TIETOTURVAN HALLINTA
Yleiset ohjeet

Tilaajan yleiset tietoturvan ohjeet Toimittajalle

Tilaajan tiedot tulee turvata riittävästi

Toimittajan tulee turvata Tilaajaan liittyvät tiedot väärinkäytöltä, vääristymiseltä, asiattomalta käytöltä sekä mahdollistaa tietojen saatavuus niitä tarvittaessa. Tiedot tulee turvata sekä toimitettaessa Palveluita, että teknisiä tieto- ja viestintäjärjestelmiä. Toimittajan tulee noudattaa voimassa olevan henkilötietoja ja muuta tietojenkäsittelyä koskevan lainsäädännön edellyttämää hyvää tietojen käsittelytapaa ja tietojen suojaamista koskevia säännöksiä, sekä antaa henkilöstölleen ja omille palvelutoimittajilleen näitä koskevat ohjeensa.

Tässä asiakirjassa annetaan yleisiä tietoturvan ohjeita, joita voidaan täydentää sopimuskohtaisella kuvauksella täsmällisistä tietoturvajärjestelyistä. Nämä ohjeet koskevat toimittajaa Tilaajan tietojen käsittelyä koskevilta osin. Teknisten tieto- ja viestintäjärjestelmien tietoturvajärjestelyt kuvataan osana järjestelmän kuvausta.

Toimittajan tulee edellyttää Tilaajan tietojen käsittelyyn liittyviltä omilta alihankkijoiltaan samat tietoturvan vaatimukset kuin Tilaaja edellyttää Toimittajalta itseltään.

Toimittajan tietoturvan hallinnan kuvaus

Toimittaja voi osoittaa hallinnollisen tietoturvansa esimerkiksi jonkin laatujärjestelmän mukaisella tietoturvan hallintajärjestelmällä. Tietoturvan hallinnassa Toimittajalta vaaditaan seuraavaa.

Toimittajan tietoturvan yleisperiaatteet

Toimittajan tulee voida esittää johtonsa hyväksymät tietoturvan yleisperiaatteet, jotka Toimittajan henkilöstölle ja alihankkijoille on tiedotettu. Tällainen voi olla esimerkiksi tietoturvapolitiikka, tietoturvan linjaukset tai tietoturvan periaatteet niminen asiakirja.

Järjestelmällinen tietoturvan hallinta

Tietojen turvaamiseen sekä teknisiin tieto- ja viestintäjärjestelmiin liittyvän toiminnan vastuut on määritelty. Nämä voivat olla kuvattu esimerkiksi laatujärjestelmässä tai toimintakäsikirjana.

Toimittajan omat palvelutoimittajat

Toimittajan tietoturvan hallinta kattaa sen omat alihankkijat, joiden töistä toimittaja vastaa samalla tavalla kuin omasta työstään. Tämä voidaan osoittaa sopimuksilla sekä tietoturvan yleisperiaatteissa.

Tarkastusoikeus

Tilaajalla on oikeus tarkastaa toimittajan tietoturvan hallinta Tilaajan tietojen käsittelyä koskevilta osin. Toimittaja vastaa siitä, että tällainen tarkastus voidaan ulottaa Toimittajan käyttämiin alihankkijoihin. Tietoturvan hallinnan tarkastaminen kattaa myös tietojenkäsittelyyn liittyvän toiminnan sekä teknisten tieto- ja viestintäjärjestelmien tarkastamisen.

Henkilöstö osana tietoturvassa onnistumista

Toimittajan henkilöstöhallinnon menettelyillä toteutetaan osaltaan tietoturvaa. Toimittajan tulee voida osoittaa kuinka henkilöstöhallinto on järjestetty. Tämä voidaan osoittaa esimerkiksi henkilöstöhallinnon käsikirjalla tai työohjeilla.

