RAPORT

OTWARTE DRZWI

BADANIA POKAZUJĄ, ŻE DRUKARKI POZOSTAJĄ NARAŻONE NA CYBERATAKI

Zespoły informatyków skupiają się na innych punktach końcowych, zaniedbując bezpieczeństwo drukarek firmowych

Drukarki stanowią łatwe cele: zbyt wiele drukarek połączonych z siecią nie ma odpowiednich zabezpieczeń czy blokad.

Drukarki biznesowe stały się zaawansowanymi urządzeniami sieciowymi, podlegając tym samym zagrożeniom, co każdy inny punkt końcowy w sieci. Te zazwyczaj niezabezpieczone punkty dostępu stwarzają bardzo realne możliwości przeprowadzania cyberataków; mogą także dawać dostęp do danych finansowych i prywatnych firmy, co prowadzi do bardzo poważnych konsekwencji biznesowych.

Pomimo tego, ostatnia ankieta firmy Spiceworks, przeprowadzona wśród ponad 300 osób decyzyjnych z działów IT przedsiębiorstw, wykazała, że zaledwie 16% respondentów uważa, że drukarki podlegają wysokiemu ryzyku naruszenia zabezpieczeń — znacznie mniej niż w przypadku komputerów stacjonarnych/laptopów i urządzeń przenośnych.[1] Taki pogląd wpływa na sposób podejścia personelu IT do zabezpieczeń sieciowych. Tylko niecałe trzy na pięć firm stosuje odpowiednie praktyki w zakresie bezpieczeństwa drukarek — to znacznie mniej niż w przypadku innych punktów końcowych. Skutkiem jest podatność drukarek na zagrożenia w sytuacji, gdy istnieją rozwiązania chroniące te konkretne punkty dostępu do sieci.

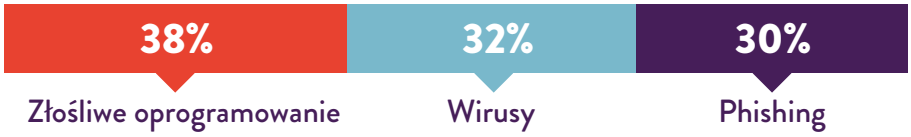
W niniejszym raporcie przedstawiono, oparte na wynikach ankiety Spiceworks, dane dotyczące bezpieczeństwa drukarek, skutki naruszenia zabezpieczeń oraz niektóre z wbudowanych, nowoczesnych zabezpieczeń chroniących przed cyberatakami.

ZALEDWIE 16% RESPONDENTÓW UWAŻA, ŻE DRUKARKI STANOWIĄ WYSOKIE RYZYKO DLA BEZPIECZEŃSTWA.[1]

