Whitepaper

La cybersécurité dans les transports publics

Le risque grandissant de cybermenaces pour les transports publics

À l'heure où la connectivité numérique révolutionne le secteur des transports, les entreprises de transport sont exposées à une menace croissante de cyber-attaques. Ces dangers invisibles ne visent pas seulement les données sensibles, mais aussi l'intégrité et la sécurité de l'ensemble de l'infrastructure de transport. Les défis qui en résultent et auxquels les entreprises de transport sont confrontées montrent à quel point il est urgent de se protéger contre les cybermenaces et de prendre les mesures de sécurité nécessaires.

A quelles cybermenaces les transports publics sont-ils exposés ?

Différentes menaces potentielles se cachent, comme par exemple :

Les points vulnérables dans les véhicules connectés
Les moyens de transport modernes sont de plus en plus interconnectés. Des vulnérabilités dans ces systèmes pourraient être exploitées par des pirates pour perturber leur fonctionnement.

L'absence de mise à jour des logiciels
Si les logiciels des systèmes de transport ne sont pas régulièrement mis à jour, les failles de sécurité connues sont une invitation aux attaques.

Les interfaces numériques
Des interfaces insuffisamment sécurisées vers des services et des plateformes externes pourraient constituer des portes d'entrée pour des attaques.

Le vol et la manipulation de données
Les cybercriminels dérobent des données personnelles afin de les analyser et de les utiliser, par exemple pour des attaques supplémentaires, de les vendre sur le Darknet ou de les manipuler.

Cette manipulation peut avoir pour but de causer des dommages aux victimes ou de perturber le fonctionnement normal de l'entreprise.

Les attaques par ransomware
La prévalence croissante des ransomwares signifie que les entreprises de transport sont de plus en plus exposées à des attaques de chantage qui perturbent les opérations et impliquent des demandes de rançon élevées.

Les risques de sécurité physiques
Les cyberattaques ne peuvent pas être uniquement virtuelles. La manipulation des signaux de trafic, des aiguillages ou d'autres éléments d'infrastructure peut entraîner des risques physiques pour les passagers et le personnel.

Besoins d'action urgents

Les médias rapportent régulièrement des cyberattaques contre les infrastructures de transport public. Les conséquences sont aussi désagréables pour les passager·ère·s que pour les exploitant·e·s et nuisent à la confiance du public dans la sécurité des transports publics.

Avec la directive NIS2 et le Cyber Resilience Act (CRA), l'UE a obligé les États membres à renforcer la protection des infrastructures critiques. Les premières évaluations de la résilience des TIC dans ces infrastructures par les autorités locales montrent qu'il est nécessaire d'améliorer la gestion des risques cyber. Attendre n'est donc pas une option.

Comment se protéger et comment prévenir les risques potentiels ?

Gestion active des risques de sécurité

La mesure la plus importante est la mise en place d'un système de gestion de la sécurité de l'information (ISMS) appliqué activement. Ce système définit les mesures techniques et organisationnelles nécessaires pour gérer activement les risques de sécurité.

Identification, analyse et atténuation des risques cyber
L'élaboration d'un inventaire des systèmes TIC et leur analyse en termes de risques cyber constituent la base des politiques de sécurité et des mesures techniques à mettre en place.

Prévention et formation
Grâce à l'information et à la formation, les employés sont sensibilisés à l'identification des dangers tels que l'ingénierie sociale et le phishing.

Audits réguliers de la sécurité
En effectuant des contrôles continus des réseaux et des systèmes afin d'identifier les vulnérabilités potentielles et d'y remédier.

Plans d'urgence et responsabilités

Prévoir des dispositions en cas de cyberattaque afin de garantir une réaction rapide et un rétablissement des activités.

Conclusion

La menace de cyber-attaques contre les entreprises de transport et leurs infrastructures est réelle et croissante. Ce n'est qu'en prenant des mesures proactives, comme entre autres une stratégie de cybersécurité robuste, une gestion des risques bien vécue et des vérifications régulières, que les entreprises de transport peuvent protéger leurs systèmes et leurs passagers contre les dangers des cyberattaques. Une étroite collaboration au sein du secteur permet de réduire les ressources et les coûts nécessaires à cet effet.

Besoin d'action et solutions possibles

En octobre 2023, onway ag a posé la première pierre de la sensibilisation à la cybersécurité dans le secteur des transports publics en organisant un événement destiné aux client·e·s et aux personnes intéressées. Pour aller plus loin, nous proposons, en collaboration avec notre partenaire Compass Security, des ateliers axés sur la mise en œuvre pratique des politiques de sécurité via un Système de Gestion de la Sécurité de l'Information (ISMS), ainsi que sur la compréhension de leur impact sur l'exploitation et les processus. Nous transmettons également les connaissances sectorielles nécessaires à la mise en œuvre efficace des mesures de cybersécurité dans les domaines des systèmes, réseaux et applications.

onway accompagne les entreprises du transport public dans l'analyse de leurs risques cyber, ainsi que dans l'Implémentation et l'optimisation des mesures de protection. Nous adoptons une approche structurée : Évaluer, Concevoir, Appliquer, Contrôler et Réagir. Les mécanismes de protection techniques et organisationnels qui en résultent sont alignés sur les normes EN 62443 et TS 50701 et s'intègrent parfaitement dans un Système de Gestion de la Sécurité de l'Information (ISMS), tel que ISO 27001.

Une initiative pour la sécurité dans les transports publics

- Lien vers l'atelier
- Lien vers l'explication de la solution onway
- Lien vers Conseil en sécurité « 5 étapes vers une infrastructure sûre »
- Lien vers la video «La solution intelligente pour le monde mobile»
- Lien vers notre partenaire Compass Security

onway ag | Stauffacherstrasse 16 | 8004 Zurich | Suisse | Tél. +41 55 214 18 30 | info@onway.ch | www.onway.ch