RICOH
imagine. change.

Ricoh Security Solutions

Autamme turvaamaan liiketoimintaasi

Kyberturvallisuus on nykyään yksi suurimmista haasteista yritysten pärjäämiselle ja menestymiselle. Kaikenkokoiset yritykset ovat jatkuvassa vaarassa joutua vahingollisten hyökkäysten, kuten tietojen kalastelun, palvelunestohyökkäysten tai kiristysohjelmien kohteeksi. Näiden hyökkäysten todelliset kustannukset nousevat miljooniin. Vuonna 2017 Ponemon Institute selvitti, että yksittäisen tietoturvahyökkäyksen keskimääräiset kustannukset ovat 3,62 miljoonaa dollaria. Tämä luku tulee tulevina vuosina vielä kasvamaan, sillä hallituksen säännökset ja EU:n yleinen tietosuoja-asetus (GDPR) asettavat uusia vaatimuksia, ja yrityksiä, jotka eivät onnistu turvaamaan järjestelmiään ja tietojaan asianmukaisesti, rankaistaan ankarasti. Jotta yritykset voivat välttää rangaistukset, niiden on osoitettava, että ne kykenevät suojaamaan tietonsa. Tämä edellyttää kaikkien yritystä koskevien haavoittuvuuksien kokonaisvaltaista huomiointia.

Osansa yritysten kyberturvallisuushaasteesta muodostaa nykyaikaisen työympäristön laajeneminen ja digitalisointi sekä tietomäärien räjähdysmäinen kasvu. Työnkulut leviävät usein moniin eri laitteisiin, verkkoihin ja fyysisiin paikkoihin. Tiedot ovat eniten vaarassa juuri liikkuessaan ympäri yritystä. Ne on voitava turvata matkan joka vaiheessa. Tästä aiheutuu niin suuri tietoturvariski, että yritysten on pakko varmistaa toimintansa ottamalla käyttöön tietoturvallinen asiakirjojen ja tietojen hallintajärjestelmä. Samaan aikaan toimistojen tulostimien ja monitoimilaitteiden toiminnot ovat kymmenkertaistuneet viime vuosien aikana. Ne hoitavat nykyisin valtavan määrän liiketoimintaan liittyvien tietojen syötöstä, tulostuksesta, siirrosta ja tallennuksesta. Ja tästä syystä niiden tietoturvallisuutta ei pidä aliarvioida.

Monet yritykset väittävät tarjoavansa tietoturvallisia ratkaisuja, mutta Ricoh on kehittänyt turvallisia ratkaisuja ja palveluja toimistoympäristöön jo vuosikymmeniä. Esimerkiksi monitoimilaitteissamme on ollut jo yli 20 vuotta käytössä turvallinen kiintolevyn päällekirjoitustoiminto.

Tietoturva on keskeisessä roolissa koko digitaalisen työympäristön ratkaisuvalikoimassamme. Maailmalla on käytössä yli neljä miljoonaa toimistotuotettamme. Jokainen näistä tuotteista ja kaikki niihin liittyvät palvelumme sisältävät tietoturvaominaisuudet sisäänrakennettuina. Monissa tuotteissa on lisäksi käytössä vain Ricohin käyttämä käyttöjärjestelmä. Tämä on tietoturvapuolustuksemme olennainen tekijä, sillä se mahdollistaa valvonnan ja suojan yleisesti käytössä oleviin käyttöjärjestelmiin kohdistuvilta uhilta.

Ricohilla on maailmanlaajuinen palvelu- ja tukirakenne, joka varmistaa, että uhkiin liittyvä tieto jaetaan tehokkaasti, ja toimitaan viiveettä. Tulostavat laitteemme ovat vakiona IEEE 2600 -sertifioituja, ja lisäksi Ricoh on johtava jäsen ja merkittävä tekijä IEEE-standardointiyhdistyksessä. Ricoh on ISO 27001 -sertifioitu yritys, ja sitoutunut noudattamaan tätä tietoturvallisuuden hallintajärjestelmää. Me keskitymme tuotekehityksessämme asiakkaan liiketoimintatarpeisiin ja turvallisuuskysymyksiin useiden globaalien asiakaslähtöisten innovaatio-ohjelmiemme kautta.

Jotta tehokkaan ja todistettavan kyberturvallisuuden käytäntöjä koskevat tiukat vaatimukset voidaan täyttää, Ricohin valikoiman jokaiseen tuotteeseen ja palveluun sisältyy tietoturvanäkökulma jo suunnittelusta alkaen – ei koskaan jälkikäteen lisättynä. Uskomme, että haavoittuvuuksien kokonaisvaltainen tarkastelu on olennaista nykyaikaisessa liike-elämässä selviytymiselle.

ASIAKKAIDEN TIETOTURVAHAASTEET

TRENDI: Tietomäärien kasvaessa myös haavoittuvuudet, hyökkäykset ja rangaistukset lisääntyvät.

Digitaalisten työpaikkojen turvaaminen ja vahvistaminen

Ricoh haluaa mahdollistaa ja turvata digitaalisen työn kaikkialla, missä ihmiset toimivat. Modernissa digitaalitaloudessa tämä tarkoittaa sitä, että tarjoamme edistyneille ja yli perinteisen toimiston rajojen toimiville yrityksille lisäarvoa. Etätoimistot ja -työntekijät tuovat liike-elämään paljon joustavuutta ja parantavat päivittäisten toimintojen tuottavuutta. Tämä auttaa yrityksiä täyttämään paremmin asiakkaiden odotukset ja palveluun kohdistuvat vaatimukset.

