

Turvallisen tulostus- ekosysteemin ylläpitäminen

Osa Brotherin
digimuutoksen sarjaa



Tutkimukseen perustuva
ajatusjohtamisen raportti

brother.fi

Tulostus- turvallisuuden investoimisen esteet

Paljon julkisuutta saaneiden tietosuojarikkomusten ja tietomurtojen vuoksi useimmat pienet ja keskisuuret yritykset ovat tulleet hyvin tietoisiksi siitä, että IT-järjestelmien turvallisuudesta on tärkeää huolehtia.

IT-järjestelmien tietoturvan hallitseminen on haaste, johon pitää suhtautua kokonaisvaltaisesti: tulostimien, skannereiden ja kopiokoneiden tietoturvasta on huolehdittava siinä missä muidenkin tietoteknisten laitteiden. Jos näiden laitteiden tietoturva ei ole kunnossa, ne saattavat tarjota hakkereille helpon pääsyn yrityksen verkkoon. Tietoisuus näistä ongelmista on kasvussa pk-yrityksissä, joista **72 %** kertoo pitävänsä tulostimien, skannereiden ja kopiokoneiden tietoturvaa erittäin tärkeänä asiana. Vieläkin akuutimpi asia on yrityksissä, joissa käsitellään arkaluonteisia tietoja, kuten asiantuntijapalveluiden (**82 %**) ja terveydenhuollon (**81 %**) aloilla.

Kuitenkin lähes kolmannes yrityksistä ei ole tietoisia tietoturvan tärkeydestä. Lähes puolessa yrityksistä ei uskota, että yrityksessä on tehty riittäviä investointeja tulostinturvallisuuteen.

Jos yrityksissä ymmärretään tulostusturvallisuuden investoimisen merkitys, miksi investointeja ei kuitenkaan toteuteta?

Tutkimuksemme osoittaa, että selkeitä pääsyitä on kaksi:



riittämättömästi määritetyt vastuut tulostinturvallisuudesta



riittämätön ymmärrys ja tieto tietoturvauhkista ja -standardeista

Tämä raportti on laadittu pk-yritysten päättäjille. Tarkoituksena on auttaa heitä ymmärtämään tulostusturvallisuuden merkitystä ja ottamaan käyttöön turvallisia tulostusratkaisuja. Raportti on osa sarjaa, joka tarjoaa tietoa digiteknologian mahdollisuuksista pk-yritysten päättäjille. Raportit perustuvat kattaviin tutkimuksiin, jotka on tehty EMEA-alueen pk-yritysten päättäjien keskuudessa. Sarja käsittää neljä raporttia, joissa käsitellään seuraavia aiheita:

- Digitaaliset työkulut
- Oikeiden ratkaisujen valinta
- Tietoturva
- Vastuullisuus



Kenen vastuulla tulostusturvallisuus on?

On aivan liian yleistä, että tulostusturvallisuuteen liittyviä vastuita ei ole määritelty riittävän selkeästi eikä vastuuta ole osoitettu tietyille taholle. Lähes puolet (**44 %**) Länsi-Euroopan pk-yrityksistä kertoo, että yrityksessä ei ole selvyyttä siitä, kenen vastuulla tulostusturvallisuus on. Kun vastuutahoa ei ole määritelty, tulostusturvallisuuteen liittyvä päätöksenteko ja siitä huolehtiminen kärsivät, mikä altistaa yrityksen tietomurroille.

Vastuuta tulostusturvallisuudesta ei usein ole määritelty, sillä tulostimia ei ole totuttu näkemään tietoturvan kannalta heikkona kohtana samalla tavalla kuin esimerkiksi kannettavia tietokoneita. Tutkimuksemme kuitenkin osoittaa, että päättäjät ovat alkaneet ymmärtää tulostusturvallisuuden olevan elintärkeää. Se vain ei vielä näy pk-yritysten työtehtävien jaossa.

Puutteita vastuunjaossa esiintyy erityisesti pk-yrityksissä, joissa koko yrityksen laitteisto- ja ohjelmistokannasta vastaavia työntekijöitä on yleensä hyvin vähän. Jos yrityksen IT-asiantuntijat eivät ole tietoisia tulostusjärjestelmiin liittyvistä riskeistä, asia voi jäädä liian vähälle huomiolle.

