HISCOX

Informe Hiscox sobre la Siniestralidad Cibernética 2018

Hiscox, compañía internacional de seguros especializados tiene su sede en Bermuda y cotiza en la Bolsa de Londres. La empresa suscribe mediante las divisiones – Hiscox Retail (que incluye Hiscox UK y Hiscox Europa, Hiscox Guernesey, Hiscox USA y la empresa subsidiaria DirectAsia), Hiscox London Market y Hiscox Re & ILS. Aunque su negocio de venta al por menor esté en el mercado de Reino Unido, Europa y EE.UU., Hiscox ofrece seguros especializados para profesionales y empresas así como propietarios de viviendas de alto patrimonio. Hiscox suscribe a nivel internacional empresas de gran tamaño y reasegura a través de Hiscox London Market y Hiscox Re & ILS. Para más información, visite www.hiscoxgroup.com.

Introducción

Desde la desviación de fondos fraudulenta hasta el cryptojacking...

Los riesgos cibernéticos sí se pueden gestionar

Un seguro cibernético puede parecer un producto nuevo, sin embargo, Hiscox lleva casi 20 años ofreciendo este producto. Solo en los últimos 12 meses, hemos tramitado más de 1.000 siniestros relacionados con la seguridad cibernética de diferentes empresas. La principal causa de estos siniestros ha sido el ransomware, en el que un atacante desactiva por completo el sistema informático de una empresa hasta que se pague un rescate. Un análisis completo del mercado indica que esta táctica se encuentra en declive ya que las personas y las empresas son cada vez más conscientes de la amenaza después de los famosos ataques de Wannacry y Petya de 2017, aunque aún seguimos viendo algunos siniestros relacionados con ransomware en 2018.

Este último año ha llamado la atención el creciente número de siniestros relacionados con las transacciones fraudulentas, donde un criminal se las apaña para persuadir de forma fraudulenta a una organización para que le pague a él, en lugar de a un proveedor. Creemos que esto se debe a que los incidentes de este tipo requieren niveles relativamente bajos de complejidad técnica. Con frecuencia, los atacantes solo necesitan usar sus teléfonos para llevar a cabo sencillos ataques de ingeniería social o crean direcciones de correo falsas para atraer a víctimas potenciales.

El auge del cryptojacking

Lo que estas tácticas sugieren es que, mientras los criminales cibernéticos seguramente siguen muy interesados en robar y usar información personal y confidencial para beneficio económico, actualmente hay maneras más directas de lucrarse mediante los ciberdelitos. Una de las últimas tendencias, cuyo impacto examinaremos más adelante en este informe, es el cryptojacking, por el cual los criminales utilizan clandestinamente la capacidad de procesamiento de los sistemas informáticos de una empresa para hacerse con criptomonedas.

Los ejemplos que mostramos en este informe ofrecen una visión general del tipo de siniestros que hemos visto este último año, que afectan a diferentes tipos de empresa, industrias y zonas geográficas. Para que quede claro, ninguna empresa es inmune a la creciente amenaza de los delitos cibernéticos.

Nos hemos dado cuenta de que los atacantes están desarrollando sus métodos y tienen como objetivo de ataque dos elementos clave de la empresa: su red informática que cada vez se encuentra mejor protegida el perímetro y su a los empleados, su verdadero talón de Aquiles. Las negligencias de los empleados se perfilan como un factor de riesgo clave y mostramos en este informe ejemplos de ataques relacionados con phishing. La amenaza va más allá e incluye infecciones conocidas como drive-by, que ocurren al visitar una página web, y el peligro de que el personal mande información confidencial de manera insegura o pierda dispositivos móviles que no tengan las debidas medidas de seguridad. En este caso, las empresas deben asegurarse de que sus empleados cuentan con lo necesario para hacer frente a estos riesgos. Para ello, la formación del personal es esencial.

¿Cómo respondemos a la amenaza?

En cada uno de los casos que hemos nombrado, nuestro seguro cibernético fue más allá del compromiso de pago y jugó un rol fundamental a la hora de responder ante las amenazas. Las compañías afectadas contaron con la rápida ayuda de diversos expertos; entre ellos, tramitadores de seguros con experiencia en seguridad cibernética que les asistieron durante el incidente, especialistas forenses que repararon la amenaza, y un equipo de relaciones públicas y apoyo legal que les ayudó a reducir los daños a la reputación de las empresas. Nuestro objetivo es ayudar a nuestros clientes a volver a su actividad lo antes posible al mismo tiempo que les ofrecemos apoyo económico por cualquier pérdida de ingresos relacionada.

Se espera que el mercado de seguros cibernéticos alcance un valor de 36.000 millones de dólares americanos en el año 2027 (su valor actual asciende a 3200 millones de dólares). En este contexto, este informe sobre siniestros cibernéticos de Hiscox 2018, será el primero de una serie de informes y material relacionado sobre esta temática que iremos presentando. Nace con el fin de ayudar a nuestros clientes y a los empresarios a entender mejor los ciberriesgos actuales y emergentes; mostrar cómo pueden reducir el riesgo en sus organizaciones; e ilustrar cómo la cobertura de seguros puede formar parte de una estrategia de gestión de riesgos cibernéticos.

