IES EDUARDO PRIMO MARQUÉS

GOBIERNO DE ESPAÑA
MINISTERIO DE EDUCACIÓN Y FORMACIÓN PROFESIONAL

Unió Europea
Fons social europeu
L'FSE inverteix en el teu futur

Seguridad en redes en el mundo moderno

Fabiana Hung

Seguridad en redes en el mundo moderno

IES Eduardo Primo Marqués. Curso 2024/25

Contenido

1. Introducción

1.1 Importancia de la seguridad en redes en el mundo moderno

En la era digital actual, la seguridad en redes se ha convertido en un pilar fundamental para la protección de la información crítica que circula a través de Internet y redes privadas. A medida que la tecnología avanza y se integra cada vez más en nuestras vidas diarias, la cantidad de datos sensibles que se transmiten y almacenan en línea ha aumentado exponencialmente. Esta realidad ha generado una necesidad imperiosa de implementar medidas de seguridad robustas para salvaguardar la integridad, confidencialidad y disponibilidad de la información.

Importancia de la Seguridad en Redes

Protección de Datos Sensibles

La información personal, financiera y corporativa que se maneja en línea es un objetivo atractivo para los ciberdelincuentes. La protección de estos datos es esencial para prevenir fraudes, robos de identidad y pérdidas económicas significativas.

Prevención de Ataques Cibernéticos

Los ataques cibernéticos, como el phishing, ransomware y malware, son cada vez más sofisticados y frecuentes. La seguridad en redes juega un papel crucial en la detección y mitigación de estas amenazas, protegiendo tanto a individuos como a organizaciones.

Cumplimiento Normativo

Las regulaciones y leyes de protección de datos, como el GDPR en Europa, exigen que las organizaciones implementen medidas de seguridad adecuadas para proteger la información de sus usuarios. El incumplimiento de estas normativas puede resultar en sanciones severas y daños a la reputación.

Continuidad del Negocio

La seguridad en redes es vital para garantizar la continuidad operativa de las empresas. Un incidente de seguridad puede interrumpir las operaciones, causando pérdidas de productividad y afectando negativamente la confianza de los clientes.

2. Conceptos fundamentales de seguridad en redes

2.1 Definición de seguridad informática y seguridad en redes

La seguridad informática se refiere a la protección de los sistemas de información contra el acceso no autorizado, el uso indebido, la divulgación, la interrupción, la modificación o la destrucción. Incluye medidas para proteger tanto el hardware como el software y los datos.

Por otro lado, la seguridad en redes se centra específicamente en la protección de la infraestructura de red y los datos que se transmiten a través de ella. Esto incluye la protección contra ataques que buscan interceptar, alterar o destruir la información en tránsito.

Diferencias Clave

- **Seguridad Informática:** Enfocada en la protección de sistemas y datos en general.
- **Seguridad en Redes:** Enfocada en la protección de la infraestructura de red y los datos en tránsito.

2.2 Principios de la seguridad en redes

Confidencialidad

La confidencialidad asegura que la información solo sea accesible a las personas autorizadas. Esto se logra mediante técnicas como la encriptación y el control de acceso.

Integridad

La integridad garantiza que la información no sea alterada de manera no autorizada. Se utilizan métodos como las sumas de verificación y las firmas digitales para verificar la integridad de los datos.

Disponibilidad

La disponibilidad asegura que los sistemas y datos estén accesibles cuando se necesiten. Esto implica la implementación de medidas de redundancia y recuperación ante desastres.

Autenticación

La autenticación verifica la identidad de los usuarios y dispositivos que intentan acceder a los sistemas de red. Esto se puede lograr mediante contraseñas, tarjetas inteligentes, biometría, etc.

No Repudio

El no repudio asegura que una vez que una acción ha sido realizada, no se pueda negar su autoría. Esto es crucial para la responsabilidad y el seguimiento de actividades.

2.3 Tipos de redes

LAN (Local Area Network)

Las redes LAN conectan dispositivos dentro de un área geográfica limitada, como una oficina o un edificio. La seguridad en LAN incluye el uso de firewalls y sistemas de detección de intrusos.

