Dokument techniczny

Spełnianie wymogów dotyczących zgodności w zakresie bezpieczeństwa sieci i danych

Zalecenia dotyczące bezpieczeństwa floty urządzeń drukujących

Spis treści

Niezgodność z przepisami może mieć szkodliwe skutki dla firmy

Oprócz wysokich kar i kosztownych pozwów sądowych naruszenie bezpieczeństwa może spowodować utratę przychodów i negatywnie wpłynąć na renomę przedsiębiorstwa. Opracowując plan zabezpieczeń, należy pamiętać, że miarą bezpieczeństwa całej sieci jest bezpieczeństwo najsłabszego ogniwa. Urządzenia drukujące, podobnie jak komputery, są narażone na wiele zagrożeń bezpieczeństwa. Dlatego też niezwykle ważne jest wdrożenie urządzeń i rozwiązań, które spełniają wymogi dotyczące zgodności z przepisami oraz ochronią informacje firmy przed zagrożeniami.

O jakich zagrożeniach mowa?

Nieprzestrzeganie wymogów i przepisów prawnych prowadzi do ogromnych strat finansowych wśród organizacji z całego globu; obejmuje kary pieniężne, utraty transakcji, nadszarpnięcie reputacji oraz postępowania sądowe z powództwa zbiorowego.

Brak lub niewystarczająca ochrona urządzeń to więcej okazji dla cyberprzestępców. Przeprowadzone niedawno przez instytut Ponemon badania na wybranych organizacjach wykazały, że w 2016 r. doświadczyły one średnio dwóch ataków na tydzień (co stanowi 23-procentowy wzrost w skali roku), tracąc tym samym 9,5 mln USD rocznie na walkę z cyberprzestępstwami[1]. Tylko w zeszłym roku na całym świecie zostały naruszone 4 miliardy zapisów danych, co stanowi 400-procentowy wzrost w stosunku do dwóch poprzednich lat[2].

Mimo że wiele działów IT rygorystycznie stosuje środki bezpieczeństwa, zarówno w stosunku do pojedynczych komputerów, jak i całej sieci, urządzenia drukujące są często pomijane. Drukarki natomiast mogą stanowić punkt dostępu do sieci i zabezpieczenie ich jest równie ważne. 26% wszystkich znaczących naruszeń bezpieczeństwa danych zgłaszanych przez menedżerów IT miało związek z drukarkami[3].

Aby przeciwdziałać rosnącemu zagrożeniu, organy rządowe z całego świata wdrażają surowe przepisy bezpieczeństwa, które wymuszają na organizacjach lepszą ochronę danych klienta. Na przykład nowe unijne ogólne rozporządzenie o ochronie danych (GDPR) to jedna z kluczowych ustaw, które wejdą w życie w 2018 r. GDPR zaostrza wymagania dotyczące nacisku, jaki firmy będą musiały kłaść na ochronę danych. Dlatego też należy się upewnić, że każde urządzenie podłączone do sieci – od komputerów przez drukarki aż po urządzenia mobilne – jest właściwie zabezpieczone. Nowe rozporządzenie wpłynie nie tylko na kraje Unii Europejskiej – firmy z całego świata będą musiały spełniać te wymogi, jeśli gromadzą i przetwarzają dane mieszkańców UE. Organizacje będą musiały monitorować każde urządzenie, tak aby zgłaszać przypadki naruszenia bezpieczeństwa w ciągu 72 godzin od momentu ich wykrycia. Jeśli kontrola zgodności wykaże, że monitoring nie był prowadzony lub nie zgłoszono włamania, firma może zapłacić karę w wysokości maks. 20 mln Euro lub 4% rocznych obrotów.

