Moderne Sicherheitsanforderungen und -lösungen für Unternehmen

Das Problem mit dem flexiblen Arbeitsplatz

Moderne Unternehmen müssen schneller denn je auf eine Unmenge an Informationen zugreifen, diese verschieben und teilen. Mitarbeiter erwarten flexiblere und effizientere Möglichkeiten der Zusammenarbeit. Da der moderne Arbeitsplatz nicht auf die Büroräume beschränkt ist, müssen Ihre Informationen so mobil sein wie Ihre Mitarbeiter.

Das sind Szenarien, mit denen heute fast jedes Unternehmen konfrontiert ist. Obwohl sie einerseits grossartige Möglichkeiten für Produktivität und Innovation bieten, stellen sie andererseits eine möglicherweise ernsthafte Bedrohung für die Sicherheit Ihrer Unternehmensdaten dar.

Wie erfüllen Sie die Erwartungen Ihrer Mitarbeiter und schützen gleichzeitig Ihre Informationen? In dieser Broschüre erhalten Sie einen Überblick über die Herausforderungen eines flexiblen und sicheren digitalen Arbeitsplatzes. Ausserdem erfahren Sie mehr zu potentiellen Sicherheitsrisiken und den Lösungen, mit denen Ricoh Sie unterstützen kann.

RICOH
imagine. change.

Die Situation

Ihre Mitarbeiter erwarten einen flexiblen Arbeitsplatz und mehr Mobilität.

In Anbetracht der heute zur Verfügung stehenden Technologien erwarten Arbeitnehmer, standortunabhängig arbeiten zu können.

Selbst wenn Ihre Mitarbeiter nicht von unterwegs arbeiten, bedeutet der Ausbau mobiler Technologien und Cloud-Lösungen doch, dass die Arbeit nicht mehr auf den Schreibtisch begrenzt ist. Mobiles Arbeiten bedeutet heutzutage weit mehr als nur E-Mails über das Smartphone zu versenden. Es beinhaltet den nahtlosen Zugriff auf Dokumente und Daten sowie einen problemlosen Austausch mit Kollegen und Kunden, überall und zu jeder Zeit. Diese Freiheit ist zu einem Schlüsselfaktor geworden, und sie unnötig einzugrenzen ist keine Option, wenn Sie neue qualifizierte Mitarbeiter für sich gewinnen und halten möchten.

Aber ein flexibler und mobiler Arbeitsplatz kann Ihr Unternehmen einer neuen Art von potenziellen Sicherheitsbedrohungen aussetzen. Was passiert, wenn ein Laptop oder ein Telefon gestohlen wurde? Wie gewährleisten Sie die Sicherheit Ihrer Informationen, wenn Ihre Mitarbeiter über ihre persönlichen Geräte auf sie zugreifen können? Wie schützen Sie sich vor unerwünschten Mitlesern, wenn sich Ihre Mitarbeiter mit einem öffentlichen WLAN verbinden?

RICOH
imagine. change.

Die Herausforderungen

Ein unzureichend geschütztes System zum Speichern und Teilen von Informationen mit Ihren Mitarbeitern innerhalb und ausserhalb Ihrer Büroräume kann sich drastisch auf die Produktivität und Sicherheit auswirken.

Wenn Ihren Mitarbeitern nicht die Tools zur Verfügung stehen, die sie ihrer Meinung nach benötigen, füllen sie diese Lücke mit dem, was sie kennen. Dateien werden per E-Mail an persönliche Konten gesendet und auf privaten Rechnern geöffnet. Dokumente werden in Consumer-Clouds hochgeladen und geteilt. Die nicht genehmigte Verwendung verschiedener Cloud-Services kann ein gut aufgebautes Informationssystem schnell unterwandern.

Solche Workarounds können zu dem allgemein als „Datenschutzverletzung" bekannten Problem führen, einem permanenten Verlust der Kontrolle über Ihre Informationen.