Verkossa ja sen ulkopuolella työskentely aiheuttaa kuitenkin myös merkittäviä riskejä liiketoiminnan turvallisuudelle. Mobiilitöitä tekevien työntekijöiden luomien tietojen ja heidän tietojen keruuseen käyttämiensä etälaitteiden täytyy olla asianmukaisesti suojattuja. Työntekijät toimivat usein eri verkoissa ja eri alueilla, mikä vaikeuttaa asiaa entisestään. Ratkaisevaa on, että viranomaissäännökset, kuten EU:n yleinen tietosuoja-asetus edellyttävät yrityksiä suojaamaan tietonsa todistettavalla tavalla koko toimintansa ajan merkittävien rangaistusten uhalla. Työpaikat kehittyvät jatkuvasti, ja niissä on käytössä entistä enemmän digitaalisia työnkulkuja, joten liiketoimintatietojen elinkaari muuttuu vähitellen entistä monimutkaisemmaksi. Tarkastellaanpa sitä vaihe vaiheelta.

Ensimmäinen vaihe on tietojen syöttöön ja asiakirjojen skannaukseen käytettävät laitteet – olennainen osa Ricohin tietoturvasuojausta. Tämän jälkeen tietoja on siirrettävä eri verkoissa, ja ne on tallennettava turvallisesti. Tässä vaiheessa tietojen eheys on olennaisen tärkeää. Ricohin järjestelmät rajoittavat laitteen ja verkkotoimintojen käyttöä, jotta varmistetaan, ettei tietoja voida peukaloida siirron aikana tai muulloin. Tämän vaiheen tietoturvatoimintoja ovat muun muassa käytönvalvonta, salaus ja kopiointisuojaus. Me kutsumme tätä vaihetta kokonaisuudessaan ”hallinnaksi”.

Kun asiakirjat on tallennettu, niiden täytyy kuitenkin olla oikeaan aikaan käytettävissä henkilöille, jotka tarvitsevat niitä liiketoiminnassa. Mahdollisuus käyttää tietoja juuri silloin kun niitä tarvitaan ja saada ne tehokkaasti näkyviin riippuu niiden saatavuudesta. Tietojen analysointi on olennainen osa tehokasta digitaalista työympäristöä. Se tarjoaa käsityksen kaikista liiketoiminnan osista myynnistä henkilöstöhallintoon. Käyttöoikeuksien hallintatyökalut tarjoavat nopean ja turvallisen käytön käyttäjän sijainnista tai käytettävästä laitteesta riippumatta. On olennaisen tärkeää, etteivät tietoturvaprotokollat vaikeuta innovointia tai toimivuutta tai aiheuta tyytymättömyyttä työntekijöiden keskuudessa. Me kutsumme tätä vaihetta ”suojaukseksi”.

Lopulta tiedot on hävitettävä turvallisella ja auditoitavalla tavalla. Tämä vaihe on tärkeä lakisäädösten noudattamisen kannalta, ja sillä minimoidaan varkauden tai häviämisen mahdollisuudet. Prosessi on itse asiassa käytössä asiakirjan koko elinkaaren ajan sekä sen lopullisessa käytöstä poistossa. Tiedoston tulostaminen jättää monitoimilaitteen kiintolevylle aina jäljen, joka on päällekirjoitettava luvattoman käytön estämiseksi. Ricohin tietojenpoistopalveluihin kuuluu kiintolevyn puhdistus, muistin tyhjennys, tulostamattomien tiedostojen poisto ja tiedoston poisto uloskirjautumisen yhteydessä. Nämä estävät hakkereita saamasta arkaluonteisia tietoja asiakirjojen jättämistä jäljistä. Me kutsumme tätä vaihetta ”käytöstä poistoksi”.

Ricoh käyttää ”CIA”-periaatteita (Confidentiality, Availability, Integrity) työpaikan tietojen tehokkaaseen turvaamiseen niiden koko elinkaaren ajan: Luottamuksellisuus, käytettävyys ja eheys. Nämä ovat ohjenuoramme suunnitellessamme tuotteita ja ratkaisuja, jotka täyttävät kaikki tarpeelliset standardit ja säädökset. Tämä lähestymistapa mahdollistaa työpaikan innovaatiot ja kasvun säilyttäen silti tehokkaat ja turvalliset prosessit.

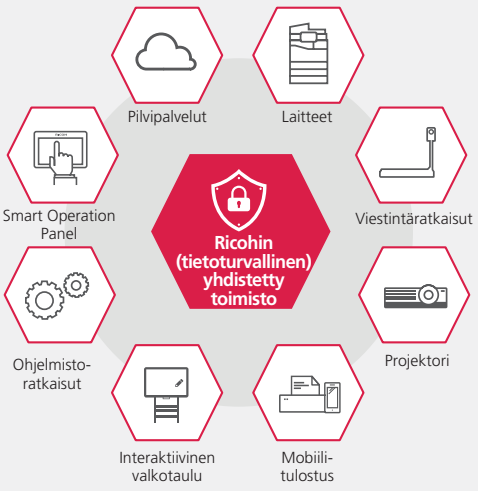
RICOHIN LÄHESTYMISTAPA TIETOTURVAAN

Pääsyä tietoihin ja asiakirjoihin on rajoitettava asiakkaan määrittämien tietoturvavaatimusten ja -käytäntöjen mukaan.

Pääsy tietoihin ja asiakirjoihin paikasta ja ajasta riippumatta.

Asiakirjan luvattoman muokkauksen estäminen siirto- ja säilytysvaiheessa.

Ratkaisujemme keskiössä ovat ”CIA”-periaatteet koskien tietosuojaa ja turvallisuutta: Luottamuksellisuus, eheys ja saatavuus.



Turvallisuus on toimintamme ytimessä. Jokainen Ricohin tuote ja palvelu sisältää tietoturvaominaisuudet ja -ratkaisut sisäänrakennettuna.