Wykorzystanie popularnych środków kontroli bezpieczeństwa w celu poprawy zgodności

Pozostawanie na bieżąco z branżowymi przepisami i regulacjami stanowi poważne wyzwanie. Na szczęście Centrum Bezpieczeństwa w Internecie (ang. Center for Internet Security, CIS) opracowało zestaw ogólnych środków bezpieczeństwa w celu uproszczenia zaleceń z zakresu cyberbezpieczeństwa. Krytyczne środki bezpieczeństwa według CIS to 20 działań, które mogą pomóc w powstrzymaniu cyberataków (szczegóły pod adresem https://www.cisecurity.org/critical-controls.cfm). Zalecane środki są zgodne z wieloma innymi regulacjami branżowymi, takimi jak PCI-DSS, ISO 27001, zalecenia US CERT, HIPAA, FFIEC oraz NIST. Środki te nie mają na celu zastąpienia innych zabezpieczeń, ale są często stosowane przez przedsiębiorstwa w celu ich uzupełnienia.

Krytyczne środki bezpieczeństwa według CIS to przede wszystkim mniejsza liczba działań, które zapewniają skuteczniejsze rezultaty. Odpowiadają one najczęstszym schematom ataków zgłaszanym w wiodących raportach dotyczących zagrożeń. W ich opracowaniu pomagało szerokie grono ekspertów branżowych – w tym specjaliści kryminalistyki i grupy reagowania na incydenty. Ponadto lista środków jest stale aktualizowana na podstawie zmieniających się zagrożeń i ataków.

Krytyczne środki bezpieczeństwa CIS pomagają w opracowaniu planu działania i spełnieniu wymogów regulacyjnych w zakresie bezpieczeństwa. Niniejszy dokument prezentuje sugerowane działania w ramach każdego z 20 środków z listy w celu zabezpieczenia urządzeń drukujących, danych i dokumentów w ramach szerszego planu zabezpieczeń. Kontrole 4, 6, 8, 12, 13 i 15 stawiają szczególny nacisk na ochronę danych i monitoring aktywności związanych z wymogami GDPR.

Krytyczne środki bezpieczeństwa CIS i zalecane działania

Środek nr 1: inwentaryzacja urządzeń autoryzowanych i nieautoryzowanych

Działania – aktywne zarządzanie (inwentaryzacja, monitorowanie i korygowanie) wszystkimi urządzeniami działającymi w sieci, tak aby dostęp do niej miał wyłącznie sprzęt autoryzowany; identyfikacja i uniemożliwienie dostępu dla urządzeń nieautoryzowanych, pozostających bez kontroli.

Zalecenie – należy upewnić się, że wszystkie urządzenia drukujące w sieci zostały zidentyfikowane i są aktywnie zarządzane w celu uzyskania zgodności z zasadami bezpieczeństwa obowiązującymi w firmie. Skuteczne narzędzie do zarządzania bezpieczeństwem druku może zapewnić widoczność wszystkich urządzeń podłączonych do sieci oraz komputerów stacjonarnych.

Środek nr 2: inwentaryzacja autoryzowanego i nieautoryzowanego oprogramowania

Działanie – aktywne zarządzanie (inwentaryzacja, monitorowanie i korygowanie) wszystkimi elementami oprogramowania w sieci, tak aby umożliwić instalowanie i obsługę wyłącznie autoryzowanego oprogramowania; identyfikacja i zapobieganie instalowaniu oraz korzystaniu z nieautoryzowanego oprogramowania pozostającego poza kontrolą.

Zalecenie – należy upewnić się, że wszelkie oprogramowanie wbudowane i inne rozwiązania zainstalowane w urządzeniach drukujących są aktualne, posiadają certyfikaty oraz potwierdzoną oryginalność. Należy wybierać urządzenia drukujące z wbudowaną ochroną systemu BIOS i oprogramowania wbudowanego, tak aby mieć pewność, że wczytywany jest tylko autentyczny kod. W przypadku flot, w ramach których zastosowano rozwiązania do zarządzania flotą urządzeń drukujących, możliwe jest ustawienie proaktywnych aktualizacji oprogramowania wbudowanego. Oprogramowanie (zarówno na serwerach, jak i na urządzeniach klienta) powinno posiadać odpowiednie podpisy oraz potwierdzoną autentyczność.

