Tietoturvaraportti

Tulostuksen tietoturva

Painettujen ja sähköisten tulosteiden suojaaminen

SHARP
Be Original.

www.sharp.fi

Sisältö

.

Johdanto

Monitoimilaitteilla ja tulostimilla tuotettujen fyysisten ja sähköisten tulosteiden suojaamisen tarve on tietoturvan usein unohdettu osa-alue.

Sharpin määrittelyn mukaan tulostuksen tietoturva tarkoittaa monitoimilaitteilla tai tulostimilla paperille tai sähköisesti lähetettyjen asiakirjojen tietoturvaa. Määritelmä sisältää kaikki tulostetut asiakirjat ja sähköisessä muodossa olevat tiedostot, joita siirretään tietokoneelta tulostettaviksi (myös tulostus erillispalvelimien kautta), skannattavaksi (mukaan lukien skannaus kansioon, skannaus sähköpostiin, skannaus pilveen ja skannaus kiintolevylle) sekä faksattavaksi.

Tässä raportissa käsitellään seuraavat pääasiat:

- **Tausta**
  Tässä osiossa kerrotaan, miksi tulostus on monesti laiminlyöty tietoturvan osa-alue. Käsitellään myös mahdollisia haavoittuvuuksia, joista kaikkien IT-pääkäyttäjien on oltava tietoisia, esimerkkinä seuraavat:
  - Yhä yleisemmin organisaatioissa monitoimilaitteet tai tulostimet jaetaan entistä useampien käyttäjien kesken
  - Laitteisiin yhteydessä olevien käyttäjien määrä kasvaa, ja heidät on tunnistettava ja heidän toimintaansa hallittava
  - Tulostettavien ja valvontaa edellyttävien asiakirjojen määrä kasvaa
  - Ei ole sopivia työkaluja kaikkien tulostustoimintojen jäljittämiseen ja raportointiin.

- **Ongelma**
  Tässä osiossa käsitellään niitä tulostuksen hallintaan liittyviä haasteita, joita IT-päälliköt, loppukäyttäjät ja yritysjohto saattavat kohdata. Tällaisia haasteita ovat esimerkiksi tulostettujen asiakirjojen käyttöoikeuksien hallinta, käyttäjien toiminnan jäljitys, raportointi, tulostus mobiililaitteilta, asiakirjojen skannaus moneen kohteeseen sekä faksien lähettäminen organisaation ulkopuolelle.

  Käsitellään myös joitakin tutkimustuloksia, jotka osoittavat aiheen monimutkaisuuden ja ongelman suuruusluokan.

- **Ratkaisu**
  Tässä osiossa esitellään Sharpin tuotteita (ohjelmistoratkaisuja) sekä parhaita käytäntöjä. Niiden avulla voidaan rakentaa turvallinen tulostusympäristö sekä estää monitoimilaitteiden ja tulostimien luvaton käyttö sekä luvaton pääsy laitteilla tuotettaviin ja niihin tallennettuihin asiakirjoihin (mukaan lukien sähköisessä muodossa olevat kuvat asiakirjoista), kopioihin, fakseihin, skannattuihin tiedostoihin ja paperitulosteisiin.

  Kerromme myös, miten Sharp voi ratkaista ongelmia auttamalla

  - valitsemaan oikean ratkaisun, joka vastaa vaatimuksianne ja auttaa rakentamaan vahvan perustan omalle tulostuksen tietoturvapolitiikallenne. Tulostuksen hallintajärjestelmällä voidaan valvoa käyttöoikeuksia, soveltaa tulostussääntöjä, rajoittaa toimintoja sekä varmistaa kaikkien tulostettujen asiakirjojen tarkka jäljitys ja raportointi.
  - valitsemaan sopivimman ratkaisutoimittajan tulostuksen hallintaan ja siihen liittyviin tulostustoimintoihin.

- **Yhteenveto**
  Yhteenvedossa kootaan yhteen aiheen pääkohdat ja keskitytään

  - merkittävimpiin jokaisen asiakirjatulostuksen aiheuttamiin liiketoiminnan haavoittuvuuksiin.

