Die Netzsicherheit stellt die größte Bedrohung für den Erfolg und das Überleben eines modernen Unternehmens dar. Unternehmen jeglicher Größe sind täglich den Gefahren von zerstörerischen Angriffen wie Phishing, DDoS oder Ransomware ausgesetzt. Diese Angriffe können Kosten in Milliardenhöhe nach sich ziehen. Laut einer 2017 durchgeführten Studie des Ponemon Institute belaufen sich die Kosten verursacht durch Datenschutzverletzungen weltweit auf durchschnittlich 3,62 Mio. US-Dollar. Diese Kosten werden in den nächsten Jahren steigen, da Verordnungen wie die DSGVO (Datenschutz-Grundverordnung) vorsehen, Unternehmen beachtliche Strafgebühren aufzuerlegen, wenn diese ihrer Verpflichtung zur Absicherung ihrer Systeme und zum ordnungsgemäßen Schutz der Daten nicht nachkommen. Damit Unternehmen von diesen drakonischen Strafen verschont bleiben, müssen sie ihre Maßnahmen zum Datenschutz nachweisen können. Dazu ist eine ganzheitliche Betrachtung aller Schwachstellen des Unternehmens erforderlich.

Weitere Herausforderungen für die unternehmensweite Netzsicherheit stellen die Erweiterung und Digitalisierung des modernen Arbeitsplatzes sowie die explosionsartige Zunahme von Datenmengen dar. Workflows erstrecken sich häufig über mehrere Systeme, Netzwerke und Standorte. Daten sind vor allem dann gefährdet, wenn sie im Unternehmen bewegt werden. Sie müssen also während jeder Phase der Übertragung geschützt sein. Angesichts der hiermit einhergehenden Sicherheitsrisiken können moderne Unternehmen nicht mehr ohne grundlegend abgesicherte Dokumenten- und Datenmanagementsysteme arbeiten. Gleichzeitig hat sich der Funktionsumfang von Druck- und Multifunktionssystemen in den letzten Jahren enorm erweitert. Mittlerweile sind diese Systeme für einen großen Teil des Ein- und Ausgangs sowie für die Übertragung und Speicherung von Daten zuständig. Hierdurch werden sie häufig zu einem der gefährlichsten, aber oftmals unterschätzten Risiko für den modernen Arbeitsplatz.

Viele Unternehmen geben zwar an, Sicherheitslösungen anzubieten, doch Ricoh entwickelt bereits seit Jahrzehnten sichere Lösungen und Services für Arbeitsplätze. Seit über 20 Jahren sind unsere Drucker beispielsweise mit einer sicheren Festplatten-Überschreibungsfunktion ausgerüstet.

Das Thema Sicherheit ist ein grundlegender Bestandteil unserer gesamten Produktpalette für digitale Arbeitsplätze. Mehr als 4 Millionen unserer Office-Produkte sind heute im Feld in Betrieb. Jedes dieser Produkte und jeder damit verbundene Service zeichnen sich durch integrierte Sicherheitsfunktionen aus. Zudem ist ein Großteil unserer Produkte mit einem Ricoh-eigenen Betriebssystem ausgestattet. Dies ist eine wichtige Komponente unserer Sicherheitsstrategie und gewährleistet die Kontrolle und die Isolierung von betriebssystemspezifischen Bedrohungen, die auf weit verbreitetere Betriebssysteme abzielen.

Ricoh bietet seinen Kunden eine weltweit einheitliche Service- und Supportinfrastruktur, durch die sichergestellt wird, dass das Wissen über Bedrohungen effizient geteilt und genutzt wird. Neben der standardmäßigen IEEE 2600-Zertifizierung für unsere Multifunktionssysteme ist Ricoh eines der führenden Mitglieder und Hauptautor der IEEE Standards Association. Zudem ist Ricoh nach der Norm ISO 27001 für Informationssicherheitsmanagement zertifiziert. Durch eine Reihe globaler, kundenorientierter Innovationsprogramme richten wir die Entwicklung unserer Produkte entsprechend den Geschäftsanforderungen und Sicherheitsbelangen unserer Kunden aus.

Um die hohen Anforderungen an effektive und nachweisbare Best Practices zur Netzsicherheit einzuhalten, wird der Aspekt der Sicherheit bereits in der Designphase jedes Produkts und jedes Services von Ricoh berücksichtigt und nicht erst nachträglich integriert. Wir sind davon überzeugt, dass dieser ganzheitliche Ansatz essentiell für das Überleben und den Erfolg eines modernen Unternehmens ist.

KUNDENSPEZIFISCHE SICHERHEITSHERAUSFORDERUNGEN

TRENDS: Mit zunehmender Datenmenge erhöht sich auch die Zahl der Angriffspunkte und Bedrohungen.

Schutz und Förderung von digitalen Arbeitsplätzen

Ricoh hat sich zum Ziel gesetzt, digitale Arbeitsprozesse – unabhängig vom Ausführungsort – zu ermöglichen und abzusichern. Für eine moderne digitale Wirtschaft bedeutet dies einen Mehrwert, der über den traditionellen Arbeitsplatz hinausgeht. Außenstellen und mobile Mitarbeiter bieten Unternehmen bei der Ausübung von täglichen Aufgaben große Flexibilität und Produktivitätszuwächse. Zudem können die Erwartungen der Kunden sowie Service-Anforderungen besser erfüllt werden.

