LIBRO ELECTRÓNICO

Protección de su identidad con Proofpoint

Casos de uso e historias de éxito

proofpoint.

Introducción

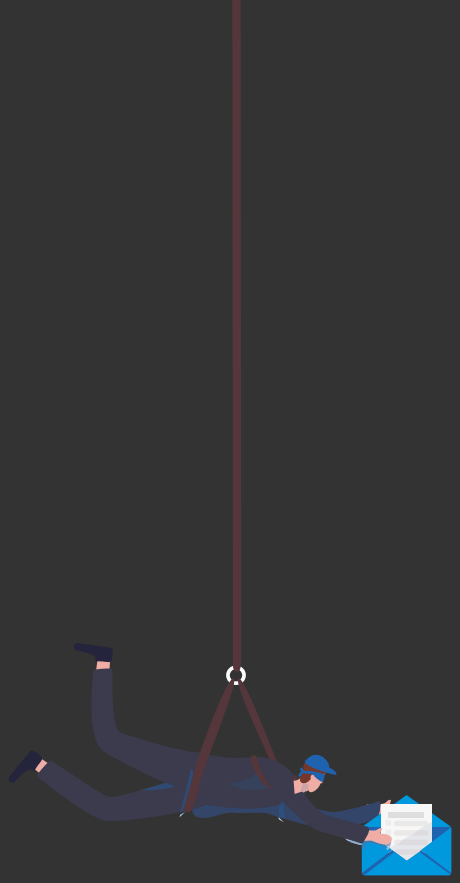
El escalamiento de privilegios y el desplazamiento lateral son un reto permanente para la mayoría de los equipos de seguridad, incluso en las empresas más grandes del mundo. Microsoft es el ejemplo perfecto. En enero de 2024, la empresa anunció que había sufrido un ataque realizado por un conocido grupo de ciberdelincuentes apoyados por Rusia.

Los atacantes explotaron una antigua cuenta de prueba desprotegida. Una vez comprometida la cuenta, escalaron sus privilegios y se desplazaron lateralmente a los sistemas en la nube de Microsoft. Pero aquí está el problema: como se hacían pasar por usuarios legítimos, pasaron desapercibidos durante más de un mes[1].

Compromisos como estos ponen de relieve la debilidad en la zona central de la cadena de ataque. Es aquí donde los ciberdelincuentes utilizan cuentas comprometidas para infiltrarse en las siguientes capas de las defensas de una empresa. Para ello, aprovechan errores de configuración e identifican vulnerabilidades relacionadas con la identidad para acceder a cuentas con privilegios cada vez mayores.

Escalamiento de privilegios y desplazamiento lateral

1 Bleeping Computer. "Microsoft Reveals How Hackers Breached Its Exchange Online Accounts" (Microsoft revela el pirateo de sus cuentas online de Exchange por parte de un grupo de hackers), enero de 2024.



Esta parte de la cadena de ataque juega un papel determinante en los ciberataques. Con una identidad robada, los ciberdelincuentes parecen usuarios legítimos, lo que los hace invisibles. Y puesto que son invisibles, pueden hacer prácticamente cualquier cosa: restablecer contraseñas, cambiar políticas, instalar software, extraer y cifrar datos para pedir rescates, etc.

¿Qué se puede hacer para detenerlos?

Proofpoint Identity Protection proporciona el análisis que necesita para identificar las identidades vulnerables y corregirlas antes de que los ciberdelincuentes las encuentren. Pero no solo eso. También identifica a los ciberdelincuentes activos una vez que se han infiltrado en su entorno.

