**Nowoczesne drukarki na celowniku cyberprzestępców**

**Niewielu zdaje sobie sprawę z tego, że współczesne drukarki mogą zostać wykorzystane przez przestępców – na równi z innymi urządzeniami IoT – jako najsłabsze ogniwo w ochronie bezpieczeństwa sieciowego. Dlatego coraz częściej stają się celem ataków.**

W Internecie mamy tysiące zdalnie dostępnych drukarek. Niska świadomość społeczna dotycząca możliwości ich wykorzystania dla penetracji infrastruktury IT sprawia, że wiele z nich jest fatalnie zabezpieczona. Dane telemetryczne zebrane przez firmę Bitdefender – czołowego producenta oprogramowania antywirusowego – jednoznacznie wskazują na problem stosowania przez użytkowników drukarek bardzo słabych haseł chroniących przed nieautoryzowanym dostępem do tych urządzeń.

Warto pamiętać, że drukarki bardzo często wykorzystywane są do drukowania wrażliwych informacji, takich jak dane osobowe, finansowe, księgowe czy medyczne. Ponadto, przechwycenie ruchu sieciowego kierowanego do tych urządzeń pozwala przestępcom na zdobycie cennych informacji o firmie i jej pracownikach. Im więcej danych pozyskają, tym skuteczniejsze będą kolejne ataki wykorzystujące np. inżynierię społeczną, prowadzone w celu zinfiltrowania całej infrastruktury IT przedsiębiorstwa.

Słabe zabezpieczenia drukarek sieciowych umożliwiają również hakerom manipulowanie treścią wydruków. Przykład takiego ataku, polegający na podmianie dokumentu zleconego do druku na inny, został zaprezentowany na konferencji Black Hat 2017 i jest dostępny w postaci filmu pod adresem:

[https://www.youtube.com/watch?v=DwKzSO4yA\_s&ab\_channel=BlackHat](https://www.youtube.com/watch?v=DwKzSO4yA_s&amp;amp;ab_channel=BlackHat)

Słabe hasła i luki bezpieczeństwa w udostępnionych za pośrednictwem Internetu drukarkach, np. osobom zdalnie współpracującym z przedsiębiorstwem, mogą zostać wykorzystane przez przestępców jako furtka do sieci wewnętrznej. W efekcie atakujący otrzymuje dostęp do kolejnych urządzeń w sieci lokalnej, które – jeśli posiadają luki w zabezpieczeniach – zostają przejęte. W najgorszym przypadku przestępcy zyskają pełen wgląd i kontrolę nad Twoim ruchem sieciowym.

*Dla użytkowników korporacyjnych dostępne są sprzętowe rozwiązania monitorujące sieć pod kątem potencjalnego włamania. Od niedawna znajdują się one również w zasięgu tych użytkowników indywidualnych, którzy chcą chronić swoją sieć domową przed nieautoryzowanym dostępem. Ciekawą propozycją jest Bitdefender BOX, domowy router i punkt dostępowy WiFi wyposażony w sprzętowy firewall, technologię monitoringu (pod kątem zagrożeń) ruchu sieciowego oraz funkcję nadzorowania obecnych w Twoim domu urządzeń IoT (w tym drukarek) ze znanymi lukami oraz słabymi hasłami*, komentuje Dariusz Woźniak, inżynier techniczny Bitdefender z firmy Marken.