Am Rande des Netzwerks zu arbeiten bringt große Sicherheitsrisiken mit sich. Die von den Mitarbeitern erzeugten Daten sowie deren mobile Endgeräte, die für die Erfassung der Daten genutzt werden, müssen ordnungsgemäß geschützt werden. Zudem sind mobile Mitarbeiter häufig in verschiedenen Netzwerken und an unterschiedlichen Standorten tätig, wodurch der Datenschutz zusätzlich erschwert wird. Gesetzliche Verordnungen wie die DSGVO schreiben vor, dass Unternehmen Daten auf Lebenszeit nachweisbar absichern müssen. Andernfalls drohen drastische Strafen. Mit der Weiterentwicklung digitaler Workflows am Arbeitsplatz wird auch der Lebenszyklus von Unternehmensdaten immer komplexer. Sehen wir uns diesen Lebenszyklus Schritt für Schritt genauer an.

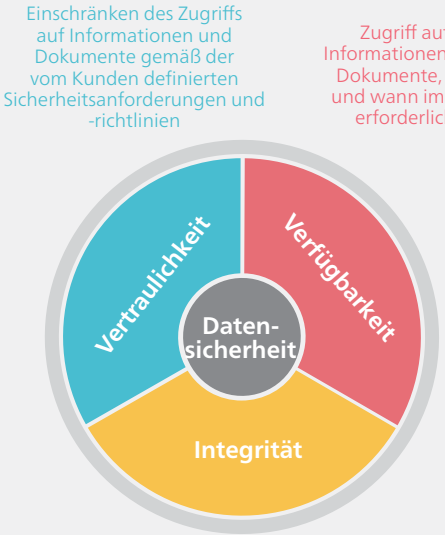
Der erste Schritt sind Systeme zur Dateneingabe sowie -erfassung – eine wesentliche Komponente der Sicherheitsstrategie von Ricoh. Von hier aus müssen diese Daten nun über Netzwerke übertragen und sicher gespeichert werden. In dieser Phase ist die Aufrechterhaltung der Datenintegrität von großer Bedeutung. Die Systeme von Ricoh schränken den Anwenderzugriff auf Geräte- und Netzwerkfunktionen ein, um sicherzustellen, dass die übertragenen und gespeicherten Daten nicht manipuliert werden können. Hierzu dienen die Zugriffskontrolle, die Verschlüsselung und der Kopierschutz. Wir nennen diesen Schritt „Kontrolle".

Nachdem die Daten gespeichert wurden, müssen diese Daten auch für alle Mitarbeiter verfügbar sein, die sie benötigen. Datenverfügbarkeit bedeutet, dass sich die Daten je nach Bedarf abrufen und effektiv visualisieren lassen. Eine wichtige Komponente eines leistungsfähigen digitalen Arbeitsplatzes ist die Datenanalyse. Diese bietet Einblicke in jeden Bereich eines Unternehmens – vom Vertrieb bis zum Personalwesen. Mithilfe von Autorisierungstools kann der schnelle und sichere Zugriff, unabhängig vom Gerät oder Standort, gewährleistet werden. Entscheidend in dieser Phase ist, dass Innovation und Funktionalität nicht durch Sicherheitsprotokolle aufgehalten werden. Wir nennen diese Phase „Aufbewahrung".

Schließlich müssen Daten sicher und nachweisbar beseitigt werden. Hierbei ist zu beachten, dass rechtliche Vorschriften eingehalten werden und die Möglichkeit späterer Datenverluste oder -diebstähle minimiert wird. Dies gilt nicht nur bei der endgültigen Löschung der Daten, sondern auch während der Lebenszeit eines Dokumentes. Zu den von Ricoh angebotenen Dienstleistungen zählen das Bereinigen von Festplatten sowie das Löschen von Arbeitsspeichern und Adressdaten. Wir nennen diesen Prozessschritt „Vernichtung“.

Damit Geschäftsdaten während ihres gesamten Lebenszyklus effektiv gesichert sind, wendet Ricoh die „CIA“-Prinzipien in Bezug auf Datenschutz und Sicherheit an. Confidentiality (Vertraulichkeit), Availability (Verfügbarkeit) und Integrity (Integrität). Auf diesen Prinzipien baut die Entwicklung unserer Produkte und Services auf, damit die erforderlichen Standards und Verordnungen eingehalten werden. Dieser Ansatz ermöglicht Innovation und Wachstum am Arbeitsplatz und gewährleistet gleichzeitig die Einhaltung effektiver und sicherer Verfahren.

DER ANSATZ VON RICOH ZUM THEMA SICHERHEIT



Wir orientieren uns an den „CIA“-Prinzipien für den Schutz und die Sicherheit von Daten: Vertraulichkeit, Integrität und Verfügbarkeit

Sicherheit ist für uns maßgeblich. Jedes von Ricoh hergestellte Produkt und jeder bereitgestellte Service sind mit integrierten Sicherheitsfunktionen ausgestattet.

Um ein sicheres Erstellen von Dokumenten - vom Anfang bis zum Ende - zu ermöglichen, bietet Ricoh eine umfassende Palette an Sicherheitsfunktionen und -dienstleistungen. Die entscheidenden Phasen – Kontrolle, Aufbewahrung, Vernichtung und Support – werden nachfolgend erörtert.

