Analiza przypadku

Gdy londyńskie lotnisko stało się celem niszczycielskiego cyberataku, drukarki HP wykryły zagrożenie

Oficjalny raport podsumowujący przypadek naruszenia bezpieczeństwa danych

Branża
Lotnictwo

Cel
Identyfikacja słabych punktów w praktykach cyberbezpieczeństwa i ich eliminacja

Podejście
Opracowanie kompleksowego planu zabezpieczeń we współpracy z ekspertami HP ds. bezpieczeństwa

Kwestie IT
- Zastosowanie zabezpieczeń do punktów końcowych IoT
- Włączenie wbudowanych funkcji zabezpieczeń w drukarkach HP
- Usprawnienie monitorowania bezpieczeństwa całej sieci

Kwestie biznesowe
Poprawa cyberbezpieczeństwa w celu ochrony kluczowej infrastruktury międzynarodowej oraz utrzymania bezpieczeństwa pasażerów

Przegląd

Londyńskie lotnisko* obsługuje dziennie ponad 300 000 pasażerów udających się do 94 krajów na całym świecie. Pracuje na nim niemal 50 000 osób z 300 firm, zatem praktycznie jest to „miasto w pigułce”.

W miarę rozbudowy lotniska jego infrastruktura stawała się w coraz większym stopniu połączona z siecią i zautomatyzowana. Systemy wewnętrzne — od ogrzewania, wentylacji i klimatyzacji (HVAC) przez oświetlenie po drukarki — są obecnie połączone z siecią lotniska. Drukowanie, skanowanie i kopiowanie obsługuje flota ponad 60 urządzeń wielofunkcyjnych HP rozproszonych po całym lotnisku.

23 kwietnia 2018 r. cyberterrorysta znany wyłącznie z pseudonimu — „The Wolf” — wykorzystał połączone z siecią systemy oświetlenia, aby uzyskać dostęp do sieci i zainfekować ją złośliwym oprogramowaniem. Jako że osobnik ten jest znany z wykorzystywania niedostatecznie zabezpieczonych punktów końcowych, w ramach dochodzenia eksperci w dziedzinie bezpieczeństwa IT niezwłocznie przystąpili do analizy dzienników zagrożeń z drukarek HP Enterprise w celu rozpoznania i powstrzymania ataku. Co ciekawe, dzienniki zawierały wskazówki od Wilka co do miejsca, w którym włamanie miało swój początek. Następnie przedstawiciele londyńskiego lotniska zwrócili się do HP z prośbą o pomoc we wzmocnieniu zabezpieczeń punktów końcowych.

Przebieg wydarzeń

Po znalezieniu luki w zabezpieczeniach, prawdopodobnie przez rozesłanie do użytkowników sieci wiadomości e-mail typu phishing, Wilk mógł zainfekować złośliwym oprogramowaniem system oświetlenia wykorzystujący technologię IoT. Następnie mógł rozprzestrzenić swoje złośliwe oprogramowanie w całej sieci, tworząc punkty zaczepienia w innych niemonitorowanych urządzeniach końcowych.

Ukrywając swą obecność w niemonitorowanych urządzeniach IoT, ekipa Wilka uniknęła wykrycia przez systemy monitorowania sieci i mogła swobodnie przygotować liczne punkty uruchomienia masywnego, niszczącego ataku.

Kierownictwo lotniska desperacko starało się wyłączyć wiele systemów, z zachowaniem mobilności kluczowych elementów infrastruktury, jak samoloty i pasażerowie.

Reakcja na atak

Wilk zaatakował sieć lotniska na zlecenie. Personel ds. bezpieczeństwa IT lotniska *sądził*, że sieć lotniska jest dobrze zabezpieczona przed hakerami, nie dostrzegając zagrożeń kryjących się w urządzeniach IoT.

Na szczęście lotniskowe drukarki HP Enterprise były wyposażone w technologię HP Connection Inspector, która powstrzymała złośliwe oprogramowanie przy próbach nawiązania połączenia z serwerami centrum dowodzenia hakerów, które uznała za podejrzane.

