X-Force

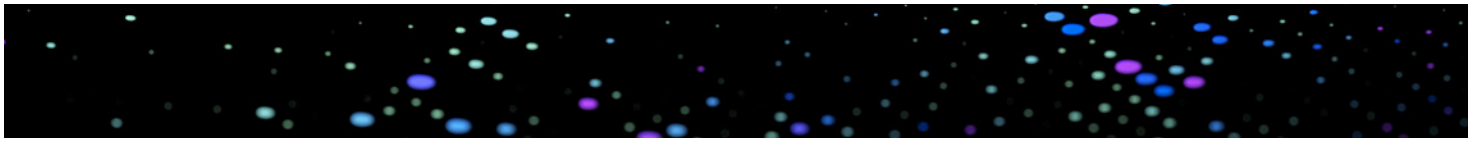
Informe IBM Security X-Force sobre amenazas internas, 2021

IBM Security X-Force Threat Intelligence

Informe de inteligencia especial T2 2021

IBM

Índice



Introducción

El panorama de las ciberamenazas se halla en evolución constante, ya que tanto quienes atacan como quienes se defienden no dejan de innovar en cuanto a tecnologías y procesos. Las empresas, en conjunto, gastan cerca de 60 000 millones de dólares al año para defender sus activos y contratar a personal que evite los ataques y reaccione a ellos, con un aumento del gasto en seguridad de otro 10 % en 2021.[1]

Mientras que, en gran medida, la atención y el gasto en seguridad de las empresas se centran en frustrar los ataques que proceden del exterior de la compañía, a menudo se pasan por alto las amenazas internas, aquellas que proceden del interior de la empresa. Las amenazas internas, muchas de las cuales resultan ser accidentales o no maliciosas, pueden causar daños inmensos en forma de robo de datos, pérdidas económicas, robo de propiedad intelectual y daño a la reputación. En una encuesta realizada en 2020, Ponemon Institute estimó que las empresas gastan de media 644 852 dólares para recuperarse de un caso de amenaza interna, con independencia de su origen.[2] Esto incluye el coste de controlar e investigar los eventos internos sospechosos y la respuesta al incidente, la contención, la erradicación y la mitigación de la incidencia interna.

En el contexto de este documento, IBM Security X-Force define «interno» como:

— Usuario interno accidental: empleado o proveedor/contratista externo negligente.[3]

— Usuario interno malicioso: delincuente, o bien empleado o proveedor/contratista externo que actúa con malas intenciones.

1. https://www.infosecurity-magazine.com/news/global-cybersecurity-spending-to/
2. https://securityintelligence.com/posts/gaining-insight-into-the-ponemon-institutes-2020-cost-of-insider-threats-report/
3. El usuario interno negligente se define como aquel que, por accidente, causa un incidente que afecta a la confidencialidad, integridad o disponibilidad de los datos o sistemas dentro de una empresa. Esto no incluye los incidentes de phishing/ingeniería social.

Usando datos protegidos por derechos de propiedad exclusivos recopilados mediante el estudio de reacciones a incidentes reales, X-Force analizó supuestos casos de amenazas internas —tanto accidentales como maliciosas— que afectaron a empresas entre 2018 y 2020. Unido a informes de código abierto sobre los ataques de amenazas internas más destacadas, este documento examinará descubrimientos críticos obtenidos con dichos datos, como:

— Cómo se descubren la mayoría de los ataques internos.

— El papel que el nivel de acceso desempeña en los ataques internos.

— Prácticas recomendables para mitigar las amenazas internas.

Hallazgos clave de la investigación

El 40 % de los incidentes se detectaron a través de alertas generadas por una herramienta de control interno.

