ManageEngine
DataSecurity Plus

El enemigo interno:

Manual de gestión de **amenaza** internas

www.datasecurityplus.com

Índice

1. Introducción

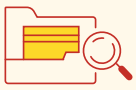
> **Si no conoces al enemigo ni a ti mismo, sucumbirás en todas las batallas.**

Sun Tzu

Las mayores amenazas para cualquier organizació en día suelen provenir de los empleados y socios e que más confía. Las amenazas internas plantean a organizaciones un problema único, ya que pueden ataques intencionados llevados a cabo por actores maliciosos o errores involuntarios de empleados bienintencionados. Este e-book está diseñado para identificar y explicar los diversos indicadores de las amenazas internas, así como las últimas tendencia prácticas utilizadas para prevenir las amenazas inte y mitigar sus efectos.

2. ¿Qué es una amenaza in

Una amenaza interna es cualquier amenaza de seguridad no autorizada o no intencionada a los datos o sistemas de información de una organización que se origina en un individ que opera dentro de la organización. La persona con informa privilegiada no tiene que ser necesariamente un empleado ac puede ser un contratista, un empleado temporal o un antiguo empleado. Las amenazas internas pueden provocar el robo d datos, el uso indebido de los mismos, el sabotaje, el espiona fraude, así como comprometer la integridad, la disponibilidad confidencialidad de los datos de una organización, entre otra cosas.

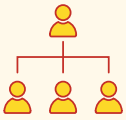


Según el informe de Verizon sobre , las amenazas internas son más frecuentes en el sector salud que las externas. El 68% de los incide pérdida de datos de información de salud protegida (PHI) entre 201 2017 implicaron a personas con acceso a información privilegiada.

Según el informe de Trend Micro , un conjunto completo de P de una persona fallecida puede venderse en la web oscura po menos 1.000 dólares

3. Peligros de una amenaza interna

Algunos de los mayores incidentes de seguridad que han producido -como las violaciones de Equifax, Fed y la Agencia de Seguridad Nacional (NSA)- fueron ro de datos perpetrados por una persona con informaci privilegiada. Comprender los motivos de un ataque interno, los indicadores potenciales de un ataque inte inminente y prepararse para las consecuencias de u esencial para cualquier organización. Los factores que se exponen a continuación explican qué las amenazas internas son uno de los problema seguridad más peligrosos y persistentes a los que se enfrentan las organizaciones.



Según el de Protenus, una organización tarda una de 308 días en identificar una violación.

Según el informe de Protenus, la PHI de 1.129.744 miembros del sector salud fue expuesta, robada o vis por personas no autorizadas en el primer trimestre de 2018.

3.1

Las violaciones pueden pasar desapercibida durante largos periodos de tiempo

Según el informe 2018 , se tarda una media de más de dos meses en contener una a interna. Cuanto más tiempo se tarda en descubrir un incidente después de que se pr más se tarda en evaluar los daños infligidos, detener a las personas implicadas y ado medidas reactivas adicionales para evitar futuros incidentes.

3.2

La amplitud y la escala de las amenazas internas pueden ser enormes

Las vulnerabilidades de seguridad pueden surgir de casi cualquier persona y de cualquier lugar. Ya sea un empleado descontento, un usuario descuidado, un lad datos enmascarado o un socio que carece de las medidas de seguridad necesar variedad de amenazas internas es lo que hace que cada departamento de cada organización sea vulnerable a un ataque interno

3.3

Prevenir las amenazas internas es difíc

No todos los incidentes internos son intencionados; la mayoría de las veces son ca por la falta de atención o la negligencia de un usuario. Esto hace que sea difícil ten solución holística que detecte tanto los incidentes de seguridad intencionados com intencionados. Además, muchos usuarios con información privilegiada malintencio introducen credenciales legítimas en sus propios equipos utilizando privilegios que fueron concedidos, lo que hace aún más difícil detectar y frustrar los ataques en cu

4. ¿Cuáles son los diferentes tipo de amenazas internas?

Las amenazas internas son de todo tipo y tamaño, pero lo habitual es que entren en una de estas tres categorías:

- Personas con información privilegiada maliciosas
- Usuarios negligentes o descuidados
- Terceros contratistas

4.1

Persona con información privilegiada maliciosa

Las personas con información privilegiada maliciosas socavan deliberadamente los de seguridad de una organización. Ya sea que se trate de un empleado descontento un agente criminal, estos individuos utilizan sus credenciales legítimas o robadas pa acceder a los sistemas de la organización con la intención de interrumpir, robar o ha uso indebido de los datos o sistemas de TI.

