IBM Security

¿Un infiltrado o un usuario real? Las amenazas internas son las más difíciles de combatir.

Los atacantes son inteligentes, ágiles y, a menudo, aparentan ser alguien que no son, lo que hace que las conclusiones sobre seguridad sean más importantes que nunca.

IBM Security
White Paper

Su personal interno: El negocio requiere confianza. Pero la seguridad exige precaución.

Una empresa tiene que confiar en sus empleados, socios y proveedores. Los negocios simplemente no pueden funcionar sin ellos. Pero cuando este personal interno de confianza accede a sus valiosos recursos digitales, usted necesita saber quiénes son y qué están haciendo, y saber si los recursos se han visto comprometidos. Sin esas consideraciones, su riesgo de robo de datos o comprometimiento de aplicaciones puede ser innecesariamente alto.

Considere: El costo promedio de una violación de datos empresariales es de USD 3,26 millones.[1] Hasta el 60 por ciento de los ataques se han atribuido a personal interno.[2] Los números son convincentes. Pero reducir este peligro escapa a muchas empresas.

Esto se debe a que el estereotipo de personal interno amenazador, un empleado descontento que intenta vengarse u obtener ganancias, no es necesariamente cierto. La gente puede ser descuidada. Pueden ser engañados fácilmente por esquemas de ingeniería social bien ejecutados. Y a medida que trabajan para mantener la productividad, pueden comprometer la seguridad. En el sector de servicios financieros, por ejemplo, las amenazas de acciones internas inadvertidas son 10 veces más que la cantidad de acciones internas maliciosas.[3] La configuración incorrecta del servidor de su administrador de sistemas puede crear una vulnerabilidad que sea fácil de explotar. O más comúnmente, el clic de su contador en un correo electrónico de phishing puede generar credenciales robadas. Esto puede abrir la puerta para que los ciberdelincuentes ingresen libremente a su infraestructura y permanezcan allí durante mucho tiempo, sin ser detectados, porque los atacantes parecen ser usuarios legítimos.

Estos ataques son los más difíciles de vencer porque, en la superficie, no parecen ser ataques en absoluto. No se destacan como agentes externos maliciosos que han invadido su red. En cambio, son autorizados y simplemente descuidados o disfrazados e inteligentes. Puede combatirlos solo identificando lo que hacen, analizando el comportamiento para descubrir acciones que se salgan de la norma. Una vez que tenga esa información, puede identificar estas amenazas, tomar medidas para bloquear nuevas acciones y recuperarse del daño que pueden haber causado.

60 %

de los ciberataques se atribuyen al personal interno.[1]

Obtenga más información en el Índice de inteligencia de amenazas IBM® X-Force® 2017.

1 "Estudio de costos de la fuga de datos de 2017: Visión global," *Ponemon Institute*, junio de 2017.
2 "Revisión anual de graves violaciones de datos, ataques importantes y nuevas vulnerabilidades," *Investigación de IBM X-Force: Índice de inteligencia de seguridad cibernética 2016*, abril de 2016.
3 "IBM X-Force Threat Intelligence Index 2017," *IBM Corp.*, marzo de 2017.

Señales de peligro: Cuidado con estas acciones del usuario

Las amenazas internas tienen menos que ver con irrumpir en la infraestructura que con estar ya dentro. Por supuesto, tiene que haber una manera de entrar, ya sea tan simple como un error derivado de la falta de capacitación de los empleados o tan sofisticado como una campaña de spear phishing que roba credenciales. Pero lo que hace que estas amenazas sean tan difíciles de descubrir y manejar es que el agente ya tiene acceso y opera de manera desconocida.

¿Qué debe tener en cuenta? Hay tres signos reveladores:

Robo y corrupción: Los internos se están portando mal

- Acceso y descargas de activos de alto valor que ocurren con más frecuencia de lo normal.
- Uso de una cuenta por primera vez en mucho tiempo o desde una nueva ubicación por primera vez
- Actividad del usuario que se desvía de la normalidad durante un período corto o cambia gradualmente durante un período prolongado
- Patrones de actividad que son diferentes de los patrones de actividad de los compañeros de un usuario.