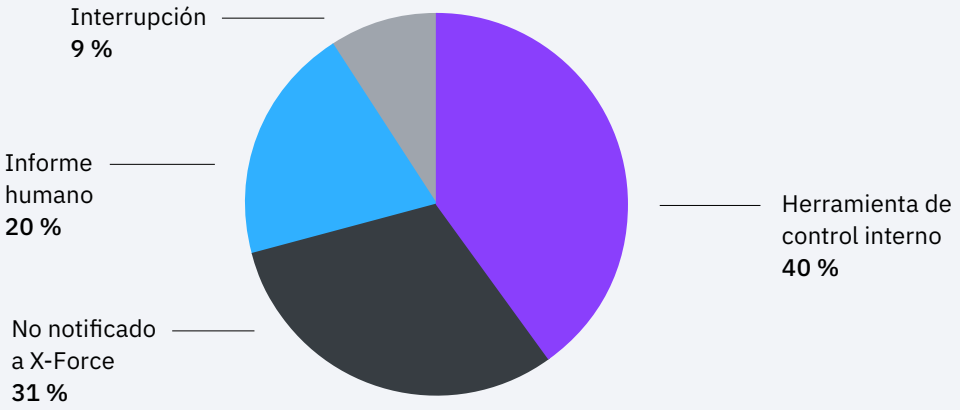
En el 40 % de los incidentes se vio implicado un empleado con acceso privilegiado a los activos de la empresa.

En el 100 % de los incidentes en los que el usuario interno contaba con acceso administrativo confirmado o probable, este acceso elevado desempeñó un papel en el propio incidente.

Cómo se descubren los ataques de amenazas internas

Las amenazas internas suelen definirse como ataques en los que usuarios legítimos que poseen cierto nivel de acceso a los activos de la empresa aprovechan dicho acceso, ya sea accidental o intencionadamente, y acaban causando un daño a la organización. Estas amenazas pueden proceder de un empleado actual o antiguo, o bien de un contratista o proveedor externo que disponga de acceso para ejercer una función empresarial determinada.

Cómo se descubrió el ataque interno



Un análisis de las amenazas internas al que X-Force lleva respondiendo desde 2018 revela que el 40 % de estos incidentes fueron detectados a través de alertas generadas mediante una herramienta de control interno. Los informes humanos —por ejemplo, por parte de empleados que alertan a la empresa de una actividad anómala— supusieron el 20 % de las detecciones, mientras que una interrupción en el sistema alertó a los equipos de seguridad en el 9 % de los casos.

En el 2020 Cost of Insider Threats: Global Report de Ponemon Institute, patrocinado por ObserveIT e IBM, se estimó que herramientas como User Behavior Analytics (UBA), Privileged Access Management (PAM), la gestión de eventos e información de seguridad (SIEM) y los programas de intercambio de información sobre amenazas y de formación y concienciación de los usuarios ahorraron a las empresas una media de 3 millones de dólares al reducir o eliminar los riesgos internos.[4]

Ahorro de 3 millones de USD en costes

Se estima que herramientas como UBA o PAM, SIEM y los programas de uso compartido de inteligencia de amenazas y de formación y concienciación ahorraron de media a las empresas 3 millones de dólares al reducir o eliminar los riesgos internos.[4]

4. https://securityintelligence.com/posts/gaining-insight-into-the-ponemon-institutes-2020-cost-of-insider-threats-report/

Falta de pruebas e incógnitas en el estudio de X-Force

Con respecto a los incidentes internos cuyo método de detección fue «no notificado a X-Force» o «falta de pruebas», los equipos de respuesta a incidentes de X-Force no recibieron información suficiente para llegar a determinar cómo se descubrieron. Esto suele deberse a que numerosas empresas carecen de visibilidad de las características y el funcionamiento de su entorno base. Para poder detectar actividades anómalas dentro de cualquier sistema, resulta crucial entender cómo es la actividad normal, para que las anomalías puedan detectarse de forma fácil y con seguridad. En 2019, IBM patrocinó un informe SANS[5] que examinaba el panorama de las amenazas avanzadas a empresas. El estudio demostró que:

— El 48 % de las empresas consideraban que la falta de visibilidad de su infraestructura era la mayor laguna de seguridad.

— El 35 % sentían que carecían de la capacidad necesaria para detectar usos indebidos por parte de usuarios internos de la empresa.

— El 47 % de las organizaciones admitieron carecer de la capacidad necesaria para entender cómo era la actividad básica normal en sus redes.

5. https://www.ibm.com/account/reg/us-en/signup?formid=urx-39989

Acceso privilegiado frente a acceso administrativo

Al analizar los casos de amenazas internas, X-Force clasificó dos tipos de usuarios distintos.

Un **usuario privilegiado** es un miembro de la organización que cuenta con acceso a datos confidenciales. Estos datos pueden ser propiedad intelectual, datos de clientes o información de recursos humanos. Estos usuarios también pueden tener acceso a información empresarial confidencial, como datos sobre fusiones y adquisiciones u otra información legal.

