proofpoint

CASO DE CLIENTE

Una empresa de financiación de vehículos amplía su programa de gestión de vulnerabilidades a los riesgos relacionados con la identidad con Proofpoint

El desafío

- Integrar los riesgos relacionados con la identidad al programa de gestión de vulnerabilidades.
- Dificultad para admitir aplicaciones tradicionales por parte de la solución de administración de acceso con privilegios (PAM).
- Falta de visibilidad permanente de los riesgos asociados a las identidades con privilegios.

La solución

Proofpoint Identity Threat Defense

- Proofpoint Spotlight

Los resultados

- Mayor concienciación de los principales riesgos relacionados con la identidad.
- Reducción inmediata del nivel de riesgo.
- Incorporación al programa de gestión de vulnerabilidades del principal vector de ataque, la identidad.

La empresa

La empresa es un proveedor global de soluciones de financiación del automóvil, con más de 9000 empleados y operaciones en Norteamérica, Sudamérica y Asia. Ofrece programas de financiación minorista y leasing a consumidores y concesionarios de automóviles, así como productos de préstamo comercial para ayudar a los concesionarios a financiar y desarrollar su actividad. Cuenta con unos 60 000 millones de dólares en activos.

El desafío

Esta empresa cuenta con una infraestructura de TI amplia y diversificada y está experimentando dificultades con sus aplicaciones de antigua generación. Aunque había implementado una solución de administración de acceso con privilegios (PAM), no protegía muchas aplicaciones antiguas, sobre todo las que resultaban demasiado caras de actualizar o cuya retirada estaba prevista. Además, algunas cuentas administrativas y de servicio no pudieron asegurarse. Como resultado, la empresa no tenía un control total sobre las identidades y credenciales con privilegios, ni una buena visibilidad de los riesgos potenciales relacionados con la identidad. Esto preocupaba tanto a los administradores de TI como a los usuarios habituales.

Como explica el vicepresidente sénior de Estrategia y operaciones de Ciberseguridad Global de la empresa: "Si dispone de una gran infraestructura local y lleva años utilizando Active Directory, las vulnerabilidades son habituales debido a decisiones tomadas hace mucho tiempo. El déficit técnico es enorme. Además, la migración a la nube y las actividades de fusión y adquisición están aumentando la complejidad".

La solución

La empresa consideró Proofpoint Identity Threat Defense como una importante ampliación de su estrategia global de gestión de vulnerabilidades. Anteriormente, el enfoque de la empresa había sido centrarse en las vulnerabilidades CVE y CWE. Sin embargo, la empresa era consciente de que los errores de configuración de identidad también creaban muchos riesgos potenciales. Por ello, había empezado a supervisar todos los elementos de su entorno que presentaban un riesgo de ciberseguridad, estuvieran o no asociados a una vulnerabilidad CVE. Utilizando el modelo OSI de siete capas como guía, revisó su enfoque de la evaluación automatizada de riesgos para asegurarse de que cubría todo su entorno de TI y descubrió que carecía de capacidades de gestión de riesgos asociados a las identidades.

"La herramienta de Proofpoint nos ha proporcionado nuevas perspectivas. Antes, sabíamos que teníamos que centrarnos más en los riesgos relacionados con la identidad pero no teníamos forma de hacerlo".

Vicepresidente adjunto de Vulnerabilidades de TI

En respuesta, la empresa implementó la solución de gestión de riesgos de identidad de Proofpoint a principios de 2021. Proofpoint Identity Threat Defense se integra con la infraestructura de Active Directory (AD) de la empresa y analiza periódicamente cada endpoint para generar un repositorio de riesgos relacionados con la identidad, que la empresa recupera mediante la API. El equipo de seguridad de TI revisa estos riesgos y se reúne periódicamente con el equipo de corrección de vulnerabilidades de TI para aplicar y supervisar los cambios con el fin de reducir los riesgos de su entorno. Se trata de un esfuerzo colectivo, como explica el vicepresidente adjunto de Vulnerabilidades de TI de la empresa: "Hacemos todo lo posible por trabajar en colaboración con el equipo de TI".

Los acuerdos de nivel de servicio (SLA), que varían según el nivel de importancia, se utilizan para priorizar los elementos más críticos, junto con los esfuerzos de la empresa para corregir las vulnerabilidades.

Los resultados

Inmediatamente después de implementar la solución, la empresa notó mejoras evidentes en su nivel de riesgo. Tras más de un año de uso, la empresa suele observar varios problemas críticos nuevos a la semana, que resuelve rápidamente. "Estos problemas suelen estar causados por descuidos de los usuarios. Los usuarios no tienen malas intenciones, pero a veces cometen errores o actúan con precipitación".

Cuando le preguntamos qué haría sin la solución Proofpoint, el equipo no sabía cómo responder, ya que desconocía cualquier otra forma de obtener el tipo de información sobre identidades (en particular sobre puntos finales) que proporciona la solución. El vicepresidente adjunto de Vulnerabilidades de TI añade, "No tenemos forma de ver una contraseña registrada en PuTTY, por ejemplo".

"Las fusiones y adquisiciones son un caso de uso interesante, ya que se analizan antes y después de la integración. Con Proofpoint Identity Threat Defense, puedo evaluar la integridad del entorno y el nivel de déficit técnico".

Vicepresidente sénior de Estrategia y operaciones de ciberseguridad globales

El Vicepresidente sénior de Estrategia y operaciones de Ciberseguridad Globales añade, "Las fusiones y adquisiciones son un caso de uso interesante, ya que se analizan antes y después de la integración. Con la solución, puedo evaluar la integridad del entorno y el nivel de déficit técnico".

Cuando se le preguntó si recomendaría Proofpoint Identity Threat Defense a otros profesionales, su respuesta fue: "Dados los resultados que he visto y la dirección que estamos tomando, recomendaría esta solución a cualquier profesional que busque mejorar su gestión de la vulnerabilidad. Esta herramienta le permite verlo todo: vulnerabilidades tradicionales, vulnerabilidades relacionadas con la identidad y errores de configuración".

Y añade, "Solo hace falta una vulnerabilidad relacionada con la identidad para poner en peligro todo su entorno. Cualquier herramienta para mejorar la gestión de la vulnerabilidad ofrece un valor añadido, sobre todo cuando se pueden ver los riesgos y reducirlos con el tiempo. La solución de Proofpoint nos ha permitido cerrar cientos de miles de puertas: eso tiene un valor incalculable".

MÁS INFORMACIÓN

Para obtener más información, visite **proofpoint.com/es**.

proofpoint.

0613-003-06-01 06/24