Informe sobre Investigaciones de Violaciones de la Información de 2016

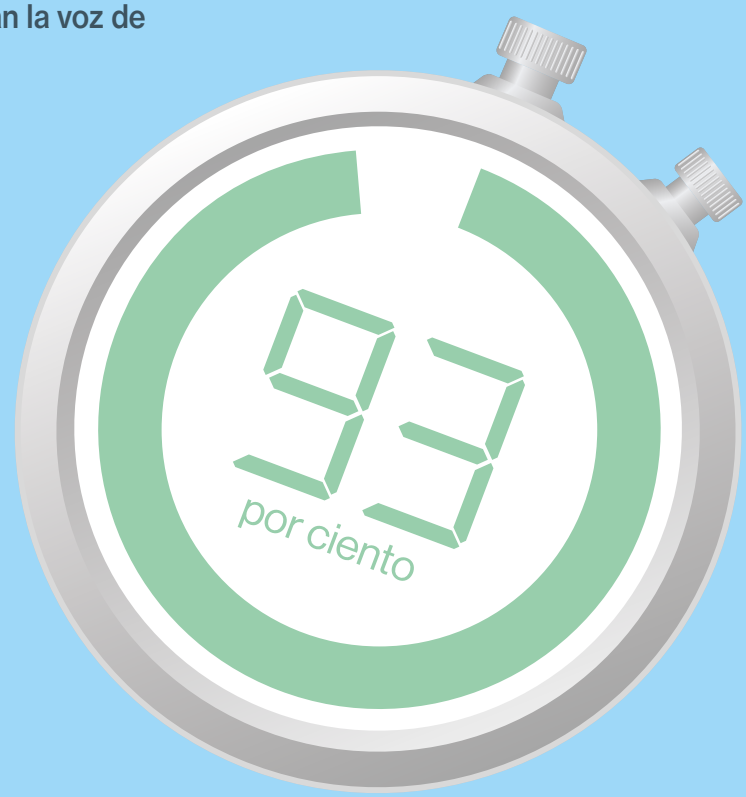
Resumen ejecutivo

La ciberseguridad no compete únicamente a los expertos en la materia. Lea la siguiente guía para altos directivos y obtenga toda la información que debe conocer.

verizon

¿Ya han puesto en peligro su seguridad?

En el 93% de los casos, penetrar en un sistema es cuestión de minutos o incluso segundos. Sin embargo, las organizaciones tardan semanas o incluso meses en descubrir el mero hecho de que se ha producido una filtración y por lo general son los clientes o las fuerzas de seguridad, y no sus propias medidas de seguridad, las que dan la voz de alerta.



+100.000 incidentes. Análisis de 2.260 filtraciones. 82 países. 67 organizaciones colaboradoras.

El Informe sobre Investigaciones de Violaciones de la Información (DBIR) es considerado una fuente de información inigualable por los expertos en seguridad y nuestra novena edición es la más exhaustiva de todas las publicadas. Sin embargo, si trabaja como director informático, director de marketing o consejero delegado de una empresa, también es responsable de conocer los riesgos que afectan a esta, y esta guía ha sido concebida específicamente para usted.

La seguridad debería ser una medida previa, no una solución posterior

Los datos –el potente motor que impulsa la innovación– están acelerando las cadenas de suministro y redefiniendo las experiencias de los clientes. Sin embargo, la seguridad es una de las principales preocupaciones tanto para las empresas como para los consumidores, razón por la cual es fundamental que aborde los riesgos existentes con el fin de infundir confianza en sus clientes y, al mismo tiempo, subirse a la ola de la aceleración digital.

Todas las organizaciones dependen en cierta medida de sistemas digitales, ya sea para comunicarse, operar o competir con sus rivales y, hoy por hoy, obtener una ventaja competitiva radica en ser mejor que los competidores en el ámbito digital. Sin embargo, para alcanzar esta meta nuestros sistemas deben ser fiables y seguros y ello exige que todos nos preocupemos por la seguridad de los datos.

Las filtraciones de datos no solo resultan caras por las indemnizaciones y las sanciones que conllevan, sino por los elevados costes de los servicios jurídicos y de recuperación. Las filtraciones también pueden resultar costosas para la reputación de las marcas, un aspecto especialmente relevante en una coyuntura en la que la confianza de los clientes y socios es más importante que nunca.

