Clase 1. Ciberseguridad *18 de mayo del 2024*

---

1. Introducción a la ciberseguridad

1.1 ¿Qué es la ciberseguridad? La ciberseguridad, también denominada seguridad de las tecnologías de la información, se centra en la protección de los sistemas informáticos, las redes y los datos frente a robos, daños o accesos no autorizados. En el mundo interconectado de hoy en día, las ciberamenazas pueden proceder de diversas fuentes, como piratas informáticos, software malicioso e incluso empleados descontentos. El objetivo principal de la ciberseguridad es garantizar la confidencialidad, integridad y disponibilidad de los datos.

Por ejemplo, el ataque de ransomware WannaCry en 2017 afectó a cientos de miles de computadoras en todo el mundo, incluyendo hospitales, lo que demuestra el impacto significativo de las ciberamenazas en diferentes sectores.

La ciberseguridad es el conjunto de procedimientos y herramientas que se implementan para proteger la información que se genera y procesa a través de computadoras, servidores, dispositivos móviles, redes y sistemas electrónicos. De acuerdo con los expertos de la Information Systems Audit and Control Association (ISACA), la ciberseguridad se define como "una capa de protección para los archivos de información". También, para referirse a la ciberseguridad, se utiliza el término seguridad informática o seguridad de la información electrónica.

Estadísticas recientes muestran que los ciberataques han aumentado un 67% en los últimos cinco años, y se espera que las inversiones en ciberseguridad superen los $170 mil millones para 2024.

Según Cisco, la ciberseguridad es la práctica de proteger sistemas, redes y programas de ataques digitales. Por lo general, estos ciberataques apuntan a acceder, modificar o destruir la información confidencial, extorsionar a los usuarios o interrumpir la continuidad del negocio.

Cisco ofrece soluciones como Cisco Umbrella y Cisco Advanced Malware Protection (AMP), que ayudan a prevenir y detectar amenazas.

1.2 Historia de la ciberseguridad La ciberseguridad no nació hasta que se comenzaron a conectar los equipos y a desarrollarse redes de computadoras, lo cual ocurrió en los años 50, cuando se crearon las primeras redes informáticas y módems. Fue en los años 60 cuando la ciberseguridad comenzó a tomar la forma que conocemos en la actualidad.

Por ejemplo, en 1971, el virus Creeper fue el primer programa que se movía a través de ARPANET, y su contraparte Reaper fue desarrollado para eliminarlo, marcando el inicio de la ciberseguridad proactiva.

El malware en los años 80 incrementó su presencia y a la par se desarrollaron antivirus más eficientes. A finales de esta década, Kevin Mitnick utilizó ingeniería social para tener acceso a información personal y confidencial; este tipo de ciberataque, que comenzó a tener mayor uso en aquella época, sigue siendo uno de los métodos más populares para vulnerar los activos de una empresa. Sin embargo, se pueden prevenir y reducir con una buena estrategia, formación a colaboradores y protocolos de security awareness.

Otros casos famosos como el del Morris Worm en 1988, que infectó alrededor del 10% de las computadoras conectadas a Internet, llevaron a un mayor enfoque en la seguridad de la red y el desarrollo de CERTs (Computer Emergency Response Teams).

En 1970, el investigador Bob Thomas desarrolló un programa informático llamado Creeper, que podía moverse a través de la red de ARPANET (la primera red de computadoras). Para evitar esto, Ray Tomlinson, el creador del correo electrónico, desarrolló el programa Reaper, que se encargaba de perseguir y eliminar a los Creepers. Reaper fue el primer sistema antivirus de malware y el primer programa con la capacidad de autorreplicarse, es decir, fue el primer virus y a partir de esto se crearon los primeros gusanos y troyanos informáticos (es importante mencionar que no eran para nada programas maliciosos).

La evolución de los virus y el malware, como el famoso virus "ILOVEYOU" en el año 2000, llevó a la creación de una industria dedicada a los antivirus, incluyendo empresas como McAfee y Symantec, que desarrollaron soluciones para proteger contra estas amenazas.