- tiivistelmään Sharpin tietoturvaratkaisujen pohjalta tehdyistä suosituksista
- seuraavaksi toteutettaviin vaiheisiin yhtenäisen tulostuksen tietoturvapolitiikan kehittämiseksi, mukaan lukien luotettavat työkalut, jotka soveltuvat käytettäväksi kaikkialla yrityksessä.

Taustaa

Kun yrityksissä pohditaan mahdollisia tietoturvariskejä, tullaan harvoin (jos koskaan) ajatelleeksi, että verkossa olevat monitoimilaitteet tai tulostimet voisivat olla ongelma, tulostetuista asiakirjoista puhumattakaan.

Quocirca-tutkimuslaitoksen mukaan 60 % organisaatioista on joutunut vähintään kerran puutteellisesti suojatuista tulostustoiminnoista johtuvan tietoturvaloukkauksen kohteeksi. Uhka on todellinen sekä pienissä että suurissa yrityksissä[1]. Vaikka käytössä olisikin tietoturvaratkaisuja tietojen suojelemiseksi eteviltä hakkereilta ja verkkorikollisilta, tämä ei välttämättä aina riitä.

Yksi yleisimmistä rikkeistä on nimittäin hyvin yksinkertainen: väärä henkilö ottaa tulostetun asiakirjan haltuunsa. Jos luottamuksellisia asiakirjoja jätetään monitoimilaitteelle tai tulostimelle liian pitkäksi aikaa, kuka tahansa voi päästä niihin käsiksi ja käyttää tietoja hyväkseen. Tästä voi aiheutua vakavia ongelmia.

56 % yrityksistä ei ota tulostimia huomioon päätelaitteiden tietoturvastrategiassaan.[2]

Kun ajattelee asiaa mahdollisen varkaan näkökulmasta, niin laitteen luovutustaso on helpoin paikka luottamuksellisten tietojen haltuun ottamiselle. IT-pääkäyttäjien usein aliarvioitu haaste onkin varmistaa, että tulostetut asiakirjat eivät jää suojaamattomina lojumaan monitoimilaitteen tai tulostimen päälle, mistä ne voivat joutua vääriin käsiin.

Kuitenkin kaikkien nykyaikaisten organisaatioiden kohtaamat tulostamisen tietoturvaan liittyvät haasteet kasvavat jatkuvasti monestakin syystä:

1. **Laitteiden määrä kasvaa**
   Yhä yleisemmin organisaatioissa monitoimilaitteet tai tulostimet jaetaan entistä useampien käyttäjien kesken, ja yritykset pyrkivät yhtenäistämään ja standardoimaan. Tästä aiheutuu monia haasteita, kun ei ole välineitä valvoa monitoimilaitteen ja tulostimen

   - toimintaa
   - tulosteita
   - tietoturvaa (osana verkkoa).

2. **Laitetta verkossa käyttävien henkilöiden määrä**
   Joissakin suurissa organisaatioissa saattaa olla satoja käyttäjiä, jotka käyttävät tulostamiseen kymmentä tai jopa yli sataa laitetta. Kun tähän lisätään tietoturvamääräysten (kuten GDPR) lisääntyminen, haasteet voivat olla huomattavia seuraavilta osin:

   - Käyttäjän tunnistus
   - Käyttäjätilien hallinta (kuten yhteydessä olevien käyttäjien määrän valvonta)
   - Käyttäjien ja olemassa olevien toimistojärjestelmien keskinäinen integrointi
   - Rajoitukset organisaatioiden järjestelmässä olevien käyttäjäkohtaisesti tunnistettavien tietojen hallinnassa, kuten käyttäjien tunnistamattomaksi tekeminen GDPR:n mukaisesti.

3. **Valvottavana olevien tulostettujen asiakirjojen määrä**
   Jatkuvasti kasvava käyttäjämäärä ja käyttäjäkohtaisten tulostettujen sivumäärien kasvu tarkoittaa, että valvottavana on huomattavan suuri määrä tulosteita:

- kopioidut asiakirjat
- tulostetut asiakirjat
- skannatut asiakirjat
- faksatut asiakirjat
- Älypuhelimilta ja tableteilta tulostetut asiakirjat (mobiilitulostus / BYOD).

4. **Valvontatyökalujen puute**
   Yleisesti ottaen on pulaa työkaluista, joilla kaikki tulosteet voidaan jäljittää ja raportoida luotettavasti.

