TECHNOLOGIE OPÉRATIONNELLE D'INFRASTRUCTURES ROUTIÈRES

GUIDE D'INTRODUCTION SUR LA CYBERSÉCURITÉ

Décembre 2022

Transport Canada Transports Canada

Canada

This publication is also available in English under the following title Road Infrastructure Operational Technology Cyber Security Primer.

TP 15529F

Cat. T89-14/2022F-PDF

ISBN 978-0-660-42294-7

Préparé par Transports Canada.

TABLE DES MATIÈRES

1. Sommaire

Le présent guide d'introduction a été créé pour fournir des directives et des pratiques exemplaires aux propriétaires et exploitants d'infrastructures (PEI) canadiens afin que ces derniers élaborent des programmes de cybersécurité pour les systèmes de transport intelligents et les systèmes de gestion du trafic (SGT).

Les systèmes de transport intelligents (STI) intègrent différentes technologies de l'information et de communication dans l'infrastructure et les véhicules de transport routier, dans le but de rendre le système de transport plus sécuritaire et plus efficace. Les SGT sont un type de technologie opérationnelle (TO) qui aident à contrôler et à produire des produits et services comme les systèmes de feux de circulation et les systèmes de gestion routière active.

Les STI et les SGT sont combinés à des systèmes de technologie de l'information (TI) pour optimiser et améliorer l'efficacité et la sécurité des routes canadiennes.

Cependant, la plupart des anciens équipements de STI n'ont pas été conçus pour être combinés et connectés à d'autres systèmes et réseaux, et n'ont souvent pas été développés en tenant compte des risques émergents en matière de cybersécurité. Au fur et à mesure que ces systèmes sont combinés, les PEI doivent tenir compte des nouvelles menaces et mettre en place des contrôles de sécurité appropriés.

Le présent guide d'introduction donne un aperçu du paysage actuel des STI, des cybermenaces et des vulnérabilités existantes et émergentes à prendre en compte, et des répercussions potentielles des cyberattaques. Ce guide présente également des outils, des ressources et des cadres qui peuvent être utilisés pour évaluer et améliorer la position de votre organisation en matière de cybersécurité (la robustesse de la cybersécurité de votre organisation et sa capacité à résister aux cybermenaces et à y répondre).

La section recommandations énumère six mesures que les PEI devraient envisager de mettre en place :

1. **Comprendre l'environnement.** Il est essentiel de comprendre l'environnement, y compris la sensibilité et l'exposition des données qui circulent au sein du réseau, pour planifier et mettre en œuvre de nouvelles technologies tout en gérant les risques.
2. **Comprendre la position actuelle en matière de cybersécurité.** Améliorer les systèmes et les protéger contre les vulnérabilités connues. Cette mesure commence par l'évaluation de l'état actuel de la position de votre organisation en matière de cybersécurité, la détermination des domaines à améliorer et la priorisation du travail.
3. **S'assurer que la structure organisationnelle et les processus de planification soutiennent la cybersécurité des TO.** Il faut s'assurer que la structure organisationnelle et les processus de planification aident à comprendre les risques de cybersécurité des TO et à affecter suffisamment de ressources pour y remédier.
4. **Recourir aux politiques et aux pratiques exemplaires en matière de cybersécurité.** Utiliser les normes de l'industrie et les cadres de conformité pour s'assurer que les contrôles et les considérations de cybersécurité sont appliqués aux actifs de TI et de TO.
5. **Mettre au point des processus et des plans d'intervention en cas d'incident et les mettre à l'essai.** Élaborer des plans officiels d'intervention en cas d'incident, qui sont

compréhensibles par les principaux intervenants, mis à l'essai et actualisés régulièrement.

6. **Réaliser une évaluation continue des cyberrisques.** Les cyberrisques sont en constante évolution. L'utilisation rapide de technologies de l'information et de technologies opérationnelles nouvelles signifie que vous devez être conscient des vulnérabilités de jour zéro (vulnérabilités dont l'existence n'est pas encore connue des fournisseurs) et des risques émergents.

En utilisant ces pratiques exemplaires et d'autres activités de cyberhygiène, les PEI ont la faculté de limiter les cyberrisques aujourd'hui et à l'avenir.

2. Comment utiliser ce guide

Les technologies de transport routier évoluent rapidement. Cette évolution peut améliorer la sécurité routière, introduire de nouvelles formes de mobilité et créer des possibilités économiques. Ces technologies apportent de nombreux avantages, mais elles introduisent aussi de nouvelles vulnérabilités en matière de cybersécurité.

L'intégration de ces technologies à l'environnement de votre organisation ainsi que les menaces à la cybersécurité en constante évolution ont introduit de nouveaux risques au sein du système de transport routier du Canada.

Le transport routier est une responsabilité partagée entre les administrations fédérales, provinciales, territoriales et municipales. Bien que Transports Canada établisse des normes et des règlements sur la sécurité des véhicules, les provinces, les territoires et les municipalités du Canada (collectivement appelés « administrations routières ») sont responsables de la planification, de la conception, de la construction, de l'exploitation et de l'entretien de la majeure partie du réseau routier du Canada.

Le présent guide d'introduction a pour objectif d'aider les PEI à mieux comprendre les considérations uniques en matière de cybersécurité des systèmes de gestion du trafic (SGT) et des systèmes de transport intelligents (STI). La plupart des organisations ont déjà mis en place des pratiques bien établies en matière de cybersécurité des technologies de l'information (TI), mais la sécurisation de la technologie opérationnelle (TO) utilisée par les SGT et les STI nécessite une approche fondée sur les pratiques de cybersécurité des systèmes de contrôle industriels (SCI). Le guide comprend également des exemples concrets qui soulignent la nécessité d'une approche proactive.

Étant donné la constante évolution de la cybersécurité, l'objectif du présent guide est d'aider les organisations à comprendre cette tâche complexe; il comprend donc des étapes pratiques et des pratiques exemplaires pour améliorer la position en matière de cybersécurité. Bien que certaines des normes techniques de ce guide finissent par devenir obsolètes, les pratiques exemplaires et la nécessité de rester vigilant et de se tenir au courant des dernières technologies perdureront.

Les recommandations de ce guide d'introduction offrent des directives stratégiques en matière de cybersécurité. Il ne s'agit pas de standard techniques ou de solutions exhaustives pour la cybersécurité des SGT et STI.

