Cyberdefence 24

aut. Andrzej Kozłowski 09.10.2017

„WYDRUKUJ WIRUSA”. DRUKARKA ZAGROŻENIEM DLA DANYCH [ANALIZA]

Świat w cyberprzestrzeni staję się coraz bardziej niebezpieczny. Zagrożenia przestały już pochodzić tylko od grup nastoletnich hakerów, kradnących informacje i wywołujących chaos. W samym 2016 roku ponad 4 miliardy urządzeń zostało zhakowanych na całym świecie. To o 400 proc. więcej niż w poprzednich dwóch latach. Początkiem infekcji może być nawet niezabezpieczona drukarka.

W dzisiejszym świecie włamania do sieci i systemów teleinformatycznych administracji publicznej i sektora prywatnego to ogromny biznes, w który zaangażowane jest wiele różnych grup przestępczych i państw. Ich celem są szpitale, szkoły, banki, firmy kredytowe i inne miejsce w których przechowuję się dane personalne, które następnie można spieniężyć w darknecie.

Fot. HP/Twitter

W powszechnym przekonaniu źródłem zakażenia złośliwym oprogramowaniem może być komputer, laptop, telefon. Niewiele osób podejrzewa, że hakerzy mogą włamać wykorzystując do tego drukarkę.

Na świecie używanych są setki milionów drukarek, tylko 2 proc. jest zabezpieczone. Większość z nich nie ma wbudowanych żadnych narzędzi chroniących je przed złośliwym oprogramowaniem. Najbardziej znanym przykładem włamania jest zhakowanie 150 tys. niezabezpieczonych drukarek. Napastnicy nie mieli jednak złych zamiarów i wydrukowali tylko informacje dla użytkowników ostrzegając, że ich sprzęt jest niezabezpieczony. Łatwo jednak wyobrazić sobie konsekwencje takiego włamania, jeżeli atakujący chcieliby dokonać zniszczeń.

Czytaj też: Drukowanie 3-D zagrożeniem dla bezpieczeństwa?

Jednak to nie tylko kwestia złego zabezpieczenia sprzętu podłączonego do komputera, ale również brak świadomości pracowników go używających. Słabe hasła, odchodzenie od komputerów bez ich wyłączenia lub blokowania ułatwiają dokonanie włamań. Niewinny komputer pojedynczego pracownika może być początkiem bardzo poważnej infekcji.

Cel – Chief Security Officer (CSO)

Hipotetycznie załóżmy, że celem hakerów jest chmura, w której przechowywane są dane setek tysięcy pacjentów. W celu ich wykradnięcia i sparaliżowania ochrony trzeba wprowadzić chaos organizacyjny, czasowo eliminując główną osobą zarządzającą bezpieczeństwem (Chief Security Officer, CSO).

Haker, korzystając z nieuwagi osoby obsługującej komputer w przychodni lekarskiej, wprowadza złośliwe oprogramowanie. W tej placówce leczy się cel operacji czyli osobą zarządzająca bezpieczeństwem. Haker uzyskuje możliwość dozowania lekarstwa dla pacjentów. Dodaje on takie medykamenty do tych przypisywanych dla CSO, które doprowadzają go do problemów zdrowotnych, wskutek czego trafia do szpitala. Wystarczyłoby wprowadzić automatyczną blokadę na komputerze, która włącza się w momencie odejścia pracownika do stanowiska, aby zapobiec atakowi.

Również szpitale, mimo posiadania najbardziej zaawansowanego sprzętu, nie są odpowiednio zabezpieczone przed włamaniami. Haker wykorzystując starą niezabezpieczoną drukarkę, korzystając z jej portu USB, wczytuje złośliwe oprogramowanie, które otwiera mu „tylną furtkę" do sieci i systemów. Drukarka podłączona jest do sieci niepodzielonej na segmenty, haker może uzyskać dostęp do serwerów podłączonych do baz danych informacji wrażliwych. Pozwala mu to na podjęcie wielu działań, przykładowo może zmienić imię i nazwisko pacjenta, nadając CSO nową tożsamość. Na tym się jednak nie kończy. Może bowiem sfałszować wyniki badań laboratoryjnych i w ten sposób doprowadzić do podania pacjentowi konkretnych leków, które wprowadzą go przykładowo w stan śpiączki. Wystarczyłoby, że drukarka posiadałaby ochronę BIOS-u i miała system wykrywania zagrożeń. Działanie hakera byłoby dużo trudniejsze, jeśli nie niemożliwe.