WAN (Wide Area Network)

Las redes WAN abarcan áreas geográficas amplias, como ciudades, países o incluso continentes. La seguridad en WAN implica el uso de encriptación y VPNs para proteger los datos en tránsito.

MAN (Metropolitan Area Network)

Las redes MAN cubren áreas metropolitanas y son más grandes que las LAN pero más pequeñas que las WAN. La seguridad en MAN puede incluir medidas como el control de acceso y la segmentación de red.

PAN (Personal Area Network)

Las redes PAN conectan dispositivos personales en un área muy limitada, como un escritorio. La seguridad en PAN puede incluir el uso de encriptación y autenticación para proteger los datos.

Redes Inalámbricas

Las redes inalámbricas permiten la conexión de dispositivos sin cables. La seguridad en redes inalámbricas incluye el uso de protocolos de encriptación como WPA3 y la configuración de redes seguras.

Redes VPN (Virtual Private Network)

Las redes VPN permiten la creación de conexiones seguras a través de redes públicas. La seguridad en VPN se basa en la encriptación y la autenticación para proteger los datos transmitidos.

3. Amenazas y vulnerabilidades comunes en redes informáticas

3.1 Tipos de ataques a redes

3.1.1 Ataques de denegación de servicio (DoS y DDoS).7

Los ataques de denegación de servicio (DoS) y de denegación de servicio distribuido (DDoS) buscan hacer que un sistema o red no esté disponible para sus usuarios legítimos. Esto se logra sobrecargando el sistema con una cantidad excesiva de solicitudes, lo que provoca que los recursos se agoten y el sistema se vuelva inoperativo.

3.1.2 Ataques de intermediario (Man-in-the-Middle).

En un ataque de intermediario, el atacante intercepta y posiblemente altera la comunicación entre dos partes sin que estas lo sepan. Esto permite al atacante robar información confidencial, como credenciales de inicio de sesión, o manipular los datos transmitidos.

3.1.3 Ataques de inyección (SQL Injection, Cross-Site Scripting, etc.).

Los ataques de inyección, como la inyección SQL y el Cross-Site Scripting (XSS), implican la inserción de código malicioso en una aplicación para que esta ejecute comandos no autorizados. Estos ataques pueden permitir a los atacantes acceder a bases de datos, robar información o modificar el contenido de una página web.

3.1.4 Phishing y Spear Phishing.

El phishing es una técnica en la que los atacantes envían correos electrónicos fraudulentos que parecen provenir de fuentes confiables para engañar a los destinatarios y hacer que revelen información sensible. El spear phishing es una variante más dirigida, donde los atacantes personalizan los correos electrónicos para un individuo o una organización específica.

3.1.5 Malware en redes.

El malware es software malicioso diseñado para dañar, interrumpir o robar información de sistemas y redes. Los tipos comunes de malware incluyen virus, gusanos, troyanos y ransomware. El malware puede propagarse a través de correos electrónicos, descargas de software y vulnerabilidades en la red.

3.2 Vulnerabilidades más comunes en redes.

- **Contraseñas Débiles:** El uso de contraseñas fáciles de adivinar o reutilizadas en múltiples cuentas puede facilitar el acceso no autorizado.
- **Falta de Actualizaciones:** No mantener el software y los sistemas actualizados puede dejar vulnerabilidades conocidas sin parchear, lo que los hace susceptibles a ataques.
- **Configuraciones Incorrectas:** Configuraciones de red incorrectas o inseguras pueden abrir puertas a los atacantes.
- **Falta de Cifrado:** La transmisión de datos sin cifrar puede permitir a los atacantes interceptar y leer la información.

- **Acceso No Autorizado:** No implementar controles de acceso adecuados puede permitir que usuarios no autorizados accedan a recursos sensibles.

4. Protocolos y tecnologías de seguridad en redes

4.1 Protocolos de encriptación y autenticación

4.1.1 SSL/TLS.

SSL (Secure Sockets Layer) y TLS (Transport Layer Security) son protocolos que proporcionan comunicaciones seguras a través de una red. Utilizan encriptación para proteger los datos transmitidos entre el cliente y el servidor, asegurando la confidencialidad e integridad de la información.

