CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Passer à une approche axée sur la cyberrésilience

May 2024 ITSAP.10.190

La cyberrésilience est la capacité d'anticiper des conditions défavorables et des compromissions sur les systèmes dont l'utilisation et le fonctionnement dépendent de cyberressources, de résister et de s'adapter à ceux-ci et de reprendre ses activités.

Une approche axée sur la cyberrésilience tient compte de la sécurité selon l'angle d'un système de systèmes et reconnaît la complexité associée à la planification et à l'intervention. La collaboration entre les éléments d'un système, comme les plateformes informatiques, les réseaux, les applications d'entreprise, les personnes et les processus est essentielle à cette approche.

Le Centre pour la cybersécurité se concentre sur la cyberrésilience en tant qu'approche pouvant aider les propriétaires et les exploitants de systèmes de TI qui appuient les activités opérationnelles à atténuer les potentielles répercussions d'un cyberévénement. La technologie opérationnelle (TO) et les systèmes de contrôle industriels (SCI) sont de plus en plus connectés à Internet et leur fonctionnement devient dépendant des systèmes de TI. Une approche axée sur la cyberrésilience peut aider les propriétaires et exploitants d'infrastructures essentielles (IE) à accroître la sécurité de leur TO et de leurs SCI.

Comment passer à une approche axée sur la cyberrésilience

Les aspects suivants peuvent aider votre organisation à passer à une approche axée sur la cyberrésilience.

1. **Collaboration et gouvernance:** Mettez en œuvre de bons mécanismes d'engagement et de gouvernance qui définissent clairement les rôles et responsabilités. Assurez la participation des principales parties prenantes en vous accordant sur des objectifs et en tâchant d'atteindre une vision commune. Faites participer des partenaires non traditionnelles et non traditionnels, comme des spécialistes des secteurs en sécurité et gestion de TO, planification de continuité des activités, reprise après catastrophe, organisations de la société civile, et autres communautés, comme les communautés rurales, éloignées ou autochtones.

2. **Compréhension des risques:** Déterminez vos fonctions, systèmes et actifs essentiels ainsi que leurs dépendances. Comprenez vos capacités actuelles à protéger ces éléments, réduire la probabilité qu'une compromission survienne, et établir la priorité des façons de minimiser les répercussions éventuelles d'un cyberévénement. Intensifiez l'échange d'information entre les parties prenantes en vue d'améliorer la compréhension globale de l'environnement de menaces dans votre secteur.

3. **Prévention et attenuation:** Déterminez, élaborez et mettez en œuvre des initiatives et des solutions permettant de vous adapter aux risques liés à la cybersécurité ou les atténuer. Pour ce faire, vous pouvez accroître la robustesse, la redondance, l'adaptabilité et la rapidité de reprise de vos systèmes.

4. **Préparation, détection et intervention en cas d'incident:** Mettez en œuvre les capacités requises pour détecter les cyberincidents sur vos systèmes. Veillez à avoir des formations, des plans de reprise et des ressources efficaces afin d'intervenir en cas d'incident et de minimiser les répercussions d'un incident.

5. **Reprise axée sur l'avenir:** Tirez des leçons des cyberincidents et communiquez-les avec d'autres parties prenantes afin d'encourager une culture d'échange d'information proactif sur les menaces. Servez-vous des cyberincidents comme d'une occasion de corriger les lacunes sous-jacentes et de réduire les vulnérabilités afin d'accroître votre résilience après l'événement.

SÉRIE SENSIBILISATION

No de cat. D97-1/10-190-2024F-PDF
ISBN 978-0-660-71816-3

Canada

Pourquoi la cyberrésilience est importante pour votre organisation

L'interconnectivité et les dépendances entre les secteurs, comme l'énergie, les finances, les télécommunications et les transports, accroissent le potentiel que les répercussions soient plus grandes et successives lorsqu'un incident survient. Les systèmes physiques et de TI ont convergé de façon à remettre en question les approches traditionnelles en sécurité dans ces domaines, ce qui ajoute une nouvelle couche de complexité. Une approche axée sur la cyberrésilience tient compte des connexions et des dépendances accrues entre les systèmes et aide à atténuer les risques de répercussions successives entre les secteurs, les menaces en évolution et les changements dans l'environnement.

Les IE sont employées pour appuyer beaucoup des services qu'utilisent les Canadiennes et Canadiens tous les jours. Comme il est noté dans l'Évaluation des cybermenaces nationales, la cyberrésilience des systèmes des IE est cruciale et est de plus en plus à risque de devenir la cible d'auteures et auteurs de cybermenace. Toute perturbation de la confidentialité, de l'intégrité ou de la disponibilité des systèmes essentiels entraînera de grandes répercussions sur les processus industriels, la clientèle desservie et l'économie.

Les auteures et auteurs de menace et ceux parrainés par des États ciblent les IE dans le but d'obtenir un gain financier, de provoquer des perturbations et de recueillir de l'information en se livrant à de l'espionnage. Pour ce faire, ils se prépositionnent en injectant des implants malveillants dans les systèmes des IE. Certains implants ont pour objectif l'espionnage aux fins d'exfiltration d'information. D'autres sont en état de latence comme capacité pouvant servir à provoquer des perturbations dans l'avenir.

Avantages de la cyberrésilience

- Meilleure compréhension des menaces et des risques contre les systèmes des IE, qui permet de faire des investissements efficaces dans la cyberdéfense
- Prise de mesures proactives afin de restaurer et de récupérer les fonctions essentielles ainsi que de réduire la période d'indisponibilité, les coûts et les répercussions de l'interruption
- Meilleures capacités de cyberdéfense, qui font en sorte qu'il est plus difficile de créer des interruptions dans les systèmes des IE
- Coordination de la réponse, de l'état de préparation et des communications, de sorte à améliorer la confiance du public lorsqu'un cyberincident survient
- Cyberrésilience des systèmes des IE, qui améliore la sécurité nationale en minimisant les risques de répercussions successives entre les secteurs.

La National Institute of Standards and Technology (NIST) des États-Unis a également publié des conseils visant l'adoption d'une approche axée sur l'ingénierie en sécurité des systèmes pour développer des systèmes cyberrésilients. Cette approche partage des objectifs semblables aux conseils sur la résilience du Centre pour cybersécurité et fait référence à des contrôles de sécurité pertinents.

Pour en savoir plus sur les contrôles de sécurité et les approches axées sur la cyberrésilience, consultez le document NIST SP 800-160 Vol.2 Rev.1: Developing Cyber-Resilient Systems: A Systems Security Engineering Approach (en anglais seulement) et le document de l'International Organization for Standardization, intitulé Security and resilience: Organizational resilience - Principles and attributes (ISO 22316:2017) (en anglais seulement).

Pour en savoir plus

- La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie (ITSG-33)
- Un cadre de sécurité civile pour le Canada
- Stratégie de sécurité civile pour le Canada : Vers un 2030 marqué par la résilience
- Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information (ITSM.10.089)
- Considérations en matière de sécurité pour les infrastructures essentielles (ITSAP.10.100)
- Protect your operational technology (ITSAP.00.051)