Ce guide doit être utilisé dans le cadre de la mise en place des pratiques exemplaires, des directives et des normes élaborées par :

- Sécurité publique Canada;
- le Centre de la sécurité des télécommunications;

- d’autres ministères fédéraux ayant une expertise en cybersécurité;
- des organismes de réglementation internationaux de confiance;
- des associations industrielles;
- des ressources de cybersécurité pertinentes dans d’autres secteurs;
- des organismes de normalisation internationaux.

3. État actuel des systèmes de transport intelligents et des systèmes de gestion du trafic

Les SGT d’aujourd’hui sont composés de systèmes fortement interconnectés qui s’appuient sur des outils technologiques pour améliorer le flux de circulation et la sécurité. Un biproduit reliant ces technologies constitue un environnement de plus en plus connecté qui expose les vulnérabilités à davantage de menaces.

Comme le montre la figure 1, il convient de tenir compte de trois facteurs clés lors de l’intégration d’un environnement de TO habituellement séparé à un environnement de TI :

- **Convergence :** L’unification des infrastructures de TI et de TO atténue l’écart entre le monde physique et le cybermonde, ce qui pourrait faire en sorte qu’une organisation a de la difficulté à comprendre et à protéger l’environnement entier.

- **Interopérabilité :** La combinaison de systèmes et de plateformes anciens et nouveaux peut se révéler compliquée et difficile à gérer et à protéger.

- **Intégration et connectivité :** La combinaison de services entre les domaines via l’« Internet des objets » (IdO – le réseau d’appareils de tous les jours qui peuvent se connecter et partager des informations entre eux) et les technologies numériques peut être compliquée et difficile à gérer et à protéger.

Convergence

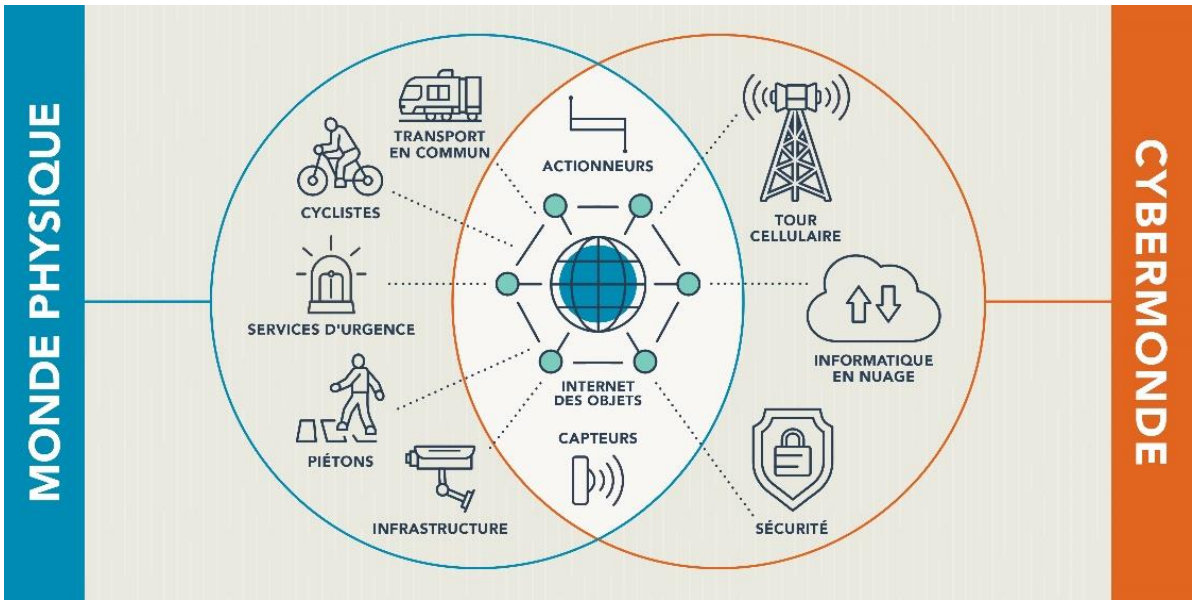

Figure 1 : Facteurs clés à prendre en considération lors de l'intégration d'un environnement de technologies opérationnelles distinct à un environnement de TI