Aunque lo normal es que una filtración de datos no hunda una empresa inmediatamente, lo cierto es que puede afectar gravemente a su evolución futura.

Imagine que fuese propietario de una tienda de bricolaje. Aunque los clientes podrían seguir acudiendo a su punto de venta, donde posiblemente pagarían en efectivo, podrían también descargar su nueva aplicación o adquirir su nueva solución doméstica conectada.

El objetivo de la mayoría de filtraciones es el dinero

Olvídese de todo lo que ha visto en las películas de Hollywood. La mayoría de los ciberataques son indiscriminados y su móvil es la avaricia y no la venganza ni el bien público. La mayoría de ciberatacantes tratan de sustraer datos por su valor y no por la persona a la que pertenecen. Cualquier cosa que pueda convertirse en dinero es susceptible de atraer su atención y, a medida que el valor de la información de las tarjetas de pago se reduce gracias a que los bancos mejoran sus sistemas de detección de fraude, es posible que los atacantes comiencen a centrarse en ámbitos como la propiedad intelectual o la información sanitaria protegida.

Los atacantes siguen el camino más fácil

Sería un error pensar que el mayor riesgo al que se enfrenta tiene que ver con vulnerabilidades nuevas. La mayoría de atacantes explotan vulnerabilidades conocidas para las cuales no existe una solución desde hace meses, sino años.

El 63% de las filtraciones de datos confirmadas se asocia con el aprovechamiento de contraseñas débiles, predeterminadas o robadas.

Con frecuencia, la razón por la cual los delincuentes fueron capaces de penetrar en el sistema rápidamente es que ya disponían de las claves. De hecho, la denominada "ingeniería social" sigue teniendo una eficacia preocupante (¿quién no ha recibido en alguna ocasión un correo diciendo "haga clic aquí para restablecer la contraseña de su cuenta bancaria online"?). Verizon ha detectado que casi un tercio (el 30%) de los mensajes de *phishing* se abrieron, lo cual supone un incremento con respecto al 23% registrado en 2014. Además, el 12% de los objetivos –porcentaje próximo al registrado en 2014 (11%)– fueron más allá y abrieron los documentos adjuntos maliciosos o hicieron clic en el correspondiente enlace.

Complíqueles la vida

Aunque por desgracia no existen sistemas impenetrables, con frecuencia una batería de medidas de defensa medianamente decente disuadirá a un gran número de ciberdelincuentes, que al toparse con ella se irán a buscar un objetivo más fácil. Sin embargo, muchas organizaciones no poseen siquiera esta modesta aspiración.

El 95% de las filtraciones pueden clasificarse en nueve categorías.

Este año, el DBIR vuelve a centrarse en los nuevos patrones de incidente que identificamos en 2014. Conocerlos le ayudará a concentrar sus iniciativas de seguridad en los ámbitos adecuados.

Destine sus recursos de una forma más inteligente

Los *hackers* nunca dejan de mejorar y sus infraestructuras evolucionan más rápido que nunca. ¿Cómo puede entonces mantenerse protegido sin arruinarse?

Cada día que pasa, las organizaciones se ven más obligadas a adoptar sistemas y tecnologías digitales y la cantidad de dispositivos que proteger, las personas con acceso a datos y el número de socios que es necesario integrar crecen incesantemente.

Las nuevas tecnologías –como los dispositivos móviles o el Internet de las Cosas (IoT)– amenazan con ofrecer nuevas oportunidades a los atacantes.

Aunque aún no hemos apreciado un volumen significativo de incidentes que afecten a estos dos segmentos, no nos cabe la menor duda de que se trata de una amenaza real. Las vulneraciones "prueba de concepto" ya han sido demostradas y que veamos una infiltración a gran escala es solo una cuestión de tiempo.

Nueve categorías describen + 80%

Filtraciones
Incidentes

Cambio de visualización

Los *hackers* están viéndose obligados a modificar sus estrategias debido a que el valor de mercado de determinados tipos de datos está reduciéndose, en especial el de la información de tarjetas de pago. Para mantener su volumen de ingresos, los atacantes deben sustraer más datos o encontrar nuevas fuentes de información cuya venta resulte más lucrativa, como la información sanitaria protegida o la propiedad intelectual.

