CID
COMPETENCIAS EN INFORMACIÓN DIGITAL

SEGURIDAD INFORMÁTICA

BUA
Biblioteca de la Universitat d' Alacant
Biblioteca de la Universidad de Alicante

Universitat d'Alacant
Universidad de Alicante

SEGURIDAD INFORMÁTICA

Objetivos

- Conocer el concepto de seguridad informática
- Saber qué es una vulnerabilidad informática
- Conocer las principales amenazas lógicas de los sistemas informáticos y cómo actúan
- Comprender los riesgos que supone la navegación en internet y el uso del correo electrónico

SEGURIDAD INFORMÁTICA

Cuando hablamos de seguridad informática nos estamos refiriendo, en lo fundamental, a la protección de la información digital y de los dispositivos y redes de comunicación frente a cualquier tipo de amenaza, entendiendo por tal todo aquél factor que pueda afectar al desempeño directo del sistema informático o de la información y resultados obtenidos del mismo.

En resumidas cuentas, la seguridad informática tiene por fin proteger la integridad y privacidad de la información almacenada o tratada por un sistema informático frente a cualquier amenaza.

"El único sistema seguro es aquel que está apagado y desconectado, enterrado en un refugio de hormigón, rodeado por gas venenoso y custodiado por guardianes bien pagados y muy bien armados. Aún así, yo no apostaría mi vida por él" (Eugene Spafford, experto en seguridad de datos)..

Aunque ningún sistema puede considerarse seguro al 100%, sí que podemos aplicar una serie de protocolos, normas, restricciones, políticas de acceso y planes de contingencia que permitan mantener la seguridad en un nivel óptimo. Además, como suele ocurrir en la mayoría de ámbitos relacionados con la seguridad, uno de los factores fundamentales a tener en cuenta sigue siendo la formación de las personas usuarias, para que conociendo cómo protegerse de las amenazas, sepan utilizar los recursos de que dispone de la mejor manera posible.

El factor humano es fundamental para lograr un nivel de seguridad óptimo

Otros expertos, dado que hablar de seguridad en términos absolutos es imposible, prefieren hablar de Fiabilidad del sistema.

Fiabilidad es la probabilidad de que un sistema se comporte tal y como se espera de él.

En el blog del Servicio de Informática de la Universidad de Alicante hay entradas acerca de la seguridad que pueden resultarte de interés como información complementaria a este tema.

Puedes consultar las entradas relacionadas con temas de seguridad en el siguiente enlace http://blogs.ua.es/si/tag/seguridad/.

Características de un sistema seguro

Los sistemas informáticos seguros cumplen estas características:

1. Integridad
2. Confidencialidad
3. Disponibilidad
4. Autenticación
5. Irretutabilidad (No-Rechazo o No Repudio)

A continuación, veremos estos puntos con más detenimiento

1 - INTEGRIDAD

La información no puede ser modificada por quien no esté autorizado. La información ha de mantenerse con exactitud, tal cual fue generada, sin ser alterada por personas o procesos informáticos no autorizados para ello.

Se produce una violación de la integridad cuando una persona, aplicación o proceso modifica o borra datos importantes, bien accidentalmente, bien de forma dolosa.

La modificación de los datos por personas autorizadas debe quedar registrada, asegurando su precisión y confiabilidad.
¿Cómo podemos asegurar la integridad de la información contenida en un mensaje? Pues adjuntando un conjunto de datos (metadatos) de comprobación de esa integridad.

La firma digital es uno de los pilares de la seguridad de la información

2 - CONFIDENCIALIDAD

Los datos sólo pueden ser legibles para las personas autorizadas; la información no ha de divulgarse a personas, entidades o procesos no autorizados.

La pérdida o violación de la confidencialidad de la información puede adoptar múltiples formas, no todas relacionadas con medios informáticos: puede producirse, por ejemplo, cuando alguien mira por encima de nuestras espaldas mientras tenemos información confidencial en la pantalla, o si en una transacción electrónica el número de nuestra tarjeta de crédito no se envía cifrado.

3 - DISPONIBILIDAD

La información ha de estar disponible para las personas, procesos o aplicaciones que deban acceder a ella en el momento en el que lo requieran.

Hablamos de alta disponibilidad cuando un sistema está implementado o diseñado de tal manera que garantiza la continuidad operacional absoluta durante un periodo de tiempo dado, es decir, que se garantiza que el sistema esté disponible en todo momento, evitando cualquier interrupción del servicio (ya sea por cortes de energía, fallos del hardware o problemas de software).

4 - AUTENTICACIÓN

El generador de la información, o el que acceda o la edite, ha de estar perfectamente identificado en todo momento, de forma unívoca e inequívoca.

En los sistemas informáticos, la autenticación se implementa mediante una combinación de cuentas de la persona usuaria (que gradúa el privilegio de acceso a los distintos niveles de información) y contraseña de acceso.

5 – IRREFUTABILIDAD (NO-RECHAZO O NO-REPUDIO)

En caso de participar en un proceso de comunicación, podemos hablar de:

- no repudio de origen: la persona emisora no puede negar que realizó un envío porque la persona receptora tiene una prueba infalsificable del origen del envío.
- no repudio de destino: la persona receptora no puede negar que recibió el mensaje porque la persona emisora tiene pruebas de la recepción.

El no repudio evita que la persona emisora o la persona receptora puedan negar la transmisión de un mensaje.

La seguridad informática, por tanto, protege la integridad, confidenciabilidad y disponibilidad de la información.

