Co dla druku oznacza RODO?

Poznaj funkcje modeli Brother, które zapewnią bezpieczeństwo danych wrażliwych w Twojej firmie.

brother
at your side

Spis treści:

1. Wstęp

RODO, a wydruk dokumentacji w biurze.

W świetle nowego rozporządzenia RODO przedsiębiorcy mają obowiązek zapewnienia poufności i bezpieczeństwa przetwarzanych przez siebie danych wrażliwych.

Każda firma będzie musiała wdrożyć odpowiednie procedury bezpieczeństwa. Brak przestrzegania zaostrzonych standardów, które wejdą w życie 25 maja 2018 roku, może się zakończyć nałożeniem kary administracyjnej. Jej wysokość może wynosić do 20 milionów euro lub równowartość 4% globalnych rocznych przychodów firmy.

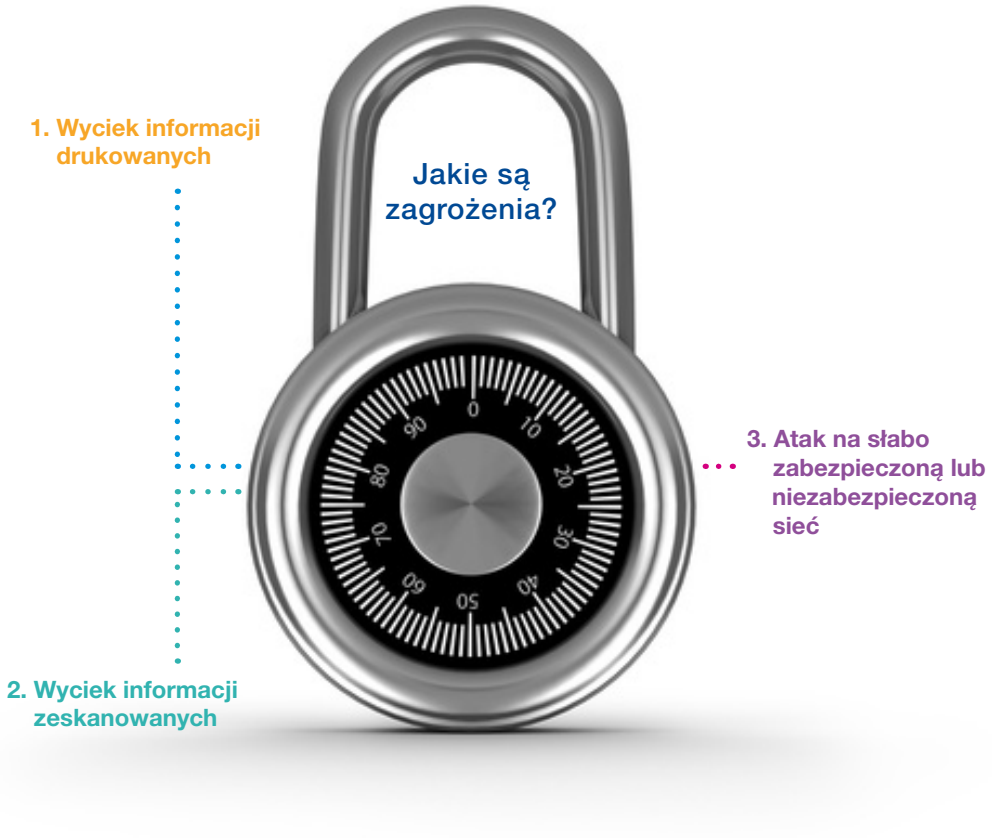
Należy pamiętać, że początek tej drogi to przede wszystkim **ochrona obiegu dokumentów w formie drukowanej.** Bardzo często wyciek danych, to po prostu sytuacja, w której wydruk z drukarki trafia do rąk osoby, nie posiadającej uprawnień do przechowywania danych osobowych.

Co więcej, w prostych urządzeniach drukujących dane osobowe podczas drukowania są często przesyłane bez szyfrowania w sieci. Ponadto, są także przechowywane bez szyfrowania na serwerach, a nawet na dysku drukarki.

„ Zapewnij bezpieczeństwo wrażliwych danych dzięki funkcjom modeli Brother ”.

Ukryte zagrożenia związane z funkcjonowaniem urządzenia drukującego

Funkcje drukarek i skanerów są coraz lepiej dopasowane do zróżnicowanych potrzeb użytkowników. Równocześnie z nowymi możliwościami pojawiają się nowe wyzwania. Niestety, w wielu firmach brakuje świadomości i wiedzy jak zapewnić systemom, sprzętowi oraz wrażliwym danym odpowiedniej ochrony związanej z drukiem.



