SEGURIDAD Y MEJORES PRÁCTICAS DE PREVENCION

Consejos de Ciberseguridad

Andrés Fernando García Delgado 187134
León Ernesto Marmolejo Torres 186828

01 MALWARE

Software malicioso diseñado para dañar, espiar o controlar dispositivos.

COMO PREVENIRLO :

- Antivirus/antimalware actualizado
- No descargar archivos sospechosos
- Actualizaciones del sistema

02 WEB-BASED ATTACKS

¿Qué son?
Ataques realizados mediante versiones vulnerables de sitios web.

COMO PREVENIRLO :

- Utilizar la ultima version de HTTPS
- Firewalls para aplicaciones web (WAF)
- Actualizar CMS y plugins

03 DOS / DDOS

¿En qué consisten?
Saturar un servidor para impedir su funcionamiento.

COMO PREVENIRLO :

- Protección anti-DDoS
- Balanceadores de carga
- Monitoreo de tráfico

04 ATAQUES DE INFORMACIÓN Y CREDENCIALES (FUERZA BRUTA)

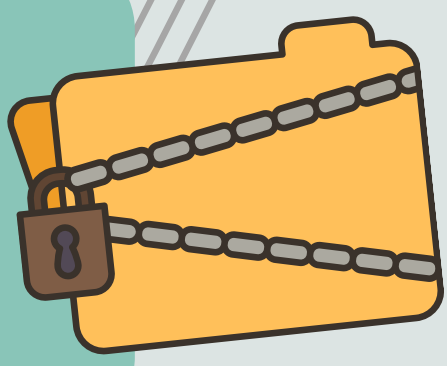
¿Qué es?
Intentos repetidos para adivinar contraseñas.

COMO PREVENIRLO :

- Políticas de contraseñas fuertes
- Autenticación multifactor (MFA)
- Bloqueo automático de intentos

05 ATAQUES DE CONFIGURACIÓN Y SERVIDOR

Consiste en:
Aprovechar configuraciones inseguras o servicios expuestos.

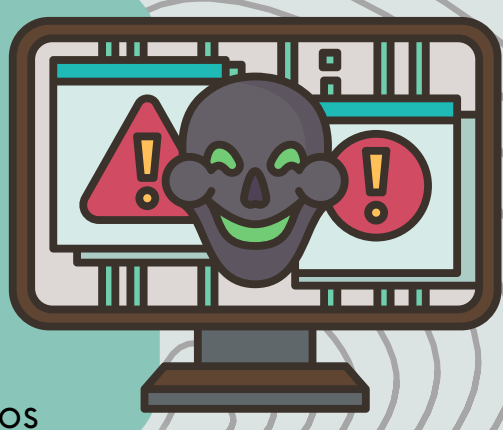


COMO PREVENIRLO :

- Hardening del servidor
- Cerrar puertos no usados
- Revisiones periódicas de configuración

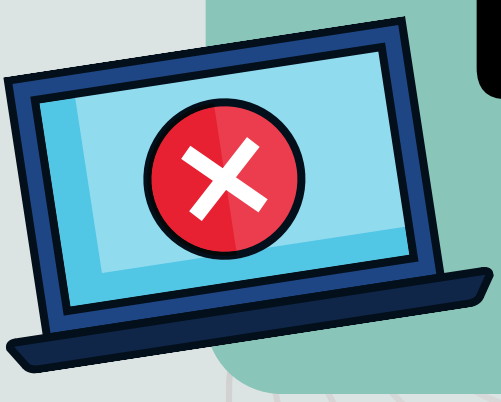
06 PHISHING

¿Qué es?
Suplantación de identidad para robar datos mediante correos, mensajes o enlaces falsos



COMO PREVENIRLO :

- Educación al usuario
- Filtros antiphishing
- Revisar enlaces antes de abrirlos



07 WEB APPLICATION ATTACKS

Ataques dirigidos a aplicaciones web aprovechando vulnerabilidades.

COMO PREVENIRLO :

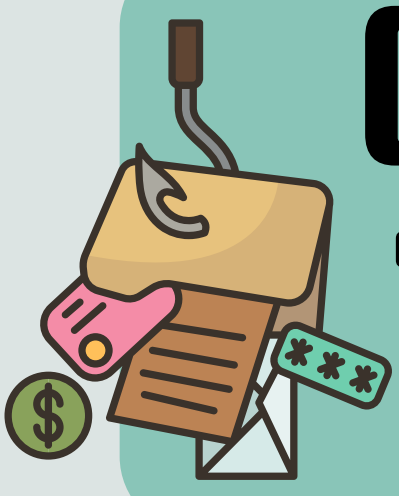
- WAF
- Pruebas de penetración
- Uso de frameworks seguros

08 SQL INJECTION (SQLI)

Inserción de código SQL malicioso en formularios o URLs.