DIE VIER PHASEN FÜR DIE SICHERHEIT AM DIGITALEN ARBEITSPLATZ

1 KONTROLLE

Wirksame Datenkontrollen sind ein entscheidender Faktor für die Wahrung der Vertraulichkeit und Integrität von Daten. Unternehmensinformationen stellen einen elementaren Wert dar und müssen geschützt werden. Bei der Hardware von heute handelt es sich um Informationsterminals, die Zugang zu Unternehmensinformationen gewähren und somit eine Schwachstelle darstellen. Ricoh setzt daher eine Reihe an Tools zur Anwenderauthentifizierung und Geräteverwaltung ein, mit denen Unternehmensdaten kontrolliert und geschützt werden. Mit diesen Tools lassen sich die Einstellungen für Systeme so anpassen, dass der Zugriff auf bestimmte Funktionen und Daten zugelassen oder unterbunden werden kann. Ein bewährtes Verfahren zur Wahrung der Dokumentensicherheit besteht darin, den Mitarbeiterzugriff auf die durch Multifunktionssysteme (MFPs) verarbeiteten Informationen einzuschränken. Zur Kontrollphase gehört auch der Schutz vor Malware durch Ricohs dreistufigen Ansatz zur Geräte-Firmware.

Schutz vor unautorisiertem Kopieren

Damit sich Unternehmen vor unautorisierten Kopierversuchen schützen können, bietet Ricoh eine elegante Lösung zur Gewährleistung der Sicherheit von Papierdokumenten an. Mit der Kopierschutz-Funktion werden Dokumente so gedruckt oder kopiert, dass sich auf dem Hintergrund besondere unsichtbare Muster befinden. Wird das gedruckte oder kopierte Dokument erneut kopiert und/oder gescannt, werden die Muster in den Kopien sichtbar. Das MFP kann mittels der Kopierschutz-Funktion die eingebetteten Muster erkennen und das kopierte Bild durch ein graues Bild ersetzen. Diese Funktion ist besonders für das Drucken von vertraulichen Informationen hilfreich. Indem die Vervielfältigung vertraulicher Informationen eingeschränkt wird, können Informationslecks verhindert werden.

Vertraulicher Druck

Wird ein Dokument von einem PC an ein MFP gesendet, kann dieses Dokument auf der Festplatte des MFP gespeichert werden. Wenn ein Anwender die Funktion „Vertraulicher Druck“ verwendet, wird er im Druckertreiber dazu aufgefordert, dem Druckauftrag ein Passwort mitzugeben. Erst wenn er dieses Passwort am System eingegeben hat, wird der Druckjob gestartet. Auf diese Weise wird gewährleistet, dass der Eigentümer die Kontrolle über das Dokument behält.

Erweiterte Sicherheit bei der Datenerfassung

Die erweiterten Erfassungslösungen von Ricoh bieten eine nahtlose Ver- und Entschlüsselung in allen Verarbeitungsphasen. Mit der Anwenderanmeldung können Administratoren die Verwendung einzelner Funktionen für bestimmte Anwender bzw. Anwendergruppen sperren oder freigeben. Zusätzliche Sicherheitsebenen umfassen Security Assertion Markup Language (SAML) für ein Single-Sign-On-Framework (SSO), Personal Identity Verification (PIV) und Verschlüsselung per Public Key Infrastructure (PKI).

Integrierte Authentifizierungskontrollen

Gerätezugriffs- und Authentifizierungsprotokolle können zentral verwaltet werden. Zu den verfügbaren Authentifizierungsmethoden zählen ID-Karten, PIN-Nummern, die Netzwerkanmeldung oder eine Mehrfachkombination (Multi-Faktor-Authentifizierung) aus den zuvor erwähnten Methoden. Die Multi-Faktor-Authentifizierung erhöht zwar die Sicherheit, kann jedoch die Produktivität von vielbeschäftigten Anwendern senken. Darüber hinaus ist auf unseren gesamten Systemen die Anwendung Quick Authentication von Ricoh vorinstalliert. Die Verwendung eines NFC-Kartenlesers vereinfacht den Anmeldevorgang für Anwender und schützt gleichzeitig wirksam den Zugriff auf das MFP. Diese Zugriffsmethode funktioniert auch mit bestehenden MFP-Berechtigungseinstellungen, die den Anwenderzugriff auf vom Kunden festgelegte Gerätefunktionen einschränken.

Streamline NX (SLNX)

Das in Streamline NX integrierte Device Management dient zur Verwaltung und Überwachung von Systemen in einem Netzwerk. Mittels vordefinierter Vorlagen und benutzerdefinierter Parameter können Administratoren mit dieser Software Sicherheitseinstellungen für Systeme anzeigen oder konfigurieren. Zu den wichtigsten Sicherheitseinstellungen gehören das Aktivieren und Deaktivieren von Protokollen, IP-Adresseinstellungen, Passwörter für Administratoren, E-Mail-Adressen für den Empfang von Warnmeldungen, Verschlüsselungseinstellungen und vieles mehr.

