Estudio de caso

Cuando el aeropuerto de Londres fue el blanco de un destructivo ataque cibernético, las impresoras HP detectaron la amenaza

Informe oficial final sobre la violación de datos

Sector
Aviación

Objetivo
Identificar puntos débiles en las prácticas de seguridad cibernética y corregirlos.

Enfoque
Se desarrolló un plan de seguridad completo junto a los expertos en seguridad de HP.

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

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

Visión general

El aeropuerto de Londres* atiende más de 300 000 pasajeros por día que viajan a 94 países del mundo. Allí trabajan cerca de 50 000 personas de 300 compañías, lo que lo convierte prácticamente en una ciudad condensada.

Conforme el aeropuerto fue creciendo, su infraestructura se volvió cada vez más conectada y automatizada. Los sistemas internos, desde la climatización hasta la iluminación y las impresoras, ahora están en la red del aeropuerto. La impresión, el escaneo y el copiado se llevan a cabo en una flota de más de 60 impresoras multifunción HP distribuidas en las instalaciones.

El 23 de abril de 2018, el terrorista cibernético conocido como “The Wolf” (el lobo) utilizó los sistemas de iluminación conectados del aeropuerto para obtener acceso y propagar su malware en toda la red. Como es conocido por sus hazañas usando puntos de conexión mal protegidos, los expertos en seguridad de TI inmediatamente recurrieron a 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 sobre “The Wolf”, como dónde se había originado la intrusión. Posteriormente, el aeropuerto de Londres recurrió a HP para avanzar aún más en la seguridad de los puntos de conexión.

Qué sucedió

Una vez que "The Wolf" encontró una vulnerabilidad, probablemente espiando los correos electrónicos de los usuarios de la red, pudo infectar con malware el sistema de iluminación de IoT. Luego pudo extender su malware por toda la red y creó bases en otros dispositivos conectados no supervisados.

Escondiendo su presencia en dispositivos de IoT no supervisados, el equipo de «The Wolf» pudo permanecer oculto a los sistemas de supervisión de la red mientras desarrollaba múltiples puntos de lanzamiento para ejecutar un ataque destructivo masivo.

La dirección del aeropuerto intentó desesperadamente cerrar varios sistemas mientras mantenía funcionando la infraestructura crítica, que afecta a los aviones y los 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 del aeropuerto estaba bien protegida contra los piratas informáticos, pero no podían ver las amenazas ocultas en los dispositivos de IoT.

Afortunadamente, las impresoras HP Enterprise del aeropuerto contaban con HP Connection Inspector, que detuvo el malware cuando este hizo intentos sospechosos de conectarse con el comando del pirata informático y controlar los servidores.

Las acciones fueron capturadas en los syslogs de la impresora. Una vez que el personal de TI se dio cuenta de que algo andaba mal, verificaron los syslogs para ver los detalles del ataque. Pero el tiempo es crucial cuando el malware se está propagando por toda la red. Si el personal de seguridad de TI hubiera conectado los syslogs de detección de amenazas de las impresoras a su sistema de supervisión de eventos e información de seguridad (SIEM), habrían sido alertados inmediatamente cuando se produjo la intrusión.

Seguridad más sólida que nunca

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

Al instalar impresoras HP Enterprise, el aeropuerto de Londres ya estaba en el camino correcto. Solo las impresoras y multifunción HP Enterprise ofrecen detección de intrusiones en tiempo de funcionamiento y HP Connection Inspector para detectar y detener el malware durante las operaciones y forzar un reinicio. Al inicio, HP Sure Start verifica el BIOS y puede autorrepararse si se ha comprometido el código, mientras que las listas blancas verifican el firmware.

El proveedor de servicios de impresión administrada implementó HP JetAdvantage Security Manager para verificar automáticamente las configuraciones de seguridad cada vez que una impresora se reinicia y restablece cualquier configuración alterada.

El personal de seguridad de TI del aeropuerto también decidió conectar los syslogs de la impresora a su herramienta de SIEM. A diferencia de las impresoras de otros fabricantes, los dispositivos HP pueden suministrar registros específicos de amenazas a varias herramientas de SIEM para que el personal de TI obtenga alertas inmediatas sobre posibles incidentes de seguridad. Esto convierte a las impresoras HP en «ojos» invaluables dentro de su red.

Conclusión

Gracias a las impresoras HP Enterprise del aeropuerto y las pistas que dejó «The Wolf», el equipo de seguridad pudo aislar el ataque lo suficientemente rápido como para evitar la interrupción de las operaciones, la publicidad negativa, las multas por incumplimiento y el daño a la marca.

Mediante la utilización de sólidas prácticas de seguridad y el aprovechamiento total de los recursos de seguridad integrados de sus impresoras HP, el aeropuerto ha reforzado la seguridad en toda la red.

**El aeropuerto de Londres es una organización ficticia amenazada por un ataque cibernético en la película "THE WOLF: TRUE ALPHA de HP Studio".*

Para obtener más información sobre las soluciones HP:
Seguridad de la impresión:
hp.com/go/reinventsecurity
Seguridad de la PC:
hp.com/go/ComputerSecurity

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

Regístrese para recibir actualizaciones
hp.com/go/getupdated

Compartir con colegas

4AA7-3560SPL, noviembre de 2018