Ricoh tarjoaa kattavan valikoiman tietoturvaratkaisuja, joiden avulla asiakirjat suojataan alusta loppuun.

Perehdymme nyt vuorollaan jokaiseen tärkeään vaiheeseen: hallintaan, suojaukseen, poistamiseen ja tukeen.

DIGITAALISEN TYÖPAIKAN TURVALLISUUDEN NELJÄ VAIHETTA

1 HALLINTA

Tietojen tehokas hallinta on ratkaisevan tärkeää luottamuksellisuuden ja eheyden säilyttämiseksi. Liiketiedot ovat yrityksen tärkein omaisuus ja ne on suojattava. Nykypäivän laitteet ovat tietopäätteitä, jotka voivat toimia liiketietojen haavoittuvaisina väylinä. Ricoh käyttää käyttäjän tunnistuksessa ja laitehallinnassa useita työkaluja, joiden avulla voidaan valvoa ja suojata liiketietoja. Näihin kuuluvat fyysisten laitteiden asetukset, jotka sallivat ja estävät pääsyn tiettyihin toimintoihin ja tietoihin. Erittäin tärkeä vaihe asiakirjan turvallisuuden säilyttämisessä on se, että rajoitetaan työntekijöiden pääsyä tietoihin, jotka kulkevat toimistojen monitoimilaitteiden kautta. Hallintavaihe sisältää myös laitteiden haittaohjelmasuojauksen Ricohin laiteohjelmistojen kolmitasoisen varmistusmenetelmän avulla.

Luvattoman kopioinnin esto

Luvattomilta kopiointiyrityksiltä suojaa Ricohin hieno ratkaisu, joka takaa tulostettujen asiakirjojen turvallisuuden. Kopiointisuojaustoiminto tulostaa tai kopioi asiakirjat siten, että taustalle on upotettu näkymätön erikoiskuvio. Jos tulostettu tai kopioitu asiakirja kopioidaan ja/tai skannataan, upotetut kuviot tulevat näkyviin. Luvattomalta käytöltä suojaavan kopiointisuojatoiminnon avulla monitoimilaite voi estää tietovuodot havaitsemalla upotetut kuviot ja korvaamalla kopioidut kuvat harmaalla kuvalla. Tämä toiminto on hyödyllinen, kun tulostetaan luottamuksellisia tietoja. Luottamuksellisten tietojen kopioinnin rajoittaminen estää tietovuotoja.

Lukittu tulostus

Tietokoneelta tulostettu asiakirja voidaan tallentaa monitoimilaitteen kiintolevylle. Ricohin lukittu tulostus -toiminnon avulla käyttäjä voi määrittää salasanan lähettäessään asiakirjan tulostettavaksi, ja tämä salasana on annettava monitoimilaitteella ennen kuin asiakirjan voi tulostaa. Koska asiakirjaa ei tulosteta ennen kuin sen omistaja on itse laitteella, lukittu tulostus takaa, että asiakirja pysyy omistajansa hallinnassa.

Edistyksellinen skannauksen suojaus

Ricohin edistyksellisten skannausratkaisujen valikoima sisältää erilaisia salaus- ja salauksenpurkutasoja käsittelyn kaikilla tasoilla ja skannausprosessin kaikissa eri vaiheissa. Pääkäyttäjät voivat antaa pääsyn prosessijonoihin yksittäisten käyttäjien sisäänkirjautumisten tai ryhmän tietojen perusteella. Lisäsuojaustasoihin kuuluvat SAML-tekniikka (Security Assertion Markup Language) kertakirjautumisten (SSO) yhteydessä sekä henkilökorttiin perustuva PIV-salaus ja julkisen avaimen infrastruktuuri eli PKI-salaus.

Käyttäjäoikeuksien hallinta

Ricoh-laitteiden käyttöä ja henkilöllisyyden tunnistustapaa voidaan hallinnoida keskitetysti. Mahdollisia tapoja tunnistautua ovat henkilökortti, PIN-tunnus, sisäänkirjautuminen verkkotunnuksilla tai jokin edellisten yhdistelmä. Moninkertainen tunnistus parantaa tietoturvaa, mutta voi tuntua kiireisten käyttäjien näkökulmasta liikaa käyttöä hidastavalta. Kertakirjautuminen (Single Sign On, SSO) auttaa tässä, sillä sen avulla käyttäjät voivat käyttää saumattomasti useita laitteita. Lisäksi laitteisiin on esiasennettuna Ricohin pikatunnistus, joka liitetään NFC-kortinlukijaan ja konfiguroidaan. Tämä on käyttäjille nopea tapa päästä käsiksi asiakirjoihin. NFC-lukija/-kirjoittaja helpottaa valtavasti käyttäjän sisäänkirjautumista ja tarjoaa samalla tehokkaan ja turvallisen tavan hallita pääsyä monitoimilaitteelle. Tulostuksenhallinnan avulla yrityksen on helppo rajata käyttäjien pääsyä eri toimintoihin, ja kirjautumalla laitteelle käyttäjä pääsee vain hänelle tarkoitettuihin toimintoihin.

Laitehallinta

Ricohin Streamline NX -ratkaisuun sisältyvä laitehallintamoduuli on Ricohin verkon laitteiden hallintaan ja valvontaan tarkoitettu ohjelmisto. Ohjelmiston avulla pääkäyttäjät voivat nähdä laitteiden suojausasetukset tai muuttaa niitä käyttämällä esipakattuja malleja ja muokattuja parametreja. Tärkeitä suojausasetuksia ovat protokollien käyttöönotto/käytöstä poisto, IP-osoitteiden asetukset, pääkäyttäjien salasanat, sähköpostiosoitteet ilmoituksia varten, salausasetukset ja paljon muuta. SLNX voi myös raportoida tulostimista, jotka eivät ole yhdenmukaisia asiakkaan käytäntöjen kanssa.