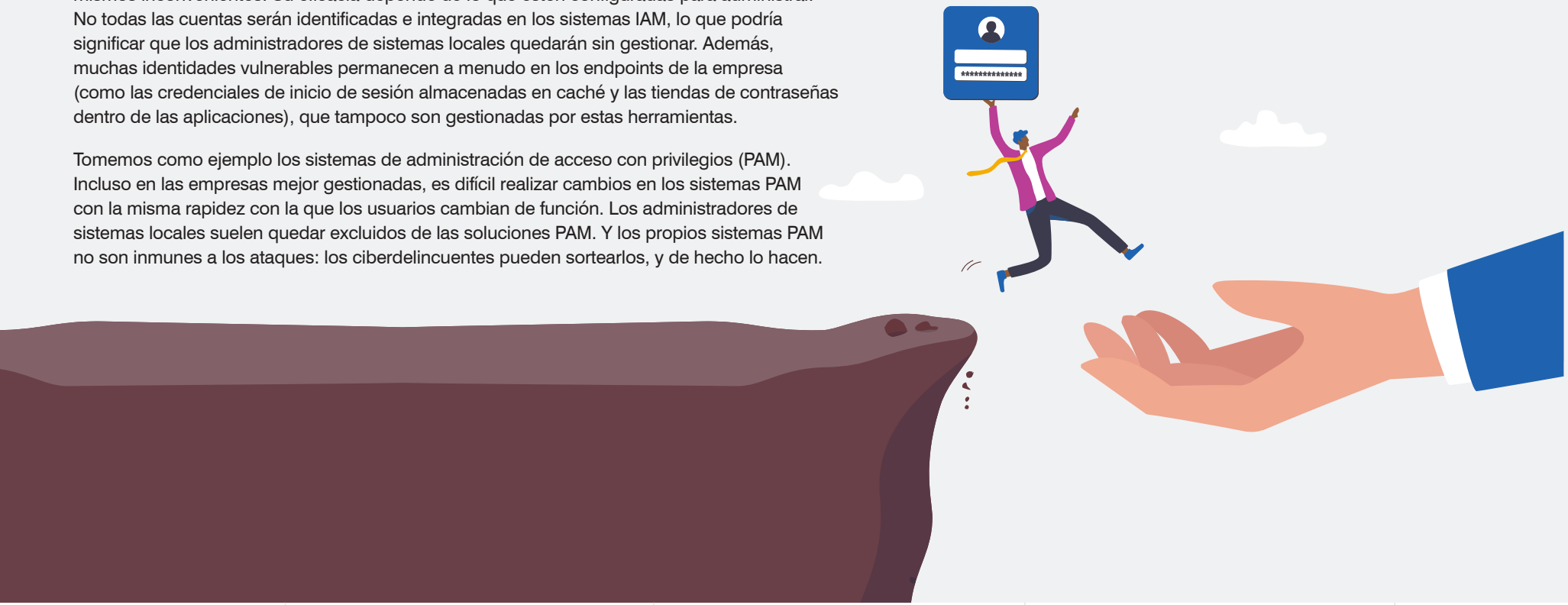
Este libro electrónico presenta tres casos de uso para explicar cómo funciona esta solución. También contiene historias de clientes para mostrarle Proofpoint Identity Protection en acción.

CASO DE USO 1:

Corregir los fallos de seguridad que dejan las herramientas IAM

Todas las herramientas comunes de administración de identidades y acceso (IAM) tienen los mismos inconvenientes. Su eficacia depende de lo que estén configuradas para administrar. No todas las cuentas serán identificadas e integradas en los sistemas IAM, lo que podría significar que los administradores de sistemas locales quedarán sin gestionar. Además, muchas identidades vulnerables permanecen a menudo en los endpoints de la empresa (como las credenciales de inicio de sesión almacenadas en caché y las tiendas de contraseñas dentro de las aplicaciones), que tampoco son gestionadas por estas herramientas.

Tomemos como ejemplo los sistemas de administración de acceso con privilegios (PAM). Incluso en las empresas mejor gestionadas, es difícil realizar cambios en los sistemas PAM con la misma rapidez con la que los usuarios cambian de función. Los administradores de sistemas locales suelen quedar excluidos de las soluciones PAM. Y los propios sistemas PAM no son inmunes a los ataques: los ciberdelincuentes pueden sortearlos, y de hecho lo hacen.



