Clase 2-U3
Métodos de ataques

Que hemos visto hasta el momento

✓ Generación y distribución de llaves.

Seguridad Informática

La seguridad informática, también conocida como ciberseguridad, es el área relacionada con la informática y la telemática que se enfoca en la protección de la infraestructura computacional y todo lo vinculado con la misma, y especialmente la información contenida en una computadora o circulante a través de las redes de computadoras. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas, y leyes concebidas para minimizar los posibles riesgos a la infraestructura y/o a la propia información.

La ciberseguridad comprende software (bases de datos, metadatos, archivos), hardware, redes de computadoras, y todo lo que la organización entienda y valore como un riesgo si la información confidencial involucrada pudiera llegar a manos de otras personas, por ejemplo, convirtiéndose así en información privilegiada.

La forma más simple de definir qué es un **ciberataque** es la explotación deliberada de sistemas informáticos, empresas y redes dependientes de la tecnología. Estos ataques utilizan códigos maliciosos para alterar la lógica o los datos del ordenador, lo que genera consecuencias perjudiciales que pueden comprometer información y provocar delitos cibernéticos, como el robo de identidad.

Vulnerabilidad y Amenaza

Es bastante normal confundir vulnerabilidad con amenaza, ambos conceptos están relacionados pero son diferentes a la vez:

Vulnerabilidad

Una vulnerabilidad es un fallo o debilidad de un sistema de información que pone en riesgo la seguridad de la misma. Se trata de un “agujero” que puede ser producido por un error de configuración, una carencia de procedimientos o un fallo de diseño. Los ciberdelincuentes aprovechan las vulnerabilidades de los sistemas informáticos (por ejemplo, de los sistemas operativos) para poder entrar en los mismos y realizar actividades ilegales, robar información sensible o interrumpir su funcionamiento.

Las vulnerabilidades son una de las principales causas por las que una empresa puede sufrir un ataque informático contra sus sistemas. Por eso siempre es recomendable actualizar a las últimas versiones, las aplicaciones informáticas, sistemas de protección y sistemas operativos, pues esas actualizaciones contienen muchas correcciones sobre vulnerabilidades descubiertas.

Algunas pueden ser:

- humanas
- físicas
- de comunicación
- de software
- del hardware
- en los medios de almacenamiento

Vulnerabilidad y Amenaza

Es bastante normal confundir vulnerabilidad con amenaza, ambos conceptos están relacionados pero son diferentes a la vez:

Amenaza

Esta directamente relacionado con la vulnerabilidad, y eso es que la amenza es la explotación de una vulnerabilidad o un fallo, del cual el atacante se vale para vulnerar un sistema.

Algunos ejemplos pueden ser:

- Malware.
- Inyección SQL injection.
- Cross-Site Scripting (XSS).
- Intercepción.
- Ataques de contraseñas.
- Ataque DDoS.
- Configuración de seguridad incorrecta.

