RICOH
imagine. change.

حلول الأمان من Ricoh

نساعدك في حماية أعمالك

إن الأمن السيبراني هو أكبر تهديد لبقاء الشركات الحديثة ونجاحها. فتتعرض الشركات من جميع الأحجام بصورة مستمرة لخطر الوقوع ضحية للهجمات التخريبية، مثل هجمات التصيد الاحتيالي أو حجب الخدمة الموزع (DDoS) أو فيروسات الفدية. فالتكلفة الحقيقية جراء هذه الهجمات تقدر بالملايين ففي عام 2017، وجد معهد بونيمون (Ponemon Institute) إن متوسط التكلفة العالمية لاختراق البيانات بلغ 3.62 مليون دولار. ستتضاعف هذه التكلفة في السنوات القادمة؛ كالقوانين الحكومية مثل قانون حماية البيانات العام (GDPR)، تنص على معاقبة الشركات بفرض غرامات مالية ضخمة في حالة فشلها في تأمين أنظمتها وبياناتها بصورة مناسبة. ولتجنب هذه العقوبات المنهكة، يجب أن تكون الشركات قادرة على إظهار قدرتها على حماية بياناتها.
يتطلب هذا الأمر نظرة شاملة على جميع الثغرات في جميع أقسام المؤسسة.

وتزداد تحديات الأمن السيبراني التي تواجه الشركات تعقيدًا نتيجة التوسع والتحول الرقمي في أماكن العمل الحديثة، فضلاً عن الزيادة الهائلة في أحجام البيانات. كثيرًا ما تنتشر مهام سير العمل عبر الأجهزة والشبكات والمناطق الجغرافية. وفي الغالب تتعرض المعلومات للخطر أثناء نقلها من مكان لآخر بالشركة. لذا يجب أن تظل محمية في كل مرحلة من مراحل رحلتها. بالنظر إلى المخاطر الأمنية الناجمة عن ذلك، لا شك أن الشركات الحديثة لا تستطيع مزاولة نشاطها دون تأمين أنظمة إدارة المستندات والبيانات في الأساس. وفي الوقت نفسه، تزايدت إمكانات الطابعات المكتبية والأجهزة المتعددة الوظائف بمقدار عشرة أضعاف في السنوات الأخيرة. إذ تُستَخدم الآن في إجراء عمليات إدخال بيانات الشركات وإخراجها ونقلها وتخزينها على نطاق واسع. وهذا ما يجعلها واحدة من أخطر التهديدات في أماكن العمل اليوم. إلا أنه لا يُلتفت إليها في الغالب.

ورغم انتشار الكثير من الشركات التي تزعم أن لديها إمكانات أمنية، فقد تميزت Ricoh بتطوير الحلول والخدمات الأمنية المستخدمة في أماكن العمل منذ عقود طويلة. فعلى سبيل المثال، اشتملت طابعاتنا على إمكانات الكتابة الآمنة فوق البيانات على القرص الثابت منذ أكثر من 20 عامًا.

لا شك أن الأمان هو السمة الرئيسية التي تميز حافظة منتجاتنا الرقمية بالكامل الخاصة بأماكن العمل. واليوم لدينا أكثر من 4 ملايين منتج في مجال الأعمال المكتبية. وينبغي العلم بأن كل منتج من هذه المنتجات وكل خدمة ننشرها تشتمل معها على إمكانات أمان مضمنة. كما أننا نستخدم نظام تشغيل خاصًا بشركة Ricoh فقط في كثير من منتجاتنا. ويعد ذلك النظام مكونًا هامًا في برامج الحماية الأمنية التي نطورها؛ ما يوفر السيطرة والبعد عن التهديدات الخاصة بأنظمة تشغيل معينة والتي تستهدف أنظمة التشغيل الأوسع انتشارًا.

توفر Ricoh خدمة متسقة وبنية دعم موحدة على مستوى العالم للعملاء الذين يحرصون على مشاركة معلومات التهديدات بفاعلية واتخاذ الإجراءات بناءً عليها. فنحن في شركة Ricoh لا نطبق شهادة IEEE 2600 كمعيار في جميع أجهزة الطباعة الخاصة بنا فحسب، بل تعد شركتنا عضوًا أساسيًا ومؤلفًا مهمًا في جمعية معايير IEEE. كما حصلت Ricoh أيضًا على شهادة الأيزو ISO 27001، وتتعهد بمواصلة الالتزام بنظام إدارة أمان المعلومات هذا. وهكذا نحرص دائمًا على أن تركز عملية تطوير منتجاتنا على تلبية احتياجات الأعمال ومعالجة المخاوف الأمنية لدى العملاء من خلال سلسلة من البرامج العالمية المبتكرة الموجهة للعملاء.

لتلبية المتطلبات المتزايدة لأفضل ممارسات الأمن السيبراني الفعالة والمثبتة، فإن مبدأ الأمان موجود في كل منتج وخدمة من حافظة منتجات Ricoh من الأساس - وليس فكرة لاحقة تطرأ بعد فوات الأوان. جدير بالذكر أننا نعتقد أن هذه النظرة الشاملة للثغرات الأمنية عنصر أساسي لضمان البقاء في عصر الأعمال الحديثة.

التحديات الأمنية التي تواجه العملاء

الاتجاهات: كلما زادت أحجام البيانات، زادت الثغرات الأمنية والهجمات والخسائر.

تأمين أماكن العمل الرقمية وتزويدها بالإمكانات المناسبة

تسعى شركة Ricoh إلى تمكين العمل الرقمي وتأمينه حيثما كانت هناك مشاركة من الأفراد. وفي الاقتصاد الرقمي الحديث، وهذا يعني إضافة قيمة تتجاوز حدود المكاتب التقليدية في أماكن العمل التي تتعامل مع العملاء مباشرةً. هذا فضلاً عن أن المكاتب البعيدة والعاملين عن بُعد يمنحون الشركات مرونة كبيرة وزيادة في الإنتاجية خلال العمليات اليومية. فهم يساعدون الشركات في تلبية توقعات العملاء ومتطلبات الخدمات بصورة أفضل.