Resumen

Una empresa de financiación de vehículos utiliza Proofpoint para ampliar sus funciones de seguridad para incluir la gestión de riesgos asociadas a las identidades.

Perfil del cliente

Sector: Financiero

Empleados: 9000

Ubicación: A nivel mundial

Solución

Producto: Proofpoint Identity Protection

Componente: Proofpoint Spotlight

Cómo puede ayudarle Proofpoint

Proofpoint Spotlight es un componente de Proofpoint Identity Protection que le ayuda a identificar las identidades vulnerables y a corregir los fallos de seguridad de la identidad antes de que los aprovechen los ciberdelincuentes. Para ello, analiza sus endpoints, sistemas IAM y repositorios de identidades para detectar cualquier identidad no gestionada, mal configurada o expuesta. Los resultados de estos análisis se presentan en un informe de fácil comprensión. El informe le muestra todas las vías de ataque disponibles y le proporciona una lista de las identidades que debe corregir en primer lugar.

Proofpoint en acción

Una empresa de financiación de vehículos está reforzando sus dispositivos de seguridad para proteger mejor sus identidades.

A lo largo de sus 30 años de vida, la multinacional había creado una infraestructura informática grande y compleja. Aunque había desplegado un sistema PAM, este solo gestionaba una pocas cuentas de sus aplicaciones antiguas. Incluso se excluyeron algunas cuentas de administrador y de servicio. Esto quería decir que la empresa no podía administrar completamente sus identidades y credenciales con privilegios, ni visualizar todos los riesgos asociados a sus identidades.

Durante una revisión rutinaria del enfoque de la empresa para la evaluación automatizada de riesgos, el equipo de seguridad descubrió que no disponía de medios para gestionar los riesgos asociados a sus identidades. Y entonces eligieron Proofpoint Spotlight para corregir este fallo de seguridad. Poco tiempo después, se integró Proofpoint en los endpoints (clientes y servidores) y en la infraestructura de Active Directory (AD) de la empresa. A continuación, comenzó a analizar todos sus endpoints, su sistema PAM y otros repositorios de identidad en busca de vulnerabilidades.

El equipo de seguridad de TI de la empresa organizó una reunión con el equipo responsable de corregir las vulnerabilidades de TI para revisar sus conclusiones. Los dos equipos decidieron que lo mejor sería que trabajaran juntos para aplicar cambios que redujeran los riesgos relacionados con la identidad. También realizaron un seguimiento del impacto de estos cambios a lo largo del tiempo.

Después de utilizar Proofpoint Spotlight, los equipos obtuvieron resultados impresionantes. Aunque seguían apareciendo nuevos problemas críticos cada semana, disponían de nuevos procesos para corregirlos rápidamente.

"[Proofpoint Spotlight] nos ha proporcionado nuevas perspectivas. Antes, sabíamos que teníamos que centrarnos más en estos riesgos relacionados con la identidad, pero no teníamos forma de hacerlo".

–Vicepresidente adjunto, vulnerabilidades de TI de una empresa de financiación de vehículos

Principales conclusiones

Basta una vulnerabilidad relacionada con la identidad para comprometer todo su entorno. Necesita herramientas que puedan poner de relieve las vulnerabilidades vinculadas a sus identidades para poder identificar los riesgos y reducirlos con el tiempo. Esto le permitirá bloquear miles de puertas que conducen a identidades antes de que los ciberdelincuentes tengan la oportunidad de probarlas.

Los sistemas de AD y de identidad son complejos y están en constante evolución, y esto multiplica los riesgos relacionados con la identidad.

Cuando una persona hace que una identidad se vea comprometida, no suele hacerlo de manera malintencionada, sino más bien porque cometió un error o tenía prisa.

