Analiza przypadku

Testy penetracyjne wykazują, że drukarki HP mogłyby zapobiec naruszeniu cyberbezpieczeństwa firmy Torvik Undustries przez „Wilka”

Oficjalny raport podsumowujący przypadek naruszenia bezpieczeństwa danych

Branża
Spedycja

Cel
Analiza i eliminacja luk w zabezpieczeniach sieci

Podejście
Testy infiltrujące mające na celu znalezienie luk w zabezpieczeniach, które doprowadziły do ataku

Wnioski i zalecenia
- Uświadomienie użytkownikom konieczności zachowania ostrożności przy otwieraniu podejrzanych wiadomości e-mail i drukowaniu załączników
- Wdrożenie drukarek HP z technologią wykrywania zagrożeń
- Właściwe skonfigurowanie zabezpieczeń wszystkich punktów końcowych, w tym elementów infrastruktury, które są przenoszone lub znajdują się w lokalizacjach tymczasowych

Kwestie biznesowe
Zastosowanie mocniejszych zabezpieczeń w celu uniknięcia przestojów w działalności i zwiększenia zaufania do marki. Poprawa zasad monitorowania punktów końcowych sieci w lokalizacjach tymczasowych.

Przegląd

Torvik Industries* wysyła 8 mln kontenerów rocznie. Stanowi kluczowy łącznik między produktami i klientami na całym świecie dla 22 000 producentów i dystrybutorów. Majątek firmy obejmuje doki, statki, magazyny i całe zaplecze techniczne obsługujące rozległą sieć firmy Torvik.

Infrastruktura techniczna firmy nie nadąża za jej rozwojem. Wprawdzie personel ds. bezpieczeństwa IT skonfigurował serwery, ale niektóre drukarki w odległych oddziałach lub tymczasowych lokalizacjach nie są zarządzane w sposób gwarantujący bezpieczeństwo.

23 kwietnia 2018 r. cyberrterrorysta znany wyłącznie z pseudonimu — “The Wolf” — wykorzystał niezabezpieczoną drukarkę, aby dokonać sabotażu działalności Torvik Industries — od komputerów, przez suwnice, po kontenerowce. Doradca firmy ds. bezpieczeństwa przeprowadził testy infiltrujące, aby zanalizować incydent i wydać zalecenia w kwestii wzmocnienia zabezpieczeń i szkolenia personelu.

Przebieg wydarzeń

Kierownictwo Torvik Industries przywykło do dyktowania warunków w grze o dużą stawkę, zatem nie spodziewało się, że hakerzy mogą zinfiltrować ich sieć tak głęboko, aby unieruchomić suwnice bramowe i zmienić trasy statków na pełnym morzu.

Wystarczyło, że Wilk zmanipulował drukarkę wielkoformatową na placu budowy. Mógł wtedy penetrować sieć firmy, docierając do celów o dużym znaczeniu dla działalności. W jednej chwili to czołowe przedsiębiorstwo spedycyjne stanęło w obliczu poważnych zakłóceń w działalności, fali międzynarodowej krytyki i wściekłości tysięcy klientów.

Jak do tego doszło

Personel ds. bezpieczeństwa IT firmy sądził, że sieć jest dobrze zabezpieczona. Działy techniczne i logistyczne na bieżąco monitorowały działalność w skali całego świata, aby wykryć potencjalne problemy z bezpieczeństwem. Były nawet wdrożone procedury dotyczące punktów końcowych, takich jak drukarki. Jedną rzecz jednak przeoczono: konfigurację zabezpieczeń drukarki wielkoformatowej tymczasowo zainstalowanej na przyczepie budowlanej.

Haker nie potrzebował nawet bezpośredniego dostępu do drukarki — wystarczyło że wysłał wiadomość e-mail z załącznikiem PDF do pracownika firmy odpowiedzialnego za drukowanie dokumentów dużego formatu. Taki dokument PDF zawierał ukryty szkodliwy plik PostScript, który mógł zostać otwarty i uruchomiony po wysłaniu dokumentu PDF do drukarki. Gdy pracownik wysłał zlecenie drukowania, złośliwe oprogramowanie przeniknęło do drukarki, a następnie rozprzestrzeniło się w całej sieci. Przez osadzenie złośliwego oprogramowania w niewinnie wyglądającym załączniku e-mail haker ominął oprogramowanie przeciwdziałające złośliwemu oprogramowaniu na komputerach firmy.

Naruszenie bezpieczeństwa było możliwe, ponieważ drukarka wielkoformatowa nie miała wbudowanych solidnych zabezpieczeń, takich jak wykrywanie zagrożeń. Ponadto firma zaniedbywała monitorowanie konfiguracji i zarządzania konfiguracją niektórych drukarek we flocie — w tym tymczasowo umieszczonych w odległych oddziałach.

Działania podjęte w reakcji na naruszenie bezpieczeństwa

Firma Torvik Industries zatrudniła czołową firmę zajmującą się testami infiltrującymi w celu przeprowadzenia szczegółowej analizy jej cyberzabezpieczeń.

Zespół przeprowadzający testy penetracyjne zalecił zainstalowanie drukarek HP z wbudowanymi zabezpieczeniami, w tym drukarek z serii HP DesignJet z funkcjami Secure Boot i kontroli oprogramowania sprzętowego metodą Whitelisting. Dzięki tym funkcjom, w razie zainfekowania złośliwym kodem drukarka wykrywa go i wyłącza się, a następnie ostrzega personel IT o konieczności ponownego zainstalowania oryginalnego oprogramowania sprzętowego HP.

Zalecił również korzystanie z funkcji zabezpieczającej Instant-On programu HP JetAdvantage Security Manager do zarządzania bezpieczeństwem na poziomie całej floty, w celu automatycznego stosowania zasad bezpieczeństwa z chwilą dodania urządzeń do sieci. Program HP Security Manager umożliwia też tworzenie raportów zgodności, które uwzględniają każdądrukarkę HP, nawet znajdującą się w odległej lub tymczasowej lokalizacji. Dzięki temu można łatwiej wykazać, że utrzymywane są właściwe konfiguracje zabezpieczeń floty.

Ponadto doradca ds. bezpieczeństwa zasugerował program szkoleń pracowników mający na celu zdobycie umiejętności rozpoznawania podejrzanych wiadomości e-mail i w ten sposób unikania drukowania nieznanych załączników.

Podsumowanie

Torvik Industries nadal odczuwa skutki naruszenia cyberbezpieczeństwa w codziennej działalności oraz nasilenie krytyki medialnej dla niekonwencjonalnych poglądów i aktów przestępczych jej prezesa. Podczas gdy przedsiębiorstwo stara się wypracować nowy kierunek pod względem stylu zarządzania, kierunek w dziedzinie zabezpieczeń jest jasny: przejście na drukarki i rozwiązania HP w celu powstrzymania zapędów kolejnego „wilka", który ruszy na łowy.

**Torvik Industries to fikcyjne przedsiębiorstwo, które stało się celem szeroko zakrojonego cyberataku w wyprodukowanym przez HP Studio filmie „THE WOLF: TRUE ALPHA".*

Więcej informacji o rozwiązaniach HP:
HP DesignJet: hp.com/go/designjetsecurity
Bezpieczeństwo druku: hp.com/go/reinventsecurity
Aby obejrzeć filmiki z serii „The Wolf", odwiedź stronę: hp.com/thewolf

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

Udostępnij współpracownikom

4AA7-3562PLE, sierpień 2018 r.