Mögliches Szenario

Als der Londoner Flughafen Ziel eines zerstörerischen Cyberangriffs wurde, konnten Drucker von HP die Bedrohung erkennen

Offizieller Abschlussbericht über das Datenleck

Branche
Luftfahrt

Ziel
Ausmachen von Schwachstellen in Cybersicherheitsverfahren und deren Behebung

Vorgehensweise
Entwicklung eines umfassenden Sicherheitsplans in Zusammenarbeit mit HP Sicherheitsexperten

IT-Aspekte
- Angewandte Sicherheitsmaßnahmen auf IoT-Endpunkte
- Aktivierung der integrierten Sicherheitsfunktionen in HP Druckern
- Optimierung der Sicherheitsüberwachung im gesamten Netzwerk

Geschäftliche Aspekte
Optimierte Cybersicherheit zum Schutz wichtiger internationaler Infrastruktur und der Sicherheit von Passagieren

Überblick

Der Londoner Flughafen* fertigt jeden Tag über 300.000 Passagiere auf ihren Reisen in 94 Länder der Erde ab. Fast 50.000 Menschen aus 300 Unternehmen arbeiten am Flughafen und machen ihn im wahrsten Sinne zu einer Stadt auf engstem Raum.

Mit dem Wachstum des Flughafens wurde seine Infrastruktur immer weiter vernetzt und automatisiert. Interne Systeme von HLK über die Beleuchtung bis hin zu Druckern sind heute im Flughafennetzwerk miteinander verbunden. Das Drucken, Scannen und Kopieren erledigen über 60 HP MFPs, die überall im Flughafen verstreut sind.

Am 23. April 2018 nutzte ein als „The Wolf“ bekannter Cyberterrorist das vernetzte Beleuchtungssystem, um sich Zugang zu verschaffen und seine Malware durch das gesamte Netzwerk zu schicken. Seine Vorgehensweise über schlecht gesicherte Endpunkte ist berüchtigt und so nutzten die IT-Sicherheitsexperten die Bedrohungsprotokolle der HP Enterprise Drucker im Rahmen ihrer Ermittlungen, um den Angriff zu isolieren und aufzuhalten. Erstaunlicherweise enthielten die Protokolle Angaben zum Ursprung des Eindringens durch The Wolf. Nach dem Angriff wandte sich der Londoner Flughafen an HP, um die Sicherheit der Endpunkte weiter auszubauen.

Was ist passiert?

Nachdem The Wolf die Schwachstelle ausgemacht hatte (vermutlich über Phishing-Mails an Nutzer im Netzwerk), konnte er das IoT-Beleuchtungssystem mit Malware infizieren. Anschließend konnte er diese Malware über das gesamte Netzwerk ausbreiten und Ankerpunkte in anderen Endpunkt-Geräten anlegen, die nicht überwacht waren.

Aus dem Versteck in unüberwachten IoT-Geräten konnte das Team von The Wolf von den Überwachungssystemen des Netzwerks unbemerkt verschiedene Ausgangspunkte für einen massiven, verheerenden Angriff aufbauen.

Das Flughafenmanagement versuchte verzweifelt verschiedene Systeme herunterzufahren, während die entscheidende Infrastruktur für die Bewegung von Flugzeugen und Passagieren aufrechterhalten werden musste.

Reaktion auf den Angriff

The Wolf wurde mit dem Angriff auf das Flughafennetzwerk beauftragt. Das IT-Sicherheitsteam des Flughafens hatte *geglaubt*, das Flughafennetzwerk sei gegen Hacker gut geschützt. Sie hatten übersehen, welche Bedrohung in den IoT-Geräten lauerte.

Zum Glück verfügten die Flughafendrucker

über HP Enterprise über HP Connection Inspector, das die Malware aufhalten konnte, als diese sich dadurch verdächtig machte, die Kommando- und Kontrollserver der Hacker „anzurufen".

Die Aktion wurde im syslog des Druckers registriert. Sobald die IT bemerkte, dass etwas nicht stimmte, kontrollierte sie die syslogs auf genaue Informationen zum Angriff. Doch wenn sich eine Malware in einem Netzwerk ausbreitet, zählt jede Sekunde. Hätte das IT-Sicherheitsteam das syslog für die Bedrohungserkennung im Drucker mit dem Security Information and Event Monitoring (SIEM) System verbunden, wäre es sofort nach dem Eindringen alarmiert worden.

Bessere Sicherheit als je zuvor

Nach dem Leck überprüften die IT-Mitarbeiter die Sicherheitspraktiken gemeinsam mit ihrem Anbieter von Managed Print Services und den HP Sicherheitsberatern.
Mit der Installation von HP Enterprise Druckern befand sich der Londoner Flughafen bereits auf dem richtigen Weg. Nur HP Enterprise Drucker und MFPs bieten Angriffserkennung im laufenden Betireb (Run-Time Intrusion Detection) und HP Connection Inspector, um Malware bei laufendem Betrieb zu erkennen und aufzuhalten und einen Neustart zu erzwingen. Beim Hochfahren prüft HP Sure Start das BIOS und heilt sich selbst, wenn der Code beschädigt wurde und gleichzeitig die Firmware anhand einer Whitelist kontrolliert wird.

Der Anbieter von Managed Print Services hat HP JetAdvantage Security Manager eingesetzt, der bei jedem Neustart des Druckers automatisch die Sicherheitseinstellungen prüft und veränderte Einstellungen zurücksetzt. Das IT-Sicherheitsteam am Flughafen hat außerdem das syslog des Druckers mit dem SIEM-Tool verknüpft. Im Gegensatz zu Druckern anderer Hersteller können Geräte von HP bedrohungsspezifische Protokolle an viele SIEM-Tools übertragen, sodass IT-Mitarbeiter in Echtzeit alarmiert werden, wenn ein Sicherheitsvorfall passiert. Dadurch werden die Drucker von HP zu unersetzlichen „Horchposten" im Netzwerk.

Zusammenfassung

Durch die HP Enterprise Drucker am Flughafen und die Spuren, die The Wolf hinterlassen hatte, konnte das Sicherheitsteam den Angriff schnell genug isolieren und eine Störung des Flughafenbetriebs, negative Publicity, Strafen wegen Verletzung von Sicherheitsvorschriften und einen Schaden an der Marke verhindern.

Mit Einsatz besserer Sicherheitspraktiken und Nutzung der integrierten Sicherheitsfunktionen in den HP Druckern hat der Flughafen die Sicherheit im gesamten Netzwerk gesteigert.

**Der Londoner Flughafen ist ein fiktives Unternehmen, das im Film „THE WOLF: TRUE ALPHA" von HP Studio Ziel eines großangelegten Cyberangriffs wird. TRUE ALPHA."*

Weitere Informationen zu den Lösungen von HP siehe
Druckersicherheit. hp.com/go/reinventsecurity
PC-Sicherheitslösungen: hp.com/go/ComputerSecurity

Hier können Sie die Filme über „The Wolf" sehen:
hp.com/thewolf

Melden Sie sich noch heute an.
hp.com/go/getupdated

An Kollegen weiterleiten

4AA7-3560DEE, August 2018