Schutz vor Malware

Ricoh nutzt einen dreistufigen Ansatz zum Schutz der Systeme vor Malware. Zum einen können die Systeme nur mit einer Ricoh-eigenen Maschinensprache bzw. einem eigenen Betriebssystem betrieben werden. Zum anderen müssen zum Schutz vor Manipulation jegliche Firmware-Updates in dieser Ricoh-eigenen Maschinensprache geschrieben und genehmigt worden sein. Des Weiteren benötigt jedes Firmware-Update eine digitale Signatur von Ricoh. Dank dieses dreistufigen Ansatzes werden Malware, Spyware und Viren wirksam abgewehrt.

Sicherheit von Papierdokumenten

Bewährte Sicherheitsverfahren müssen nicht immer kompliziert sein. In stark frequentierten Büros stellen Papierdokumente ein beachtliches Risiko dar, sei es aufgrund der Gefahr von Diebstählen oder durch die Fahrlässigkeit von Mitarbeitern. Ricoh bietet eine Reihe zusätzlicher physischer Sicherheitsoptionen an, um den unbefugten Zugriff auf Papierdokumente zu verhindern. So lässt sich beispielsweise durch das Abschließen von Papierkassetten verhindern, dass sensible Druckmedien wie beispielsweise Rezeptvordrucke gestohlen werden. Mittels Lösungen zur sicheren Dokumentenfreigabe (Print-to-me) wird gewährleistet, dass Dokumente nur in Anwesenheit des Auftragsgebers gedruckt werden. So wird das Risiko eliminiert, dass gedruckte Dokumente im Ausgabefach vergessen werden.

2 AUFBEWAHRUNG

Im Rahmen neuer und bestehender Verordnungen sind Unternehmen dazu verpflichtet, die Vertraulichkeit von Dokumenten sowie deren Integrität sicherzustellen. Dokumente müssen vor Diebstahl und Lecks sowie vor Änderungen geschützt werden. Dies lässt sich erreichen, indem das Unternehmen den Zugriff auf vertrauliche Dokumente beschränkt. Dadurch werden unbefugte Änderungen und Verfälschungen verhindert. Zudem fungiert eine Zugriffsbeschränkung auch als Schutz vor gezielten oder opportunistischen Bedrohungen innerhalb des Unternehmens.

Die Komplexität der Netzsicherheit nimmt durch mobile Arbeitsweisen weiter zu. Es müssen zusätzliche Sicherheitsmaßnahmen getroffen werden, um den Austausch von Dokumenten von jedem Standort aus zu ermöglichen. Für diese Dokumente gelten während der Übertragung über Netzwerke und Systeme dieselben Sicherheitsanforderungen wie auch bei der Speicherung. Sichere Verschlüsselungstechnologien können Daten während ihres gesamten Lebenszyklus wirksam schützen. Obwohl sich diese Maßnahmen auf Dokumente beziehen, können sie auch auf weitere wichtige sicherheitsrelevante Elemente wie gespeicherte Passwörter, Makroeinstellungen oder Adressbücher angewendet werden. Durch die Nutzung von Verschlüsselungstechnologien wird es Hackern deutlich erschwert, Zugriff auf Ihr Netzwerk und somit auf nützliche Informationen zu erlangen. Somit ist die Integrität Ihrer Daten auch bei einer Sicherheitsverletzung gewährleistet.

Viele Branchen müssen rund um die Uhr online sein. Daher können unvorhersehbare Ereignisse wir Naturkatastrophen ein direktes Unternehmensrisiko darstellen. In einer solchen Situation sind Papierdokumente besonders gefährdet. Mit einem sicheren, cloud-basierten Archiv für digitale Dokumente können Sie den Zugriff auch im Falle von Natur- und von Menschen verursachten Katastrophen sicherstellen. Es müssen jedoch entsprechende Sicherheitsmaßnahmen ergriffen werden, um diese digitalen Daten zu schützen.

Unverzichtbare Datenverschlüsselung

Durch die Festplattenverschlüsselung wird sichergestellt, dass Daten die auf der Festplatte des MFPs abgelegt werden, vor unbefugtem Zugriff geschützt sind. Integrierte Softwareoptionen stellen eine End-to-End-Verschlüsselung für gescannte und gedruckte Dateien über den PKI-Schlüssel (Public Key Infrastructure) des Anwenders bereit. Dadurch wird der Schutz vor „Man in the middle"-Angriffen in der IT-Umgebung des Kunden gewährleistet.

Zusätzliche Sicherheit bietet Ricoh mit seinem Data Overwrite Security System (DOSS), durch das Druckdaten kontinuierlich überschrieben werden. Einzelheiten hierzu werden im Abschnitt zur Datenvernichtung beschrieben.

Schutz von BIOS und Betriebssystem

Die MFPs von Ricoh nutzen ein so genanntes Trusted Platform Module (TPM). Dabei handelt es sich um ein manipulationsgeschütztes Modul, das zur Sicherheit der Hardware beiträgt. Das TPM führt kryptografische Funktionen aus und legt kryptografische Daten sicher ab. Ricoh nutzt das TPM zur Speicherung des Root-Verschlüsselungscode, der den Verschlüsselungscode für die Festplattendaten und das digitale Zertifikat der MFPs schützt. Zudem können Administratoren ein Trusted-Boot-Verfahren durchführen, um vor Inbetriebnahme des MFP die Echtheit der MFP-Firmware zu überprüfen.