Vulnerabilidades

Una vulnerabilidad es la debilidad de cualquier tipo que compromete la seguridad de un sistema informático.

Hace falta aclarar también que esa vulnerabilidad es usualmente desconocida tanto para las personas programadoras del software como para el gran público (que ignoran que tienen una brecha potencialmente peligrosa en sus sistemas), pero no así para los potenciales atacantes, entre los cuales sí circulan listados con estas vulnerabilidades. Entonces, ¿qué es exactamente una vulnerabilidad?

Para construirnos una imagen mental más clara, podemos representarnos el software informático como una malla metálica compuesta por millones de líneas de código entretejidas. Pero ojo, en el caso del software, esta malla no sería plana, sino tridimensional, con un nivel de complejidad notable.

Esta complejidad dificulta la tarea de encontrar fallos, puntos débiles o funciones erróneas dentro del código, de tal manera que estos errores suelen escapar a las complejas herramientas de verificación automatizada del código.

¿Cómo se encuentran entonces estos puntos débiles, estas vulnerabilidades del código? Pues

- por un análisis minucioso y detallado
- por un uso indebido
- sencillamente, de manera accidental.

Cuando se produce una vulnerabilidad, el punto débil generado puede causar que los programas o los sistemas operativos se comporten de manera extraña, no deseada o no planificada.

Un atacante que conozca esta vulnerabilidad puede utilizar este comportamiento extraño (y, por tanto, no deseado) para crear una brecha por donde penetrar en el sistema y lograr que se ejecute su código malicioso, o apoderarse de información sensible.

Clasificación de las amenazas informáticas

De forma general, podemos agrupar las amenazas informáticas en dos bloques principales:

- Amenazas físicas
- Amenazas lógicas

Estas amenazas, tanto físicas como lógicas, son materializadas básicamente por:

- Personas
- Programas o aplicaciones específicas
- Catástrofes naturales

Mucho más sencillo que acceder a un sistema bien protegido es acceder (y engañar o manipular) a las personas que tienen acceso al mismo

INGENIERÍA SOCIAL

La ingeniería social es la práctica de obtener información confidencial mediante la manipulación de usuarios con acceso al sistema.

Contra lo que pudiera parecer, el punto más débil en la seguridad de los sistemas informáticos es el factor humano: suele ser mucho más fácil obtener acceso a un sistema

gracias a la manipulación y el engaño de las personas que mediante ataques informáticos de fuerza bruta.

Recuerda: En cualquier sistema, las personas usuarias siempre son el eslabón más débil.

Según el famoso hacker Kevin Mitnick, la ingeniería social tiene su base en cuatro elementales principios:

- Todos queremos ayudar
- No nos gusta decir NO
- La primera actitud suele ser la de confiar en la otra persona
- A todas las personas nos gusta ser alabadas

Técnicas de Ingeniería Social

1 - Pretextos

Se crea un escenario ficticio para que la víctima revele una información que, en circunstancias normales, no revelaría.

Normalmente la creación de escenarios ficticios requiere una investigación previa de la víctima para conseguir datos personales sensibles y hacer así más creible la suplantación y hacer creer a las víctima que es legítima.

2 – Shoulder Surfing

Consiste en espiar físicamente a las personas usuarias hasta poder obtener las claves de acceso al sistema.

El caso típico es el de las personas usuarias que apuntan sus contraseñas de acceso en un papel junto al monitor pegadas al teclado

3 – Phising (Suplantación de la personalidad)

El o la atacante se hace pasar por una persona o empresa de confianza, mediante una comunicación oficial electrónica con apariencia de veracidad (mails, mensajes de mensajería instantánea, incluso llamadas telefónicas) para hacerse con las contraseñas, las claves de acceso de la víctima o sus datos bancarios

La víctima, al confiar en el remitente, envía los datos al atacante.

4 – Masquerading (Mascarada)

Consiste en suplantar la identidad de una persona usuaria legítima de un sistema informático, o del entorno del mismo.

Esta suplantación puede realizarse electrónicamente (un usuario o usuaria utiliza para acceder a una máquina un login y password que no le pertenecen) o en persona.

El masquerading es más habitual en entornos donde existen controles de acceso físico, y donde un intruso puede `engañar' al dispositivo o persona que realiza el control

Dos ejemplos podrían ser el acceso a un area restringida con una tarjeta de identificación robada que un lector automatizado acepta, o con un carné falsificado que un guardia de seguridad da por bueno.

5 - Baiting

Lo podríamos traducir de forma más o menos libre como cebar, o hacer picar el anzuelo

Se utiliza un dispositivo de almacenamiento extraíble (CD, DVD, USB) infectado con un software malicioso, dejándolo en un lugar en el cual sea fácil de encontrar (por ejemplo, baños públicos, ascensores, aceras, etc.) por parte de la víctima o víctimas cuyos datos

precisa el o la atacante. Cuando la víctima encuentre dicho dispositivo y lo introduzca en su ordenador, el software malicioso se ejecutará de manera inadvertida y posibilitará que el hacker pueda acceder a los datos del usuario o usuaria.

