CYBERSÉCURITÉ

Livre blanc sur la cybersécurité

INTRODUCTION

La numérisation apporte des avantages substantiels en matière d'efficacité opérationnelle des transports (disponibilité, capacité, ponctualité et maintenabilité), ainsi qu'une meilleure expérience et un plus grand confort pour les voyageurs. Mais elle accroît aussi inévitablement la vulnérabilité aux cybermenaces. Ces tendances exposent les opérateurs de mobilité et le public à des niveaux sans précédent de risques en matière de cybersécurité.

Ces risques peuvent affecter la qualité de service (QoS) du réseau de transport (fiabilité du réseau de transport), la sécurité des voyageurs et, plus généralement, la réputation des opérateurs. Les cybermenaces peuvent également toucher les ordinateurs et les téléphones portables des voyageurs.

L'approche en matière de cybersécurité doit prévoir la protection approfondie nécessaire afin de se défendre contre les menaces de sécurité, tout en veillant à ce que les opérateurs de transport soient prêts à remplir leurs obligations réglementaires.

Un défi supplémentaire réside dans la tendance à intégrer de plus en plus de technologies informatiques et de télécommunications standard (TCP/IP, 4 et 5G, WiFi) dans un réseau de transport essentiel. Cela aura un impact non seulement sur la conception de l'architecture du réseau de transport, mais également sur la phase de maintenance afin de prendre en compte les nouvelles menaces pendant toute la durée de vie dudit réseau.

CAF : UN PARTENAIRE FIABLE À LONG TERME EN MATIÈRE DE SÉCURITÉ ET D'EFFICACITÉ OPÉRATIONNELLE DES CLIENTS

La technologie numérique (intelligence artificielle, Internet industriel des objets, big data, télécommunications, chaînes de blocs, etc.) et les produits standard tels que les produits informatiques COTS seront déterminants pour aider les opérateurs de mobilité à faire face à leurs nouveaux défis, en d'autres termes :

- À augmenter la qualité du service (disponibilité, fiabilité),
- À augmenter la capacité des réseaux de transport, en minimisant le niveau d'investissement,
- À réduire les coûts d'exploitation sous la pression d'une concurrence de plus en plus ouverte.

Cette évolution technologique majeure doit être mise en œuvre en conservant les principales caractéristiques du réseau de transport essentiel et en accordant une attention particulière à la sécurité.

CAF est présent dans le secteur de la mobilité grâce à un portefeuille de transport complet, et notamment : 1) le transport ferroviaire, qui constitue l'épine dorsale des réseaux de mobilité, 2) le transport routier, en tant que leader européen dans le domaine des bus. En termes de chaîne de valeur, CAF est également présent dans des activités telles que le

financement, les projets globaux clés en main, le matériel roulant, la signalisation, les composants et les services, par exemple, la maintenance traditionnelle ou prédictive.

Le principal objectif de CAF a toujours été de fournir des réseaux sûrs dans le respect de l'efficacité opérationnelle des opérateurs. Face à ces nouvelles menaces, CAF a décidé très tôt de lancer une initiative qui vise à atteindre le bon niveau de maturité des compétences de l'équipe interne de CAF ainsi qu'à disposer d'un portefeuille de produits et de réseaux cybersécurisés dès la conception, destiné aussi bien aux opérateurs ferroviaires que routiers.

CAPACITÉ ET PORTEFEUILLE DE CAF EN MATIÈRE DE CYBERSÉCURITÉ

La cybersécurité a un impact sur les télécommunications, les produits, la gestion des risques liés à la cybersécurité, y compris la sécurité, la sécurité des opérations, la maintenance pendant toute la durée de vie des réseaux de transport et, enfin et surtout, la sensibilisation et la formation du personnel des clients et des fournisseurs. Le programme de cybersécurité de CAF a été structuré autour de plusieurs axes de sorte à couvrir tous les aspects nécessaires, y compris les partenaires et les sous-traitants de CAF.

- L'un des principaux axes du programme de cybersécurité est lié à la sensibilisation et à la formation des employés clés de CAF. L'objectif ne vise pas uniquement à garantir le niveau de maturité culturelle de CAF, mais également à soutenir les clients dans toutes les phases d'un projet, de la phase commerciale aux phases de livraison et de maintenance.

- Un deuxième axe vise à garantir la fourniture de solutions « cybersécurisées dès la conception ». Outre les normes nationales, il a été décidé de suivre les normes industrielles bien établies telles que la norme CEI 62443 et la norme CENELEC TS-50701 dans le cadre des applications ferroviaires ou la norme UNECE R155/156 dans le cadre des applications de bus.

