2022

Maria Emilia Suárez

Seminarios de actualización

29-6-2022

VULNERABILIDADES INFORMÁTICAS



VULNERABILIDADES INFORMÁTICAS

Cada día más empresas digitalizan sus procesos y mueven en la nube sus activos, lo que aumenta exponencialmente su exposición a una vulnerabilidad informática. El coste de sufrir una pérdida de información o de un ciberataque sigue creciendo año tras año, por lo cual es necesario protegerse.

Una vulnerabilidad informática es una debilidad en el software – o en el hardware – que permite a un atacante comprometer la integridad, disponibilidad o confidencialidad del sistema o de los datos que procesa. Las vulnerabilidades pueden ser debidas tanto a fallos de diseños, errores en la configuración o a procedimientos no robustos. Las vulnerabilidades más peligrosas son las que permiten a un atacante ejecutar código dañino en el sistema comprometido.

**Principales tipos de vulnerabilidad informática**

Las vulnerabilidades se pueden producir en todas las etapas de desarrollo, implementación y mantenimiento de un software o de un sistema de información.

Una vulnerabilidad de día cero es un fallo no conocido en un software y que puede permitir a un atacante utilizar un código para explotarla – conocido como “exploit” – para introducirse en el sistema. Su peligrosidad reside en el hecho de que, al no ser conocida, todavía el fabricante no dispone de una actualización de seguridad. Esto genera también un mercado ilegal de compra-venta de vulnerabilidades. Dos casos relevantes de este tipo de vulnerabilidad son Meltdown y Spectre , relacionadas con hackeo de microprocesadores informáticos, que existen desde mediados de los noventa, pero que han sido descubiertas solamente ahora.

Además, existen vulnerabilidades de diseño, debidas tanto a fallos en el diseño de protocolos de redes o a deficientes políticas de seguridad. También, hay vulnerabilidades de implementación, debidas a errores de programación o a descuidos de los fabricantes. Por otro lado, las vulnerabilidades por falta de mantenimiento se dan cuando un software ya no recibe actualizaciones por su fabricante.

Por último, las vulnerabilidades informáticas por uso o debidas al factor humano suelen ser menos consideradas, aunque su impacto puede ser mayor que las anteriores. Tienen que ver con la falta de formación o concienciación de los usuarios o empleados de una organización sobre prácticas de seguridad.

**¿Cómo protegerse? El análisis de vulnerabilidad informática**

* La mejor solución suele ser la prevención, y también en el caso de nuestros sistemas de información es importante realizar un análisis previo para detectar previamente posibles vulnerabilidades.
* Para ello, deberemos previamente realizar un inventario de nuestros activos TI: servidores, infraestructura de redes, aplicaciones y periféricos (impresoras, etc.).
* A continuación, deberemos realizar pruebas de penetración para detectar posibles vulnerabilidades tanto externas como internas, simulando a un hacker externo (lo también se conoce como hacking ético) o a personal interno con determinados privilegios.
* Finalmente, deberemos determinar y aplicar las medidas correctivas necesarias, para reparar vulnerabilidades o reducir las amenazas.
* Por otro lado, no tenemos que olvidarnos de las buenas prácticas de seguridad internas a la empresa, por lo cual deberemos concienciar constantemente a nuestro personal para evitar vulnerabilidades informáticas de factor humano.
* Realizar copias de seguridad periódicas.
* Llevar una correcta gestión de contraseñas.
* Mantener nuestros sistemas informáticos siempre actualizados.
* Monitorizar constantemente los avisos de últimas vulnerabilidades conocidas. Una herramienta útil en este sentido es el repositorio de vulnerabilidades del CERTSI.
* Cumplir con normas como la ISO 27001.

Hoy en día, cualquier empresa se expone a vulnerabilidades y amenazas desde el momento en que se crean. Por lo que un correcto análisis de riesgos y gestión de vulnerabilidades nos ayuda a protegernos de las amenazas.

**El Phishing**

Phishing es un término informático que distingue a un conjunto de técnicas que persiguen el engaño a una víctima ganándose su confianza haciéndose pasar por una persona, empresa o servicio de confianza (suplantación de identidad de tercero de confianza), para manipularla y hacer que realice acciones que no debería realizar (por ejemplo, revelar información confidencial o hacer click en un enlace).

