Prípadová štúdia

Keď sa letisko v Londýne stalo terčom deštruktívneho kyberútoku, hrozbu odhalili tlačiarne HP

Oficiálna záverečná správa o narušení dát

Odvetvie
Letecká doprava

Cieľ
Identifikácia a odstránenie slabých miest v postupoch kybernetickej bezpečnosti

Prístup
Vývoj komplexného plánu zabezpečenia v spolupráci s odborníkmi na zabezpečenie zo spoločnosti HP

IT hľadisko
- Aplikovanie bezpečnostných opatrení na koncové body internetu vecí
- Povolenie zabudovaných funkcií zabezpečenia v tlačiarňach HP
- Vylepšené monitorovanie zabezpečenia v celej sieti

Obchodné hľadisko
Zlepšená kybernetická bezpečnosť za účelom ochrany kritickej medzinárodnej infraštruktúry a udržania bezpečnosť cestujúcich

Prehľad

Letisko Londýn* obslúži každý deň viac ako 300 000 ľudí cestujúcich do 94 krajín sveta. Na letisku pracuje takmer 50 000 zamestnancov z 300 spoločností, ktorí tvoria prakticky jedno husto obývané mesto.

S rozvojom letiska sa jeho infraštruktúra čoraz viac prepájala a automatizovala. Letisko má dnes v sieti napojené interné systémy počnúc tlačiarňami cez osvetlenie až po vzduchotechniku. Na tlač, skenovanie a kopírovanie využíva dovedna viac ako 60 multifunkčných zariadení HP.

23. apríla 2018 prenikol cez systém osvetlenia do siete letiska kyberterorista známy ako The Wolf s cieľom šíriť v nej svoj malvér. Keďže je známy zneužívaním nedostatočne chránených koncových bodov, odborníci na zabezpečenie IT sa pri vyšetrovaní ihneď obrátili na tlačiarne HP Enterprise, aby ich záznamy o hrozbách využili na izoláciu a zastavenie útoku. Na ich prekvapenie, denníky obsahovali informácie od hackera s prezývkou The Wolf o mieste, odkiaľ bol útok vedený. Letisko sa potom obrátilo na spoločnosť HP, aby posilnilo zabezpečenie svojich koncových bodov.

Čo sa stalo

Keď The Wolf objavil zraniteľné miesto, pravdepodobne použitím phishingových e-mailov odoslaných používateľom v sieti, mohol infikovať systém osvetlenia IoT malvérom. Ten potom mohol po sieti šíriť a vytvoriť si zázemie v iných nemonitorovaných koncových zariadeniach.

Tím hackera s prezývkou The Wolf sa skrýval v nemonitorovaných zariadeniach internetu vecí (IoT). Keďže bol pre sieťové monitorovacie systémy neviditeľný, mohol pripraviť spustenie masívneho a deštruktívneho útoku z viacero miest súčasne.

Vedenie letiska sa zúfalo snažilo vypnúť viacero systémov a zároveň udržať v prevádzke kritickú infraštruktúru na riadenie letovej prevádzky a odbavenie cestujúcich.

Reakcia na útok

The Wolf bol najatý, aby zaútočil na sieť letiska. Pracovníci zabezpečenia IT letiska si *mysleli*, že ich sieť je pred hackermi dobre chránená, ale chýbala im viditeľnosť hrozieb, ktoré sa ukrývajú v zariadeniach internetu vecí (IoT).

Našťastie, letisko má tlačiarne HP Enterprise vybavené nástrojom HP Connection Inspector, ktorý zastavil malvér, pri podozrivých pokusoch „zavolať domov" na riadiace a príkazové servery hackerov.

Tieto akcie boli zachytené v systémových denníkoch tlačiarní. Keď zamestnanci oddelenia IT spozorovali, že niečo nie je v poriadku, skontrolovali systémové denníky a hľadali v nich podrobnosti o útoku. Kľúčovú rolu pri šírení malvéru hrá čas. Ak by pracovníci zabezpečenia IT prepojili systémové denníky s detekciou hrozieb v tlačiarňach so svojím systémom SIEM (Security Information and Event Monitoring), boli by na prienik okamžite upozornení.

Účinnejšie zabezpečenie než kedykoľvek predtým

Po prieniku do siete prehodnotili IT pracovníci používané postupy zabezpečenia.s poskytovateľom spravovaných tlačových služieb a poradcami pre zabezpečenie zo spoločnosti HP.

Už samotnou inštaláciou tlačiarní HP Enterprise bolo londýnske letisko na správnej ceste. Iba tlačiarne a multifunkčné zariadenia HP Enterprise robia monitoring narušení počas prevádzky (run time), majú nástroj HP Connection Inspector na odhaľovanie a zastavenie malvéru počas prevádzky a dokážu si vynútiť reštart. Pri spúšťaní softvér HP Sure Start kontroluje systém BIOS a dokáže ho automaticky opraviť, ak bol kód napadnutý, zatiaľ čo funkcia whitelisting kontroluje načítavaný firmvér.

Poskytovateľ spravovaných tlačových služieb nasadil aplikáciu HP JetAdvantage Security Manager, aby automaticky skontrolovala nastavenia zabezpečenia pri každom reštarte tlačiarne a vynulovala všetky zmenené nastavenia.

Zamestnanci letiska zodpovední za zabezpečenie IT taktiež prepojili systémové denníky s nástrojom SIEM. Na rozdiel od tlačiarní od iných výrobcov dokážu zariadenia HP generovať špeciálne denníky podľa jednotlivých hrozieb pre rôzne nástroje SIEM, takže pracovníci IT môžu získať upozornenia o možných bezpečnostných incidentoch v reálnom čase. Vďaka tomu sa tlačiarne HP menia na neoceniteľných strážcov siete.

Záver

Vďaka tlačiarňam HP Enterprise a stopám, ktoré The Wolf zanechal, dokázal bezpečnostný tím rýchlo izolovať útok, a predísť narušeniu prevádzky letiska, negatívnej publicite, pokutám a poškodeniu dobrého mena.

Používaním efektívnejších bezpečnostných postupov a plným využitím vstavaných bezpečnostných prvkov v tlačiarňach HP zvýšilo letisko úroveň zabezpečenia v celej svojej sieti.

** Letisko Londýn je fiktívna organizácia, ktorá čelí veľkému kyberútoku vo filme THE WOLF: TRUE ALPHA od spoločnosti HP Studio.*

Ďalšie informácie o riešeniach od HP:
Zabezpečenie tlače: hp.com/go/reinventsecurity
Zabezpečenie počítačov: hp.com/go/ComputerSecurity
Ak si chcete pozrieť film The Wolf, navštívte stránku: hp.com/thewolf

Registrácia na príjem noviniek
hp.com/go/getupdated

Zdieľať s kolegami

4AA7-3560SKE, august 2018