Kaikille yrityksen työntekijöille kuuluu kuitenkin tietty vastuu huolehtia siitä, että arkaluonteiset tiedot pysyvät suojassa.



IT- ja teknologia-asiantuntijat vastaavat itse laitteiden turvallisuudesta, mutta vastuu tietojen suojaamisesta on jokaisella työntekijällä. Tietosuoja onkin mahdollisesti merkittävin kaupallisesti arkaluonteiseen yritystietoon liittyvä riski.

Tietosuojaan liittyy monenlaisia uhkia, kuten



tulosteiden joutuminen väärin käsiin



uloskirjautumisen unohtaminen luottamuksellisten asiakirjojen tulostamisen jälkeen



jäljitettävyyden puute siitä, kuka on vapauttanut mitkään asiakirjat tulostimelta

Lähes yhdeksässä yrityksessä kymmenestä on ilmennyt tulostamiseen liittyvä tietoturvaongelma...



...ja seitsemän kymmenestä (**72 %**) kertoo, että tietosuoja on suurempi uhka kuin laiteturvallisuus. Tällä hetkellä kuitenkin alle yksi kolmesta yrityksestä kertoo olevansa varmoja siitä, että yrityksen tulostusinfrastruktuuri on riittävästi suojattu. **53 %** yrityksistä puolestaan uskoo, että yrityksen laiteturvallisuus on kunnossa.

Suurin osa pk-yrityksistä (**64 %**) kertoo myös, että tietoturvasta huolehtiminen on niille tärkeä asia. Sitä pidetään tärkeänä haasteena, joka voi myös estää tehokasta toimintaa.

Tällä hetkellä lähes puolet pk-yrityksistä (**48 %**) kertoo, että yrityksessä on käytössä vain vähän tai ei lainkaan prosesseja, jotka mahdollistavat tulosteiden käytön seurannan. Siksi ei ole yllätys, että lähes yhdeksän yritystä kymmenestä (**86 %**) kertoo, että niissä on ilmennyt tulostamiseen liittyvä turvallisuuspuute.

Tavallisimmin tietoturvaongelmat liittyvät tulostimeen valvomatta jääneisiin luottamuksellisiin asiakirjoihin, tulosteiden noutamatta jättämiseen ja muiden kuin omien tulosteiden noutamiseen tulostimesta.

Siksi suurin osa pk-yrityksistä (**64 %**) on nyt alkanut ottaa käyttöön ratkaisuja tulostusturvallisuuden parantamiseksi, kuten rajoittamaan käyttäjien oikeuksia tiettyihin tulostimiin tai ottamalla käyttöön tunnisteita tai PIN-koodeja tulosteiden vapauttamiseen.

Tämä on askel oikeaan suuntaan. Tulevina vuosina kaikkien yritysten on tärkeää ottaa käyttöön tietoturvallisempia prosesseja. Tällä matkalla jo nyt olevien yritysten taas tulee ylläpitää ja kehittää vastuujärjestelmäänsä ja auditointikäytäntöjään.

Aito tietoturva syntyy, kun yrityksessä täytetään kolme tärkeää tavoitetta.

Ne liittyvät sekä laitteiden että tietojen suojaamiseen:

Luottamuksellisuus

Luottamuksellisten yritystietojen suojaaminen takaa, että tiedot päätyvät vain tarkoitettujen vastaanottajien saataville. Tämä tunnistus- ja valtuutusmenetelmä edellyttää, että käyttäjät tunnistautuvat tulostimia käyttäessään ja että heillä on valtuudet kyseisiin tietoihin tai tehtäviin, ennen kuin tulosteet voidaan vapautta.

Laiteturvallisuus

Laitteiston laiteohjelmiston tulee olla ajan tasalla ja turvallinen sekä ehkäistä hakkerointia ja muita ulkoisia uhkia.

Käytettävyys

Yrityksen pitää huolehtia siitä, että laitteet ovat käytettävissä ja valtuutetut käyttäjät voivat käyttää niitä.

