TULOSTUKSEN TIETOTURVAOPAS

2025

Canon

ESIPUHE

Tietoturva koskee kaiken kokoisia yrityksiä kaikilla toimialoilla. Erilaisten tietomurtojen tarkkaa lukumäärää on hankala arvioida, koska vain osa raportoidaan yleiseen tietoisuuteen. On kuitenkin selvää, että tietomurrot ja haittaohjelmat yleistyvät vuosi vuodelta ja kasvun voidaan suurella todennäköisyydellä olettaa jatkuvan myös tulevaisuudessa.

Työasemien ja mobiililaitteiden tietoturvaa pidetään itsestäänselvyytenä, mutta tulostusympäristöjen tietoturvan merkitystä ei aina ymmärretä. Monitoimilaitteet ja tulostimet ovat yhtä lailla alttiita hyökkäyksille ja tietovuodoille ja siksi olennainen osa kokonaisvaltaista tietoturvastrategiaa.

Canon on saanut tunnustusta alan johtavana toimijana tietoturvan näkökulmasta (*Quocirca Print Security Landscape* -raportti) ja siksi koemme vastuullemme jakaa tietoa turvallisuudesta tulostusympäristön kontekstissa suomalaisille yrityksille, olivat he asiakkaitamme tai eivät. Tämä opas on tietääksemme ensimmäinen tietoturvaan liittyvä opas toimialallamme. Oppaan tarkoituksena on avata tietoturvan moninaisuutta tulostusympäristöissä ja tarjota käytännönläheisiä keinoja sen vahvistamiseksi.

Jaakko Heinola
Marketing Director
Canon Oy

MIKSI TULOSTUKSEN TIETOTURVAOPAS?

Tulostuksen tietoturva on jäänyt hälyttävän pieneen rooliin, kun sitä verrataan tulostus- ja skannausinfrastruktuurin käsittelemän tiedon kokonaisarvoon. Parhaiten tietoturvaa tulostusympäristöissä voidaan parantaa lisäämällä tietoisuutta ja asiantuntemusta. Tämä opas on kattava katsaus aiheesta tarjoten sekä käytännöllisiä että strategisia suosituksia. Suositukset ovat mahdollisimman toimittajariippumattomia, jotta IT-päälliköt, tietoturva-asiantuntijat sekä tulostus- ja monitoimilaitteiden hankinnasta vastaavat saavat objektiivista tietoa tulostuksen tietoturvan tehostamisesta.

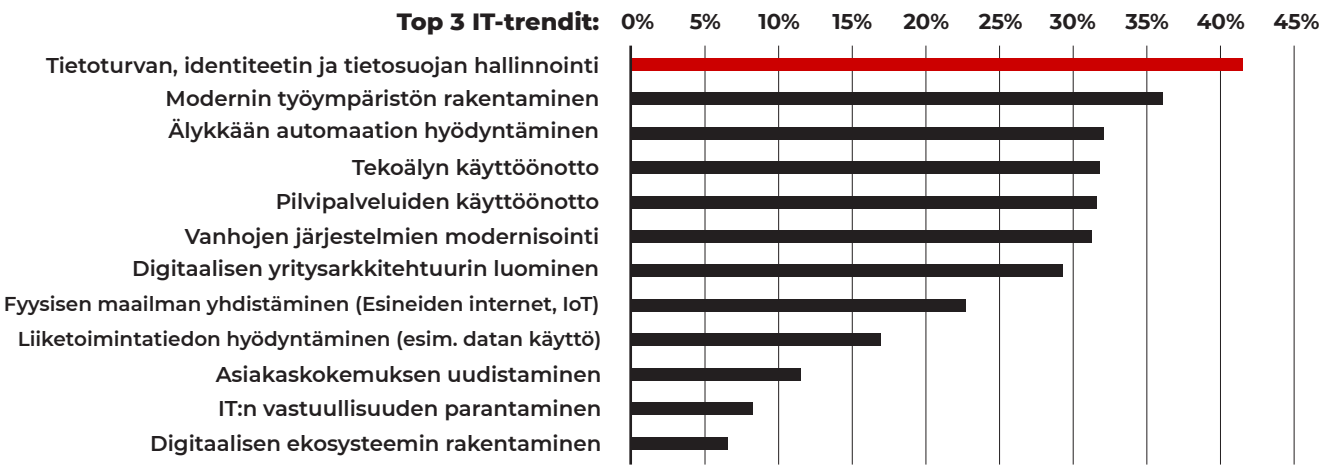
Taustaa

Omdian ***IT Enterprise Insights 2024*** **-tutkimus** osoittaa, että tietoturvan, identiteetinhallinnan ja yksityisyyden suojan hallinta on edelleen yksi merkittävimmistä IT-trendeistä globaalisti. **Yli 41 % organisaatioista** pitää sitä yhtenä kolmesta suurimmasta haasteestaan, ja haasteen ratkaiseminen koetaan entistä vaikeammaksi. Tutkimuksen mukaan yhä harvemmat organisaatiot kuvailevat tietoturvakäytäntöjään ”hyvin kehittyneiksi”, mikä viittaa siihen, että yritykset kamppailevat nopeasti kehittyvän uhkakentän ja kasvavien tietoturvavaatimusten kanssa.

