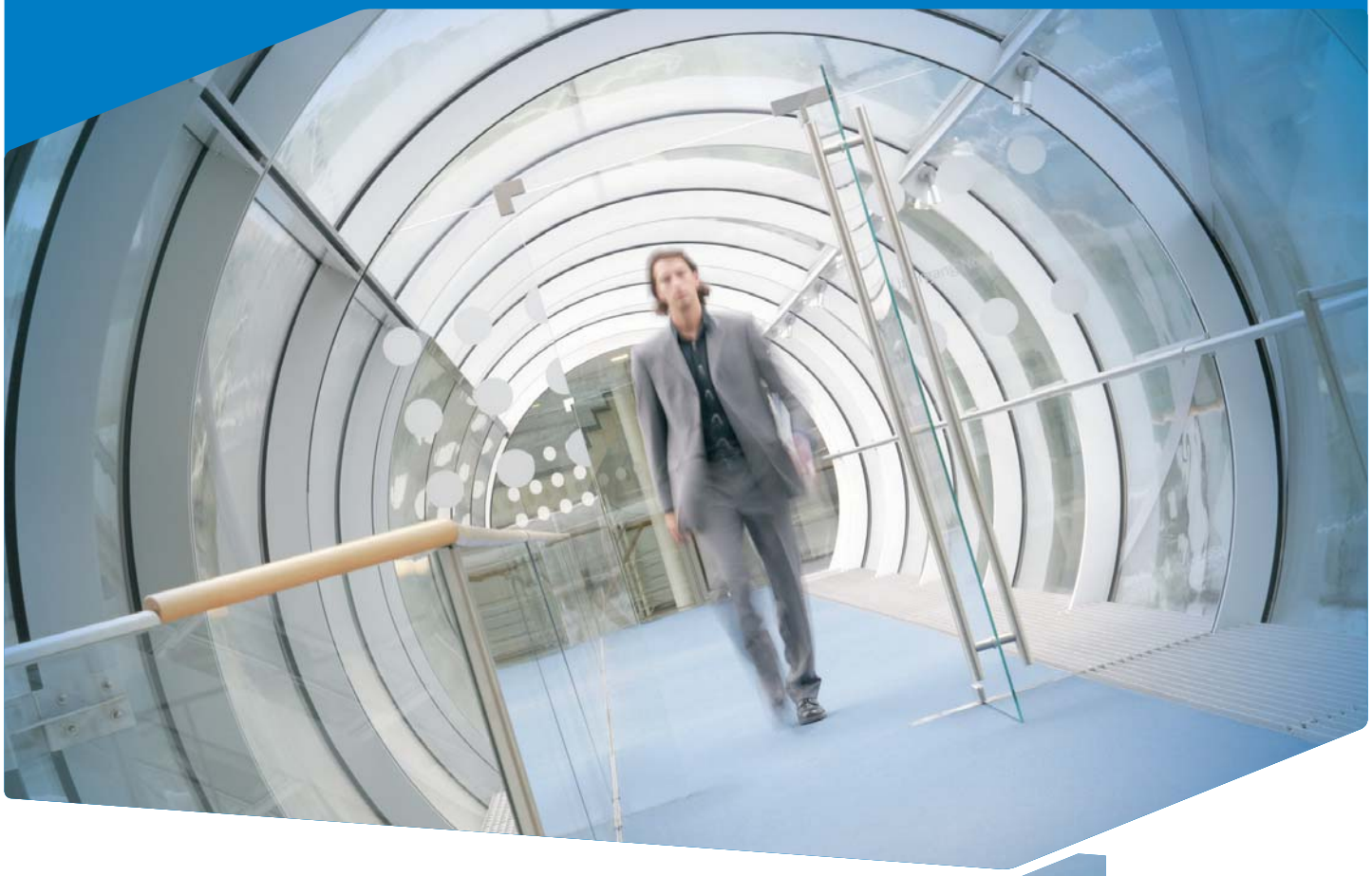
KONICA MINOLTA

TIETOTURVA
TINKIMÄTÖNTÄ YKSITYISYYDEN SUOJAA

Konica Minoltan tietoturvastandardit



JULKAISUT
TIETOTURVA

Giving Shape to Ideas

ALANSA JOHTAVAA TIETOTURVAA

Digiaikakauteen siirtyminen on merkinnyt maailmanlaajuisen viestinnän valtavaa kasvua ja sen myötä myös tietoturvariskien jyrkkää lisääntymistä. Jokaisessa organisaatiossa kopiointi-, tulostus-, skannaus- ja faksilaitteiden päivittäinen käyttö kuuluu keskeisesti työmenetelmiin ja työnkulkuihin, joten monitoimijärjestelmistä on tullut monin tavoin korvaamattomia. Siksi on tärkeää, että nämä laitteet ja järjestelmät suojataan niiden tietoturvaan kohdistuvilta uhkilta.

Konica Minoltan tietoturvakäytännöt sisältävät runsaasti 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 ja mainetta. Konica Minolta on alansa tietoturvaratkaisujen edelläkävijä ja johtava asiantuntija.

Konica Minoltan laitteet ja järjestelmät täyttävät lähes poikkeuksetta Common Criteria/ISO 15408 EAL3 -tietoturvanormit. Nämä ovat ainoita kansainvälisesti hyväksyttyjä standardeja digitaalisten toimistotuotteiden IT-tietoturvaominaisuuksien arviointiin. ISO 15408 -sertifioidut tulostimet, monitoimijärjestelmät ja ohjelmistot ovat läpäisseet tiukat arviointikriteerit, joten riskeihin ennalta varautuvat yritykset voivat olla vakuuttuneita tuotteiden turvatasosta.

