CONSIDÉRATIONS EN MATIÈRE DE SÉCURITÉ POUR LES INFRASTRUCTURES ESSENTIELLES

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

AVRIL 2022 | ITSAP.10.100

Les infrastructures essentielles (IE) jouent un rôle dans la prestation et le soutien des nécessités la vie quotidienne. Elles comprennent des services couramment utilisés tels que l'eau, l'électricité et les finances. La perturbation de ces infrastructures essentielles pourrait mener à la perte de services essentiels, causer des torts à la population ou même se traduire par des pertes de vie. Le présent document explique les sources de compromission des secteurs des IE et les mesures de sécurité pouvant être mises en œuvre pour atténuer les risques.

DÉFINITION DES IE

On entend par infrastructures essentielles l'ensemble des processus, des systèmes, des installations, des technologies, des réseaux, des biens et des services nécessaires pour assurer la santé, la sûreté, la sécurité ou le bien-être économique des Canadiens et des Canadiennes ainsi que l'efficacité du gouvernement. Il s'agit souvent d'infrastructures autonomes ou caractérisées par des interdépendances au sein d'une province ou d'un territoire, entre eux ou au-delà des frontières du pays. La *Stratégie nationale sur les infrastructures essentielles* classe les IE en dix secteurs :

Énergie et services publics

Finances

Alimentation

Gouvernement

Santé

Technologies de l'information et de la communication

Secteur manufacturier

Sécurité

Transport

Eau

Les technologies opérationnelles (TO) et les systèmes de contrôle industriels (SCI) ciblés par des menaces

Les TO comprennent les systèmes informatiques servant à automatiser les opérations et les procédés industriels dans de nombreux secteurs, notamment le secteur manufacturier. Les SCI représentent un sous-ensemble important des TO qui permettent aux fournisseurs d'IE d'assurer la surveillance de leurs procédés à distance et de contrôler les dispositifs physiques dans leurs infrastructures.

Les TO et SCI qui sont connectés à Internet ou à d'autres réseaux et systèmes constituent des cibles de choix pour les auteurs de menace, dont l'objectif premier peut consister à perturber les TO ou les SCI, ou à les compromettre afin de les utiliser comme voie de distribution pour les stratagèmes d'hameçonnage, les pourriels et les attaques par maliciel.

MENACES PRINCIPALES POUR LES IE

L'appât du gain peut motiver des cybercriminels à cibler les secteurs des IE. Certains de ces secteurs, comme le secteur manufacturier et celui de la santé, représentent des cibles attrayantes puisque leurs propriétaires et exploitants ne peuvent pas tolérer une interruption prolongée des services essentiels et qu'ils disposent souvent de ressources financières considérables pour payer une rançon. Les auteurs de menace interne peuvent être mus par des motifs personnels et commettre, à titre d'exemple, des actes de vengeance parce qu'ils sont des clients ou d'anciens employés mécontents. Il se peut également que des auteurs de cybermenace parrainés par un État s'en prennent à des secteurs des IE pour recueillir de l'information qui appuie des objectifs stratégiques plus larges, comme influencer l'opinion publique ou l'élaboration de politiques.

Les cybermenaces visant les secteurs des IE peuvent entraîner le vol d'information essentielle à la mission, le verrouillage de fichiers sensibles ou la fuite de renseignements exclusifs ou compromettants. Voici quelques exemples parmi les cybermenaces les plus courantes :

Un **rançongiciel** est un type de maliciel qui empêche les utilisateurs d'accéder à des systèmes ou à des données jusqu'à ce qu'une rançon soit versée. D'autres types de maliciels (comme les effaceurs et les espiogiciels) sont employés pour infiltrer ou endommager les systèmes connectés des IE.

Un **déni de service (DoS pour Denial of Service)** désigne une activité visant à rendre un service inutilisable ou à ralentir l'exploitation et les fonctions d'un système. Un auteur de menace pourrait ainsi rendre indisponibles des parties substantielles d'un secteur des IE et causer des pannes potentiellement catastrophiques.

On entend par **menace interne** toute personne qui connaît l'infrastructure ou l'information d'une organisation, ou qui y a accès, et qui l'utilise, consciemment ou non, pour nuire à l'organisation. Les menaces internes pourraient avoir une incidence notable sur un secteur des IE et ses opérations.

Les dommages subis par les IE peuvent menacer la sécurité nationale, la sécurité publique et la stabilité économique

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada

CONSIDÉRATIONS EN MATIÈRE DE SÉCURITÉ POUR LES INFRASTRUCTURES ESSENTIELLES

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

AVRIL 2022 | ITSAP.10.100

RÉPERCUSSIONS

Les cyberattaques contre les IE peuvent avoir des conséquences graves et désastreuses, y compris les suivantes :

- l'interruption de services essentiels de base sur lesquels compte toute la population, comme l'électricité, l'eau et le gaz naturel
- l'interruption de l'approvisionnement en denrées alimentaires et en fournitures médicales, et l'interruption de leur production
- une perte de confiance générale du public à l'égard de l'économie, de la sécurité et de la défense nationales, ainsi que des processus démocratiques
- des dommages à l'environnement et des risques pour la santé publique découlant de déversements chimiques ou toxiques, ou d'émissions atmosphériques dangereuses
- des pertes de revenus, des atteintes à la réputation, des pertes d'emplois ou des conséquences juridiques (p. ex., la responsabilité quant à une atteinte à la vie privée) pour les entreprises et les employés
- la perturbation des opérations dans un hôpital, ou même la compromission d'appareils médicaux, ce qui pourrait entraîner des pertes de vie

