkoituksena on avustaa valmiiden teknologiatuotteiden, kuten ohjelmistojen, palveluiden ja laitteiden turvallisuuden alustavassa arvioinnissa.

Laite- ja ohjelmistopohjaisten ratkaisujen valikoima on laaja ja niiden tietoturvan taso vaihtelee suuresti. Valmiin teknologiatuotteen arvioinnissa tulee ottaa huomioon mahdollisuuksien mukaan tuotteen ominaisuudet, valmistajan maine sekä tuotteen nykyinen tietoturvatilanne, pitäen sisällään tunnetut haavoittuvuudet. Myös tuotteen kehittämisvaiheen tietoturvatyöhön on syytä kiinnittää huomiota, sillä puutteet siinä ennakoivat sitä, kuinka paljon ja kuinka vakavia käytön aikaisia tietoturvaongelmia tuotteessa mahdollisesti ilmenee.

Teknologiatuotteiden arviointia on tarkasteltu oppaassa usean eri osa-alueen kautta. Jokaisella niistä pyritään tuomaan esiin, millaiset ominaisuudet tai seikat osoittavat hyvää tietoturvan tasoa ja ovat suositeltavia, sekä sitä, mitkä puolestaan ovat vältettäviä, tietoturvariskejä lisääviä ominaisuuksia tai asioita. Ulkopuolisia lähteitä, esimerkkejä ja viitteitä on esitetty tarpeen mukaan.

Voit antaa palautetta tästä tukimateriaalista lähettämällä sähköpostia osoitteeseen digiturva@dvv.fi.

2 Valmiin tuotteen arviointi

Tässä luvussa käydään läpi valmiin, mahdollisesti harkittavan ohjelmisto-, palvelu- tai laiteratkaisun arviointia useista eri näkökulmista. Nämä näkökulmat kattavat valmistajan aikaisemman toiminnan sekä itse tuotteen aikaisemman historian tietoturvaongelmien osalta. Arvioinnin tueksi on koostettu vinkkejä, joilla tuotteesta voidaan etsiä tietoturvan kannalta haitallisia tai kyseenalaisia toiminnallisuuksia.

2.1 Maine ja historia

2.1.1 Valmistajaan kohdistuva lainsäädäntö

Silloin kun ohjelmistolla tai laitteella käsiteltäviin tietoihin voidaan ajatella kohdistuvan merkittävää ulkopuolista valtiollista mielenkiintoa, on syytä ottaa huomioon ohjelmisto- ja laitetoimittajan kotimaa ja laitteiston tuotantomaa sekä näihin liittyvä kansallinen lainsäädäntö. Esimerkiksi pilvipalvelut tai IoT-laitteiden hallintapalvelut voivat olla ulkomaisen lainsäädännön piirissä, jolloin palveluun tallennettavat tiedot altistuvat suoralle ulkomaiselle lainkäytölle. Paikallinen lainsäädäntö voi sisältää kirjauksia esimerkiksi paikallisen turvallisuustoimijan pääsystä palvelussa sijaitsevaan tietoon.

Teknologiatuotteen valmistusmaan kansallisen lainsäädännön ja kyberkyvykkyyksien vaikutuksia itse tuotteen tietoturvallisuuteen on usein hankalaa arvioida. Avoimista lähteistä löytyy kuitenkin arvioita, uutisointia sekä tutkimuksia, joita voi hyödyntää arvioinnin tukena. Esimerkiksi *Harvard Kennedy School, Belfer Center for Science and International Affairs* julkaisee säännöllisesti useaan osa-alueeseen jaettua kartoitusta valtiollisista kyberkyvykkyyksistä ja niiden käyttämisestä erilaisiin tarkoituksiin[1].

Huomioitavia seikkoja:

- Tunnetut, valmistajan tarkoituksellisesti asettamat takaportit tai haavoittuvuudet sovelluksissa, verkkolaitteissa, IoT -laitteissa[2] tai muissa komponenteissa.
- Takaportit ja tarkoitukselliset haavoittuvuudet avoimessa lähdekoodissa:
    - Esimerkiksi versionhallinta-alustaa ohjelmistoprojekteille tarjoava *Github* huomautti vuonna 2020 avoimen lähdekoodin nykytilaa käsittelevässä *Octoverse*-raportissaan, että jopa 17 % tietoturvahaavoittuvuuksista sen sisältämissä avoimissa lähdekoodeissa on tahallisesti tehtyjä[3].
    - Vaikeasti havaittavien tietoturvahaavoittuvuuksien lisääminen avoimen lähdekoodin ohjelmistoon on helppo tapa luoda takaportti kaikkiin ohjelmistoihin, jotka käyttävät kyseistä avoimen lähdekoodin komponenttia osana ohjelmistoaan.

[1] https://www.belfercenter.org/sites/default/files/files/publication/CyberProject_National%20Cyber%20Power%20Index%202022_v3_220922.pdf
[2] ”Internet of Things” -laitteet ovat älykkäitä laitteita ja järjestelmiä, jotka muodostavat yhteyden internettiin, ja joiden käyttöä voidaan säätää ja ohjata internetin kautta
[3] https://octoverse.github.com/2020/

- Avoimen lähdekoodin kirjastojen käyttäminen osana ohjelmistoa on yleistä myös kaupallisissa ohjelmistoissa.