  La cybersécurité de CAF soutient les clients tout au long du déploiement des réseaux de transport ainsi que lors des phases d'exploitation, et ce, pendant plusieurs décennies, y compris la maintenance et la supervision de la sécurité : Pendant la phase de déploiement des réseaux, en identifiant, en partenariat avec le client, les principaux risques associés à la cybersécurité et en mettant en œuvre des mesures d'atténuation appropriées à l'aide des produits de CAF « cybersécurisés dès la conception »,

- Outre la réalisation de projets, il est nécessaire de soutenir les clients grâce à la veille et à la gestion des vulnérabilités et des menaces, la gestion des correctifs et le centre d'opérations de sécurité (SOC) afin de superviser et d'améliorer en permanence une posture de sécurité tout en prévenant, détectant, analysant et répondant aux incidents liés à la cybersécurité CAF a défini une feuille de route visant à concevoir des outils permettant de mettre en œuvre ces activités. Les prochaines étapes tiendront compte du retour d'expérience des premières livraisons et anticiperont les nouveaux besoins des clients en raison de la maturité croissante du secteur des transports.

- Un axe est consacré à l'innovation en matière de cybersécurité. La cybersécurité a été incluse dans le processus global d'innovation de CAF. En maintenant l'offre de CAF en matière de cybersécurité à la pointe de la technologie, les clients de CAF pourront garantir la sécurité des voyageurs, l'efficacité opérationnelle des réseaux de transport et le confort des voyageurs.

Les réseaux de transport ferroviaire, en tant que réseaux essentiels, doivent pouvoir fonctionner en toute sécurité lorsqu'ils font face aux attaques inévitables en protégeant les réseaux critiques conçus dans le cadre du concept de cybersécurité. Il ne s'agit pas là seulement d'une question de qualité des services, d'attaques des équipements électroniques des voyageurs ou de pertes économiques, mais également d'une question de sécurité pour les voyageurs.

Conformément aux meilleures pratiques et aux normes de cybersécurité, CAF s'engage à soutenir les opérateurs en leur fournissant les compétences adéquates et des solutions cybersécurisées dès la conception dans le cadre de la mise en œuvre des réseaux de transport, de la maintenance et des activités de supervision de la sécurité.

QUESTIONS & RÉPONSES

Le secteur des transports est-il confronté à de nombreuses cyberattaques ?
Si on le compare au domaine de la cybersécurité informatique, le secteur des transports est confronté à un nombre plutôt faible d'attaques. Cependant, les réseaux de transport sont essentiels. Les conséquences d'une attaque pourraient être désastreuses et porter atteinte à la réputation de l'opérateur. En termes de pirates, les menaces persistantes avancées (APT) sont les plus dangereuses pour notre secteur. Ces pirates disposent de moyens financiers importants et sont sous le contrôle des États. Des événements récents, comme la guerre en Ukraine, ont mis en évidence l'urgence de renforcer la cyberprotection. La tendance à la numérisation et à la standardisation des télécommunications va accroître le nombre d'attaques.

Quels sont les besoins et les exigences des opérateurs ?
Le niveau de maturité en matière de cybersécurité est encore très différent d'un opérateur à l'autre. CAF met actuellement en œuvre quelques projets dans des pays où le niveau d'exigence est élevé. Le minimum pour ces pays est de fournir des produits et réseaux « cybersécurisés dès la conception ». En outre, pendant la durée de vie du réseau de transport essentiel, des mises à jour fréquentes doivent être effectuées afin de faire face à l'évolution des menaces.

Quel est l'impact de la cybersécurité sur les réseaux sans conducteur ?
La technologie des trains sans conducteur est utilisée dans les métros, mais sera intégrée dans un proche avenir dans les grandes lignes, les bus et les tramways. Il s'agit là d'une tendance majeure du secteur compte tenu de la nécessité d'accroître la capacité et la qualité de service des réseaux de transport. Elle sera à l'origine d'un besoin supplémentaire en matière d'analyse des risques. Cela est dû au fait qu'aucun humain ne contrôlera le processus décisionnel et que le niveau d'automatisation sera basé sur une télécommunication plus standard entre les produits à bord des trains/bus et le sol.

Quel est l'impact de la cybersécurité dans l'activité quotidienne des projets de CAF ?
Il est de la plus haute importance que la cybersécurité soit intégrée dans l'ensemble du cycle de vie du projet, de l'analyse des besoins à la certification du réseau à la fin du projet. Cette activité est très similaire à celle liée à la sécurité. Une différence majeure spécifique à la cybersécurité réside dans l'importance de s'assurer, dès le stade de conception, que la maintenabilité du réseau sera prise en compte, car la cybersécurité impliquera des correctifs fréquents afin d'atténuer les nouvelles menaces.