brother
at your side

# BIAŁA KSIĘGA BEZPIECZEŃSTWA BROTHER


Sierpień **2016**

## UKRYTE ZAGROŻENIA ZWIĄZANE Z FUNKCJONOWANIEM URZĄDZENIA DRUKUJĄCEGO (I JAK MOŻESZ IM ZARADZIĆ)

Funkcje drukarek i skanerów zarówno dla sektora biznesowego jak i publicznego są coraz lepiej dopasowane do zróżnicowanych potrzeb użytkowników i oferują coraz liczniejsze możliwości. Jednak wraz z nowymi możliwościami pojawiają się nowe wyzwania i w wielu firmach i instytucjach brakuje świadomości na temat zapewnienia systemom, sprzętowi i wrażliwym danym wystarczającej ochrony związanej z zarządzaniem drukiem.

Środki bezpieczeństwa w pracy stały się częścią naszego codziennego życia. Od kart identyfikacyjnych po oprogramowanie służące ochronie sieci i danych – do ochrony zasobów stosuje się wiele różnych rozwiązań. W dzisiejszych czasach nawet pomysł korzystania z konta e-mail niezabezpieczonego hasłem uznano by za lekkomyślny.

Wciąż jednak jest obszar, w którym wiele firm i instytucji jest szczególnie narażonych na ataki: jest to ochrona drukarek i skanerów – urządzeń także połączonych z siecią.

W przeprowadzonym w 2015 roku wśród 2,500 małych i średnich przedsiębiorstw badaniu firma Brother zapytała o najbardziej palące wyzwania, z jakimi się mierzą. Dla 75% ankietowanych przedsiębiorców najistotniejsze były kwestie bezpieczeństwa systemów informatycznych, a 59% wskazało na bezpieczeństwo informacyjne związane z procesem drukowania i zarządzaniem dokumentami.

Te kwestie i związane z tym obawy narastają i są odpowiedzią na szerokie spektrum problemów dotyczących bezpieczeństwa w różnych sektorach. Także w roku 2015 ośrodek Quocirca opublikował wyniki badania, w której ankietowano 200 przedsiębiorstw. Ujawniło ono, że sprawy bezpieczeństwa są dla respondentów kwestiami najistotniejszymi, a 75% uznało je za „bardzo ważne" (4,01 na 5). W 74% przedsiębiorstw wdrożono lub planowano wdrożyć rozwiązania w zakresie bezpieczeństwa procesów drukowania.

Jakiego typu są to zagrożenia? Zarówno jeśli chodzi o proces drukowania jak i skanowania, są cztery obszary krytyczne dla bezpieczeństwa firmy:

1. **Przypadkowy wyciek wydrukowanych już informacji**
2. **Przypadkowy wyciek informacji zeskanowanych**
3. **Atak na słabo zabezpieczoną lub niezabezpieczoną sieć**
4. **Fizyczny dostęp nieuprawnionego użytkownika do urządzenia**

Aby pomóc w eliminacji zagrożeń i podnieść świadomość osób administrujących systemami firma Brother opracowała analizę, w której wyszczególniona została specyfika zagrożeń i technologie, których działanie oparte jest na istniejącej infrastrukturze.

## 1. PRZYPADKOWY WYCIEK WYDRUKOWANYCH INFORMACJI

### Jakie niesie ryzyko?

Nie ma znaczenia, jak wiele mówi się o polityce bezpieczeństwa w Twojej firmie, jeśli przypadkowa, niepowołana osoba ma dostęp do drukarki, może zabrać wydruki i się z nimi oddalić. Jeśli może dojść do takiej sytuacji, Twoje poufne dokumenty przestają być poufne.

Większość stanowisk pracy nie znajduje się w bezpośredniej bliskości drukarki, dlatego istnieje wysokie ryzyko, że wydrukowane dokumenty będą narażone na ekspozycję dla osób trzecich.

### Jak można temu przeciwdziałać?

Aby przeciwdziałać efektywnie, należy odłożyć proces drukowania do momentu, w którym przy urządzeniu znajduje się uprawniony użytkownik. Uwierzytelnienie następuje przy pomocy numeru PIN lub czytnika kart identyfikacyjnych.

