Analiza przypadku

Atak hakerski na system AV szwajcarskiego centrum konferencyjnego, któremu mogłyby zapobiec zabezpieczenia komputerów HP

Oficjalny raport podsumowujący przypadek naruszenia bezpieczeństwa danych

Branża
Centra organizacji wydarzeń

Cel
Audyt praktyk bezpieczeństwa w celu wzmocnienia ochrony centrum konferencyjnego i poufnych danych klienta

Podejście
Analiza praktyk bezpieczeństwa i identyfikacja nieprawidłowości we współpracy z konsultantem klienta ds. bezpieczeństwa

Kwestie IT
- Modernizacja floty o komputery HP Elite z wbudowanymi zabezpieczeniami przed złośliwym oprogramowaniem
- Zamknięcie niepotrzebnych portów w celu uniemożliwienia nieautoryzowanego użycia
- Integracja dodatku HP Manageability Integration Kit z programem Microsoft® System Center Configuration Manager (SCCM) w celu zdalnego zarządzania flotą komputerów

Kwestie biznesowe
Modernizacja cyberzabezpieczeń w celu wzmocnienia ochrony obiektu przed wyrafinowanymi atakami i odzyskania zaufania klientów

Przegląd

Szwajcarskie centrum konferencyjne* w pobliżu Genewy obsługuje ponad 230 wydarzeń rocznie. Jako popularne w Europie miejsce organizacji konferencji biznesowych i prezentacji produktów dużych przedsiębiorstw, centrum gości liderów branżowych z całego świata.

Kierownictwo obiektu zainwestowało znaczne środki w infrastrukturę techniczną, aby spełniać wszelkie potrzeby klientów w tym uroczo położonym ośrodku. Niestety nie zadbano równocześnie o modernizację zabezpieczeń floty komputerów.

23 kwietnia 2018 r. haker o pseudonimie „The Wolf” zinfiltrował jeden z komputerów, aby zakłócić przebieg ważnej prezentacji dla międzynarodowego audytorium. Po tym incydencie szwajcarskie centrum konferencyjne zwróciło się do swego konsultanta ds. bezpieczeństwa, aby odnalazł i zlikwidował luki w cyberzabezpieczeniach.

Przebieg wydarzeń

Jako renomowany na świecie ośrodek spotkań korporacyjnych, szwajcarskie centrum konferencyjne nie miało sobie równych w dostarczaniu gościom wyjątkowych wrażeń, jednak jego cyberzabezpieczenia nie były już tak imponujące. Wilk przesłał złośliwe oprogramowanie do jednego z komputerów ośrodka, a następnie podmienił prezentację na własną. W całym zamieszaniu, które pojawiło się w sali wykładowej, personel ds. bezpieczeństwa IT rozpaczliwie starał się odzyskać kontrolę nad siecią.

Szkody nie ograniczyły się do jednej zrujnowanej prezentacji. Utratę przychodów w związku z anulowaniem rezerwacji aktualnie szacuje się na 3,2 mln EUR.

Jak do tego doszło

Wystarczyło, że Wilk dostał się do jednego z niezabezpieczonych komputerów przez skłonienie jednego pracowników do kliknięcia szkodliwego łącza w wiadomości e-mail lub pobrania niewinnie wyglądającego załącznika. Mógł też włożyć napęd flash do nienadzorowanego portu USB, ponieważ fizycznie był na miejscu.

Flocie komputerów szwajcarskiego centrum konferencyjnego brakowało podstawowych zabezpieczeń, które poddałyby złośliwe oprogramowanie kwarantannie, aby zablokować tę próbę infiltracji. Wprawdzie oprogramowanie antywirusowe *było* zainstalowane, ale żaden komputer nie miał wbudowanych zabezpieczeń egzekwowanych sprzętowo.

Wzmacnianie zabezpieczeń

Wraz z konsultantem ds. bezpieczeństwa szwajcarskie centrum konferencyjne przeprowadziło szczegółowy audyt istniejących cyberzabezpieczeń. Kontrola doprowadziła do wymiany całej floty na komputery HP Elite z wbudowanymi zabezpieczeniami przed złośliwym oprogramowaniem, takimi jak technologia HP Sure Start Gen4, która automatycznie wykrywa i powstrzymuje atak na system BIOS bądź jego uszkodzenie przy rozruchu czy podczas pracy komputera, eliminując ewentualne szkody.[1]

Nowe komputery HP Elite mają też funkcję HP Sure Click, która wzmacnia ochronę przez fizyczne rozpoznanie każdej karty przeglądarki albo pobranego dokumentu PDF czy Microsoft w mikromaszynie wirtualnej (VM), blokując rozprzestrzenianie się złośliwego oprogramowania z Internetu lub załącznika e-mail do innych urządzeń połączonych z siecią.[2]

Zespół IT teraz korzysta z programu HP Device Access Manager do zarządzania portami i nośnikami wymiennymi oraz narzędzia HP Manageability Integration Kit dla programu SCCM firmy Microsoft w celu usprawnienia zarządzania zabezpieczeniami i systemami BIOS w całej flocie.[3]

Podsumowanie

Szwajcarskie centrum konferencyjne doznało szkód w postaci utraty przychodów i ograniczenia zaufania do marki ze strony najważniejszych klientów. Jednakże poprzez wdrożenie kompleksowych zabezpieczeń i skutecznych rozwiązań do zarządzania dostępnych w komputerach HP centrum mogło wykazać większą dbałość o cyberbezpieczeństwo.

**Szwajcarskie centrum konferencyjne to fikcyjna firma, która stała się celem cyberataku w wyprodukowanym przez HP Studio filmie „THE WOLF: TRUE ALPHA."*

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

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

[1] Rozwiązanie HP Sure Start Gen4 jest dostępne w produktach HP Elite i HP Pro 600 wyposażonych w procesory Intel® lub AMD 8. generacji.
[2] Aplikacja HP Sure Click jest dostępna na większości komputerów HP i obsługuje przeglądarki Microsoft® Internet Explorer oraz Chromium™. Obsługiwane załączniki obejmują pliki pakietu Microsoft Office (Word, Excel, PowerPoint) oraz pliki PDF tylko w trybie do odczytu, jeśli na komputerze zainstalowane jest oprogramowanie Microsoft Office lub Adobe Acrobat.
[3] Narzędzie HP Manageability Integration Kit nie jest zainstalowane fabrycznie, ale dostępne na stronie hp.com/go/clientmanagement.

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

Udostępnij współpracownikom

4AA7-3561PLE, sierpień 2018 r.