RICOH
imagine. change.

Ricoh Security Solutions

Pomagamy chronić Twoją firmę

Bezpieczeństwo danych ma decydujące znaczenie dla funkcjonowania i sukcesu współczesnych firm. Przedsiębiorstwa każdej wielkości są narażone na ataki typu phishing, DDoS czy ransomware. Ich koszty osiągają wielomilionowe kwoty. Analitycy z Ponemon Institute obliczyli w 2017 roku, że średni globalny koszt wykradzenia danych wyniósł 3,62 mln USD. Co więcej, regulacje prawne, takie jak Ogólne rozporządzenie o ochronie danych (GDPR), coraz częściej przewidują dotkliwe kary finansowe dla firm, które nie zabezpieczą odpowiednio swoich systemów i informacji. Uniknięcie tych kar wymaga zadbania o ochronę danych. Należy do tej kwestii podejść w sposób kompleksowy.

Coraz większy zasięg cyfryzacji, korzystanie z nowoczesnych narzędzi technologicznych i konieczność przetwarzania rosnącej liczby danych to kolejne wyzwania, którym muszą sprostać firmy w kontekście bezpieczeństwa. Obiegi dokumentów obejmują znacznie więcej różnych urządzeń oraz sieci. Informacje na największe ryzyko są narażone wtedy, gdy są przesyłane wewnątrz firmy, dlatego też ważne jest, aby były chronione na każdym etapie swojej drogi. Ze względu na związane z tym zagrożenia, nowoczesne firmy nie mogą już funkcjonować bez zabezpieczonych systemów zarządzania dokumentami i danymi. W ciągu ostatniej dekady zmieniły się możliwości i zadania, które wykonują nabiurkowe drukarki i wielofunkcyjne urządzenia drukujące. Odpowiadają za druk, cyfryzację i archiwizację dużej części dokumentów i danych firmowych. W związku z tym stanowią jedno z najistotniejszych, lecz często niedostrzeganych ogniw łańcucha obiegu danych.

W Ricoh od wielu lat projektujemy rozwiązania podnoszące poziom bezpieczeństwa informacji. Nasze drukarki już od 20 lat oferują funkcję bezpiecznego nadpisywania danych na dysku twardym.

Jako producent i dostawca nowoczesnych rozwiązań traktujemy kwestie związane z ochroną danych w sposób priorytetowy. U naszych klientów działają obecnie ponad 4 miliony urządzeń biurowych Ricoh. Każdy z tych produktów oraz wdrażanych wraz z nimi usług wyposażyliśmy w funkcje podnoszące poziom bezpieczeństwa dokumentów. Nasze rozwiązania sprzętowe działają w oparciu o system operacyjny Ricoh. Pozwala to uniknąć wielu zagrożeń, którym ulegają dominujące na rynku systemy.

Ricoh oferuje klientom dostęp do rozbudowanej struktury usług i wsparcia. Wszystkie nasze urządzenia drukujące mają standardowo certyfikat IEEE 2600, a kompetencje w dziedzinie ochrony danych potwierdza certyfikat ISO 27001 przyznany całej naszej organizacji. Rozwiązania i produkty Ricoh powstają z myślą o potrzebach biznesowych klientów oraz konieczności podniesienia poziomu ochrony informacji.

Dostęp do funkcji związanych z bezpieczeństwem danych wyróżnia nasze urządzenia i usługi. Firma musi chronić dane w sposób holistyczny i mieć na uwadze cały cykl życia dokumentu.

WYZWANIA W ZAKRESIE BEZPIECZEŃSTWA DANYCH

TRENDY: Wraz ze wzrostem ilości danych rośnie prawdopodobieństwo wystąpienia zagrożeń cyberatakiem.

Tworzenie bezpiecznej infrastruktury

Ricoh zapewnia dostęp do innowacyjnych narzędzi pozwalających na bezpieczną pracę z dokumentami. Funkcjonowanie i odniesienie sukcesu wymaga większej efektywności i elastyczności. Praca zdalna i możliwość wydajnego wykonywania swoich obowiązków poza biurem pozwalają realizować tę strategię. Dzięki temu firmy mogą spełnić oczekiwania swoich klientów i usprawnić ich obsługę.

Wiąże się to również z większymi zagrożeniami. Dane i urządzenia muszą być odpowiednio chronione. Szczególnie, że pracownicy działają w różnych lokalizacjach. Duże znaczenie mają również regulacje prawne, takie jak np. rozporządzenie GDPR. Wraz z rozwojem nowoczesnych narzędzi technologicznych i cyfryzacją, cykl życia danych biznesowych jest coraz bardziej skomplikowany. Przyjrzyjmy się jego poszczególnym etapom.

