KONICA MINOLTA

TIETOTURVA

Konica Minolta – alansa johtava tietoturvan kehittäjä

Globaalin tietoliikenteen kasvu on digitaalisella aikakaudella ollut ennen näkemätöntä ja sen myötä ovat myös tietoturvariskit lisääntyneet jyrkästi. Kaikessa yritystoiminnassa on kopiointi-, tulostus-, skannaus- ja faksilaitteiden päivittäinen käyttö keskeinen osa työmenetelmiä ja työnkulkuja, joten monitoimijärjestelmistä on tullut monin tavoin korvaamattomia. Sen vuoksi on tärkeää, että nämä laitteet ja järjestelmät suojataan niiden tietoturvaan jatkuvasti kohdistuvilta uhkilta.

Giving Shape to Ideas

TIETOTURVA

KONICA MINOLTAN TIETOTURVASTANDARDIT

Konica Minoltan tietoturvakäytännöt sisältävät laajan joukon vakio-ominaisuuksia ja optioita, joista muodostuu tehokas perusta ammattitason tietoturvaratkaisuille. Ne tunnistavat ja estävät tietoturvaan kohdistuvia hyökkäyksiä, jotka voisivat vahingoittaa joko yrityksen tai yksilön taloutta tai mainetta. Konica Minolta on alansa tietoturvan edelläkävijä ja johtava asiantuntija.

Monitoimijärjestelmät (MFP) tarjoavat valtavan määrän yksittäisiä toimintoja ja toimintokokonaisuuksia, mutta samalla ne luovat runsaasti mahdollisia tietoturva-aukkoja. Monitoimijärjestelmien tietoturvaratkaisut voidaan jakaa kolmeen pääryhmään:

- **Pääsyn- ja käytönvalvonta**
- **Asiakirjojen ja tietojen suojaus**
- **Verkon tietoturva**

Konica Minoltan tietoturva – toiminnot lyhyesti

Pääsyn- ja käytönvalvonta	Kopioinnin/tulostuksen seuranta
	Toimintojen rajoitus
	Turvatulostus (työn lukitus)
	Kansioiden suojaus salasanalla
	Käyttäjävarmennus (käyttäjätunnus + salasana)
	Sormenpään verisuoniston skanneri
	IC-kortinlukija
	Tapahtumaloki
Tiedon suojaus	Kiintolevyn sisällön salaus
	Kiintolevyn ylikirjoitus
	Kiintolevyn suojaus salasanalla
	Tietojen automaattinen poisto
Verkon tietoturva	IP-osoitteen suodatus
	Porttiliikenteen ja protokollien valvonta
	SSL/TLS-salaus (HTTPS)
	IPsec-tuki
	S/MIME
	802.1x-tuki
Skannauksen tietoturva	Käyttäjävarmennus
	POP-protokollan suosiminen (SMTP)
	SMTP-varmennus (SASL)
	Manuaalisen osoitteen esto
Muita ominaisuuksia	Huoltotilan suojaus
	Ylläpitotilan suojaus
	Tiedonkaappaus
	Luvattoman kirjautumisen esto
	Kopiosuojaus vesileimalla
	PDF-tiedostojen salaus
	PDF-tiedostojen allekirjoitus
	PDF-tiedostojen digitaalinen salaus
	Copy Guard/Salasanallinen kopiointi

COMMON CRITERIA
JA ISO 15408 EAL3

Konica Minoltan laitteet täyttävät lähes poikkeuksetta Common Criteria/ISO 15408 EAL3 -tietoturvanormit.

Common Criteria ja ISO 15408 EAL3 -tietoturvanormit ovat ainoita kansainvälisesti hyväksyttyjä standardeja digitaalisten toimistotuotteiden IT-tietoturva-arviointeihin. ISO 15408 EAL3 -sertifioitujen tulostinten, kopiokoneiden ja ohjelmistojen tietoturva on evaluoitu, joten riskeihin ennalta varautuvat yritykset voivat olla vakuuttuneita tuotteiden tietoturvatasosta.

Konica Minolta on alansa johtava asiantuntija, joka määrittää tietoturvan vaatimustason!

Common Criteria Validated

“Tietoturva on olennainen osa Konica Minoltan kokonaisstrategiaa…

Konica Minolta on kehittänyt lukuisia tulostusta ja asiakirjoja suojaavia tietoturvaominaisuuksia, joista monet ovat vakio-toimintoja yhtiön bizhub-mallistossa. ”Yksittäisille turva-ratkaisuille haettujen hyväksyntöjen sijasta Konica Minolta katsoo, että sillä on markkinoiden laajin valikoima kokonaan ISO 15408 -sertifioituja monitoimijärjestelmiä.”