Następnym celem hakerów jest już właściwy atak skierowany przeciwko przedsiębiorstwu odpowiedzialnemu za administrowanie chmurą. Pracownicy pozbawieni swojego szefa i nie mogący się z nim skontaktować, nie wiedzą co mają zrobić i jak walczyć z zagrożeniem. Zhakowane zostały nawet zapasowe bazy danych. Pomimo tego, że spędzono wiele czasu żeby zabezpieczyć sieci.

Hakerowi udało się w ten sposób pozyskać dane miliony pacjentów, a infekcja rozpoczęła się od włamania do biura jednej przychodni na skutek zaniedbania pracownika.

Podsumowując ten scenariusz. Pierwszym problemem bezpieczeństwa jest niezablokowany komputer, kiedy użytkownik od niego odchodzi. Drugą kwestią jest brak konieczności uwierzytelniania portu USB drukarki przed użyciem. Ponadto sprzęt ten nie jest monitorowany pod kątem zdarzeń naruszających ochronę bezpieczeństwa Nagminnym problemem jest również brak szyfrowania plików.

Czytaj też: Nadchodzi internetowa apokalipsa? [ANALIZA]

W celu zmniejszenia ryzyka udanego ataku należy wzmocnić system ochrony tożsamości poprzez stosowanie wieloczynnikowego uwierzytelnienia na komputerach HP Elite.

Równie ważna jest ochrona danych. Konieczne jest zastosowanie uwierzytelniania drukarki i szyfrowania. Zamknięcie nieużywanych portów lub kontrola dostępu za pomocą kontroli użytkownika. Stosowanie silnej kontroli szyfrowania dla wszystkich danych przechowywanych i przesyłanych.

Skuteczną ochronę urządzeń zapewnia przejście na komputery HP Elite z procesem Intel Core vPro , które zostały całościowo zaprojektowane w celu ochrony urządzenia, tożsamości i danych oraz drukarki HP Enterprise. Powinno się również wprowadzić urządzenia wielofunkcyjne z wbudowaną ochroną przed złośliwym oprogramowaniem w celu niedopuszczenia do ataków i mechanizmami auto-naprawy do poziomu systemu BIOS za pomocą HP Sure Start.

Dodatkowo powinny zostać użyte narzędzia monitoringu i zarządzania. Wdrożenie HP JetAdvantage Security Manager, który sprawdza i jeśli zachodzi taka konieczność, to naprawia ustawienia dotyczące bezpieczeństwa urządzenia drukującego przy jego restarcie, lub też Management Integration Kit zabezpieczający komputery. Oba te systemy mają na celu zapewnienie automatycznej konfiguracji polityk bezpieczeństwa urządzań w całej flocie, umożliwienie centralnym systemom Syslog śledzenie zdarzeń bezpieczeństwa oraz umożliwiają także podłączanie drukarek do narzędzi typu Security Information and Event Management (SIEM) w celu uzyskiwania powiadomień i ingerencjach w czasie rzeczywistym.

Drukarka – cel hakera

Drukarki mogą być poważnym źródłem problemów. W hipotetycznym scenariuszu haker wykorzystuje najbardziej narażone na atak punkty końcowe. Za pomocą urządzenia zdalnego haker uzyskuje dostęp do drukarki i wprowadza do niej złośliwe oprogramowanie umożliwiające przechwytywanie i odczytywanie danych. W ten sposób może dowiedzieć się kto z pracowników ma urodziny i wysłać spreparowanego e-maila ze złośliwym załącznikiem, który następnie zostaje wydrukowany. Złośliwe oprogramowanie łamie zaporę sieciową i rozprzestrzenia się w komputerach spółki. Kod znajduję się na poziomie BIOS-u, wiec może stale przekazywać dane, a nawet przywrócić działanie po aktywacji systemów ochrony sieci. Na koniec zostaje odkryty poufny dokument na odbiorniku urządzenia wielofunkcyjnego. Wyciek danych powoduje znaczne straty finansowe i wizerunkowe firmy.