Interopérabilité

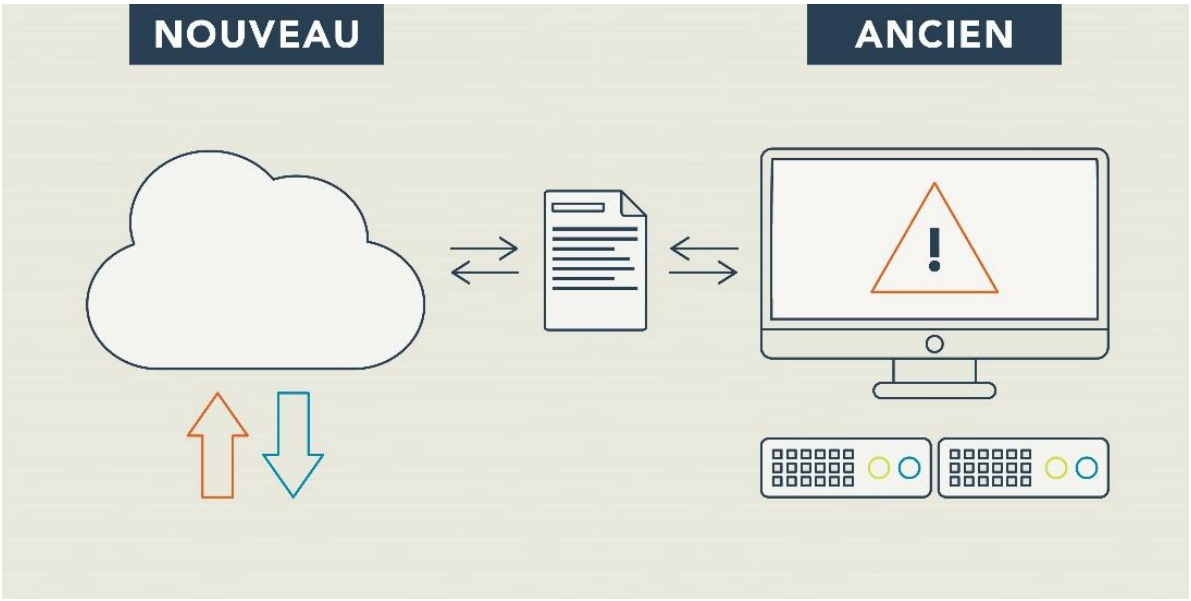

Figure 2 : L'interopérabilité entre les nouveaux et anciens systèmes

Intégration

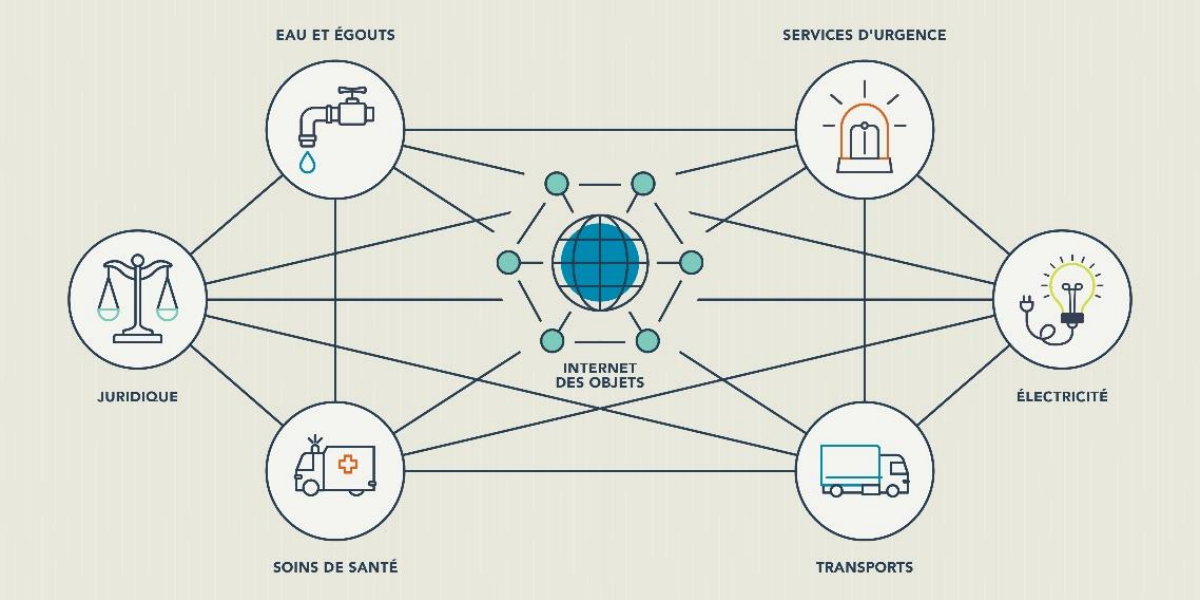

Figure 3 : L'intégration et la connectivité entre des éléments de l'infrastructure critique

Les SGT traditionnels comportent de nombreux éléments comme les contrôleurs de signal (logiciels qui contrôlent les feux de circulation), les capteurs de circulation, la télévision en circuit fermé (CCTV) et les panneaux de message variables. Les divers éléments de nombreux SGT existants n'ont pas été conçus pour se connecter à des réseaux externes.

Par conséquent, les contrôles de sécurité standard qui sont communs aux systèmes de TI, comme l'authentification et l'autorisation obligatoires, peuvent ne pas avoir été mis en œuvre ou priorisés lorsque les systèmes ont été développés. L'absence de contrôles de sécurité de base pose un risque grave lorsqu'on prévoit l'ajout à des systèmes aussi sophistiqués.

Les SGT recueillent et envoient de grandes quantités de données à divers points d'extrémité et par l'intermédiaire de dispositifs connectés. Ces données permettent au système de fonctionner correctement, efficacement et en toute sécurité. Les dispositifs de points d'extrémité qui envoient et reçoivent des données dans un SGT sont des dispositifs Internet des objets (IdO) connectés avec un accès intégré à Internet.

Dans de nombreux cas, ces dispositifs IdO ne sont pas suffisamment protégés avant leur déploiement, et les données peuvent être déchiffrées. Si un individu a obtenu l'accès au réseau avec ces dispositifs IdO, il peut ainsi voler ou modifier les données ou encore ajouter des données nuisibles.

Si un SGT est piraté, le système peut alors être manipulé, les modèles de trafic perturbés ou la sécurité compromise. Sachant que les données au sein du SGT ont une incidence directe sur l'expérience de l'utilisateur et sa sécurité, il est essentiel de sécuriser ces systèmes.

Enfin, il est important de comprendre que le cycle de vie du nouvel équipement STI numérique peut être plus court que dans le cas des générations précédentes de systèmes électromécaniques. Il peut également nécessiter une maintenance logicielle plus fréquente (telles que des mises à jour de micrologiciel), comme pour les systèmes et équipements de TI plus récents.

3.1. Nouvelles menaces

L'année 2020 a connu une hausse des cybermenaces contre les systèmes de TO et les propriétaires de systèmes de TO dans le monde entier. Prenant acte des vulnérabilités introduites par l'association des technologies informatiques et opérationnelles, les cybercriminels ciblent de plus en plus les infrastructures essentielles des TO dans le monde entier. Ces groupes varient en sophistication (gravité des attaques) et leurs motifs varient eux aussi[1].

> « Les organisations canadiennes de toutes tailles, comme les petites et moyennes entreprises, les municipalités, les universités et les fournisseurs d'infrastructures essentielles (processus, systèmes, installations, technologies, réseaux, actifs et services qui assurent le bon fonctionnement de l'État et la santé, la sécurité et la sûreté des Canadiens), sont confrontées à un nombre croissant de cybermenaces.
>
> Ces organisations contrôlent un vaste éventail d'actifs pouvant intéresser les auteurs de cybermenace, dont la propriété intellectuelle, les données financières, les systèmes de paiement, les données des clients, les partenaires et les fournisseurs, ainsi que les installations industrielles et leur machinerie. En règle générale, plus une organisation possède d'actifs connectés à Internet, plus elle court le risque de faire face à une cybermenace. »
>
> - Centre canadien pour la cybersécurité – Évaluation des cybermenaces nationales 2020

La motivation la plus courante chez les cybercriminels est le gain financier. Une méthode populaire consiste à utiliser une attaque par rançongiciel pour bloquer l'accès à un système ou à une application critique et à exiger une rançon contre le rétablissement de l'accès. La vie privée des utilisateurs peut être compromise lors d'une attaque par rançongiciel en cas de vol, de divulgation ou de revente de données.

