Fallstudie

När London Airport utsattes för en skadlig cyberattack upptäckte HP-skrivare hotet

Officiell sammanfattningsrapport över dataintrånget

Industri
Flyg

Målsättning
Identifiera svaga länkar i cybersäkerhetsrutiner och åtgärda dem.

Metod
Utvecklade en heltäckande säkerhetsplan i samarbete med HPs säkerhetsexperter.

IT-frågor
- Tillämpade säkerhetsåtgärder för IoT-slutpunkter.
- Aktiverade inbyggda säkerhetsfunktioner i HP-skrivare.
- Förbättrade säkerhetsövervakningen i hela nätverket.

Verksamhetsfrågor
Förbättrad cybersäkerhet för att skydda viktig internationell infrastruktur och bibehålla passagerarnas säkerhet.

Översikt

London Airport* betjänar fler än 300 000 passagerare varje dag under deras resor till fler än 94 länder världen över. Nästan 50 000 människor från 300 olika företag arbetar på flygplatsen, så den är praktiskt taget en egen stad i miniformat.

I och med att flygplatsen har vuxit har dess infrastruktur blivit allt mer ansluten och automatiserad. Interna system, från värme, ventilation och luftkonditionering, till belysning och skrivare, är nu anslutna till flygplatsens nätverk. Utskrift, skanning och kopiering utförs med en skrivarpark på över 60 HP-multifunktionsskrivare utspridda över området.

Den 23 april 2018 använde cyberterroristen som endast är känd som "The Wolf" flygplatsens anslutna belysningssystem för att få åtkomst till nätverket och sprida sin malware. The Wolf är känd för att utnyttja enheter som inte är tillräckligt skyddade, så IT-säkerhetsexperterna vände sig omedelbart till loggarna över hot från HP Enterprise-skrivarna, som en del i sin utredning och för att isolera och stoppa attacken. Något överraskade innehöll loggarna ledtrådar från The Wolf angående var intrånget startade. När det hela var över bad London Airport HP om hjälp med att ytterligare stärka sin enhetssäkerhet.

Vad hände?

När The Wolf väl hittat en sårbarhet, sannolikt nätfiskemeddelanden till nätverkets användare, kunde cyberterroristen infektera IoT-belysningssystemet med malware. Malware kunde sedan spridas genom nätverket, där fästen skapades i andra oövervakade enheter.

Genom att de dolde sin närvaro i oövervakade IoT-enheter kunde The Wolfs team förbli oupptäckta av nätverksövervakningssystemen medan de utvecklade flera attackpunkter för ett massivt förödande angrepp.

Flygplatsens ledning försökte desperat stänga ner flera system, och samtidigt hålla igång viktig infrastruktur som flygplanen och passagerartrafiken.

Svar på attacken

The Wolf hade anlitats för att angripa flygplatsens nätverk. Flygplatsens IT-säkerhetspersonal *trodde* att flygplatsens nätverk var väl skyddat mot hackare, men de saknade insikt i hot som dolde sig i IoT-enheter.

Lyckligtvis var flygplatsens HP Enterprise -skrivare utrustade med säkerhetsfunktionen HP Connection Inspector, och den stoppade malware när koden gjorde misstänkta försök att "ringa hem" till hackarnas kommando- och kontrollservrar.

Åtgärderna sparades i skrivarnas systemloggar. När IT-personalen insåg att något var fel tittade de i systemloggarna för uppgifter om attacken. Men snabbt agerande är viktigt när malware sprider sig i nätverket. Om IT-säkerhetspersonalen hade anslutit skrivarnas hotupptäcktslogg till sitt SIEM-system (säkerhetsinformation och händelseövervakning) så skulle de ha larmats omedelbart när intrånget skedde.

Starkare säkerhet än någonsin

Efter intrånget granskade IT-personalen sina säkerhetsrutiner tillsammans med sin leverantör av managerade utskriftstjänster och HPs säkerhetsrådgivare.

Genom att ha HP Enterprise-skrivare installerade var London Airport redan på rätt väg. Endast HP Enterprise-skrivare och MFP:er erbjuder intrångsidentifiering under körning och HP Connection Inspector för att stoppa aktiviteter från malware och tvinga fram en omstart. Vid omstarten kontrollerar HP Sure Start BIOS, och programvaran kan vid behov självläka BIOS om koden har ändrats. Via vitlistning kontrolleras även den inbyggda programvaran.

Leverantören av utskrift som tjänst driftsatte HP JetAdvantage Security Manager för automatisk kontroll av säkerhetsinställningarna varje gång en skrivare startas om, samt återställning av alla ändrade inställningar.

Flygplatsens IT-säkerhetspersonal vidtog även åtgärden att ansluta skrivarnas systemloggar till sitt SIEM-verktyg. Till skillnad från skrivare från andra tillverkare kan HP-enheter tillhandahålla hotspecifika loggar till många SIEM-verktyg, så att IT-personal kan få varningar i realtid om möjliga säkerhetsincidenter. Det gör att HP-skrivare är värdefulla "ögon" i nätverket.

Sammanfattning

Tack vare flygplatsens HP Enterprise-skrivare och de ledtrådar som The Wolf lämnat efter sig kunde säkerhetsteamet isolera attacken snabbt för att undvika både störningar i verksamheten, negativ publicitet, böter till följd av bristande efterlevnad och skador på sitt varumärke.

Genom att anta starkare säkerhetsrutiner och till fullo dra nytta av de inbyggda säkerhetsfunktionerna i sina HP-skrivare har flygplatsen skärpt säkerheten i hela nätverket.

** London Airport är en fiktiv organisation som utsätts för en stor cyberattack i HP Studios film "THE WOLF: TRUE ALPHA."*

Mer information om HPs lösningar finns på:
Skrivarsäkerhet: hp.com/go/reinventsecurity
Datorsäkerhet: hp.com/go/ComputerSecurity
Du kan se filmerna om "The Wolf" genom att besöka: hp.com/thewolf

Registrera dig för att få uppdateringar
hp.com/go/getupdated

Dela med kollegor

4AA7-3560SVE, augusti 2018