Gut gemeinte Workarounds geben wertvolle Informationen preis

84 % der Mitarbeiter nutzen persönliche E-Mails zum Versenden von sensiblen Dateien[1]

„Bring Your Own Device" immer beliebter

Über die Hälfte der nordamerikanischen und europäischen Unternehmen entwickelt als Reaktion auf die steigende Nachfrage seiner Mitarbeiter BYOD-Ansätze[2]

Viele Datenschutzverletzungen passieren aus Versehen

In Grossbritannien wurden 2017 über 28 Millionen Datensätze kompromittiert. 38 % davon wurden als versehentliche Datenschutzverletzungen eingestuft[3]

Öffentliches WLAN als Minenfeld

Schätzungsweise nur 5 % der öffentlichen WLAN-Hotspots sind verschlüsselt, aber 95 % der Leute nutzen sie mindestens einmal pro Woche für ihre Arbeit[4]

Das Ausmass des Risikos ist unbekannt

Über die Hälfte der IT-Manager hat keine Einsicht in den Datei- und Datentransfer ihres Unternehmens[5]

1. Ipswitch File Transfer, „Are Employees Putting Your Company's Data at Risk? Survey Results Exposing Risky Person-to-Person File Sharing Practices: An eBook report", www.ipswitchft.com. 2. www.forrester.com/Bring-Your-Own-Device-(BYOD). 3. www.theregister.co.uk/2017/09/20/gemalto_breach_index/ 4. gfi.com/blog/survey-95-6-of-commuters-in-the-us-put-company-data-at-risk-over-free-public-wi-fi/ 5. Ipswitch File Transfer eBook report www.ipswitchft.com

RICOH
imagine. change.

Die Lösungen

Mehr Mobilität beginnt mit dem Verständnis dafür, wie Informationen in Ihrem Unternehmen fließen, wo sie gespeichert und wie sie genutzt werden. Daten werden in Ihrem Unternehmen wahrscheinlich über zahllose Geräte geteilt, sodass sie mit ausgeklügelten Sicherheitsmassnahmen geschützt werden müssen.

Informationen in das System einpflegen

Das beste Datensynchronisierungs- und Freigabesystem nützt nicht viel, wenn sich die Informationen, die Sie benötigen, in einem Aktenschrank befinden. Cloud-Lösungen können hier Abhilfe schaffen und das sichere Speichern von Informationen ermöglichen. **Mit der Software-Lösung Streamline NX von Ricoh scannen Sie direkt und sicher in die Cloud.**

Informationen bei Bedarf abrufen

Digitale Dateien bieten viel Komfort und Flexibilität, dennoch müssen sie ab und zu ausgedruckt werden. Mit unseren sicheren Drucklösungen wie Streamline NX Print2Me **stellen Sie sicher, dass die richtigen Informationen immer in die richtigen Hände gelangen.**

Mobiles Drucken und Drucken als Gast

Wenn Mitarbeiter aus anderen Niederlassungen oder Gäste dringend etwas ausdrucken müssen, wird dies häufig darüber gelöst, dass der Anhang an einen Kontakt vor Ort geschickt wird. Dies kann das Risiko einer Übertragung von Viren und Schadsoftware erhöhen. Die Peer-to-Peer-Kommunikation zwischen dem Drucksystem und dem Mobiltelefon sowie Cloud-basiertes Pull Printing minimiert dieses Risiko. **Erfahren Sie mehr über das mobile Drucken mit MyPrint von Ricoh.**

Informationen verwalten

Mit der Implementierung einer Lösung für das Dokumentenmanagement können Sie sicherstellen, dass jeder Mitarbeiter über eine angemessene Zugangsberechtigung zu den benötigten Informationen verfügt. Zudem lässt sich so festlegen, wie, wann und von wem Dokumente eingesehen oder bearbeitet werden dürfen. **Erfahren Sie, wie Ricoh und DocuWare zusammen eine sichere und effiziente Dokumentenverwaltung ermöglichen.**

Fragen Sie einen Experten

Besuchen Sie unsere Website **www.ricoh.ch**, oder kontaktieren Sie Ihren lokalen Ricoh-Vertreter, um mehr darüber zu erfahren, wie wir Sie auf dem Weg zu einem digitalen Arbeitsplatz, der nicht nur sicher, sondern auch produktiv ist, unterstützen können.

Ricoh Schweiz AG
Hertistrasse 2
8304 Wallisellen

+41 844 360 360

www.ricoh.ch

RICOH
imagine. change.