Tulostuksen tietoturva on ajankohtainen aihe myös siksi, että tulostimet kohtaavat muiden päätelaitteiden tapaan viikoittain lukuisia tietoturvauhkia. Tulostimet ja monitoimilaitteet jäävät silti usein tietoturvastrategioiden ulkopuolelle ja monesti ne laiminlyödään myös tietoturvakäytäntöjen osalta. Tämä on huolestuttavaa, kun otetaan huomioon monitoimilaitteiden rooli mm. arkaluonteisten asiakirjojen käsittelyssä.

TIETOTURVA ON YKKÖSPRIORITEETTI

• Suurimmat teknologiset/digitaaliset haasteet liittyvät tietoturvaan ja tietosuojaan.



Tietoturva osaksi arkea

Kun tulostus sisällytetään organisaation tietoturvakäytäntöihin, voidaan paitsi vähentää tietomurtojen ja -vuotojen riskiä myös vahvistaa yksityisyydensuojaa ja yleistä tietoturvaa. Tämä edellyttää aktiivista viestintää laitetoimittajien kanssa uusien tietoturvaominaisuuksien ja -palveluiden hyödyntämiseksi sekä jatkuvan oppimisen kulttuurin edistämistä työntekijöiden keskuudessa.

Tietoturva osaksi strategiaa

Tulostuksen tietoturvan haasteiden ratkaisemiseksi vaaditaan kattava strategia, joka sisältää tulostus- ja skannauslaitteiden kartoituksen, riskien tunnistamisen, tulostimien sisällyttämisen nykyisiin tietoturvakäytäntöihin, riskiperusteisten toimenpiteiden toteuttamisen sekä tulostuksen tietoturvaan liittyvän tiedon ja käytäntöjen jatkuvan parantamisen.

Lue lisää Canonin tietoturvaratkaisuista:

canon.fi/business/solutions/security/

SISÄLLYS

OSA 1: TULOSTUKSEN TIETOTURVAN PERUSTEET

Monitoimilaitteet ja tulostimet ovat yleensä Linux-pohjaisia tietokoneita, joilla on lukuisia rajapintoja ja riippuvuuksia organisaation sisällä. Täten kaikki tulostimet kuuluvat IT-päätelaitteiden alle myös tietoturvan osalta.

Quocircan raportin ”*Print Security Landscape 2024*” mukaan vain 13 % yrityksistä ilmaisee täydellistä luottamusta tulostusinfrastruktuurinsa tietoturvaan. Samanaikaisesti hieman yli puolet ilmoittaa suorittaneensa virallisia tulostusympäristön tietoturva-auditointeja. Usein ero johtuu asiantuntemuksen puutteesta, mikä johtaa tulostuksen tietoturvan aliarviointiin ja mahdollistaa skenaarion, jossa tulostuslaitteita käytetään tietoturvahyökkäysten välineenä.

Miksi tulostuksen tietoturva pitäisi ottaa huomioon?

Tietokoneita, palvelimia ja sovelluksia koskevat vakiintuneet tietoturvakäytännöt, mutta usein tulostimet jäävät organisaatioiden IT-tietoturvastrategiassa huomiotta tai niitä pidetään sen näkökulmasta toissijaisina.

Todellisuudessa tulostimen on kyettävä kommunikoimaan kaikkien käyttäjien tietokoneiden ja organisaation kriittisten järjestelmien kanssa. Tulostimien on lisäksi kyettävä käsittelemään sekä arkaluonteisten asiakirjojen tulostusta että skannausta, säilyttämään odottavia tiedostoja ja toimimaan ympäristöissä, joissa yhdistyvät sekä suojatut että suojaamattomat verkot tai käyttöoikeudet.

Tulostimet saatetaan suojata vain epäsuorasti verkon tietoturvaprotokollien avulla. Suuret yksiköt toimivat usein ilman suoraa valvontaa, ulkopuolisten henkilöiden, työntekijöiden tai sisäisen IT-henkilöstön valvonnassa. Paikallisilla IT-osastoilla ei puolestaan välttämättä ole laajaa asiantuntemusta näiden järjestelmien suojaamisessa.

Tulostuslaitteisiin kohdistuu samanlaisia uhkia kuin muihin IT-päätelaitteisiin

Lisäksi niihin kohdistuu omia ainutlaatuisia haasteita, sillä ne tuottavat digitaalisia tai paperikopioita asiakirjoista ja lähettävät ne sallittuihin kohteisiin. Samanaikaisesti nämä laitteet saavat vain vähän huomiota IT-päälliköiltä. Tämän seurauksena tulostuslaitteista voi muodostua helppoja kohteita erilaisille hyökkäyksille, joten pienetkin parannukset tulostuksen tietoturvassa voivat johtaa merkittäviin parannuksiin suhteessa tehtyyn hankintaan.

Tulostuksen tietoturvan peruspilarit

Perehtyminen

Tulostimien ylläpito ja konfigurointi on usein ulkoistettu, mikä on saattanut jättää ne vähemmälle huomiolle tietoturvan näkökulmasta. Tulostusympäristön tietoturvan kohdalla tärkein tekijä onnistumisessa onkin asiaan perehtyminen. Tavoitteena ei ole tehdä tulostuksen tietoturvasta ensisijaista prioriteettia, vaan kehittää dokumentoitu ja organisaatiolle sopiva tapa hoitaa asia. Käytännössä tämä tarkoittaa monesti muutoksia vakiintuneisiin käytäntöihin.