Los usuarios con **acceso administrativo**, también llamados «administradores», se definen como personas con un nivel de acceso elevado a sistemas de TI dentro de la red. En teoría, estos tipos de accesos no deberían solaparse. Sin embargo, X-Force descubrió que es frecuente que los usuarios finales estén sobreaprovisionados en sus entornos de TI.

Los usuarios internos con acceso administrativo son distintos de aquellos con acceso confidencial a un entorno corporativo. En estos últimos se incluyen empleados y contratistas/proveedores con acceso al entorno de TI de la organización, los cuales representan un singular riesgo para la empresa por su elevado nivel de privilegios de red.

Ejemplos de puestos con acceso privilegiado

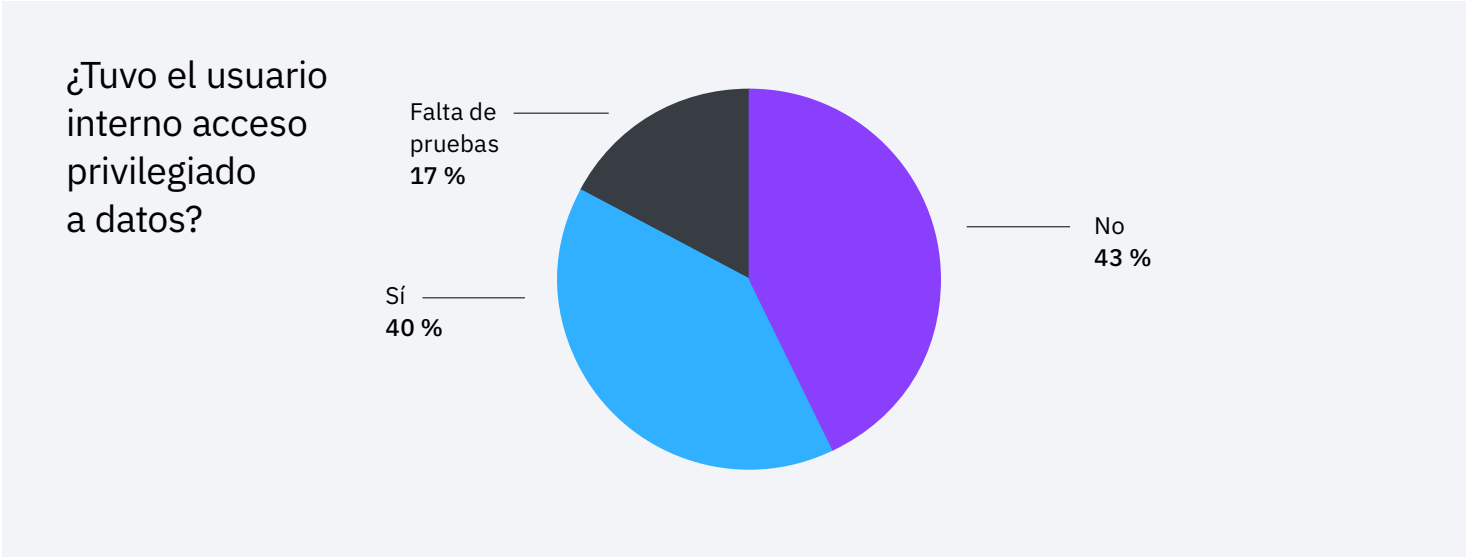
- Puestos de RR. HH.
- Directivos superiores
- Puestos en finanzas
- Puestos del departamento jurídico
- Puestos de investigación
- Otros puestos con acceso a la propiedad intelectual, a las «joyas de la corona» o a datos de los clientes de la empresa

Ejemplos de puestos con acceso administrativo

- Administradores de servidores
- Administradores de TI
- Miembros de servicios de asistencia técnica
- Proveedores de TI externos
- Otros puestos que puedan modificar configuraciones de los sistemas de TI

¿Quién vigila a los vigilantes?

¿Los usuarios internos que causan incidentes suelen tener acceso privilegiado? La respuesta breve es que sí.



