TECNOLOGÍA | SEGURIDAD INFORMÁTICA

**Cómo saber si se encuentra involucrado en una violación de datos, y qué hacer**

*Si se sospecha estar involucrado en una violación de datos, este informe puede ayudará a saber dónde y cuándo ocurrió, y que pasos debe seguir a continuación.*

**Por Julián M. Zappia.  
Diplomatic Week.**

Las violaciones de datos son incidentes de seguridad de los que ahora escuchamos todos los días. Golpean todas las industrias, todos los sectores.

Las organizaciones de víctimas pueden ser de todo, desde pequeñas empresas independientes hasta compañías.

IBM estima que el costo promedio de una violación de datos en 2022 para las empresas de EE. UU. fue de $ 4,24 millones.

Los daños aumentaron en un promedio de $ 1,07 millones cuando se trataba de trabajo remoto, una estadística desalentadora para las empresas que ahora se adaptan al trabajo híbrido y desde casa.

Sin embargo, hablar de los millones de dólares que gastan las corporaciones para reparar sistemas dañados, realizar análisis forenses cibernéticos, mejorar sus defensas y cubrir los honorarios legales no necesariamente transmite todos los costos que sienten los clientes individuales involucrados en una violación de datos.

Para las personas, los costos pueden ser más personales.

Y si bien el daño financiero puede ser un factor, la pérdida puede ser en forma de salarios, ahorros y fondos en inversiones.

**¿Cómo ocurren las filtraciones de datos?**

Según IBM, el vector de ataque inicial más común que usan los ciberatacantes para ingresar a la red de una empresa es el uso de credenciales comprometidas, un enfoque que es responsable del 20% de las infracciones.

Estas credenciales pueden incluir nombres de usuario y contraseñas de cuentas filtrados en línea, robados en un incidente de seguridad separado u obtenidos a través de ataques de fuerza bruta, en los que los scripts automáticos prueban diferentes combinaciones para descifrar contraseñas fáciles de adivinar.

Otros posibles métodos de ataque son:

* Ataques de Magecart: empresas como British Airways y Ticketmaster han sufrido estos ataques, en los que se inyecta silenciosamente un código malicioso en las páginas de pago de comercio electrónico para recopilar la información de su tarjeta de pago.
* Código malicioso inyectado en dominios y formularios de sitios web: se pueden usar las mismas tácticas para obtener otras formas de datos de clientes y visitantes, con datos robados directamente de víctimas desprevenidas que visitan un servicio legítimo.
* Estafas de Business Email Compromise (BEC): las estafas BEC requieren que un atacante pretenda ser un empleado, contratista o proveedor de servicios de la empresa. Se aferran a hilos de correo electrónico o se ponen en contacto con un miembro del personal, como uno que trabaja en los departamentos de pagos o servicio al cliente, para engañarlos para que entreguen información o paguen una factura a una cuenta bancaria equivocada.
* Amenazas internas: a veces, los empleados tienen cosas que hacer o los ciberdelincuentes les hacen una oferta que no rechazan. Esto puede llevar a que su información cambie de manos, como en el caso de un ciudadano ruso arrestado por tratar de reclutar trabajadores de una empresa estadounidense para instalar malware en la red de su empleador.
* Negligencia: los servidores no seguros, que se dejan abiertos y expuestos en línea probablemente debido a configuraciones incorrectas, son una de las razones principales de la exposición y las filtraciones de datos. La información también puede ser filtrada accidentalmente por los empleados.
* Caer en el spam y los intentos de phishing: a nivel individual, los ciberdelincuentes intentarán que el usuario final cometa el error de enviar la información de la cuenta a través de correos electrónicos no deseados, dominios de phishing y más.

**¿Qué sucede cuando un atacante está dentro?**

El atacante lleva a cabo, en primera instancia, lo que se conoce como vigilancia; tiene la posibilidad de “mapear” (detectar completamente) una red para determinar dónde están los recursos más valiosos, o para descubrir vías potenciales para saltar a otros sistemas.

Verizon dice que el 71% de los incidentes relacionados con datos tienen una motivación financiera. Los atacantes pueden implementar ransomware para chantajear a sus víctimas para que paguen y recuperen su acceso a la red.

En las llamadas tácticas de “doble extorsión”, los grupos de hackers intentan, primero, robar información confidencial y luego amenazar con filtrarla en línea.

Alternativamente, algunos hackers aprovechan la situación y “desaparecen”, robando la propiedad intelectual por la que ingresaron ilegalmente a un sistema, para luego borrando sus huellas.

Otros pueden probar su punto de acceso y venderlo a otros ciberatacantes a través de la dark web.

En algunos casos, las intrusiones en la red tienen una sola razón: interrumpir los servicios y dañar una empresa.

Algunos de estos delincuentes informáticos descargan datos y vuelcan los datos robados para que estén disponibles gratuitamente en línea, publicándolos en recursos de fácil acceso.

**¿Qué es la web oscura?**

Internet, como sistema, se puede dividir en tres capas: la web clara, la profunda y la oscura.

