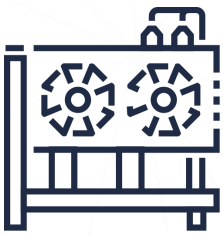
FACTEURS RELATIFS À LA SÉCURITÉ À CONSIDÉRER POUR LES SYSTÈMES DE CONTRÔLE INDUSTRIELS

JUILLET 2021 ITSAP.00.050

Un système de contrôle industriel (SCI) automatise et contrôle les processus industriels (p. ex. la fabrication, la manutention des produits, la production et la distribution) et les fonctions mécaniques pour s'assurer que les processus et la machinerie fonctionnent sans problème. Il peut aussi appuyer les infrastructures essentielles (p. ex. les secteurs de l'énergie et des services publics, des transports, de la santé, de l'alimentation et de la gestion de l'eau, et le secteur manufacturier) nécessaires à la sécurité et au bien-être des Canadiens et des Canadiennes. Comme un SCI est le contrôleur de base pour les autres couches d'une infrastructure (c.-à-d. de production, de bureautique et d'entreprise), il doit être sécurisé pour en assurer le fonctionnement. Ce document présente certains risques et menaces en matière de sécurité liés aux SCI et les mesures de sécurité que vous pouvez mettre en place pour protéger ces systèmes.

QU'EST-CE QU'UN SCI?



Le terme « système de contrôle industriel » regroupe plusieurs types de systèmes de contrôle comme les systèmes numériques de contrôle-commande, les systèmes de télésurveillance et d'acquisition de données, et les automates programmables industriels. Un SCI met en place des processus et des contrôles pour atteindre un objectif industriel. Les systèmes peuvent être complètement automatisés ou comporter des éléments de contrôle nécessitant une intervention humaine. Que votre SCI gère un système de contrôle plus simple ou un réseau de systèmes complexes, vous devez le sécuriser pour protéger l'intégrité et la disponibilité des processus industriels.

Si les SCI traditionnels n'étaient pas interconnectés avec un aussi grand nombre de systèmes et de réseaux, il serait possible de les isoler et de les sécuriser physiquement. Ces appareils hérités étaient seulement accessibles à distance par un compte d'accès unique que les utilisateurs employaient pour gérer le système à partir de leur réseau domestique ou d'autres réseaux. Le système était donc vulnérable aux cybermenaces, puisqu'il ne permettait pas de surveiller les utilisateurs.

QUELLES SONT LES MENACES PRINCIPALES?

Votre SCI est une cible de choix pour les auteurs de menace, puisque ces derniers peuvent en tirer avantage pour avoir de réelles répercussions sur la population, que ce soit en causant de petits désagréments (p. ex. allumer et éteindre les lumières) ou en provoquant des incidents ou susceptibles d'entraîner des coûts importants ou de poser un danger à la vie humaine (p. ex. entraîner la défaillance de l'équipement ou des dommages permanents). Les auteurs de menace mènent des attaques ciblées pour compromettre directement votre organisation ou des attaques non ciblées pour propager un maliciel dans le but de compromettre les systèmes, le cas échéant. Certaines des principales cybermenaces touchant votre SCI peuvent inclure entre autres les menaces ci-dessous.

RANÇONGICIELS

Un auteur de menace implante un maliciel par un point d'entrée dans le système (p. ex. hameçonnage, menace interne ou piratage ciblé) afin de restreindre l'accès à toutes les fonctions jusqu'au paiement de la rançon.

MENACE INTERNE

Quiconque a accès au SCI peut causer des dommages au système, que ce soit intentionnellement (p.ex. compromission des données pour obtenir un gain personnel) ou involontairement (p. ex. traiter sans le savoir l'équipement de façon inappropriée).

ATTAQUES PAR DÉNI DE SERVICE (DoS)

Un auteur de menace attaque votre système rendant les services inaccessibles aux utilisateurs prévus. Des attaques par DoS peuvent retarder l'exécution des fonctions et des activités, ce qui oblige votre organisation à utiliser plus de ressources pour assurer la reprise des activités.

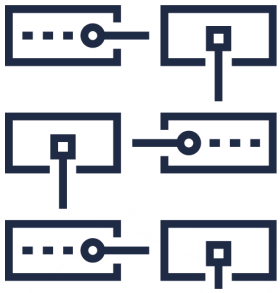
Si votre SCI n'est pas adéquatement sécurisé, il est plus vulnérable aux cybermenaces. Les parties de votre SCI qui ne sont pas bien configurées ou qui sont connectées à un réseau privé virtuel (RPV) non corrigé peuvent donner lieu à un plus grand nombre de vulnérabilités sur le plan de la sécurité. Si vous avez de l'équipement distant qui accède à votre SCI, faites preuve de vigilance quand vous y avez recours. En raison de la récente augmentation du nombre de télétravailleurs, l'accès à distance et les technologies distantes sont devenus une cible attrayante pour les auteurs de menace. S'ils arrivent à compromettre votre équipement et vos dispositifs distants (p. ex. par un maliciel), les auteurs de menace peuvent mener plus d'attaques sur le SCI et causer la perte d'information, endommager l'équipement ou provoquer des incidents susceptibles de poser un danger à la vie humaine.

SÉRIE SENSIBILISATION

No de cat. D97-1/00-050-2021F-PDF
ISBN 978-0-660-39675-0

QUELS SONT LES RISQUES?