Lähde: Quocirca (2011), Markkinatutkimus “Closing the print security gap. The market landscape for print security”, sivu 11. Tämän puolueettoman raportin on julkaissut Quocirca Ltd., perustutkimusta ja analysointia tekevä yhtiö, joka on erikoistunut selvittämään tieto- ja viestintätekniikan (ITC) vaikutuksia yritystoiminnassa

KÄYTÖN- JA PÄÄSYNVALVONTA

Vaikka tietoturva onkin näkyvästi esillä sekä julkisuudessa että yritystasolla, silti monitoimijärjestelmien aiheuttamaa tietoturvariskiä usein vähätellään. Jotkut riskit ehkä tunnistetaan, mutta ne jätetään monesti vaille huomiota. Tämä koskee varsinkin asiakirjojen ja informaation luottamuksellisuutta. Erityisen riskialttiita ovat yleisiin tiloihin sijoitetut monitoimijärjestelmät, jotka ovat henkilökunnan, asiakkaiden ja jopa satunnaisten vierailijoiden ulottuvilla.

Nykyiset monitoimijärjestelmät ovat erittäin kehittyneitä, joten tietoja on helppo kopioida ja jaella yrityksen sisällä ja yrityksen ulkopuolelle. Ensimmäiseksi on syytä estää monitoimijärjestelmien käyttö ulkopuolisilta, ottamalla käyttöön kirjautuminen. Yritysten kannattaa luoda tietoturvapolitiikka laitteiden hyväksytylle käytölle. Tietoturvapolitiikan käyttöönotto Konica Minoltan tietoturvaratkaisuilla ei estä tai heikennä järjestelmien käyttömukavuutta.

Käyttäjävarmennus

Käyttäjävarmennuksessa määritellään ensin ne käyttäjät ja käyttäjäryhmät, joilla on oikeus kirjautua monitoimijärjestelmille. Kirjautumisoikeudet voivat sisältää rajoituksia, missä joillekin käyttäjille annetaan lupa tiettyihin toimintoihin, kuten väritulostukseen ja toisilta käyttäjiltä se evätään.

Konica Minolta tarjoaa käyttäjävarmennukseen kolme perusteknologiaa:

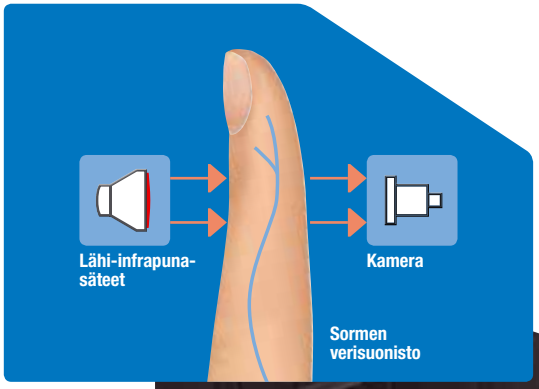
1. **Henkilökohtainen salasana:**
   Salasana on enintään 8 merkistä koostuva alfanumeerinen tunnus, joka näppäillään monitoimijärjestelmän valintapaneelista. Salasanat luodaan järjestelmien ylläpitäjille ja käyttäjille. Huomaa se, että salasanoja voidaan hallinnoida keskitetysti.

2. **IC-kortinlukija**
   Useimpiin Konica Minoltan laitteisiin voidaan ottaa käyttöön IC-kortinlukija. Se nopeuttaa ja helpottaa kirjautumista, sillä IC-kortti asetetaan lukijaan tai lähelle tunnistinta.

Käyttäjävarmennus

3. **Biometrinen sormen verisuoniskanneri**
   Tämä varmennustapa on huippunykyaikainen ja kehitetty perinteisestä sormenjälkitunnistuksesta. Menetelmässä verrataan käyttäjän skannattua sormenpään verisuonikuviota ja laitteen muistiin tallennettuja kuvioita. Biometristä sormen verisuonistoa on käytännössä mahdoton väärentää ja siksi tämä henkilön fyysiseen ominaispiirteeseen perustuva tunnistus on äärimmäisen luotettava. Perinteisistä sormenjälkitunnistuksista poiketen sormen verisuonistoa ei voi skannata henkilön huomaamatta tai poissa ollessa.
   Biometrinen sormen verisuoniskanneri on nopea varmennustapa eikä käyttäjän tarvitse muistaa salasanoja tai pitää mukanaan erillistä korttia.