ولكن العمل عبر الشبكات الطرفية يعرض أمان الشركات لبعض المخاطر الكبيرة. لذا يتوجب تأمين البيانات التي ينشئها الموظفون والأجهزة البعيدة التي تُستخدم في التقاط هذه البيانات تأمينًا مناسبًا. وغالبًا ما يعمل الموظفون في شبكات ومناطق جغرافية مختلفة؛ ما يزيد من صعوبة المهمة. لقد كان لإصدار القوانين الحكومية، مثل قانون حماية البيانات العام (GDPR)، آثارًا حاسمة حيث تُلزم الشركات بتقديم إثباتات بتأمين بياناتها خلال دورة حياتها، وإلا واجهت عقوبات رادعة. ومع تطور أماكن العمل وتبنيها لمهام سير العمل الرقمية، فإن دورة حياة بيانات العمل تتزايد في التعقيد شيئًا فشيئًا. سنفحص هذا الأمر الآن، مرحلة تلو الأخرى.

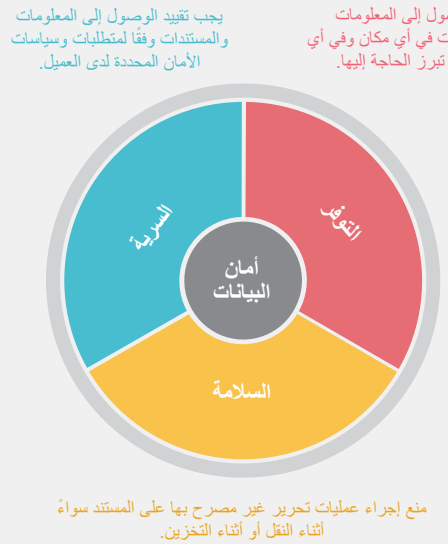
الخطوة الأولى هي أجهزة إدخال البيانات والتقاطها - وهي مكون حيوي في سياسة الدفاع الأمني لدى Ricoh. من هنا، يجب أن تُنقَل البيانات عبر الشبكات وتُخزَّن في أمان تام. ففي هذه المرحلة، من المهم للغاية المحافظة على سلامة البيانات. لذا تقيِّد أنظمة Ricoh صلاحية وصول المستخدمين إلى وظائف الأجهزة والشبكات لضمان عدم العبث بالبيانات أثناء نقلها أو حفظها. تشمل هذه الخدمات التحكم في الوصول والتشفير والحماية من النسخ. ونطلق على هذه المرحلة اسم "الرقابة".

لكن بعد تخزين المستندات يجب أن تكون جاهزة للوصول للمستخدمين الذين يحتاجون إليها في الشركة. لذا فإن القدرة على سحب المعلومات عند الحاجة اليها حاجة إليها وعرضها بطريقة فعّالة تعتمد على حالة توفرها. ومن هنا تبرز أهمية تحليل البيانات الذي يُعد مكونًا حيويًا في مكان العمل الرقمي المزود بالإمكانات المناسبة. فهو يوفر -بكفاءة كبيرة- رؤية ثاقبة لكل قسم في الشركة، من المبيعات حتى الموارد البشرية. علاوة على ذلك، تتيح أدوات البنية الأساسية لمنح التصريحات وصولاً آمنًا سريعًا، بصرف النظر عن موقع المستخدم أو الجهاز المختار. من المهم للغاية ألا تقف بروتوكولات الأمان عقبة أمام إبداع الموظفين أو استخدامهم للوظائف أو دفع المخاطر عنهم. ونحن نطلق على هذه المرحلة اسم "الوقاية".

في النهاية، يجب التخلص من هذه البيانات بطريقة آمنة خاضعة للتدقيق. هذه الخطوة ضرورية من أجل الالتزام بالمتطلبات التنظيمية وتقليل احتمالية تعرض البيانات للسرقة أو الفقد لاحقًا. في الواقع، تحدث هذه العملية خلال دورة حياة المستند مثلما تحدث خلال مرحلة الحذف النهائي له. تجدُر الإشارة إلى أن طباعة أي ملف تترك صورة مخفية على القرص الثابت للطابعات متعددة الوظائف (MFP)؛ لذا تجب الكتابة فوق هذه الصورة لمنع الوصول إليها دون تصريح. تشمل خدمات التخلص من البيانات لدى Ricoh وظائف تطهير بيانات القرص الثابت ومسح الذاكرة وحذف الملفات غير المطبوعة والحذف عند الخروج لمنع المتسللين من تجميع معلومات حساسة من آثار المستند التي يتركها وراءه. ونحن نطلق على هذه المرحلة اسم "إتلاف البيانات".

من أجل تأمين بيانات مكان العمل بفاعلية كبيرة خلال دورة حياتها، تتّبع Ricoh مبادئ "CIA" للخصوصية والأمان: السرية (Confidentiality) والتوفر (Availability) والسلامة (Integrity) هذه هي مبادئنا التوجيهية في تصميم منتجاتنا وحلولنا لاستيفاء المعايير اللازمة والامتثال للقوانين الضرورية. ما من شك أن هذا النهج يتيح الإبداع والنمو في مكان العمل، فضلاً عن المحافظة على أمان العمليات وكفاءتها في الوقت نفسه.

نهج RICOH في تحقيق الأمان



نحن نصمم منتجاتنا بالاستناد إلى مبادئ "CIA" للخصوصية والأمان: السرية (Confidentiality) والتوفر (Availability) والسلامة (Integrity)

أو Ricoh الأمان هو سمتنا الأساسية؛ لذا لا تجد منتجًا صممته خدمة نشرتها تخلو من الميزات والإمكانات الأمنية.

تقدم Ricoh مجموعة متكاملة من منتجات وخدمات الأمان لتأمين عملية إنشاء المستندات من البداية حتى النهاية. والآن سنستعرض كل مرحلة مهمة من المراحل الأربعة على التوالي: الرقابة، والوقاية، وإتلاف البيانات، والدعم.

أربع مراحل لأمان أماكن العمل الرقمية

1 الرقابة

تعد الضوابط الرقابية الفعالة للبيانات مهمة للغاية في المحافظة على سرية البيانات وسلامتها. ويُعزى ذلك إلى أن معلومات العمل من الأصول الأساسية وتجب حمايتها. هذا فضلاً عن أن الأجهزة المستخدمة اليوم عبارة عن محطات طرفية للمعلومات يمكنها أن تصبح بوابات غير حصينة للولوج إلى معلومات العمل من خلالها. ولذلك، تستخدم Ricoh عددًا من أدوات إدارة الأجهزة ومصادقة المستخدمين للتحكم في بيانات العمل وتأمينها. وهي تتعلق بالإعدادات على الأجهزة الفعلية التي تسمح بالوصول إلى وظائف وبيانات معينة كما يمكنها تقييد هذا الوصول. وفي الواقع أن تقييد وصول الموظفين إلى المعلومات التي تنتقل عبر أي طابعة متعددة الوظائف (MFP) بالمكتب يُعد خطوة مهمة في إطار تطبيق أفضل الممارسات المتعلقة بالمحافظة على أمان المستندات. تشمل مرحلة الرقابة أيضًا حماية الأجهزة من البرامج الضارة من خلال نهج Ricoh ثلاثي المستويات في البرنامج الثابت للجهاز.