W zależności od wielkości przedsiębiorstwa i związanych z tym uwarunkowań dotyczących środowiska bezpieczeństwa, Brother posiada zdywersyfikowaną ofertę rozwiązań.

Funkcję **Secure Print** stworzono z myślą o osobach, które drukują dokumenty zawierające poufne dane sporadycznie. Secure Print umożliwia wstrzymanie polecenia druku do czasu, aż uprawniony użytkownik znajdzie się przy urządzeniu. Aby wydrukować dokumenty, potwierdza proces numerem PIN, który wcześniej wpisał zlecając drukowanie. Jeśli drukujesz dokumenty zawierające dane poufne częściej, Twoje oczekiwania spełni usługa **Active Directory Secure Print**. Blokuje ona dostęp do wszelkich funkcji drukarki nieautoryzowanym osobom. Do odblokowania drukarki i druku dokumentów możesz korzystać z posiadanego w Windows® Active Directory loginu i hasła. W obu przypadkach zlecenie wydruku jest wstrzymane w wewnętrznej pamięci urządzenia do momentu wprowadzenia hasła.

Funkcja Active Directory Secure Print może być wykorzystywana w środowisku, w którym korzysta się już z usługi Microsoft® Active Directory, ale tam, gdzie nie jest ona używana, Brother także zapewnia bezpieczne drukowanie przy użyciu serwerów z bazami danych użytkownika, obsługujące protokół LDAP.

Dla jeszcze doskonalszej ochrony administrator ma możliwość określenia limitów czasu przechowywania zadań wydruku w pamięci urządzenia. Dzięki temu poufne dokumenty nie zalegają w urządzeniu w nieskończoność.

W sytuacji, gdy różni użytkownicy mają różne zapotrzebowanie na drukowanie poufnych danych, najodpowiedniejsze będą usługi Brother oparte na sieci, np. PrintSmart Secure Pro, dzięki której dokumenty przechowywane są na głównym serwerze zamiast na urządzeniu. Użytkownicy mogą zlecać druk na każdym urządzeniu na terenie budynku, które jest połączone z serwerem PrintSmart Secure Pro uwierzytelniając się numerem PIN lub kartą identyfikacyjną, a administrator ma możliwość monitorowania tych procesów.

Nawet przy zastosowaniu powyższych środków, należy pamiętać o jeszcze jednym niebezpieczeństwie związanym z procesem drukowania. Może się zdarzyć, że przy wykorzystaniu odpowiedniego programu ktoś będzie próbował przechwycić Twoje dane w drodze do urządzenia. Aby je chronić urządzenia Brother mają wbudowaną obsługę protokołów szyfrowania TLS (Transport Layer Security) i SSL (Secure Socket Layer) – technologie używane w e-commerce dla bezpieczeństwa danych z kart płatniczych. Twoje poufne dane mogą być chronione podczas przesyłania przy użyciu 256-bitowego szyfrowania.