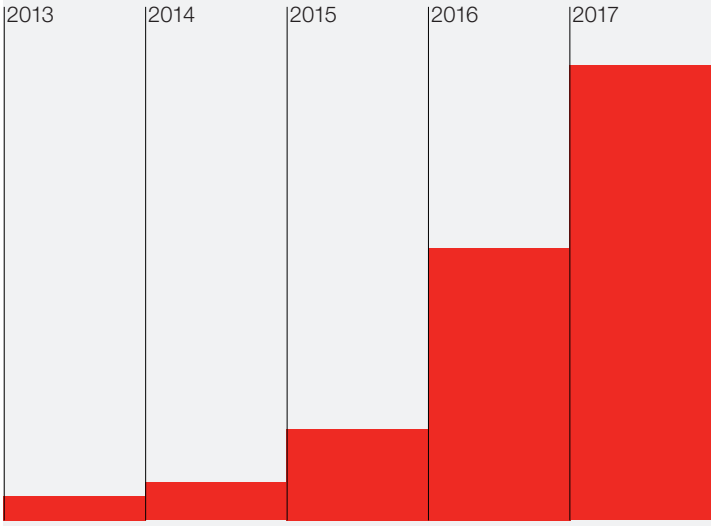
Gareth Wharton
Cyber CEO
Hiscox

Siniestros de Cyber en cifras

Más de 1.000 siniestros en los últimos 12 meses

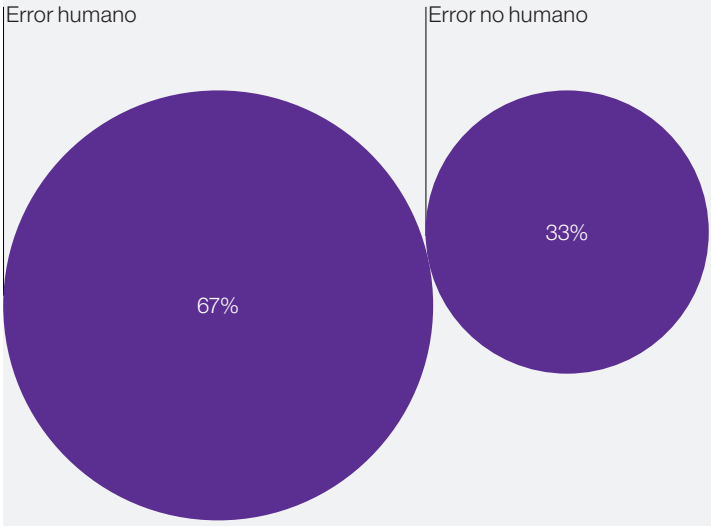
Crecimiento del número de siniestros

En todos los mercados con presencia de Hiscox



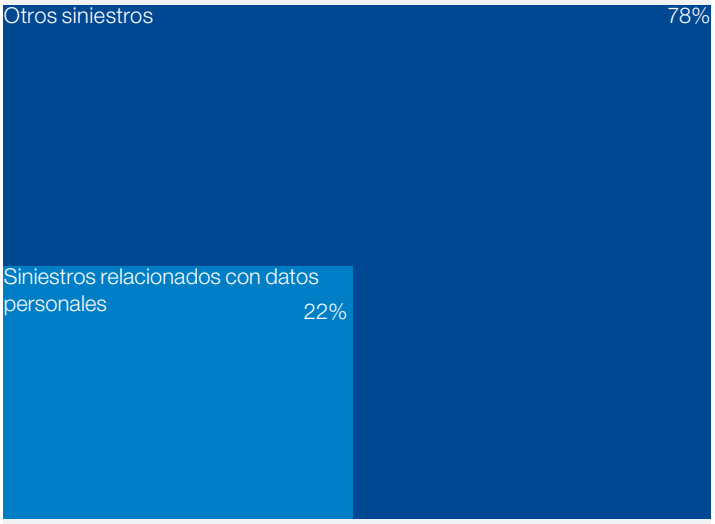
Desde 2013, el número de siniestros relacionados con la ciberseguridad que hemos tramitado han aumentado en más de un 1.700%. Esto proviene de una posición relativamente baja pero es un buen indicador de que las empresas de todos los tamaños y en todos los mercados en los que tenemos presencia están experimentando mucha más actividad relacionada con la amenaza cibernética que hace cinco años. Por lo tanto, sus consecuencias pueden derivar en una pérdida económica y de reputación bastante mayor.

Siniestros de Hiscox en los últimos 12 meses



Más de dos tercios (un 67%) de todos los siniestros entrañan un factor de negligencia por parte de un empleado. Los ejemplos incluyen a empleados que hacen click en correos electrónicos maliciosos, visitan páginas web dañinas o simplemente son descuidados y pierden los dispositivos de la empresa. Es esencial que las empresas no solo inviertan en tecnología, sino también en procesos y personas; así se aseguran de que su personal es una primera línea de defensa efectiva ante estos ataques.