En dehors des signes de message variables dans l'exemple Deutsche Bahn – Wanna Cry il n'y a eu aucune cyberattaque majeure signalée publiquement contre le SGT depuis le début de 2022. Cependant, de nombreux autres systèmes d'infrastructures essentielles (comme les générateurs d'énergie, le pétrole et le gaz, les produits chimiques) ont été et continuent d'être la cible de cyberattaques. Vous trouverez d'autres exemples d'attaques à la section 4.2.

Les infrastructures essentielles peuvent également être la cible d'attaques motivées par des raisons politiques, en raison de leur importance cruciale pour la nation et les citoyens.

Outre les gains politiques ou financiers, les attaques peuvent être motivées par la curiosité ou le vandalisme. Ces attaques sont moins probables en raison des compétences et des connaissances requises pour qu'elles aboutissent. L'annexe A présente une description détaillée des auteurs de menace potentielle et de leurs motivations habituelles.

Alors que de plus en plus d'infrastructures connectées sont mises en place, les PEI doivent recourir à des méthodes de conception sécurisées pour limiter l'amplitude d'attaque du SGT. Il est important,

[1] Canada. Centre de la sécurité des télécommunications *Introduction à l'environnement de cybermenace*. https://cyber.gc.ca/sites/default/files/publications/Intro-to-cyber-threat-environment-e.pdf. Consulté le 22 avril 2022.

non seulement de concevoir des systèmes sécurisés, mais aussi pour les PEI de concevoir leurs infrastructures et leur environnement de TO afin de protéger et de gérer de grands volumes de données. Ces données, qu'elles soient inactives ou en transit, devront être protégées au moyen de technologies de cryptage et de pratiques exemplaires au sein du secteur.

La mise en œuvre de ces technologies de cryptage à grande échelle n'est pas facile et peut entraîner des problèmes de performance. Une compréhension approfondie de l'environnement, notamment de la sensibilité et de l'exposition des données traversant le réseau, est essentielle pour planifier et mettre en œuvre correctement la technologie de cryptage.

Il est également important de s'assurer de ce qui suit :

- Gérer correctement les configurations;
- Surveiller les comportements malveillants;
- Appliquer des correctifs de sécurité, dans la mesure du possible.

Les auteurs de menace s'engouffrent souvent dans la brèche de moindre résistance. Grâce à une gestion diligente des vulnérabilités et à l'atténuation des vulnérabilités connues, les PEI peuvent réduire la probabilité de faire l'objet d'une attaque de la part d'un auteur malveillant.

Il est crucial que les systèmes d'infrastructures essentielles (comme les générateurs d'énergie, les usines de gaz et de produits pétroliers, les usines de produits chimiques) restent isolés par rapport à Internet en n'y étant pas directement connectés, car il s'agirait d'une vulnérabilité importante et facile à exploiter. En général, divers réseaux informatiques existent à l'avant des systèmes d'infrastructures essentielles. En appliquant les contrôles de sécurité requis à ces réseaux informatiques, les organisations peuvent commencer à renforcer leurs systèmes de TO contre les risques posés par les menaces externes. Les pratiques exemplaires générales en matière de cybersécurité, notamment celle consistant à suivre le principe du privilège le moins élevé, aident à protéger les ordinateurs et les serveurs utilisés par les organisations. Consultez la section des recommandations pour obtenir plus de pratiques exemplaires.

Il est essentiel de cerner et d'évaluer les risques potentiels et de déterminer la tolérance au risque de votre organisation. Cela aidera à prendre des décisions fondées sur les risques lors du choix des contrôles de sécurité appropriés à mettre en place. Dans la mesure du possible, les organisations doivent remplacer les systèmes et le matériel non pris en charge. Les organisations peuvent toujours utiliser des appareils non pris en charge (non sécurisés), en effectuant des évaluations appropriées de la gestion des risques de cybersécurité, en mettant en œuvre les contrôles de sécurité appropriés au moyen de techniques de conception d'architecture (comme la segmentation des réseaux) et d'autres mesures de défense en profondeur.

4. Répercussions potentielles des cyberattaques

4.1. Répercussions potentielles des systèmes de transport intelligents

Comme mentionné précédemment, divers groupes sont susceptibles de cibler des systèmes d'infrastructures essentielles pour remplir certains objectifs spécifiques. Selon la nature de l'attaque, les objectifs servis et l'organisation ciblée, les répercussions sont variables.

Le vol de données, les réseaux perturbés, les logiciels malveillants et autres cyberattaques peuvent avoir des conséquences importantes pour l'organisation ou les personnes victimes. La probabilité et l'incidence de ces menaces continueront d'augmenter. Il est aussi important de comprendre les répercussions potentielles d'une cyberattaque, car elles peuvent éclairer les décisions concernant les contrôles de sécurité.

Sécurité

Les infrastructures régissant la circulation et le transport sont développées en intégrant des mesures de sécurité pour protéger les usagers, les navetteurs et les travailleurs. Si les systèmes de sécurité et leurs dispositifs à sécurité intégrée sont compromis, les usagers, les navetteurs et les opérateurs risquent d'être gravement blessés. Les systèmes de sécurité représentent des cibles potentielles, car ils peuvent procurer un outil puissant pour extorquer une organisation.

Opérations

Une attaque bien exécutée peut entraîner la perturbation de l'infrastructure de transport sous-jacente. Du point de vue des systèmes d'infrastructures essentielles, une attaque largement étendue pourrait avoir un effet d'entraînement, ayant des répercussions considérables sur d'autres secteurs publics. Ces répercussions pourraient avoir des effets économiques négatifs comme des perturbations de la chaîne d'approvisionnement. Par exemple, une attaque ciblée pourrait entraîner la perte de fonctionnement d'un système de contrôle des voies de circulation, entraînant une congestion accrue, le risque d'accidents de la circulation et des perturbations des principales voies de transport.

Réputation

Une violation ou une perturbation importante pourrait nuire à la perception que le public a des STI et des organisations concernées (PEI, fournisseurs de technologie, etc.). Dans les situations où il y a violation de données personnelles (à titre d'exemple, noms, adresses ou numéros de plaques d'immatriculation), des effets sur la protection de la vie privée pour le public pourraient avoir une incidence sur la réputation de l'organisation concernée.

Finances

Les organisations qui ont subi une cyberattaque majeure sont susceptibles de subir des conséquences d'ordre financier. Cela peut prendre diverses formes, qu'il s'agisse du paiement d'une rançon (rançongiciel), de frais juridiques, d'une diminution de la confiance du public ayant une

incidence sur les revenus et enfin des dépenses de fonctionnement et d'immobilisations pour atténuer l'attaque et réparer/remplacer les équipements endommagés. Par exemple, un pirate peut cibler un système vulnérable, en encodant un actif de grande valeur comme un système de contrôle du trafic. Les pirates demandent alors qu'une rançon soit payée pour recouvrer le contrôle du réseau.