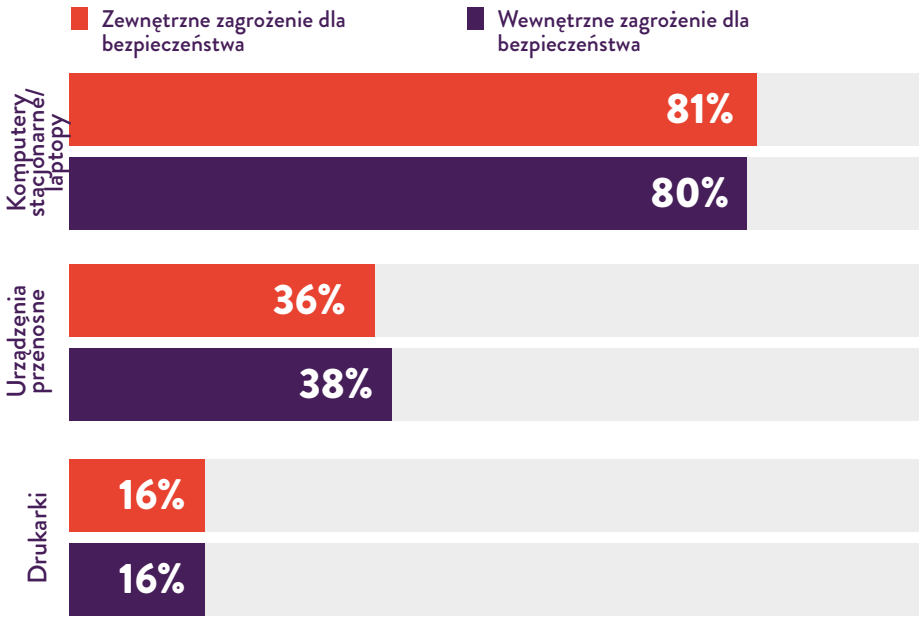
DROGI ATAKU

W ankiecie Spiceworks 74% respondentów stwierdziło, że w ich firmach w ubiegłym roku miały miejsce przypadki zewnętrznego zagrożenia lub naruszenia bezpieczeństwa IT. Natomiast u 70% wystąpiły przypadki wewnętrznego zagrożenia lub naruszenia bezpieczeństwa IT, wynikające najczęściej z błędów użytkowników oraz używania urządzeń osobistych albo sieci domowych czy publicznych do celów służbowych.[1]

CZOŁOWE ZEWNĘTRZNE ZAGROŻENIA DLA BEZPIECZEŃSTWA IT



Główne zagrożenia znajdowały drogę dostępu przez komputery stacjonarne i laptopy, natomiast inne przez urządzenia przenośne i drukarki.[1] (16% w przypadku drukarek to znacznie więcej w porównaniu z 4% z podobnego badania Spiceworks z roku 2014.) Możliwe jest także, że liczba ataków przeprowadzanych za pośrednictwem drukarek jest zaniżona, ponieważ drukarki nie są tak ściśle monitorowane jak komputery i urządzenia przenośne.



LEKCEWAŻYMY NASZE DRUKARKI

W każdym przypadku ankieta Spiceworks pokazuje, że bezpieczeństwo drukarek jest często zaniedbywane.

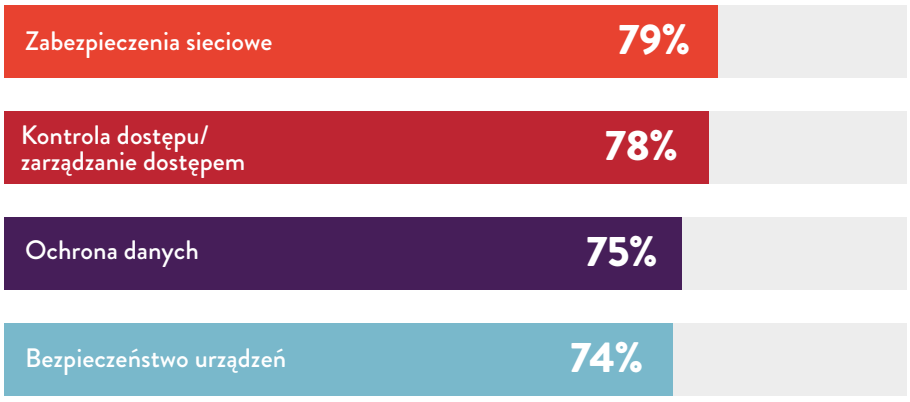
Firmy doskonale zdają sobie sprawę ze znaczenia zabezpieczeń sieci, punktów końcowych i danych. Ponad trzy czwarte respondentów stosuje zabezpieczenia sieciowe, systemy kontroli dostępu/zarządzania dostępem, systemy ochrony danych lub zabezpieczenia punktów końcowych — albo ich kombinację.[1]

Jednakże takie rozwiązania są stosowane dużo rzadziej w przypadku drukarek. 83% respondentów stosuje zabezpieczenia sieciowe w komputerach stacjonarnych/laptopach, 55% w urządzeniach przenośnych i tylko 41% w drukarkach.[1]

Taka dysproporcja jest jeszcze większa w przypadku zabezpieczeń punktów końcowych:

Ponadto mniej niż jedna trzecia (28%) respondentów wdraża certyfikaty zabezpieczeń dla drukarek, podczas gdy 79% z nich stosuje takie zabezpieczenia w przypadku komputerów i 54% w przypadku urządzeń przenośnych.[1]

