HISCOX

El ABC de la ciberseguridad
Para empresas

Ciberguía ABC de Hiscox: prólogo

¿Sabía que el coste total en 2017 de la ciberdelincuencia contra las empresas se situó en torno a los 14.000 millones de euros, solo en España? Puede parecer sorprendente, aunque no tanto si tenemos en cuenta que la mayor parte de la información actual se encuentra en algún tipo de activo digital almacenado en lugares que van mucho más allá de las cuatro paredes de la empresa a la que pertenece. Lo cual quiere decir que la mayor parte de los datos son accesibles potencialmente para cualquiera que pertenezca a una organización, además de proveedores, socios y multitud de personas externas que cuentan con las herramientas y los conocimientos apropiados.

A medida que envejecen los sistemas y están más interconectados a través de Internet, aumenta el número de vulnerabilidades de seguridad, y los fallos de seguridad más sonados copan los titulares con cierta frecuencia. Todo ello, junto con la rapidez con que evolucionan sin cesar las ciberamenazas, ha colocado la ciberseguridad en un lugar prioritario de la agenda para muchos pequeños empresarios.

Un estudio de Accenture publicado en 2018 sobre el negocio cibernético en España refleja que las organizaciones españolas sufren entre dos y tres violaciones de seguridad al mes. Aunque el 65% de las compañías estén protegidas, el 33% de los CISO (Chief Information Security Officer o director de la seguridad de la información) reconoce que una tercera parte de su organización no está protegida por un programa de ciberseguridad, dato preocupante, ya que los ataques externos no son los únicos que tienen lugar en las empresas, la información publicada accidentalmente por los empleados supone un 58% de los ciberataques.

La mayoría de las empresas españolas tienen previsto aumentar el gasto de TI en ciberseguridad y centrar más esfuerzos en reducir el ciberriesgo y otra parte importante prevé el aumento de la formación, un 27% aumentará la formación de sus empleados.

Para poder gestionar de manera efectiva los riesgos de la ciberseguridad, los pequeños empresarios han de procurar formarse y formar a sus empleados en dicha materia. Necesitan entender el idioma de la seguridad con el fin de identificar los ciberataques y asegurarse de que se tomen las medidas adecuadas.

Este ABC examina algunos de los términos habituales utilizados en asuntos de ciberseguridad, además de ofrecer asesoramiento experto: un primer paso para los pequeños empresarios que quieren protegerse mejor. Es un compañero sencial para quienes quieran pasar a la acción y afrontar los retos que supone la ciberdelincuencia a medida que nos adentramos en un futuro donde está demasiado presente.

Andrew Rogoyski
Vicepresidente de Ciberseguridad de CGI
www.cgi-group.co.uk

[1] Fuente: INCIBE (Instituto Nacional de Ciberseguridad)

A

Nombre de la amenaza

Acceso no autorizado

Acceso ilegal a un sitio web, programa, servidor, servicio o datos. Popularmente se le llama hackeo.

Descripción

El acceso no autorizado es el uso de un ordenador o de una red sin permiso y es ilegal en muchos países de todo el mundo.

¿Cómo funciona?

El acceso no autorizado suele efectuarse mediante ataques internos o externos y de distintas maneras. Credenciales débiles, robadas o perdidas están entre los métodos más comunes para comprometer un ordenador y eludir el control de acceso. Un hacker también puede infectar su objetivo con malware utilizando, por ejemplo, un troyano, o explotando una vulnerabilidad del sistema operativo, del hardware o de las aplicaciones. Asimismo, los hackers pueden recurrir a tácticas de ingeniería social (véase la letra I), o utilizar herramientas como el registro de pulsaciones de teclado para conseguir acceso no autorizado a un ordenador o a una red. Con un ataque interno, se podría conseguir acceso mediante el robo de las credenciales de otros usuarios, o se podría sobornar a alguien con privilegios de alto nivel con el fin de acceder a información para un tercero malicioso. De hecho, un estudio de BT y KPMG ha descubierto que el 51% de las empresas no poseen una estrategia para hacer frente al chantaje.

Consejos de protección

Las credenciales débiles o aquellas que se pierden son una forma de ponérselo fácil a quienes intentan conseguir acceso no autorizado a un sistema, de manera que es imperativo para cualquier empresa establecer una política clara de contraseñas. No olvide aplicar los últimos parches de seguridad para protegerse contra vulnerabilidades y errores: podría tapar los agujeros de seguridad que un hacker utiliza para conseguir acceso no autorizado. Tampoco es mala idea revisar los privilegios de seguridad de la red y dar a los empleados acceso únicamente a los datos y áreas que estén dentro de sus competencias, pues tanto el personal de informática como el que no pertenece al departamento muy rara vez necesitan ‘todas las llaves del reino’.

B

Nombre de la amenaza

Botnet

Red de robots informáticos que se ejecutan de manera automática y autónoma para controlar equipos informáticos de forma remota.

Descripción

No todos los botnets son maliciosos ya que se trata de un número de ordenadores interconectados llevando a cabo una serie de tareas con el fin de que las páginas web sigan en funcionamiento. Estos botnets son legales y ayudan a que la experiencia del usuario sea satisfactoria. El problema es cuando el botnet es malicioso. Un ejemplo fue en 2012 con el botnet 'Gameover Zeus' que propagó el malware Cryptolocker infectando a casi un millón de ordenadores mediante una ciberestafa.

¿Cómo funciona?

El dispositivo hackeado funciona con normalidad pese a estar controlado por un tercero de forma remota. Va adquiriendo derechos de administrador dándole el control sobre el dispositivo a los ciberdelincuentes.

Consejos de protección

Para reducir el riesgo de esta amenaza debe actualizar con frecuencia las contraseñas de sus dispositivos, instalar las últimas actualizaciones del software. Además, si suele descargarse archivos de Internet, utilice un buen antivirus para comprobar que ningún archivo está infectado.

B

Nombre de la amenaza

Bulo informático

Los Hoaxes son avisos, normalmente transmitidos por correo electrónico, con contenido falso, engañoso o atrayente. Aunque no representan un peligro para los sistemas, ya que no contienen código malicioso, sí que son un peligro para la sociedad.

Descripción

A través de un mensaje de denuncia, de noticia (puede ser un ataque, un ciberataque etc) o una situación que llame la atención, se extienden por gran cantidad de dispositivos gracias a su mensaje viral y la incitación a compartirlo.

¿Cómo funciona?

El objetivo es compartir una noticia, ya sea falsa o modificada, debido a titulares y contenido llamativo y la facilidad para compartirla con otras personas (por email). El problema es que puede llegar a extenderse de tal manera que desvirtúe la noticia real, haga que la real parezca falsa o haga cundir el pánico. Provoca un peligro social más que en el sistema.

Consejos de protección

En este caso lo mejor es no difundir de forma masiva información de la que no se esté seguro de su veracidad, pero hay algunas formas de identificar un Hoax:

- suele provenir de un individuo, no una empresa o una institución.
- suele avisar de una situación negativa y puede dar soluciones fáciles para solucionarla.
- urge a compartir el mensaje.
- suele buscar credibilidad citando alguna fuente con autoridad.

C

Nombre de la amenaza

Cadenas de mensajes

Las cadenas de mensajes hacen referencia a esos correos electrónicos que urgen al destinatario a que los envíen a otras personas.

Descripción

El acceso no autorizado es el uso de un ordenador o de una red sin permiso y es ilegal en muchos países de todo el mundo.

¿Cómo funciona?

