INFOGRAFÍA

Amenazas en Seguridad de Redes

PHISHING Y CORREOS MALICIOSOS

Descripción breve: Suplantación de identidad para robar credenciales o datos mediante correos, SMS o sitios falsos. Posibles impactos: Robo de cuentas, acceso no autorizado, fraudes, filtración de información. Soluciones:

- Capacitación continua para reconocer mensajes sospechosos y URLs falsas.
- Filtros antispam/antiphishing y antivirus actualizados.
- Autenticación multifactor (MFA) y uso de contraseñas únicas/gestores de contraseñas.

RANSOMWARE

Descripción breve: Malware que cifra archivos/sistemas y exige un rescate para liberarlos. Posibles impactos: Pérdida/indisponibilidad de información, interrupción de operaciones, costos de recuperación. Soluciones:

- Respaldos probados y desconectados (3-2-1) + plan de respuesta a incidentes.
- Parcheo constante de SO y aplicaciones; deshabilitar macros no firmadas.
- Principio de mínimo privilegio y segmentación de red.

INGENIERÍA SOCIAL

Descripción breve: Manipulación psicológica para que usuarios revelen información o realicen acciones inseguras. Posibles impactos: Compromiso de cuentas, apertura de puertas lógicas/físicas, fuga de datos. Soluciones:

- Campañas de concientización con simulaciones periódicas y políticas claras de verificación.
- Procedimientos de doble validación para solicitudes sensibles (AP, pagos, accesos).
- Cultura de "detenerse y verificar"; canales oficiales para reportar intentos.

CREDENCIALES DÉBILES Y ATAQUES DE FUERZA BRUTA

Descripción breve: Contraseñas previsibles o reutilizadas que pueden adivinarse o filtrarse. Posibles impactos: Acceso no autorizado a sistemas críticos y movimientos laterales. Soluciones:

- Políticas de contraseñas robustas + gestor de contraseñas.
- MFA en todas las cuentas; bloqueo/retardo tras intentos fallidos.
- Revisiones de exposición (haveibeenpwned, monitoreo de filtraciones) y rotación de claves.

WI-FI INSEGURO Y ATAQUES MAN-IN-THE-MIDDLE

Descripción breve: Interceptación/manipulación del tráfico en redes abiertas o mal configuradas. Posibles impactos: Robo de sesiones/credenciales, inyección de contenido, espionaje. Soluciones:

- Uso de VPN para accesos remotos y políticas de TLS en servicios internos.
- Configurar Wi-Fi con WPA3/WPA2-AES, desactivar WPS, separar redes de invitados.
- Detección de APs falsos y protección contra ARP spoofing (DHCP Snooping/DAI).

LA PEOR AMENAZA EN MI OPINION

Para mí, la peor amenaza es la ingeniería social. Al final, el punto débil casi siempre somos las personas ya que con un correo o llamada bien hecha te convence y ya abriste la puerta al resto de las amenazas. Además, los estafadores se adaptan a lo que está de moda y se cuelan aunque haya buenas herramientas. Por eso importante dar capacitaciones constantes, verificación por otro canal antes de hacer algo delicado y una cultura de reportar rápido cuando algo se ve raro. Eso baja el riesgo de todo lo demás.