Henkilöllisyyden todentamistieto voidaan tallentaa salattuna monitoimijärjestelmälle tai hyödyntää Windows Active Directory -hakemiston tietokantaa.
Kaikkien laitteiden kirjautumis- ja käyttöhistoriaa seurataan jatkuvasti, joten tietoturvarikkomukset havaitaan ja kirjataan välittömästi.



Tiliseuranta

Valvonta ja tietoturva edellyttävät kirjautumista laitteelle, joten käyttäjiä, ryhmiä ja/tai osastoja ja niiden laitekäyttäytymistä voidaan seurata kattavasti. Kopiointi, skannaus ja faksaus yksi- tai monivärisenä sekä mustavalko- ja väritulostus voidaan jäljittää suoraan monitoimijärjestelmältä tai tarkistaa Konica Minoltan etätyökaluilla.
Tietojen tarkastelu ja kehityssuunnan arviointi antavat vankkaa informaatiota monitoimijärjestelmien käyttötavoista. Seurantatiedoista voidaan varmistaa laitteiden ohjeiden mukainen käyttö sekä havaita mahdolliset rikkeet. Organisaation, yrityksen tai toimiston koko tulostinlaitteiston ja kaikkien monitoimijärjestelmien käytönseuranta on täysin aukotonta.

Toimintojen valvonta ja rajoitukset

Monitoimijärjestelmien käytölle voidaan asettaa henkilökohtaisia rajoituksia. Konica Minoltan valvonta- ja tietoturvaominaisuudet torjuvat tehokkaasti varallisuutta ja mainetta vahingoittavia uhkia ja sen lisäksi ominaisuuksia voidaan hyödyntää hallinnoinnin tehostamisessa ja käyttövastuullisuuden lisäämisessä.

ASIAKIRJOJEN JA TIETOJEN SUOJAUS

Monitoimijärjestelmä ja tulostimet sijoitetaan usein yleisiin tiloihin, joihin henkilökunnan lisäksi pääsevät asiakkaat ja jopa satunnaiset vierailijat. Sen vuoksi tietoturvapolitiikan käyttöönotto on välttämätöntä. Monitoimijärjestelmän kiintolevylle ajan myötä tallentunut luottamuksellinen tieto tai laitteen luovutustasolla lojuvat tulosteet ovat täysin suojattomia ja voivat päätyä vääriin käsiin. Konica Minolta tarjoaa valikoiman räätälöityjä tietoturvaratkaisuja, joilla asiakirjat ja tiedot suojataan.

Kiintolevyn tietoturva

Useimmissa tulostimissa ja monitoimijärjestelmissä on kiintolevy ja muistia, joihin pitkän ajan kuluessa kertyy megatavuittain luottamuksellista aineistoa.
Ne on suojattava hyvin, jotta organisaation salassa pidettävät tiedot eivät joutuisi ulkopuolisten ulottuville.
Tietoturvan varmistamiseen Konica Minolta tarjoaa useita ja osittain toisiaan tukevia ratkaisuja:

- **Automaattinen poisto:**
  Automaattinen poisto pyyhkii kiintolevyn tiedot määrätyn viiveajan kuluttua.

- **Sisäisen kiintolevyn suojaus salasanalla:**
  Jos kiintolevy poistetaan, sen sisällön lukeminen vaatii salasanan. Salasana on laitekohtainen, joten laitteesta poistetun kiintolevyn sisältöä ei voi avata.

- **Kiintolevyn ylikirjoitus:**
  Kaikkein varmin tapa tietojen poistamiseen kiintolevyltä on sen ylikirjoitus, johon on useita eri menetelmiä.

- **Kiintolevyn sisällön salaus:**
  Konica Minoltan laitteiden kiintolevyjen sisältö voidaan tallentaa salatussa muodossa, joka perustuu 128-bittistä salausavainta käyttävään algoritmiin. Tämä tuo lisävahvistusta organisaation tietoturvaan. Salatun kiintolevyn sisältöä on mahdoton lukea, vaikka levy irrotettaisiin monitoimijärjestelmästä.

Turvatulostus

Tulostuslaitteet muodostavat tietoturvariskin, jota ei pidä aliarvioida. Yksinkertaisin esimerkki on laitteen luovutustasolle unohtuneet asiakirjat, jotka ovat ohikulkijoiden nähtävillä ja luettavissa. Näin ulkopuolisten on äärimmäisen helppoa päästä käsiksi luottamukselliseen aineistoon.
Turvatulostus pitää yksityiset asiakirjat muiden ulottumattomissa, sillä töiden tulostamiseen vaaditaan tekijän asettama ja työn lukituksen vapauttava salasana.
Suojatut asiakirjat voidaan tulostaa vain näppäilemällä bizhub-laitteelle oikea salasana – ilman sitä tulostus ei käynnisty. Tämä estää luottamuksellisia asiakirjoja joutumasta vääriin käsiin.