Ongelma

Tulosteiden tietoturva tulisi nähdä yhtenä keskeisenä osa-alueena jokaisessa monitoimilaitteita ja tulostimia käyttävässä nykyaikaisessa yrityksessä.

Oikeat työkalut

Tutkimusanalyytikot korostavat tarvetta varmistaa työkalujen ja toimenpiteiden riittävyys, kun käsiteltävänä ja hallittavana on suuri joukko tulosteita sekä tulostuslaitteita ja niiden käyttäjiä.

Tulosteiden suojaaminen

Jokaisen IT-pääkäyttäjän haasteena on ratkaista, miten hallita yrityksen verkkoon rekisteröityneiden käyttäjien joukkoa ja heidän käyttäjätilejään. Käyttäjien määrä tietenkin vaikuttaa hallinnollisen työn määrään. Se myös lisää käyttäjien ja heidän tulostamiseen liittyvän toimintansa (kopiointi, tulostus, skannaus ja faksaus) hallintaprosessin monimutkaisuutta. Haasteena on siten tulostamisen tietoturvan tehokas hallinta.

Jotkin yleisimmistä menetelmistä, kuten PIN-koodit, käyttäjätunnukset ja salasanat, kortit sekä avaimenperät (fob), ovat tehokkaita tulosteiden suojaamistapoja. Huonosti toteutettuna ja hallittuna nämä menetelmät voivat kuitenkin olla varsinainen pääkäyttäjän painajainen. Tämä korostuu entisestään, kun monet IT-pääkäyttäjät haluavat myös liittää laitteita ja niiden tulosteita olemassa oleviin järjestelmiin, kuten Microsoft-tileihin.

Asiakirjojen ja valvomattomien tulosteiden määrä

Tulosteiden määrän kasvu on suuri haaste. Tämä koskee sekä perinteisiä paperisia asiakirjoja, joita tulostetaan tai kopioidaan laitteilla, sekä sähköisiä asiakirjoja, jotka lähetetään monitoimilaitteille tai tulostimille yrityksen verkon kautta tai jotka skannataan tai faksataan.

Uudet määräykset, kuten GDPR, ovat myös aiheuttaneet monia kysymyksiä: miten valvomattomat tulosteet voidaan suojata ja miten hyvin edellä mainituissa tulostus- ja viestintäkanavissa säilytettävät henkilötiedot todellisuudessa on suojattu.

Riskien ymmärtäminen

Tehokkaan suojan toteuttaminen edellyttää perinpohjaista ymmärrystä eri toimintoihin liittyvistä riskeistä:

- **Kopiointi**
  Kopiointi oli yleisin asiakirjojen jakamistapa 1980- ja 90-luvuilla, mutta tulostus on syrjäyttänyt sen. Kopiointi on silti edelleen tulostuksen hallintajärjestelmissä merkittävä valvontakohde etenkin yrityksen luottamuksellisten asiakirjojen osalta.

- **Tulostus**
  Tulostus on ilman muuta tänä päivänä erittäin yleinen tapa jakaa yrityksen asiakirjoja. Jos tulostusta ei valvota tai se ei ole keskitetysti hallinnassa, siihen liittyy monia riskejä. Riskejä ovat muun muassa

  - Suojaamaton ja valvomaton pääsy monitoimilaitteisiin ja tulostimiin sekä laitteiden toimintoihin ja ominaisuuksiin, kuten kiintolevyihin.
  - Avoin pääsy tulostettuihin asiakirjoihin, jolloin kaikki toimiston käyttäjät ja työntekijät (ja mahdollisesti jopa vierailijat) pääsevät käsiksi valvomattomiin asiakirjoihin.
  - Ei ole mahdollista jäljittää ja raportoida käyttäjien toimintaa, eli kuka on tulostanut mitäkin tiettynä ajanjaksona.
  - Ei ole mahdollista jäljittää ja ehkäistä käyttäjien tietoturvaloukkauksia, joista saattaa seurata huomattavia sakkoja tai syytteitä GDPR:n kaltaisten tiukkojen tietoturvamääräysten takia.
  - Ei ole mahdollista jäljittää mobiilikäyttäjiä eikä mobiililaitteilta (esimerkiksi älypuhelimilta ja tableteilta) tulostamista.