Riskien arviointi

Nykyään organisaatioilla on mahdollisuus arvioida tietoturvariskejä järjestelmällisesti ja yhä laajemmin. Proaktiivisen riskien arvioinnin avulla voidaan määrittää tulostusinfrastruktuurille sopivat toimenpiteet ja keskittyä oikeisiin asioihin. Lisääntynyt kyberrikollisuus onkin nopeuttanut kehitystä, jossa myös pienet yritykset ottavat käyttöön tulostuksen tietoturvan hallintajärjestelmiä.

Kokonaisvaltaisuus

Mikään ei toimi eristyksissä, eivät edes tulostus- ja skannauslaitteet. Yksi yleisimmistä haasteista uusien järjestelmien integroinnissa liittyy siihen, että muutoksen vaikutuksia päivittäiseen työhön ei ehditä analysoimaan riittävästi. Kattavan tietoturvan saavuttamiseksi tulostusinfrastruktuuria tulisi kuitenkin analysoida vähintään kolmesta ohessa esitellystä näkökulmasta.

IT-infrastruktuurin näkökulma

- Mitkä ovat tulostimen tekniset tiedot?
- Mistä verkon sijainneista tulostimeen pääsee käsiksi?
- Missä määrin tulostin noudattaa sisäisiä käytäntöjä esimerkiksi salasanojen hallinnan ja päivitysten osalta?

Asiakirjan näkökulma

- Mitkä ovat yleisimmät dokumenttien työnkulut?
- Missä vaiheessa prosessia havaitaan ongelmia, jotka voivat johtaa asiakirjojen katoamiseen?
- Onko henkilökunnalla tiedossa organisaation hyväksytyt tulostus- ja skannauskäytännöt, joiden avulla vältetään tietoturvariskejä dokumenttien käsittelyssä ja lähetyksessä?

Laitetoimittajan näkökulma

- Tarjoaako toimittaja tarvittavat palvelut ja seurannan, jotka auttavat parantamaan tietoturvavalmiuksia nyt ja tulevaisuudessa?
- Onko toimittaja vaarassa rikkoa turvallisuuskäytäntöjä?
- Ottaako toimittaja tietoturvan kattavasti huomioon jo ennen laitteen toimitusta, sen käytön aikana sekä elinkaaren päättyessä?

Tulostuksen tietoturva – mistä aloittaa?

Kaikkien tulostuksen tietoturvan parantamiseen ja kehittämiseen vaikuttavien tekijöiden hahmottaminen voi olla haastavaa. Ohessa muutamia tärkeitä seikkoja, jotka toimivat riskienhallinnan perustana.

1. **Helppokäyttöisyys vs. turvallisuus**
   Kompromisseja on syytä välttää, kun kyse on tietoturvasta. Yksinkertaiset salasanat ovat laitehallinnan kannalta helpompia, mutta ne aiheuttavat huomattavan tietoturvariskin. Vahvat, yksilölliset salasanat yhdistettynä säännöllisiin salasanapäivityksiin parantavat laitteiden laitteiden tietoturvaa.

2. **Tulostuksenhallinnan käyttöönotto**
   Tulostuksenhallintaan sisältyvän turvatulostuksen kautta asiakirjat tulostetaan vain, kun valtuutettu käyttäjä on läsnä tulostimella. Asiakirjat tallennetaan ja siirretään turvallisesti yhdestä päätelaitteesta toiseen. Tämä minimoi riskin, että arkaluonteiset asiakirjat jäävät tulostimelle luvattomien henkilöiden saataville, mikä on yleinen syy tietojen hallinnan menetykseen tulostimia käytettäessä.

3. **Sijainnin huomioiminen**
   Tulostimen sijoittelu vaikuttaa sen käyttöön ja turvallisuuteen. Julkisissa tiloissa tai helposti ulkopuolisten saatavilla olevat tulostimet ovat alttiimpia luvattomalle käytölle ja tietoturvariskeille. On tärkeää ymmärtää, millaisia tietoja kullakin laitteella yleisesti tulostetaan ja harkita sijaintia tämän pohjalta. Tulostin, jolla käsitellään toistuvasti luottamuksellisia tietoja, tulisi sijoittaa valvottuun ympäristöön.

4. **Asiantuntemuksen taso**
   Tulostinten ja monitoimilaitteiden tietoturvan hallinta vaatii muiden laitteiden tavoin erikois-osaamista. On tärkeää varmistaa, että IT-osastolla on asianmukainen koulutus ja ymmärrys tulostuksen tietoturvasta. Yhteistyö toimittajien kanssa, jotka tarjoavat tietoturvaan liittyviä koulutus- tai konsultointipalveluja on hyvä vaihtoehto.

5. **IT-arkkitehtuurin arviointi**
   Tulostimen integroituminen organisaation IT-arkkitehtuuriin on syytä suunnitella huolella. Tämä kattaa verkon suunnittelun, integroinnin muihin järjestelmiin, tulostimen valvonnan ja sen toimintalokin tallennuksen.

