CLASE 15- AMENAZAS INFORMATICAS

INTRODUCCION A LA SEGURIDAD INFORMATICA:

CIBERSEGURIDAD Y TIPOS DE AMENAZA:

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 a la infraestructura y a la información se han creado a lo largo de la historia múltiples métodos, como estándares, protocolos, reglas, herramientas y obviamente leyes informáticas.

Debemos tener en cuenta que la seguridad informática únicamente se va a centrar en el medio de comunicación por el cual va a viajar la información. No debemos confundir este término con el de seguridad de la información, ya que esta última puede estar en diferentes medios y no solo en los medios informáticos.

Bajo este último concepto, la seguridad informática 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.

VIDEO PARTE 1:

Amenazas tecnológicas causadas por seres humanos el atacante utiliza un tipo de software maligno denominada Malware para que realice todo el proceso de piratería. Malware quiere decir Malicious Software, es un término que se usa para describir a todos los softwares maliciosos que tienen como objetivo infiltrarse o dañar un sistema de información sin el consentimiento del usuario.   
Para que este software malicioso pueda completar sus objetivos es primordial que este oculto el usuario ya que esto le permite seguir actuando. Cuando el usuario nota que hay algún tipo de malware hará lo necesario para eliminarlo.  
Malware: Virus, Troyanos, Gusanos.  
Amenazas tecnologías mas comunes:  
-Virus: Este tipo de malware 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. Así cuando intentamos eliminar un archivo o programa infectado, el virus seguirá ahí en memoria ya que ha infectado otras partes del sistema. Si lo pensamos, el virus informático actúa de manera similar al virus biológico. El objetivo de estos virus puede variar, pero en esencia va a ser destruir o inhabilitar archivos o programas que tengamos en nuestros dispositivos y además de afectar el funcionamiento de este.  
La mayoría de estos virus se dividen en archivos ejecutables o también en registro maestro de arranque. Estos virus no tienen la capacidad de por si mismos afectar a otros dispositivos a menos que lo pasemos de un hardware como un USB. Por eso decimos que son de poca inspección porque se replican a si mismos solo dentro del mismo dispositivo. Este es de los primeros malwares que afectaban a las computadoras mas antiguas antes de que estuvieran conectadas a la red.   
-Gusanos: Todo cambia cuando las computadoras con el tiempo se empiezan a conectar en la red y propicia la aparición de malware llamado gusano. Este malware no solo se copia a si 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 la seguridad. Por ello tiene una mayor capacidad de infección esto a su vez se debe a la evolución misma de la tecnología. Este avión (ejemplo covid, que antes el virus se quedaba en una ciudad, pero ahora con los aviones se traslada a más lugares) funciona como la red en la que viajan los gusanos para infectar otras máquinas. Por lo general, automáticamente sin que el usuario intervenga. El objetivo de estos gusanos es replicar a si mismos hasta saturar el funcionamiento del sistema.  
-Troyanos: no causan daño en si mismo, sino que están basados en el mítico caballo de troya. O sea, una estructura utilizada para cargar cosas ocultas en este caso, virus, gusanos y demás malwares. Los troyanos generalmente son esos programas sin licencias y cracks que instalamos pensando que no harán ningún daño porque no somos conscientes de que pueden ser un troyano. Requieren de la ejecución del usuario ya que no pueden duplicarse en si mismos.   
El troyano también puede generar pactos, es una puerta trasera para que un dispositivo pueda ser controlado (Backdoors) de forma remota por alguien más. Pueden usarlo como un servidor proxy para ocultar ataques o lo más común para introducir spam a nuestro equipo.  
Estos últimos son muy similar a los adwares cuyo objetivo es bombardear nuestro dispositivo con publicidad. No son adinos y usualmente vienen dentro de troyanos.