Tiedon puute saa aikaan heikkoja turvallisuus-käytäntöjä

Alle kolmannes (**32 %**) pk-yritysten ylimmistä IT-päätäjistä kertoo, että heillä on syvällistä tietoa tulostamiseen liittyvistä turvallisuuskäytännöistä ja mahdollisista uhkista. Jos IT-päätäjillä ei ole riittävää tietoa uhkista, yritykset eivät pysty huolehtimaan riittävästä tietoturvasta. Pk-yrityksissä IT-päätöksenteosta vastaavat yleensä henkilöt, joiden vastuulle kuuluu monia erilaisia teknisiä ratkaisuja. Siksi he eivät voikaan aina olla tulostusturvallisuuden asiantuntijoita.

Usein ongelmana on ammattikieli. Yli puolet (**51 %**) pk-yrityksistä kertoo, että tulostusturvallisuudesta puhuttaessa käytetään liikaa ammattisanastoa. Näin on erityisesti Ranskassa ja Italiassa.

Lähes 60 % pk-yrityksistä kertoo, että niissä ymmärretään hyvin kaikki vaaditut turvallisuusstandardit.

Tähän liittyen päätäjillä ei todennäköisesti ole tulostintoimittajan asiantuntemusta oikean tietoturvan määrittämiseksi. Ei siis ihme, että yritykset kääntyvät ”tuntemiensa” merkkien puoleen tulostusturvallisuusasioissa ymmärtämättä aidosti, mitä turvallisuuskäytäntöjä yrityksessä oikeasti tarvitaan.

Tulostuskumppanien on pystyttävä selittämään turvavaatimukset selkeästi ja varmistamaan, että yritys valitsee itselleen parhaan ratkaisun.



Brotherin näkemykset

Koska tulostusturvallisuus on monisyinen asia, Brother on laatinut seitsemän tärkeän kohdan luettelon, joka auttaa pk-yrityksiä suojautumaan tietojen katoamiseen liittyviltä tuhoisilta talous-, oikeus- ja mainehaitoilta.



Tulostusturvallisuus lähtee hallituksesta

Kyberhyökkäyksien ja tietomurtojen aiheuttamien tuojen laajuus sekä tietosuojalainsäädännön vaatimukset ulottavat tulostusturvallisuuden huomattavasti yrityksen IT-osastoa laajemmalle. Tulostusturvallisuusstrategia tulee laatia yrityksen hallituksen tasolla tietohallintojohtajan ja tietoturvajohtajan myötävaikutuksella.



Perusteellinen auditointi

Yritysten on selvitettävä kaikki mahdolliset tulostamiseen liittyvät haavoittuvuudet ulottamalla säännölliset tietoturva-auditoinnit myös tulostusympäristöön. Se on erityisen tärkeää, jos yrityksessä on eri-ikäisiä laitteita. Useimmat tulostuksenhallintapalveluja (MPS) tarjoavat yritykset tekevät kattavia arviointeja, ja palveluun sisältyy laitekannan optimoinnin ja tietosuojauksen jälkeen jatkuva valvonta.



Esiasetettujen salasanojen vaihtaminen

Oletussalasana tai esiasetetut ylläpitosalasana ovat tulostuslaitteiden heikko kohta. Onneksi se on helppo korjata: kun laite on asennettu, salasana vain vaihdetaan vahvoihin ja tietoturvallesiin.



Laiteohjelmisto- ja suojauspäivitysten asentaminen

Tulostuslaitteiden mahdollisia tietosuojahaavoittuvuuksia voidaan vähentää merkittävästi asentamalla uusimmat laiteohjelmistopäivitykset ja asettamalla laite asentamaan päivitykset automaattisesti. Jos sinulla on kysyttävää aiheesta, käänny laitevalmistajan puoleen.



Tulostustöiden suojaaminen

Itse laitteet eivät ole ainoa suojattava asia, vaan suojausta kaipaavat myös tulostettavaksi lähetetyt tiedostot. Verkkoliikenteen päästä päähän -salaus takaa tulostustöille turvallisen matkan tulostimiin. Salauksesta huolehtiminen on tärkeää, sillä useimmat tulostimet säilyttävät tulostustöitä väliaikaisesti.