- **Skannaus**
  Skannauksesta voi aiheutua lisäpulmia tietoturvaprosessin kannalta, sillä verkkokansioiden ja sähköpostien lisäksi

asiakirjoja voidaan skannata myös ulkopuolisiin pilvipohjaisiin järjestelmiin. Skannaukseen liittyy myös seuraavia riskejä:

- yrityksen luottamuksellisten tietojen skannaaminen ulkoisiin kohteisiin, eli skannaaminen henkilökohtaisiin sähköpostiosoitteisiin yritysosoitteiden sijasta
- skannaus ilman IT-pääkäyttäjän hyväksyntää samanaikaisesti moneen kansioon sen sijaan, että skannataan määrättyihin henkilökohtaisiin yrityskansioihin tai verkkokansioihin
- skannaus ilman indeksointia, mistä saattaa aiheutua pahoja ongelmia, kun yritetään löytää ja tarkastaa skannattuja asiakirjoja ja tarkastaa skannaukseen liittyviä toimintoja (skannauksen tulokset ja kohteet).

- **Faksaus**
  Skannauksen tavoin faksien lähettäminen on yrityksen tulostuksen tietoturvastrategian mahdollinen heikko kohta. Riippumatta siitä, lähetetäänkö faksit analogisesti vai sähköpostitse, faksattuihin asiakirjoihin liittyy yhtä suuri tietomurtojen vaara kuin skannattuihin asiakirjoihin.

- **Mobiilitulostus – BYOD (Bring Your Own Device)**
  Monien tutkimusyritysten mukaan mobiilitulostuksen merkitys tulee olemaan tulevaisuudessa erittäin suuri. Se tuo kuitenkin mukanaan haasteita. Yrityksen on mietittävä, miten mobiilit tulostusratkaisut sovitetaan nykyaikaiseen organisaatioon tai miten mobiilikäyttäjien toimintaa voidaan seurata ja hallita luotettavasti. On myös tärkeää pohtia, miten mobiilitulostusstrategia sopii organisaation kokonaisstrategiaan. Valitettavasti monissa yrityksissä ei ole vielä ymmärretty, että työntekijöiden liikkuvuus on kasvava trendi tai suoranainen liiketoiminnan edellytys. Siksi tulostuksen tietoturva usein unohdetaankin tältä osin.

- **Jäljitys ja raportointi**
  Asiakirjojen tulostuskanavien tietoturvan lisäksi tulostettujen tietojen jäljitys ja raportointi ovat yrityksille melkoinen ongelma.

  On tärkeää, että tarkastusraportti on myös luotettava ja suojattu:

  - Kuka pääsee käsiksi tietoihin?
  - Ovatko tiedot luotettavia?
  - Voidaanko tiedot tehdä tunnistamattomiksi?
  - Kuka hallinnoi järjestelmää?

Suositukset

On erittäin tärkeää ymmärtää, että tulostuksen tietoturva on vain yksi toimiston tietoturvan osa-alue, ja sen sopiva toteutus voi vaihdella organisaatiosta toiseen.

Joissakin yrityksissä saatetaan tulla siihen tulokseen, että kunhan verkon tietoturvaan liittyviin menettelyihin suhtaudutaan vakavasti ja ne toteutetaan huolellisesti, muuta ei tarvita. Kuitenkin liiketoiminnan kasvaessa myös laadittujen asiakirjojen määrä kasvaa – ja samalla myös niihin liittyvät tietoturvahaasteet.

Tietoturvan osalta on omaksuttava laajempi lähestymistapa, jossa verkon suojaamisen lisäksi suojataan kaikki tulostettu tieto ja asiakirjat, jotka luodaan ja jaetaan organisaation ulkopuolelle.

Toisin sanoen verkon ja siihen liitettyjen päätelaitteiden suojaaminen on välttämätöntä. Tulosteiden tietoturvan varmistaminen on luonnollinen askel verkon tietoturvan parantamiseen suurten yritysten lisäksi myös nopeasti kasvavissa PK-yrityksissä.

Tulostuksen hallintasovellukset, kuten Sharpin optimoidut tulostusratkaisut ja optimoidut skannausratkaisut, auttavat suojaamaan kaikki toimiston tulosteet, integroimaan laitteet nykyisten järjestelmien (Windows) kanssa sekä ottamaan nopeasti käyttöön johdonmukaisen tulostuksen ja skannauksen tietoturvapolitiikan.