مراقبة النسخ غير المصرح به

للحماية من محاولات إنشاء نُسَخ غير مصرح بها، تقدم Ricoh حلاً ممتازًا لضمان أمان المستندات الورقية. تقوم وظيفة الحماية من النسخ بطباعة المستندات أو نسخها مع تضمين أنماط خاصة غير مرئية على الخلفية. وفي حالة استخراج نسخة فوتوغرافية من المستند المطبوع أو المنسوخ و/أو مسحه ضوئيًا، تظهر الأنماط المضمنة في النُسَخ. حيث تتيح وحدة الحماية من النسخ غير المصرح به للطابعة متعددة الوظائف (MFP) اكتشاف الأنماط المضمنة واستبدال صورة النسخة الفوتوغرافية بصورة رمادية لمنع تسرب المعلومات. ولهذه الوظيفة فائدة عظيمة عند طباعة المعلومات السرية؛ فحظر نسخ المعلومات السرية يحول دون حدوث هذا النوع من تسرب المعلومات.

تأمين الطباعة

من الممكن تخزين المستند المستلم من جهاز كمبيوتر على محرك الأقراص الثابتة في الطابعة متعددة الوظائف. باستخدام وظيفة تأمين الطباعة من Ricoh، تُحدَد كلمة مرور عندما يرسل المستخدم المستند، ويجب إدخال كلمة المرور هذه في الطابعة متعددة الوظائف قبل أن يُسمَح بطباعة المستند. وبما أن المستند لن يُسمَح بطباعته حتى يصل مالكه للجهاز، فإن وظيفة تأمين الطباعة تضمن بقاء المستند تحت سيطرة مالكه.

أمان الالتقاط المتقدم للبيانات

تقدم حافظة Ricoh لحلول التقاط البيانات المتقدم طبقات متنوعة للتشفير وفك التشفير خلال طبقات المعالجة وعبر مراحل عملية التقاط البيانات. ويمكن للمسؤولين منح صلاحية الوصول إلى قوائم انتظار العمليات باستخدام بيانات فردية لتسجيل دخول المستخدم أو بيانات اعتماد مجمعة. تشمل طبقات الأمان الإضافية التشفير باستخدام معيار Security Assertion Markup Language (SAML) لإطار عمل تسجيل الدخول الأحادي (SSO) وتقنية التحقق من الهوية الشخصية Personal Identity Verification (PIV) والبنية الأساسية للمفتاح العام Public Key Infrastructure (PKI).

عناصر التحكم في المصادقة المضمنة

يمكن إدارة بروتوكولات مصادقة الهوية والوصول إلى الأجهزة عبر منتجات Ricoh على نطاق مركزي. تشمل الأساليب المتاحة بطاقة الهوية أو رقم PIN أو بيانات تسجيل الدخول للشبكة أو مجموعة متعددة العوامل مما سبق. وعلى الرغم من أن المصادقة متعددة العوامل تساعد في تحسين الأمان، إلا أنها تقلل سرعة المستخدمين المنشغلين. على الجانب الآخر، يساعد تسجيل الدخول الأحادي (SSO) في تحقيق ذلك عن طريق السماح للمستخدمين بالوصول إلى مجموعة من الأجهزة بسهولة بالغة. فضلاً عن ذلك، تقدم Ricoh برنامج المصادقة السريعة، وهي المصادقة القائمة على نظام "اسحب البطاقة وانطلق"، الذي يُثبَّت مسبقًا على جميع أجهزتنا؛ ما يمنح المستخدمين طريقة سهلة للوصول إلى مستنداتهم. وباستخدام أجهزة قراءة/كتابة البيانات عبر تقنية NFC، تصبح عملية تسجيل دخول المستخدم في غاية البساطة والسهولة مع تأمين الوصول إلى الطابعة متعددة الوظائف والتحكم فيها بفاعلية كبيرة. يعمل هذا النموذج من الوصول أيضًا مع إعداد الأذونات الموجودة للطابعة متعددة الوظائف لتقييد وصول المستخدم إلى وظائف الجهاز كما هو محدد من طرف العميل.

نظام Streamline NX (SLNX)

وحدة إدارة الجهاز في نظام Streamline NX هي برنامج Ricoh لإدارة الأجهزة المتصلة بالشبكة ومراقبتها. يتيح البرنامج للمسؤولين عرض إعدادات الأمان أو تكوينها للأجهزة باستخدام قوالب جاهزة ومعلمات مخصصة. تشمل إعدادات الأمان المهمة للغاية تمكين/تعطيل البروتوكولات، وإعدادات عنوان IP، وكلمات مرور المستخدم الذي يقوم بدور المسؤول، وعناوين البريد الإلكتروني للتنبيهات، وإعدادات التشفير، وما إلى ذلك. كما يستطيع نظام SLNX الإبلاغ عن أي طابعات غير ممتثلة بناءً على سياسة العميل.

حماية الأجهزة من البرامج الضارة

تتبع Ricoh نهجًا من ثلاث طبقات لتوفير الحماية من البرامج الضارة على أجهزتها. في البداية، لا يمكن تشغيل أجهزة Ricoh إلا باستخدام لغة آلة أو نظام تشغيل خاص بشركة Ricoh فقط. بعد ذلك، لمنع عبث البرامج الضارة ببرنامج الجهاز، يجب كتابة أي تحديثات للبرنامج الثابت واعتمادها بطريقة حصرية بلغة الآلة الخاصة بشركة Ricoh. في النهاية، يجب أن تحمل جميع تحديثات البرنامج الثابت التوقيع الرقمي لشركة Ricoh. وباستخدام هذا الأسلوب ثلاثي الخطوات، لا يمكن تحميل البرنامج الثابت غير المعتمد على أجهزة Ricoh ونتيجة لذلك نتخلص من البرامج الضارة وبرامج التجسس والفيروسات بكفاءة عالية.

