Tietoturvaraportti

Verkon tietoturva

Toimiston verkossa olevien laitteiden suojaaminen

www.sharp.fi

SHARP
Be Original.

Sisältö

Johdanto

Tehokkaan tietoturvan varmistaminen yrityksen koko verkossa on nykypäivän verkottuneessa maailmassa tärkeämpää kuin koskaan.

Joka päivä yritetään lukemattomia kertoja varastaa, muokata laittomasti, siepata tai levittää luottamuksellisten asiakirjojen tietoja tai päästä luvattomasti käsiksi yksityisiin ja yritysverkkoihin. Tässä raportissa käsitellään yritysten IT-infrastruktuurinsa suojaamisessa kohtaamia haasteita verkossa olevien toimistolaitteiden osalta. Tällaisia laitteita ovat esimerkiksi monitoimilaitteet ja tulostimet.

Raportti on jaettu seuraaviin osa-alueisiin:

- **Tausta**
  Jokainen yritys kohtaa verkon tietoturvaan liittyviä haasteita, mutta nykyisten verkkoon liitettyjen monitoimilaitteiden ja tulostimien haavoittuvuudet jäävät usein vähälle huomiolle. Näiden tietoturva-aukkojen kautta hakkerit ja verkkorikolliset pääsevät sisään organisaatioihin varastamaan kiintolevyille ja muille verkossa oleville laitteille talletettuja luottamuksellisia tietoja. Tästä aiheutuu myös vahinkoa ja häiriötä yritystoiminnalle. Tällaisen tapauksen vaikutus tuottavuuteen ja kannattavuuteen voi olla valtava.

- **Ongelma**
  Suojaamattomiin monitoimilaitteisiin ja tulostimiin liittyviä riskejä ei aina ymmärretä tai niistä ei välitetä. Yritykseltä voi myös puuttua ongelman torjumiseen tarvittava osaaminen ja resurssit. Käyttäjien tietämättömyys usein vielä pahentaa ongelmaa, kun huonot käytännöt altistavat asiakirjat ja tiedot väärinkäytöksille täysin tarpeettomasti. Yrityksissä ymmärretään, mitä tulostuksen tietoturvapolitiikan laatiminen edellyttää, mutta prosessi voi olla monimutkainen ja aikaa vievä.

- **Suositukset**
  Kuvailemme joukon laitteisto- ja ohjelmistoratkaisuja sekä parhaita käytäntöjä, joiden avulla voitte rakentaa turvallisen tulostusympäristön sekä torjua luvattoman pääsyn ja hyökkäykset yrityksen verkossa oleviin laitteisiin. Tässä osiossa tarjotaan yksityiskohtaisia ratkaisuja muutamiin tärkeimpiin tietoturvahaasteisiin:

  - Kuusi vaihetta tulostuksen tietoturvatason määrittelyyn ja ylläpitoon Sharpin tekniikan ja Sharpin optimoitujen ohjelmistoratkaisujen avulla.
  - Valmiit ominaisuudet ja asetukset kaikissa Sharpin nykyisen malliston verkossa olevissa laitteissa, kuten salasanasuojaus, tietojen päällekirjoitus, salaus jne.
  - Valinnaisia ratkaisuja yhtenäisen tulostuksen tietoturvapolitiikan laatimiseen sekä helppoon ja tehokkaaseen tulostuslaitteistojen hallintaan, kuten Sharp Remote Device Manager (SRDM)
  - Valinnaiset monitoimilaitteen ja tulostimen edistyneet toiminnot ja ominaisuudet, kuten Tietoturvakitti
  - Sharpin suorakanavan kautta saatavilla olevat valinnaiset palvelut, kuten tietoturvatarkastus, tietoturva palveluna, tietojen poisto vuokrauksen päätyttyä jne.

- **Yhteenveto**
  Esitetään yhteenveto seuraavista:

  - Liiketoiminnan haavoittuvuuteen liittyvät löydökset jokaisen verkossa olevan monitoimilaitteen ja tulostimen osalta
  - Sharpin sisäänrakennettuihin ominaisuuksiin ja muihin Sharpin tietoturvaratkaisuihin perustuvat suosituksemme
  - Seuraavat vaiheet tulostuksen tietoturvapolitiikan laatimiseksi joko sisäisesti tai Sharpin Professional Services -tiimin asiantuntemuksen tukemana.

