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

IES EDUARDO PRIMO MARQUÉS

SEGURIDAD INFORMÁTICA

- Javier Herraiz Calatayud

- Seguridad informática
- IES Eduardo Primo Marqués. Curso 2024/25

ÍNDICE

1. Introducción

La importancia de la seguridad en redes es crucial en un mundo cada vez más digitalizado. Con el creciente volumen de información crítica que viaja a través de redes locales e Internet, asegurar la integridad y confidencialidad de los datos se ha convertido en un desafío prioritario.

2. Conceptos fundamentales de seguridad en redes

2.1. Definición de seguridad informática y seguridad en redes

- Seguridad informática: Se refiere a la protección de los sistemas de información contra el acceso no autorizado, el uso indebido o el daño.
- Seguridad en redes: Focalizada en proteger la integridad, confidencialidad y disponibilidad de los datos mientras se transmiten por redes.

2.2. Principios de la seguridad en redes

- Confidencialidad: Garantizar que la información solo sea accesible para quienes tienen permisos.
- Integridad: Asegurar que los datos no sean alterados durante la transmisión.
- Disponibilidad: Asegurar que los sistemas y datos estén accesibles cuando se necesiten.
- Autenticación: Verificar la identidad de usuarios o dispositivos.
- No repudio: Garantizar que las acciones realizadas no puedan ser negadas por sus autores.

2.3. Tipos de redes

- LAN: Redes de área local.
- WAN: Redes de área amplia.
- MAN: Redes metropolitanas.
- PAN: Redes de área personal.
- VPN: Redes privadas virtuales.

3. Amenazas y vulnerabilidades comunes en redes informáticas

3.1. Tipos de ataques a redes

3.1.1. Ataques DoS/DDoS: Saturación del ancho de banda o recursos del sistema.

3.1.2. Man-in-the-Middle: Interceptación de comunicaciones entre dos partes.

3.1.3. Inyección: Exploits como SQL Injection.

3.1.4. Phishing: Obtención de credenciales mediante engaños.

3.1.5. Malware en redes: Software malicioso como ransomware.

3.2. Vulnerabilidades más comunes en redes

- Configuraciones por defecto.
- Falta de actualizaciones.
- Credenciales débiles.

4. Protocolos y tecnologías de seguridad en redes

4.1. Protocolos de encriptación y autenticación

4.1.1. SSL/TLS: Protocolo para comunicaciones seguras.

4.1.2. IPsec: Seguridad en el nivel de red.

4.1.3. WPA3: Estándar moderno para redes inalámbricas.

4.1.4. VPN: Redes privadas para conexiones seguras.

4.2. Firewalls

4.2.1. Filtros de paquetes: Controlan el tráfico según reglas.

4.2.2. Firewalls de aplicación: Inspeccionan tráfico a nivel de aplicación.

4.3. IDS/IPS

4.3.1. IDS: Detección de intrusos.

4.3.2. IPS: Prevención de intrusos.

5. Estrategias de mitigación y buenas prácticas

5.1. Modelos de seguridad en capas

Implementar controles en diferentes niveles de la infraestructura.

5.2. Segmentación de redes

Uso de VLANs y subredes.

5.3. Seguridad en la nube

Herramientas como CASB y cifrado en reposo y en tránsito.

5.4. Concienciación y formación

Capacitar a los usuarios para identificar amenazas comunes.

6. Conclusiones

6.1. Recomendaciones

Mantener las actualizaciones al día.

Implementar protocolos seguros.

6.2. Futuras investigaciones

Seguridad en IoT y redes 5G.