A principios de los años 90, la necesidad de hacer frente a los ataques cibernéticos se convirtió en un tema de discusión internacional. La falta de conocimiento sobre el ciberespacio, de medidas de seguridad, jurisdicción y competencia afectaba sobre todo a los países desarrollados, donde el uso de la tecnología y el abuso de usuarios mermaban en la economía y sociedad. Las primeras acciones para crear mecanismos legales frente a los ciber delitos fueron locales. En 1986, en Estados Unidos, se creó la Computer Fraud and Abuse Act (CFAA), sin embargo, su capacidad se vio sobrepasada por la transformación tecnológica.

El ataque a la base de datos de la Universidad de Cornell por Robert Tappan Morris en 1988 fue uno de los primeros casos significativos que llevaron a la aplicación de la CFAA.

En 1995, se formó en Europa un comité de expertos en delitos informáticos para trabajar en estrategias y contrarrestar los ataques a través de Internet. Convencidos de la necesidad de aplicar una política penal para proteger a la sociedad frente a la ciberdelincuencia y la importancia de fortalecer la cooperación internacional, para 2001 se aprobó y firmó el Convenio de Budapest, que hoy en día es integrado por 56 países. El futuro de la seguridad cibernética está en la cooperación internacional, donde trabajar en el análisis de riesgos se vuelve imprescindible.

El Convenio de Budapest establece marcos legales para delitos informáticos, incluyendo la cooperación en la investigación de delitos cibernéticos, lo que ha facilitado la colaboración entre naciones para combatir la ciberdelincuencia.

1.3 Tipos de seguridad informática

1.3.1 Seguridad informática La seguridad informática constituye un amplio conjunto de medidas multidisciplinarias de protección para evitar que una red informática y sus datos sufran algún tipo de vulneración, filtración, publicación de información privada o ataque. La seguridad informática contempla cuatro áreas principales:

- Confidencialidad: Solo usuarios autorizados pueden acceder a recursos, datos e información.

- Integridad: Solo los usuarios autorizados deben ser capaces de modificar los datos cuando sea requerido.
- Disponibilidad: Los datos deben estar disponibles para los usuarios cuando sea necesario.
- Autenticación: Verificar que realmente se está en comunicación con quien se está comunicando.

Ejemplos prácticos incluyen el uso de cifrado para garantizar la confidencialidad de los datos y sistemas de respaldo para asegurar la disponibilidad de la información.

1.3.2 Seguridad de Red La seguridad de red se enfoca en la protección de la red de una empresa u organización, mediante medidas de protección que identifiquen y repelen amenazas externas, hackers, malware y virus.

Tecnologías comunes en seguridad de red incluyen firewalls, sistemas de detección de intrusos (IDS) y redes privadas virtuales (VPN), que ayudan a monitorizar y proteger el tráfico de red.

1.3.3 Seguridad de Datos Este tipo de seguridad es fundamental, ya que sus acciones se centran en proteger los datos durante el proceso de recopilación y gestión de los mismos. Así se protege la información de la compañía, como los datos de los clientes, informes financieros y registros de empleados. Uno de los pilares de la seguridad informática es la prevención de pérdida de datos.

Técnicas específicas incluyen el cifrado de datos en reposo y en tránsito, así como políticas de gestión de datos que aseguran que solo el personal autorizado pueda acceder a información sensible.

1.3.4 Seguridad de aplicaciones La seguridad informática de las aplicaciones empresariales es sumamente importante para que una organización opere de la mejor manera. Sus acciones se encargan de proteger las aplicaciones que usa una empresa, como el correo electrónico, la mensajería instantánea y los datos almacenados en ella.

Ejemplos de vulnerabilidades comunes incluyen inyecciones SQL y ataques XSS (cross-site scripting), y las pruebas de penetración regulares y actualizaciones constantes ayudan a mitigar estos riesgos.

1.3.5 Seguridad de la nube Este tipo de seguridad es más concreto, pero sus acciones abarcan muchas plataformas y software que operan en la nube. Busca la protección de los datos y aplicaciones alojadas en la nube, incluyendo la seguridad de su infraestructura y los datos almacenados en ella.

Las prácticas de seguridad en la nube incluyen el uso de cifrado, controles de acceso basados en roles (RBAC) y auditorías de seguridad periódicas para asegurar la integridad y confidencialidad de los datos en la nube.