Si votre SCI est compromis, votre organisation peut être vulnérable à ce qui suit :



- Un flux d'information bloqué ou ralenti par les réseaux du SCI ayant une incidence sur les activités du SCI (p. ex. interruption de l'alimentation de génération d'énergie);
- Des changements non autorisés aux instructions et aux commandes qui endommagent ou désactivent l'équipement;
- L'envoi d'information erronée aux opérateurs causant des changements non autorisés et l'exécution d'actions non appropriées;
- L'infection d'un logiciel du SCI se propageant sur le réseau et les appareils de votre organisation;
- Un mauvais fonctionnement des opérations qui mène à la perte de données ou de profits, et nuit à votre réputation (p. ex. une panne de courant à une centrale électrique causera une série d'interruptions touchant toutes les connexions).

COMMENT PUIS-JE SÉCURISER MON SCI?

Pour atténuer les risques, votre organisation doit mettre en place les mesures de sécurité et les pratiques exemplaires de l'industrie ci-dessous.

ISOLER LE SYSTÈME

Isolez le SCI des fonctions habituelles de l'organisation. Connectez-le à un réseau différent afin que vous puissiez le déconnecter d'Internet sans interrompre les autres activités organisationnelles (p. ex. de bureau et d'entreprise).

GÉRER LES ACCÈS ET LES PRIVILÈGES

L'accès aux systèmes utilisés pour maintenir et gérer les systèmes industriels doit être confié à des utilisateurs autorisés qui s'en serviront aux fins prévues. L'accès à distance au système doit être considéré et évalué soigneusement en fonction des risques prévus (p. ex. un sous-traitant a besoin d'accéder à un système pour un temps limité afin de mener à bien ses tâches).

Créez des comptes individuels à authentification multifacteur et utilisez le chiffrement pour restreindre l'accès non autorisé aux données sensibles.

FORMER LES EMPLOYÉS

Formez les employés de manière à ce qu'ils connaissent vos processus de sécurité. Créez des exercices d'apprentissage sur les différentes tactiques de sécurité et mettez l'accent sur l'importance de maintenir une communication continue. Les utilisateurs qui accèdent au SCI doivent comprendre pourquoi certaines mesures de sécurité sont en place afin de ne pas les désactiver.

JOURNALISER ET SURVEILLER

Activez la journalisation et la surveillance de tous les accès et de toute l'information sur les événements. En cas de mauvais fonctionnement de votre système ou d'attaque, les journaux de vérification recueilleront l'information sur l'événement (p. ex. qui a eu accès au système, quelles mesures ont été prises, quels changements ont été effectués).

UTILISER DES LOGICIELS ET DU MATÉRIEL DE SÉCURITÉ

Protégez votre SCI contre les intrusions malveillantes et les infections par maliciel en utilisant un logiciel antivirus et des pare-feux. Analysez tous les supports amovibles avant de les connecter à votre SCI afin de réduire les risques qu'un maliciel caché infecte votre système.

Utilisez un RPV pour protéger les données transmises.

Si vous avez les ressources nécessaires pour le faire, mettez en place une passerelle de sécurité unidirectionnelle pour contrôler les cybermenaces externes. Cet outil est une solution de rechange robuste au pare-feu et doit être configuré adéquatement par une équipe de spécialistes des TI.

SAUVEGARDER VOS SYSTÈMES

Sauvegardez vos systèmes et vos données régulièrement, et préférablement hors ligne. Même s'il convient de procéder à la sauvegarde des données chiffrées en ligne, vous devez stocker ces sauvegardes hors ligne. Les sauvegardes permettent d'assurer la récupération rapide de vos systèmes en cas d'incident ou de panne imprévue.

METTRE À JOUR ET REMPLACER SI POSSIBLE

Appliquez les mises à jour et les correctifs à vos systèmes pour corriger les vulnérabilités de sécurité et maintenir leurs fonctionnalités.

Si possible, remplacez les systèmes qui ne sont plus pris en charge et les pièces périmées au sein de votre organisation et sur votre SCI. Puisqu'un SCI doit fonctionner continuellement, il est possible que vous ne soyez pas en mesure de retirer un dispositif pour faire les mises à jour matérielles. Si c'est le cas, votre organisation doit évaluer et approuver le niveau de tolérance au risque et mettre en place d'autres mesures de sécurité pour améliorer la sécurité du SCI.

POUR EN SAVOIR PLUS

Pour en savoir plus sur la sécurité liée au SCI, consultez la publication *SP 800-82 Rev. 2, Guide to Industrial Control Systems (ICS) Security* de la National Institute of Standards and Technology.

Consultez notre site Web (cyber.gc.ca) pour obtenir notre liste de publications liées à la cybersécurité, ce qui comprend notamment :

- *ITSAP.00.099 – Rançongiciels : comment les prévenir et s'en remettre*
- *ITSAP.00.101 – Ne mordez pas à l'hameçon : Reconnaître et prévenir les attaques par hameçonnage*
- *ITSAP.10.003 – Comment protéger votre organisation contre les menaces internes*
- *ITSAP.70.011 – La virtualisation de votre infrastructure*
- *ITSAP.10.094 – Gestion et contrôle des privilèges administratifs*
- *ITSAP.10.093 – Offrir aux employés une formation sur mesure en cybersécurité*
- *ITSAP.00.057 – Protéger l'organisme contre les maliciels*
- *ITSAP.40.002 – Sauvegarder et récupérer vos données*
- *ITSAP.10.096 – Application des mises à jour sur les dispositifs*

Vous avez des questions ou vous avez besoin d'aide? Vous voulez en savoir plus sur les questions de cybersécurité? Consultez le site Web du Centre canadien pour la cybersécurité (Centre pour la cybersécurité) à **cyber.gc.ca**.