Errores perjudiciales: El personal interno actúa descuidadamente

- Configuración incorrecta de las herramientas de seguridad de la organización
- Cambios en los atributos de otras personas sin solicitar permiso
- Usuarios que abren cuentas personales en servidores empresariales
- Usuarios que comparten credenciales para redes privadas virtuales
- Contratistas que verifican mensajes y correos electrónicos a través de un proveedor externo, especialmente del extranjero
- Usuarios que se conectan a un servidor en la nube o una cuenta personal en un servicio para compartir archivos

Aberturas para personas externas: Los cibercriminales están aquí

- Un número creciente de transferencias de datos hacia y desde servidores y/o ubicaciones externas
- Números de inicios de sesión más altos de lo esperado de cuentas de máquinas
- Intentos de cambiar privilegios en una cuenta existente o abrir cuentas nuevas

81 %

de los ataques internos utilizaron las credenciales de otra persona para eludir los controles u obtener derechos elevados.[1]

Mire el video de IBM para obtener más información sobre cómo identificar amenazas internas.

1 "La encuesta de Ponemon indica que afirmar que la amenaza creciente de fraude interno no es una prioridad de seguridad principal para las organizaciones, demuestra ser un error costoso," *Ponemon Institute*, 28 de febrero de 2013.

Acción necesaria: Agregue herramientas poderosas a su kit

La filtración de datos confidenciales de negocios por acciones internas maliciosas o inadvertidas, agravada por la posibilidad de que estas acciones puedan provocar el robo a gran escala y el uso indebido de aplicaciones por parte de ciberdelincuentes que usan malware y bots es una preocupación crítica para las empresas de hoy.

El desafío es que, sin las herramientas de análisis adecuadas, no hay forma de diferenciar entre empleados bien intencionados y agentes externos maliciosos que operan disfrazados, hasta que es demasiado tarde. La escasez de personal en los centros de operaciones de seguridad (SOC) agrava el problema. Y aunque la mayoría de las organizaciones implementan soluciones de seguridad, muchas de esas medidas se centran en mantener a los agentes externos fuera.

Como resultado, para hacer frente a las amenazas que ya están dentro de la organización, los SOC necesitan un nuevo enfoque. Necesitan capacidades que les permitan detectar amenazas internas más rápido, contener ataques rápidamente y limitar el impacto del incidente, todo mientras se equilibra la seguridad contra la confianza y los privilegios de acceso que otorgan a usuarios legítimos.

En esencia, la lucha contra las amenazas internas requiere tres capacidades fundamentales:

- **Análisis de seguridad:** herramientas que reúnen una amplia variedad de datos de seguridad y fuentes de amenazas para automatizar la detección de amenazas y facilitar la investigación y la respuesta.
- **Inteligencia de amenazas:** los datos provienen de fuentes externas confiables que brindan información global actualizada sobre las actividades de entidades maliciosas.
- **Búsqueda de amenazas:** investigaciones efectivas que constantemente buscan no solo ataques sino también las vulnerabilidades que los generan.

Con las capacidades básicas implementadas, los analistas de SOC pueden tomar acciones específicas contra amenazas internas, por ejemplo, utilizando flujo de datos para detectar anomalías en el comportamiento del usuario, estableciendo umbrales para el riesgo de cada usuario y bloqueando el acceso del usuario si es necesario. El SOC puede agilizar las investigaciones, mejorar la visibilidad y responder más rápido a las amenazas utilizando las mejores prácticas.

"... los ataques internos dirigidos a servicios financieros y atención médica fueron, en gran medida, el resultado de actores involuntarios [...] que tenían una mayor susceptibilidad a los ataques de phishing. Las organizaciones [...] deberían centrarse en educar a los empleados sobre el phishing y cómo evitar convertirse en una víctima..."[1]

Obtenga más información en la web sobre el enfoque integrado de IBM para combatir las amenazas internas.

1 "IBM X-Force Threat Intelligence Index 2017," *IBM Corp.*, marzo de 2017.

¿Por qué IBM? Un enfoque integrado lo ayuda a mantenerse a salvo.