”Tietoturva on olennainen osa Konica Minoltan kokonaisstrategiaa…”

Konica Minolta on kehittänyt lukuisia tulostusta ja asiakirjoja suojaavia tietoturvaominaisuuksia, joista monet ovat vakiotoimintoja yhtiön bizhub-mallistossa. ”Yksittäisille turvaratkaisuille 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

Common Criteria Validated

TIETOTURVAN HAAVOITTUVUUS **ON YHTEINEN HUOLENAIHE**

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

Kirjautumisen ja käytön valvonta

Vaikka tietoturva on näkyvästi esillä sekä julkisuudessa että yrityksissä, silti monitoimijärjestelmiä ei useinkaan pidetä tietoturvariskeinä. 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 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. Se tapahtuu valvomalla laitteille kirjautumista ja luomalla tietoturvapolitiikka laitteiden hyväksytylle käytölle. Konica Minolta toteuttaa tietoturvaratkaisunsa järjestelmien käyttömukavuudesta tinkimättä.

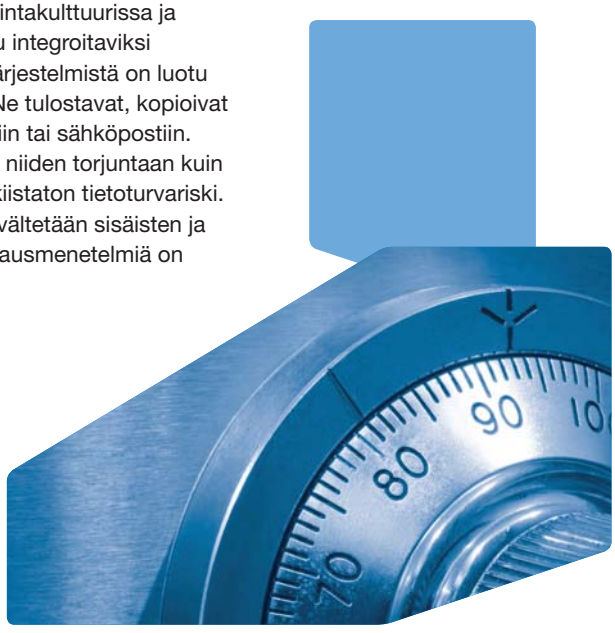
Asiakirjojen ja tietojen suojaus

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

Verkon tietoturva

Tiedonvälitys ja viestintäyhteydet ovat välttämättömiä nykyaikaisessa toimintakulttuurissa ja erityisesti yritysmaailmassa. Konica Minoltan toimistolaitteet on suunniteltu integroitaviksi erilaisiin verkkoympäristöihin. Esimerkiksi verkkotulostimista ja monitoimijärjestelmistä on luotu kehittyneitä ja tietoverkkoon liitettäviä asiakirjojen prosessointikeskuksia. Ne tulostavat, kopioivat ja skannaavat dokumentteja sekä ohjaavat ne esimerkiksi verkko-osoitteisiin tai sähköpostiin. Toimistoteknologian on siis varauduttava samanlaisiin tietoturvariskeihin ja niiden torjuntaan kuin muidenkin verkotettujen laitteiden, sillä suojaamattomat järjestelmät ovat kiistaton tietoturvariski. Konica Minoltan kaikki laitteet täyttävät tiukat tietoturvavaatimukset, joilla vältetään sisäisten ja ulkoisten verkkohyökkäysten aiheuttamat vahingot. Tehokkaita verkonsuojausmenetelmiä on useita.

Konica Minoltan laaja tietoturvaominaisuuksien valikoima tarjoaa ammattitason ratkaisuja, joilla tietomurrot havaitaan ja estetään.



KATTAVA TIETOTURVA – KONICA MINOLTAN VAKIO-OMINAISUUS

Varmennusmenettelyssä määritellään ensin ne käyttäjät ja käyttäjäryhmät, joilla on oikeus kirjautua monitoimijärjestelmiin. Kirjautumisoikeudet voivat sisältää rajoituksia, missä joillekin käyttäjille annetaan lupa tiettyihin toimintoihin kuten väritulostukseen ja toisilta käyttäjiltä se evätään. Konica Minoltan lähestymistapa on tarjota useita vaihtoehtoja käyttäjävalvonnan toteuttamiseen.

Konica Minoltan käyttäjävalvonta- ja tietoturvaominaisuudet torjuvat tehokkaasti varallisuutta ja mainetta vahingoittavia uhkia, ja sen lisäksi ominaisuuksia voidaan hyödyntää hallinnoinnin tehostamisessa ja käyttövastuullisuuden lisäämisessä.

Kirjautumisen ja käytön valvonta

- **Käyttäjävarmennus** sääntelee monitoimijärjestelmille tai tulostimille kirjautumista ja varmennus voidaan tehdä työasemalla tai suoraan monitoimijärjestelmällä. Useimmissa Konica Minoltan bizhub-järjestelmissä on vaihtoehtoisia kirjautumistapoja.

