RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

Date : 17 avril 2025
Version : 1.0
Nombre de pages : 43

TRANSPORTS URBAINS

ÉTAT DE LA MENACE INFORMATIQUE

TLP:CLEAR

Table des matières

1 SYNTHÈSE

Les entités du secteur des transports urbains sont caractérisées par une forte criticité. Les attaques informatiques à leur encontre peuvent avoir des conséquences significatives et parfois de long terme affectant la continuité des services de transport, mais également l'intégrité, la disponibilité et la confidentialité des données qu'ils hébergent. En 2024, le contexte des Jeux Olympiques et Paralympiques de Paris a notamment accentué l'exposition de ce secteur, qui a été la cible de plusieurs attaques informatiques au cours de l'année.

Différents modes de transports sont intégrés dans cet état de la menace informatique, principalement certains transports guidés, ferroviaires, routiers et fluviaux, ainsi que les entités responsables de leur opération et les systèmes nécessaires à leur fonctionnement. **Les principales caractéristiques communes de ces réseaux sont leur périmètre géographique urbain, et la nature de leur activité : le transport de passagers, parfois en très grand nombre. Certaines infrastructures de transport urbain connaissent une forte pression (plusieurs millions d'usagers par jour pour certains réseaux), ce qui explique la criticité de ce secteur.** Les exemples retenus dans ce document visent à illustrer le spectre de la menace informatique affectant les entités du secteur des transports urbains dans le monde sans se limiter à des données françaises.

Le secteur des transports urbains est caractérisé par l'importance de la taille des réseaux informatiques des entités, et l'intervention de systèmes de natures diverses. Ces réseaux font s'interconnecter de nombreuses entités : exploitants, équipementiers, chaîne de sous-traitance et prestataires, collectivités territoriales, etc. Ces interconnexions de réseaux aux niveaux de sécurisation hétérogènes augmentent leur surface d'attaque.

La menace informatique à l'encontre des transports urbains est surtout associée à des attaquants motivés par le **gain lucratif**. Du fait de la taille importante des entreprises gérant les réseaux de transport urbains, celles-ci sont des cibles d'intérêt pour des attaques cybercriminelles. La criticité des services du secteur, qui supportent mal les interruptions d'activité, renforce la pression sur les victimes d'attaques par rançongiciel, dont la remédiation difficile peut avoir des conséquences de long terme. Le grand nombre d'utilisateurs expose également ces entités à des attaques à des fins de vol de données ou d'escroqueries à l'encontre de leurs clients. Toutefois, la majorité des attaques à des fins lucratives observées semble davantage de nature opportuniste qu'orientées spécifiquement contre ces entreprises et services.

Des contextes géopolitiques de tension ou de conflits peuvent amener les réseaux de transport urbains à être également ciblés à des fins de **déstabilisation**. Celles-ci peuvent être menées par des attaquants réputés liés à des États visant à saboter ces réseaux critiques, ou des acteurs appartenant à la mouvance hacktiviste, qui conduisent des attaques par déni de service distribué. Les Jeux Olympiques et Paralympiques de Paris 2024 ont servi de caisse de résonance aux revendications de ces hacktivistes.

Les entités du secteur peuvent enfin être la cible d'**attaques à des fins d'espionnage** conduites par des modes opératoires réputés liés à des États. Le secteur représente en effet des opportunités intéressantes pour des services de renseignement, notamment à des fins d'espionnage industriel ou de surveillance d'individus. Des cyberattaques contre des entités du secteur ont été constatées dans le monde sans que la finalité exactes des attaques comme l'identité de la menace n'aient pu être établies de manière certaine, mais qui pourraient relever de l'espionnage.

Activité opérationnelle associée au ciblage des transports urbains

De janvier 2020 à décembre 2024, l'ANSSI a traité 123 événements de sécurité d'origine cyber affectant des entités du secteur des transports urbains (ferroviaire, routier, guidé, fluvial). L'ANSSI distingue deux types d'événements [a] : les signalements [b], à hauteur de 91, et les incidents [c] avec 32 occurrences sur la période.

Les événements cyber rapportés sur cette période contre des entités du secteur portent principalement sur des revendications d'attaques par déni de service distribué (DDoS), des fuites de données ainsi que des usurpations d'identité. En effet, ces trois catégories représentent plus de la moitié des signalements et incidents portés à la connaissance de l'ANSSI. Aucune conséquence significative sur le fonctionnement des entités concernées n'a été identifiée à la suite de ces activités.

a. Événements portés à la connaissance de l'agence et qui ont donné lieu à un traitement par les équipes opérationnelles

b. Les signalements regroupent tous les comportements anormaux ou inattendus pouvant avoir un caractère malveillant ou ouvrir la voie à des usages néfastes à l'encontre d'un SI. Dans le cas des transports urbains, il s'agit principalement de campagnes d'hameçonnage, de divulgation d'information (notamment couples d'authentifiants de connexion), de déclarations réglementaires, de vol ou de mauvaises pratiques de sécurité.

c. Un incident est un événement de sécurité où l'ANSSI est en mesure de confirmer qu'un acteur malveillant a conduit des actions avec succès sur le système d'information (SI) de la victime.

2 PÉRIMÈTRE & MÉTHODOLOGIE

2.1 Modes de transport urbains et acteurs associés

Le périmètre d'analyse de cet état de la menace s'intéresse à l'ensemble des modes de transports typiquement opérés en contexte urbain.

Pour le transport terrestre :

- les réseaux de **transports guidés urbains**[1] (métros, tramways, trolleybus) dont l'autorité de sécurité en France est le STRMTG[2] ;
- les réseaux de transport urbains au gabarit **ferroviaire** (en France, les lignes de RER, réseau ferré d'Île-de-France, et le Transilien) ;
- des **flottes privées** (taxis, voitures de transport avec chauffeur - VTC -, engins de déplacement individuels motorisés ou non : vélos, trotinettes...) et des modes de transport individuels empruntant des axes routiers, sous l'autorité de la DGTIM[3].

Pour les autres modes :

- le transport **fluvial** (Paris est le premier port fluvial en Europe pour le transport de passagers, avec 9,5 millions de passagers transportés en 2023) ;
- le transport aérien urbain est très faiblement représenté par des flottes de drones aériens pour le transport de personnes, encore en phase de projet.

Acteurs et opérateurs des transports urbains

Les réseaux de transport urbains font intervenir différents types d'acteurs :

- les **autorités organisatrices de la mobilité** (AOM), sous l'autorité par exemple de la **région**[4] (par exemple, l'autorité organisatrice des transports pour la région Île-de-France est ÎLE-DE-FRANCE MOBILITÉ). Les **collectivités territoriales**[5] dont notamment les **métropoles** peuvent aussi exploiter directement des réseaux de transport, par le biais de délégations de service public, de régies ou de sociétés publiques locales. Leurs réseaux sont souvent connectés à ceux des équipements de signalisation ;
- les **exploitants de réseaux de transport en commun** : en France, les entreprises TRANSDEV, KEOLIS et la RATP dominent ce marché ;
- les **industriels** et les **équipementiers** qui fournissent le matériel roulant, le matériel de signalisation, les solutions informatiques, leur maintenance en condition de sécurité (MCS) et en condition opérationnelle (MCO) ;
- des **entreprises privées ou parapubliques de flottes** de véhicules routiers (vélos, taxis, VTC, etc.).

1. Le STRMTG définit ainsi les transports guidés : « Sont dénommés "transports guidés urbains" (TGU) tous les appareils de transports publics guidés urbains de personnes : métros, tramways sur fer ou sur pneus et autres systèmes ferroviaires similaires. » [1]
2. Service technique des remontées mécaniques et des transports guidés.
3. Direction générale des infrastructures, des transports et des mobilités.
4. Depuis la loi d'orientation des mobilités (2020), les compétences mobilité, transports et infrastructures des régions se sont progressivement renforcées.
5. Une *Synthèse sur la menace ciblant les collectivités territoriales* a été publiée par l'ANSSI en février 2025 : https://www.cert.ssi.gouv.fr/cti/CERTFR-2025-CTI-002/

2.2 Problématiques de sécurité informatique spécifiques au secteur

Le secteur des transports urbains est marqué par l'utilisation importante de technologies informatiques et la numérisation croissante des services dans un souci d'augmentation de l'efficacité et d'amélioration de l'expérience client.

2.2.1 Convergence de l'IT et de l'OT

> Des recommandations destinées à la sécurisation des systèmes industriels sont présentes en fin de document.

Les réseaux informatiques des transports urbains, notamment guidés et ferroviaires, font s'interfacer des réseaux industriels utilisés pour gérer les opérations appelés **OT** (*operational technology*), et des réseaux de traitement de l'information appelés **IT** (*information technology*). Cette interconnexion, due à l'évolution des technologies, contribue à augmenter la surface d'attaque des réseaux industriels[6].

Les réseaux IT regroupent les ressources nécessaires à la mise en œuvre des services de l'information et de la communication. Pour le secteur des transports urbains, il s'agit par exemple des appareils accessibles aux employés (ordinateurs personnels, téléphones portables, périphériques de bureau, etc.) ainsi qu'aux passagers (informations aux voyageurs, points d'accès *Wi-Fi* publics, etc.).

Les réseaux OT se différencient des réseaux IT par le fait qu'ils pilotent et contrôlent des installations physiques. Les caractéristiques des ICS[7] du secteur des transports urbains sont d'une part leur **grande durée de vie** : les équipements ont été construits pour durer jusqu'à plusieurs dizaines d'années. Ceci peut entraîner des problématiques associées à l'obsolescence de la sécurisation des serveurs et postes de travail qui leur sont associés. D'autre part, les réseaux informatiques de ces équipements doivent assurer la **continuité des activités industrielles**. Leur développement, assuré par un petit nombre d'équipementiers, est centré autour de la sûreté de fonctionnement, de la disponibilité et de l'intégrité des données. Enfin, certains équipements et leurs réseaux informatiques sont conçus spécifiquement pour être opérés dans un environnement précis.

Parmi les exemples de technologies opérationnelles du secteur des transports urbains figurent les systèmes CBTC[8], les systèmes de contrôle du mouvement des véhicules, les systèmes de fourniture du courant au réseau, les systèmes de chauffage, de ventilation et de climatisation, le contrôle d'accès, les systèmes de suivi et de localisation GNSS (*Global navigation satellite system*)[9], la surveillance, la réaction aux alarmes, les systèmes de signalisation, les systèmes embarqués ou encore les systèmes de maintenance pour réaliser des rapports sur l'état du matériel roulant et des équipements périphériques [2]. Ces systèmes sont amenés à être de plus en plus connectés à Internet [3].

6. L'ANSSI publie des guides sur la cybersécurité des systèmes industriels : https://cyber.gouv.fr/publications/la-cybersecurite-des-systemes-industriels
7. *Industrial control systems*, systèmes de contrôle industriel.
8. *Communication based train control* : ce système de communication entre le sol et le train permet de transmettre des ordres, par exemple pour automatiser certaines tâches, assurer l'aiguillage, la gestion des façades des quais, la gestion des temps de pause des rames aux stations, la fréquence et l'intervalle entre les rames.
9. Géolocalisation et navigation par un système de satellites.

2.2.1.1 Automatisation croissante des transports guidés et routiers

L'**automatisation** de certains modes de transport urbains comporte des avantages pour les exploitants et les usagers. Concernant les lignes de métro, l'automatisation permet, d'après la RATP [10], d'améliorer la régularité et la fiabilité du trafic, d'augmenter la fréquence des rames, de réduire les intervalles entre les rames, et de réaliser des économies d'énergie, notamment en optimisant le freinage [4]. La sécurisation des systèmes d'automatisation doit suivre les règles de cloisonnement propres aux systèmes industriels afin de réduire leur exposition à des attaques informatiques et éviter leur interruption. L'automatisation s'appuie notamment sur les communications assurées par le système de CBTC.

Le STRMTG est également en charge de la sécurité et cybersécurité des **systèmes de transports routiers automatisés** (STRA), et a a publié en novembre 2024 un guide d'application relatif à leur cybersécurité [11].

2.2.1.2 Recours aux *IoT*

Un grand nombre de réseaux informatiques urbains s'appuie sur des appareils connectés à Internet, appartenant à l'**Internet des objets** (**IoT** pour *Internet of things*). Une vaste gamme d'équipements connectés à Internet (caméras de vidéosurveillance, appareils de billettique, etc.) intervient dans des questions cruciales de gestion du trafic, de signalisation informative, d'automatisation des équipements, ou encore de gestion de flotte.

Commentaire : l'analyse de la menace informatique affectant le secteur des transports urbains met en lumière le fait que les attaques documentées et connues de l'ANSSI concernent en majorité les environnements IT des entités. Si l'ANSSI n'a pas connaissance d'incidents ayant affecté les environnements proprement industriels des entités, ces réseaux demeurent de potentielles cibles critiques d'attaques informatiques à des fins de sabotage, aux conséquences potentiellement graves. Leurs vulnérabilités intrinsèques conjuguées à leur interconnexion au réseau IT font des ICS une cible attractive des attaques informatiques. Certains réseaux OT sont caractérisés par leur horizontalité et leur manque de cloisonnement pour faciliter leur gestion ; cela peut également faciliter les attaques informatiques et la latéralisation des attaquants sur l'ensemble du réseau.