2.1.2 Valmistajan ja tuotteen yleinen maine

Valmistajan ja tuotteen yleinen maine kertoo valmistajan pitkän aikavälin sitoutumisesta tietoturvallisuuteen, samoin kuin onnistumisesta siinä.

Suositeltavaa	Vältettävää
Valmistaja on sitoutunut tuotteen kehittämiseen ja tuotteen elinkaari on yleisesti tiedossa.	Valmistajan tuote on tuotekehityksessä tai pilottivaiheessa tai tuote on elinkaaren lopussa.
Valmistajalla on pitkäaikainen, positiivinen maine tietoturva-asioissa	Valmistajalla on historiaa tietoturvaloukkauksista tai -ongelmista.
Tuote on saanut positiivista palautetta riippumattomilta tietoturva-asiantuntijoilta.	Mikäli tuote on uusi markkinoilla eikä sen valmistajalla ole vakiintunutta mainetta, tulee tuotteen käytön muodostamien riskien arviointiin kiinnittää erityistä huomiota.
Valmistaja päivittää säännöllisesti tuotteensa tietoturvaominaisuuksia.	Negatiiviset arviot tai raportit tuotteen tietoturvasta.
Tuote on laajasti useamman organisaation käytössä.	Valmistaja ei tarjoa ohjeistusta tuotteen turvallisuusominaisuuksien hallinnasta ja turvallisesta käytöstä.

2.2 Haavoittuvuudet

Haavoittuvuudet ovat ohjelmointivirheitä, joilla on tietoturvaseuraamuksia. Julkisesti tiedossa olevat, korjaamattomat haavoittuvuudet ovat yksi tavallisimmista syistä vakaviin tietoturvapoikkeamiin ja tietomurtoihin.

Ohjelmointivirheet ovat väistämätön seuraus ohjelmistojen monimutkaisuudesta. Järjestelmiä, jotka ovat käytännössä virheettömiä (tai joissa virheen todennäköisyys on äärimmäisen pieni) on kuitenkin mahdollista rakentaa. Tällaisia ovat esimerkiksi avaruusluotainten ohjelmistot ja lentokoneiden automaattiohjausjärjestelmät. Niiden tuotantokustannukset ja usein myös operointikustannukset ovat kuitenkin kohtuuttoman korkeat arkikäyttöä ajatellen.

Käytännössä jokaisessa normaalikäytössä olevassa ohjelmistossa voidaan siis ajatella olevan tietoturvahaavoittuvuuksia. Tällöin tuotteen turvallisuutta määrittää sekä alkuperäisen työn laatu että löydettyjen haavoittuvuuksien korjausnopeus. Laitteistojen osalta on hyvä huomioida, että itse laitteistoraudassa, joita ovat esimerkiksi prosessorit ja piirisarjat, olevia haavoittuvuuksia voi olla hyvin vaikea tai mahdoton korjata.

Haavoittuvuuksien pisteytyksessä käytetään Common Vulnerability Scoring System (CVSS) -standardia, jossa asteikko on välillä 0 (ei riskiä) – 10 (kriittinen). Kokonaispisteytystä muodostettaessa on huomioitu useita eri näkökohtia. Virallinen määrittelydokumentti löytyy tietoturvaloukkauksien reagointikyvykkyyden nostoon liittyvään, globaaliin yhteistyöhön keskittyvän *FIRST-foorumin*[4] sivuilta. Kohtuullisen tiivis ja helppolukuinen yhteenveto CVSS-pisteytysjärjestelmästä löytyy esimerkiksi tietoturvakoulutuksistaan tunnetun SANS-yhtiön blogista[5].

Suositeltavaa	Vältettävää
Valmistajan reagointi raportoituihin haavoittuvuuksiin on järjestelmällinen ja nopea.	Avoimet haavoittuvuudet.
Havaituista haavoittuvuuksista ja niiden korjauksista on selkeä dokumentointi.	Puutteellinen dokumentointi korjatuista haavoittuvuuksista.
Valmistaja päivittää säännöllisesti tuotteensa tietoturvaominaisuuksia.	Korjausten viivästyminen.
Valmistaja tiedottaa laajasti ja avoimesti tuotteissaan havaituista haavoittuvuuksista ja niiden korjauksista.	Toistuvat, samankaltaiset haavoittuvuudet, mikä osoittaa ongelmia joko tuotteen suunnittelussa ja arkkitehtuurissa tai haavoittuvuuksien korjausprosessissa.
Valmistaja seuraa aktiivisesti haavoittuvuustietokantoja.	

2.2.1 Haavoittuvuuksien ja niiden korjaushistorian arviointi

Muun muassa Liikenne- ja viestintävirasto Traficom ylläpitää tietokantaa tunnetuista haavoittuvuuksista. Tietokanta löytyy Traficomin Kyberturvallisuuskeskuksen sivuilta[6]. Lisäksi on suositeltavaa tarkkailla tuotteen tai ohjelmiston valmistajan itse julkaisemia tietoturva- ja haavoittuvuusilmoituksia.