6. **Perinteinen vs. Zero Trust –malli**
   Aiemmin keskityttiin suojaamaan verkon rajoja, kun taas uusi Zero Trust –malli perustuu siihen, ettei mihinkään luoteta oletuksena ja jokainen kirjautumispyyntö vaatii vahvistuksen – olipa yhteys verkon sisä- tai ulkopuolelta. Zero Trust -mallin mukaisesti suojattu tulostin voi esimerkiksi edellyttää todennusta jokaiselle tulostustyölle tai rajoittaa pääsyä käyttäjän roolin ja tarpeiden mukaan.

7. **Tietosuojan huomioiminen**
   Asiakastietojen tietoturvallinen hävittäminen ja poistaminen on oleellista tietoturvan kannalta. Tämä tulee huomioida laitteen elinkaaren hallinnassa ja erityisesti laitteen poistuessa toimitiloista. Toimittajilla on eritasoisia palveluja tietojen poistamiseen.

Miten tietosuoja liittyy tulostukseen?

Tietoturvalla on keskeinen rooli henkilö- ja yritystietojen suojaamisessa. Tulostuksen ja skannauksen tietoturvan parantaminen parantaa täten myös koko organisaation tietosuojaa. Ja toisaalta, näiden laiminlyönti aiheuttaa huomattavan riskin tietosuojalle, sillä tulostusinfrastruktuurissa käsitellään usein arkaluonteisia tietoja kuten henkilöstöhallintoon tai terveydenhuoltoon liittyviä asiakirjoja. Lisäksi tulostuslaite ja -ohjelmisto säilyttävät tietoja, jotka joko yksinään tai yhdessä muiden tietojen kanssa edellyttävät henkilötietojen suojaa. Esimerkiksi tulostimien sisältämissä osoitekirjoissa on laitteeseen rekisteröityjen käyttäjien tiedot ja organisaation tekniset yhteydet, kun taas tulostuslokit sisältävät yleensä käyttäjänimet, asiakirjojen otsikot ja aikaleimat.

Tietosuoja on ratkaisevan tärkeä osa kokonaisvaltaista riskien arviointia ja ymmärtämistä. Toisaalta, jos käyttäjäystävällisyyteen ei panosteta, työntekijät voivat turvautua itse hankkimiinsa ja IT-osaston hallitsemattomissa oleviin ratkaisuihin. Tällaiset ns. varjo-IT-ratkaisut voivat vaarantaa tietosuojaa huomattavasti.

Monitoimilaite toimii usein keskipisteenä yksilön tai organisaation tiedonkululle. Tulostuksen ja skannauksen mahdollistavat verkkolaitteet osallistuvat tietojen käsittelyyn, mikä ei pääty tulostustyön valmistumiseen, vaan pikemminkin se alkaa siitä. Niinpä parhaat tulokset saavutetaan, kun IT-asiantuntijat toimivat yhteistyössä tietoturva-asiantuntijoiden kanssa ja arvioivat eri skenaarioita yhdessä. Tulostus- ja skannauslaitteiden käytön tietosuojaan liittyvien riskien kokonaisvaltainen arviointi kattaa aina sekä digitaaliset että fyysiset työnkulut.

OSA 2: KÄYTÄNNÖN VINKKEJÄ PK-YRITYKSILLE

Pk-yritykset kohtaavat samanlaisia haasteita tulostusturvallisuuden saavuttamisessa kuin suuret organisaatiot, mutta yleensä niillä on vähemmän resursseja tarvittavien toimenpiteiden toteuttamiseksi. Osa yrityksistä saattaa jopa uskoa olevansa liian pieniä joutuakseen kyberrikollisten kohteiksi, vaikka suurin osa tietohyökkäyksistä tehdään ensisijaisesti voiton tavoittelun vuoksi, riippumatta kohteen koosta.

Pienemmät organisaatiot ovat houkuttelevia kohteita kyberrikollisille, sillä niillä ei usein ole resursseja neuvotella esimerkiksi tietomurron tekijän kanssa eikä asiantuntemusta ylläpitää kattavia varmuuskopioita järjestelmistään. Tämä voi johtaa siihen, että pk-yritykset maksavat huomattavia summia estääkseen toimintansa keskeytymisen kokonaan.

Onneksi pienilläkin organisaatioilla on hyvät edellytykset ennakoida huomioimalla tietoturvariskit ja näin varmistaa yrityksen toimintakyky.

Aloita perusasioista

Yksinkertaisilla toimenpiteillä on monesti suurin vaikutus. Heikot salasanat, päivittämätön laiteohjelmisto, suojaamattomat tiedonsiirrot tai fyysisen valvonnan puute aiheuttavat valtaosan tietomurroista. Kun laitekanta on pieni, näiden asioiden hallinta on kohtuullisen helppoa esimerkiksi puolivuositarkastuksilla. Ohjeet salasanojen vaihtamiseen, laiteohjelmistojen päivittämiseen ja muihin tietoturvaan vaikuttaviin asetuksiin löytyvät tulostimen käyttöoppaasta.