Taustaa

Viime vuosina tietotekniikan tehokkaan tietoturvan varmistaminen on käynyt yhä tärkeämmäksi. Yksi avainalue on kuitenkin jäänyt vaarallisen vähälle huomiolle.

Useimmissa tietoturvaan vakavasti suhtautuvissa organisaatioissa on varmistettu, että niiden verkko ja tietokoneet on suojattu uusimman tekniikan avulla. On esimerkiksi asennettu palomuureja, laadittu salasanasääntöjä, edellytetty käyttäjien tunnistautumista sekä suojattu tietoja salauksen ja sähköisen allekirjoituksen avulla.

Uudet tekniikat, kuten pilvipalvelut ja mobiilikäyttö, ovat tuoneet uusia haasteita IT-pääkäyttäjille ja tietoturvavastaaville. Nykypäivän älykkäissä monitoimilaitteissa ja tulostimissa on kuitenkin myös jo monenlaisia verkkoyhteys- ja tietojensäilytysmahdollisuuksia. Niitä voi oikeastaan jo kutsua tehokkaiksi ja monipuolisiksi tietokoneiksi. Markkinatutkimusyhtiö IDC:n mukaan Länsi- ja Itä-Euroopassa on toimisto- ja kotikäytössä lähes 53 miljoonaa tulostinta ja monitoimilaitetta,[1], ja useimmat niistä ovat yhteydessä verkkoon. Tämä tarkoittaa, että ne muodostavat liitäntäpisteen, jolla on IP-osoite. Siten ne ovat aivan yhtä alttiina haittaohjelmille ja hakkereiden hyökkäyksille kuin tavalliset tietokoneet ja mitkä tahansa verkkoon liitetyt päätelaitteet. Siksi niiden tiedot ja viestintä on suojattava aivan yhtä tehokkaasti.

Jos monitoimilaitteita ei suojata, hakkerit voivat päästä tunkeutumaan valvomattomien porttien ja protokollien kautta myös verkon muihin laitteisiin ja mahdollisesti luottamuksellisiin tietoihin. Monitoimilaitteen kiintolevylle tai muistiin tallennetut viestit ja tiedot saatetaan urkkia tai lähettää luvattomasti aivan mihin tahansa. Verkossa olevat laitteet voivat joutua myös palvelunestohyökkäysten kohteeksi. Niiden tarkoituksena on estää verkkoresurssien käyttö, millä on merkittävä vaikutus yrityksen tuottavuuteen. Lisäksi ne voivat tarjota avoimen väylän verkkourkinnalle, jonka tarkoituksena on päästä käsiksi luottamuksellisiin tietoihin tai tartuttaa verkkoon jokin virus.

25 % korjaustoimia vaatineista tietoturvaloukkauksista liittyi tulostamiseen.[2]

Tämä ei ole mitään huhupuhetta tai pelottelua, vaan erittäin todellinen uhka. IDC:n hiljattain tekemässä tutkimuksessa useampi kuin yksi neljästä vastaajasta kertoi merkittävästä tietoturvaloukkauksesta, joka oli vaatinut korjaustoimia. Näistä tapauksista yli 25 prosenttia liittyi tulostamiseen.[2]

Monitoimilaitteiden ja tulostinten suojauksen laiminlyönnistä voi aiheutua valtavat vahingot yrityksen liiketoiminnalle, kuten myös maineelle ja asiakkaiden luottamukselle. Tietoturvaloukkauksen vaikutuksia voivat olla mm. seuraavat:

- Tulojenmenetys
- Tuottavuudenheikentyminen, kun tiedot ja verkko eivät ole käytettävissä
- Kilpailukyvyn heikkeneminen varastettujen tietojen myötä
- Määräysten noudattamisen laiminlyönnistä seuraavat sakkomaksut
- Oikeusjutut
- Laitteiden ja verkkoresurssien luvaton käyttö.

Ongelma

Hakkeroinnista ja verkkohyökkäyksistä on tullut arkipäivää, ja haittaohjelmiin liittyvät välittömät uhat ovat täyttä totta kaikille yrityksille toimialasta ja koosta riippumatta.