Por ello, debe golpearles donde más les duele: en sus bolsillos. Desafortunadamente, no cuenta con un presupuesto ilimitado, lo cual le obliga a destinar sus recursos de una forma más inteligente. Las nueve categorías de clasificación de incidentes que publicamos por primera vez en 2014 abordan la inmensa mayoría de incidentes y filtraciones confirmadas, tal y como muestra la Figura 1. Además, si nos fijamos en cada sector por separado, la mayoría de amenazas se encuadran en tan solo tres categorías (consulte la Figura 2). Analizar estas categorías le ayudará a entender cuál es la mejor forma de destinar sus limitados recursos económicos y personales para obtener los mejores resultados.

El 95% de las filtraciones y el 86% de los incidentes pueden englobarse en tan solo nueve categorías.

Figura 1: incidentes/filtraciones por categorías de clasificación, todos los sectores

En la mayoría de sectores, tres cuartos de los incidentes y las filtraciones se encuadran en tan solo tres categorías.

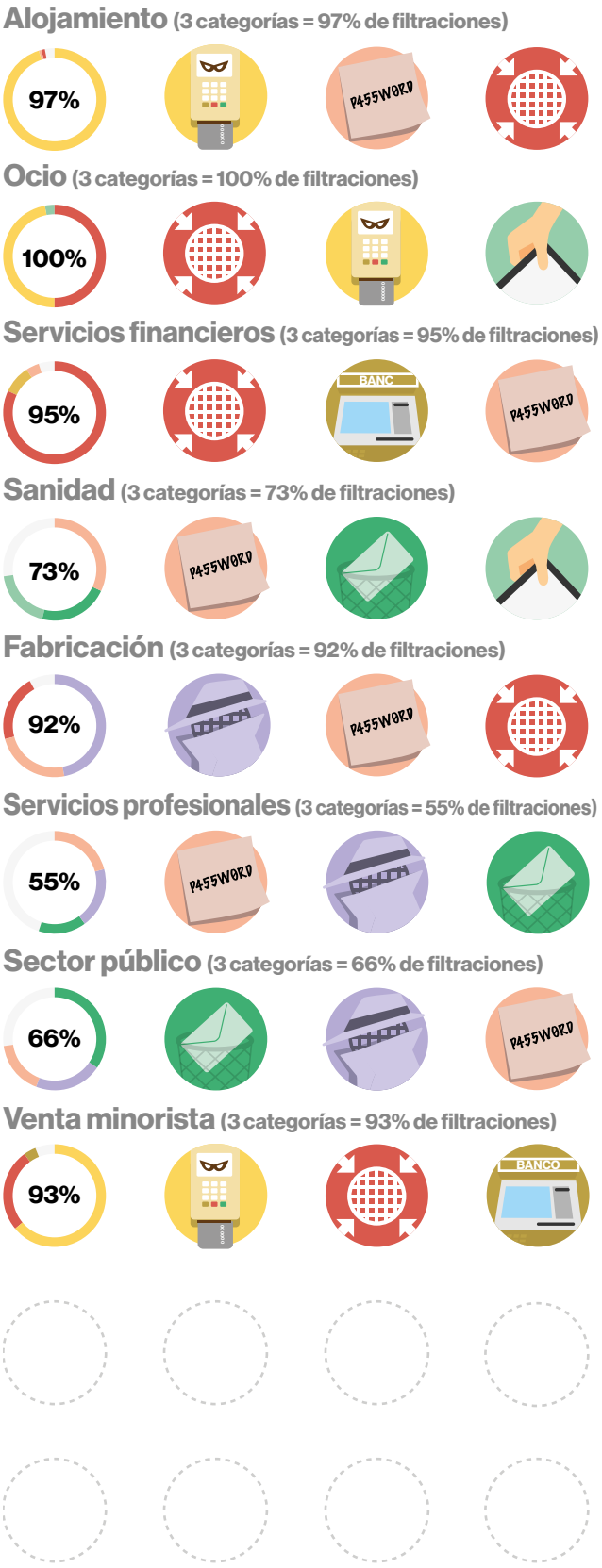


Figura 2: tres principales incidentes/filtraciones por sector

Errores varios

Cualquier acción o error no intencionado que pone en riesgo la seguridad, sin incluir la pérdida de activos.

Sectores más sensibles:
sector público, sanidad e información

El 40% de los incidentes que se producen dentro de esta categoría tienen que ver con limitaciones de capacidad de los servidores que colapsan las aplicaciones clave cuando se producen picos no maliciosos en el tráfico web. Sin embargo, con frecuencia el desencadenante del incidente es un simple error cometido por uno de sus empleados.