Środki bezpieczeństwa stały się częścią naszego codziennego życia w pracy. Do ochrony zasobów stosuje się wiele różnych rozwiązań - od kart identyfikacyjnych po oprogramowanie służące ochronie sieci i danych.

Wciąż jednak jest jeden obszar w firmie, który jest bardzo narażony na ataki – sposób, w jaki sprzęt, taki jak drukarki, łączy się z bezpieczną siecią.

W 2015 roku firma Brother przeprowadziła badanie wśród 2500 małych i średnich przedsiębiorstw, w którym zapytała o największe wyzwania, z jakim się mierzą. 75% ankietowanych firm jako najistotniejszą kwestię wymieniła bezpieczeństwo systemów informatycznych. 59% potwierdziło, że bezpieczeństwo informacji wpływa na decyzje odnośnie drukowania i zarządzania dokumentami w przedsiębiorstwie.

Takie postawy i obawy zwiększają się wraz z rosnącą liczbą problemów związanych z bezpieczeństwem w różnych sektorach. Badanie przeprowadzone przez firmę Quocirca w 200 przedsiębiorstwach, również w 2015 roku, ujawniło, iż sprawy bezpieczeństwa są kwestiami najistotniejszymi (75% respondentów wskazało je jako czynnik ważny lub bardzo ważny). Ponad 74% firm już wdrożyło lub planuje wprowadzić rozwiązania w zakresie bezpieczeństwa procesów drukowania.

2. Zabezpieczenia urządzeń przed nieautoryzowanym dostępem

Jakie są zagrożenia?

Nawet jeśli drukarki posiadają funkcje zapewniające wysoki poziom bezpieczeństwa, ale nie będą fizycznie zabezpieczone w pomieszczeniach, to zawsze ktoś będzie mógł do nich podejść i próbować pozyskać dane zapisane w ich pamięci.

W przypadku małych i średnich firm, które mają słabo rozwiniętą infrastrukturę IT, stosowanie jakiejś formy zabezpieczeń fizycznych jest szczególnie ważne. Większość stanowisk pracy nie znajduje się w bezpośredniej bliskości drukarki, dlatego też istnieje wysokie ryzyko dostania się dokumentów w niepowołane ręce.

W badaniu przeprowadzonym w 2015 roku przez firmę Brother, dwie trzecie osób decyzyjnych stwierdziło, że bezpieczeństwo informacji ma wpływ na podejmowane przez nich decyzje dotyczące druku i zarządzania dokumentami. Główne obawy decydentów dotyczą sposobu przechowywania dokumentów przez drukarkę.

W jaki sposób można temu zapobiegać?

Brother posiada zdywersyfikowaną ofertę rozwiązań, które można dopasować do wielkości przedsiębiorstwa czy też wytycznych dotyczących bezpieczeństwa druku.

Setting Lock
(Blokada Funkcji)

Setting Lock ogranicza dostęp do ustawień urządzenia poprzez panel kontrolny. Jest to idealne rozwiązanie dla organizacji, w których użytkownicy mają nieograniczony dostęp do funkcjonalności drukarki, ale administrator chce uniemożliwić nieautoryzowaną zmianę jej ustawień.

Secure Function Lock
(Blokada funkcjonalności)

Secure Function Lock to krok dalej na drodze do ograniczania dostępu do ustawień urządzenia oraz niektórych funkcji. Pozwala decydować administratorowi o uprawnieniach poszczególnych osób korzystających z drukarek.

Może na przykład określić, którzy użytkownicy mogą skanować dokumenty lub wysyłać faksy. Możliwe jest również ograniczenie funkcjonalności poprzez określenie, np. miesięcznych limitów stron do wydrukowania. Użytkownicy identyfikowani są za pomocą kodów PIN lub kart zbliżeniowych.

W następującym przykładzie:

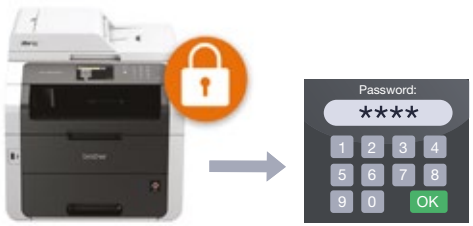
Użytkownik 1 może drukować, skanować, kopiować i faksować.

Użytkownik 2 nie może drukować i skanować.

Użytkownik 3 może tylko używać funkcji faksu.

Secure Print
(Bezpieczne drukowanie)

Funkcja stworzona z myślą o użytkownikach, którzy dokumenty poufne drukują dość rzadko. Secure Print umożliwia wstrzymanie polecenia druku do czasu, aż uprawniona osoba znajdzie się przy urządzeniu. Przy drukowaniu dokumentów poufnych użytkownik po prostu przypisuje kod PIN do danego zadania drukowania w sterowniku drukarki. Kod ten jest później wymagany do odblokowania urządzenia oraz wydrukowania zadania.