Środek nr 3: bezpieczna konfiguracja sprzętu i oprogramowania w urządzeniach przenośnych, laptopach, stacjach roboczych oraz na serwerach

Działanie – opracowanie, wdrożenie i aktywne zarządzanie (monitorowanie, raporty i działania korekcyjne) konfiguracją zabezpieczeń laptopów, serwerów i stacji roboczych poprzez stosowanie rygorystycznych standardów zarządzania konfiguracją oraz zmianę procesu kontroli w celu ochrony przed wykorzystaniem wrażliwych usług i ustawień przez niepożądane osoby.

Zalecenie – podobnie jak inne punkty końcowe sieci, drukarki powinny posiadać bezpieczną konfigurację. Należy opracować i wdrożyć zasady bezpieczeństwa obowiązujące wszystkie urządzenia drukujące oraz aktywnie eliminować wszelkie odstępstwa od tych zasad. Listy kontrolne dotyczące bezpieczeństwa (takie jak NIST) lub usługi doradztwa w zakresie zabezpieczeń mogą pomóc w opracowaniu i wdrożeniu kompleksowych zasad bezpieczeństwa druku. Skuteczne narzędzie do zarządzania bezpieczeństwem druku może zautomatyzować proces tworzenia, wdrażania i oceny zasad oraz korekty ustawień urządzeń w ramach całej floty. Urządzenia wielofunkcyjne dla przedsiębiorstw są wyposażone w ponad 250 ustawień zabezpieczeń, dlatego też automatyzacja tego procesu może zapewnić duże oszczędności czasu.

Środek nr 4: ciągła ocena słabych punktów i ich eliminacja

Działanie – ciągłe gromadzenie danych, ocena i podejmowanie działań w związku z nowymi informacjami, tak aby zidentyfikować słabe punkty oraz wyeliminować lub zminimalizować możliwości dostępu osób niepożądanych.

Zalecenie – narzędzia typu Security Information and Event Management (SIEM), takie jak ArcSight, Splunk czy SIEMonster, mogą monitorować aktywność w sieci w czasie rzeczywistym i informować administratorów o wystąpieniu incydentów. Monitorowanie urządzeń drukujących jest równie ważne jak kontrola komputerów stacjonarnych – warto upewnić się, że drukarki posiadają możliwość przesyłania komunikatów syslog do narzędzia SIEM.

Warto wybierać drukarki z funkcjami umożliwiającymi wykrywanie ataków w czasie rzeczywistym z automatycznym przywracaniem funkcjonalności, tak aby maksymalizować czas nieprzerwanej pracy urządzeń przy minimalizacji interwencji informatyków.

W zmniejszeniu podatności na ataki pomoże narzędzie do zarządzania bezpieczeństwem floty, które identyfikuje nowe drukarki i automatycznie stosuje ustawienia zasad bezpieczeństwa z chwilą podłączenia urządzenia do sieci. Aby zachować zgodność całej floty z ustalonymi zasadami, należy ustalić harmonogram regularnych ocen/rozwiązywania problemów.

Środek nr 5: kontrolowane korzystanie z uprawnień administratora

Działanie – monitorowanie, uniemożliwianie i korygowanie użytkowania, nadawanie i konfiguracja uprawnień administratora na komputerach, w sieciach oraz w ramach aplikacji.

Zalecenie – warto wybierać urządzenia i rozwiązania z możliwością uwierzytelniania użytkowników i kontrolą dostępu do funkcji w zależności od zajmowanego stanowiska, tak aby tylko personel informatyczny lub inne upoważnione osoby miały dostęp do konfiguracji urządzeń. Oprogramowanie do zarządzania bezpieczeństwem floty umożliwia wdrożenie haseł dla administratorów w ramach całej floty.

Środek nr 6: prowadzenie, monitorowanie i analiza dzienników kontroli

Działanie – gromadzenie i analizowanie dzienników kontroli zdarzeń, a także zarządzanie nimi, mające na celu wykrywanie, zrozumienie oraz przywrócenie funkcjonalności po ataku.

Zalecenie – urządzenia drukujące powinny mieć możliwość generowania komunikatów syslog dotyczących incydentów, tak aby zespół ds. zabezpieczeń mógł regularnie analizować dzienniki kontroli w celu wykrywania i rozwiązywania problemów. Warto wybierać urządzenia, które mogą wysyłać te komunikaty do systemów zarządzania bezpieczeństwem floty i narzędzi SIEM w celu umożliwienia prowadzenia monitoringu w czasie rzeczywistym i generowania raportów w ramach kontroli lub spełnienia innych wymogów dotyczących zgodności.