Para realizar el engaño, habitualmente se hace uso de la ingeniería social explotando los instintos sociales de la gente, como es de ayudar o ser eficiente. También mediante la adulación de la víctima, explotando su intrínseca vanidad o necesidad de ser reconocido, baja autoestima, o una persona que busca trabajo. Por ejemplo, enviando correos electrónicos o mostrando publicidades a la víctima diciéndole que ha ganado un premio y que siga un enlace para recibirlo, siendo aquellas promesas falsas (un cebo). A veces también se hace uso de procedimientos informáticos que aprovechan vulnerabilidades. Habitualmente el objetivo es robar información, pero otras veces es instalar malware, sabotear sistemas, o robar dinero a través de fraudes.

A quien practica el phishing se le llama phisher.

Dado el creciente número de denuncias de incidentes relacionados con el phishing, se requieren métodos adicionales de protección. Se han realizado intentos con leyes que castigan la práctica y campañas para prevenir a los usuarios con la aplicación de medidas técnicas a los programas.

**Así están robando cuentas de Instagram ¡Evítalo!**

Con un mensaje de parte de la red social (que parece real) comienza el robo de una cuenta de Instagram. Te contamos cómo lo están haciendo los hackers y las claves para evitarlo.

Entras en tu perfil de Instagram y encuentras un mensaje directo (DM) de (supuestamente) la propia red social en el que te advierten que estás sufriendo un ataque y que estás a punto de perder tu preciada cuenta. En el mensaje, provisto de un logo idéntico al original, se incluye un enlace que, en teoría, lleva al soporte y centro de ayuda de Instagram y en el que se te invita a hacer clic con la máxima celeridad para proteger tu cuenta y evitar el supuesto robo. Una vez dentro del enlace, el siguiente paso es facilitar un teléfono móvil con el pretexto de comprobar que eres el propietario de la cuenta.

¿Qué harías? De antemano, dudar. Lo lógico es pensar que es un mensaje enviado por la propia red social avisando de un posible hackeo, pero lo cierto es que este tipo de mensajes son los que últimamente están utilizando los hackers para hacerse con el control de numerosas cuentas, muchas de ellas de empresas, creadores y docentes. Precisamente, así lo denunciaba hace unos días María Lázaro, experta en redes sociales y autora del manual ‘Redes Sociales y Menores: guía práctica’, en su cuenta de Instagram.

"En los últimos meses han comenzado a proliferar los robos de cuentas en Instagram, incluso en las que tienen activada la verificación en dos pasos. Aunque varían los procedimientos, uno de los más frecuentes es recibir un mensaje directo (simulando que el emisor es Instagram) en el que se notifica que la cuenta está sufriendo un ataque. En otras ocasiones, el mensaje directo indica que se están violando las condiciones de copyright, o que tiene opción de lograr insignia azul. A veces se trata de mensajes grupales. Siempre, con un enlace a una página con diseño similar a la cuenta oficial de Instagram, pero que es falsa”, explica Lázaro.

**Un robo real y en primera persona**

****Precisamente, siguiendo este modus operandi fue como hace unas semanas una usuaria de esta red social perdió la cuenta profesional de su empresa. “A primera hora de la mañana recibimos un mensaje directo de un perfil que creíamos asociado a la propia plataforma. En él se nos alertaba de que un usuario nos había denunciado por incumplir la política de derechos de autor. Para analizar la posible infracción, el equipo de la red social tenía que comprobar que todo nuestro contenido estaba en orden y que no incumplíamos ninguna norma comunitaria”, comenta la damnificada, que prefiere mantener el anonimato.

La cosa podría haber quedado en una mera advertencia, pero a lo largo del día la situación continuó empeorando. El mismo perfil volvió a ponerse en contacto horas después para informar de que la cuenta quedaría bloqueada durante un período de tiempo si no realizaba un proceso de autenticación a través de un enlace en el que debía introducir el email del perfil y la contraseña. “No desconfié de ese mensaje”, afirma la usuaria, “ya que en su perfil contaba con el tic azul de verificación con el que Instagram confirma la autenticidad de las cuentas de interés público. Si un perfil lo tiene, significa que es de fiar”.

En ese mismo momento, Instagram informó de que alguien ubicado muy cerca estaba accediendo a la cuenta. “La red social me alertaba de que alguien se estaba intentando conectar dos calles más arriba de la mía, así que lo primero que piensas es que la plataforma está realizando sus comprobaciones y, como las ubicaciones no suelen ser muy exactas, dices que eres tú y… les permites entrar”. Lo que esta usuaria desconocía era que, aunque un hacker se encuentre en otro país, utiliza una VPN (Virtual Private Network) ubicada muy cerca del lugar habitual de conexión, ya sea el hogar o la oficina.