CASO DE USO 2:

Triunfar en los ejercicios de simulación de ataques

Aunque fallen las defensas, los verdaderos ganadores de los ejercicios de simulación de ataques son las empresas que los utilizan para reforzar su seguridad. Sin embargo, cuando un ejercicio expone identidades no gestionadas o mal configuradas dentro de su entorno, la sensación no es muy positiva. Pero tranquilícese: le pasa a casi todo el mundo. De hecho, el 95 % de las herramientas de simulación de ataques identifican las credenciales de inicio de sesión de los administradores de dominio expuestos[2].

2. Investigación de Illusive

Resumen

El equipo del SOC de un banco minorista utiliza Proofpoint para evitar que una herramienta de simulación de ataques se conecte a sus cuentas críticas y comprometa sus servidores.

Perfil del cliente

Sector: Finanzas

Empleados: 1000

Ubicación: EMEA

Solución

Producto: Proofpoint Identity Protection

Componente: Proofpoint Shadow

Cómo puede ayudarle Proofpoint

Proofpoint Identity Protection puede ayudarle a detectar ataques en la zona central de la cadena de ataque y evitar que una herramienta de simulación de ataque logre su objetivo sin ser detectada.

- **Proofpoint Shadow** crea una compleja red de datos falsos y rutas de acceso a recursos aparentemente sensibles, y luego los difunde por toda la empresa. Ni siquiera las herramientas de simulación de ataques más avanzadas pueden distinguir lo que es real de lo que es falso. La única forma que tienen de marcar la diferencia es intentar utilizar lo que han descubierto, lo que alertará a los equipos de seguridad de su presencia. Con esta red de señuelos, les resulta casi imposible desplazarse por los recursos de TI estratégicos sin ser detectados.
- **Proofpoint Spotlight** puede ayudarle a identificar cualquier identidad no gestionada, mal configurada y expuesta dentro de su entorno. Esto le permitirá corregirlos antes de que las herramientas de simulación de ataques (y los ciberdelincuentes) puedan aprovecharse de ellas.

Proofpoint en acción

Un importante banco minorista bloquea dos ataques simulados.

Un importante banco minorista y de inversión contaba con múltiples capas de controles de seguridad y varias herramientas capaces de bloquear el malware en los endpoints. Pero con la proliferación de las amenazas persistentes avanzadas (APT), quería añadir nuevas funciones de detección a su arsenal. Y por eso instaló Proofpoint Shadow. Poco después, el banco contrató a una reputada empresa especializada en pruebas de penetración para que atacara su red. Sin embargo, no advirtió a la empresa de que utilizaría Proofpoint para frustrar sus ataques.

Antes de iniciar las pruebas, Proofpoint Shadow introdujo datos falsos diseñados para atraer a los ciberdelincuentes a cada endpoint de la red de 5000 nodos del banco. Todos los datos se personalizaron para dar la impresión de que pertenecían a un entorno bancario, incluyendo datos de acceso falsos.

El primer día de la prueba, Proofpoint Shadow detectó intentos de actividad maliciosa de un usuario falso ("usuario A") en uno de los servidores Citrix del banco. Por tanto, recopiló información sobre los pormenores ("quién, qué, cuándo y dónde") del ataque y alertó al SOC y a los equipos de respuesta a incidentes.

Durante sus investigaciones, los equipos descubrieron que los especialistas de las pruebas de penetración habían instalado herramientas maliciosas en la red del banco e intentaban utilizar otras cuentas falsas, recopiladas después del compromiso inicial, para avanzar en su ataque. Los especialistas no tenían ni idea de que ya habían sido detectados por los equipos de seguridad.

Entonces, el día 22, Proofpoint Shadow envió otra alerta sobre una nueva actividad maliciosa del usuario A, pero en un servidor diferente. Cuando el equipo del SOC realizó un segundo análisis forense, descubrió intentos agresivos de inicio de sesión en cuentas críticas a través de este servidor. El ciberdelincuente había activado involuntariamente la alerta al utilizar dos conjuntos diferentes de credenciales de usuario falsos.