حماية المستند الفعلي

إن أفضل ممارسات الأمان ليست معقدة دائمًا. المكاتب عبارة عن أماكن مزدحمة واستخدام الوثائق الورقية يعرض الشركة لخطورة كبيرة سواءً من ناحية السرقة أو إهمال الموظفين. لذا تقدم Ricoh عددًا من خيارات الأمان المادي الإضافية بغرض منع الوصول غير المصرح به إلى المستندات الورقية. على سبيل المثال، يحول قفل أدراج الأوراق دون سرقة الأوراق الحساسة، مثل قوالب الوصفات الطبية في بيئة الرعاية الصحية. كما أن إحكام تثبيت أغطية جميع الكبلات يحول دون إمكانية العبث بها نتيجة تهديدات داخلية. هذا فضلاً عن حل التحرير الآمن لمهام طباعة المستندات (حل اطبع لي Print To Me) الذي يضمن عدم طباعة المستندات إلا في حضور المالك للتخلص من مخاطر المطبوعات التي لم تُجمَع من درج الطابعة.

2 الوقاية

بموجب المتطلبات التنظيمية الجديدة والقائمة، يجب على الشركات ضمان كلٍ من سرية المعلومات حتى لا تُسرَق أو تتسرب للخارج، وسلامتها الدائمة حتى لا تُبدَّل أو تُعدَّل. ولتحقيق ذلك الغرض، صار لزامًا على الشركات تقييد الوصول إلى المستندات الحساسة. فهذا يحول دون إجراء تعديلات غير مصرح بها على البيانات أو تزويرها. كما يعمل كعنصر حماية من التهديدات الموجهة أو الانتهازية داخل الشركة.

في الواقع، العمل باستخدام الأجهزة المحمولة يضيف مزيدًا من التعقيد إلى أي سيناريو للأمن السيبراني. لذا يجب اتباع تدابير أمان إضافية تلائم سياسة مشاركة الملفات من أي موقع. كما يجب تأمين تلك المستندات أثناء نقلها عبر الشبكات وعبر الأجهزة بنفس كفاءة تأمينها أثناء تخزينها. تستطيع تقنية التشفير القوية متابعة البيانات وحمايتها خلال دورة حياتها بكفاءة عالية. على الرغم من أنها تنطبق في الأساس على المستندات، لكنها تمتد لتشمل عناصر الأمان الجوهرية، مثل كلمات المرور المخزنة وإعدادات الماكرو ودفاتر العناوين. ومع تطبيق أنظمة التشفير، حتى إذا نجح المتسللون في الوصول إلى شبكتك فإنهم سيجدون صعوبة بالغة في استخراج أي معلومات مفيدة؛ وهو ما يحافظ على سلامة المعلومات حتى في حالة حدوث اختراق.

يأتي التشغيل المستمر في المقام الأول بالنسبة إلى عديد من الصناعات؛ لذلك تتسبب الأحداث غير المتوقعة كالكوارث الطبيعية في تعريض الشركة لخطر مباشر. تجدُر الإشارة هنا إلى أن المستندات الورقية بصفة خاصة تكون عرضة للتلف في هذا السيناريو. ومن ثم يضيف استخدام مخزن آمن قائم على السحابة لتخزين المستندات الرقمية مرونة كبيرة للتكيف مع الكوارث، سواء أكانت طبيعية أم من فعل البشر. لكن يجب اتخاذ خطوات أمان مناسبة للمحافظة على هذه البيانات الرقمية.

التشفير الأساسي للبيانات

لحماية المعلومات أثناء انتقالها عبر الأجهزة، يمكن تفعيل خاصية التشفير لأي بيانات تنتقل إلى القرص الثابت لطابعة Ricoh متعددة الوظائف أو يجري تخزينها عليه. توفر خيارات البرنامج المضمنة تشفيرًا متطورًا للملفات الممسوحة ضوئيًا والمطبوعة من خلال مفتاح PKI (البنية الأساسية للمفتاح العام) الخاص بالمستخدم. ويحميك ذلك من التعرض لهجمات "الوسيط" داخل بيئة تكنولوجيا المعلومات الخاصة بالعميل.

ولزيادة الأمان، تتم أيضًا الكتابة فوق بيانات الطباعة باستمرار بواسطة نظام تأمين البيانات بالكتابة فوقها (DOSS) من Ricoh الذي سنناقشه بمزيد من التفصيل لاحقًا عند الحديث عن مرحلة "إتلاف البيانات" في دورة حياة البيانات.

حماية Bios ونظام التشغيل

تستخدم الطابعات المتعددة الوظائف من Ricoh الوحدة النمطية للنظام الأساسي الموثوق به (TPM) وهي وحدة أمان للأجهزة غير قابلة للتلاعب. تقوم الطابعات المتعددة الوظائف بتنفيذ وظائف التشفير وتخزين البيانات المشفرة بصورة آمنة. في حين تستخدم Ricoh وحدة TPM في تخزين مفتاح التشفير الأولي لحماية مفتاح تشفير البيانات المخزنة على القرص الثابت والشهادة الرقمية للطابعة متعددة الوظائف. كما أنها تتيح للمسؤولين تنفيذ عملية تمهيد موثوقة بالتحقق من صحة البرنامج الثابت للطابعة المتعددة الوظائف قبل السماح بتشغيلها.

التحقق من صحة البرنامج الثابت

تُضمَّن وظائف التشفير والمفتاح الأولي دائمًا في وحدة TPM ولا يمكن تبديلهما خارج جدار الحماية؛ ما يحول دون سوء استخدام منتجاتنا أو العبث الضار بها. توفر هذه العملية مستوى عاليًا من التحقق من صحة البرنامج الثابت وهوية الجهاز وأمان القرص الثابت للطابعة متعددة الوظائف. وهذا مثال جيد آخر يجسد فكرة أن منتجات الطابعة المتعددة الوظائف من Ricoh مصممة بصورة تضع اهتمامات الأمان لدى عملاء Ricoh على قمة أولوياتها.

