



NCSA-FI:n suorittama tietojärjestelmien tietoturvallisuushyväksyntä

Tilaaajaorganisaation näkökulma

JOHDANTO

Viestintäviraston NCSA-FI-yksikön tehtäviin kuuluu toimiminen turvallisuusjärjestelyt hyväksyvänä viranomaisena (SAA, Security Accreditation Authority). NCSA-FI:n suorittama tietojärjestelmien tietoturvallisuushyväksyntä sisältää tilaaajaorganisaatiolta vaadittavia suoritteita. Tässä dokumentissa kuvataan hyväksyntä tilaaajaorganisaation näkökulmasta. Kuvauksessa määritellään käytetyt termit, esitellään hyväksynnän edellytykset ja hyväksynnästä perittävien maksujen määräytyminen, esitetään kaikki tilaaajaorganisaatiolta vaadittavat suoritteet osana hyväksyntäprosessia sekä määritellään hyväksynnän voimassaolon ehdot.

MÄÄRITELMÄT

"Hyväksynnällä/hyväksyntäprosessilla" (accreditation) tarkoitetaan prosessia, jonka päätteeksi turvallisuusjärjestelyt hyväksyvä viranomainen antaa virallisen lausunnon siitä, että järjestelmä on hyväksytty käytettäväksi määritellyssä turvaluokassa, tiettyä turvallisuuden takaavaa toimintatapaa noudattaen käyttöympäristössään ja hyväksyttävällä riskitasolla, sen pohjalta, että hyväksytyt tekniset, fyysiset, organisatoriset ja menettelyyn liittyvät turvatoimet on toteutettu.

"Tarkastuksella" (audit) tarkoitetaan riippumattoman tahon suorittamaa kohteen, sen toiminnan ja toiminnan tulosten yleensä määrääjoin tapahtuvaa tutkimista sen selvittämiseksi, vastaako järjestelmä siihen kohdistuvia vaatimuksia.

HYVÄKSYNNÄN EDELLYTYKSET JA HYVÄKSYNNÄSTÄ PERITTÄVÄT MAKSUT

NCSA-FI:n suorittamat tietoturvallisuushyväksynät edellyttävät tilaaajaorganisaatiolta aina perusteltua tarvetta käsitellä kansallista tai kansainvälistä turvaluokiteltua tietoa. Hyväksyntämenettelyn piiriin kuuluvat:

- valtionhallinnon toimijoiden järjestelmät siltä osin, kun ne liittyvät kansainvälisten tietoturvaoveltoitteiden täyttämiseen, ja
- kansainvälisiin tarjouskilpailuihin osallistuvien yritysten järjestelmät siltä osin, kun ne vaativat kansallisen tietoturvallisuusviranomaisen (NCSA) hyväksyntää.

Organisaatiolta, joka on tilannut Viestintävirastolta turvaluokiteltua tietoa käsittelevien tietojärjestelmien tietoturvallisuushyväksynnän, peritään hyväksyntään käytettyyn aikaan perustuva maksu. Tilaaajaorganisaatiolla on oikeus saada Viestintävirastolta arvio maksun suuruudesta ennen tilauksen tekoa.



HYVÄKSYNTÄPROSESSIN KUVAUS

Hyväksyntäprosessi koostuu viidestä keskeisestä suoritteesta sekä näitä täydentävistä osasuoritteista. Tässä kuvataan kukin suorite sillä tarkkuudella, että se antaa tilaajaorganisaatiolle selkeän yleiskuvan siltä vaadittavista toimista. Hyväksyntäprosessia on havainnollistettu kuvassa 1.

1. Hyväksyntäpyyntö NCSA-FI:lle

Ennen hyväksyntäpyynnön lähettämistä tilaajaorganisaatiota suositellaan tutustumaan NCSA-FI:ltä saatavaan yleiseen tarkistuslistaan. Hyväksyntäpyyntö suositellaan lähetettäväksi vasta, kun tilaajaorganisaatiossa uskotaan, että hyväksynnän kohde täyttää tarkistuslistan vaatimukset.

