Studija slučaja

Kada je zračna luka u Londonu bila meta opasnog računalnog napada, HP-ovi su pisači otkrili prijetnju

Službeno konačno izvješće o kršenju sigurnosti podataka

Djelatnost
Zrakoplovstvo

Cilj
Identificiranje slabih karika u praksama računalne sigurnosti i njihovo uklanjanje

Pristup
Razvoj sveobuhvatnog plana sigurnosti u suradnji s HP-ovim stručnjacima za sigurnost

IT
- Primjena sigurnosnih mjera na krajnje točke interneta stvari
- Ugrađene sigurnosne značajke za HP-ove pisače
- Poboljšan nadzor sigurnosti na razini mreže

Poslovanje
Poboljšana računalna sigurnost radi zaštite kritične međunarodne infrastrukture i održavanja sigurnosti putnika

Pregled

Zračna luka u Londonu* svakoga dana ima više od 300 000 putnika koji putuju u 94 države u različitim dijelovima svijeta. U zračnoj luci radi gotovo 50 000 ljudi iz 300 tvrtki, što taj prostor čini nalik gusto naseljenom gradu.

Rastom zračne luke infrastruktura je postala duboko povezana i automatizirana. Interni sustavi od HVAC-a do rasvjete i pisača sada su dio mreže zračne luke. Ispisivanje, skeniranje i kopiranje provodi se pomoću skupine uređaja koja obuhvaća više od 60 HP-ovih višenamjenskih pisača na kampusu.

Dana 23. travnja 2018. računalni je terorist poznat samo pod imenom "Vuk" iskoristio povezane sustave rasvjete u zračnoj luci da bi stekao pristup mreži i tako proširio svoj zlonamjerni softver. Budući da je poznat po svojim napadima putem nedovoljno zaštićenih krajnjih točaka, stručnjaci za sigurnost IT-ja odmah su u sklopu istrage krenuli gledati izvješća o prijetnjama na HP-ovim pisačima klase Enterprise da bi izolirali i zaustavili napad. Ono što ih je iznenadilo jest da su u izvješćima pronašli Vukove tragove koji su pokazali izvorište prodora. Zračna luka u Londonu nakon toga se obratila HP-u da bi dodatno unaprijedili sigurnost svojih krajnjih točaka.

Što se dogodilo?

Kada je Vuk pronašao slabu točku, najvjerojatnije slanjem e-pošte s ciljem krađe identiteta zaposlenika na mreži, sustav za rasvjetu interneta stvari mogao je zaraziti zlonamjernim softverom. Nakon toga je taj zlonamjerni softver mogao proširiti mrežom i tako stvoriti uporišta u drugim nenadziranim krajnjim uređajima.

Skrivanjem u nenadziranim uređajima interneta stvari Vukov je tim mogao ostati neotkriven tijekom analiza sustava za nadzor mreže i za to vrijeme razviti veći broj točaka za pokretanje velikog destruktivnog napada.

Osoblje zaduženo za upravljanje zračnom lukom očajnički je tražilo način isključivanja većeg broja sustava, a da pri tome ne zaustave kritične elemente infrastrukture, kao što su zrakoplovi i putnici.

Odgovor na napad

Vuk je bio angažiran da napadne mrežu zračne luke. Osoblje zaduženo za sigurnost IT-ja u zračnoj luci *mislilo* je da je mreža zračne luke dobro zaštićena od hakera, no nisu obratili pozornost na prijetnje koje se skrivaju u uređajima interneta stvari.

Srećom, HP-ovi pisači klase Enterprise koji su se koristili u zračnoj luci imali su značajku HP Connection Inspector, koja je zaustavila zlonamjerni softver pri pokušaju reagiranja na naredbe hakera, kao i pri preuzimanju kontrole nad poslužiteljima.

Akcije su bile zabilježene u syslog izvješćima pisača. Kada je osoblje zaduženo za IT shvatilo da nešto nije u redu, provjerili su syslog izvješća i potražili pojedinosti o napadu. U slučaju širenja zlonamjernog softvera mrežom najvažnije je vrijeme. Da je osoblje zaduženo za sigurnost IT-ja povezalo syslog izvješća o otkrivanju prijetnji sa svojim sustavom za sigurnosni nadzor informacija i događaja (SIEM), obavijest bi bila aktivirana već u trenutku prodora.

Zaštita jača nego ikada prije

Nakon kršenja sigurnosti osoblje zaduženo za IT pregledalo je sigurnosne pravilnike pružatelja usluga upravljanog ispisa i HP-ovih savjetnika za sigurnost.

Korištenje HP-ovih pisača klase Enterprise zračnu je luku u Londonu usmjerilo u pravom smjeru. Samo HP-ovi pisači klase Enterprise i višenamjenski pisači pružaju otkrivanje prodora tijekom rada i značajku HP Connection Inspector koja detektira i zaustavlja zlonamjerni softver tijekom rada te prisilno ponovno pokreće uređaj. Prilikom pokretanja sustava HP Sure Start provjerava BIOS te prema potrebi pokreće samooporavak u slučaju oštećenja koda, dok odobravanje firmvera provjerava stanje firmvera.

Pružatelj usluga upravljanog ispisa implementirao je HP JetAdvantage Security Manager da bi automatski provjeravao sigurnosne postavke prilikom svakog pokretanja pisača te prema potrebi resetirao promijenjene postavke.

Osoblje zaduženo za sigurnost IT-ja u zračnoj luci počelo je povezivati syslog izvješća s alatom SIEM. Za razliku od pisača drugih proizvođača, HP-ovi uređaji mogu pružiti izvješća o prijetnjama za mnoge SIEM alate da bi osoblje zaduženo za IT moglo dobiti upozorenja o mogućim sigurnosnim incidentima u stvarnom vremenu. Na taj će način HP-ovi pisači postati nezamjenjive "oči" mreže.

Zaključak

Zbog HP-ovih pisača klase Enterprise koji se koriste u zračnoj luci i tragova koje je Vuk ostavio, tim zadužen za sigurnost mogao je izolirati napad dovoljno brzo da spriječi prekide u radu, negativan publicitet, kazne zbog neusklađenosti i formiranje loših mišljenja o tvrtki.

Implementiranjem strožih sigurnosnih pravilnika i maksimalnim iskorištavanjem ugrađenih sigurnosnih značajki HP-pisača zračna je luka postrožila sigurnost u svim dijelovima mreže.

**Zračna luka u Londonu izmišljena je tvrtka koja je bila meta velikog računalnog napada u filmu studija tvrtke HP: "VUK: ISTINSKI ALFA".*

Dodatne informacije o HP-ovim rješenjima potražite na adresi:
Sigurnost ispisa: hp.com/go/reinventsecurity
Zaštita računala: hp.com/go/ComputerSecurity
Da biste pogledali filmove o "Vuku", posjetite:
hp.com/thewolf

Registrirajte se za ažuriranja
hp.com/go/getupdated

Podijelite s kolegama

4AA7-3560HRE, kolovoz 2018.