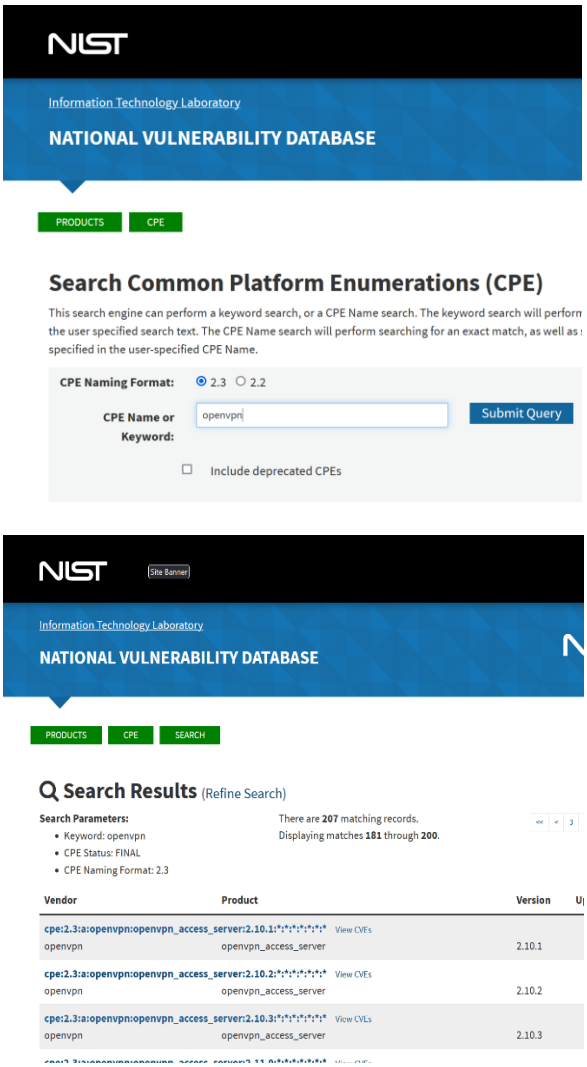
Tietoa avoimista ja korjatuista haavoittuvuuksista sekä haavoittuvuushistoriasta voi hakea myös laajoista avoimista haavoittuvuustietokannoista. Haavoittuvuuksia kannattaa hakea esimerkiksi tuotteen ja valmistajan nimellä tai myös tuotteen tarkalla versionumerolla. Hakumahdollisuudet vaihtelevat eri sivustoilla. Yksi tunnetuimpia avoimia haavoittuvuustietokantoja on yhdysvaltalaisen National Institute of Standards and Technologyn ylläpitämä NVD-tietokanta (engl. *National Vulnerability Database*)[7].

NVD-sivustolla julkaistut haavoittuvuudet ovat peräisin vuonna 1999 perustetun CVE (engl. *Common Vulnerabilities and Exposures)* -hankkeen tietokannasta, joka sisältää

[4] https://www.first.org/cvss/
[5] https://www.sans.org/blog/what-is-cvss/
[6] https://www.kyberturvallisuuskeskus.fi/fi/haavoittuvuudet
[7] https://nvd.nist.gov/

katalogin tunnetuista haavoittuvuuksista ja niiden tiedoista[8]. Tietokantaa ylläpitää voittoa tavoittelematon tutkimusorganisaatio MITRE. Oppaan kirjoitushetkellä sivustolla on meneillään siirtymä uuteen CVE – sivustoon.[9]

Hakuesimerkki NVD-sivustoa käyttäen tietystä tuotteesta ja sen tietystä versiosta:



Haun tuloksena saadaan listaus kyseisen tuotteen tietyssä versiossa havaituista haavoittuvuuksista. Listauksesta voidaan edelleen edetä tarkastelemaan yksittäisten haavoittuvuuksien ominaisuuksia ja korjaushistoriaa.

2.2.2 Säännöllisten tietoturvapäivitysten historia

Säännöllinen tietoturvapäivitysten historia kuvastaa organisaation kykyä ja sitoutumista jatkuvaan tietoturvatyöhön ja ennustaa haavoittuvuuksien tasaista korjaustyötä jatkossakin. Tietoturvapäivitysten historiaa voidaan arvioida muun muassa

[8] https://cve.mitre.org/
[9] https://www.cve.org/

tutustumalla valmistajan tietoturvapäivityskäytäntöihin sekä päivitysten säännöllisyyteen. Lisäksi julkisista lähteistä saatavat tiedot päivitysten ongelmista auttavat arvioinnin tekemisessä.

Suositeltavaa	Vältettävää
Säännölliset ja ajantasaiset päivitykset.	Päivitysten laiminlyönti tai viivästyminen.
Helposti tarkistettavissa oleva päivityshistoria.	Dokumentoinnin puute tehdyistä päivityksistä.
Nopea reagointi kriittisiin haavoittuvuuksiin ylimääräisillä tietoturvapäivityksillä päivityskalenterin ulkopuolella.	Päivitysten epäonnistumiset ja keskeytykset.
Säännöllinen ja reaaliaikainen raportointi havaittujen ja korjattujen tietoturvapäivitysten tilanteesta.	