Środek nr 7: ochrona poczty elektronicznej i przeglądarek internetowych

Działanie – minimalizacja platformy potencjalnych ataków oraz możliwości manipulowania zachowaniem pracowników w ramach interakcji z przeglądarkami i systemami poczty elektronicznej.

Zalecenie – urządzenia wielofunkcyjne często są podłączone do Internetu, na przykład by umożliwić przesyłanie zeskanowanych dokumentów pocztą elektroniczną. Aby chronić poufne dane, należy szyfrować przesyłane zeskanowane dokumenty. Warto również wdrożyć urządzenia i rozwiązania umożliwiające uwierzytelnianie użytkowników oraz kontrolę dostępu do zasobów w ramach urządzeń (takich jak serwery sieciowe czy poczta elektroniczna), w zależności od zajmowanego stanowiska. Pomocne jest również utworzenie listy „zaufanych stron" dla urządzeń wielofunkcyjnych i odpowiednie zarządzanie nimi, tak aby mieć pewność, że za pomocą urządzenia otwierane są tylko zaufane witryny internetowe. Aby uprościć zarządzanie i zwiększyć bezpieczeństwo, można połączyć kilka metod uwierzytelniania (np. kody PIN/PIC lub protokoły LDAP czy Kerberos) z technologią Active Directory. Urządzenia drukujące podłączone do sieci powinny mieć wbudowaną ochronę przed złośliwym oprogramowaniem i wirusami, a oprogramowanie wbudowane drukarek należy regularnie aktualizować, tak aby mieć pewność korzystania z najnowszych zabezpieczeń.

Środek nr 8: ochrona przed złośliwym oprogramowaniem

Działanie – kontrola nad instalowaniem, rozprzestrzenianiem i wykonywaniem złośliwego kodu w wielu punktach przedsiębiorstwa przy jednoczesnej optymalizacji korzystania z automatyzacji w celu umożliwienia szybkiej aktualizacji zabezpieczeń, gromadzenia danych i działań korekcyjnych.

Zalecenie – wybór urządzeń drukujących, które wczytują wyłącznie zweryfikowane, podpisane kody oraz mają wbudowane funkcje ochrony przed złośliwym oprogramowaniem, umożliwiające aktywne monitorowanie pamięci urządzenia i ponowne uruchomienie w razie ataku. Skuteczne narzędzie do zarządzania bezpieczeństwem druku może zautomatyzować proces oceny i rozwiązywania problemów z konfiguracją urządzeń w ramach floty. Ponadto należy upewnić się, że każdy element oprogramowania posiada podpis i potwierdzoną autentyczność.

Środek nr 9: ograniczenie i kontrola portów sieciowych, protokołów i usług

Działanie – zarządzanie (monitorowanie, kontrola i korygowanie) użytkowaniem portów, protokołów oraz korzystaniem z usług za pomocą urządzeń działających w sieci w celu minimalizacji słabych punktów dostępnych dla hakerów.

Zalecenie – jeśli wyłączenie nie nastąpiło domyślnie, należy dezaktywować niewykorzystywane porty i niezabezpieczone protokoły (takie jak FTP czy Telnet), które mogą stanowić furtkę dostępu dla hakerów. Wdrożenie narzędzia do zarządzania bezpieczeństwem druku zaoszczędzi czas informatyków i zmniejszy ryzyko, poprzez automatyczne utrzymywanie zgodności ustawień urządzeń w ramach całej floty. Hasła dla administratorów, system uwierzytelniania i uprawnienia zależne od zajmowanego stanowiska pomagają ograniczyć dostęp do funkcji i ustawień urządzeń.

Środek nr 10: możliwość odzyskiwania danych

Działanie – tworzenie kopii zapasowych najważniejszych informacji za pomocą sprawdzonych metod w celu umożliwienia ich terminowego odzyskiwania.

Zalecenie – ten środek obecnie nie dotyczy drukarek.