Principales conclusiones

Si su equipo del SOC puede llevar a cabo con éxito ejercicios de simulación de ataques, es más probable que sea capaz de bloquear a los ciberdelincuentes reales en caso de que ataquen su entorno.

La detección temprana de comportamientos sospechosos permite a los SOC y a los equipos de seguridad de la información neutralizar a los ciberdelincuentes antes de que se desplacen lateralmente y alcancen los recursos informáticos críticos de una empresa. Estas detecciones también incluyen datos valiosos, para que los equipos puedan someter los ataques a un análisis forense, lo que facilita la respuesta ante incidentes y la reducción de riesgos.

La detección de un intento de descifrado de contraseña en una cuenta falsa garantiza una alerta extremadamente fiable: un verdadero positivo que indica actividad maliciosa en la red con un índice de confianza del 100 %.

APLICACIÓN 3:

Proteger las identidades híbridas en AD y Entra ID

Active Directory (AD) es una pieza clave de la infraestructura de TI de las empresas actuales. Según algunas estimaciones, el 90 % de las empresas utilizan AD como método principal para la autenticación y autorización de usuarios. En la era de la migración a la nube, Microsoft Entra ID (antes Azure AD) también se está haciendo omnipresente.

Sin embargo, aunque populares, estas herramientas también son notoriamente difíciles de administrar y mantener, sobre todo porque afectan a casi todas las ubicaciones, usuarios y dispositivos de la red. Al igual que ocurre con las herramientas IAM, los esfuerzos nunca se ven totalmente recompensados, ya que las autorizaciones, los usuarios y las organizaciones evolucionan constantemente. Es más, no todas las identidades están cubiertas. Tomemos el ejemplo de las credenciales almacenadas en caché en los endpoints. AD y Entra ID no los administran, y tampoco los sistemas IAM. Por lo tanto, representan un riesgo importante.

Resumen

Un holding bancario utiliza Proofpoint para evaluar el nivel de seguridad de una nueva adquisición y descubrir 3000 administradores de dominio en sus estaciones de trabajo.

Perfil del cliente

Sector: Finanzas

Empleados: 25000

Ubicación: EE. UU.

Solución

Producto: Proofpoint Identity Protection

Componente: Proofpoint Spotlight

Cómo puede ayudarle Proofpoint

Proofpoint Spotlight analiza AD, Entra ID y muchos otros repositorios de identidades y detecta las cuentas que tienen privilegios que no deberían tener. También identifica las identidades no gestionadas en los endpoints, así como las identidades con privilegios que no son gestionadas por la solución PAM u otros sistemas IAM. Así podrá corregirlos antes de que caigan en malas manos.

También proporciona una visión descendente y ascendente de los riesgos asociados a sus identidades no gestionadas, mal configuradas y expuestas. Esto proporciona a los equipos de seguridad visibilidad de las rutas de ataque que los ciberdelincuentes podrían utilizar para desplegar ransomware y robar datos.

Proofpoint en acción

Un holding evalúa los riesgos relacionados con la identidad de una nueva adquisición con el fin de completar la fusión y la adquisición de forma segura.

Con casi 200 000 millones de dólares en activos y 1000 sucursales, este holding bancario regional adquiere un nuevo banco cada tres años. Con cada fusión y adquisición, su equipo de TI combina sistemas, software, datos y procesos. Pero primero, el holding debe evaluar la seguridad del banco que va a comprar. En este ejemplo, el equipo dispuso de menos de cuatro meses para completar su evaluación.

El nivel de seguridad de un banco depende totalmente de la seguridad de sus identidades. El equipo de TI del banco sabía que si podían identificar las vulnerabilidades relacionadas con la identidad de la nueva adquisición, tendrían una idea clara de su nivel de seguridad.