4.2

Persona con información privilegiada negligen o descuidada dentro de la empresa

La mayoría de las veces, es un empleado negligente el que causa un daño irreparab organización. Por ejemplo, acciones descuidadas -como hacer clic en un correo de p borrar un archivo sensible, ignorar los protocolos de intercambio de datos, utilizar un pública no segura para acceder a datos sensibles o usar credenciales débiles- cond filtración o pérdida de datos o a vulnerabilidades de seguridad que los delincuentes aprovechar.

4.3

Tercero con información privilegiada

Muchos contratistas externos, como los proveedores, tienen un acceso lim los recursos y datos de una organización. Si la propia red de un tercero ac comprometida, puede servir de p

Según el informe de 2018 Cost of Insider Threats Global report del Ponemon Institute:

- Los incidentes relacionados con el robo de credenciales son los más cost
- La causa principal de la mayoría de los incidentes es una persona con información privilegiada negligente.
- El tamaño de la organización y el sector afectan el costo por incidente.
- La incidencia de cada tipo de amenaza interna está aumentando.
- La negligencia de los empleados o contratistas es la que más cuesta a la empresas.
- En promedio, se tarda más de dos meses en contener un incidente c información privilegiada.

Según el Informe Anual de Ciberseguridad 2018 de Cisco, e de todos los ataques provocaron un daño financiero de más 500.000 dólares. Estos daños incluyen la pérdida de ingreso clientes y oportunidades, así como los gastos por cuenta pro

Según las estadísticas del Breach Level Index, cada segund pierden o roban 71 registros de datos.

5. Indicadores de una amenaza interna

Los indicadores de una amenaza interna pueden dividirse en d categorías:

- Indicadores conductuales
- Indicadores no conductuales

5.1

Indicadores conductuales de una amenaza interna

Mostrar uno o más de los rasgos que se enumeran a continuación no significa necesariamente que una persona vaya a llevar a cabo un ataque, sino simplemente organización debe vigilarla más a menudo. Los comportamientos de alto riesgo que mencionan a continuación suelen estar asociados a las amenazas internas.

Fig. 1. Posibles rasgos, comportamiento y objetivos de una pers con información privilegiada

Rasgos	Comportamie nto	Objetivos
Vengativo	Horarios de trabajo extraños	Venganza
Negligente	Estrés financiero	Beneficios financieros
Demasiado entusiasta	Insatisfecho con las políticas de la organización	Espionaje
Ingenuo	No se le ha dado un ascenso	Hacktivismo
	Rechazado o despedido; contrato n renovado	

5.2

Indicadores de sistemas de alto ries de una amenaza interna

Aparte de los indicadores conductuales, existen múltiples vulnerabilidades del sistema de las que podría aprovecharse un potencial infiltrado. Ser consciente estos indicadores tempranos podría ayudar a las organizaciones a sellar la ex y tomar medidas preventivas contra posibles ataques internos. Algunos de los indicadores son:

5.2.1 *Exceso de archivos o cuentas de usuario huérfanas*

Las organizaciones se exponen a ataques internos cuando carecen de disposicion eliminar o modificar archivos, carpetas y cuentas de usuario cuando los usuarios c de rol dentro de la organización o la abandonan por completo. Las cuentas huérfa proporcionan un medio para que los actores maliciosos obtengan acceso no autor realicen el robo de datos. Si una cuenta huérfana es una cuenta con privilegios (po ejemplo, una cuenta de usuario con privilegios administrativos para uno o más sist una cuenta de administrador de sistemas), entonces la amenaza es exponencialm mayor.

5.2.2 *Presencia de TI invisible*

La TI invisible se refiere al uso de las aplicaciones de TI de una organización y ot infraestructuras de TI sin el conocimiento del departamento de TI de la organizaci Cuando una empresa carece de información sobre los recursos de TI que se utiliz gestión y la seguridad de esos recursos se vuelven difíciles. Es más, estos recurs podrían proporcionar un canal a través del cual los actores maliciosos se infiltran red.

5.2.3 *Niveles de autenticación inapropiados*

Los protocolos de autenticación fáciles o débiles, sin el uso de la autenticación esc o multifactorial, envalentonan a los actores maliciosos en sus intentos. Por otro lad niveles inadecuados de autenticación fuerte también pueden causar múltiples prob entre ellos que los empleados justifiquen el uso de la TI invisible. Las medidas de c de acceso deben reflejar siempre la sensibilidad de la información a la que se acce.