6 – Scavening (Basureo)

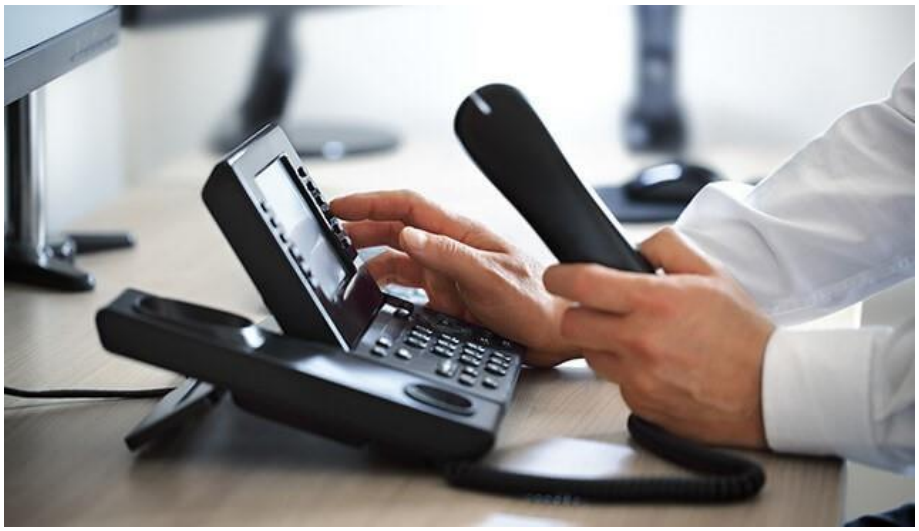
Consiste en obtener información dejada en o alrededor de un sistema informático tras la ejecución de un trabajo.

El basureo puede ser:

- Físico, como buscar en cubos de basura (trashing, traducido también por basureo) listados de impresión o copias de documentos
- Lógico, como analizar buffers de impresoras, memoria liberada por procesos, o bloques de un disco que el sistema acaba de marcar como libres, en busca de información.

7 - Vishing

El Vishing (de la unión de *voice* + *phishing*, o suplantación de voz o telefónica) consiste en ofrecer a la víctima un número de teléfono falso para comunicarse, fingiendo ser el verdadero, y a continuación obtener datos sensibles como números de tarjetas de crédito o claves y personas usuarias



TIPOS DE AMENAZAS FÍSICAS DE LOS SISTEMAS INFORMÁTICOS

Las amenazas físicas más comunes de los sistemas informáticos pueden dividirse en cuatro puntos principales:

1. Acceso físico
2. Desastres del entorno y averías del hardware
3. Radiaciones electromagnéticas
4. Desastres naturales

1. ACCESO FÍSICO

A menudo se descuida la seguridad sobre el acceso, pero hay que tener en cuenta que cuando existe acceso físico a un recurso ya no existe seguridad alguna sobre el mismo, con el consiguiente riesgo.

Un error típico de seguridad por acceso físico es el de tomas de conexión a la red informática no controladas, de acceso libre: un atacante con los suficientes conocimientos técnicos puede causar graves daños.

Por ello, en el campus de la UA todos los accesos del alumnado a la red están autenticados con tu usuario y clave de Campus Virtual, bien mediante wifi (has tenido que autenticarte previamente en eduroam), bien mediante los ordenadores de uso público (que requieren también identificación previa).

Los ordenadores de consulta de catálogo, de acceso libre, tienen limitadas las funcionalidades y la navegación. Además, las redes de acceso público y la red interna de la UA están virtualizadas y aisladas.

2. DESASTRES DEL ENTORNO Y AVERÍAS DEL HARDWARE

Dentro de este grupo estarían incluidos sucesos que, sin llegar a la categoría de desastres naturales, pueden tener un impacto igual de importante si no se habilitan las medidas de protección adecuadas: hablamos, por ejemplo, de picos de sobretensión que

puedan quemar componentes, apagones que afecten a los servidores (y dejen caída la web de la UA y todos sus servicios), incendios, apagones y similares.

Tampoco podemos olvidar los errores o daños en el hardware que se puede presentar en cualquier momento. Por ejemplo, daños en procesadores, en memoria RAM, en discos duros o, en definitiva, en cualquier elemento del hardware

3. RADIACIONES ELECTROMAGNÉTICAS

Sabemos que cualquier aparato eléctrico emite radiaciones y que dichas radiaciones se pueden capturar y reproducir si se dispone del equipamiento adecuado.

Por ejemplo, un posible atacante podría capturar los datos tecleados en un teclado inalámbrico (no decimos que sea fácil, pero es factible), por no hablar de las redes wifi abiertas, un auténtico coladero de seguridad

4. DESASTRES NATURALES

En nuestra zona geográfica no son nada raras las gotas frías, las inundaciones por riadas o las lluvias torrenciales puntuales.

La propia Universidad sufrió una grave riada en 1997, que afectó gravemente, entre otros, al edificio de la Biblioteca General, cuyo Depósito quedó totalmente anegado