- **Biometrinen varmennus sormen verisuoniskannerilla** on nykyaikainen menetelmä käyttäjän todentamiseen. Menetelmässä verrataan käyttäjän skannattua sormenpään verisuonikuviota ja laitteen muistiin tallennettuja kuvioita. Tätä henkilön ominaispiirteeseen perustuvaa todennustulosta on käytännössä mahdoton väärentää. Biometrinen varmennus on huomattavasti luotettavampi kuin perinteiset sormenjälkimenetelmät. Biometrinen verisuoniskanneri on nopea ja yksinkertainen varmennustapa eikä käyttäjän tarvitse muistaa salasanoja tai pitää mukanaan erillistä henkilökorttia.

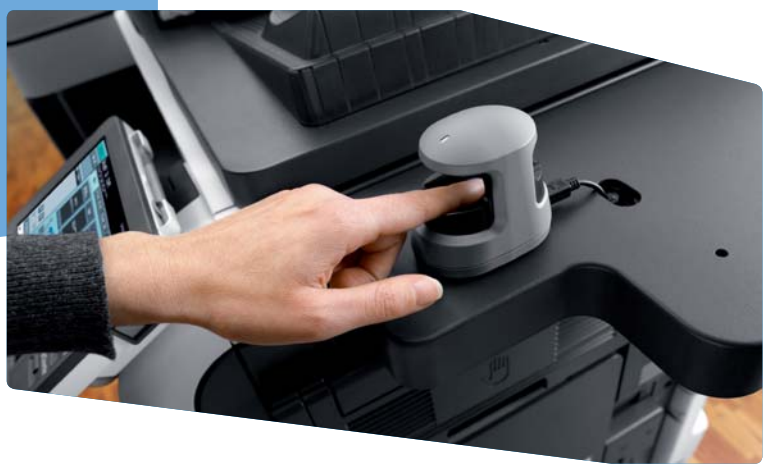
- **Kontaktiton henkilökortti** on kätevä ja nopea varmennustapa, sillä useimpiin bizhub-monitoimijärjestelmiin voidaan liittää kortinlukija. Varmennuksessa IC-kortti asetetaan lähelle lukulaitteen tunnistinta.

- Yksinkertaisin varmennustapa on **henkilökohtainen salasana tai käyttäjätunnus**, joka näppäillään monitoimijärjestelmän valintapaneelilta. Tämä laitteen sisäinen todennustapa tukee jopa 1 000 käyttäjätiliä. Alfanumeeriset ja maksimipituudeltaan 64-merkkiset salasanat voidaan luoda käyttäjille sekä ylläpitäjille ja salasanojen hallinnoinnista vastaa IT- ylläpito.

- **Varmennustiedot** voidaan tallentaa monitoimijärjestelmiin salattuna tai varmennukseen voidaan käyttää jo olemassa olevaa tietokantaa kuten Windows Active Directory -palvelua. PageScope Enterprise -sarjan Authentication Manager auttaa kirjautumiskäytäntöjen keskitetyssä hallinnassa.

- Kaikkiin bizhub-monitoimijärjestelmiin voidaan ohjelmoida tietyn viiveajan jälkeen tapahtuva **automaattinen palautus**. Tällä varmistetaan laitteen palautus turvalliseen tilaan, vaikka käyttäjä unohtaisi kirjautua ulos työnsä päätteeksi. Monitoimijärjestelmän dokumentteihin pääsyä työasemilta voidaan rajoittaa salasanalla. Monet Konica Minoltan järjestelmät tarjoavat mahdollisuuden töiden etätulostukseen ja -skannaukseen. Tämä toiminto voidaan suojata salasanalla tai estää kokonaan.

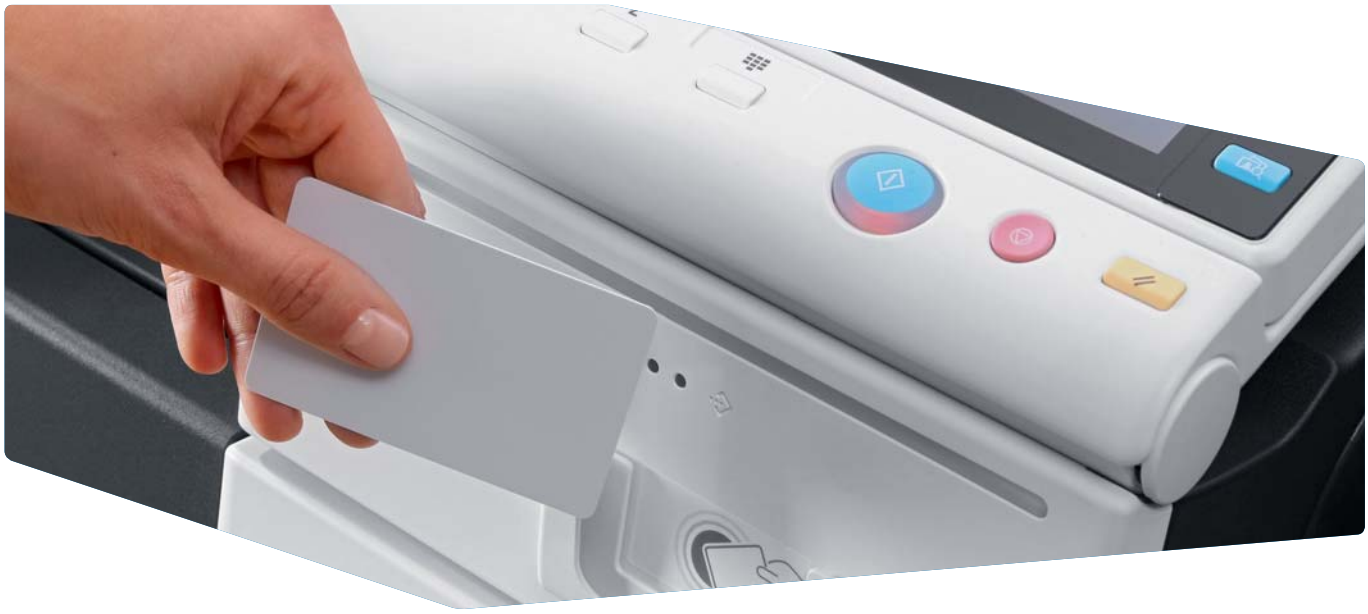
- Pankkiautomaatin tavoin voidaan jokainen bizhub-monitoimijärjestelmä ohjelmoida **torjumaan käyttäjä, joka yrittää kirjautua väärällä tunnuksella**. Kun virheellisiä yrityksiä kertyy riittävästi, laitteen toiminnot lukkiutuvat määräajaksi. Tätä luvattoman kirjautumisen estävää käyttölukkoa voidaan myös soveltaa järjestelmän kansioissa oleviin yksityisiin asiakirjoihin (turvatulostus).