5.2.4 *Lecturas excesivas de "acceso denegado"*

Múltiples intentos fallidos de acceso a recursos de TI críticos restringidos apuntan claramente a un posible ataque interno. Es esencial monitorear los intentos de acceso denegado a los recursos de TI que van más allá de lo necesario para que los empleados realicen sus funciones.

5.2.5 *Robo de datos*

El robo de datos sensibles es una señal de alarma que puede indicar la presencia de un agente interno malicioso. La descarga o adquisición de copias de información crítica o de propiedad privada, el uso de protocolos empresariales no autorizados para transmitir datos y la transferencia de datos fuera de la organización son indicadores claros de una amenaza interna.

Fig 2. La cadena de muerte de la amenaza

6. Diez buenas prácticas para luchar contra las amenazas internas

6.1

Establezca un comportamiento de referencia tanto para los individuos como para las redes

Registre y monitoree sistemáticamente el patrón normal de comportamiento de los empleados para tener algo con lo que comparar la actividad repentina o inusual. Analice el volumen neto de transferencia de archivos a través de su red, el total de intentos de acceso a sus archivos más críticos y otros puntos de acceso críticos para facilitar la detección de anomalías.

6.2

Proporcione la menor cantidad de privilegios posible

Restrinja la presencia de archivos, carpetas y recursos compartidos sobre expuestos. Utilice un sólido sistema de gestión de accesos para evitar accesos injustificados y reducir el número de puntos de acceso a través de los cuales los actores maliciosos pueden explotar fácilmente los datos de su organización.

6.3

Realice evaluaciones de riesgo periódicas en toda la organización

Determine el tipo de datos que procesa su organización, la importancia de los mismos, dónde se almacenan y quién tiene acceso a ellos. Un inventario de los datos de su organización y otros detalles relevantes ayudan a establecer el tipo de medidas de seguridad y control de acceso necesarias. Además, todos los proveedores externos que trabajen con su organización deben realizar evaluaciones de riesgo para investigar a fondo su postura de seguridad y mantener la seguridad de su organización.

6.4

Eduque a los usuarios finales

Forme regularmente a sus empleados para que sepan detectar y evitar las situaciones de ataque interno más comunes, como los correos electrónicos de phishing y los anuncios malintencionados. Eduque y advierta a sus empleados sobre las consecuencias de violar las políticas y procedimientos de la organización.

6.5

Aplique políticas estrictas de gestión de contraseñas y cuentas

Implemente la autenticación multifactor o escalonada y aplique políticas de contraseñas sólidas para fortificar la red de su organización. Además, bloquee a los usuarios de sus sesiones después de un período fijo de inactividad para evitar que los actores maliciosos hagan un mal uso de los sistemas abandonados en medio de una sesión.

6.6

Suspenda cuentas de usuario huérfanas

Monitoree de cerca a los empleados y a los terceros en busca de comportamientos sospechosos cuando se acerquen al final de su servicio. Desactive cada uno de sus puntos de acceso a los diversos recursos físicos y de TI de la organización inmediatamente después de que salgan de ella.

6.7

Evite la ejecución de bombas lógicas

Una bomba lógica es un fragmento de código malicioso oculto dentro de un script que se activa cuando se cumple una condición particular, como una fecha, hora o lanzamiento de una aplicación específica. Una clara segmentación de las funciones y la revisión del código podrían ayudar a disuadir a los actores maliciosos de hacer estallar una bomba lógica.

6.8

Aplique la corrección activa

El uso de técnicas de correción activas, como el bloqueo de USB, un fuerte filtrado de correo electrónico y ventanas emergentes que piden autorización al acceder a archivos críticos, ayuda a construir la defensa de su organización contra los ataques internos no intencionales.

6.9

Analice sus políticas de acceso remoto

Diseñe e implemente políticas de acceso remoto con un escrutinio extra para garantizar que sólo se proporciona acceso a los empleados y socios de confianza. Limite el acceso remoto sólo a los dispositivos emitidos por su organización. Monitoree y controle el acceso remoto desde todos los endpoints, especialmente los dispositivos móviles.

6.10

Audite, monitoree y registre todos los intentos de acceso

Capture y registre cada acceso y transferencia de archivos. Analice y cree una base de referencia del comportamiento de los usuarios y de la red para detectar fácilmente las desviaciones del patrón regular.

Gartner prevé que el gasto mundial en seguridad de la información supere los 124.000 millones de dólares en 2019, mostrando un crecimiento del 8,4% respecto a 2018.