2.3 Suoritetut tietoturvatarkistukset

Teknologiatuotteiden tietoturvatarkastukset ja -sertifioinnit, etenkin ulkopuolisten tahojen suorittamana, ovat erinomaisia lähteitä tuotteen turvallisuuden tilan arviointiin. Yhtä tärkeää arvioinnin kannalta on tietää, tehdäänkö tarkastuksia ylipäätään ja kuinka säännöllisesti niitä tehdään.

Tietoturvatarkastuksia voidaan arvioida muun muassa valmistajan tarkastuksista antamien tietojen sekä julkisista lähteistä saatavien loppuraporttien ja yhteenvetojen perusteella.

Suositeltavaa	Vältettävää
Valmistajan säännölliset sisäiset tietoturvatarkastukset.	Tietoturvatarkastuksia ei ole tehty lainkaan.
Valmistajan säännölliset ulkoiset tietoturvatarkastukset, etenkin ennen uusien tuotteiden tai merkittävien versioiden julkistusta.	Tietoturvatarkastusten sisältöä tai raporttia ei ole saatavilla.
Tietoturvatarkastusten loppuraportit tai yhteenveto ovat julkisesti saatavilla.	Tietoturvatarkastuksissa on havaittu puutteita, joita ei ole korjattu.

2.4 Käytetyt teknologiat

Riippumatta itse tuotteen ominaisuuksista, myös tuotteessa hyödynnetyt teknologiset valinnat vaikuttavat sen turvallisuuteen. Erityistä huomiota kannattaa kiinnittää käytettyihin ohjelmistokirjastoihin, tietoliikenneprotokolliin sekä salausteknologiaan ja salausalgoritmeihin.

Ohjelmistokehyksien ja kirjastojen turvallisuutta voi arvioida niissä raportoitujen haavoittuvuuksien kautta samaan tapaan kuin valmiiden tuotteiden osalta. Ohjelmointikielien turvallisuutta voi arvioida julkisista lähteistä saatavan tiedon perusteella.

Salaukseen ja autentikointiin liittyvien suositeltujen algoritmien ja avainpituuksien tarkistamiseen soveltuvia lähteitä ovat mm.

- Liikenne- ja viestintävirasto Traficomin NCSA-toiminnon hyväksymät salausratkaisut
- Traficomin kansalliset kryptografiset vähimmäisvaatimukset turvallisuusluokkien IV-III tiedon välittämiseen TLS-salatusti (esimerkiksi HTTPS).

Salausalgoritmeissa ja -protokollissa tunnistettuja haavoittuvuuksia julkaistaan yleisissä haavoittuvuustietokannoissa. Ohjelmisto- ja laitevalmistajien tulisi tarjota korjaukset tuotteidensa käytössä oleviin haavoittuviin tai vanhentuneisiin salausalgoritmeihin ja -protokolliin ilman viivytystä.

Suositeltavaa	Vältettävää
Tuotteessa hyödynnetty teknologia on dokumentoitu ja dokumentaatio on saatavilla.	Ohjelmistokehykset, ohjelmointikielet ja -kirjastot, joiden historiassa on esiintynyt toistuvasti vakavia haavoittuvuuksia.
Teknologiassa on käytetty turvalliseksi tunnettuja ohjelmistokehyksiä, ohjelmointikieliä ja -kirjastoja.	Epästandardit tai itse kehitetyt tietoturvaprotokollat ja salausalgoritmit.
Teknologiassa käytetyt salausalgoritmit ja niiden avainpituudet on selkeästi dokumentoitu.	Epäselvyydet avainpituuksissa ja käytetyissä algoritmeissa.
Teknologiassa on käytetty yleisesti hyväksyttyjä salausalgoritmeja, avainpituuksia ja tietoturvaprotokollia.	
Valmistajan tiekartta salausalgoritmien ja avainpituuksien kehittämiseksi on erikseen pyydettäessä saatavilla.	
Tuotteessa käytetty teknologia, kuten salausalgoritmit tai autentikointiratkaisut ovat jälkikäteen päivitettävissä tai	

vaihdettavissa kyseisen teknologian kehittyessä.	

2.5 Tuotteen toiminta

Tässä kappaleessa tarkastellaan ohjelmiston tai laitteen käytön aikaisen käyttäytymisen arviointia ja sen vaatimien käyttöoikeuksien vaikutusta tietoturvaan.

2.5.1 Ohjelmiston tai laitteen vaatimat käyttöoikeudet

Ohjelmistojen tai laitteiden vaatimien käyttöoikeuksien arviointi vaatii kriittistä tarkastelua erityisesti käyttöoikeuksien tarpeellisuuden osalta. Hyvä ja kattava dokumentaatio ohjelmiston toimintaperiaatteista auttaa arvioimaan käyttöoikeuksien tarvetta.

Suositeltavaa	Vältettävää
Sovelluksen tai ohjelmiston käyttö vaatii vähimmäisominaisuuksia ja sovellus pääsee käsiksi vain tarvitsemiinsa resursseihin.	Pyydettyjen käyttöoikeuksien yleinen perustelemattomuus ja niiden käyttötarkoituksen dokumentoimattomuus.
Käyttöoikeudet on dokumentoitu ja hyvin perusteltu.	Toimintaan nähden tarpeettoman tuntuiset oikeudet, joille ei löydy perusteita, etenkin: • Vaatimukset pääkäyttäjän oikeuksista. • Oikeudet kameran, mikrofonin tai muiden oheislaitteiden käyttöön. Oikeudet vapaaseen pääsyyn kaikkialle tiedostojärjestelmässä.
Käyttöoikeuksien muutokset vaativat hyväksynnän.	Automaattiset päivitykset, jotka pystyvät muuttamaan käytössä olevia oikeuksia ilman erillistä hyväksyntää.