- Kehittyneen tason käyttäjäturva mahdollistaa **tiettyjen laitetoimintojen sallimisen tai eston**. Pääkäyttäjä tai ylläpito voi säädellä näitä toimintoja tarpeen mukaan ja organisaation koosta riippumatta. Erityistoimintoja ovat:
  - Paikalliskopiointi bizhub-järjestelmällä ja mustavalko- tai värikopioinnin rajoittaminen tai molempien salliminen
  - Etätulostus ajurin kautta ja mustavalko- tai väritulostuksen rajoittaminen tai salliminen
  - Paikallis- ja etäskannaus bizhub-järjestelmällä
  - Paikallis- tai etäfaksaus bizhub-järjestelmällä
  - bizhub-järjestelmälle tallennettujen kansioiden paikallis- ja etäkäyttö
  - Useissa monitoimijärjestelmissä on mahdollisuus yksilölliseen käyttöoikeuksien rajoittamiseen, jolloin käyttöoikeudet liitetään varmennusmenettelyyn.

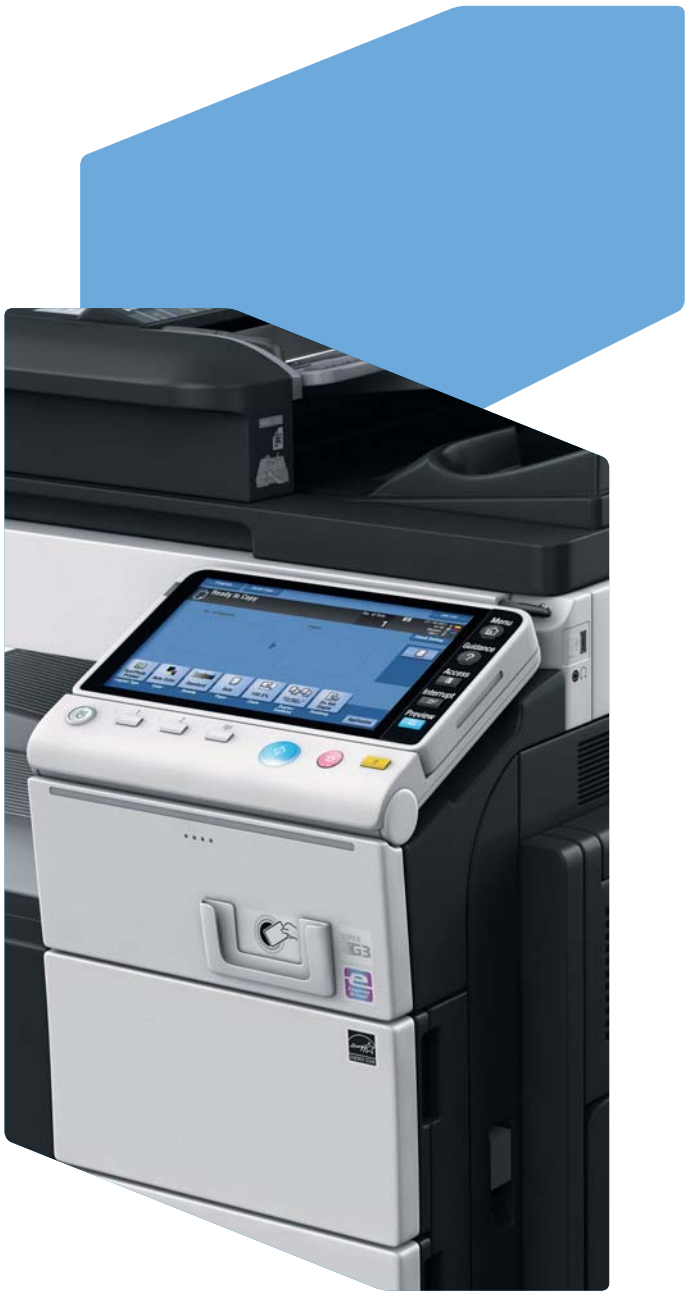
- Kunkin laitteen **kirjautumis- ja käyttöloki** paljastaa välittömästi tietoturvaloukkaukset ja on myös apuna käyttäjä- ja osastokohtaisessa kulujen seurannassa sekä niiden kohdennuksessa. Ylläpito voi tarkastella laitteiden yksittäisiä käyttäjätilejä sekä työlokeja, joista selviää mm. tiedot mustavalko- ja väritulostuksesta ja/tai kopioinnista, saapuneista ja lähetetyistä faksiviesteistä sekä skannaustoiminnoista.
  Useisiin Konica Minoltan järjestelmien tulostinpalvelimiin sisältyy sähköiset työlokit, joihin kirjautuvat kaikki tulostimille lähetetyt työt. Sen lisäksi Konica Minoltan PageScope Job Log -sovellus mahdollistaa kaikkien käyttäjätoimintojen sähköisen seurannan.

