ÉTUDE DE CAS

TRANSPORT - FERROVIAIRE

Digitalisation des usages & ouverture à la concurrence : séparation du réseau IT et du réseau de signalisation.

RÉSUMÉ DE L'ÉTUDE DE CAS

CHALLENGE

- Séparer le réseau IT du réseau de signalisation, tout en permettant une communication bi-directionnelle, sans contrainte.

SOLUTION

- Isolation réseau (physique) avec Xchange, en complémentarité d'une analyse applicative.

BÉNÉFICES

- Conformité réglementaire
- Gestion des risques
- Long term support

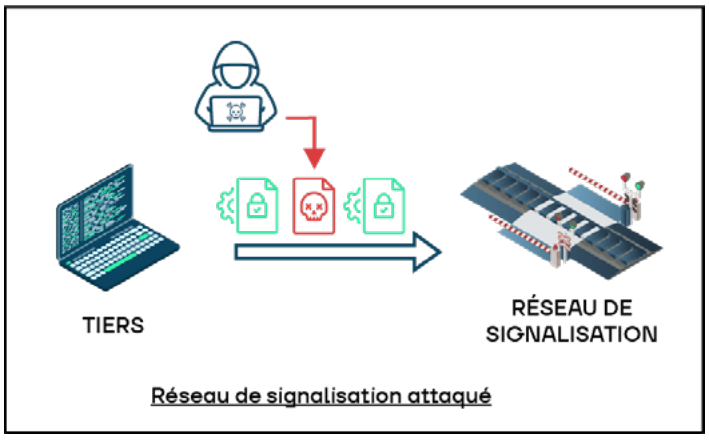
Contexte et besoin

Suite à l'ouverture à la concurrence, une entreprise ferroviaire doit permettre à des opérateurs tiers d'accéder à certaines informations (position des trains dans une gare, position de la rame, etc.) tout en garantissant un niveau de sécurité élevé car les tiers ne doivent pas pouvoir accéder au réseau de signalisation.

Attentes :
- Interconnexion IT / OT
- Mise en conformité réglementaire
- Isolation de l'interconnexion avec des tiers

Démarche

L'entreprise a comparé plusieurs types de technologie (firewall, diode, rupture protocolaire applicative et matérielle). 2 constats ont été réalisés :



Réseau de signalisation attaqué

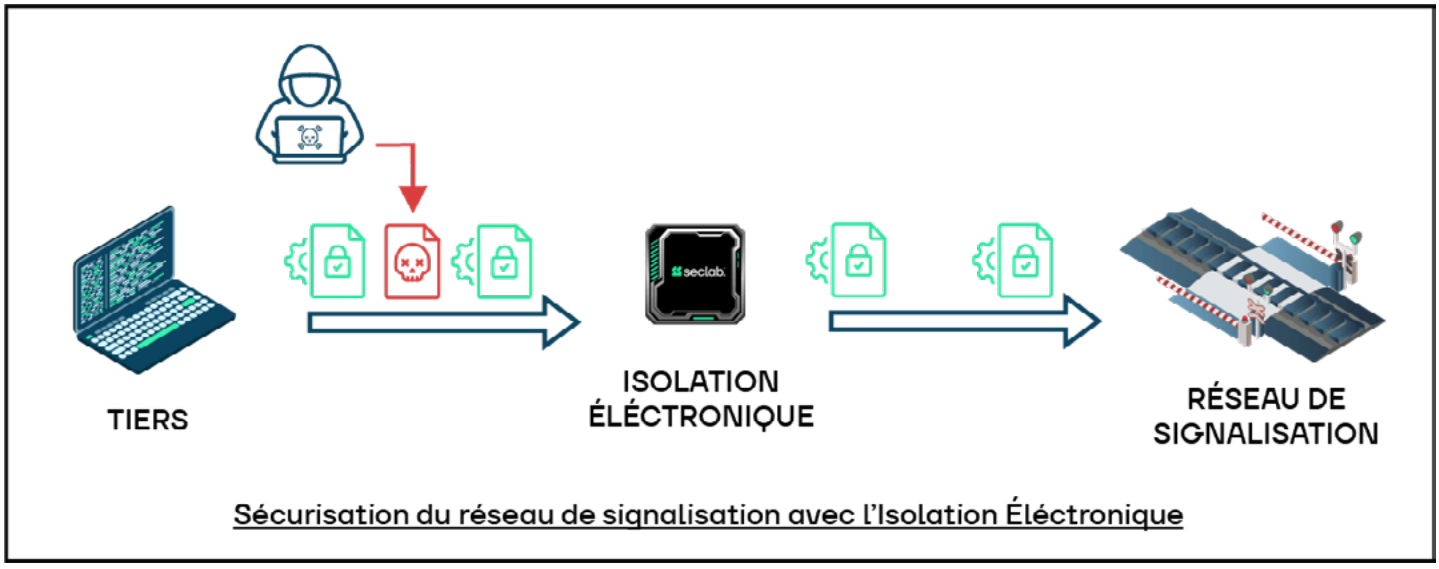
1. Un attaquant peut exploiter une faille d'un logiciel de sécurité qui n'est pas à jour.

2. L'usage d'une diode contraint le réseau à des transferts unidirectionnels dans un cas où le besoin d'échange est bidirectionnel.

Une validation du niveau de sécurité avec la valise OTAN et une validation fonctionnelle de l'architecture (flux applicatifs) étaient nécessaires.

Solution retenue

L'entreprise a retenu la solution de rupture protocolaire hardware de Seclab, en complémentarité de l'analyse applicative de Stormshield.
Cette nouvelle architecture permet à l'entreprise et au tiers de s'échanger des données de façon bidirectionnelle, sécurisée et maîtrisée grâce à la rupture protocolaire par l'électronique et au filtrage configuré selon les règles de sécurité de l'entreprise.



Sécurisation du réseau de signalisation avec l'Isolation Éléctronique

Résultats et bénéfices clients

Grâce à cette nouvelle architecture, les échanges sont sécurisés et maîtrisés entre le réseau IT et le réseau de signalisation : l'information peut circuler entre l'entreprise et le tiers, mais seuls les fichiers répondant à la politique de sécurité de l'entreprise peuvent entrer sur le réseau. L'isolation électronique isole et masque physiquement les deux environnements.

Conformité
L'architecture a été certifiée conforme par l'ANSSI (Conformité règlementaire ZEHO).

Gestion des risques
La solution couvre les risques suivants :
- Footprinting / scan
- Attaques réseau sophistiquées
- Attaques sur la couche applicative
- Exploitation zero day : pas de dépendance au correctif logiciel

Long Term Support
La solution offre une architecture stable, pérenne et maintenable sur le long terme, indépendante des cycles rapides d'évolution logicielle. Elle garantit ainsi un niveau de sécurité et de résilience durable.

À propos de Seclab

Seclab, accélérée en 2024 avec une nouvelle équipe dirigeante et des moyens renforcés, a l'ambition de devenir leader de la cybersécurité OT. Seclab apporte aux organisations industrielles et opérationnelles une confiance pérenne dans leur cybersécurité OT. Issue du rapprochement avec Seckiot, Seclab Xcore Platform est conçue pour protéger sans contraindre : une approche non-intrusive, progressive et simple à maintenir, qui s'adapte à tous les niveaux de maturité cyber. Elle offre une visibilité complète sur les actifs et les flux, une isolation des environnements critiques grâce à la technologie brevetée Electronic Air Gap, et une détection continue des menaces et anomalies. Seclab Xcore, the Next-Gen OT Cybersecurity Platform: Discover, Isolate & Detect.