10 de abril de 2019

Glosario de términos de Ciberseguridad

Ciberespacio: es un ambiente compuesto por las infraestructuras tecnológicas, los componentes lógicos de la información y las interacciones sociales que se verifican en su interior.

Ciberseguridad: es tanto una condición caracterizada por un mínimo de riesgos y amenazas a las infraestructuras tecnológicas, los componentes lógicos de la información y las interacciones que se verifican en el ciberespacio, como el conjunto de políticas y técnicas destinadas a lograr dicha condición.

Cibercrimen: son los actos delictuales donde el ciberespacio es el objeto del delito o su principal herramienta para cometer ilícitos contra individuos, organizaciones, empresas o gobiernos.

Sistema informático: todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa.

Incidente cibernetico: evento que afecta la confidencialidad, integridad o disponibilidad de la información, como también la continuidad del servicio proporcionado por los sistemas que la contienen.

Infraestructura crítica de la información: las instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya afectación, degradación, denegación, interrupción o destrucción pueden tener una repercusión importante en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de los gobiernos de los Estados.

Amenaza: Circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor. Una amenaza puede tener causas naturales, ser accidental o intencionada. Si esta circunstancia desfavorable acontece a la vez que existe una vulnerabilidad o debilidad de los sistemas o aprovechando su existencia, puede derivar en un incidente de seguridad.

Antivirus: Es un programa informático específicamente diseñado para detectar, bloquear y eliminar código malicioso (virus, troyanos, gusanos, etc.), así como proteger los equipos de otros programas peligrosos conocidos genéricamente como malware.

Ataque de fuerza bruta: Un ataque de fuerza bruta es un procedimiento para averiguar una contraseña que consiste en probar todas las combinaciones posibles hasta encontrar la combinación correcta.

B2B: Abreviatura de "Business to Business". Este término se refiere a las transacciones comerciales entre empresas, utilizando medios telemáticos.

B2C: Abreviatura de "Business to Consumer". Este término se refiere a la estrategia que desarrollan las empresas comerciales para llegar directamente al cliente o consumidor final.

Puerta trasera o Backdoor: Se denomina backdoor o puerta trasera a cualquier punto débil de un programa o sistema mediante el cual una persona no autorizada puede acceder a un sistema.

Ransomware: El ciberdelincuente, toma control del equipo infectado y «secuestra» la información del usuario cifrándola, de tal forma que permanece ilegible si no se cuenta con la contraseña de descifrado. De esta manera extorsiona al usuario pidiendo un rescate económico a cambio de esta contraseña para que, supuestamente, pueda recuperar sus datos.

SMTP: El Protocolo Simple de Transferencia de Correo (o Simple Mail Transfer Protocol del inglés) es un protocolo de red utilizado para el intercambio de mensajes de correo electrónico. Este protocolo, aunque es el más comúnmente utilizado, posee algunas limitaciones en cuanto a la recepción de mensajes en el servidor de destino (cola de mensajes recibidos).

Sniffer: Programa que monitoriza la información que circula por la red con el objeto de capturar información.

Spoofing: Es una técnica de suplantación de identidad en la Red, llevada a cabo por un ciberdelincuente generalmente gracias a un proceso de investigación o con el uso de

malware. Los ataques de seguridad en las redes usando técnicas de spoofing ponen en riesgo la privacidad de los usuarios, así como la integridad de sus datos.

De acuerdo con la tecnología utilizada se pueden diferenciar varios tipos de spoofing:

- *IP spoofing*: consiste en la suplantación de la dirección IP de origen de un paquete TCP/IP por otra dirección IP a la cual se desea suplantar.
- *ARP spoofing*: es la suplantación de identidad por falsificación de tabla ARP. ARP (Address Resolution Protocol) es un protocolo de nivel de red que relaciona una dirección MAC con la dirección IP del ordenador. Por lo tanto, al falsear la tabla ARP de la víctima, todo lo que se envíe a un usuario, será direccionado al atacante.
- *DNS spoofing*: es una suplantación de identidad por nombre de dominio, la cual consiste en una relación falsa entre IP y nombre de dominio.
- *Web spoofing*: con esta técnica el atacante crea una falsa página web, muy similar a la que suele utilizar el afectado con el objetivo de obtener información de dicha víctima como contraseñas, información personal, datos facilitados, páginas que visita con frecuencia, perfil del usuario, etc. Los ataques de phishing son un tipo de Web spoofing.
- *Mail spoofing*: suplantación de correo electrónico bien sea de personas o de entidades con el objetivo de llevar a cabo envío masivo de spam.