INPEC
Instituto Nacional Penitenciario y Carcelario

GLOSARIO: TÉRMINOS DE SEGURIDAD DE LA INFORMACIÓN QUE DEBES MANEJAR.

OFICINA DE SISTEMAS DE INFORMACIÓN

ATACANTES DE SOMBRERO BLANCO

Personas u organizaciones que se dividen en redes o sistemas informáticos para descubrir las debilidades con la intención de mejorar la seguridad de estos sistemas.

ATACANTES DE SOMBRERO NEGRO

Personas u organizaciones que aprovechan las vulnerabilidades para obtener ganancias personales, financieras o políticas ilegales.

ATACANTES ORGANIZADOS

Organizaciones de delincuentes informáticos, hacktivistas, terroristas y/o comunidades patrocinadas por el estado.

BIOMETRÍA

Método de reconocimiento de personas basado en sus características fisiológicas (huellas dactilares, retinas, iris, cara, etc.).

BOTNET

Conjunto de ordenadores (denominados bots) controlados remotamente por un atacante que pueden ser utilizados para realizar actividades maliciosas como envío de spam,

BULO

También llamados hoax, son noticias falsas creadas para su reenvío masivo ya sea a través de redes sociales, mensajería instantánea o correo electrónico, con el fin de hacer creer al destinatario que algo verdadero..

CARTAS NIGERIANAS

Comunicación inesperada mediante correo electrónico o mensajería instantánea en las que el remitente promete negocios muy rentables. Utilizado por estafadores para involucrar a las potenciales víctimas en cualquier situación engañosa.

CIBERSEGURIDAD

Conjunto de recursos, políticas, conceptos de seguridad, directrices, métodos de gestión del riesgo, y formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el Ciberespacio.

CONFIDENCIALIDAD

Propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado.

COMPONENTES DE LA TRÍADA CIA

Confidencialidad, integridad y disponibilidad.

CRACKER

Su objetivo es crear virus e introducirse en otros sistemas para robar información y luego venderla al mejor postor.

DENEGACIÓN DE SERVICIO - DDOS

Ataque que interrumpe los servicios informáticos a los usuarios, los dispositivos o las aplicaciones.

DISPONIBILIDAD

Capacidad de un servicio, un sistema o una información, a ser accesible y utilizable por los usuarios o procesos autorizados cuando éstos lo requieran.

EXPLOIT

Secuencia de comandos para provocar un comportamiento no deseado en un sistema se suele perseguir el acceso a un sistema de forma ilegítima, para lograr la denegación de servicio del sistema.

FIREWALL - CORTAFUEGOS

Hardware y software que impide que los piratas informáticos accedan a la red y6 por lo tanto a los datos personales o empresariales.

FUGA DE DATOS

O fuga de información es la pérdida de la confidencialidad de la información privada de una persona, organización o empresa.

GUERRA CIBERNÉTICA

Conflicto basado en Internet que involucra la penetración de las redes y los sistemas informáticos de otras naciones.

GUSANO

Malware en forma de código malicioso que se replica independientemente de las vulnerabilidades de las redes. Se esparce muy rápidamente en una red porque se ejecuta por sí mismo.

HACKER

Persona con grandes conocimientos de informática que se dedica a acceder ilegalmente a sistemas de información ajenos y a manipularlos.

HACKTIVISMO

Forma de protesta realizada por aficionados o profesionales de la seguridad informática (Hackers) con fines reivindicativos de derechos, promulgación de ideas políticas o quejas de la sociedad en general, haciendo uso de los fallos de seguridad de las entidades o sistemas gubernamentales.

HOMBRE EN EL MEDIO (MITM)

Técnica en la que un atacante puede tomar el control de un dispositivo sin la autorización del propietario. Intercepta y captura información que pasa a través de los dispositivos en su camino hacia otro destino.

INCIDENTE DE SEGURIDAD

Suceso que afecta la confidencialidad, integridad o disponibilidad de los activos de información de la empresa, por ejemplo: acceso o intento de acceso a los sistemas, uso, divulgación, modificación o destrucción no autorizada de información.