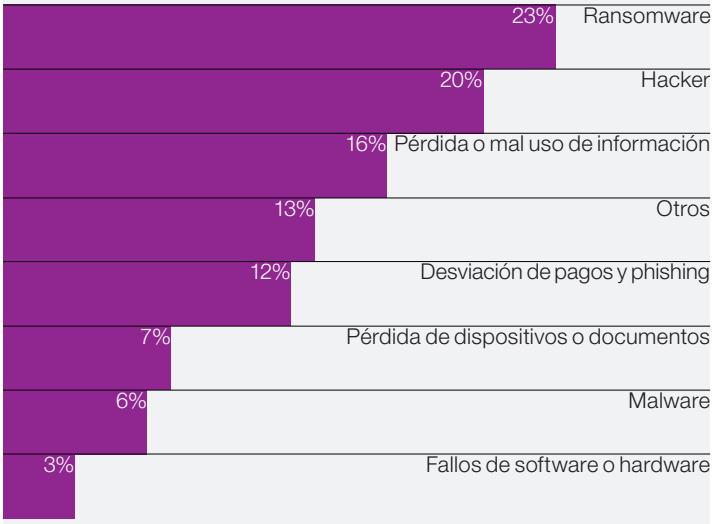
Siniestros relacionados con datos personales en los últimos 12 meses



Casi un cuarto de los siniestros (un 22%) han estado relacionados con la pérdida o el mal uso de información personal. Dado el endurecimiento de la normativa, los incidentes de este tipo pueden incluso resultar más costosos, tanto en términos económicos como de reputación de la empresa. A pesar de ello, el 78% de los siniestros no incluyeron ni pérdida ni mal uso de información, lo cual es un riesgo incluso para aquellas empresas que tienen pocos o ningun dato personal.

Causa de siniestros en los últimos 12 meses

En todos los países con presencia de Hiscox



Mientras que el ransomware ha sido la causa de siniestros más relevante en los últimos 12 meses, el gráfico anterior enseña la amplia gama de ataques de los que las empresas se tienen que proteger. Algunas de estas amenazas son externas, otras son internas y otras, accidentales. En conjunto, esto prueba la necesidad de adoptar una estrategia de defensa cibernética que abarque a personas, procesos y tecnologías.

Los siniestros de Cyber en el punto de mira
El ransomware sigue en alza

Al igual que en los últimos años, el ransomware siguió siendo la mayor causa de los siniestros relacionados con la seguridad cibernética en los últimos 12 meses, en gran medida debido a las escasas barreras de acceso para los atacantes, la facilidad de la implementación y la posibilidad de una rentabilidad decente tras una inversión mínima. Normalmente, el error humano suele ser un factor clave en el ransomware, ya que los errores cometidos por los empleados también permiten numerosos ataques de phishing e ingeniería social. A continuación les presentamos cuatro ejemplos anónimos de siniestros cibernéticos reales que hemos tramitado durante los últimos 12 meses, tres de los cuales presentaron algún elemento de error humano.

Un caso singular de ransomware

Sector
Tecnología

Facturación
Entre 10 y 50 millones de euros

Coste del siniestro
420.000 euros

Contexto
Nuestro asegurado se dio cuenta de que sus sistemas informáticos habían sido comprometidos cuando se cifraron varias de sus carpetas y recibió un mensaje donde se le pedía que pagara un rescate. El atacante había averiguado la identidad del administrador de la red de la empresa y llevó a cabo entonces un ataque de fuerza bruta para identificar su contraseña.

El atacante usó las credenciales del administrador para acceder en remoto a los sistemas de la empresa. Así fue capaz de obtener más credenciales que le procuraron un acceso todavía mayor. Tanto la información personal como la información comercial confidencial (contratos, datos de cuentas de banco, etc.) se vieron comprometidas.

Respuesta de Hiscox
La empresa se puso en contacto con nosotros y de inmediato buscamos a un asesor legal especializado en protección de datos, un paso clave para ayudar a mitigar el impacto ante una filtración de información. Pusimos a disposición del asegurado una empresa de informática forense para que investigaran el alcance del incidente y aseguraran de nuevo la red de la empresa. También le explicamos los pasos que debían dar para notificar al Regulador y los clientes afectados . A su vez, le contratamos a una agencia de RRPP para que aconsejase a la empresa en sus comunicaciones con la prensa y los clientes.
Se notificó al regulador local de protección de datos, así como a los clientes y las personas que aparecían en la información comprometida. Nuestra rápida reacción impidió que el regulador pidiese más medidas.

Conclusiones
- El atacante probó un gran número de combinaciones de contraseñas (suelen ser miles) hasta encontrar la correcta. Para protegerse contra este ataque, es fundamental una buena gestión de la cuenta del usuario. Por ejemplo, las cuentas deberían bloquearse tras un gran número de intentos fallidos de acceso.
- El Centro Nacional de Ciberseguridad de Reino Unido ofrece buenos consejos sobre esta materia y recomienda a las empresas que sigan los siguientes pasos:
  - permitir unos diez intentos para acceder a la cuenta antes de que la cuenta se bloquee;
  - poner en marcha la monitorización de protección. Se trata de una defensa potente ante ataques de fuerza bruta y supone una buena alternativa a bloqueos o reducciones de servicio
  - dotar a los administradores, usuarios que se conectan en remoto y dispositivos móviles de mayor protección, con la autenticación de doble factor.
  - comprobar que los administradores utilizan contraseñas diferentes de sus cuentas de usuario administrador y no administrador;
  - considerar la implementación de la autenticación de doble factor en todas las cuentas remotas.

