AMENAZAS INFORMATICAS

Materia	Intro Informatica

Ciberseguridad

La seguridad informática se enfoca en la protección de la infraestructura computacional y todo lo vinculado con la misma, especialmente, en la información que se transmite a través de las redes de computadoras.

Para minimizar todos los riesgos se han creado a lo largo de la historia múltiples métodos, como estándares, protocolos, reglas, herramientas y obviamente leyes informáticas.

La seguridad informática únicamente se va a centrar en el medio de comunicación por el cual va a viajar la información, esta va a identificar, eliminar vulnerabilidades y proteger de ataques maliciosos a todo aquel medio informático por el cual se transmita información.

Principios de la seguridad de la información

La informacion cuenta con ***tres dimensiones*** que los atacantes de un sistema van a tratar de vulnerar. Estas son:

- Integridad

La información se encuentre completa, entera y que los datos que están dentro del sistema sean los que deberían ser.

Ejemplo: ataque a una base de datos y la modificación de sus datos, con lo cual podemos seguir viendo la información, pero la misma es errónea debido a que la original fue alterada.

- Disponibilidad

Una persona/usuario debe poder tener acceso a la información en el momento que lo necesita, es decir, en tiempo y forma.

Ejemplo: ataque de denegación de servicio.

- Confidencialidad

La información tiene que estar disponible únicamente para las personas que tienen acceso a esta y bloqueada para terceros.

Ejemplo: datos personales e historiales médicos.

Protección de la información

Se basa en ***garantizar el completo y total funcionamiento de las 3 dimensiones***, para ello, debemos implementar medidas preventivas y reactivas.

Medidas preventivas: todas las acciones que pueden tomarse para evitar problemas no deseados.

Medidas reactivas: donde ya se ocasionó un problema de seguridad y hay que solventarlo.

- Protección de la confidencialidad

Puede romperse de varias maneras, tanto directas (hackeando la seguridad) como indirectas a través de errores humanos.

Técnicas para asegurarla:

Nombre	Descripción
Encriptación	Significa cambiar el formato de los datos con la razón de que si estos son interceptados solo las personas autorizadas sepan cómo leerlos (medida preventiva).
Controles de acceso	Asegurar que solo las personas autorizadas puedan acceder a la información (medida preventiva).
Borrado remoto	Se refiere al esfuerzo de mantener los datos siempre privados, en el caso de que se perdiera el acceso, la capacidad de bloquear el dispositivo o borrar la información (medida reactiva).
Capacitación al personal	Existe un concepto llamado **ingeniería social**, el cual es la denominación que se le da a cómo los usuarios son engañados para otorgar sus accesos, la capacitación en estos problemas es una acción preventiva para evitarlos.

- Protección de la integridad

Puede romperse de maneras similares a la de la confiabilidad, por lo cual, varias de sus acciones de seguridad son reutilizadas. A

Técnicas para asegurarla:

Nombre	Descripción
Auditorias	Se utilizan para comprobar que la información coincide con lo que debería ser correcto (medida reactiva).
El control de versiones	Si ha ocurrido un inconveniente con la información, diversas herramientas de control de versiones ayudan a "volver a un estado anterior" (medida reactiva).
Firmas digitales	Esta medida permite asegurar la autenticidad del documento (medida preventiva).
Detección de intrusos	Diseñados para detectar problemas cuando un acceso no autorizado se ha cometido (medida reactiva).

- Protección de la disponibilidad

La disponibilidad debe tenerse en cuenta para cuando ocurra un problema de seguridad como de forma preventiva al mismo.

Técnicas para asegurarla:

Nombre	Descripción
Tolerancia a fallos	La capacidad de los sistemas o servidores a que si algún tipo de fallo sucede, la información pueda ser utilizada (preventiva o reactiva dependiendo la situación).
Redundancia	De esta forma la información y las validaciones de acceso se repitan tanto que la información está segura de no perderse en su totalidad (preventiva).
Parches de seguridad	Cuando se detecta una falla, debe solucionarse el problema para que no vuelva a ocurrir, igualmente si la falla fue por un software, actualizarlo con la vulnerabilidad resuelta.

Fallas

Una falla (bug) es un error en un programa o sistema operativo que desencadena un resultado indeseado.