POUR EN SAVOIR PLUS

Consultez notre site Web (cyber.gc.ca) pour accéder à une gamme de publications liées à la cybersécurité, notamment :

- Facteurs relatifs à la sécurité à considérer pour les systèmes de contrôle industriels (ITSAP.00.050)
- Protéger l'organisme contre les maliciels (ITSAP.00.057)
- Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information (ITSM.10.089)
- La virtualisation de votre infrastructure (ITSAP.70.011)
- Système d'adressage par domaine de protection (ITSAP.40.019)
- Sauvegarder et récupérer vos données (ITSAP.40.002)
- Guide sur les rançongiciels (ITSM.00.099)
- Ne mordez pas à l'hameçon : Reconnaître et prévenir les attaques par hameçonnage (ITSAP.00.101)
- Sauvegarder et récupérer vos données (ITSAP.40.002)
- Rançongiciels : comment les prévenir et s'en remettre (ITSAP.00.099)
- Sécurisez vos comptes et vos appareils avec une authentification multifacteur (ITSAP.30.030)
- Offrir aux employés une formation sur mesure en cybersécurité (ITSAP.10.093)
- Comment protéger votre organisation contre les menaces internes (ITSAP.10.003)

MESURES VISANT À PROTÉGER VOTRE SECTEUR DES IE CONTRE LES CYBERATTAQUES

Les opérateurs réseau des IE peuvent réduire les risques de cyberattaque en appliquant les mesures de sécurité suivantes. Pour obtenir de plus amples renseignements sur les mesures d'atténuation, veuillez consulter l'avis de la CISA (en anglais seulement).

Isolez les composants et les services d'IE en mettant en place des coupe-feux, des réseaux privés virtuels (RPV) et l'authentification multifacteur (MFA pour Multi-Factor Authentication) pour les connexions d'accès distant aux réseaux organisationnels. Mettez à l'essai les contrôles manuels des SCI pour garantir que les fonctions essentielles demeurent opérationnelles si votre réseau devenait indisponible ou non fiable. Utilisez des postes de travail administratifs sécurisés pour séparer les tâches et les comptes de nature délicate des utilisations non administratives telles que le courrier électronique et la navigation Web. Mettez en œuvre des zones de sécurité de réseau pour contrôler les accès et les flux de données de manière à les restreindre aux composants et utilisateurs autorisés. *Préparez-vous à isoler d'Internet les composants et services d'IE en cas de menace imminente.*

Améliorez votre posture de sécurité en appliquant automatiquement des correctifs à vos systèmes d'exploitation et à vos applications. Remplacez les appareils et les produits à la fin de leur vie utile. Mettez en place des sauvegardes hors ligne qui font l'objet de tests fréquents pour assurer un prompt rétablissement en cas d'incident.

Protégez votre réseau contre les maliciels en le virtualisant afin d'empêcher la propagation des maliciels dans vos réseaux organisationnels. Assurez la surveillance des réseaux et des points d'extrémité au moyen de logiciels antivirus et antimaliciels qui sont configurés de manière sécurisée, et activez les coupe-feux logiciels sur les appareils connectés.

Élaborez un plan d'intervention en cas d'incident qui comprend les processus, les procédures et les documents liés aux mesures de détection, d'intervention et de reprise que doit prendre votre organisation en cas de cyberattaque. Mettez à l'essai le plan périodiquement et apportez-y des ajustements au besoin pour assurer la continuité des fonctions et des opérations essentielles advenant des interruptions imprévues ou des perturbations système.

Donnez de la formation à vos employés pour les aider à comprendre l'importance des pratiques exemplaires en matière de cybersécurité telles que l'identification des courriels et des liens malveillants, l'utilisation de phrases de passe ou de mots de passe robustes, et le signalement des incidents dès qu'ils sont détectés.

Surveillez les activités organisationnelles en recueillant, en analysant et en conservant les données qui sont associées aux activités que mènent les utilisateurs sur les systèmes d'information. Activez la journalisation pour faciliter les enquêtes sur les problèmes et les événements. Assurez la surveillance du trafic sur vos passerelles Internet et établissez la base de référence des tendances suivies par le trafic normal. Les auteurs de menace dotés de moyens sophistiqués peuvent influencer certains employés ou leur forcer la main (à l'aide de techniques de piratage psychologique, de corruption, de chantage, d'intimidation, etc.) pour qu'ils les aident à compromettre la sécurité. Vous pouvez vous défendre contre ces auteurs en intensifiant la surveillance des menaces internes et en envisageant d'appliquer la règle de l'intégrité assurée par deux personnes lorsque des fonctions administratives essentielles sont réalisées.

Centre de la sécurité des télécommunications
Communications Security Establishment

 No de cat.D97-1/10-100-2022F-PDF ISBN 978-0-660-42804-8

Canada