La mayoría de la gente probablemente recuerde haber visto cadenas de cartas circulando por su bandeja de entrada del correo electrónico o en redes sociales. Suelen pedir donaciones benéficas o describir algún juego con números sin sentido antes de urgir al destinatario a que lo envíe al mayor número de personas posible. Aunque puedan parecer hasta divertidas en cierta medida, las cadenas de cartas pueden plantear graves riesgos para la seguridad.

Uno de los ejemplos más famosos se dio a comienzos de la década de los 2000. Una carta decía que Bill Gates estaba repartiendo su fortuna y que el destinatario recibiría 245 dólares por reenviar el mensaje. Incluso se citaba a un abogado inexistente, llamado Pearlas Sandborn. Por ridículo que suene, es sorprendente la cantidad de gente que pica en timos como este.

Consejos de protección

La mejor manera de protegerse contra las cadenas de mensajes es eliminar inmediatamente cualquier mensaje en el que se pida el envío a otras personas. Evite siempre hacer clic en los adjuntos y enlaces a otros sitios web y no facilite ninguna clase de información personal salvo que sepa que es auténtica y esté seguro de que sabe dónde está haciendo clic.

Por último, asegúrese de que todos los ordenadores de su red tengan un antivirus instalado y un anti-spam efectivo y advierta a sus empleados sobre los peligros de las cadenas de mensajes.

C

Nombre de la amenaza

Ciberextorsión

Se produce una ciberextorsión cuando se roban datos con la finalidad específica de chantajear a la víctima.

Descripción

En una ciberextorsión, el hacker amenaza con hacer públicos datos sensibles de la empresa salvo que esta pague o cumpla una exigencia. En 2014, Sony anunció que fue víctima de una ciberextorsión, cuando un grupo autodenominado 'Guardianes de la Paz' (GOP) filtró datos confidenciales de Sony Pictures Entertainment. Contenía información sobre empleados, incluidos los correos electrónicos que se intercambiaban y copias de películas de Sony sin estrenar en aquel momento.

¿Cómo funciona?

Los hackers utilizan métodos muy diversos para robar información a las empresas. A menudo se concentran en los empleados –que son la principal puerta de entrada de los ciberataques– con tácticas de ingeniería social (véase la letra I), y utilizan las contraseñas y datos confidenciales que recopilan para conectarse a la red de la empresa. Además, existen diversos tipos de virus malware (véase la letra M), que se distribuyen mediante spam o aprovechando las vulnerabilidades de la red. Una vez que están dentro, los hackers pueden trazar un plano del sistema y robar los detalles que necesiten para recopilar datos privados.

Consejos de protección

La clave para evitar ser víctima de una extorsión cibernética es asegurarse de que están protegidos los datos.

C

Nombre de la amenaza

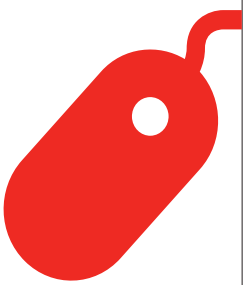
Contraseñas

Las contraseñas actúan como llave digital, dando acceso a archivos, sistemas y servicios, al tiempo que garantizan que eres quien dices ser.

Descripción

Gracias a los smartphones y a las redes sociales las contraseñas forman hoy parte integrante de nuestras vidas cotidianas, pero puede ser fácil olvidar lo importantes que son. Las contraseñas son muchas veces la única barrera para evitar que nuestros datos y dispositivos caigan en manos de los ciberdelincuentes de Internet, razón por la que es tan importante que sean seguras.

Un hacker con talento que tenga acceso a una sola de las contraseñas puede encontrar la manera de entrar en muchas otras de las cuentas online, obteniendo así acceso a información personal y privada.



¿Cómo funciona?

La fortaleza de una contraseña se basa en lo difícil que resulte de adivinar. Por eso, contraseñas como 'contraseña', 'fútbol', 'qwerty' y '12345' son malas contraseñas: todas son muy predecibles. Por desgracia, también son las más comunes. Un método para robar contraseñas se denomina 'ingeniería social' (véase la letra I), por el que los hackers confían en que les dé sus contraseñas por teléfono o en persona. Otro se denomina 'phishing' y consiste en que los hackers utilizan malware (véase la letra M) para mostrar mensajes falsos en su ordenador que dicen que tiene que volver a conectarse (introduciendo sus datos) a sitios como Facebook o la cuenta bancaria.

Consejos de protección

Una buena contraseña tiene que ser difícil de adivinar no solo para el hacker, sino también para las herramientas de software que utilizan. Estos programas prueban con una inmensa cantidad de posibles contraseñas en rápida sucesión, intentándolo con palabras y frases comunes, así como diversas permutaciones de las mismas.

Las contraseñas deben asimismo ser exclusivas para cada uno de los distintos dispositivos, sitios o servicios por razones obvias. Si reutiliza una misma contraseña varias veces, cualquier hacker que obtenga dicha contraseña tendrá acceso instantáneo a diferentes fuentes de los datos.

C

Nombre de la amenaza

Cuarentena

La cuarentena es una función que ejecutan los distintos software antivirus, por la que se aísla en el disco duro del ordenador cualquier archivo que dé indicios de infección. Dicho aislamiento garantiza que el archivo, si estuviera infectado, no pueda dañar o seguir infectando el ordenador conectado a Internet.

Descripción

La cuarentena es básicamente una forma de almacenamiento especial de objetos sospechosos en el ordenador, que estén infectados posiblemente por un virus. Estando en cuarentena, el archivo sospechoso no podrá ejecutarse y seguirá así hasta que el usuario decida eliminarlo, arreglarlo o sacarlo de la cuarentena.

¿Cómo funciona?

El software antivirus, preinstalado de serie o instalado por el usuario, no elimina automáticamente todo archivo sospechoso de estar infectado. Por eso se introdujo la cuarentena: la supresión de archivos sospechosos de estar infectados podría traer consigo que se eliminen por error archivos no infectados – e importantes para el usuario–.

Cuando el software antivirus de un ordenador detecta un archivo sospechoso, el usuario suele tener tres opciones: **limpiar, cuarentena y eliminar.**

La opción limpiar se puede utilizar para quitar la infección del archivo. Sin embargo, solo se refiere a aquellos virus de los que está infectado un archivo válido con código malicioso, generalmente viral. En cambio, amenazas como gusanos y troyanos no se pueden 'limpiar' pues no son infecciones: todo el archivo es o bien un gusano o bien un troyano. La opción eliminar suprime completamente el archivo del sistema, lo que deja la cuarentena como el punto intermedio entre limpiar y eliminar.

Consejos de protección

Cuando se enfrente a un archivo sospechoso, empiece siempre por la opción 'limpiar'. Si el antivirus informa que no ha sido posible limpiarlo, ponga el archivo directamente en cuarentena.

El archivo puesto en cuarentena está seguro y no dañará el resto del ordenador. Si está seguro al 100% de que no es un archivo válido, o si el antivirus lo recomienda, elimínelo. Pero recuerde: una vez eliminado, no suele haber manera de recuperarlo. Si no está seguro, deje el archivo en cuarentena y actualice periódicamente el software antivirus. Con cada actualización, ejecute una búsqueda y compruebe si el software sigue identificando ese archivo como amenaza.

D

Nombre de la amenaza

Denegación de servicio/DoS

El ataque de Denegación de servicio hace referencia a sus siglas en inglés DoS, Denial of Service. Se trata de un ataque a un dispositivo electrónico que provoca que el sistema no sea accesible a su dueño.