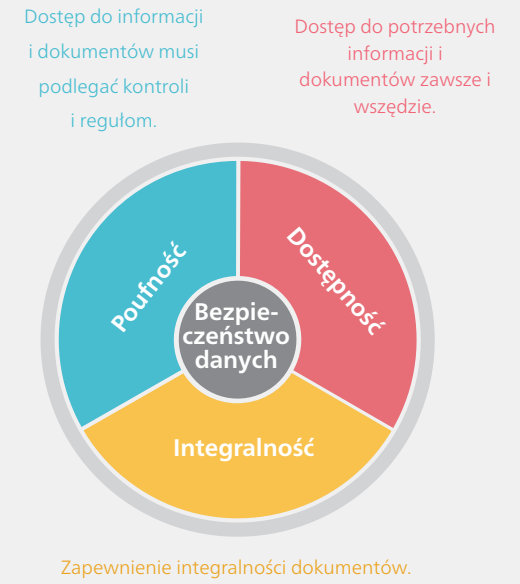
Pierwsza faza wiąże się z drukiem i cyfryzacją dokumentów. Następnie dane muszą być w bezpieczny sposób przesłane i zarchiwizowane. Na tym etapie konieczne jest zapewnienie ich integralności. Systemy Ricoh pozwalają na kontrolę i ustanowienie poziomu dostępu do urządzeń – pozwoli to zapobiec nieautoryzowanej ingerencji w treść dokumentów. Usługi te obejmują kontrolę dostępu, szyfrowanie oraz ochronę przed kopiowaniem. Ich funkcje określamy mianem Kontroli.

Zapisane dokumenty muszą być jednocześnie dostępne dla uprawnionych pracowników. Od tego zależy możliwość efektywnego wykorzystywania informacji. Efektywna analiza danych jest kluczowa we współczesnym biznesie. Sprawia, że organizacja funkcjonuje w sposób sprawny. Narzędzia uwierzytelniające pozwalają na bezpieczne korzystanie z dokumentów. Zabezpieczenia nie mogą jednak hamować innowacyjności i przeszkadzać w codziennej pracy. Etap ten nazywamy Ochroną.

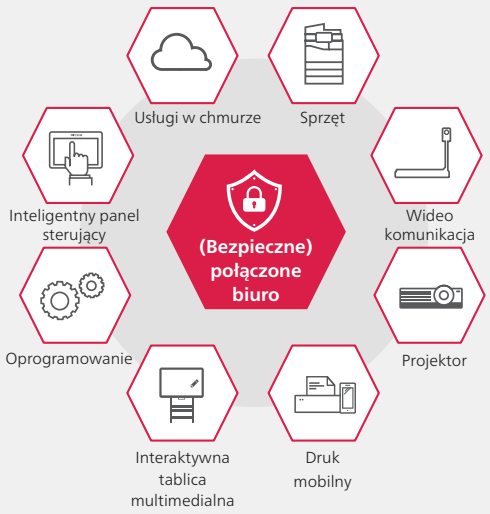
Finalnie firma musi dysponować narzędziami do bezpiecznego i kontrolowanego usuwania danych. Etap ten jest bardzo ważny ze względu na konieczność zachowania zgodności z obowiązującymi przepisami prawnymi. Ten proces ma miejsce na każdym z etapów cyklu życia dokumentu. Drukowanie każdego pliku pozostawia na dysku twardym urządzeń wielofunkcyjnych ukryty obraz, który dla bezpieczeństwa musi zostać nadpisany. Oferowane przez Ricoh usługi usuwania danych obejmują czyszczenie dysku twardego, opróżnianie pamięci, usuwanie niewydrukowanych plików oraz usuwanie danych podczas wylogowania. Nazywamy to Niszczeniem.

W każdym aspekcie naszego podejścia do bezpieczeństwa danych stosujemy zasady „CIA": poufność (Confidentiality), integralność (Integrity) i dostępność (Availability). Kierujemy się nimi w trakcie projektowania wszystkich urządzeń i usług. Dzięki temu możliwe jest stworzenie innowacyjnej i bezpiecznej infrastruktury.

PODEJŚCIE RICOH DO BEZPIECZEŃSTWA DANYCH



Stosujemy zasady "CIA": poufność (Confidentiality), integralność (Integrity) i dostępność (Availability)



Bezpieczeństwo jest zapisane w naszym DNA. Nasze urządzenia i usługi wyposażyliśmy w szereg funkcji podnoszących poziom bezpieczeństwa.

Oferujemy pełne portfolio rozwiązań pozwalających na ochronę dokumentów na każdym etapie ich cyklu życia. Przyjrzyjmy się teraz kolejnym ważnym fazom: kontroli, ochrony, niszczenia i wsparcia.