* The clear web: La web clara es el Internet que la mayoría de nosotros usamos a diario. Los motores de búsqueda indexan millones de sitios web y páginas, y puede acceder a ellos desde un navegador típico, como Safari, Chrome, Edge o Firefox.
* The deep web: La web profunda es la capa subyacente, que requiere un navegador específico para acceder. Por lo general, se requiere la red Tor y una VPN. Los sitios web se indexan con direcciones que usan la extensión .onion (en lugar de las conocidas .com y otras que conocermos) y toda la red se basa en los principios de seguridad y anonimato. Esto ayuda en las aplicaciones legales, como eludir la censura, así como en las operaciones ilegales.
* The dark web: La web oscura es la siguiente capa hacia abajo y es un área que está asociada con la actividad delictiva. Esto puede incluir la venta de información, productos ilegales, drogas, armas y otros materiales ilícitos.

Los términos web oscura y profunda se pueden usar indistintamente.

**¿Cómo afectan las filtraciones de datos?**

Si se ha estado involucrado en una violación de datos como usuario o cliente, los registros también pueden haber sido expuestos, robados o filtrados en línea, como en los casos a continuación:

* Securitas: en enero pasado, los investigadores revelaron depósitos de AWS no seguros pertenecientes a la empresa de seguridad, que quedaron expuestos en línea. Se filtraron registros de empleados del aeropuerto y sus PII.
* Base de datos de la Policía Nacional de Shanghái (SHGA): en julio de 2022, los informes sugirieron que los datos recopilados por la SHGA, que afectaron a aproximadamente mil millones de ciudadanos chinos, se vieron a la venta en la Dark Web.
* Robinhood: un incidente de seguridad de 2021 resultó en el robo de información personal y direcciones de correo electrónico de aproximadamente 5 millones de personas.
* Facebook: un volcado de datos que incluye información perteneciente a 553 millones de usuarios de Facebook se publicó en línea en 2021, dos años después de haber sido recolectado.
* Volkswagen, Audi: el año pasado, las empresas admitieron una violación de datos que afectó a 3,3 millones de clientes y compradores interesados.

Nuestra información de identificación personal (PII), incluido el nombre, dirección física, dirección de correo electrónico, historial laboral, número de teléfono, sexo y copias de documentos, incluidos pasaportes y licencias de conducir, pueden usarse para llevar a cabo el robo de identidad.

El robo de identidad es cuando alguien usa la información personal de otro sin permiso, para pasar como otra persona, que puede ser cualquiera. Los delincuentes informáticos pueden usar su identidad o datos financieros para realizar fraudes y cometer delitos.

Esto puede incluir fraude relacionado con impuestos, apertura de líneas de crédito y préstamos a su nombre, fraude médico y compras fraudulentas en línea.

Los delincuentes también pueden llamar a una empresa que utiliza, como un proveedor de telecomunicaciones, y pretender ser usted para engañar a los representantes de los clientes para que revelen información o realicen cambios en un servicio, como en el caso de ataques de intercambio de tarjetas SIM.

Dado que el delito cibernético es global, también puede ser extremadamente difícil para las fuerzas del orden procesar a los delincuentes.

El chantaje también puede ser un factor. Cuando el sitio web de relaciones extramatrimoniales Ashley Madison experimentó una violación de datos en 2015, algunos ciberdelincuentes se pusieron en contacto con usuarios de esa red y amenazaron con contarles a sus parejas, amigos y colegas sobre sus actividades a menos que les pagaran.

**Cómo saber si se está involucrado.**

Por lo general, su proveedor de servicios de Internet se comunicará con usted por correo electrónico o cartas para explicarle que su información se ha visto comprometida. Sin embargo, las empresas pueden tardar semanas o meses en ponerse en contacto, si es que lo hacen.

Por lo tanto, también depende de cada uno de nosotros estar atento a las noticias sobre cualquier violación de datos recientemente revelada; también hay herramientas útiles disponibles que puede aprovechar.

Have I Been Pwned, operado por el experto en seguridad Troy Hunt, es el primer recurso que se debería utilizar para averiguar en qué violaciones de datos podríamos haber estado involucrados y en qué medida se han filtrado los datos.

El motor de búsqueda le permite buscar por su dirección de correo electrónico o número de teléfono y marcará cualquier infracción que contenga sus datos cuando ocurra mediante la verificación cruzada de miles de millones de registros filtrados agregados a la base de datos Have I Been Pwned.

Al escribir sus datos, procesarlos, y posteriormente se visualiza una pantalla verde, no se ha estado involucrado en ningún incidente notable de seguridad de datos. Sin embargo, si es así, verá una pantalla que le indicará qué infracciones lo han afectado.

**Administradores de contraseñas.**

Si usa un administrador de contraseñas, como 1Password , Keeper o Dashlane (entre otros), puede ofrecer servicios de monitoreo de infracciones que lo alertarán cuando sus contraseñas estén expuestas en una filtración de datos.