

AMENAZAS INTERNAS

SU MAYOR RIESGO DE SEGURIDAD SE ENCUENTRA AL INTERIOR



¿Qué es una amenaza interna?

El riesgo de seguridad que suponen los empleados, asociados, socios, contratistas y proveedores de servicios de una empresa que tienen acceso a sus recursos y datos se clasifica como amenaza interna. La actividad de los agentes internos es una de las mayores preocupaciones de seguridad para los datos de la empresa porque los atacantes se encuentran más allá de la primera línea de defensa.

34% DE TODAS LAS INFRACCIONES INVOLUCRAN AGENTES INTERNOS. ^[1]

Perfiles de amenazas internas



LOS AGENTES INTERNOS NEGLIGENTES

comprometen la seguridad de la empresa al no seguir las políticas de ciberseguridad. Suelen ser víctimas de ataques de ingeniería social.

UNA ESTAFA DE PHISHING EXTENDIDA LE COSTÓ A FACEBOOK Y A GOOGLE

\$ 100 MILLONES. ^[2]



LOS AGENTES INTERNOS INVOLUNTARIOS

son empleados cuyas cuentas se ven comprometidas por actores externos. Participan en incidentes de seguridad de forma involuntaria.

5.2 MILLONES DE REGISTROS DE LOS INVITADOS DEL MARRIOTT FUERON ACCEDIDOS A TRAVÉS DE CUENTAS DE EMPLEADOS COMPROMETIDAS. ^[3]



LOS AGENTES INTERNOS MALICIOSOS

utilizan deliberadamente su acceso legítimo a los datos críticos para robarlos, borrarlos, manipularlos o filtrarlos con fines de venganza o beneficio personal

2.9 MILLONES DE REGISTROS DE PII FUERON EXPUESTOS POR UN EMPLEADO VENGATIVO DE DESJARDINS. ^[4]

Factores que motivan las amenazas internas

Según el Informe de investigaciones sobre la violación de datos, ⁽¹⁾

los principales factores que motivan el robo de datos son:

71%

Beneficios económicos

25%

Espionaje

4%

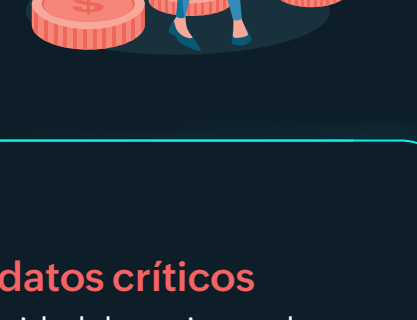
Otros (negligencia, venganza, etc.)

El impacto de los ataques internos

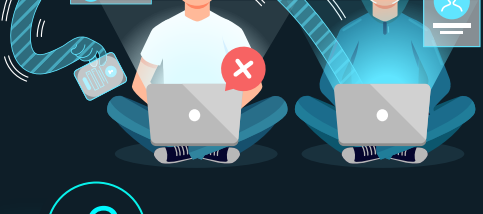
1

Grandes pérdidas monetarias

El coste de un ataque interno oscila entre los **\$100 000 Y \$2 MILLONES.** ^[5]



2



Pérdida de datos críticos

En 2020, la cantidad de registros de datos personales expuestos aumentó un **141%** ^[6]

3

Interrupción operativa

El coste de la interrupción operativa durante cinco años para una organización que sufrió una violación de datos alcanzó la impresionante cifra de **\$1,2 MIL MILLONES.** ^[7]



4



Pérdida de la credibilidad

70% de los consumidores dejaría de hacer negocios con una empresa si ésta sufriera una violación de datos. ^[8]

¿Por qué los ataques internos son difíciles de combatir?



Cómo mitigar las amenazas internas

Consolidar los informes de actividad del usuario

Cuanta más visibilidad tenga de su entorno de Active Directory, más posibilidades tendrá de detectar las amenazas internas.



Monitorear a los usuarios privilegiados

Un componente crítico de la detección de amenazas internas, el monitoreo de usuarios privilegiados, le ayudará a vigilar de cerca a los usuarios que pueden causar el mayor daño.

Supervisar el uso y movimiento de datos:

Audite todos los accesos a datos, incluyendo los cambios de permisos y transferencias de datos a dispositivos de almacenamiento externo, para detectar las anomalías rápidamente.

Automatizar las respuestas ante incidentes de seguridad

Ejecute respuestas como apagar equipos y desconectar las sesiones del usuario para mitigar las violaciones de datos.

Implementar análisis del comportamiento de los usuarios:

Detecte, investigue y mitigue las amenazas como inicios de sesión maliciosos, movimientos laterales, abuso de privilegios, violaciones de datos y malware.

ManageEngine ADAudit Plus

Combata las amenazas internas con ADAudit Plus

ManageEngine ADAudit Plus es un auditor de cambios basado en UBA que monitorea continuamente la actividad de los usuarios y proporciona informes detallados para mejorar su estrategia de detección de amenazas internas.

Explore las funciones de **detección de amenazas internas** de ADAudit Plus con una prueba gratuita de 30 días.

O programe una demostración personalizada.

[Descargar ahora](#)

Datos obtenidos en:

1. Informe de investigaciones sobre la violación de datos 2. CNBC 3. Marriott International 4. Secureworld
5. Bitglass - Informe sobre amenazas internas 6. Informe sobre la violación de datos de QuickView 7. Bajo la superficie de un ataque cibernético
8. Thales 9. Ataques internos para la ciberseguridad - Informe sobre amenazas internas 10. El costo de las amenazas internas