El análisis de los datos de X-Force demuestra que en el 40 % de los incidentes causados por usuarios internos estaba implicado un empleado con acceso privilegiado a los activos confidenciales de la empresa. Para este estudio, X-Force clasificó el acceso privilegiado como el de aquellos que trabajan en áreas como departamentos de TI, recursos humanos, seguridad o puestos ejecutivos.

En otro 17 % de los datos, no estaba claro si el usuario interno tenía o no acceso privilegiado a datos confidenciales, lo cual significa que el número de incidentes causados por un acceso privilegiado podría ser considerablemente mayor.

Las personas con un nivel de acceso elevado a activos críticos, como recursos compartidos en la red, dispositivos de seguridad, sistemas de correo electrónico, información que permite identificar a empleados o clientes, propiedad intelectual o datos financieros, pueden suponer un riesgo notablemente más alto que aquellas con privilegios más limitados.

Por tanto, resulta lógico que los incidentes causados accidentalmente por usuarios internos con acceso privilegiado acaben costando a las empresas más que aquellos causados accidentalmente por usuarios internos con un grado de acceso menor. Los incidentes en los que participan usuarios internos maliciosos con alto grado de acceso privilegiado pueden acarrear un coste mayor y los ataques en los que participan estos usuarios pueden llegar a suponer una vulneración de datos a gran escala. Por ejemplo, en 2018, un agente inmobiliario australiano que trabajaba en una importante agencia local fue declarado culpable de acceder a bases de datos confidenciales antes de marcharse de la empresa. El agente manipuló el estado de posibles ventas en el sistema rebajando el interés de los clientes potenciales. Además, el agente admitió haberse llevado 200 expedientes de clientes para ofrecerles los servicios de la nueva agencia. Se calcula que este ataque interno le costó a la agencia afectada 30 millones de dólares en posibles ventas de inmuebles.[6]

Uno de los mejores métodos para evitar incidentes internos relacionados con el nivel de acceso es ceñirse a los principios del privilegio mínimo y asegurarse de que los usuarios cuentan con el nivel de acceso mínimo necesario para desempeñar sus labores para la empresa. Esto puede materializarse como una solución de gestión de acceso privilegiado (PAM) construida en torno a un modelo zero-trust.[7,8] En este modelo, el objetivo es que todo aquel que disponga de una cuenta de usuario cuente con el nivel de privilegios mínimo posible, lo cual reduce las oportunidades de que un usuario interno obtenga acceso no deseado a datos o activos. Este concepto se vuelve aún más crítico en el cloud, donde residen más datos y los solicitantes —tanto humanos como no humanos— deben acceder a ellos para operar.

El 2020 Cost of Insider Threats: Global Report reveló que solo el 39 % de las empresas han adoptado alguna forma de gestión de acceso privilegiado.[9] Asimismo, demuestra que la adopción de una PAM ha dado como resultado ahorros de 3,1 millones de dólares, lo cual pone de manifiesto la eficacia de estas medidas.

