proofpoint.

Gestión de amenazas internas en el sector de los servicios financieros

Proteja los datos sensibles y la reputación de su marca

proofpoint.com/es

Introducción

Las empresas de servicios financieros suelen ser de las primeras en adoptar las nuevas herramientas de ciberseguridad. Sin embargo, a pesar de esa inversión, el sector sigue contabilizando casi un cuarto de todas las violaciones de la seguridad. Y el personal interno contribuye con más de la mitad de estos incidentes.

Como parte de sus funciones, los trabajadores de este sector crítico tienen acceso a flujo de dinero digital y a datos importantes de los clientes. Este acceso los convierte en un factor de riesgo inherente para su negocio, y en objetivos muy lucrativos para los ciberdelincuentes.

Algunos actúan con motivaciones maliciosas. Muchos son sencillamente descuidados. Y otros han sido comprometidos por atacantes externos que consiguen acceso a datos sensibles, sistemas y recursos. No es de extrañar que las amenazas internas sean un vector de amenazas tan complicado de abordar.

Este libro electrónico examina la gestión de amenazas internas desde el punto de vista del sector de los servicios financieros. Basándose en ejemplos de la vida real en los sectores de los seguros, la banca y la gestión de patrimonios, aborda los desafíos de la gestión de estas amenazas, y muestra de qué forma puede ayudarle Proofpoint a identificar, investigar y responder a los incidentes internos de forma rápida y eficaz.

El 24 % de todas las violaciones de la seguridad se producen en instituciones financieras. Y más de la mitad de los ataques a estas empresas son responsabilidad del personal interno[1].

[1]Informe de Verizon sobre las investigaciones de fugas de datos. 2017

SECCIÓN 1

Las amenazas internas en el dinámico sector actual de los servicios financieros

Desde 2018, el sector de los servicios financieros ha experimentado un aumento del 20,3 % en el número de amenazas internas[2].

Si bien todas las empresas tienen la obligación de proteger la información confidencial (la información de los clientes, los datos corporativos y la propiedad intelectual), este deber es incluso más crítico en el caso de bancos, empresas de crédito, sociedades de gestión de inversiones y compañías aseguradoras.

Al igual que otros sectores, el sector financiero tiene que hacer frente a la dispersión creciente de las plantillas y a la multiplicación de las aplicaciones basadas en la nube. Estas tendencias convergentes complican todavía más la gestión de las amenazas internas.

En la actualidad, la infraestructura de TI se comparte entre un mayor número de usuarios. En una empresa típica, pueden disponer de acceso contratistas, proveedores de servicios, partners de servicios y empleados. Definir qué es "personal interno" ya no es tan sencillo.

Y desafortunadamente, la definición de "amenaza" no es mucho más simple. La gestión de amenazas internas no se limita entonces a eliminar a los usuarios maliciosos, sino que también es necesario identificar y gestionar las amenazas que representan los usuarios negligentes y o que han sido víctimas de un ataque.

[2] Ponemon Institute. Informe de 2020 sobre el coste de las amenazas internas a nivel mundial.

SECCIÓN 2

Los misterios de los riesgos internos

Los riesgos internos deberían ser una prioridad para las empresas que utilizan tecnología digital. Esto es particularmente crítico para las empresas de servicios financieros.

Pero, ¿por quién y por dónde deberíamos empezar? El primer paso para crear un programa de amenazas internas habilitado mediante tecnología es resolver *los misterios* de los riesgos internos:

- ¿Quiénes son las personas que suponen un riesgo?
- ¿Qué debería proteger?

¿Quién son las personas que suponen un riesgo?

La gestión de los riesgos asociados a personal interno empieza por crear la lista de usuarios que representan la mayor amenaza. Aunque esta lista varía para cada empresa, hay algunos perfiles de usuarios comunes a tener en cuenta:

Usuarios externos. Las cadenas de suministro dinámicas y de servicio desagregadas son habituales en los servicios financieros. A menudo los contratistas, proveedores de servicios, consultores y partners comparten la infraestructura de TI con los empleados. Cualquiera de ellos puede representar un riesgo potencial.