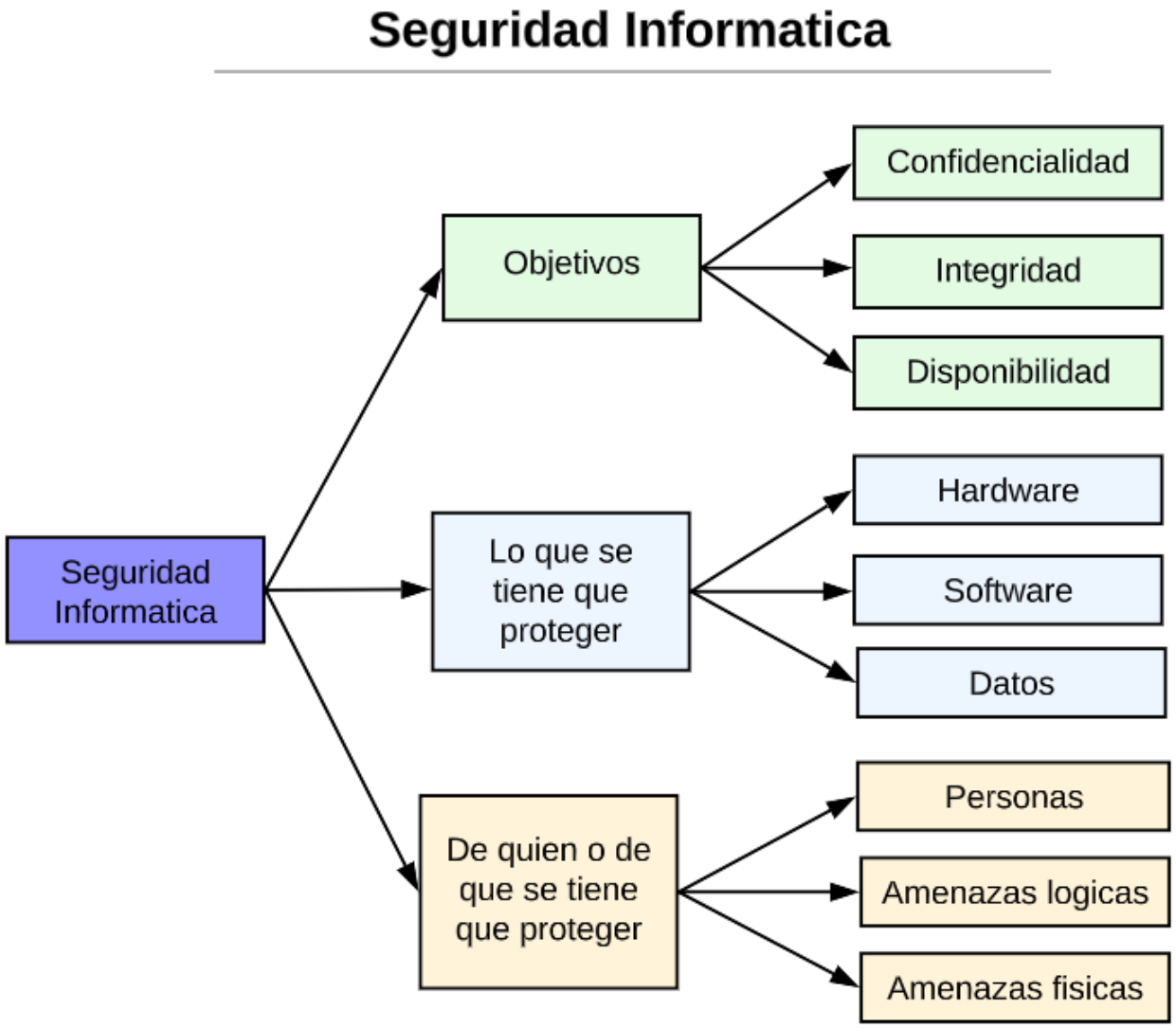
Ciberataque

En el extremo más complejo desde el punto de vista técnico, los **ciberataques** pueden implicar un equipo muy unido de hackers de élite que trabajan bajo el mandato de un estado nación. Su intención es crear **programas** que aprovechen fallas previamente desconocidas en el software. Así consiguen filtrar datos confidenciales, dañar infraestructura clave o desarrollar una bases para futuros ataques.

Los grupos de piratería más peligrosos se conocen como "**amenazas persistentes avanzadas**" (APT, por sus siglas en inglés). Pero no todos los ciberataques involucran habilidades técnicas de alto nivel o actores patrocinados por el estado. En el extremo opuesto de la escala se encuentran los hacks que aprovechan los errores de seguridad largamente fijados, las ambigüedades en las interfaces de usuario e incluso una buena supervisión humana pasada de moda.

Muchos piratas informáticos son oportunistas y no escogen los objetivos más valiosos, sino los menos defendidos, como los ordenadores que no tienen instaladas actualizaciones de seguridad o los usuarios que hacen clic en los enlaces maliciosos.

Esquema de seguridad Informática



Objetivos de la seguridad Informática

Los objetivos de la seguridad informática es mantener la Integridad, la Disponibilidad y Privacidad de los datos, por medio de aplicación de técnicas como el Control y la autenticidad de la información manejada por las sistemas informáticos, los sistemas de control y todo lo que maneje datos para su funcionamiento.

Integridad:

Los componentes del sistema permanecen inalterados a menos que sean modificados por personas con las credenciales adecuadas para hacerlo.

Disponibilidad:

Los usuarios deben tener disponibles todos los elementos del sistema, información, accesos, datos, para cuando sean necesario usar.

Privacidad:

Los elementos del sistema son accedidos solamente por los usuarios autorizados.

Lo que se tiene que proteger

Objetivos de la seguridad buscan la protección de los elementos fundamentales de la seguridad informática, que es lo que busca protegerse en un sistema informático?

Hardware:

Todo equipo relacionado a un sistema de información, seguridad física, periférica, de acceso, de procesamiento de información, de almacenamiento que gestione o procese datos.

Software:

Programas que ayudan a procesar, almacenar, controlar información, datos, acceso y controles dentro y fuera de un sistema informático.

Datos:

Información antes de ser procesada, almacenada generalmente en la combinación de HW y SW.

De quien o quienes se debe proteger

El objetivo es proteger los sistemas informáticos de en general, de amenazas de todo tipo, podríamos clasificarlas en estos 3 tipos.

Personas:

Personas con conocimientos y objetivos específicos que intentan obtener accesos no autorizados a sistemas informáticos, procesos o ambientes controlados para lo cual no tiene autorización, violaciones de accesos no autorizados de forma física.

Amenazadas lógicas:

Programas, algoritmos, virus de todo tipo diseñados para crear vulnerabilidades que permitan el acceso no autorizado.

Amenazas físicas:

Error o daño en Hardware que vulnere por permita el acceso indebido información o sistemas de forma no autorizada.

Ataques Lógicos

Afecta a la parte lógica del sistema es decir a la parte que no se puede tocar del ordenador (software). Este tipo de amenazas son más difíciles de prever y la mayoría no se pueden eliminar fácilmente hasta que no conozca la existencia del sistema.