Tulostuksen tietoturvan tärkein tekijä on valvonta: kaikkea, mitä voi valvoa, voi myös mitata ja suojata. Sharpin järjestelmien avulla kaikki tulostetut asiakirjat ja tiedot ovat täydellisesti valvonnassa, oli kyseessä sitten kopiointi, tulostus, skannaus tai faksaus.

Koska tulostushallinta on saumattomasti liitetty nykyiseen tulostuslaitteistoonne, säästätte paljon arvokasta aikaa. Esimerkiksi kaikkien käyttäjien vieminen Lightweight Directory Access -protokollan (LDAP) kautta käy helposti ja nopeasti. Kaikki käyttäjät voidaan lisätä, tunnistaa ja integroida järjestelmään muutamassa sekunnissa. Lisäksi kaikki käyttäjän tunnistetiedot siirretään Transport Layer Security (TLS) -salausprotokollalla tietojen sieppaamisen estämiseksi.

Tämän tulostuksen suurimpana etuna ovat kuitenkin edistyneet ominaisuudet, jotka helpottavat kaikkien IT-pääkäyttäjien ja käyttäjien elämää huomattavasti.

- **Käyttäjän tunnistus**
  Tämä on ensimmäinen ja tärkein tekijä tulostushallintajärjestelmässä. Ohjelmisto tarjoaa monta tapaa käyttäjien tunnistamiseen ja käyttöoikeuden antamiseen verkossa oleviin laitteisiin. Nopeimmat ja suosituimmat nykyisin käytössä ovat tavat ovat läheisyyskortit ja avaimenperät. Henkilön tunnistautumistiedot tallennetaan niihin, ja tunnistus tapahtuu laitteeseen asennetun kortinlukijan avulla. IT-pääkäyttäjien valittavana on useita muitakin tunnistusvaihtoehtoja, kuten PIN-koodi, käyttäjätunnus ja salasana sekä biometriset lukijat.

  On myös mahdollista käyttää yrityksessä jo ennestään käytössä olleita kortteja, joilla pääsee sisään rakennuksiin, tietyille osastoille tai suojattuihin huoneisiin. Kortti- ja lukijastandardeja on useita, ja niissä käytetään erilaisia viestintämenetelmiä ja taajuuksia. Siksi kehotammekin ottamaan yhteyttä Sharpin ratkaisukonsultteihin oikean järjestelmän valitsemiseksi yrityksellenne.

- **Turvallinen tulostusjono**
  Asiakirjan lähettäminen tietokoneelta tulostettavaksi tavalliseen tapaan käynnistää viestinnän tietokoneen ajurin ja tulostuksen hallinnan välillä. Ainoastaan rekisteröityneet käyttäjät voivat tulostaa järjestelmään ja ainoastaan luvallisilla laitteilla, jotka on varustettu tarvittavalla ohjelmistolla. Käyttäjä lähettää työn tulostuksenhallintapalvelimelle, ja kun käyttäjä kirjautuu laitteeseen

(läheisyyskortilla, PIN-koodilla tai käyttäjätunnuksella ja salasanalla), järjestelmä tunnistaa hänet rekisteröidyksi käyttäjäksi, jolla on tulostusoikeus.

- **Turvatulostus**
  Mahdollisuus turvalliseen tulostusjonoon ja töiden pidättämiseen palvelimella on kätevä myös siksi, että se mahdollistaa turvatulostuksen kaikilta järjestelmään liitetyiltä laitteilta. Siten käyttäjä voi tulostaa miltä tahansa laitteelta, joka voi sijaita eri osastolla, eri kerroksessa tai jopa toisessa rakennuksessa (edellyttäen, että kyseessä on sama verkko), tai mistä tahansa, missä tulostushallinta on asennettuna.

  Turvatulostus merkitsee myös vähemmän tulostuksesta aiheutuvia katkoja liiketoiminnassa. Kun jokin tulostuslaite on poissa käytöstä tai huollettavana, työnsä voi tulostaa lähimmältä käytettävissä olevalta laitteelta.