El 26% de los errores varios implicó el envío de información confidencial a la persona errónea.

¿Qué puede hacer al respecto?

- **Aprenda de sus errores:** elabore un registro de los errores comunes que se hayan producido en el pasado. Puede utilizar dichos registros para mejorar la formación de sensibilización sobre seguridad y medir la eficacia de sus controles.
- **Refuerce los controles:** valore la posibilidad de utilizar software de prevención de pérdidas (DLP), el cual puede restringir el intercambio de información confidencial fuera de la empresa.
- **Implante procedimientos de eliminación exhaustivos:** asegúrese de eliminar cualquier dato confidencial de sus activos antes de venderlos. Por evidente que parezca, hemos sido testigos de multitud de ejemplos en los que no se ha seguido esta buena práctica.

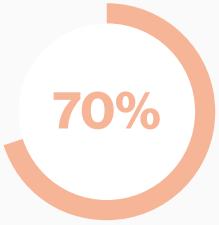
Uso indebido de privilegios por parte de usuarios internos

Aunque esta categoría está integrada principalmente por incidentes que implican usos indebidos por parte de usuarios internos, también contempla la concesión de accesos privilegiados a usuarios externos (confabulados con los primeros) y socios.

Sectores más sensibles:
sanidad, sector público y personal administrativo

Al contrario de lo que mucha gente piensa, es infrecuente que los administradores de sistemas o los desarrolladores con un nivel de privilegios elevado sean víctimas de los ataques que conforman esta categoría. De hecho, los usuarios finales representan un tercio de los usos indebidos por parte de usuarios internos. El móvil de los ataques suele ser el dinero: el 34% de las filtraciones que implican usos indebidos responden a motivaciones económicas, aunque un cuarto de ellas (el 25%) puede estar relacionado con actividades de espionaje, por ejemplo, sustracciones de propiedad intelectual.

El 70% de las filtraciones que implican un uso indebido por parte de usuarios internos no son detectadas hasta pasados meses o incluso años.



¿Qué puede hacer al respecto?

- **Conozca sus datos:** debe conocer los datos confidenciales que posee, dónde se encuentran y quién dispone de acceso a los mismos. Sus sistemas de administración deben garantizar que el acceso se limita a aquellos individuos que realmente los necesitan y que los accesos reales se verifican a partir de la lista de individuos autorizados.
- **Supervise el comportamiento de los usuarios:** realice un seguimiento del uso de los sistemas –especialmente de los accesos a datos que puedan utilizarse para obtener beneficios económicos– y revoque inmediatamente los privilegios de aquellos empleados que abandonen la organización.
- **Realice un seguimiento del uso de dispositivos USB:** evite encontrarse en la situación de descubrir que uno de sus empleados ha sustraído datos antes de marcharse de la empresa.

Sustracciones y pérdidas físicas

Pérdida o sustracción de portátiles, dispositivos USB, documentos impresos y otros activos de datos.

Sectores más sensibles:
sanidad y sector público

No es extraño encontrarse con casos en los que la pérdida de un portátil o dispositivo móvil por parte de un empleado desencadena un incidente de seguridad. Sin embargo, las mayores amenazas de filtración de datos tienen que ver con la pérdida o sustracción de documentos, ya que estos no pueden cifrarse.

El 39% de las sustracciones suceden desde las zonas de trabajo de la propia víctima y el 34% desde los dispositivos personales de los empleados.

¿Qué puede hacer al respecto?

- **Cifre sus datos:** si los dispositivos sustraídos están cifrados, será mucho más difícil que los atacantes accedan a los datos que contienen.
- **Forme a su personal:** es fundamental que desarrolle la sensibilización en materia de seguridad dentro de su organización. Colabore con su departamento de RR. HH. para incluir educación sobre seguridad física de los activos dentro de los programas de orientación y formación continua que imparte a sus empleados.
- **Reduzca el uso del papel:** aplique restricciones a la impresión de documentos. Establezca normas de clasificación de datos y cree una política empresarial que regule la impresión y transmisión de datos confidenciales.

Ataques de denegación de servicio (DoS)

Uso de *botnets* (ejércitos de ordenadores "zombis", normalmente utilizados sin permiso del propietario) para sobrecargar una organización con tráfico malicioso. Los ataques de denegación de servicio pueden interrumpir las operaciones y provocar el caos.