- Tiliseuranta vaatii kirjautumista tulostavalle laitteelle, jolloin käyttäjien, työryhmien tai osastojen käytönvalvonta toteutuu tehokkaasti. Mustavalko- ja värikopiointi, skannaus ja faksaus sekä mustavalko- ja väritulostus voidaan jäljittää suoraan monitoimijärjestelmältä tai tarkistaa Konica Minoltan työkaluilla, kuten PageScope Web Connection, PageScope Net Care Device Manager ja Page Scope Enterprise -sarjan Account Manager. Käyttäjän kirjauduttua palveluihin hänen kaikki toimet tallentuvat sähköisesti järjestelmän lokitiedostoon, jonka avaamiseen IT-ylläpidolla tai pääkäyttäjällä on oikeus. Näin esimerkiksi osastokohtainen laskutus tai henkilöstön kopiointikäytäntöjen seuranta sujuu tehokkaasti.



KONICA MINOLTA SUOJAA **YKSITYISYYDEN JA ASIAKIRJAT**

Luottamuksellisen asiasisällön, yksittäisten käyttäjien sekä verkkoliikenteen suojaamiseksi on Konica Minolta kehittänyt kattavia tietoturvakäytäntöjä, jotka varmistavat käyttäjien yksityisyyden ja tuotetun aineiston tietosuojan. Näin organisaation luottamuksellinen informaatio ei päädy vääriin käsiin.



Asiakirjojen ja tietojen suojaus

– Tulostavat laitteet muodostavat tietoturvariskin, jota ei pidä väheksyä. 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 laitteelle oikea salasana – ilman sitä tulostus ei käynnisty. Tämä estää luottamuksellisia asiakirjoja joutumasta vääriin käsiin. Tulostustöihin liitetyt salasanat ovat salattuja. Suojausta voidaan vielä vahvistaa poistamalla bizhub-järjestelmistä kaikki avaamattomat ja salasanalla suojatut työt, kun tietty viiveaika on kulunut.

– Turvatulostus voidaan myös toteuttaa kätevillä **Touch&Print-** tai **ID&Print**-toiminnoilla. Touch&Print-varmennus perustuu sormenpään verisuonikuvioiden skannaukseen tai henkilökortin lukijaan ja ID&Print vaati puolestaan käyttäjätunnuksen ja salasanan. Turvatulostus edellä mainituilla menetelmillä ei edellytä muuta tunnusta ja salasanaa, vaan hyväksytty kirjautuminen bizhub-järjestelmään riittää suojatun työn tunnistamiseen ja sen välittömään vapauttamiseen tulostettavaksi.

– Tulostettavat työt voidaan vaihtoehtoisesti siirtää käyttäjän omaan kansioon. **Käyttäjäkansiot** mahdollistavat dokumenttien tallennuksen yksityisiin kansioihin. Kansiot näkyvät vasta käyttäjävarmennuksen jälkeen ja ne avautuvat henkilökohtaisella salasanalla. Työn tulostaminen tai ohjaaminen faksiin tai sähköpostiin vaatii sekä oikean tunnuksen että salasanan. Suojattuihin kansioihin voidaan myös vastaanottaa henkilökohtaisia faksiviestejä.

- **PDF-tiedostojen sisältö voidaan suojata** 40- tai 128-bittisellä salauksella. PDF-tiedostojen suojaukseen valitun salasanan enimmäispituus on 32 merkkiä. Salaus voi myös sisältää oikeuden tiedoston tulostamiseen, kopiointiin ja jopa sisällön muokkaukseen.

- Sähköpostiin liitettävä tai FTP- tai SMB-palvelimen kansioon lähetettävä PDF-tiedosto voidaan salata **digitaalisella varmenteella**. Tämä erittäin vahva salaustapa tekee PDF-tiedostojen murtamisen käytännössä mahdottomaksi. Digitaalinen varmenteen suojaus perustuu S/MIME-salaukseen ja vaatii julkisen salausavaimen sekä yksityisen purkuavaimen.

- PDF-tiedostoihin liitetty **digitaalinen allekirjoitus** estää bizhub-monitoimijärjestelmällä luotujen PDF-tiedostojen peukaloinnin. Kaikki tiedostoihin tehdyt muutokset ovat jäljitettävissä. Digitaalisesti allekirjoitetusta tiedostosta näkyy myös PDF-suojaukseen tehdyt muutokset. Digitaalinen allekirjoitus ilmaisee lisäksi dokumentin alkuperän ja auttaa sen turvallisuuden arvioinnissa.

- Joissakin bizhub-malleissa alkuperäisdokumenttien **kopiosuojaus** voidaan toteuttaa tulostamisen yhteydessä piilotetulla vesileimalla, joka muodostuu tekstistä, kuvioista tai niiden yhdistelmästä. Kun tällainen suojattu dokumentti kopioidaan jollakin muulla laitteella, esiin ilmestyvä vesileima paljastaa, että dokumentti on kopioitu tai jaeltu ilman lupaa.