Vaadi laitetoimittajalta enemmän

Mitä ei itse pysty hoitamaan, sitä ei kannata jättää tekemättä. Esimerkiksi tulostuslaitteiden muuttuessa monimutkaisemmiksi, toimittajat tarjoavat yhä useammin mahdollisuuden ottaa vastuulleen koko tai osan ylläpidosta – mukaan lukien tietoturva. Tällaiset palvelut ovat saatavilla, vaikka organisaatiollasi olisi vain yksi laite. Keskeistä on kriittinen arvio siitä, mitä toimittaja voi tarjota suhteessa haluamaasi tietoturvatasoon sekä toimittajan kyky täyttää sopimuksen ehdot.

Muista tulostusympäristön hallinta

Turvatulostuksessa vain henkilö, joka on lähettänyt tiedoston tulostettavaksi, voi noutaa sen tulostimelta. Monille pienemmille organisaatioille tämä saattaa vaikuttaa tarpeettomalta, koska vain pieni joukko tuttuja henkilöitä käyttää tulostinta. Kannattaa kuitenkin aina varmistaa ratkaisun tietoturva, ja onko toimittajalla saatavilla pilvipohjaista tulostuksenhallinnan ratkaisua, vaikka käytössä olisi vain yksi laite. Tietoturvasertifioidut ratkaisut takaavat asiakirjojen end-to-end -salauksen, estäen tietojen päätymisen vääriin käsiin.

Tulostuksen tietoturvan tarkistuslista

Kartoita tulostusympäristö

Hanki kattava yleiskuva kaikista organisaation tulostuslaitteista, mukaan lukien niiden sijainnit ja verkkoyhteystoiminnot. Tämä luo hyvän pohjan haavoittuvuuksien tunnistamiselle ja tietoturvariskien priorisoinnille.

Ota käyttöön tulostuksenhallinnan ratkaisu

Hyödynnä pilvipohjaista tulostuksenhallintaa ja käyttäjän tunnistusta. Tämä varmistaa tulostustyön salauksen sekä sen, että asiakirjat eivät jää tulostimelle alttiiksi tietoturvaloukkauksille.

Varmista automaattiset päivitykset

Varmista, että kaikissa tulostimissa on uusimmat laiteohjelmistot ja automaattiset tietoturvapäivitykset. Laadi ohjeistus säännöllisiä tarkastuksia ja päivityksiä varten.

Rajoita pääsyä

Tiedätkö kenellä on fyysinen ja verkon kautta tapahtuva pääsy tulostimiin? Määritä pääsynhallinta sekä käyttäjä- että verkkotasolla. Poista käytöstä ne toiminnot, joita ei käytetä.

Lisää tietoisuutta

Toteuta koulutus- ja tiedotuskampanjoita, joilla koulutetaan työntekijöitä tietoturvatoimenpiteiden merkityksestä.

OSA 3: TIETOTURVAN HUOMIOIMINEN KILPAILUTUKSESSA

Uusia tulostusratkaisuja tai -palveluita hankittaessa kannattaa selkeät tietoturvavaatimukset sisällyttää jo tarjouspyyntöön, jotta tarjotut ratkaisut vastaavat nykyisiin tietoturvahaasteisiin. Teknologian nopean kehityksen ja pitkien hankintasyklien vuoksi on tärkeää, että toimittaja pysyy ajan tasalla ja tarjoaa laitteita, jotka säilyvät suorituskykyisinä ja mukautuvat tuleviin tarpeisiin vielä vuosienkin päästä.

Tulostuslaitteiden tietoturvavaatimukset tulisi kohdentaa nimenomaan näille laitteille, eikä vain soveltaa IoT- tai muiden päätelaitteiden hankintakriteereitä. Epärelevantit vaatimukset voivat aiheuttaa merkittävää työmäärää sekä toimittajille että ostajille, eivätkä ne varsinaisesti paljasta eroja tuotteissa tai toimittajan asiantuntemuksessa.

Kokosimme ehdotuksia vaatimuksista ja arviointikohdista, joita voidaan hyödyntää tulostukseen ja tulostuspalveluihin liittyvien tietoturvavaatimusten määrittelyssä. Vaatimukset on jaettu kolmeen kategoriaan: laitetoimittajaa, palvelua ja itse laitteita koskevat vaatimukset.

Laitetoimittajaa koskevat vaatimukset

ISO/IEC 27001-sertifikaatin vaatiminen on hyvä lähtökohta, sillä se osoittaa toimittajan kypsyystason sisäisen IT-turvallisuuden suhteen. Toimittajan on pyydettäessä eriteltävä kaikki erityisalueet, jotka jäävät sertifikaatin tavanomaisen kattavuuden ulkopuolelle. Tätä voi kartoittaa esimerkiksi kysymällä, onko sertifioinnin valvontatoimenpiteissä kohtia, joita ei ole huomioitu.

Toimittajan on sitouduttava noudattamaan yleistä tietosuoja-asetusta (GDPR) ja kyettävä kuvaamaan omilla ehdoillaan, miten se hallitsee tietosuojaa sekä paikallisesti että globaalisti. Henkilötietosuojan ymmärtäminen luo myös suotuisat olosuhteet poikkeamien hallinnalle ja viranomaisille raportoinnille tarvittaessa.

Palvelua koskevat vaatimukset

Tietoturvapalveluiden tulisi olla yksityiskohtaisesti määriteltyjä, jotta ostajan on helppo ymmärtää niiden hyödyt sekä mahdollisuus vertailla saatavilla olevia palveluita. Selkeästi määritellyt palvelut antavat ostajalle myös paremmat edellytykset arvioida palvelutoimitukseen liittyviä riskejä ja kehittää tarvittavia kompensoivia strategioita.