Środek nr 11: zabezpieczenie konfiguracji urządzeń sieciowych, takich jak zapory ogniowe, routery i przełączniki

Działanie – opracowanie, wdrożenie i aktywne zarządzanie (monitorowanie, raporty i działania korekcyjne) konfiguracją urządzeń infrastruktury w ramach sieci poprzez stosowanie rygorystycznych standardów oraz zmianę procesu kontroli w celu ochrony przed wykorzystaniem wrażliwych usług i ustawień przez niepożądane osoby.

Zalecenie – drukarki pracują w sieci, dlatego też powinny posiadać bezpieczną konfigurację, tak jak inne punkty końcowe sieci. Skuteczne narzędzie do zarządzania bezpieczeństwem druku może zautomatyzować proces wdrażania, oceny i korekty ustawień urządzeń w ramach floty w celu utrzymania bezpieczeństwa sieci – jednocześnie oszczędzając czas informatyków.

Środek nr 12: ochrona granic

Działanie – wykrywanie, uniemożliwianie i korekta przepływu informacji przez sieci o różnych poziomach zaufania z naciskiem na dane naruszające bezpieczeństwo.

Zalecenie – stosowanie szyfrowania w celu ochrony przesyłanych danych (przesyłanie zadań druku lub skanowania do i z drukarki) oraz przechowywanych na dysku twardym urządzenia. Warto wybierać urządzenia i rozwiązania z możliwością uwierzytelniania użytkowników i kontrolą dostępu do funkcji w zależności od zajmowanego stanowiska, tak aby – przykładowo – tylko autoryzowani użytkownicy mogli przesyłać zeskanowane dokumenty e-mailem lub pliki do miejsc docelowych w chmurze. Utworzenie listy zaufanych witryn w urządzeniu zapobiegnie dostępowi do złośliwych stron internetowych. Rozwiązania bezpiecznego drukowania z urządzeń przenośnych ułatwiają drukowanie z urządzeń przenośnych, jednocześnie chroniąc sieć.

Środek nr 13: ochrona danych

Działanie – zapobieganie wyprowadzaniu danych, łagodzenie skutków wyprowadzenia danych oraz zapewnienie ochrony i spójności informacji poufnych.

Zalecenie – stosowanie szyfrowania w celu ochrony przesyłanych danych (przesyłanie zadań druku lub skanowania do i z drukarki) oraz przechowywanych na dysku twardym urządzenia. Wdrożenie rozwiązań drukowania na żądanie w celu uniknięcia pozostawiania poufnych dokumentów w odbiornikach urządzeń. Należy upewnić się, że dane przechowywane na dyskach twardych urządzeń zostaną bezpiecznie usunięte przed zwrotem leasingowanych urządzeń lub utylizacją sprzętu po zakończeniu jego użytkowania.

Środek nr 14: kontrola dostępu na zasadzie niezbędnej wiedzy

Działanie – monitorowanie, kontrola, uniemożliwianie, korygowanie i zabezpieczenie dostępu do krytycznych elementów (np. informacji, zasobów i systemów) zgodnie z formalnymi ustaleniami dotyczącymi tego, które osoby, komputery i aplikacje mają potrzebę i prawo do dostępu do tych krytycznych elementów w oparciu o zatwierdzoną klasyfikację.

Zalecenie – warto wybierać urządzenia i rozwiązania z możliwością uwierzytelniania użytkowników i kontrolą dostępu do funkcji w zależności od zajmowanego stanowiska. Aby uprościć zarządzanie i zwiększyć bezpieczeństwo, można połączyć kilka metod uwierzytelniania (np. kody PIN/PIC lub protokoły LDAP czy Kerberos) z technologią Active Directory. Rozwiązania druku na żądanie pomagają chronić poufne dokumenty przed trafieniem w niepowołane ręce.

Środek nr 15: kontrola dostępu bezprzewodowego

Działanie – monitorowanie, kontrola, uniemożliwianie, korygowanie bezpieczeństwa korzystania z sieci bezprzewodowych (LAN), punktów dostępu i klientów bezprzewodowych.