39 %

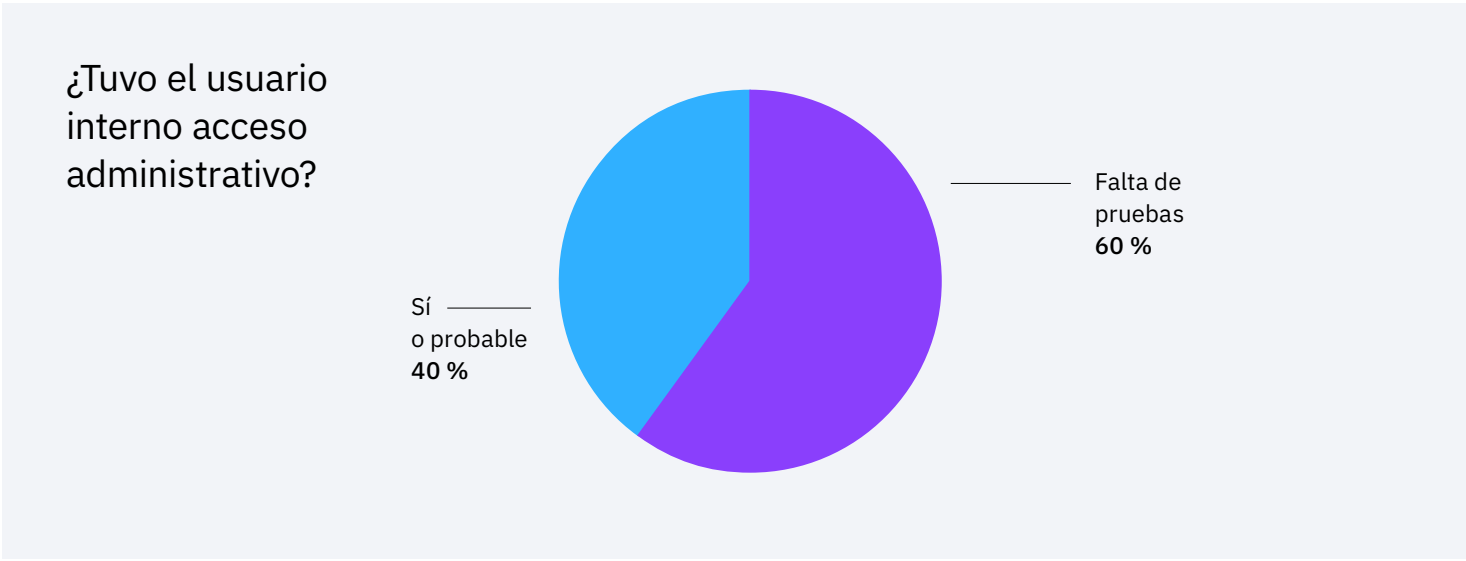
El 39 % de las empresas ha adoptado alguna forma de PAM.[9] Esto ha supuesto un ahorro de 3,1 millones de dólares.

6. https://indaily.com.au/news/2018/10/23/harris-director-resigns-from-top-real-estate-post/
7. https://www.ibm.com/security/identity-access-management/privileged-access-management
8. https://www.ibm.com/security/zero-trust
9. https://www.ibm.com/security/digital-assets/services/cost-of-insider-threats/

El acceso administrativo abusivo es un problema costoso

En numerosas ocasiones, se han producido casos públicos de usuarios internos que han abusado de su poder como administradores de una organización con fines ilícitos, incluidos la venganza, el beneficio económico u otras intenciones perversas. En febrero de 2020, Volodymyr Kvashuk, antiguo ingeniero de Microsoft, fue declarado culpable de usar su acceso privilegiado para robar más de 10 millones de dólares en activos digitales de la compañía.[10] El robo fue posible porque Kvashuk disponía de acceso administrativo a la plataforma de ventas minoristas de cuya gestión era responsable.[11] Concretamente, Kvashuk usó las direcciones de correo electrónico de sus compañeros y cuentas de prueba válidas en el sistema para ocultar su actividad y, por ejemplo, exfiltrar tarjetas de regalo digitales. El ingeniero robó estos y otros activos para luego revenderlos en internet y obtener un beneficio personal con el que, más tarde, se compró una vivienda de 1,6 millones de dólares y un vehículo Tesla de 160 000 dólares.[12]

