Wyzwania w zakresie bezpieczeństwa danych - problemy i rozwiązania

Elastyczny model pracy

Nowoczesne firmy potrzebują szybkiego dostępu do informacji oraz możliwości udostępniania ich w sposób szybszy niż kiedykolwiek wcześniej. Pracownicy oczekują bardziej elastycznego, wydajniejszego i zorientowanego na współpracę modelu pracy. Współczesne miejsca pracy nie zamykają się w budynku, w którym znajduje się firma lecz wykraczają poza jego mury. Dlatego tak ważna jest mobilność pracowników oraz łatwy a zarazem bezpieczny dostęp do informacji.

Ten nowy model pozwala na podniesienie produktywności i innowacyjności, z drugiej strony wymaga również większej koncentracji na kwestiach związanych z bezpieczeństwem danych.

Jak spełnić oczekiwania pracowników zapewniając równocześnie bezpieczeństwo informacji? W tym dokumencie ukazano, w jaki sposób stworzyć elastyczne i jednocześnie bezpieczne, innowacyjne środowisko pracy. Wskazano także na zagrożenia związane z bezpieczeństwem danych oraz propozycje konkretnych rozwiązań.

RICOH
imagine. change.

Kontekst biznesowy

Twoi pracownicy oczekują elastycznego modelu pracy i większej mobilności.

Dzięki nowoczesnym technologiom pracownicy mogą być bardziej mobilni i realizować swoje obowiązki w ramach bardziej elastycznego modelu pracy.

Nawet jeśli twoja firma nie zatrudnia osób pracujących „zdalnie", powszechność technologii mobilnych i rozwiązań w chmurze oznacza, że pracę można świadczyć z dowolnego miejsca i nie musi być wykonywana zza biurka w siedzibie firmy. Profesjonalistom nie wystarcza już możliwość przeglądania wiadomości e-mail na telefonie – niezbędny natomiast jest łatwy dostęp do dokumentów, danych, współpracowników oraz klientów - zawsze i wszędzie, gdzie jest to potrzebne. Elastyczny model pracy ma duże znaczenie - rezygnując z niej zmniejszasz szanse swojej firmy na przyciągnięcie i zatrzymanie wartościowych pracowników.

Stworzenie nowoczesnego środowiska pracy dostosowanego do tych oczekiwań może narazić twoją firmę na nowe, potencjalne zagrożenia. Co w sytuacji, gdy służbowy laptop czy telefon zostanie zgubiony lub skradziony? Jak zarządzać bezpieczeństwem informacji, gdy pracownicy mają do nich dostęp z osobistych urządzeń? W jaki sposób bronić się przed nieautoryzowanym dostępem do plików, gdy pracownicy korzystają z publicznych sieci Wi-Fi?

RICOH
imagine. change.

Wyzwania

Nieodpowiedni system przechowywania i udostępniania informacji może mieć katastrofalny wpływ na wydajność i bezpieczeństwo firmy.

Firma powinna zapewnić pracownikom dostęp do odpowiednich narzędzi do współdzielenia dokumentów i informacji. Pozwoli to uniknąć sytuacji w których pliki są przesyłane pocztą elektroniczną na konta osobiste, dostępne na komputerach domowych, a także przechowywane i udostępniane za pomocą rozwiązań chmurowych. Niekontrolowane korzystanie z takich rozwiązań może mieć katastrofalne skutki dla bezpieczeństwa kluczowych danych.

Taki sposób pracy może prowadzić do wycieku poufnych informacji i utraty kontroli nad danymi.

Pracownicy nieświadomie narażają firmy na wyciek cennych informacji

84% pracowników używa osobistej poczty e-mail do wysyłania poufnych plików[1]

Rosnąca popularność trendu Bring Your Own Device

Ponad połowa firm w Ameryce Północnej i Europie wdraża rozwiązania BYOD (Bring Your Own Device) w odpowiedzi na potrzeby pracowników[2]

Wyciek danych jest często przypadkowy

Ponad 28 milionów rekordów danych zostało naruszonych w Wielkiej Brytanii w 2017 roku. Spośród nich 38% przypisano przypadkowej utracie[3]

Publiczne sieci Wi-Fi to pole minowe

Szacuje się, że 95% osób wykorzystuje w pracy publiczne hotspoty Wi-Fi przynajmniej raz w tygodniu, a tylko 5% z nich jest szyfrowanych[4]

Pracodawcy często nie są świadomi skali ryzyka

Ponad połowa menedżerów IT nie ma żadnego wglądu w transfer plików i danych w swoich firmach[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. E-book z raportem Ipswitch File Transfer, www.ipswitchft.com

RICOH
imagine. change.

Rozwiązania

Polityka bezpieczeństwa informacji musi opierać się na bardzo dobrym zrozumieniu jej cyklu życia w firmie. W jaki sposób wygląda obieg danych, gdzie są przechowywane i w jaki sposób są wykorzystywane. Ponieważ dane przetwarzane są w obrębie Twojej firmy przez bardzo dużą liczbę urządzeń, muszą być odpowiednio chronione.

Wprowadzanie informacji do systemu

Najlepszy system synchronizacji i udostępniania plików nie będzie spełnić swojej roli właściwie jeśli nadal będą przechowywane głównie w formie drukowanej. Funkcja skanowania do chmury może w sposób inteligentny wysyłać dokumenty bezpośrednio do wybranej usługi i umożliwiając ich bezpieczne przechowywanie. **Skanuj dokumenty do chmury łatwo i bezpiecznie dzięki oprogramowaniu Ricoh Streamline NX.**

Pobieranie danych, gdy ich potrzebujesz

Pomimo wygody i elastyczności korzystania z plików cyfrowych, sa sytuacje w których potrzebny jest wydruk. Upewnij się, że właściwe dokumenty zawsze trafią jedynie do upoważnionej osoby dzięki **rozwiązaniom podnoszącym bezpieczeństwo środowiska druku takim jak Print2Me dostępnym dzięki Streamline NX.**

Wydruk plików przez osoby z zewnątrz oraz druk mobilny

Pilny wydruk dokumentów przez gości i pracowników zewnętrznych można zrealizować wysyłając załączniki do osoby na miejscu. Zwiększa to jednak ryzyko nieumyślnego przesłania wirusów i złośliwego oprogramowania. Komunikacja typu „peer to peer" między urządzeniem a telefonem komórkowym oraz drukowanie z chmury zmniejsza to ryzyko. **Dowiedz się więcej o drukowaniu mobilnym MyPrint firmy Ricoh.**

Zarządzanie informacjami

Wdrożenie rozwiązania do zarządzania dokumentami zapewni każdemu pracownikowi odpowiedni poziom dostępu do potrzebnych danych. Może również dostarczyć informacje o tym jak, kiedy i przez kogo dokumenty są przeglądane lub edytowane. **Odkryj, jak Ricoh i DocuWare współpracują, aby umożliwić bezpieczne i wydajne zarządzanie dokumentami.**

Zapytaj eksperta

Odwiedź stronę **ricoh.pl** lub skontaktuj się z lokalnym przedstawicielem firmy Ricoh, aby dowiedzieć się, w jaki sposób możemy Ci pomóc w stworzeniu bezpiecznego i produktywnego cyfrowego środowiska pracy.

Ricoh Polska Sp. z o.o.
ul. Żwirki i Wigury 18A
02-092 Warszawa

(22) 256 15 55

www.ricoh.pl

RICOH
imagine. change.