Zalecenie – skuteczne narzędzie do zarządzania bezpieczeństwem druku może zautomatyzować proces wdrażania, oceny oraz korekty ustawień urządzeń, w tym ustawień bezprzewodowych, w ramach całej floty. Rozwiązania z zakresu kontroli dostępu ograniczają dostęp do funkcji urządzeń, takich jak przesyłanie zeskanowanych dokumentów e-mailem, na podstawie uprawnień użytkownika na danym stanowisku. Z kolei rozwiązania bezpiecznego drukowania z urządzeń przenośnych ułatwiają drukowanie, jednocześnie chroniąc sieć. Przykładowo urządzenia obsługujące bezprzewodowe drukowanie peer-to-peer umożliwiają użytkownikom bezpośrednie drukowanie przy użyciu dedykowanego sygnału bezprzewodowego – bez dostępu do sieci firmowej czy usługi bezprzewodowej.

Środek nr 16: monitorowanie i kontrola kont użytkowników

Działanie – aktywne zarządzanie cyklem życia systemów i kont w ramach aplikacji – ich tworzeniem, użytkowaniem, bezczynnością i usuwaniem – tak aby zminimalizować możliwości wykorzystania przez hakerów.

Zalecenie – warto wybierać urządzenia i rozwiązania z możliwością uwierzytelniania użytkowników i kontrolą dostępu do funkcji w zależności od zajmowanego stanowiska. Integracja procesu uwierzytelniania z technologią Active Directory pomaga scentralizować zarządzanie i zwiększyć bezpieczeństwo. Pomocne jest też regularne analizowanie kont użytkowników i dezaktywacja zbędnych kont oraz korzystanie z rozwiązań do monitorowania w celu kontrolowania sposobu użytkowania kont. Kolejna możliwość to szyfrowanie nazw użytkowników i danych uwierzytelniających, zarówno w trakcie przesyłania, jak i podczas przechowywania w pamięci urządzenia. Konsultanci ds. bezpieczeństwa pomogą w opracowaniu kompleksowego planu bezpieczeństwa druku w celu minimalizacji zagrożeń – w niektórych przypadkach mogą pomóc również w zarządzaniu bezpieczeństwem, w tym w monitorowaniu i kontroli nad kontami użytkowników.

Środek nr 17: ocena umiejętności z zakresu bezpieczeństwa i odpowiednie szkolenia w celu uzupełnienia braków

Działanie – identyfikacja wiedzy, umiejętności i możliwości potrzebnych do wspierania środków ochrony przedsiębiorstwa; opracowanie i realizacja zintegrowanego planu oceny, identyfikacji i eliminacji braków poprzez zasady, planowanie, szkolenia i programy zwiększające świadomość pracowników.

Zalecenie – konsultanci ds. bezpieczeństwa druku posiadają specjalistyczną wiedzę, dzięki której mogą pomóc w ocenie zagrożeń bezpieczeństwa, opracowaniu kompleksowych zasad i planu bezpieczeństwa, a także we wdrożeniu zaleceń dotyczących procesów i technologii. Niektóre usługi obejmują również zarządzanie zgodnością z przepisami z zakresu bezpieczeństwa druku.

Środek nr 18: bezpieczeństwo aplikacji

Działanie – zarządzanie bezpieczeństwem każdego opracowanego wewnętrznie, a także zakupionego oprogramowania w celu ochrony, wykrywania i eliminowania słabych punktów.

Zalecenie – stosowanie najlepszych praktyk z zakresu bezpiecznego programowania w przypadku wszystkich opracowywanych rozwiązań druku. Należy wybierać oprogramowanie posiadające podpis oraz zweryfikowaną autentyczność.

Środek nr 19: reagowanie i zarządzanie incydentami

Działanie – ochrona informacji w ramach przedsiębiorstwa, a także jego renomy, poprzez opracowanie i wdrożenie infrastruktury reagowania na incydenty (takiej jak plany, zdefiniowane role, szkolenia, komunikacja czy nadzór kierownictwa).

Zalecenie – warto upewnić się, że środowisko druku zostało uwzględnione w planie reagowania w przypadku incydentów.