Sectores más sensibles:
ocio, ámbito profesional y educación

No subestime el impacto que un ataque de denegación de servicio puede tener en su organización. Según nuestros datos, constituyen la cuarta categoría más frecuente de incidentes de seguridad. De hecho, un ataque a gran escala podría forzar a su sitio web o sistemas de importancia crítica a permanecer fuera de línea durante semanas.

El tráfico mediano de un ataque de denegación de servicio es de 1,89 millones de paquetes por segundo, lo que equivale a más de 113 millones de personas intentando acceder a su servidor cada minuto.

1,89 Mpps

¿Qué puede hacer al respecto?

- **Segregue los servidores clave:** separe los sistemas principales para protegerlos frente a posibles ataques.
- **Elija a sus proveedores con precaución:** asegúrese de que sus proveedores de servicios en la nube cuentan con soluciones capaces de proteger la disponibilidad de sus servicios e infraestructura.
- **Compruebe el funcionamiento de su servicio de prevención de ataques de denegación de servicio:** no se limite a instalarlo y confiar en que funcionará correctamente. Asegúrese de que conoce en profundidad los acuerdos de nivel de servicio relativos a la mitigación de los ataques de denegación de servicio.

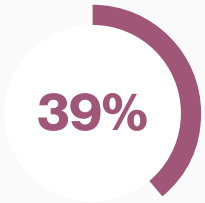
Crimeware

Esta clasificación incluye cualquier *malware* que no encaja en una categoría más específica. El *crimeware* a menudo afecta a los consumidores.

Sectores más sensibles:
sector público, fabricación e información

Los ataques suelen ser oportunistas y responder a motivaciones económicas. El *malware* penetra en su sistema cuando un individuo hace clic en un enlace incluido en un correo electrónico malicioso o visita un sitio web infectado. El uso de *ransomware* no deja de aumentar e implica el cifrado del contenido de un dispositivo por parte de un atacante hasta hacerlo inservible. Posteriormente, el atacante solicita el pago de un rescate para desbloquear los datos.

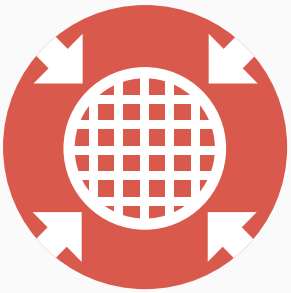
El 39% de los incidentes de *crimeware* en 2015 implicaron algún tipo de *ransomware*.



¿Qué puede hacer al respecto?

- **Aplique una reparación local tan pronto como resulte posible:** los ciberdelincuentes son expertos en explotar las vulnerabilidades conocidas; una reparación local aplicada a tiempo puede bloquear muchos ataques.
- **Monitorice los cambios en la configuración:** muchos métodos de ataque pueden detectarse fácilmente observando algunos indicadores clave.
- **Realice copias de seguridad de sus sistemas regularmente:** esta práctica le permitirá continuar su actividad empresarial en caso de que alguno de sus sistemas resulte infectado con *ransomware*.
- **Registre los datos relativos a los ataques:** examine los distintos tipos de *malware* que han afectado a sus sistemas y, si es posible, los puntos de acceso. Estos datos le ayudarán a priorizar los lugares en los que debe centrar sus esfuerzos.

Ataques a aplicaciones web

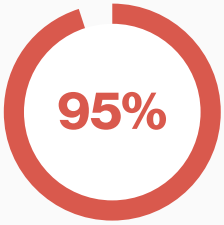


Ataques en los que se utilizó una aplicación web (como un sistema de gestión de contenidos, o CMS, o una plataforma de comercio electrónico) para acceder.

Sectores más sensibles:
servicios financieros, comercio minorista e información

Muchos de los ataques a aplicaciones web son indiscriminados: los atacantes descubrieron un objetivo débil cuya vulnerabilidad podían aprovechar o detectaron un punto de acceso a través de una campaña de *phishing*. Los ciberdelincuentes solían utilizar plugins para CMS para implantar fácilmente *software* malicioso. Una vez dentro del sistema, lograban invalidar el sitio web objetivo tras varios ataques. Sin embargo, descubrimos prácticamente 20.000 incidentes en los que los sitios web eran utilizados para acometer ataques distribuidos de denegación de servicio o se empleaban como plataforma de *phishing*.

El 95% de los ataques a aplicaciones web con sustracción de datos tenían motivaciones económicas.



¿Qué puede hacer al respecto?