## 2. PRZYPADKOWY WYCIEK INFORMACJI ZESKANOWANYCH

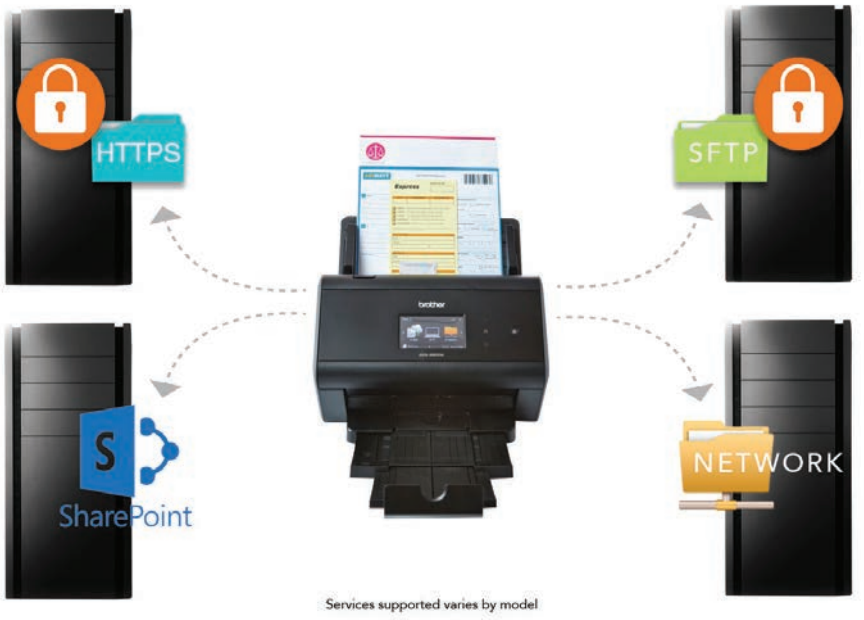
### Jakie niesie ryzyko?

Nawet jeśli Twoja drukarka jest chroniona przed wyciekiem informacji, niezabezpieczony może być proces skanowania dokumentów. Po zeskanowaniu dokumentu jest wiele możliwości zapisania go lub udostępnienia. Udostępnianie ich przez e-mail lub umieszczanie ich w sieci to ryzykowna strategia w przypadku poufnych danych, gdyż mogą je odczytać w relatywnie krótkim czasie osoby niepowołane. Nie ma też limitu kopii, które mogą być powielone na bazie jednego dokumentu.


### Jak można temu przeciwdziałać?

Najprostszym rozwiązaniem jest zapisanie zeskanowanego dokumentu w formacie pliku PDF chronionego dodatkowo numerem PIN. Urządzenia wielofunkcyjne oraz skanery Brother mogą automatycznie zabezpieczać każdy nowy plik PDF czterocyfrowym numerem PIN, dzięki czemu nikt nie może otworzyć dokumentu bez autoryzacji.

Używając skanerów lub urządzeń wielofunkcyjnych Brother możesz korzystać z usługi **Scan to FTP**, czyli skanowania do serwera SFTP (Secure File Transfer Protocol). Zapewnia on poufny i bezpieczny przesył danych; kontrolując dostęp do serwera SFTP użytkownik podnosi bezpieczeństwo sieci poprzez monitorowanie bramek systemu.



## 3. ATAK NA SŁABO ZABEZPIECZONĄ LUB NIEZABEZPIECZONĄ SIEĆ

### Jakie niesie ryzyko?

Loginy i hasła są standardowo wymagane w przypadku tabletów i laptopów, nie jest to jednak praktykowane w przypadku drukarek, mimo że jak urządzenia połączone z siecią, są narażone na podobne zagrożenia.

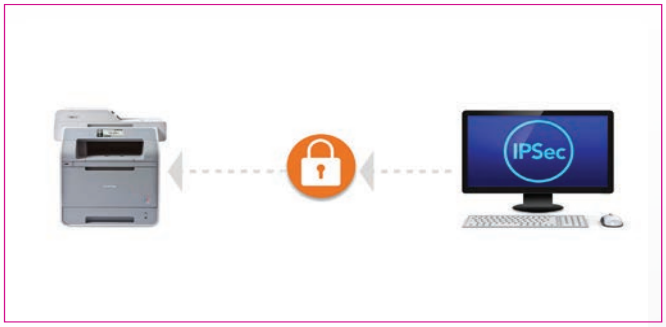
### Jak można temu przeciwdziałać?

### Standardy sieciowe

Jako że urządzenia mają wbudowaną obsługę szyfrowania różnych typów, Brother oferuje kilka sposób poprawienia bezpieczeństwa.

**802.1**x: urządzenia Brother spełniają rygorystyczne normy wyznaczone przez IEEE w ramach standardu 802.1x zarówno te połączone przewodowo jak i te będące częścią bezprzewodowej infrastruktury firmy.