Laitteiden valvonta

Tulostuslaitteiden kulloisenkin tilan tunteminen tarjoaa kokonaisvaltaisen näkemyksen koko tulostusympäristöstä. Yritysten tulisi harkita ohjelmistotyökaluja tulostuslaitteiden valvontaan, jotta ongelmat voidaan korjata nopeasti. Laitteisiin kertyy valtavasti tietoa, jonka avulla voidaan tunnistaa mahdollisia tietoturvaongelmia ja reagoida hyökkäyksiin nopeasti. Tulostuksenhallintapalvelujen käyttäjät saavat myös säännöllisesti raportteja, joiden tulisi sisältää tiedot tietomurtojen valvonnasta ja raportoinnista.



Työntekijöiden kouluttaminen

Tietoja katoaa usein vahingossa. Siksi on elintärkeää kouluttaa työntekijät suojaamaan arkaluonteisia tietoja ja lisätä tietoisuutta tietoturvauhista. Tällaisia koulutuksia tarjoavat monet tulostuksenhallintapalvelujen tarjoajat.



Lopuksi

Tulostusjärjestelmät ovat aiemmin saattaneet jäädä yrityksen turvallisuussuunnitelmissa paitsioon, mutta pk-yritykset ovat nyt alkaneet ymmärtää niiden merkitystä. Siitä huolimatta tulostusturvallisuuden toteuttamisessa on yhä merkittäviä haasteita.

Pk-yrityksissä tulostusturvallisuuteen liittyvät vastuut tulee jakaa selkeästi, jotta laitteiston suoja on asianmukainen ja pysyy ajan tasalla. Laitteiston suojaamisen lisäksi tulee kiinnittää huomiota myös tietosuojaan. Tietosuojariskien pienentäminen edellyttää yhteistyötä yrityksen työntekijöiden kanssa.

Vaikka vastuut olisi pk-yrityksessä jaettu selkeästi, tiedon puute on silti merkittävä haaste tehokkaan tulostusturvallisuuden hallinnan kannalta. Tulostustekniikka monimutkaistuu jatkuvasti, ja alalla käytetään paljon ammattikieltä. Yritysten tulee kääntyä luotettavien toimittajien puoleen voidakseen tehdä järkeviä päätöksiä.

Tehokas tulostusratkaisu on muutakin kuin vain turvallinen. Muut digitaalista muutosta käsittelevät raportit sisältävät tietoa digitaalisista työnkuluista, tuottavuuden tehostamisesta ja ratkaisujen vastuullisuudesta.