4.2 Exemples d'attaques

Avec l'arrivée de toutes les nouvelles technologies au niveau des systèmes de transport, apparaissent de nouvelles dimensions aux cyberrisques associés à ces systèmes. Le secteur des transports est devenu la proie de cyberattaques malveillantes et risque également d'être compromis accidentellement.

La probabilité d'événements nouveaux ou plus importants augmente avec le coût des cyberincidents et de la cybercriminalité. En analysant les violations antérieures, les administrations routières peuvent se préparer à des cyberévénements. Vous trouverez ci-dessous quelques exemples généraux de cyberattaques contre des secteurs ou des systèmes comparables.

Commission des transports en commun de Toronto – Rançonlogiciel (2021)

La Commission des transports en commun de Toronto a révélé qu'elle avait été la cible d'une attaque par rançongiciel qui a touché les systèmes de communication essentiels. Les systèmes utilisés pour communiquer avec les conducteurs de véhicules, les écrans de plateforme, les applications externes, les systèmes de courriel et de nombreux autres éléments se sont trouvés cryptés et inutilisables. Le jour de sa découverte, l'attaque a eu une incidence limitée, mais le lendemain, les pirates ont renforcé leur attaque en contaminant plusieurs systèmes et services du réseau[2].

Usine de traitement des eaux d'Israël – Menace sophistiquée et persistante (2020)

Une menace sophistiquée et persistante nécessite des compétences élevées et un financement important. Il s'agit généralement d'un groupe financé par un État ou un État-nation, qui accède à un réseau informatique et reste non détecté pendant longtemps.

Israël a révélé que ses infrastructures de traitement des eaux avaient été ciblées dans le but d'accroître les niveaux de produits chimiques dans les stations de fourniture d'eau potable et de saboter les usines de pompage d'eaux destinées à l'agriculture. Si les attaques avaient abouti, les produits chimiques auraient rendu l'eau toxique, ce qui aurait peut-être déclenché l'arrêt des pompes, laissant ainsi des milliers de personnes sans eau potable[3].

Deutsche Bahn – WannaCry (2017)

Deutsche Bahn a annoncé avoir été ciblée par le rançongiciel « WannaCry ». Bien que le service ferroviaire n'ait pas été perturbé, les panneaux d'affichage électroniques des gares de tout le pays ont affiché les messages du pirate exigeant le paiement d'une rançon par Deutsche Bahn. Le

[2] https://www.thestar.com/news/gta/2021/10/29/ransomware-attack-on-ttc-shuts-down-vital-communication-systems.html
[3] https://www.timesofisrael.com/cyber-attacks-again-hit-israels-water-system-shutting-agricultural-pumps/

gouvernement allemand a assuré au public que l'attaque n'avait pas touché les systèmes informatiques du gouvernement[4].

Agence des transports municipaux de San Francisco – Logiciel malveillant HDDCCryptor (2016)

L'agence des transports municipaux de San Francisco a été la cible d'une attaque par rançongiciel à grande échelle utilisant une version du logiciel malveillant HDDCryptor. Les représentants de l'agence ont déclaré que l'attaque avait infecté 2 112 ordinateurs, les cryptant pour exiger une rançon de 100 bitcoins (soit 73 086 $ US à l'époque). L'attaque a gelé les terminaux des points de vente et les portillons d'accès de l'agence afin de les désactiver. Pour réduire l'incidence sur les clients du système ferroviaire, l'agence a été forcée d'offrir l'accès gratuit aux usagers[5].

Ces exemples prouvent que les auteurs de menace peuvent utiliser de nombreux types d'attaques pour exploiter les vulnérabilités des TO. Ces attaques peuvent varier en complexité, mais force est de constater le mode opératoire récurrent de ces attaques, qui utilisent plusieurs points d'entrée, techniques et vecteurs d'attaque.

Nous recommandons aux PEI d'analyser plus en détail les études de cas pour déterminer les pratiques positives et les possibilités d'amélioration afin de minimiser l'incidence d'un cybévénement potentiel.

5. Recommandations

Comme nous l'avons expliqué, l'introduction des TI dans les systèmes de TO et SGT traditionnellement physiques rend ces systèmes « intelligents » et permet d'améliorer leurs fonctionnalités de base. Dans ces scénarios, le logiciel et le matériel des TO/SCI/SGT demeurent les mêmes, mais ont introduit un élément de numérisation par l'intermédiaire de logiciels et de réseaux connectés. Cela peut englober les dispositifs de communication de véhicules connectés et automatisés (VCA), la surveillance et la gestion centralisées du trafic, l'infrastructure urbaine intelligente, la gestion du trafic prise en charge par l'IA et la coordination des transports en commun, entre autres cas d'utilisation. Bien que la fonctionnalité de base dans le secteur des transports ait considérablement augmenté en raison de la convergence TI/TO, l'exposition à de multiples menaces provenant de sources locales et éloignées s'est considérablement renforcée. Les PEI doivent améliorer leur position en matière de cybersécurité pour se rendre moins vulnérables aux attaques. Les perturbations de la fonction du logiciel de TO sous-jacent peuvent avoir des conséquences importantes, comme la perturbation des chaînes d'approvisionnement, des répercussions socioéconomiques négatives et, pire encore, la mise en péril de la sécurité publique et de la sécurité nationale. Les PEI peuvent limiter l'incidence d'une cyberattaque en utilisant les pratiques exemplaires pour améliorer la résilience de leur organisation. Voici quelques exemples de pratiques exemplaires et des mesures que votre organisation pourrait prendre pour gérer les cyberrisques.

ⓘ Ces recommandations ne sont pas exhaustives. Elles ont pour mission de donner aux PEI quelques pistes à suivre quant aux prochaines étapes à suivre pour améliorer la résilience de leur organisation.

[4] https://www.reuters.com/article/us-cyber-attack-germany-rail-idUSKBN1890DM
[5] https://www.theguardian.com/technology/2016/nov/28/passengers-free-ride-san-francisco-muni-ransomeware

Comprendre l’environnement

Une bonne compréhension de l’environnement d’exploitation, notamment la sensibilité et l’exposition des données traversant le réseau, est essentielle pour planifier et mettre en œuvre adéquatement de nouvelles technologies, tout en gérant les risques.