Descripción

El DoS es un ataque de una red o sistema de ordenadores hacia un objetivo, esto provoca una denegación de servicio a los propietarios del sistema afectado. Esta denegación se genera mediante la saturación de este sistema a causa de la gran cantidad de solicitudes que se envían. Este tipo de ataque se usa para dejar fuera de servicio un dispositivo.

¿Cómo funciona?

Este tipo de ciberataques suelen ser perpetrados por un hacker, quien comienza buscando una vulnerabilidad en un sistema informático para posteriormente crear una red de equipos que han sido infectados anteriormente y son controlados de forma remota. Con esta red es con la que se enviarán las millones de solicitudes que terminarán colapsando el sistema objetivo.

Consejos de protección

La forma más efectiva de protegerse de este tipo de ataques es tener identificadas las partes más propensas a ser atacadas, monitorizar estos puntos y evaluar si es necesario optimizar su rendimiento y resistencia. Una medida de control es otorgar visibilidad al equipo que regule estos sistemas dentro de su empresa sobre el tráfico de entrada y de salida, de tal forma que puedan reaccionar cuando se alteren los volúmenes habituales.

E

Nombre de la amenaza

Encriptar

La encriptación de un mensaje consiste en ocultar la información que contiene para que solo pueda visualizarse introduciendo una contraseña.

Descripción

El proceso de encriptado de información o archivos consiste en hacer ilegible estos archivos o esta información a través de un algoritmo que desordena sus componentes. A través de una clave, el algoritmo reordena la información para que sea legible de nuevo.

¿Cómo funciona?

Aunque la encriptación ha existido desde hace mucho años, actualmente los procesos son realmente sofisticados. Los dos principales métodos de encriptación son:

- encriptado simétrico: utiliza la misma clave para encriptar y desencriptar la información, de tal forma que con una sola clave puedes acceder a la información una vez la hayas encriptado.
- encriptado asimétrico: se utilizan dos claves diferentes, una para encriptar la información y que solo el propietario de la misma debería tener y otra para desencriptar el archivo. Esta última se puede compartir para que otras personas puedan acceder al contenido.

Consejos de protección

Esta metodología puede ahorrarle muchos disgustos, ya que actualmente en Internet se comparte gran cantidad de información, si encripta esta información, aunque caiga en manos no deseadas, estará a salvo.

F

Nombre de la amenaza

Falsos programas de seguridad

El falso antivirus es un tipo de programa malicioso cuya finalidad es extorsionar al usuario para sacarle dinero. Lo hacen afirmando que el dispositivo de la víctima está infectado y que necesita comprar un falso antivirus para combatir el problema.

Descripción

El antivirus falso es una de las amenazas más persistentes en Internet actualmente. También se le llama 'scareware' (que podríamos traducir como 'softaware de miedo'), pues muestra mensajes alarmantes al usuario, al que anima a tomar cartas en el asunto. Esta clase de malware tiene la capacidad de tomar el control del dispositivo y desactivar el software de seguridad original, lo que lo hace aún más difícil de eliminar.

¿Cómo funciona?

El falso antivirus suele aparecer en forma de ventana emergente o pop-up cuando navega por Internet. Las pop-up suelen advertir al usuario de que su dispositivo puede estar infectado, instándole a descargar un nuevo software disponible en un enlace que se le facilita. Pero si hace clic en el enlace es probable que instale más malware, y más peligroso, en el sistema informático. Las pop-up pueden redirigir sencillamente al usuario a un sitio web que vende software antivirus falso y que le pide al usuario que introduzca los datos de la tarjeta de crédito.

Consejos de protección

El primer paso para protegerse del antivirus falso es no hacer clic nunca en una ventana emergente. En vez de ello, utilice siempre la función 'Forzar salida' o 'Control + Alt + Suprimir' para cerrar la ventana. Si le preocupa la seguridad del dispositivo puede ejecutar un análisis utilizando software de seguridad legítimo. En general, es importante que mantenga actualizados los dispositivos con la última versión del antivirus para protegerle de esas amenazas online.

G

Nombre de la amenaza

Gusano

En el mundo cibernético, un gusano es un programa software malicioso cuya función es duplicarse a sí mismo para ralentizar el sistema infectado.

Descripción

Los gusanos suelen utilizar partes automáticas de un sistema para propagarse que generalmente no son accesibles para los usuarios. A diferencia de un virus más general, este tipo de software malicioso se duplica a sí mismo sin necesidad de una persona, este es su rasgo más característico.

¿Cómo funciona?

Gracias a la posibilidad de duplicarse de forma autónoma, los gusanos pueden propagarse por un sistema infectándolo con millones de copias sin que la persona llegue a darse cuenta. Esto provoca un gran consumo de memoria o del ancho de banda del sistema lo que puede provocar que deje de responder.

Consejos de protección

Dado que el gusano suele infectar el sistema a través de un elemento externo; enlaces, mensajes, redes externas etc, la mejor forma de prevenir este tipo de ataque es a través de un antivirus y un firewall. Realice de forma periódica análisis en busca de malware para evitar la excesiva propagación y posteriormente elimínelos.

H

Nombre de la amenaza

Hackers

Los hackers online son personas que pueden intentar colarse, destruir o causar daños a su ordenador o red informática.

Descripción

Existen diferentes tipos y grupos de hacker. Algunos escogen sus objetivos al azar por mera diversión, otros actúan de acuerdo con creencias políticas o ideológicas, y finalmente otros que están en esto por el lucro económico. Cada hacker es diferente y tiene su propio nivel personal de destreza. Incluso dentro de los grupos de hackers, las acciones y respuestas de sus miembros pueden variar radicalmente. No todos los hackers son malos: algunos son hackers 'éticos', que informan de los fallos de seguridad que les permiten llegar a sus víctimas.

Lo que tienen todos en común es que su empresa es un objetivo potencial para todos ellos. Para ellos no existe una empresa demasiado pequeña para hackear y los datos de los clientes son siempre valiosos en el mercado negro.

¿Cómo funciona?

Hay muchas técnicas que pueden utilizar los hackers para atacar los sistemas y cada día se inventan otras nuevas. Entre ellas están muchas de las amenazas activas que se enumeran en el presente glosario, como el phishing, el malware (véase la letra M) o los kits de explotación (secuencia de acciones destinados a explotar los agujeros de seguridad que encuentren en las aplicaciones de software).

Una vez dentro de la red, un hacker puede hacer muchas cosas. Puede husmear en los archivos, robar bases de datos e información sensible, o puede dedicarse inmediatamente a destruir o desfigurar el sistema. Por otro lado, puede suceder que usted no sepa en absoluto que ha sido hackeado. Un intruso puede, de forma sencilla, permanecer en la red durante semanas, incluso meses, esperando el momento adecuado para pasar a la acción. En algunos casos, los hackers han esperado años antes de manifestarse.

Consejos de protección

Los hackers tienen acceso a un arsenal inmenso de herramientas, por lo que necesita protegerse contra la mayor parte de ellas. Siga las mejores prácticas de seguridad, tales como utilizar contraseñas sólidas, no descargar archivos dudosos y alejarse de sitios web que no sean de confianza. El mejor escudo es el conocimiento. Para los hackers, un objetivo desinformado es un objetivo fácil. Intente en lo posible estar al tanto de las noticias de ciberseguridad, buscar tendencias o pautas de ataque que pudieran utilizar contra su empresa.

Nombre de la amenaza

Incumplimiento normativo

El incumplimiento normativo es la omisión de acatar las normas y regulaciones del Estado. En este caso, las relativas a ciberseguridad y privacidad de los datos.