Quocirca-tutkimusyhtiön toteuttamassa tutkimuksessa 63 % osallistuneista yrityksistä ilmoitti joutuneensa vähintään yhden tulostamiseen liittyvän tietoturvaloukkauksen kohteeksi. Tämä voi olla monelle yllättävä tieto.[3].

Miksi sitten yritykset eivät ole ryhtyneet järeämpiin vastatoimiin uhan torjumiseksi?

Valitettavasti riskit jäävät usein huomiotta, koska ei ymmärretä, miten haavoittuvaksi yrityksen verkkoon liitetyt monitoimilaitteet ja tulostimet tekevät koko järjestelmän. Niinpä monissa yrityksissä tulostuksen tietoturva tai verkossa oleviin laitteisiin liittyvät tietoturvajärjestelmät ja -välineet ovat puutteellisia. Puutteet voivat liittyä esimerkiksi henkilökunnan koulutukseen, parhaisiin käytäntöihin tai tietoturvamenettelyihin. Yrityskäytössä saattaa myös olla lähinnä kotikäyttöön tarkoitettuja laitteita, joiden tietoturvaominaisuudet ovat riittämättömät.

Etenkin pienissä ja keskisuurissa yrityksissä ei välttämättä ole käytössä mitään tulostuksen tietoturvatoimia eikä niissä välttämättä ole koskaan tehty tulostuksen tietoturvatarkastusta. Suuremmissa organisaatioissa puolestaan voi olla kokoon nähden riittämättömät henkilöresurssit tai laatutyökalut verkossa oleviin laitteisiin ja niihin liittyvään tekniikkaan kohdistuvien verkkohyökkäysten mittaamiseen, valvontaan ja torjumiseen.

Lisäksi käyttäjien huonot toimintatavat ovat usein huomattava haaste IT-pääkäyttäjille, sillä niistä voi aiheutua yritykselle merkittäviä tietoturvaongelmia. Huonoja toimintatapoja ovat esimerkiksi suojaamaton tulostus, asiakirjojen jättäminen ilman valvontaa monitoimilaitteelle tai tulostimelle, tulostus suojaamattomista USB-laitteista, tulostus ilman kattavaa salausta ja luottamuksellisten asiakirjojen tallennus monitoimilaitteen tai tulostimen kiintolevylle.

Lähes kaksi kolmesta yrityksestä on kokenut tulostamiseen liittyvän tietoturvaloukkauksen.[3]

Monissa organisaatioissa myös tietojen hävittäminen sopimuksen päättyessä voi olla todellinen ongelma. Tulostusprosessin yhteydessä monitoimilaitteen tai tulostimen kiintolevylle voi jäädä kopio laitteella tulostetuista tiedoista. Mitä tiedoille sitten tapahtuu, kun sopimus päättyy?

Valitettavasti verkon yhtenäisen tietoturvajärjestelmän tai tulostuksen tietoturvapolitiikan käyttöönotto verkossa toimivien monitoimilaitteiden ja tulostimien luvattoman käytön havaitsemiseksi ja estämiseksi voi olla erittäin monimutkainen ja aikaa vievä tehtävä. Seuraavat päävaiheet ovat lähes aina välttämättömiä:

- Ennustetaan ja arvioidaan verkon tietoturvajärjestelmän puuttumisen mahdolliset seuraukset.
- Todetaan mahdolliset haavoittuvuudet ja selvitetään, miten ne voisivat vahingoittaa verkon infrastruktuuria.
- Sisäistetään tehtävän vaikeusaste, joka on aina erilainen eri yrityksissä.
- Etsitään sisäisiä tai ulkoisia resursseja, jotka voivat auttaa ongelman ratkaisemisessa.
- Selvitetään, minkä työkalujen avulla voidaan seurata yrityksen kaikkia monitoimilaitteita tai tulostimia, estää luvaton pääsy verkossa oleviin laitteisiin ja hälyttää kaikesta epäilyttävästä toiminnasta
- Toteutetaan luotettava verkon tietoturvajärjestelmä, joka kattaa kaikki yrityksen erityishaasteet, ja ylläpidetään järjestelmää.