CZTERY ETAPY BEZPIECZEŃSTWA CYFROWEGO W MIEJSCU PRACY

1 KONTROLA

Odpowiednie środki kontroli pozwalają zapewnić zachowanie poufności i integralności danych. Informacje biznesowe to kluczowe aktywa firmy i muszą być odpowiednio chronione. Współczesne urządzenia mogą potencjalnie stanowić furtkę dostępu do ważnych informacji biznesowych. W związku z tym Ricoh stosuje różne narzędzia do uwierzytelniania i zarządzania infrastrukturą druku, które umożliwiają kontrolę nad tym kto i kiedy korzysta z konkretnych danych. Dotyczy to tworzenia reguł dostępu do konkretnych funkcji i informacji. Jest
to bardzo ważny element procedur związanych z bezpieczeństwem dokumentów. Na tym etapie bardzo ważna jest również ochrona przed złośliwym oprogramowaniem.
Pozwala na to nasze trzystopniowe podejście.

Kontrola nieautoryzowanej kopii

Urządzenia Ricoh wyposażono w opcję zabezpieczenia wydrukowanego dokumentu przed nieautoryzowanym kopiowaniem. Podczas drukowania sterownik nakłada na dokumenty niewidoczny wzór. Jeżeli wydrukowany lub skopiowany dokument zostanie skopiowany lub zeskanowany, wzory będą widoczne na kopiach. Gdy ktoś będzie próbował skopiować taki dokument na dowolnym urządzeniu Ricoh, włączone zostanie powiadomienie dźwiękowe o próbie wykonania nieautoryzowanej kopii, a sama kopia pokryta zostanie szarą planszą uniemożliwiającą odczytanie. Funkcja ta jest szczególnie przydatna przy ochronie informacji poufnych. Skutecznie zapobiega powielaniu wrażliwych dokumentów.

Wydruk bezpieczny

To funkcja, która zapobiega przechwyceniu dokumentu przez osobę nieuprawnioną oraz ogranicza liczbę niepotrzebnie wydrukowanych dokumentów. Użytkownik lub administrator podczas generowania wydruku z komputera nadaje PIN. Wydruk oczekuje w kolejce wydruków na serwerze dokumentów i może być zwolniony dopiero po wprowadzeniu poprawnego kodu PIN. Ponieważ dokumentu nie można wydrukować, zanim użytkownik dotrze do urządzenia, funkcja blokowania wydruku zapewnia kontrolę użytkownika nad dokumentem.

Zaawansowane zabezpieczenia rejestracji obrazu

Zaawansowane rozwiązania Ricoh przeznaczone do cyfrowej rejestracji obrazu wykorzystują szereg metod szyfrowania i odszyfrowania danych na każdym etapie procesu. Administratorzy mogą przyznawać uprawnienia do poszczególnych funkcji procesów zarówno dla indywidualnych użytkowników jak i grup. Dodatkowe warstwy zabezpieczeń obejmują protokół SAML dla funkcjonalności pojedynczego logowania (SSO), elektroniczne karty identyfikacyjne (PIV) oraz szyfrowanie z wykorzystaniem infrastruktury klucza publicznego (PKI).

Wbudowane środki kontroli uwierzytelniania

Dostępem do urządzeń Ricoh oraz stosowanymi w nich protokołami uwierzytelniania można zarządzać centralnie. W tym procesie wykorzystywane są karty identyfikacyjne, numery PIN, funkcje logowania sieciowego lub kombinacje tych narzędzi. Wieloetapowy proces uzyskiwania dostępu zwiększa poziom bezpieczeństwa, ale jest niestety czasochłonny. Rozwiązaniem może być opcja Single Sign On (SSO) pozwalająca na uzyskanie dostępu do kilku urządzeń. Ponadto produkty Ricoh wyposażono w przeinstalowane oprogramowanie Quick Authentication umożliwiające korzystanie na urządzeniu z czytnika kart dostępowych. Moduł do zapisu i odczytu znaczników NFC upraszcza proces logowania użytkowników, a jednocześnie skutecznie zabezpiecza i kontroluje dostęp do urządzenia wielofunkcyjnego. Ta forma dostępu współdziała też z ustawieniami uprawnień w urządzeniu wielofunkcyjnym, ograniczając dostęp użytkowników do funkcji urządzenia zgodnie z potrzebami klienta.

Streamline NX (SLNX)

Moduł menedżera urządzeń na platformie Ricoh Streamline NX to oprogramowanie umożliwiające zarządzanie urządzeniami w sieci i ich monitorowanie. Za jego pomocą administratorzy mogą wyświetlać i konfigurować ustawienia zabezpieczeń urządzeń, stosując gotowe szablony oraz niestandardowe parametry. Najważniejsze ustawienia zabezpieczeń umożliwiają włączanie i wyłączanie protokołów oraz ustawianie adresu IP, haseł administratorów, adresów e-mail do wysyłania powiadomień, szyfrowania i innych funkcji. SLNX może także sygnalizować jeśli urządzenie drukujące nie działa zgodnie z polityką druku określoną w danej firmie.