CATÁLOGO DE LAS PRINCIPALES AMENAZAS LÓGICAS DE LOS SISTEMAS INFORMÁTICOS

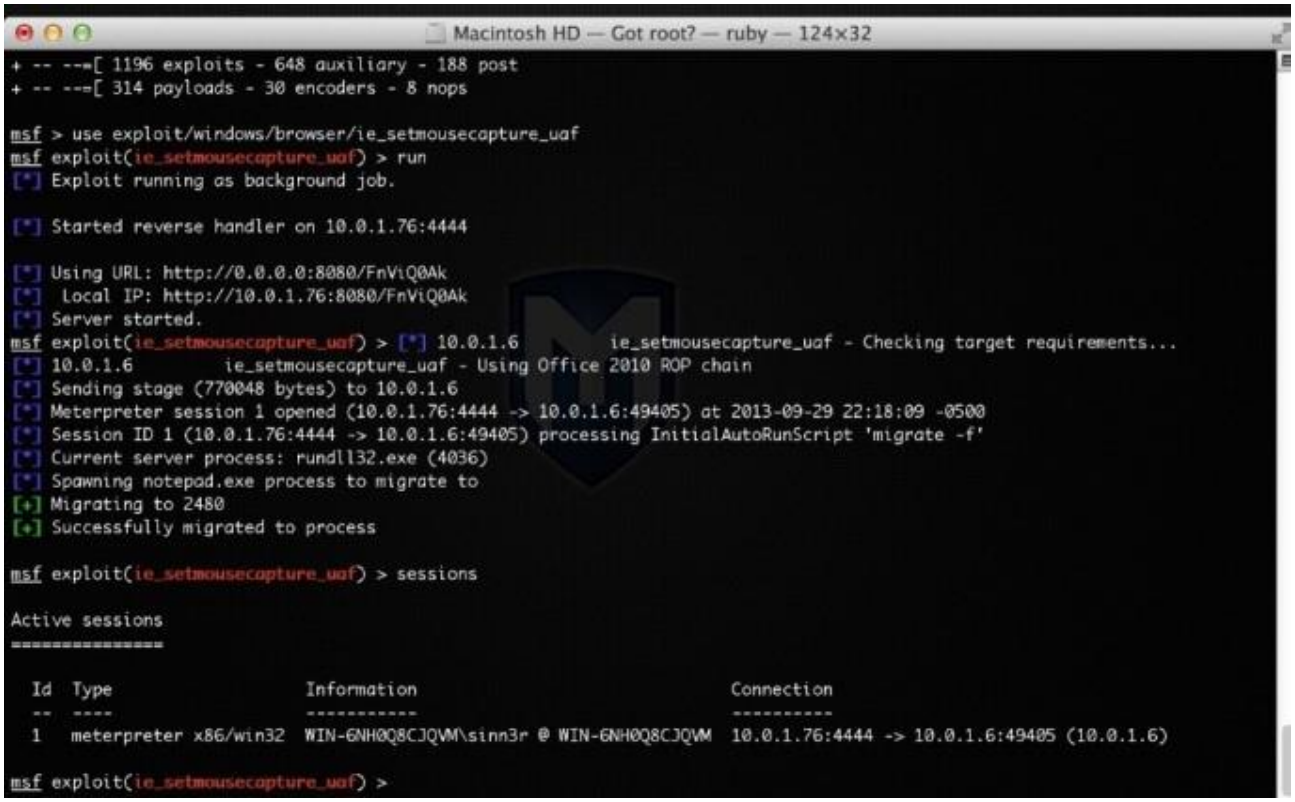
Las amenazas lógicas comprenden una extensa serie de aplicaciones que amenazan la integridad de los sistemas informáticos, y que pueden ser de dos tipos principales:

- **Malware** (*malicious software*, o software malicioso): aplicaciones diseñadas intencionalmente para dañar el sistema o para proporcionar acceso al mismo.
- **Bugs o errores de programación**: software mal diseñado que, por error, ocasiona un agujero de seguridad que puede acabar provocando los mismos riesgos que el malware.

Exploits

Un exploit (de explotar, o aprovechar) es una aplicación, fragmento de software o archivo de secuencia de comandos (script) diseñado para aprovechar una determinada brecha de seguridad o vulnerabilidad de un sistema informático para conseguir un comportamiento no previsto o no deseado del mismo

Ejemplos de exploits: obtener un acceso no autorizado, tomar el control de todo el sistema o conseguir los niveles de privilegio de usuario o usuaria más altos, o conseguir un ataque de denegación de servicio.



Estos ficheros llegan a la máquina objetivo principalmente mediante email o un pendrive infectado.

Una vez la persona usuaria lanza el archivo, el programa objetivo (por ejemplo, Word) lo cargará y ejecutará y, a menos que sea detectado por el firewall o el antivirus, aprovechará la brecha de seguridad para lograr sus objetivos.

Los exploits son específicos de cada sistema operativo, de cada configuración particular de un sistema y del tipo de red en la que se encuentren. Pueden haber exploits diferentes para atacar la misma vulnerabilidad en una aplicación que corra en diferentes sistemas operativos

Virus Infomáticos

Un virus informático es un malware (software malicioso) que 'infecta' con su código a otros archivos o ejecutables básicos del sistema con la intención de modificarlos y lograr así alterar el funcionamiento de la máquina atacada sin el conocimiento ni el consentimiento de la persona usuaria.

Sus objetivos pueden ser varios, desde ralentizar el sistema a destruir toda la información del mismo o corromper la partición de arranque. En cualquier caso, los daños se centran en cada una de las máquinas infectadas.

Los virus sólo infectan al sistema operativo para el cual fueron diseñados; hay muy pocos casos de virus multiplataforma.

Principales vías de infección de los virus

- Archivos adjuntos en Spam (correos no solicitados)
- Sitios web inseguros que han sido infectados
- Cualquier dispositivo externo infectado (pendrive USB, CDs, DVDs)
- Redes de descargas P2P
- Redes sociales

Mecanismos de infección de los virus. ¿Cómo infectan los virus?

Los virus pueden infectar de dos maneras diferentes:

- La más usual consiste en 'inyectar' una porción de código malicioso en un archivo ejecutable normal. De esta forma, el virus se mantiene latente en el archivo y cuando la persona usuaria ejecute ese archivo, además de las acciones normales codificadas, se ejecutan las instrucciones del virus.

- La segunda forma de infectar consiste en sustituir al archivo original y renombrar éste por un nombre conocido sólo por el virus. Así, al ejecutar el archivo primero se ejecuta el malicioso y, al finalizar las instrucciones, éste llama al archivo original, ahora renombrado.