- **Utilice la autenticación de doble factor:** bloquee las cuentas tras varios intentos de acceso fallidos. Además, es recomendable utilizar métodos de biometría.
- **Aplique una reparación local tan pronto como resulte posible:** adopte un proceso sólido para reparar localmente las plataformas CMS, incluidos los *plugins* de terceros, y los sistemas de comercio electrónico. Consulte la sección "Una reparación local eficaz puede detenerlos" en la página 10.
- **Supervise todos los puntos de entrada:** revise todos sus registros para identificar cualquier actividad maliciosa.

Intrusiones en el punto de venta

Ataques para penetrar en ordenadores y servidores que ejecutan aplicaciones de punto de venta con el objetivo de interceptar datos de pago.

Sectores más sensibles:
alojamiento y venta minorista

En 2015, saltaron a los medios de comunicación las filtraciones remotas de datos de tarjetas de pago desde los sistemas de varias cadenas hoteleras. En 2014, las víctimas fueron las grandes empresas de venta minorista. A menudo, las filtraciones se acometieron a través de un proveedor de punto de venta y no fueron resultado de una configuración deficiente en los dispositivos de punto de venta conectados a Internet.

El 95% de las filtraciones confirmadas en el sector de la hostelería implicó intrusiones en el punto de venta.

¿Qué puede hacer al respecto?

- **Aplique una reparación local en los servidores tan pronto como resulte posible:** únicamente permita el acceso a los individuos estrictamente necesarios.
- **Elija a sus proveedores con precaución:** asegúrese de que sus proveedores de servicios en la nube cuentan con soluciones capaces de proteger sus sistemas.
- **Reserve los sistemas de punto de venta para las actividades de punto de venta:** no permita que sus empleados utilicen los sistemas de punto de venta para navegar por Internet, consultar sus correos electrónicos o jugar a juegos.
- **Utilice la autenticación de doble factor:** su proveedor de punto de venta debe utilizar una autenticación de doble factor.

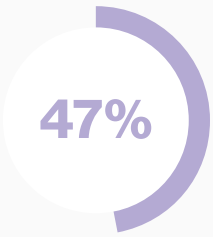
Ciberespionaje

Ataques con fines de espionaje realizados por actores relacionados con organizaciones públicas, a menudo en busca de propiedad intelectual.

Sectores más sensibles:
fabricación, información y ámbito profesional

Antes de pasar a emplear métodos más sofisticados, estos ataques suelen iniciarse con las mismas herramientas y técnicas que en otras ocasiones dieron buenos resultados. Por ello, las medidas de seguridad básicas resultan sorprendentemente eficaces para prevenir el ciberespionaje y no deben ser olvidadas en favor de una protección más especializada.

El 47% de todas las filtraciones confirmadas en el sector de la fabricación podrían clasificarse como ciberespionaje.



¿Qué puede hacer al respecto?

- **Aplique una reparación local tan pronto como resulte posible:** los ciberdelincuentes son expertos en explotar las vulnerabilidades conocidas; una reparación local aplicada a tiempo puede bloquear muchos ataques.
- **Monitorice los cambios en la configuración:** muchos métodos de ataque pueden detectarse fácilmente observando algunos indicadores clave.
- **Separe los sistemas:** asegúrese de que un ordenador vulnerado no constituye la puerta de acceso a sistemas y datos más importantes.

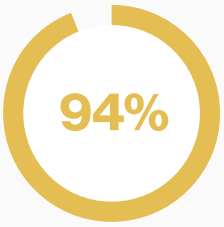
Skimmers de tarjetas de pago

Incidentes que implican la instalación física de un dispositivo en un cajero automático, surtidor de combustible o terminal de punto de venta para interceptar datos de tarjetas.

Sectores más sensibles:
servicios financieros, comercio minorista y alojamiento

La mayoría de estos ataques se dan en cajeros automáticos, aunque los surtidores de combustible y otros dispositivos no están exentos de riesgo. Los *skimmers* (pequeños dispositivos que copian los datos de las tarjetas) son prácticamente imposibles de detectar, incluso para los más expertos.

El 94% de las filtraciones de los datos de tarjetas de pago con skimmers se dio en cajeros automáticos.



¿Qué puede hacer al respecto?

