Caso práctico

Cuando el aeropuerto de Londres se convirtió en el objetivo de un ciberataque destructivo, las impresoras HP detectaron la amenaza

Informe oficial final relativo a la brecha de datos

Sector
Aviación

Objetivo
Identificar los eslabones más débiles de las prácticas de ciberseguridad y corregirlos.

Enfoque
Se desarrolló un plan de seguridad completo conjuntamente con los expertos de seguridad de HP.

La TI importa
- Se aplicaron medidas de seguridad en los puntos de conexión del IoT.
- Se habilitaron las funciones de seguridad integradas en las impresoras HP.
- Se mejoró la supervisión de la seguridad en toda la red.

Los negocios importan
Se mejoró la ciberseguridad para proteger una infraestructura internacional crítica y mantener la seguridad de los pasajeros.

Información general

El aeropuerto de Londres* presta servicio a más de 300 000 pasajeros cada día, con vuelos a 94 países de todo el mundo. Casi 50 000 personas de 300 compañías trabajan en el aeropuerto, lo que lo convierte en una ciudad a pequeña escala.

Con el crecimiento del aeropuerto, su infraestructura se ha vuelto cada vez más conectada y automatizada. Los sistemas internos, desde la calefacción y el aire acondicionado hasta la iluminación y las impresoras, se conectan ahora a su red. Los trabajos de impresión, escaneado y copia se realizan con una flota de más de 60 impresoras multifunción de HP distribuidas por todas las instalaciones.

El 23 de abril de 2018, el ciberterrorista conocido como «The Wolf» utilizó los sistemas de iluminación conectados del aeropuerto para acceder a la red y extender su malware por ella. Dado que es famoso por realizar sus ataques a través de puntos de conexión insuficientemente protegidos, los expertos en seguridad de TI consultaron inmediatamente los registros de amenazas de sus impresoras HP Enterprise, como parte de la investigación, para aislar y detener el ataque. Sorprendentemente, los registros contenían pistas que había dejado «The Wolf» sobre el origen de la intrusión. Posteriormente, el aeropuerto de Londres recurrió a HP para mejorar la seguridad de sus puntos de conexión.

¿Qué sucedió?

Una vez que «The Wolf» encontró una vulnerabilidad, probablemente enviando mensajes de correo electrónico de suplantación de identidad a usuarios conectados a la red, pudo infectar el sistema de iluminación del Internet de las cosas (IoT) con el malware. A continuación, pudo extender el malware por la red, creando puntos de apoyo en otros dispositivos no supervisados que operaban como puntos de conexión.

Al ocultar su presencia en los dispositivos del IoT no supervisados, el equipo de «The Wolf» podía mantenerse invisible a los sistemas de supervisión de la red, al tiempo que desarrollaba varios puntos de lanzamiento para un ataque destructivo masivo.

La gestión del aeropuerto se dedicó a intentar desconectar frenéticamente diversos sistemas, mientras mantenía en funcionamiento la infraestructura más crucial: el tráfico de aviones y pasajeros.

Respuesta al ataque

«The Wolf» había sido contratado para atacar la red del aeropuerto. El personal de seguridad de TI del aeropuerto creía que la red estaba protegida de los hackers, pero no tenían ninguna visibilidad de las amenazas ocultas en los dispositivos del IoT.

Afortunadamente, las impresoras HP Enterprise del aeropuerto contaban con HP Connection Inspector, que detuvo el malware cuando intentó realizar unas sospechosas «llamadas a casa» dirigidas a los servidores de control de los hackers.

Las acciones se capturaron en los registros de sistema de las impresoras. Una vez el personal de TI fue consciente de que pasaba algo, comprobó los registros de sistema en busca de una información más detallada sobre el ataque. Pero el tiempo es esencial cuando el malware se está extendiendo por la red. Si el personal de seguridad de TI hubiera conectado los registros de sistema de detección de amenazas de las impresoras a su sistema de información de seguridad y supervisión de eventos (SIEM), habría recibido una alerta inmediata en el momento de producirse la intrusión.

Más seguridad que nunca

Después de la brecha, el personal de TI revisó las prácticas de seguridad con su proveedor de servicios gestionados de impresión y los asesores de seguridad de HP.

Gracias a la instalación de impresoras HP Enterprise, el aeropuerto de Londres ya se encontraba en la senda correcta. Solo las impresoras e impresoras multifunción HP Enterprise ofrecen detección de intrusiones en tiempo real, así como HP Connection Inspector, que permite detectar y detener el malware durante las operaciones y forzar un reinicio. En el arranque, HP Sure Start comprueba la BIOS y puede recuperarse automáticamente si el código está afectado, mientras las listas blancas comprueban el firmware.

El proveedor de servicios gestionados de impresión implementó HP JetAdvantage Security Manager para comprobar automáticamente la configuración de seguridad cada vez que se reiniciaba una impresora y restablecer cualquier ajuste que hubiera sido modificado.

El personal de seguridad de TI del aeropuerto igualmente conectó los registros de sistema de las impresoras a la herramienta SIEM. A diferencia de las impresoras de otros fabricantes, los dispositivos de HP pueden proporcionar registros específicos sobre amenazas a diversas herramientas SIEM, de modo que el personal de TI recibe alertas en tiempo real sobre posibles incidencias de seguridad. Esto convierte a las impresoras HP en «ojos» de incalculable valor dentro de las redes.

Conclusión

Gracias a las impresoras HP Enterprise del aeropuerto y las pistas que dejó «The Wolf» a su paso, el equipo de seguridad pudo aislar el ataque lo bastante rápido como para evitar disrupciones en las operaciones, publicidad negativa, multas por incumplimiento y daños a la reputación de la marca.

Al emplear prácticas de seguridad más seguras y aprovechar al máximo las funciones de seguridad integradas de las impresoras HP, el aeropuerto ha fortalecido la seguridad en toda la red.

**El aeropuerto de Londres es una organización ficticia que sufre un grave ciberataque en la película de HP Studio: «THE WOLF: TRUE ALPHA».*

Para obtener más información sobre las soluciones de HP:
Seguridad de la impresión:
www.hp.es/seguridad-impresion
Seguridad para ordenadores:
https://www8.hp.com/es/es/solutions/computer-security.html

Para ver las películas de «The Wolf», visite:
hp.com/thewolf

Suscríbase para recibir novedades
hp.com/go/getupdated

Compartir con compañeros

4AA7-3560ESE, agosto de 2018