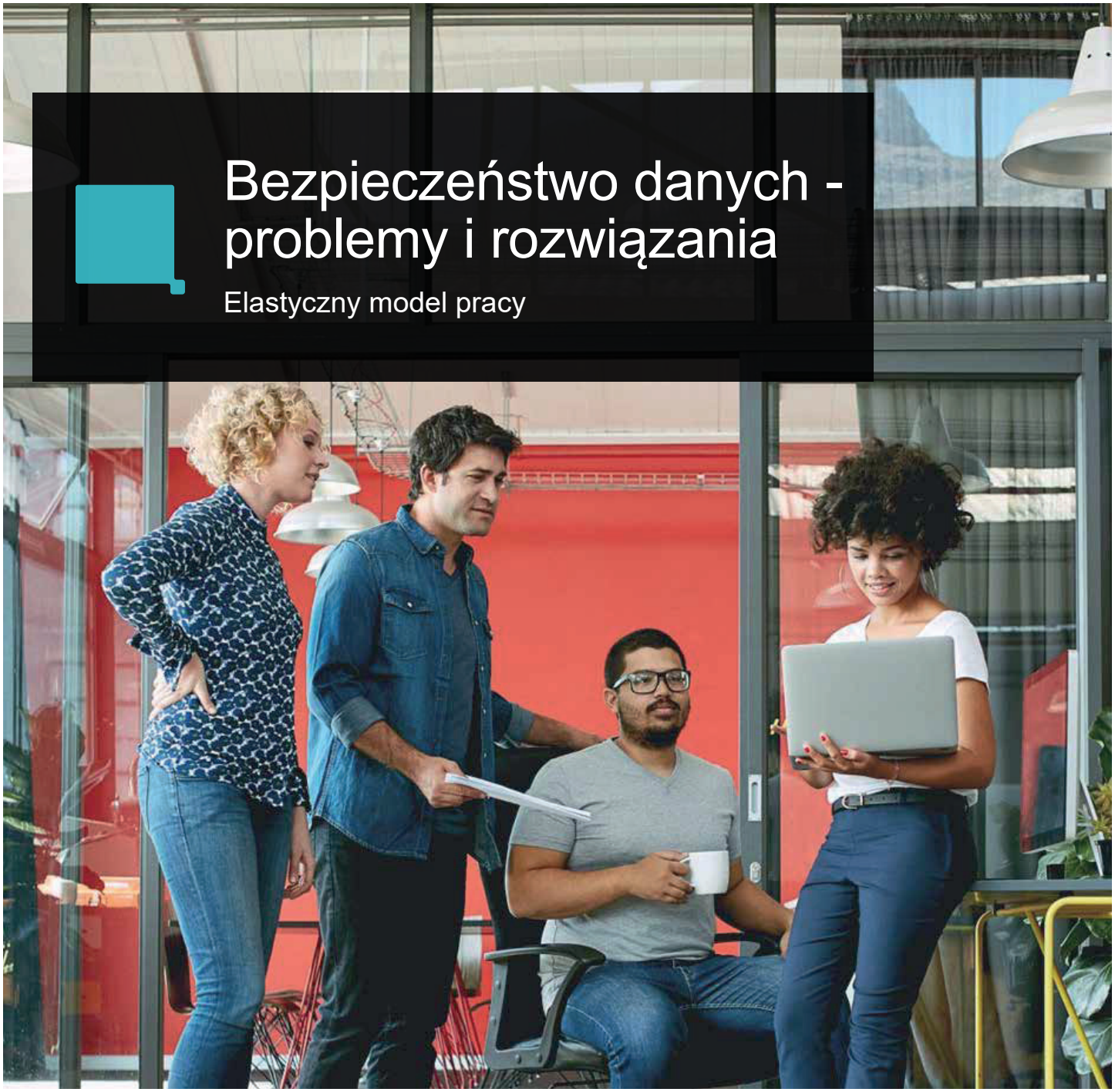
Bezpieczeństwo danych - problemy i rozwiązania

Elastyczny model pracy



Szybki i bezpieczny dostęp do informacji ma obecnie większe znaczenie niż kiedykolwiek wcześniej.

Firmy muszą działać w sposób dużo bardziej elastyczny i zwinnie reagować na zmiany zachodzące na rynku. W związku z tym kładą ogromny nacisk na efektywne wykorzystanie potencjału, który drzemie w danych biznesowych, które posiadają. Jednocześnie muszą sprostać coraz wyższym oczekiwaniom klientów, których lojalność zależy w dużej mierze od szybkiej i dobrej obsługi.

Zmienia się również rynek pracy i podejście do tego jak ta powinna wyglądać. Pracownicy chcą móc wykonywać swoje obowiązki w ramach elastycznego modelu i realizować zadania poza biurem. Te trendy wymagają od firm inwestycji w nowoczesne rozwiązania. Przedsiębiorstwo, które chce funkcjonować na rynku musi stworzyć wydajną i bezpieczną infrastrukturę technologiczną, która pozwoli na dzielenie się danymi, ułatwi współpracę i przyczyni się do podniesienia efektywności procesów.

