Dlaczego każda firma potrzebuje inteligentnej strategii w zakresie usług druku?

Wszystkie firmy potrzebują strategii usług druku zapewniającej bezpieczeństwo i wydajność. Doradcy HP ds. bezpieczeństwa druku, Jason O'Keefe i Micahel Howard, tłumaczą, dlaczego strategia ta odgrywa tak ważną rolę.

Dowiedz się więcej

„Większość firm nie uważa, że zabezpieczenie floty urządzeń drukujących jest konieczne i bagatelizuje bezpieczeństwo druku"

Jason O'Keefe, HP Print Security Advisor

Drukarki sieciowe wiążą się ze znacznym ryzykiem, z czego większość organizacji nie zdaje sobie sprawy. W świetle rosnących i niezwykle poważnych zagrożeń dla bezpieczeństwa, przedsiębiorstwa potrzebują strategii w zakresie usług druku, aby chronić organizację i minimalizować ryzyko. W przypadku wielu firm opracowanie rzetelnej strategii wymaga współpracy z dostawcą usług MPS, który zidentyfikuje i załata luki w systemie bezpieczeństwa, a także zajmie się innymi kwestiami (np. konserwacją urządzeń), dzięki czemu problemy z drukowaniem nigdy nie staną na drodze do produktywności.

Rozwiązywanie problemów z bezpieczeństwem drukarek

W ankiecie przeprowadzonej przez Ponemon Institute wśród ponad 2000 specjalistów ds. bezpieczeństwa IT z całego świata 60% respondentów przyznało, że prawdopodobnie doszło do naruszenia danych przy użyciu drukarki sieciowej, a większość ankietowanych przewiduje, że w kolejnych 12 miesiącach dojdzie do naruszenia danych, wynikającego z niezabezpieczonych drukarek sieciowych.

Tylko 34% ankietowanych twierdzi, że w ich organizacji wdrożono procedury ograniczania dostępu do drukarek narażonych na wysokie ryzyko, obejmujące również dokumenty papierowe. Te wyraźne luki w systemie bezpieczeństwa narażają firmy, szczególnie małe i średnie przedsiębiorstwa, na ataki, które mogą być kosztowne w najlepszym przypadku, a w najgorszym – opłakane w skutkach.

Jason O'Keefe, specjalista HP ds. bezpieczeństwa drukarek, tłumaczy, że większość organizacji nie zdaje sobie sprawy, jak bardzo są narażone na ataki poprzez ich infrastrukturę drukarek. „Większość firm nie uważa, że zabezpieczenie floty urządzeń drukujących jest konieczne i bagatelizuje bezpieczeństwo druku", powiedział. „Przedstawiamy im nasz model zawierający ponad 200 punktów kontrolnych, które oceniamy pod kątem narażenia infrastruktury drukarek na ataki. Wówczas firmy zupełnie zmieniają podejście do sprawy. Sceptycyzm zamienia się w niedowierzanie i szok. Możemy wtedy przeprowadzić bardzo szczerą i żywą rozmowę".

Pierwszym krokiem na drodze do dobrej strategii bezpieczeństwa druku jest ocena zagrożeń. Według Michaela Howarda, dyrektora HP ds. bezpieczeństwa, większość zagrożeń związanych z drukarkami sprowadza się do czterech czynników: przestarzała technologia; brak odpowiednio wdrożonych środków bezpieczeństwa; różnorodne środowiska dostawców; oraz niezarządzane środowiska druku.

Czy wiesz, że w przeciętnej organizacji z jednej drukarki korzysta około sześciu użytkowników? Podczas gdy komputery i laptopy są chronione hasłem, drukarki nie przestrzegają tych samych standardów, w wyniku czego dane każdego z sześciu użytkowników są zagrożone. „Wiele zespołów ds. bezpieczeństwa nie wiedziało, ile drukarek jest używanych w biurze. W firmie może być 5000 urządzeń, z których żadne nie jest zabezpieczone", powiedział Howard. „Jeśli pomyśleć, jak często drukuje się dokumenty w większości firmach, brak proaktywnego podejścia do bezpieczeństwa jest zaskakujący i przerażający".

Dlaczego każda firma potrzebuje inteligentnej strategii w zakresie usług druku?

Dlaczego strategie dotyczące usług druku mają znaczenie?