Suositukset

Jos edellä esitetty on saanut sinut huolestumaan oman verkkosi turvallisuudesta, niin... oikein hyvä! Yritykseesi kohdistuvaa riskiä ei pidä aliarvioida. Mutta ei syytä huoleen.

Haluamme esitellä yksinkertaisen tavan toteuttaa kattavat tulostuksen tietoturvatoimet yrityksessänne sekä kertoa, miten Sharp voi auttaa ymmärtämään ja parantamaan verkon tietoturvatasoa helposti ja vaivattomasti.

Aloita suojaus heti

IDC-tutkimuslaitoksen analyytikoiden tutkimuksessa kävi ilmi, että paperitulosteisiin perustuvan tulostus- ja asiakirjahallintatekniikan toimittajat keskittyvät tulostuslaitteiden tietoturvan parantamiseen estääkseen hakkerien pääsyn yritysten verkkoihin tulostuslaitteiden kautta."[4] Monissa yrityksissä tulostuksen tietoturva kuitenkin ohitetaan tai asetukset eivät ole asianmukaiset, jolloin yritykset ovat alttiina hyökkäyksille.

Seuraavassa esitetään luettelo tietoturvaominaisuuksista ja asetuksista, jotka ovat valmiina Sharpin monitoimilaitteissa ja tulostimissa ja voivat tarjota pika-apua. Ne kaikki voidaan helposti kytkeä päälle ja pois. Pääkäyttäjät voivat myös säätää asetuksia sekä muuttaa oletusturvatasoa, jolloin saatte yrityksellenne paljon tehokkaamman suojaustason omien erityistarpeidenne mukaisesti:

- Paikalliset hallinta-asetukset, kuten pääkäyttäjän salasanan vaihto, laitteen verkkosivulle pääsy, etäkäytön tietoturva
- Vakiotilan tietoturvaominaisuudet: porttiliikenteen valvonta, protokolla-asetukset, SNMP MIB -asetus, käyttöoikeuksien suodatus, SSL, S/MIME, IPSEC, IEEE802.1X, mobiilitulostuksen sallivat ja estävät protokollat, ulkoisten palvelujen asetukset, julkinen kansio - hajautettu palvelin (jaettu levy), seurantatunnus (seurantatietojen tuloste), käyttäjäasetukset, käyttäjien tietoturvan kiertoteiden salliminen ja estäminen, tallennettujen tiedostojen automaattinen poistaminen, koko tulostusjonon poistaminen virheen tapahduttua.
- Parannetut tietoturvaominaisuudet (perustietoturvatilassa): kiintolevyn tietojen ylikirjoitus (kiintolevyn tyhjennys) jokaisen kopiointi-, tulostus-, skannaus- ja faksaustoiminnon jälkeen, tallennusvälineen salaus, salasanasuojaus
- Samassa ryhmässä on useita edistyneitä valinnaisia asetuksia. Näiden asetusten avulla pääkäyttäjät voivat käyttää Sharpin edistyneitä tietoturvaominaisuuksia. Ne ovat hyödyllisiä suurinta mahdollista tietoturvatasoa tarvitseville organisaatioille, kuten puolustusvoimille, hallitukselle tai mille tahansa yritykselle, joka haluaa korkeimman mahdollisen tietoturvan:

  - Tietoturvakitti sisältää tietoturvakitin asennuksen, tietoturvan parannukset, tulostuksen tietoturvan parannukset, laiteohjelmiston validoinnin
  - Edistyneen tietoturvakitin sisältö on seuraava: HCD-PP Certified Advanced Security -tila (sisältää tavallisen tietoturvakitin), tallennusvälineen salauksen parannus, salasanavaatimuksen parannus, laiteohjelmiston turvallisuustarkastukset

Kuusi yksinkertaista vaihetta

Kun ajatellaan pitkän aikavälin tietoturvaa, seuraavat kuusi vaihetta tarjoavat rakenteisen tavan kehittää ja ottaa käyttöön oma yhtenäinen verkon tietoturvan runko.