2.5.2 Ohjelmiston tai laitteen tietoliikenne

Ohjelmiston tai laitteen tietoliikenteen osalta on hyvä ymmärtää sen käyttämän tietoliikenteen tarkoitus ja se, ovatko muodostetut tietoliikenneyhteydet salattuja. Tietoliikenteen turvallisuuden arvioinnissa tulisi hyödyntää sekä valmistajan dokumentaatiota että tietoliikenteen seurantaan tarkoitettuja työkaluja.

Ohjelmiston tai laitteen tietoliikenteen arvioinnissa auttaa esimerkiksi lähde- ja kohdeosoitteiden sekä tietoliikenneporttien selvittäminen verkon aktiivilaitteiden, kuten palomuurin tai erityisesti tietoliikenteen arviointiin tarkoitettujen pakettianalysaattoreiden

avulla. Lähde- tai kohdeosoitteiden fyysisen sijainnin voi selvittää useimmiten julkisesti saatavilla olevilla IP-osoitteiden geolokaatiopalveluilla[10] ja osoitteet omistava organisaatio voidaan tunnistaa mahdollisuuksien mukaan osoitteiden rekisteröintitiedoista.

IP-tunnelointi on tekniikka, jossa tietoliikenne paketoidaan ("tunneloidaan") toisen protokollan sisään, jolloin mikä tahansa verkkoliikenne saadaan kulkemaan verkon ylitse näennäisesti tunnelointipaketteja kuljettavan yhteyden mukaisena liikenteenä. Tietoliikenteen tunnelointi on esimerkiksi useiden VPN-toteutuksien keskeinen tekniikka. Sovellusten tekemä, hallitsematon tunnelointi on myös tietoturvauhka, sillä tunneloinnin keskeinen ajatus on kiertää verkkoihin ja niiden välille hallinnollisista ja turvallisuussyistä rakennetut, yhteyksiä estävät rajoitukset.

Suositeltavaa	Vältettävää
Tietoliikenne on päästä-päähän salattua tai muulla tavoin suojattua. Päästä-päähän salaus varmistaa tiedon luottamuksellisuuden ja estää siirron aikana tapahtuvat hyökkäykset.	Ohjelmisto tai laite muodostaa tietoliikenneyhteyksiä, jotka eivät ole toiminnallisuuden kannalta välttämättömiä.
Tietoliikenteen tarkoitus tiedetään eikä se muodosta turvallisuusriskiä.	Suorat tunnelointiyhteydet tuntemattomien tahojen hallussa olevin ulkopuolisiin laitteisiin.
Tietoliikenne tapahtuu turvalliseksi tunnettuihin organisaatioihin.	Ohjelmisto tai laite käyttää tietoliikenneportteja dokumentaatiosta poikkeavasti.
Ohjelmisto tai laite ei mahdollista tarpeettomia sisäänpäin tulevia yhteyksiä, eli sen muodostama hyökkäyspinta-ala on mahdollisimman pieni.	Tarpeettoman laajamittainen tietoliikenneporttien käyttö, joka mahdollistaa ei-toivotut tai haitalliset verkkohyökkäykset.
Ohjelmiston tai laitteen tietoliikenneportit ovat vähälukuisia, hyvin dokumentoituja ja perusteltavissa ohjelmiston tai laitteen toiminnallisuuksilla.	Ohjelmisto tarjoaa toiminnallisuutta, jota voidaan väärinkäyttää ulkopuolelta otetulla yhteydellä tietoturvan rikkomiseksi.

[10] IP-osoitteiden geolokaatiopalveluita on julkisesti saatavilla useita. Yksi esimerkki tällaisista palveluista on ipstack (https://ipstack.com/). Palvelu tarjoaa myös rajapintaa tarkastusten automatisointiin.

2.5.3 Tietojen säilytys, siirto ja poistaminen

Osa ohjelmistoista tai laitteista tallentaa tietoja oletusarvoisesti esimerkiksi palveluntarjoajan pilvipalveluun. Tällöin vastuu tietoturvallisuudesta siirtyy enenevissä määrin palveluntarjoajalle. Tietojen säilytyksen, siirron ja poistamisen turvallisuutta voi arvioida valmistajan tai palveluntarjoajan dokumentaation sekä palveluntarjoajalle tehtyjen riippumattomien tietoturva-arviointien avulla.