Descripción

La normativa en materia de protección de datos tiene por objeto garantizar que las empresas adopten las medidas oportunas a la hora de tratar los datos e información de sus clientes, asegurándose de que no caigan en manos de hackers o ciberdelincuentes. Lo cual incluye establecer unos estándares mínimos de ciberseguridad que las empresas tienen que cumplir, establecer procedimientos y prácticas sobre cómo responder si se produce una vulneración de la seguridad de los datos y multar a las empresas que incumplan la normativa.

¿Cómo funciona?

Un ejemplo es el Reglamento General de Protección de Datos, un conjunto de normas que rige el tratamiento de los datos de los ciudadanos de la UE por parte de las empresas, y que ha entrado en vigor en mayo de 2018. El reglamento se aplica a cualquiera que archive o trate datos de ciudadanos europeos, incluidas las pequeñas empresas. En dicho reglamento están por ejemplo las normas que exigen a las empresas notificar a las autoridades una vulneración de la seguridad de los datos en el plazo de 72 horas desde que se produzca, junto con otras medidas. La multa máxima por el incumplimiento de esta legislación se fija en el 4% de la facturación global de una empresa.

Consejos de protección

La legislación –y en particular la legislación comunitaria, tan densa y amplia– puede resultar difícil de entender, pero tiene que asegurarse de que conoce y cumple todas las normas relativas a la actividad o campo específicos.

Hay muchos recursos oficiales online para ayudarle a ello, entre ellos se incluye asistencia y orientación respecto a las leyes que le son aplicables y cómo puede cumplirlas. También puede contratar a profesionales especializados en el cumplimiento normativo para asegurarse de que evita problemas en aquellas cuestiones jurídicas confusas.

Nombre de la amenaza

Ingeniería Social

La ingeniería social es una técnica que emplean los hackers para manipular presencialmente (es decir, no en línea) a las personas para que lleven a cabo una acción o compartan datos.

Descripción

La ingeniería social supone engañar a la gente, es en su nivel más básico una estafa popular, o 'timo', que los delincuentes llevan utilizando muchos años. En 2007, con la sola ayuda de su encanto personal, un tipo engañó a los empleados de un banco de ABN Amro en Bélgica y salió por la puerta con 21 millones de euros en diamantes. En 2013, la cuenta de Twitter de Associated Press fue secuestrada después de que un empleado hiciera clic en un correo electrónico. La cuenta de Twitter secuestrada hundió la media del Dow Jones Industrial (DOW) después de tuitear 'Última hora: dos explosiones en la Casa Blanca, Barack Obama está herido'. Tanto el golpe de los diamantes como el secuestro del Twitter de AP son ejemplos de ingeniería social: ganarse la confianza a cambio de acceso, datos o fraude.

¿Cómo funciona?

Existen numerosos tipos de ataques de ingeniería social; algunos juegan con la vanidad de la persona objetivo, otros con la autoridad y la codicia. Y muchos son increíblemente simples. Uno de los métodos supone dejar sin recoger un dispositivo infectado, como una memoria USB, con la esperanza de que alguien la coja y la enchufe en el ordenador. En ese momento la memoria instalaría malware o un virus. Otra técnica de uso habitual se denomina phishing.

Consejos de protección

Es aconsejable que las empresas proporcionen formación y asesoramiento sobre ingeniería social a todos los empleados. Cuando los empleados están formados en protocolos de seguridad y se les dice cómo deben manejar los datos y la información, es menos probable que tenga éxito un ataque. También es buena idea tener implantado un marco de confianza y una evaluación de riesgos, y que los empleados tengan acceso únicamente a los datos de su área de competencia.

J

Nombre de la amenaza

John Brennan

En 2015, un estudiante de enseñanza secundaria hackeó la cuenta de correo AOL del director de la CIA.

Descripción

El método que utilizaron el hacker y sus cómplices se suele denominar 'ingeniería social' (véase la letra I), que consiste en que el hacker se apoya en la interacción humana para obtener acceso a datos confidenciales. El hacker llevó a cabo una búsqueda inversa del número de teléfono de Brennan para descubrir que era cliente de la red móvil de Verizon. Después él o uno de sus cómplices llamaron a la compañía fingiendo ser un técnico de Verizon y pidieron detalles de la cuenta de Brennan. Aportando un 'Vcode' (número de empleado de Verizon) totalmente falso, los hackers obtuvieron suficientes datos personales de Brennan como para conseguir conectarse a su cuenta de AOL, accediendo así a docenas de correos electrónicos altamente confidenciales.

¿Cómo funciona?

Existen numerosos tipos de ataques de ingeniería social que se pueden utilizar para atacar de diferentes maneras. En este caso, el ataque se basó en que una persona diera información confidencial a alguien en cuya identidad confiaba.

Otra de estas técnicas se denomina 'baiting' y consiste en dejar un dispositivo infectado, como un USB, en un lugar fácil de encontrar. La persona que se encuentra con el USB lo pone en su ordenador (por pura curiosidad) e instala sin saberlo un malware o un virus. Véase la letra M para más información.

Consejos de protección

Las empresas deben proporcionar formación y orientación sobre ingeniería social a todos los empleados. Véase la letra I (ingeniería social).

K

Nombre de la amenaza

Keylogger

El registro de pulsaciones en el teclado o ‘keylogging’ hace referencia al proceso de registrar cada pulsación en el teclado de un ordenador. El keylogger es el dispositivo de software o hardware que registra las pulsaciones.

Descripción

El ‘keylogging’ es un método habitual que emplean los hackers y supone registrar todo lo que alguien teclea con la finalidad de robarle información confidencial. Una vez que los hackers instalan el software o hardware necesario para ello, tienen acceso completo a toda la información, como nombres de usuario, contraseñas y datos bancarios.

¿Cómo funciona?

El keylogger se suele instalar por medio de malware (véase la letra M), pero también lo pueden instalar en forma de hardware, por ejemplo, empleados descontentos, cónyuges celosos o progenitores protectores. Estos keyloggers de hardware suelen venir en forma de memoria USB o de dispositivo que se puede enchufar al teclado. Tienen una ventaja sobre el software, pues comienzan a reconocer pulsaciones nada más encender el ordenador, lo que quiere decir que pueden capturar los datos de conexión iniciales.

Consejos de protección

Para detectar keyloggers de hardware fíjese en todos los dispositivos que estén conectados físicamente al ordenador y asegúrese de saber por qué está ahí cada uno de ellos. También merece la pena recordar que el keylogger de software se ejecuta de manera invisible en segundo plano, pues es otra forma de malware. Para más consejos de protección, vaya a la letra M (malware).

L

Nombre de la amenaza

LastPass

En 2015, un investigador de seguridad hizo pública una herramienta capaz de robar datos confidenciales a la empresa de servicio de contraseñas LastPass.

Descripción

Aunque no se robaron las contraseñas almacenadas durante este hackeo, los delincuentes accedieron a las direcciones de correo electrónico, recordatorios de contraseñas y registros criptográficos de autenticación de LastPass. Aunque LastPass afirmó creer que no se había accedido a ninguna cuenta de usuario en este ataque, aconsejaron a todos los clientes que cambiaran sus contraseñas maestras.

¿Cómo funciona?

Al igual que la mayoría de gestores de contraseñas, LastPass almacenaba las contraseñas maestras de sus clientes en la nube, en una caja fuerte cifrada. La caja fuerte estaba protegida por un solo nombre de usuario y contraseña. Este ataque se basó en que un usuario visitó un sitio web malicioso, para luego detectar si el navegador utilizaba LastPass. Una vez detectado, imitó una notificación de LastPass, desconectó al usuario y luego le pidió su contraseña y clave de autenticación de dos factores. Este método se conoce como ‘phishing’.