- **Copy Guard -suojaus** ja sen **kumoaminen salasanalla** on optio. Siinä alkuperäiseen asiakirjaan piilotetaan tulostuksen yhteydessä vesileima, joka estää asiakirjan uudelleen kopioinnin. Vaikka vesileima on lähes näkymätön, se estää kopiotoiminnon käynnistämisen. Tarvittaessa suojaus voidaan kumota ja dokumentti kopioida, mikäli käyttäjä näppäilee monitoimijärjestelmän valintapaneelille oikean salasanan.

- Useimmissa tulostimissa ja monitoimijärjestelmissä on **kiintolevy** ja **asiakirjamuisti**, 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.
  Konica Minolta tarjoaa useimpiin bizhub-tuotteisiinsa **kiintolevyn salaustyökalut**. Niistä on hyötyä organisaatioille, jotka haluavat vahvistaa järjestelmän kiintolevylle salasanalla suojattujen kansioiden ja niissä olevan sähköisen aineiston tietoturvaa. Tieto voidaan salata 128-bittistä salausavainta tukevalla AES-algoritmilla *(Advanced Encryption Standard)*. Salausta käyttävän kiintolevyn sisältöä on mahdoton lukea, vaikka levy irrotettaisiin monitoimijärjestelmästä.
  TPM-sirun *(Trusted Platform Module)* avulla tallennetaan ja salataan kiintolevyn salausavain. Tämä siru mahdollistaa luottamuksellisten tietojen tallennuksen, kuten varmenteiden ja monitoimijärjestelmien salasanojen varastoinnin.

- **Automaattinen poisto** pyyhkii sisäisen kiintolevyn tiedot määrätyn ajan kuluttua. Kiintolevyn alustus ja tyhjennys suojelee Konica Minoltan monitoimijärjestelmien kiintolevyille tallennettua luottamuksellista aineistoa. Asiakirjat ensimmäisenä tallentanut käyttäjä voi ne myös poistaa.

- Pääkäyttäjä, ylläpito tai huoltoteknikko voi lisäksi alustaa ja tyhjentää kiintolevyn, jos monitoimijärjestelmä on esimerkiksi sijoitettava uuteen paikkaan. **Kiintolevyjen ylikirjoitusmenetelmiä** on useita ja eri käyttäjien sekä käyttäjäryhmien vaatimuksiin soveltuvia. Ylläpitäjät voivat määritellä bizhub-järjestelmiin toiminnon, jolla työkohtaiset väliaikaistiedostot poistetaan automaattisesti kiintolevyltä. Jos automaattinen ylikirjoitus on kytketty, käyttäjäkansioista manuaalisesti poistetut työt ylikirjoitetaan kolme kertaa.

- **Sisäisen kiintolevyn suojaus** salasanalla estää levyn luvattoman irrotuksen. Salasana on laitekohtainen, joten poistetun kiintolevyn sisältöä ei voi avata.

KONICA MINOLTA VARMISTAA TIETOTURVALLISEN VERKKOLIIKENNÖINNIN

Konica Minoltan toimistojärjestelmien perustana ovat monipuoliset viestintävalmiudet ja liitettävyys. Myös käyttäjien kirjautumista, tiedostojen salausta ja tiedonsiirtoprotokollia koskevat tietoturvanormit ovat erittäin tiukkoja.

Verkon tietoturva

– Monitoimijärjestelmien ja tulostinten käyttöä säätelevä **varmennusmenettely** estää myös luvattoman kirjautumisen tietoverkkoon. Jokainen hyväksytty käyttäjä saa oman tunnuksen sekä salasanan, jotka oikeuttavat kirjautumaan verkkoon tai paikallisesti bizhub-laitteelle.

– **SSL- ja TLS-salaus** suojaavat monitoimijärjestelmille tai tulostimille saapuvan ja niiltä lähtevän liikenteen sekä esimerkiksi ylläpidon sovellustyökalut, PageScope Enterprise -palvelinliikenteen ja tietojen siirrot Active Directory -hakemistosta.

– bizhub-järjestelmät tukevat myös IPsec-protokollaa, joka salaa täysin verkon ja monitoimijärjestelmien välisen kaksisuuntaisen viestinnän. **IPsec** salaa kaiken verkkoliikenteen paikallisverkon (palvelin, työasema) ja bizhub-järjestelmän välillä.

– Sisäinen peruspalomuuri suodattaa IP-osoitteet sekä valvoo protokollia ja porttiliikennettä. **IP-osoitteen suodatus** voidaan asettaa ohjelmoimalla monitoimijärjestelmän verkkokortti niin, että laitteelle pääsee vain työasemien tietyistä IP-osoitteista.

- Ylläpito voi **avata, sulkea, sallia tai estää portti- ja protokollaliikenteen** joko suoraan laitteelta tai hyödyntämällä PageScope Web Connection - tai PageScope Net Care Device Manager -sovelluksia. Laite- ja verkkoasetusten luvaton peukalointi on estetty tehokkaasti, sillä ylläpitotilaan kirjaudutaan 8-merkkisellä salasanalla, jonka muuttamiseen tarvitaan huoltoteknikon tai ylläpidon valtuudet.

– Tarvittaessa kaikilta käyttäjiltä voidaan **estää verkkoon pääsy** kokonaan sulkemalla rajapintana toimiva sovellus – esimerkiksi PageScope Web Connection. Näin verkkoon kirjautuminen rajoitetaan pelkästään ylläpitäjille ja ulkopuolisilta poistetaan mahdollisuus muuttaa asetuksia tai järjestelmien kokoonpanoa.