Las cifras del acceso administrativo abusivo

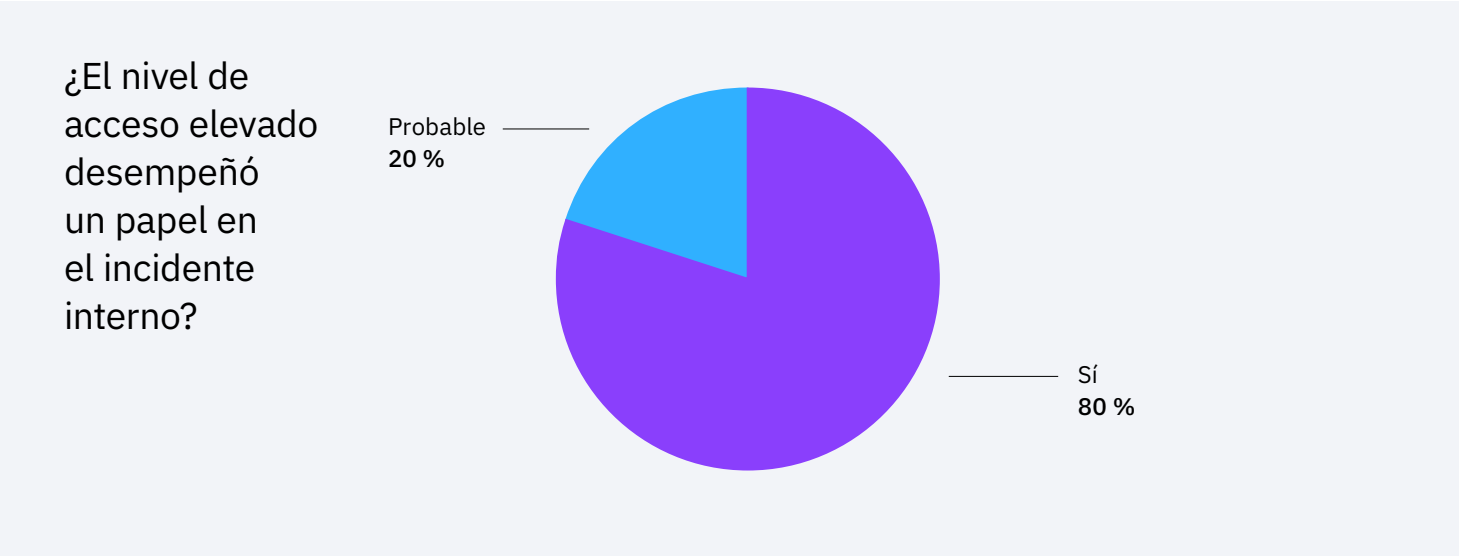


En el 40 % de los incidentes a los que X-Force respondió entre 2018 y 2020, el usuario interno contaba con acceso administrativo confirmado o probable a la red. Cuando el cliente no facilitó el puesto específico del usuario, los analistas de X-Force determinaron el tipo de acceso interno basándose en los detalles del incidente.

10. https://www.justice.gov/usao-wdwa/pr/former-microsoft-software-engineer-sentenced-nine-years-prison-stealing-more-10-million
11. https://apnews.com/article/seattle-retail-sales-james-robart-13f5a86053533b40034246ef37ecad8d
12. https://www.redmond-reporter.com/news/former-microsoft-employee-convicted-of-18-federal-felonies/

Estos incidentes incluían exfiltración de datos, exposición y borrado de datos confidenciales e instalación de software no autorizado, entre otros. Concretamente, algunas organizaciones perdieron petabytes de registros borrados de los servidores, sufrieron filtraciones de código fuente intencionadas o afrontaron costosas interrupciones por culpa de un usuario interno con acceso administrativo.

Y lo que es más interesante: en el 100 % de los incidentes en los que el usuario interno contaba con acceso administrativo confirmado o probable, este acceso elevado desempeñó una función en el propio incidente. (Véase el gráfico a continuación)



Para explicar este punto de distinta manera, si el usuario interno no hubiera contado con acceso administrativo, es probable que el incidente hubiera tenido un impacto mucho menor en la organización o, en muchos casos, no se hubiera producido en absoluto. X-Force ha respondido a varios incidentes internos en los que se habían borrado de los servidores bases de datos y registros críticos. Si el usuario interno no hubiera tenido acceso a esos sistemas, el evento no habría tenido lugar.

Recomendaciones

X-Force considera que la cantidad de incidentes internos está poco representada en los datos de terceros. Es probable que haya muchos más incidentes de este tipo gestionados internamente por las organizaciones y que no se hagan públicos por miedo a las responsabilidades o al daño que puedan conllevar para la imagen de la empresa.[13]

La investigación y los datos de X-Force ponen de manifiesto la necesidad de que las posibles amenazas internas sean un componente primordial de los programas de seguridad de la información, teniendo en cuenta el impacto que estos incidentes pueden tener en una empresa. En concreto, IBM Security recomienda lo siguiente con respecto a las amenazas internas:

Las estrategias de defensa en profundidad funcionan bien para detectar amenazas internas.

Tradicionalmente, se cree que un enfoque multicapa de las tecnologías y los procesos implantado por las empresas sirve para atajar las amenazas externas. Sin embargo, el estudio de X-Force indica que muchas de estas herramientas, incluidas las soluciones de gestión de eventos e información de seguridad (SIEM), también resultaron cruciales a la hora de detectar amenazas internas.

Entender lo que es normal en su entorno.