La venganza se sirve mejor con un ataque DDoS

Sector
Servicios financieros

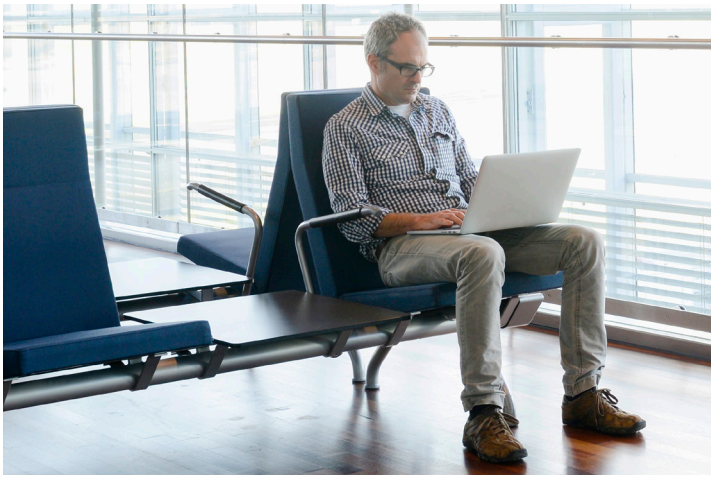
Facturación
Entre 10 y 50 millones de euros

Coste del siniestro
150.000 euros

Contexto
Una empresa intermediaria de préstamos sufrió una serie de ataques DDoS, un ciberataque que sobrecarga las redes con más tráfico del que puede gestionar para que no funcione, que paralizó su página web durante varios días, por lo que no pudo operar.

Respuesta de Hiscox
Una investigación policial reveló que los ataques provenían de un empleado descontento. Nosotros cubrimos los costes del asegurado, que tuvo que pagar a sus proveedores de servicios informáticos para que restauraran sus sistemas. La empresa también sufrió una importante interrupción en su negocio por culpa de esta transgresión.

Conclusiones
- Las organizaciones que dependen de que sus clientes sean capaces de acceder a sus servicios online deberían considerar obtener un servicio de mitigación de DDoS. Sus técnicas filtran el tráfico no deseado antes de mandar peticiones legítimas a la página web adecuada.



La cuenta del restaurante ha salido un poco cara

Sector
Alimentación

Facturación
Entre 1 y 10 millones de euros

Coste del siniestro
20.000 euros

Contexto

Un ataque de ransomware cifró todo el servidor de un restaurante al impactar en sus terminales de punto de venta. La consecuencia: el sistema no funciona.

Respuesta de Hiscox

Tras agotar todas las demás opciones, quedó claro que el método más efectivo de restaurar los sistemas del restaurante era pagar el rescate.

Cubrimos los gastos del rescate, junto a los costes adicionales de informática de utilizar la clave de cifrado y asegurarse de que el negocio del asegurado se ponía en marcha de nuevo. También contratamos a un experto en violación de datos para confirmar si algun dato personal había sido comprometido. Además de estos costes, cubrimos la interrupción del negocio que sufrió el restaurante como resultado de no poder utilizar los sistemas.

Conclusiones

- Las empresas pueden reducir de manera notable el riesgo de ataques de phishing ayudando a sus empleados a reconocer el estilo de los correos electrónicos que pueden contener phishing o enseñándoles qué buscar en los datos de los remitentes para identificar emails sospechosos.
- Es también importante asegurarse de que se hacen copias de seguridad. Se debería llevar un control regular a través de un sistema que no esté conectado a la red principal, por ejemplo en un disco duro.

Si un jefe te pide dinero…

Sector
Servicios financieros

Facturación
Más de 50 millones de euros

Coste del siniestro
260.000 euros

Contexto

Un empleado de una agencia de servicios financieros fue víctima de un ataque de phishing tras recibir un email falso de uno de los jefes de la empresa pidiéndole que transfiriera 260.000€ en una cuenta de banco específica. Creyendo que el correo era real, el empleado emitió la transferencia fraudulenta y tanto el banco de la agencia como el banco destinatario no pudieron recuperar los fondos. El correo procedía en realidad de una cuenta de Gmail que imitaba a la perfección la dirección real del jefe.

Respuesta de Hiscox

Al darse cuenta de lo que había pasado, la agencia nos llamó y contactamos de inmediato con un experto en violación de datos y forenses informáticos para que confirmaran si había habido una filtración en los sistemas del asegurado o si los datos personales habían sido comprometidos.

Ofrecimos una indemnización por la pérdida de beneficios en el plazo de un mes a partir de la fecha de la comunicación. Al mismo tiempo se confirmó que no había tenido lugar ninguna violación de datos, por lo que no se tuvo que hacer ninguna notificación a los clientes.

Las pérdidas por desviación de pagos fraudulenta están cubiertas por defecto en nuestra póliza de seguro cibernético de Estados Unidos y ofrecidas como una cobertura adicional en otros territorios.