Cette compréhension aidera à cerner les vulnérabilités et les risques qui peuvent survenir lorsque vous commencez à intégrer de nouvelles technologies. Pour ce faire, une organisation doit rester informée des dernières normes et directives et des derniers cadres en vigueur. L’annexe C regroupe des documents de référence utiles à toute organisation pour rester informée des outils et des pratiques exemplaires en matière de cybersécurité.

Comprendre votre position en matière de cybersécurité

Pour atteindre la position cible en matière de cybersécurité, les organisations doivent se protéger de manière significative contre les cybermenaces et corriger les faiblesses du système. Les organisations ne peuvent se préparer à réagir qu’aux vulnérabilités connues et à s’en protéger. Pour ce faire, les organisations devront :

- évaluer leur position actuelle en matière de cybersécurité;
- déterminer les points à améliorer;
- donner la priorité au travail de cybersécurité, au besoin.

L’annexe B comprend des détails sur différents types d’attaques.

L’outil d’évaluation de la maturité en matière de cybersécurité des infrastructures routières de Transports Canada, disponible sur le site web sur la cybersécurité du transport routier, aidera les PEI à évaluer leur position actuelle en matière de cybersécurité. De plus, l’outil permettra aux PEI d’établir un état cible et fournira des recommandations pour y parvenir.

Le profil cible est personnalisable, de sorte que les PEI peuvent mettre en œuvre des contrôles de sécurité qui reflètent leur évaluation unique des risques. L’outil sera fondé sur le cadre de cybersécurité du NIST et personnalisé pour les SGT et STI.

Soutenir la cybersécurité des technologies opérationnelles

Il est essentiel pour les organisations d’avoir un programme holistique de cybersécurité qui tient compte des menaces et des vulnérabilités potentielles dans l’ensemble de l’organisation, y compris les technologies de l’information et les technologies opérationnelles. Les PEI doivent examiner leur structure organisationnelle actuelle en matière de cybersécurité pour s’assurer que les processus de planification soutiennent la cybersécurité des TO.

Les hauts dirigeants doivent insister sur la nécessité d’appliquer des contrôles de cybersécurité et des pratiques exemplaires à l’échelle de l’organisation et de diffuser les objectifs et les priorités en matière de sécurité par le biais de messages descendants. Les plans stratégiques – relatifs aux

finances, aux opérations, aux ressources humaines – devraient refléter la nature continue de la cyberrésilience en matière de TO.

La capacité d'une organisation à satisfaire à sa position de cybersécurité cible dépend de la planification et de l'allocation de fonds pour l'équipement de TO, l'achat, la formation et le maintien en poste du personnel.

Utiliser des politiques et des pratiques exemplaires

Les organisations doivent élaborer une approche intégrée et des politiques adaptées pour gérer la cybersécurité dans l'ensemble des actifs des technologies de l'information et des technologies opérationnelles. Utiliser les normes et les cadres de conformité de l'industrie pour évaluer et modéliser la politique de gestion des risques des organisations en ce qui concerne les actifs du SGT, de TI, les processus, les procédures et les fournisseurs.

Que les organisations gèrent les TI ou le SGT, les cadres de l'annexe C peuvent être utilisés par les PEI comme base pour mettre en place les personnes, les processus, la technologie et les pratiques de gouvernance adaptées pour gérer les cyberrisques.

Ces cadres volontaires vous aideront à créer, à maintenir et à améliorer la maturité de la cybersécurité et la préparation générale. Ces cadres aideront les PEI à subdiviser ces domaines en catégories gérables, pour ainsi mieux atteindre leurs objectifs de maturité et de préparation en matière de cybersécurité.

Mettre en pratique

Même les organisations les plus matures subiront une cyberviolation à un moment donné. La façon dont une organisation peut cerner et évaluer le cyberévénement, y réagir et s'en rétablir dictera les répercussions sur son organisation.

Les PEI doivent donc élaborer des plans officiels d'intervention en cas d'incident qui sont communiqués aux principaux intervenants, mis à l'essai pour assurer leur efficacité et actualisés de façon continue. Un plan conjoint d'intervention en cas de cyberincident lié aux technologies de l'information et aux technologies opérationnelles peut aider à s'assurer qu'une organisation peut réagir aux cybermenaces. Pour en savoir plus, consultez l'annexe C.

Continuer d'évaluer les cyberrisques

La gestion des cyberrisques est un processus permanent qui doit être intégré à la fonction de gestion des risques d'une organisation. Du fait de l'utilisation rapide des technologies émergentes et de la combinaison des technologies de l'information et des technologies opérationnelles, les cyberrisques sont en constante évolution. À ce titre, les PEI doivent rester à l'affût des vulnérabilités de jour zéro et des risques émergents, afin qu'ils puissent réagir en conséquence.

En comprenant l'évolution du paysage des menaces et en mettant en œuvre de manière proactive les pratiques exemplaires de cybersécurité susmentionnées, les PEI peuvent réduire leur niveau de cyberrisque, tout en améliorant leur résilience.

Annexe A : Menaces et motivations

Aperçu des auteurs de menaces potentielles et de leurs motivations[6].

Attaque financée par un État ou un État-nation

Les menaces financées par un État sont généralement considérées comme les plus sophistiquées. Les groupes sont financés et formés par des États-nations antagoniques, ce qui augmente considérablement leurs capacités et leurs ressources. Une distinction importante dans cette catégorie d'auteurs de menace est qu'ils ne sont généralement pas motivés par un gain financier. Au lieu de cela, les attaques sont perpétrées pour des intérêts géopolitiques.

Cybercriminels

Les cybercriminels lancent généralement des attaques modérément sophistiquées. Ils n'ont pas les ressources dont disposent habituellement les groupes financés par un État, mais représentent toujours une menace majeure. Leur motivation est généralement financière, et ils utilisent souvent un rançongiciel pour extorquer de l'argent à leurs victimes. Certains des groupes de cybercriminels les plus sophistiqués sont liés au crime organisé.

Hacktivistes, groupes terroristes et amateurs de sensations fortes

Ces groupes sont généralement moins sophistiqués que les groupes mentionnés précédemment. Ils comptent sur des outils facilement accessibles pour leurs attaques et n'ont pas les compétences techniques des pirates professionnels. Ils sont souvent motivés par le désir de perturber les systèmes et constituent une nuisance dans les systèmes de TO.