4.1.2 IPsec.

IPsec (Internet Protocol Security) es un conjunto de protocolos que aseguran las comunicaciones a través de redes IP mediante la autenticación y encriptación de cada paquete IP en una sesión de comunicación. Es ampliamente utilizado en VPNs para proteger los datos en tránsito.

4.1.3 WPA3 y seguridad en redes inalámbricas.

WPA3 (Wi-Fi Protected Access 3) es el estándar de seguridad más reciente para redes inalámbricas. Ofrece mejoras significativas en la encriptación y autenticación, incluyendo una protección más robusta contra ataques de fuerza bruta y una mayor seguridad para redes abiertas.

4.1.4 VPN (Virtual Private Network).

Una VPN (Red Privada Virtual) crea una conexión segura y encriptada a través de una red pública, como Internet. Esto permite a los usuarios enviar y recibir datos de manera segura, protegiendo la información sensible de posibles interceptaciones.

4.2 Firewalls

4.2.1 Tipos de firewalls.

Filtros de Paquetes: Inspeccionan los paquetes de datos que entran y salen de la red, permitiendo o bloqueando el tráfico basado en reglas predefinidas.

Firewalls de Aplicaciones: Monitorean y filtran el tráfico de aplicaciones específicas, proporcionando una capa adicional de seguridad al centrarse en el contenido de las aplicaciones.

Firewalls de Inspección de Estado: Combinan las características de los filtros de paquetes y los firewalls de aplicaciones, manteniendo un registro del estado de las conexiones de red y tomando decisiones de filtrado basadas en el contexto de la comunicación.

4.2.2 Reglas de firewall.

Las reglas de firewall son configuraciones que determinan qué tráfico está permitido o bloqueado en una red. Estas reglas se basan en criterios como direcciones IP, puertos, protocolos y el estado de la conexión. La correcta configuración de estas reglas es esencial para mantener la seguridad de la red.

4.3 Sistemas de detección y prevención de intrusiones (IDS/IPS)

4.3.1 Función y tipos de IDS: Detección de actividades maliciosas.

Los Sistemas de Detección de Intrusiones (IDS) monitorean el tráfico de red en busca de actividades maliciosas o violaciones de políticas. Existen dos tipos principales de IDS:

- **IDS Basados en Red (NIDS):** Monitorean el tráfico de red en tiempo real.
- **IDS Basados en Host (HIDS):** Monitorean la actividad en un solo host o dispositivo.

4.3.2 Sistemas de prevención (IPS): Diferencias y mejoras sobre los IDS.

Los Sistemas de Prevención de Intrusiones (IPS) no solo detectan actividades maliciosas, sino que también toman medidas para prevenirlas. A diferencia de los IDS, los IPS pueden bloquear o rechazar el tráfico sospechoso automáticamente, proporcionando una capa adicional de protección.

5. Estrategias de mitigación y buenas prácticas en la seguridad de redes

5.1 Modelos de seguridad en capas: Explicar cómo proteger redes utilizando la seguridad por capas (física, red, transporte, aplicación).

La seguridad en capas es un enfoque integral para proteger redes y sistemas mediante la implementación de múltiples niveles de defensa. Cada capa aborda diferentes aspectos de la seguridad, proporcionando una protección más robusta y completa.

Capa Física

La capa física se refiere a la protección del hardware y los dispositivos físicos. Esto incluye medidas como el control de acceso a los centros de datos, el uso de cerraduras y cámaras de seguridad, y la protección contra desastres naturales.

Capa de Red

La capa de red se enfoca en la protección de la infraestructura de red. Esto incluye el uso de firewalls, sistemas de detección y prevención de intrusiones (IDS/IPS), y la segmentación de redes para limitar el acceso a recursos críticos.

Capa de Transporte

La capa de transporte asegura que los datos transmitidos a través de la red estén protegidos. Esto se logra mediante el uso de protocolos de encriptación como SSL/TLS e IPsec, que garantizan la confidencialidad e integridad de los datos en tránsito.