- **Automaattinen töiden poisto**
  IT-pääkäyttäjien haasteena on myös tulostusta tai indeksointia odottavien tilapäisesti talletettujen asiakirjojen suuri sivumäärä. Tämä ei kuitenkaan ole ongelma, jos tulostuksen hallinta on käytössä. Automaattisen töiden poistotoiminnon ansiosta pääkäyttäjät voivat määritellä asiakirjojen säilytyspolitiikan. Jos asiakirja esimerkiksi on tulostettu kahdeksalta aamulla eikä sitä ole vapautettu laitteelta 24 tunnin kuluessa, se poistetaan automaattisesti palvelimen jonosta. Tämä ominaisuus on täysin konfiguroitavissa ja riippuu kunkin organisaation tarpeista.

84 % organisaatioista pitää tietoturvaa ykkösprioriteettina nykyhetkestä vuoteen 2025, ja tietoturva-asiantuntemus tulee olemaan tärkein toimittajan valintakriteeri 58 %:lle organisaatioista.[3]

- **Kaksoiskappaleiden estäminen**
  Tulostuksenhallintaratkaisujen etuna on myös tulosteiden kaksoiskappaleiden estäminen. Tunnistauduttuaan ja kirjauduttuaan valittuun laitteeseen käyttäjät näkevät luettelon kaikista tulostettavaksi lähetetyistä tiedostoista. Tällöin on helppo huomata, onko jokin asiakirja lähetetty tulostettavaksi useaan kertaan, ja käyttäjä voi päättää, mitkä työt tulostetaan ja mitkä poistetaan jonosta. Lisäksi käyttäjät voivat valita, poistetaanko asiakirja jonosta tulostuksen jälkeen vai jääkö se edelleen jonoon.

- **Turvallinen skannaus, faksaus ja kopiointi**
  Tulostuksen hallinnan avulla laitteen kaikki toiminnallisuudet ovat valvonnassa. Kopiointi-, skannaus- ja faksaustoimintoja valvotaan samojen laitteen käyttöoikeuksien avulla, ja kaikkia näitä toimintoja voidaan vastaavasti seurata. Lisäksi:

  - Sharpin laitteissa käytetään TLS-protokollaa SMTP- ja S/MIME-sähköpostisalaukseen turvallisten sähköpostiyhteyksien takaamiseksi.
  - Monitoimilaitteen ohjaimen LAN-verkkoliittymäkomponentti on täysin erillinen faksin PSTN-puhelinlinjasta. Tämä estää mahdollisten hyökkääjien pääsyn monitoimilaitteen tai paikallisverkon sisäisiin järjestelmiin.

- **Jäljitys ja raportointi**
  Monille organisaatioille jäljitys ja raportointi ovat tärkeimmät pohdittavat alueet. Tulostuksen hallintajärjestelmän avulla kaikki toiminnot ovat jäljitettävissä. Riippumatta siitä, onko kyseessä tulostus, skannaus, kopiointi vai faksaus, kaikki työt kirjataan järjestelmään. Yksityiskohtaisia raportteja voidaan luoda henkilökohtaisen tilin, osaston tai erityisen asiakaslaskutusvaihtoehdon perusteella.

- **Käyttäjätietojen peittäminen GDPR:n mukaisesti**
  GDPR:n 17 artiklassa annetaan yksityiskohtaiset ohjeet henkilötietojen käsittelystä. Siihen sisältyy "oikeus saada rekisterinpitäjä poistamaan rekisteröityä koskevat henkilötiedot ilman aiheetonta viivytystä, ja rekisterinpitäjällä on velvollisuus poistaa henkilötiedot ilman aiheetonta viivytystä". Sharpin tulostuksenhallintajärjestelmälle tämä ei ole ongelma. Sen avulla kaikki käyttäjätiedot voidaan tehdä tunnistamattomiksi määräysten mukaisesti. Silloinkin, kun käyttäjätiedot on poistettu, IT-pääkäyttäjillä on edelleen käytettävissä tilastotietoja käyttöraporttien luomista varten.