2.2.2 Réseaux billettiques et gestion des abonnements

Les **réseaux billettiques** de distribution des titres de transport et de gestion des abonnements sont concernés par des problématiques de sécurisation informatique spécifiques, comme la complexité de leur architecture, ou la sécurisation des bases de données personnelles des usagers, dont la taille peut être très importante. Les bases de données des entités du secteur des transports urbains, potentiellement partagées à des prestataires, sont régulièrement sujettes à des exfiltrations ou susceptibles d'être accédées lors d'attaques informatiques [12]. La dématérialisation des billets sur les téléphones personnels des usagers renforce potentiellement l'exposition des données personnelles non maîtrisées sur des appareils vulnérables.

10. Avec 450 kilomètres de lignes automatisées et semi-automatisées dans le monde, la RATP est le deuxième opérateur mondial de lignes automatisées.

11. https://www.strmtg.developpement-durable.gouv.fr/guide-d-application-relatif-a-la-cybersecurite-a807.html?lang=fr

12. Plusieurs ressources sur la sécurisation des données personnelles ont été publiées, par la CNIL : https://www.cnil.fr/fr/cybersecurite/securite-des-donnees et l'ANSSI : https://cyber.gouv.fr/publications/se-proteger-des-fuites-de-donnees, https://www.cert.ssi.gouv.fr/uploads/CERTFR-2024-CTI-009.pdf

2.2.3 Sûreté de fonctionnement, sécurité informatique et sécurité physique

Plusieurs menaces sont rendues possibles par des faiblesses dans la mise en place de mesures liées aux notions de sûreté de fonctionnement, de sécurité informatique et de sécurité physique :

- La **sûreté de fonctionnement** a pour objectif d'éviter les accidents, les erreurs, les pannes et les causes de défaillance des composants des systèmes. Pour être robuste, la sûreté de fonctionnement doit ainsi prendre en compte la malveillance et le fait qu'un ordre ou qu'un état communiqué n'a pas forcément de valeur légitime ;
- la **sécurité de l'information** a pour objectif d'assurer l'intégrité, la disponibilité et l'authenticité des informations, en prenant en compte des actions malveillantes dans l'analyse de la menace ;
- la **sécurité physique** a pour objectif d'entraver les accès physiques aux SI par des tiers malveillants, afin d'intervenir en cas d'attaque, de retarder et de réduire au maximum les conséquences des attaques.

Concernant les transports guidés, les accès physiques aux réseaux informatiques peuvent entraîner des conséquences dont les niveaux de gravité varient. Plusieurs menaces sont induites par l'utilisation de systèmes de CBTC, qui est un élément important de sûreté de fonctionnement. Ce système est très exposé physiquement et des équipements informatiques présents dans des lieux ouverts au public ou embarqués dans les véhicules peuvent servir de point d'entrée sur le réseau informatique : d'une part, des attaquants pourraient porter atteinte aux communications sans fil entre les bornes et les antennes du train, et les mécanismes de chiffrement qui assurent leur intégrité peuvent être cassés. D'autre part, les systèmes de CBTC s'appuient sur des câbles qui courent le long des voies et qui peuvent être accédées par des tiers malveillants. Enfin, des attaques peuvent être effectuées *via* **la chaîne d'approvisionnement logiciel**, ou les attaquants peuvent exploiter des failles ou mauvaises configuration de protocoles de communication utilisés.

Concernant les transports routiers, les **réseaux informatiques de certains équipements routiers**, à l'image des **équipements de signalisation et d'affichage** (feux tricolores, panneaux à message variable), ou encore des **tunnels** ou de **ponts** (systèmes de ventilation, d'éclairage, d'affichage, d'alarmes en cas d'accidents ou d'incendies), sont exposés à des attaques informatiques, dont les conséquences sur la sécurité physique des usagers sont potentiellement graves. Le niveau de sécurité des équipements de sécurité physique - comme la **vidéoprotection** ou les **systèmes de contrôle d'accès physiques** - est régulièrement remis en cause [13]. Leur potentielle connexion à Internet les expose à une grande variété d'attaques, facilitées par les vulnérabilités affectant ces équipements.

2.2.4 Systèmes d'information aux voyageurs

Les réseaux informatiques soutenant l'**information aux voyageurs** (SIV), par le biais d'applications mobiles ou d'affichage en station et aux arrêts, sont également susceptibles d'être compromis à des fins de **déstabilisation** par des défigurations, des attaques par déni de service distribué (DDoS) [14], ou de subir les conséquences d'attaques informatiques contre des SI qui leurs seraient

13. L'ANSSI met à disposition un guide pour la Sécurisation des systèmes de contrôle d'accès physique et vidéoprotection : https://cyber.gouv.fr/publications/securisation-des-systemes-de-controle-dacces-physique-et-videoprotection

14. Une attaque par déni de service distribué, ou DDoS, est une action ayant pour effet d'empêcher ou de limiter fortement la capacité d'un système à fournir le service attendu. Lors qu'il s'agit d'une attaque, l'action est malveillante ; elle peut également être la conséquence d'un mauvais dimensionnement du service. On parle de « déni de

interconnectés.

2.2.5 Recours généralisé aux GNSS

Les **systèmes d'information de gestion des flottes** sont nécessaires au fonctionnement de réseaux de transport. Parmi ces technologies, les données fournies par les systèmes GNSS (par exemple GALILEO ou GPS) sont nécessaires à l'opération de nombreux services du secteur des transports, afin de connaître leur PNT (*position, navigation & timing*). Ce paramètre est par exemple indispensable pour la gestion des flottes d'entités du secteur des transports urbains comme les VTC, les sociétés de taxis, ou mettant à disposition des engins de déplacement personnel. Ce type de signal peut subir des interférences ou des interruptions [5].

> Des recommandations liées aux systèmes informatiques dépendants aux signaux radio et GNSS sont présentes en fin de document.

2.2.6 Un recours croissant aux prestataires

Les acteurs du secteur des transports urbains recourent à l'externalisation et à la sous-traitance dans plusieurs domaines. Certains opérateurs font appel à des prestataires pour réaliser certaines parties de la production dans une logique de mutualisation des coûts. Des prestataires peuvent également être engagés pour affréter des lignes quand les opérateurs n'ont pas les moyens matériels ou humains de les exploiter seuls [6]. Les entités du secteur peuvent également remplir la fonction de prestataire et gérer des systèmes d'information spécifiques pour le compte de clients. Ces systèmes, qui sont susceptibles d'être la cible d'attaques informatiques, augmentent la surface d'exposition du prestataire comme du client du fait de leurs interconnexions.

Les entités du secteur recourent également à des prestataires pour gérer leur informatique, y compris leur sécurité informatique, tels que des entreprises de services numériques (ESN), des infogérants, des hébergeurs, des fournisseurs de logiciel ou de solutions numériques [15].

Le recours à l'externalisation ou à la chaîne de sous-traitance au sein du secteur des transports implique une augmentation de la surface d'exposition à la menace informatique, notamment lors de l'interconnexion des systèmes d'information.

> Des recommandations liées au recours aux prestataires sont présentes en fin de document.

2.2.7 Ouverture à la concurrence

L'opération de mêmes réseaux de transport (notamment guidés et ferroviaires) par des entités différentes est de plus en plus fréquente. Du fait de l'augmentation du nombre d'acteurs et d'interconnexions, **l'ouverture à la concurrence est un facteur aggravant la complexité des questions de sécurité informatique** et fait apparaître de nouveaux enjeux de gestion.

service distribué » (de l'anglais *Distributed Denial of Service*) lorsque l'attaque fait intervenir un réseau de machines (souvent compromises) afin d'interrompre le ou les services visés.

15. Voir le rapport du CERT-FR sur les *Supply chain attacks : menaces sur les prestataires de service et les bureaux d'études* du 7 octobre 2019, disponible en ligne : https://www.cert.ssi.gouv.fr/cti/CERTFR-2019-CTI-004/

2.2.8 Les transports urbains dans les « territoires intelligents »

L'informatisation croissante des réseaux de transport urbains s'inscrit dans l'économie des « territoires intelligents » ou « *smart cities* ». Ce concept renvoie à la centralisation de la gestion informatique d'une variété importante d'infrastructures urbaines, dont certaines sont critiques, à des fins de facilitation de leur gestion et d'amélioration de leur fonctionnement. Ces infrastructures sont par exemple les systèmes de gestion de l'eau [16], de gestion technique des bâtiments et de chauffage, de vidéosurveillance des lieux publics (dont des axes de transport), de transport d'électricité locale, ainsi que de signalisation ou de transports publics.

La ville d'Olsztyn, située au nord de la Pologne, est un exemple de « *smart city* ». La régie de transport de la ville opère un centre de gestion du trafic, permettant notamment d'adapter les paramètres des équipements de signalisation aux conditions réelles de circulation. Dans la nuit du 24 au 25 juin 2023, une attaque informatique dont la nature n'a pas été précisée a affecté différents modes de transports de la ville. La vente de billets pour les transports en commun a été rendue indisponible, l'affichage en temps réel des horaires de bus et de tram a été passé en mode automatique ainsi que les feux de signalisation, ralentissant considérablement le trafic routier [7, 8].

> Des recommandations liées à la continuité des activités et au passage en mode dégradé suite à des incidents informatiques sont disponibles en fin de document.

16. Un état de la menace informatique affectant le secteur de l'eau a été publié par l'ANSSI en novembre 2024 : https://www.cert.ssi.gouv.fr/uploads/CERTFR-2024-CTI-011.pdf

3 MENACE À FINALITÉ LUCRATIVE

La menace à finalité lucrative affectant le secteur des transports urbains est caractérisée par la diversité des acteurs, des objectifs de leurs attaques et des capacités mises en œuvre. Les **intentions** des attaquants sont multiples : ils peuvent chercher à attaquer des entreprises de transport ou leurs usagers pour leur extorquer des fonds, notamment *via* le déploiement de rançongiciels ou par exemple tirer profit de l'exfiltration de données d'usagers ou de personnels, qui sont par ailleurs potentiellement réutilisables lors de compromissions ultérieures.

Les **capacités** mises en œuvre pour conduire des attaques à finalité lucrative sont propres à l'écosystème cybercriminel. Le principal vecteur de compromission identifié est l'hameçonnage. Il n'en reste pas moins que l'exploitation de vulnérabilités sur des logiciels et équipements couramment utilisés, qui ne sont pas forcément spécifiques au secteur, demeure un vecteur courant de compromission. Les attaquants conduisent des activités d'énumération (*scan*) pour obtenir de manière opportuniste des accès permettant une compromission ultérieure du système d'information [9].

Les attaques informatiques à des fins lucratives à l'encontre des entités du secteur sont en grande partie de nature **opportuniste**. Les attaquants, en recherche de la rentabilité maximale de leurs attaques, choisissent par exemple leurs victimes en fonction de leur taille importante (*big game hunting*[17]).

Plusieurs recommandations liées aux attaques par rançongiciel sont présentes en fin de document :

- Assurer la sauvegarde des données ;
- Mettre en œuvre une passerelle d'interconnexion à Internet ;
- Cloisonner et filtrer les différents systèmes d'information ;
- Cloisonner et filtrer les différents sous-systèmes d'un système d'information ;
- Durcir la configuration des équipements ;
- Maintenir à jour le système d'information.

17. Cette notion de « chasse au gros gibier » renvoie à un type particulier de victimologie : les entités ciblées sont choisies en fonction de la rentabilité potentielle de leur compromission et de leur capacité à payer une rançon importante.

Chiffrement d'entités du secteur

Parmi les compromissions à des fins de chiffrement menées contre des entités françaises du secteur des transports urbains et portées à la connaissance de l'ANSSI, aucune n'a provoqué de perturbation significative dans le fonctionnement des entités attaquées.

L'ANSSI a eu connaissance d'au moins quatre compromissions ou tentatives de compromission par rançongiciel ayant touché des entités françaises du secteur entre 2020 et 2024 :

- en 2020, une compromission a touché l'infrastructure de virtualisation du comité d'entreprise d'une entité du secteur ;
- en 2022, une souche de rançongiciel a été observée sur l'infrastructure d'un réseau de bus lors d'une tentative de compromission ;
- en 2023, un groupe opérateur de rançongiciel a revendiqué le chiffrement d'une entité du secteur specialisée dans les services de mobilité ainsi que d'une de ses filiales ;
- en 2024, plusieurs ressources du SI d'une entité du secteur des transports urbains ont été chiffrées, ce qui a entraîné l'indisponibilité de différentes solutions de l'entreprise.

3.1 Extorsions et attaques par rançongiciel contre des entités du secteur

3.1.1 Extorsions et attaques par rançongiciel contre des exploitants de réseaux de transports urbains guidés

Les **exploitants de réseaux de transports urbains guidés** sont régulièrement la cible d'attaques par rançongiciel. Ces attaques, qui peuvent aboutir au chiffrement d'une partie ou de la totalité des SI de la victime, sont potentiellement suivies de conséquences importantes et parfois de long terme. Elles peuvent affecter les services internes des exploitants de réseaux de transports urbains, qui gèrent d'importantes ressources humaines, et toucher un grand nombre d'usagers dépendants de ces services de transport. Elles sont susceptibles de compromettre la disponibilité de l'ensemble des services des entreprises, d'interrompre la continuité des activités, et de porter atteinte à leur image de marque.