Laitteen suojaaminen haittaohjelmilta

Ricohin laitteissa on kolmitasoinen suojaus haittaohjelmia vastaan. Ensinnäkin Ricohin laitteita voi käyttää ainoastaan Ricohin omaa konekieltä tai käyttöjärjestelmää käyttäen. Toisekseen, laitteen ohjelmiston haitallinen peukalointi on estetty siten, että kaikkien laiteohjelmistopäivitysten tekemiseen ja hyväksymiseen kelpaa ainoastaan kyseinen Ricohin konekieli. Lopuksi, kaikkiin laiteohjelmistopäivityksiin tarvitaan Ricohin digitaalinen allekirjoitus. Tämän kolmivaiheisen menetelmän ansiosta Ricohin laitteisiin ei voida ladata hyväksymättömiä laiteohjelmistoja, joten haitta- ja vakoiluohjelmat sekä virukset voidaan eliminoida tehokkaasti.

Fyysinen asiakirjaturvallisuus

Parhaiden turvallisuuskäytäntöjen ei tarvitse olla aina monimutkaisia. Toimistot ovat usein kiireisiä paikkoja, ja tulostetut asiakirjat aiheuttavat merkittävän liiketoimintariskin sekä varkauksien että työntekijöiden huolimattomuuden osalta. Ricohilla on myös useita lisäsuojausvaihtoehtoja, joilla voidaan estää tulosteiden luvaton käyttö. Esimerkiksi paperikasettien lukitus estää arkaluonteisten paperien varkaudet – hyvä esimerkki tästä on terveydenhuoltoalan reseptipaperi. Suojalevyjen asentaminen kaikkiin johtoihin estää sisäisten uhkien aiheuttamalta peukaloinnilta. Turvatulostus eli turvallinen asiakirjan vapautus (Print-to-me) takaa, että asiakirjoja voidaan tulostaa ainoastaan omistajan ollessa läsnä. Näin voidaan ehkäistä noutamattomien tulosteiden aiheuttama tietoturvariski.

2 SUOJAUS

Uusien ja olemassa olevien säädösten mukaisesti yritysten on varmistettava sekä tietojen luottamuksellisuus, eli suojaus tietovarkauksilta ja -vuodoilta, sekä tietojen eheys, eli muuttumattomuus. Saavuttaakseen nämä tavoitteet yritysten on rajoitettava pääsyä arkaluontoisiin asiakirjoihin. Näin estetään luvattomat muutokset ja väärennökset. Samalla suojaudutaan yritykseen kohdistetuilta tai opportunistisilta uhilta.

Mobiilityöskentely monimutkaistaa kyberturvallisuusnäkymiä. Jotta tiedostojen jakaminen olisi mahdollista sijainnista riippumatta, on otettava käyttöön lisäsuojaustoimia. Tiedostojen tulee olla yhtä turvassa verkkojen yli ja laitteelta toiselle siirrettäessä kuin tallennettuinakin. Vahvan salausteknologian avulla tietoja voidaan seurata ja suojata tehokkaasti niiden koko elinkaaren ajan. Tämä koskee luonnollisesti asiakirjoja, mutta ulottuu myös tärkeisiin suojauselementteihin kuten tallennettuihin salasanoihin, makroasetuksiin ja osoitekirjoihin. Vaikka hakkerit onnistuisivat tekemään tietosuojamurron, on salausta käytettäessä erittäin vaikeaa saada ulos käyttökelpoista tietoa. Näin ollen tiedon eheys on tässäkin tapauksessa turvattu.

Jatkuva valmius on monilla aloilla kaikkein tärkeintä. Ennakoimattomat tapahtumat, kuten luonnonkatastrofit, aiheuttavat tästä syystä suoran liiketoimintariskin. Paperiset asiakirjat ovat erityisen haavoittuvia tässä skenaariossa. Digitaalisten asiakirjojen turvallinen pilvipohjainen säilytys lisää olennaisesti palautumiskykyä niin luonnon kuin ihmistenkin aikaansaamista katastrofeista. Digitaalisten tietojen säilyttämiseksi on kuitenkin ryhdyttävä tarvittaviin suojaustoimiin.

Luottamuksellisten tietojen salaus

Tietoja voidaan suojata niiden liikkuessa laitteesta toiseen käyttämällä salausta kaikkiin Ricoh-monitoimilaitteen kiintolevylle tuleviin tai sinne tallennettuihin tietoihin. Sisäänrakennettu ohjelmisto mahdollistaa skannattujen ja tulostettujen tiedostojen päästä päähän -salauksen PKI-infrastruktuurin avulla. Se suojaa väliintulohyökkäyksiltä asiakkaan tietojärjestelmässä.

Lisäturvaa antaa se, että tulostettavat tiedot päällekirjoitetaan toistuvasti Ricohin DOSS-järjestelmän (Data Overwrite Security System) avulla, josta kerromme tarkemmin jäljempänä tietojen elinkaaren hävittämistä käsittelevässä osiossa.

BIOS-tason ja käyttöjärjestelmän suojaus

Ricohin monitoimilaitteissa käytetään TPM-salausmoduulia (Trusted Platform Module), joka on väärinkäytöltä suojattu laitteiston suojausmoduuli. TPM suorittaa salausteknisiä toimintoja ja tallentaa turvallisesti salakirjoitetut tiedot. Ricoh tallentaa TPM-salauksen avulla juurihakemiston salakirjoitusavaimen, joka suojaa kiintolevyn salakirjoitusavainta ja monitoimilaitteiden digitaalista varmennetta. Se antaa myös pääkäyttäjille mahdollisuuden suorittaa suojattu käynnistys ja vahvistaa monitoimilaitteen laiteohjelmiston aitous ennen sen toiminnan sallimista.