Secure Print+
(Bezpieczne drukowanie+)

Funkcja stworzona z myślą o osobach, które drukują dokumenty zawierające poufne dane sporadycznie. Secure Print+ pozwala na opóźnienie drukowania do momentu podejścia użytkownika do drukarki. Przy przetwarzaniu danych chronionych osoba uprawniona po prostu przypisuje kartę zbliżeniową do danego zadania drukowania w sterowniku drukarki. Zeskanowanie karty jest później wymagane do odblokowania urządzenia oraz wydrukowania zadania.

PrintSmart Secure Pro

Ta funkcja pozwala na przechowywanie dokumentów do drukowania na centralnym serwerze zamiast na urządzeniu. W związku z tym użytkownicy mogą odbierać zadania drukowania z dowolnego urządzenia w budynku, które jest podłączone do serwera PrintSmart Secure Pro.

Przed odebraniem zadania drukowania użytkownik musi wpisać swój kod PIN bądź zeskanować kartę zbliżeniową.

PrintSmart SecurePro Powered by b-guard

Active Directory Secure Print
(Uwierzytelnianie w oparciu o usługę Active Directory)

Active Directory Secure Print fizycznie uniemożliwia osobom nieupoważnionym korzystanie z jakichkolwiek funkcji drukarki. Chcąc odblokować urządzenie i pobrać wydrukowane dokumenty, użytkownik musi najpierw podać swoje dane uwierzytelniające (nazwę użytkownika i hasło). W usłudze tej zadanie drukowania przechowywane jest w wewnętrznej pamięci urządzenia do czasu jego odbioru.

Firma Brother udostępnia również funkcję bezpiecznego drukowania przy użyciu serwerów LDAP (Lightweight Directory Access Protocol). Działają one analogicznie do Active Directory Secure Print, ale uwierzytelnienie następuje przez protokół LDAP.

Przy korzystaniu z funkcji bezpiecznego drukowania po zalogowaniu do usługi Active Directory lub serwera LDAP, administrator może – jako dodatkowe zabezpieczenie – określić limit czasu, przez jaki nieodebrane zadania drukowania będą przetrzymywane w pamięci urządzenia.

3. Bezpieczne skanowanie

SSL / TLS Print

Nawet przy zastosowaniu wcześniej wspomnianych zabezpieczeń, należy pamiętać o jeszcze jednym niebezpieczeństwie związanym z procesem drukowania. Może się bowiem zdarzyć, że ktoś będzie próbował przechwycić Twoje dane w drodze do drukarki używając do tego celu wyspecjalizowanego oprogramowania. Aby temu zapobiec, urządzenia Brother zostały wyposażone w funkcję szyfrowania z użyciem protokołów TLS (Transport Layer Security) i SSL (Secure Socket Layer). Taka technologia jest stosowana w handlu elektronicznym w celu ochrony danych kart płatniczych i kredytowych. W ten sposób Twoje najbardziej poufne pliki mogą być szyfrowane podczas transmisji przez sieć przy użyciu klucza o długości 256 bitów.

Wyłączanie interfejsów

Urządzenia firmy Brother można skonfigurować tak, aby ograniczyć dostęp do poszczególnych funkcji poprzez wyłączenie wybranych interfejsów, np. wyłączenie USB do druku i skanowania bezpośredniego lub wyłączenie funkcji sieci bezprzewodowej.

Jakie są zagrożenia?

Nawet jeśli drukarka jest zabezpieczona, to istnieje jeszcze jedno potencjalne źródło wycieku danych: proces skanowania. Po zeskanowaniu poufnego dokumentu użytkownik ma do dyspozycji wiele opcji jego przechowywania lub udostępniania. Udostępnianie go przez e-mail lub umieszczanie w sieci, to ryzykowna strategia w przypadku poufnych danych. W relatywnie krótkim czasie może zostać odczytany przez osoby niepowołane. Ponadto, nie ma żadnych ograniczeń co do liczby skanów, które można wykonać.

W jaki sposób można temu zapobiegać?

Skanery, znajdujące się w urządzeniach Brother, posiadają kilka funkcji dzięki którym można skutecznie zabezpieczyć dokumenty.

Secure PDF
(Zabezpieczanie plików PDF)

Skanowane dokumenty można zabezpieczyć czterocyfrowym kodem PIN. Urządzenia wielofunkcyjne i skanery firmy Brother mogą automatycznie zabezpieczać każdy nowo zeskanowany plik PDF czterocyfrowym kodem PIN, aby nikt nie mógł go otworzyć bez zgody użytkownika.