Durante los últimos seis meses, el equipo había utilizado Proofpoint Identity Protection para analizar sus propias estaciones de trabajo y repositorios de identidades. Por tanto, estaba familiarizado con su valiosa información. Por eso decidió utilizar Proofpoint Spotlight para realizar la valoración inicial del banco adquirido.

"Estoy muy contento de que utilizáramos [Proofpoint Spotlight]; todo el mundo ha visto sus ventajas. Utilizaremos el mismo enfoque para nuestra próxima fusión y adquisición".

–Director de Ingeniería de ciberseguridad

Tras analizar el entorno de TI de la nueva adquisición, Proofpoint generó una puntuación de riesgo en la que se detallaban una serie de áreas de riesgo relacionadas con la identidad. Una de ellas destacó rápidamente sobre el resto: las estaciones de trabajo tenían 3000 cuentas de administrador de dominio activas. Bastaría con que uno de ellos se viera comprometido por un ciberdelincuente para que el equipo perdiera el control de todo el entorno.

Tras familiarizarse con las prácticas de seguridad del nuevo banco, la dirección decidió que, dados los riesgos que entrañaba, era preferible mantener separados los dos entornos de TI, al menos al principio. Con Proofpoint, habría sido mucho más difícil justificar el aumento de la protección que el equipo de TI consideraba necesario.

Principales conclusiones

Muy a menudo, los riesgos relacionados con la identidad son el resultado de procesos empresariales y de TI ordinarios que han estado vigentes durante muchos años. Por lo tanto, son difíciles de detectar y fáciles de pasar por alto, en especial en entornos adquiridos recientemente mediante fusiones y adquisiciones.

Es esencial analizar constantemente AD, Entra ID, los endpoints y otros repositorios en busca de vulnerabilidades relacionadas con la identidad. Un ciberdelincuente solo necesita comprometer una única estación de trabajo con un único usuario para hacerse con el control de todo un entorno.

Conclusión

La mayoría de las empresas buscan regularmente software y aplicaciones vulnerables, pero suelen olvidarse de las identidades vulnerables. Sin embargo, las identidades tienen un valor incalculable. En muchos sentidos, son los recursos más valiosos de una empresa, ya que se relacionan con todos sus demás activos digitales.

Por ello, protegerlos es de vital importancia. Los ciberdelincuentes actuales tienen acceso a una amplia gama de herramientas que les permiten aprovecharse de las credenciales de inicio de sesión de forma rápida, fácil y eficaz. Peor aún, a las empresas les resulta difícil detectar su uso.

Para romper la cadena de ataque, necesita proteger sus identidades como protege cualquier otro activo valioso. Esto comienza con la adopción de medidas proactivas. Debe corregir sus identidades vulnerables antes de que los atacantes las descubran y utilizar señuelos para interceptar a los ciberdelincuentes antes de que causen daños.

Para obtener más información sobre cómo puede ayudarle Proofpoint a proteger sus identidades, visite: https://www.proofpoint.com/us/products/identity-protection.

MÁS INFORMACIÓN

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

ACERCA DE PROOFPOINT

Proofpoint, Inc. es una compañía líder en ciberseguridad y cumplimiento de normativas que protege el activo más importante y de mayor riesgo para las organizaciones: las personas. Gracias a una suite integrada de soluciones basadas en cloud, Proofpoint ayuda a empresas de todo el mundo a detener las amenazas dirigidas, a salvaguardar sus datos y a hacer a los usuarios más resilientes frente a ciberataques. Compañías líderes de todos los tamaños, entre las que se encuentra el 85 % del Fortune 100, confían en las soluciones de Proofpoint para su seguridad centrada en personas y su cumplimiento regulatorio, mitigando los riesgos más críticos en sus sistemas de correo electrónico, cloud, redes sociales y web. Encontrará más información en **www.proofpoint.com/es**.