Conclusiones

- Aquí es clave ofrecer una mejor formación a los empleados para ayudarles a identificar correos electrónicos que puedan contener phishing.
- Es importante comprobar con cuidado las direcciones de correo electrónico antes de emprender ninguna acción. Las empresas pueden ayudar a sus empleados si incluyen un identificador en todos los correos que se reciben de fuentes externas, por ejemplo si incluyen “este correo electrónico procede de fuentes externas a la organización” o algo similar.
- Un cambio de cultura puede contribuir notablemente a la hora de mitigar este tipo de amenaza. La alta dirección debería crear un ambiente donde los empleados tengan más probabilidad de hacer las cosas “bien” que de simplemente satisfacer una petición “urgente” de un cliente o un jefe. Lo ideal sería que las peticiones de transferencias de dinero a cuentas nuevas o modificadas se verificaran llamando a la otra parte interesada en un número de teléfono predeterminado, uno que ya tuvieran los empleados, no el que viene en un email con phishing, ya que los atacantes suelen dar números falsos.

La nueva moda: el cryptojacking
Más lucro y menos esfuerzo para los criminales

Los criminales están empezando a dejar atrás los ataques de ransomware más obvios e invasivos y se inclinan ahora por un ciberdelito que pasa mucho más desapercibido: el cryptojacking. Según la empresa estadounidense Symantec, los casos de cryptojacking aumentaron en un 8.500 % en el último trimestre de 2017. Una vez que el atacante tiene acceso a un sistema informático comprometido, en vez de descargar un programa dañino para cifrar los archivos de la víctima y pedir posteriormente un rescate, el ataque de cryptojacking instalará software para buscar datos, también denominado como "software mining". El programa se instala sin que nadie se dé cuenta y utiliza los recursos de procesamiento de reserva del dispositivo de la víctima o el entorno del servidor de la oficina y va buscando criptomonedas para el hacker. Hemos visto casos donde el software de minería de datos ha sido tan invasivo que los dispositivos de las víctimas no podían completar sus propias tareas. Sin embargo, somos de la opinión de que los atacantes más inteligentes solo usarán un pequeño porcentaje de la capacidad de procesamiento del ordenador. De esta manera, nadie detectará su actividad y podrán ganar más a largo plazo.

Cuando la víctima es una empresa tecnológica

Sector
Tecnología

Facturación
Más de 50 millones de euros

Coste del siniestro
80.000 euros

Contexto
Una empresa tecnológica se dio cuenta de que se había instalado un programa de malware en uno de sus servidores.

Respuesta de Hiscox
De inmediato pedimos a una empresa de informática forense que investigara lo que el malware estaba haciendo y cómo se había instalado en los sistemas de nuestro asegurado. El servidor contenía una gran cantidad de datos personales, por lo que también investigamos si había una violación o riesgo mayor de que se hubiese comprometido dichos datos.

Dada la gravedad potencial de la transgresión, pedimos además a un experto en violación de datos que llevara a cabo la investigación. Este confirmó que el malware estaba minando pero afortunadamente se quedó ahí la cosa y no tuvo un alcance mayor.

Publicidad para Bitcoin

Sector
Marketing

Facturación
Hasta un millón de euros

Coste del siniestro
50.000 euros

Contexto
Una empresa de RRPP observó que había un problema con sus correos electrónicos. Su proveedor habitual de servicios informáticos investigó y concluyó que la causa más probable es que hubiera actividad maliciosa. El asegurado se puso en contacto con nosotros y contratamos un equipo informático forense que acudió rápidamente para hacer indagaciones y confirmó que el asegurado había sido víctima de un ataque.
Los sistemas informáticos de la empresa de RRPP habían sido infectados con malware de cryptojacking para minar criptomonedas. También vieron que los atacantes que filtraron el malware habían accedido a los sistemas del asegurado y los datos personales de sus clientes se habían visto comprometidos.

Respuesta de Hiscox
Tras estudiar el alcance de la violación, el equipo informático quitó el malware y solucionó el problema de seguridad de la empresa que había permitido la infiltración. Después procuramos asesoramiento legal para nuestro asegurado en cuanto a la obligación de las notificaciones y más tarde, organizamos la notificación al Regulador y de las personas que aparecían en la información comprometida.

Conclusiones

En ambos casos (junto a la recomendación habitual de gestionar bien las contraseñas y actualizar el software frecuentemente para asegurarse de que ofrece una protección completa), las organizaciones pueden también utilizar software de control de servidores con el fin de conocer las métricas claves de los servidores como el uso del disco, el procesador, la memoria y la red. Con el tiempo, el software de control creará un punto de referencia desde el que se pueden fijar los umbrales. Este puede ser un método efectivo para controlar las interrupciones del servidor, así como para detectar niveles poco habituales del tráfico de la red, que pueden indicar cuándo se está extrayendo información sin permiso. Si el uso del procesador es más alto de lo habitual durante largos periodos, esto puede ser una prueba de que en el servidor hay malware minando criptomoneda.

Glosario de términos

Agente de amenaza. Un individuo, grupo, organización o gobierno que realiza o tiene el propósito de realizar actividades perjudiciales (en otras palabras, un atacante).

Air gap. En español, brecha de aire. El aislamiento o separación física de un sistema de otros sistemas o redes.

Amenaza interna. Una persona o grupo de personas dentro de una empresa que supone un riesgo potencial al poder infringir las políticas de seguridad, ya sea intencionadamente o mediante una negligencia.