En octobre 2021, les activités de la TORONTO TRANSIT COMMISSION (TTC), troisième plus grand système de transport en commun en Amérique du Nord, ont été perturbées à la suite d'une attaque par rançongiciel dont la souche n'a pas été précisée [10, 11, 12]. Les attaquants auraient accédé aux SI de l'entité *via* hameçonnage afin de déposer un code malveillant pour chiffrer les réseaux IT. Le chiffrement des serveurs de l'entreprise a affecté différents SI internes, comme la messagerie électronique, mais également des systèmes liés à la conduite et à la gestion des trains : les informations sur l'arrivée des véhicules, la visualisation en temps réel de leurs déplacements, ou encore le système vidéo de communication des conducteurs. Ce dernier a été remplacé par un système de communication radio jusqu'à la remédiation de la compromission d'après le média The Record [11]. L'attaque aurait également affecté des services destinés aux usagers, comme la billetterie réservée aux personnes en situation de handicap, les applications de planification de trajets et le site internet de la TTC. D'après les investigations de la TTC [10], des informations personnelles de 25 000 employés et anciens employés pourraient avoir été volées au cours de l'attaque.

Le 6 octobre 2021, les opérateurs du *Ransomware-as-a-Service*[18] Lockbit[19] ont revendiqué avoir mené une attaque contre l'exploitant de transport français TRANSDEV et détenir 200 gigaoctets de données appartenant à la victime. Selon l'entreprise, citée par le média Le Mag IT, l'attaque aurait été détectée le 20 septembre 2021 sur les serveurs informatiques (gérés par TRANSDEV) de l'un de ses clients aux États-Unis dont l'identité n'a pas été précisée [13]. Les conséquences de l'attaque auraient été limitées au périmètre de ce client de TRANSDEV, grâce aux mesures de mitigation mises en place par l'entreprise.

Commentaire : cet exemple illustre la nécessité, pour des entreprises de grande taille dont les SI sont interconnectés avec ceux de leurs clients ou prestataires, d'assurer un cloisonnement suffisant afin d'éviter que les compromissions potentielles ne s'étendent à d'autres réseaux.

3.1.2 Extorsions et attaques par rançongiciel contre des exploitants de réseaux de transports urbains routiers

Un certain nombre d'exploitants de transports urbains sont de plus petite taille : leurs activités sont notamment concentrées sur le transport routier (des lignes de bus), et les conséquences des attaques dont ils sont des cibles régulières sont en général plus facilement remédiables.

En novembre 2022, l'entreprise TUSSAM qui assure les transports de la ville de Séville en Espagne a été victime d'une attaque informatique dont la nature n'a pas été précisée, qui a entraîné l'indisponibilité de l'application et du site Internet de l'entité ainsi que des panneaux d'information des abribus, d'après des informations de la municipalité citées par le média Viva Sevilla [14]. Les attaquants n'auraient pas accédé aux données personnelles des clients ni aux données des opérations de l'entreprise. La circulation des services de bus assurés par l'entreprise n'a pas été affectée, grâce à la mise en œuvre de moyens manuels.

En décembre 2023, la compromission par rançongiciel de l'entreprise GREATER RICHMOND TRANSIT COMPAGNY, gestionnaire de services de transports par bus dans l'État américain de Virginie, a été revendiquée par le rançongiciel Play[20] [17]. D'après l'entreprise, l'attaque aurait été rapidement détectée et remédiée, sans affecter durablement les services de transport.

3.1.3 Extorsions et attaques par rançongiciel contre des entreprises de VTC et taxis

Les **entreprises de VTC et de taxis** sont des cibles régulières d'attaques informatiques à des fins lucratives visant à leur extorquer des fonds par le biais de chantage à la divulgation de données exfiltrées ou suite au déploiement de rançongiciels chiffrant leurs SI.

Entre au moins septembre 2019 et septembre 2021, deux citoyens américains résidant aux États-Unis, ainsi que deux citoyens russes résidant en Russie, auraient compromis le système de répartition des taxis de l'aéroport J. F. Kennedy de New York afin de le détourner, d'après le *Department of Justice américain* [18]. La compromission du système informatique de répartition des

18. Le terme de « Rançongiciel en tant que service » (RaaS pour *Ransomware-as-a-Service*) signifie que les opérateurs du rançongiciel ne sont pas nécessairement ses développeurs. Plusieurs groupes d'attaquants peuvent mener des attaques délivrant le rançongiciel, et les chaînes d'infection peuvent différer d'une compromission à l'autre. Les attaquants accèdent au rançongiciel en échange d'une commission sur leurs gains ou d'un prix négocié.

19. Apparu en septembre 2019, LockBit (et ses variantes disribuées telles que Lockbit 2.0) fonctionne sous le modèle économique de RaaS ; ce rançongiciel est associé à un grand nombre de compromissions dans le monde entier.

20. Le groupe opérateur du rançongiciel Play serait actif depuis au moins juin 2022. Les attaquants utilisent des techniques de double extorsion contre des victimes des secteurs des télécommunications, de la santé, des médias, des technologies et des assurances, principalement en Europe et en Amérique du Nord [15, 16].

taxis par les accusés leur a permis de mettre en place un système favorisant certains taxis dans la liste d'attente contre une rétribution financière. D'après la mise en accusation, les attaquants ont utilisé divers moyens pour accéder au système de répartition, notamment en soudoyant un agent pour qu'il insère une clé USB contenant des logiciels malveillants dans les ordinateurs connectés au système, en obtenant un accès non autorisé au système *via* une connexion Wi-Fi et en volant des tablettes connectées au système [18].

En juillet 2022, un groupe opérateur de rançongiciel non précisé aurait compromis une entité sud-coréenne du secteur des taxis dans la province de Gangwon, entraînant le chiffrement de serveurs et l'indisponibilité de services tels que les applications mobiles [19]. Les commandes de taxi de la région ainsi que des taxis réservés aux personnes en situation de handicap de la région de Busan ont été gérées manuellement, retardant considérablement les services. L'entreprise aurait accédé à la demande de rançon des attaquants afin d'obtenir des moyens de déchiffrement, d'après l'éditeur de sécurité BitDefender [19].

Commentaire : dans le cas d'une attaque par rançongiciel, l'ANSSI recommande de ne jamais payer la rançon qui ne garantit pas l'obtention d'un moyen de déchiffrement, incite les cybercriminels à poursuivre leurs activités et entretient ce système frauduleux. De plus, le paiement de la rançon n'empêchera pas l'entité compromise d'être à nouveau la cible de cybercriminels, et catégorise la victime comme encline à payer de futures rançons, sans combler les failles exploitées par les attaquants. L'expérience montre par ailleurs que l'obtention de la clé de déchiffrement ne permet pas toujours de reconstituer l'intégralité des fichiers chiffrés. En particulier, les fichiers modifiés par une application et chiffrés dans le même temps par le rançongiciel ont de fortes chances d'être corrompus (par exemple : un fichier de base de données).

En septembre 2022, l'entreprise de transport avec chauffeurs Uber a déclaré avoir subi une attaque informatique ayant entraîné la compromission de plusieurs comptes d'employés par des attaquants associés au groupe cybercriminel Lapsus$[21] [22]. Les attaquants auraient obtenu des accès au compte d'un contractant externe d'Uber[22] [22, 23], et seraient parvenus à contourner l'authentification à deux facteurs pour accéder à son compte. Suite à des manœuvres d'ingénierie sociale, les attaquants auraient compromis les comptes d'autres employés d'Uber pour accéder à des outils internes, tels que la plateforme de travail collaborative Slack et la suite d'outils G Suite. Le périmètre de la compromission de l'entreprise aurait été limité à des réseaux internes, comme des messages publiés sur son Slack ainsi que des informations comptables. D'après Uber, les attaquants n'auraient pas accédé aux systèmes de production (opérations de transport liées au public), et aucune donnée d'utilisateur (informations relatives aux trajets ou données financières) n'aurait été exposée [22]. Les services de transport et de livraison n'auraient pas été affectés par l'attaque informatique.

Commentaire : cette tentative de compromission d'Uber souligne que la surface de compromission des entités est augmentée par les interconnexions de contractants externes à l'entreprise.

> Des recommandations liées à la sensibilisation des collaborateurs sont présentes en fin de document.

21. Le groupe Lapsus$, actif depuis au moins 2021 et démantelé en 2022 après l'arrestation de plusieurs de ses membres, est responsable d'un grand nombre d'attaques informatiques à des fins d'extorsion : les attaquants menacent de publier les données exfiltrées à leurs victimes afin d'obtenir le paiement d'une rançon[20, 21].
22. « An Uber EXT contractor ».

3.2 Attaques contre des bases de données à des fins d'exploitation, d'exfiltration et de reventes

Si les attaques contre les bases de données à des fins d'exploitation, d'exfiltration et de revente ne sont pas spécifiques au secteur des transports urbains, les entités du secteur en sont couramment les cibles. Les entreprises de transport urbain gèrent un grand nombre d'informations personnelles relatives aux usagers et à leurs employés, de nature bancaire et d'authentification. Un grand nombre des incidents affectant ce type d'entités observés par l'ANSSI aboutissent à l'exfiltration de données personnelles. Ces entreprises possèdent également des données propres à la nature de leurs activités et potentiellement stratégiques (données comptables, savoir-faire, etc.). Ces données ont une valeur à la revente du fait de leur sensibilité.

Ces données peuvent être dérobées pour être revendues à d'autres acteurs cybercriminels sur des forums spécialisés, des *marketplaces* sur le *darknet* ou encore sur des plateformes de messagerie. Ces données peuvent être exploitées pour conduire d'autres attaques informatiques ou réaliser des fraudes.

Des opérateurs de rançongiciel peuvent chercher à utiliser ce moyen de pression sur des victimes dans des cas de double extorsion en menaçant de publier ces données en plus de chiffrer les SI de leurs victimes, afin d'accélérer le paiement de la rançon.

Fuites de données d'entités du secteur

Les fuites de données recensées entre 2020 et 2024 ont porté sur des données de natures diverses (personnelles, métier, authentifiants). Ces fuites de données ont tendance à être issues de la compromission de prestataires détenant des informations appartenant à des entités du secteur des transports urbains. Cette caractéristique illustre une nouvelle fois les risques que peuvent représenter les interconnexions à des entités externes en matière de sécurité informatique.

Les fuites de données mettent également en avant l'enjeu particulier que représente la protection des données personnelles pour ces entités, qui centralisent un grand nombre d'informations de ce type.

Plusieurs recommandations liées à la sécurisation des bases de données sont présentes en fin de document :

- Mettre en œuvre une passerelle d'interconnexion à Internet ;
- Cloisonner et filtrer les différents systèmes d'information ;
- Cloisonner et filtrer les différents sous-systèmes d'un système d'information ;
- Protéger les données par mécanisme cryptographique ;
- Mettre en place une politique de mots de passe robuste ;
- Mettre en place une authentification forte pour les comptes d'accès sensibles et tout accès distant ;
- Durcir la configuration des équipements ;
- Maintenir à jour le système d'information.

Pour les mesures portant spécifiquement sur la protection des données, l'entité doit se référer à la réglementation qui lui est applicable comme par exemple le Règlement général sur la protection des données (RGPD) [24] pour les données personnelles.

3.2.1 Attaques contre des bases de données d'exploitants de réseaux de transport urbains

Le 6 octobre 2023, ÎLE-DE-FRANCE MOBILITÉS, autorité organisatrice de la mobilité pour la région Île-de-France, a déclaré que le service ÎLE-DE-FRANCE MOBILITÉS CONNECT avait été victime d'une tentative de piratage. Cet incident aurait entraîné l'exfiltration de 4 000 adresses de messagerie électronique et mots de passe actifs d'utilisateurs par les attaquants, qui ont été utilisés pour se connecter aux comptes, d'après un communiqué d'ÎLE-DE-FRANCE MOBILITÉS cité par plusieurs médias [25, 26].

Le 2 septembre 2024, l'opérateur de transports londonien TRANSPORT FOR LONDON a déclaré avoir subi un incident de cybersécurité lors duquel des attaquants non précisés ont accédé aux données de remboursement de la carte de transport « Oyster Card » d'environ 5 000 clients [27]. D'après TRANSPORT FOR LONDON, les attaquants auraient pu accéder aux numéros de comptes bancaires et aux *sort codes*[23] de certains clients. Par ailleurs, en 2019, des attaquants ont ciblé des utilisateurs de la « Oyster Card » par une attaque par *credential stuffing*[24]. TRANSPORT FOR LONDON a estimé qu'environ 1 200 comptes de clients avaient été accédés par les attaquants. Le site internet de TRANSPORT FOR LONDON associé aux « Oyster Cards » a été temporairement suspendu lors de la remédiation de l'incident.

Commentaire : les grandes entités du secteur des transports urbains sont des cibles régulières de ce type d'attaque, puisqu'elles sont détentrices d'un grand volume de données. Ces attaques ont de potentielles conséquences sur les utilisateurs quand les données sont exploitées dans le cadre de fraude.

3.2.2 Exfiltrations et expositions de données gérées par des gestionnaires de flottes

Les gestionnaires de flottes de taxis ou de VTC sont également détenteurs de données personnelles relatives aux usagers, dont la divulgation peut exposer des informations précises telles que des trajets, des informations financières ou encore associées à la santé des usagers.

En septembre 2023, le groupe d'attaquants informatiques Irleaks[25] a revendiqué avoir exfiltré des données appartenant à 27 millions d'usagers et conducteurs de l'entreprise iranienne de taxis TAPSI, et aurait réclamé une rançon de 35 000 $ à la victime. Ces données ont par la suite été mises en vente sur le réseau TELEGRAM d'Irleak [28, 29]. Les détails de cette attaque informatique n'ont pas été précisés par la victime.