Usuarios con privilegios de acceso. Algunos trabajadores necesitan acceso a infraestructura e información protegidas. Por ejemplo:

- Administradores de TI
- Empleados del servicio de asistencia
- Agentes del centro de llamadas
- Administradores financieros

Empleados de alto riesgo. El equipo de RR. HH. puede considerar de alto riesgo a algunos usuarios por factores como:

- Comportamiento
- Cambios de empleo
- Problemas de rendimiento o disciplinarios
- Riesgo de dimisión

Los empleados afectados por fusiones y adquisiciones. El sector de los servicios financieros experimenta cambios permanentes. Las empresas participan habitualmente en fusiones, adquisiciones y desinversiones. Las bases de usuarios autorizados de una empresa pueden disminuir o aumentar rápidamente. Estos cambios pueden generar presión en la organización y pueden dar lugar a fugas de datos.

Teletrabajadores. En la actualidad, un porcentaje mucho mayor de las plantillas en todo el mundo trabaja de forma remota. Trabajar fuera de los perímetros de red protegidos puede aumentar el riesgo de incidentes con personal interno.

No se trata exclusivamente de usuarios maliciosos

El concepto de "amenaza interna" se asocia comúnmente a usuarios malintencionados, en los que las motivaciones pueden ser económicas, políticas o de venganza personal. Sin embargo, los usuarios negligentes o víctimas de una usurpación de identidad ("usuarios comprometidos") se encuentran con mayor frecuencia en el origen de compromisos internos.

El término "usuarios negligentes" designa a las personas que actúan al margen de los procesos autorizados. Inconscientemente exponen su infraestructura o datos y aumentan el riesgo.

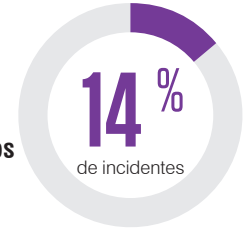
El término "usuarios comprometidos" designa a las personas que están bajo la influencia de ciberdelincuentes externos: algunos son engañados mediante técnicas de ingeniería social para que envíen datos; otros sencillamente pierden el control de sus cuentas.

En cualquier caso, los usuarios negligentes y comprometidos constituyen, por lo general, la mayor amenaza interna.

Usuarios internos negligentes

Usuarios internos maliciosos

Usuarios internos comprometidos



¿Qué debería proteger?

Como la mayoría de las empresas, las firmas de servicios financieros deben contar con una protección óptima de sus transacciones digitales. Asimismo, esta protección depende de la infraestructura de TI orientada a empleados y clientes. A continuación enumeramos algunas de sus mayores preocupaciones:

Protección de datos sensibles. Las firmas de servicios financieros gestionan grandes volúmenes de datos de carácter privado, como datos de tarjetas de pago y datos médicos personales. Dado el enorme atractivo para los estafadores, estos datos son objetivo frecuente de ataques.

Cumplimiento de normativas. El sector de los servicios financieros está sometido a una gran cantidad de regulaciones y exigencias de cumplimiento normativo. Estas normas regulan la forma en la que las empresas protegen los datos, la información y la integridad de sus procesos. Las lagunas de cumplimiento y las fugas de datos puedes ser muy costosas.

Fraude financiero. Las firmas de servicios financieros gestionan grandes volúmenes de transacciones y capital. Los estafadores se aprovechan de los trabajadores y utilizan su acceso privilegiado para robar efectivo a través de una gran cantidad de estratagemas.

Interrupción del servicio. Las firmas de servicios financieros dependen de la infraestructura de TI para dar soporte a los servicios orientados a clientes y empleados. Si un ciberdelincuente obtiene acceso interno, puede dañar o alterar sus sistemas. El tiempo de inactividad puede suponer la pérdida de ingresos, de oportunidades y de confianza.

Protección de la información confidencial. Muchas sociedades de inversión dependen de información y algoritmos de negociación (trading) para garantizar su competitividad. El éxito de sus servicios depende de su capacidad para proteger esos datos.

Daños a la reputación. Los servicios financieros forjan su reputación sobre la base de la confianza, ya sea de clientes, de partners comerciales o de reguladores. Cuando se produce una violación de la seguridad, sobre todo si la responsabilidad es de personal interno, se vulnera esa confianza y se empaña su reputación.

SECCIÓN 3

El papel de la tecnología de gestión de amenazas internas

La gestión de amenazas internas ayuda a los equipos de seguridad a controlar este vector de amenazas único.