Ochrona urządzeń przed złośliwym oprogramowaniem

Ricoh stosuje trójetapowe podejście do ochrony infrastruktury druku przed złośliwym oprogramowaniem. Po pierwsze, urządzenia mogą działać wyłącznie z językiem maszynowym Ricoh lub naszym autorskim systemem operacyjnym. Po drugie, aby zapobiec manipulowaniu oprogramowaniem urządzenia, wszelkie aktualizacje firmware muszą zostać zapisane i zatwierdzone wyłącznie w języku maszynowym Ricoh. Po trzecie, każda aktualizacja oprogramowania firmware musi być podpisana cyfrowo przez Ricoh. Dzięki temu na naszych urządzeniach nie można umieścić niezatwierdzonego firmware'u. To skutecznie eliminuje zagrożenia ze strony złośliwego i szpiegującego oprogramowania oraz wirusów.

Bezpieczeństwo dokumentów

Polityka bezpieczeństwa dokumentów nie musi być skomplikowana. W biurze często zdarzają się sytuacje, w których pracownik przez zaniedbanie zostawia ważny dokument w nieodpowiednim miejscu. Ricoh oferuje dostęp do dodatkowych możliwości pozwalających na podniesienie poziomu ochrony wydrukowanych dokumentów. Na przykład opcja zabezpieczonych kaset na papier. To rozwiązanie służy m.in. do bezpiecznego przechowywania szablonów recept w urządzeniu. Stosowanie zaślepek do wszystkich kabli redukuje ryzyko wewnętrznego naruszenia bezpieczeństwa. Bezpieczne zwolnienie wydruku (Print-to-me) – druk realizowany jest na urządzeniu dopiero po autoryzacji użytkownika.

2 OCHRONA

Przepisy prawne zobowiązują firmy do zapewnienia poufności informacji oraz ich integralności. Wymaga to wprowadzenia kontroli dostępu do ważnych dokumentów. Pozwala to zapobiec nieuprawnionej modyfikacji i sfałszowaniu. Stanowi również element ochrony przed zagrożeniami wewnętrznymi.

Ten scenariusz komplikuje konieczność zapewnienia zdalnego dostępu do dokumentów. Wymaga to zastosowania dodatkowych środków zabezpieczających. Aby udostępniane dokumenty były na każdym etapie w odpowiedni sposób zabezpieczone. Technologia silnego szyfrowania to metoda pozwalająca na zapewnienie skutecznej ochrony dokumentu w każdej fazie jego cyklu życia. Zabezpiecza również przechowywane hasła, ustawienia makr i książki adresowe zapisane na urządzeniu. Nawet, gdyby hakerzy przedostali się do sieci, szyfrowanie uniemożliwi im uzyskanie dostępu do informacji i zapewni ochronę integralności dokumentów.

Ograniczenie przestojów jest kluczowe dla firm z wielu branż. Nieprzewidziane zdarzenia, takie jak np. klęski żywiołowe, stanowią bezpośrednie zagrożenie biznesowe. Szczególnie wrażliwe w takich sytuacjach są dokumenty papierowe. Korzystanie z bezpiecznego, elektronicznego repozytorium umieszczonego w chmurze, pozwala zadbać o archiwizację i ochronę kluczowych danych. Stworzenie odpowiedniego środowiska dla tych danych wymaga jednak podjęcia odpowiednich kroków.

Niezbędny element – szyfrowanie danych

Szyfrowanie danych przesyłanych z i na oraz przechowywanych na urządzeniu to niezbędne działanie w procesie ochrony informacji. Rozwiązania Ricoh wyposażono w oprogramowanie pozwalające na kompleksową enkrypcję skanowanych i drukowanych plików przy użyciu klucza infrastruktury publicznej (PKI) użytkownika. Chroni to przed atakami typu „man in the middle" we własnym środowisku IT.

Bezpieczeństwo zwiększa dodatkowo funkcja stałego nadpisywania danych wydruku przez Data Overwrite Security System (DOSS). Ten system zostanie szczegółowo omówiony w części poświęconej fazie cyklu życia danych „Niszczenie".

Ochrona BIOS i systemu operacyjnego

W urządzeniach wielofunkcyjnych Ricoh jest stosowany zabezpieczony moduł sprzętowy Trusted Platform Module (TPM). TPM wykonuje funkcje kryptograficzne i pozwala na bezpieczne przechowywanie kluczy szyfrowania. TPM służy również do przechowywania głównego klucza szyfrowania, chroniącego klucz szyfrowania danych na dysku twardym oraz certyfikat cyfrowy urządzenia wielofunkcyjnego. Moduł ten umożliwia też administratorom dokonywanie zaufanego rozruchu z weryfikacją autentyczności oprogramowania firmware urządzenia, zanim urządzenie będzie dopuszczone do działania.

Weryfikacja oprogramowania firmware

Główny klucz szyfrujący i funkcje kryptograficzne znajdują się zawsze w TPM i nie mogą być zmienione. Zapobiega to niewłaściwemu wykorzystaniu naszych produktów i nieuprawnionej zmianie ustawień. Proces ten zapewnia wysoki poziom weryfikacji oprogramowania firmware, tożsamości urządzenia oraz zabezpieczeń dysku twardego. Pokazuje to nasze podejście do kwestii bezpieczeństwa danych.