- **SMTP-protokolla** *(Simple Mail Transfer Protocol)* tarjoaa kehittynyttä turvaa sähköpostien välitykseen. Toiminnon ollessa aktivoituna SMTP antaa laitteelle luvan postin lähetykseen. Ne asiakkaat, joilla ei ole omaa sähköpostipalvelinta, voivat käyttää muun internet-palvelujen tarjoajan (ISP) postipalvelinta, jota laite tukee. AOL vaatii SMTP-varmennusta roskapostin estämiseksi. Tiedonsiirron suojauksessa voidaan yhdistää POP before SMTP, APOP ja SMTP-todennus tai SSL/TLS-salaus.

- Jotta sähköpostiliikenne monitoimijärjestelmältä vastaanottajille olisi tietoturvallista, monitoimijärjestelmät tukevat **S/MIME**-standardia *(Secure/Multipurpose Internet Mail Extensions)*. S/MIME salaa viestit ja niiden sisällön varmenteella. S/MIME-varmentimet tai salausavaimet (julkinen avain) voidaan tallentaa monitoimijärjestelmän osoitekirjan sähköpostiosoitteisiin. S/MIME-salatut sähköpostit voi avata vain purkuavaimen (salainen avain) haltija.

- **Kun käyttäjävarmennus on aktivoitu, ei viestin lähetysosoitetta voi muuttaa.** Vaikka lähetysosoitteen muuttaminen olisi sallittu, sähköpostiin skannatun työn lähetysosoite on aina kirjautuneen käyttäjän sähköpostiosoite. Tämä ominaisuus estää vilpin ja mahdollistaa viestien aukottoman jäljityksen.

- Jos **vastaanottajan manuaalinen valinta on estetty**, ei skannaus- tai sähköpostiosoitetta voi syöttää valintanäppäimillä. Vain monitoimijärjestelmän osoitekirjaan tai LDAP-tietokantaan tallennettujen vastaanottajien osoitteet ovat käytettävissä.

- **Faksilinjan kehittynyt tietoturva** varmistetaan käyttämällä bizhub-faksiyhteyksissä ainoastaan faksiprotokollaa – muita siirtoprotokollia ei edes tueta. Kaikki Konica Minoltan laitteisiin kohdistuvat tunkeutumisyritykset torjutaan. Näitä ovat mm. puhelinlinjojen kautta ja eri protokollia käyttämällä tapahtuvat hyökkäykset sekä yritykset siirtää dataa, jota ei voi purkaa faksimuotoon.

- **Faksiviestien reititys** mahdollistaa saapuneiden viestien automaattisen ohjauksen vastaanottajille, jotka löytyvät bizhub-järjestelmän osoitekirjasta – kuten sähköpostiosoitteet tai bizhub-järjestelmän kiintolevylle tallennetut kansiot. Käyttäjäkansioihin tallennus parantaa tietoturvaa, koska faksiviestit eivät jää lojumaan laitteen luovutustasolle. Reititys vauhdittaa tiedonkulkua, koska viestit tavoittavat vastaanottajansa nopeammin ja paperia säästyy, sillä vastaanottaja voi päättää viestin tulostustarpeesta.

- Useimmat Konica Minoltan laitteet tukevat **IEEE802.11x -standardia**. Se on porttipohjainen todennusstandardi, joka suojaa WAN- ja LAN-verkkoliikennöintiä. Nämä standardit varmistavat verkon tietoturvan estämällä luvattoman liikennöinnin (esimerkiksi DHCP- tai HTTP-tiedonsiirron) ulkopuolisille laitteille todentamispyyntöjä lukuun ottamatta.

TIETOTURVARISKEILTÄ SUOJAUTUMINEN ON JATKUVA HAASTE

Tosiasioiden tiedostaminen on välttämätöntä, sillä yksikään yritys tai organisaatio ei ole suojassa hyökkäyksiltä, joita niiden tietoturvaan jatkuvasti kaikkialta kohdistuu. Järkevästi toimivat yritykset osaavat ennakoida vaarat ja ryhtyä varotoimiin ennen kuin on liian myöhäistä. Varautumiseen kuuluu, että digitaalisten tulostinten, kopiokoneiden ja monitoimijärjestelmien kiintolevyt ja muistit sekä niiden luottamuksellinen sisältö eivät ole ulkopuolisten saatavilla tai peukaloitavissa.

Tietoturvaan vakavasti suhtautuvat yrittäjät ja yritysjohtajat pitävät huolta, että verkkoyhteydet ovat suojattuja ja että luvaton pääsy organisaation tietoihin sisäverkossa on estetty. Valveutunut johto tietää, että yrityksen tiloihin sijoitetut tulostimet ja monitoimijärjestelmät voivat helposti muodostua vakavien tietovuotojen lähteeksi.

Laitteen luovutustasolle unohdettu luottamuksellinen asiakirja saattaa joutua vääriin käsiin ja välittyä ulkopuolisille esimerkiksi sähköpostin tai faksin kautta. Tietoturvasta huolehtiva yritysjohto ja IT-ammattilaiset suojautuvat näiltä riskeiltä rajoittamalla laitteiden käytön vain siihen oikeutetuille henkilöille sekä estämällä valvomattoman tulostuksen.

