Casestudy

Toen London Airport getroffen werd door een destructieve cyberaanval, hebben HP printers de dreiging gedetecteerd

Officieel afsluitend rapport van de data-inbreuk

Industrie
Luchtvaart

Doelstelling
Identificeren van zwakke schakels in cyberbeveiligingsmethoden en deze aanpakken

Aanpak
Een uitgebreid beveiligingsplan ontwikkeld in samenwerking met HP beveiligingsexperts

IT-voordelen
- Beveiligingsmaatregelen op IoT-eindpunten toegepast
- Ingebouwde beveiligingskenmerken ingeschakeld in HP printers
- Beveiligingsbewaking in het hele netwerk verbeterd

Bedrijfsmatige aspecten
Cyberbeveiliging verbeterd om kritieke internationale infrastructuur te beschermen en de veiligheid van passagiers te handhaven

Overzicht

Dagelijks maken meer dan 300.000 passagiers gebruik van London Airport* die naar 94 landen over de hele wereld reizen. Er werken bijna 50.000 mensen van 300 bedrijven op de luchthaven, waardoor het bijna een compacte stad is.

Naarmate de luchthaven is gegroeid, is de infrastructuur steeds meer verbonden en geautomatiseerd. Interne systemen van HVAC tot verlichting en printers bevinden zich nu op het netwerk van de luchthaven. Printen, scannen en kopiëren wordt uitgevoerd door een vloot van meer dan 60 HP MFP's, verspreid over de hele campus.

Op 23 april 2018 heeft de cyberterrorist die alleen bekend staat als “The Wolf” de aangesloten verlichtingssystemen van de luchthaven gebruikt om toegang te krijgen en zijn malware over het netwerk te verspreiden. Omdat hij bekendstaat om zijn prestaties met behulp van onvoldoende beveiligde eindpunten, hebben de IT-beveiligingsexperts onmiddellijk de dreigingslogboeken van hun HP Enterprise-printers geraadpleegd als onderdeel van het onderzoek om de aanval te isoleren en te stoppen. Verrassend genoeg bevatten de logboeken aanwijzingen van The Wolf over waar de indringing vandaan kwam. Naderhand heeft London Airport zich tot HP gericht om hun eindpuntbeveiliging verder te verbeteren.

Wat er gebeurde

Nadat The Wolf een kwetsbaarheid had gevonden, waarschijnlijk door phishing-e-mails naar gebruikers op het netwerk te sturen, kon hij het IoT-verlichtingssysteem met malware infecteren. Vervolgens kon hij zijn malware via het netwerk uitbreiden, waardoor hij voet aan de grond kreeg in andere niet-gecontroleerde eindpuntapparaten. Door hun aanwezigheid in niet-bewaakte IoT-apparaten te verbergen, kon het team van The Wolf onopgemerkt blijven door de netwerkbewakingssystemen terwijl ze meerdere startpunten ontwikkelden voor een massale vernietigingsaanval.

Het luchthavenbeheer merkte dat het wanhopig probeerde om meerdere systemen uit te schakelen en tegelijkertijd kritische infrastructuur zoals vliegtuigen en passagiers in beweging te houden.

Reageren op de aanval

The Wolf was ingehuurd om het netwerk van de luchthaven aan te vallen. IT-beveiligingsmedewerkers van de luchthaven *dachten* dat het netwerk van de luchthaven goed beschermd was tegen hackers, maar ze konden niet e bedreigingen zien die in IoT-apparaten waren verborgen.

Gelukkig bevatten de HP Enterprise-printers van de luchthaven HP Connection Inspector waarmee de malware werd gestopt toen er verdachte pogingen waren gedaan om "naar huis" te bellen naar de commando- en controleservers van de hackers.

De acties zijn vastgelegd in de systeemlogboeken van de printer. Zodra de IT-medewerkers zich realiseerden dat er iets mis was, controleerden ze de systeemlogboeken voor informatie over de aanval. Maar tijd is van essentieel belang wanneer malware zich via het netwerk verspreidt. Als de IT-beveiligingsmedewerkers de systeemlogboeken van de printer voor het detecteren van bedreigingen met hun SIEM-systeem (Security Information and Event Monitoring) hadden verbonden, zouden ze onmiddellijk zijn gewaarschuwd voor de inbreuk.

Sterkere beveiliging dan ooit

Na de inbreuk hebben de IT-medewerkers de beveiligingsmethoden met hun managed print services-provider en HP beveiligingsadviseurs beoordeeld.

Door HP Enterprise-printers te installeren, was London Airport al op de goede weg. Alleen HP Enterprise-printers en MFP's bieden runtime-inbraakdetectie en HP Connection Inspector om malware te detecteren en te stoppen tijdens bewerkingen en een reboot te forceren. Bij het opstarten controleert HP Sure Start het BIOS en kan het zichzelf genezen als de code is aangetast, terwijl whitelisting de firmware controleert.

De managed print services-provider heeft HP JetAdvantage Security Manager geïmplementeerd om automatisch de beveiligingsinstellingen te controleren wanneer een printer opnieuw wordt opgestart en om eventuele gewijzigde instellingen opnieuw in te stellen.

Het IT-beveiligingspersoneel van de luchthaven heeft ook de stap gezet om de systeemlogboeken van de printer aan hun SIEM-tool te koppelen. In tegenstelling tot printers van andere fabrikanten, kunnen HP apparaten dreigingsspecifieke logboeken leveren aan vele SIEM-tools, zodat IT-medewerkers in real time meldingen kunnen ontvangen over mogelijke beveiligingsincidenten. Zo houden HP printers als het ware 'zicht' op hun netwerk.

Conclusie

Vanwege de HP Enterprise-printers van de luchthaven en de aanwijzingen die The Wolf heeft achtergelaten, kon het beveiligingsteam de aanval snel genoeg isoleren om verstoring van de activiteiten, negatieve publiciteit, boetes wegens niet-naleving en schade aan het merk te voorkomen.

Door strengere beveiligingsmethoden toe te passen en volledig te profiteren van de ingebouwde beveiligingsfuncties van hun HP printers heeft de luchthaven de beveiliging in het hele netwerk aangescherpt.

**London Airport is een fictieve organisatie die het doel is van een grote cyberaanval in de film van HP Studio, "THE WOLF: TRUE ALPHA."*

Kijk voor meer informatie over HP oplossingen op:
Printerbeveiliging: hp.com/go/reinventsecurity
Pc-beveiliging: hp.com/go/ComputerSecurity

Als u films van "The Wolf" wilt zien, gaat u naar:
hp.com/thewolf

Meld u aan voor updates op
hp.com/go/getupdated

4AA7-3560NLE, augustus 2018