Todavía quedaba el último paso para hacer efectivo el robo. “Por la noche la amenaza regresó con un ultimátum: nuestra cuenta iba a ser bloqueada inminentemente”. El miedo, la tensión y el cansancio después de todo el día dando vueltas sobre el mismo tema fueron los ingredientes necesarios para que esta usuaria respondiera al mensaje, en el que le solicitaban un teléfono de contacto para comprobar su conexión. Y ahí comenzó la odisea: una vez que tenían el número de teléfono accedieron a sus sistemas, contraseñas, aplicaciones, perfiles de redes sociales y, después, enviaron mensajes de WhatsApp con extorsiones y realizaron llamadas intentando conseguir dinero a cambio de recuperar la cuenta. “Yo le permití atacarnos: les proporcioné las llaves de nuestra casa y les dejé entrar para que se lo llevaran todo. Es una sensación a caballo entre la vergüenza y el miedo”.

**Importantísimo saber...**

Para que esto no suceda y evitar el ataque y posterior robo de una cuenta personal o profesional, hay que tener en cuenta dos aspectos fundamentales:

Instagram nunca se dirige a los usuarios a través de un mensaje directo. El equipo de esta red social siempre contacta a través de correo electrónico a la cuenta con la que se haya registrado el perfil.

Es primordial fijarse en detalle en los enlaces y comprobar que sean los oficiales del centro de ayuda de la red social. La URL oficial que lleva al soporte de Instagram es help.instagram.com. Por su parte, en estos mensajes fraudulentos utilizan enlaces similares en los que tan solo modifican un símbolo: help-instagram.com o support-instagram.com, ambos falsos. Lógicamente no es fácil diferenciarlos a primera vista; por ello, es importante recurrir al centro de ayuda de Instagram para comprobar su autenticidad.

“Es esencial por tanto estar muy alerta: nunca iniciar sesión en una página que no sea www.instagram.com o www.help.instagram.com y jamás proporcionar el código de seguridad de acceso a la cuenta si alguien nos lo pide".

**Consejos de seguridad de Instagram**

****No obstante, y antes de ponerse en el peor de los casos, la propia red social facilita una serie de consejos de seguridad para evitar el robo de la cuenta.

* Activar la autenticación en dos pasos. Con esta función de seguridad, la red social pedirá al usuario un código de inicio de sesión especial o una confirmación de intento de inicio de sesión cada vez que alguien intente acceder con un dispositivo desconocido (esto último resulta útil cuando es una cuenta de empresa y son varias las personas que acceden a ella). Este tipo de autenticación funciona mediante códigos de seis dígitos que se envían en forma de mensajes de texto a un teléfono móvil o se generan a través de aplicaciones de terceros como Duo Mobile o Google Authenticator, permitiendo confirmar la identidad cuando se inicie sesión por primera vez en un nuevo dispositivo.
* Cuidar la contraseña. Puede sonar algo obvio, pero es fundamental contar con una contraseña segura, utilizando una combinación de al menos seis números, letras y signos de puntuación (como "!" y "&"), además de no hacer uso de ella en ningún otro sitio de Internet. Y si hay sospechas de que han podido ‘entrar’ a la cuenta, otra opción interesante es la de enviarte un correo electrónico pidiendo a Instagram el cambio inmediato de contraseña.
* Observar con detalle los correos recibidos por la red social. Para reconocer los correos oficiales provenientes de Instagram, la red social ha puesto en marcha la función ‘Correos electrónicos de Instagram’ y que se encuentra en Configuración-Seguridad. Con ella, se pretende que los usuarios identifiquen los mensajes oficiales a través de dos listas: en la de ‘Seguridad’ aparecen todos los correos electrónicos relacionados con seguridad e inicio de sesión que la red social ha enviado al usuario en los últimos catorce días; mientras que en la lista ‘Otros’ aparecen diversos mensajes, también de la red social, pero con otros asuntos.
* Cierre de sesión. En la oficina es probable que inicies sesión en un equipo que, a su vez, se comparte con otras personas. Por ello, es importante automatizar siempre la acción de cerrar sesión y no darle a ‘recordarme’, ya que se continúa conectado incluso después de cerrar la ventana del navegador.

https://es.wikipedia.org/wiki/Phishing

https://blog.mdcloud.es/vulnerabilidad-informatica-como-protegerse/

https://www.educaciontrespuntocero.com/tecnologia/robo-instagram/