Firmware-Überprüfung

Der Root-Key sowie kryptografische Funktionen verbleiben immer im TPM und können von außerhalb der Firewall nicht verändert werden. Dadurch werden die missbräuchliche Nutzung und die Manipulation unserer Produkte verhindert. So wird eine Validierung der MFP-Firmware, der Geräteidentität sowie der Sicherheit der Festplatte gewährleistet. Mit dieser Funktion beweist Ricoh einmal mehr, dass bei der Entwicklung seiner Multifunktionssysteme die Sicherheitsanforderungen des Kunden im Vordergrund stehen.

Passwortverwaltung

Auf den Systemen können mehrere Administratoren eingerichtet werden, denen unterschiedliche Rollen und Passwörter zugewiesen werden. Die Passwörter für diese Anwender lassen sich aus der Ferne mithilfe von webbasierten Administratortools einrichten und regelmäßig verifizieren. Dadurch wird die Funktionstrennung ermöglicht – eine Anforderung, die in zahlreichen Unternehmensbestimmungen vorzufinden ist.

Beschränkung des Anwenderzugriffs

Mittels der Anwenderverwaltung von Ricoh können Systemadministratoren die Berechtigungen einzelner Anwender beschränken. So kann der Administrator beispielsweise festlegen, welche Anwender auf das im System hinterlegte Adressbuch zugreifen können. Auf diese Weise wird verhindert, das Unbefugte Zugriff auf persönliche Informationen oder auf Dokumente erhalten, die auf den Systemen gespeichert sind.

Sperren von Anwendern

Wenn bei der Anwenderanmeldung wiederholt ein falsches Passwort eingegeben wird, kann ein MFP von Ricoh erkennen, ob versucht wird, das Passwort zu knacken. Dadurch wird die Sperrfunktion ausgelöst und der entsprechende Anwendername blockiert. Eine Anmeldung mit diesem gesperrten Namen ist auch dann nicht möglich, wenn er später zusammen mit dem korrekten Passwort eingegeben wird. Die Sperre kann erst nach gewissen Zeit oder durch den Administrator aufgehoben werden – eine Maßnahme, die mögliche Hacker-Angriffe verhindert.

3 DATENVERNICHTUNG

Die sichere Vernichtung von Daten macht einen wesentlichen Teil jeder ganzheitlichen Netzsicherheitsstrategie aus. Allzu oft wird angenommen, dass Daten, die das Unternehmensnetzwerk verlassen haben, nicht mehr in den Zuständigkeitsbereich des Unternehmens fallen. Viele Verordnungen verlangen jedoch einen umfassenden Prozess zur Datenvernichtung, sodass gelöschte Daten nicht nachträglich gestohlen oder missbräuchlich verwendet werden können. Unternehmen sind nicht nur für die Vernichtung der Daten verantwortlich, sondern müssen diesen Vorgang auch nachweisen können.

Bürosysteme, die nicht mehr gebraucht oder an Recyclingunternehmen übergeben werden, stellen oftmals ein unterschätztes Risiko für Unternehmensdaten da. Ricoh bietet für diese Fälle einen speziellen Service an, um Daten von nicht mehr benötigten Drucksystemen zu entfernen. Zu solchen Daten zählen auch oft unbeachtete Informationen wie gespeicherte Netzwerkeinstellungen und Anwenderdaten sowie Daten auf der Festplatte des Systems. Werden diese Informationen nicht ordnungsgemäß vernichtet, können vertrauliche Unternehmens- und Mitarbeiterinformationen an die Öffentlichkeit gelangen. Zudem muss die Einhaltung der rechtlichen Compliance-Vorschriften sicher gestellt werden. Auf diese Weise besitzen Unternehmen die maximale Kontrolle über die Daten, für die sie die Verantwortung tragen.

Data Overwrite Security System (DOSS)

Auf der Festplatte eines Multifunktionssystems werden latente Bilder von Daten für die weitere Jobverarbeitung abgelegt. Mit dem Data Overwrite Security-Kit von Ricoh wird sichergestellt, dass diese Daten regelmäßig gelöscht werden. Sollten also Unbefugte in den Besitz der Festplatte gelangen, ist ein Zugriff auf die Daten vorheriger Druckjobs nicht möglich. Wir sind stolz darauf, diese bewährte Sicherheitsfunktion seit mehr als 20 Jahren anzubieten.

Datenlöschung

Ricoh bietet einen Service zur Datenlöschung am Ende der Vertragslaufzeit an. Bei dieser Dienstleistung werden die Daten auf den Arbeitsspeichern und Festplatten der Systeme gelöscht, sodass die Daten nicht wiederhergestellt werden können. Zudem bietet Ricoh die Geräteentsorgung einschließlich mehrerer Services für die Datenlöschung an.

Festplattenaustausch

Ein weiterer Service ist der Ausbau der Festplatte am Ende der Vertragslaufzeit und deren Verbleib beim Kunden - bei Rückgabe des Systems am Ende des Leasing-Vertrags wird dabei die alte Festplatte durch eine neue, leere Festplatte ersetzt. Unternehmen profitieren so von einer vollständigen, nachweisbaren Kontrolle über ihre Datenumgebung.