1. **Verkkoon pääsyn suojaus**
   Jokainen verkkoon liitetty laite on yhtä turvallinen kuin verkon haavoittuvaisin kohta. Siten porttien ja protokollien valvonta kuuluu erittäin tärkeänä osana verkon tietoturvan ylläpitoon. Järkevän kokoonpanon avulla pääkäyttäjät voivat estää ei-toivotun toiminnan ja mahdolliset infrastruktuuriin kohdistuvat hyökkäykset. Seuraavat tekniikat sisältyvät turvallisen viestinnän varmistamiseen kunkin laitteen ja verkon välillä:

   - Käytetään IP-suodatusta (rajoitetaan tiettyjen IP-osoitteiden käyttöä) sekä MAC (Media Access Control) -suodatusta. Nämä suodatukset auttavat suojaamaan

verkkoa ja viestintäkanavia, sillä ne sallivat käytön vain määritellyistä IP-osoitteista tai -osoitealueista.
- Käyttämättömien porttien esto (niin, että vain tarvittavat toimivat) antaa lisäsuojaa ja mahdollistaa tehokkaamman verkon valvonnan estämällä luvattoman pääsyn kaikkiin verkkoon liitettyihin laitteisiin.
- Varmistetaan, että IPSec (Internet Protocol Security, tietoliikenneprotokolla suojattuun ja salattuun tiedonsiirtoon), TLS (Transport Layer Security, tietoliikenteen salausprotokolla) ja HTTPS (Hypertext Transfer Protocol Secure tiedon suojattuun siirtoon verkossa) on konfiguroitu suurimman suojaustason mukaisesti.

2. Laitteen suojaus (tietojen suojaaminen)
Monitoimilaitteiden ja tulostimien kiintolevyille tallennettujen tietojen suojaus voidaan varmistaa kahdella tavalla:

- Tietojen salaus on toiminto, jossa asiakirjat salataan monimutkaisella 256-bittisellä algoritmilla.
- Tietojen ylikirjoituksella poistetaan tiedot laitteen kiintolevyltä. Se varmistaa, että kaikki levyllä ennestään olevat tiedot sekä kaikki tulostettujen asiakirjojen sähköisessä muodossa olevat kuvat poistetaan pysyvästi kirjoittamalla ne yli jopa kymmeneen kertaan.

Mielenrauhan varmistamiseksi Sharp tarjoaa myös palvelun (esimerkiksi vuokrakauden päättyessä), jossa kaikki laitteessa oleva digitaalinen tieto poistetaan ja fyysinen kiintolevy tuhotaan.

3. Käytön suojaus (tunnistautumisen ja käyttöoikeuksien avulla)
Yksi tärkeimpiä vaiheita on varmistaa käyttäjien valvonta hallinnoinnin ja käyttöoikeuksien avulla. Tämän vaiheen tärkeimpiä toimintoja ovat seuraavat:

- Käyttäjien tunnistautuminen on prosessi, jossa pääkäyttäjä antaa monitoimilaitteiden ja tulostimien käyttöoikeuden ainoastaan rekisteröityneille käyttäjille. Käyttäjät on tunnistettava joko omaan käyttäjäluetteloon perustuvalla paikallisella tunnistautumisella tai verkkotunnistautumisella autentikointipalvelimella.

- Käyttäjätunnistuksen avulla ohjataan pääsyä yrityksen verkossa oleviin laitteisiin ja valvotaan laitteiden käyttöä. Käyttäjätunnusten avulla voidaan antaa käyttöoikeus vain tietyille henkilöille sekä rajoittaa pääsyä laitteen tiettyihin toimintoihin tai estää käyttö kokonaan. Pääkäyttäjä voi myös konfiguroida laitteisiin pääsyn käyttäjän tunnistetiedot sisältävien tunnistekorttien avulla.

4. Luottamuksellisten tietojen turvallinen tulostaminen
Luottamukselliset asiakirjat tulee aina tulostaa turvallisesti niin, etteivät ulkopuoliset pääse näkemään eivätkä kopioimaan niitä. Tyypillisessä suojauksessa työ jää tulostuskomennon jälkeen laitteen kiintolevylle odottamaan ja tulostuu vasta sitten, kun käyttäjä on syöttänyt etukäteen konfiguroidun PIN-koodin. Kun asiakirja on tulostettu, kaikki tiedot poistetaan automaattisesti kiintolevyltä.