Działania zostały zarejestrowane w dziennikach zdarzeń drukarek. Gdy personel IT uświadomił sobie, że coś jest nie tak, sprawdził dzienniki zdarzeń w celu identyfikacji szczegółów ataku. Jednakże w sytuacji, gdy złośliwe oprogramowanie rozprzestrzenia się poprzez sieć, kluczowe znaczenie ma czas. Gdyby personel ds. bezpieczeństwa IT połączył dostępne w drukarkach dzienniki zdarzeń wykrywania zagrożeń ze swoim systemem monitorowania bezpieczeństwa informacji i zdarzeń (SIEM), zostałby niezwłocznie ostrzeżony w chwili dokonywania włamania.

Zabezpieczenia mocniejsze niż kiedykolwiek wcześniej

Po tym przypadku naruszenia bezpieczeństwa personel IT zrewidował praktyki bezpieczeństwa za pomocą swego dostawcy usług zarządzania drukiem i doradców HP w dziedzinie zabezpieczeń.

Londyńskie lotnisko obrało właściwy kierunek z chwilą zainstalowania drukarek HP Enterprise. Tylko drukarki i urządzenia wielofunkcyjne HP Enterprise oferują funkcję wykrywania włamań podczas pracy i technologię HP Connection Inspector, wykrywającą i powstrzymującą złośliwe oprogramowanie podczas pracy oraz wymuszającą ponowne uruchomienie. Przy uruchamianiufunkcja HP Sure Start sprawdza system BIOS i automatycznie go naprawia, jeśli został zmanipulowany, a jednocześnie funkcja Whitelisting sprawdza oprogramowanie sprzętowe.

Dostawca usług zarządzania drukiem wdrożył oprogramowanie HP JetAdvantage Security Manager, które automatycznie sprawdza ustawienia zabezpieczeń przy każdym ponownym uruchomieniu drukarki i przywraca je do pierwotnego stanu w razie jakichkolwiek modyfikacji.

Personel ds. bezpieczeństwa IT lotniska w końcu połączył też dzienniki zdarzeń drukarek ze swym narzędziem SIEM. W przeciwieństwie do drukarek innych producentów urządzenia HP mogą przekazywać specjalne dzienniki zagrożeń do wielu narzędzi SIEM, umożliwiając ostrzeganie personelu IT w czasie rzeczywistym o potencjalnych incydentach związanych z bezpieczeństwem. Dzięki temu drukarki HP stają się nieocenionymi „strażnikami" sieci.

Podsumowanie

Dzięki lotniskowym drukarkom HP Enterprise i wskazówkom pozostawionym przez Wilka personel bezpieczeństwa był w stanie rozpoznać atak na tyle szybko, aby uniknąć unieruchomienia całego lotniska, krytyki w mediach, kar z tytułu niezgodności z przepisami oraz szkód wizerunkowych.

Przez zastosowanie bardziej rygorystycznych praktyk bezpieczeństwa i pełne wykorzystanie wbudowanych zabezpieczeń drukarek HP lotnisko zwiększyło bezpieczeństwo całej sieci.

**Londyńskie lotnisko to fikcyjna organizacja, która stała się celem szeroko zakrojonego cyberataku w wyprodukowanym przez HP Studio filmie „THE WOLF: TRUE ALPHA".*

Więcej informacji o rozwiązaniach HP:
Bezpieczeństwo druku: hp.com/go/reinventsecurity
Bezpieczeństwo komputerów PC: hp.com/go/ComputerSecurity

Aby obejrzeć filmiki z serii „The Wolf", odwiedź stronę: hp.com/thewolf

Zarejestruj się, aby otrzymywać aktualne informacje: hp.com/go/getupdated

Udostępnij współpracownikom

© Copyright 2018 HP Development Company, L.P. Przedstawione informacje mogą ulec zmianie bez powiadomienia. Jedyne gwarancje, jakich HP udziela na swoje produkty i usługi, są określone w oświadczeniach gwarancyjnych dostarczanych wraz z takimi produktami i usługami. Żadne informacje zawarte w niniejszym dokumencie nie powinny być rozumiane jako dodatkowa gwarancja. Firma HP nie ponosi odpowiedzialności prawnej za błędy techniczne lub redakcyjne ani za ewentualne braki w niniejszym opracowaniu.

4AA7-3560PLE, sierpień 2018 r.