Capa de Aplicación

La capa de aplicación se centra en la seguridad de las aplicaciones y los datos que manejan. Esto incluye la implementación de controles de acceso, la encriptación de datos almacenados, y la protección contra vulnerabilidades como la inyección SQL y el Cross-Site Scripting (XSS).

5.2 Segmentación de redes: Uso de VLANs y subredes para mitigar riesgos.

La segmentación de redes es una estrategia para dividir una red en segmentos más pequeños y manejables, conocidos como subredes o VLANs (Virtual Local Area Networks). Esto ayuda a mitigar riesgos al limitar el alcance de un posible ataque y facilitar la implementación de políticas de seguridad específicas para cada segmento.

Uso de VLANs

Las VLANs permiten la creación de redes lógicas independientes dentro de una misma infraestructura física. Esto mejora la seguridad al aislar diferentes tipos de tráfico y restringir el acceso a recursos sensibles.

Uso de Subredes

La creación de subredes implica dividir una red más grande en segmentos más pequeños, cada uno con su propio rango de direcciones IP. Esto facilita la gestión del tráfico y la implementación de medidas de seguridad específicas para cada subred.

5.3 Seguridad en la nube: Herramientas y estrategias para asegurar redes y servicios en entornos de nube.

La seguridad en la nube se refiere a las herramientas y estrategias utilizadas para proteger los datos y servicios en entornos de nube. Esto incluye la encriptación de datos, la autenticación multifactor, y el uso de herramientas de monitoreo y gestión de seguridad.

Herramientas de Seguridad en la Nube

- **Encriptación de Datos:** Protege los datos en tránsito y en reposo mediante el uso de algoritmos de encriptación robustos.
- **Autenticación Multifactor (MFA):** Añade una capa adicional de seguridad al requerir múltiples formas de verificación antes de conceder acceso.
- **Monitoreo y Gestión de Seguridad:** Utiliza herramientas de monitoreo para detectar y responder a amenazas en tiempo real.

Estrategias de Seguridad en la Nube

- **Implementación de Políticas de Seguridad:** Definir y aplicar políticas de seguridad claras y coherentes para todos los usuarios y servicios en la nube.
- **Evaluaciones de Riesgos:** Realizar evaluaciones periódicas de riesgos para identificar y mitigar posibles vulnerabilidades.
- **Capacitación y Concienciación:** Educar a los usuarios sobre las mejores prácticas de seguridad y los riesgos asociados con el uso de servicios en la nube.

5.4 Concienciación y formación: Capacitar a los usuarios como primera línea de defensa.

La capacitación y concienciación de los usuarios es una parte crucial de la seguridad en redes. Los usuarios bien informados y capacitados actúan como la primera línea de defensa contra las amenazas de seguridad.

Capacitar a los Usuarios

- **Programas de Formación:** Implementar programas de formación regulares para educar a los usuarios sobre las mejores prácticas de seguridad y cómo identificar posibles amenazas.
- **Simulaciones de Ataques:** Realizar simulaciones de ataques, como ejercicios de phishing, para evaluar y mejorar la capacidad de respuesta de los usuarios.
- **Políticas de Seguridad:** Establecer y comunicar políticas de seguridad claras y accesibles para todos los usuarios.

Concienciación

- **Campañas de Concienciación:** Llevar a cabo campañas de concienciación para mantener a los usuarios informados sobre las últimas amenazas y tendencias en seguridad.
- **Recursos Educativos:** Proporcionar recursos educativos, como guías y tutoriales, para ayudar a los usuarios a mantenerse actualizados sobre las mejores prácticas de seguridad.