- **Utilice terminales a prueba de manipulaciones:** algunos terminales son más susceptibles a las manipulaciones que otros. Seleccione aquellos cuyo diseño disuada a los delincuentes.
- **Busque signos de manipulación:** establezca un proceso de comprobación regular de la integridad de los dispositivos lectores instalados en sus cajeros o surtidores de combustible. Forme a sus empleados en la detección de *skimmers* y adopte medidas que agilicen la notificación de cualquier aspecto sospechoso.
- **Utilice controles de garantía:** puede optar por algo tan sencillo como instalar un precinto en la compuerta del surtidor de combustible.

Los *hackers* son más rápidos

Los ciberdelincuentes son capaces de acceder y sustraer (exfiltrar) datos en cuestión de minutos. En el 93% de los casos de sustracción de datos, los sistemas fueron penetrados en minutos o incluso menos. Las exfiltraciones se realizaron en minutos en el 28% de los casos. Incluso cuando las exfiltraciones se demoraron durante días, los delincuentes actuaban con total tranquilidad. En el 83% de los casos, las víctimas no descubrían las filtraciones hasta pasadas semanas o meses.

Cuanto más se tarda en detectar una filtración, más tiempo tienen los delincuentes para localizar los datos de valor que buscan e interrumpir sus operaciones. Por ello, no es suficiente con estar protegido. Es necesario contar con sistemas y procesos de detección y recuperación para frustrar posibles ataques y reducir los daños potenciales.

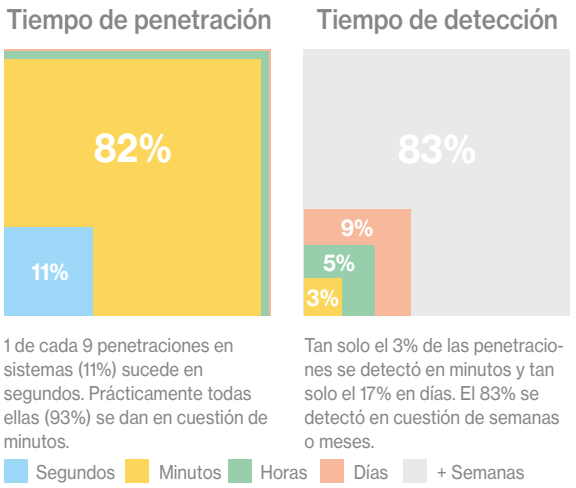


Figura 3: Cronograma de filtraciones

Figura 4: Nacimiento y renacimiento de una filtración de datos

La táctica de ataque

Conocer los fundamentos de un ataque puede ayudarle a levantar una defensa sólida y detectar una filtración rápidamente en caso de que se produzca.

Incluso los ataques más sofisticados tienen puntos en común con los más sencillos. Sin embargo, las distintas partes de un ataque no siempre se dan en el mismo orden. Además, las víctimas no se enfrentan a ataques individuales. Los gráficos sobre ataques pueden ayudarle al describir el perfil completo del ataque y no simplemente las rutas que ha descubierto.

Una reparación local eficaz puede detenerlos

Las 10 principales vulnerabilidades [Vulnerabilidades y Riesgos Frecuentes, o CVE, por sus siglas en inglés] constituyeron el 85% del tráfico explotado con éxito. Más del 15% implica una cifra superior a 900 CVE.

Las reparaciones locales tempranas son un elemento importante pero, a la luz de las innumerables nuevas vulnerabilidades descubiertas, resulta complicado determinar por dónde empezar. El DBIR de este año proporciona información de gran valor para ayudarle a resolver este problema.

Los datos ofrecidos por Kenna Security sugieren que las vulnerabilidades de los productos de Adobe fueron las más rápidamente explotadas, mientras que las de los productos de Mozilla fueron más lentamente aprovechadas, tal y como se muestra en la Figura 5. El análisis de esta información le ayudará a evitar los "simulacros" y dirigir sus iniciativas de reparación local.

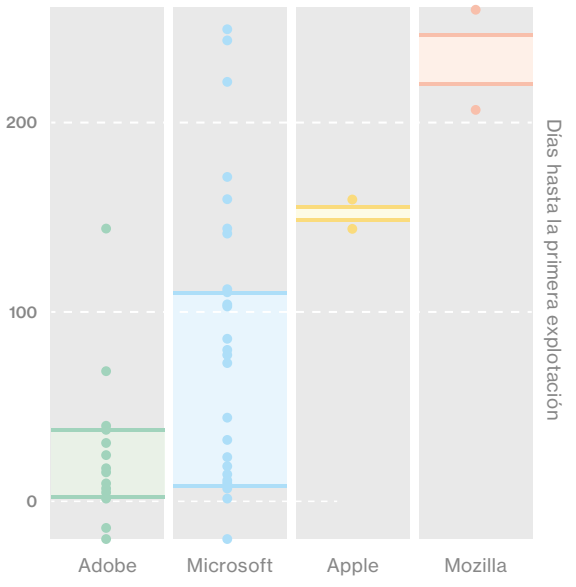


Figura 5: Días hasta la primera explotación

Utilice la inteligencia, ¡los ladrones lo hacen!