PARTE 2

En la red, nuestros equipos están constantemente expuestos a amenazas informáticas. Si bien todos los Malwares son bastante peligrosos porque siempre intentan robar nuestros datos. Existen malwares especialmente peligrosos que cuentan con un modo más sutil (más silenciosos y evidente) para robar que los diferencia de otros malwares como virus, gusanos y adwares.  
-Spyware (o software espía): este malware no daña los dispositivos, pero si roba toda la información del sistema. Su objetivo es permanecer oculto para robar todo tipo de datos, desde contraseñas, robo de información bancaria, redes sociales, entre otros. También puede acceder por la cámara o micrófono del dispositivo sin que el usuario lo note. Los Spyware suelen ingresar en troyanos o también puede ser instalados como es el caso de Keylover: un spyware que registra las pulsaciones del teclado para obtener la información de que es lo que el usuario escribe.   
-Rootkits: Existen malwares más complejos como Rootkits que en realidad son un conjunto de software. Los demás malwares atacan al sistema operativo entonces una vez que se reinstala el sistema desaparece el malware. Por lo contrario, los Rootkits van dirigidos al firmware del sistema o los programas de usuario y tienen acceso al dispositivo en modo sistema o kernel. Este acceso les permite a los Rootkits realizar modificaciones a los procesos internos del sistema operativo, a los archivos del sistema como los registros e incluso a las cuentas de usuario. Además los rootkits logran esconderse de los software antimalwares o antivirus.   
-Botnets(Bot=robot, net=red) que es la mezcla entre bot y net. Esto quiere decir que es una red de robots o un ejercito de zombies que es puesto por un atacante a una red de computadoras para ser controladas todas al mismo tiempo. Principalmente es utilizado para realizar crímenes digitales (crimeware) como robo de identidad o de información bancaria, chantaje, entre otros. Los troyanos también suelen ser los principales causantes de la propagación de botnets.

Todos los malwares anteriores se caracterizan por permanecer ocultos a los usuarios. Sin embargo, los Ransomware no lo hacen.  
-Ransomware: (o software de secuestro) suele ser usados por atacantes contra empresas para secuestrarle la información de sus productos y servicios y luego, pedir dinero a cambio del 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 pueden encontrar en archivos adjuntos de correos no deseados o al hacer clic en vínculos que aseguran venir de bancos o instituciones legales. También se encuentran en redes para compartir archivos como las p2p.

Existen muchos tipos de malware que amenzan la seguridad informática. Es importante:  
\*Ser cuidadosos con las descargas que realizamos en nuestros dispositivos y el uso de aplicaciones no autorizadas   
\*Evitar paginas peligrosas  
\*Usar un software antimalware.

PROTECCION DE LA INFORMACION:

Principios de la seguridad de la información:   
Información: La información es recurso clave para tomar decisiones, dimensionar cosas, y disminuir riesgos. La misma cuenta con tres dimensiones conocidas como: integridad, disponibilidad y confidencialidad, también llamadas CIA por sus siglas en ingles. Los atacantes de un sistema van a tratar de vulnerar algunas de esas dimensiones.

\*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.  
\*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.  
\*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.

![Texto

Descripción generada automáticamente con confianza media]()Protección de la información:   
La 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 se refiere a todas las acciones que pueden tomarse para evitar problemas no deseados. Por otro lado, las medidas reactivas son aquellas donde ya se ocasiono un problema de seguridad y hay que solventarlo.

![Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente]()![Tabla

Descripción generada automáticamente]()

FALLAS: una falla, también conocida como bug, es un error en un programa o sistema operativo que desencadena un resultado indeseado. El termino bug viene desde 1947 cuando Grace Hopper, mientras estaba programando el Mark II, descubrió que un insecto (bug) había provocado un error en uno de sus relés electromagnéticos.   
En el desarrollo del software existen muchos tipos de fallas, pero en general se pudieron establecer unos tipos generales de bugs según su comportamiento.

![Texto

Descripción generada automáticamente con confianza baja]()

VULNERABILIDADES: Una vulnerabilidad es una debilidad o fallo de un sistema informatico 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 metodo único para detectar vulnerablidades, es posible armar una serie de ítems a tener en cuenta para considerar nuestra información segura.   
\*Evaluar como esta constituida la red e infraestructura de la empresa.  
\*Delimitar quien puede y debe acceder a la información confidencial.  
\*Probar que las copias de seguridad realizadas funcionen.  
\*Identificar las partes mas sensibles y esenciales del sistema.  
\*Realizar auditorias del estado de la seguridad informática.