15 - Amenazas Informáticas

lunes, 3 de mayo de 2021 17:55

MALWARE: Malicious Software. Necesita estar oculto del usuario.

- **Virus**: el objetivo es permanecer en el sistema copiandose en varios lugares. El objetivo es destruir o inhabilitar archivos y programas. No pueden afectar a otros dispositivos (son de poca infección).
- **Gusanos**: también se copia a otras máquinas mediante vulnerabilidades de la red. Se replica hasta saturar el funcionamiento del sistema. Es altamente infeccioso.
- **Troyanos**: suelen ser programas sin licencias y cracks.
- **Adwares**: bombardean el dispositivo con publicidad.

- **Spywares**: roban todo tipo de información (contraseñas, información bancaria, detectan teclas, usan cámara).
- **Rootkits**: tienen acceso al dispositivo en modo sistema o kernel, y les permite realizar cambios a los procesos internos del SO y a los archivos. Se pueden esconder de antimalwares.
- **Botnets**: red de bots para realizar crímenes digitales (crimeware).
- **Ransomware**: secuestran la información de una empresa (las encriptan con contraseñas) y luego pedir dinero a cambio de liberarlo.

INGENIERÍA SOCIAL: Se basa en distintos métodos para engañar al usuario, para conseguir datos como contraseñas o información bancaria.

- **Pretexting**: 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 para que puedan infectar sus computadoras.
- **Phishing**: consiste en engañar a un grupo de personas mediante correos electrónicos, páginas webs, sms falsos, etc., para robar información.
- **Vishing**: llamads telefónicas suplantando a personas del gobierno/empresas para engañar a las víctimas.
- **Redes Sociales**: obtener información de la víctima y generar una relación con la persona para así ser estafada.
- **Ciberbullying**: se utiliza para amenazar con difundir textos e imágenes que dañen o avergüencen a la víctima.
- **Grooming**: persona adulta engaña a un menor para abusar sexualmente de la víctima.
- **Sextortion**: extorsión en la que se chantajea a una persona involucrada en contenido sexual gracias al sexting (intercambio digital de contenido sexual en imágenes).

La INFORMACIÓN cuenta con tres dimensiones conocidas como **Confidenciality**, **Integrity**, **Accesibility**. Los atacantes de un sistema intentarán vulnerar alguna de esas dimensiones:

Para proteger la información, se toman MEDIDAS PREVENTIVAS, como la Encriptación, los Controles de Acceso, el Borrado Remoto, la Capacitación de Personal, la Detección de intrusos, el Control de Versiones y los Parches de Seguridad.

FALLA (BUG): error en un programa con resultado indeseado.

- **Heisenbugs**: alteran o desaparecen su comportamiento al tratar de depurarlos.
- **Bohrbugs**: error de software inusual que siempre produce una falla al reiniciar la operación que causó la falla.
- **Mandelbugs**: son fallos con causas tan complejas que su comportamiento es totalmente caótico.
- **Schrödinbugs**: no aparecen hasta que alguien lee el código y descubre que el programa podría fallar. A partir de ese momento, el "schrödinbug" aparece una y otra vez.

VULNERABILIDAD: es una debilidad o fallo de un sistema informático que pone en riesgo la integridad, confidencialidad o disponibilidad de la información.