Gusanos Infomáticos

Un gusano es un programa malicioso que realiza copias de sí mismo en diferentes ubicaciones del ordenador infectado con el objetivo de propagarse a otros ordenadores, contagiar al mayor número posible de máquinas y terminar colapsando las redes informáticas, impidiendo el trabajo de las personas usuarias..

A diferencia de los virus clásicos, los gusanos no infectan archivos ni precisan de la intervención de las personas usuarias para expandirse. Pueden hacerlo de dos formas:

- Utilizando vulnerabilidades del sistema operativo para copiarse a todos los ordenadores conectados en una red
- Propagándose por internet a través del correo electrónico, redes P2P (peer-to-peer, o comunicación entre pares) o mensajería instantánea.

Una diferencia importante entre los virus clásicos y los gusanos informáticos es que los virus siempre corrompen archivos de la máquina a la que infectan, mientras que los gusanos no necesitan alterar archivos: se copian a si mismos y se quedan residentes en memoria

También mencionaremos que los virus suelen centrarse en causar daños a las máquinas individuales, mientras que los gusanos casi siempre causan problemas a las redes.

El objetivo de los gusanos no es necesariamente provocar un daño al sistema, sino expandirse a la mayor cantidad de equipos que le sea posible

En algunos casos, los gusanos transportan otros tipos de malware, como troyanos o rootkits; en otros, simplemente intentan agotar los recursos del sistema como memoria o ancho de banda mientras intenta distribuirse e infectar más ordenadores.

Troyanos

Un troyano informático es un tipo particular de malware que, de cara al usuario o usuaria, se presenta como un programa inofensivo. Al ser ejecutado, sin embargo, proporciona al atacante acceso remoto al equipo infectado.

Toma su nombre, como puedes imaginar, de la historia del Caballo de Troya narrada por Homero en la Odisea.

Hay multitud de tipos de troyano, pero en su inmensa mayoría lo que hacen es crear una puerta trasera (backdoor) para que el atacante malicioso puede acceder al sistema de forma remota y realizar diferentes acciones sin necesitar permisos.

En los últimos tiempos, los troyanos se usan, sobre todo, para robar datos confidenciales y bancarios de las personas.

Algunas de las acciones que pueden llevar a cabo los troyanos:

- Robo de información personal: información bancaria, contraseñas, códigos de seguridad...
- Borrado, modificación o transferencia de archivos (descarga o subida)
- Monitorización del sistema y seguimiento de las acciones del usuario o usuaria
- Monitorizar las pulsaciones del teclado
- Realizar capturas de pantalla
- Utilizar la máquina como parte de una botnet (para realizar ataques de denegación de servicio o envío de spam).
- Sacar fotos por la webcam (si tiene)

A diferencia de los virus y los gusanos, los troyanos no pueden replicarse por sí mismos.

Ransonware

Un ransomware (acrónimo de ransom por rescate + ware por software), es un tipo de malware que restringe el acceso a determinados archivos y carpetas del sistema infectado, o incluso al sistema completo, y que pide un rescate monetario a cambio de eliminar esa restricción de acceso. Los archivos y carpetas suelen ser cifrados

El ramsomware se transmite normalmente bien como un troyano (camuflado en archivos adjuntos, vídeos descargados, o programas bajados de sitios dudosos), bien como un gusano (infectando al sistema operativo a través de las vulnerabilidades del mismo).

Una vez activado, el ramsonware bloquea los archivos y lanza los mensajes de advertencia, a veces incluso con fotos sacadas con nuestra propia camara web.

La última infección importante de ransomware ha sido la de WannaCry, en mayo de 2017, que en España llegó a afectar a grandes empresas como Gas Natural, Iberdrola o la propia Telefónica, mientras que en el Reino Unido afecto a una gran parte del sistema hospitalario.

Otras infecciones famosas han sido las de CryptoLocker, CryptoWall o el letal Mamba, un ramsomware de cifrado de disco completo (FDE o Full Disk Encryption: cifra el disco completo y el sistema ni siquiera puede arrancar)

Rootkits

Un encubridor o rootkit es una aplicación de software que oculta a otras aplicaciones maliciosas y a sí misma evitando su detección tanto por parte del usuario o usuaria atacada como de los antivirus .

Los rootkits no pueden considerarse malware por sí mismos puesto que, en realidad, no realizan acciones maliciosas, pero sí se les asocia al malware porque ocultan acciones perjudiciales que otras aplicaciones, procesos, archivos, directorios, claves de registro y puertos desarrollan en el equipo atacado.

Spyware

Son programas espía que recopilan información de la persona usuaria sin su consentimiento, y luego la envían a la persona atacante.

El spayware se autoinstala en el sistema de tal forma que se ejecuta cada vez que se arranca el ordenador, consumiendo recursos de procesador y memoria

Típicamente, el spyware recopila datos sobre los hábitos de navegación o comportamiento en la web del usuario o usuaria atacada, las webs que visita, con qué frecuencia y el tiempo que permanece en el sitio, o monitorizando las aplicaciones que se ejecutan en el ordenador.

El spyware provoca inestabilidad en el sistema y ralentización del mismo.

Adware

Es un software malicioso que se instala en el ordenador de la víctima con el fin de descargar y mostrar en el ordenador de la víctima todo tipo de contenidos publicitarios, en forma de ventanas emergentes (pop-ups) o banners y, en los casos más agresivos, instalando barras de herramientas, modificando los favoritos de los navegadores y cambiando la página de inicio de los mismos para que siempre naveguemos por sus redes publicitarias.