Las amenazas Lógicas son más difíciles de reparar y causas mucho más daño que las amenazas Físicas y no influye sólo al funcionamiento del sistema informático si no que también se pueden perder fácilmente los datos del sistema.

- **Malware**: Es un software malicioso diseñado para infiltrarse o dañar una computadora o red sin el consentimiento del propietario. Esto puede incluir virus, gusanos, troyanos, ransomware, spyware y adware, entre otros.
- **Ataques de fuerza bruta**: Consisten en intentar descifrar contraseñas o claves de acceso mediante la prueba de múltiples combinaciones hasta encontrar la correcta.
- **Ataques de phishing**: Son intentos de engañar a los usuarios para que revelen información confidencial, como contraseñas o datos bancarios, a través de mensajes de correo electrónico o sitios web falsificados.
- **Ataques DDoS** (Denegación de Servicio Distribuido): Consisten en inundar un servidor o sistema con un gran volumen de tráfico, abrumándolo y haciéndolo inaccesible para los usuarios legítimos.
- **Ingeniería social**: Implica manipular a las personas para obtener información confidencial o acceso a sistemas, a menudo a través de la manipulación psicológica y social.
- **Ataques de inyección de SQL**: Consisten en aprovechar las vulnerabilidades en las aplicaciones web para inyectar código SQL malicioso y acceder, modificar o eliminar datos en una base de datos.

Ataques Lógicos

- **Ataques de interceptación o sniffing**: Implican el monitoreo y captura de datos transmitidos a través de una red para obtener información confidencial, como contraseñas o datos de tarjetas de crédito.
- **Ataques de suplantación o spoofing**: Consisten en falsificar la identidad de una entidad o usuario legítimo para obtener acceso no autorizado o engañar a otros usuarios.
- **Malware de rescate (ransomware):** Es un tipo de malware que cifra archivos o bloquea el acceso a un sistema y exige un rescate para desbloquearlo o descifrar los archivos.
- **Ataques de redes sociales**: Implican el uso de plataformas de redes sociales para obtener información confidencial o realizar actividades maliciosas, como la suplantación de identidad o la difusión de contenido malicioso.

Seguridad Lógica

Aplicación de barreras y procedimientos que resguarden el acceso a los datos y solo permita acceder a ellos a las personas autorizadas para hacerlo.

Dentro de la seguridad lógica tenemos:

Identificación:

El usuario se da a conocer en el sistema, demostrando ser quien dice ser, generalmente se usa un usuario.

Autenticación:

Verificación en el sistema antes la identificación, validar que el usuario es quien dice ser.

Criterios de autenticación - Verificación:

1. Algo que el usuario conoce – Password
2. Aldo que el usuario es – Huella digital, rostro, iris
3. Algo que el usuario hace – firmar
4. Algo que el usuario posee – Token

Algunos ataques famosos

https://www.computing.es/seguridad/noticias/1116703002501/10-ciberataques-mas-grandes-de-decada.1.html

https://www.bbc.com/mundo/internacional/2010/09/100926_virus_stuxnet_iran_planta_nuclear_aw

Algunos datos

Las 10 Principales Predicciones Y Estadísticas De Ciberseguridad Para 2023 según **CiberCrimeMagazine**

1. Se Prevé Que El Daño Global Por Ciberdelincuencia Alcance Los 10,5 Billones De Dólares Anuales Para 2025.
2. El Gasto Global En Ciberseguridad Superará Los 1,75 Billones De Dólares De Forma Acumulativa Entre 2021 Y 2025.
3. El Mundo Tendrá 3,5 Millones De Puestos De Trabajo De Ciberseguridad Sin Cubrir En 2023.
4. Se Prevé Que Los Costos Globales De Daños Por Ransomware Superen Los $ 265 Mil Millones Para 2031.
5. El Mundo Necesitará Ciberproteger 200 Zettabytes De Datos Para 2025.
6. Se Prevé Que El Mercado De Ciberseguros Alcance Los 14 800 Millones De Dólares Anuales Para 2025.
7. Se Prevé Que El Criptocrimen Le Costará Al Mundo 30.000 Millones De Dólares Anuales Para 2025.
8. Se Prevé Que Las Mujeres Ocupen El 30 % De Los Puestos De Seguridad Cibernética A Nivel Mundial Para 2025.
9. El 90 Por Ciento De La Población Humana, De 6 Años O Más, Estará En Línea Para 2030
10. El Mundo Necesitará Asegurar 338 Mil Millones De Líneas De Código De Software Nuevo En 2025.

Fuente (Actividad)

https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2021-to-2025/

Algunos datos

Laboratorio (60%)

Presentación de una amenaza y/o vulnerabilidad.

- El concepto de una de las dos.
- Demostración (técnicamente estoy solicitando una demo, para lo cual hay suficiente tiempo para investigar)
- Deberá hacerse un parejas (ya definidas en clase)

La clase del próximo sábado: Sábado 22

Laboratorio de Redes – 4to. nivel del EBLE

“Una computadora puede ser llamada inteligente si logra engañar a una persona haciéndole creer que es un humano”.

– Alan Mathison Turing.

Gracias