Clase 15“Amenazas informáticas”

Seguridad informática (Ciberseguridad)

- ✓ En las últimas dos décadas, las TIC han adquirido un valor en dimensiones que nunca antes había ocurrido en la historia, generando profundas transformaciones en todos los ámbitos socioeconómicos y, por supuesto, de la mano aparecieron conductas ilícitas cometidas sobre los datos, la información, los programas y todo aquel recurso tecnológico susceptible de ser manipulado ilícitamente.
- ✓ La seguridad informática, o ciberseguridad, es una disciplina que se encarga de proteger la integridad y la privacidad de los datos y toda la información que se encuentre alojada en un sistema informático.
- ✓ Va a identificar, eliminar vulnerabilidades y proteger de ataques maliciosos a los equipos de cómputo, servidores, redes informáticas y todo aquel medio informático por el cual se transmita información, ya que se centra en el medio de comunicación por el cual va a viajar la información.
- ✓ Se han implementado medidas de seguridad física y lógicas en conjunto con la seguridad en Internet.

Tipos de amenazas (Malwares)

MALWARE (Malicious software): termino que describe a todos los software maliciosos, que tienen como objetivo infiltrarse o dañar un sistema de información sin el consentimiento del usuario (no se muestra al usuario, siempre esta oculto).
Los más conocidos y comunes son los virus, gusanos y troyanos.

Virus:

- → Su objetivo es permanecer en un sistema copiándose a sí mismo en varios lugares, desde el momento que se ejecuta en el sistema, por eso cuando intentamos eliminar un archivo que ha infectado, el virus seguirá en otras partes del sistema.
- → Destruye o inhabilita archivos o programas del dispositivo, además de afectar el funcionamiento del mismo.
- → No tiene la capacidad por sí mismos de infectar a otros dispositivos a menos que lo pasemos por medio de un hardware (son de poca infección) porque se replican a sí mismos solo dentro del mismo dispositivo.

Gusanos:

- → Aparecieron cuando las computadoras se conectaron a la red, este no solo se copia a sí mismo en el sistema, sino que además utiliza la red para copiarse a otras máquinas a través de las vulnerabilidades de la red o agujeros de seguridad.
- → El objetivo de estos es replicarse a si mismos hasta saturar el funcionamiento del sistema.
- → Tiene una mayor capacidad de infección, esto se debe a la evolución misma de la tecnología.

Troyanos:

- → Basados en el “Caballo de Troya” son una estructura utilizada para cargar ocultos virus, gusanos y otros malwares.
- → Requieren de la ejecución del usuario ya que no pueden duplicarse a sí mismo, por ejemplo, pueden estar en esos programas sin licencia que instalamos.
- → Pueden crear backdoors, que es una puerta trasera para que el dispositivo pueda estar controlado de forma remota por alguien más, por ejemplo para introducir spam.

Malwares más peligrosos

Spyware:

- → "software espías", no daña los dispositivos pero si roban toda la información del sistema.
- → Su objetivo es permanecer oculto para robar todo tipo de datos desde contraseñas, información bancaria, redes sociales, etc. También puede acceder a la cámara y el micrófono del dispositivo.
- → Suelen ingresar mediante un troyano o también pueden ser instalados como es el caso de kylo, un spyware que registra las pulsaciones del teclado para tener la información de qué es lo que el usuario escribe.

Rootkits:

- → Son un conjunto de software que van dirigidos al firmware del sistema o los programas de usuario.
- → Tienen acceso al dispositivo en modo sistema o kernel, esto les permite modificar procesos internos del sistema operativo, los archivos del sistema como los registros y a las cuentas de usuario
- → Se esconden de los software antivirus.

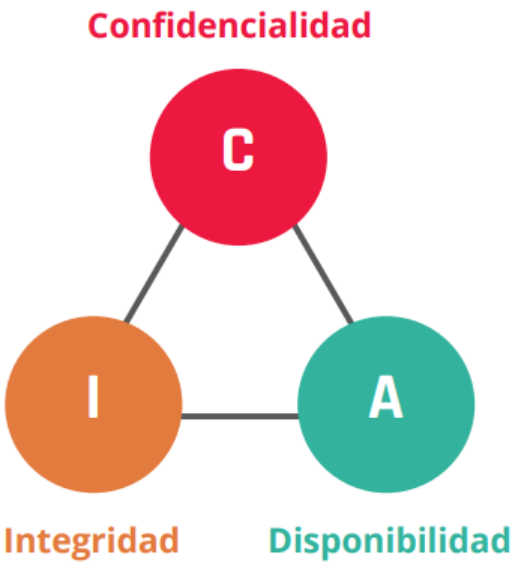
Botnet:

- → Es una red robot controlada por un atacante.
- → El artífice de la botnet puede controlar todos los ordenadores/servidores infectados de forma remota.
- → Se usa con el objetivo de cometer crímenes digitales o crimeware, como robo de identidad o información bancaria, chantaje, etc.
- → Suelen propagarse a través de troyanos.

Ransomware:

- → Software de secuestro que encrypta la información, te pide un rescate y generalmente igual te estafan (los archivos quedan con extensión ".conti").
- → Suelen ser usados por atacantes contra empresas para secuestrar la información de sus servicios y productos y luego pedir dinero a cambio de rescate, es un chantaje evidente ya que luego suele pedir una contraseña para poder acceder de nuevo a los datos.
- → Se pueden encontrar en archivos adjuntos de correos electrónicos no deseados, o supuestos mail de bancos o instituciones legales.

Principios de la seguridad de la información



*La información y sus 3 dimensiones (CIA)

1) INFORMACIÓN:

La información es recurso clave para tomar decisiones, dimensionar cosas, y disminuir riesgos. Los atacantes de un sistema van a tratar de vulnerar algunas de sus dimensiones.

