**Mochila del viajero**

Introducción a la informática

Clase 15. AMENAZAS INFORMATICAS

# **Resumen de clase:**

**Malware**

**Software malicioso**

Infiltración, daño al sistema de información.

**Virus**

Objetivo: permanecer en un sistema copiándose a sí mismo en varios lugares para que cuando el usuario borre el archivo infectado, el virus quede en memoria ya que ha infectado otras partes del sistema.

* El virus destruye o inhabilita archivos o programas.
* De poca infección ya que se replica dentro del mismo dispositivo.

**Gusano**

Objetivo: Usar la red para copiarse a otras máquinas.

* El gusano se replica así mismo hasta saturar el funcionamiento del sistema.
* De mayor capacidad de infección.
* Una forma para actuar y atacar el gusano es apagar la red y desinfectar equipo por equipo.

**Troyano**

* Objetivo: actuar como estructura para otros malwares, no hace daño en sí mismo.
* Pueden ser programas sin licencia, cracks.
* No pueden replicarse a sí mismos. Requieren la ejecución del usuario.
* Pueden crear BACKDOORS (puerta trasera para que un dispositivo pueda ser controlado de forma remota).
* Pueden usarlo como un servidor proxy para ocultar ataques.
* Pueden introducir spam a nuestro equipo (**adwares)** bombardeo de publicidad, no son dañinos y generalmente vienen dentro de troyanos.

**Spyware**

* Malware más sutil. Software espía. No daña los dispositivos pero si roba toda la información del sistema. (contraseñas, información bancaria, pueden entrar por cam o micrófono). Objetivo: permanecer oculto para robar.
* Suelen ingresar en troyanos o instalados (keyloguer).

**Rootkits**

* Son un conjunto de softwares. Los demás malwares atacan al S.O, entonces al reinstalar el sistema desaparece. Por lo contrario, los rootkits van dirigidos al firewall de sistema o programas de usuario teniendo acceso a dispositivo en modo sistema o kernel. Lo que les permite modificar procesos internos del S.O, archivos del sistema como los registros o cuentas de usuario.
* Logran esconderse de los software antimalwares, o antivirus.

**Botnets**

**Bot:** robot **Net:** red

* Red de robots puesto por un atacante en una red de pc para ser controladas todas al mismo tiempo. Objetivos: crímenes digitales o crimeware, como robo de identidad o información bancaria, chantaje entre otros.
* Troyanos suelen ser causantes de la propagación de botnets.

**Ransomware**

* Software de secuestro. Encripta toda la información y pide rescate.
* Para secuestrar información de productos y luego pedir dinero a cambio del rescate. Hace evidente chantaje por secuestro. Se pueden encontrar en archivos emails no deseados o links según de bancos o instituciones legales.
* Se puede evitar: haciendo backups.

**Protección de la información**

* **Confidencialidad:** disposición de la información privada únicamente a quién tenga acceso, y bloquearse a terceros, como datos personales o historiales médicos.

**PROTECCION:**

**\*Encriptación:** cambiar formato de los datos por si son interceptados no puedan ser leídos (preventivo).

**\*Control de acceso:** asegurar que solo personal autorizado pueda acceder a la información (preventivo).

**\*Borrado remoto:** en caso de perder acceso, tener la capacidad de bloquear el dispositivo o borrar la información (reactivo).

**\*Capacitación de personal:** concepto de ingeniería social. Capacitar a los usuarios que generalmente son engañados para otorgar sus accesos (preventivo).

* **Integridad:** información completa y entera. Se vulnera esta propiedad atacando la base de datos y alterándolos. Podemos seguir viendo los datos pero modificados.

**PROTECCION:**

**\*Auditorías:** comprobar si la información coincide con su estado correcto (reactivo).

**\*Control de acceso:** herramienta para volver a un estado anterior (reactivo).

**\*Firmas digitales:** asegurar autenticidad del documento (preventivo).

**\*Detección de intrusos:** detectar problemas al acceder un agente no autorizado (reactivo).

* **Disponibilidad:** Poder tener acceso a la información al momento de necesitarlo. Un típico ataque sería la denegación del servicio.

**PROTECCION:**

**\*Tolerancia a fallos:** capacidad de los sistemas ante un fallo poder utilizar la información (preventivo o reactivo).

**\*Redundancia:** información y validaciones de acceso repetidas para asegurarlas (preventivo).

**\*Parches de seguridad:** ante una falla, solucionar la vulnerabilidad y actualizar para que no vuelva a ocurrir.

**Fallas y Vulnerabilidades**

* **Fallas:** error, bug. Error en programa o s. operativo que desencadena resultado indeseado. Bug (1947) cuando Grace Hopper mientras programaba el Mark II, descubre que un insecto (bug) había provocado el error en uno de sus relés electromagnéticos.

**Tipos de Bugs:**

**1. Heisenbug:** basados en el principio de incertidumbre de Heinserberg. Son aquellos bugs que alteran o desaparecen su comportamiento al tratar de depurarlos.

**2. Bohrbug:** basados en el modelo atómico de Bohr. Errores de software inusual que siempre produce una falla al reiniciar la operación que causó la falla.

**3. Mandelbug:** basado en el matemático Benoit Mandelbrot. Son fallos con causas tan complejas que su comportamiento es totalmente caótico.

**4. Schroedinbugs:** errores que no aparecen hasta que alguien lee el código y descubre que en determinadas circunstancias el programa podría fallar.

* **Vulnerabilidades:** debilidad de un sistema que puede poner en riesgo la integridad, confidencialidad o disponibilidad de la información.

**Pasos para detectarlas:**

1. Evaluar la constitución de la red e infraestructura.

2. Delimitar quién puede acceder a la información confidencial.

3. Probar funcionamiento de las copias de seguridad.

4. Identificar las partes más sensibles y esenciales.

5. Realizar auditorías del estado de la seguridad.