



Ciberataque a Renfe y Adif

Anatomía del Pivotaje Lateral Asistido por IA y el Colapso de la Confianza Perimetral

[OBJETIVO TÉCNICO] ~500 GB de datos comprometidos y la lección definitiva sobre Zero-Trust en redes interconectadas.

1. El Incidente: ¿Qué ocurrió?

- › Jueves 24/09: Detección de tráfico anómalo en servidores de Adif.
- › Viernes 25/09: Caída temporal del portal de Adif y aislamiento de emergencia.
- › Salto Lateral: Los atacantes cruzaron hacia Renfe a través de enlaces de interconexión interna compartida.
- › Alcance: Presunta exfiltración de hasta 500 GB; Renfe confirma exposición de nombres y emails de viajeros.
- › Investigación oficial abierta con el CCN-CERT y notificación legal a la AEPD.

[CLAVE DE SEGURIDAD] Los sistemas OT de señalización y control de trenes permanecieron intactos gracias al aislamiento físico.

2. El Vector: Confianza Transitiva

- › Escisión sin aislamiento: Ambas entidades comparten túneles MPLS y APIs para surcos y andenes.
- › Reconocimiento con IA: Escaneo automatizado y mutación de payloads para eludir WAFs perimetrales.
- › Abuso de Cuentas de Servicio: Al comprometer Adif, el atacante usó tokens y credenciales con acceso legítimo a Renfe.
- › Exfiltración Silenciosa: Fragmentación en chunks cifrados hacia nubes públicas sin saturar ancho de banda.

[CLAVE DE SEGURIDAD] Si tu red confía ciegamente en una entidad externa o filial, su brecha es automáticamente tu brecha.

3. Marco Regulatorio: NIS2 y RGPD

- › Directiva NIS2 (UE 2022/2555): Alerta temprana al CCN-CERT obligatoria en menos de 24 horas para entidades esenciales.
- › Gestión de Cadena de Suministro: NIS2 Art. 21 sanciona expresamente la falta de control sobre redes de socios interconectados.
- › RGPD Art. 33 y 34: Notificación en 72h a la AEPD y posible comunicación a pasajeros ante riesgo de spear phishing masivo.
- › Ley de Infraestructuras Críticas (PIC): Auditoría forzosa de los Planes de Seguridad del Operador.

[CLAVE DE SEGURIDAD] Las multas bajo NIS2 alcanzan hasta 10 M€ o el 2% de la facturación global anual.

4. Arquitectura: Insegura vs Zero-Trust

[X] PATRÓN VULNERABLE

INSEGURO

```
# Confianza perimetral por IP (Vulnerable)
allow 10.50.0.0/16; # Toda la red de Adif
location /api/v1/passengers/ {
    proxy_pass https://renfe-internal-db;
    # Sin mTLS ni inspección L7 de roles
}
```

[OK] PATRÓN SEGURO

MITIGADO

```
# Microsegmentación eBPF Zero-Trust (Segura)
ingress:
- fromEndpoints:
  - matchLabels: { app: adif-slot-service }
  toPorts:
  - port: 8443
    rules:
      http:
      - method: GET
        path: /api/v1/rail-slots/. * # SOLO surcos
```

[REGLA TÉCNICA] Aplica el principio de menor privilegio: una API de coordinación ferroviaria jamás debe tener acceso a datos de clientes.



GARANTÍA COMERCIAL 100%

¿Tu Stack Conecta con Redes de Terceros?

- ✓ El 68% de las brechas graves en 2026 aprovechan enlaces de socios o APIs sin mTLS.
- ✓ En InitIA-Sec auditamos tus interconexiones y puntos ciegos antes de que un adversario los explote.
- ✓ Screening de Seguridad No Win, No Fee: Si no detectamos vulnerabilidades Medias o Críticas, no pagas nada.

Auditoría Ofensiva Garantizada

initia-sec.com · Contacta por DM o reserva tu screening técnico

initia-sec.com