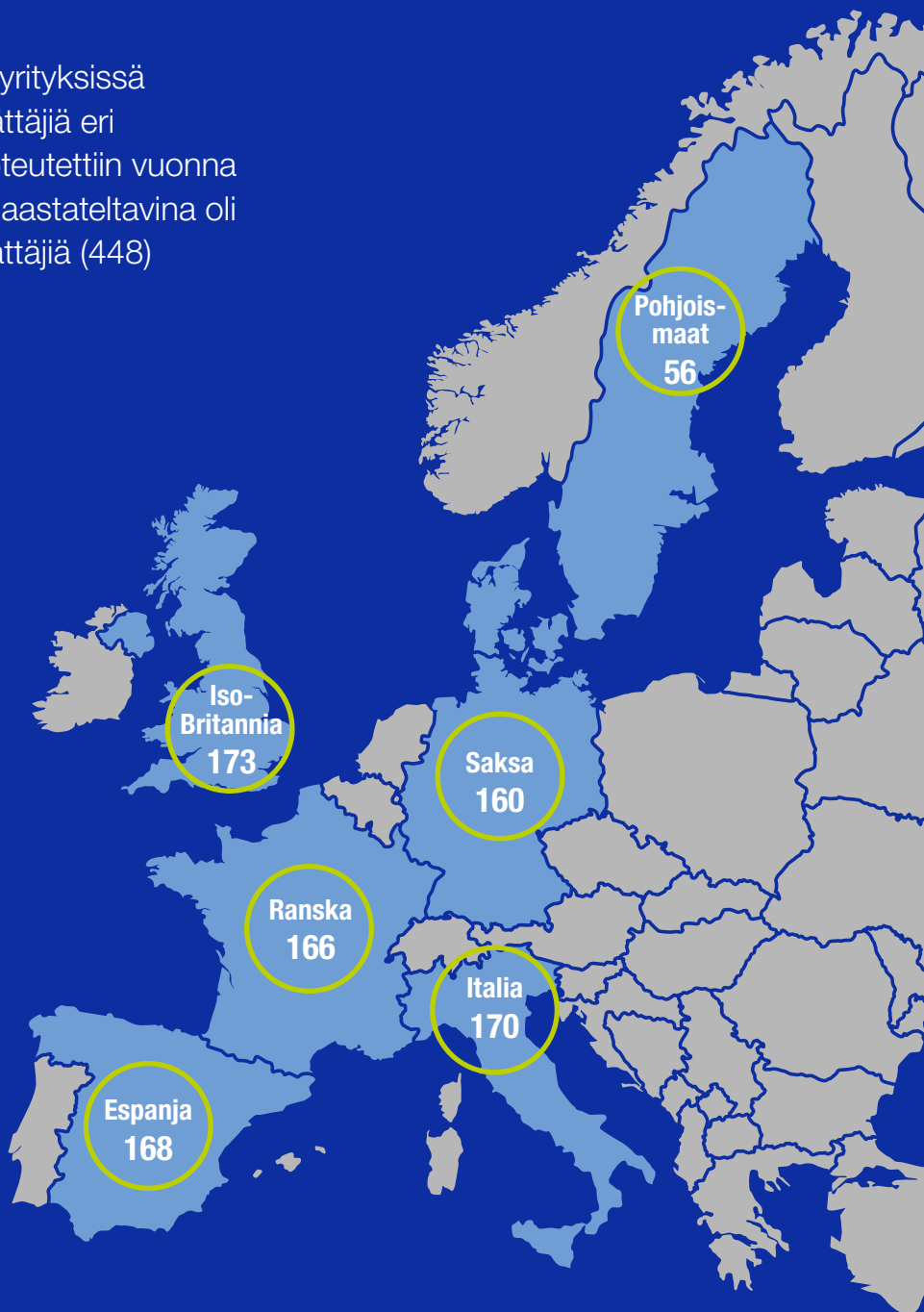
Tutkimusmenetelmä

Tämä raportti perustuu
893 verkkokyselyyn, joihin vastasi
IT-alan ja yritysten päättäjiä.

Vastaajina oli 10–499 työntekijän pk-yrityksissä
työskenteleviä IT-alan ja yritysten päättäjiä eri
Länsi-Euroopan maista. Kenttätyö toteutettiin vuonna
2019 ja vuoden 2020 alkupuolella. Haastateltavina oli
yhtä suuri määrä strategisista yrityspäättäjiä (448)
ja yritysten IT-päättäjiä (445).

Tärkeimmät alat:

-  Terveydenhuolto – 152
-  Vähittäiskauppa – 117
-  Logistiikka – 113
-  Majoitusala – 81
-  Kuljetus ja varastointi – 62
-  Asiantuntijapalvelut – 65
-  Valmistus – 54
-  Rahoituspalvelut – 53
-  Koulutus – 51
-  Rakentaminen – 39



Lisäksi haastateltiin muun muassa energia-alan, lääkealan,
maatalouden, puolustusteollisuuden, kiinteistöalan, urheilun ja
viihdealan toimijoita.

Tilaa uusimmat näkemykset aiheesta

Seuraavat
Brotherin digitaalisen
muutossarjan raportit.

Tulossa pian.



brother

at your side

brother.fi

Brother Finland

Äyritie 12 B, 3. kerros, 01510 Vantaa
Puh. 09 875 921

Kaikki tiedot ovat paikkansapitäviä painohetkellä. Tietoja voidaan muuttaa ilman ennakkoilmoitusta. Brother on Brother Industries Ltd:n rekisteröity tavaramerkki.

Muut tuotenimet ovat niiden omistajien rekisteröityjä tavaramerkkejä.