5. Verkon käytön valvonta
Oikein käytetyillä verkon tietoturvavälineillä kaikki verkossa olevat laitteet ovat kokonaan pääkäyttäjien valvonnassa suoraan työpöydältä käsin. Pääkäyttäjät voivat siten valvoa kaikkia monitoimilaitteita ja tulostimia sekä havaita, korjata ja hallita useimpia mahdollisia tietoturvauhkia. Laitteiden kloonausmahdollisuus myös yksinkertaistaa pääkäyttäjien työtä ja antaa lisää mielenrauhaa, kun kaikki laitteiden asetuksiin tehdyt muutokset on helppo viedä koko laitteistoon.

6. Oikean kumppanin valinta
Monet yritykset tarjoavat tulostuksen tietoturvaan liittyviä ammattilaisten palveluja, mutta asiantuntemuksen taso voi vaihdella melkoisesti. Sharp suhtautuu verkon tietoturvaan erittäin vakavasti, ja tietoturva on jokaisen uuden tuotekehityshankkeen keskiössä. Laitevalmistajana arvioimme laitteemme Common Criteria -sertifikaatissa määriteltyjen kattavien ohjeiden mukaisesti. Maailmanlaajuisesti tunnettu JISEC (Japan's IT Security Evaluation and Certification) on arvioinut riippumattomasti Sharpin verkkoon liitettävät monitoimilaitteet, joissa on sisäänrakennettu tietoturvatoiminto. Sharpin monitoimilaitteiden todettiin olevan Common Criteria -normien Hard Copy Device Protection Profile v1.0 (HCD-PP v1.0) standardin mukaisia. Tämä tarkoittaa, että Sharpin laitteet soveltuvat maailman luottamuksellisimpia tietoja käsitteleville asiakkaille.

Asiantuntija-apu

Kaikki edellä esitetty saattaa kuulostaa pelottavalta, mutta on tärkeää muistaa, ettet ole yksin – asiantuntija-apua on aina saatavilla.

Sharp tarjoaa monia eri ratkaisuja, työvälineitä ja palveluita verkkonne haavoittuvuuksien tarkistamiseen ja mittaamiseen, parannussuunnitelman laatimiseen sekä mahdollisten toteutusvaihtoehtojen suunnitteluun.

- **Tulostuksen tietoturvatyöpaja**
  Sharpilla on käytettävissään monia työkaluja ja tekniikoita, joiden avulla organisaationne voi oppia ymmärtämään tietoturvauhkia ja jotka auttavat tekemään johtopäätökset ja rakentamaan räätälöidyn parannussuunnitelman.

  Tarkastuksessa keskitytään kaikkiin verkossa oleviin oheislaitteisiin ja niiden turvallisuuteen. Mittaamme kaikki laitteissa käytettävissä olevat vakio- ja edistyneet ominaisuudet sekä tarjoamme työkalut tehokkaaseen uhkien havaitsemiseen ja torjuntaan. Tarkastamme myös, ovatko yrityksessänne käytössä olevat laitteet tarkoituksenmukaisia. Voimme tarjota yrityksellenne ja laitteiden käyttäjille parhaan mahdollisen tietoturvan. Lisäksi tulostuksen tietoturvatarkastuksessa hahmotellaan seuraavaksi toteutettavat vaiheet johdonmukaisen tietoturvapolitiikan kehittämiseksi tulostukseen sekä käsitellään kaikki yrityksen tietoturvan osa-alueet:

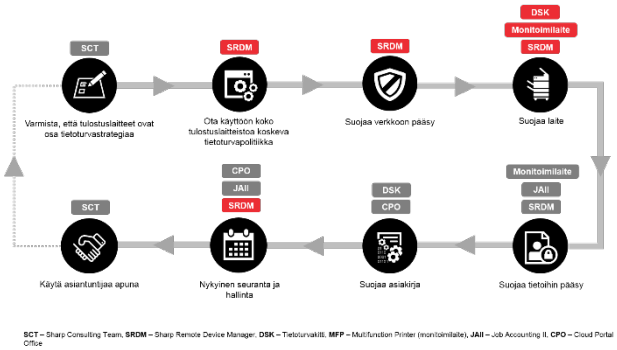
Office

- Verkon tietoturva – tässä asiakirjassa kuvattuna
- Tulosteiden tietoturva – kattaa kaikki asiakirjojen monistamiseen liittyvät toiminnot, kuten tulostuksen, skannauksen, faksauksen ja lähettämisen sähköpostitse
- Asiakirjojen tietoturva – liittyy toimistossanne käytettävien sähköisten ja paperiasiakirjojen hallintaan.
- GDPR:n noudattaminen – varmistetaan EU:n viimeisimpien tietoturvaan ja henkilötietojen suojaukseen liittyvien määräysten noudattaminen.

