GLOSARIO DE CIBERSEGURIDAD

INSTITUTO FEDERAL DE TELECOMUNICACIONES

Actualización de seguridad

Actividad que consiste en la aplicación de parches que corrigen vulnerabilidades de los sistemas, dispositivos y aplicaciones

Adware

Se refiere al software o programa que muestra algún tipo de publicidad no deseada o engañosa en una página web o cuando se instala algún programa. Su objetivo es obtener algún beneficio económico o incluso almacenar información privada. Existe cierto tipo de adware que también supervisa el comportamiento en línea para ofrecer anuncios específicos.

Antispyware

Es una tecnología de seguridad que ayuda a proteger a los dispositivos contra el spyware y software no deseado. El antispyware ayuda a reducir los efectos causados por el spyware tales como: lento desempeño del equipo, ventanas de mensajes emergentes, cambios no deseados en configuraciones de Internet y uso no autorizado de la información privada.

Antivirus

Es un tipo de software cuyo principal objetivo es detectar y bloquear acciones maliciosas en dispositivos generadas por malware y, en caso de que se haya producido una infección, eliminarla.

Ataque de "agujero de agua" o "watering"

Creación de un sitio web falso o comprometer uno real, con el objetivo de explotar a los usuarios visitantes. Se trata de un tipo de ataque informático.

Auditoría

Análisis exhaustivo de sistemas y aplicaciones para identificar y localizar vulnerabilidades, fallos de software o errores de configuración que pudieran ser aprovechadas por ciberdelincuentes.

Autenticación

Proceso mediante el cual un equipo de cómputo, dispositivo móvil, programa, aplicación o servicio, corrobora la identidad de un usuario.

Borrado Seguro

Medida de seguridad mediante la cual se establecen métodos y técnicas para la eliminación definitiva de los datos personales, de modo que la probabilidad de recuperarlos sea mínima.

BOTNET

Conjunto de ordenadores, denominados bots, infectados con un tipo de malware que son controlados remotamente por un atacante y que pueden ser utilizados de manera conjunta para realizar actividades maliciosas.

Bug

Error o fallo en un programa de dispositivo o sistema de software que desencadena un resultado indeseado.

Ciberacoso

Es el uso de redes sociales para molestar o acosar a una o más personas, mediante ataques personales y divulgación de información confidencial.

Ciberamenaza

Se refiere a una circunstancia, evento, acción, ocurrencia o persona con el potencial de explotar vulnerabilidades basadas en la tecnología e impactar adversamente en las operaciones, activos de la organización (incluyendo la información y sistemas de información), individuos, otras organizaciones o en la sociedad.

GLOSARIO DE CIBERSEGURIDAD

INSTITUTO FEDERAL DE TELECOMUNICACIONES

Ciberataque

Se refiere al intento de dañar, interrumpir u obtener acceso no autorizado a una computadora, sistema informático o red de comunicaciones electrónicas a través del ciberespacio, el cual es dirigido a una institución con el propósito de interrumpir, deshabilitar, destruir o controlar maliciosamente un entorno o infraestructura de computación, destruir la integridad de los datos o robar la información controlada.

Ciberseguridad

Es el conjunto de herramientas políticas, conceptos, acciones, prácticas idóneas y tecnologías que pueden utilizarse para proteger a los usuarios, sus dispositivos y la información transmitida y/o almacenada, de los riesgos de seguridad que hay en el ciberentorno.

Cifrado

Proceso para garantizar la confidencialidad e integridad de la información. La información se codifica con una función matemática que utiliza una clave.

Contraseña o clave

Medida de seguridad que se utiliza para controlar el acceso a un equipo de cómputo, dispositivo móvil, programa, aplicación o servicio, a través de una palabra, frase o un conjunto de caracteres alfanuméricos. Las contraseñas basadas sólo en números se conocen como PIN (Personal Identification Number), mientras que las basadas en varias palabras o frases tienen el nombre de passphrase.

Control parental

Conjunto de herramientas o medidas que se pueden tomar para evitar que los menores de edad hagan uso indebido del ordenador, accedan a contenidos inapropiados o se expongan a riesgos a través de Internet.

Cookies

Son aquellos paquetes de información definidos por un sitio web y almacenados por un navegador de forma automática en el dispositivo del usuario cuando éste visita dicho sitio.

Cryptojacking

Es una forma de malware que se oculta en el dispositivo y roba los recursos del equipo para hacer minería de monedas online como el bitcoin.