Laiteohjelmiston validointi

Juuritiedoston avain ja salaustekniset toiminnot sisältyvät aina TPM-salaukseen eikä niitä voida muuttaa palomuurin ulkopuolelta. Näin estetään tuotteidemme väärinkäyttö tai haitallinen peukalointi. Prosessi mahdollistaa monitoimilaitteen laiteohjelmiston ja laiteidentiteetin korkeatasoisen validoinnin sekä kiintolevyn tietoturvan. Tämäkin on hyvä esimerkki siitä, että Ricohin monitoimilaitteiden suunnittelussa asiakkaiden turvallisuusnäkökulma tulee aina ensimmäisenä.

Salasanojen hallinta

Ricohin laitteita voivat määrittää useat järjestelmänvalvojatason käyttäjät, joista kullakin on oma roolinsa laitteilla sekä yksilölliset salasanat. Näiden käyttäjien salasanat voidaan määrittää etänä verkkopohjaisten hallintatyökalujen avulla ja ne varmennetaan säännöllisesti. Tämä mahdollistaa tehtävien eriyttämisen, mikä on edellytys useissa liiketoimintaa koskevissa säädöksissä.

Käyttöoikeuksien rajoitukset

Ricohin käyttäjähallintatyökalun avulla pääkäyttäjät voivat rajoittaa käyttäjän käyttöoikeuksia. Pääkäyttäjä voi esimerkiksi asettaa valituille käyttäjille oikeuden käyttää monitoimilaitteen tallennettua osoitekirjaa. Tämä estää henkilökohtaisten tietojen ja toimiston laitteisiin tallennettujen tietojen luvattoman käytön.

Käyttäjän lukitustoiminto

Jos sisäänkirjautuessa annetaan toistuvasti vääriä salasanoja, Ricohin monitoimilaite voi arvioida, että joku yrittää murtaa salasanaa. Tämä kytkee päälle lukitustoiminnon, joka estää laitteen käytön kyseiseltä käyttäjätunnukselta. Lukittua käyttäjätunnusta ei hyväksytä, vaikka sen yhteydessä annettaisiin myöhemmin oikea salasana. Lukitus voidaan vapauttaa vain pääkäyttäjän asettaman ajan kuluttua. Näin estetään tehokkaasti mahdolliset hakkerointiyritykset.

3 POISTAMINEN

Tietojen turvallinen poisto on olennainen osa kattavaa kyberturvallisuuden puolustusta. On helppo langeta siihen ansaan, että uskottelee yritysvelvoitteiden päättyvän tiedon lähtiessä organisaatiosta. Monissa säädöksissä kuitenkin määrätään, että tietojen hävittämisen täytyy olla kattava prosessi, jolla eliminoidaan kaikki myöhemmän varkauden tai käytön aiheuttamat väärinkäytökset. Yritysten tietoja koskevat velvollisuudet eivät pääty ennen kuin tämä voidaan todistaa.

Käyttöikänsä loppuun tulleet ja myyjälle palautetut toimistolaitteet aiheuttavat yrityksen tiedoille vaaran, joka jää usein tunnistamatta. Ricoh tarjoaa sertifioitua ja auditoitavaa palvelua tietojen poistamiseen näistä käyttöikänsä loppuun tulleista tulostimista. Tähän sisältyy usein huomiotta jäävä materiaali, kuten tallennetut verkkoasetukset, käyttäjätiedot, kiintolevyn tiedot tai vaikkapa laitteessa olevat tarrat. Jos näitä tietoja ei poisteta, on merkittävä vaara, että luottamuksellisia liike- ja henkilötietoja pääsee vuotamaan. Säädösten noudattamiseksi tämä prosessi pitäisi suorittaa toistuvasti myös laitteen koko käyttöiän ajan. Näin varmistetaan, että yritykset valvovat mahdollisimman hyvin vastuullaan olevia tietoja.

Tiedon ylikirjoitus: Data Overwrite Security System (DOSS)

Monitoimilaitteiden kiintolevyt toimivat tehokkaasti tallentamalla muistiinsa latenttikuvia asiakirjatiedoista työn käsittelyä varten. Ricohin tietojen ylikirjoitusratkaisu DOSS varmistaa, että kuva ylikirjoitetaan aina ennen seuraavan työn aloittamista. Jos joku onnistuisikin pääsemään kiintolevylle vahingoittamistarkoituksessa, hän ei pääsisi käsiksi minkään aiemman työn tietoihin. Me Ricohilla olemme ylpeitä siitä, että olemme tarjonneet tämän parhaan käytännön mukaisen toiminnon jo yli 20 vuoden ajan.

Tietojenpoistopalvelu käyttöajan päätyttyä

Ricoh tarjoaa kattavan tietojenpoistopalvelun, eli käyttöiän tai sopimuksen päättymisen jälkeisen palvelun monitoimilaitteille ja tulostimille. Siinä kaikki laitteiden muistimoduulit ja levytallennustilat tyhjennetään käyttämällä alan sertifioituja turvallisuusratkaisuja, kun laite poistuu yrityksen käytöstä. Ricohin IT-palvelut tarjoavat myös kattavaa laitteiden hävittämispalvelua, johon sisältyy monen tasoisia sertifioituja tietojen poistopalveluja.

Kiintolevyn vaihtaminen ja muistilaitteet

Ricoh tarjoaa kiintolevyjen irrotus- ja palautuspalvelua, jonka avulla asiakkaat saavat takaisin oman kiintolevynsä, kun se vaihdetaan uuteen tyhjään kiintolevyyn, kun laitteesta luovutaan. Näin taataan yrityksen kattava ja todistettava tietoympäristön valvonta.