1.3.6 Seguridad de la identidad Esta tiene que ver con la protección de la identidad digital de los empleados y los clientes, incluyendo el control de acceso y la autenticación de usuarios, como el SSO.

Métodos avanzados de autenticación, como la autenticación multifactor (MFA) y el uso de biometría, pueden aumentar significativamente la seguridad de la identidad digital.

1.4 Tipos de ciberataques y soluciones de seguridad Un ciberataque es un intento malicioso y deliberado por parte de un individuo o una organización para irrumpir en el sistema de información de otro individuo u otra organización. Usualmente, el atacante busca algún tipo de beneficio con la interrupción de la red de la víctima. Los cibercriminales utilizan diversas técnicas para acceder a redes corporativas, secuestrar información, instalar malware y comprometer los activos de las empresas o usuarios. A continuación, se muestran los tipos de ataques más comunes.

1.4.1 Ransomware El ransomware es un tipo de malware que cifra los archivos de la víctima y exige un rescate, generalmente en criptomonedas, para devolver el acceso a los datos. El número de ataques de ransomware ha crecido de forma exponencial, afectando a usuarios y empresas a través de diferentes técnicas. Para hacer frente a este ataque se recomienda hacer copias de seguridad de la información y utilizar servicios de almacenamiento en la nube.

Además, se sugiere el uso de software anti-ransomware específico y la formación de los empleados para reconocer correos electrónicos de phishing, que a menudo son el vector de ataque inicial.

1.4.2 Phishing El phishing es un ataque dirigido a usuarios a través del correo electrónico. Consiste en engañar al usuario para que comparta información confidencial, como contraseñas, números de tarjeta de crédito o datos personales. El atacante se hace pasar por una fuente confiable para obtener la información. Para prevenir este tipo de ataque se recomienda utilizar autenticación multifactor, capacitar a los empleados y tener filtros antiphishing.

Es importante explicar variantes del phishing, como spear phishing, que son ataques dirigidos a individuos específicos, y whaling, que se enfoca en objetivos de alto perfil como ejecutivos. Detectar estos ataques implica estar atento a correos inusuales y verificar siempre la autenticidad de las solicitudes de información.

1.4.3 Malware El malware es un término general para referirse a cualquier programa o código malicioso que daña los sistemas. Un atacante utiliza diferentes tipos de malware para destruir archivos, extraer información confidencial, espiar la actividad de un equipo o red y tomar el control de los sistemas. Entre los diferentes tipos de malware se encuentran los troyanos, gusanos, virus, spyware, adware y ransomware. Para prevenir estos ataques se recomienda mantener actualizados los sistemas, hacer uso de antivirus, evitar descargar archivos sospechosos y limitar los permisos de usuarios.

Algunos ejemplos recientes de malware incluyen Emotet, un troyano bancario que se propaga a través de correos electrónicos maliciosos, y TrickBot, que se utiliza para robar credenciales y desplegar ransomware.

1.4.4 Ataques de ingeniería social La ingeniería social no es un ataque en sí mismo, sino una técnica que aprovecha la confianza, la urgencia o la ignorancia del usuario para que éste realice acciones que comprometan la seguridad de la empresa. Ejemplos de esto son llamadas telefónicas fraudulentas, correos electrónicos falsos y engaños presenciales. Para mitigar este tipo de ataque es fundamental la formación y concienciación de los empleados.

Eemplos específicos de tácticas de ingeniería social, como el pretexting, donde el atacante inventa una historia creíble para obtener información, y el baiting, que utiliza promesas falsas para atraer a las víctimas. Las empresas pueden educar a sus empleados mediante simulaciones de ataques y programas de formación continua.

1.4.5 Ataques de denegación de servicio (DDoS) Un ataque de denegación de servicio distribuido (DDoS) consiste en saturar un servidor con una cantidad masiva de solicitudes, lo que provoca la interrupción del servicio para los usuarios legítimos. Los atacantes utilizan redes de computadoras comprometidas, llamadas botnets, para lanzar estos ataques. Para prevenir un ataque DDoS se recomienda contar con medidas de mitigación específicas, como el uso de firewalls, sistemas de detección de intrusos y servicios de mitigación de DDoS ofrecidos por proveedores de servicios en la nube.