W scenariuszu tym doszło do wielu naruszeń bezpieczeństwa. Drukarka wyposażona w moduł Wi-Fi lub Bluetooth jest otwarta i zazwyczaj w domyślnej konfiguracji nie wymaga uwierzytelnienia użytkownika. Dodatkowo pliki z danymi drukarki nie są szyfrowane. Kolejnym problemem jest to, że użytkownicy nie rozpoznają podejrzanych wiadomości e-mail i plików do wydruku. Ponadto dokumenty pozostawione na odbiorniku drukarki mogą zawierać informacje wrażliwe.

Z wykorzystaniem narzędzi firmy HP można przeciwdziałać takim atakom. Ochrona danych może zostać wzmocniona przez wyłączenie połączenia Wi-Fi/Bluetooth oraz zabezpieczenie dostępu do usług uruchomianych na urządzeniu przy pomocy HP JetAdvantage Connect lub HP Access Control. To pierwsze rozwiązanie umożliwia wykorzystanie istniejących narzędzi sieciowych oraz zdefiniowanych polityk bezpieczeństwa IT do zarządzania drukowaniem ze smartfonów bądź tabletów, przy jednoczesnym zapewnieniu użytkownikom możliwości bezpiecznego wydruku, bez konieczności instalacji dodatkowych aplikacji. Drugie rozwiązanie, to HP Access Control, który zapewnia bezpieczeństwo poprzez wdrożenie mechanizmów kontroli dostępu do urządzeń, jak również pozwala na ograniczenie kosztów. Realizowane jest to dzięki możliwości przypisania użytkownikom praw dostępu do poszczególnych funkcjonalności urządzenia w oparciu o ich role w naszej organizacji, jak również poprzez szczegółowe raportowanie ich aktywności w zakresie druku, skanowania, czy tez

realizacji innych czynności na wspomnianym urządzeniu.

Nie tylko jednak ochrona danych jest ważna, ale również bezpieczeństwo samego urządzenia. Rekomendowane jest tutaj przejście na komputery HP Elite i drukarki oraz urządzenia wielofunkcyjne HP Enterprise z ochroną przed złośliwymi oprogramowaniem w celu, nie tylko automatycznego wykrywania ale przede wszystkim, zatrzymywania ataków oraz przywracanie stabilności ich działania bez interwencji działu IT. W trakcie procesu uruchamiania się urządzenia, zaimplementowana w nich technologia HP SureStart - sprawdza BIOS. W przypadku wykrycia jakichkolwiek anomalii, samoczynnie rozpoczyna proces auto-naprawy – polegający na przywróceniu tzw. „złotej kopii BIOSu", zapewniając tym samym naszej organizacji najwyższy poziom bezpieczeństwa poprzez nadpisanie skompromitowanego BIOSu oryginalna jego wersją. Dodatkowe środki, które możemy wykorzystać tworząc kompleksową politykę bezpieczeństwa w naszej organizacji to szyfrowanie dysków twardych oraz wszelkiej transmisji – z czy do - urządzenia, szerokie możliwości konfiguracji w zakresie filtrowania ruchu sieciowego oraz wiele innych.

Zabezpieczenie urządzeń to jedna strona medalu. Drugą stroną jest natomiast wdrożenie mechanizmów ochrony dokumentów, które umożliwiają ich bezpieczne drukowanie. Pomocne w tym mogą być rozwiązania - HP Access Control lub też HP JetAdvantage Secure Print. Pierwsze z nich to tradycyjny system wydruku podążającego, w ramach którego nie tylko zabezpieczymy urządzenia ale również zapewnimy naszej organizacji bezpieczeństwo drukowanych dokumentów instalując serwer(y) w naszej infrastrukturze sieciowej. Drugie rozwiązanie przeznaczone jest natomiast dla firm, które otwarte są na rozwiązania chmurowe preferując zakup oprogramowania w formie usługi.

Podsumowanie

Powyższe hipotetyczne scenariusze mogą być bardzo szybko wcielone w życie, a ofiarą hakerów działających w opisany powyżej lub podobny sposób może zostać praktycznie każdy. Rozwiązania HP zapewniają ciągłą kontrolę i stały monitoring bezpieczeństwa urządzeń poprzez wykrywanie wszelkich anomalii w trakcie ich działania, jak również sprawdzanie oprogramowania sprzętowego podczas ich uruchamiania się.