4 SUPPORT

Mit dem Unternehmen wächst auch die Anzahl der Netzwerkverbindungen. Damit das Infrastrukturwachstum nicht zum Risiko wird, müssen Unternehmen Strategien entwickeln. Hier gilt es, die Schwachstellen zu identifizieren und Schritte einzuleiten, um gezielten und opportunistischen Angriffen vorzugreifen.

Zur Analyse der Unternehmensinfrastruktur und zur Erkennung dieser Schwachstellen sind oftmals umfassende Kenntnisse in der IT-Sicherheit erforderlich. Viele Unternehmen haben jedoch nicht die Möglichkeit, eigene IT-Mitarbeiter mit dem erforderlichen Fachwissen zur Verwaltung einer sicheren Netzinfrastruktur zu beschäftigen. Die Kosten und die Ineffizienz dieses Ansatzes haben jedoch oft zur Folge, dass Unternehmen gefährlicherweise untätig bleiben.

Bei Ricoh können Unternehmen von IT-Beschaffungs- und Konfigurationsdienstleistungen profitieren. Darüber hinaus werden Remote-Überwachungs-, Service-Desk- und Change-Management-Services angeboten. Die Netzsicherheit erfordert ein ganzheitliches Verständnis der Unternehmensrisiken. Das Security Incident Response Team (SIRT) von Ricoh stellt sicher, dass wichtige Informationen über Bedrohungen weltweit gesammelt und effektive Gegenmaßnahmen umgehend koordiniert werden können.

Sicherheitsbewertung der Infrastruktur

Die Device-Manager-Funktion von Ricoh Streamline NX (SLNX) dient der Durchführung eines unverzichtbaren Audits der Sicherheitsrichtlinien. Mit SLNX können IT-Manager Systeme gemäß der Unternehmensrichtlinien einrichten, Einstellungen verteilen und analysieren. Zudem informiert SLNX darüber, wenn ein System die Richtlinien nicht einhält.

Optimierung der Drucksicherheit

Ricoh bietet verschiedene Beratungsdienstleistungen zur Identifizierung von Sicherheitslücken. So können Produktempfehlungen ausgesprochen und Risiken minimiert werden.

Product Security Incident Response Team (PSIRT)

Dank des Product Security Incident Response Team (PSIRT) kann Ricoh aktiv auf neue Bedrohungen reagieren und wirksame Gegenmaßnahmen entwickeln. Auf diese Weise stellt Ricoh sicher, dass das gesamte Produktportfolio (Hardware und Software) kontinuierlich weiterentwickelt wird und vor neuen Bedrohungen und Schwachstellen geschützt ist. So können wir weltweit einen gleichbleibend hochqualitativen Service bieten und die Auswirkungen von Sicherheitsproblemen auf Ricoh-Produkte minimieren.

Begleitende Dokumentation

Ein weiterer nicht zu unterschätzender Faktor für die Gewährleistung der Netzsicherheit sind vorbereitende und schulische Maßnahmen. Dokumentationen zu Backups, Anwenderanleitungen, Whitepaper zu Sicherheitsthemen und Schulungen sollten dem Kunden zur Verfügung gestellt werden. Wie bei vielen Aspekten der Netzsicherheit ist auch hier der Compliance-Nachweis von großer Bedeutung und spielt eine wichtige Rolle für den geschäftlichen Erfolg des Unternehmens.

WIE KANN RICOH HELFEN?

Die Position von Ricoh als führender Anbieter von Sicherheitslösungen für die gesamte IT- und Druckumgebung eines Unternehmens basiert auch auf unserem ausgeprägten Verständnis für sich ändernde Marktbedingungen und der Anpassung unserer Entwicklungen an diesen Wandel. Unsere Lösungen sind auf den Schutz sämtlicher Informationen während ihres gesamten Lebenszyklus ausgelegt und bauen auf den vier in diesem Bericht erläuterten Phasen auf.

Unsere Experten analysieren sorgfältig den Marktbedarf, einschließlich branchenspezifischer Anforderungen, und initiieren die Anpassung bestehender Produkte und die Entwicklung neuer Lösungen.

Zudem arbeiten wir daran, unsere internen Kapazitäten zur Entwicklung und Umsetzung von sicherheitsorientierten Lösungen zu vergrößern. Hierzu wurden dedizierte Teams eingerichtet, die sich darauf konzentrieren, neue Services in den Bereichen Steuerung, Risikomanagement, Compliance und Netzsicherheit zu entwickeln.

Authentifizierung und Autorisierung von Anwendern

- Vertraulicher Druck
- Standardmäßig integrierte Software zur Authentifizierung
- Anwenderauthentifizierung/Anwenderbeschränkung
- Single sign-on
- Mehrere Administratorrollen
- PDF-Passwortschutz (Passwort für gescannte Dokumente)
- Schutz vor unautorisiertem Kopieren
- Zugriffskontrolle nach IP-Bereichen
- Sichere Geräte- und Druckverwaltung
- PKI (Public Key Infrastructure) / Unterstützung von SmartCards
- Sicheres Drucken (print2me / vertraulicher Druck)

Schutz vor Malware

- Serversicherheit
- Keine bzw. geringere Anfälligkeit für Malware
- SOP – spezielle Version von Android
- Ricoh-eigenes Geräte-OS (Maschinensprache) für MFP
- 3-stufiger Ansatz – digitale Signatur, Download über Ricoh-Tool, muss in spezifischer Kontrollsprache geschrieben sein