Suositeltavaa	Vältettävää
Ohjelmisto tai laite ei siirrä tietoa automaattisesti ulkopuoliselle taholle, tai siirrettävällä tiedolla ei ole merkitystä.	Minkäänlainen epäselvyys siitä, mitä tietoa siirretään, miten tietoa suojataan, miten varmuuskopiointi on toteutettu ja tapahtuuko tietojen poistaminen riittävän turvallisesti.
Ohjelmiston tai laitteen käyttäjä voi kontrolloida mitä tietoja palveluntarjoajan palveluihin siirretään.	Ohjelmisto tai laite siirtää tai säilyttää tietoja toisin kuin dokumentaatiosta tai valmistajan antamista tiedoista käy ilmi.
Tietojen poisto on hallittua ja poistotoimenpiteet sisältöineen voidaan tarvittaessa jäljittää.	Ohjelmisto poistaa tietoa automaattisesti, esim. tietyn säilytysajan ylittyessä ja poistoista ei jää lokitietoja.
Ohjelmisto tai laite tukee tietojen vientiä yleisesti tuetussa muodossa tai formaatissa.	

2.6 Tuotteen tietoturvallista käyttöä tukevat ominaisuudet

Itse tuotteen tietoturvatason arvioinnin lisäksi on hyvä ymmärtää miten sen käyttöönotto vaikuttaa organisaation tietoturvaan. Keskeistä tuotteen ominaisuuksien arvioinnin kannalta on ymmärtää, mahdollistavatko ne organisaation tietoturvakäytäntöjen mukaisen käytön. Tässä kappaleessa on esitetty muutamia olennaisimpia tietoturvallista käyttöä tukevia ominaisuuksia. Tuotteen tietoturvaominaisuuksien asettaminen ja käyttöönotto tulisi olla riittävän yksinkertaista ja tuotteen dokumentaation tulisi tukea käyttäjiä tietoturvallisessa käytössä.

2.6.1 Käyttäjien tunnistus

Käyttäjien tunnistuksella varmistetaan, että vain oikeutetut henkilöt pääsevät käsiksi järjestelmään ja sen tietoihin.

Suositeltavaa
Tuki federoidulle tai keskitetylle tunnistautumiselle.
Tuki monivaiheiselle tunnistautumiselle.

Salasanavaatimukset ovat riittävän vahvoja tai itse asetettavissa.

2.6.2 Käyttöoikeuksien ja käyttäjäroolien määrittäminen

Käyttäjäoikeuksien hallintaa ja käyttäjärooleja tarvitaan silloin, kun kyse on yhteiskäyttöisestä laitteesta tai ohjelmistosta, jossa kaikilla käyttäjille ei tule olla oikeuksia kaikkeen tietoon tai kaikkiin toimintoihin.

Suositeltavaa
Roolit palvelevat hyvin käyttötarkoitusta ja vähimpien tarvittavien oikeuksien antamisen periaatetta.
Roolit on selkeästi määritelty ja dokumentoitu.
Tuote tukee integroitumista organisaation keskitettyyn identiteetin- ja pääsynhallintajärjestelmään.

2.6.3 Lokitus

Riittävä lokitus auttaa seuraamaan ja analysoimaan järjestelmän toimintaa sekä käytön aikana että jälkikäteen, mukaan lukien tietoturvaan liittyviä tapahtumia.

Suositeltavaa
Lokit ovat selkeitä, kattavuudeltaan riittäviä ja integroitavissa keskitettyyn lokienhallintajärjestelmään.

2.6.4 Varmuuskopiointi

Riittävä varmuuskopiointi on välttämätöntä organisaation kyvylle varautua poikkeustilanteisiin. Kaikkien laitteiden ja ohjelmistojen osalta säännöllisen varmuuskopioinnin järjestäminen ei välttämättä ole kovin yksinkertaista eikä automaattista. Vähintään laitteen tai ohjelmiston sisältämä tieto ja sen asetukset tulisi pystyä varmuuskopioimaan riittävän yksinkertaisesti.

Suositeltavaa
Dokumentaation perusteella on selkeää, miten varmuuskopiointi tapahtuu ja mitä tietoja laitteesta tai ohjelmistosta varmuuskopioidaan.
Tuki automaattiselle varmuuskopioinnille.
Tuote mahdollistaa tietojen, asetusten sekä ohjelmiston varmuuskopioinnin ja palauttamisen.

3 Ohjelmiston tai laitteen kehitysaikaisen työn arviointi

Usein teknologisten tuotteiden toiminnalliset vaatimukset ja toteutusaikataulu on kehitystyössä huomioitu korkeammalla prioriteetilla kuin ei-toiminnalliset vaatimukset. Usein tuotteiden ei-toiminnallisiin vaatimuksiin lukeutuvat tietoturvan lisäksi mm. skaalautuvuus, suorituskyky ja vakaus.

Toimenpiteet rakentaa tietoturva jälkikäteen lähes valmiiseen tuotteeseen johtavat järjestelmällisesti huonompaan lopputulokseen kuin tietoturvan huomioiminen kehitystyön alusta alkaen osana tuotteen ominaisuuksia ja vaatimuksia. Jos tietoturvaa ei oteta huomioon alusta alkaen, ohjelmiston suunnittelun ja toteutuksen aikana tehdyt päätökset saattavat johtaa perustavanlaatuisiin tietoturvaongelmiin, joita on myöhemmin hankala korjata. Tämä puolestaan johtaa vaihtelevalla menestyksellä toimiviin, ohjelmistokehityksen loppuvaiheessa tehtyihin paikkausluonteisiin ratkaisuihin, joilla toivotaan saavutettavan riittävän hyvä tietoturvan taso.