2) INTEGRIDAD:

Consiste en que la información se encuentre completa, entera y que los datos que están dentro del sistema sean los que deberían ser. Un ejemplo de esta dimensión sería el ataque a una base de datos y la modificación de los datos que hay en la misma, con lo cual podemos seguir viendo la información, pero la misma es errónea debido a que la original fue alterada.

3) DISPONIBILIDAD:

Significa que la información una persona/usuario debe poder tener acceso a la información en el momento que lo necesita, es decir, en tiempo y forma. Un típico ataque a este tipo de dimensión es el ataque de denegación de servicio.

4) CONFIDENCIALIDAD:

Refiere a que la información tiene que estar disponible únicamente para las personas que tienen acceso a esta información y bloqueada para el acceso a terceros. Por ejemplo, los datos personales e historiales médicos.

Fallas y vulnerabilidades

Una falla, también conocida como bug, es un error en un programa o sistema operativo que desencadena un resultado indeseado. Existen varios tipos según su comportamiento:

Nombre	Descripción
Heisenbug	Basados en el principio de incertidumbre de Heisenberg se denominan a aquellos bugs que alteran o desaparecen su comportamiento al tratar de depurarlos.
Bohrbug	Nombrados así por el modelo atómico de Bohr, es una clasificación de un error de software inusual que siempre produce una falla al reiniciar la operación que causó la falla.
Mandelbug	Llamado así por el matemático Benoit Mandelbrot, un mandelbug es un fallo con causas tan complejas que su comportamiento es totalmente caótico.
Schroedinbugs	Son errores que no aparecen hasta que alguien lee el código y descubre que, en determinadas circunstancias, el programa podría fallar. A partir de ese momento, el "Schroedinbug" comienza aparecer una y otra vez.

Una vulnerabilidad es una debilidad o fallo de un sistema informático que puede poner en riesgo la integridad, confidencialidad o disponibilidad de la información.
La evaluación o detección de vulnerabilidades permite reconocer, clasificar y caracterizar los agujeros de seguridad.
Ítems recomendados:

- ✓ Evaluar cómo está constituida la red e infraestructura de la empresa.
- ✓ Delimitar quién puede y debe acceder a la información confidencial.
- ✓ Probar que las copias de seguridad realizadas funcionen.
- ✓ Identificar las partes más sensibles y esenciales del sistema.
- ✓ Realizar auditorías del estado de la seguridad informática.

Ingeniería Social

→ La ingeniería social es el método de obtener información confidencial a través de usuarios legítimos del sistema a atacar. Obtienen información de los usuarios a través de medios como teléfonos, emails, correo tradicional o contacto directo.

Técnicas de ingeniería social: varían según la interacción con la víctima: pueden ser de manera pasiva, no presenciales, presenciales no agresivas y agresivas.

Pretexting	Se presenta cuando un supuesto representante de algún servicio pregunta por información de la cuenta del cliente
Baiting	Consiste en colocar pendrives o memorias externas con malwares en lugares de personas escogidas puedan infectar sus computadoras
Phishing	Consiste en engañar a un grupo de personas mediante correos electrónicos, páginas web, perfiles de redes sociales o sms falsos con el fin de robar información
Vishing	Llamadas telefónicas mediante las cuales se busca engañar a la víctima suplantando a personas del gobierno o empresas para que la víctima revele información privada
Redes sociales	Esta técnica tiene dos grandes objetivos, obtener información de la víctima y por otro lado generar una relación con la misma por otro lado para poder así ser estafada
Ciberbullying	Esto puede o no limitarse al uso de internet, se utiliza para amenazar con difundir textos o imágenes que dañen o avergüencen a la victima
Grooming	Conjunto de estrategias en la que una persona adulta busca ganarse la confianza de un menor, para que a través de la tecnologia poder abusar o explotar sexualmente de la víctima
Sexting	Comprende el envío o recepción de contenido sexual a través de medios electrónicos, el mismo consiste en el intercambio de imágenes o videos sexuales, en especial a través de celular.
Sextortion	Forma de extorsión en la que se chantajea a una persona por medio de una imagen o video de si misma desnuda.

Actividad grupal- Grupo 9

NOTICIA: [Facebook Busts Palestinian Hackers' Operation Spreading Mobile Spyware (thehackernews.com)]

- ¿Qué tipo de amenaza es?
- ¿Cómo comienza y cómo se propaga esta amenaza?
- ¿Hay más de una amenaza aplicada?

1) Es un Spyware. *

2) Utilizaron ingeniería social en un intento de atraer a la gente a hacer clic en enlaces maliciosos e instalar malware en sus dispositivos. Para esto hicieron cuentas falsas y comprometidas para crear personas ficticias, a menudo haciéndose pasar por mujeres jóvenes, y también como partidarios de Hamas, Fatah, varios grupos militares, periodistas y activistas con el objetivo de construir relaciones con los objetivos y guiarlos hacia páginas de phishing y otros sitios web maliciosos.

3)Si, usaron un malware Android personalizado que se disfrazó como aplicaciones de chat seguras para capturar sigilosamente metadatos del dispositivo, capturar pulsaciones de teclas, y cargar los datos a Firebase y también desplegaron otro malware Android llamado SpyNote que venía con la capacidad de monitorear llamadas y acceder de forma remota a los teléfonos comprometidos.

** El spyware móvil existe desde que se generalizó el uso de dispositivos móviles. Dado que los dispositivos móviles son pequeños y los usuarios no pueden ver todo lo que se está ejecutando, es posible que estas acciones se desarrollen de forma inadvertida en segundo plano.*