Combina elementos de prevención de la pérdida de datos (DLP) y análisis del comportamiento de los usuarios para reducir el riesgo de tres maneras:

Identificación del riesgo asociado a los usuarios

Las soluciones de gestión de amenazas internas (ITM) permiten a los equipos de seguridad detectar rápidamente violaciones potenciales de la seguridad. Las herramientas más eficaces le ayudan a diferenciar entre falsos positivos y actividad de personal interno que precisa seguimiento. Esto supone conocer todo el contexto sobre la actividad de los usuarios de riesgo y el movimiento de los datos, sobre todo en el caso de los usuarios considerados de alto riesgo.

Protección frente a la pérdida de datos

La mayoría de las firmas financieras tienen datos que deben proteger: algoritmos exclusivos, secretos comerciales, información de identificación personal, etc. Ninguna de estas empresas desea que estos datos abandonen indebidamente su entorno. Identificar y detener rápidamente las fugas de datos es una función esencial de una solución ITM moderna.

Aceleración de la respuesta a incidentes

El coste de las amenazas internas depende del tiempo que se tarde en responder a un incidente. Los sistemas ITM modernos pueden ayudar a los equipos de seguridad a hacerlo hasta 10 veces más rápido. Si se cuenta con la solución ITM adecuada, tareas que podrían haber llevado días o semanas pueden finalizarse en minutos. Investigaciones más rápidas dan lugar a tiempos medios de reparación más cortos.

SECCIÓN 4 – La solución Proofpoint ITM en acción

Casos de clientes del mundo real

Empresa internacional de correduría de seguros – Mayor visibilidad de la actividad de los empleados dispersos

El desafío

Una empresa internacional de correduría de seguros buscaba una solución para proteger los datos relativos a los siniestros de los clientes.

Para ello, su equipo de seguridad necesitaba una mayor visibilidad de las fugas de datos potenciales asociadas a personal interno. Aunque la empresa podía supervisar su plantilla dispersa a través de una aplicación basada en la web, la revisión e interpretación de los registros de actividad de la aplicación llevaba mucho tiempo y trabajo. Al mismo tiempo, las leyes de protección de datos no hacían sino aumentar la preocupación sobre los datos recogidos y gestionados a través de la aplicación.

La solución

La empresa necesitaba una herramienta de gestión de amenazas internas para proteger de manera proactiva los datos confidenciales dondequiera que se encontraran y desplazaran, sobre todo en endpoints remotos. Buscaba una mayor visibilidad sobre la manera de interactuar de los usuarios con los datos y de sus actividades en los endpoints. Necesitaba una solución que pudiera identificar activamente el comportamiento de alto riesgo, enviar alertas de cumplimiento y facilitar las auditorías a los equipos de cumplimiento de normativas.

El resultado

Gracias a la solución ITM, la empresa ahora puede:

- Detectar el movimiento peligroso de los archivos de datos de siniestros desde las aplicaciones empresariales, en los servidores y fuera de los endpoints.
- Formar y advertir, en tiempo real, a los usuarios de comportamientos al margen de la política.
- Correlacionar pruebas irrefutables (quién ha hecho qué, cuándo, dónde, por qué y cómo) al investigar una alerta. Las capturas de pantalla de la actividad de los endpoints proporcionan contexto sobre qué ocurrió antes y después de un incidente. Esta información ayuda a determinar si se trató de un acto negligente, malicioso o resultado de un compromiso externo.
- Conservar una pista de auditoría detallada de la actividad de empleados y terceros a fin de cumplir las exigencias de cumplimiento financieras.

Empresa de gestión de patrimonios independiente – Protección de los activos y la confianza de los clientes

El desafío

Las firmas de gestión de patrimonios independientes tienen la responsabilidad de mantener protegida la información sensible y privada de los clientes. Su éxito depende de la confianza.

Como parte de sus tareas diarias, la plantilla de la empresa procesa datos privados de los clientes. Para la empresa, las amenazas internas pueden proceder de gestores de fondos, administradores y otros empleados, pero también de contratistas externos. La firma se enfrentaba a amenazas constantes: ciberdelincuencia, espionaje empresarial y financiado por estados, fraude monetario, etc.

La solución

La empresa necesitaba un sistema de seguridad robusto que les protegiera frente a la ciberdelincuencia y el fraude monetario. El equipo de seguridad necesitaba una forma más sencilla de supervisar la actividad de riesgo potencial en toda la empresa. Eso incluía a los usuarios dispersos y usuarios externos.