- **Mobiilitulostus**
  Mobiilitulostus on hyvin yksinkertainen käsite – käyttäjät voivat tulostaa tavalliseen tapaan omalta älypuhelimeltaan tai tabletiltaan. IT-pääkäyttäjät voivat päättää, mikä sovellus on heidän organisaatiolleen paras. Sharpin optimoitu mobiilisovellus voidaan kokonaisvaltaisen konfiguraationsa ansiosta jäljittää tulostushallinnan kautta. Kaikki mobiilisti tulostetut asiakirjat raportoidaan järjestelmään, ja niitä voidaan käyttää tilastoihin ja raportteihin.

Vieläkin vahvempaa tietoturvaa

Tulostuksen tietoturvalla on tärkeä rooli oman tulostuksen tietoturvapolitiikkanne määrittelylle, rakentamiselle ja toteuttamiselle.

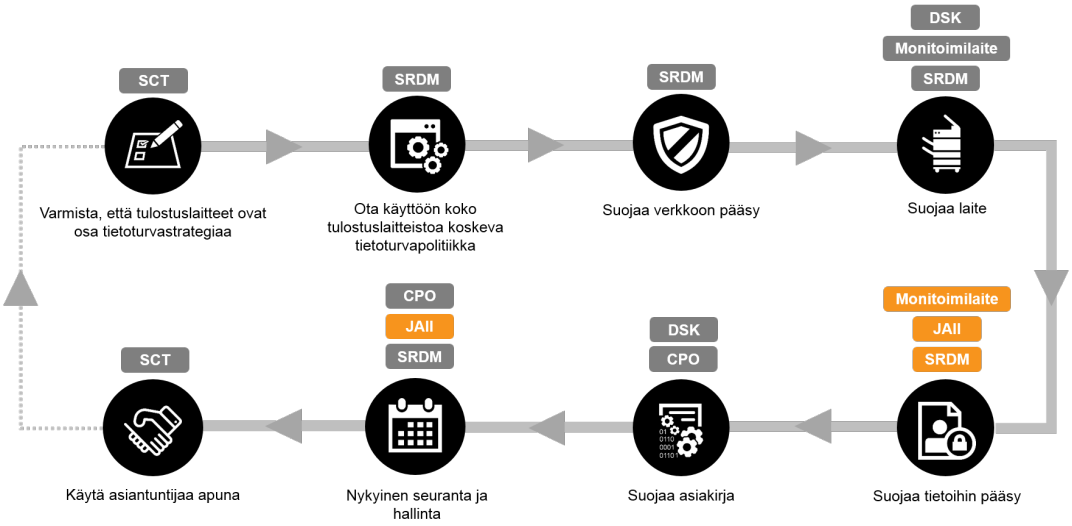
- Sharpin optimoidun portfolion tulostuksenhallintatuotteet ovat erityisen arvokkaita tällaisen politiikan yhteydessä käytettynä lähinnä siksi, että ne tehostavat tietoihin pääsyn suojausta sekä jatkuvan hallinnan ja valvonnan vaiheita.

- Kun otetaan mukaan vielä muita tuotteita Sharpin valikoimasta, kuten Tietoturvakitti (DSK), Sharp Remote Device Manager (SRDM) ja Cloud Portal Office (CPO), voidaan rakentaa ainutlaatuinen, järeä ja yhtenäinen tietoturvajärjestelmä, joka täyttää sekä IT-vastaavien että liiketoiminnan tarpeet täydellisesti.

Parhaan mahdollisen tietoturvatason takaamiseksi yritysten kannattaa tehdä yhteistyötä sellaisten toimittajien kanssa, jotka tulostushallinnalla saavutettavien etujen lisäksi pystyvät luotettavasti ja vahvalla kokemuksella liittämään eri osa-alueet yhteen.

Sharpilla on vuosien kokemus tietoturvallisimpien monitoimilaitteiden ja tulostimien valmistajana, tulostushallintasovellusten kehittäjänä ja monimutkaistenkin ratkaisujen toteuttajana. Siksi olemme todella päteviä neuvomaan ja ohjaamaan asiakkaitamme kaikilla tietoturvan osa-alueilla, mukaan lukien tulostuksen tietoturvamenettelyt.

Tulostuksen tietoturvapolitiikan rakentuminen ja Sharpin tarjoamat tulostuksen tietoturvaratkaisut



SCT – Sharp Consulting Team, **SRDM** – Sharp Remote Device Manager, **DSK** – Tietoturvakitti, **MFP** – Multifunction Printer (monitoimilaite), **JAII** – Job Accounting II, **CPO** – Cloud Portal Office

Yhteenveto

Tämän päivän yritysmaailmassa on tosiasia, että aina, kun jokin asiakirja tulostetaan, kopioidaan, skannataan tai faksataan, se voi joutua varkauden tai vahingonteon kohteeksi.

