ABC DE SEGURIDAD DIGITAL

· GLOSARIO BÁSICO ·

ESCUELA DE SEGURIDAD DIGITAL

Colnodo
Uso estratégico de Internet para el desarrollo

WWW.ESCUELADESEGURIDADDIGITAL.CO

A

Acceso no autorizado

La obtención de acceso a un sistema informático o a una red sin la autorización del propietario

Adware

Software que muestra publicidad no deseada en el dispositivo del usuario.

Algoritmo de cifrado

Proceso matemático o función operativa que, junto con una clave específica, se emplea para transformar un texto en claro en un texto cifrado.

Amenaza externa

Cualquier cosa fuera de la organización que tenga el potencial de dañar los activos de esta.

Amenaza interna

Riesgo a la seguridad producido por una persona que pertenece o perteneció a una empresa o tiene una relación directa o de confianza con ella.

Antivirus

Software que escanea un dispositivo o una red para detectar y eliminar malware.

Ataque de fuerza bruta

Ataque que intenta adivinar la contraseña de un usuario mediante la prueba de muchas combinaciones diferentes de caracteres

Ataque DDoS

Los ataques de denegación distribuida de servicio (DDoS) son aquellos que aprovechan los límites de capacidad específicos que se aplican a cualquier recurso de red, tal como la infraestructura que habilita el sitio web de la empresa.

Autenticación

El proceso de verificar la identidad de un usuario.

Autenticación multifactor (MFA)

Un método de autenticación que requiere que el usuario proporcione dos o más factores de autenticación para acceder a un sistema o servicio.

Autorizar

Sexto paso del Marco de Gestión de Riesgos (RMF) del NIST, que se refiere a asumir la responsabilidad de los riesgos de seguridad y privacidad que puedan existir en una organización

B

Backdoor

Puerta trasera en un sistema informático que permite al atacante obtener acceso no autorizado.

Backup

Copia de seguridad que se realiza sobre ficheros o aplicaciones contenidas en un ordenador con la finalidad de recuperar los datos en el caso de que el sistema de información sufra daños o pérdidas accidentales de los datos almacenados.

Biometría

La biometría es un método de reconocimiento y verificación basado en el análisis de las características fisiológicas (huellas dactilares, retinas, iris, cara, etc.) o de comportamiento (firma, forma de andar, tecleo, etc.).

Botnet

Red de dispositivos infectados con malware que se pueden controlar de forma remota.

Bug

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

C

Captcha

Acrónimo en inglés de Completely Automated Public Turing test to tell computers and Humans Apart; es un tipo de medida de seguridad que consiste en la realización de pruebas desafío-respuesta controladas por máquinas que sirven para determinar cuándo el usuario es un humano o un bot según la respuesta a dicho desafío.

Categorizar

Segundo paso del Marco de Gestión de Riesgos (RMF) del NIST, que se lleva a cabo para desarrollar procesos y tareas de gestión de riesgos.

Catfishing

Se refiere a la fabricación de una identidad falsa online por parte de un ciberdelincuente con fines de engaño, fraude o explotación.

Ciberataque

Cualquier acción que intente dañar o inhabilitar un sistema informático o una red.

Ciberbullying

Acoso a través de medios electrónicos, como las redes sociales o el correo electrónico.

Cifrado

Conversión de datos en un formato que solo puede ser leído por alguien que tenga la clave de descifrado.

Cifrado asimétrico

Tipo de cifrado que utiliza dos claves, una pública y otra privada. Estas claves están vinculadas, pero no son idénticas. La clave pública se comparte con cualquiera que necesite cifrar información para el propietario de la clave privada. El propietario de la clave privada mantiene la clave en secreto para poder descifrar la información con la clave pública.

Cifrado asimétrico

Este modo de encriptación utiliza una sola clave para cifrar y descifrar los datos. Esto lo hace más conveniente para usuarios individuales y sistemas cerrados, ya que solo es necesario compartir una clave.

Sin embargo, también debemos considerar el riesgo de que la clave quede comprometida si es interceptada por un tercero. Este método es más rápido que el método asimétrico.

Cifrado de extremo a extremo

Es la propiedad de algunos sistemas de comunicación que hace que los mensajes intercambiados sean ilegibles durante la comunicación en caso de interceptación al estar cifrados. Al ser de extremo a extremo, implica que solo emisor y receptor podrán descifrar y conocer el contenido del mensaje.

Cookie

Pequeño fichero que almacena información enviada por un sitio web y que se almacena en el equipo del usuario, de manera que el sitio web puede consultar la actividad previa del usuario.

Copia de seguridad

Copia de datos que se puede utilizar para restaurar el sistema en caso de un fallo o un ataque.

Correo spam

El spam, también conocido como correo electrónico comercial no solicitado (UCE), consiste en anuncios no deseados y cuestionables enviados por correo electrónico de forma masiva

Cortafuegos o firewall

Programa o dispositivo de hardware que analiza el tráfico de red entrante y saliente y, basándose en reglas predeterminadas, crea una barrera para bloquear tanto a virus como a atacantes.