4 TUKI

Yritysten kasvaessa myös laitteiden ja verkkojen välisten yhteyksien määrä väistämättä kasvaa. Yritykset tarvitsevat strategioita varmistamaan ettei ympäristön kasvu aiheuta turvallisuusuhkaa. Järjestelmän heikot kohdat täytyy tuntea, jotta voidaan ennaltaehkäistä virushyökkaukset ja tietovarkaudet.

Usein tarvitaan tietoturva-asiantuntija analysoimaan yrityksen infrastruktuuri ja tunnistamaan haavoittuvuudet. Monilla yrityksillä ei ole mahdollisuutta palkata omaa riittävän asiantuntevaa IT-henkilöstöä valvomaan verkkoturvallisuutta. Kulut ja kustannukset pakottavat yritykset usein vaaralliseen suvantotilaan.

Liiketoiminnan riskien kokonaisvaltainen ymmärtäminen on olennaista verkkoturvallisuuden kannalta. Ricohin turvallisuusasioihin perehtynyt tiimi (Security Incident Response Team; SIRT) varmistaa, että asiakkaille ympäri maailman välitetään tärkeät uhkia koskevat tiedot, jotta voidaan välittömästi koordinoida tehokkaat vastatoimet.

Infrastruktuurin turvallisuuden arviointi

Ricohin Streamline NX (SLNX) -laitehallintatoiminto on suunniteltu suorittamaan äärimmäisen tärkeää turvallisuuskäytäntöjen valvontaa. Hallintaratkaisu tarjoaa IT-vastaaville mahdollisuuden tehdä yrityksen käytäntöjen mukaisia laiteasetuksia, jakaa näitä asetuksia ja analysoida asetuksia visuaalisten raporttien avulla. Laitehallinta voi myös varoittaa, jos laite ei täytä yrityksen vaatimuksia.

Tulostusturvallisuuden optimointi

Ricoh tarjoaa kattavan tulostusturvallisuuden optimointipalvelun (Print Security Optimisation, PSO) sekä ammattimaiset ja hallitut neuvontapalvelut laitekohtaisten tietoturva-aukkojen tunnistamiseen. Kyseessä on verkkopohjainen työkalu, jonka graafinen ohjattu toiminto näyttää nykyisen tilan ja antaa Ricohin tehdä tuotesuosituksia riskien vähentämiseksi.

Tuoteturvallisuustiimi (PSIRT)

Ricohin aktiivinen vastaus uusiin uhkiin ja tehokkaiden vastatoimien kehittämiseen on Ricohin tuoteturvallisuustiimin (Product Security Incident Response Team, PSIRT) käsissä. Näin Ricoh varmistaa, että koko tuotepakettia (laitteistoa ja ohjelmistoa) päivitetään jatkuvasti sekä suojataan uusilta havaituilta uhilta ja haavoittuvuuksilta. Tämä auttaa ylläpitämään korkean palvelutason maailmanlaajuisesti sekä vähentämään haavoittuvuuden aiheuttamia ongelmia Ricohin tuotteissa.

Tukidokumentaatio

Valmistautuminen ja koulutus on olennaisen tärkeää kaikissa kyberturvallisuuteen liittyvissä järjestelyissä. On tärkeä huolehtia, että yrityksellä on käytettävissään tietoturvaan liittyvä tukidokumentaatio, käyttöoppaat, tietoturvaraportit sekä koulutus. Kuten monissa verkkoturvallisuusympäristöön liittyvissä seikoissa, todennettava vaatimustenmukaisuus on tärkeää ja tällä dokumentaatiolla on olennainen merkitys liiketoiminnan tuloksen turvaamisessa.

MITEN RICOH VOI AUTTAA?

Ricoh on vahvasti mukana muuttuvassa markkinassa ja on yksi alan johtavista tietoturvallisten asiakirjaratkaisujen toimittajista. Autamme asiakkaitamme huomioidaan asiakirjojen luottamuksellisuuden ja tietoturvan käsittelyn eri vaiheissa: tietoturvallinen tulostus ja laitehallinta, jäljitettävät, vaatimustenmukaiset skannaustyönkulut sekä turvallinen tietojenpoisto laitteiden käytöstä poiston yhteydessä.

Käyttäjän tunnistus ja valtuudet

- Lukittu tulostus
- Tunnistuksessa vakiona sulautettu ohjelmisto
- Käyttäjän tunnistus/käytön rajoitus
- Kertakirjautuminen
- Pääkäyttäjän monet roolit
- PDF-salasanasuojaus (skannatun asiakirjan salasana)
- Luvattoman kopioinnin suojaus
- IP-osoitteeseen pohjautuva käytön valvonta
- Turvallinen laite- ja tulostushallinta
- PKI (julkisen avaimen infrastruktuuri) / SmartCard-tuki
- Turvatulostus (print2me/lukittu tulostus)

BIOS-tason ja käyttöjärjestelmän suojaus

- Turvallinen käynnistys TPM-salausmoduulilla

Tiedon päällekirjoitus ja muistivälineet

- Levyn päällekirjoitustoiminto (DOSS)
- Irrotettava kiintolevy

Laitteen suojaaminen haittaohjelmilta

- Palvelimet
- Ei altis/vähemmän altis haittaohjelmille
- Smart Operation Panel – Androidin tietoturvallisempi versio
- Ricohin oma käyttöjärjestelmä (koneen komentokieli) monitoimilaitteille
- Kolmitasoinen järjestelmä – digitaalinen allekirjoitus, lataus Ricoh-työkalulla, kirjoitettava erityisellä komentokielellä