إدارة كلمات المرور

يمكن تكوين أجهزة Ricoh باستخدام عدة مستخدمين يقومون بدور المسؤول، وتُعيَّن لكل واحد منهم أدوار مختلفة على الأجهزة وكلمات المرور المميزة. ويمكن تكوين كلمات المرور الخاصة بهؤلاء المستخدمين عن بُعد باستخدام أدوات الإدارة القائمة على الويب، كما يمكن التحقق منها بانتظام. يتيح ذلك مبدأ "فصل المهام" الذي يُعد متطلبًا أساسيًا في عدد من لوائح الشركات.

تقييد وصول المستخدم

تتيح أداة إدارة المستخدمين من Ricoh لمسؤولي النظام تقييد امتيازات وصول المستخدمين. على سبيل المثال، يستطيع المسؤول إعداد امتيازات تمنح مستخدمين محددين صلاحية الوصول إلى دفتر عناوين مسجل على طابعة متعددة الوظائف. ومن شأن ذلك حظر الوصول غير المصرح به إلى السجلات والمعلومات الشخصية المخزنة على أجهزة المكتب.

وظيفة تأمين حساب المستخدم

عند إدخال كلمات المرور بطريقة غير صحيحة على نحو متتالٍ أثناء عملية تسجيل الدخول، تحدد طابعة Ricoh المتعددة الوظائف إذا كان هناك شخص يحاول كسر حماية كلمة المرور من عدمه. وذلك يؤدي إلى تشغيل وظيفة تأمين الحساب وحظر اسم المستخدم ذي الصلة؛ فلا يمكن مصادقة اسم المستخدم المحظور حتى إذا اقترن بعد ذلك بكلمة المرور الصحيحة. ولا يمكن تحرير تأمين الحساب إلا بعد انقضاء وقت محدد أو بواسطة المسؤول؛ ما يخيب آمال المتسللين الطامحين.

3 إتلاف البيانات

إن التخلص من البيانات بطريقة آمنة يعد جزءًا جوهريًا في أي دفاع أمني سيبراني شامل. حيث من السهل السقوط في خديعة أنه لا مسؤولية على الشركة عندما تغادرها البيانات. ولكن عديدًا من اللوائح تشترط أن يتم إتلاف البيانات من خلال عملية شاملة للتخلص من أي مخاطر تتعلق بوقوع سرقة أو سوء استخدام لاحقًا. وحتى حدوث ذلك، لا يمكن الزعم بانتهاء الالتزامات تجاه بيانات الشركة.

يُرجى العلم أن أجهزة المكاتب التي انتهى عمرها الافتراضي والمعادة تعرِّض معلومات الشركة لخطر لا يلقى الاهتمام الكافي في الغالب. تقدم Ricoh خدمة معتمدة قابلة للتدقيق للتخلص من البيانات من الطابعات التي انتهى عمرها الافتراضي. يشمل ذلك المواد التي يُغفَل عنها، مثل إعدادات الشبكة المحفوظة أو بيانات المستخدم أو بيانات القرص الثابت أو حتى الملصقات التي تُترك على الجهاز. جدير بالذكر أن عدم تنفيذ هذه العملية يضع الشركات في خطر كبير بالكشف عن معلومات الشركة السرية والمعلومات الشخصية. لكن من أجل المحافظة على الالتزام التنظيمي، يجب إجراء هذه العملية بصورة مستمرة خلال دورة حياة الجهاز أيضًا. ومن شأن ذلك أن يوفر للشركة أقصى درجة من السيطرة على البيانات التي تقع تحت مسؤوليتها.

الكتابة فوق النُسَخ نظام تأمين البيانات بالكتابة فوقها (DOSS)

تعمل الأقراص الثابتة للطابعة المتعددة الوظائف بكفاءة كبيرة عند تخزين صور مخفية من بيانات المستند في ذاكرتها من أجل تيسير معالجة المهام. هنا تبرز أهمية حل تأمين البيانات بالكتابة فوقها من Ricoh الذي يضمن الكتابة بإستمرار فوق هذه الصور قبل أن تبدأ المهمة التالية. بهذه الطريقة، لو حاول أي شخص الوصول إلى القرص الثابت بسوء نية، فلن يتمكن من الوصول إلى "آثار" أي بيانات تخلفت عن المهام السابقة. وما يدعونا للفخر في Ricoh هو أننا قدمنا إجراء الأمن المثالي هذا لمدة تزيد عن 20 عامًا.

خدمة تطهير البيانات بعد انتهاء عمرها الافتراضي

تقدم Ricoh خدمة تطهير البيانات الشاملة؛ وهي خدمة لما بعد انتهاء العمر الافتراضي للطابعات المتعددة الوظائف والطابعات التي تم مسح جميع وحدات الذاكرة وأقراص التخزين بالجهاز بعد إجراء عملية استعادة باستخدام حلول الأمان المعتمدة في هذا المجال. كما تقدم خدمات تقنية المعلومات من Ricoh خدمة شاملة للتخلص من الأجهزة، ويشمل ذلك تطبيق مستويات متعددة من الخدمات المعتمدة لمسح البيانات.

استبدال القرص الثابت ووحدات التخزين القابلة للإزالة

تقدم Ricoh أيضًا خدمة للتخلص من القرص الثابت تسمح للعملاء بالاحتفاظ بالقرص الثابت الخاص بهم عن طريق استبداله بقرص ثابت جديد فارغ عند إرجاع الجهاز بنهاية عقد الإيجار. ومن شأن ذلك أن يضمن للشركات سيطرة تامة مثبتة على بيئة البيانات التي تديرها.

4 الدعم

مع نمو الشركات، حتمًا تتزايد أعداد الإتصالات بين الأجهزة والشبكات أيضًا. تحتاج الشركات لإستراتيجيات تضمن لها ألا يشكل نمو البنية الأساسية خطرًا أمنيًا. لذلك يجب على تلك الشركات إدراك نقاط الضعف في نظامها وإتخاذ الخطوات اللازمة إستباق الهجمات الموجهة أو الإنتهازية.

في الغالب، يلزم توفر خبرة متخصصة في أمان تقنية المعلومات لتحليل البنية الأساسية للشركة وتحديد هذه الثغرات الأمنية. بالنسبة إلى عديد من الشركات، لا يُعد الاحتفاظ بطاقم موظفين متخصص في تقنية المعلومات داخل الشركة ولديه المعرفة اللازمة لإدارة بيئة الأمن السيبراني خيارًا مطروحًا. فكثيرًا ما تتسبب التكاليف وعدم كفاءة هذا النهج في دفع هذه الشركات نحو حالة من التراخي الخطير.

