

Środowisko druku jako element strategii bezpieczeństwa w instytucjach finansowych



Wydajne i elastyczne drukowanie przy najwyższym możliwym bezpieczeństwie danych i minimalnym wysiłku administracyjnym - z korzyścią dla doradców klientów, ekspertów ds. finansów, managerów i administratorów systemów.

W instytucjach finansowych gromadzone i przetwarzane są duże ilości danych wrażliwych, którym należy zapewnić najwyższy możliwy poziom zabezpieczeń. Należy to zapewnić na wielu poziomach i etapach:

- urzędnicy muszą używać technologii zapewniających bezpieczeństwo przechowywanych i przetwarzanych w nich danych
- komunikacja urzędników z systemami zewnętrznymi czy pozostałymi komponentami całego ekosystemu musi zapewniać właściwy poziom szyfrowania i zabezpieczeń
- urzędnicy muszą gwarantować autentyczność przetwarzanych w nich danych

URZĄDZENIA

Wbudowane technologie

W urządzeniach zaimplementowano takie rozwiązania jak TPM (ang. Trusted Platform Module), Secure Boot czy Run-Time Integrity Checks, które mają zapobiegać potencjalnej infiltracji urządzeń przez złośliwe lub nieautoryzowane oprogramowanie.

Monitorowanie podatności

Kyocera we współpracy z ekspertami wielu organizacji zajmujących się tematyką bezpieczeństwa IT wkłada wiele wysiłku w jak najszersze zbieranie informacji o podatnościach oraz analizę możliwego zagrożenia i wpływu na nasze urządzenia. Informacje o wykrytych zagrożeniach są natychmiast publikowane, a wykryte podatności w najkrótszym możliwym czasie likwidowane poprzez aktualizacje oprogramowania wbudowanego.

Zabezpieczenie danych w urządzeniach

Wbudowane mechanizmy (Data Security Kit) zapewniają odpowiedni poziom szyfrowania zapisanych na wbudowanych w urządzeniu nośnikach danych, takich jak HDD, czy SSD oraz zgodne z właściwymi regulacjami metody pozbywania się danych gwarantując, że dane wrażliwe nie dostaną się w niepowołane ręce. Przykładem jest 3 lub 7 krotne czyszczenie danych na nośnikach zgodne z metodą U.S. Department of Defense DoD 5220.22-M ECE lub VSITR German Federal Office for Information Security (BSI).

O NAS

ARCUS to polska grupa kapitałowa, która od prawie 35 lat rozszerza portfolio Klientów o wiodące na rynku banki oraz instytucje finansowe.

WYBRANI KLIENTI Z SEKTORA FINANSOWEGO



Kontrola dostępu do urządzeń

Nasze rozwiązania podnoszą poziom bezpieczeństwa na etapie autoryzacji użytkowników. Kradzież np. karty zbliżeniowej nie wystarczy do korzystania z urządzeń drukujących. Dzięki autoryzacji dwuetapowej dostęp do funkcji przetwarzania dokumentów będą miały tylko osoby upoważnione. Po wstępnym zalogowaniu użytkownik musi potwierdzić swoją tożsamość za pomocą PIN lub poprzez wpisanie hasła. U naszych Klientów wdrożyliśmy również możliwość uwierzytelniania się za pomocą smartfonów z systemem iOS oraz Android. Kopiować, drukować lub skanować mogą tylko te osoby, które otrzymają odpowiednie uprawnienia w systemie, co wzmacnia bezpieczeństwo dokumentów zgodnie z wytycznymi RODO.

Monitorowanie incydentów

Dzięki implementacji protokołu SYSLOG urządzenie wysyła log audytu do systemów klasy SIEM, dzięki czemu mogą być w łatwy sposób monitorowane incydenty dotyczące np. prób nieautoryzowanych dostępu do urządzeń.

Bezpieczeństwo w czasach COVID-19

Dzięki wielu aplikacjom mobilnym np. Kyocera Mobile Print jest możliwa bezdotykowa obsługa urządzeń.

KOMUNIKACJA

Szyfrowanie komunikacji

Urządzenia Kyocera wspierają wiele protokołów zapewniających szyfrowaną komunikację już na poziomie warstwy sieciowej dzięki IPsec. Implementacja najnowszej wersji TLSv1.3 zapewnia najwyższy poziom bezpieczeństwa na poziomie warstwy prezentacji. Również protokoły warstwy aplikacji zapewniają komunikację szyfrowaną, a są to między innymi: HTTPS, IPPS, SNMPv3, LDAP over TLS, POP3 over TLS, SMTP over TLS, eSCL over TLS, DNS over TLS, REST over TLS, VNC over TLS, FTP over TLS itp.

Zarządzanie certyfikatami

Dzięki implementacji protokołu SCEP staje się możliwa automatyzacja procesu wydawania i odnawiania certyfikatów urządzeń Kyocera np. dla celów IEEE 802.1X.

Podczas nawiązywania komunikacji opartej na certyfikatach urządzenia sprawdzają przeznaczenia certyfikatu, jego ważność oraz potwierdzają, że certyfikat nie został skompromitowany dzięki obsłudze CRL (Certificate Revocation List) i/lub OCSP (Online Certificate Status Protocol).

Komunikacja bezpośrednia

Dzięki WiFi Direct jest możliwa bezpośrednia komunikacja urządzenia mobilnego, laptopa z urządzeniem co eliminuje konieczność korzystania z jakiegokolwiek punktu dostępowego WiFi. Dzięki temu dane są transferowane jedynie pomiędzy urządzeniem Kyocera a urządzeniem mobilnym. Analogicznie dzieje się w przypadku drukowania poprzez BLE dzięki wsparciu technologii iBeacon.

ZABEZPIECZENIE PRAC

Automatyczna archiwizacja przetwarzanych prac

Ważnym procesem jest przechwytywanie dokumentów i automatyzacja ich przepływu. Pozwala to na wykorzystanie urządzeń wielofunkcyjnych w procesie przetwarzania i archiwizacji danych nie tylko podczas drukowania czy skanowania, ale także podczas **kopiowania**. Automatycznie konwertowane dokumenty są przesyłane do właściwej lokalizacji wraz z metadanymi pracy, co może zostać wykorzystane nie tylko do celów archiwizacji, lecz również do analizy treści i wyszukiwania podejrzanych słów kluczowych w przetwarzanych dokumentach.

Autentyczność dokumentów

Urządzenia posiadają wiele funkcjonalności gwarantujących autentyczność przetwarzanych dokumentów.

- S/MIME - zapewnia szyfrowanie i cyfrowy podpis wiadomości email wysyłanych z urządzenia
- Podpis cyfrowy skanowanych dokumentów certyfikatem urządzenia gwarantuje, że dokument nie został zmodyfikowany
- Bezpieczny znak wodny gwarantuje autentyczność oryginalnego wydruku. Po jego skopiowaniu pojawia się niewidoczny na oryginale znak wodny, co pozwala odróżnić nieautoryzowaną kopię od oryginalnego wydruku