Certaines failles de sécurité affectant des solutions de traitement informatique entraînent l'exposition de données personnelles en dehors de contextes d'attaques. Par exemple, en novembre 2024, la plateforme irlandaise de réservation de taxi ICABBI a corrigé une faille logicielle qui avait entraîné l'exposition de données personnelles (adresses de messagerie électronique) de

23. Les *sort codes* sont des codes bancaires en usage au Royaume-Uni dans les transferts entre entités financières.

24. Le terme *credential stuffing*, traduit par « bourrage d'identifiants », renvoie à une méthode d'attaque consistant en la réutilisation de combinaisons d'identifiant-mot de passe obtenus lors de compromissions précédentes pour tenter d'accéder à d'autres comptes créés avec les mêmes identifiants.

25. Irleaks est un groupe actif depuis au moins 2022, responsable d'attaques informatiques à des fins de déstabilisation et lucratives à l'encontre de plusieurs entités iraniennes des secteurs de la finance, des assurances, de la livraison de nourriture et des transports urbains. Les attaquants demandent une rançon aux victimes et proposent les données exfiltrées à la vente sur leur canal Telegram, ce qui suggère que leur motivation principale est le gain lucratif. L'échelle importante des fuites de données revendiquées par Irleaks, concernant plusieurs millions d'individus, suggère que les attaquants disposent de fortes ressources offensives : certains observateurs font l'hypothèse que de capacités étatiques sont impliquées dans les campagnes d'Irleaks, dans le contexte de tensions géopolitique liées à l'Iran [28].

près de 300 000 personnes au Royaume-Uni et en Irlande [30]. Les données divulguées semblent être liées aux applications destinées aux clients et utilisant ICABBI, d'après le média The Register. De même, en décembre 2024, une vulnérabilité affectant une des API[26] de traitement de données de l'application mobile de l'entreprise indienne de taxis RAPIDO, découverte par l'entreprise TECHCRUNCH, a entraîné l'exposition en ligne de données appartenant aux utilisateurs, dont les noms, adresses de messagerie électronique, et les numéros de téléphone [31].

Commentaire : ce type d'exposition de données met en évidence l'exploitation des vulnérabilités informatiques et des failles de sécurité affectant les applications développées pour les besoins du secteur des transports urbains. Ces informations sont potentiellement réutilisables par des attaquants informatiques dans le cadre de campagnes d'hameçonnage à des fins d'extorsion.

3.3 Attaques contre les usagers à des fins d'extorsion

Usurpation d'entités du secteur

Les acteurs malveillants exploitent la visibilité et la réputation des principaux acteurs du secteur des transports urbains ainsi que les liens de confiance avec les usagers en créant des pages frauduleuses aux couleurs de ces entités.

Si ce type de détournement, au même titre que les fuites de données, demeure relativement peu sophistiqué, ces actions peuvent toutefois avoir des effets réputationnels délétères pour ces entités.

Ainsi que d'autres secteurs associés à un grand nombre d'usagers, les usagers des services de transports urbains sont des cibles fréquentes de tentatives d'extorsion par des attaques frauduleuses, qui s'appuient couramment sur l'usurpation de l'identité d'entités existantes. La création de noms de domaines (*spoofing* et *typosquatting*) aux couleurs d'entités du secteur est courante, et peut entraîner la compromission de comptes personnels d'usagers.

Les attaquants exploitent des temporalités spécifiques comme les campagnes annuelles d'abonnement ou de remboursement de cartes d'abonnement [32]. De même, le contexte des Jeux Olympiques et Paralympiques de Paris 2024 a entraîné une recrudescence des campagnes de fraudes à destination des usagers d'ÎLE-DE-FRANCE MOBILITÉS [33].

Des recommandations liées à l'enregistrement des variations du nom de domaine des entités sont présentes en fin de document.

26. *Application Programming Interface* (interface de programmation d'application).

4 MENACE À FINALITÉ DE DÉSTABILISATION

Les entités du secteur des transports urbains sont prises pour cible par des attaques à des fins de déstabilisation. Les **intentions** des attaquants sont de rompre ou perturber la continuité des services assurés. Les **capacités** mises en œuvre sont diverses. Les codes destructeurs sont propres aux attaquants dotés de ressources étatiques, tandis que les attaques par déni de service distribué ou qui visent à détourner les transports urbains seraient davantage le fait de groupes hacktivistes. Les **opportunités** saisies par les attaquants sont liées aux contextes de guerre ou de contextes géopolitiques conflictuels ; les Jeux Olympiques et Paralympiques de Paris 2024 ont servi de caisse de résonance à des revendications d'attaques par DDoS contre des entités françaises du secteur des transports urbains.

4.1 Attaques à des fins de destruction contre des entités de transport urbain

Ce type d'attaque s'inscrit généralement dans des contextes de tensions internationales : des attaquants réputés liés à des États peuvent chercher à immobiliser les réseaux de transport d'un État dans le cadre d'un conflit, en sabotant les SI supportant ces services.

En octobre 2017, le métro de Kiev en Ukraine ainsi que plusieurs entités notamment ukrainiennes et russes ont été victimes d'une attaque au moyen du code BadRabbit, conçu comme un rançongiciel afin de chiffrer et rendre inopérants les SI compromis [34]. D'après Reuters, le système de paiement du métro a été affecté, mais les trains ont pu circuler normalement [35]. Cette campagne d'attaques a été attribuée avec une confiance élevée au service russe de renseignement militaire (GRU) par le NCSC britannique [36].

Mi-décembre 2023, Gonjeshk Darand *alias* Predatory Sparrow, décrit comme un groupe hacktiviste pro-israélien opposé au régime iranien, a revendiqué une attaque informatique ciblant des stations-services iraniennes [27] [37]. D'après le média Security Affairs, l'attaque aurait notamment eu des conséquences importantes sur le fonctionnement des stations situées à Téhéran, qui auraient été forcées de passer à un mode manuel. D'après le ministre iranien du Pétrole, l'attaque aurait affecté 70% des stations du pays. Le groupe Predatory Sparrow a revendiqué cette attaque dans le contexte du conflit opposant Israël au Hamas palestinien.

Commentaire : si les exemples de sabotage ou de tentatives de sabotage informatique d'entités de transports urbains sont rares, ces entités demeurent des cibles d'intérêt pour des attaquants réputés étatiques, étant données les vastes répercussions potentielles que peuvent avoir les perturbations de ces secteurs.

4.2 Attaques revendiquées par des groupes hacktivistes

Des groupes hacktivistes cherchant à faire valoir leurs positions dans des contextes géopolitiques conflictuels sont notamment auteurs d'attaques informatiques à des fins de déstabilisation. Ces attaques visent notamment à nuire à l'image de leurs victimes et leurs effets sur les SI ciblés sont généralement plus rapidement remédiés, à l'image des attaques par déni de service

27. Ce groupe est associé à des attaques destructrices contre la corporation nationale des médias iranienne (Radio-Télévision de la République islamique d'Iran), le système ferroviaire national iranien en 2021, ainsi que la Société iranienne de raffinage et de distribution du pétrole en 2021, qui a entraîné la défiguration des équipements d'affichage des distributeurs d'essence [37]. Ce groupe pourrait être lié à l'État d'Israël d'après des sources médiatiques [38].

distribué (DDoS) ou des défigurations de ressources en ligne. Les grands événements porteurs de forte visibilité, comme les Jeux Olympiques et Paralympiques de Paris 2024, peuvent servir de caisse de résonance pour amplifier les effets de ces attaques.

4.2.1 Attaques à des fins de déstabilisation revendiquées par des groupes hacktivistes contre des entités de transport urbain

Depuis le début de l'invasion de l'Ukraine par la Russie en février 2022, un nombre important d'attaques hacktivistes a été recensé à l'encontre d'entités ukrainiennes ou de pays soutiens de l'Ukraine. Les ressources en ligne appartenant aux entités du secteur des transports urbains sont régulièrement victimes d'attaques de type DDoS ou défiguration revendiquées par des groupes hacktivistes. Ceci s'explique par le grand nombre d'usagers des services de transports en commun, qui donne une visibilité importante aux attaques contre les sites internet ciblés. Les attaques DDoS ou défiguration des groupes hacktivistes prorusses ciblant des entités européennes ou américaines interviennent généralement en réaction au soutien des gouvernements occidentaux à l'Ukraine.

En avril 2022, des panneaux de signalisation dans la ville de Krasnoïarsk en Russie ont été défigurés. D'après le média russe spécialisé SECURITYLAB.RU, des canaux Telegram ukrainiens auraient évoqué la compromission de systèmes routiers à la même période [39].

En septembre 2022, le collectif hacktiviste Anonymous et le groupe hacktiviste pro-ukrainien IT Army of Ukraine ont revendiqué la compromission de l'entreprise russe de mise en relation entre chauffeurs et particuliers YANDEX TAXI [40, 41] à Moscou. Les attaquants seraient parvenus à compromettre l'application YANDEX TAXI pour transmettre des ordres à tous les taxis disponibles de la flotte, afin de les diriger à l'adresse d'un bâtiment appelé « Hotel Ukraine ». L'attaque informatique a entraîné la concentration de plusieurs dizaines de taxis, causant un embouteillage qui aurait duré au moins trois heures [40].

4.2.2 Attaques DDoS contre des entités du secteur

Les entités du secteur des transports urbains sont très régulièrement la cible d'attaques et de tentatives d'attaques par DDoS. Une partie des attaques DDoS observées contre des entités européennes et nord-américaines s'inscrit dans le contexte de la tentative d'invasion de l'Ukraine par la Russie. Ces attaques, relativement simples à mettre en œuvre, sont majoritairement le fait de groupes hacktivistes pro-russes qui disposent de capacités offensives techniquement limitées. Les attaques DDoS ciblant des entités du secteur en Europe ou en Amérique du Nord interviennent généralement en réaction au soutien des pays occidentaux à l'Ukraine contre la Russie. Les effets réels des attaques DDoS sur l'activité et les opérations des entités du secteur des transports urbains sont toutefois limités et rapidement remédiés.

Différents groupes pro-russes ont ainsi revendiqué le ciblage d'entités françaises du secteur des transports urbains au cours des dernières années. Par exemple :

- au cours de l'année 2023, le groupe hacktiviste pro-ruse NoName057(16) a revendiqué plusieurs attaques contre différents sites internet, dont celui de la RATP [42] et de TRANSILIEN [43];
- le 14 juillet 2024, le groupe hacktiviste pro-russe « Narodnaya CyberArmiya » a revendiqué sur son canal Telegram une attaque DDoS contre le site Internet de l'entreprise française de taxis ARAMIS [44].

Ces attaques n'ont pas eu d'effets importants sur les entités ciblées.

Attaques DDoS contre des entités du secteur

Dans la majorité des cas connus de l'ANSSI, les attaques DDoS contre des entités françaises du secteur ont pu être contenues par les mesures de sécurité en place et ont provoqué, dans les cas les plus graves, des indisponibilités de très courte durée des sites visés.

Des recommandations liées à la mise en œuvre des mécanismes anti-DDoS sont présentes en fin de document.

4.3 Détournement d'équipements de signalisation

Le **détournement d'équipements de signalisation** par des acteurs malveillants est potentiellement porteur de conséquences importantes sur la sécurité des transports urbains. Dans certains cas, ce détournement ne nécessite pas de capacités avancées et exploite des équipements généralement mal sécurisés ou dont les exigences de sécurité sont obsolètes.

En 2020, les chercheurs en sécurité informatique néerlandais Rik van Dujin et Wesley Neelen ont démontré la possibilité de manipuler des feux de signalisation [45]. Le détournement consiste à tromper le système de signalisation connecté à Internet en simulant le passage de vélos à une intersection, afin qu'il donne un feu vert sur une voie et un feu rouge aux véhicules de la voie perpendiculaire. Les chercheurs ont injecté des données falsifiées dans des applications de localisation de cyclistes conçues pour donner un feu vert à l'approche des vélos dès que c'est possible. Ils sont parvenus à manipuler les temps d'attente entre les changements de feux de signalisation afin d'accélérer le passage au vert pour les cyclistes.

En 2022, des chercheurs en sécurité informatique sont parvenus à manipuler les systèmes de feux de signalisation à certaines intersections de la ville d'Hanovre en Allemagne, au moyen d'ordinateurs, d'une radio et d'une antenne [46]. Les chercheurs ont exploité une technologie obsolète conçue pour permettre à certains véhicules (voitures de police et de pompiers, ambulances, bus locaux) de circuler plus rapidement sans s'arrêter aux feux. Cette technologie équiperait au moins 80 villes en Allemagne. D'après les chercheurs, il serait techniquement impossible de causer des accidents en abusant de cette technologie ; toutefois, elle pourrait être exploitée par des acteurs malveillants afin de perturber le trafic routier, ce qui pourrait entraîner des conséquences importantes dans des contextes dangereux (évacuations, incendies...).

En 2024, le chercheur en sécurité informatique néerlandais Alwin Peppels a démontré la possibilité de détourner des feux de signalisation, en manipulant un signal radio défini de manière informatique afin d'envoyer des commandes aux boîtes de contrôle des feux [47]. Ce détournement exploite une fonctionnalité prévue pour faciliter le trafic des véhicules de police, de pompiers et des ambulances. Ce système est utilisé aux Pays-Bas et en Belgique depuis 2005. D'après le ministère néerlandais de la Gestion des Infrastructures et de l'Eau, le remplacement de ces équipements est requis pour pallier à ce problème. D'après le média spécialisé Cybernews.com, il s'agirait de remplacer des dizaines de milliers de feux de signalisation d'ici 2030.