تقدم خدمة دعم تقنية المعلومات التي توفرها Ricoh خدمات شراء تقنية المعلومات وتكوين إعداداتها، فضلاً عن إمكانات المراقبة عن بُعد وإدارة التحولات ومكتب الخدمات، لتوفير مزيد من الدعم لعملية الأمن السيبراني. يعتمد الأمن السيبراني على اكتساب فهم شامل لمخاطر الأعمال. ويضمن فريق الاستجابة للحوادث الأمنية (SIRT) لدى Ricoh مشاركة المعلومات الحيوية للتهديدات مع العملاء حول العالم، ويمكن تنسيق الاستجابات الفعالة على الفور.

تقييم أمان البنية الأساسية

صُممت وظيفة إدارة الأجهزة في نظام Streamline NX (SLNX) من Ricoh لتؤدي وظيفة عالية القيمة في تدقيق سياسات الأمان. يوفر نظام SLNX وظيفة يفعّلها مديرو تقنية المعلومات لإعداد الأجهزة وفقًا لسياسة الشركة، وتوزيع هذه الإعدادات، وتحليل الإعدادات باستخدام تقرير يقدم البيانات بتنسيق رسومي. كما يمكن أن ينبه نظام SLNX الإدارة بحالة عدم إمتثال أحد الأجهزة لسياسة الشركة.

تحسين أمان الطباعة

تقدم Ricoh خدمة تحسين أمان الطباعة (PSO) الشاملة إضافة إلى خدمات إستشارية إحترافية ومدارة لتحديد الثغرات الأمنية المتعلقة بالأجهزة. هذا الأداة مستندة إلى الويب ومزودة بمعالج رسومي يوفر طريقة عرض للحالة الحالية ويتيح لشركة Ricoh تقديم توصيات للمنتجات بغرض تقليل المخاطر.

فريق الاستجابة لحوادث أمان المنتجات (PSIRT)

يتولى فريق الاستجابة لحوادث أمان المنتجات (PSIRT) من Ricoh إدارة الاستجابة السريعة للتهديدات الجديدة وتطوير الإجراءات المضادة الفعالة. تستخدم Ricoh هذا البرنامج لضمان تحديث مجموعة منتجاتنا بالكامل (الأجهزة والبرامج) وحمايتها من التهديدات والثغرات الأمنية التي تُكتَشف حديثًا. وذلك يساعدنا في المحافظة بإستمرار على مستوى مرتفع من الخدمة على الصعيد العالمي وتقليل تأثير مشكلات الثغرات الأمنية على منتجات Ricoh.

وثائق الدعم

إن الإستعداد والمعرفة عنصران جوهريان لأي هيكل خاص بالأمن السيبراني. يجب تزويد العميل بجميع وثائق النسخ الاحتياطي وأدلة المستخدم والمستندات التقنية للأمان والتدريبات. فمع تعدد عناصر بيئة الأمن السيبراني، يُعد الإمتثال المثبت عنصرًا جوهريًا، وتؤدي هذه الوثائق دورًا أساسيًا في ضمان تحقيق النتيجة النهائية للشركة.

كيف يمكن لشركة RICOH أن تساعدك؟

إن الموقع المتفرد الذي تحتله شركة Ricoh في تقديم حلول أمان رائدة في المجال عبر بيئة الطباعة وتقنية المعلومات بالكامل يستند -جزئيًا- على اكتساب فهم عميق لظروف السوق المتغيرة؛ ومن ثم تطوير مسارنا وفقًا لذلك. وقد صُممت حلولنا لحماية جميع المعلومات خلال دورة حياتها بالكامل وللتعبير بشكل دقيق عن الجوانب الأربعة لأمان البيانات التي نوقشت في هذا التقرير.

كما أننا كرسّنا فريقًا من الخبراء في المجال تتمثل مسؤوليتهم الأساسية في تحليل احتياجات السوق، بما في ذلك المتطلبات الخاصة بمجال معين والتي يمكن تصميم حلول جديدة لها أو تخصيص الحلول الموجودة بالفعل لتلبية تلك المتطلبات.

ونحن ملتزمون أيضًا بتطوير قدراتنا الداخلية لهندسة ونشر حلول تركز على الاهتمام بالأمان. لذا من أجل تحقيق هذه الغاية، أنشأنا فرقًا مكرسة داخل مؤسسة تطوير الخدمات لدينا تركز على تطوير خدمات جديدة للحكومات وإدارة المخاطر والإمتثال للسياسات فضلاً عن خدمات الأمن السيبراني.

تصديق ومصادقة المستخدم

- تأمين الطباعة
- برنامج مضمن قياسي للمصادقة
- مصادقة المستخدم/تقييد الوصول
- تسجيل الدخول الأحادي
- عدة أدوار للمستخدمين
- حماية ملفات PDF بكلمة مرور (كلمة مرور للمستند الممسوح ضوئيًا)
- الحماية من النسخ غير المصرح به
- التحكم في الوصول القائم على نطاق من عناوين IP
- الإدارة الآمنة للأجهزة ومهام الطباعة
- دعم تقنية PKI (البنية الأساسية للمفتاح العام) / البطاقة الذكية (SmartCard)
- الطباعة الآمنة (حل "اطبع لي"print2me / تأمين الطباعة)

حماية Bios ونظام التشغيل

- التمهيد الآمن للجهاز باستخدام الوحدة النمطية للنظام الأساسي الموثوق به (TPM)

حماية الأجهزة من البرامج الضارة

- الخوادم
- ليست/أقل عُرضة للبرامج الضارة
- SOP – إصدار قوي الحماية من Android
- إصدار خاص بشركة Ricoh فقط من نظام تشغيل (لغة التحكم في الجهاز) الجهاز للطابعة المتعددة الوظائف
- نهج ثلاثي الطبقات – التوقيع الرقمي، التنزيل باستخدام أداة Ricoh، وجوب الكتابة بلغة تحكم معينة

الكتابة فوق النُسَخ واستخدام وسائط التخزين القابلة للإزالة

- نظام تأمين البيانات على القرص بالكتابة فوقها (DOSS)
- استخدام محرك أقراص قابل للإزالة

