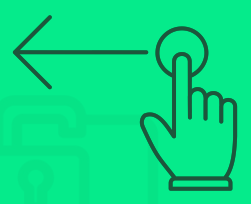
Los ciberataques más comunes y cómo evitarlos

DEFINICIÓN
IMPACTO
PREVENCIÓN



¡Desliza!

ATAQUE DDoS

Denegación de servicio distribuida

DEFINICIÓN

Un ataque que sobrecarga tus servidores con miles de «usuarios» accediendo desde múltiples fuentes, haciendo que tus servicios dejen de funcionar para usuarios reales.

IMPACTO

Caída del servicio web, pérdida de ventas online, daño a la reputación de la marca, costes de mitigación.

PREVENCIÓN

Implementa protección contra DDoS con firewalls y monitoreo de tráfico. Tener un plan B por si se cae la web.

ATAQUE MITM

Man in the Middle

DEFINICIÓN

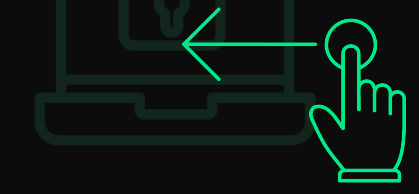
Un ciberdelincuente intercepta la comunicación entre dos partes para robar información o manipular los datos transmitidos. (Ej: Un número de cuenta bancaria).

IMPACTO

Robo de datos sensibles, interceptación de credenciales, modificación de transacciones, violación de privacidad.

PREVENCIÓN

Uso de protocolos seguros (HTTPS), certificados SSL/TLS, VPN para conexiones remotas, encriptación punto a punto.



SPEAR PHISHING

Suplantación de identidad

DEFINICIÓN

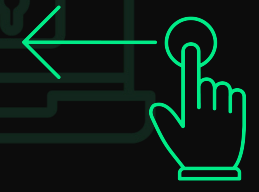
Un ataque de phishing dirigido específicamente a una persona o empresa, usando información personalizada para hacerlo más convincente.

IMPACTO

Compromiso de cuentas corporativas, acceso a sistemas internos, robo de propiedad intelectual

PREVENCIÓN

Análisis de correos sospechosos, verificación de remitentes, formación continua, herramientas anti-phishing



RANSOMWARE

Malware

DEFINICIÓN

Malware que cifra tus archivos y sistemas, exigiendo un rescate para recuperar el acceso. Puede paralizar completamente las operaciones de la empresa.

IMPACTO

Pérdida de acceso a datos críticos, costes de rescate, tiempo de inactividad, pérdida de productividad.

PREVENCIÓN

Copias de seguridad regulares, parches de seguridad, segmentación de red, plan de recuperación ante desastres. evita abrir archivos adjuntos de fuentes desconocidas.

INYECCIÓN SQL

Código malicioso

DEFINICIÓN

Un ataque que aprovecha vulnerabilidades en bases de datos para acceder, modificar o eliminar información.

IMPACTO

Pérdida de acceso a datos críticos, costes de rescate, tiempo de inactividad, pérdida de productividad.

PREVENCIÓN

Copias de seguridad regulares, parches de seguridad, segmentación de red, plan de recuperación ante desastres. evita abrir archivos adjuntos de fuentes desconocidas.

SPOOFING

Suplantación de identidad

DEFINICIÓN

Técnica que falsifica direcciones IP, correos, DNS o dispositivos para engañar a sistemas y usuarios, haciéndose pasar por fuentes confiables.

IMPACTO

Robo de datos confidenciales, información financiera, daños reputacionales y consecuencias legales.

PREVENCIÓN

Verifica remitente y enlaces, activa la autenticación en dos pasos, usa filtros de seguridad en emails, no compartas información confidencial y mantén tus sistemas actualizados.

FUERZA BRUTA

Ensayo y error

DEFINICIÓN

Ataques que intentan descubrir contraseñas o claves probando sistemáticamente todas las combinaciones posibles hasta encontrar la correcta.

IMPACTO

Compromiso de cuentas, acceso no autorizado, robo de datos, modificación de credenciales

PREVENCIÓN

Políticas de contraseñas robustas, bloqueo tras intentos fallidos, autenticación multi-factor, monitorización de intentos de acceso

¿QUIERES MÁS CONSEJOS PARA MANTENER TU NEGOCIO SEGURO?

Síguenos y mantente al día
en **seguridad digital**.

Si necesitas expertos en ciberseguridad no dudes en contactar con nostros

www.sshteam.com

S S
H {}