Henkilöstön tietoturvan osaaminen

Toimittajan tulee järjestää Tilaajan tietojen käsittelyyn osallistuvalle henkilöstölle riittävä koulutus, joka huomioi tietoturvaan liittyvän osaamisen. Tämä koskee henkilöstöä, joilla on pääsy Tilaajalle Palvelua tuottaviin tieto- ja viestintäjärjestelmiin tai tiloihin, joissa tuotetaan palvelua Tilaajalle. Toimittajan tulee voida osoittaa Tilaajan tietojen käsittelyyn liittyvän henkilöstön koulutus. Henkilöstön osaaminen voidaan osoittaa esimerkiksi tehtäväkohtaisilla ammattitaitotodistuksilla, koulutustilaisuuksien osallistujaluetteloilla tai Toimittajan koulutusohjelmien kurssiaineistoilla.

Henkilöstön luotettavuuden varmistaminen ja salassapitovelvollisuus

Toimittajan tulee pystyä ilmoittamaan Tilaajalle Tilaajan tietoihin pääsevän henkilöt.

Toimittajalla tulee olla määritelty menettely, jolla se varmistaa Tilaajan tietoja käsittelevien henkilöiden luotettavuuden tai jotka pääsevät tiloihin, joissa tuotetaan Palvelua Tilaajalle. Menettely voi olla esimerkiksi kuuluminen turvallisuusselvitysmenettelyn piiriin.

Toimittajan tulee tiedottaa henkilöstölle, että salassapitovelvollisuus säilyy lain mukaan myös työsuhteen päättymisen jälkeen.

Henkilön siirtyminen pois Tilaajan palvelutuotannosta

Toimittajan tulee välittömästi sulkea käyttövaltuudet Tilaajan tietoihin kaikilta henkilöiltä, jotka eivät enää työskentele Toimittajan palveluksessa tai Tilaajaan liittyvissä Palveluissa. Toimittajan tulee varmistaa, että henkilöt palauttavat kaikki sellaiset työlaitteet, jotka sisältävät Tilaajan tietoa.

Mikäli Toimittajan työntekijälle oli myönnetty käyttövaltuuksia tai kulkuoikeuksia muihin Tilaajan järjestelmiin tai tiloihin, tulee Toimittajan viipymättä ilmoittaa työntekijän siirtymisestä pois Tilaajan palvelutuotannosta ja käyttövaltuuden perusteen päättymisestä.

Luottamuksellisuuden hallinta, salassapito

Toimittaja saa käsitellä Tilaajan tietoa vain Tilaajan kanssa sovittuun tarkoitukseen. Tilaajan tietoja ei saa käsitellä, tallentaa tai saattaa muille, kuin ainoastaan Tilaajan kanssa sovitulla tavalla ja kun se on Tilaajalle Palvelun tuottamisen kannalta tarpeellista.

Ohjeet luottamuksellisuuden vaalimiseen

Toimittajalla tulee olla kirjalliset ohjeet henkilökunnalleen ja käyttämilleen alihankkijoille tietojen luottamuksellisuuden säilyttämisestä ja turvallisesta tietojenkäsittelystä.

Tallenteen ja tietoliikenteen salakirjoittaminen

Tilaajan Palveluissa salasanat tms. tulee aina tallentaa ei-selväkielisinä. Salasanoja, PIN-lukuja, yksityisiä avaimia tai muita vastaavia tietoja ei saa tallentaa selväkielisenä.

Tilaajan salassa pidettävä tieto tulee salakirjoittaa, kun se tallennetaan siirrettäville tallennusvälineille, kuten USB-muistit tai mobiililaitteet. Salakirjoitusmenetelmän valinta tulee perustella joko kyseiseen käyttöympäristöön liittyvällä riskiarviolla tai julkishallinnolle annetuilla suosituksilla. Myös varmuuskopioiden turvallinen käsittely on voitava osoittaa.

Toimittajan tulee siirtää Tilaajan salassa pidettävää tieto tietoverkoissa aina suojattuna, esimerkiksi VPN, HTTPS, SFTP tms. yhteydellä. Tilaajan salassa pidettävää tietoa ei saa siirtää avoimessa tietoverkossa suojaamattona selväkielisesti. Vaatimus koskee myös järjestelmien kirjautumistietoja. Teknisen suojausratkaisun valinta tulee perustella joko kyseiseen käyttöympäristöön liittyvällä riskiarviolla tai sen tekniikkaan liittyvillä alan yleisillä suosituksilla.

