TEMA 125

LA SEGURIDAD EN REDES. TIPOS DE ATAQUES Y HERRAMIENTAS PARA SU PREVENCIÓN: CORTAFUEGOS, CONTROL DE ACCESOS E INTRUSIONES, TÉCNICAS CRIPTOGRÁFICAS, ETC. MEDIDAS ESPECÍFICAS PARA LAS COMUNICACIONES MÓVILES.

Versión	**30.1**
Fecha de actualización	**09/09/2024**

1. La Seguridad en las Redes

La **guía CCN-STIC 817 Gestión de ciberincidentes** resume en la siguiente tabla la clasificación de los ciberincidentes atendiendo a la ruta o camino que utiliza un atacante para tener acceso al activo atacado (vector de ataque).

Vector de ataque		**Tipo de ciberincidente**
Código dañino	Software cuyo objetivo es infiltrarse o dañar un ordenador, servidor u otro dispositivo de red, sin el conocimiento de su responsable o usuario y con finalidades muy diversas.	• Virus • Gusanos • Troyanos • Spyware • Rootkit • Ransonware • Remote Access Tools (RAT)
Disponibilidad	Ataques dirigidos a poner fuera de servicio los sistemas, al objeto de causar daños en la productividad y/o la imagen de las instituciones atacadas.	• Denegación de servicio (DoS) y Denegación de servicio distribuida (DDoS) • Fallo (HW/SW) • Error humano • Sabotaje
Obtención de información	Ataques dirigidos a recabar información fundamental que permita avanzar en ataques más sofisticados, a través de ingeniería social o de identificación de vulnerabilidades	• Identificación de vulnerabilidades (scanning) • Sniffing • Ingeniería social • Phishing

Intrusiones	Ataques dirigidos a la explotación de vulnerabilidades de diseño, de operación o de configuración de diferentes tecnologías, al objeto de introducirse de forma fraudulenta en los sistemas de una organización.	• Compromiso de cuenta de usuario • Cross-Site Scripting (XSS) • Cross-Site Request Forgery (CSRF, Falsificación de petición entre sitios cruzados) • Inyección SQL • Spear Phishing • Pharming • Ataque de fuerza bruta • Inyección de ficheros remota • Explotación de vulnerabilidad sw • Explotación de vulnerabilidad hw
Compromiso de la información	Incidentes relacionados con el acceso y fuga (Confidencialidad), modificación o borrado (Integridad) de información no pública.	• Acceso no autorizado a la información • Modificación y borrado no autorizada de información • Publicación no autorizada de información • Exfiltración de información
Fraude	Incidentes relacionados con acciones fraudulentas derivadas de suplantación de identidad, en todas sus variantes.	• Suplantación/Spoofing • Uso de recursos no autorizado • Uso ilegítimo de credenciales • Violaciones de derechos de propiedad intelectual o industrial.
Contenido abusivo	Ataques dirigidos a dañar la imagen de la organización o a utilizar sus medios electrónicos para otros usos ilícitos (tales como la publicidad, la extorsión o, en general, la ciberdelicuencia).	• Spam (Correo basura) • Acoso/ extorsión/ mensajes ofensivos • Pederastia/ racismo/ apología de la violencia, etc.

Política de seguridad	Incidentes relacionados por violaciones de usuarios de las políticas de seguridad aprobadas por la organización.	• Abuso de privilegios por usuarios • Acceso a servicios no autorizados • Sistema desactualizado
Otros	Otros incidentes no incluidos en los apartados anteriores.	

1.1 Normativa de Seguridad

ENS y medidas relacionadas con seguridad en redes (Gestión de la configuración, perimetro seguro, interconexiones) + Guías CCN STIC Serie 800 como la 811 de Interconexión de sistemas de información.

- La familia de normas ISO 27000
- MAGERIT + PILAR
- Normativa Europea: NIS2 y Cibersecurity Act

2. Tipos de Ataques y herramientas para su prevención

2.1 Tipos de Ataques

2.1.1 Ataques de Denegación de Servicio (Disponibilidad comprometida)

- ***DDoS (Distributed Denial of Service)/ Teardrop***: / **Connection Flood/ICMP flooding/UDP flooding/ SYN flooding / *Buffer overflow***

2.1.2 Ataques de suplantación

- MAC-spoofing /ARP-spoofing/IP-spoofing/DHCP-spoofing/DNS-spoofing/Mail-spoofing/Web-spoofing/ Hijacking/ ***Phising***

2.1.3 Ataques de Monitorización, Escucha y Manipulación

- *Port* ***Scanning*** (SYN Scan, RST Scan, TTL Scan/ ***Sniffing/ MitM (Man In The Middle) /Keylogger/Tampering o data diddling/Malware***: virus, gusanos, troyanos, bombas lógicas...