Commentaire : les preuves de concept de détournement de feux de signalisation permettent de mesurer la vulnérabilité de ce type d'équipement à des attaques. Elles démontrent que le détournement ne nécessite pas de capacités sophistiquées. Toutefois, l'ANSSI n'a pas connaissance d'exploitation réelle de ces capacités à des fins de nuisance par des acteurs offensifs.

5 MENACE À FINALITÉ D'ESPIONNAGE

Les entités du secteur des transports urbains sont détentrices d'informations industrielles et personnelles de valeur, ce qui les rend susceptibles d'être la cible d'attaques à des fins d'espionnage. Ces attaques sont conduites au moyen de mode opératoires des attaquants (MOA) réputés liés à des États ou des entreprises privées. Elles peuvent viser différents objectifs : la préparation d'attaques ultérieures (potentiellement à des fins de sabotage), la collecte de renseignement d'intérêt industriel, ou encore l'espionnage d'individus.

Les incidents connus de l'ANSSI concernant le ciblage d'entités des transports urbains à des fins d'espionnage sont rares. Il n'en reste pas moins que les attaquants mettent en œuvre des capacités importantes pour échapper à la détection : il est donc fort probable que la proportion réelle des attaques à des fins d'espionnage contre le secteur des transports urbains soit plus importante que celle disponible à l'analyse.

Espionnage d'exploitants de transports urbains

En avril 2021, la METROPOLITAN TRANSPORTATION AUTHORITY américaine, plus grand réseau de transports en commun d'Amérique du Nord[28], aurait été victime d'une attaque informatique aux motivations non précisées. D'après différentes sources médiatiques [48, 49], les attaquants soupçonnés d'être liés au gouvernement chinois auraient exploité une vulnérabilité affectant le VPN PULSE CONNECT SECURE. L'attaque aurait affecté trois des 18 systèmes d'information de l'entité, sans conséquence sur ses opérations. Les vulnérabilités qui auraient été exploitées par les attaquants lors de la compromission du MTA n'ont pas été décrites par les sources disponibles.

À la même période, des vulnérabilités affectant PULSE CONNECT SECURE auraient été exploitées - sans qu'il soit possible d'affirmer qu'il s'agisse des mêmes vulnérabilités. Les vulnérabilités affectant PULSE CONNECT SECURE[29] ont été documentées dans le Bulletin d'alerte du CERT-FR en avril 2021, mis à jour en juin 2021 [50]. L'exploitation de la CVE-2021-22893 (score CVSS de 9.9) permet à un attaquant non authentifié d'exécuter du code arbitraire à distance.

Commentaire : l'origine supposée chinoise de cette attaque n'a pas été confirmée par d'autres sources. Toutefois, il est crédible que des attaquants réputés liés à des États aient exploité une vulnérabilité critique à l'encontre d'une entité importante du secteur des transports urbains à des fins d'espionnage.

Les sources disponibles ne détaillent pas les ressources auxquelles les attaquants auraient eu accès. Au vu des éléments à disposition, cette attaque n'aurait pas été conduite pour des motivations lucratives. De plus, le lien à un acteur étatique établi par les médias laisse penser que cette attaque a potentiellement eu lieu à des fins d'espionnage contre cette entité critique.

Les entités du secteur sont par ailleurs susceptibles d'être la cible d'attaques à des fins d'espionnage industriel. Les équipementiers et les exploitants sont détenteurs de connaissances fines dans des domaines industriels de pointe qui intègrent des technologies d'intérêt pour des États, comme par exemple l'automatisation des lignes de métro.

Les attaques informatiques destructrices sont par ailleurs rendues possibles par la collecte de renseignements, par des moyens cyber ou non, contre les entités ciblées. L'exfiltration de connais-

28. La MTA exploite les transports dans la ville de New-York, son agglomération, une partie de l'État de New-York et du Conneticut.
29. CVE-2021-22893, CVE-2021-22894, CVE-2021-22900.

sances sur la cartographie des réseaux industriels et bureautiques permet l'exploitation de capacités de sabotage par des attaquants.

Enfin, les informations personnelles détenues par les entreprises du secteur sont susceptibles d'être d'intérêt pour des services de renseignement afin de suivre les trajets régulièrement employés par des individus.

6 RECOMMANDATIONS

Les recommandations suivantes sont principalement destinées aux entreprises du secteur des transports urbains pour se prémunir au mieux des menaces exposées précédemment. L'ANSSI rappelle l'importance d'avoir une approche globale de la sécurité, notamment *via* l'analyse des risques qui pèsent sur l'entité et la cartographie des systèmes d'information pour identifier :

- les actifs devant être protégés ;
- l'état actuel du ou des systèmes d'information et la maturité des utilisateurs en matière de sécurité informatique ;
- les types de menaces affectant l'entité ;
- les risques affectant l'entité ;
- les mesures de sécurité appropriées et leur maintien dans le temps.

La mise en pratique de ces **recommandations** doit être réalisée dans une démarche d'amélioration continue : il est recommandé de se concentrer dans un premier temps sur l'état des lieux du SI, la sensibilisation des ressources humaines et les mécanismes de résilience, avant d'aborder la mise en œuvre des mesures de protection et de défense.

Les recommandations portent sur les thématiques suivantes :

- **la sécurité des ressources humaines** ;
- **la gestion des risques** ;
- **l'acquisition, le développement et la maintenance de produits ou systèmes** ;
- **l'architecture** ;
- **les accès physiques et systèmes exposés au public** ;
- **la gestion des identités et des accès** ;
- **la gestion des vulnérabilités** ;
- **la journalisation et détection de sécurité** ;
- **la résilience du système d'information.**

Ces recommandations sont accompagnées de liens vers des guides de l'ANSSI ; d'autres publications complémentaires de l'ANSSI peuvent également être consultées (notamment le *Guide ANSSI Attaques par rançongiciels, tous concernés* [51], et le *Guide d'hygiène informatique* [52]).

En complément, une attention particulière doit être portée aux annuaires *Active Directory*, éléments critiques des SI qui permettent la gestion centralisée des comptes, des ressources et des permissions. Pour les entités qui peuvent y prétendre, l'utilisation du service ADS[30] et l'application des recommandations fournies par le service permettent d'améliorer considérablement la sécurité des annuaires *Active Directory*.

Le CERT-FR offre également un service de veille sur les vulnérabilités, qui permet d'être alerté sur les vulnérabilités critiques et d'obtenir des recommandations et mesures de contournement associées[31].

Ces recommandations ne sont pas exhaustives et ne se substituent pas aux normes et réglementations de cybersécurité spécifiques aux secteurs (transport guidé, transport urbains au gabarit ferroviaire, flottes privées, engins de déplacement individuels, transport fluvial, transport aérien urbain, signalisation, informatique véhiculaire, etc.).

30. Voir le site du CERT-FR : https://www.cert.ssi.gouv.fr/scans/
31. https://www.cert.ssi.gouv.fr/alerte/

6.1 Sécurité des ressources humaines

R1

Sensibiliser les collaborateurs

L'organisation régulière de sessions de sensibilisation pour les utilisateurs et administrateurs du SI permet de transmettre les enjeux de cybersécurité et les bonnes pratiques à adopter.

Pour les utilisateurs et administrateurs du SI, communiquer les précautions suivantes :

- ne pas ouvrir les messages dont la provenance ou la forme est inconnue : il pourrait s'agir d'un contenu malveillant ;
- se méfier des extensions de pièces jointes douteuses qui peuvent contenir des codes malveillants ;
- adopter de bonnes pratiques de navigation sur Internet : vérifier l'authenticité d'un site Web, télécharger des logiciels uniquement depuis le site de leur éditeur) ;
- ne pas connecter sur son poste de travail un support USB d'origine inconnue.

Pour les administrateurs de SI, il est important d'axer la communication autour des thèmes suivants :

- les administrateurs sont des cibles privilégiées pour les attaquants de par la nature de leurs missions, leurs accès et les secrets d'authentification dont ils disposent ;
- les administrateurs doivent protéger les moyens techniques mis à leur disposition avec un niveau de vigilance et de sécurité supplémentaire par rapport aux utilisateurs.

6.2 Gestion des risques

R2

Réaliser une cartographie de son SI et de son environnement

Tous les éléments constitutifs du SI doivent être recensés dans un document de **cartographie** afin d'obtenir une meilleure lisibilité et un meilleur contrôle. La cartographie doit répondre à des enjeux variés :

- **écosystème** : identifier l'ensemble des parties avec lesquelles le SI interagit pour remplir sa fonction et notamment les **prestataires de services** ;
- **métier** : identifier les processus métiers et informations essentiels du SI. Une attention particulière doit être portée à l'**inventaire des données sensibles** (données personnelles ou liées au savoir-faire de l'entité) ;
- **physique** : identifier les composants physiques du SI (serveurs, automates, commutateurs, etc.) qui soutiennent les processus et informations essentiels ainsi que leur localisation géographique (permettant par exemple d'identifier où les données sensibles sont hébergées, ou si l'accès aux SI est exposé dans des espaces partagés avec le public) ;
- **logique** : identifier la segmentation logique du réseau et les liens logiques

entre ses segments. Cela inclut notamment la segmentation du réseau au niveau 2 du modèle OSI (par exemple le VLAN) et au niveau 3 (par exemple la découpe de l'adressage IP) ainsi que les équipements réseaux et de sécurité permettant l'interconnexion de ces segments (par exemple le routage, le filtrage, etc.) ;
- **applicatif** : identifier les composants logiciels du système qui soutiennent les processus et informations essentiels du SI. En particulier, les échanges d'informations entre ces composants doivent être répertoriés dans une matrice de flux.

À noter : **la constitution d'une cartographie est un processus itératif**. L'entité doit adapter la granularité de sa cartographie à l'outillage dont elle dispose. Ce document doit rester avant tout une aide à la prise de décision dans la maîtrise des risques ou en cas d'incident.

Pour aller plus loin : ANSSI, *Cartographie du système d'information* [53].

R3

Mener une analyse de risque

Une analyse de risque doit être réalisée et maintenue à jour régulièrement (par exemple annuellement) ou en cas d'évolution notable de la menace, en prenant en compte l'ensemble des dépendances et prestataires sur lesquels s'appuie l'entité.

Cette analyse doit notamment identifier les risques numériques que des entités externes pourraient faire peser sur l'organisation, ainsi que les conséquences sur le secret professionnel ou tout autre information protégée en lien avec les activités de l'entité. Il convient de s'interroger systématiquement sur le niveau de confiance à accorder aux services numériques utilisés pour protéger les informations. Cette évaluation du niveau de confiance doit s'appuyer par exemple sur l'**origine** du fournisseur du service, la **localisation** du service (en prenant en compte le contexte géopolitique) ou encore son **niveau de sécurisation**.

Pour aller plus loin : ANSSI, *La méthode EBIOS Risk Manager* [54].

6.3 Acquisition, développement et maintenance

R4

Inclure des exigences de sécurité dans les cahiers des charges

Dès la conception de projets internes et lors de l'établissement de contrats de sous-traitance ou d'achat de logiciels, des exigences de cybersécurité issues de référentiels normatifs et de l'analyse de risque doivent être incluses dans les cahiers des charges. Ces exigences doivent notamment :
- **assurer la protection des données hébergées par le sous-traitant** en définissant les exigences de sécurité adaptées à la criticité des données de l'entité et les exporter à son sous-traitant ;
- **assurer la sécurité des développements** en définissant des exigences de sécurité applicables au cycle de développement, incluant les exigences du

contrat dans les documents de spécification, les tests de sécurité à réaliser et la fourniture des document nécessaires à l'utilisation du système et à son maintien en condition opérationnelle et de sécurité ;
- **assurer le maintien en condition de sécurité** en s'assurant de sa capacité à maintenir à jour les composants de son système pour toute sa durée de fonctionnement : par exemple, le suivi d'obsolescence des produits, la veille sur les vulnérabilités, l'application des correctifs de sécurité, etc. Lorsque la maintenance est réalisée à partir de dispositifs appartenant aux sous-traitants, l'entité doit exporter des contraintes techniques sur ces dispositifs et plus particulièrement pour les accès distants ;
- **assurer la sécurité de la réversibilité** : l'entité doit définir des exigences de sécurité pour assurer la continuité de service lors du transfert des activités d'une prestation vers l'exploitant ou un autre sous-traitant. Par exemple, l'ensemble des données et des moyens techniques qui auraient été confiés par le donneur d'ordre au titulaire pour la réalisation de ses missions doivent être restitués. De la même manière, des formations s'appuyant sur les procédures d'exploitation de sécurité doivent être dispensées aux personnels du futur titulaire ou du donneur d'ordre.

Afin d'évaluer le niveau de conformité du soumissionnaire, un plan d'assurance sécurité (PAS) doit lui être demandé en réponse aux cahiers des charges. Les engagements du soumissionnaire dans ce document doivent être audités en cours de prestation en accord avec les conventions d'audit établies au titre du marché.

Type d'attaque : attaque contre la chaîne d'approvisionnement.

