Aperçu de la sécurité chez Ricoh

RICOH
imagine. change.
imaginer. changer.

Vous vous inquiétez de la vulnérabilité de vos appareils?

Les menaces en matière de cybersécurité ne se limitent plus seulement aux ordinateurs personnels, aux serveurs ou aux réseaux. Les appareils d'impression — y compris les imprimantes laser de base — nécessitent des contre-mesures face à un vaste éventail de menaces. Au fur et à mesure que les imprimantes multifonctions sont devenues de véritables terminaux d'information, elles sont devenues des actifs de TI à part entière. La capacité informatique de la catégorie d'appareils « imprimantes et copieurs » a marqué une forte croissance et les menaces potentielles se sont multipliées parallèlement à celle-ci. Parmi ces menaces, mentionnons :

- L'accès malveillant par l'entremise des réseaux;
- L'espionnage et l'altération des informations contenues sur les réseaux;
- La fuite d'informations à partir d'une unité de stockage possédant un lecteur de disque dur;
- L'accès non autorisé par l'entremise du panneau de commande d'un appareil;
- l'accès inapproprié au moyen de lignes de télécopieurs;
- La fuite d'informations par l'entremise des sorties imprimées;
- et les infractions aux politiques de sécurité causées par l'inadvertance.

Espérer simplement que vous ne serez pas touché n'est pas une solution. Des technologies supérieures, un engagement et un savoir-faire sont essentiels. Ricoh peut vous aider à résoudre les problèmes potentiels causés par la vulnérabilité de vos appareils, des données qu'ils traitent et des réseaux auxquels ils se connectent.

La sécurité des données fait partie de notre ADN

Les imprimantes et les copieurs de Ricoh sont conçus, fabriqués et installés avec la sécurité des données comme exigence de base. La sécurité est une préoccupation première dès le départ dans tous les domaines, de la conception du produit à sa mise en vente. C'est dans notre ADN — nous tenons à informer nos clients à la fois de notre philosophie de conception et de notre engagement à travailler continuellement en vue d'appuyer nos clients avec des solutions au fur et à mesure que les menaces évoluent.

Sécurité des appareils

Nos capacités en matière de sécurité des appareils peuvent aider à protéger les appareils multifonctions et les imprimantes laser contre les menaces potentielles, y compris toute menace contre les micrologiciels, les disques durs des appareils, la mémoire non volatile, les ports réseau ouverts et les systèmes d'authentification. Ricoh a obtenu des certifications fondées sur les « critères communs » (ISO/IEC 15408) pour une vaste gamme de ses produits. Les fonctions de sécurité des appareils en voie d'obtenir la certification « critères communs » sont testées par des laboratoires indépendants agréés par le gouvernement afin de s'assurer que les fonctionnalités de sécurité fonctionnent correctement et sont conformes aux normes établies par le gouvernement et l'industrie.

Dans le cadre de notre engagement continu à empêcher que vos informations importantes soient exposées à des menaces, nous développons et offrons des fonctions de sécurité et des produits visant la protection de vos documents électroniques et papier — sans entraver l'utilisation et la productivité.