Touch & Print/ID & Print

Touch & Print-varmennus perustuu sormenpään verisuonikuvioiden skannaukseen tai IC-kortinlukijaan.
ID & Print-varmennus tehdään käyttäjätunnuksella ja salasanalla. Työn tulostus käynnistyy heti, kun monitoimijärjestelmän käyttäjä on tunnistautunut kortinlukijaan asettamallaan henkilökortilla tai biometrisesti sormenpään verisuoniskannerilla eikä muuta tunnusta ja salasanaa tarvita.

Kopiosuojaus

Kopiosuojauksessa alkuperäisdokumentin tulostamisen yhteydessä kopioihin ja tulosteisiin lisätään vesileima. Se on lähes näkymätön, mutta kun suojattu dokumentti kopioidaan jollakin muulla laitteella, esiin ilmestyvä vesileima paljastaa, että kyseessä on kopio.

Copy Guard/Vapautus salasanalla

Alkuperäisdokumenttiin piilotetaan tulostuksen yhteydessä vesileima, joka estää dokumentin uudelleen kopioinnin. Suojatun dokumentin vesileima on lähes näkymätön, mutta se estää kopiotoiminnon käynnistämisen. Suojaus voidaan kumota ja dokumentti kopioida, mikäli käyttäjä näppäilee monitoimijärjestelmän valintapaneelille oikean salasanan.

PDF-tiedostojen salaus

Salatut PDF-tiedostot on suojattu salasanalla.
Oikeudet PDF-tiedostojen tulostukseen, kopiointiin tai sisällön muokkaamiseen voidaan määritellä skannauksen yhteydessä.

PDF-tiedostojen digitaalinen allekirjoitus

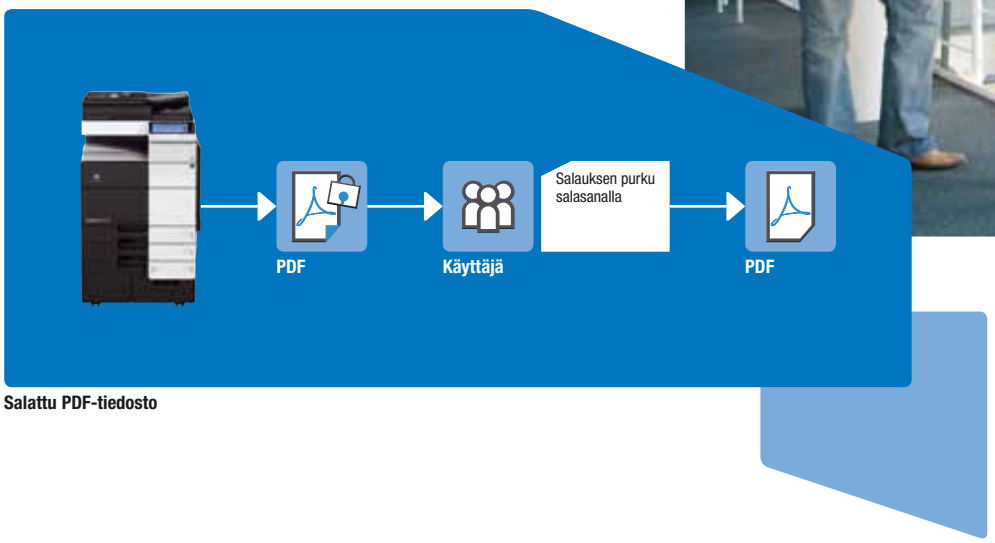
PDF-tiedostoihin liitetty digitaalinen allekirjoitus estää monitoimijärjestelmällä luotujen PDF-tiedostojen peukaloinnin ja kaikki tiedostoihin myöhemmin tehdyt muutokset voidaan jäljittää.

Faksiviestien suojattu vastaanotto

Kaikki saapuvat faksiviestit ovat tallennettavissa käyttäjän omaan ja muilta suojattuun kansioon.

Käyttökansioiden tietoturva

Monitoimijärjestelmän kiintolevylle voidaan luoda nimetyille henkilöille tai ryhmille kansioita, joihin kopioitavat tai tulostettavat asiakirjat tallennetaan tietoturvallisesti. Kansiot voidaan suojata 8 merkkiä sisältävällä salasanalla, jolloin kansioiden avaaminen ja tiedostojen katselu vaatii oikean salasanan. Näin varmistetaan, että luottamukselliset asiakirjat ovat vain niihin oikeutettujen käyttäjien katseltavissa.