Amenaza persistente avanzada. También conocida por sus siglas en inglés, APT (advanced persistent threat), es un tipo de ataque selectivo llevado a cabo de manera concienzuda por un agente con el tiempo y los recursos suficientes para planificar una infiltración en una red. El principal objetivo suele ser obtener información de carácter patrimonial o económico, más que conseguir simple información financiera. Las APT son persistentes porque los atacantes pueden quedarse en la red durante algún tiempo y suelen eludir los controles periódicos de seguridad.

Anti-malware/anti-virus. Software que usa un escáner para identificar programas que son o pueden ser maliciosos.

APT. Véase "amenaza persistente avanzada".

Asesor de seguridad cualificado. En inglés, QSA o qualified security assessor. Persona homologada para inspeccionar comercios en relación al cumplimiento de la normativa PCI-DSS.

Ataque de denegación de servicio distribuido. Las siglas DDoS corresponden al término en inglés: distributed denial-of-service attack. Ataque que sobrecarga un ordenador o una página web con peticiones y/o instrucciones, de manera que impide a los usuarios acceder correctamente. Se suele utilizar una botnet para llevar a cabo este tipo de ataque.

Ataque de fuerza bruta. Un ataque en el que los crackers utilizan software para probar un gran número de combinaciones de contraseñas posibles para obtener acceso sin autorización a un sistema o archivo.

Autenticación. El proceso de verificar la identidad u otros atributos de una entidad. También se puede hacer referencia a la autenticación multifactorial (o de dos factores), que atañe al proceso en el que se utilizan varios métodos para identificar y autenticar a un individuo.

AV. Véase "anti-malware/anti-virus".

Backdoor (troyano). Un programa de software malicioso que permite a alguien controlar el ordenador de un usuario sin su permiso.

Blacklist. Véase "lista negra".

Bot. Véase "zombie".

Botnet. Colección de ordenadores o dispositivos conectados a Internet que han sido infectados por programas nocivos y son controlados a distancia por un cracker o atacante. Esta información se manda a un servidor de mando y control.

Bug. Un defecto, falta, imperfección o error inesperado y relativamente pequeño en un sistema, un código de software o un terminal.

Certificado SSL. En inglés, secure sockets layer. Un antiguo protocolo (reemplazado por TLS) por el que se enviaba información privada a través de Internet utilizando sistemas criptográficos que usaban dos claves para cifrar los datos.

Cifrado. También llamado encriptación. El procedimiento por el cual se usa una clave secreta para convertir información legible en un formato ilegible para cualquiera que no posea dicha clave.

Comité de normas de seguridad de la industria de tarjetas de pago. Conocido por sus siglas en inglés, PCI-SSC. Organismo responsable de desarrollar y promover el PCI-DSS y las herramientas relevantes para facilitar su cumplimiento. Ha sido fundado por las cinco compañías de tarjetas más importantes (Visa, Mastercard, American Express, JCB and Diners) y cuenta con el apoyo de un "consejo asesor" conformado por representantes de sus principales socios (minoristas, procesadores de pago, bancos, etc.).

Control de acceso. El proceso de conceder o denegar las solicitudes específicas o intentos de obtener y utilizar la información y los servicios de procesamientos de la información, así como de entrar en las instalaciones físicas específicas.

Control de acceso a la red. Conocido como NAC, network access control. Un método que aumenta la seguridad de la empresa mediante la restricción del acceso a la red solo a aquellos terminales que acatan una política de seguridad definida.

Cookie. Archivos ubicados en su ordenador que permiten recordar datos a las páginas web.

Cryptojacking. El uso no autorizado, por parte de un atacante, de los sistemas de ordenador de un usuario para minar criptomonedas.

Cuestionario de autoevaluación. Los pequeños comercios utilizan los SAQ (self-assessment forms) para verificar que cumplen la normativa PCI-DSS.

Cyber Essentials. Un plan de certificación de seguridad cibernética desarrollado por el Gobierno británico, que sirve como una excelente base de referencia para el sector. El nivel básico requiere completar un cuestionario de autoevaluación, que será posteriormente revisado por un organismo certificador externo. El plan Cyber Essentials Plus incluye una garantía adicional; un organismo certificador externo realiza pruebas de los sistemas de control de seguridad.

Encriptación. Véase "cifrado".

DDoS. Véase "ataque de denegación de servicio distribuido".

Día cero. Se trata de una vulnerabilidad. Un bug de software, desconocido para los desarrolladores de la empresa, que los atacantes han detectado y pueden aprovechar para comprometer ordenadores, programas, información o una red.

DLP. Véase "prevención de pérdida de datos".

DNS, domain name system. En español, sistema de nombres de dominio. Listín telefónico de Internet. Permite a los ordenadores traducir nombres de páginas web, como hiscox.es, a direcciones IP para que se pueden comunicar entre ellos. Véase también "secuestro de DNS".

Drive-by download. La infección de un ordenador con malware cuando un usuario visita una página web maliciosa, sin que el usuario sea consciente de la descarga realizada.

Ejercicio red team. Un ejercicio, en un entorno en el que se reflejan las condiciones del mundo real, en el que un adversario (equipo rojo o red team) simula atacar o aprovechar las vulnerabilidades de la red de una empresa. El fin de esta práctica es conocer las propias debilidades para mejorarlas.