Les micrologiciels non sécurisés peuvent être compromis

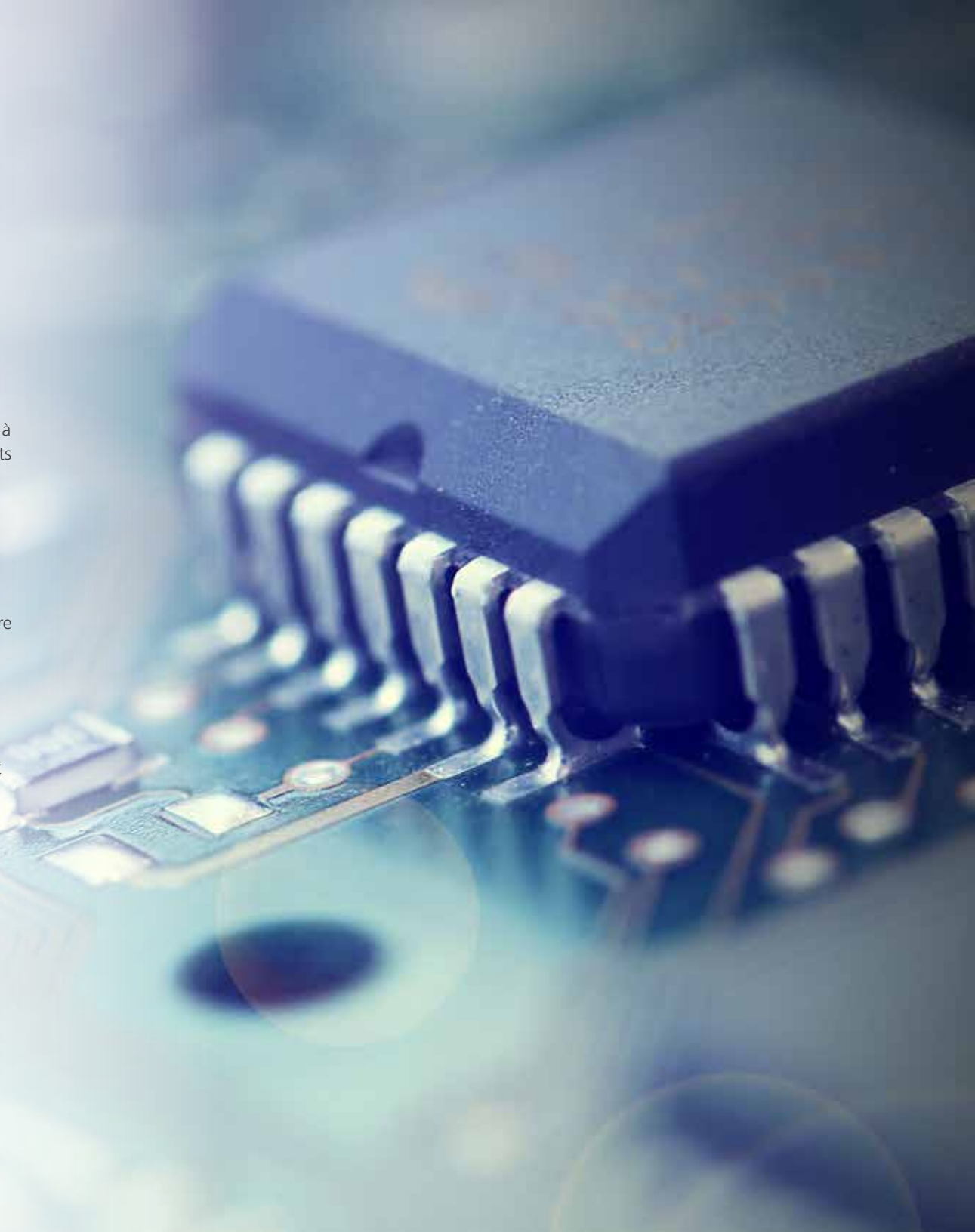
Signature numérique des mises à jour des micrologiciels

Si le logiciel intégré d'une MFP ou d'une imprimante traditionnelle — également connu sous le nom de micrologiciel — est modifié ou compromis, celui-ci peut alors être utilisé comme méthode d'intrusion dans le réseau de l'entreprise, servir de moyen pour endommager l'appareil ou constituer une plate-forme ouvrant la porte à d'autres fins malveillantes. Les appareils conçus par Ricoh sont construits à l'aide d'un module de plate-forme sécurisée (TPM) et sont conçus pour ne pas démarrer si un micrologiciel a été compromis. Le TPM de Ricoh est un module de sécurité matérielle qui valide les logiciels de base du contrôleur, le système d'exploitation, le BIOS, le chargeur de démarrage et les applications de micrologiciels.

Les MFP et les imprimantes de Ricoh utilisent la technologie de signature numérique afin de juger de la validité du micrologiciel. La clé publique utilisée pour cette vérification est stockée dans une région non volatile et protégée contre l'écrasement de la plate-forme TPM. Une clé de cryptage racine et des fonctions cryptographiques sont également contenues dans le TPM et ne peuvent pas être modifiées de l'extérieur. Ricoh utilise la procédure d'amorçage validé (Trusted Boot) comprenant deux méthodes de vérification de la validité des logiciels/micrologiciels :

1. Détection des altérations
2. Validation des signatures numériques

Les appareils Ricoh ne démarreront pas de logiciels/micrologiciels avant d'avoir obtenu la confirmation que ceux-ci sont authentiques et sûrs pour les utilisateurs.



La vulnérabilité des données éphémères

Système de sécurité par écrasement des données (DOSS)

Lorsqu'un document est numérisé ou lorsque des informations sont reçues à partir d'un ordinateur, certaines données peuvent être temporairement stockées sur le disque dur ou le périphérique de mémoire de l'appareil. Cela peut inclure la numérisation, l'impression et la copie des fichiers d'image, les données saisies par l'utilisateur et les configurations. Ces données temporaires — ou « latentes » — représentent une brèche potentielle de la sécurité.

Le système de sécurité par écrasement des données (DOSS) de Ricoh referme cette brèche de sécurité en détruisant les données temporaires stockées sur le disque dur du MFP en les écrasant avec des séquences aléatoires de « 1 » et de « 0 ». Les données temporaires sont activement écrasées et ainsi effacées à chaque fois qu'une nouvelle tâche est exécutée. La solution de Ricoh :

- Respecte les recommandations de la National Security Agency (NSA) et du ministère de la Défense en matière de traitement d'informations classifiées;
- Rend virtuellement impossible l'accès aux données latentes des tâches de copie, d'impression, de numérisation et de télécopie une fois que le processus d'écrasement est terminé (le processus d'écrasement peut être réalisé entre 1 et 9 fois);
- Fonctionne avec le système de sécurité de disque dur amovible (RDH) de Ricoh, fournissant une approche à plusieurs échelons;
- Facilite le respect des exigences de la LPRPS et de la LAIPVP pour les clients;
- Fournis une rétroaction visuelle relativement au processus d'écrasement (c.-à-d. processus terminé, processus en cours) à l'aide d'un simple icône.