- **Tietoturvapaketti**
  Tietoturvapaketti kokoaa yhteen asiakastyöpajan, Sharp Remote Device Managerin asennuksen sekä valinnaisen tulostushallintajärjestelmän konfiguroinnin ja käyttöönoton toimiston tietoturvan tehostamiseksi – verkon tietoturva ja tulostuksen tietoturva

- **Sharp Remote Device Manager (SRDM)**
  Tämän Sharpin työkalun avulla saatte kriittiset tietoturva-asetukset käyttöön muutamassa sekunnissa. Toteutuksesta huolehtii Sharpin ammattitaitoinen tiimi palveluna. Kaikki tarpeidenne ja vaatimustenne mukaiset tärkeät tietoturva-asetukset toteutetaan IT-ympäristöönne, ja kaikki Sharpin monitoimilaitteet ja tulostimet ovat tällöin hallinnassa.

Tulostuksen tietoturvapolitiikan kehittäminen ja Sharpin tarjoamat verkon tietoturvaratkaisut



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

Yhteenveto

Mitä siis opimme tästä? Hyvä uutinen on se, että kaikki uutiset eivät suinkaan ole huonoja!

Vaikka monitoimilaitteisiin ja tulostimiin liittyykin vakava (ja edelleen aliarvioitu) uhka yrityksen tietoturvalle, riskin pienentämiseen on tarjolla monia tehokkaita keinoja.

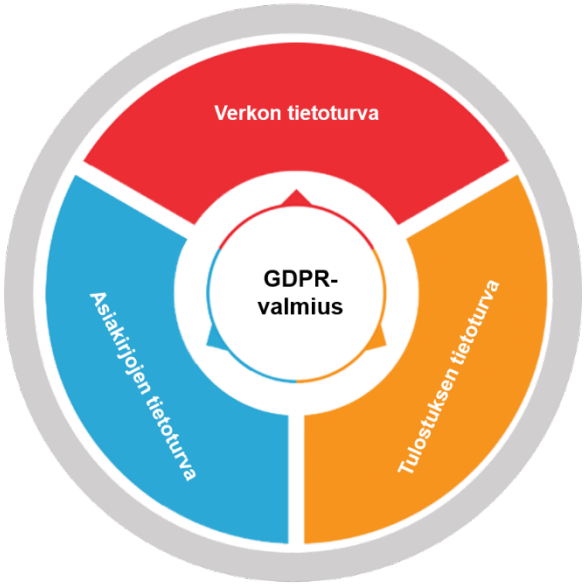
- **Et ole yksin – uhat koskevat kaikkia.** Päivittäin saamme kuulla tietomurroista, verkkohyökkäyksistä, viruksista ja muusta kaikenkokoisiin yrityksiin kohdistuvasta vahingonteosta. Tärkeintä on ymmärtää, mitä omalle yrityksellenne tapahtuisi, jos se joutuisi hyökkäyksen kohteeksi. On kysyttävä itseltään: "Kykeneekö yritykseni puolustautumaan tositilanteessa?"

- **Ratkaisu ei ole aina yksinkertainen.** Tarvittavien tietoturvatoimien ja -toimintojen selvittäminen, hankkiminen ja toteuttaminen voi kestää varsin kauan ja olla todella hankalaa. Koska jokainen organisaatio on erilainen, on käytettävä erilaisia välineitä ja kehitettävä yksilöllisiä strategioita, jotka sopivat juuri teidän yritykseenne kohdistuvien uhkien torjuntaan. Olivatpa erityistarpeenne millaiset tahansa, Sharp voi auttaa toteuttamaan tehokkaan tietoturvaratkaisun monitoimilaitteidenne ja tulostimienne suojaksi.