Tietojen salaus

- Kiintolevyn salaus TPM-moduulilla
- Salausavaimet TPM-moduulilla
- Tulostettujen ja skannattujen tiedostojen päästä päähän -salaus PKI-avaimen avulla
- FIPS-sertifioitu kiintolevy (Federal Information Processing Standards, optio)
- Tulostuksen päästä päähän -salaus
- Skannauksen päästä päähän -salaus

Kiintolevyn hävittäminen

- Kiintolevyn hävittäminen, kuvan päällekirjoitus
- Tietojenpoistopalvelu
- Käyttöiän tai sopimuksen päättymisen jälkeinen palvelu: tietojen tuhoaminen muistimoduuleista ja kiintolevyltä

Laiteohjelmistopäivitykset ja salasanojen hallinta

- Salasanojen etävalvonta
- Käyttäjän lukitustoiminto
- Laiteohjelmiston validointi TPM-moduulilla

Laitehallinta

- Kiintiöasetus / tilirajoitus
- DMNX – turvallisuusauditointi, salasanan hallinta, valvonta ja ilmoitustoiminnot samassa paketissa

Alan standardien noudattaminen

- ISO 27001 -serfikaatti
- IEEE 2600.2 -sertifikaatti tietyille tuotteille
- ISO 15408 -sertifikaatti tietyille tuotteille
- Turvallisuusdokumentaatio ja koulutus

RICOHIN MONITASOINEN LAITESUOJAUS

On selvää, että monitoimilaitevalmistajan rooli on muuttunut paljon – emme ole enää vain laitevalmistaja vaan mukana myös tietojen hallinnassa. Monitoimilaitteiden tehtävät ulottuvat nyt eri lähteistä tulevien asiakirjojen tallennuksesta aina tietojen luokitteluun ja työnkulun integrointiin sekä tietojen turvalliseen ja suojattuun tallennukseen ja analysointiin. Tilanne muodostaa monimutkaisen verkon, jossa on huomioitava tiukat säännökset ja tietojen säilytysvaatimukset sekä vielä sisäiset ja ulkoiset tallenteiden häviämiseen, tuhoutumiseen tai peukalointiin kohdistuvat uhat. Siksi Ricoh käyttääkin laiteturvallisuuden takaamiseksi monitasoista suojausta. Sen avulla voimme varmistaa monitoimilaitteesi ja siihen liittyvien järjestelmien parhaan mahdollisen suojauksen.

1. Laite

Jokaisen Ricoh-mallin ytimen muodostaa itse laite. Turvallisuus on ollut keskiössä jo heti laitteiden suunnittelussa, valmistuksessa ja toteutuksessa. Ricohin omassa käyttöjärjestelmässä ei ole samoja haavoittuvuuksia kuin monissa kaupallisissa ja yleisesti saatavissa käyttöjärjestelmissä, ja laitteemme on sertifioitu IEEE2600.2 -standardin mukaisesti. Kiintolevyn salaus ja levyn ylikirjoitustoiminto takaavat, että käsiteltävät tiedot pysyvät luottamuksellisina.

2. Smart Operation Panel -älykäyttöpaneeli toimii käyttöliittymänä

Samalla tavalla kuin monitoimilaitteissa, myös Smart Operation Panel -älykäyttöpaneelissamme on Ricohin oma käyttöjärjestelmä. Siihen ei ole asennettu mitään tarpeettomia osia eikä juurihakemistoa pääse käyttämään. Ricoh on tehnyt paljon töitä varmistaakseen, ettei Smart Operation Panelin käyttöönotto heikennä laiteturvallisuutta.