Zarządzanie hasłami

Urządzenia Ricoh można skonfigurować z wieloma kontami administratorów wykonujących różne role na urządzeniach i używających różnych haseł. Hasła tych użytkowników można konfigurować zdalnie przy użyciu narzędzi dostępnych w przeglądarce internetowej i regularnie weryfikować. Umożliwia to uregulowanie podziału obowiązków.

Określanie poziomów dostępu użytkowników

Narzędzie Ricoh do zarządzania użytkownikami umożliwia administratorom systemu ograniczanie uprawnień dostępu użytkowników. Administrator może na przykład skonfigurować je w taki sposób, aby tylko wybrani użytkownicy mieli dostęp do książki adresowej zarejestrowanej na urządzeniu wielofunkcyjnym. Blokuje to nieupoważniony dostęp do informacji osobistych i rejestrów przechowywanych na urządzeniu.

Funkcja blokowania użytkownika

Po wielokrotnym wprowadzeniu przez użytkownika nieprawidłowego hasła w procesie logowania urządzenie wielofunkcyjne Ricoh może ocenić, czy ktoś próbuje złamać hasło. Powoduje to uruchomienie funkcji blokady danej nazwy użytkownika. Zablokowany użytkownik nie może się uwierzytelnić, nawet jeżeli wprowadzi prawidłowe hasło. Blokadę można zdjąć dopiero po upływie pewnego czasu lub może to zrobić administrator.

3 NISZCZENIE

Usuwanie danych zgromadzonych na urządzeniu drukującym to bardzo ważny etap procesu ochrony informacji. Firma jest odpowiedzialna za zapewnienie odpowiedniego poziomu bezpieczeństwa również w tej fazie. Wiele przepisów wymaga, aby dane były niszczone w ramach kompleksowego procesu, który eliminuje wszelkie ryzyko kradzieży lub niewłaściwego wykorzystania danych. Dopóki nie będzie można dowieść zastosowania takiego procesu, obowiązki firmy względem danych pozostają w mocy.

Często nie zdajemy sobie sprawy jak wiele ważnych informacji pozostaje na urządzeniach wycofywanych z eksploatacji lub zwracanych z wypożyczenia. Ricoh oferuje certyfikowaną i audytowaną usługę usuwania danych. Obejmuje ona usuwanie zapisanych ustawień sieciowych, danych użytkowników, oraz tych przechowywanych na dysku twardym, czy nawet naklejki widocznej na urządzeniu. Te informacje nie powinny nigdy trafić w niepowołane ręce. A procedura usuwania danych musi być standardowo wpisana w cykl życia urządzenia. Tylko w takim przypadku firma ma całkowitą kontrolę nad swoimi danymi.

Nadpisywanie obrazu: Data Overwrite Security System (DOSS)

Urządzenia MFP działają wydajnie, ponieważ przetwarzają obraz dokumentu na wewnętrznym dysku twardym. Dzięki rozwiązaniu Ricoh Data Overwrite Security Solution te dane są na bieżąco nadpisywane przed rozpoczęciem następnego zadania, a w wypadku nieuprawnionego dostępu do dysku twardego urządzenia będą niewidoczne. Ricoh oferuje tę funkcję już od ponad 20 lat.

Usługa usuwania danych z urządzeń wycofanych z eksploatacji

Ricoh realizuje usługę pełnego czyszczenia danych (Full Data Cleansing Service), polegającą na nieodwracalnym usuwaniu informacji z modułów pamięci i dysków twardych urządzeń wielofunkcyjnych oraz drukarek wycofanych z eksploatacji. Ricoh oferuje także wszechstronną utylizację sprzętu obejmującą kilka poziomów certyfikowanych usług związanych z usuwaniem danych.

Wymiana dysku twardego i pamięci wymiennej

Po zakończeniu okresu najmu urządzenia drukującego klienci Ricoh mogą zatrzymać dysk twardy, który użytkowali. Gwarantuje to firmom pełną i wyraźną kontrolę nad środowiskiem danych.

4 WSPARCIE

Rozwój przedsiębiorstwa wiąże się z rozrostem infrastruktury. Aby odpowiednio i bezpiecznie zapanować nad tym procesem konieczne jest opracowanie szczegółowej strategii. Aby zapobiegać ukierunkowanym oraz doraźnym atakom firma musi mieć pełną świadomość swoich słabych punktów.

Analiza infrastruktury firmowej i identyfikacja luk w zabezpieczeniach wymaga często specjalistycznej wiedzy informatycznej. Wiele firm nie ma w swoich strukturach zespołu specjalistów, którym może powierzyć to zadanie. W związku z tym obserwowane jest zjawisko określane mianem niebezpiecznej bezczynności.

