

Drukarka jako potencjalna luka w systemie. Jak chronić urządzenia wielofunkcyjne w firmie

W agencji kreatywnej zatrudniającej kilkanaście osób, ktoś przypadkiem znalazł we współdzielonej drukarce wydrukowany projekt nowej kampanii reklamowej. Nie byłoby w tym nic dziwnego, gdyby nie to, że dokument należał do konkurencyjnej firmy, z którą agencja wynajmowała przestrzeń coworkingową. Po weryfikacji okazało się, że urządzenie wielofunkcyjne zostało wcześniej kupione „na spółkę”, ale nikt nie zadbał o podstawowe zabezpieczenia. Hasło administratora pozostało domyślne, a panel zarządzania był dostępny z każdego komputera w sieci Wi-Fi. Co więcej, kolejka drukowania nie była czyszczona – można było ponownie wydrukować zapisane w pamięci urządzenia dokumenty lub też zapisać je w formacie PDF. Dopiero po tym incydencie obie firmy wprowadziły zabezpieczenia – zmieniono hasła, zablokowano dostęp do ustawień i rozpoczęto rejestrowanie aktywności. Sytuacja pokazała, że nawet zwykła drukarka biurowa, jeśli nie zostanie odpowiednio skonfigurowana, może stać się źródłem poważnego wycieku danych.

Drukarki i urządzenia wielofunkcyjne (MFP) to podstawowe elementy infrastruktury IT każdej firmy, które często są pomijane w planach bezpieczeństwa. Tymczasem nowoczesne drukarki mają dostęp do sieci, posiadają panele administracyjne, zapisują dane na wbudowanych dyskach i oferują zdalne zarządzanie. Ich błędna konfiguracja lub pozostawienie ustawień domyślnych może otworzyć drzwi do ataku lub wycieku danych.

Konfiguracja i kontrola dostępu do urządzeń wielofunkcyjnych

Aby zabezpieczyć tego typu sprzęt, należy przede wszystkim **zmienić domyślne hasła administracyjne**. Wiele urządzeń drukujących dostarczanych jest z domyślnym loginem i hasłem administratora, które są publicznie znane typu „admin” i łatwe hasła jak „1234”. Pozostawienie ustawień fabrycznych jest jedną z najczęstszych luk w bezpieczeństwie urządzeń biurowych. Wprowadzenie silnych, unikalnych haseł i ograniczenie dostępu administracyjnego tylko do uprawnionych osób to pierwszy krok do skutecznego zabezpieczenia urządzeń przed nieautoryzowanym dostępem i potencjalnymi atakami z sieci lokalnej lub zewnętrznej. Dzięki temu minimalizujemy ryzyko przejęcia kontroli nad drukarką, podglądu wydruków, zmiany ustawień lub wykorzystania jej jako furtki, przez którą atakujący uzyskają dostęp do infrastruktury IT firmy.

Drugim ważnym elementem jest **ograniczenie dostępu do panelu zarządzania**. Panel administracyjny drukarki powinien być dostępny wyłącznie dla administratorów IT z wybranych adresów IP lub zabezpieczony dodatkowymi hasłami. Należy zablokować dostęp z poziomu przeglądarki internetowej, jeśli nie jest on niezbędny. Zaleca się również rejestrowanie aktywności użytkowników korzystających z panelu i cykliczną analizę logów. Nieautoryzowany dostęp do panelu może pozwolić na zmianę ustawień lub kradzież danych w postaci plików przechowywanych w pamięci urządzeń.

Kolejnym krokiem powinno być **regularne czyszczenie historii wydruków i kolejki drukowania**. Niektóre urządzenia przechowują pliki tymczasowe nawet przez kilka dni lub tygodni. Jeżeli ich nie usuniemy, każdy użytkownik może ponownie wydrukować lub skopiować dokumenty przesłane do urządzenia, narażając firmę na ujawnienie poufnych informacji. Zalecane jest ustawienie automatycznego kasowania danych po wykonaniu zadania, unikanie drukowania

dużej liczby dokumentów „na zapas” oraz włączenie funkcji usuwania zadań po określonym czasie. Dane w buforze powinny być traktowane jako wrażliwe i chronione przed dostępem osób postronnych.

Istotną sprawą **jest szyfrowanie transmisji i druk poufny**. Aby chronić dane przesyłane do urządzeń drukujących należy włączyć szyfrowanie połączenia z drukarką (HTTPS, IPsec), korzystać z funkcji druku bezpośredniego z autoryzacją PIN lub kartą użytkownika. Szczególnie ważne jest to w firmach przetwarzających dane osobowe lub dane poufne.

Monitoring i ochrona danych drukowanych

Warto także **monitorować, rejestrować i analizować aktywność użytkowników**. Większość nowszych urządzeń umożliwia zapisywanie logów wydruków – z informacją kto, kiedy i z jakiego komputera zlecał zadania. W małych firmach wystarczą miesięczne raporty, w większych warto wdrożyć system zarządzania drukiem, który pozwala kontrolować liczbę wydruków i przeciwdziałać nadużyciom. Aby kontrolować bezpieczeństwo urządzeń drukujących należy:

- włączyć funkcję logowania zdarzeń (drukowane dokumenty, dostęp do panelu, zmiany konfiguracji),
- regularnie analizować logi – zwłaszcza pod kątem prób nieautoryzowanego dostępu,
- rozważyć centralne zarządzanie flotą urządzeń (Print Management Systems).

Monitoring pozwala wykryć nietypowe działania i zareagować, zanim dojdzie do incydentu.

Nie można zapominać o **kontroli dostępu sieciowego**. Drukarki pracujące w sieci LAN lub Wi-Fi powinny być odseparowane od sieci ogólnodostępnych, z silnym szyfrowaniem i zaporą sieciową. Należy zablokować dostęp z zewnątrz do portów administracyjnych oraz ograniczyć funkcje zdalne tylko do uprawnionych administratorów.

Podsumowując, choć drukarka kojarzy się z prostym urządzeniem biurowym, to w dobie cyfryzacji może być równie podatna na ataki i próby nadużyć co komputer czy telefon służbowy. Wystarczy chwila nieuwagi, by przez jedno niepozorne urządzenie doszło do poważnego incydentu bezpieczeństwa.

Najważniejsze zasady:

- Zmieniaj domyślne hasła i stosuj silne hasła do logowania.
- Ogranicz dostęp do panelu konfiguracji tylko do uprawnionych osób.
- Ustaw automatycznie usuwanie historii i plików tymczasowych po wykonaniu zadania.
- Rejestruj aktywność użytkowników i analizuj logi.
- Odseparuj drukarki od sieci publicznych i zabezpiecz ich interfejsy.

Checklista - bezpieczna konfiguracja urządzeń wielofunkcyjnych w firmie - pytania kontrolne

- Czy wszystkie drukarki mają zmienione fabryczne hasła administracyjne?
- Czy panel zarządzania jest dostępny tylko dla uprawnionych osób?
- Czy kolejka wydruków i historia są regularnie czyszczone?
- Czy działania użytkowników są rejestrowane i archiwizowane?
- Czy urządzenia są odseparowane od sieci ogólnodostępnych?
- Czy wyłączono nieużywane porty i funkcje zdalne?