Luotettava tuhoaminen

Toimittajan tulee tuhota Tilaajan tiedot luotettavasti sen jälkeen, kun Tilaaja on pyytänyt tiedot tuhoamaan, kun niitä ei enää tarvita ja säilytysaikavaatimukset sallivat tuhoamisen. Vaatimus koskee myös niitä käytöstä poistettavia fyysisiä välineitä, joilla on ollut tallennettuna Tilaajan salassa pidettävää tietoa. Luotettava tuhoaminen voidaan osoittaa työohjeilla sekä tuhoamisesta pidetyllä kirjanpidolla.

Työskentelytilan suojaaminen

Toimittajan tulee järjestää Tilaajan salassa pidettävien tietojen työskentelytilat siten, että ne on suojattu. Toimitilojen ja tietoteknisten laitetilojen suojausratkaisuiden riittävyyden voi perustella vertaamalla niitä esimerkiksi toimitilojen VAHTI-suosituksiin (2/2013 Toimitilojen tietoturvaohje, http://www.vahtiohje.fi/).

Salassa pidettävien tietojen käsittelytilojen lähtökohtana on perustason tietoturvallinen työskentelytila. Tilassa tulee kuitenkin huomioida korotetun tason työskentelytilan vaatimuksia, mikäli tiloissa käsitellään esimerkiksi erityissuojattavaa henkilötietoa, arkaluonteista tietoa, turvakiellon alaisia tietoja tai muuta tietoa, jonka oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa tai jopa merkittävää vahinkoa yleiselle tai yksityiselle edulle. Tällainen tieto voisi koskea esimerkiksi rakennusten, laitosten, rakennelmien tai tieto- ja viestintäjärjestelmien turvajärjestelyjä, tai onnettomuuksiin ja poikkeusoloihin varautumista. Toimittajalla tulee olla salassa pidettävien tietojen käsittelytilasta tehty riskiarvio.

Oleellista on se, että työskentelytilat mahdollistavat Tilaajan tietojen säilymisen vain niihin oikeutetuilla ja estää tietojen tuhoamista tai katoamista.

Käyttöoikeudet ovat henkilökohtaisia

Toimittajan tulee käyttää henkilökohtaisia käyttäjätunnuksia kaikissa Tilaajalle Palvelua tuottavissa järjestelmissä. Jaettujen, yhteiskäyttöisten tunnusten käyttäminen on kielletty, ellei käyttöä pystytä yksilöimään. Mikäli Palvelun tuottaminen vaatii jaettuja tunnuksia, niin tunnusten käyttöperiaatteet tulee hyväksyttää kirjallisesti Tilaajalla. Yhteiskäyttötunnusten käyttöperiaatteiden tulee yksilöidä millä henkilökohtaisella käyttötunnuksella tai kuka henkilö on yhteiskäyttötunnusta käyttänyt. Yksilöitävyys voidaan osoittaa käyttöperiaatteilla, työohjeilla ja käyttökirjanpidolla (lokeilla).

Pääkäyttäjät

Pääkäyttäjän oikeuksia saa käyttää vain ja ainoastaan ylläpitotehtäviin, vianselvityksiin ja Tilaajan toimeksiannosta. Käyttäjä saa kirjautua pääkäyttäjän tunnuksella järjestelmään vain ja ainoastaan niissä tilanteissa, jossa käyttäjän tulee toteuttaa ylläpitotehtäviä, vianselvityksiä tai kyseessä on Tilaajan toimeksianto. Pääkäyttäjätunnusten käytön liittyminen vain ylläpitotehtäviin, vianselvityksiin tai Tilaajan toimeksiantoihin voidaan osoittaa käyttöperiaatteilla, työohjeilla ja käyttökirjanpidolla (lokeilla).