Ricoh realizuje kompleksowe usługi polegające na zakupie i konfiguracji urządzeń IT, a także zdalnym monitorowaniu, świadczeniu pomocy technicznej i zarządzaniu zmianą. Zapewnienie odpowiedniego poziomu bezpieczeństwa danych wymaga całościowego zrozumienia zagrożeń. Zespół Security Incident Response Team (SIRT) Ricoh przygotowuje raport o możliwych zagrożeniach oraz rekomendację działań, które powinny być podjęte aby im skutecznie zapobiec.

Ocena bezpieczeństwa infrastruktury

Menedżer urządzeń dostępny w pakiecie oprogramowania Ricoh Streamline NX (SLNX) umożliwia zrealizowanie audytu zasad zabezpieczeń. SLNX pozwala menedżerom IT na konfigurację urządzeń zgodnie z przyjętymi zasadami, dystrybucję tych ustawień oraz ich analizę. SLNX może także powiadamiać uprawnione osoby, jeśli urządzenie działa w sposób niezgodny z przyjętymi regułami.

Optymalizacja bezpieczeństwa druku

Ricoh oferuje kompleksową usługę Print Security Optimisation (PSO). Poza dostępem do efektywnych rozwiązań klient otrzymuje również wsparcie konsultantów, którzy określają poziom bezpieczeństwa środowiska druku. Z tego narzędzia można wygodnie korzystać w przeglądarce internetowej. Użytkownik uzyskuje szybki dostęp do informacji o stanie zabezpieczeń oraz rekomendacji rozwiązań pozwalających na obniżenie zagrożenia bezpieczeństwa dokumentów.

Product Security Incident Response Team (PSIRT)

Zespół Product Security Incident Response Team (PSIRT) odpowiada za szybką i efektywną reakcję na incydenty związane z naruszeniem procedur i zagrożeniem wystąpienia ryzyka. W ramach tego programu Ricoh zapewnia stałe aktualizowanie i zabezpieczanie całej oferty produktów (sprzętu i oprogramowania) przed nowymi zagrożeniami. Dzięki temu możemy utrzymać konsekwentnie wysoki poziom obsługi w skali globalnej i zminimalizować wpływ luk w zabezpieczeniach, które mogą wystąpić.

Dokumentacja pomocnicza

Budowanie świadomości i edukacja są bardzo ważne. Klienci powinni mieć dostęp do wymaganej dokumentacji, instrukcji obsługi, opracowań dotyczących zabezpieczeń, a także uczestniczyć w szkoleniach. Zdolność do wykazania zgodności z przepisami bezpieczeństwa danych ma bardzo duże znaczenie.

JAK RICOH MOŻE POMÓC?

Ricoh oferuje innowacyjne rozwiązania pozwalające na efektywne zabezpieczenie infrastruktury IT i druku. Dysponujemy wieloletnim doświadczeniem, które zdobyliśmy podczas realizacji tego typu projektów na całym świecie. Nasze narzędzia służą do ochrony danych w perspektywie całego cyklu życia dokumentu i są ściśle związane z czterema aspektami ochrony informacji omawianymi w tym raporcie.

Nasi eksperci analizują potrzeby rynkowe, w tym wymagania konkretnych branż. Na tej podstawie rozwijają rozwiązania dostosowane do tych potrzeb.

Tworzymy także nowe usługi.
Zespoły specjalistów pracują nad nową ofertą dla klientów sektora rządowego, z zakresu zarządzania ryzykiem, przestrzegania przepisów oraz bezpieczeństwa cyfrowego.

Uwierzytelnianie i autoryzacja użytkowników

- Wydruk bezpieczny
- Wbudowane oprogramowanie do uwierzytelniania
- Uwierzytelnianie użytkowników i kontrola dostępu
- Jednokrotne logowanie
- Wiele ról administratorów
- Skanowanie do pliku PDF zabezpieczonego hasłem
- Kontrola nieautoryzowanej kopii
- Kontrola dostępu na podstawie adresów IP
- Zarządzanie bezpieczeństwem urządzeń i druku
- Obsługa PKI (infrastruktury klucza publicznego) i kart inteligentnych
- Bezpieczne drukowanie (print2me /wydruk bezpieczny)

Ochrona urządzeń przed złośliwym oprogramowaniem

- Serwery
- Brak lub zmniejszenie zagrożenia atakiem złośliwego oprogramowania
- SOP — rozbudowana wersja systemu Android
- Autorski system operacyjny (język maszynowy) w wielofunkcyjnych urządzeniach drukujących Ricoh
- Podejście trójetapowe — podpis cyfrowy, pobieranie za pośrednictwem narzędzia Ricoh, wymaganie określonego języka programowania

Utylizacja dysku twardego

- Utylizacja dysku twardego, nadpisanie obrazu
- Usługa Full Data Cleansing
- Usługa wycofania z eksploatacji: niszczenie danych w modułach pamięci operacyjnej i w pamięci masowej

Zarządzanie urządzeniami

- Ustawianie limitów przydziału i kont
- DMNX — audyt zabezpieczeń, zarządzanie hasłami, monitorowanie i powiadamianie z jednego miejsca