Le cryptage permet de protéger contre le vol de données

Cryptage du disque dur

Même si le disque dur est physiquement retiré d'un appareil Ricoh, les données cryptées ne peuvent pas être lues. La fonction de cryptage du disque dur peut aider à protéger le disque dur d'une imprimante multifonction contre le vol de données tout en aidant les entreprises à se conformer aux politiques de sécurité en vigueur. Le cryptage comprend les données stockées dans le carnet d'adresses d'un système, ce qui réduit le risque que les employés, les clients ou les fournisseurs d'une organisation voient leurs informations détournées et potentiellement ciblées. Voici les autres types de données (qui sont stockées dans la mémoire non volatile ou sur le disque dur des imprimantes multifonctions) pouvant être cryptées :

- Carnet d'adresses
- Données sur l'authentification des utilisateurs
- Documents stockés
- Fichiers éphémères
- Registres
- Configurations de l'interface réseau
- Informations sur les configurations

La fonction de cryptage de Ricoh utilise la méthode de chiffrement avancé standard (AES) de 256 bits.

La ligne de votre télécopieur constitue-t-elle une brèche de sécurité?

Ligne de télécopie sécurisée

L'activation de la fonction de télécopie d'un appareil peut exiger de le connecter via une ligne téléphonique, ce qui signifie qu'il est essentiel de bloquer l'accès non autorisé potentiel via la ligne de télécopie. Le logiciel intégré Ricoh est conçu pour ne traiter que les types de données appropriées (c'est-à-dire les données de relatives aux télécopies) et envoyer ces données directement aux fonctions appropriées de l'appareil. Étant donné que seules les données de télécopie peuvent être reçues à partir de la ligne téléphonique, le risque d'accès non autorisé à partir de la ligne, du réseau ou des logiciels intégrés de l'appareil est éliminé.

Ricoh utilise diverses fonctions visant à assurer la sécurité des télécopieurs :

- Un contrôleur de télécopie à un seul modem assure que toutes les communications passées par le protocole de télécopie G3.
- Les données d'images ne sont pas enregistrées dans la mémoire de page du contrôleur ou dans la mémoire de stockage temporaire, ce qui rend impossible l'accès aux données à partir du contrôleur.
- Les données stockées dans la mémoire de page du contrôleur et la mémoire temporaire sont uniquement envoyées à l'unité d'impression.
- Il n'y a pas de connexion active entre les buses d'impression/de numérisation vidéo et le contrôleur du système, faisant en sorte qu'il est impossible d'accéder aux données stockées dans la mémoire de page du contrôleur du système ou dans la mémoire temporaire du contrôleur du télécopieur.
- Les données d'emplacement de page sont effacées après chaque tâche.

Certification de sécurité indépendante

IEEE 2600

La norme de sécurité IEEE 2600 définit les exigences minimales des fonctions de sécurité utilisées par les appareils qui exigent un niveau élevé de sécurité des documents ce qui permet d'établir une base de référence commune relativement aux attentes en matière de sécurité pour les MFP et les imprimantes. Afin de s'assurer qu'un appareil est conforme à la norme établie, un laboratoire indépendant effectue des essais en laboratoire et vérifie les fonctions de sécurité du fabricant.

Les aspects suivants, qui ont été identifiés comme représentant le plus grand risque en matière de brèche de sécurité des données, sont certifiés dans plusieurs des appareils Ricoh conformément à la norme IEEE 2600 et peuvent être activés :

- Systèmes d'identification et d'authentification des utilisateurs
- Technologies de cryptage des données compatibles avec les imprimantes multifonctions (MFP)
- Fonction de validation des micrologiciels du système
- Séparation de la ligne de télécopie analogue et du contrôleur de copie, d'impression et de numérisation
- Validation des algorithmes de cryptage des données
- Sécurité des opérations par écrasement de données

Ricoh offre une vaste gamme de MFP et d'imprimantes certifiés conformément à la norme de sécurité IEEE 2600. De plus, notre gamme de produits est constamment améliorée afin de répondre aux besoins changeants de notre clientèle.

Contrôler l’accès afin de réduire les risques

Authentification des utilisateurs aux appareils

Les fonctions d’authentification permettent aux utilisateurs autorisés d’accéder aux imprimantes multifonctions de Ricoh, tout en restreignant l’accès à ceux qui n’entrent pas les informations d’identification appropriées. Ricoh vous donne également la possibilité de contrôler les niveaux d’autorisation accordés à chaque utilisateur ou groupe d’utilisateurs. Il peut s’agir de restreindre la possibilité de modifier les paramètres de l’appareil et de visualiser les entrées du carnet d’adresses ou de donner accès à des flux de travaux de numérisation, à des serveurs de documents et à d’autres fonctions. De plus, la fonction de verrouillage des utilisateurs, qui se déclenche en cas de la détection d’une fréquence élevée de tentatives de connexion réussies ou échouées, aide à se prémunir contre les attaques par déni de service et les perçages de mots de passe par force.

Parmi les différentes méthodes d’authentification, mentionnons :

- Authentification de base — les utilisateurs doivent entrer un nom d’utilisateur et un mot de passe, lesquels sont enregistrés dans le carnet d’adresse de l’imprimante multifonction.
- Authentification par code d’utilisateur — les utilisateurs doivent entrer un code pouvant aller jusqu’à huit chiffres, lequel est comparé aux données contenu dans le carnet d’adresses.
- Authentification Windows/LDAP — l’accès aux imprimantes multifonctions de Ricoh peut être lié aux contrôleurs de domaines Windows® et aux serveurs LDAP.
- Authentification par carte — plutôt que d’entrer un nom d’utilisateur et un mot de passe, les utilisateurs doivent tenir une carte enregistrée pendant quelques secondes au-dessus d’un lecteur de carte optionnel.

Sécurité des données

Les fuites d'informations peuvent se produire plus facilement qu'on le pense. Un document laissé dans le bac de sortie d'une imprimante multifonction peut constituer un risque pour la sécurité au même titre que le détournement d'un fichier ou d'une erreur humaine. Les appareils multifonctions de Ricoh utilisent des algorithmes validés au moyen du programme de validation des algorithmes cryptographiques pour la plupart des fonctions de cryptage de nos produits. De plus, tous les appareils ont obtenu la certification « critères communs » (CC) sous certaines conditions. Veuillez consulter les produits certifiés CC sur notre site Web.

174 million

d'archives numériques ont été compromises par des intrusions en 2011 – il s'agit d'une hausse de 4 000 % par rapport à 2010*.

* Rapport d'enquête sur les violations de données de Verizon® de 2012

Ricoh protège vos données grâce à des technologies et à des fonctions conçues en vue d'appuyer les politiques de sécurité, prévenir l'utilisation malveillante et les erreurs d'inadvertance, ainsi que faciliter la conformité par l'entremise de la comptabilité.

Protection des documents numérisés

Solutions de numérisation sécurisées

Le processus de numérisation des documents papier et d'acheminement des fichiers électroniques qui en résultent, qu'il s'agisse de systèmes d'arrérages ou de courrier électronique, peut constituer un risque de compromis des données s'il n'est pas correctement sécurisé. Les processus de numérisation, bien que conçus afin d'être faciles pour les utilisateurs, devraient également offrir une protection robuste pour l'information numérique acheminée. Cela commence par la restriction de l'accès. Limiter les opérations d'analyse aux utilisateurs autorisés grâce à plusieurs options d'authentification, dont la connexion réseau, l'authentification Kerberos en option ou l'authentification unique par carte.

Le cryptage des communications de type numérisation vers courrier électronique aide à réduire les risques de compromis de l'information. Envoyez des messages électroniques en utilisant la cryptographie par clé publique et un certificat de vérification de l'utilisateur préalablement enregistré dans le carnet d'adresses de l'appareil de numérisation. Prévenez également l'usurpation et l'altération des messages en joignant une signature électronique utilisant une clé secrète fondée sur le certificat d'un appareil.

Les imprimantes multifonctions, les copieurs et les numériseurs de Ricoh sont équipés des protocoles SSL (Secure Sockets Layer) et TLS (Transport Layer Security) et peuvent utiliser des algorithmes de cryptage puissants (256 bits AES et SHA-2) ainsi que des pistes de vérification et un contrôle administratif.

Les impressions non récupérées peuvent constituer un risque de fuites d'informations

Impression verrouillée

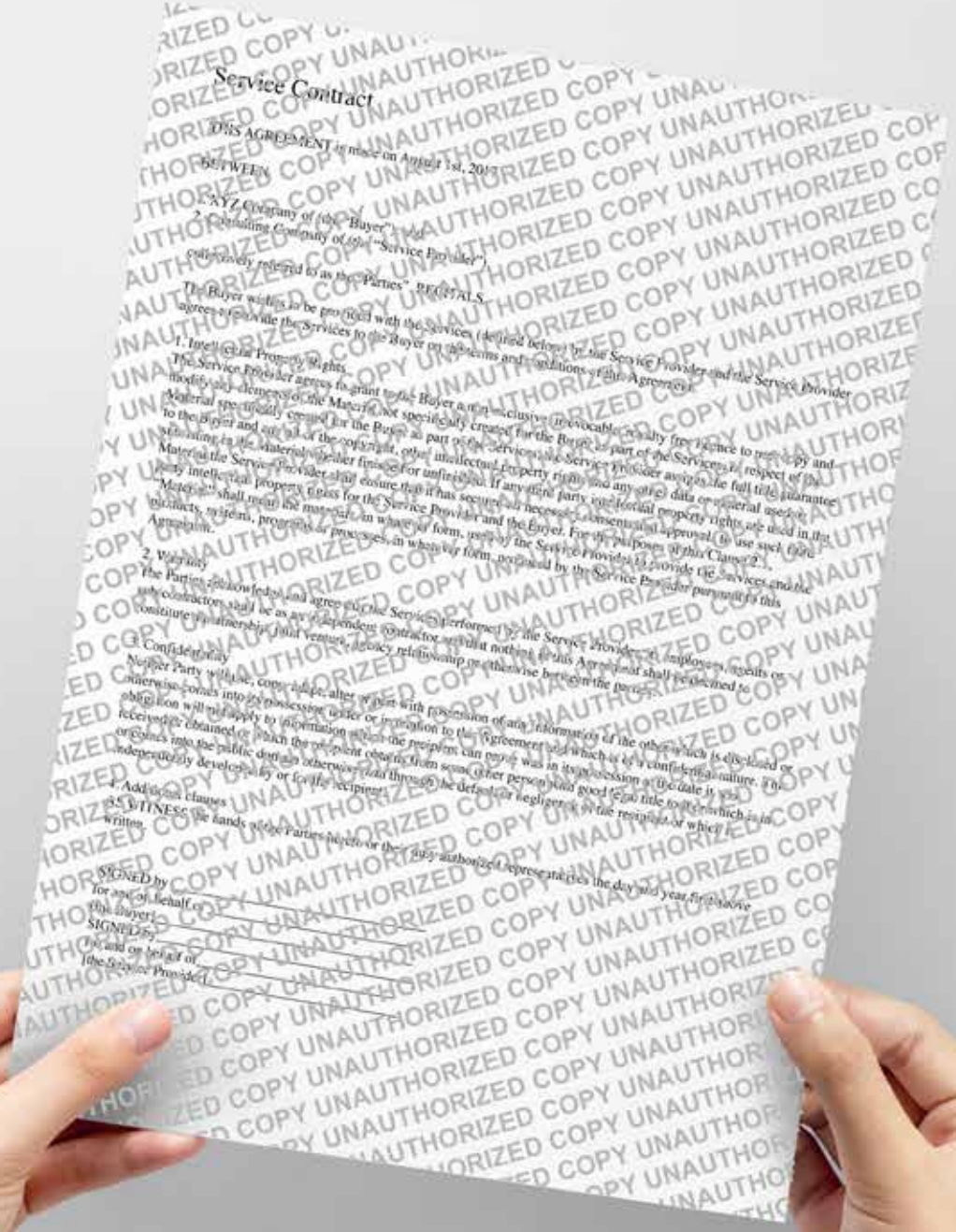
Les documents imprimés laissés sur les bacs de sortie ou oubliés peuvent être récupérés par n'importe qui. Cela constitue un risque relativement à la sécurité de l'information, d'autant plus lors de l'impression de documents confidentiels. Les capacités d'impression verrouillée de Ricoh permettent de retenir les documents cryptés sur le disque dur de l'appareil jusqu'à ce qui l'utilisateur se présente devant l'appareil et entre le bon numéro d'identification personnel. En plus de cette fonction d'impression verrouillée de base, Ricoh offre aussi l'option d'impression verrouillée avancée, une fonction de sécurité liée aux comptes d'utilisateurs et pouvant être jumelée avec la technologie d'authentification par carte. Pour encore plus de capacités, des logiciels comme Streamline NX de Ricoh (illustré) peuvent assurer de documents entièrement sécurisé en offrant aux utilisateurs des options relativement aux flux d'impressions tout en conférant un certain contrôle à l'administrateur.

Protection contre les copies non autorisées

Copy data security

Ricoh offre des fonctions visant à empêcher les copies non autorisées de documents papier afin de contribuer à prévenir les fuites d'informations. Cette fonction de copie protégée permet d'imprimer et de copier des documents avec des masques invisibles spéciaux intégrés au fond. Si le document imprimé ou copié tente d'être photocopié de nouveau, le masque intégré deviendra visible sur les copies.

La fonction de contrôle de copie non autorisée protège de deux façons. L'option « Masque pour copie » intègre un motif de masquage et un message à l'intérieur de l'impression originale. Si des copies non autorisées sont faites, le message intégré apparaît sur la copie. Il peut s'agir du nom de l'auteur du document ou d'un message d'avertissement. L'option « Sécurité des données de copie » aide à protéger l'information elle-même. Lorsque l'appareil Ricoh détecte le motif de masquage, les données imprimées sont masquées par une boîte grise qui couvre toute la page sur laquelle le motif de masquage est détecté, à l'exception d'une marge de 4 mm de chaque côté.



Les documents anonymes sont difficiles à contrôler

Impression obligatoire des renseignements sur la sécurité

Identifiez les documents avec des informations clés pour une responsabilisation et un contrôle sur la gestion accrus. La fonction d'impression obligatoire des renseignements sur la sécurité intègre obligatoirement des renseignements sur le document imprimé, dont le nom de la personne ayant imprimé le document, à quel moment et à partir de quel appareil. Cette fonctionnalité peut être configurée pour les copies, les impressions, les télécopies et les fonctions de serveur de documents. Les administrateurs peuvent choisir à quel endroit les informations obligatoires seront imprimées et quels types de renseignements seront inclus. Ces renseignements peuvent comprendre :

- La date et l'heure de l'impression
- Le nom ou le code d'utilisateur de la personne ayant imprimé le document
- L'adresse IP et/ou le numéro de série de l'appareil utilisé

Éviter l’usage à mauvais escient des appareils

Comptabilité et récupération des coûts

L’utilisation non contrôlée de l’équipement d’imagerie peut engendrer des dépenses inattendues et la violation de politiques d’entreprise. Le logiciel de comptabilité et de récupération des coûts de Ricoh assure le suivi de l’utilisation et automatise le processus de réattribution des coûts aux utilisateurs ou aux services. Améliorez la comptabilité de votre entreprise grâce à l’établissement de quotas d’utilisation et de limites budgétaires par compte. Établissez des permissions afin de restreindre l’accès à certaines fonctions selon le besoin (p. ex. capacité d’impression couleur). Le contrôle de l’utilisation de l’équipement par authentification des utilisateurs et la restriction des permissions réduit les risques d’utilisation à mauvais escient.

Sécurité réseau

Les imprimantes multifonctions échangent des informations importantes avec les ordinateurs et les serveurs sur les réseaux. Si elles ne sont pas protégées, ces informations risquent d'être altérées par ceux qui se connecteraient au réseau en vue d'en faire un usage malveillant. Les produits et les technologies de Ricoh offrent des caractéristiques qui peuvent aider à protéger contre les accès non autorisés via les réseaux. Les techniques employées comprennent le cryptage des communications réseau et des flux d'impression, l'authentification des utilisateurs du réseau et une foule de contre-mesures administratives, comme la fermeture des ports réseau et la gestion proactive des appareils.

Les fonctions de sécurité de Ricoh peuvent aider à réduire les risques d'exploitation des réseaux et de fuites d'informations causés par des brèches de sécurité relativement aux appareils et aux imprimantes multifonctions.

Les utilisateurs non autorisés peuvent constituer une menace

Authentification des utilisateurs réseau

Les appareils Ricoh permettent l'authentification des utilisateurs réseau afin de restreindre l'accès aux utilisateurs non autorisés. Par exemple, la fonction d'authentification Windows® vérifie l'identité de l'utilisateur à partir de l'appareil multifonction grâce à la comparaison des identifiants (nom d'utilisateur et mot de passe) avec les informations sur les utilisateurs non autorisés contenues dans la base de données du serveur réseau Windows. Pour ce qui est de l'accès au carnet d'adresses principal, l'authentification LDAP valide l'identité de l'utilisateur selon le serveur LDAP (Light-weight Directory Access Protocol), ce qui permet d'assurer que seuls les utilisateurs ayant un nom d'utilisateur et un mot de passe valide puissent avoir accès aux adresses courriel contenues sur le serveur LDAP.

Les logiciels comme Streamline NX de Ricoh, une suite modulaire prenant en charge les processus de numérisation, de télécopie, d'impression, de gestion des appareils, de sécurité et de comptabilité, fournissent des options d'authentification supplémentaires. Il s'agit notamment de l'authentification LDAP, Kerberos et SDK avec possibilité d'intégrations personnalisées.

Des appareils « invisibles » de l’extérieur

Fermeture des ports réseau inutilisés

En vue de faciliter l’ajout d’appareils réseau, les systèmes réseau de nombreux fournisseurs sont régulièrement expédiés au client avec tous les ports réglés sur « ouvert ». Toutefois, les ports ouverts non utilisés sur les imprimantes et les MFP posent un risque de sécurité. Les ports compromis peuvent mener à diverses menaces extérieures, y compris la destruction ou la falsification des données stockées, les attaques par déni de service (DoS) et les virus ou les logiciels malveillants entrant sur le réseau. Il existe une solution simple, quoique souvent négligée, en ce qui concerne cette source de risque particulière : fermer les ports. Les administrateurs des appareils Ricoh peuvent facilement verrouiller les ports réseau inutilisés, ce qui rend les appareils virtuellement « invisibles » au piratage. De plus, des protocoles spécifiques, tels que SNMP ou FTP, peuvent être complètement désactivés afin d’éviter qu’ils ne soient exploités.

La vulnérabilité des données non cryptées sur le réseau

Cryptage des réseaux

Il est possible pour un pirate informatique connaisseur d'intercepter des trains de données brutes, des fichiers et des mots de passe lorsque les données circulent au sein du réseau. Sans la protection adéquate, les informations intelligibles peuvent être volées, altérées, falsifiées et réintégrées dans le réseau à des fins malveillantes. Ricoh utilise des protocoles de sécurité réseau robustes qui peuvent être configurés en fonction des besoins du client. Le protocole de sécurité de la couche de transport (TLS) est utilisé afin de maintenir l'intégrité des données transmises d'un point à l'autre.

Les appareils Ricoh prennent en charge WPA2, WPA2-PSK avec cryptage AES (accès sans fil protégé), un système de cryptage de données pour les réseaux sans fil offrant une meilleure protection que le système de cryptage WEP (Wired Equivalent Privacy). Le système WPA2, WPA2-PSK comprend une fonction d'authentification et le protocole de cryptage CCMP (AES), qui met automatique à jour les clés de cryptage à des intervalles prédéfinis.

Empêcher l'exploitation des données envoyées aux imprimantes

Cryptage des flux d'impression

Les données envoyées dans un flux d'impression peuvent être exploitées si elles ne sont pas cryptées et être interceptées en cours de route. Ricoh peut permettre le cryptage des données d'impression au moyen des protocoles de cryptage SSL et TLS via le protocole d'impression Internet (IPP), ce qui sécurise les données entre les postes de travail et les imprimantes et appareils multifonctions du réseau. Ceci peut être accompli en utilisant IPP sur SSL/TLS. Comme il s'agit d'un protocole qui aide à maintenir l'intégrité des données, une personne tentant d'intercepter les flux de données d'impression cryptées en transit n'obtiendrait que des données indéchiffrables.

La gestion des appareils peut exiger beaucoup de temps

Device Manager NX

Comme la gestion des appareils peut prendre beaucoup de temps, des failles de sécurité peuvent apparaître involontairement lorsque des aspects essentiels de la gestion des appareils ne sont pas adéquatement surveillés. Les logiciels de gestion des appareils de Ricoh, tels que Device Manager NX et Streamline NX, offrent aux directeurs des TI un point de contrôle central pour surveiller et gérer un nombre pratiquement illimité d'appareils d'impression connectés à un réseau, peu importe si ceux-ci sont répartis sur plusieurs serveurs ou dans diverses régions géographiques. Les communications cryptées SNMPv3 assurent la surveillance de l'état de fonctionnement des appareils et de leurs services, tout en incorporant des fonctions d'authentification des utilisateurs et de cryptage des données qui aident à protéger les données et les informations sur les appareils réseau.

Grâce au contrôle centralisé, les administrateurs peuvent déterminer qui peut accéder et utiliser un appareil ou une imprimante multifonction, surveiller les paramètres de la solution de sécurité par écrasement des données (DOSS) et gérer les certificats des appareils. Les tâches automatisées peuvent également réduire l'exposition potentielle des micrologiciels obsolètes. Les micrologiciels des appareils Ricoh sont comparés aux versions des micrologiciels approuvées par le client ou au dernier micrologiciel disponible pour l'appareil auprès du Global Software Center de Ricoh. Si le micrologiciel qui tente d'être lancé est différent de celui-ci, le micrologiciel correct sera déployé automatiquement.

Permettre aux fournisseurs de services de répondre rapidement à l'appel

@Remote

Le connecteur NX @Remote de Ricoh collecte les alertes de services imminentes et les transmet directement à votre fournisseur de services à l'aide d'une méthode sécuritaire. Votre fournisseur est donc en mesure de planifier les mises à jour des micrologiciels à distance et d'utiliser le connecteur afin de les mettre en œuvre immédiatement. Le connecteur @Remote collecte aussi les lectures de l'appareil et les rend disponibles selon un horaire préétabli, de pair avec les alertes de niveaux de consommables, afin de maintenir le temps de fonctionnement et de diminuer le fardeau administratif.

Programmes et ressources

Les organisations qui traitent ou entreposent des renseignements médicaux, financiers ou personnels, ou tout autre type de données confidentielles peuvent être assujetties à diverses exigences réglementaires, comme la Loi sur la protection des renseignements personnels sur la santé (LPRPS) et la Loi sur l'accès à l'information et la protection de la vie privée (LAIPVP). Que votre organisation doive se conformer à des exigences externes ou démontrer l'efficacité de ses propres politiques de sécurité, Ricoh peut vous aider à y parvenir. Nous fournissons des programmes et des ressources à nos clients qui visent à les aider à respecter les exigences spécifiques qui s'appliquent à leur entreprise.

Chez Ricoh, nous appuyons nos clients en leur fournissant l'assistance technique, les connaissances, la formation et la documentation relative à la sécurité dont ils ont besoin relativement à notre équipement. De plus, nous offrons aussi le service d'effacement de toutes les données contenues sur les appareils en fin de vie.

Soutien technique à l'échelle nationale et internationale

Ricoh a mis en place des centres de technologies dans chaque région afin de fournir du soutien technique et de répondre rapidement et efficacement aux besoins de ses clients partout à travers le monde. L'équipe des services mondiaux de Ricoh fournit des solutions uniformes, normalisées et complètes. Couvrant approximativement 200 pays et territoires autour du globe, Ricoh emploie plus de 30 000 spécialistes de la prestation de service. Notre réseau de partenaires détaillants de vente et de soutien se démarque par sa capacité de servir 95 % des employés des entreprises dans le Fortune Global 500, ce qui signifie que vous pouvez compter sur un seul partenaire pour l'ensemble de vos besoins. Grâce à nos bureaux et à nos professionnels de la prestation de service situés dans un si grand nombre de pays, nous sommes en mesure de répondre rapidement aux demandes des clients, peu importe leur emplacement.

Documentation d'appui sur la sécurité

Ricoh fournit de la documentation technique afin d'appuyer ses clients relativement aux exigences de sécurité en matière de l'information, notamment les documents sur les certifications IEEE 2600 et ISO 15408 pour certains produits offerts. Cette documentation comprend la validation d'un tiers relativement aux réclamations en matière de sécurité et peut être fournie sur demande. De plus, un livre blanc sur la sécurité relativement aux appareils et aux réseaux ainsi que des guides sur l'installation sécuritaire des appareils sont disponibles pour les clients. Ces guides fournissent des informations détaillées sur la manière dont l'équipement de Ricoh transmet les données de l'appareil et dans quelle mesure celui-ci interagit-il avec le réseau.

Formation des administrateurs et des utilisateurs

Maintenir un niveau de vigilance élevé et adhérer à des pratiques exemplaires en matière de sécurité impliquent bien plus que la simple technologie — cela concerne aussi les gens. Ricoh offre des formations à l'intention des administrateurs comme des utilisateurs directs. Équipés des bonnes connaissances, les membres de votre personnel seront en mesure de comprendre les capacités de sécurité à leur disposition et apprendre comment en faire un usage approprié afin de contribuer à protéger les informations de votre organisation et à respecter les politiques en vigueur.

Faites confiance à Ricoh pour faire face à vos plus grands défis en matière de sécurité

Perte/vol de données

Les risques de perte de données sont une des préoccupations premières des dirigeants de niveau C et maintenir la confidentialité et la sécurité des informations est un combat constant. Les cybercriminels sont toujours à la recherche d'une faille dans votre armure qu'il serait possible d'exploiter. L'équipement d'imagerie de Ricoh peut constituer un élément clé en matière de prévention de la perte de données.

Corruption/altération de données

Les attaques par virus faisant de plus en plus les têtes d'affiches démontrent à quel point l'ensemble des organisations sont vulnérables aux cybercriminels. Les logiciels malveillants, les virus, les chevaux de Troie et les vers informatiques s'attaquent à de vastes plates-formes comprenant des vulnérabilités. Les plates-formes de Ricoh, bien qu'elles soient très répandues, utilisent des systèmes d'exploitation exclusifs afin de se prémunir contre les tentatives de piratage.

Accessibilité des données

L'accessibilité des informations et des données est un concept multifacette exigeant à la fois d'assurer et de restreindre l'accès. Les produits de Ricoh répondent parfaitement aux deux exigences en accélérant les échanges sanctionnés d'informations par l'entremise de l'impression, de la copie, de la numérisation et du routage, en assurant un contrôle sur ces processus, en cryptant les données en transit et en contrôlant qui sont les utilisateurs autorisés à récupérer l'information traitée par l'équipement.

Comprendre la réglementation

Les organisations sont tenues de se conformer à diverses réglementations internationales, nationales et industrielles, sans compter les politiques de sécurité obligatoires propres à chaque entreprise et aux exigences en matière de vérification. Ricoh fournit les outils et l'expertise afin de soutenir ses clients en ce qui concerne leurs besoins relatifs à la sécurité.

Assurer la conformité

Les pénalités en cas de non-conformité peuvent coûter cher et les nouveaux règlements lèvent la barre en matière d'incidence potentielle sur les entreprises. Avoir la documentation appropriée à portée de la main est un élément essentiel afin de démontrer la conformité de votre organisation. La certification IEEE 2600 procure la validation d'un tiers relativement au fait que les déclarations de sécurité des TI fonctionnent comme indiqué. Ricoh peut vous fournir cette certification, en plus d'autre documentation, afin d'appuyer vos clients.

Faites appel l'expertise technique de Ricoh

Les clients sont à la recherche d'organisations auxquelles ils peuvent faire confiance et qui peuvent les aider à assurer la sécurité de leurs informations ainsi que leur conformité. Ricoh s'engage à fournir à ses clients des technologies, des services, des logiciels et des ressources de pointe et à les aider à respecter les exigences applicables en matière de sécurité. Pour toute question ou pour obtenir davantage d'information, communiquez avec votre professionnel de la vente Ricoh ou visitez notre site Web.

Apprenez-en davantage au **www.ricoh.ca**

RICOH
imagine. change.
imaginer. changer.

Ricoh Canada Inc., 100-5560 Explorer Drive, Mississauga, ON L4W 5M3, 1-888-742-6417
Ricoh® et le logo Ricoh sont des marques de commerce enregistrées de Ricoh Company, Ltd. Toutes les autres marques de commerce sont la propriété de leur propriétaire respectif ©2017 Ricoh Canada Inc. Tous droits réservés. Le contenu de ce document, de même que l'apparence, les fonctions et les caractéristiques des produits de Ricoh peuvent changer de temps à autre sans préavis. Les produits illustrés comportent des options. Même après avoir pris toutes les précautions possibles pour assurer l'exactitude de l'information, Ricoh ne fait aucune déclaration ni ne garantit l'exactitude de l'information contenue dans le présent document et n'accepte aucune responsabilité à l'égard de toute erreur ou omission dans ledit texte. Les résultats réels peuvent varier selon l'utilisation faite des produits et des services, ainsi que les conditions et les facteurs pouvant affecter la performance. Les seules garanties relatives aux produits et services de Ricoh sont exposées dans les énoncés de garantie formelle s'y rattachant.