2.1.4 Ataques de Inyección

- **SQL Injection/Code Injection/Cross-Site Scripting (XSS)**

2.1.5 Ataques a contraseñas

- **Brute Force Attack/Dictionary Attack/Credential Stuffing**

2.1.6 Ataques de Software y Sistemas

- **Exploits/ Zero-Day / Ransomware**

2.1.7 Contramedidas y protecciones

Para protegerse contra estos ataques, es esencial implementar buenas prácticas de seguridad, como:

- **Actualización y Parcheo de sistemas y sw**
- **Cifrado de Datos** con algoritmos de cifrado robustos y sin vulnerabilidades.
- **Autenticación Multifactor (MFA):** con capas adicionales de verificación para sistemas críticos.
- **Monitorización y Auditoría:** Revisar regularmente registros de actividad y tráfico de red
- **Educación en Seguridad:** Capacitar a los usuarios y empleados sobre los riesgos de seguridad

2.2 Herramientas de Prevención

✓ **FIREWALL**: **"*CCN-STIC-811 Interconexión en el ENS*"**.

Modo típico de funcionamiento de un **FIREWALL:** lista de patrones y decisión por reglas DENY o ACCEPT. Política restrictiva (DENY ALL), Política permisiva (ACCEPT ALL).

Además de realizar el filtrado de tráfico, los firewalls suelen proporcionar servicios adicionales como **NAT**, terminación túneles **VPN** o sistemas **IPS/IDS (Prevención de intrusiones/Detección de intrusiones)**.

TIPOS DE FIREWALL SEGÚN EL NIVEL EN EL QUE OPERAN:

- **FIREWALL DE RED**: el filtrado de paquetes se basa en información de cabeceras IP y TCP. Pueden ser ***Stateless packet filter (estático)*** o ***Statefull packet filter (dinámico).***
- **FIREWALL DE NIVEL DE APLICACIÓN**: reconstruyen los paquetes a nivel de aplicación y analizan protocolos específicos (ej. http, smtp, ftp, etc).

✓ **HOST BASTIÓN**: sistema expuesto a posibles ataques desde el exterior, pero altamente securizado

2.2.1 Control de accesos

- Modelos de control de acceso: DAC, MAC, RBAC

- Factores de autenticación: algo que se sabe, algo que se tiene, algo que se es.
- Protocolos de acceso y autenticación: PPP, PAP, CHAP, EAP.
- Acceso a redes WiFI: WEP, WPA, WPA-2, WPA-3
- Autenticación a nivel 3: IPSec
- Autenticación a nivel de aplicación: TLS
- Autenticación a nivel de aplicación: Radius, TACACS+, Diameter, Kerberos, SAML.

3. Medidas específicas para las comunicaciones móviles

Existe una guía de seguridad **CNN-STIC 496 para Sistemas de Comunicaciones Móviles seguras**. En ella se define la obligación de cada organismo de implementar una política para los sistemas de información en movilidad, que debe estar alineada con la política de seguridad de la información de la organización.

En la actualidad, tanto la AGE como las corporaciones privadas están introduciendo herramientas **MTD** (Mobile Threat Defense) para la protección de los dispositivos móviles y no solo de las comunicaciones, un dispositivo móvil está expuesto a estos vectores de ataque:

- Ataques de acceso físico al dispositivo (fuerza bruta, móviles sin pantalla de bloqueo).
- Explotaciones de vulnerabilidad del SO o de las apps instaladas.
- Aplicaciones maliciosas (apps disponibles incluso en las tiendas oficiales y que pueden contener malware ya que escapan de los controles de Google y Apple).
- Ataques de red

Las herramientas MTD se suelen integrar con herramientas de gestión de la movilidad corporativa (**EMM**) para la distribución de políticas a todos los terminales de la organización. Realizan detección de anomalías, análisis inteligente por perfiles de comportamiento, prevención de intrusiones, firewall de host, etc. Con todo ello se intenta mitigar la posible pérdida/robo de información corporativa valiosa y posibles accesos a la red interna de la organización que puedan originarse desde terminales corporativos

OWASP ha lanzado en 2024 una lista con las vulnerabilidades más comunes en móvil, y sus posibles medidas de prevención:

- M1: Uso inadecuado de credenciales
- M2: Seguridad inadecuada de la cadena de suministro
- M3: Autenticación/autorización insegura
- M4: Validación de entrada/salida insuficiente
- M5: Comunicación insegura
- M6: Controles de privacidad inadecuados
- M7: Protecciones binarias insuficientes
- M8: Mala configuración de seguridad
- M9: Almacenamiento de datos inseguro
- M10: Criptografía insuficiente


09:30
preparatic
¿Tienes alguna sugerencia de mejora?
Háznoslo saber
O haz clic en la imagen