Koska kehittämisvaiheessa oleva tuote on vielä keskeneräinen, arviointi perustuu käytännössä valmistajan antamaan tietoon. Kehittämisen aikaisesta tietoturvatyöstä on yleisesti ottaen vaikeaa saada kunnollista tietoa, sillä kehitystyön aikana syntyneet dokumentit eivät useinkaan ole julkisia ja laajoissa avoimen lähdekoodin ohjelmistoissa ei välttämättä ole edes tiettyä tahoa, joka johtaisi toimintaa ja johon ottaa yhteyttä. Alla olevia vinkkejä tuleekin soveltaa ja arviointi tehdä saatavissa olevan tiedon mukaisesti.

Jonkin verran arviointia voi kuitenkin suorittaa sen perusteella, mitä valmistaja kertoo julkisesti esimerkiksi dokumentaatiossaan tai muissa lähteissä. Lisäksi ohjelmiston tai laitteen valmistajalta tiedustelemalla voi saada lisätietoa käytettyjen kehitysmenetelmien tietoturvasta. Valmistajalta voi tiedustella esimerkiksi ohjelmistolle tai laitteelle toteutetusta uhka- ja riskianalyysista, tietoturvavaatimuksista, ohjelmistoarkkitehtuurista tai tietoturvatestausraporteista.

Suositeltavaa	Vältettävää
Valmistaja noudattaa jotain tunnettua tietoturvallista tuotekehitysprosessia tai sen räätälöityä versiota.	Valmistaja antaa sivuillaan ja muissa julkisissa lähteissä hyvin vähän tai ei ollenkaan tietoa ohjelmiston tai laitteen tietoturvasta.
Valmistaja pystyy esittämään dokumentaatiota kehitysaikaisen tietoturvatyön vaiheista.	Valmistaja pyrkii sivuuttamaan tiedustelut ja tarjoaa kysyttäessäkin hyvin niukalti tai ei ollenkaan tietoa tuotteen tietoturvasta.
Kehittämisessä on ollut mukana tietoturvaan erikoistuneita asiantuntijoita tai muilla keinoin on varmistuttu riittävästä tietoturvaosaamisesta kehitystyössä.	Tietoturva-asiantuntijuuden puute ohjelmistokehitystiimissä.

Tuotteelle on tehty huolellinen tietoturva-auditointi ennen julkaisua.	Arkkitehtuurin monimutkaisuus ja yleinen vaikeus ymmärtää, miten tietoturva rakentuu tuotteessa.
Arkkitehtuuri on looginen ja tietoturva on sisäänrakennettuna tuotteen toimintalogiikassa.	Arkkitehtuuria ei ole dokumentoitu tai sen tietoturvan tasoa ei voida arvioida arkkitehtuuridokumentaation perusteella.
Tietoturvaan liittyvien toimintojen sijoittuminen arkkitehtuuritasolla on selkeää ja loogista.	Tietoturvaan liittyviä toimintoja ja kokonaisuuksia ei voida selkeästi tunnistaa arkkitehtuurista.
Tuotteen eri komponenteilla on selkeät roolit tietoturvan eri osa-alueiden toteuttamisessa.	
Tuotteen kehityksessä on noudatettu sisäänrakennetun ja oletusarvoisen tietoturvan sekä tietosuojan toteutusperiaatteita.	
Tuotteen turvallinen käyttö ja käyttötapaukset on ohjeistettu ja kuvattu selkeästi käyttöohjeissa.	

4 Uudet teknologiat

Käsitystä uudempien teknologioiden tietoturvasta on vielä vaikeampi muodostaa kuin vakiintuneista teknologioista. Uudet teknologiat mahdollistavat usein uuden tyyppisiä riskejä, jotka tunnistetaan vasta ajan kuluessa. Usein tuotteet pyritään saamaan markkinoille mahdollisimman nopeasti, mikä tarkoittaa suurta todennäköisyyttä sille, että panostus ei-toiminnallisiin piirteisiin, kuten tietoturvaan on vähäinen.

Usein turvallisuusriskit uusien teknologioiden ja niihin perustuvien tuotteiden kohdalla ovatkin yleisempiä kuin vakiintuneisiin teknologioihin perustuvien tuotteiden kohdalla. Tämä ei kuitenkaan tarkoita, että kaikki vakiintumattomat teknologiat olisivat lähtökohtaisesti turvattomampia, vaan että vakiintumattomien teknologioiden osalta riskiarvioon ja riskienhallintaan on syytä kiinnittää erityistä huomiota.

4.1 IoT (Internet of Things) -laitteet

IoT -laitteiden tietoturvalla on yleisesti ottaen melko huono maine. Varsinkin alkuvaiheessa useat laitteet toimitettiin heikoilla oletussalasanoilla, ilman päivitysmahdollisuuksia ja ilman asianmukaista salausta. Seurauksena oli useita merkittäviä tietoturvaloukkauksia ja hyökkäyksiä, mukaan lukien IoT-laitteista muodostetut haitalliset bottiverkot.

Viime aikoina kehitys on ollut positiivisempaa, mutta siitä huolimatta IoT-laitteiden monimuotoisuus, rajoitukset prosessointikyvykkyydessä, päivitysmahdollisuuksissa ja ohjelmoitavuudessa sekä puutteelliset mahdollisuudet ottaa IoT-laitteet automatisoidun hallinnan piiriin esimerkiksi työasemien tavoin, tekevät niiden suojaamisesta haasteellista.