Ochrona BIOS i systemu operacyjnego

- Bezpieczne uruchamianie przy użyciu Trusted Platform Module (TPM)

Nadpisywanie obrazu i wymienne nośniki pamięci

- Disk Overwrite Security System (DOSS)
- Wymienny dysk twardy

Szyfrowanie danych

- Szyfrowanie dysku twardego za pośrednictwem TPM
- Klucze szyfrowania za pośrednictwem TPM
- Kompleksowe szyfrowanie plików do druku i zeskanowanych przy użyciu klucza PKI
- Dysk twardy z certyfikatem FIPS (Federal Information Processing Standards)
- Kompleksowe szyfrowanie na potrzeby druku
- Kompleksowe szyfrowanie na potrzeby skanowania

Aktualizacje oprogramowania firmware i zarządzanie hasłami

- Zdalny audyt haseł
- Funkcja blokowania użytkowników
- Weryfikacja oprogramowania firmware za pośrednictwem TPM

Zgodność z branżowymi normami

- Certyfikat ISO 27001
- Certyfikat IEEE 2600.2 dla wybranych produktów
- Certyfikat ISO 15408 dla wybranych produktów
- Dokumentacja zabezpieczeń i szkolenia

WIELOPOZIOMOWE PODEJŚCIE RICOH DO BEZPIECZEŃSTWA URZĄDZEŃ

Rola producentów urządzeń drukujących wykracza poza dostarczanie prostych rozwiązań sprzętowych i ewoluuje w kierunku narzędzi do zarządzania danymi. Nowoczesne MFP stanowią ważne ogniwo w procesie cyfryzacji danych, ich archiwizacji, integracji z obiegiem dokumentów oraz przechowywaniem i analizą. Wieloetapowe podejście Ricoh do ochrony informacji uwzględnia wymogi prawne, zagrożenia wewnętrzne i zewnętrzne. Dlatego zarówno nasze urządzenia jak i systemy pozwalają utrzymać wysoki poziom bezpieczeństwa.

1. Urządzenie

Urządzenie drukujące stanowi centralny element każdego systemu. Możliwości i funkcje w zakresie bezpieczeństwa mają kluczowe znaczenie w procesie projektowania nowych rozwiązań. Nasz system operacyjny jest w mniejszym stopniu narażony na ataki, a urządzenia standardowo są certyfikowane IEEE 2600.2. Funkcje szyfrowania i nadpisywania danych zapewniają poufność przetwarzanych danych.

2. Inteligentny panel sterujący oparty na platformie Android (SOP) wpływa pozytywnie na jakość obsługi

Podobnie, jak urządzenia wielofunkcyjne SOP, działa w oparciu o autorski system operacyjny Ricoh. Instalacja jakichkolwiek dodatkowych komponentów nie jest konieczna, a dostęp na poziomie konta „root" jest niemożliwy. Specjaliści Ricoh dołożyli wszelkich starań, by to rozwiązanie nie wpłynęło na obniżenie poziomu bezpieczeństwa.

