Kasusstudie

Da London lufthavn ble angrepet av et destruktivt cyberangrep, registrerte HP-skrivere trusselen

Offisiell avslutningsrapport for databruddet

Bransje
Luftfart

Mål
Finne svake ledd i cybersikkerhetspraksiser
Og rette opp i dem

Tilnærming
Utvikle en omfattende sikkerhetsplan i partnerskap med HPs sikkerhetseksperter

IT-forhold
- Iverksatte sikkerhetstiltak for IoT-sluttpunkter
- Aktiverte innebygde sikkerhetsfunksjoner i HP-skrivere
- Forbedret sikkerhetsovervåking over hele nettverket

Forretningsforhold
Forbedret cybersikkerhet for å beskytte kritisk viktig internasjonal infrastruktur og ivareta passasjerenes sikkerhet

Oversikt

London lufthavn* betjener over 300 000 passasjerer hver dag, mens de reiser mellom 94 land verden rundt. Nesten 50 000 mennesker fra 300 selskaper arbeider ved lufthavnen, hvilket praktisk talt gjør den til en komprimert by.

Etter hvert som lufthavnen har vokst, har infrastrukturen i stadig større grad blitt tilkoblet og automatisert. Interne systemer fra HVAC til belysning og skrivere er nå på lufthavnens nettverk. Utskrift, skanning og kopiering utføres av en flåte på over 60 HP-flerfunksjonsskrivere distribuert gjennom campuset.

23. april, 2018, brukte cyberterroristen kun kjent som «The Wolf» lufthavnens tilkoblede belysningssystemer for å få tilgang og spre skadelig programvare gjennom nettverket. Siden han er kjent for å benytte utilstrekkelig sikrede sluttpunkter, fant IT-sikkerhetsekspertene umiddelbart frem til trussellogger fra HP Enterprise-skriverne, som en del av granskningen for å isolere og stoppe angrepet. Overraskende nok inneholdt loggene spor fra The Wolf om hvor inntrengningen stammet fra. Etterpå henvendte London lufthavn seg til HP for å bedre sluttpunktsikkerheten sin ytterligere.

Hva skjedde

Da The Wolf fant en sårbarhet, sannsynligvis gjennom phishing-e-post til nettverkets brukere, kunne han infisere IoT-belysningssystemet med skadelig programvare. Han kunne så spre programvaren gjennom nettverket, og gi seg selv fotfeste i andre uovervåkede sluttpunktenheter.

Ved å skjule sin tilstedeværelse i uovervåkede IoT-enheter kunne The Wolfs team gjemme seg for nettverkets overvåkingssystemer mens de utviklet flere startpunkter for et omfattende ødeleggende angrep.

Lufthavnens administrasjon var plutselig i en desperat situasjon der de prøvde å deaktivere flere systemer mens de holdt kritisk viktig infrastruktur som fly og passasjerer i gang.

Svar på angrepet

The Wolf hadde blitt hyret for å angripe lufthavnens nettverk. Lufthavnens IT-sikkerhetsansatte *mente* at lufthavnens nettverk var godt beskyttet mot hackere, men de hadde ikke oversikt over trusler som var skjult i IoT-enheter.

Heldigvis hadde lufthavnens HP Enterprise-skrivere HP Connection Inspector inkludert, som stoppet den skadelige programvaren mens den gjorde mistenkelige forsøk på å «ringe hjem» til hackernes kommando- og kontrollservere.

Handlingene ble registrert i skriverens systemlogger. Da IT-personalet forsto at noe var galt, sjekket de systemloggene for informasjon om angrepet. Men tiden er avgjørende når skadelig programvare sprer seg gjennom nettverket. Dersom de IT-sikkerhetsansatte hadde koblet skrivernes trusselregistrerende systemloggfiler til sitt SIEM-system (security information and event monitoring), ville de ha blitt varslet med en gang inntrengningen skjedde.

Sterkere sikkerhet enn noensinne

Etter hendelsen gjennomgikk de IT-ansatte sikkerhetsrutinene med leverandøren av den styrte utskriftstjenesten og HP Security Advisors.

Ved å installere HP Enterprise-skrivere var London lufthavn allerede på rett spor. Kun HP Enterprise-skrivere og MFP-er tilbyr inntrengerregistrering i under drift og HP Connection Inspector for å registrere og stoppe skadelig programvare ved drift og tvinge en omstart. Ved oppstart kontrollerer HP Sure Start BIOS, og den kan selvhelbrede dersom koden har blitt kompromittert, mens den også hvitelister fastvaren.

Leverandøren av styrte utskriftstjenester distribuerte HP JetAdvantage Security Manager for å automatisk kontrollere sikkerhetsinnstillinger hver gang en skriver startes på nytt, og tilbakestille alle endrede innstillinger.

Lufthavnens IT-sikkerhetsansatte gikk også til det skritt å koble skrivernes systemlogger til sitt SIEM-verktøy. I motsetning til skrivere fra andre produsenter, kan HPs enheter levere trusselspesifikke logger til mange SIEM-verktøy, slik at de IT-ansatte kan varsles i sanntid om mulige sikkerhetshendelser. Dette gjør HP-skrivere til uvurderlige «øyne» på nettverket deres.

Konklusjon

På grunn av lufthavnens HP Enterprise-skrivere og sporene The Wolf etterlot seg, kunne sikkerhetsteamet isolere angrepet hurtig nok til å unngå driftsavbrudd, negativ publisitet, bøter for manglende samsvar og skade på merkevaren.

Ved å ta i bruk sterkere sikkerhetspraksiser og dra full nytte av de innebygde sikkerhetsfunksjonene i HP-skriverne har lufthavnen fått bedre sikkerhet gjennom hele nettverket.

**London lufthavn er en fiktiv organisasjon som var målet i et omfattende cyberangrep i HP Studios-filmen, «THE WOLF: TRUE ALPHA."*

For mer informasjon om HP-løsninger:
Utskriftssikkerhet:
hp.com/go/reinventsecurity
PC-sikkerhet: hp.com/go/ComputerSecurity
Hvis du ønsker å se «The Wolf»-filmer, kan du gå til: hp.com/thewolf

Registrer deg for oppdateringer
hp.com/go/getupdated

Del med kolleger

4AA7-3560NOE, august 2018