W tym dokumencie skupiliśmy się na tym, w jaki sposób stworzyć elastyczne i jednocześnie bezpieczne, innowacyjne środowisko pracy. Zwracamy w nim też uwagę na zagrożenia związane z bezpieczeństwem danych oraz propozycje konkretnych rozwiązań.

RICOH
imagine. change.

Kontekst biznesowy

W jaki sposób efektywnie zarządzać bezpieczeństwem informacji, gdy pracownicy mają zdalny dostęp do danych biznesowych?

Nawet jeśli twoja firma nie zatrudnia osób pracujących „zdalnie", powszechność technologii mobilnych i rozwiązań w chmurze pozwalają na uwolnienie się z firmowych murów. Profesjonalistom nie wystarcza już możliwość przeglądania wiadomości e-mail na telefonie. Natomiast niezbędny jest łatwy dostęp do dokumentów, danych, współpracowników oraz klientów – 24/7.

Stworzenie nowoczesnego środowiska pracy dostosowanego do tych oczekiwań daje wiele korzyści, ale jednocześnie wymaga zastosowania odpowiednich środków bezpieczeństwa.

Co w zrobić w sytuacji, gdy służbowy laptop czy telefon zostanie zgubiony lub skradziony?
W jaki sposób bronić się przed nieautoryzowanym dostępem do plików, gdy pracownicy korzystają z publicznych sieci Wi-Fi?

RICOH
imagine. change.

Wyzwania

Nieodpowiedni sposób przechowywania i udostępniania informacji może mieć katastrofalny wpływ na wydajność, zachowanie ciągłości biznesowej i bezpieczeństwo firmy.

Biorąc ten fakt pod uwagę inwestycja w narzędzia do współdzielenia dokumentów i informacji oraz stworzenie odpowiednich procedur to konieczność. Pozwoli to uniknąć sytuacji, w których pliki są przesyłane pocztą elektroniczną np. na osobiste skrzynki, lub są dostępne na komputerach domowych albo przechowywane i udostępniane w chmurze. Korzystanie z rozwiązań będących poza kontrolą firmy może mieć fatalne skutki dla bezpieczeństwa kluczowych danych.

Pracownicy nieświadomie narażają firmy na wyciek cennych informacji

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

Trend 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

W 2017 roku w Wielkiej Brytanii odnotowano ponad 28 milionów przypadków naruszeń danych. Spośród nich 38% przypisano przypadkowemu działaniu[3]

Publiczne sieci Wi-Fi to pole minowe

Szacuje się, że 95% osób pracuje korzystając z publicznych hotspotów 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

[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, takich kwestii jak:

- W jaki sposób wygląda obieg danych?
- Gdzie są przechowywane?
- W jaki sposób są wykorzystywane?

Dane przetwarzane są w obrębie Twojej firmy przez dużą liczbę urządzeń, wymaga to odpowiednich środków bezpieczeństwa.

Wprowadzanie informacji do systemu

Nawet najlepszy system synchronizacji i udostępniania plików nie będzie spełnić swojej roli właściwie, jeśli dokumenty nadal będą przechowywane głównie w formie drukowanej. Jeżeli chcesz zadbać o ich bezpieczeństwo, możesz skorzystać z bezpiecznej funkcji skanowania do chmury. Pozwala ona w sposób inteligentny wysyłać skanowane materiały bezpośrednio do wybranej usługi lub archiwum. **Skanuj dokumenty do chmury łatwo i bezpiecznie dzięki oprogramowaniu Ricoh Streamline NX.**

Pobieranie danych, gdy ich potrzebujesz

Korzystanie z plików cyfrowych pozwala zwiększyć wygodę i elastyczność pracy. Są jednak sytuacje, w których niezbędna jest drukowana wersja dokumentu. Jeśli chcesz zyskać pewność, że np. poufna umowa nie trafi w niepowołane ręce, **skorzystaj z funkcji Print2Me oferowanej przez oprogramowanie Ricoh Streamline NX.**

Wydruk plików przez osoby z zewnątrz oraz druk mobilny

Twoi goście potrzebują czasem wydrukować coś na Twoich urządzeniach? Pracownicy chcieliby drukować pliki z urządzeń mobilnych? Komunikacja typu „peer to peer" między urządzeniem drukującym, a telefonem komórkowym oraz drukowanie z chmury zmniejsza ryzyko przesłania wirusów i złośliwego oprogramowania z zewnątrz systemu. **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. Pozwala też lepiej kontrolować to jak, kiedy i przez kogo dokumenty są przeglądane lub edytowane. **Odkryj, jak Ricoh i DocuWare współpracują, aby umożliwić bezpieczne i wydajne zarządzanie dokumentami.**

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

(22) 256 15 55

www.ricoh.pl

RICOH
imagine. change.