Deepfakes

Son videos manipulados para hacer creer a los usuarios que, un personaje público o anónimo, realiza declaraciones o acciones que nunca ocurrieron. Para la creación de dichos videos, se utilizan herramientas o programas de inteligencia artificial que permiten el intercambio de rostros en imágenes y la modificación de la voz.

Defacement

Es un tipo de ciberataque que se realiza contra un sitio web, en el que se modifica la apariencia de alguna de sus páginas, para llevar a cabo algún tipo de acción fraudulenta o de vandalismo.

Dirección IP

Número con el que se identifica a los dispositivos electrónicos que están conectados a una red la cual utiliza el protocolo IP (Internet Protocol).

Dispositivos periféricos

Son los dispositivos de hardware a través de los cuales, la computadora se comunica con el exterior y que se conectan por cualquier puerto a un equipo de cómputo o dispositivo móvil. Por ejemplo, teclados, monitores, cámaras, memorias USB o discos duros extraíbles.

Emotet

Es un tipo de malware diseñado originalmente como un troyano bancario dirigido a robar datos financieros, se considera una amenaza importante para los usuarios en todo el mundo.

GLOSARIO DE CIBERSEGURIDAD

ift INSTITUTO FEDERAL DE TELECOMUNICACIONES

Encriptación

Función matemática que protege la información al hacerla ilegible para cualquiera, excepto para quienes tengan la llave para decodificarla.

Equipo de cómputo

Dispositivo electrónico que se utiliza para procesar y almacenar información, está compuesto por hardware, software y dispositivos periféricos.

Filtro o control de contenido

Programa que permite limitar el acceso a contenido no deseado, al navegar en Internet.

Firewall

Son mecanismos de protección informática utilizados para establecer un control de acceso de los paquetes que entran y salen de una red.

Grooming

A través del engaño, los cibercriminales ganan la confianza de niñas, niños y adolescentes con la finalidad de recibir o intercambiar contenido de índole sexual.

Hacker

Persona apasionada por la seguridad informática. Esta descripción concierne principalmente a personas que realizan entradas remotas no autorizadas por medio de redes de comunicaciones, conocidas como 'Black hats'. También incluye a aquellos que depuran y arreglan errores en los sistemas, llamados 'White hats'. Este concepto incluye aquellos conocedores que realizan conductas ambigüas, conocidos como 'Grey hats'.

Hardware

Conjunto de elementos físicos y materiales que constituyen un equipo de cómputo o dispositivo móvil.

Huella digital

Rastro de información digital que el usuario deja durante sus actividades en línea.

Identidad digital

Conjunto de características atribuibles y otros valores definidos (un número de identificación de usuario generado al azar, etc.) que se han asignado y se pueden verificar de una manera que puede distinguir una persona o entidad de otra.

Incidente

Evento que surge de circunstancias deliberadas o accidentales, violando las políticas de seguridad y/o protocolos establecidos que pueden resultar en consecuencias perjudiciales para los activos, aplicaciones, sistemas, plataformas y/u otros elementos críticos de la infraestructura.

Ingeniería Social

Son tácticas de persuasión que aprovechan la buena voluntad o la falta de precaución de los usuarios para obtener, mediante engaños, información confidencial o contraseñas.

Internet

Conjunto descentralizado de redes de telecomunicaciones en todo el mundo, interconectadas entre sí, que proporciona diversos servicios de comunicación y que utiliza protocolos y direccionamiento coordinados internacionalmente para el enrutamiento y procesamiento de los paquetes de datos de cada uno de los servicios. Estos protocolos y direccionamiento garantizan que las redes físicas que en conjunto componen Internet funcionen como una red lógica única.

GLOSARIO DE CIBERSEGURIDAD

INSTITUTO FEDERAL DE TELECOMUNICACIONES

Malware o software malicioso

Término que engloba a todo tipo de programa o código malicioso cuyas funciones incluyen: extraer, borrar e incluso 'secuestrar' la información de equipos de cómputo o generar malfuncionamiento en los sistemas. Algunos ejemplos de malware son: los virus, los troyanos, los gusanos y el ransomware.

Mediación parental

Es el conjunto de estrategias para acompañar, orientar y supervisar a menores de edad, con el propósito de que niñas, niños y adolescentes hagan un uso responsable y seguro de Internet, aplicaciones y dispositivos. La mediación parental es útil para prevenir riesgos y solucionar problemas en línea.