En el desarrollo del software existen muchos tipos de fallas, pero en general se pudieron establecer tipos de bugs según su comportamiento.

Tipos de fallas

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.

Vulnerabilidades

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.

Pasos para detectar una vulnerabilidad

Si bien no existe un método único para detectar vulnerabilidades, los siguientes ítems son recomendables para considerar nuestra información segura:

- 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 auditorias del estado de la seguridad informática

Tipos de amenazas informáticas

Sofware maligno = malware = malicius software

Se usa este termino para describir a todos los software maliciosos que tienen como objetivo infiltrarse o dañar un sistema de información sin el consentimiento del usuario.

Grupo 1:

Para que este pueda completar sus objetivos, debe estar oculto al usuario para que no lo note y elimine.

Virus

El mas antiguo, es un componente de software cuyo objetivo es permanecer en un sistema, copiándose a si mismo en varios lugares desde el momento que se ejecuta en el sistema. Asi, cuando eliminamos un archivo/programa infectado, el virus seguirá en memoria.

Su objetivo principal es eliminar o inhabilitar archivos/programas de nuestros dispositivos, ademas de afectar su funcionamiento.

La mayoria se adhieren a los archivos ejecutables o tambien al registro maestro de arranque.

En sí mismos no tienen la capacidad de afectar a otros dispositivos, a menos que lo pasemos por medio de un hardware como un USB, por ello es que se dice que **son de poca infección.**

Gusanos

Apareció cuando las computadoras comenzaron a conectarse a la red. No solo se copia a sí mismo en el sistema si no que utiliza la red para copiarse a otras máquinas a través de las vulnerabilidades de la red o agujeros de seguridad, usualmente sin que el usuario intervenga. Por ello es que tiene **mayor capacidad de infección.**

Su objetivo es replicarse a sí mismos hasta saturar el funcionamiento del sistema.

Troyanos

No causan daños en sí mismos si no que es una estructura utilizada para ccargar cosas ocultas (malwares).

Generalmente son programas sin licencia que instalamos pensando que no haran ningun daño porque no imaginamos que pueden ser un troyano.

Requieren de la ejecución el usuario ya que no pueden replicarse a si mismos.

Tambien puede crear Backdoors, una puerta trasera para que un dispositivo pueda ser controlado de forma remota por alguien más.

Pueden utilizarlo como un **servidor proxy** para ocultar ataques o para introducir **Spam a nuestro equípo → Adwares (bombardear nuestro dispositivo con publicidad),** estos no son dañinos y usualmente vienen dentro de troyanos.

Grupo 2:

Los siguientes malwares son cosiderados más peligrosos porque atacan de manera mas sútil y permanecen ocultos al usuario - excepto el Ramsonware-

Spyware

Softare espía, no daña los dispositivos pero roba toda la información del sistema.

Su objetivo es permanecer oculto para robar todo tipo de dato desde contraseñas, info bancaria, cuentas o acceder a nuestra cámara o micrófono.

Pueden ingresar en troyanos o ser instalados como el caso de Keyloger, el cual registra las pulsaciones del teclado para tener la información de lo que el usuario escribe.

Rootkits

Conjunto de software que van dirigidos al firmware o a los programas de usuario y no al sistema operativo. De esta forma tienen acceso al dispositivo en modo sistema o kernel.

Le permite realizar modificaciones a los procesos internos del sistema operativo, a los archivos del sistema como los registros e incluso a las cuentas usuario.

Logran esconderse de los antivirus.

Botnet

Red de robot puesto por un atacante en una red de computadoras para ser atacadas todas al mismo tiempo.

Principale¿mente tiene el objetivo de crear crimenes digitales (crimeware) como robo de identidad, de info bancaria, chantaje y mas.

Los troyanos tambien suelen ser los responsables de su propagación.

Ransomware

Sofwares de secuestro, suelen ser usados por atacantes contra empresas para secuestrar la información de sus servicios y productos y luego pedir dinero a cambio de rescate.

El ciberatacante hace evidente el chantaje por el secuestro y generalmente suele pedir una contraseña para poder acceder de nuevo al sistema.

Este tipo de malwares se puede encontrar en archivos adjuntos de mails no deseados, en vinculos que aseguran venir de bancos o instituciones legales o en redes para compartir archivos como las P2P.