D

Deepfake

Video o audio manipulado para hacer que parezca que alguien está diciendo o haciendo algo que en realidad no dijo o hizo.

DNS

Es aquel sistema que traduce los nombres de dominio y hace la función de un directorio de Internet. En lugar de memorizar las direcciones IP numéricas de cada sitio web que queremos visitar, los DNS nos permiten usar nombres de dominio fáciles de recordar, cómo www.google.com.

Dirección IP

Número único e irrepetible con el cual se identifica a todo sistema conectado a una red.

Doxing

Es una táctica de ciberataque que conlleva la recopilación y divulgación de información personal con malas intenciones.

E

Espionaje cibernético

Robo de información confidencial a través de medios electrónicos.

Estafas y fraudes online

Intentos de engañar a las personas para que les den dinero o información personal.

Email Spoofing

También conocido como suplantación de correo electrónico, es una técnica utilizada en ataques de spam y phishing para engañar a los usuarios haciéndoles creer que un mensaje proviene de una persona o entidad que conocen o en la que pueden confiar.

Encriptar

En criptografía, cifrar o encriptar es el proceso de codificar o darle un nuevo sentido a un mensaje o información de modo tal que sólo los individuos autorizados sean capaces de acceder a este, y aquellos que no estén autorizados no puedan hacerlo.

Evaluar

Quinto paso del Marco de Gestión de Riesgos (RMF) del NIST, para determinar si los controles establecidos se han implementado correctamente.

Exploit

Secuencia de comandos utilizados para aprovecharse de un fallo o vulnerabilidad en un sistema.

F

Firewall

Sistema de seguridad que protege una red de accesos no autorizados.

Firma digital

Una firma digital es un protocolo matemático que utiliza técnicas criptográficas para verificar la autenticidad e integridad de los mensajes o documentos digitales.

G

Gestor de contraseñas

Programa o aplicación que permite generar contraseñas robustas y almacenarlas cifradas junto con los nombres de usuario para diferentes sitios web y aplicaciones, con la facilidad de tener que recordar solo la contraseña de acceso al gestor.

Gusano

Es un programa malicioso que tiene como característica principal su alto grado de contagio, es decir, lo rápidamente que se propaga.

H

Hacker

Persona que tiene habilidades técnicas avanzadas en informática.

Hackeo ético

Hackeo realizado con fines de seguridad para identificar y corregir vulnerabilidades.

Honeypot

Sistema informático diseñado para atraer a los ciberatacantes, para que así los investigadores de seguridad puedan determinar cómo operan y qué es lo que buscan.

HTTP

Protocolo de transmisión de datos diseñado para transferir información entre los dispositivos conectados de la red, y se ejecuta sobre otras capas del conjunto de protocolos de la red sin ningún tipo de cifrado.

HTTPS

Es un protocolo de transmisión de datos que te permite navegar de forma segura al cifrar tu información y mantener tus actividades en línea protegidas.

Huella Digital

Es el registro del intercambio de información mediante internet que dejamos al utilizar dispositivos (Hardware) o aplicaciones (Software).

Implementar

Cuarto paso del Marco de Gestión de Riesgos (RMF) del NIST, que consiste en aplicar planes de seguridad y privacidad en una organización

Ingeniería social

Técnica de manipulación utilizada para engañar a las personas para que revelen información confidencial o realicen acciones que no deberían.

Insider

Persona perteneciente a una organización o empresa que divulga información sensible sobre dicha empresa de forma intencionada.

Información sensible

Término utilizado para referirse a los datos confidenciales que deben ser resguardados contra el acceso no autorizado.

Inyección SQL

Tipo de ataque que se aprovecha de una vulnerabilidad en la validación de los contenidos introducidos en un formulario web y que puede permitir la obtención de forma ilegítima de los datos almacenados en la base de datos del sitio web, entre ellos las credenciales de acceso.

K

Keyloggers

Son programas maliciosos que se ejecutan como un proceso en segundo plano en un ordenador u otro dispositivo y registran las pulsaciones de teclas que realiza un usuario sobre su teclado.

L

LAN

Una LAN (del inglés Local Area Network) o Red de Área Local es una red que interconecta dispositivos en un espacio limitado (oficina, casa, edificio) y permite conectar ordenadores, impresoras, servidores, discos duros externos, etc.

M

Malware

Es un programa malicioso, también conocido como programa maligno, programa malévolo, programa malintencionado o código maligno, es cualquier tipo de software que realiza acciones dañinas en un sistema informático de forma intencionada y sin el conocimiento del usuario.

Man-in-the-middle attack

Modalidad digital de interceptación en la comunicación entre dos partes.

Metadatos

Conjunto de datos relacionados con un documento y que recogen información fundamentalmente descriptiva del mismo, así como información de administración y gestión. Los metadatos es información que enriquece el documento al que está asociado.

Monitorear

Séptimo paso del Marco de Gestión de Riesgos (RMF) del NIST, que consiste en evaluar cómo están funcionando los sistemas.