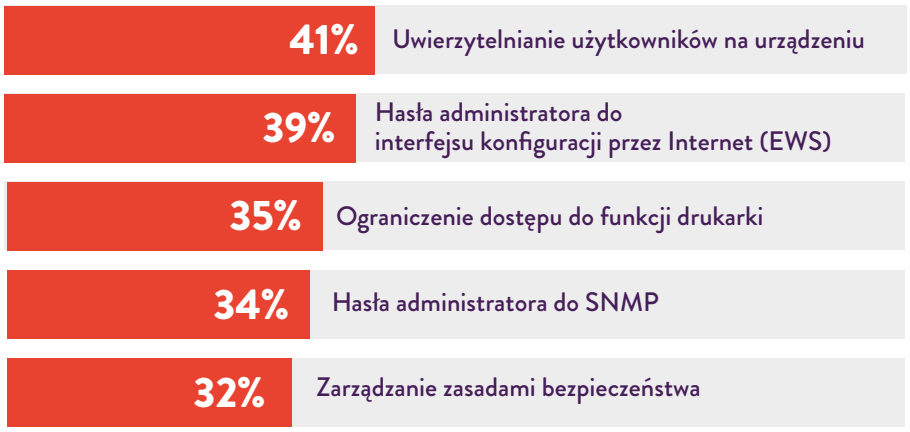
GŁÓWNE PRAKTYKI ZABEZPIECZENIA PUNKTÓW KOŃCOWYCH



Wśród zabezpieczeń stosowanych do ogólnych urządzeń, w przypadku drukarek najczęściej były to zabezpieczenia dokumentów, sieci i kontrola dostępu, jednak mniej niż połowa respondentów stwierdziła, że w ich firmach stosuje się je do drukarek.[1]

Niektóre firmy stosują pewne praktyki zabezpieczenia drukarek, jednak nawet u nich są one bardzo zróżnicowane. Tylko nieco ponad 40% firm wdrożyło uwierzytelnianie użytkowników, a mniej niż 40% stosuje hasła administratora do interfejsu konfiguracji przez Internet.[1] Aby zapewnić silną ochronę, każda firma powinna stosować kombinację wszystkich tych i innych metod.

GŁÓWNE PRAKTYKI ZABEZPIECZENIA DRUKAREK



Jeśli chodzi o praktyki w zakresie zgodności i audytu punktów końcowych, drukarki pozostają w tyle za niemal wszystkimi innymi punktami końcowymi. Niemal 90% firm wdrożyło zasady bezpieczeństwa informacji, które jednak zazwyczaj nie obejmują drukarek. Na przykład 57% respondentów wdrożyło zabezpieczenia przed złośliwym oprogramowaniem na komputerach, ale tylko 17% na drukarkach.[1]

NIEMAL 9 NA 10 SPECJALISTÓW IT TWIERDZI, ŻE ICH FIRMY WDROŻYŁY ZASADY BEZPIECZEŃSTWA INFORMACJI Z NASTĘPUJĄCYCH POWODÓW:

Najwyraźniej firmy nie traktują zabezpieczeń drukarek dostatecznie poważnie — a z pewnością powinny.

„Wiele drukarek nadal ma domyślne hasła lub w ogóle ich nie ma, albo dziesięć drukarek ma takie same hasła" — stwierdził Michael Howard, główny doradca firmy HP ds. bezpieczeństwa, w czerwcowym wydaniu Computerworld. „Drukarka niezabezpieczona hasłem to skarb dla hakera. Jedno z często spotykanych zagrożeń to atak „na pośrednika", polegający na przejęciu drukarki i przekierowywaniu [przychodzących dokumentów] na laptopa przed wydrukowaniem. Haker widzi wszystko, co drukuje dany dyrektor firmy".[2]

POTENCJALNE SKUTKI WŁAMAŃ DO DRUKAREK

Według starszego analityka e-zagrożeń w firmie Bitdefender Bogdana Botezatu, drukarki stanowią wymierną, potencjalną lukę w zabezpieczeniach. „W naszych pracowniach oceny zagrożeń w znacznym stopniu korzystamy z telemetrii. Router już nie jest najgorszym urządzeniem w Internecie. Obecnie jest to drukarka".[3]

Ten słaby punkt może być przyczyną poważnych konsekwencji dla firmy. Jedna niezabezpieczona drukarka może narażać na atak całą sieć połączonych urządzeń, dając hakerom możliwość szpiegowania urządzeń sieciowych i naruszając bezpieczeństwo całej sieci.

