Audit de la résilience informatique des infrastructures critiques – mise en œuvre des exigences minimales des installations de sécurité ferroviaire

Office fédéral des transports, Lausanne-Échallens-Bercher, Transports publics fribourgeois, Zentralbahn et Rhätische Bahn

L'essentiel en bref

Les infrastructures critiques (IC) garantissent l'approvisionnement de la Suisse en biens et services indispensables. Afin de protéger ces IC, il faut assurer leur fonctionnement si possible permanent. La résilience des technologies de l'information et de la communication (TIC), soit la protection des infrastructures critiques (PIC) face aux cybermenaces, revêt ici une grande importance. Le 8 décembre 2017, le Conseil fédéral a adopté la stratégie nationale PIC (2018–2022). Le trafic ferroviaire en fait partie. La Confédération consacre près de 4,5 milliards de francs par an à l'entretien de la substance de l'infrastructure ferroviaire et à l'extension du réseau.

Dans le cadre d'un audit transversal, le Contrôle fédéral des finances (CDF) a vérifié le respect des exigences minimales de protection des TIC face aux cyberattaques auprès de quatre compagnies ferroviaires[1]. La « norme minimale pour améliorer la résilience informatique », publiée par l'Office fédéral pour l'approvisionnement économique du pays (OFAE), a été utilisée à cet effet. Elle couvre en substance les cinq thèmes « identifier », « protéger », « détecter », « réagir » et « récupérer », et propose une série de mesures concrètes à mettre en œuvre. L'OFAE recommande aux exploitants d'IC de mettre en place cette norme minimale des TIC.

Grandes disparités en matière de sécurité de l'information

Selon l'audit, le niveau de protection en place est très hétérogène, son degré de maturité allant de « nettement en dessous de la valeur minimale recommandée » à « valeur minimale largement dépassée ». Toutes les compagnies auditées ont encore des efforts à réaliser dans la mise en œuvre de la sécurité de l'information.

D'un point de vue organisationnel, il est apparu que les rôles en matière de sécurité de l'information n'avaient pas ou pas suffisamment été définis dans trois des quatre compagnies auditées. De plus, leur personnel a une perception très différente des risques informatiques.

Un inventaire exhaustif des informations et systèmes à protéger est la base la plus importante pour la mise en œuvre de la sécurité des TIC. Les compagnies ferroviaires en sont conscientes et tiennent un inventaire de leurs valeurs. Ces dernières figurent en partie dans différentes sources de données sans être reliées entre elles. Divers projets doivent améliorer la situation à l'avenir.

[1] Compagnie du chemin de fer Lausanne-Échallens-Bercher, Transports publics fribourgeois, Zentralbahn et Rhätisch Bahn.

La gestion des accès doit être améliorée dans trois compagnies ferroviaires. Tant la gestion des comptes utilisateur que l'attribution des droits comportent à bien des égards de graves défauts. L'accès à distance par les fournisseurs doit être contrôlé par les clients et clairement documenté. Il y a là un grand besoin de prendre des mesures pour ces compagnies.

De façon générale, la sécurité tant physique que liée à l'environnement doivent faire l'objet d'une attention accrue. Dans un cas, l'accès à la centrale de régulation du trafic n'était pas sécurisé, de sorte que les systèmes TIC s'y trouvant n'étaient pas protégés contre des accès non autorisés. Les appareils servant à la maintenance du matériel roulant sont déverrouillés et accessibles dans certains cas. Quant à la protection anti-incendie, les mesures en place varient fortement d'un cas à l'autre. Alors que divers postes d'enclenchement sont dépourvus de tout système de détection de fumée et d'alarme en cas d'incendie ainsi que de matériel de première intervention (extincteurs), le CDF a repéré dans les équipements critiques d'une autre compagnie ferroviaire des dispositifs redondants d'extinction automatique.

La moitié des compagnies ferroviaires auditées gèrent des centrales de régulation du trafic redondantes situées à des endroits différents, de manière à ne pas perturber l'exploitation en cas de panne.

Tester des scénarios d'urgence et des procédures de restauration devrait être considéré comme un processus permanent. Il serait ainsi possible de s'assurer du fonctionnement des systèmes et processus en cas d'incident. Pour parvenir à un niveau adéquat dans ce domaine, il y a encore du travail à faire dans certaines compagnies.

Exigences de sécurité de l'information: un défi majeur pour les petites compagnies ferroviaires

L'audit transversal a montré que les grandes compagnies ferroviaires sont mieux parées en termes de sécurité des TIC que les petites. Ces dernières sont confrontées ici à un réel défi, en termes financiers et de personnel. Une étroite collaboration avec de grandes compagnies ferroviaires et le recours à des services externes peuvent toutefois avoir un effet positif.

Cette année, l'Office fédéral des transports (OFT) a révisé et adopté les dispositions d'exécution de l'ordonnance sur les chemins de fer. Pour la première fois, la question de la sécurité de l'information y est explicitement inscrite. Avec l'entrée en vigueur des nouvelles dispositions, toutes les entreprises ferroviaires sont tenues de mettre en place et d'exploiter un système de gestion de la sécurité de l'information depuis le 1er novembre 2020. Cependant, l'OFT ne précise ni les exigences minimales, ni le délai pour la mise en œuvre. En précisant ses attentes et en mettant à disposition des outils de travail, l'OFT pourrait apporter un soutien important aux entreprises ferroviaires.

Texte original en allemand