Vahva tunnistaminen

Jos käyttäjän tunnistaminen perustuu vain käyttäjätunnuksen salasanan tietämiseen, niin salasanojen tulee olla riittävän vahvoja (vähintään 10 merkkiä pitkiä, ja pääkäyttäjällä vähintään 15 merkkiä).

Tietoturvalliset toimintatavat palvelutuotannossa

Toimittajan palvelutuotannon turvallisuus voidaan osoittaa esimerkiksi voimassa olevilla laatusertifikaateilla ja siihen voi liittyä palveluiden kannalta kattava valvomotoiminne (tietoturvavalvomo, kyberturvakeskus).

Päätelaitteiden turvaaminen

Kannettavissa tietokoneissa tai vastaavissa laitteissa Tilaajan tiedot tulee suojata käyttöoikeuksilla ja salakirjoittamalla. Tämä voidaan toteuttaa esimerkiksi käyttämällä käyttöjärjestelmän omaa levynsalausta.

Ohjelmistopäivitykset

Laitteiden tai järjestelmien päivitykset tulee asentaa ilman tarpeetonta viivettä erityisesti tietoturvapäivitysten osalta. Mikäli päivityksien asennusta joudutaan viivyttämään, niin Toimittajan tulee toteuttaa tarvittavat vaihtoehtoiset menettelyt riskien pienentämiseksi. Vaihtoehtoiset rajoitusratkaisut voidaan perustella esimerkiksi Viestintäviraston Kyberturvallisuuskeskuksen haavoittuvuustiedotteiden suosituksilla.

Kun laitteiden päivitysten puuttumisesta seuraa tietoturvariski Tilaajan tiedoille tai Tilaajalle Palvelua tuottaville järjestelmille, niin kyseessä on tietoturvapoikkeama Toimittajalle. Toimittaja vastaa siitä, että Toimittajan tai sen alihankkijoiden hallinnassa olevien laitteiden päivitykset ovat ajan tasalla.

Turvaohjelmistot

Toimittajan tulee käyttää ajan tasalla olevia haittaohjelmien torjuntaratkaisuita niissä ympäristöissä, joihin on saatavilla Tilaajan Palvelulle soveltuva suojaus. Toimittajan tulee valvoa ja varmistaa turvaohjelmistojen ajan tasaisuus sekä toimivuus.

Toimittajan tulee käyttää ja ylläpitää palomuuria tai vastaavaa tietoliikenteen suojausratkaisua kaikissa sellaisissa laitteissa, jotka voidaan kytkeä suoraan julkiseen verkkoon ja jotka liittyvät Tilaajan tietojen käsittelyyn suoraan tai välillisesti. Tällainen laite voi olla esimerkiksi asiantuntijan kannettava tietokone, joka siis tulee suojata sekä haitalliselta tietoliikenteeltä että haittaohjelmilta (”viruksilta”).

Palvelinten turvaamisesta

Tilaajalle Palvelua tuottavissa järjestelmissä tulee kaikki oletussalasanat vaihtaa. Oletussalasanoja ei saa jättää käyttöön. Suositeltavaa on myös vaihtaa oletushallinnointitunnukset, eli järjestelmien oletusasetusten mukaiset hallinnointi- tai pääkäyttäjätunnukset on hyvä korvata muilla tunnuksilla.

Tilaaja varaa oikeuden kohdistaa tekninen haavoittuvuustarkastus järjestelmään Toimittajan kanssa yhdessä sovittavalla tavalla.

Tilaaja ei ota vastaan eikä hyväksy järjestelmää ja sen toimitusta, jos järjestelmässä on kriittisiä haavoittuvuuksia. Kriittiseksi voidaan katsoa esimerkiksi Viestintäviraston Kyberturvallisuuskeskuksen haavoittuvuustiedotteiden mukaan kriittiset viat tai kyseisen laitteen tai ohjelmiston päivityssuositusten mukaan kriittiset viat. Kriittinen haavoittuvuus vakavasti vaarantaa tarkoitetun käytön ja tiedot, ja Toimittajan on voitava riskiarviolla esittää miksi kriittiseltä vaikuttava asia ei aiheuta vaaraa, jos se on jäämässä järjestelmään.