Środek nr 20: wnikliwe testy i ćwiczenia grup reagowania

Działanie – sprawdzenie łącznych środków zabezpieczających przedsiębiorstwa (technologia, procesy i ludzie) poprzez symulację celów i działań hakera.

Zalecenie – uwzględnienie środowiska druku podczas testów penetracyjnych. Warto regularnie analizować środowisko druku pod kątem słabych punktów i aktualizować plan bezpieczeństwa w celu ich eliminacji.

Idź o krok dalej

Wdrożenie zaleceń zawartych w tym dokumencie może pomóc zwiększyć bezpieczeństwo druku i spełnić wymogi prawne. Potrzebna pomoc? Usługi z zakresu zarządzania drukiem i doradztwa pomogą w opracowaniu planu i wdrożeniu procesów oraz technologii, które zwiększą bezpieczeństwo urządzeń, danych i dokumentów.

Załącznik A: funkcje, rozwiązania i usługi HP z zakresu bezpieczeństwa druku

Funkcje bezpieczeństwa, w które wyposażone są urządzenia HP, wraz z wiodącym oprogramowaniem i usługami, pomagają w spełnieniu wymogów regulacyjnych i prawnych oraz chronią informacje w firmie przed zagrożeniami.

Wbudowane funkcje bezpieczeństwa w drukarkach i urządzeniach wielofunkcyjnych HP Enterprise chronią przed złośliwym oprogramowaniem i mogą automatycznie wykrywać ataki oraz przywracać funkcjonalność systemu. Tylko usługi HP z zakresu bezpieczeństwa druku zapewniają wykrywanie w czasie rzeczywistym, automatyczny monitoring i wbudowane funkcje walidacji oprogramowania, tak aby eliminować zagrożenia, gdy tylko się pojawią[4]. (Pomoc w realizacji środków nr 2, 4, 6 i 8). hp.com/go/PrintersThatProtect

Rozwiązania HP Access Control obejmują szeroki zakres funkcji uwierzytelniania i ograniczenia dostępu w celu zmniejszenia liczby potencjalnych naruszeń zabezpieczeń, a także umożliwiają śledzenie i rozliczanie zadań. (Pomoc w realizacji środków nr 5, 7, 10, 12, 13, 14, 15 oraz 16). hp.com/go/hpac

Szyfrowanie oraz **rozwiązania HP JetAdvantage Workflow Solutions** chronią dane zarówno podczas przechowywania w urządzeniach HP Enterprise, jak i podczas ich przesyłania z lub do urządzeń do drukowania lub chmury. (Pomoc w realizacji środków nr 12 i 13). hp.com/go/upd, hp.com/go/documentmanagement

Funkcja drukowania na żądanie chroni poufne dokumenty poprzez przechowywanie zadań druku na chronionym serwerze, w chmurze lub na komputerze użytkownika. Użytkownicy dokonują uwierzytelnienia przy wybranym urządzeniu, aby wydrukować swoje dokumenty. (Pomoc w realizacji środków nr 10, 13 i 14). hp.com/go/hpac, hp.com/go/JetAdvantageSecurePrint

HP JetAdvantage Connect zapewnia użytkownikom urządzeń przenośnych łatwy dostęp do funkcji drukowania za pomocą smartfonów i tabletów, z zachowaniem niezbędnego poziomu bezpieczeństwa i kontroli. (Pomoc w realizacji środków nr 12 i 15). hp.com/go/JetAdvantageConnect

Pochodzące z drukarek HP dane dotyczące zdarzeń mogą być przesyłane do narzędzi SIEM, takich jak ArcSight, Splunk czy SIEMonster. Informatycy mają łatwy dostęp do urządzeń w ramach szerszego układu infrastruktury informatycznej, co umożliwia im podejmowanie działań korekcyjnych. (Pomoc w realizacji środków nr 4 i 6).