Nube

Lugar digital donde la información es almacenada y compartida. Sustituye o complementa el resguardo en discos compactos, memorias, USB, discos duros, etcétera.

Pentesting

Consiste en la simulación de un ataque a un sistema software o hardware con el objetivo de encontrar vulnerabilidades para prevenir ataques externos.

Phishing

Estafa a través de una página web, correo electrónico, SMS o llamada telefónica en la que se suplanta a una persona o empresa de confianza para obtener datos privados del usuario, como claves de acceso o tarjetas de crédito. Dicha actividad se realiza con el propósito de robar información personal y utilizarla para suplantar su identidad u ocasionar daños financieros.

Plan de continuidad

Es un plan de actuación en caso de que ocurra un incidente grave que afecte dispositivos, sistemas o redes y que sirve para mantener en funcionamiento los servicios mínimos del negocio y permitir su recuperación en el menor tiempo y costo.

Privacidad en redes sociales

Mecanismos de protección de datos íntimos o confidenciales en el perfil de redes sociales de una persona, con la finalidad de no exponerlos abiertamente y evitar que alguien los utilice de forma negativa.

Protocolo IP

Se refiere al conjunto de reglas que establecen cómo se transmiten los paquetes de datos a través de una red.

Ransomware

Es un tipo de malware que impide el acceso a archivos del sistema infectado, en ocasiones cifrándolos. A través de este malware se busca coaccionar al usuario a pagar un rescate a cambio de la liberación de la información.

Riesgo cibernético

Constituye la posibilidad de que un ciberataque ocurra y que potencialmente se presente la pérdida financiera, interrupción operativa o daño, debido a la falla de las tecnologías digitales empleadas para funciones informativas y/o operativas.

Smishing

Es una técnica que consiste en el envío de un SMS por parte de un ciberdelincuente a un usuario simulando ser una entidad legítima -red social, banco, institución pública, etc. - con el objetivo de robarle información privada o realizarle un cargo económico. Generalmente el mensaje invita a llamar a un número de tarificación especial o acceder a un sitio web falso.

Spam

Uso de mensajes masivos no solicitados y no deseados para intentar convencer al destinatario para comprar algo o revelar información personal, como un número de teléfono, dirección o información de cuenta bancaria. El correo electrónico es el medio en el que más se presentan estos mensajes; sin embargo, el spam también se produce en otras áreas, como: mensajes de texto, mensajes instantáneos y sitios de redes sociales.

Spyware

Es un tipo de malware que recopila información confidencial de un dispositivo, como datos bancarios y contraseñas, la cual envía a una entidad remota sin el conocimiento ni consentimiento del propietario del equipo.

Suplantación de identidad

Se refiere a la actividad maliciosa en la que un atacante se hace pasar por otra persona o entidad por diferentes motivos: robo de datos, fraudes y engaños para obtener información confidencial o un beneficio económico.

Typosquatting

Es un fenómeno por el cual un usuario teclea mal, en su navegador, la dirección de una página web y abre una página diferente a la que estaba buscando. Los cibercriminales a menudo aprovechan esta situación para llevar al usuario a una página web maliciosa al reservar dominios similares a los legítimos.

Virus

Son programas informáticos o secuencias de comandos que intentan propagarse, sin el consentimiento y conocimiento del usuario, para realizar alguna acción maliciosa en dispositivos.

Vishing

Es un tipo de estafa de ingeniería social a través de una llamada telefónica mediante la cual se suplanta la identidad de una empresa, organización o persona de confianza, con el fin de obtener información personal y sensible de la víctima.

Vulnerabilidad

Es un fallo o problema de seguridad de un programa, aplicación, plugin o sistema operativo, el cual es aprovechado por los ciberdelincuentes para infectar equipos, incluso sin necesidad de que el usuario tenga que realizar ninguna acción peligrosa de manera consciente. Para evitar que esto suceda, los fabricantes generan actualizaciones que solucionan los problemas de seguridad, de ahí la importancia de tener siempre actualizado nuestro dispositivo.

Fuentes:

- Instituto Nacional de Ciberseguridad. España.
- Ley Federal de Telecomunicaciones y Radiodifusión.
- Comisión Nacional de Seguros y Fianzas. SHCP.
- Procuraduría Federal del Consumidor.
- Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.
- Universidad Autónoma de México.
- Secretaría de Seguridad Ciudadana CDMX.
- Asociación de Internet MX.