1. Większa liczba połączeń z help deskiem i czas poświęcony na pomoc techniczną

2. Obniżona wydajność/efektywność

3. Dłuższy czas przestoju systemów

4. Dłuższy czas połączeń z pomocą techniczną

5. Większa potrzeba egzekwowania zasad przez użytkowników

Wszyscy znamy skutki naruszenia bezpieczeństwa. W ankiecie Spiceworks respondenci wymienili pięć głównych skutków naruszeń[1]

Ale naruszenie zabezpieczeń drukarki może mieć jeszcze poważniejsze konsekwencje, zwłaszcza jeśli jest to urządzenie wielofunkcyjne z możliwością przechowywania drukowanych danych w postaci elektronicznej.

Zadania drukowania przechowywane w pamięci podręcznej drukarki umożliwiają hakerom dostęp do poufnych informacji osobistych lub służbowych.

Jeszcze bardziej niepokoi fakt, że poprzez niezabezpieczoną drukarkę hakerzy mogą uzyskać dostęp do szerszej sieci firmowej, wykradając takie dane jak numery ubezpieczenia społecznego, dane finansowe lub notatki i dokumenty wewnętrzne. Kradzież takich informacji może mieć skutki nie tylko dla pojedynczych pracowników, lecz także przynieść korzyść konkurencji lub źle wpłynąć na reputację firmy.

PROSTE ROZWIĄZANIE: WBUDOWANE ZABEZPIECZENIA

Firmy z pewnością muszą zadbać o bezpieczeństwo drukarek. Niektóre z dzisiejszych nowoczesnych drukarek klasy enterprise posiadają wbudowane, łatwe w obsłudze zabezpieczenia, które przeciwstawiają się zagrożeniom typowym dla drukarek. Są to:

- Automatyczne wykrywanie ataków, ochrona przed atakami i usuwanie ich skutków
- Monitorowanie użycia dla ochrony przed nieautoryzowanym użyciem
- Opcje prostego logowania, takie jak kody PIN czy karty elektroniczne
- Zbliżeniowy czytnik kart pozwalający na szybkie uwierzytelnianie użytkowników i bezpieczne drukowanie na drukarce przy użyciu identyfikatorów
- Bezpieczne drukowanie z szyfrowaniem w przypadku poufnych dokumentów

Jeśli rozważasz zakup kolejnej drukarki — biurkowej czy wielofunkcyjnej — sprawdź jej wbudowane zabezpieczenia i pamiętaj o ich aktywacji. Za pomocą prostych funkcji właściwych dla drukarek można wyeliminować zagrożenia kierowane właśnie przez nie; wszak w dzisiejszym Internecie jest wiele potencjalnych punktów dostępu dla hakerów — **drukarki nie muszą być jednym z nich.**

POSZUKUJESZ BEZPIECZNIEJSZYCH DRUKAREK?
WIĘCEJ INFORMACJI ›

Źródła:

[1] Przeprowadzona na zlecenie HP ankieta firmy Spiceworks wśród 309 osób decyzyjnych w dziedzinie IT w regionach Ameryki Północnej, EMEA i APAC, listopad 2016 r.

[2] „Printer Security: Is your company's data really safe?" Computerworld, 1 czerwca 2016 r. http://www.computerworld.com/article/3074902/security/printer-security-is-your-companys-data-really-safe.html

[3] „Printers Now the Least-secure Things on the Internet", The Register, 8 września 2016 r. http://www.theregister.co.uk/2016/09/08/the_least_secure_things_on_the_internet/