Yritysten pitäisi olla paljon paremmin selvillä suojaamattomiin luottamuksellisiin asiakirjoihin ja tiedostoihin liittyvistä riskeistä, olivatpa ne sitten fyysisessä tai sähköisessä muodossa. Tärkeimmät seikat voidaan kiteyttää seuraavasti:

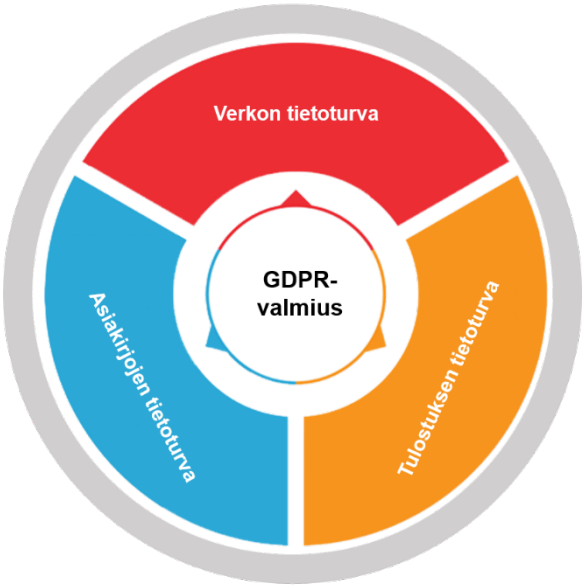
- Tulostuksen tietoturvasta huolehtiminen on nykyaikaisessa yrityksessä ensiarvoisen tärkeää yrityksen koosta riippumatta. Yrityksissä syntyvien asiakirjojen määrän kasvu on merkittävä haaste IT-ympäristön valvonnalle. Haasteet liittyvät erityisesti kasvavan käyttäjämäärän hallintaan, asiakirjojen koon kasvuun, jaettavan tiedon määrään, verkon ylikuormittumiseen sekä tulostuslaitteistoon.

- Tulostuksenhallintajärjestelmä mahdollistaa joustavan konfiguroinnin. IT-pääkäyttäjät voivat rajata toimiston laitteiden käyttöoikeudet tiettyyn ryhmään ja lisäksi jäljittää kaiken monitoimilaitteen käytön (kopiointi, tulostus, skannaus ja faksaus).

- Sharp ymmärtää tietoturvan merkityksen nykyaikaiselle yritykselle ja tarjoaa ainutlaatuisen kokonaisvaltaisen menettelytavan. Se kattaa verkon tietoturvan (kaikki yrityksen verkot ja kaikki niihin liitetyt päätelaitteet), tässä raportissa kuvatun tulostuksen tietoturvan sekä asiakirjojen tietoturvan kaikilta osin.

- Kokonaisvaltainen lähestymistapa tietoturvaan takaa myös sen, että organisaationne tietoturva noudattaa kaikilta osin uusimpia määräyksiä, kuten EU:n tietosuoja-asetusta (GDPR).

Sharpin tietoturvan runko



Mahdollisten haavoittuvuuksien ehkäisemiseksi muilla yrityksenne osa-alueilla ehdotamme, että tutustutte myös seuraaviin alueisiin liittyvän tietoturvan tehostamiseen:

- Verkon tietoturva
- Asiakirjojen tietoturva
- GDPR-asetuksen noudattaminen

Sharpin verkkosivuston Tietoturva-osiossa: https://www.sharp.fi/cps/rde/xchg/fi/hs.xsl/-/html/tietoturvallisuus.htm

Vaihtoehtoisesti voit ottaa yhteyttä Sharp Solutionsin konsultointitiimiin.

Lähteet

1. “Print 2025: Print Security in the IoT Era”, Quocirca, 2018
2. "Annual Global IT Security Benchmark Tracking Study", Ponemon Institute, maaliskuu 2015
3. “Print 2025: The future of print in the digital workplace”, Quocirca, 2018

www.sharp.fi

SHARP

Be Original.