Lisäksi palvelun toimitusprosessista on annettava selkeä kuvaus. Osallistuuko siihen esimerkiksi kolmansia osapuolia? Tai miten asiakkaan tietoja käsitellään palvelun toimituksen aikana? Tällaiset kysymykset auttavat tunnistamaan toimitusketjuun liittyviä riskejä.

Laitteita koskevat vaatimukset

Laitteiden tulisi olla mahdollisimman hyvin tulevaisuuden vaatimuksiin mukautuvia. Laitteiden tulisi esimerkiksi tukea TPM 2.0 -teknologiaa, jotta ne täyttävät vähimmäisvaatimukset salausominaisuuksille, erityisesti NIS2-direktiivin näkökulmasta.

Laitteiden suojausominaisuudet käynnistyksen ja käytön aikana ovat myös oleellisia. Suojausten aktivointi estää luvattomat järjestelmämuutokset ja haittaohjelmien asennukset ja laite on suojattu hyökkäyksiltä käytön aikana.

SaaS-ratkaisujen osalta on tarpeen käsitellä tietosuojaan liittyviä riskejä, jotka liittyvät tietojen siirtoon kolmansiin maihin tai johtuvat riittämättömästä sisäänrakennetusta tietosuojasta. Käytännössä tämä voi tarkoittaa esimerkiksi sitä, kuinka yksinkertaista käyttäjätilien poistaminen on.

OSA 4: NIS2 JA UUSIEN KRITEERIEN VAIKUTUS TULOSTUKSEN TIETOTURVAAN

Kasvavan digitalisaation myötä kyberturvallisuus on noussut yhdeksi keskeisimmistä huolenaiheista. EU onkin ottanut käyttöön uuden NIS2-direktiivin (*Network and Information Security Directive 2*) torjuakseen yhä kehittyneempiä kyberuhkia. Direktiivi korvaa alkuperäisen 2016 NIS-direktiivin ja asettaa tiukemmat tietoturvavaatimukset verkoille ja tietojärjestelmille. NIS2 velvoittaa järjestelmälliseen kyberturvallisuuden ylläpitoon, mukaan lukien kyberturvaan liittyvien haavoittuvuuksien kartoittaminen ja korjaaminen, tietoturvakäytäntöjen kirjaaminen, henkilökunnan kouluttaminen sekä riskienhallinnan ja jatkuvuussuunnitelmien laatiminen.

Lainsäädäntö on laaja ja Suomessa sen täytäntöönpanossa on vielä tulkinnanvaraisuuksia. Seuraavaksi esittelemme arviomme tärkeimmistä kysymyksistä.

NIS2-direktiivi kattaa laajan kirjon erilaisten kriittisten alojen organisaatioita. Pääluokat sisältävät internet-palvelujen tarjoajat, terveydenhuoltopalvelut, julkishallinnon palvelut sekä energia- ja infrastruktuurialan toimijat. Yhteenvetona voi todeta, että monet organisaatiot kuuluvat joko suoraan NIS2:n piiriin tai toimivat alihankkijoina sen piiriin kuuluville organisaatioille.

Organisaation koolle on myös määritelty rajoja: alle 50 henkilöä työllistävät organisaatiot luokitellaan pieniksi organisaatioiksi, jotka on vapautettu direktiivistä. 50–250 työntekijän organisaatioilla on supistetut vaatimukset. Kriittiset organisaatiot eivät kuitenkaan ole vapautettuja direktiivistä, riippumatta työntekijöiden määrästä.

NIS2-direktiivin keskeinen osa velvoittaa sen piiriin kuuluvat organisaatiot arvioimaan toimitusketjunsa riskit ja asettamaan asianmukaiset tietoturvavaatimukset tarjousprosesseihin. Tämän seurauksena on kohtuullista odottaa, että suoraan NIS2-direktiivin alaiset organisaatiot asettavat toimittajilleen samanlaisia vaatimuksia kuin ne, joihin suhteessa ne itse ovat vastuussa. NIS2 auttaa luomaan vähimmäiskypsyystason IT-tietoturvan osalta useimmissa organisaatioissa, ottaen huomioon sen laajan soveltamisalan.

Mitä NIS2 sisältää?

NIS2 ei aseta tarkkoja vaatimuksia tietoturvaominaisuuksille, mutta se määrittelee vaatimuksia menettelyille ja tietoturvan hallinnalle kymmenellä keskeisellä osa-alueella. NIS2 korostaa, että organisaatioiden on arvioitava omat vastuunsa. Prosessi on kattava, ja onkin suositeltavaa viitata vakiintuneisiin standardeihin, riskiarviointeihin sekä tietojärjestelmien tietoturvakäytäntöihin. ISO/IEC 27001-sertifikaatin hankkiminen, jossa on määritelty valvontatoimenpiteet tietoturvan eri alueilla, osoittaa todennäköisesti myös NIS2-direktiivin noudattamisen.

Koskeeko NIS2 painettuja materiaaleja?