La mejor forma de detectar actividad sospechosa por parte de cualquier tipo de atacante es comprender qué tipo de actividad se considera normal dentro de su red. Llegar a entender perfectamente la actividad básica facilita la detección de comportamientos anómalos y una reacción ágil y eficaz a los mismos. Una solución robusta de análisis de comportamiento del usuario (UBA) puede ofrecer esta funcionalidad e ir adaptándose a los cambios de su entorno a lo largo del tiempo.

Revisar el acceso administrativo regularmente.

X-Force descubrió que varios incidentes internos que implicaban a administradores se debieron, probablemente, a la existencia de usuarios con demasiados privilegios. Deben aplicarse cambios y controles de proceso rigurosos en torno al acceso administrativo, sobre todo en servidores críticos. Plantéese soluciones tecnológicas que generen un registro y conceda acceso administrativo temporal a sistemas y funciones confidenciales.

13. https://www.darkreading.com/edge/theedge/fbi-encounters-reporting-an-insider-security-incident-to-the-feds-/b/d-id/1340016

Separar a los equipos administrativos de TI y seguridad de la información.

La experiencia de X-Force ha demostrado que un enfoque equilibrado de la gestión de la independencia y el control de los equipos de seguridad y administrativos ayuda a mejorar la seguridad. Esto también permite a los equipos administrativos tener la flexibilidad y creatividad necesarias para optimizar su exploración y descubrimiento de las amenazas al tiempo que ofrecen a la empresa una supervisión y un control suficientes para minimizar los riesgos dentro del equipo.

Crear perfiles de riesgo para puestos de empresa delicados.

Puesto que en numerosos incidentes internos a los que respondió X-Force estuvo implicado un nivel de acceso elevado, recomendamos a las organizaciones que se planteen crear perfiles de riesgo para los puestos que dispongan de acceso confidencial o administrativo a sistemas o datos. La implantación de una solución de gestión de acceso privilegiado (PAM) en torno a un modelo zero-trust crea accesos de privilegio mínimo para los usuarios y podría reducir el impacto de los incidentes internos.

Actualizar los informes de estrategias de respuesta a incidentes para incluir amenazas internas.

En estos incidentes, la formación general no es suficiente. Pese a que la mayoría de los informes de estrategias de respuesta a incidentes tienen en cuenta los ataques de adversarios externos, las empresas deberían plantearse añadir situaciones para incluir escenarios de amenazas internas maliciosas o accidentales. Piense en un colaborador que pueda ayudarlo a desarrollar planes de respuesta a incidentes e informes de estrategias específicos para estos ataques para estar mejor preparado y poder reaccionar ante los ciberataques.

Seguir formando a los empleados.

En los programas de formación anuales de numerosas empresas se incluyen prácticas empresariales éticas, además de formación en ingeniería social. Muchas de los incidentes internos a los que respondió X-Force fueron descubiertos por otros empleados y no mediante la tecnología. En las iniciativas de formación anuales sobre ética empresarial o ingeniería social, las organizaciones deberían incluir cómo informar de un supuesto incidente interno. Asimismo, un curso específico para cada puesto dirigido a empleados con acceso privilegiado puede ayudarlos a detectar señales que delaten la existencia de algún problema.

Aprovechar servicios de inteligencia sobre amenazas de confianza.

A menudo, los clientes se ven en la complicada tesitura de crear, gestionar y poner en funcionamiento inteligencia sobre amenazas. Busquen una solución que ofrezca la agregación, automatización e integración necesarias para poner en funcionamiento la inteligencia sobre amenazas a escala.

Los servicios de detección y respuesta gestionadas ofrecen protección las 24 horas.

Los servicios de seguridad de detección y respuesta gestionadas (MDR) son esenciales para prevenir, detectar y reaccionar rápidamente a las amenazas internas. Las soluciones que van más allá de la prevención tradicional usando antivirus de nueva generación para el bloqueo basado en comportamientos, las investigaciones y la gestión continua de las políticas resultan cruciales.

Averigüe cómo IBM Security ayuda a sus clientes a proteger los entornos más complejos y críticos frente a amenazas externas e internas.

Más información sobre IBM Security

IBM Security

IBM España, S.A.
Tel.: +34-91-397-6611
Santa Hortensia, 26-28
28002 Madrid
Spain

Producido en los Estados Unidos de América.
Mayo de 2021

IBM