Salattu PDF-tiedosto

VERKON TIETOTURVA

Tiedonvälitys ja viestintäyhteydet ovat välttämättömiä nykyaikaisessa liiketoiminnassa. Konica Minoltan toimistolaitteet on suunniteltu integroitaviksi erilaisiin verkkoympäristöihin. Esimerkiksi verkkotulostimista ja monitoimijärjestelmistä (MFP) on luotu huippukehittyneitä ja tietoverkkoon liitettäviä asiakirjojen prosessointikeskuksia. Ne tulostavat, kopioivat ja skannaavat dokumentteja ja ohjaavat ne verkko-osoitteisiin sekä lähettävät sähköpostiviestejä. Tämä suuntaus merkitsee, että toimisto-teknologian on varauduttava samanlaisiin tietoturvariskeihin ja niiden torjuntaan kuin muidenkin verkotettujen laitteiden kohdalla, sillä suojaamattomat järjestelmät ovat kiistaton tietoturvariski. Konica Minoltan kaikki laitteet täyttävät tiukat tietoturvavaatimukset, joilla vältetään sisäisten ja ulkoisten verkkohyökkäysten aiheuttamat vahingot. Tehokkaita suojaus-menetelmiä on useita:

IP-osoitteen esto

Sisäinen peruspalomuuri suodattaa IP-osoitteet sekä valvoo protokollia ja porttiliikennettä.

Porttiliikenteen valvonta

Ylläpito voi avata, sulkea, sallia tai estää portti- ja protokol-laliikenteen joko suoraan laitteelta tai etäohjausta hyödyntä-mällä.

S/MIME

Useimmat Konica Minoltan monitoimijärjestelmät tukevat S/MIME-standardia (Secure/Multipurpose Internet Mail Extensions), jotta sähköpostiliikenne monitoimijärjestelmältä vastaanottajille olisi turvallista. S/MIME salaa viestit ja niiden sisällön varmenteella.

SSL/TLS -salaus

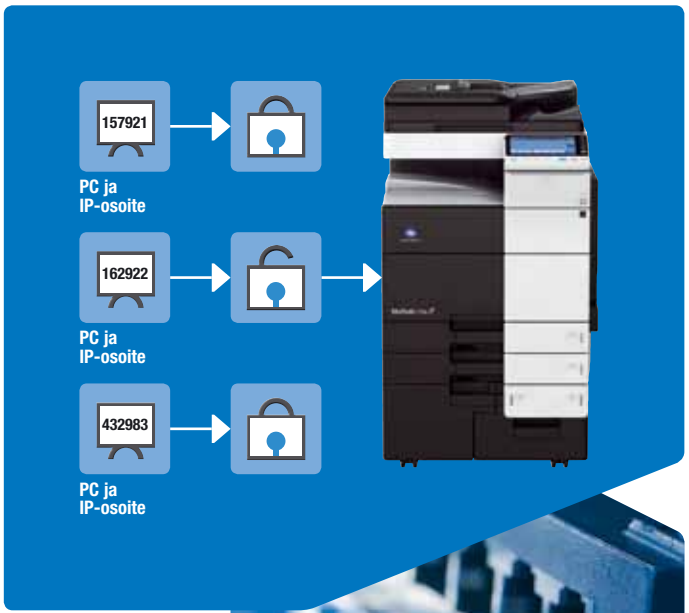
SSL/TLS-protokolla suojaa kaksisuuntaisesti laitteiden verkkoliikennöintiä siirrettäessä esimerkiksi ylläpitotietoja sekä Windows Active Directory -hakemiston tunnuksia.

IPsec-tuki

Useimmat bizhub-laitteet tukevat myös IPsec-protokollaa, joka täysin ja kaksisuuntaisesti salaa verkon ja monitoimi-järjestelmien välisen liikennöinnin. IPsec salaa kaiken verkkoliikenteen paikallisverkon (palvelin, työasema) ja bizhub-laitteen välillä.

IEEE 802.1x -tuki

IEEE802.1x on porttipohjainen todennusstandardi, jolla suojataan WAN- ja LAN-verkkoliikennöintiä. Nämä standardit varmistavat verkon tietoturvan estämällä luvattoman liikennöinnin (esimerkiksi DHCP- tai HTTP-tiedonsiirron) ulkopuolisille laitteille lukuun ottamatta todennuspyyntöjä.



IP-osoitteen suodatus