El Adware, o *Advertising-Supported Software* (aplicación apoyada con publicidad) suele venir camuflado en programas shareware y, se instala al aceptar los términos legales durante la instalación de los mismos.

Es un malware más molesto que peligroso, aunque puede llegar a bloquearnos el ordenador si abre demasiadas ventanas emergentes.

El adware no produce una modificación explícita que dañe el sistema operativo, pero sí disminuye el rendimiento del equipo y de la navegación por la red ya que utiliza buena parte de los recursos del sistema.

Backdoors o puertas traseras

Las puertas traseras son brechas de seguridad intencionadas implementadas en la codificación de un sistema operativo o una aplicación, que permiten saltarse los sistemas de seguridad para dar acceso al sistema.

En resumidas cuentas, los backdoors son entradas secretas que permiten entrar al sistema y hacerse con el control del mismo.

En teoría, los programadores incluyen estos atajos en los sistemas de autenticación de las aplicaciones porque permiten depurar los fallos con mayor velocidad.

Las agencias de seguridad nacionales y los gobiernos presionan a los fabricantes de software para que implementen puertas traseras para así poder espiar y hacerse con la información de las personas usuarias potencialmente peligrosas (terroristas, delincuentes)

MEDIDAS DE PROTECCIÓN

Cada uno de nosotros somos, en última instancia, responsables de mantener nuestros equipos en condiciones óptimas para minimizar el riesgo de un ataque, lo que impllica, entre otras cosas, tener actualizado el antivirus, instalar y configurar un firewall o cortafuegos (que monitorice las conexiones entrantes y salientes del ordenador), tener actualizado el sistema operativo con las últimos parches y actualizaciones, evitar navegar por sitios fraudulentos, mantener los navegadores libres de complementos o extensiones que no sean de confianza o ajustar los niveles de privacidad en nuestros perfiles de las redes sociales.

Esto en cuanto a la parte técnica, que es relativamente sencilla de implementar. La parte de ingeniería social es, como ya hemos mencionado, el eslabón más débil de la cadena, y es ahí donde debemos guiarnos siempre por el principio de la prudencia para evitar robo de identidades o de claves.

A continuación lo veremos con más detenimiento.

Protección en el correo electrónico

El correo electrónico es una de las herramientas más utilizadas y un canal muy usado por los atacantes. Es por esto que has de tratar de aumentar la seguridad en él con el objetivo de prevenirte de ataques debidos al uso descuidado del e-mail.

Spam

Se llama spam (o correo basura) al envío de mensajes masivos no deseados, normalmente de remitente desconocido.

La forma más común en la que puedes advertir el spam es en el correo electrónico pero también se puede ver de manera parecida en el uso de mensajería instantánea, búsquedas en Internet, blogs, móviles, foros de Internet, etc.

Recomendaciones para evitar el envío de correo masivo y la propagación de código:

- No confíes en correos cuyo remitente no resulte conocido o pueda resultar sospechoso; menos aún en archivos adjuntos que puedan contener dichos correos.
- Presta atención a la extensión de los archivos adjuntos (indica que tipo de archivo es), ya que algunas técnicas de engaño alteran las extensiones para ocultarse.
- Evita publicar tu dirección de correo en páginas web que tengan una dudosa reputación. Utilizar otra cuenta de correo electrónico puede ser útil para proteger tu cuenta de correo principal.
- No respondas nunca a un correo no deseado. De esta manera no se pierde tiempo ni se confirma a las personas responsables de hacer spam, que la cuenta de correo está activa.
- Utiliza los filtros anti-spam que proporcione el proveedor de correo electrónico; filtrarán los correos en otra carpeta y no te molestarán.
- Bloquea las imágenes en correos recibidos y acéptalas sólo cuando consideres que el correo no es dañino (esta técnica la suelen utilizar los proveedores de correo).

Phising

El phishing es una forma de intentar adquirir información (como nombres de personas, contraseñas, detalles de tarjetas de crédito, etc.) tratando de enmascararse como una entidad de confianza utilizando una comunicación electrónica.

Su ámbito principal es **la banca,** y normalmente consiste en obtener de manera fraudulenta información confidencial e intentar realizar algún tipo de estafa relacionada con obtener dinero de las personas.

Ejemplos de phishing son aquellos correos que piden introducir los datos en una página para evitar que una cuenta sea cancelada, enviar datos personales por correo electrónico, confirmación de datos, etc.

Algunas medidas para evitar ser víctimas del phishing son las siguientes:

- Las entidades bancarias no piden nunca datos confidenciales por correo electrónico para minimizar las posibilidades de que la técnica tenga éxito. Por tanto, nunca reveles datos confidenciales pese a que el correo tenga un aspecto que pueda parecer confiable.
- No hagas clic en enlaces que aparecen en el cuerpo del mensaje ya que pueden llevarte a una página web clonada de una página de entidad financiera y hacerte creer que te encuentras en la verdadera página web.
- Comprueba que la dirección de la página web utiliza un protocolo seguro. Para ello fíjate en que la dirección no comience por http:// sino por https://, la 's' final en http indica que es una página segura y que la información que se deposita viaja de manera cifrada.

- Verifica que existe un certificado digital en la página web. El certificado se puede visualizar haciendo clic sobre el icono de candado que debe aparecer.
- Si tienes dudas de la legitimidad del correo electrónico, llama a la entidad financiera o acude a una oficina para descartar un posible engaño.
- Nunca envíes contraseñas, números de tarjeta de crédito u otra información confidencial a través de correo electrónico.
- Examina periódicamente las cuentas bancarias, con el fin de detectar posibles irregularidades relacionadas con la manipulación de la cuenta o transacciones no autorizadas.
- Denuncia casos de phishing (cuando puedas) a la entidad de confianza. De esta manera también colaboras con la seguridad en la navegación en Internet y ayudas a cortar la actividad del sitio malicioso.