INFORMÁTICA FORENSE

Consiste en un proceso de investigación en un evento de seguridad de los sistemas de información para detectar toda evidencia que pueda ser presentada como prueba fehaciente en un procedimiento judicial.

INGENIERÍA SOCIAL

Tácticas utilizadas para obtener información física o electrónica de una persona. Estas técnicas de persuasión suelen valerse de la buena voluntad y falta de precaución de la víctima.

INTEGRIDAD

Término que indica precisión, uniformidad y confiabilidad de los datos.

MALWARE

Código informático que se puede utilizar para robar datos, evitar los controles de acceso o dañar o comprometer un sistema.

NO REPUDIO

Permite probar la participación de las diferentes partes de una comunicación. El objetivo que se pretende es certificar que los datos, o la información, provienen realmente de la fuente que dice ser.

PARCHE DE SEGURIDAD

Conjunto de cambios que se aplican a un *software* para corregir errores de seguridad en programas o sistemas operativos.

PHISHING

Estafa cometida a través de medios telemáticos mediante la cual el estafador intenta conseguir, de usuarios legítimos, información confidencial (contraseñas, datos bancarios, etc.) de forma fraudulenta.

POLÍTICA DE SEGURIDAD

Decisiones o medidas de seguridad que una empresa ha decidido tomar respecto a la seguridad de sus sistemas de información después de evaluar el valor de sus activos y los riegos a los que están expuestos.

RANSOMWARE

Tipo de malware que mantiene un sistema de computación cautivo, con frecuencia mediante el cifrado de los datos esenciales, hasta que se realiza un pago al atacante.

· ROOTKIT

Malware diseñado para modificar los sistemas operativos a fin de permitir el acceso remoto no autorizado a través de una puerta trasera. Los rootkits pueden modificar los privilegios de usuario, los archivos de sistema, la informática forense del sistema y las herramientas de supervisión, por lo que son extremadamente difíciles de detectar y eliminar.

·

SNIFFER

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

SPOOFING

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.

SPYWARE

Malware diseñado para hacer un seguimiento de las acciones de los usuarios y capturar datos sin el conocimiento o el consentimiento del propietario del ordenador

TROYANO

Tipo de *malware* cuyo principal propósito es *dar acceso remoto a un sistema*. Trata de pasar desapercibido, para que un atacante remoto se introduzca en el ordenador.

VIRUS

Código malintencionado ejecutable que se adjunta a programas legítimos. Usualmente, los virus requieren la activación del usuario final y pueden ser relativamente inofensivos o muy destructivos. Con frecuencia se esparcen por las unidades USB, los medios ópticos, los recursos de red compartidos o los correos electrónicos.

VULNERABILIDAD

Estado viciado en un sistema informático (o conjunto de sistemas) que afecta las propiedades de confidencialidad, integridad y disponibilidad de los sistemas.

WHOIS

Base de datos de Internet pública que contiene información sobre nombres de dominio de Internet y las personas o las organizaciones que registraron los dominios. Es una fuente de información que se puede utilizar para atacar las vulnerabilidades del sistema.

ZOMBIE

Nombre que se da a los ordenadores controlados de manera remota por un ciberdelincuente al haber sido infectados por un *malware*.

FUENTES DE REFERENCIA

[1] http://www.iso27000.es/glosario.html#section10g

[2] Symantec Glosario de seguridad.
https://www.symantec.com/es/es/security_response/glossary/

[3] Viruslist. Glosario. https://securelist.com/encyclopedia/

[4] https://www.wikipedia.org/

[5] Glosario Seguridad de la Información MINTIC. https://www.mintic.gov.co/portal/604/w3-propertyvalue-1051.html

OFICINA DE SISTEMAS DE INFORMACIÓN

Grupo Proyección, Seguridad e Implementación Tecnologica.
proyecciontecnologica@inpec.gov.co