Inteligentna strategia drukowania zabezpiecza drukarki (tak samo jak komputery), ogranicza dostęp do funkcji administracyjnych, wdraża wytyczne dotyczące nazw użytkowników i haseł oraz umożliwia nadzór. To klucz do zapewnienia przejrzystości, wykrywalności i odpowiedzialności.

„Przejrzystość to podstawa", powiedział O'Keefe. Skuteczna strategia drukowania powinna również uwzględniać współpracę. Aby pozyskać cenne informacje niezbędne do wdrożenia niezawodnego systemu bezpieczeństwa, firmy muszą znieść bariery między administratorami drukarek, specjalistami ds. bezpieczeństwa i wewnętrznym personelem ds. audytów. Te grupy pracowników muszą być gotowe do współpracy w celu zabezpieczenia ważnej części sieci, która od tak wielu lat jest pomijana".

Organizacje mogą też ograniczyć ryzyko związane z drukowaniem poprzez:

- Stałe aktualizowanie oprogramowania sprzętowego,
- Ograniczanie administracji w zakresie infrastruktury drukowania,
- Ulepszenie baz danych drukowania z wersji Express do Enterprise,
- Wdrożenie procedur i wytycznych, które pozwolą zadbać o spójność i wymierność bezpieczeństwa,
- Organizowanie szkoleń z zakresu bezpieczeństwa dla administratorów drukarek.

„Podobnie jak bezpieczeństwo w firmie, bezpieczeństwo drukarek to proces nieustannych zmian", powiedział Howard. „Należy dążyć do ciągłego doskonalenia poprzez analizy i konsultacje ze specjalistami". Wnikliwe, stałe analizy są związane z zarządzaniem. W przypadku drukowania zarządzanie powinno obejmować zarządzanie kontami użytkowników (kto ma dostęp do infrastruktury drukarek), zgodność z zasadami firmy, zarządzanie ryzykiem, dokumentację dot. bezpieczeństwa oraz rejestrowanie zdarzeń.

Zarządzane czy niezarządzane – oto jest pytanie

Rzetelna strategia musi zawierać wiele elementów. W przypadku większości przedsiębiorstw, szczególnie małych i średnich , opracowanie i wdrożenie takiej strategii po prostu nie jest wykonalne. Wolą one poświęcić czas i energię na prowadzenie interesów. Optymalnym rozwiązaniem jest współpraca z dostawcami usług MPS, którzy zatroszczą się o wszelkie szczegóły i zapewnią poziom bezpieczeństwa niezbędny do bezproblemowej pracy.

Pierwszym krokiem na drodze do inteligentnej strategii drukowania jest zadawanie pytań. Przede wszystkim jakie drukarki są właściwe dla naszej organizacji? Czy powinniśmy korzystać z drukarek atramentowych, czy laserowych? Jakich funkcji drukowania potrzebujemy? Odpowiadając na te pytania, należy dążyć do równowagi między niezawodnością, kosztem i wydajnością. Następnie firmy powinny zastanowić się nad bezpieczeństwem, konserwacją i wsparciem. Czy chcemy zarządzać drukarkami wewnętrznie, czy korzystać z usług zewnętrznego dostawcy? To pytanie prowadzi do innych, takich jak: Czy nasz zespół IT jest przygotowany na problemy z drukarkami? Czy w dalszej perspektywie obsługa drukowania wewnątrz firmy będzie droższa? W przypadku małych przedsiębiorstw, odpowiedź często jest twierdząca.

Firmy, które zdecydują się na usługi zarządzania drukiem, powinny zastanowić się, kiedy i z którym dostawcą zawrzeć umowę. Wymaga to odpowiedzenia na pytania takie jak: Jakich usług potrzebujemy? Co zawiera umowa gwarancji jakości świadczonych usług? Ile to kosztuje? Jak szybko planujemy rozwój sieci drukarek? Czy w miarę rozwoju nasza strategia drukowania będzie wymagała zmiany?

Zagrożenia związane z niezabezpieczonymi drukarkami sieciowymi są oczywiste, a firmy, niezależnie od wielkości, muszą uwzględnić usługi druku w ogólnym podejściu do strategii i produktywności. Na szczęście istnieją dostawcy, którzy pomogą w tym zakresie.

„Podobnie jak bezpieczeństwo w firmie, bezpieczeństwo drukarek to proces nieustannych zmian"

Jason O'Keefe,
HP Print Security Advisor

Dowiedz się więcej
hp.com

4AA7-1720PLE, Listopad 2017