6. Conclusiones

6.2 Recomendaciones: Sugerir acciones concretas o mejores prácticas para garantizar la seguridad en redes.

- **Implementar Políticas de Seguridad Claras:** Establecer y comunicar políticas de seguridad claras y coherentes para todos los usuarios y dispositivos en la red.
- **Mantener el Software Actualizado**: Asegurarse de que todos los sistemas y aplicaciones estén actualizados con los últimos parches de seguridad.
- **Utilizar Autenticación Multifactor (MFA):** Añadir una capa adicional de seguridad mediante el uso de MFA para acceder a sistemas y datos sensibles.
- **Encriptar Datos Sensibles:** Utilizar encriptación para proteger los datos tanto en tránsito como en reposo
- **Realizar Auditorías de Seguridad Regulares**: Llevar a cabo auditorías de seguridad periódicas para identificar y corregir vulnerabilidades.
- **Capacitar a los Usuarios:** Implementar programas de formación y concienciación para educar a los usuarios sobre las mejores prácticas de seguridad y cómo identificar posibles amenazas.
- **Segmentar la Red:** Utilizar VLANs y subredes para limitar el alcance de posibles ataques y mejorar la gestión del tráfico.
- **Monitorear la Red en Tiempo Real:** Utilizar herramientas de monitoreo para detectar y responder a amenazas en tiempo real.
- **Implementar Firewalls y Sistemas IDS/IPS:** Utilizar firewalls y sistemas de detección y prevención de intrusiones para proteger la red contra ataques.

6.3 Futuras investigaciones: Áreas de la seguridad en redes que necesitan más estudios o que están en rápido desarrollo (como la seguridad en IoT o 5G).

- **Seguridad en IoT (Internet de las Cosas):** Con el creciente número de dispositivos conectados, es crucial desarrollar métodos para asegurar estos dispositivos y las redes a las que están conectados.
- **Seguridad en Redes 5G:** La implementación de redes 5G trae consigo nuevos desafíos de seguridad que requieren soluciones innovadoras para proteger la infraestructura y los datos.
- **Inteligencia Artificial y Ciberseguridad:** Investigar cómo la inteligencia artificial puede ser utilizada tanto para mejorar la seguridad en redes como para identificar y mitigar amenazas de manera más eficiente.
- **Seguridad en la Nube:** Con la creciente adopción de servicios en la nube, es esencial desarrollar nuevas estrategias y herramientas para proteger los datos y aplicaciones en estos entornos.
- **Blockchain y Seguridad en Redes:** Explorar cómo la tecnología blockchain puede ser utilizada para mejorar la seguridad y la integridad de los datos en redes distribuidas.

- **Privacidad y Protección de Datos**: Investigar nuevas técnicas para proteger la privacidad de los usuarios y asegurar que los datos personales estén adecuadamente protegidos.
- **Ciberseguridad en Infraestructuras Críticas:** Desarrollar métodos para proteger infraestructuras críticas, como redes eléctricas y sistemas de transporte, contra ciberataques.

7. Referencias

Protocolos de Encriptación y Autenticación

- Guía de Encriptación de Datos: Métodos y Protocolos
- Encriptación: Métodos y Tipos - IONOS España
- ¿Qué son los protocolos de encriptación? - VPN Unlimited

Firewalls

- ¿Qué es un firewall? Funcionamiento de los firewalls y tipos de firewalls - Kaspersky
- Firewall: qué es un cortafuegos, para qué sirve y cómo funciona - Xataka
- ¿Qué es un firewall? | Firewalls de red | Cloudflare

Sistemas de Detección y Prevención de Intrusiones (IDS/IPS)

- Los 7 Mejores Sistemas de Prevención de Intrusiones (IPS)
- ¿Qué es un sistema de prevención de intrusiones (IPS)? | IBM
- ¿Qué es un sistema de detección de intrusiones (IDS)? - IBM

Modelos de Seguridad en Capas

- La importancia de la seguridad por capas
- Seguridad por capas
- Modelo OSI: 7 capas y ciberataques habituales | Stackscale

Recomendaciones para Seguridad en Redes

- 15 consejos y normas de seguridad en Internet - Kaspersky
- 10 consejos para mejorar la seguridad en Internet - MuyComputer
- 15 Consejos de SEGURIDAD en las Redes Sociales - Ignacio Santiago

Futuras Investigaciones en Seguridad en Redes

- AriSe2: Redes IoT Futuras y Nanorredes - TrustLab
- Seguridad en Redes Sociales: problemas, tendencias y retos futuros - UC3M
- Seguridad en Redes 5G: Retos y Soluciones para el Futuro