**IPsec**: urządzenia wielofunkcyjne Brother mogą być przyłączone bezpośrednio do sieci wewnętrznej lub zewnętrznej bezpiecznie, dzięki IPsec, oszczędzając tym samym Twój czas, pieniądze i siły. Jako że funkcja IPsec jest już wbudowana na urządzeniach, nie ma potrzeby instalacji oprogramowania pośredniczącego lub używania sprzętu innych firm do uruchomienia usługi na posiadanym sprzęcie.




**SNMPv3**: Niektóre instrumenty zarządzania flotą drukarek, w tym usługa Brother BRAdmin wykorzystują protokół SNMP (Simple Network Management Protocol) do komunikacji z urządzeniami. Urządzenia Brother obsługują wersję 3 protokołu SNMP, która umożliwia komunikację chronioną szyfrowaniem podlegającym wymaganym w branży standardom.

Nawet w przypadku, gdy w firmie używany jest własny system zarządzania flotą drukarek zamiast usługi Brother BRAdmin, drukarki Brother można zaadaptować do istniejącego systemu szybko i łatwo.

## Rozwiązania zapewniające ochronę przed potencjalnym wewnętrznym zagrożeniom

Choć szyfrowanie zabezpiecza przed zagrożeniami zewnętrznymi, dostęp pracowników do połączonych z siecią drukarek również może być obarczony ryzykiem. Aby zapobiegać korzystaniu niezgodnemu z przeznaczeniem czy wprowadzaniu nieautoryzowanych zmian w ustawieniach drukarki, urządzenia Brother obsługują chronione hasłem wbudowane serwery internetowe.

Ponadto umożliwiają także filtrowanie **adresów IP**, dzięki czemu ograniczony zostaje dostęp do urządzenia z sieci, na przykład drukarka zaakceptuje połączenie tylko od użytkowników z adresów IP takich jak 10.45.12.1, 12.45.12.45, 10.45.12.46 i 10.45.12.47.

Mniej restrykcyjnym rozwiązaniem jest **Protocol Control** umożliwiający administratorowi wyłączenie niepotrzebnych protokołów bez blokowania dostępu do FTP czy SMTP.

Przykład poniżej pokazuje,  w jaki sposób administrator sieci uniemożliwił działanie następujących funkcji:  Telnet, AirPrint, Proxy i FTP Server.

## 4. FIZYCZNY DOSTĘP NIEUPRAWNIONEGO UŻYTKOWNIKA DO URZĄDZENIA

### Jakie niesie ryzyko?

Mimo wszystkich zabezpieczeń drukarki – o ile nie są zamknięte w oddzielnym, zabezpieczonym pomieszczeniu – mogą stać się obiektem ataku: osoby nieuprawnione mogą próbować pozyskać z nich dane. Dla małych i średnich przedsiębiorstw nieposiadających rozbudowanej infrastruktury IT pewne formy ochrony fizycznego dostępu do urządzeń są szczególnie istotne.

W raporcie Brother z roku 2010 dwie trzecie przedsiębiorców uznało zagadnienia związane z bezpieczeństwem informacji za mające wpływ na podejmowanie decyzji dotyczących zarządzania drukiem i dokumentami. Niepokój budziło zwłaszcza sposób przechowywania informacji na urządzeniach drukujących.

### Jak można temu przeciwdziałać?

Dla tych firm urządzenia Brother oferują szeroką gamę funkcji zabezpieczających urządzenie przed próbami włamania się do niego.

**Setting Lock** – założenie blokady – ograniczy dostęp do urządzenia z poziomu panelu sterowania. To wyjście idealne w firmach, gdzie nie jest oczekiwane ograniczenie funkcjonalności drukarki, ale pewność, że nieautoryzowani użytkownicy nie będą mieli do nich dostępu.

**Secure Function Lock** – to jeden krok dalej na drodze do ograniczenia dostępności funkcji urządzenia. Pozwala administratorowi decydować o tym, kto i z jakich funkcji może korzystać na określonym urządzeniu, na przykład, kto może faksować lub skanować. Może też decydować o wprowadzeniu miesięcznych limitów, dzięki unikalnym numerom PIN lub kartom identyfikacyjnym.