Menaces internes

Les intervenants internes peuvent cibler intentionnellement ou non les actifs des TO et TI. Un employé mécontent peut intentionnellement cibler un système, un nouvel employé peut accidentellement causer des dommages ou contaminer un système.

[6] Canada. Centre de la sécurité des télécommunications *Introduction à l'environnement de cybermenace*. https://cyber.gc.ca/sites/default/files/publications/Intro-to-cyber-threat-environment-e.pdf. Consulté le 22 avril 2022.

Annexe B : Types d’attaques

Intrusion sur réseau

Les acteurs malveillants sont toujours à la recherche de vulnérabilités exploitables pour accéder aux réseaux et aux systèmes. Dans certains cas, les pirates utilisent ces vulnérabilités pour obtenir un accès à distance afin de modifier un système.

Une fois identifiées, ces vulnérabilités peuvent être traitées en utilisant des correctifs émanant des fournisseurs de logiciels.

Ces vulnérabilités sont importantes pour les réseaux STI et TO. Ces systèmes, souvent constitués de matériel existant, ne sont pas pris en charge et sont sans correctif. Ces anciens systèmes peuvent souvent présenter un risque réel important.

Vulnérabilités de jour zéro

Malheureusement, les fournisseurs d’équipement ne connaissent pas toutes les vulnérabilités, de sorte que ces systèmes peuvent toujours être ciblés par des pirates qui, eux, les connaissent. C’est ce qu’on appelle des « vulnérabilités de jour zéro ». Les vulnérabilités de jour zéro sont particulièrement difficiles à détecter si elles sont exploitées, car le problème est inconnu à moins qu’il ne soit divulgué ou découvert par quelqu’un d’autre qu’un pirate.

Maliciels

Les logiciels malveillants, appelés « maliciels », sont souvent utilisés pour attaquer des systèmes internes. Il existe de nombreux types de maliciels, certains développés par les pirates eux-mêmes, d’autres achetés puis utilisés par les pirates, notamment :

- **les chevaux de Troie à distance** insèrent un « accès dérobé » dans un réseau qui permet à un pirate d’y accéder. Cet accès peut alors être utilisé pour voler des données, endommager des systèmes ou manipuler des contrôles;
- **le rançongiciel** crypte les systèmes infectés, bloquant l’accès aux fichiers jusqu’à ce qu’une rançon soit payée. Cela peut rendre les systèmes inexploitables, une situation qui peut ne pas être corrigée une fois la rançon payée;
- **les logiciels malveillants sur le point de vente** infectent les systèmes de paiement et sont utilisés pour recueillir les informations de paiement des clients qui sont ensuite vendues par l’intermédiaire des marchés en ligne;
- **les enregistreurs de frappe** sont utilisés pour enregistrer les frappes d’un utilisateur. Les pirates peuvent utiliser cette méthode pour voler des informations d’identification qu’ils peuvent ensuite utiliser pour accéder aux systèmes;
- **les logiciels espions** sont utilisés pour regarder secrètement un utilisateur d’ordinateur. Ils peuvent être utilisés pour accéder à des renseignements confidentiels ou pour voler des identifiants;

- **les programmes malveillants furtifs** sont un type de maliciel difficile à détecter, conçu pour masquer les activités malveillantes qui interviennent sur un ordinateur. Ils peuvent permettent à un pirate de prendre le contrôle d'un système à distance.

Déni de service (DdS)

Les attaques par déni de service impliquent que les pirates coordonnent plusieurs ressources, souvent des robots, pour diriger le trafic vers les systèmes afin de les submerger et de les mettre en panne. Les attaques par déni de service distribué sont devenues plus courantes dans la deuxième moitié des années 2010.

Les attaques par déni de service distribué sont connues pour leur simplicité. Des outils ont été créés et distribués sur Internet afin que les utilisateurs inexpérimentés puissent lancer des attaques coordonnées contre différentes cibles. Les outils de déni de service distribué réduisent considérablement le niveau technique des attaques et ont le potentiel de perturber considérablement les systèmes.

Ingénierie sociale et hameçonnage

Le piratage social est un terme large utilisé pour décrire l'exploitation des interactions humaines. Les pirates peuvent se faire passer pour quelqu'un qu'ils ne sont pas (un employé, un FSI, etc.) et ainsi abuser de la confiance des cibles. Tout d'abord, ces pirates recueillent le plus de renseignements possible auprès de la personne ciblée. Cela peut inclure des adresses, l'accès à des zones restreintes ou même des mots de passe.

L'hameçonnage et une forme d'ingénierie sociale. Très courantes, les attaques par hameçonnage peuvent aller de basiques à très sophistiquées, certaines ciblant même les cadres supérieurs avec des informations très spécifiques et des messages spécialement conçus. Les attaques d'hameçonnage utilisent des courriels pour manipuler les utilisateurs et les inciter à cliquer sur des liens malveillants ou à partager des données sensibles. L'hameçonnage est couramment utilisé pour installer des maliciels.

D'autres formes d'hameçonnage sont l'hameçonnage par connexion vocale (vishing) et l'hameçonnage par message texte (smishing). Ces types d'attaques sont moins courantes et agressives, mais posent tout de même le problème du risque de fuites de données et d'intrusion malveillante.

Attaques par des canaux auxiliaires

Une attaque par un canal auxiliaire cible les réponses indirectes du matériel informatique, comme les émissions électriques ou d'autres effets physiques, pour comprendre, puis extraire des données confidentielles. Les systèmes cryptographiques (systèmes qui protègent l'information et les communications à l'aide d'algorithmes de cryptage) constituent une cible courante des attaques par les canaux auxiliaires.

Les attaques par canaux auxiliaires sont rendues possibles parce que les cryptosystèmes produisent des effets physiques lorsqu'ils fonctionnent (comme le son émis par une opération ou la puissance de traitement qu'elle consomme), ce qui peut fournir des indices sur le système. Les fuites d'informations de ce type peuvent ne pas sembler importantes, mais les pirates sophistiqués sont susceptibles d'utiliser ces informations pour deviner les clés algorithmiques utilisées pour chiffrer les données.

Une fois en possession des informations, les pirates peuvent décrypter les données sensibles et compromettre le système. Ces attaques sont très difficiles à exécuter, mais un pirate qualifié et engagé peut coordonner ce type d'attaque avec d'autres.

Dans l'espace TO, les attaques par des canaux auxiliaires peuvent servir à deviner le lien entre les signaux de commandes et leur effet sur le système, autant d'informations extrêmement précieuses pour un pirate.