Consejos de protección

Para recabar consejos de protección de contraseñas véase la letra C (contraseñas) y la I (ingeniería social).

M

Nombre de la amenaza

Malware

El malware o, 'software malicioso', es un programa o líneas de código colocados en un sistema informático con fines delictivos. También se lo conoce como virus informático.

Descripción

El malware adopta muchas formas, desde troyanos véase la letra T) al ransomware (véase la letra R). Cuando el malware hizo sus primeras apariciones allá por las décadas de 1980 y 1990, se solía utilizar para cometer actos de vandalismo, destruir ordenadores o mostrar mensajes de burla.

Hoy en día, en cambio, es mucho más siniestro y lo suelen utilizar bandas de ciberdelincuentes con el fin de lucrarse. Gracias al auge de Internet y a los mercados anónimos de la 'dark web' o Internet oscura, los hackers pueden comprar y vender malware ya preparado, listo para implantar en los ordenadores de sus víctimas.

El objetivo de la mayor parte del malware es enriquecer a sus creadores a través de tácticas como extorsionar a la víctima a cambio de dinero o hacerse con su información personal, nombres de usuarios y contraseñas, y venderlos en línea.

¿Cómo funciona?

El malware se puede distribuir de muchas maneras diferentes. Una de las más comunes es a través de un código incrustado en adjuntos de correo electrónico. Los hackers envían a la víctima un correo para intentar engañarle y que abra el archivo adjunto. Es lo que se conoce como 'phishing'.

También se puede instalar por medio de una 'descarga involuntaria', cuando se engaña a la víctima para que visite un sitio web que contiene malware. Estos sitios web suelen estar diseñados para que se parezcan a sitios web que conoce y en los que confía, como redes sociales o páginas de bancos. Otro método habitual de distribución es el de incluir el malware dentro de otro archivo o elemento de software que se decide descargar. Barras de herramientas de navegadores, protectores de pantallas y descargas ilegales de música y películas son ejemplos populares de esta táctica.

Consejos de protección

Para recabar consejos de protección de contraseñas vaya a la letra C (contraseñas) y a la I (ingeniería social).

N

Nombre de la amenaza

Nube

La Nube o The Claud en inglés, es una tecnología que permite el almacenamiento de datos y ofrecer servicios a través de un servidor externo.

Descripción

El Cloud Computing (término completo en inglés) se basa en una tecnología que, por un lado permite trasladar archivos y programas propios a un conjunto de servidores a los que se puede acceder a través de Internet, y por otro lado ofrecer servicios alojados en estos servidores de tal forma que su acceso sea a través de sistemas digitales. En ambos casos La Nube permite reducir costes y espacio de almacenamiento, acceder a los datos y servicios desde cualquier sitio y dispositivo y escalar el servicio a las necesidades del momento.

¿Cómo funciona?

Su funcionamiento se fundamenta en dos entornos, el primero en el que entra en juego el ordenador u ordenadores de la persona que usa el servicio de La Nube y el programa que usa para acceder. El segundo entorno está compuesto por los ordenadores, servidores y sistemas de almacenamiento que conforman La Nube. Cada uno de estos elementos está unido a un servidor central que se encarga de controlar el tráfico para dar respuesta a los usuarios que usan el servicio.

Consejos de protección

Al estar vinculado a Internet, el uso de este servicio tiene sus peligros, pero hay métodos para protegerse; realice copias de seguridad de forma periódica, suba información encriptada (véase E encriptar), cambie las contraseñas con frecuencia e infórmese de las medidas de protección que tengan los posibles servicios alojados en La Nube que vaya a contratar.

P

Nombre de la amenaza

Puerta Trasera

Los ‘backdoor trojans’ permiten a los hackers tomar el control del ordenador de alguien sin su permiso a través de Internet

Descripción

Los virus troyanos han sido bastante mediáticos en los últimos años, con casos como por ejemplo Skype y Readers Digest como ejemplos notables. Tanto los sistemas de Windows como Mac han caído víctimas de los ataques de troyanos. Los hackers a menudo los dejan ‘durmientes’ durante muchos años antes de activarlos.

Entre los incidentes más recientes figuran; BackDoor. TeamViewer.49 (que se disfraza como una actualización de Adobe Flash Player), Bayrob (descubierto por primera vez en 2007 con el fin de robar información sensible) y Pinkslipbot (capaz de robar datos bancarios, contraseñas de correo electrónico y certificados digitales).

¿Cómo funciona?

El malware troyano se disfraza a menudo de software legítimo y permite a los hackers hacer cosas como espiar, robar datos personales o acceder y controlar sistemas. Los ‘backdoor trojans’ proporcionan a los ciberdelincuentes acceso remoto al ordenador infectado, lo que les permite hacer cualquier cosa que quieran – como enviar y recibir archivos, ejecutar programas o reiniciar el ordenador– como si fueran el administrador del sistema.

Los ‘backdoor trojans’ suelen contener también amenazas añadidas como registro de pulsaciones en el teclado (por el que un dispositivo o elemento de software registra todas las acciones que se llevan a cabo en el teclado), capturas de pantalla y cifrado de ficheros, todo combinado forma una grave amenaza para la seguridad que es casi imposible de detectar.

A menudo, se utilizan para unir un grupo de ordenadores y formar lo que se conoce como ‘botnet’ o ‘red zombi’ que se puede explotar para fines delictivos. Los ‘backdoor trojans’ suelen obtener acceso a un ordenador a través de técnicas de ‘ingeniería social’ (véase la letra I) mediante las que se persuade a los usuarios a hacer clic en un enlace de un correo spam o visitar un sitio web que afecta a su seguridad.

Consejos de protección

La mejor manera de protegerse frente los ‘backdoor trojans’ y del malware troyano es mantener al día todos los ordenadores de la red con los parches más actualizados ya que solucionan las vulnerabilidades conocidas del sistema. Debería también instalar un software antivirus y anti-spam efectivo, y además, no abrir nunca correos electrónicos que parezcan spam. Para identificarlos, observe si encuentra una gramática deficiente y errores ortográficos o una redacción intimidante o apremiante, pues son indicios claros de que no son fiables. Si cree que ha abierto un correo spam, no abra los adjuntos ni haga clic en enlaces a sitios web externos.

R

Nombre de la amenaza

Ransomware

Ransomware es un tipo de malware que permite a los hackers chantajear a un usuario restringiéndole el acceso a un sistema informático infectado.

Descripción

El ransomware se ha convertido en una amenaza generalizada, en constante evolución para la ciberseguridad e incluso algunos expertos lo describen como una epidemia. Según Kaspersky cerca de 950.000 usuarios únicos fueron víctimas de ataques 'Ransomware' en 2017 de los cuales 26% afectaron a empresas. Hay dos tipos de ransomware, ransomware de bloqueo de pantalla y ransomware de cifrado, siendo este último uno de los tipos de malware más peligrosos creados jamás.

¿Cómo funciona?

El ransomware se suele extender por medio de un troyano (véase la letra T) que infecta el sistema a través de un archivo descargado o una vulnerabilidad de la red (véase la letra V). Una vez dentro del sistema, el troyano ejecuta la carga del ransomware, que es el que realiza la acción maliciosa.

En el caso del ransomware de bloqueo de pantalla, se muestra un mensaje a toda pantalla que impide al usuario utilizar el ordenador y acceder a sus archivos. Da instrucciones al usuario de pagar una cantidad de dinero para recuperar el acceso y la funcionalidad de su ordenador.