Jos tulostimet ovat olennaisia liiketoiminnallesi tai jos tulostimiin liittyvät tietoturvaloukkaukset voivat vaikuttaa haitallisesti toimintaasi, tämä on merkityksellinen alue. Näin ollen organisaatiosi tulostusinfrastruktuuriin tulisi tehdä riskinarviointi ja toteuttaa soveltuvat tietoturvatoimenpiteet.

Mitä toimenpiteitä voin tehdä tulostusympäristössä, jotta noudatan NIS2-vaatimuksia?

Vaadittavat toimenpiteet vaihtelevat riskiarvioinnin tulosten perusteella. Ei ole haittaa soveltaa järeämpää tietoturvaa kuin mitä on välttämätöntä. Canonilla suosittelemme turvallisimman mahdollisen perustason luomista, edellyttäen ettei siitä koidu muita haittoja liiketoiminnalle.

Miten tulostintoimittajat voivat auttaa NIS2-vaatimusten noudattamisessa?

Useimmat tulostintoimittajat ja tulostusratkaisujen tarjoajat voivat tarjota sekä neuvontaa että maksullisia tietoturvapalveluja. Canonin tapauksessa laitteiden tietoturvan vahvistaminen perustuu asiantuntijatietoon ja on linjassa parhaiksi havaittujen tietoturvakäytäntöjen kanssa.

Sertifioitu toiminta ja kyvykkyys tarjota tietoturvapalveluja antavat vankan perustan luottamukselle. Erityisesti organisaatioiden, joilla on korkeat tietoturvavaatimukset, tulisi pyrkiä arvioimaan toimittajan kyvykkyydet ennen tietoturvapalvelujen hankintaa.

OSA 5: VIISI ASKELTA TULOSTUKSEN TIETOTURVAN PARANTAMISEEN

Tässä osiossa esitellään järjestelmälliset käytännöt tulostimien tietoturvan parantamiseksi. Havainnot perustuvat vakiintuneisiin IT-tietoturvakäytäntöihin, joissa korostuu Canonin pitkällinen tulostuslaitteiden asiantuntemus. Lisäksi olemme tarkistaneet Kyberturvallisuuskeskuksen voimassa olevat tietoturvakäytäntöjen perusperiaatteet. Kyberturvallisuuskeskuksen ehdottamat toimenpiteet verkkolaitteiden osalta voivat olla laajempia esittämiimme toimiin verrattuna, joten tämä katsaus ei välttämättä kata kaikkia verkkolaitteisiin suositeltuja toimenpiteitä.

RISKIENHALLINNAN ALUEET

1: Tunnista tulostuslaitteet

Tulostuslaitteiden tietoturvan parantamiseksi on ensisijaisen tärkeää tunnistaa laitteiden ominaisuudet, sillä ylläpitoon liittyvät ominaisuudet voivat vaihdella paljonkin. Suosittelemme, että vähintään oheiset ominaisuudet dokumentoidaan ja tätä kartoitusta päivitetään säännöllisesti. Tämä on ratkaisevan tärkeää tietoturvallisten tulostuskäytäntöjen luomisessa.

Tärkeitä laiteominaisuuksia

- Mallityyppi ja merkki
- Laiteohjelmiston versio
- Käyttötarkoitus ja laitteen fyysinen sijainti
- Pääsyoikeudet asetusten muutoksiin ja pääsynhallinta
- Avoimet rajapinnat ja niiden roolit

TOIMENPITEET

- Tunnista tulostinten tietoturvaominaisuudet laiteominaisuuksien avulla
- Analysoi työskentelytavat ja tiedonkulku organisaatiossasi
- Laadi menettely, jolla tunnistetaan organisaatiossa käytössä olevat laitteet ja ohjelmistot

2: Tutustu organisaatiosi tulostimiin liittyviin riskitekijöihin

On tärkeää tiedostaa, mikä erottaa tulostimet muista päätelaitteista. Nämä ominaisuudet vaikuttavat tulostimien käytön riskiarvioon. Riskit voivat johtua sekä tulostimien normaaleista ominaisuuksista että tavasta, jolla ne on integroitu IT-infrastruktuuriin.

Jäävätkö tulostimet jäävät usein pitkäksi aikaa ilman valvontaa?

Tämä lisää todennäköisyyttä, että tulostimeen tehdään luvattomia muutoksia täysin huomaamatta.

Käyttääkö tulostimia sekä henkilöstö että ulkopuoliset käyttäjät (asiakkaat, muut vierailijat, huoltoteknikot, tilapäiset työntekijät)?

Tämä lisää riskiä, että luvattomat henkilöt pääsevät laitteelle huomaamatta.

Sijaitsevatko tulostimet turvavyöhykkeen ulkopuolella?

Tämä lisää riskiä, että arkaluonteisia asiakirjoja käsittelevällä laitteella ei ole asianmukaisia tietoturva-asetuksia.

Toimivatko tulostimet ”kaksoisroolissa” sekä sisäisinä että ulkoisina laitteina?

Tämä lisää riskiä siihen, että ulkopuoliset pääsevät käsiksi sisäiseen käyttöön tarkoitettuihin asiakirjoihin.

