Introducción a la informática

Módulo 5. Evitando el naufragio

Clase 24. Amenazas y Seguridad Informática

Julio 22 de 2021

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.

Malware: Software malicioso: Virus, Troyanos, Gusanos.

Virus:
Componente de software cuyo objetivo es permanecer en un sistema copiándose a sí mismo. Buscar destruir o inhabilitar archivos o programas. Se adhieren a los archivos ejecutables o al registro maestro de arranque.

Gusanos:
Utiliza la red para copiarse a otras máquinas a través de la vulnerabilidad de la red o agujeros de seguridad. Su objetivo es saturar el funcionamiento del sistema.

Troyanos:
Estructura utilizada para cargar componentes ocultos como virus y gusanos. Con frecuencia son programas sin licencia y cracks. No pueden replicarse a sí mismo. Pueden generar "backdoors", puertas traseras que podrían permitir que el dispositivo sea controlado de forma remota.

Adware:
Su objetivo es bombardear el dispositivo con publicidad.

Spywares:
Software espía. Puede robar toda la información del sistema. Algunos pueden acceder a la cámara y al micrófono del dispositivo. Suelen ingresar por troyanos o pueden ser instalados como keylogger.

Rootkits:
Conjuntos de software. Van dirigidos al Firmware(?) del sistema o los programas de usuario y tienen acceso al dispositivo en modo sistema o kernel. Pueden modificar los procesos internos del sistema operativo, a los archivos del sistema como los registros y a las cuentas de usuario. Logran ocultarse del software antimalware o antivirus.

Botnet:

Red de bots controladas por un mismo dispositivo. Se utiliza para cometer crimeware, como robo de identidad o de información bancaria. Se propagan por troyanos.

Ransomware:
Software de secuestro. Utilizados contra empresas para secuestrar su información de sus servicios y productos. Se encuentran en correos no deseados o en links, y en redes P2P.

Información:
Integridad – Disponibilidad – Confidencialidad

Integridad
Que la información se encuentre completa y que los datos sean los que deberían ser. Que la información no haya sido modificada.

Disponibilidad
Que el usuario tenga acceso a la información en el tiempo y la forma que lo requiera.

Confidencialidad
Que la información esté disponible únicamente para los usuarios a quienes corresponde y bloqueada para los demás.

Protección de la Información
- Medidas preventivas
- Medidas reactivas

Protección de la confidencialidad
- Encriptación (preventiva)
- Controles de acceso (preventiva)
- Borrado remoto (reactiva)
- Capacitación al personal (preventiva)

Protección de la Integridad
- Auditorías (reactiva)
- Control de versiones (reactiva)
- Firmas digitales (preventiva)
- Detección de intrusos (reactiva)

Protección de la disponibilidad
- Tolerancia a fallos (preventiva/reactiva)
- Redundancia (preventiva)
- Parches de seguridad (reactiva)

Fallas y vulnerabilidades
Fallas
Una falla o bug es un error en un programa que desencadena un resultado indeseado.

Tipos de fallas:

Heisenbug: Alteran o desaparecen su comportamiento al tratar de depurarlos.

Bohrbug: Es una clasificación de un errorde software inusual que siempre produce una falla al reiniciar la operación quecausó la falla.

Mandelbug: Es un fallo con causas tan complejas que su comportamiento es totalmente caótico.

Schrodinbug: 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.

Vulnerabilidad:
Es una debilidad o falla de un sistema informático que pone en riesgo la integridad, confidencialidad o disponibilidad de la información.

Sincrónico

https://docs.google.com/document/d/1bKsOP-mrGNX50V0HKZkJGL6gj1kQklf5-HdbuEXYj-E/edit

https://docs.google.com/presentation/d/15EDOU0dWmkDyTx43FUmUi_5SxwshFC3GnNLCUySOBp4/edit#slide=id.p

En la mochila:
Hasta clase 21. Para la clase 21 subir un archivo cualquiera.