HP JetAdvantage Security Manager to jedyne w branży oparte na zasadach narzędzie do zapewniania zgodności zabezpieczeń druku z wymogami[5]. Za jego pomocą można opracować zasady bezpieczeństwa dla całej floty, zautomatyzować korektę ustawień urządzeń, a także instalować i odnawiać unikatowe certyfikaty oraz generować raporty potrzebne do potwierdzenia zgodności. Funkcja Instant-On automatycznie konfiguruje nowe urządzenia po dodaniu ich do sieci lub ponownym uruchomieniu. (Pomoc w realizacji środków nr 1, 2, 3, 4, 5, 6, 8, 9, 11 oraz 15). hp.com/go/securitymanager

Usługi **HP Secure Managed Print Services** zapewniają najmocniejsze i najbardziej kompleksowe zabezpieczenia w branży[6]. Bezpieczeństwo druku to skomplikowane zagadnienie. Warto powierzyć je firmie HP, która zajmie się zarządzaniem bezpieczeństwem druku od wzmocnienia urządzeń po zaawansowane rozwiązania obejmujące ludzi, procesy i wymogi z zakresu zgodności. (Pomoc w realizacji środków nr 2, 3, 12, 16, 17, 18 oraz 19). hp.com/go/SecureMPS

Profesjonalne usługi HP z zakresu bezpieczeństwa druku obejmują pomoc specjalistów ds. zabezpieczeń w ramach oceny środowiska druku, proaktywnego ustalania zasad bezpieczeństwa i aktualizacji planu zabezpieczeń. Oferujemy również usługę zarządzania zgodnością z przepisami z zakresu bezpieczeństwa druku. (Pomoc w realizacji środków nr 2, 3, 12, 16, 17 oraz 19). hp.com/go/SecureMPS

Uwagi

[1] Badanie Ponemon przeprowadzone na zlecenie HPE: „2016 Cost of Cyber Crime Study & the Risk of Business Innovation", 2016 r.

[2] Raport 2016 Year End Data Breach QuickView firmy RiskBased Security, styczeń 2017.

[3] 26,2% respondentów doświadczyło poważnego naruszenia bezpieczeństwa środowiska IT z koniecznością przeprowadzenia naprawy, a ponad 26,1% incydentów dotyczyło druku. IDC, „IT and Print Security Survey 2015" IDC nr US40612015, wrzesień 2015 r.

[4] Dotyczy urządzeń klasy HP Enterprise wprowadzonych do sprzedaży w 2015 r. i bazuje na przeprowadzonym przez HP przeglądzie opublikowanych w 2016 r. informacji na temat zintegrowanych funkcji bezpieczeństwa konkurencyjnych drukarek tej samej klasy. Tylko HP oferuje połączenie funkcji bezpieczeństwa do sprawdzania integralności do poziomu BIOS z narzędziami do samonaprawy. Aby aktywować funkcje bezpieczeństwa, może być wymagany pakiet aktualizacji FutureSmart. Listę kompatybilnych produktów można znaleźć na stronie hp.com/go/PrintersThatProtect. Więcej informacji na stronie: hp.com/go/printersecurityclaims.

[5] Oprogramowanie HP JetAdvantage Security Manager należy zakupić oddzielnie. Więcej informacji na stronie hp.com/go/securitymanager. Stwierdzenie oparte na wynikach wewnętrznych badań HP dotyczących oferty konkurencyjnej (porównanie bezpieczeństwa urządzeń, styczeń 2015 r.) i raportu Solutions Report dotyczącego oprogramowania HP JetAdvantage Security Manager 2.1, przygotowanego przez Buyers Laboratory LLC w lutym 2015 r.

[6] Obejmuje narzędzia w dziedzinie bezpieczeństwa urządzeń, danych i dokumentów od czołowych dostawców usług zarządzania drukiem. W oparciu o przeprowadzony przez HP przegląd publicznie dostępnych informacji z okresu 2015–2016 na temat usług bezpieczeństwa, oprogramowania w dziedzinie bezpieczeństwa i zarządzania oraz wbudowanych funkcji bezpieczeństwa konkurencyjnych drukarek tej samej klasy. Więcej informacji na stronach hp.com/go/MPSsecurityclaims lub hp.com/go/mps.

Zarejestruj się, aby otrzymywać aktualizacje
hp.com/go/getupdated

Udostępnij współpracownikom

4AA6-8821PLE, Czerwiec 2017, wer. 1