TOIMENPITEET

- Tutustu tulostimien ainutlaatuisiin ominaisuuksiin ja mahdollisiin riskeihin, joita valvomaton käyttö voi aiheuttaa liiketoiminnallesi
- Kartoita nykytilanne, mukaan lukien fyysinen sijaintipaikka, kulunvalvonta ja huoltomenettelyt

3: Sisällytä tulostimet tietoturvakäytäntöihin

Tulostuslaitteiden ominaisuuksien ymmärtäminen on olennaista, jotta sekä yleiset että tulostimiin liittyvät tietoturvatoimenpiteet voidaan toteuttaa kokonaisuutena. Riippumatta siitä, kuinka pitkälle organisaatiossa on edetty riskienhallinnassa, on tärkeää arvioida riskit, jotta toimenpiteet voidaan kohdistaa sinne, missä niitä tarvitaan eniten. Edelliset vaiheet toimivat pohjatyönä riskiarvion laatimiselle ja organisaatiokohtaiselle lähestymistavalle.

TOIMENPITEET

- Hyödynnä uutta tietämystä riskinarvioinnin tekemiseksi
- Toteuta riskiperusteisia strategioita
- Aikatauluta seurantatoimet
- Suorita säännöllisiä haavoittuvuusarviointeja

4: Tulostuksen tietoturvan vieminen käytäntöön – itsenäisesti tai palveluntarjoajan avustuksella

Kun tulostimet on sisällytetty olemassa oleviin tietoturvakäytäntöihin ja käytössä on kattava lista tulostuslaitteista ominaisuuksineen, on jatkotoimenpiteiden tunnistaminen ja priorisointi helpompaa. Tulostuksen tietoturvan toteutuksen kannalta on loogista hyödyntää toimittajan asiantuntemusta; pyörää ei tarvitse keksiä uudelleen.

Nykyään toimittajat voivat tarjota kokonaan tai osittain hallittuja palveluja, jotka ovat räätälöitävissä yrityksen erityisvaatimuksiin. Tämä keventää organisaation operatiivisten vastuuhenkilöiden työtaakkaa. Samalla se edellyttää, että organisaatiolla on riittävästi osaamista toimittajan seurantaan ja yhteistyön kehittämiseen. Näin molemmat osapuolet hyötyvät yhteistyöstä, kun organisaatiolla on kyky arvioida sekä laitetoimittajaa että itse laitteita.

TOIMENPITEET

- Keskustele toimittajan kanssa ymmärtääksesi mahdollisuudet ja toimintatavat laitekantaasi liittyen
- Lisää tietoturva kaikkiin hankintaprosesseihin
- Ota vastuu yrityksen tietoturvasta myös palvelujen käyttöönoton aikana

5: Pysy ajan tasalla - mukaan lukien tulostuslaitteet

Tulostuksen tietoturvaan liittyvät kartoitukset, riskiarvioinnit ja käytännön toimenpiteet toimivat myös perustana tulevaisuudessa, jolloin tulostusympäristön tietoturvaa kehitetään ja ylläpidetään. Tehokas jatkuva hallinta edellyttää ajantasaista tietoa tulostimien tietoturvasta ja ennakoivaa asennetta uusiin uhkiin ja parhaisiin käytäntöihin. Tulostuslaitteisiin liittyvien haavoittuvuuksien tunnistamisessa voidaan käyttää työkaluja, jotka ilmoittavat yleisistä haavoittuvuuksista ja paljastuneista tietoturvapuutteista (CVE).

Jos tietoturvapalveluiden hankintaa on päätetty lykätä, aktiivinen viestintä toimittajien kanssa on ratkaisevan tärkeää uusimpien tietoturvaominaisuuksien ja -palvelujen hyödyntämiseksi. Samanaikaisesti on tärkeää pitää toimittaja vastuullisena ja tarkistaa, että toimittaja pysyy teknologian ja palvelujen kehittämisen tasalla.

TOIMENPITEET

- Käynnistä osaamisen kehittäminen
- Määritä toimittajan vastuut ja kriteerit
- Hyödynnä tietoturvaan liittyviä asiantuntijapalveluita
- Käytä automatisoituja ja keskitettyjä työkaluja haittaohjelmien ja muiden tunnettujen uhkien hallintaan
- Selvitä palveluntarjoajan tietoturva ennen ulkoistamista

LÄHTEET JA TUKIAINEISTO

OTSIKKO JA VERKKO-OSOITE	QR-koodi
Managing security, identity, and privacy leads top three IT trends again in Omdia's latest IT Enterprise Insights survey, Omdia, 2025 omdia.tech.informa.com/om128365/managing-security-identity-and-privacy-leads-top-three-it-trends-again-in-omdias-latest-it-enterprise-insights-survey	
What are the key trends for print security in 2024 and beyond? Quocirca Print Security Landscape, 2024 quocirca.com/quocirca-print-security-landscape-2024/	
Security White Paper Guidance for Canon Printers and Multifunction Devices Functionality in Support of NIST SP 800-171 and NIST SP 800-172, Hardening Guide Security Whitepaper oip.manual.canon/USRMA-8995-zz-CSPS-enUS.pdf?webmnl=	
NIS2 tietoturvadirektiivi kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/nis2-euroopan-unionin-kyberturvallisuusdirektiivi	
Canon-laitteiden tietoturva canon.fi/business/solutions/security/device-security/	

Lisätiedot Canonin tietoturvaratkaisuista ja tuesta:

Ota yhteyttä verkkosivujemme kautta.
Canonin tietoturvapalvelut - Canon Oy