7. Estadísticas de amenazas internas

Industria	Organización	Tipo de ataque	Método	Consecuencia	Otros
Salud	Anthem	Negligencia, falta de atención de persona con información privilegiada	Correo electrónico de phishing	Puede haber expuesto información personal de salud de más de 78,8 millones de personas	Anthem gastó más de 260 millones de dólares en medidas de seguridad tras la violación
Ingeniería	Omega Engineering	Persona con información privilegiada maliciosa	Implementó una bomba lógica	Los daños costaron a la organización 10 millones de dólares	El motivo principal fue la venganza por haber sido despedido
Fabricación	Toyota	Persona con información privilegiada maliciosa	Se infiltró a través de una antigua credencial de trabajo	Robó datos personales críticos y datos de pruebas beta, y saboteó 13 aplicaciones	La cuenta de usuario huérfana no fue suspendida
Gobierno	FBI	Persona con información privilegiada maliciosa	Robo de datos en unidades de memoria utilizando el acceso remoto	20.000 archivos o más robados	El motivo principal fue el hacktivismo
Tecnología	Facebook y Google	Negligencia, falta de atención de persona con información privilegiada	Whaling, un tipo de esquema de phishing	Más de 100 millones de dólares robados	El motivo principal fue el hacktivismo
Energía	Tesla	Persona con información privilegiada maliciosa	Código malicioso	Realizó cambios en el sistema operativo de fabricación de Tesla y exportó datos sensibles de Tesla a terceros	El motivo principal fue el hacktivismo

DataSecurity Plus

ManageEngine DataSecurity Plus es una solución de visibilidad y seguridad de datos. Supervisa y alerta sobre las modificaciones y el movimiento de archivos críticos en servidores de archivos, failover clusters, estaciones de trabajo y USB. Los usuarios pueden localizar y analizar los archivos que contengan PII/ePHI almacenados en servidores de archivos de Windows, failover clusters y entornos de OneDrive mediante reglas de detección de datos integradas. Su función de prevención de pérdida de datos (DLP) ayuda a detectar y responder al robo de datos sensibles a través de USB, correo electrónico, impresoras y más. También proporciona informes de auditoría detallados que ayudan a las organizaciones a agilizar el cumplimiento de múltiples normativas de TI.

Para explorar estas funciones y ver DataSecurity Plus en acción, .
Para saber más sobre DataSecurity Plus, visite www.datasecurityplus.com.

Download free trial $ Get a quote

Explore **las soluciones de DataSecurity Plus**

Auditoría del servidor de archivos
Audite e informe sobre los accesos y modificaciones de los archivos, con alertas en tiempo real y respuestas automatizadas para las actividades críticas de los archivos.

Learn more

Análisis de archivos
Analice la seguridad y el almacenamiento de los archivos, gestione los archivos basura, optimice el uso del espacio en disco e identifique las vulnerabilidades de los permisos.

Learn more

Evaluación del riesgo de los datos
Descubra y clasifique los archivos que contienen datos confidenciales, como PII, PCI y ePHI, combinando la inspección de contenidos y el análisis contextual.

Learn more

Prevención de la pérdida de datos
Detecte e interrumpa las pérdidas de datos a través de los USB, el correo electrónico, las aplicaciones web y las impresoras; monitoree la actividad de los archivos en los endpoints; y mucho más.

Learn more

Protección en la nube
Supervise el tráfico web de la empresa y aplique políticas para bloquear el uso de aplicaciones web inapropiadas, de riesgo o maliciosas.

Learn more

Referencias

https://www.ictsecuritymagazine.com/wp-content/uploads/2017-Data-Breach-Investigations-Report.pdf

https://www.trendmicro.com/content/dam/trendmicro/global/en/security-intelligence/research/reports/wp-cybercrime-&-other-threats-faced-by-the-healthcare-industry.pdf

https://cdn2.hubspot.net/hubfs/2331613/Press_Releases/Breach%20Barometer%202017%20Annual%20Report%20-%20Press%20Release%20-%20Jan%202018.pdf

https://cdn2.hubspot.net/hubfs/2331613/Press_Releases/Q1%202018%20Breach%20Barometer-%20Press%20Release.pdf

https://www.verizon.com/about/news/ransomware-still-top-cybersecurity-threat-warns-verizon-2018-data-breach-investigations-report

https://protenus.com/breach-barometer-report

https://www.databreaches.net/

https://heimdalsecurity.com/blog/insider-threat/

https://images.idgesg.net/assets/2017/08idg_presentation_cybercrime_07202017_final_compressed.pdf

https://www.nbcnews.com/news/world/how-snowden-did-it-flna8C11003160