El ransomware de cifrado, o cripto-ransomware, cifra archivos del usuario o datos de alto valor y pide de nuevo una cantidad de dinero a cambio de una clave de descifrado. El uso de este tipo de ransomware ha aumentado enormemente por parte de los hackers que pretenden extorsionar a sus víctimas a cambio de dinero, con el ejemplo destacado de CryptoLocker. Tomando como diana los ordenadores que ejecutaban Microsoft Windows, CryptoLocker llegó a Internet en septiembre de 2013 y se informa que ha conseguido extorsionar a sus víctimas obteniendo unas 271.679€.

En el caso del ransomware, la extorsión es el objetivo y los hackers suelen utilizar tácticas de scareware con el fin de obligar al pago. Los programas de scareware están concebidos para manipular al usuario, generalmente mediante el despliegue de tácticas de choque, de manera que la víctima cumpla lo que pide el ransomware. Por ejemplo, el programa de scareware puede mostrar un mensaje que procede en apariencia de la policía sobre actividades ilegales en el ordenador. Esta táctica funciona de dos maneras: obliga a la víctima a pagar y evita además que le cuente a otras personas lo del mensaje en pantalla, pues el contenido es embarazoso o perjudicial para su reputación.

Consejos de protección

Siga esta sencilla regla: en caso de duda, no haga clic. No haga clic en correos electrónicos o adjuntos de gente que no conozca, no visite sitios web no seguros o falsos y no haga clic en enlaces dudosos en medios sociales. Asegúrese de hacer copia de respaldo de su ordenador, utilice una solución de seguridad fiable y mantenga actualizado el software informático.

R

Nombre de la amenaza

Reglamento General de Protección de Datos (RGPD)

El Reglamento General de Protección de Datos (RGPD) armoniza la legislación de protección de datos en el ámbito europeo, aumentando las responsabilidades y niveles de sanciones que se imponen a las organizaciones que cometan errores en el tratamiento de datos personales sensibles.

Description

La nueva RGPD que entró en vigor en mayo 2018 a nivel europeo sustituye al reglamento de protección de datos anterior, que se desarrolló originariamente como parte de la normativa europea en 1995.

¿Cómo funciona?

Unido al acuerdo reciente de la Directiva relativa a la Seguridad de las Redes y Sistemas de Información (NISD), una poderosa fuerza de cambio en materia de ciberseguridad recorre ahora toda Europa. La amenaza de multa, que podría ser ni más ni menos que del 4% de los ingresos globales, debería impulsar cambios de comportamiento reales en lo que se refiere a que las organizaciones garanticen la seguridad de los datos sensibles. La RGPD se aplica a cualquier empresa que opere en Europa. Con esta ley las direcciones IP, las cookies y las etiquetas de identificación mediante radiofrecuencia (RFID), así como los datos médicos, incluidos los de tipo genético, se tratan ahora como información personal sensible. Esto podría suponer un reto para algunas empresas.

El RGPD supone asimismo que el 'derecho al olvido' está amparado por ley. De esta manera, los consumidores tendrán ahora el derecho a pedir a una empresa que suprima su información de sus bases de datos y sistemas y las empresas tienen que cumplir esa petición.

R

Nombre de la amenaza

Respuesta a Incidentes

Una respuesta al incidente es un enfoque organizado sobre cómo afrontar y gestionar las consecuencias de un fallo de seguridad o de un ataque.

Descripción

El objetivo de una respuesta al incidente es gestionar una situación volátil en el que se ha producido un fallo de la seguridad de manera que se limiten los daños causados, el tiempo de recuperación y los costes. Se podrá declarar un incidente cuando resulte obvio que un sistema ha sufrido pérdida de datos o ha habido una interrupción de las operaciones. El plan de respuesta al incidente incluye una política que define los elementos constitutivos del mismo y dispone un proceso que se debe seguir paso a paso en cuanto se produzca dicho incidente.

¿Cómo funciona?

El equipo de respuesta a incidentes está formado normalmente por personal de los departamentos de TI, Seguridad, Jurídico, Recursos Humanos y Relaciones Públicas. Su cometido es establecer si se ha producido un incidente de seguridad o no, y contener a continuación el ataque para impedir que continúe extendiéndose. Una vez contenido, el equipo se centra en encontrar la raíz del problema y erradicarlo. Por último, propondrá cuándo restaurar los sistemas hasta devolverlos a su estado operativo.

Los incidentes pueden salir a la luz tras un análisis de carácter preventivo, lo que se denomina ir a la 'caza' de ataques. También cuando se encuentra información confidencial fuera de la organización o los atacantes 'tumban' los sistemas.

Consejos de protección

Una forma de proteger la empresa de los ataques online es formar a todo el personal en las medidas de seguridad internas. Y es aconsejable tener por si acaso una estrategia alternativa. Encontrará más consejos sobre cómo protegerse consulten la letra I (ingeniería social) y la C (contraseñas).

S

Nombre de la amenaza

Software publicitario

‘Adware’ hace referencia a los banners de publicidad que se muestran dentro de aplicaciones de software. Su autor escribe un código extra dentro del software que muestra los anuncios mientras se está ejecutando la aplicación.

Descripción

Uno de los fallos de ciberseguridad más sonados relacionados con adware se produjo en 2015 cuando se supo que la multinacional de tecnología, Lenovo, estaba preinstalando un tipo de adware al que se llamó ‘Superfish’. El adware emitía e instalaba sus propios certificados de seguridad, lo que le permitía interceptar la información que enviaba y recibía el dispositivo del usuario, poniéndole en mayor riesgo.

Lenovo se vio obligada a lanzar una actualización de software y un tutorial explicando cómo eliminar el programa Superfish y el escándalo perjudicó gravemente a la reputación de la empresa.

También se ha descubierto adware en la Google Play Store, por ejemplo Android.Spy.510, que funcionaba mostrando anuncios encima de las aplicaciones normales.

¿Cómo funciona?

Una vez instalado en el dispositivo, el adware muestra automáticamente anuncios no deseados con el fin de generar ingresos para la marca, además de recopilar datos de marketing y otra información sin el conocimiento del usuario. Lo delicado del adware es que suele estar sin proteger, por lo que puede resultar muy lucrativo para los ciberdelincuentes.

No todo el adware es malo, pero algunas variaciones socavan los ajustes de seguridad y muestran anuncios que luego pueden explotar hackers más peligrosos. La infección puede tener diversos efectos, en función del tipo de adware, pero entre los más comunes figuran la ralentización del dispositivo, la aparición incesante de ventanas emergentes o pop-ups (que son tan molestas como suenan) y el seguimiento permanente de las actividades online, lo que se conoce como ‘spying’ o espionaje.

Consejos de protección

La forma más común de contagiarse con adware es descargando freeware o shareware que lo lleve integrado o visitando un sitio web infectado. Los primeros pasos para protegerse deberían ser; evitar descargar programas de sitios web que no conozca y lo mismo con el software, salvo que sea absolutamente necesario.

Aparte de eso, puede comprar herramientas específicas para eliminar el adware que ofrecen la mayoría de fabricantes de software de seguridad y asegúrese de analizar los dispositivos periódicamente en busca de posibles virus.

T

Nombre de la amenaza

Troyanos

Aunque venga disfrazado a menudo de software legal, un troyano o caballo de Troya es un malware que oculta una intención maliciosa con el fin hackear un ordenador.

