Casestudie

Da London Lufthavn blev målet for et ødelæggende cyberangreb, registrerede HP's printere truslen

Officiel sammendragsrapport om databruddet

Industri
Luftfart

Mål
Identificering af svage led i cybersikkerhedspraksisser og håndtering af dem

Fremgangsmåde
Udvikling af en omfattende sikkerhedsplan i samarbejde med HP's sikkerhedseksperter

IT-anliggender
- Implementering af sikkerhedstiltag i IoT-slutpunkter
- Aktivering af indbyggede sikkerhedsfunktioner i HP-printere
- Forbedring af sikkerhedsovervågning i hele netværket

Virksomhedsanliggender
Forbedring af cybersikkerhed til beskyttelse af international infrastruktur og opretholdelse af passagersikkerhed

Oversigt

London Lufthavn* servicerer mere end 300.000 passagerer hver dag, der rejser til 94 lande i hele verden. Næsten 50.000 personer fra 300 virksomheder arbejder i lufthavnen, hvilket reelt gør den til en komprimeret by.

Efterhånden som lufthavnen er vokset, er dens infrastruktur blevet mere forbundet og automatiseret. Interne systemer, fra HVAC til belysning og printere, er nu på lufthavnens netværk. Udskrivning, scanning og kopiering udføres af en flåde på mere end 60 HP-multifunktionsprintere, der er spredt over hele lufthavnsområdet.

D. 23. april 2018 brugte cyberterroristen "The Wolf" lufthavnens forbundne belysningssystem til at få adgang til netværket og sprede malware. Da han er kendt for at udnytte mindre sikre slutpunkter, fokuserede it-sikkerhedseksperter øjeblikkeligt på trusselslogfiler fra deres HP Enterprise-printere som en del af efterforskningen for at isolere og stoppe angrebet. Overraskende nok indeholdt logfilerne spor fra The Wolf om, hvor indtrængningen startede. Herefter henvendte London Lufthavn sig til HP for at forbedre deres slutpunktssikkerhed yderligere.

Hvad skete der?

Da The Wolf fandt en sårbarhed, der sandsynligvis stammede fra phishing-e-mails til brugere på netværket, kunne han inficere IoT-belysningssystemet med malware. Derefter kunne han udbygge sin malware gennem netværket og få fodfæste i andre slutpunktsenheder, der ikke var under opsyn.

Ved at skjule deres tilstedeværelse i IoT-enheder, der ikke var under opsyn, kunne The Wolfs team forblive uopdaget af netværksovervågningssystemerne, imens de udviklede flere startpunkter for et massivt og ødelæggende angreb.

Ledelsen i lufthavnen forsøgte desperat at lukke flere systemer ned, imens de bevarede den vigtigste infrastruktur, som fly og passagerer, aktive.

Reaktion på angrebet

The Wolf var hyret til at angribe lufthavnens netværk. It-sikkerhedspersonalet i lufthavnen *troede*, at lufthavnens netværk var tilstrækkeligt beskyttet imod hackere, men de manglede synlighed mod trusler, der skjulte sig i IoT-enheder.

Heldigvis havde lufthavnens HP Enterprise-printere HP Connection Inspector, der stoppede malwaren, da den udførte mistænkelige forsøg på at "ringe hjem" til hackernes kommando- og kontrolservere.

Handlingerne blev fanget af printerens systemlogfiler. Da it-personalet indså, at noget var galt, kontrollerede de systemlogfilerne for oplysninger om angrebet. Men tiden er altafgørende, når malware spreder sig på netværket. Hvis it-sikkerhedspersonalet havde forbundet printernes trusselsregistreringssystemlogfiler til deres sikkerheds- og hændelsesovervågningssystem (SIEM), ville de være blevet underrettet øjeblikkeligt, da indtrængningsforsøget fandt sted.

Stærkere sikkerhed end nogensinde før

Efter bruddet evaluerede it-personalet sikkerhedspraksisserne sammen med deres leverandør af administrerede udskriftstjenester samt HP's sikkerhedsrådgivere.

Ved at installere HP Enterprise-printere var London Lufthavn allerede på rette vej. Kun HP Enterprise-printere og MFP'er leverer run-time-registrering af indtrængen og HP Connection Inspector, der registrerer og stopper malware, mens enheden kører, og gennemtvinger en genstart. Ved opstart kontrollerer HP Sure Start BIOS og kan reparere sig selv, hvis koden er blevet kompromitteret, samtidig med at den hvidlistekontrollerer firmwaren.

Leverandøren af administrerede udskriftstjenester implementerede HP JetAdvantage Security Manager, så den automatisk kontrollerer sikkerhedsindstillingerne, hver gang en printer genstartes, og nulstiller eventuelle ændrede indstillinger.

Lufthavnens it-sikkerhedspersonale besluttede også at tilslutte printersystemlogfilerne til deres SIEM-system. I modsætning til printere fra andre producenter kan HP's enheder levere trusselsspecifikke logfiler til mange SIEM-værktøjer, så it-personalet får advarsler i realtid ved mulige sikkerhedshændelser. Dette gør HP's printere til uvurderlige "øjne" på deres netværk.

Konklusion

På grund af lufthavnens HP Enterprise-printere og de spor, som The Wolf efterlod, var sikkerhedsteamet i stand til hurtigt at isolere angrebet og undgå driftsafbrydelser, negativ omtale, bøder for manglende kontraktoverholdelse og skade på deres brand.

Ved at anvende stærkere sikkerhedspraksisser og drage fordel af de indbyggede sikkerhedsfunktioner i deres HP-printere har lufthavnen strammet op på sikkerheden i hele deres netværk.

** London Lufthavn er en fiktiv organisation , der blev målrettet i et stort cyberangreb i HP Studios film, "THE WOLF: TRUE ALPHA".*

Få flere oplysninger om HP's løsninger:
Printersikkerhed: hp.com/go/reinventsecurity
PC-sikkerhed: hp.com/go/ComputerSecurity
Se "The Wolf"-filmene på:
hp.com/thewolf

Tilmeld dig for at få opdateringer
hp.com/go/getupdated

Del med kolleger

4AA7-3560DAE, august 2018