- **Jos yrityksenne ei ole valmistautunut tietoturvauhkiin, pyrkikää sisäistämään ongelma.** Miksi yrityksenne on haavoittuvainen? Onko käytössä riittävän hyvät työvälineet ja resurssit verkon ja tulostuksen tietoturvapolitiikan laatimiseen tai parantamiseen? Vai kannattaisiko yrityksenne kääntyä Sharpin asiantuntijoiden puoleen ja pyytää heitä tarkastamaan verkkonne ja siihen liitetyt laitteet sekä tarjota yrityksellenne asianmukaiset tietoturvatyökalut?

- **Asettakaa omat tietoturvatavoitteenne.** Jotta voisitte ymmärtää mahdolliset heikot kohdat sekä suojattavat kohteet, vastatkaa seuraaviin kysymyksiin: "Missä organisaatiomme pitäisi olla muutaman vuoden päästä?" ja "Miten yrityksemme voi valmistautua toteuttamaan asianmukaisten menettelytapojen ja välineiden käyttöönottovaiheet verkkohyökkäysten, haittaohjelmien ym. riskien estämiseksi tulevaisuudessa?"

Sharpin tietoturvan runko



- **Varmista, että käytettävissä on oikea asiantuntemus.** Jos yrityksellänne on itsellään tarvittavat resurssit, voitte kehittää oman tulostuksen tietoturvapolitiikkanne. Toisena vaihtoehtona on käyttää Sharp Professional Services -tiimiä, joka auttaa rakentamaan tehokkaan tietoturvajärjestelmän ja ottamaan käyttöön oman yrityksenne toiminnan ja tarpeiden kannalta olennaisia työkaluja, kuten:

  - Sharpin turvalliset verkkolaitteet, jotka ovat viimeisimpien tietoturvasertifikaattien mukaisia
  - Sharpin tietoturvaohjelmistot, ratkaisut ja palvelut, jotka auttavat laatimaan

tulostuksen tietoturvapolitiikan: DSK, SRDM, Print Security Audit jne.

- **Me olemme sinua varten.** Me voimme varmistaa, ettei tulostamisen tietoturvapolitiikkanne tarkistuksessa ja toteuttamisessa esiinny odottamattomia viivytyksiä. Sharpin edustajat ovat valmiita auttamaan liiketoimintanne nykyisen tietoturvatason selvittämisessä ja arvioimisessa. He ehdottavat strategiaa, jonka tuloksena syntyy yrityksenne tarpeisiin ja vaatimuksiin sopiva johdonmukainen tulostamisen tietoturvapolitiikka. Asiantuntijamme auttaa teitä valitsemaan sopivat työkalut ja palvelut seuraavista:

  - Sharpin vakiotietoturvaominaisuudet
  - Valinnaiset välineet, kuten SRDM
  - Valinnaiset parannukset, kuten DSK
  - Sharpin verkon tietoturvapaketti
  - Sharpin tietoturvatarkastus
  - Tulostamisen tietoturvapolitiikka.

- **Katso aina kokonaiskuvaa.** Organisaationne muilla alueilla mahdollisesti esiintyvien haavoittuvuuksien torjumiseksi voimme auttaa valitsemaan muita tietoturvamenettelyjä Sharpin portfoliosta, niin että voitte varmistaa täydellisen kattavan suojan kaikille yrityksenne osa-alueille:

  - Verkon tietoturva
  - Tulostuksen tietoturva
  - Asiakirjojen tietoturva
  - GDPR-asetuksen noudattaminen.

Kaikista Sharpin tietoturvaratkaisuista on lisätietoja Sharpin White Paper -kirjastossa ja Tietoturva-osiossa verkkosivustollamme: https://www.sharp.fi/cps/rde/xchg/fi/hs.xsl/-/html/tietoturvallisuus.htm

Voit myös ottaa yhteyttä Sharp Solutionsin konsultointitiimiin.

Lähteet

1. “Eastern and Western Europe Single-Function Printer & MFP Market Placements in the last five years” report, IDC, Q4 2018
2. “IT and Print Security Survey 2015” IDC, syyskuu 2015
3. “Printing: a false sense of security”, Quocirca, 2013
4. “Transformative Technology in Document Security”, IDC, toukokuu 2015

www.sharp.fi

SHARP

Be Original.