COMO PREVENIRLO :

- Consultas preparadas
- Validación de entradas
- Principio de mínimo privilegio.



09 CROSS-SITE SCRIPTING (XSS)

Inyección de scripts maliciosos en sitios web.

COMO PREVENIRLO :

- Escape/filtrado de datos
- CSP (Content Security Policy)
- Sanitización de entradas

10 CSRF

Forzar a un usuario autenticado a ejecutar acciones sin querer.

COMO PREVENIRLO :

- Tokens CSRF
- Verificación de origen
- Cookies seguras

11 FILE INCLUSION

Incluir archivos remotos o locales no autorizados.

COMO PREVENIRLO :

- Validar rutas
- Deshabilitar funciones peligrosas
- Configurar el servidor correctamente

12 CONFIGURACIÓN ERRÓNEA DEL SERVIDOR

Permisos incorrectos, puertos abiertos o servicios inseguros.

COMO PREVENIRLO :

- Auditorías
- Hardening
- Actualizaciones

13 SPAM

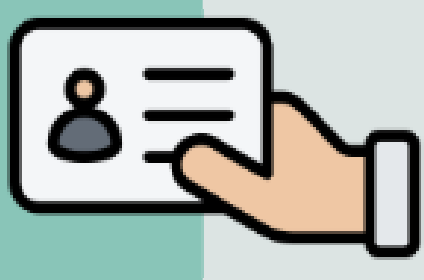
Mensajes no solicitados, generalmente para estafas o malware.

COMO PREVENIRLO :

- Filtros de correo
- Educación del usuario
- Protección de formularios web

14 IDENTITY THEFT

Robo de información personal para suplantar identidad.



COMO PREVENIRLO :

- MFA
- No compartir datos sensibles
- Monitoreo de cuentas

15 DATA BREACH

Exposición de datos por hackeo o error humano.

COMO PREVENIRLO :

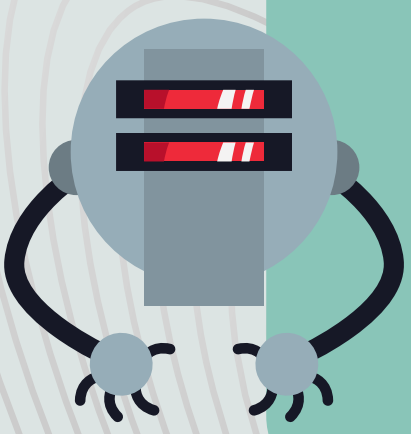
- Cifrado
- Control de accesos
- Respaldo seguro

16 INSIDER THREAT

Amenazas internas de empleados o personal con acceso.

COMO PREVENIRLO :

- Segmentar privilegios
- Monitoreo
- Políticas de seguridad



17 BOTNETS

Red de dispositivos infectados controlados por un atacante.

COMO PREVENIRLO :

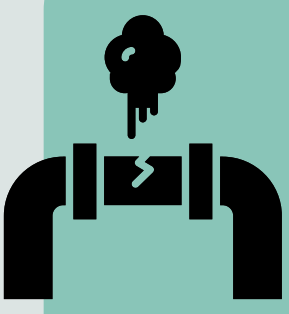
- Antivirus
- Evitar descargas sospechosas
- Actualizar dispositivos IoT

18 MANIPULACIÓN FÍSICA, DAÑO, ROBO O PÉRDIDA

Intervención física para robar dispositivos o dañar sistemas.

COMO PREVENIRLO :

- Control de acceso físico
- Cámaras, candados
- Cifrado de discos



19 INFORMATION LEAKAGE

Filtración accidental de información sensible.

COMO PREVENIRLO :

- Cifrado
- Clasificación de datos
- Control de permisos

20 RANSOMWARE

Secuestro de información con cifrado y petición de rescate.

COMO PREVENIRLO :

- Backups regulares
- No abrir archivos sospechosos
- Antivirus y EDR

21 CYBER ESPIONAGE

Robo de información estratégica mediante ataques sofisticados.

COMO PREVENIRLO :

- Seguridad avanzada (EDR/SIEM)
- Segmentación de redes
- Actualizaciones constantes

22 CRYPTOJACKING

Secuestro de recursos del equipo para minar criptomonedas.

COMO PREVENIRLO :

- Extensiones anti-minería
- Evitar descargas no confiables
- Monitorear consumo de CPU