■ ANÁLISIS DE RED · HERRAMIENTA REAL

Wireshark: lo que ven cuando espían tu red

01 — ¿QUÉ ES WIRESHARK?

Un analizador de red gratuito y legítimo, usado por administradores TI y también por atacantes. Captura todo el tráfico que pasa por una red en tiempo real — cada paquete, cada petición, cada respuesta.

■ HTTP sin cifrar
Cualquier página sin HTTPS muestra texto plano: usuario, contraseña, datos de formulario — todo visible.

■ Correo sin TLS
Correos enviados sin cifrado muestran el contenido completo del mensaje y los archivos adjuntos.

■ Cookies de sesión
Si roban tu cookie pueden acceder a tu cuenta sin necesitar tu contraseña.

■ DNS Queries
Revelan todos los sitios que visitas, aunque el contenido esté cifrado.

02 — ¿POR QUÉ IMPORTA PARA TU NEGOCIO?

Si alguien conecta Wireshark en la red de tu oficina — un empleado, un visitante con WiFi, o un intruso — puede capturar credenciales de sistemas internos, datos de clientes y comunicaciones confidenciales.

■ Red WiFi abierta o débil
Cualquiera en el rango puede capturar el tráfico de todos los dispositivos conectados.

■ Sistemas sin HTTPS
Paneles de administración, sistemas POS o ERPs sin cifrado exponen todo.

■ Redes planas sin segmentación
Un solo punto de acceso comprometido expone toda la red de la empresa.

03 — CÓMO PROTEGERTE

■ Usa HTTPS en todo
Nunca accedas a sistemas críticos desde páginas sin HTTPS. El candado importa.

■ WPA3 en tu red WiFi
Usa el cifrado más reciente en tu router. WPA2 mínimo, WPA3 ideal.

■ Segmenta tu red
Separa la red de empleados, clientes y dispositivos IoT. Un intruso en WiFi de clientes no debe ver los sistemas internos.

■ VPN en redes externas
Cualquier trabajo fuera de la oficina debe hacerse con VPN activa.

¿Tu red tiene tráfico expuesto?

Diagnóstico de red en 30 min — wa.me/527771631152

// REGLA DE ORO

La ciberseguridad no es tecnología — es conocimiento. Comparte esta infografía.