Protéger vos technologies opérationnelles

Juillet 2022 **ITSAP.00.051**

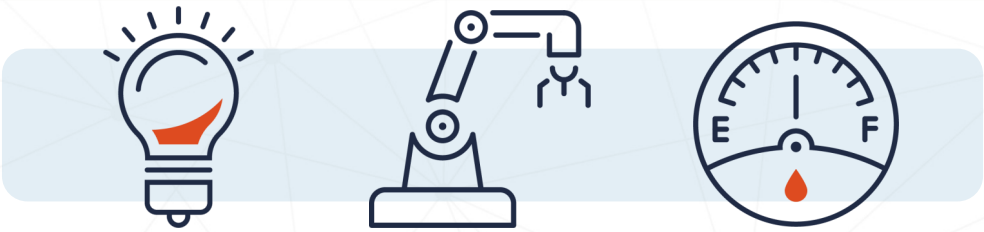
Les technologies opérationnelles (TO) sont essentielles à la gestion des infrastructures essentielles (IE) du Canada. Les TO désignent le matériel et les logiciels utilisés pour surveiller et changer des processus qui affectent le monde physique. Le présent document contient de l'information sur les risques liés aux TO et les mesures de sécurité que vous pouvez prendre pour réduire les risques de cybermenaces.

Comment fonctionnent les TO?

On utilise les TO pour contrôler et automatiser les processus industriels dans de nombreux secteurs (p. ex. la fabrication, l'extraction de ressources et les services essentiels). Auparavant, les TO consistaient en des systèmes hors ligne de contrôle des processus industriels, mais elles intègrent maintenant le traitement des données et les protocoles de communication des technologies de l'information (TI) afin que les opérations soient sécuritaires et efficaces. Les systèmes de TO sont de plus en plus connectés aux réseaux de TI et potentiellement à Internet, ce qui accroit la possibilité que des cyberattaques surviennent.

Les systèmes de contrôle industriels (SCI) sont des TO spécialisées qui surveillent et contrôlent des processus industriels. Les SCI peuvent détecter et changer l'état physique d'un équipement industriel afin de livrer le produit ou le service approprié.

Les systèmes cyberphysiques (SCP) sont des TO avancées qui contrôlent et surveillent les systèmes physiques au moyen d'algorithmes informatiques. Les SCP intègrent la gestion de procédés informatiques, physiques et de réseautage aux IE, de sorte à créer des systèmes intelligents qui mesurent et contrôlent le monde physique pour atteindre des objectifs.



Quels sont les risques?

Les TO accordent la priorité à la sécurité personnelle et à la fiabilité des processus avant la sécurité des données. Des systèmes ou des dispositifs de TO compromis peuvent exposer les processus essentiels à des défaillances. Selon les ressources disponibles et l'intensité de l'attaque, vos TO pourraient arrêter des processus et les forcer à fonctionner manuellement (c.-à-d. que des systèmes d'exploitation fonctionneraient sans processus automatisé). La compromission de vos TO peut entraîner les conséquences suivantes :

- Défectuosité de l'équipement et perturbation des processus et des produits livrables;
- Compromission de la propriété intellectuelle et de l'information sensible (p. ex. des données financières ou de clients);
- Perte de revenu en raison de la perturbation des processus, de réparations coûteuses et du paiement d'une rançon;
- Atteinte à la crédibilité de l'organisation;
- Compromission des mesures de sécurité (p. ex. services d'urgence);
- Accidents et désastres majeurs (p. ex. blessure ou perte de vie).

La panne d'un dispositif de TO peut entraîner des répercussions sur l'ensemble d'un processus industriel et la sécurité des exploitants. L'objectif des auteurs de menace est de frapper là où ils savent que la destruction et la perte de services peuvent provoquer des dommages importants aux systèmes, aux processus et aux infrastructures de grande valeur.

SÉRIE SENSIBILISATION

No de cat. D97-1/00-051-2022F-PDF
ISBN 978-0-660-44027-9

Quelles sont les menaces?

Les cybermenaces contre les TO peuvent affecter les IE du Canada et d'autres processus importants. Voici quelques exemples parmi les cybermenaces les plus courantes :

- **Accès à distance :** Si vos TO sont connectées à un réseau de TI ou à Internet, les cybercriminels peuvent en prendre le contrôle à distance de différentes façons.
- **Rançongiciel :** Il s'agit d'un type de maliciel qui empêche un utilisateur légitime d'accéder à des ressources (systèmes ou données) jusqu'à ce qu'il ait payé une rançon.
- **Maliciel :** Il s'agit d'un logiciel malveillant conçu pour infiltrer ou endommager un système informatique sans le consentement du propriétaire.
- **Menace interne :** On entend par une menace interne toute personne qui connaît l'infrastructure ou l'information de votre organisation, ou qui y a accès, et qui utilise, consciemment ou non, ses connaissances ou son accès pour nuire à l'organisation.
- **Attaque par déni de service (DoS pour *Denial of Service*) :** Cette menace désigne des activités visant à rendre des services inutilisables ou à ralentir l'exploitation et les fonctions d'un système.