R5

Contractualiser la traçabilité des composants

Il est important de connaître les configurations déployées sur les systèmes industriels et embarqués afin de suivre les vulnérabilités et d'être capable de réinstaller les logiciels nécessaires aux opérations en cas d'incident entraînant la destruction des données et logiciels (rançongiciel, code de sabotage, etc.).

Concernant les composants complexes non maîtrisés en interne, il est recommandé de s'assurer par des moyens contractuels de la détention des données de références des *firmwares* présents sur les systèmes afin de pouvoir revenir à un état initial de fonctionnement de confiance. Cela implique de lister les logiciels, leurs configurations et les programmes du processus industriel, leur historique, leurs dépendances, leurs versions. Pour satisfaire ce besoin, il peut être proposé de contractualiser la fourniture de nomenclature logicielle (ou *Software Bill of Material*[a]) avec toute livraison de composant.

a. La *Software Bill of Material* ou SBOM est la liste des composants logiciels inclus dans un sous-système.

R6

Inclure des clauses de traitement d'incidents dans les contrats

La contractualisation de prestation de service et la mise à disposition de matériel doit prévoir des clauses de traitements d'incident. Ces clauses doivent au moins prévoir :

- les conditions et modes de déconnexion de tiers ;
- la capacité à effectuer des prélèvements forensiques sur les équipements raccordés au système d'information ;
- les modes de coopération en environnement dégradé[a] ;
- les contacts et intervenants en cas d'incident cyber.

Pour aller plus loin : ANSSI, *Maîtriser les risques de l'infogérance. Externalisation des systèmes d'information, Guide Version 1.0* [55].

6.4 Architecture

R7

Mettre en œuvre une passerelle d'interconnexion à Internet

Une passerelle d'interconnexion à Internet doit être mise en œuvre afin de protéger le SI interne des menaces qui pourraient provenir d'Internet. Cette passerelle doit :

- être incontournable pour les flux entrants et sortants du système d'information ;
- inclure des pares-feux après le routeur d'accès Internet et devant le SI interne pour constituer une ou plusieurs zones démilitarisées (DMZ) ;
- inclure en coupure des services applicatifs de relais dans la ou les DMZ avec notamment un serveur mandataire pour les accès web, un serveur relais de messagerien et un résolveur DNS pour les requêtes de noms de domaine public ;
- imposer la mise en œuvre d'un VPN (de préférence IPSec) pour les accès distants aux ressources internes du SI.

Type d'attaque : rançongiciel, exfiltration de données, usurpation de compte, attaque contre la chaîne d'approvisionnement

Pour aller plus loin : ANSSI, *Recommandations relatives à l'interconnexion d'un système d'information à Internet* [56].

a. Le terme environnement dégradé renvoie aussi bien à un contexte d'opération dans un environnement de continuité d'activité qu'à des scénarios moins drastiques pendant lesquels les systèmes de coopération comme gestion de ticket ou partages de fichiers sont compromis ou indisponibles.

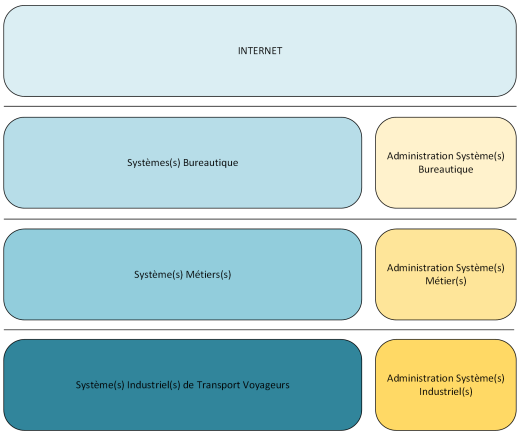
R8

Cloisonner et filtrer les différents systèmes d'information

L'ensemble des systèmes de l'entité doit être cloisonné de manière logique (par exemple par VLAN au niveau réseau, par VM au niveau des équipements, etc.) afin d'éviter la propagation et la latéralisation d'une attaque sur l'ensemble des processus métiers et des systèmes industriels d'une entité. Les interconnexions entre les différents SI doivent être contrôlées par des dispositifs de filtrage autorisant uniquement les flux nécessaires au bon fonctionnement des activités de l'entité.

Les systèmes à cloisonner sont par exemple :

- les SI bureautique ;
- les systèmes métiers (infrastructure de gare ou de station, etc.) ;
- les systèmes industriels de transport voyageurs (billettique, infrastructure de transport embarquant les voyageurs, etc.) ;
- les SI d'administration par type de système.



Type d'attaque : rançongiciel, exfiltration de données, attaque contre la chaîne d'approvisionnement

Pour aller plus loin sur le cloisonnement de l'administration : ANSSI, *Recommandations relatives à l'administration sécurisée des systèmes d'information* [57].

R9

Cloisonner et filtrer les différents sous-systèmes d'un système d'information

Chaque SI de l'entité doit être cloisonné de manière logique en plusieurs zones de sécurité homogènes (par sensibilité, criticité et/ou exposition) afin de limiter la propagation et la latéralisation d'un attaquant en sein d'un SI (par exemple depuis les postes de travail utilisateurs vers les serveurs internes du SI bureautique). Les interconnexions entre ces différentes zones doivent être contrôlées par des dispositifs de filtrage autorisant uniquement les flux nécessaires au bon fonctionnement du SI.

Type d'attaque : rançongiciel, exfiltration de données, attaque contre la chaîne d'approvisionnement

Pour aller plus loin sur le cloisonnement de l'administration : ANSSI, *Recommandations relatives à l'administration sécurisée des systèmes d'information* [57].

R10

Protéger les données par mécanisme cryptographique

Les données du SI transitant sur un réseau tiers ou ayant un fort besoin en confidentialité doivent être protégées systématiquement par l'utilisation de mécanismes cryptographiques à l'état de l'art. Cela concerne plus particulièrement :

- toute donnée transitant sur un réseau tiers ;
- les données d'administration transitant sur tout réseau interne ou tiers ;
- les données sensibles (données personnelles des usagers, etc.) transitant sur tout réseau interne ou tiers ;
- les données sensibles (données personnelles des usagers, etc.) au repos en cas d'hébergement chez un prestataire ou fournisseur de services nuagiques ;
- les données sensibles stockées sur des supports amovibles (clé USB, disque dur portable).

Type d'attaque : exfiltration de données

Pour aller plus loin sur la protection des données dans une base de données : ANSSI, *Base de données relationnelles, Les Essentiels* [58].

R11

Mettre en œuvre des mécanismes anti-DDoS

Les risques d'attaques DDoS sur tout service exposé sur Internet doivent être pris en compte. Pour les **services exposés sur Internet**, une solution de protection anti-DDoS gérée en propre par l'entité ou via un service souscrit auprès d'un fournisseur d'accès à Internet (FAI) doit être mise en œuvre. **En particulier, l'entité ne devrait pas exposer de services ou faire transiter des données sur Internet dont l'indisponibilité pourrait affecter le bon fonctionnement de ses infrastructures assurant le transport des voyageurs.**

Un point d'attention particulier devrait être apporté à la protection des infrastructures non applicatives pour lesquelles les protections applicatives habituelles sont peu efficaces. Un exemple courant de ce type de complexité est la prévention des dénis de service sur les concentrateurs VPN.

Type d'attaque : DDoS

Pour aller plus loin : ANSSI, *Les essentiels - Dénis de service distribués (DDoS)* [59].

R12

Limiter la dépendance aux technologies GNSS

Les **technologies GNSS** (« Géolocalisation et navigation par un système de satellites » ou « *Global navigation satellite system* ») sont exposées à des risques d'attaques par brouillage et à des attaques pouvant altérer la synchronisation, la datation et la géolocalisation d'un utilisateur. Ces technologies ne disposant pas nativement

de mécanismes de sécurité contre ces menaces, il est recommandé de limiter leur utilisation à des services non critiques à l'entité. Le cas échéant, des capteurs supplémentaires devraient être utilisés lors de l'estimation de la position, de la vitesse et du temps *via* l'emploi d'algorithmes d'hybridation. La position précise de l'utilisateur peut être définie ou recaler à partir d'équipement de mesures de l'odométrie par exemple.

Type d'attaque : brouillage, leurrage, DDoS

6.5 Accès physiques et systèmes exposés au public

R13

Contrôler les accès physiques aux sites et locaux de l'entité

L'entité doit définir et mettre en œuvre une politique de contrôle d'accès physique et de vidéoprotection pour l'accès à ses locaux qui soit adaptée aux missions de ses différents systèmes. En particulier, de nombreux systèmes industriels sont obsolètes ou ne disposent pas nativement de fonctions de sécurité logiques communément disponibles dans les technologies IT. La protection physique est donc une thématique majeure de la défense en profondeur des systèmes industriels.
Les principales mesures à prendre en compte sont, pour les sites maîtrisés par l'entité (bâtiment, gare, station, etc.) et les véhicules transportant des voyageurs :

- assurer la génération et la remontée des événements d'accès physiques aux locaux techniques et armoires/coffrets directement accessibles au public ;
- définir et mettre en œuvre des alertes métiers nécessitant une prise de décision rapide et/ou une levée de doute sur des événements inattendus (par exemple, en cas d'ouverture d'un coffret à bord d'un véhicule durant les heures d'exploitation) ;
- s'appuyer sur les systèmes de vidéoprotection utilisés pour la sûreté des voyageurs afin de superviser l'accès aux locaux techniques et armoires/coffrets directement accessibles au public.

Pour les sites maîtrisés par l'entité (bâtiment, gare, station, etc.) :

- généraliser l'utilisation d'un système de contrôle d'accès physique centralisé par badge pour identifier et authentifier les accès aux locaux techniques ou armoires directement accessibles au public.

Pour les sites publics non maîtrisés par l'entité ou difficilement maîtrisables par l'entité (voirie, etc.) :

- assurer la génération et la remontée d'alertes d'accès physiques aux coffrets directement accessibles au public ;
- privilégier une approche par logique cablée pour limiter la capacité d'un attaquant à remonter vers le système de l'entité au travers de ces points d'accès fortement exposés.

Type d'attaque : accès physique au système

Pour aller plus loin : ANSSI, *Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection* [60].

6.6 Gestion des identités et des accès

R14

Enregistrer les variations du nom de domaine de l'entité

Afin de protéger les comptes personnels des usagers, l'entité doit s'assurer de limiter les risques d'usurpation d'URL et donc de son identité pour les services mis à disposition des usagers sur Internet. L'entité doit notamment enregistrer les multiples variations de son nom de domaine selon toutes les erreurs de frappe ou d'orthographe qu'un utilisateur est susceptible de faire ou de ne pas identifier et enregistrer ces noms de domaine sous de multiples extensions (« .fr », « .com », « .net », etc.). Une attention particulière doit aussi être portée sur le choix du bureau d'enregistrement et des mécanismes offerts par celui-ci.

Type d'attaque : usurpation d'URL

Pour aller plus loin : ANSSI, *Bonnes pratiques pour l'acquisition et l'exploitation de noms de domaine* [61].

R15

Identification unique des utilisateurs sur des périmètres bureautiques

Tous les accès des utilisateurs aux ressources du SI de l'entité doivent être identifiés de manière unique. Les comptes uniques doivent être centralisés afin d'en faciliter la gestion. La gestion d'identités (notamment avec Microsoft Active Directory) créant également un point de vulnérabilité unique, elle doit donc être configurée avec soin et faire l'objet d'audits réguliers.

Type d'attaque : exfiltration de données

Pour aller plus loin : ANSSI, *Recommandations relatives à l'administration sécurisée des systèmes d'information reposant sur Microsoft Active Directory* [62].

R16

Mettre en place une politique de mots de passe robuste

Les mots de passe permettant de prouver l'identité d'un utilisateur avant tout accès à une ressource du SI doivent être protégés notamment par :

- l'utilisation d'un mot de passe fort mémorisé par les utilisateurs, sans qu'il soit nécessaire de forcer un renouvellement à intervalles courts ;
- la limitation du nombre de tentatives d'authentification sur une période de temps donnée, afin de réduire les probabilités d'authentification frauduleuses en ligne par force brute ;
- le stockage des authentifiants *via* l'utilisation d'un sel choisi aléatoirement et des fonctions de dérivation de mot de passe (par exemple PBKDF2, etc.), afin de réduire la probabilité de retrouver un mot de passe hors ligne à partir de son empreinte (par exemple par attaque par *rainbow table*) ;
- l'utilisation d'un coffre-fort de mots de passe permettant l'utilisation de se-

crets d'authentification distincts pour accéder à différents services en limitant le nombre d'authentifiants à retenir par les utilisateurs.

Type d'attaque : exfiltration de données

Pour aller plus loin : ANSSI, *Authentification multifacteurs et mots de passe* [63].

R17

Mettre en place une authentification forte pour les comptes sensibles et les accès distants

Les accès à privilèges ou à des ressources sensibles du SI ainsi que les accès distants au SI doivent s'appuyer sur une authentification forte, non vulnérable aux attaques par hameçonnage.

Par exemple, les mécanismes suivants peuvent être envisagés :

- l'authentification des utilisateurs par certificats ou clés secrètes ;
- en cas d'authentification utilisateur par mot de passe, imposer un deuxième facteur pour l'authentification utilisateur ou l'associer obligatoirement à une authentification forte de l'équipement client ;
- pour établir une connexion par VPN, mettre en place une authentification mutuelle forte par certificat entre le client et le service (par exemple mTLS ou IPSec).