تشفير البيانات

- تشفير القرص الثابت باستخدام الوحدة النمطية للنظام الأساسي الموثوق به (TPM)
- استخدام مفاتيح تشفير باستخدام الوحدة النمطية للنظام الأساسي الموثوق به (TPM)
- تشفير متطور لملفات الطباعة والمسح الضوئي باستخدام مفتاح PKI
- محرك الأقراص الثابتة معتمد من FIPS (معايير معالجة المعلومات الفيدرالية)
- تشفير متطور للطباعة
- تشفير متطور للمسح الضوئي

التخلص من القرص الثابت

- التخلص من القرص الثابت، الكتابة فوق النُسَخ
- خدمة تطهير البيانات الشاملة
- خدمات ما بعد انتهاء العمر الافتراضي: إتلاف البيانات الموجودة في وحدات الذاكرة ووحدات التخزين

إدارة تحديثات البرنامج الثابت وكلمات المرور

- تدقيق كلمات المرور عن بُعد
- وظيفة تأمين حساب المستخدم
- التحقق من صحة البرنامج الثابت باستخدام الوحدة النمطية للنظام الأساسي الموثوق به (TPM)

إدارة الأجهزة

- تعيين الحصص/تقييد الحساب
- DMNX – تدقيق الأمان عبر وحدة تحكم إدارية واحدة، إدارة كلمات المرور، المراقبة، التنبيه

الإمتثال لمعايير الصناعة

- شهادة ISO 27001
- شهادة IEEE 2600.2 لمنتجات معينة
- شهادة ISO 15408 لمنتجات معينة
- وثائق الأمان والتدريب

نهج متعدد الطبقات لأمان الأجهزة من RICOH

ما من شك أن دور موفر الطابعات المتعددة الوظائف قد تطور واختلف كثيرًا عن مجرد التوفير الإجرائي أحادي البعد للأجهزة حتى وصل إلى إدارة البيانات إدارةً فعلية. فالآن صارت إمكانات الطابعات المتعددة الوظائف تشمل التقاط المعلومات من وحدات الإدخال متعددة القنوات، وتصنيف البيانات الملتقطة وتكامل مهام سير العمل، وتوفير تحليلات ووحدات تخزين آمنة محمية. وفي ظل هذه الشبكة المعقدة من متطلبات الاحتفاظ بالبيانات والقواعد متعددة الآليات التنظيمية الصارمة - إضافة إلى التهديدات الداخلية والخارجية التي تعرّض السجلات لمخاطر الفقد أو التلف أو العبث بها - قدمنا نهجًا متعدد الطبقات في أمان الأجهزة لضمان أن توفر لك الطابعة متعددة الوظائف والأنظمة المتصلة بها أفضل حماية ممكنة.

1. الجهاز

تحتل الأجهزة دائمًا موضعًا بارزًا في أي نموذج من نماذج Ricoh. إذ يجري تصميمها وتصنيعها وتنفيذها مع النظر إلى الشق الأمني على أنه متطلب أساسي. فلا يعاني نظام التشغيل الخاص بشركة Ricoh فقط من الثغرات الأمنية الموجودة في عديد من أنظمة التشغيل التجارية الجاهزة، كما أن أجهزتنا معتمدة وفقًا لمعيار IEEE2600.2. هذا إضافةً إلى أن تشفير القرص الثابت وحماية بيانات القرص بالكتابة فوقها تضمنان سرية البيانات التي تجري معالجتها.

2. لوحة العمليات الذكية (SOP) توفر واجهة المستخدم

تستخدم لوحة العمليات الذكية -مثل الطابعة المتعددة الوظائف- نظام تشغيل خاصًا بشركة Ricoh فقط. فلا توجد مكونات غير ضرورية مثبتة على الجهاز، كما أن الوصول غير المقيد (root) إلى جميع موارد النظام غير متاح. ولم تدخر Ricoh وسعًا في ضمان عدم إضعاف أمان الجهاز بتقديم لوحة العمليات الذكية.

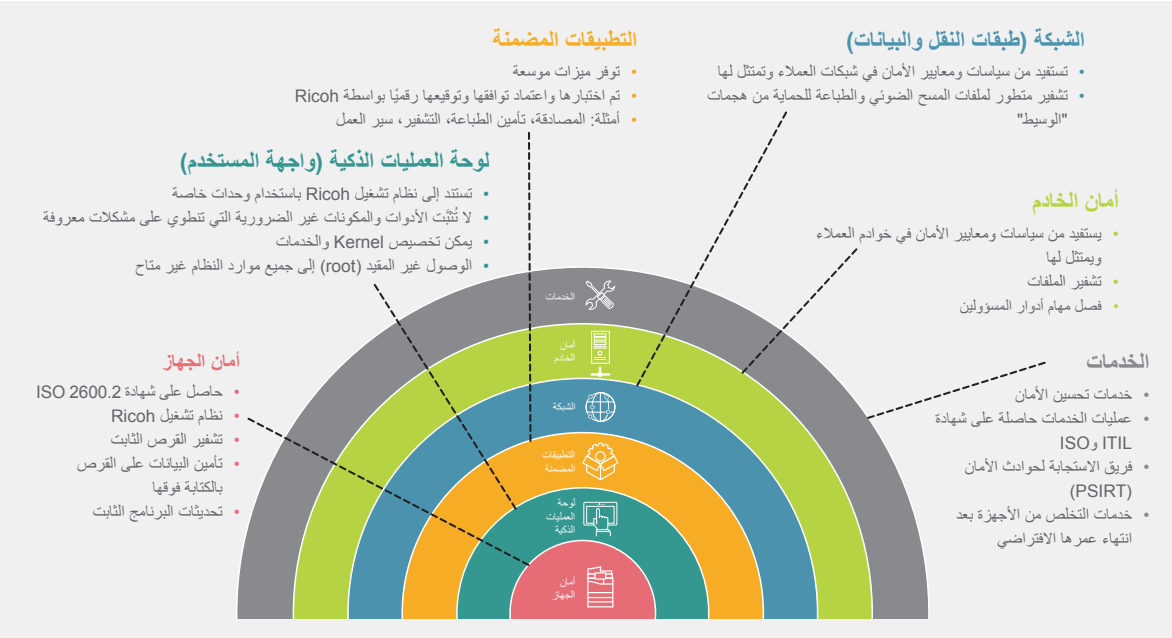
3. التطبيقات الذكية

يمكن تضمين هذه التطبيقات في لوحة العمليات الذكية؛ ما يوفر وظائف إضافية للمستخدم، بما في ذلك التقاط البيانات ومهام سير العمل. وتجدُر الإشارة إلى أن بعض التطبيقات توفر ميزات أمان أساسية، من بينها إمكانات تأمين الطباعة والوصول بالبطاقة والتشفير. تتولى Ricoh أو أحد أعضاء برنامج مطوري Ricoh تطوير هذه التطبيقات، ويجب أن تنجح جميع التطبيقات في اجتياز اختبار التوافق مع متطلبات Ricoh، كما يلزم توقيعها رقميًا قبل أن يُسمَح بتشغيلها في لوحة العمليات الذكية.