Järjestelmäkuvauksien tulee osoittaa mistä laitteista ja ohjelmistoista palvelun toteutus koostuu. Kuvauksien tulee kattaa laitteet, varusohjelmistot ja ohjelmistoversiot sellaisella tarkkuudella, että Palvelun toteutus on mahdollista koota kuvauksien avulla.

Palvelimien koventaminen suositellaan tehtävän soveltamalla alalla yleisesti käytössä olevia asennusohjeita. Tällaisia ohjeita ovat esimerkiksi NIST, SANS ja laite- tai järjestelmävalmistajien ohjeet. Kovennusohjeilla on tarkoitus parantaa palvelimen kestokykyä tietoturvahyökkäyksiä tai muita uhkia vastaan.

Kun haavoittuvuus havaitaan, tulee Toimittajan aloittaa haavoittuvuuden korjaaminen ilman tarpeetonta viivettä sekä tiedottaa Tilaajaa.

Lokit

Järjestelmien lokien (käyttökirjanpidon) tulee kattaa Tilaajalle toimitettavan Palvelun tai tietojenkäsittelyn tarpeet. Lokien hallinnasta on voitava osoittaa toimintaohjeet. Lokit tulee aina tallentaa niin, että ne säilyvät luotettavina. Lokeja tutkittaessa tulee aina käsitellä lokien luotettavasta talletuspaikasta otettua kopiota.

Tyypillisesti lokien perusteella tulee voida seurata tietojen tai järjestelmän komponenttien muutoksia, lisäyksiä ja poistoja. Erityisesti suojattavien tietojen, kuten esimerkiksi arkaluonteisiksi katsottavien henkilötietojen, katselu tai saataville haku on voitava osoittaa lokeista.

Lokien avulla pitää voida valvoa järjestelmän toimintaa. Tämä voidaan mahdollistaa esimerkiksi lokien ohjelmistorajapinnalla (API, application programming interface), jonka kautta lokit voidaan liittää ulkopuoliseen valvontajärjestelmään. Yksinkertaisimmillaan lokeja pitää voida selailla toiminnan aikana (on-line).

Poikkeamatilanteiden hallinta

Toimittajalla tulee olla määritelty menettely, jonka mukaisesti se hallinnoi Tilaajaaan vaikuttavia tietoturvapoikkeamia. Poikkeamatilanteiden hallinta voidaan osoittaa työohjeilla ja työnohjausjärjestelmällä (tiketöintijärjestelmä).

Toimittajan tulee raportoida Tilaajalle ilman tarpeetonta viivettä kaikki sellaiset poikkeamat, joissa

- Tilaajaan liittyvien tietojen, kuten esimerkiksi henkilötietojen, luottamuksellisuus, eheys tai saatavuus on vaarantunut tai
- Tilaajalle tuotettavien Palvelujen turvallisuus on vaarantunut.

Poikkeamat tulee ilmoittaa Tilaajan yhteistyöhön nimeämälle yhteyshenkilölle.

Tilaajan suorittama valvonta

Tilaaja varaa mahdollisuuden kerätä käyttötietoja (lokia) Tilaajan tietoverkon ja tieto- ja viestintäjärjestelmien käytöstä virhetilanteiden ja tietoturvapoikkeamien selvittämiseen sekä yleiseen Tilaajan tietohallinnon tilannekuvan muodostamiseen.

Yhteystiedot ja Palvelun seuranta

Palvelun tai järjestelmän yhteyshenkilöt, yhteydenottotavat sekä Palvelun seurantatavat tulee kirjata ja jakaa kaikille osapuolille. Tietoturva-asioiden yhteydenpidon kannalta on tärkeä kirjata tietoturvapäälliköiden tai vastaavien yhdyshenkilöiden yhteystiedot sekä poikkeamahallintaan liittyvät menettelyt.