Konica Minolta tukee asiakkaidensa pyrkimyksiä suojautua tietoturvariskeiltä. Niinpä yhtiö on ohjannut runsaasti teknisiä resursseja bizhub-monitoimijärjestelmien ja -tulostinten tietoturvaominaisuuksien kehittelyyn. Konica Minolta tarjoaa asiakkailleen huipputeknologiaa, jota vastuu työympäristön tietoturvasta vaatii.

Jos verkkohyökkäykset, tietovarkaudet tai tietoturvamenettelyt askarruttavat tai laitteisiin kirjautumista ja toimintojen käyttöä halutaan rajoittaa, Konica Minoltan bizhub-teknologia tarjoaa ammattitason ratkaisuja tietomurtojen tunnistamiseen ja estämiseen. Nykyisin eri toimialojen asiakkaat sekä viranomaiset edellyttävät tasokasta ja kattavaa tietojen suojausta.

Tietoturvaominaisuudet ja niiden laitekohtainen saatavuus

Ominaisuudet	Värimonitoimijärjestelmät				Mustavalkomonitoimijärjestelmät						Tulostimet		
	bizhub C25	bizhub C3350 C3850	bizhub C224e C284e C364e C454e C554e	bizhub C654e C754e	bizhub 25e	bizhub 215	bizhub 3320 4020	bizhub 4050 4750	bizhub 224e 284e 364e 454e 554e	bizhub 654e 754e	bizhub C3100P	bizhub 3300P	bizhub 4000P 4700P
Kirjautumisen ja käytön valvonta													
Kopio-/tulostusseuranta	-	+	+	+	+	+	-	+	+	+	-	-	-
Toimintojen rajoitus (kopio/tulostus/ skannaus/faksaus/kansiot/väri)	+***	-	+	+	+	-	-	-	+	+	0	-	-
Turvatulostus (työn lukitus)	+	+	+	+	+	+	+	+	+	+	0	-	+
Kansioiden suojaus salasanalla	-	-	+	+	-	-	-	-	+	+	-	-	-
Käyttäjävarmennus (tunnus + salasana)	0	+	+	+	+	+	-	+	+	+	-	-	-
Biometrinen (sormen verisuonisto)	-	-	0	0	-	-	-	-	0	0	-	-	-
IC-kortinlukija	-	+	0	0	-	-	-	+	0	0	0	-	-
Tapahtumaloki	-	+	+	+	-	-	+	+	+	+	-	+	+
Asiakirjojen ja tietojen suojaus													
Kiintolevyn sisällön salaus	-	+	+	+	-	-	+	+	+	+	0	-	-
Kiintolevyn ylikirjoitus	-	+	+	+	-	-	+	+	+	+	0	-	-
Kiintolevyn suojaus salasanalla	-	-	+	+	-	-	-	-	+	+	0	-	-
Tietojen automaattinen poisto	-	-	+	+	-	-	-	-	+	+	0	-	-
Trusted Platform Module (TPM)	-	-	0	0	-	-	-	-	0	0	-	-	-
Verkon tietoturva													
IP-osoitteen suodatus	+	+	+	+	+	-	+	+	+	+	+	+	+
Portti- ja protokollakohtainen valvonta	+	+	+	+	+	+***	+	+	+	+	+	+	+
SSL/TLS-salaus (HTTPS)	+	+	+	+	+	+	+	+	+	+	+	+	+
IPsec-tuki	+	+	+	+	-	-	+	+	+	+	+	+	+
S/MIME	-	+	+	+	-	-	-	+	+	+	-	-	-
IEEE 802.1x -tuki	+	+	+	+	-	-	+	+	+	+	+	+	+
Skannauksen tietoturva													
Käyttäjävarmennus	-	+	+	+	+	-	-	+	+	+	-	-	-
POP before SMTP	+	+	+	+	+	+	-	-	+	+	-	-	-
SMTP-varmennus (SASL)	+	+	+	+	+	-	+	+	+	+	-	+	-
Manuaalisesti valitun osoitteen esto	-	+	+	+	-	-	+	+	+	+	-	-	-
Muita ominaisuuksia													
Huoltotilan suojaus	+	+	+	+	-	-	+	+	+	+	+	-	+
Ylläpitotilan suojaus	+	+	+	+	+***	+	-	-	+	+	+	-	+
Datan kaappaus	-	-	+	+	+	-	-	-	+	+	-	-	-
Luvattoman kirjautumisen esto	-	-	+	+	-	-	-	-	+	+	+	-	-
Kopiosuojaus vesileimalla	-	+	+	+	+	-	-	+	+	+	-	-	-
PDF-tiedostojen salaus	-	+	+	+	+	-	-	+	+	+	-	-	-
PDF-tiedostojen allekirjoitus	-	-	0	0	-	-	-	-	0	0	-	-	-
PDF:n salaus digitaalisella ID:llä	-	-	0	0	-	-	-	-	0	0	-	-	-
Copy Guard/Kopiointi salasanalla	-	-	0	0	-	-	-	-	0	0	-	-	-
ISO 15408 -sertifiointi													
ISO 15408 EAL3 -sertifioitu	-	+**	+	+	-	-	+**	+**	+	+	+""	-	-
IEEE std 2600.1 (-2009)	-	+**	+**	+**	-	-	-	+**	+**	+**	-	-	-

X = vakio O = optio / = ei saatavilla * vain tulostus ** arviointi meneillään * rajoitetusti**

KONICA MINOLTA

Common Criteria Validated

Konica Minolta Business Solutions Finland Oy ✒ Keilaranta 10 E ✒ 02150 ESPOO ✒ Puh. 010 442 9000 ✒ www.konicaminolta.fi

05/2014