Services rund um die Festplatte

- Festplattenentsorgung
- Service zur Datenlöschung
- End-of-Life-Service: Vernichtung von Daten auf Arbeitsspeichern und Festplatten

Geräteverwaltung

- Kontingentvergabe
- DMNX – Grundlage für Sicherheits-Audits, Passwortverwaltung, Überwachung, Warnungen

Schutz von BIOS und Betriebssystem

- Sicher durch Trusted Platform Module (TPM)

Datenüberschreibung und Wechselspeichermedien

- Data Overwrite Security System (DOSS)
- Entfernbare Festplatte

Datenverschlüsselung

- Festplattenverschlüsselung über TPM
- Verschlüsselungscodes über TPM
- End-to-End-Verschlüsselung von gedruckten und gescannten Dokumenten mittels PKI-Schlüssel
- FIPS-zertifizierte HDD (Federal Information Processing Standards)
- End-to-End-Verschlüsselung für Druckjobs
- End-to-End-Verschlüsselung für Scanjobs

Firmware-Updates und Passwortverwaltung

- Passwortprüfung mittels Remote-Verbindung
- Sperren von Anwendern
- Firmware-Überprüfung über TPM

Einhaltung von Branchenstandards

- Zertifizierung nach ISO 27001
- Zertifizierung nach IEEE 2600.2 für ausgewählte Produkte
- Zertifizierung nach ISO 15408 für ausgewählte Produkte
- Sicherheitsrelevante Dokumentationen und Schulungen

RICOHS MEHRSTUFIGER ANSATZ ZUR GERÄTESICHERHEIT

Ohne Zweifel hat sich die Rolle von MFP-Anbietern über das eindimensionale Anbieten von Hardware weit hinaus entwickelt und umfasst nun auch die eigentliche Verwaltung von Daten. Moderne Multifunktionssysteme erfassen Daten, klassifizieren sie und integrieren sie in den Workflow. Dazu kommt die sichere Speicherung und die Analyse der Daten. In diesem komplexen Netz von strengen Regeln und Anforderungen - verbunden mit internen und externen Bedrohungen und damit der Gefahr des Verlustes, der Zerstörung und der Manipulation von Daten - verfolgen wir für die Gerätesicherheit einen mehrstufigen Ansatz, um für ihr MFP und die damit verbundenen Systeme die größtmögliche Sicherheit zu gewährleisten.

1. Hardware

Der Kern des Ansatzes von Ricoh ist die Hardware. Bei der Entwicklung und Fertigung unserer Systeme ist das Thema Sicherheit immer im Fokus. Das Ricoh-eigene Betriebssystem hat den Vorteil, dass die bei vielen handelsüblichen Betriebssystemen vorhandenen Schwachstellen hier nicht vorzufinden sind. Zudem sind unsere Multifunktionssysteme standardmäßig nach IEEE2600.2 zertifiziert. Festplattenverschlüsselung und Festplattenüberschreibung gewährleisten, dass die verarbeiteten Daten immer vertraulich bleiben.

2. Smart Operation Panel (SOP)

Ähnlich wie das MFP nutzt auch das SOP ein Ricoh-eigenes Betriebssystem. Unnötige Komponenten werden weggelassen, und es ist kein Root-Zugriff verfügbar. Somit wird die Sicherheit des Systems nicht durch das SOP beeinträchtigt.