Suojaamisen lisäksi IoT -laitteiden tietoturvan tason arviointi on haasteellista. Ne ovat lähtökohtaisesti tiukasti yhteen paketoituja laite- ja ohjelmistoratkaisuja, ja valmistajasta riippuen niistä saattaa olla vaikea saada riittävästi tietoa. Sinänsä tuotteiden tietoturvallisuuden arviointi voidaan tehdä samaan tapaan ja samoja perusperiaatteita noudattaen kuin muillekin ohjelmisto- ja laiteratkaisuille.

Valmistajan ja valmistusmaan lainsäädännön osalta IoT-laitteiden arvioinnissa ei ole eroa muihin tuotteisiin, ja haavoittuvuustietokannat sisältävät yhtä lailla myös IoT-laitteiden ja niiden ohjelmistojen haavoittuvuuksia. IoT-laitteiden kehittämisvaiheen tietoturvan, ominaisuuksien ja teknologisten valintojen osalta tietoturvan tasoa voidaan arvioida samoin metodein kuin muidenkin laitteiden tai ohjelmistojen kohdalla, mutta suurimmaksi haasteeksi tässä tapauksessa nousee tiedon puute. Myös IoT-laitteiden suorittamaa tietoliikennettä voidaan tarvittaessa tarkkailla ulkoapäin pakettianalysaattorilla ja laitteiden avoimia tietoliikenneportteja voidaan kartoittaa porttiskannerilla.

IoT -laitteiden suojaamisen kohdalla yksi mahdollinen lähestymistapa onkin selvittää se, mitä on selvitettävissä, ja tarvittaessa eristää laite omaan, tiukasti tarkkailtuun ja liikennöinniltään rajoitettuun verkkosegmenttiin.

4.2 Pilvipalvelut

Etenkin suurten, kansainvälisten palveluntarjoajien pilvipalveluista on julkisesti saatavilla varsin kattavasti tietoa. Tietoja palveluihin toteutetuista tietoturvasertifioinneista ja niiden noudattamista tietoturvakontrolleista ja -standardeista voi hyödyntää arvioinnin tukena.

Tunnettujen ja vakiintuneiden pilvipalveluiden tietoturva on yleisesti ottaen hyvällä tasolla. Tämä johtuu pitkälti pilvipalveluiden palveluntarjoajalleen tuottamista mittakaavaeduista ja sen mukaisesta kyvystä resursoida tietoturvatyötä huomattavan hyvin. Tämän lisäksi vakuuttava ja todennettu tietoturva on kynnyskysymys niiden asiakashankinnalle.

Mittakaavaetujen vuoksi pilvipalveluihin ja niiden tietoturvaan kohdistuu myös vastaavasti suuremmat uhat. Pilvipalvelut ovat erittäin houkuttelevia kohteita tietomurroille, sillä ne ovat toimintalogiikkansa mukaisesti usein saavutettavissa kaikkialta, ja niiden kautta voidaan päästä käsiksi kerralla useiden organisaatioiden tietoihin.

Pilvipalveluiden todellista tietoturvaa arvioitaessa kannattaakin tutustua julkisista lähteistä saatavilla oleviin kokemuksiin kyseisen pilvipalvelun turvallisuusongelmista ja palvelussa mahdollisesti tapahtuneista tietoturvaloukkauksista.

Tietoturvan ohella keskeistä on selvittää myös pilvipalvelun tietosuojan taso ja mahdolliset riskit tietosuojan toteutumiselle henkilötietojen käsittelyssä. Aihetta on käsitelty laajemmin muun muassa Digi- ja väestötietoviraston oppaassa Tietosuoja pilvipalveluissa[11].

[11] Tietosuoja pilvipalveluissa – VAHTI hyvät käytännöt -tukimateriaali (pdf, 11/2022)

5 Oppaassa esitellyt keskeiset linkit

Keskeiset linkit arvioinnin tueksi
Kansallisvaltioiden kyberkyvykkyydet
• National Cyber Power Index 2022
Haavoittuvuustilanteen kartoitus / CVSS-standardi
• FIRST (*Forum of Incident Response and Security Teams*) • SANS
Haavoittuvuustilanteen kartoitus / haavoittuvuustietokantoja
• NVD (National Vulnerability Database) • Mitre CVE (Common Vulnerabilities and Exposures) • CMU CERT Vulnerability Database
Haavoittuvuustilanteen kartoitus / ajantasaista haavoittuvuustietoa
• Liikenne- ja viestintävirasto Traficomin haavoittuvuustiedotteet • Liikenne- ja viestintävirasto Traficomin uutiskirjeet
Käytettyjen teknologioiden arviointi / salausalgoritmit ja avainpituudet
• Liikenne- ja viestintävirasto Traficomin NCSA-toiminnon hyväksymät salausratkaisut • Traficomin kansalliset kryptografiset vähimmäisvaatimukset turvallisuusluokkien IV-III tiedon välittämiseen TLS-salatusti (esimerkiksi HTTPS)
Pilvipalvelut
• Tietosuoja pilvipalveluissa – VAHTI hyvät käytännöt -tukimateriaali