El resultado

Gracias a la solución ITM la empresa fue capaz de:

- Simplificar las políticas de uso aceptable y cumplimiento.
- Detectar automáticamente el movimiento peligroso de información sensible y confidencial en tiempo real.
- Optimizar las investigaciones de incidentes mediante la correlación del movimiento de todos los datos y la actividad de los usuarios en tiempo real. Las capturas de pantalla de la actividad en los endpoints proporcionaron pruebas irrefutables de lo que hizo el usuario.
- Conservar una pista de auditoría detallada de la actividad de los usuarios a fin de cumplir las exigencias de cumplimiento financieras.

Banco regional – Protección frente a amenazas internas en los centros de llamadas

El desafío

Como consecuencia de la generalización del teletrabajo, un banco regional necesitaba garantizar la protección de sus centros de llamadas.

Los empleados de la institución accedían a datos de miembros del personal en cada llamada. Por su parte, el equipo de seguridad necesitaba seguir supervisando las actividades internas y responder a incidentes potenciales incluso si los empleados trabajaban desde casa. Al banco le preocupaba particularmente los empleados de alto riesgo, concretamente los que disponían de acceso a información personal valiosa, que podía ser objeto de robo, filtración o alteración. El equipo también necesitaba identificar, recopilar y compartir datos forenses al responder a un incidente.

La solución

El equipo de seguridad buscaba una solución capaz de detectar comportamientos anormales en tiempo real. Pero tenía que mejorar la recopilación y supervisión de datos en un contexto de teletrabajo sin perjudicar la productividad y servicio al cliente.

El resultado

La solución ITM ha permitido al centro de llamadas resolver sus desafíos de amenazas internas gracias a que consiguió:

- Hacer más resilientes a los usuarios. ITM aumentó la concienciación en materia de seguridad con escenarios de amenazas internas del mundo real. También ayudó al banco a clarificar las políticas de datos corporativos.
- Desplegar, en los endpoints, recolectores ligeros y ejecutados en modo de usuario. Este método ha permitido mantener la productividad de los usuarios gracias a que no ralentizó sus dispositivos.
- Detectar comportamientos peligrosos de los usuarios y el movimiento de los datos en tiempo real.
- Colaborar con los distintos equipos: RR. HH., jurídico, cumplimiento de normativas y de TI. Los equipos trabajaron conjuntamente para acordar la recopilación de datos de usuarios y archivos, las necesidades de detección de comportamientos y los flujos de trabajo de respuesta a incidentes.
- Acelerar las investigaciones. Además de proporcionar inteligencia contextual sobre el usuario, la solución ITM simplifica la recopilación de pruebas y facilita la colaboración entre los equipos.

Conclusiones y recomendaciones

Por qué Proofpoint: un asesor de confianza y soluciones ITM de gran rendimiento

Cada día, sus equipos de TI y de seguridad trabajan duro para identificar, detectar y responder a las ciberamenazas. La solución Proofpoint Insider Threat Management (ITM) puede ayudarle. Puede protegerle frente a la pérdida de datos, perturbaciones de la actividad y otros daños provocados, voluntaria o involuntariamente, por los usuarios.

Nuestra galardonada solución ha ayudado a más de 1200 empresas líderes en más de 100 países a:

- Reducir el tiempo medio de detección de riesgos potenciales a la información sensible y confidencial de las amenazas internas.
- Reducir la frecuencia, gravedad y coste de las fugas con tiempo medios de respuesta a incidentes más cortos.
- Aumentar la productividad de los equipos de seguridad reduciendo costes. Con Proofpoint, puede consolidar varias tecnologías (como análisis basado en usuarios y DLP para endpoints) en una sola plataforma ITM.

Así es como podemos ayudarle:

- Trabajaremos con usted en una prueba de concepto (PoC) que le ayude a visualizar su programa ITM.
- Podemos ayudarle a diseñar y crear su programa de gestión de amenazas internas. Podemos fraccionar sus proyectos en una seria de tareas fáciles de gestionar y priorizarlas en función de los comportamientos de alto riesgo. La prueba de concepto le ayuda a visualizar su programa ITM y nuestros servicios ITM Jump Start le garantizan alcanzar rentabilidad mucho antes.
- Por último, fortalecemos la resiliencia de usuarios con nuestro programa Proofpoint Security Awareness Training.

Nuestro objetivo es el mismo que el suyo: proteger los activos empresariales importantes y las personas que los producen.

MÁS INFORMACIÓN

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

ACERCA DE PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT) es una compañía líder en ciberseguridad 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 encuentran más de la mitad del Fortune 1000, 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**.

0512-002-01-01 10/21