Endpoint. Un dispositivo de hardware con conexión a Internet. El término se puede aplicar a ordenadores de sobremesa, portátiles, smartphones, tabletas, cliente liviano, impresoras, etc.

Exploit. Un ataque que se aprovecha de una vulnerabilidad (normalmente en el código de software) para acceder o infectar a un ordenador.

Firewall. Una barrera entre redes o partes de una red que bloquea el tráfico malicioso o impide los intentos de ataque. El firewall inspecciona todo el tráfico, tanto entrante como saliente, para comprobar que se cumplen ciertos criterios. Si se cumplen, se permite el tráfico; si no, el firewall lo bloquea.

Gestión de eventos e información de seguridad. Conocido como SIEM, se trata de una herramienta que ofrece visibilidad de la seguridad cibernética de una empresa mediante la agregación de alertas y registros de actividad generados por varias fuentes y recursos de seguridad (IPD, IDS, AV, etc.).

Gusano. Véase "worm".

Hacktivismo. Se utiliza para describir aquellos ataques motivados por fines políticos, éticos o sociales.

Hashing. Un proceso que utiliza un algoritmo de cifrado irreversible para convertir una entrada de datos en un código alfanumérico aleatorio. Se suele usar para proteger las contraseñas en el caso de que un adversario malicioso obtenga acceso a la base de datos donde están guardadas. A menudo se ve este término acompañado de "salting" (véase más abajo).

IDS. Véase "sistema de detección de intrusiones".

Informe sobre el cumplimiento. Más conocido como RoC, report on compliance. Un QSA emite un RoC cuando al inspeccionar los sistemas informáticos de los comercios, estos cumplen la normativa PCI-DSS.

Ingeniería social. Métodos que los atacantes usan para engañar a las víctimas y conseguir que hagan algo. A menudo incluye phishing, así como llamadas de teléfono, cuentas falsas de LinkedIn, etc. Normalmente, estas acciones abren una página web maliciosa o ejecutan un archivo adjunto no deseado.

Inyección SQL. SQL es un lenguaje de programación que le dice a una base de datos qué tiene que hacer. Un ataque de inyección SQL ocurre cuando se manipula ese lenguaje para alterar el funcionamiento normal de la base de datos y se le pide que realice una tarea diferente de lo que se pretendía.

IPS. Véase "sistema de prevención de intrusiones".

IRP. Véase "plan de respuesta a incidentes".

ISO 27001. Una norma internacional que describe las mejores prácticas respecto a la gestión de la seguridad de la información de una empresa.

Keylogger. Un tipo de malware que puede grabar en secreto las pulsaciones que efectúa un usuario en el teclado y mandarlas a terceros sin autorización.

Lista blanca. En inglés, whitelist. Lista de entidades, direcciones IP, aplicaciones, etc. que se consideran de confianza y a las que se les conceden accesos o privilegios.

Lista negra. En inglés, blacklist. Lista de entidades, direcciones de IP, etc. que son bloqueadas o a las que se les deniegan accesos o privilegios.

Malware. Término genérico para software malicioso. El malware incluye virus, gusanos, troyanos y spyware. Los términos malware y virus se suelen utilizar indistintamente.

Marco de referencia de ciberseguridad NIST. Un conjunto de normas, buenas prácticas y recomendaciones para mejorar la seguridad cibernética. No está restringido a una sola industria, zona geográfica o norma y se centra en los resultados, más que en las aportaciones.

NAC. Véase "control de acceso a la red".

NIST. Instituto Nacional de Normas y Tecnología. Véase "marco de referencia de ciberseguridad NIST".

Normas de seguridad de datos de la industria de tarjetas de pago. PCI-DSS son sus siglas en inglés. Una normativa sobre seguridad de la información creada por el comité PCI-SSC (véase …) que rige el modo en el que las empresas que aceptan pagos con tarjetas de crédito o débito deben manejar y proteger esa información. Hay cuatro niveles de gestión, dependiendo del volumen de transacciones que maneja una compañía; empezando por el nivel cuatro hasta llegar al nivel uno. Son las compañías de tarjetas de pago las que establecen a nivel individual los límites exactos de estos niveles.

Parches. Extensiones de software y/o firmware que corrigen bugs y vulnerabilidades de seguridad.

PCI-DSS. Véase "normas de seguridad de datos de la industria de tarjetas de pago".

PCI-SSC. Véase "comité de normas de seguridad de la industria de tarjetas de pago".

Phishing. Práctica fraudulenta en la que se mandan correos electrónicos, que fingen provenir de fuentes de confianza, con el objetivo de manipular a los usuarios e intentar que lleven a cabo acciones particulares como revelar información, transferir fondos o abrir enlaces o archivos adjuntos.

Phreaking. Utilizar un ordenador u otro dispositivo para engañar a un sistema de telefonía. Se emplea a menudo para hacer llamadas de teléfono gratis o cargar llamadas a una cuenta diferente.

Plan de respuesta a incidentes. Conocido también por sus siglas en inglés IRP (incident response plan). Un conjunto de procedimientos predeterminados y documentados para detectar y responder a un ataque cibernético.

