Caso práctico

Las pruebas de penetración muestran que la brecha de ciberseguridad en Industrias Torvik provocada por «The Wolf», podría haberse detenido con impresoras HP

Informe oficial final relativo a la brecha de datos

Sector
Envío de mercancías

Objetivo
Analizar y resolver áreas de vulnerabilidad de la red.

Enfoque
Pruebas de penetración para encontrar las vulnerabilidades que facilitaron el ataque.

Resultados y recomendaciones
- Educar a los usuarios para que sean precavidos al abrir mensajes de correo electrónico sospechosos e imprimir archivos adjuntos.
- Implementar impresoras HP con detección de amenazas.
- Configurar todos los puntos de conexión con seguridad, incluida la infraestructura que se haya trasladado o que se encuentre en ubicaciones temporales.

Los negocios importan
Aplicar mejores medidas de seguridad para evitar el tiempo de inactividad de las operaciones y mejorar la confianza en la marca. Mejorar las políticas para supervisar los puntos de conexión de la red en ubicaciones temporales.

Información general

Industrias Torvik* envía 8 millones de contenedores al año. Para 22 000 fabricantes y mayoristas, Torvik es la conexión vital entre sus productos y las personas de todo el mundo. Entre las propiedades de la empresa, se incluyen astilleros, buques, almacenes y toda la tecnología sobre la que se asienta la gigantesca red de Torvik.

Su infraestructura tecnológica ha tenido problemas para adaptarse al crecimiento de la empresa. Aunque el personal de seguridad de TI ha configurado los servidores de la empresa, ha obviado la gestión de la seguridad de algunas impresoras situadas en oficinas satélites o ubicaciones temporales.

El 23 de abril de 2018, el ciberterrorista conocido como «The Wolf» utilizó una impresora desprotegida para sabotear las operaciones de Industrias Torvik, un ataque que afectó a toda la organización, desde los ordenadores hasta las grúas y portacontenedores. Su asesor de seguridad llevó a cabo pruebas de penetración para analizar el incidente y elaboró una serie de recomendaciones para mejorar la seguridad y la formación del personal.

¿Qué sucedió?

La dirección de Industrias Torvik estaba acostumbrada a llevar las riendas en operaciones de alto riesgo. Por ello, no esperaba que unos hackers pudieran infiltrarse tan profundamente en su red como para inhabilitar los puentes grúa y redirigir sus barcos en alta mar.

Lo único que tuvo que hacer «The Wolf» fue poner en peligro una impresora de gran formato ubicada en un solar en obras. Posteriormente, pudo desplazarse lateralmente por la red de la empresa hacia los grandes objetivos de las operaciones de la empresa. En un instante, esta empresa de transportes líder tuvo que enfrentarse a disrupciones operativas masivas, un escrutinio internacional profundo y miles de clientes furiosos.

Cómo ocurrió

El personal de seguridad de TI de la empresa pensaba que estaban protegidos. Sus equipos tecnológicos y logísticos supervisaban continuamente las operaciones globales en busca de potenciales problemas de seguridad. Incluso habían establecido procedimientos de seguridad para puntos de conexión como las impresoras. Pero ignoraron una cosa: la configuración de seguridad de una impresora de gran formato, temporalmente ubicada en un remolque de obra.

El hacker ni siquiera tuvo que acceder directamente a la impresora. Le bastó con enviar un mensaje de correo electrónico con un archivo PDF adjunto al empleado de Torvik responsable de imprimir los documentos de gran formato. Ese archivo PDF incluía un archivo Postscript oculto, preparado para abrirse y ejecutarse automáticamente cuando se enviara el archivo PDF a la impresora. Cuando el empleado envió el trabajo de impresión, el malware se integró en la impresora, para extenderse después por toda la red.
Al implantar malware en un archivo adjunto de correo electrónico con aspecto inocente, el hacker evitó el software antimalware de los ordenadores de la empresa.

La brecha fue posible porque la impresora de gran formato no contaba con una seguridad integrada sólida, como la detección de amenazas. Asimismo, la empresa no supervisó ni gestionó la configuración de todas las impresoras de la flota, y entre ellas, aquellas ubicadas temporalmente en oficinas satélites.

Reparación de la brecha

Industrias Torvik conservó a una empresa líder en pruebas de penetración para realizar un análisis completo de la ciberseguridad de la organización.

El equipo de pruebas de penetración recomendó la instalación de impresoras HP con funciones de seguridad integradas, que incluyen la serie HP DesignJet, con arranque seguro y listas blancas de firmware. Estas funciones permiten a la impresora detectar código malicioso y apagarse, para alertar a la organización de TI de la necesidad de reinstalar el firmware legítimo HP.

Asimismo, recomendaron la utilización de funciones de seguridad Instant-On de HP JetAdvantage Security Manager, un programa de software de gestión de seguridad para toda la flota, con el fin de aplicar automáticamente las políticas de seguridad en el momento de añadir los dispositivos a la red. HP Security Manager también puede crear informes de cumplimiento que muestran cada impresora HP, incluso las que se encuentran en ubicaciones remotas o temporales. Ello permite demostrar que las configuraciones de seguridad de la flota se han mantenido.

Además, el asesor de seguridad sugirió el establecimiento de un programa de formación que ayudara a los empleados a reconocer mensajes de correo electrónico sospechosos y evitar la impresión de archivos adjuntos desconocidos.

Conclusión

Industrias Torvik sigue tambaleándose a consecuencia de los impactos que sufrió después de la brecha en sus operaciones, así como por la enorme publicidad generada por las opiniones poco convencionales y acciones delictivas de su presidente. Mientras la organización busca una nueva dirección para su liderazgo, el rumbo que debe seguir la ciberseguridad es claro: la elección de impresoras y soluciones de HP permitirá frustrar al siguiente «The Wolf» que intente realizar un ataque.

**Torvik Industries es una empresa 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:
HP DesignJet:
hp.com/go/designjetsecurity
Seguridad de la impresión:
www.hp.es/seguridad-impresion

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

Suscríbase para recibir novedades
hp.com/go/getupdated

Compartir con compañeros

4AA7-3562ESE, agosto de 2018