Les applications incompatibles avec une authentification forte peuvent être placées derrière un serveur mandataire inverse (*reverse proxy*) remplissant ces tâches d'authentification à leur place.

Type d'attaque : exfiltration de données, usurpation de compte

Pour aller plus loin : ANSSI, *Authentification multifacteurs et mots de passe* [63].

6.7 Gestion des vulnérabilités

R18

Durcir la configuration des équipements

Un durcissement de la configuration des équipements du SI doit être réalisé afin d'en limiter la surface d'attaque.

Au niveau matériel, il convient de rendre l'authentification obligatoire pour modifier le paramétrage du BIOS et le chiffrement des disques pour les équipements mobiles et, lorsque cela est possible, sur les équipements fixes.

Au niveau logiciel (OS et applications), il convient de supprimer ou désactiver les services inutiles afin d'en limiter la surface d'attaque et d'en faciliter le maintien en condition de sécurité, de supprimer les comptes et authentifiants par défaut, et d'activer les fonctions de filtrage local à l'équipement.

Type d'attaque : exfiltration de données, rançongiciel

R19

Maintenir à jour le système d'information

Une politique de maintien en condition opérationnelle (MCO) et de maintien en condition de sécurité (MCS) doit être définie et mise en œuvre afin de renforcer la sécurité et la stabilité de tous les SI de l'entité. Les logiciels doivent être dans des versions maintenues par les éditeurs et les correctifs de sécurité appliqués en priorité sur les équipements et services directement exposés sur Internet (par exemple, le pare-feu périmétrique, les postes utilisateurs avec accès à Internet, etc.), en tant qu'équipements particulièrement exposés aux attaques informatiques.

Des exigences de MCO et le MCS doivent être systématiquement intégrées dans les cahiers des charges pour chaque nouveau projet.

Type d'attaque : exfiltration de données, rançongiciel

6.8 Journalisation et détection de sécurité

R20

Utiliser une solution de protection contre les logiciels malveillants

Une solution de protection contre les logiciels malveillants doit être mise en œuvre en priorité sur les ressources exposées à Internet (par exemple les postes de travail) et sur tout contenu externe au système d'information. Les courriels entrants et leurs pièces jointes devront être vérifiés *via* un serveur relais de messagerie en DMZ ou par l'utilisation d'une station de décontamination pour les médias amovibles.

Ces outils ne garantissent pas une protection contre l'ensemble des logiciels malveillants mais ils peuvent participer à empêcher des compromissions courantes.

Type d'attaque : toutes

R21

Centraliser les journaux d'événements et les alertes des capteurs de sécurité

Les journaux d'événements des composants, des systèmes d'exploitation, des applications, etc., ainsi que les alertes de sécurité générées par des capteurs de sécurité (par exemple par la solution de protection contre les logiciels malveillants) doivent être activés et centralisés. Cela permet d'investiguer les incidents de sécurité *post-mortem*, voire de détecter un incident de sécurité avant que l'attaquant ne parvienne à réaliser son objectif. La centralisation des événements de sécurité contribue d'une part à sécuriser la collecte des événements et d'autre part à faciliter les opérations de détection et d'analyse en cas d'incident.

Il est recommandé :

- d'identifier les scénarios de menaces à détecter incluant notamment les menaces présentées dans ce document ;
- d'activer et centraliser les événements utiles aux objectifs de détection les plus critiques, dans la limite des capacités de l'entité à traiter les événements

sous 24 heures ;
- d'améliorer de manière itérative la capacité de traitement des événements par l'entité afin de couvrir l'ensemble des scénarios de menaces à détecter.

Type d'attaque : toutes

Pour aller plus loin : ANSSI, *Recommandations de sécurité pour l'architecture d'un système de journalisation*, *Recommandations de sécurité pour la journalisation des systèmes Microsoft Windows en environnement Active Directory* [64].

R22

Utiliser la télémétrie pour détecter les événements de sécurité

Les systèmes industriels répartis génèrent une télémétrie importante pendant leur fonctionnement. Les attaques informatiques sur ces systèmes peuvent entraîner des mesures anormales ou manquantes. La télémétrie de ces systèmes est généralement supervisée uniquement du point de vue de l'opération et de la maintenance du système. Il est recommandé de prévoir une supervision de sécurité informatique sur ces remontées d'information.

En particulier, il est recommandé d'identifier les motifs générés par les scénarios identifiés dans les analyses de risques spécifiques au système et de détecter les indicateurs de leur survenue dans les flux de télémétrie. En cas d'alerte, ces informations peuvent ensuite être qualifiées en lien avec la supervision habituelle du processus industriel (capteurs et journaux) ou par des relevés forensiques.

6.9 Résilience du système

R23

Prévoir le fonctionnement en mode dégradé des systèmes d'information industriels

L'opération en mode dégradé des systèmes associés à des transports urbains doit être prévue. Les modes d'opération manuels devraient faire l'objet de tests réguliers pour s'assurer du maintien à jour des procédures, des documents nécessaires et des compétences des opérateurs.

La norme IEC 62443-3-3 prévoit une dégradation vers un mode d'opération « insulaire » (*island mode*), soit une dégradation volontaire des communications pour isoler les systèmes les plus sensibles face à un risque d"attaque informatique. Il est recommandé d'en considérer la mise en œuvre afin de limiter les conséquences d'incidents comportant des risques de latéralisation par les attaquants.

R24

Définir un PCA et un PRA

L'entité doit mettre en œuvre les moyens techniques et humains lui permettant de maintenir ses activités ou ses services dans un mode dégradé et de faciliter le retour à la normale suite à un incident de sécurité. Ces éléments doivent être formalisés au travers d'un **Plan de Continuité d'Activité** (**PCA**) et d'un **Plan de**

Reprise d'Activité (PRA). Le PCA doit assurer la continuité des activités face à un événement d'origine cyber, mais également la protection cyber des moyens de continuité.

Le PCA et le PRA doivent couvrir les risques accidentels mais aussi les différents types d'attaques malveillantes, notamment :

- les attaques par **rançongiciel** ou par **code de sabotage** (type *wiper*) qui visent à affecter la disponibilité des systèmes ou les données de l'entité ;
- les **exfiltrations de données** qui peuvent nuire à la disponibilité, la confidentialité et l'intégrité des données de l'entité ;
- les attaques affectant notamment les prestataires de services avec lesquels le ou les SI de l'entité ont une forte dépendance (par exemple la prise de contrôle des dispositifs de télémaintenance du prestataire, etc.) ;
- les attaques par **DDoS** qui peuvent affecter la disponibilité des ressources exposées sur Internet (sites web, etc.).

Outre les aspects spécifiquement industriels, la durée de continuité d'activité en mode dégradé doit être évaluée. Beaucoup d'activités industrielles dépendant d'échange d'information dans le domaine bureautique, les liens entre ces activités et les conséquences de leur coupure doivent être spécifiquement pris en compte. La perte de productivité due à un passage en traitement manuel de processus habituellement automatisés peut être anticipée.

Par ailleurs, faute de prise en compte, beaucoup de plans de continuité présentent des vulnérabilités aux attaquants encore présents dans les SI après un incident initial. Il est recommandé de planifier la continuité et la reprise d'activité avec l'hypothèse qu'un acteur malveillant pourrait être présent sur les SI au moment du déclenchement du PCA.

Enfin, un plan de communication devrait être prévu et testé afin de permettre une communication efficace en cas de crise, celui-ci devrait notamment :

- identifier la liste des parties prenantes à alerter, par exemple : les autorités, partenaires, clients, prestataires, etc. ;
- identifier les informations attendues, ainsi que la forme, les moyens et les relais pour alerter les parties prenantes ;
- sur la base de l'appréciation des risques et des scénarios identifiés, des canevas de communication à adapter peuvent être établis pour faciliter la gestion de crise le jour venu ;
- identifier les éléments devant être disponibles hors ligne.

Type d'attaque : toutes

R25

Assurer la sauvegarde des données

Une politique de sauvegarde régulièrement mise à jour doit être définie, appliquée et testée afin de pallier la corruption ou l'indisponibilité de données dues à un incident ou une compromission (par exemple lié à un rançongiciel). Pour les éléments les plus critiques, une sauvegarde hors ligne doit être prévue afin de garantir une restauration en cas d'attaque par un rançongiciel. En fonction du niveau de sensibilité des données, les sauvegardes doivent être chiffrées afin d'en garantir la confidentialité.

En particulier :

- définir une liste des données et services vitaux pour l'organisme et les serveurs concernés ;
- définir la fréquence des sauvegardes ;
- réaliser des sauvegardes des données critiques et prévoir au minimum une sauvegarde hors ligne à intervalles réguliers afin de se prémunir d'attaques de type rançongiciel ;
- rédiger et tester régulièrement les procédures de restauration ;
- rédiger et tester les procédures d'administration et d'exécution des sauvegardes ;
- définir des restrictions d'accès aux sauvegardes.

Type d'attaque : rançongiciel

Pour aller plus loin : ANSSI, *Sauvegarde des systèmes d'information* [65].

R26

Mettre en œuvre un plan de réponse aux cyberattaques

L'entité doit être préparée à la gestion d'une crise cyber pour assurer une réaction rapide et adaptée en cas d'attaque réelle. Il est recommandé :

- de prévoir une organisation et des procédures de gestion de crise ;
- de consolider un cahier de gestion de crise avec les coordonnées de l'ensemble des acteurs utiles sur un format non numérique ;
- d'identifier et de préparer les équipes aux premières actions d'urgence et conservatoires pour restreindre les activités malveillantes ;
- de réaliser des exercices de gestion de crise.

Les exercices sont particulièrement importants et ne doivent pas être négligés. Ils permettent de démontrer l'efficacité du dispositif de gestion de crise mis en œuvre et l'appropriation par les équipes des procédures et des réflexes à avoir en cas d'incident avéré.

Type d'attaque : toutes

Pour aller plus loin : ANSSI, *Crise d'origine cyber, les clés d'une gestion opérationnelle et stratégique* [66], *Organiser un exercice de gestion de crise cyber* [67].

A Références

[1] STRMTG. *Transports guidés urbains : tramways et métros*.
URL : https://www.strmtg.developpement-durable.gouv.fr/transports-guides-urbains-tramways-et-metros-r28.html?lang=fr.

[2] COMMISSION EUROPÉENNE. *Boîte à outils pour la cybersécurité dans le domaine des transports*. 1er janvier 2021.
URL : https://transport.ec.europa.eu/system/files/2021-10/cybersecurity-toolkit_fr.pdf.

[3] GLOBAL RAILWAY REVIEW. *Cyber-Security : A Necessary Component of Railway Businesses in the Digital Age*. 21 février 2018.
URL : https://www.globalrailwayreview.com/article/66228/cybersecurity-railway-digital-age/.

[4] GROUPE RATP. *Métro automatique : découvrez notre expertise*. 1er novembre 2023.
URL : https://ratpgroup.com/fr/realisations/metro-automatique/.

[5] CISA. *Global Positioning System (GPS) Interference*. 1er décembre 2022.
URL : https://www.cisa.gov/sites/default/files/publications/CISA-Insights_GPS-Interference_508.pdf.

[6] TRANSBUS. *Sous-traitance dans les réseaux de transport urbain*. 17 novembre 2024.
URL : https://www.transbus.org/dossiers/affretement.html.

[7] LE MAG IT. *Olsztyn, Pologne : quand une cyberattaque fait dérailler la Smart City*. 28 juin 2023.
URL : https://www.lemagit.fr/actualites/366543032/Olsztyn-Pologne-premiere-Smart-City-touchee-par-une-cyberattaque.

[8] RMF. *Olsztyn nadal walczy ze skutkami ataku hakerskiego*. 28 juin 2023.
URL : https://www.rmf24.pl/regiony/olsztyn/news-olsztyn-nadal-walczy-ze-skutkami-ataku-hakerskiego,nId,6869004#crp_state=1.

[9] ANSSI. *Panorama de la cybermenace 2023*. 27 février 2024.
URL : https://www.cert.ssi.gouv.fr/uploads/CERTFR-2024-CTI-001.pdf.

[10] TORONTO TRANSIT COMMISSION. *Cybersecurity Incident*. 10 novembre 2021.
URL : https://www.ttc.ca/riding-the-ttc/Updates/Cybersecurity-incident.

[11] THE RECORD. *Ransomware Attack Disrupts Toronto's Public Transportation System*. 1er novembre 2021.
URL : https://therecord.media/ransomware-attack-disrupts-torontos-public-transportation-system.

[12] ZDNET. *Toronto Subways Hit by Ransomware as US Lawmakers Slam 'burdensome' Cybersecurity Rules*. 2 novembre 2021.
URL : https://www.zdnet.com/article/toronto-subways-hit-by-ransomware-as-us-lawmakers-slam-burdensome-cybersecurity-rules/.

[13] LEMAGIT. *Ransomware LockBit : Transdev évoque un client attaqué outre-Atlantique*.
URL : https://www.lemagit.fr/actualites/252507869/Ransomware-face-a-LockBit-Transdev-reste-silencieux.

[14] VIVA SEVILLA. *Un ciberataque inutiliza la App de Tussam y los paneles informativos de las marquesinas*. 8 novembre 2022.
URL : https://vivasevilla.es/sevilla/1113109/un-ciberataque-inutiliza-la-app-de-tussam-y-los-paneles-informativos-de-las-marquesinas/?utm_source=dlvr.it&utm_medium=twitter#!.