Annexe C : Normes et autres ressources

La cybersécurité est un domaine en constante évolution. Comprendre les derniers risques, les tendances, les types d'attaques et la façon de réduire les répercussions des attaques est une approche essentielle pour toute organisation.

Normes et cadres

Les contrôles de cybersécurité essentiels du Centre pour la sécurité Internet (en anglais seulement)

Une norme élaborée par le Centre pour la sécurité Internet, qui se concentre sur les mesures de protection prioritaires pour réduire les risques de cybersécurité à l'aide de contrôles de gouvernance et techniques.

Cadre sur la cybersécurité du National Institute of Standards and Technology (en anglais seulement)

Ce cadre peut aider une organisation à créer ou à améliorer un programme de cybersécurité. Il s'agit des pratiques exemplaires pour aider les organisations à améliorer leur position en matière de cybersécurité. Le cadre est organisé en cinq fonctions clés : détermination, protection, détection, réaction et récupération.

Guide de sécurité des systèmes de contrôle industriels (SCI) du National Institute of Standards and Technology (en anglais seulement)

Ce guide offre notamment des directives sur la façon de sécuriser les systèmes de contrôle industriels, tout en répondant à leurs exigences uniques en matière de performance, de fiabilité et de sécurité. Le document fournit un aperçu des systèmes de contrôle industriels et des topologies de système typiques (la structure d'un réseau qui comprend la façon dont les différentes parties sont interconnectées), présente les menaces et les vulnérabilités typiques de ces systèmes et fournit des contre-mesures de sécurité recommandées pour réduire les risques.

Ingénierie de sécurité des systèmes du National Institute of Standards and Technology : Réflexions sur l'approche multidisciplinaire de l'ingénierie de systèmes fiables et sécurisés (en anglais seulement)

Cette publication explique la façon de développer des systèmes plus défendables et durablement inviolables. Il comprend les pièces mécaniques, physiques et humaines qui composent les systèmes et les capacités et services fournis par ces systèmes.

ISO/IEC/IEEE 15288 – Ingénierie des systèmes et du logiciel – Processus du cycle de vie du système (en anglais seulement)

Une norme qui aide les organisations à gérer les processus de développement de solutions et de maintenance des systèmes.

Ressources du gouvernement du Canada

Le Centre canadien pour la cybersécurité

Le **Centre canadien pour la cybersécurité** est l'autorité canadienne en matière de cybersécurité. Il réunit l'expertise en cybersécurité de Sécurité publique Canada, de Services partagés Canada et du Centre de la sécurité des télécommunications dans une seule organisation.

Cyberalertes

Le **Centre publie des alertes et des avis** lorsque des cybermenaces, des vulnérabilités ou des incidents possibles, imminents ou réels touchent ou pourraient toucher les infrastructures essentielles du Canada.

Documents d'orientation

Les experts en cybersécurité du Centre travaillent avec des partenaires, des services et des agences du secteur pour élaborer des **conseils sur la cybersécurité**. Ces documents d'orientation comprennent des recommandations et des mesures qu'une organisation peut mettre en œuvre pour protéger ses réseaux, ses systèmes et ses renseignements.

Cyberappel du secteur des transports

Pour vous joindre à la liste de distribution de l'équipe des partenariats avec le secteur des transports du Centre, merci d'envoyer un courriel à l'adresse **transport-par@cyber.gc.ca.**

Élaborer un plan d'intervention en cas d'incident (ITSAP.40.003)

Votre plan d'intervention en cas d'incident doit comprendre les processus, les procédures et les documents liés à la détection des incidents, à la réaction de votre organisation et à la reprise des activités.

Élaborer un plan de reprise des activités de TI (ITSAP.40.004)

Pour s'assurer qu'une organisation peut continuer à travailler avec un temps d'arrêt limité et dispose d'un plan de reprise des activités de TI dans le cadre de l'approche de continuité des activités. Dans le cadre de ce plan, une organisation doit déterminer les données, les applications et les processus critiques et définir la façon dont elle récupérera les services informatiques qui soutiennent les opérations, les produits et les services commerciaux.

Sécurité publique Canada

Communauté des systèmes de contrôle industriels (SCI)

Sécurité publique Canada organise des événements pour améliorer la résilience des systèmes de contrôle industriels.

Création d'un plan d'intervention en cas de cyberincident

Il est essentiel de pouvoir réagir aux cybermenaces de manière coordonnée et efficace. Un plan conjoint d'intervention en cas de cyberincident de TI/TO permet d'assurer que votre organisation

possède les compétences nécessaires pour réagir aux cybermenaces. Le document fournit une approche générale, ainsi que des facteurs particuliers à prendre en compte selon la taille, la fonction, l'emplacement et les spécificités sectorielles de l'organisation.

Transports Canada

Lignes directrices sur la cybersécurité des véhicules de Transports Canada

Ces lignes directrices établissent des principes directeurs neutres en matière de technologie pour renforcer la cybersécurité tout au long du cycle de vie d'un véhicule. Les principes de ces lignes directrices encouragent les organisations à :

- déterminer leur approche de gestion des risques sur le plan de la cybersécurité;
- protéger l'écosystème des véhicules au moyen de mesures appropriées;
- détecter et surveiller les événements touchant la cybersécurité et intervenir lorsque de tels événements surviennent;
- assurer une reprise rapide et sécuritaire de leurs activités et renforcer leur sécurité à la suite d'événements mettant en cause la cybersécurité.

Ressources du gouvernement des États-Unis

Département des Transports des États-Unis – Intelligent Transportation Systems Joint Program Office (ITS JPO) – Programme de recherche en cybersécurité STI (en anglais seulement)

Ce programme a été élaboré pour répondre au besoin imminent de protéger les STI des cyberattaques. L'objectif du programme est de partager des ressources, des renseignements et des outils avec les parties prenantes pour favoriser des STI sécurisés et cyberrésilients.

Cybersecurity and Intelligent Transportation Systems: A Best Practice Guide, Département des Transports des États-Unis (en anglais seulement) Guide des pratiques exemplaires (FHWA-JPO-19-763)

Ce rapport présente les pratiques exemplaires en matière de cybersécurité des STI, en particulier en matière de planification et de tests d'intrusion. Le rapport détaille la façon de définir un test, y compris les objectifs, les exigences, les critères de réussite, le type de test, la gestion et le degré de préparation au test. Le rapport comprend un modèle de plan d'essai pour aider le service de transport local et d'État à exécuter son propre plan de cybersécurité et ses propres tests d'intrusion.