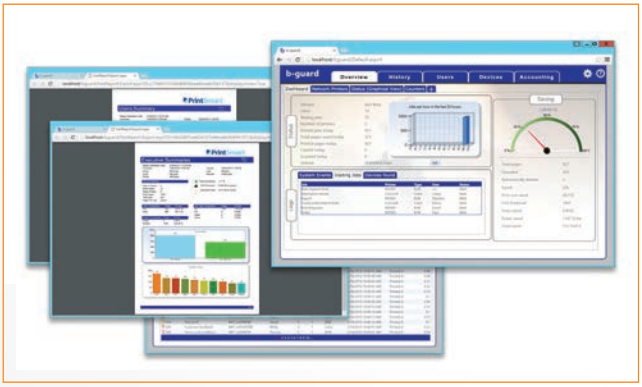
Ten przykład pokazuje sytuację, w której Dyrektor może korzystać z funkcji druku, skanowania, kopiowania i faksowania, Menadżer może drukować i skanować, a Asystent Menadżera może wysyłać faksy.

Można nie tylko blokować poszczególne funkcje, ale też ograniczyć to, w jaki sposób z funkcji się korzysta, na przykład, zamiast blokować funkcję drukowania, można ograniczyć liczbę drukowanych w miesiącu stron.


W przypadku, gdy urządzenie udostępnia się dużej liczbie użytkowników lub znajduje się ono w miejscu publicznym, kontrolowanie dostępu do niego może być trudne. Jednak dzięki funkcji Active Directory lub weryfikacji LDAP (Lightweight Directory Access Protocol) ,pracownicy mogą używać istniejących haseł sieciowych gdziekolwiek są, aby korzystać z określonej drukarki.

## CAŁY PAKIET

Tam, gdzie wymagana jest większa kontrola i potrzebna jest szczegółowa wiedza w kwestii sposobu korzystania z urządzeń, Brother oferuje usługę **PrintSmart Secure Pro**, innowacyjne i przystępne cenowo rozwiązanie, które podnosi bezpieczeństwo i efektywność, sprawia, że oszczędności stają się mierzalne, redukuje zużycie papieru chroniąc środowisko naturalne. Nieskomplikowany interfejs użytkownika pozwala administratorowi na większą kontrolę, prezentując dane dotyczące procesów druku w firmie, dając mu możliwość redukcji kosztów druku, dzięki monitorowaniu ich i zarządzaniu nimi.



## Korzystania z innych rozwiązań w zakresie druku

Rozwiązania w zakresie druku m.in. PaperCut, Ubiquitech i RingDal korzystały z **Brother Solutions Interface (BSI)** w celu zintegrowania własnych rozwiązań bezpiecznego drukowania z urządzeniami Brother.

BSI pozwala połączyć kwestie bezpieczeństwa, cykl pracy i rozwiązania w zakresie zarządzania i zintegrować je z urządzeniami Brother szybko i łatwo, przy zachowaniu kontroli nad UI (User Interface), funkcjami urządzenia i bezpieczeństwem. Dowiedz się więcej na: www.brother.eu/developers

## Rekomendacje:

Nie ma wątpliwości, że wiele firm i instytucji powinno zadbać o bezpieczeństwo sieci i danych w kontekście zagrożeń związanych z działaniem drukarek i skanerów. Nie ma jednego rozwiązania dla wszystkich, i w każdym środowisku powinny być one dopasowane do istniejących potrzeb i zagrożeń w tym zakresie. Jednak jeśli w firmie/instytucji:

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

…wtedy można mieć pewność, że zarówno procesy drukowania, jak i skanowania są prawidłowo zabezpieczone przed potencjalnymi zagrożeniami.

Źródło: Raport SMB Brother przeprowadzony przez B2B International na 2 502 firmach w Wielkiej Brytanii, Francji, Niemczech i w USA.
Źródło: Quocirca Managed Print Services Landscape, 2015. Sonda przeprowadzona w 200 organizacjach zatrudniających 1 000 i więcej pracowników w Wielkiej Brytanii, Francji, Niemczech i w USA