Případová studie

Když se Londýnské letiště stalo cílem ničivého kybernetického útoku, tiskárny HP dokázaly tuto hrozbu odhalit

Oficiální závěr k neoprávněnému přístupu k datům

Odvětví
Letectví

Cíl
Odhalení nedostatků v metodách kybernetického zabezpečení a jejich odstranění

Přístup
Vyvinutí uceleného plánu zabezpečení ve spolupráci s odborníky na zabezpečení HP

IT záležitosti
- Nasazení zabezpečení pro koncové body IoT
- Využití integrovaných bezpečnostních funkcí v tiskárnách HP
- Vylepšené monitorování zabezpečení v síti

Obchodní záležitosti
Zdokonalení ochrany před kybernetickými útoky z důležité infrastruktuře a zajištění bezpečí pro cestující

Přehled

Londýnské letiště* odbaví denně více než 300 000 osob, které cestují do některé z 94 zemí z celého světa. Na letišti pracuje téměř 50 000 zaměstnanců ze 300 společností. Jedná se prakticky o město v budově.

Společně s rozrůstáním letiště dochází i k neustálému propojování a automatizaci použité infrastruktury. Vnitřní systémy, od vzduchotechniky přes osvětlení až po tiskárny, jsou nyní součástí samotné letištní sítě. Více než 60 víceúčelových tiskáren HP po celé budově neustále něco tiskne, skenuje nebo kopíruje.

23. dubna 2018 se kybernetickému útočníkovi známému pouze pod přezdívkou „The Wolf“ (Vlk) podařilo připojit se k systému osvětlení a začít rozesílat svůj malware po celé síti. Tento útočník je známý svými metodami využívajícími nedostatečně chráněné koncové body a odborníci se proto v rámci vyšetřování útoku a ve snaze tento útok izolovat a zastavit okamžitě obrátili na protokoly hrozeb odeslané z tiskáren HP Enterprise. K překvapení všech tyto protokoly obsahovaly informace o napadení sítě a o místě, kde k průniku došlo. Po ukončení kauzy se Londýnské letiště obrátilo na společnost HP a společně dále posílili zabezpečení koncových bodů.

Co se stalo

Jakmile Vlk odhalil potřebné slabé místo v zabezpečení (pravděpodobně v podobě phishingových e-mailů odeslaných uživatelům v síti), odeslal připravený malware do systémů osvětlení v IoT. Po proniknutí mohl začít šířit svůj malware v síti a ukrýt jej do dalších nemonitorovaných koncových zařízení.

Ukrytý v nesledovaných zařízeních IoT se mohl tým útočníka nepozorovaně pohybovat v síti a vytvářet další body pro zahájení hromadného destruktivního útoku.

Vedení letiště vyvíjelo veškerou svoji energii ve snaze odpojit řadu systémů a současně zachovat v provozu důležitou infrastrukturu koordinující letadla a cestující.

Odpověď na útok

Vlk měl za úkol napadnou síť letiště. Oddělení letiště mající na starost zabezpečení IT bylo *přesvědčeno*, že je letištní síť dostatečně chráněná před hackery, ale bohužel měli nedostatečný přehled o hrozbách ukrytých v zařízeních IoT.

Naštěstí pro letiště jejich tiskárny HP Enterprise obsahují funkci HP Connection Inspector, která dokázala zastavit malware při jeho podezřelém pokusu o odpověď na ovládací servery hackera.

Tyto akce byly zaznamenány v sysLog protokolu tiskárny. Jakmile si zaměstnanci IT uvědomili, že se děje něco nekalého, mohli si jednoduše přečíst protokoly se záznamem o útoku. Kdykoli se malware šíří sítí, je včasné zakročení zásadní. Pokud by pracovníci IT zapojili výstup z protokolů tiskárny s detekcí hrozby do svého systému pro správu bezpečnostních informací a událostí (SIEM) byli by na proniknutí do sítě upozorněni okamžitě.

Lepší zabezpečení než kdy dříve

Po proniknutí hackera došlo k revizi bezpečnostních postupů ve spolupráci s poskytovatelem spravovaných tiskových služeb a poradcem pro zabezpečení HP.

Použití tiskáren HP Enterprise na Londýnském letišti již byl první krok správným směrem. Jedině tiskárny a víceúčelová zařízení HP Enterprise nabízí funkci neustálé detekce narušení a nástroj HP Connection Inspector dokáže odhalit a zastavit malware a vynutit restart zařízení. Během spouštění zařízení HP Sure Start prověří systém BIOS a dokáže zařízení zregenerovat v případě neoprávněných změn v kódu. Funkce povolování programů potom zkontroluje firmware.

Poskytovatel spravovaných tiskových služeb nasadil software HP JetAdvantage Security Manager, který automaticky kontroluje nastavení zabezpečení při každém restartu tiskárny a obnoví výchozí nastavení, pokud došlo k jeho úpravě.

Oddělení letiště mající na starost zabezpečení IT propojilo výstup protokolu tiskárny s nástrojem SIEM. Zařízení HP mají na rozdíl od tiskáren jiných výrobců schopnost odesílat výstup protokolů do nejrůznějších nástrojů SIEM a zaměstnanci IT tak mají neustále v reálném čase k dispozici upozornění na možné narušení zabezpečení. Tiskárny HP tak fungují jako nenahraditelní pohraniční strážci sítě.

Závěr

Letištní tiskárny HP Enterprise a stopy zanechané Vlkem umožnily oddělení pro zabezpečení velmi rychle izolovat probíhající útok a předejít tak narušení provozu, negativnímu názoru veřejnosti, pokutám za nedodržení souladu a poškození reputace.

Zavedením důslednějších bezpečnostních postupů a plným využitím integrovaných bezpečnostních funkcí tiskáren HP se letiště postaralo o celkové zvýšení zabezpečení své sítě.

**Londýnské letiště je fiktivním místem, které se stalo cílem rozsáhlého kybernetického útoku v krátkém filmu společnosti HP Studio: „THE WOLF: TRUE ALPHA“.*

Další informace o řešení HP:
Zabezpečení tisku: hp.com/go/reinventsecurity
Zabezpečení PC: hp.com/go/ComputerSecurity

Film „The Wolf“ můžete vidět zde:
hp.com/thewolf

Přihlásit se k odběru novinek
hp.com/go/getupdated

Sdílet dokument s kolegy

4AA7-3560CSE, srpen 2018