4. الشبكة والخوادم

بصرف النظر عمّن يتولى إدارة البنية الأساسية لتقنية المعلومات، تضمن Ricoh أن تمتثل منتجاتنا وخدماتنا لسياسات أمان تقنية المعلومات والشبكات المطبقة لديك. ومن الأساليب المتبعة للحماية من هجمات "الوسيط" أو "الأعمال المدبرة من الداخل": التشفير المتطور لملفات الطباعة والمسح الضوئي، وتشفير البيانات على الخوادم، وفصل مهام المسؤولين.

لدينا مجموعة شاملة من خدمات الأمان تستوعب ما نطرحه من منتجات بالكامل. يشمل ذلك الخدمات الإستشارية والخدمات المدارة لمساعدة العملاء في مراقبة أمان معلوماتهم ومستنداتهم وتحسينه وإدارته. كما لدينا مجموعة من خدمات ما بعد انتهاء العمر الافتراضي التي تضمن تطهير ذاكرة RAM ومحرك الأقراص الثابتة - في أجهزة العميل التي خرجت من الخدمة - قبل التخلص منها.



كيف تحمي RICOH مكان العمل الرقمي؟

يعاني عملاؤنا من مجموعة من المشاكل الأمنية الأساسية، والتي تعززها جميعًا الحقيقة السائدة في مجال الأعمال التي مفادها أنه كلما زادت أحجام البيانات، زادت الثغرات الأمنية والهجمات والخسائر. وبذلك تصبح المحافظة على سرية البيانات وأمانها وبُعدها عن العبث بها معركة لا تنقضي أبدًا. على سبيل المثال، نحن في Ricoh نصد نحو 8 ملايين هجمة على جدار الحماية كل شهر. هذا فضلاً عن عشرات الآلاف من القوانين المتعلقة بالبيانات على المستوى العالمي والوطني وعلى مستوى الصناعة، والتي يتعين على الشركات إثبات امتثالها الدائم لكل منها. ولسبب مفهوم، تتطلع المؤسسات من جميع الأحجام إلى شريك تثق به، يستطيع مساعدتها في المحافظة على أمانها عبر حافظة منتجات تشمل مكان العمل الرقمي بالكامل.

لقد طورت Ricoh مجموعة كبيرة من الحلول التي تساعد على الحد من المخاطر المتنوعة التي تواجه الشركات. ومع تنامي خريطة التهديدات الأمنية للمعلومات بسرعة مذهلة، تستلهم Ricoh الأفكار والرؤى من برامجها التي تحمل شعار "صوت العميل" لزيادة مجهودها في التطوير وتقديم الخدمات.

تعمل اللجان الإستشارية المشكلة من العملاء كمجموعات اختبارية استراتيجية في غاية الأهمية. ونحن نستفيد من ذلك في تحسين فهمنا للاتجاهات والموجهات والأولويات التي تشكل رؤية شركات عملائنا. كما توفر المؤتمرات الإستشارية التقنية التي نعقدها معلومات حيوية صادرة من كبار صناع القرار. وتستفيد فرَق الهندسة والتطوير والبحث في Ricoh من هذه المؤتمرات بالحصول على ملاحظات العملاء القيّمة حول الأفكار والمفاهيم والنماذج المبدئية. وفي النهاية، تتعاون Ricoh مع عملاء من الأفراد لتطوير ميزات أمان جديدة ومتقدمة لعملاء في أسواق عامة وأسواق متخصصة. لا شك أن هذا النهج الموجه للعملاء يساعدنا في التحقق من صحة خريطة منتجاتنا، كما يساعد عملاءنا في الاستفادة من شبكة عالمية من الخدمات والدعم.

يجب أن يكون مكان العمل الرقمي الحديث بنفس سرعة وتيرة التهديدات السيبرانية التي يواجهها وبنفس مرونة ممارسات العمل بداخله. لذلك نعتقد أن الأمن السيبراني يجب أن يعمل بسلاسة ويسر عبر التقنيات التي يختارها عملاؤنا لتزويد مكان عملهم بالإمكانات اللازمة. إن التزامنا بشهادة ISO 27001 في مؤسستنا وشهادة IEEE 2600 في منتجاتنا، إضافة إلى نظام التشغيل الخاص بشركة Ricoh فقط الذي ننشره في تلك المنتجات، يعني أن ضوابط الأمان المصممة وفقًا لأفضل الممارسات مطبقة في موضعها الصحيح، ولكن عليك اختيار هيكلة شركتك وتنميتها.

إن ظهور مجموعة متنوعة من التهديدات الأمنية والمتطلبات التشريعية ومعايير الصناعة المعقدة تعني أن احتمالية وقوع خسارة في سمعة الشركة وخسارة مالية بسبب المخاطر السيبرانية صارت أكبر من أي وقت مضى. لذا نجد أنه من المناسب الآن العمل مع شريك موثوق لمساعدتك على تأمين أصول شركتك الأكثر عُرضة للهجمات وحماية طموحاتك المستقبلية.

تتعلق البيانات والأرقام المعروضة في هذا الكتيب بحالات شركات معينة. وقد تختلف النتائج باختلاف ظروف كل حالة على حدة. جميع أسماء الشركات والعلامات التجارية والمنتجات والخدمات مملوكة لأصحابها المعنيين، وهي علامات تجارية مسجلة لهم. حقوق النشر © لعام 2017 محفوظة لشركة Ricoh Europe PLC. جميع الحقوق محفوظة. لا يجوز تعديل هذا الكتيب و/أو محتوياته و/أو تنسيقاته و/أو تكييفها و/أو نسخها جزئيًا أو بصورة كاملة و/أو دمجها في أعمال أخرى دون الحصول على إذن كتابي مسبق من شركة Ricoh Europe PLC.

RICOH
imagine. change.

www.ricoh-me.com