Esettanulmány

Amikor a Londoni Reptér egy pusztító kibertámadás célpontja lett, a HP nyomtatók észlelték a veszélyt

Hivatalos jelentés a támadásról

Iparág
Légi közlekedés

Cél
A kiberbiztonsági gyakorlatok gyenge pontjainak azonosítása és azok megoldása

Megközelítés
Átfogó biztonsági terv kifejlesztése HP biztonsági szakértőkkel

IT-pontok
- Alkalmazott védelmi intézkedések az IoT végpontjaira
- Engedélyezett beágyazott biztonsági funkciók a HP nyomtatókban
- A hálózat biztonságosabb felügyelete

Üzleti pontok
Javított kiberbiztonság a kulcsfontosságú nemzetközi infrastruktúra védelme és az utasok biztonsága érdekében

Áttekintés

A Londoni Repülőtér* naponta több mint 300 000 utast szolgál ki, akik 94 országba utaznak szerte a világon. Közel 50 000 ember dolgozik a repülőtéren 300 cégnél, amely így szinte egy sűrűn lakott város.

A repülőtér növekedésével infrastruktúrája egyre inkább összekapcsolódott és automatizálttá vált. Az olyan belső rendszerek, mint a HVAC-tól a világításon át a nyomtatókig, már a repülőtér hálózatán vannak. A nyomtatást, beolvasást és másolást egy 60+ HP MFP eszközből álló flotta végzi a repülőtér területén.

2018. április 23-án a „The Wolf” néven ismert kiberterrorista a reptér világítási rendszerét használta, hogy elérhesse és elterjessze a rosszindulatú programokat a hálózaton keresztül. Mivel The Wolf az alacsony biztonsággal rendelkező végpontok kihasználásáról ismert, az IT biztonsági szakértők azonnal a HP Enterprise nyomtatók fenyegetésnaplóihoz fordultak a vizsgálat részeként a támadás elszigetelése és leállítása érdekében. Meglepő módon, The Wolf nyomokat hagyott a naplófájlokban azzal kapcsolatban, hogy honnan ered a behatolás. Ezt követően a Londoni Reptér a HP-hoz fordult, hogy tovább növelje végpontbiztonságát.

Mi történt?

Miután The Wolf találta meg a biztonsági rést, valószínűleg a hálózaton lévő felhasználók számára küldött adathalász e-mailekkel megfertőzheti az IoT világítási rendszert rosszindulatú programokkal. Ezt követően kiterjesztheti a rosszindulatú programokat a hálózaton keresztül, és gyökereket verhet a többi nem felügyelt végponteszközön.

Jelenlétük elfedésével a nem felügyelt IoT eszközökön, The Wolf csapata rejtve maradhatott a hálózat felügyeleti rendszerei elől, miközben számos indítási pontot hoztak létre a pusztító erejű támadáshoz.

A reptér vezetése kétségbeesetten próbálta leállítani a rendszereket, miközben szükség volt a létfontosságú infrastruktúrára, amely a repülőgépeket és az utasokat kezelte.

Válasz a támadásra

The Wolfot felbérelték, hogy támadja meg a reptér hálózatát. A reptér IT biztonsági alkalmazottai *azt hitték*, hogy a reptér hálózata megfelelő védelemmel rendelkezik a hekkerekkel szemben, azonban az IoT eszközökben rejlő veszélyekkel nem számoltak.Szerencsére a reptér HP Enterprise nyomtatói HP Connection Inspectorral rendelkeztek, amely megállította a rosszindulatú programot, amikor gyanús „jelzési” próbálkozásokat indított a hekkerek parancs- és vezérlőszervereire.

A műveletek rögzítésre kerültek a nyomtatók naplófájljaiban. Miután az IT-személyzet észrevette, hogy baj van, ellenőrizték a naplófájlokat a támadásokkal kapcsolatban. Azonban az idő fontos tényező, amikor rosszindulatú programok terjednek a hálózaton. Ha az IT biztonsági személyzet a nyomtatók fenyegetésérzékelő naplófájljait összekapcsolta volna a biztonsági információ- és eseménykezelő (SIEM) rendszerrel, azonnal figyelmeztették volna őket a behatolás bekövetkezésekor.

Az eddigi legerősebb biztonság

A behatolást követően az IT-személyzet áttekintette a biztonsági gyakorlatokat a felügyelt nyomtatási szolgáltatójával és a HP biztonsági tanácsadóival.

A HP Enterprise nyomtatók telepítésével a Londoni Reptér már jó úton haladt. Csak a HP Enterprise nyomtatók és az MFP eszközök kínálnak futásidejű behatolásészlelést és HP Connection Inspectort, hogy észleljék és leállítsák a rosszindulatú programokat a műveletek során, és kényszerítsék az újraindítást. Az indításkor a HP Sure Start ellenőrzi a BIOS-t, amely meggyógyíthatja önmagát, ha a kód sérült, míg az engedélyezési lista ellenőrzi a firmware-t.

A felügyelt nyomtatási szolgáltatások biztosítója HP JetAdvantage Security Managert telepített, hogy automatikusan ellenőrizze a biztonsági beállításokat minden egyes alkalommal, amikor a nyomtató újraindul, és visszaállítsa a módosított beállításokat.

A reptéri IT biztonsági alkalmazottak emellett összekapcsolták a nyomtatók naplófájljait a saját SIEM-eszközükkel. Más gyártóktól származó nyomtatókkal ellentétben a HP eszközök számos SIEM-eszközhöz fenyegetés-specifikus naplót tudnak szolgáltatni, így az IT-személyzet képes valós időben figyelmeztetni a lehetséges biztonsági eseményekre. Így a HP nyomtatók felbecsülhetetlen értékű „megfigyelők” lettek a hálózatukban.

Összegzés

A repülőtér HP Enterprise nyomtatói és a The Wolf által hagyott nyomok miatt a biztonsági csapat képes volt elég gyorsan elszigetelni a támadást, hogy megakadályozza a műveleteket, a negatív nyilvánosságot, a megfelelőségi bírságokat és a márkát érő károkat.

Az erősebb biztonsági gyakorlatok alkalmazásával és a HP nyomtatók beépített biztonsági funkcióinak teljes kihasználásával a repülőtér biztonságossá tette az egész hálózatot.

**A Londoni Reptér egy fiktív szervezet, amelyet egy hatalmas kibertámadás ért a HP Studio filmjében, amelynek címe: „THE WOLF: IGAZI ALFA”.*

További tudnivalók a HP megoldásokról:
Nyomtatási biztonság: hp.com/go/reinventsecurity
PC biztonság: hp.com/go/ComputerSecurity

A „The Wolf” filmek megtekintéséhez:
hp.com/thewolf

Iratkozzon fel a friss hírekre
hp.com/go/getupdated

Megosztás a kollégákkal

4AA7-3560HUE, 2018. augusztus