N

Nube pública

Una nube pública o public cloud, es un modelo en el que un proveedor externo aloja un servicio que incluye soluciones de hardware, software, monitoreo y registro, gestión de identidad, recursos remotos para teletrabajadores y otras soluciones de centros de datos.

Open source o código abierto

Es un modelo compartido en que los desarrolladores de una aplicación comparten abiertamente la base de código entera de un proyecto, en vez de solo un proyecto compilado con archivos ejecutables.

P

Parche de seguridad

Actualización de software que corrige una vulnerabilidad de seguridad.

Pentesting

También conocido como pruebas de penetración, también llamadas pentesting, por la contracción en inglés de penetration testing, sirven como medida de protección para identificar vulnerabilidades en los sistemas y redes de una organización.

PGP

Pretty Good Privacy, es un programa para proteger la información transmitida por internet mediante el uso de criptografía de clave pública, así como facilitar la autenticación de documentos mediante firma electrónica.

Phishing

Ataque en el que el atacante envía correos electrónicos o mensajes de texto falsos para engañar a las personas para que revelen información confidencial.

Pharming

Ciberataque que redirige a los usuarios a sitios web fraudulentos o manipula sus sistemas informáticos para recopilar información delicada.

PIN

Acrónimo del inglés Personal Identification Number; en español, número de identificación personal. Tipo de contraseña, generalmente de cuatro dígitos, usada en determinados dispositivos y servicios para identificarse y obtener acceso al sistema.

Postura de seguridad

Capacidad de una organización para administrar la defensa de sus activos y datos críticos, y de reaccionar ante los cambios.

Preparar

Primer paso del Marco de Gestión de Riesgos (RMF) del NIST, relacionado con las actividades necesarias para gestionar los riesgos de seguridad y privacidad antes de que se produzca una vulneración.

R

Ransomware

Malware que cifra los datos del usuario y exige un rescate para descifrarlos. Hace referencia al secuestro de datos.

Reducción del riesgo

Proceso de disponer de los procedimientos y reglas adecuados para reducir rápidamente el impacto de un riesgo, como una vulneración.

Responsabilidad compartida

Idea de que todos los individuos dentro de una organización asumen un papel activo en la reducción del riesgo y el mantenimiento de la seguridad física y virtual.

Riesgo

Cualquier cosa que pueda afectar a la confidencialidad, integridad o disponibilidad de un activo.

S

Seleccionar

Tercer paso del Marco de Gestión de Riesgos (RMF) del NIST, que consiste en elegir, personalizar y capturar la documentación de los controles que protegen a una organización.

Smishing

El smishing es un ciberataque que se dirige a las personas a través de SMS (servicio de mensajes cortos) o mensajes de texto. El término es una combinación de “SMS” y “phishing”.

Software antivirus

Software que detecta y elimina malware.

Spear Phishing

Los ataques de spear phishing (literalmente “pesca con arpón”), al igual que los de phishing en general, son estafas en las que se intenta engañar al destinatario para que revele al atacante información confidencial, tales como credenciales de sus cuentas.

Suplantación de identidad

Robo de la identidad de una persona para cometer un delito.

Spyware

Es un software malicioso que se instala sin tu consentimiento, ya sea por medio de un ordenador tradicional, una aplicación en el navegador web o una aplicación móvil y busca tener el control de tu información, credenciales de acceso, servicios y dispositivos sin que te des cuenta

Stealers

Son aquellos programas informáticos maliciosos de tipo troyano que buscan rastrear y capturar información sensible que luego será enviada a los ciberdelincuentes que lo crearon.

T

Troyano

Son programas maliciosos que realizan acciones que no han sido autorizadas por el usuario. Estas acciones pueden incluir eliminación de datos, bloqueos, modificaciones, copias de datos e interrumpir el funcionamiento de un computadores o redes.

V

Virus informático

Un virus informático es una aplicación o código malintencionado que se emplea para ejecutar actividades destructivas en un dispositivo o red local.

Vishing

La mayoría de las personas han oído hablar del phishing; sin embargo, aunque el vishing es un ataque diferente, está dentro de la misma clasificación que el phishing y tiene objetivos en común.

VPN

Una VPN es una red privada virtual (del inglés, virtual private network) que agrega un nivel adicional de seguridad y anonimato a los usuarios cuando estos se conectan a servicios y páginas web.

Vulnerabilidad

Debilidad en un sistema informático o una red que puede ser explotada por un atacante.

W

White hat hacker

Hacker que utiliza sus habilidades para realizar hackeos éticos.

Z

Zero-day attack

Ataque contra una aplicación o sistema informático que tiene como objetivo la ejecución de código malicioso gracias al conocimiento de vulnerabilidades que son desconocidas para los usuarios y para el fabricante del producto.

FUENTES

- https://latam.kaspersky.com
- https://keepersecurity.com
- https://telefonica.com

ABC DE SEGURIDAD DIGITAL

· GLOSARIO BÁSICO ·

ESCUELA DE SEGURIDAD DIGITAL

Colnodo
Uso estratégico de Internet para el desarrollo

ESCUELADESEGURIDADDIGITAL.CO

@COLNODO