Prevención de pérdida de datos. También conocida por sus siglas en inglés, DLP (data loss prevention), se trata de un conjunto de procedimientos y herramientas de software que impide que los datos confidenciales puedan salir de una red.

Protocolo de escritorio remoto. El RDP o remote desktop protocol es una metodología que permite a los usuarios conectarse a distancia a sistemas informáticos a través de Internet.

Protocolo SFTP. Las siglas hacen referencia a secure file transfer protocol. Metodología utilizada para enviar archivos a través de Internet en un formato cifrado.

Pruebas de penetración. Proceso por el cual los peritos buscan las vulnerabilidades de una empresa e intentan sortear las medidas de seguridad de una red o un sistema de información.

QSA. Véase "asesor de seguridad cualificado".

Ransomware. Un programa de software malicioso que cifra o bloquea el acceso a la información o los sistemas. Los usuarios afectados solo pueden acceder a la clave de descifrado si pagan una tarifa al atacante.

RDP. Véase "protocolo de escritorio remoto".

Red privada virtual. Una VPN (en inglés, virtual private network) es un método de conectar ordenadores remotos a una red central, lo que permite a los usuarios comunicarse o acceder a los servidores de la organización de manera segura a través de Internet.

Redundancia. Sistemas, subsistemas, activos (assets) o procesos adicionales o alternativos que mantienen un grado de funcionamiento general en caso de pérdida o fallo (failure) de otro sistema, subsistema, activo o proceso.

Resiliencia. La capacidad de una red de:

- garantizar un funcionamiento continuo (por ejemplo, ofrecer mucha resistencia a las perturbaciones y ser capaz de funcionar a menor escala si se han sufrido daños);
- recuperarse con eficacia si se produce una avería; y
- hacer frente a solicitudes rápidas o impredecibles, como ataques de DDoS.

RoC. Véase "informe sobre el cumplimiento".

Rootkit. Unidad de software que oculta los programas o procesos que se están ejecutando en un ordenador.

Salting. La incorporación de una cadena de caracteres aleatorios y únicos a una contraseña antes de que se lleve a cabo el hashing. De esta manera, es más difícil descifrar la contraseña.

SAQ. Véase "cuestionario de autoevaluación".

Secuestro de DNS. Un ataque que cambia los ajustes de un ordenador para ignorar el DNS o para utilizar un servidor de DNS controlado por atacantes maliciosos. Estos adversarios pueden redireccionar la comunicación del usuario hacia páginas web fraudulentas.

Seguridad de la capa de transporte. Conocida como TLS, transport layer security. Al igual que su predecesor SSL, es un protocolo por el que se envía información privada a través de Internet usando sistemas criptográficos que utilizan dos claves para cifrar los datos. Muchos navegadores de Internet indican que la conexión está protegida por TLS mostrando el icono de un candado o un certificado de seguridad cerca de la barra del navegador, donde se encuentra la URL de una página web. Todavía se le sigue llamando SSL.

Servidor de mando y control. Un ordenador que manda instrucciones a miembros de una botnet.

SFTP. Véase "protocolo SFTP".

SIEM. Véase "gestión de eventos e información de seguridad".

Sistema de detección de intrusiones. Más conocido como IDS, intrusion detection system. Un terminal o programa de software que controla una red o varios sistemas en busca de actividades maliciosas o infracciones de normas. Identifica y señala cualquier actividad sospechosa o inusual.

Sistema de prevención de intrusiones. También conocido como IPS o intrusion prevention system. Una versión proactiva de un IDS que puede bloquear automáticamente cualquier comportamiento sospechoso.

Spear phishing. Un ataque de phishing dirigido a un individuo en concreto.

Spoofing. Un ataque de ingeniería social o phishing por el cual se suplanta la identidad del remitente de un correo electrónico.

Spyware. Software que permite a los anunciantes o los atacantes conseguir información confidencial sin el permiso del usuario.

SSL. Véase "certificado SSL".

Superficie de ataque. Todos los activos de una organización expuestos a Internet. Esto incluye hardware y software. A mayor número de activos, mayor número de vulnerabilidades potenciales y por lo tanto, mayor "oferta" para aquellos adversarios que quieran atacar a una organización.

TLS. Véase "seguridad de la capa de transporte".

Troyano. Programa malicioso que tiene la apariencia de un programa legítimo e inocente pero que en realidad lleva a cabo funciones perjudiciales de forma oculta.

Vector de amenaza. Método que un agente de amenaza utiliza para conseguir acceso a una red.

Virus. Programa malicioso que se puede extender a otros archivos.

VPN. Véase "red privada virtual".

Vulnerabilidades. Bugs en el software que los adversarios aprovechan para afectar negativamente a los ordenadores.

Whitelist. Véase "lista blanca".

Worm. En español, gusano. Tipo de malware que puede replicarse y propagarse solo, sin la intervención de personas o sistemas. Se podría decir que es malware en modo automático.

Zombie. También conocido como bot. Un ordenador infectado, controlado a distancia por un atacante. Forma parte de una botnet.

Hiscox España

Paseo de la
Castellana 60.
7ª Planta.

28046 Madrid

T +34 91 515 99 00
E info_spain@hiscox.com
hiscox.es

19300 09/18