CANADIAN CENTRE FOR CYBER SECURITY

Avis et conseils pour les petites et moyennes organisations

1 Évaluations des menaces

Les liens suivants mènent à des évaluations de menaces récentes et pertinentes.

1. Évaluation des cybermenaces nationales
2. Incidence continue de la COVID-19 sur les activités de cybermenaces
3. Les cyberattaques visant le secteur canadien de l'électricité
4. La menace des rançongiciels en 2021
5. Les cybermenaces visant les technologies opérationnelles
6. Cybermenaces provenant de la Russie et de l'Ukraine
   - Le CCC exhorte les exploitants des infrastructures essentielles du Canada à prendre conscience des activités de cybermenace connues qui sont parrainées par la Russie et à prendre des mesures d'atténuation contre celles-ci
   - Le CCC rappelle aux exploitants des infrastructures essentielles du Canada de prendre conscience des activités de cybermenace connues qui sont parrainées par la Russie et de prendre des mesures d'atténuation contre celles-ci

2 Publications

2.1 Rançongiciels

Les rançongiciels sont les cybermenaces les plus courantes qui guettent la population canadienne, et ils sont en hausse.
Ce lien offre des ressources du Centre pour la cybersécurité visant à aider les organisations à comprendre la menace que représentent les rançongiciels et à prendre les mesures appropriées pour se protéger.

Guide sur les rançongiciels

- Liste de vérification d'un plan d'intervention en cas d'incident
- Lignes directrices pour élaborer un plan de reprise
- Contrôles de sécurité pour réduire le risque lié aux rançongiciels
- Liste de vérification des mesures d'intervention immédiates et de reprise

Rançongiciels : comment les prévenir et s'en remettre
Rançongiciel : Comment vous en remettre

CANADIAN CENTRE FOR CYBER SECURITY

2.2 Éviter les attaques par hameçonnage

L'hameçonnage est actuellement la méthode la plus courante utilisée par les auteurs de menace pour déployer un rançongiciel. Les publications suivantes vous aideront à reconnaître et à éviter une attaque par hameçonnage.

Ne mordez pas à l'hameçon : Reconnaître et prévenir les attaques par hameçonnage
Les 7 signaux d'alarme de l'hameçonnage
Reconnaître les courriels malveillants

2.3 Sécuriser les dispositifs mobiles

Votre dispositif mobile vous offre une façon commode et souple de travailler n'importe où, n'importe quand. Les dispositifs mobiles jouent un rôle essentiel dans les activités quotidiennes des organisations et des organismes, mais leur utilisation représente aussi une menace pour l'information et les réseaux.

Utiliser son dispositif mobile en toute sécurité
Liste de conseils pour un nouvel appareil
Dispositifs mobiles et voyages d'affaires
Conseils sur les appareils mobiles à l'intention des voyageurs connus du public

2.4 Cybersécurité pour les petites et moyennes organisations (PMO)

Cherchez-vous des façons de protéger les réseaux et l'information de votre entreprise des cybermenaces?

Les meilleures mesures pour renforcer la cybersécurité des petites et moyennes entreprises
Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information
Contrôles de cybersécurité de base pour les petites et moyennes entreprises
Sécurisez vos comptes et vos appareils avec une authentification multifacteur
Élaboration d'un plan de reprise informatique personnalisé
Élaborer un plan d'intervention en cas d'incident
Sécurité de la chaîne d'approvisionnement pour les petites et moyennes organisations
La cybersécurité à la maison et au bureau
Protection de l'information de grande valeur : Conseils pour les petites et moyennes organisations

3 Évaluation de la situation en matière de cybersécurité

CANADIAN CENTRE FOR CYBER SECURITY

3.1 Outil canadien de cybersécurité (OCC)

L'Outil canadien de cybersécurité (OCC) est un outil virtuel et gratuit d'auto-évaluation conçu par Sécurité publique Canada (SP) en collaboration avec le Centre pour la cybersécurité. L'OCC présente au participant un aperçu de la résilience opérationnelle et de la situation en matière de cybersécurité de son organisation ainsi que des résultats comparatifs dans l'ensemble de son secteur.

https://www.securitepublique.gc.ca/cnt/ntnl-scrt/cbr-scrt/cbr-scrt-tl/index-fr.aspx

4 Formation sur la cybersécurité en ligne

4.1 CyberSécuritaire Canada

CyberSécuritaire Canada est un programme fédéral de certification pour les petites et moyennes organisations (PMO). CyberSécuritaire Canada offre une série de cours en ligne gratuits conçus pour aider les PMO à mettre en place des contrôles de cybersécurité de base et à améliorer leur situation en matière de cybersécurité.

https://www.ic.gc.ca/eic/site/137.nsf/fra/h_00017.html

5 Signalement des incidents de cybersécurité

Signalez les cybercrimes dans le portail en ligne du Centre pour la cybersécurité afin d'obtenir du soutien et des conseils pour protéger votre organisation et éviter de qu'elle devienne une cible.

Portail de signalement des cyberincidents

6 Produits du Centre pour la cybersécurité

Souhaitez-vous recevoir du renseignement sur les menaces, des alertes et des avis du Centre pour la cybersécurité? Envoyez un courriel à contact@cyber.gc.ca.