Descripción

El término troyano con que se denomina a esta forma de malware procede de la famosa historia de la Antigua Grecia, en la que los griegos engañaron a los troyanos con un enorme caballo de madera. La expresión 'Caballo de Troya' en nuestros días sirve para describir cualquier ardid o engaño que hace que alguien invite a un enemigo a un lugar seguro, y el malware troyano es ese tipo de engaño. Si el troyano se instala correctamente, el malware suele tener acceso completo al sistema. Con este acceso ilimitado, el hacker puede hacer cosas muy diversas: destruir el ordenador, reclutar la máquina para que forme parte de un botnet (una red de ordenadores particulares infectados con software malicioso y controlados como grupo), robar datos, instalar ransomware o espiar al usuario.

¿Cómo funciona?

Lo más frecuente es que se utilice una técnica de ingeniería social (véase la letra I) para engañar a los usuarios y que carguen y ejecuten troyanos en su ordenador. Por ejemplo, un usuario puede bajarse sin darse cuenta un troyano mediante descarga involuntaria, o se le puede engañar para que abra un adjunto en un sencillo correo electrónico. La carga o acción del troyano dependerá de para qué esté diseñado: un troyano de puerta trasera (véase la letra P) entrega a los hackers el control a distancia sobre el ordenador infectado, mientras que un troyano banquero roba los datos de cuenta de banca en línea y sistemas de pago electrónico.

Consejos de protección

El primer paso para protegerse contra los troyanos es instalar un producto anti-malware fiable y efectivo. Un buen producto anti-malware debería detectar e impedir que los troyanos ataquen su ordenador y dispositivos. También es aconsejable utilizar un proveedor de servicios de Internet que posea sólidos procedimientos anti-spam y anti-phishing.

Como los troyanos se distribuyen por medio de ingeniería social, es importante evitar cualquier cosa que tenga apariencia maliciosa, esté fuera de lugar o no proceda de una fuente digna de confianza. Recuerde: si no está seguro, no haga clic.

T

Nombre de la amenaza

Trampa/ Honeypot

‘Honeypot’ es un proceso avanzado de ciberdefensa por el que se monta un sistema informático como señuelo para atraer a los ciberatacantes. El sistema se utiliza para detectar, desviar y estudiar las estrategias que se emplean para acceder a los sistemas de información.

Descripción

Un honeypot necesita un ordenador, representado a menudo como una red de máquinas virtuales, junto con aplicaciones y datos capaces de simular el comportamiento de sistemas reales que parezcan formar parte de una red. En realidad, ese sistema está aislado minuciosamente y es objeto de vigilancia muy estrecha.

¿Cómo funciona?

Los honeypots pueden facilitar un análisis inmediato de la actividad de los hackers y de cómo estos evolucionan y progresan, proporcionando a las organizaciones conocimientos sobre cómo proteger mejor sus sistemas. Los honeypots se pueden utilizar también como sistemas de detección de la red, al constituir una forma de alarma cuando penetra un intruso en el sistema. Están diseñados deliberadamente para parecer reales y contienen información de interés para atraer y mantener ocupados a los hackers.

U

Nombre de la amenaza

URL

Las siglas URL provienen de la palabra en inglés Uniform Resource Locator, sirve para denominar recursos en Internet de tal forma que sirva a modo de identificador único.

Descripción

Una URL es una dirección específica que se asigna a cada uno de los recursos disponibles en la red (WWW). Documentos, imágenes y webs que se suban a la World Wide Web tendrán este identificador único que funciona a modo de link o enlace.

¿Cómo funciona?

Cada URL está formada por un conjunto de caracteres que permiten asignar una dirección exclusiva a cada elemento. Dentro de cada URL existen diferentes partes que la componen, la primera parte se denomina protocolo de acceso, por ejemplo https://, a esta le sigue la dirección del recurso, 'www' es una de ellas, a continuación viene el dominio, en el caso de Hiscox sería hiscox y por último el tipo de dominio, .com y .es son los más comunes en España.

Consejos de protección

Muchos de los ciberataques comienzan con una URL, es importante identificar las que pueden llegar a ser maliciosas. Lo más importante es asegurarse de que el dominio es conocido y seguro, muchas veces los ciberdelincuentes pueden asemejar las URL a las originales con el fin de engañar, ya que en Internet leemos muy rápido, por esto e importante augurarse de que está compuesta por toda las partes necesarias y que el origen es fiable.

V

Nombre de la amenaza

Vulnerabilidades

En este contexto, el término ‘vulnerabilidades’ hace referencia a errores en los programas de software que dejan los ordenadores abiertos al hackeo.

Descripción

Una de las vulnerabilidades más famosas de los últimos tiempos es Heartbleed. Se trata de una vulnerabilidad grave en el popular software OpenSSL, que se utiliza para asegurar las comunicaciones entre ordenadores. Cuando la vulnerabilidad salió a la luz en abril de 2014, se cree que cerca de medio millón de servidores web seguros eran vulnerables.

¿Cómo funciona?

Las vulnerabilidades pueden ser fallos de diseño o errores de programación incluidos en el código de un elemento de software. Se pueden explotar de muy distintas maneras. Heartbleed fue especialmente peligrosa, pues exponía las contraseñas y las credenciales de conexión, así como las claves secretas utilizadas para mantener segura esta información sensible.

Consejos de protección

Para protegerse de las vulnerabilidades, es buena idea actualizar el software cada vez que haya nuevas versiones disponibles, y descargar los parches que se publiquen para el mismo. Si tiene algún software sin que reciba ya asistencia técnica por parte del fabricante, se deberán activar reglas restrictivas de cortafuegos para impedir que el ordenador conectado a la red acceda a Internet, y que otros ordenadores conectados accedan al servicio vulnerable.

V

Nombre de la amenaza

Vandalismo Web

Por vandalismo web se entiende cuando un hacker accede al sitio web de alguien sin que este lo sepa y lo desconfigura.

Descripción

El vandalismo web se podría ver como una especie de 'grafiti electrónico' que pueden utilizar los 'hacktivistas' para difundir mensajes con motivaciones políticas o, en algunos casos, para encubrir otros comportamientos maliciosos que el hacker está llevando a cabo en otra parte del servidor.

En 2012, la página de Pakistán de Google, Google.com.pk, fue objeto de vandalismo junto con cientos de otros dominios .pk (dominios alojados en Pakistán). En la página de Google, quitaron el logotipo y lo sustituyeron por una imagen de dos pingüinos. Pero no hay que ir muy lejos, en España un grupo de hacktivistas clonó la web oficial del referéndum sobre la independencia de Catalunya el 1 de Octubre 2017 cuando las originales se cerraron por orden judicial.

¿Cómo funciona?

Un hacker accede a un servidor web aprovechando una vulnerabilidad o con ayuda de credenciales débiles, tras lo cual es libre para cambiar el contenido del sitio web de la manera que quiera.

Consejos de protección

Para protegerse del vandalismo web, debe asegurarse de que:

- el sistema operativo y el software están actualizados.
- los sistemas de archivo utilizados para almacenar contenido estático en los servidores web están configurados como de solo lectura.
- la bases de datos que alberguen contenido web son seguras, en zonas independientes desmilitarizadas (sistemas de red internos con acceso limitado por parte de las personas ajenas a una organización).

También puede implantar una autenticación más fuerte (como la autorización de dos factores, en la que se utiliza seguridad como un código texto junto con una contraseña para entrar) para que los administradores puedan realizar cambios. Por último, la supervisión de la integridad de los archivos –un control o proceso interno que valida la integridad de los archivos del sistema operativo y del software de aplicaciones– puede alertar a los administradores cada vez que algo cambie.