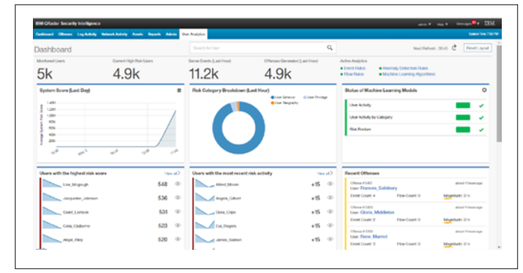
Para detectar mejor las amenazas internas, IBM ofrece un enfoque diseñado para mejorar la capacidad del SOC de supervisar usuarios e investigar actividades sospechosas. Basado en IBM QRadar® Security Intelligence Platform, un motor de análisis que recopila continuamente datos de seguridad, este enfoque crea una línea base de patrones de comportamiento del usuario y perfiles de actividad, luego utiliza algoritmos para detectar anomalías y desviaciones.

Para satisfacer las demandas específicas de combatir las amenazas internas, la plataforma QRadar se puede ampliar con dos soluciones conectadas, ambas descargables desde IBM Security App Exchange.

- **IBM QRadar User Behavior Analytics** proporciona un enfoque fácil de usar. que emplea el aprendizaje automático, el análisis del comportamiento del usuario individual y el análisis del comportamiento del grupo de usuarios para detectar actividades anómalas y asignar puntajes de riesgo a los individuos en función de las acciones. Su panel de control se integra directamente en la consola IBM QRadar SIEM y permite a los analistas ver usuarios de alto riesgo en cualquier momento y determinar las acciones de seguridad necesarias.
- **IBM QRadar Advisor con Watson™** utiliza capacidades cognitivas para investigar la información que recibe de QRadar User Behavior Analytics, califica el incidente e identifica la causa raíz. Operando a 60 veces la velocidad de las investigaciones manuales,[1] se basa en fuentes estructuradas y no estructuradas para proporcionar contexto y alcance al ataque.

La solución también se puede integrar con IBM Security Identity Governance and Intelligence para revocar automáticamente el acceso del usuario cuando se detecta actividad de alto riesgo. Y se puede integrar con IBM i2® Analyze para permitir que los equipos de seguridad mapeen visualmente los datos relevantes para un incidente y compartan fácilmente el análisis con los miembros del equipo.

Haga clic en la imagen para ampliar. Haga clic nuevamente para ver en tamaño original.



IBM QRadar User Behavior Analytics

IBM QRadar Advisor con Watson

- Lea más sobre cómo IBM QRadar ayuda a las organizaciones a detectar e investigar amenazas internas.
- Descargue la aplicación QRadar User Behavior Analytics de IBM Security App Exchange.
- Descargue una prueba gratuita de 30 días de QRadar Advisor con Watson.

1 Resultados observados por clientes que participaron en el programa de prueba beta de QRadar Advisor con Watson.

Para obtener más información

Para obtener más información sobre QRadar, comuníquese con su representante de IBM o Business Partner de IBM, o visite: **ibm.com**/security/qradar/

Acerca de las soluciones de IBM Security

IBM Security ofrece uno de los portafolios de productos y servicios de seguridad empresarial más avanzados e integrados. El portafolio, respaldado por la investigación y el desarrollo X-Force de renombre mundial, proporciona inteligencia de seguridad para ayudar a las organizaciones a proteger de manera integral a sus personas, infraestructuras, datos y aplicaciones, ofreciendo soluciones para la gestión de identidad y acceso, seguridad de bases de datos, desarrollo de aplicaciones, gestión de riesgos, gestión de terminales, seguridad de red y más. Estas soluciones permiten que las organizaciones gestionen el riesgo de manera efectiva e implementen una seguridad integrada para dispositivos móviles, nubes, redes sociales y otras arquitecturas de negocios empresariales. IBM opera una de las organizaciones de investigación, desarrollo y entrega de seguridad más amplias del mundo, monitorea 15 mil millones de eventos de seguridad por día en más de 130 países y posee más de 3.000 patentes de seguridad.

Además, IBM Global Financing ofrece diversas formas de pago para ayudarle a adquirir la tecnología que necesita para hacer crecer su empresa. Proporcionamos una gestión de todo el ciclo de vida de los productos y servicios de TI, desde su adquisición hasta su eliminación. Para obtener más información, visite: **ibm.com**/financing

IBM Security
New Orchard Road
Armonk, NY 10504

Producido en Estados Unidos
Septiembre de 2017

WGW03340-USEN-00