Hyväksyntäpyynnöstä on selvittävä:

- Järjestelmän nimi
- Lyhyt luonnehdinta järjestelmästä ja sen laajuudesta
- Käsitteleekö järjestelmä kansallista vai kansainvälistä turvaluokiteltua tietoa
- Korkein käsiteltävä turvaluokka
- Järjestelmän omistaja, rakentaja ja ylläpitäjä
- Järjestelmän tila: valmis / rakenteilla / suunnitteilla
- Järjestelmään liittyvät ulkoiset tai sisäiset vaatimukset, sekä suunniteltu käyttöönottopäivä
- Yhteyshenkilön nimi ja yhteystiedot

Hyväksyntäpyyntöön on NCSA-FI:ltä saatavissa esitäytetty lomake. Hyväksyntäpyyntö on lähetettävä kirjallisesti Viestintäviraston kirjaamoon osoitteeseen:

NCSA-FI / Rauli Paananen, Viestintäviraston kirjaamo, Itämerenkatu 3A, PL 313, 00181 Helsinki

2. NCSA-FI:n vastaus

NCSA-FI pyrkii antamaan vastauksensa kahden viikon kuluessa pyynnön saapumisesta. Vastauksesta selviää:

- Mahdollinen hyväksyntäaikataulu, mukaan lukien ehdotus esipalaverin ajaksi
- Esipalaveriin tilaajaorganisaatiolta vaadittavat dokumentit

3. Esipalaveri tilaajaorganisaation kanssa

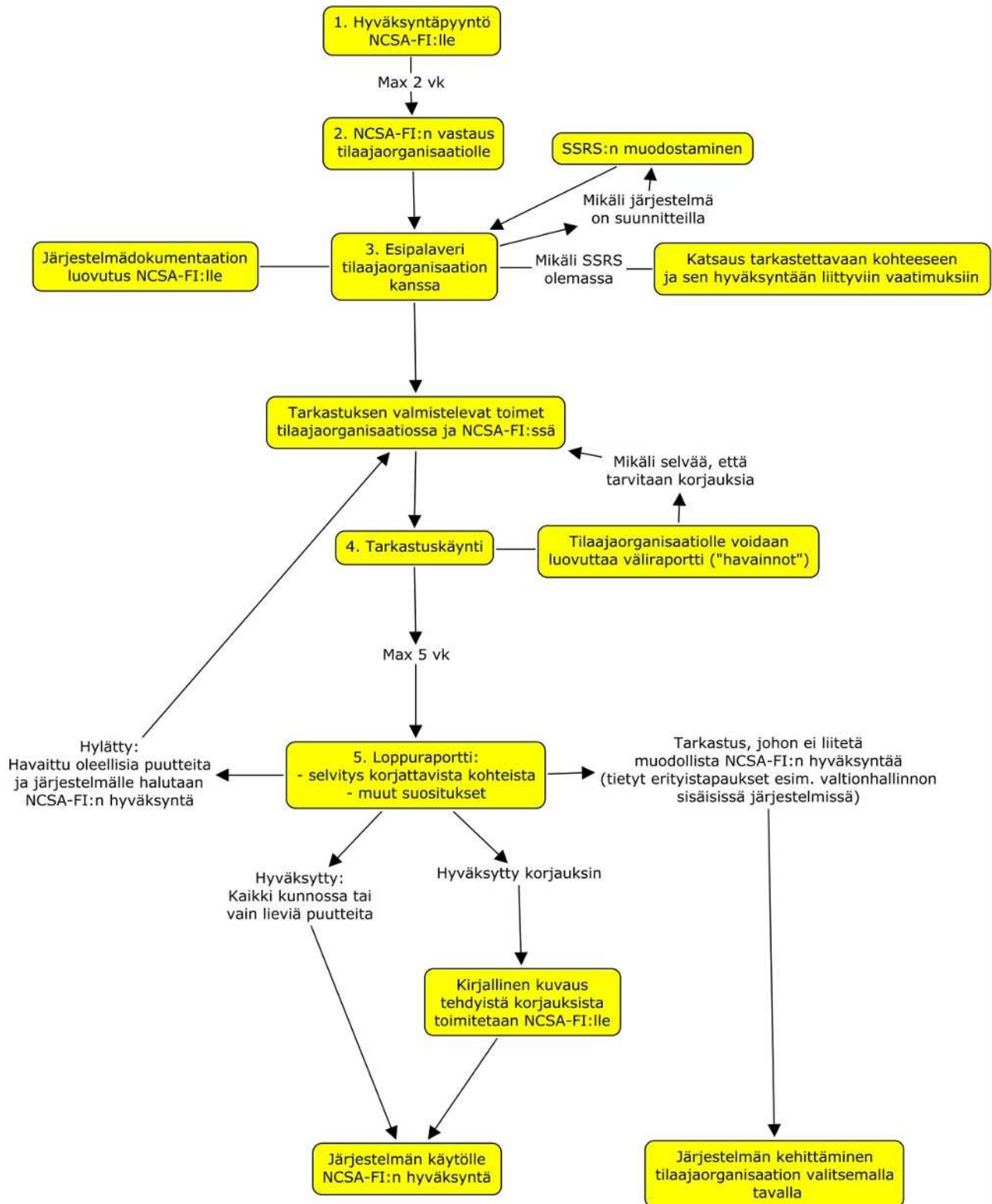
Esipalaveri pidetään seuraavien toimijoiden kesken:

- Tarkastajat (SAA:n edustajat)
- Järjestelmän omistaja
- Järjestelmän rakentaja
- Järjestelmän ylläpitäjä
- Fyysisten turvallisuusvaatimusten tarkastaja(t)

Esipalaverissa NCSA-FI:lle luovutetaan mahdollisuuksien mukaan seuraavat dokumentit:

- Vaatimusmäärittely, erityisesti SSRS (System-Specific Security Requirements Statement)
- Verkkokuvat
- Lista käytetyistä käyttöjärjestelmistä ja ohjelmistoista versiotietoineen
- Tiedot mahdollisista aikaisemmista tarkastuksista ja/tai hyväksynnistä raportteineen

Ideaalitilanteessa dokumenteista selviää verkon rakenne, IP-osoitteet, vyöhykkeet, segmentit, palomuurisäännöt, verkkolaitteiden käyttöjärjestelmä-/firmware-versiot, palvelinten ja tuotantojärjestelmien ohjelmistoversiot ja asetukset, ja muut vastaavat tiedot sillä tarkkuudella, että niiden perusteella ulkopuolinen pystyy saattamaan vikaantuneet verkot ja järjestelmät käyttökuntoon.



Kuva 1. Hyväksyntäprosessi.



4. Tarkastuskäynti tai -käynnit

Tarkastuskäynti tai -käynnit sisältävät kohteen tietoturvallisuuden tutkimisen sen selvittämiseksi, vastaako kohteen tietoturvallisuuden tila siihen kohdistuvia vaatimuksia. Tarkastus koostuu yleensä hallinnollisesta ja teknisestä osuudesta. Tarkastukseen sisältyy myös toisen tahon suorittama fyysisen turvallisuuden osuus.

5. Loppuraportti

Loppuraportti toimitetaan lähtökohtaisesti viiden viikon kuluessa viimeisimmästä tarkastuskäynnistä. Raportti voidaan toimittaa myös erivälillä aikataululla sopimuksen mukaan. Loppuraportista käy ilmi:

- Korjattavat kohteet
- Muut suositukset
- Hyväksyntätulos

Hyväksyntätulos on jokin seuraavista:

- Hyväksytty
- Hyväksytty korjauksin
 - Hyväksyntä astuu voimaan vasta, kun korjaukset on tehty ja tehdyistä korjauksista on toimitettu kirjallinen kuvaus NCSA-FI:lle.
- Hylätty
 - Vaaditaan korjausten tekeminen ja uusintatarkastus.

HYVÄKSYNNÄN VOIMASSAOLO

NCSA-FI:n myöntämä hyväksyntä on voimassa kaksi vuotta myöntämispäivästä lukien. Hyväksyntä raukeaa, mikäli tarkastetussa kohteessa tapahtuu merkittävä sen turvallisuuteen vaikuttava muutos. Tällaisia voivat olla esimerkiksi merkittävät verkkorakenteen, henkilöstön, turvakäytäntöjen tai toimitilojen muutokset. Tavanomaisesta ylläpidosta aiheutuvat muutokset, kuten esimerkiksi ohjelmistojen turvapaikkojen asennukset, eivät aiheuta voimassaolevan hyväksynnän raukeamista. Tapauskohtaiset ehdot hyväksynnän raukeamiselle määritellään yksityiskohtaisesti hyväksynnän yhteydessä. Merkittävät muutokset tulee hyväksyttää NCSA-FI:llä.