W

Nombre de la amenaza

Wanna Cry

Wanna Cry es un tipo de virus clasificado como ransomware (véase R ransomware) cuyo objetivo es encriptar los datos de un dispositivo electrónico para pedir un rescate para hacerlos accesibles de nuevo. Ha llegado a infectar a más de 230.000 equipos en todo el mundo.

Descripción

El virus Wanna Cry es un ransomware que encripta los datos para posteriormente pedir un rescate por desencriptarlos, en el caso de Wanna Cry el rescate es de 300$ en Bitcoins. Este virus ha atacado a los dispositivos con sistema operativo Windows que no tenían la última actualización del sistema. Se ha hecho tan famoso por la gran extensión que ha tenido, las empresas e instituciones que ha afectado y los países en los que ha atacado.

¿Cómo funciona?

A raíz de un email con links o archivos maliciosos, accede a los dispositivos, una vez dentro se extiende como un gusano (véase G gusano) por toda la red interna y busca vulnerabilidades a las que poder atacar, una vez infectados los equipos pasa a cifrar los archivos. Cuándo esto ha sucedido, se recibe un mensaje avisando de que no se puede acceder a los archivos o incluso no se puede iniciar sesión, para poder hacerlo se pide un rescate.

Consejos de protección

El cifrado de Wanna Cry es especialmente complejo, es por esto que es preferible evitar el ataque. Usar un software antimalware es una muy buena forma de protegerse, pero es muy recomendable realizar copias de seguridad periódicas, para que, en el caso de que su equipo resulte infectado, pueda recuperar los datos sin problema. Es importante actualizar con los últimos parches de seguridad y no clicar en enlaces o descargarse archivos sospechosos. Siempre hay que comprobar que el email y la fuente son fiables.

X

Nombre de la amenaza

XSS

El cross-site scripting, abreviado XSS, hace referencia a un tipo de vulnerabilidad de seguridad informática que es habitual en aplicaciones web.

Descripción

XSS es un ataque de inyección de código, por el que un atacante puede ejecutar scripts maliciosos dentro de un sitio web o de una aplicación web. Al incrustar el script malicioso, o la 'carga' dentro de la información que se envía a las páginas web, el atacante puede conseguir que el navegador de la víctima ejecute el código malicioso. Hay dos variantes habituales de XSS: almacenado o rechazado. Un ataque de XSS almacenado quiere decir que la carga maliciosa (la parte del malware que lleva a cabo la actividad maliciosa) está almacenada en el sitio web de manera permanente. Un ataque de XSS rechazado quiere decir que la carga es de tipo singular, y que el usuario tiene que cargar un enlace que el atacante le envía.

¿Cómo funciona?

Si algo que envía el usuario al servidor web se puede devolver desde una página web diferente, como dejar un comentario en un vídeo, el sitio web podría ser vulnerable a un ataque XSS. Si el atacante introduce datos que se puedan representar como parte del código del sitio web, también el sitio es vulnerable a un ataque XSS. Para evitarlo se debe 'desinfectar' la información que se envía al servidor web o desde este, de manera que no contenga nada que se pueda interpretar como código.

Consejos de protección

Tanto el XSS almacenado como rechazado se pueden resolver llevando a cabo la validación y las salidas adecuadas en el lado del servidor. A la hora de desarrollar aplicaciones web, es una buena norma dar por supuesto que todos los datos recibidos por la aplicación proceden de una fuente no autorizada. Por tanto, hay que validar el tipo, longitud, formato y el rango de los datos que procedan de un formulario web al script de una aplicación, y luego codificarlos antes de volver a mostrarlo en una página dinámica. Antes de activar u sitio o una aplicación al público, hay que pasarle un test de infiltración con el fin de detectar fallos de XSS.

Y

Nombre de la amenaza

YTCracker

Bryce Case Jnr., alias ‘YTCCracker’, es un antiguo hacker convertido en artista de hip hop, al que se conoce más por desconfigurar varios sitios web de la administración norteamericana.

Descripción

Desde 1999, cuando era un estudiante de secundaria de diecisiete años, YTCracker desconfiguró numerosos sitios web, incluidos los del Centro de Vuelos Espaciales Goddard de la NASA, el centro de formación nacional de la Agencia de Gestión del Suelo, la Agencia de Auditoría de Contratos de Defensa, Airspace USA, Altamira, Nissan Motors, Honda, la estación de vigilancia de Estudios Geológicos de los Estados Unidos y el Departamento de Seguridad Pública de Texas.

Pese a declarar que había entrado en los sitios web con el fin de alertarles de los problemas de seguridad más que con intenciones maliciosas, en mayo de 2000 se le condenó por delito doloso en perjuicio de la administración pública y delito informático por irrumpir en el sitio web de la ciudad de Colorado Springs, causando daños por un importe estimado de 25.000 $.

¿Cómo funciona?

Cuando desfiguró el Centro de Vuelos Espaciales Goddard de la NASA mediante un grafiti digital, YTCracker utilizó una fachada modificada de un exploit (fragmentos de software) convencional, msadc.pl. Estos fragmentos de software aprovechan un fallo de seguridad, una vulnerabilidad de software, por medio de un script de ataque. En este caso, el hacker lo hizo para hacerse con la portada del sitio web. La página que colocó mostraba una caricatura de un encapuchado con un símbolo de la paz, junto con un mensaje que advertía de los peligros de los fallos de seguridad de los sitios web y de los ciberataques.

Consejos de protección

Para protegerse de hackers como YTCracker, asegúrese de que las redes y sistemas superan tests periódicos de infiltración: un test de infiltración es un ataque concertado previamente contra un sistema informático en busca de debilidades de seguridad. Y manténgase al día con los parches de software y las actualizaciones de versión que hayan salido.

Z

Nombre de la amenaza

Zombie

Un zombi es un ordenador conectado a Internet tomado por un hacker o un virus, y que se puede controlar a distancia con el fin de realizar actividades maliciosas.

Descripción

Hay un gran mercado en torno a controlar los ordenadores de otras personas sin su consentimiento. Los hackers infectan miles de máquinas para poder controlarlas a distancia. Así forman una red de 'zombis' denominada 'botnet'.

¿Cómo funciona?

Los dueños no suelen ser conscientes de que sus máquinas se han convertido en zombis. La infección suele estar automatizada, por lo que probablemente la mayoría de los integrantes de la botnet hayan ejecutado un programa que no deberían tener, o no hayan aplicado los parches correspondientes.

Una vez infectados, los zombis se pueden utilizar para lo que quiera el hacker. Pueden servir para echar abajo sitios web bombardeándoles con tráfico hasta que los servidores colapsan, o para enviar spam, o infectar más máquinas. Una vez que el hacker ha terminado, puede vender su botnet a otra persona.

Consejos de protección

Para proteger un ordenador y evitar que se convierta en zombi, instale/actualice el software anti-virus y asegúrese de tener un cortafuegos. Puede intentar vigilar todo el tráfico entrante y saliente para identificar peticiones repetidas de la misma aplicación dirigidas a un cierto número de destinos: suele ser indicio de una aplicación zombi. También es buena idea borrar los mensajes de spam sin abrirlos, y no abrir nunca los adjuntos. Evite descargar aplicaciones que no procedan de una fuente de confianza. Si cree que el ordenador está infectado y quiere asegurarse de que no queda rastro de su pasado zombi, tendría sentido hacer una copia de respaldo de los archivos, formatear el disco duro y reinstalar el sistema operativo desde cero.

Hiscox SA
Paseo de la Castellana
60, 7ª Planta, 28046
Madrid

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

19787 02/19

Una exhaustiva guía de ciberseguridad para empresas.
www.hiscox.es/blog

HISCOX