[15] CISA. *#StopRansomware : Play Ransomware*. 18 décembre 2023.
URL : https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-352a.

[16] TREND MICRO. *Ransomware Spotlight : Play*. 21 juillet 2023.
URL : https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-play.

[17] THE RECORD. *Central Virginia Transit System Affected by Cyber Incident*. 12 août 2023.
URL : https://therecord.media/central-va-transit-system-cyberattack.

[18] US DEPARTMENT OF JUSTICE. *Sealed Indictment*. 15 mai 2022.
URL : https://www.justice.gov/usao-sdny/press-release/file/1558891/dl?inline=.

[19] BITDEFENDER. *Ransomware Paralyzes Taxi System in South Korea*. 19 juillet 2022.
URL : https://www.bitdefender.com/en-us/blog/hotforsecurity/ransomware-paralyzes-taxi-system-in-south-korea.

[20] MICROSOFT THREAT INTELLIGENCE. *DEV-0537 Criminal Actor Targeting Organizations for Data Exfiltration and Destruction*. 22 mars 2022.
URL : https://www.microsoft.com/en-us/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction/.

[21] BLACKBERRY. *Threat Alert : LAPSUS$ – Real Threat or Minor Menace ?* 24 mars 2022.
URL : https://blogs.blackberry.com/en/2022/03/threat-alert-lapsuss-real-threat-or-minor-menace.

[22] UBER. *Security Update*. 16 septembre 2022.
URL : https://www.uber.com/en-GB/newsroom/security-update/.

[23] LE MONDE. « Uber attribue son piratage au groupe Lapsus$ ». 20 septembre 2022.
URL : https://www.lemonde.fr/pixels/article/2022/09/20/uber-attribue-son-piratage-au-groupe-lapsus_6142402_4408996.html.

[24] UNION EUROPÉENNE. *Le règlement général sur la protection des données – RGPD, Règlement (UE) 2016/679*. 24 mai 2016.
URL : https://www.cnil.fr/fr/reglement-europeen-protection-donnees.

[25] LE PARISIEN. *Passe Navigo : Ile-de-France Mobilités porte plainte après une tentative de piratage*. 6 octobre 2023.
URL : https://www.leparisien.fr/info-paris-ile-de-france-oise/transports/passe-navigo-idfm-porte-plainte-apres-une-tentative-de-piratage-06-10-2023-YFIHTI2DG5GFFMFXIAQKFRUXGQ.php.

[26] L'USINE DIGITALE. *4000 adresses emails et mots de passe d'Ile-de-France Mobilités Connect volés par des hackers*. 9 octobre 2023.
URL : https://www.usine-digitale.fr/article/4000-adresses-emails-et-mots-de-passe-d-ile-de-france-mobilites-connect-voles-par-des-hackers.N2180027.

[27] TRANSPORT FOR LONDON | EVERY JOURNEY MATTERS. *Cyber Security Incident*. 26 novembre 2024.
URL : https://www.tfl.gov.uk/campaign/cyber-security-incident.

[28] THE MOLOCH. *"Irleaks" Threat Actor Claims Massive Dataleaks Against Major Iranian Companies, Draws Speculation*. 3 janvier 2024.
URL : https://themoloch.com/analysis/irleaks-threat-actor-claims-massive-dataleaks-against-major-iranian-companies-draws-speculation/.

[29] DYAMI. *Intel Brief : Irleaks' Massive Cyber Campaign In Iran Highlights Fragility Of Data Economy*. 12 janvier 2024.
URL : https://www.dyami.services/post/intel-brief-irleaks-massive-cyber-campaign-in-iran-highlights-fragility-of-data-economy.

[30] THE REGISTER. *Taxi Software Vendor Exposes Personal Details of Nearly 300K*. 11 avril 2024.
URL : https://www.theregister.com/2024/04/11/icabbi_database_exposure/.

[31] THE TIMES OF INDIA. *Researcher Claims Rapido Exposed Customers' Data : Here's What the Company Has to Say - Times of India*. 20 décembre 2024.
URL : https://timesofindia.indiatimes.com/technology/tech-news/researcher-claims-rapido-exposed-customers-data-heres-what-the-company-has-to-say/articleshow/116492017.cms.

[32] OUEST-FRANCE. *Remboursement du pass Navigo : attention à cette arnaque qui circule par mail*. 15 mars 2023.
URL : https://www.ouest-france.fr/faits-divers/arnaques/remboursement-du-pass-navigo-attention-a-cette-arnaque-qui-circule-par-mail-a428012c-c317-11ed-bfea-b6d5f064726b.

[33] OUEST-FRANCE. *JO 2024. Attention, de plus en plus d'arnaques ciblent les abonnés Navigo selon IDFM*. 25 juillet 2024.
URL : https://www.ouest-france.fr/economie/transports/jo-2024-attention-de-plus-en-plus-darnaques-ciblent-les-abonnes-navigo-selon-idfm-ba0711d2-4a6a-11ef-bfeb-1153a1dd3579.

[34] ESET. *Bad Rabbit : Not-Petya Is Back with Improved Ransomware*. 24 octobre 2017.
URL : https://www.welivesecurity.com/2017/10/24/bad-rabbit-not-petya-back/.

[35] REUTERS. « New Wave of Cyber Attacks Hits Russia, Other Nations ». 24 octobre 2017.
URL : https://www.reuters.com/article/world/new-wave-of-cyber-attacks-hits-russia-other-nations-idUSKBN1CT21A/.

[36] NCSC-UK. *Reckless Campaign of Cyber Attacks by Russian Military Intelligence Service Exposed*. 4 octobre 2018.
URL : https://web.archive.org/web/20181004185816/https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed.

[37] SECURITY AFFAIRS. *Pro-Israel Predatory Sparrow hacker group disrupted services at around 70% of Iran's fuel stations*. 18 décembre 2023.
URL : https://securityaffairs.com/156065/hacktivism/pro-israel-predatory-sparrow-iran-fuel-stations.html.

[38] TIMES OF ISRAEL. *Israel-linked hackers claim to paralyze gas stations across Iran*. 18 décembre 2023.
URL : https://www.timesofisrael.com/liveblog_entry/israel-linked-hackers-claim-to-paralyze-gas-stations-across-iran/.

[39] SECURITYLAB.RU. *À Krasnoïarsk, Des Inconnus Ont Piraté Un Panneau d'information à l'entrée de La Ville*. 16 avril 2022.
URL : https://www.securitylab.ru/news/531170.php.

[40] HACKREAD. *Anonymous Hacked Russian Yandex Taxi App Causing a Massive Traffic Jam*. 2 septembre 2022.
URL : https://hackread.com/anonymous-russian-yandex-taxi-app-hacked/.

[41] SECURITY AFFAIRS. *Anonymous Hacked Yandex Taxi Causing a Traffic Jam in Moscow*. 4 septembre 2022.
URL : https://securityaffairs.com/135280/hacktivism/anonyomus-hacked-yandex-taxi.html.

[42] LE PARISIEN. *Pourquoi un groupe de hackers russophones parasite les sites internes de la RATP*. 29 juin 2023.
URL : https://www.leparisien.fr/high-tech/pourquoi-un-groupe-de-hackers-russophones-parasite-les-sites-internes-de-la-ratp-29-06-2023-JIADU44NARH3VKDYTD6MT6NOXQ.php.

[43] @NONAME05716ENG . *Telegram - Transilien Traffic Route Search Site Down*. 8 juillet 2023.
URL : https://t[.]me/s/noname05716eng?q=transilien.

[44] FALCONFEEDS.IO (SUR X). *Russian Cyber Army, in collaboration with HackNet claims to have targeted the website of Arams Paris*. 14 juillet 2024.
URL : https://x.com/FalconFeedsio/status/1812600327025434982.

[45] ZOLDER. *Hacking traffic lights*. 8 juin 2020.
URL : https://media.defcon.org/DEF%20CON%2028/DEF%20CON%20Safe%20Mode%20presentations/DEF%20CON%20Safe%20Mode%20-%20Wesley%20Neelen%20%26%20Rik%20van%20Duijn%20-%20Hacking%20Traffic%20Lights.pdf.

[46] STARCARSIFU. *Hackers turn red traffic lights green using flaw in German system*. 15 décembre 2022.
URL : https://www.carsifu.my/news/hackers-turn-red-traffic-lights-green-using-flaw-in-german-system.

[47] CYBERNEWS. *Dutch government will replace hackable traffic lights to avoid movie-like carnage*. 11 octobre 2024.
URL : https://cybernews.com/news/dutch-government-will-replace-hackable-traffic-lights/.

[48] ABC NEWS. *Hackers Breached Several of MTA's Computer Systems in April*. 2 juin 2021.
URL : https://abc7ny.com/mta-hack-computer-nyc-new-york-city/10734358/.

[49] THE NEW YORK TIMES. « The M.T.A. Is Breached by Hackers as Cyberattacks Surge ». 2 juin 2021.
URL : https://www.nytimes.com/2021/06/02/nyregion/mta-cyber-attack.html.

[50] CERT-FR. *[MàJ] Vulnérabilité dans Pulse Connect Secure - CERT-FR*. 21 juin 2021.
URL : https://www.cert.ssi.gouv.fr/alerte/CERTFR-2021-ALE-007/.

[51] ANSSI. *Attaques par rançongiciels, tous concernés, Guide ANSSI-GP-077 v1.0*. 4 septembre 2020.
URL : https://cyber.gouv.fr/guide-rancongiciels.

[52] ANSSI. *Guide d'hygiène informatique*. 23 janvier 2017.
URL : https://cyber.gouv.fr/publications/guide-dhygiene-informatique.

[53] ANSSI. *Cartographie du système d'information, Guide ANSSI-PA-046 v1.0*. 21 novembre 2018.
URL : https://cyber.gouv.fr/publications/cartographie-du-systeme-dinformation.

[54] ANSSI. *La méthode EBIOS Risk Manager - Le Guide, ANSSI-PA-048 v1.5*. 27 mars 2024.
URL : https://cyber.gouv.fr/ebios-rm.

[55] ANSSI. *Maîtriser les risques de l'infogérance. Externalisation des systèmes d'information, Guide Version 1.0*. 3 décembre 2010.
URL : https://cyber.gouv.fr/guide-externalisation.

[56] ANSSI. *Recommandations relatives à l'interconnexion d'un système d'information à Internet, Guide ANSSI-PA-066 v3.0*. 19 juin 2020.
URL : https://cyber.gouv.fr/guide-interconnexion-si-internet.

[57] ANSSI. *Recommandations relatives à l'administration sécurisée des systèmes d'information, Guide ANSSI-PA-022 v3.0*. 11 mai 2021.
URL : https://cyber.gouv.fr/guide-admin-si.

[58] ANSSI. *Base de données relationnelles, Les Essentiels, v1.0*. 31 janvier 2025.
URL : https://cyber.gouv.fr/publications/bases-de-donnees-relationnelles.

[59] ANSSI. *Les essentiels - Dénis de service distribués (DDoS), Guide Version 2.0*. 5 septembre 2023.
URL : https://cyber.gouv.fr/publications/denis-de-service-distribues-ddos.

[60] ANSSI. *Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection, Guide ANSSI-PA-72*. 14 novembre 2023.
URL : https://cyber.gouv.fr/publications/securisation-des-systemes-de-controle-dacces-physique-et-videoprotection.

[61] ANSSI. *Bonnes pratiques pour l'acquisition et l'exploitation de noms de domaine, Guide ANSSI-BP-038 v1.3*. 10 novembre 2017.
URL : https://cyber.gouv.fr/publications/bonnes-pratiques-pour-lacquisition-et-lexploitation-de-noms-de-domaine.

[62] ANSSI. *Recommandations relatives à l'administration sécurisée des systèmes d'information reposant sur Microsoft Active Directory, Guide ANSSI-BP-099 v1.0*. 18 octobre 2023.
URL : https://cyber.gouv.fr/guide-admin-si-ad.

[63] ANSSI. *Authentification multifacteurs et mots de passe, Guide ANSSI-PG-078 v1.0*. 8 octobre 2021.
URL : https://cyber.gouv.fr/guide-authentification.

[64] ANSSI. *Recommandations de sécurité pour la journalisation des systèmes Microsoft Windows en environnement Active Directory, Guide ANSSI-PB-090 v1.0*. 28 janvier 2022.
URL : https://cyber.gouv.fr/guide-journalisation.

[65] ANSSI. *Sauvegarde des systèmes d'information, Guide ANSSI-BP-100 v1.0*. 25 octobre 2023.
URL : https://cyber.gouv.fr/publications/fondamentaux-sauvegarde-systemes-dinformation.

[66] ANSSI. *Crise d'origine cyber, les clés d'une gestion opérationnelle et stratégique, Guide ANSSI-PA-089 v1.0*. 6 décembre 2021.
URL : https://cyber.gouv.fr/publications/crise-dorigine-cyber-les-cles-dune-gestion-operationnelle-et-strategique.

[67] ANSSI. *Organiser un exercice de gestion de crise cyber, Guide ANSSI-PA-081 v1.0*. 14 octobre 2020.
URL : https://cyber.gouv.fr/publications/organiser-un-exercice-de-gestion-de-crise-cyber.

Version : 1.0 – 17 avril 2025

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI – 51, boulevard de la Tour-Maubourg – 75700 PARIS 07 SP
cyber.gouv.fr • cert.ssi.gouv.fr

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité