Estudio de caso

Las pruebas de penetración muestran que la violación de la seguridad cibernética de Torvik Industries perpetrada por “The Wolf” podría haber sido detenida por las impresoras HP

Informe oficial final sobre la violación de datos

Sector
Envío

Objetivo
Analizar y resolver las áreas de vulnerabilidad de la red.

Enfoque
Pruebas de penetración para descubrir las vulnerabilidades que permitieron el ataque.

Hallazgos y recomendaciones
- Educar a los usuarios para que sean cautelosos al abrir correos electrónicos y documentos de impresión adjuntos que sean sospechosos.
- Instalar impresoras HP con detección de amenazas.
- Configurar medidas de seguridad en todos los puntos de conexión, incluida la infraestructura que se migra a ubicaciones temporales.

Los negocios importan
Aplicar medidas de seguridad más sólidas para evitar el tiempo de inactividad operativo y aumentar la confianza en la marca. Mejorar las políticas de supervisión de los puntos de conexión de la red en las ubicaciones temporales.

Visión general

Torvik Industries* despacha más de 8 millones de contenedores por año. Para 22 000 fabricantes y mayoristas, Torvik es la conexión vital entre sus productos y las personas de todo el mundo. Los bienes de la compañía incluyen astilleros, buques, depósitos y toda la tecnología que apoya la extensa red de Torvik.

La infraestructura de la compañía viene luchando para adaptarse al crecimiento de la empresa. Pero si bien el personal de TI ha configurado los servidores, algunas impresoras de las oficinas satélites o las ubicaciones temporales no cuentan con gestión de la seguridad.

El 23 de abril de 2018, el ciberterrorista conocido como «The Wolf» usó una impresora sin protección para sabotear las operaciones de Torvik Industries, desde las PC hasta las grúas y los buques de carga. Su asesor de seguridad utilizó pruebas de penetración para analizar el evento y les hizo recomendaciones para mejorar la seguridad y la capacitación del personal.

Qué sucedió

El liderazgo de Torvik Industries solía estar a la vanguardia de las operaciones de alto riesgo en todo el mundo, por lo que no esperaban que un pirata informático infiltrara su red tan profundamente como para cerrar los puentes de grúa de la compañía y redirigir sus buques hacia mar abierto.

Todo lo que tuvo que hacer «The Wolf» fue comprometer una impresora de formato grande en una obra en construcción. Luego pudo moverse lateralmente dentro de la red y llegar a los grandes objetivos en las operaciones de la compañía. En un instante, esta importante compañía naviera se vio frente a interrupciones masivas en sus operaciones, un intenso escrutinio internacional y miles de clientes furiosos.

Cómo sucedió

El personal de TI de la compañía creía que estaban protegidos. Sus equipos técnicos y logísticos supervisaban constantemente las operaciones globales en busca de problemas de seguridad. Incluso habían implementado procedimientos de seguridad para los puntos de conexión, como las impresoras. Pero pasaron por alto algo: la configuración de seguridad de una impresora de formato grande colocada en forma transitoria en un remolque de construcción.

El hacker ni siquiera tuvo que acceder a la impresora directamente, simplemente envió un correo electrónico con un PDF adjunto al empleado responsable de la impresión de documentos de formato grande en Torvik. Ese PDF contenía un archivo postscript dañino que podía abrirse y autoejecutarse cuando se enviaba el PDF a la impresora. Una vez que el empleado envió el trabajo de impresión, el malware se incorporó a la impresora y luego se propagó por toda la red. Mediante el parasitismo informático («piggybaking») en un correo electrónico que parecía inofensivo, el hacker pudo eludir el software antimalware de las PC de la compañía.

Esta violación fue posible porque la impresora de formato grande no contaba con una sólida seguridad integrada, como la detección de amenazas. Además, la compañía falló en la supervisión y gestión de la configuración de todas y cada una de las impresoras de la flota, como las que se colocan temporalmente en las oficinas satélite.

Reparación del daño

Torvik Industries contrató una importante firma dedicada a pruebas de penetración para que realizara un análisis exhaustivo de la seguridad cibernética de la organización.

El equipo de pruebas de penetración recomendó instalar impresoras HP con recursos de seguridad integrados, como la serie HP Design Jet con Secure Boot y listas blancas de firmware. Estos recursos ayudan a la impresora a detectar código malicioso y apagarse, para luego alertar a la TI de que deben reinstalar firmware legítimo HP.

También recomendaron usar el recurso de seguridad Instant-On de HP JetAdvantage Security Manager, un programa de software de gestión de seguridad de toda la flota, para que aplique automáticamente las políticas de seguridad apenas se agregue un dispositivo a la red. HP Security Manager también puede generar informes de cumplimiento que muestran todas las impresoras HP, incluso las que están en ubicaciones remotas o temporales. Esto ayuda a demostrar que se mantienen las configuraciones de seguridad a nivel de la flota.

Además, el asesor de seguridad sugirió llevar a cabo un programa de educación para ayudar a los empleados a reconocer los correos electrónicos sospechosos y evitar imprimir documentos adjuntos desconocidos.

Conclusión

Torvik Industries todavía se está recuperando del impacto de la violación a su seguridad cibernética en sus operaciones, además de la publicidad intensificada de las visiones poco convencionales y los actos criminales de su presidente. Mientras la organización busca desarrollar una nueva dirección en el liderazgo, la dirección de la seguridad cibernética está muy clara: cambiar a impresoras y soluciones HP ayudará a detener al próximo “lobo” que salga de caza.

**Torvik Industries es una compañía ficticia amenazada por un ataque cibernético en la película «THE WOLF: TRUE ALPHA de HP Studio».*

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

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

Regístrese para recibir actualizaciones
hp.com/go/getupdated

Compartir con colegas

4AA7-3562SPL, noviembre de 2018