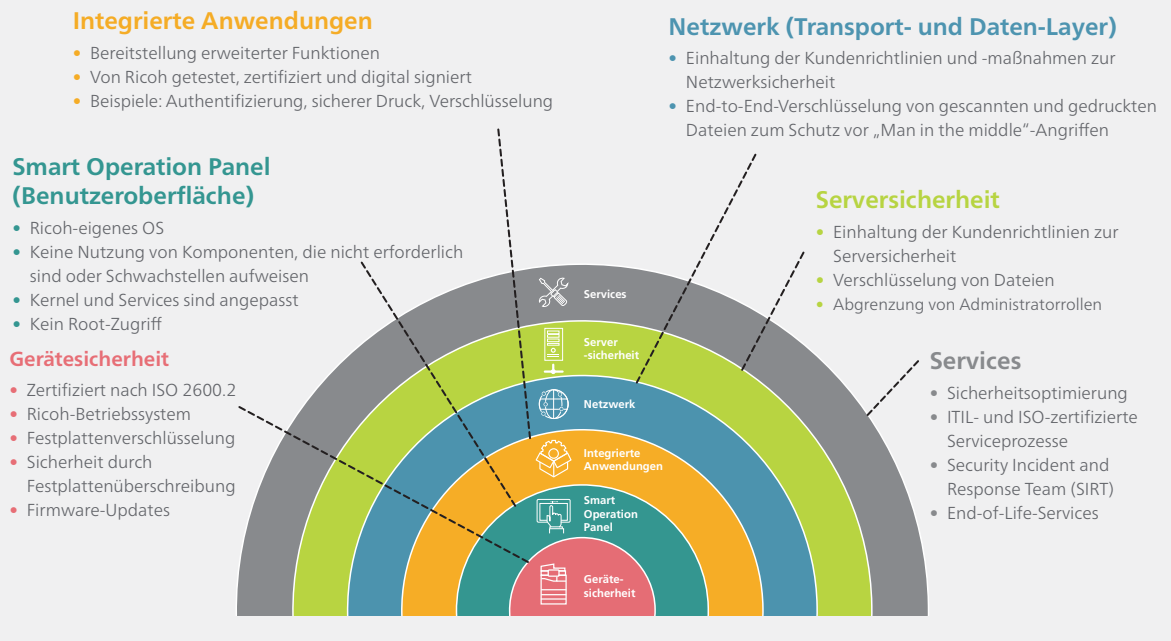
3. Smart Applications

Smart Applications können in das SOP integriert werden, um dem Anwender zusätzliche Funktionen zu ermöglichen. Einige Anwendungen bieten wichtige Sicherheitsfunktionen. Dazu zählen sicheres Drucken, Kartenauthentifizierung und Verschlüsselung. Die Anwendungen werden von Ricoh selbst oder von den Mitgliedern des Ricoh-eigenen Entwicklerprogramms entwickelt. Alle Anwendungen müssen die Kompatibilitätsprüfung von Ricoh bestehen und werden digital signiert, bevor sie bereitgestellt werden.

4. Netzwerk und Server

Unabhängig davon, wer die IT-Infrastruktur verwaltet, gewährleistet Ricoh, dass die Produkte und Services von Ricoh Ihre IT- und Netzwerksicherheitsrichtlinien erfüllen. Eine End-to-End-Verschlüsselung für gedruckte und gescannte Dateien, die Verschlüsselung von auf Servern abgelegten Daten und die Abgrenzung von Administratorfunktionen sind Verfahren, die dem Schutz vor „Man in the middle"-Angriffen oder unternehmensinternen Gefahren dienen.

Unser Angebot wird durch umfassende Sicherheitsdienstleistungen abgerundet. Dazu zählen Beratungsdienstleistungen, um Kunden bei der Überwachung, Optimierung und Verwaltung der Dokumenten- und Informationssicherheit zu unterstützen. Darüber hinaus bieten wir eine Reihe von Services an, Arbeits- und Festplattenspeicher von ausgedienten Kundensystemen vor der Entsorgung vollständig von ihren Daten bereinigt werden.



SO SCHÜTZT RICOH DEN DIGITALEN ARBEITSPLATZ

Unsere Kunden haben eine Reihe an grundlegenden Bedenken hinsichtlich der IT-Sicherheit in ihrem Unternehmen. Diese werden von der Tatsache begleitet, dass sich mit zunehmender Datenmenge auch die Zahl der Angriffspunkte, Bedrohungen und Sanktionen erhöht. So sind Unternehmen permanent damit beschäftigt sicherzustellen, dass Daten vertraulich, sicher und vor Manipulationen geschützt sind. Bei Ricoh werden beispielsweise 8 Mrd. Firewall-Angriffe pro Monat abgewehrt. Es gibt Zehntausende von globalen, nationalen und branchenweiten Datenverordnungen und Unternehmen müssen stets nachweisen können, dass sie diese einhalten. So ist es nachvollziehbar, dass sich Unternehmen einen vertrauenswürdigen Partner an die Seite holen möchten, mit dem sie ihre digitalen Arbeitsplätze absichern können.

Ricoh hat eine breite Palette an Lösungen entwickelt, um die unterschiedlichen Gefahren, denen Unternehmen ausgesetzt sind, zu minimieren. Da die Zahl der Sicherheitsbedrohungen rasch zunimmt, stehen die Kundenanforderungen bei der Entwicklung und Erbringung von Services stets im Fokus.

Dank unserer „Voice of the Customer"-Programme erhalten wir wichtige Einblicke in die Themen und Trends, mit denen sich unsere Kunden beschäftigen. Des Weiteren können unsere Entwickler wertvolles Feedback zu Ideen, neuen Konzepten und Prototypen sammeln. Ferner arbeitet Ricoh mit einzelnen Kunden an der Entwicklung neuer und erweiterter Sicherheitsfunktionen. Dieser kundenorientierte Ansatz hilft uns dabei, unsere Produktstrategie kontinuierlich zu überprüfen, während unsere Kunden gleichzeitig von einem weltweiten Service- und Supportnetzwerk profitieren.

Der moderne digitale Arbeitsplatz muss genauso dynamisch wie die ihm gegenüberstehenden Sicherheitsbedrohungen sein. Aus diesem Grund sind wir der Meinung, dass Netzsicherheit nahtlos alle Technologien, die den Arbeitsplatz des Kunden ausmachen, abdecken muss. Dadurch, dass unser Unternehmen gemäß ISO 27001 und unsere Produkte nach IEEE 2600 zertifiziert sind, wird deutlich, dass wir auf bewährte Sicherheitstechniken setzen.

Durch das Zusammenspiel von Sicherheitsbedrohungen, rechtlichen Anforderungen und komplexen Branchenstandards ergibt sich ein nie dagewesenes Potenzial, mit Rufschädigungen oder finanziellen Sanktionen konfrontiert zu werden. Arbeiten Sie deshalb mit einem vertrauenswürdigen Partner zusammen, der Sie dabei unterstützt, Ihre kostbarsten Unternehmenswerte zu schützen.

RICOH
imagine. change.

www.ricoh.de