Incluir información sobre herramientas y servicios específicos como Cloudflare, Akamai y Arbor Networks, que ofrecen soluciones avanzadas para mitigar ataques DDoS, puede ayudar a las empresas a protegerse eficazmente.

1.5 Técnicas de ciberseguridad y mejores prácticas Existen diversas técnicas de ciberseguridad que pueden implementar las empresas para proteger sus activos y datos.

Una referencia importante es el marco de ciberseguridad del NIST (National Institute of Standards and Technology), que proporciona una guía detallada para gestionar y reducir los riesgos de ciberseguridad.

1.5.1 Análisis de riesgos Una evaluación de riesgos implica identificar y analizar las posibles amenazas que pueden afectar a la infraestructura tecnológica y a los datos de una organización. El objetivo es comprender la probabilidad y el impacto de estos riesgos y desarrollar estrategias para mitigarlos. Este análisis debe realizarse regularmente para adaptarse a las nuevas amenazas y tecnologías.

Un ejemplo de metodología de evaluación de riesgos es el análisis FODA (Fortalezas, Oportunidades, Debilidades y Amenazas) adaptado a la ciberseguridad, que puede ayudar a identificar áreas críticas de mejora.

1.5.2 Definición de la política de seguridad Una política de seguridad de la información es un documento que establece las directrices y procedimientos que una organización debe seguir para proteger sus activos de información. Esta política debe incluir aspectos como la gestión de contraseñas, el control de acceso, la gestión de incidentes y la formación de empleados.

Una lista de elementos clave que deben estar presentes en una política de seguridad de la información eficaz incluye: clasificación de datos, políticas de uso aceptable, procedimientos de respuesta a incidentes y gestión de acceso y autenticación.

1.5.3 Auditorías de ciberseguridad Las auditorías de ciberseguridad son revisiones sistemáticas de los controles y procedimientos de seguridad de una organización para garantizar que son efectivos y cumplen con las regulaciones y estándares aplicables. Estas auditorías pueden ser internas o externas y deben realizarse periódicamente.

Mencionar algunos estándares y marcos de auditoría reconocidos, como ISO/IEC 27001 y COBIT, puede proporcionar una referencia para las organizaciones que buscan implementar prácticas de auditoría robustas.

1.5.4 Protección del perímetro La protección del perímetro implica asegurar los puntos de entrada y salida de la red de una organización para evitar accesos no autorizados. Esto incluye el uso de firewalls, sistemas de detección de intrusos (IDS) y sistemas de prevención de intrusos (IPS).

Proporcionar ejemplos de tecnologías específicas como Palo Alto Networks para firewalls y Snort para IDS puede ayudar a ilustrar cómo se implementan estas soluciones en la práctica.

1.5.5 Concienciación y formación del personal La formación y la concienciación de los empleados son cruciales para una estrategia de ciberseguridad efectiva. Los empleados deben estar informados sobre las amenazas de seguridad y las mejores prácticas para evitarlas. Esto puede incluir capacitación regular, simulacros de phishing y campañas de concienciación.

Incluir ejemplos de programas de formación exitosos, como los de SANS Security Awareness, y sus resultados en términos de reducción de incidentes de seguridad, puede proporcionar inspiración y modelos a seguir para otras organizaciones.

1.5.6 Uso de software antivirus y anti-malware El uso de software antivirus y anti-malware es esencial para detectar y eliminar amenazas en los sistemas de la organización. Este software debe mantenerse actualizado para proteger contra las amenazas más recientes.

Explicar la importancia de tener múltiples capas de defensa, como firewalls, antivirus y anti-malware, y cómo el uso combinado de estas herramientas contribuye a una estrategia de seguridad más robusta.

1.5.7 Contar con un equipo de seguridad Los responsables de la ciberseguridad deben contar con un equipo confiable de profesionales capacitados para dar soluciones y atender a las necesidades de una empresa para proteger sus activos. Este equipo debe estar preparado para responder a incidentes de seguridad y realizar mejoras continuas en las políticas y procedimientos de seguridad.

Describir los roles y responsabilidades típicos dentro de un equipo de seguridad de la información, como los analistas de seguridad, los ingenieros de seguridad y los responsables de cumplimiento normativo, puede ayudar a definir claramente las expectativas y funciones dentro de la organización.