Los ciberdelincuentes no se conforman con el *statu quo*. Conforme se reduce el valor de determinados datos, los atacantes vuelven a lanzar sus redes para abarcar más terreno y mejorar sus tácticas.

Si bien es cierto que ningún sistema es totalmente seguro, son muchas las organizaciones que se lo ponen demasiado fácil a los ciberdelincuentes. No subsanan sus vulnerabilidades conocidas y permiten que sus empleados utilicen contraseñas fáciles de descifrar, e incluso *utilicen* las contraseñas predeterminadas suministradas con los dispositivos.

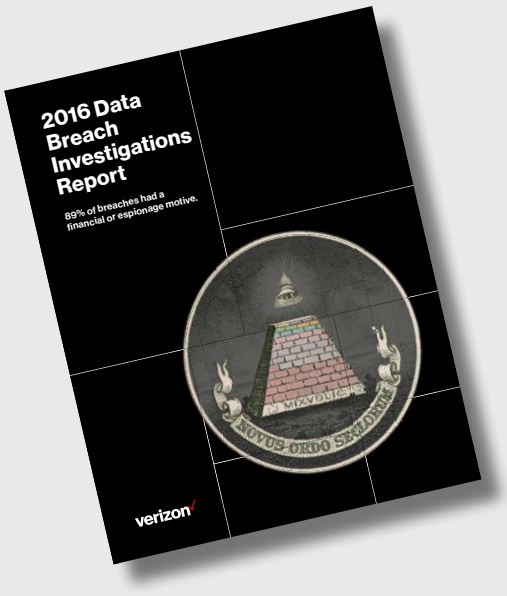
De esto se deriva que muchas de las filtraciones sufridas se habrían podido evitar si las organizaciones hubiesen adoptado determinadas medidas de seguridad básicas. Los siete consejos de la derecha repasan los errores más simples que se repiten una y otra vez.

En cualquier caso, su equipo de TI debe conocer profundamente las amenazas a las que debe hacer frente su organización. Los ciberdelincuentes utilizan toda la información a su alcance para mejorar su estrategia. Usted debería hacer lo mismo. El Informe sobre Investigaciones de Violaciones de la Información de 2016 es una lectura obligada para cualquier organización que se tome en serio la ciberseguridad.

Resumen de conclusiones

- **Permanezca alerta:** los archivos de registro y los sistemas de gestión de cambios pueden alertarle de forma temprana de cualquier posible filtración.
- **Convierta a los individuos de su organización en la primera línea de defensa:** forme a su personal para detectar señales de alerta.
- **Revele sus datos únicamente cuando sea estrictamente necesario:** únicamente el personal que necesite acceder a sus sistemas para realizar su trabajo deberá poder llegar hasta sus datos.
- **Aplique una reparación local tan pronto como resulte posible:** esta práctica puede evitar muchos ataques.
- **Cifre sus datos confidenciales:** asegúrese de que sus datos son prácticamente inutilizables en caso de ser sustraídos.
- **Utilice la autenticación de doble factor:** esta medida puede limitar el daño derivado de la pérdida o sustracción de credenciales.
- **No se olvide de la seguridad física:** no todas las sustracciones de datos se realizan a través de Internet.

Consiga el Informe sobre Investigaciones de Violaciones de la Información de 2016



El DBIR es nuestra principal publicación anual en materia de seguridad y una de las fuentes de información más valiosas del sector. Además del informe completo y el presente resumen, publicamos otros recursos que le ayudarán a conocer las amenazas y mejorar su defensa. Le invitamos a consultarlos.

Consiga el DBIR de 2016 completo y muchos otros recursos de gran utilidad.

Seguir leyendo >

¿Cuenta con una estrategia de ciberseguridad acertada? Vea nuestro SlideShare.

SlideShare >

VerizonEnterprise.com