Protección frente a ventanas emergentes

Durante la navegación, es posible que aparezcan ventanas emergentes (conocidas como *popups*)..

Estas ventanas emergentes resultan pueden resultar molestas o bien atraerte para que hagas click en ellas

Hay que tener cuidado ya que la algunas se tratan de publicidad simplemente, pero otras animan a descargar un programa (para ver un video, por ejemplo) y pueden contener algún tipo de virus.

Existen utilidades para bloquear las ventanas emergentes, tanto a nivel del propio navegador como de software externo.

Uso de contraseñas seguras y renovación periódica

La contraseña es la forma de autentificación que utilizas para probar tu identidad u obtener acceso a un recurso.

Debido a la importancia de la contraseña, existen varias **recomendaciones** aque puedes tener en cuenta a la hora de definirla:

- Crea una contraseña que utilice diferentes tipos de caracteres, como letras, números y símbolos. Te aconsejamos que tenga una longitud mínima de 8 caracteres y que no pueda ser encontrada en un diccionario.
- Utiliza una contraseña creada de manera aleatoria, aunque tengan el inconveniente de que son más difíciles de memorizar.
- Cambia las contraseñas de manera periódica.
- Te recomendamos, en la medida de lo posible, que utilices opciones de autentificación que ofrezcan las entidades bancarias u otras entidades, ya sea mediante un certificado digital o DNI electrónico, en lugar de autentificarte mediante el uso de contraseña.

Es importante que crees una contraseña difícil de averiguar para otras personas pero que sea fácil de recordar para ti.

Ajusta la privacidad en navegación y redes sociales

Recomendaciones para mejorar la seguridad en la navegación:

- Realiza la descarga de aplicaciones de seguridad únicamente desde la página web oficial, de manera que se evita la posibilidad de descargar archivos que puedan haber sido previamente manipulados con fines maliciosos.
- En caso de instalar complementos extras como barras de tareas, extensiones, protectores de pantalla, comprueba previamente su autenticidad.
- Realiza ajustes en la configuración del navegador web para poder minimizar el riesgo de ataques maliciosos.
- Instala un programa antivirus que tenga la capacidad de detectar páginas web maliciosas mientras se navega por Internet y que explora los archivos descargados; cada vez son más los antivirus que incluyen estas características.
- Utiliza un cortafuegos (firewall) que bloquee comunicaciones entrantes y salientes; de esta manera se evitará la posibilidad de que alguna aplicación maliciosa intente conectarse con el ordenador e incluso extraer datos.
- Intenta, a ser posible, no acceder a servicios bancarios u otros que utilicen datos confidenciales en ordenadores públicos (como cibers, bibliotecas, hoteles, etc.) incluso en redes Wi-Fi abiertas sin contraseña.
- En caso de navegar por Internet utilizando ordenadores públicos, te recomendamos eliminar los archivos temporales, caché, cookies, historial, contraseñas y formularios en los que hayas introducido datos para evitar que otra persona usuaria tenga acceso a tu información privada.

Recomendaciones en Redes Sociales

Las redes sociales actualmente son muy populares y masivamente utilizadas. Las personas atacantes intentan aprovecharse de aquellas personas usuarias que son más desprevenidas y utilizan las redes sociales con fines maliciosos. Es por esto que es necesario tomar medidas para utilizarlas de la manera más segura posible.

- Algunas **recomendaciones** son las siguientes:

- Trata de no publicar información privada, ya que personas desconocidas pueden aprovechar dicha información.
- Cuida, e incluso evita, la publicación de imágenes propias y de tus familiares. Las imágenes se pueden utilizar incluso para complementar actos delictivos de cualquier ámbito.
- Configura los ajustes de privacidad del perfil de usuario ; puedes configurarlos para que sea privado y sólo puedan verlo personas a quienes se lo permitas.
- Asegúrate de la veracidad de las personas que envían solicitudes antes de aceptarlas.
- Cambia las contraseñas de manera periódica.

Realiza copias de seguridad regularmente

Las copias de seguridad (o *backups*) se realizan para tener almacenadas copias de archivos e incluso del estado de un ordenador para que, en caso de pérdida de información (ya sea por una catástrofe informática o por alguna causa accidental), puedas restablecer o restaurar el estado previo de tu ordenador.

Actualiza el sistema operativo y las aplicaciones

Es recomendable que actualices el sistema operativo y las aplicaciones instaladas en tu ordenador.

Las actualizaciones, además de agregar alguna nueva funcionalidad, sirven para solucionar fallos y agregar nuevas funcionalidades. Por ello estar al día con las actualizaciones de seguridad más importantes ayudará a prevenir ataques maliciosos.

Es importante que descargues actualizaciones de sitios que sean de confianza. Descargar actualizaciones de aquellos de los que se dude su reputación o sitios no oficiales aumenta el riesgo de infección.

Siempre que sea posible, te recomendamos descargar las actualizaciones a través de los mecanismos que ofrece el fabricante.

Configura de manera óptima el sistema operativo

Es importante que realices ajustes el sistema operativo para hacerlo más seguro.