Grâce à ces attaques, les cybercriminels peuvent obtenir un accès qui leur permet de manipuler des données dans des systèmes (p. ex. changer des calculs ou la façon dont s'affiche l'information) en vue de présenter de l'information fausse ou d'affecter les systèmes connectés.

Voici certaines vulnérabilités contre lesquelles votre organisation peut prendre des mesures :

- **Systèmes périmés ou en fin de vie :** Des dispositifs ne sont plus pris en charge et mis à jour.
- **Logiciels et micrologiciels non corrigés :** Des systèmes et des dispositifs sont vulnérables aux menaces connues.
- **Périphériques :** Des dispositifs externes connectés peuvent servir à compromettre des systèmes et des réseaux.

En plus de ces menaces, les cybercriminels continuent d'évoluer et de peaufiner leurs méthodes d'attaque.

Comment protéger vos TO?

Voici quelques pratiques exemplaires en matière de cybersécurité afin de protéger vos TO :

Mettre à l'essai le mode manuel :
Mettez à l'essai vos systèmes et vos processus en mode manuel. Mettez en place un plan d'intervention en cas d'incident afin d'optimiser vos systèmes si certaines TO doivent être déconnectées d'Internet. Préparez-vous à isoler d'Internet les composants et les services de TO en cas de menace imminente.

Surveiller et journaliser :
Surveillez les systèmes et l'équipement au moyen de journaux d'audit en vue de détecter les vulnérabilités et les points d'accès pour les attaques. La surveillance des points d'entrée vous permet d'empêcher les attaques de se propager.

Appliquer les mises à jour et les correctifs :
Par l'intermédiaire d'une approche fondée sur les risques, déterminez les TO qui nécessitent une mise à jour. Il est essentiel d'évaluer vos TO afin de vous assurer que les mises à jour ne diminuent pas la fiabilité de vos TO et de vos systèmes connectés.

Isoler les processus système :
Mettez en place des pare-feux, des réseaux privés virtuels (RPV) et l'authentification multifacteur sur les systèmes connectés à vos TO, y compris l'accès en travail à distance. Établissez des zones dans les réseaux afin de séparer les secteurs contenant des TO sensibles des réseaux d'accès à distance.

Appliquer le principe du droit d'accès minimal :
Assurez-vous que seules les personnes qui en ont besoin peuvent accéder aux TO. Employez l'authentification multifacteur et les contrôles d'intégrité par deux personnes (TPI pour *Two-Person Integrity*) sur les TO qui gèrent de l'équipement ou de l'information sensibles. Les contrôles TPI nécessitent deux personnes autorisées pour déverrouiller l'accès à des systèmes restreints.

Que faire si mes TO sont compromises?

Si vos TO et vos systèmes connectés sont compromis par des auteurs de menace, prenez les mesures suivantes :

1. Évaluer les conséquences sur l'équipement et déconnecter les systèmes d'Internet, dans la mesure du possible, afin d'empêcher que l'attaque se propage.
2. Consulter les journaux d'audit pour détecter l'attaque et déterminer les systèmes et les comptes connectés qui pourraient être affectés.
3. Déconnecter et isoler les comptes, les TO et les systèmes affectés des processus qui sont contrôlés, si possible.
4. Demander à votre équipe de TI de réparer l'équipement endommagé et de le balayer pour déceler les menaces résiduelles.
5. Appliquer les correctifs et les mises à jour aux TO afin que les versions logicielles appropriées permettent le bon fonctionnement des TO.
6. Signaler l'incident au Centre pour la cybersécurité et à la Gendarmerie royale du Canada (GRC), selon la nature de l'incident et sa gravité.

Renseignements supplémentaires

Visitez le site Web du Centre pour la cybersécurité pour trouver des publications connexes :

- *Facteurs relatifs à la sécurité à considérer pour les systèmes de contrôle industriels (ITSAP.00.050)*
- *Considérations en matière de sécurité pour les infrastructures essentielles (ITSAP.10.100)*
- *Rançongiciels : comment les prévenir et s'en remettre (ITSAP.00.099)*
- *Comment protéger votre organisation contre les menaces internes (ITSAP.10.003)*
- *Protéger l'organisme contre les maliciels (ITSAP.00.057)*
- *Protéger son organisation contre les attaques par déni de service (ITSAP.80.100)*
- *Gestion et contrôle des privilèges administratifs (ITSM.10.094)*
- *Sécurisez vos comptes et vos appareils avec une authentification multifacteur (ITSAP.30.030)*
- *Exigences de base en matière de sécurité pour les zones de sécurité de réseau (Version 2.0) (ITSP.80.022)*
- *Les outils de sécurité préventive (ITSAP.00.058)*