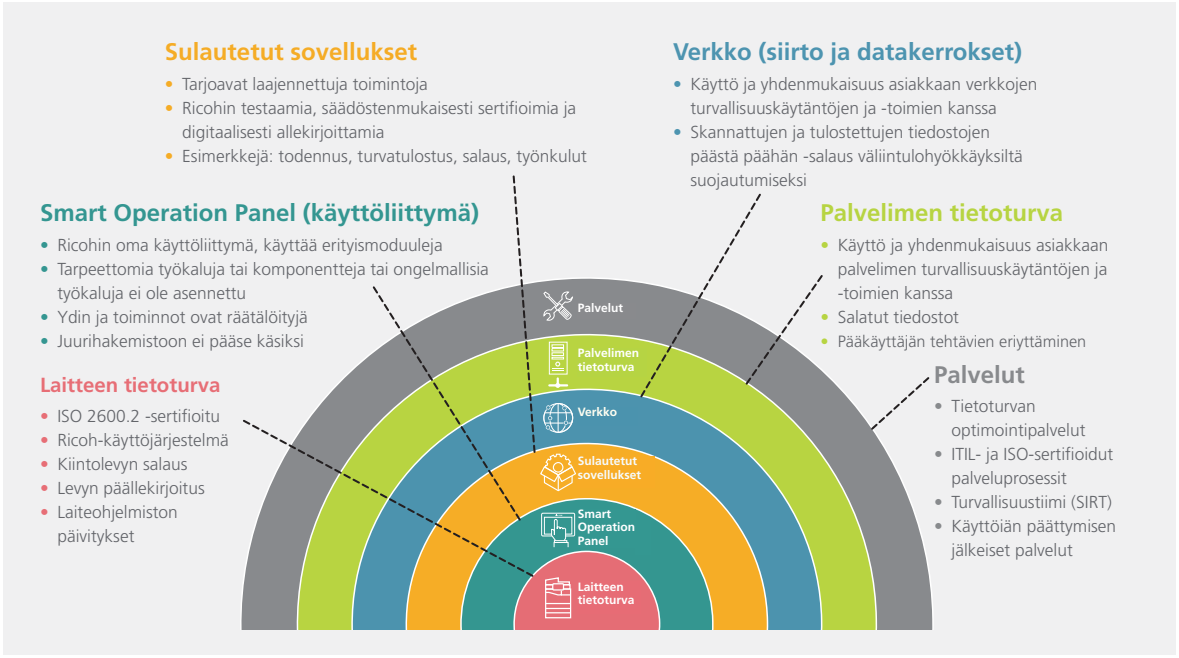
3. Älykkäät sovellukset

Smart Operation Paneliin voidaan sulauttaa sovelluksia, jotka tarjoavat käyttäjälle lisätoimintoja, kuten työnkulkujen automatisointia ja tietojen tallennusta. Jotkin sovellukset tarjoavat tärkeitä lisätoimintoja. Näitä ovat muun muassa turvatulostus, kirjautuminen henkilökortilla ja salaus. Sovellukset ovat Ricohin tai Ricoh Developer Programme -ohjelman jäsenten kehittämiä, ja kaikkien sovellusten täytyy läpäistä Ricohin yhdenmukaisuustestit ja olla digitaalisesti allekirjoitettuja ennen kuin niitä voidaan käyttää Smart Operation Panelissa.

4. Verkko ja palvelimet

Riippumatta siitä, kuka hallinnoi IT-ympäristöä, Ricoh takaa, että tuotteemme ja palvelumme täyttävät kaikki tietotekniikkaa ja verkon turvallisuutta koskevat käytännöt. Tulostettujen ja skannattujen tiedostojen päästä päähän -salaus, tietojen salaus palvelimilla ja pääkäyttäjän tehtävien eriyttäminen ovat tekniikoita, joilla suojaudutaan väliintulohyökkäyksiltä tai sisäpiirin tekemiltä vuodoilta.

Ricoh tarjoaa tuotteisiinsa kattavia tietoturvapalveluja, kuten neuvonta- ja hallintapalveluja, joilla autetaan asiakkaita valvomaan, optimoimaan ja hallitsemaan asiakirjojen ja tietojen turvallisuutta. Tarjoamme myös käyttöiän päättymisen jälkeisiä palveluja, joilla varmistetaan, että asiakkaiden vanhojen laitteiden RAM-muisti ja kiintolevy tyhjennetään ennen laitteiden hävittämistä.



MITEN RICOH SUOJAA DIGITAALISEN TYÖPAIKAN

Asiakkaillamme on lukuisia turvallisuuteen liittyviä huolenaiheita, joita kaikkia vahvistaa se liike-elämän tosiasia, että datamäärien kasvaessa myös haavoittuvuudet, hyökkäykset ja lakisääteiset rangaistukset lisääntyvät. Tietojen pitäminen luottamuksellisina, turvallisina ja peukaloinnilta suojattuina on jatkuvaa taistelua. Esimerkiksi Ricoh torjuu kuukausittain noin 8 miljardia palomuurihyökkäystä. Globaaleja, kansallisia ja alakohtaisia tietoja koskevia säädöksiä on kymmeniä tuhansia, ja yritysten täytyy jatkuvasti todistaa noudattavansa näitä kaikkia. On ymmärrettävää, että kaikenkokoiset organisaatiot etsivät luotettavia kumppaneita – sellaisia, jotka auttavat säilyttämään tietoturvan kaikissa laitteissa, joita digitaalisella työpaikalla tarvitaan.

Ricoh on kehittänyt laajan valikoiman sovelluksia lieventämään monia yritysten kohtaamia riskejä. Koska tietoturvauhkien maailma kehittyy uskomattoman nopeasti, Ricoh käyttää asiakkaan ääni (VOC) -ohjelmia apuna palvelujen kehittämisessä ja tuottamisessa.

Asiakasryhmät toimivat tärkeinä strategisina neuvoa-antavina ryhminä. Niiden avulla voimme ymmärtää paremmin asiakkaiden liiketoimiin vaikuttavia suuntauksia, tekijöitä ja prioriteetteja. Teknologiakonferensseissamme esitellään tärkeitä tietoja päätöksenteon huipulta. Ricohin suunnittelu- ja tuotekehitystiimit hyödyntävät näitä konferensseja saadakseen arvokasta asiakaspalautetta ideoista, suunnitelmista ja prototyypeistä. Ricoh tekee lisäksi yhteistyötä yksittäisten asiakkaiden kanssa uusien ja innovatiivisten turvaominaisuuksien kehittämisessä niin vertikaalisissa asiakassuhteissa kuin yleisemminkin. Asiakaslähtöinen lähestymistapa auttaa meitä vahvistamaan tuotesuunnitelmaamme, ja asiakkaamme hyötyvät globaalista palvelu- ja tukiverkostosta.

Nykyaikaisen digitaalisen työpaikan täytyy olla yhtä dynaaminen kuin kohtaamansa verkkouhat, ja yhtä joustava kuin työmenetelmänsä. Tästä syystä uskomme, että kyberturvallisuuden täytyy toimia saumattomasti kaikessa asiakkaidemme työpaikoillaan käyttämässä teknologiassa. Olemme sitoutuneet noudattamaan koko organisaatiossamme ISO 27001 -standardia ja kaikissa tuotteissamme IEEE 2600 -sertifointia. Laitteissamme käytettävä Ricohin oma käyttöjärjestelmä takaa, että parhaat tietoturvan valvontakeinot ovat käytössä yrityksen rakenne- tai kasvumuutoksista riippumatta.

Erilaiset tietoturvauhkat, lakisääteiset vaatimukset ja monimutkaiset alan standardit tarkoittavat, että kyberuhkien aiheuttamat potentiaaliset mainetta ja taloutta koskevat vaarat ovat suurempia kuin koskaan. Nyt on oikea aika hyödyntää luotettua kumppania, joka auttaa suojaamaan sekä yrityksesi haavoittuvimman omaisuuden ja että myös sen tulevat hankkeet.

RICOH
imagine. change.

www.ricoh.fi