STORMSHIELD

INDUSTRIE

SNCF RÉSEAU

RENFORCER LA SÉCURITÉ DES RÉSEAUX IT ET OT

Entretien avec Yseult Garnier, responsable CyberSécurité Industrielle

SNCF RÉSEAU

+ de 52 000
COLLABORATEURS

+ de 150
NATIONALITÉS

+ de 500
MÉTIERS

SNCF Réseau

Deuxième investisseur public français, comptant 52 000 collaborateurs pour un chiffre d'affaires prévisionnel de 6,5 milliards d'euros en 2017, SNCF Réseau est né de la fusion de Réseau Ferré de France (RFF), SNCF Infra et de la Direction de la Circulation Ferroviaire (DCF). L'entreprise gère, maintient, développe et commercialise les services offerts par le Réseau Ferré National.

Pour mener à bien ses missions, cet EPIC (Établissement public à caractère industriel et commercial) s'appuie sur des équipes décentralisées en région. Il est le garant de l'accès au réseau et aux infrastructures de services pour ses 39 clients.

Le contexte

« **Quand on s'attaque au monde du transport, on peut vite avoir des effets absolument dramatiques y compris sur les vies humaines** », avouait Guillaume Poupard, Directeur général de l'Agence Nationale de la Sécurité des Systèmes d' Information (ANSSI) à l'occasion du Forum International de la Cybersécurité (FIC), à Lille en 2017.

La menace doit être prise au sérieux par tous les industriels, car il y a aujourd'hui une convergence des réseaux informatiques (IT - Information Technology) et industriels (OT - Operational Technology). Mais **« à la différence de la cybersécurité des SI conventionnels, la cybersécurité industrielle est déployée sur le réseau ferroviaire avec des contraintes techniques. Il y a trois grands domaines : la signalisation, les télécoms (réseau IP et téléphonie ferroviaire) et l'alimentation électrique »**, précise Yseult Garnier, responsable cybersécurité industrielle chez SNCF Réseau.

Les réseaux industriels (OT) présentent également une seconde particularité : l'absence de solutions de sécurité ad hoc les rend très vulnérables aux cyberattaques en tout genre. La sécurisation des interconnexions entre ces différents réseaux devient donc un enjeu stratégique.

La solution retenue

En retenant une solution bicéphale, symbolisée par le partenariat entre Stormshield et Seclab, SNCF Réseau est capable de relever deux défis : optimiser sa transformation numérique (en proposant des offres innovantes aux utilisateurs) et renforcer la sécurité de ses applications métiers et de l'OT.

Les enjeux de protection et de filtrage sont prioritaires, car le périmètre de SNCF Réseau est articulé autour de 4 zones avec des niveaux de sécurité spécifiques : l'internet grand public, un internet en mode cloud privé, une zone avec une sécurité supplémentaire et enfin une zone homologuée (en mode coffre-fort).

L'interconnexion bidirectionnelle de l'infrastructure de SNCF Réseau l'oblige à sécuriser sa zone industrielle par rapport à l'IT conventionnel, en s'appuyant sur des solutions de filtrage.

La complémentarité des solutions de Stormshield (le filtrage des flux de données échangés entre l'IT et l'OT) et de Seclab (l'isolation au niveau électronique des systèmes industriels) permet d'assurer une protection optimale des échanges entre les deux réseaux séparés et d'endiguer tout type de menaces (parmi lesquelles : opération de sniffing, attaque bas niveau, corruption des transferts de fichiers par FTP...). Schématiquement, cette complémentarité peut être représentée par des camions et des cartons. Les premiers sont fournis par Seclab et les seconds sont analysés par les solutions de Stormshield.

Isolation et filtrage

D'un côté, la solution Denelis de Seclab agit comme un sas conservant l'isolation de chaque réseau, tout en permettant des échanges répondant à une politique de sécurité. Aucune menace présente sur la couche de transport ne peut contaminer le système isolé par Seclab. Ce procédé évite ainsi toute contamination au niveau des couches de transport.

« La mise en place d'une solution d'isolation permet de bloquer un attaquant qui aurait réussi à contrepasser le pare-feu. L'attaquant se retrouve alors dans une impasse, dans l'incapacité de poursuivre son déplacement. C'est la somme des technologies de Stormshield et de Seclab qui permet d'avoir le niveau de filtrage du pare-feu Stormshield, qui est impossible à implémenter en électronique, et le niveau d'isolation du boitier électronique Seclab, dont le fonctionnement ne peut être altéré par l'attaquant », explique Xavier Facélina, CEO de Seclab.

Mais les fonctionnalités de Stormshield Network Security (SNS) ne se limitent pas qu'au filtrage. Cette solution garantit l'intégrité des paquets de données en contrôlant leur contenu pour éviter les attaques sur les flux métier. Ce pare-feu applicatif intègre un moteur de prévention d'intrusion (IPS) et permet de bénéficier d'une analyse proactive du système afin de détecter les attaques, même inconnues.

Pour le pare-feu, SNCF Réseau s'est intéressé aux boitiers de Stormshield, notamment pour leurs capacités d'analyses des réseaux industriels, et notamment pour le fait que la SNCF Réseau, comme de nombreux industriels, utilise des protocoles non standards.

Un test a été mis en place en 3 mois sans développement particulier. « **Le seul travail porte sur l'intégration des protocoles propriétaires avec la capacité de personnalisation et la reconnaissance de patterns** », souligne Yseult Garnier. Un point important, car l'intégration de nouveaux protocoles dans la zone d'échange homologuée est primordiale pour répondre à la problématique de convergence de l'IT et l'OT, dans le cadre de la transformation numérique.

La fiabilité et la complémentarité des solutions de Stormshield et de Seclab sont de bonnes augures pour les futurs « chantiers » de SNCF Réseau. Cette entité se prépare à sécuriser les données d'exploitation ferroviaire. Un enjeu majeur, car il s'agira d'interconnecter les systèmes de gestion de la circulation avec les systèmes de contrôle commande.

Le partenaire : Seclab

Basé à Montpellier, Seclab innove dans la cyber protection des systèmes industriels depuis 2011. Ses produits **« made in France »** permettent une interconnexion sécurisée entre les réseaux OT et IT des industries et OIV (production et réseaux électriques et gaziers, traitement de l'eau, industries chimiques et pétrolières, etc.). Seclab a développé sa technologie électronique entièrement maîtrisée et fabriquée en France. **En assurant un cloisonnement électronique, sa technologie assure une parfaite complémentarité avec les pare-feux, antivirus, IDS ou data diodes.**

STORMSHIELD

Stormshield, filiale à 100% d'Airbus CyberSecurity, propose des solutions de sécurité de bout en bout innovantes pour protéger les réseaux (Stormshield Network Security), les postes de travail (Stormshield Endpoint Security) et les données (Stormshield Data Security).

www.stormshield.com