Studiu de caz

Când aeroportul din Londra a fost vizat de un atac cibernetic distructiv, imprimantele HP au detectat ameninţarea

Raportul oficial privind breşa de date

Industrie
Aviatică

Obiectiv
Identificarea verigilor slabe din practicile de securitate cibernetică şi abordarea acestora

Abordare
A fost dezvoltat un plan de securitate cuprinzător în parteneriat cu experţi în securitate de la HP

IT contează
- S-au aplicat măsuri de securitate la punctele terminale IoT
- S-au activat caracteristicile de securitate încorporate în imprimantele HP
- S-a îmbunătăţit monitorizarea securităţii prin reţea

Afacerea contează
S-a îmbunătăţit securitatea cibernetică pentru a proteja infrastructura internaţională critică şi a menţine siguranţa călătorilor

Prezentare generală

Aeroportul din Londra* deserveşte zilnic peste 300.000 de călători, care zboară spre 94 de ţări de pe glob. Aproape 50.000 de oameni din 300 de companii lucrează la aeroport, acesta devenind practic un oraş condensat.

Pe măsură ce aeroportul s-a dezvoltat, infrastructura acestuia a devenit din ce în ce mai conectată şi mai automatizată. Sistemele interne, de la încălzire, ventilaţie şi aer condiţionat, până la iluminat şi imprimante sunt acum în reţeaua aeroportului. Operaţiile de imprimare, scanare şi copiere sunt efectuate de o flotă de peste 60 de echipamente MFP HP, instalate în diverse clădiri.

Pe 23 aprilie 2018, teroristul cibernetic cunoscut sub numele „The Wolf” a utilizat sistemele de iluminare conectate ale aeroportului pentru a obţine acces şi a răspândi malware-ul său în reţea. Deoarece el este cunoscut pentru metodele sale de a utiliza punctele terminale insuficient protejate, experţii în securitate IT au examinat imediat jurnalele de ameninţări de la imprimantele HP Enterprise în cadrul investigaţiei, pentru a izola şi a opri atacul. În mod surprinzător, jurnalele conţineau indicii de la The Wolf referitoare la locul de iniţiere a intruziunii. Ulterior, aeroportul din Londra a apelat la HP pentru a perfecţiona securitatea punctelor terminale.

Ce s-a întâmplat

Odată ce The Wolf a găsit vulnerabilitatea, probabil trimiţând e-mailuri infectate utilizatorilor din reţea, a putut să infecteze cu malware sistemul de iluminare IoT. El a putut apoi să-şi extindă malware-ul prin reţea, creând avanposturi în alte dispozitive terminale nemonitorizate.

Ascunzându-şi prezenţa în dispozitivele IoT nemonitorizate, echipa lui The Wolf a putut rămâne nedescoperită de sistemele de monitorizare a reţelei, în timp ce îşi dezvolta mai multe puncte de lansare pentru un atac distructiv masiv.

Într-o situaţie disperată, conducerea aeroportului a încercat să oprească mai multe sisteme, în timp ce infrastructura critică, precum avioanele şi pasagerii, era menţinută în mişcare.

Răspunsul la atac

The Wolf a fost angajat să atace reţeaua aeroportului. Personalul de securitate IT al aeroportului *credea* că reţeaua aeroportului este bine protejată împotriva hackerilor, dar nu aveau vizibilitate asupra ameninţărilor ascunse în dispozitivele IoT.

Din fericire, imprimantele HP Enterprise ale aeroportului includeau HP Connection Inspector, care a oprit malware-ul când făcea încercări suspecte de a pătrunde în sistem la comanda hackerilor şi de a controla serverele.

Acţiunile au fost înregistrate în jurnalele de sistem ale imprimantelor. Odată ce personalul IT şi-a dat seama că ceva nu este în regulă, acesta a verificat jurnalele de sistem pentru a vedea detalii despre atac. Dar timpul este esenţial când malware-ul se răspândeşte prin reţea. Dacă personalul de securitate IT ar fi conectat jurnalele de sistem ale imprimantelor pentru detectarea ameninţărilor la sistemul lor de monitorizare a evenimentelor şi informaţiilor de securitate (Security information and event monitoring - SIEM), aceştia ar fi fost alertaţi imediat ce s-ar fi produs intruziunea.

Securitate mai puternică decât oricând

După breşă, personalul IT a revizuit practicile de securitate împreună cu furnizorul lor de servicii de imprimare gestionată şi cu consultaţii în securitate de la HP.

Prin instalarea imprimantelor HP Enterprise, aeroportul din Londra era deja pe calea cea bună. Numai imprimantele şi echipamentele MFP HP Enterprise oferă detectarea intruziunilor în timpul funcţionării şi instrumentul HP Connection Inspector pentru a detecta şi a opri malware-ul în timpul operaţiilor şi a forţa o repornire. La pornire, HP Sure Start verifică BIOS-ul şi îl poate repara automat dacă codul a fost compromis, efectuând totodată verificări ale firmware-ului conform listelor de acces permis.

Furnizorul de servicii de imprimare gestionată a implementat HP JetAdvantage Security Manager pentru a verifica automat setările de securitate de fiecare dată când o imprimantă este repornită şi pentru a reseta orice setare alterată.

De asemenea, personalul de securitate IT al aeroportului a făcut pasul de a conecta jurnalele de sistem ale imprimantelor la instrumentul lor SIEM. Spre deosebire de imprimantele de la alţi furnizori, dispozitivele HP pot să furnizeze jurnale specifice despre ameninţări multor instrumente SIEM, astfel încât personalul IT să poată primi alerte în timp real despre posibilele incidente de securitate. Aceste caracteristici transformă imprimantele HP în „ochi" nepreţuiţi, aţintiţi asupra reţelei lor.

Concluzie

Datorită imprimantelor HP Enterprise ale aeroportului şi indiciilor lăsate de The Wolf, echipa de securitate a fost capabilă să izoleze atacul suficient de rapid pentru a evita întreruperea operaţiilor, publicitatea negativă, amenzile de neconformitate şi discreditarea brandului.

Utilizând practici pentru o securitate mai puternică şi profitând la maximum de caracteristicile de securitate încorporate ale imprimantelor HP pe care le deţine, aeroportul a intensificat securitatea în întreaga reţea.

**Aeroportul din Londra este o organizaţie fictivă, supusă unui atac cibernetic amplu, în filmul realizat de Studiourile HP, „THE WOLF: TRUE ALPHA".*

Pentru mai multe informaţii despre soluţiile HP:
Securitatea imprimării:
hp.com/go/reinventsecurity
Securitatea PC-urilor:
hp.com/go/ComputerSecurity

Pentru a vedea filmele „The Wolf", vizitaţi:
hp.com/thewolf

Înregistraţi-vă pentru actualizări
hp.com/go/getupdated

Partajaţi cu colegii

4AA7-3560ROE, august 2018