Algunos **consejos** que te ofrecemos son:

- Deshabilita las carpetas compartidas si no las utilizas. Esto evita la propagación de programas maliciosos que las aprovechen para infectar el ordenador.
- Utiliza contraseñas seguras y fáciles de recordar tanto en aplicaciones como a nivel de acceso al ordenador para evitar que puedan acceder personas no deseadas.
- Crea perfiles de usuario con privilegios restringidos, de manera que se limiten las acciones de algunas personas que puedan provocar un aumento de posibilidades de infección.
- Deshabilita la ejecución automática de dispositivos de almacenamiento extraíbles (como USB), ya que pueden contener aplicaciones maliciosas que se ejecuten en segundo plano, invisibles a la persona usuaria.
- Ten en cuenta que el soporte técnico en versiones antiguas de sistemas operativos y aplicaciones recibe menos atención que en el de las últimas versiones, por lo que por norma general las versiones más antiguas están más expuestas a vulnerabilidades.
- Normalmente los archivos maliciosos se esconden en el sistema como ficheros ocultos, por lo que muchas veces se encuentran configurando el sistema para que se permitan ver los archivos ocultos.
- Es posible configurar la visualización de las extensiones de archivos para que puedas identificar las extensiones de archivos que se hayan descargado y evitar ser víctima de técnicas como la doble extensión.

Navegación segura, de incógnito / privada y anónima

Navegación segura

El protocolo **HTTPS** (*Hypertext Transfer Protocol Secure*, o protocolo HTTP seguro) garantiza que las sesiones de navegación están cifradas, por lo que la transferencia de datos es segura.

Verás que te encuentras en una sesión de navegación segura cuando, en la barra de navegación, te encuentres las siglas **https**.

Es fundamental que te encuentres dentro de una sesión segura cuando introduzcas o manejes datos sensibles, como datos bancarios, académicos o de compras.

Si estás en una página de comercio electrónico y, a la hora de efectuar el pago o introducir los códigos de la tarjeta de crédito la conexión no es segura, jamás debes introducir los datos

Navegación privada

Con la navegación privada, el navegador no deja en el ordenador ningún rastro de las páginas que visita (cookies, caché e historial).

Sin embargo, hay que tener en cuenta que este tipo de navegación no oculta la IP (dirección de internet del ordenador) ni proporciona navegación anónima real.

¿Para qué puede sernos útil la navegación privada?

- Para abrir sesiones paralelas de una misma aplicación desde un mismo ordenador: por ejemplo, podemos tener varias cuentas de GMail abiertas, en lugar de tener que cerrar una sesión y abrir otra, o abrir sesión en otro navegador
- Para mantener la privacidad de cada persona usuaria en ordenadores compartidos y, evitar, por ejemplo, que datos personales o privados queden expuestos inadvertidamente (formularios, claves..)
- Para visitar páginas sospechosas o que generen poca confianza: así se evita que se pueda instalar 'malware' (aplicaciones dañinas) por medio de cookies

Qué hace y qué no hace la navegación privada

Si bien cada navegador realiza esta función a su manera, en términos generales, la navegación privada implica que el navegador:

- Elimina las cookies tras cerrar la sesión
- No se guarda ningún tipo de historial o formularios de auto-completado
- No se guardan las contraseñas
- Se borra la caché automáticamente al salir

- De igual modo, es preciso recordar **lo que no hace**:

- No proporciona conexiones seguras o cifradas
- No oculta tu dirección IP
- No evita que las páginas de Internet almacenen información sobre ti
- No impide que tu navegación sea supervisada por el administrador de la red
- No supone un anonimato total (aplicaciones de terceros como Flash pueden guardar sus propias cookies, etcétera)

Navegación Anónima: TOR, I2P y proxies gratuitos

Aún cuando naveguemos en modo privado, seguimos siendo identificables en la red: nuestra IP es visible y a partir de ahí se puede obtener nuestra posición geográfica aproximada, nuestro proveedor de servicio o incluso el nombre de la empresa en que trabajamos (si disponemos de una IP institucional.

La única forma de lograr un anonimato casi completo cuando navegamos es usar una conexión segura a una máquina denominada servidor http proxy.

Un servidor http proxy es un ordenador que funciona como una pasarela a través de la cual se filtran nuestras peticiones de navegación por la web

Así, si queremos conectarnos a una página web, primero haremos la petición al servidor proxy, y será esta máquina la que haga la petición de carga a la página a la que queramos conectarnos, quedando nuestro ordenador "oculto" a ojos del servidor de esa página web, pues la IP que le consta a ese servidor web es la del proxy.

Cuando usamos este mecanismo varias veces seguidas, es casi imposible rastrear la IP original de nuestro ordenador, con lo que nuestra navegación es totalmente anónima.

TOR es el sistema de navegación anónima más popular.

Se trata de una red gratuita gracias a la cual se puede navegar, chatear o descargar archivos de forma totalmente anónima. Al mismo tiempo, es un conjunto de programas que posibilita el acceso a esta red.

Para usar TOR, debemos descargar la aplicación e instalarla. Existen también complementos para Firefox que facilitan la navegación anónima con TOR, así como versiones portables de la propia aplicación (Portable TOR), o basadas en el navegador Opera (Opera-TOR)

Además de TOR, existe una red de servidores proxy no cifrados y túneles VPN anónimos a través de los cuales poder hacer nuestra conexión, pero la fiabilidad es variable

I2P y Freenet son redes P2P privadas, que sirven a comunidades anónimas a través de los cuales se intercambian grandes volúmenes de datos. La red I2P es una red dentro de internet, de tal forma que sus comunicaciones son invisibles para el resto de usuarios de internet.