Skanowanie do SFTP

Bezpieczny protokół transferu plików (SFTP - Secure File Transfer Protocol), zapewnia prywatny i bezpieczny przekaz danych. Poprzez kontrolę dostępu do serwera SFTP firma może przyczynić się do podniesienia bezpieczeństwa całej sieci.

4. Zabezpieczenie dostępu sieciowego

Jakie są zagrożenia?

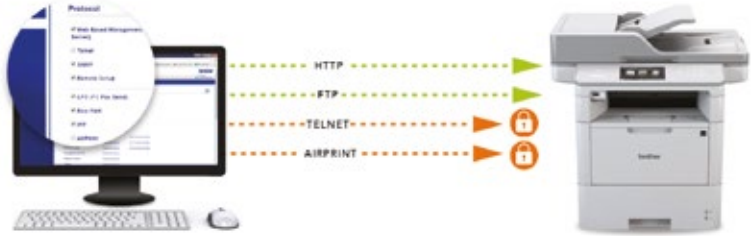
Standardową praktyką podczas łączenia się tabletu czy notebooka z zabezpieczoną siecią jest wymaganie certyfikatów, nazw użytkownika i haseł.
Nie oczekuje się tego na ogół od drukarek, chociaż ich podłączenie może stanowić równie duże zagrożenie dla bezpieczeństwa całej sieci.

W jaki sposób można temu zapobiegać?

Modele Brother mają wbudowaną obsługę szyfrowania różnego typu. Poniżej kilka sposobów na poprawienie bezpieczeństwa.

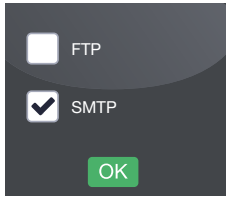
Filtr IP

Ta funkcja zapobiega dostępowi do plików przez sieć. Oznacza to, że urządzenia będą przyjmowały połączenia tylko od określonych adresów IP.



Kontrola protokołów

Ta funkcja pozwala administratorowi na wyłączenie niepotrzebnych protokołów, np. FTP lub SMTP.



802.1x

Urządzenia Brother odpowiadają bardzo wysokim standardom bezpieczeństwa określonym przez IEEE zgodnie z zasadami 802.1x, niezależnie od tego, czy są one podłączone przewodowo czy stanowią część infrastruktury bezprzewodowej.

IPsec

Wiele urządzeń Brother można podłączyć bezpośrednio do wewnętrznych lub zewnętrznych bezpiecznych środowisk za pomocą IPsec, oszczędzając czas oraz pieniądze.

Modele Brother mają wbudowaną obsługę protokołu IPsec, dlatego też nie ma potrzeby instalowania oprogramowania pośredniego, ani używania zewnętrznego sprzętu.

SNMPv3

Niektóre narzędzia do zarządzania flotą urządzeń, takie jak Brother BRAdmin, wykorzystują do komunikacji z urządzeniami protokół zwany SNMP. Modele Brother obsługują wersję SNMPv3, która umożliwia szyfrowaną komunikację.

Nawet jeśli organizacje nie używają programu Brother BRAdmin, lecz swojego własnego narzędzia do scentralizowanego zarządzania urządzeniami, drukarki Brother będzie można podłączyć do tego systemu szybko i tym samym łatwo.

Rekomendacje

Nie ulega wątpliwości, że firmy powinny zadbać o bezpieczeństwo swojego środowiska druku. Nie ma jednak jednego uniwersalnego rozwiązania dobrego dla wszystkich. Środki bezpieczeństwa powinny być dopasowane do istniejących potrzeb i zagrożeń w konkretnym środowisku.

Jeśli jednak w firmie:

1. **Chronione są urządzenia**
2. **Chronione są informacje w trakcie drukowania i po jego zakończeniu**
3. **Chroniona jest przed atakiem sieć**

to możemy mieć wówczas pewność, że procesy drukowania i skanowania są prawidłowo zabezpieczone przed potencjalnym zagrożeniem.

Źródło: Badanie przeprowadzone przez B2B International na zlecenie firmy Brother wśród 2502 firm w Wielkiej Brytanii, Francji, Niemczech i USA.

Źródło: Badanie przeprowadzone przez Quocirca w 2015 roku wśród 200 firm zatrudniających 1000 lub więcej pracowników i prowadzących działalność w Wielkiej Brytanii, Francji, Niemczech i USA.

Brother Central and Eastern Europe GmbH

Oddział w Polsce
ul. Cybernetyki 7b, 02-677 Warszawa

www.brother.pl