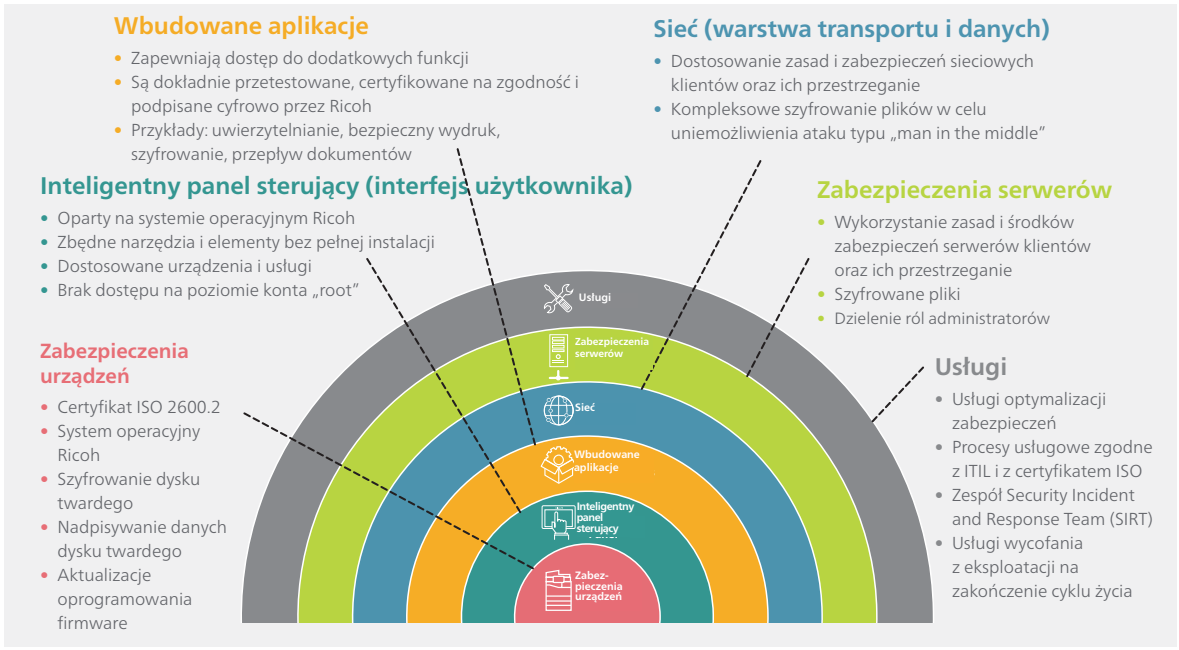
3. Inteligentne aplikacje

Można je bezpiecznie instalować i zyskać dodatkowe funkcje dla użytkowników. Niektóre aplikacje wprowadzają istotne funkcje bezpieczeństwa, takie jak bezpieczny wydruk, autoryzację przy użyciu karty i szyfrowanie. Aplikacje są rozwijane przez Ricoh lub uczestników Ricoh Developer Programme. Wszystkie przechodzą testy Ricoh Compatibility i są dostępne dopiero po uzyskaniu zatwierdzenia.

4. Sieć i serwery

Niezależnie od tego, kto zarządza infrastrukturą IT, Ricoh dba o to, by nasze produkty i usługi były zgodne z Twoimi zasadami zabezpieczeń IT i sieci. Kompleksowe szyfrowanie danych oraz dzielenie obowiązków administratorów pozwalają zmniejszyć zagrożenie atakami typu „man in the middle" i sabotażem wewnętrznym.

Świadczymy wszechstronne usługi związane z zapewnianiem bezpieczeństwa danych. Konsultujemy i proponujemy rozwiązania dopasowane do potrzeb naszych klientów. Ci mogą nam również powierzyć zarządzanie procesami związanymi z monitorowaniem urządzeń oraz infrastruktury. Dbamy również o odpowiednie usunięcie danych z urządzeń wycofywanych z eksploatacji.



JAK RICOH CHRONI CYFROWE MIEJSCE PRACY

Nasi klienci borykają się z problemami związanymi z ochroną danych. Skala zagrożeń, którym muszą sprostać jest wprost proporcjonalna do tempa wzrostu liczby danych, które muszą analizować i zarządzać. Dbanie o poufność i bezpieczeństwo danych oraz zapewnienie integralności to ciągła walka. W Ricoh odpieramy około 8 miliardów ataków na zapory sieciowe miesięcznie. Na świecie obowiązują dziesiątki tysięcy regulacji dotyczących danych, które muszą być przestrzegane przez firmy. Dlatego tak ważne jest znalezienie zaufanego partnera biznesowego, który będzie mógł doradzić i pomóc stworzyć bezpieczną oraz efektywną infrastrukturę.

Oferujemy szeroką gamę rozwiązań i usług związanych z ochroną informacji. Zagrożenia ewoluują bardzo szybko, Ricoh stale usprawnia i dostosowuje swoje narzędzia do nowych realiów.

Bacznie śledzimy trendy. Obserwujemy rynek, szukamy nowych możliwości. Pozwala nam to proponować rozwiązania dopasowane do wymagań rynku i potrzeb naszych klientów. Nasze technologiczne konferencje doradcze dostarczają wartościowej wiedzy od kluczowych decydentów. Pracownicy działów inżynieryjnych oraz badawczo-rozwojowych Ricoh pozyskują podczas tych konferencji cenne opinie klientów na temat pomysłów, koncepcji i prototypów. Ricoh współpracuje też z klientami indywidualnymi w celu opracowywania nowych i zaawansowanych funkcji zabezpieczeń dla poszczególnych branż i do ogólnego zastosowania. Takie zorientowane na klientów podejście pomaga nam weryfikować plany produktowe, a klienci mogą korzystać dzięki temu z globalnej sieci usług i wsparcia.

Nowoczesne cyfrowe miejsca pracy muszą być tak dynamiczne, jak cyfrowe zagrożenia, którym muszą sprostać. Dlatego tak ważne jest zadbanie o kwestie bezpieczeństwa danych w każdym aspekcie funkcjonowania firmy. Nasze kompetencje w dziedzinie ochrony danych potwierdza certyfikat ISO 27001 przyznany całej naszej organizacji oraz IEEE 2600, którym wyróżniono wszystkie produkty Ricoh.

Nieumiejętność sprostania zagrożeniom i brak działania w zgodzie z regulacjami prawnymi, przepisami oraz standardami branżowymi wiąże się z dużymi stratami finansowymi i wizerunkowymi. Podjęcie takiego ryzyka wiąże się z poważnymi konsekwencjami, dlatego warto podjąć współpracę z doświadczonym partnerem biznesowym.

RICOH
imagine. change.

www.ricoh.pl