CSN

Informatique

SENSIBILISATION DES SYNDICATS DE LA FNCC À LA SÉCURITÉ INFORMATIQUE

CSN

CSN

Contexte

- Cette présentation fait suite à la demande de la FNCC de sensibiliser les syndicats au sujet de la sécurité informatique en lien avec les cybermenaces les plus courantes et les meilleures pratiques à mettre en place pour s'en défendre.

- Note: cette présentation est un outil de sensibilisations et ne constitue pas un guide complet et exhaustif de mise en place de tous les moyens à prendre pour assurer la sécurité des informations détenues par les syndicats.

CSN

Quelques questions aux syndicats

- Quelles informations détenez-vous au sujet de vos membres?
- Où ces informations sont-elles conservées?
- Pensez-vous que ces informations sont conservées en sécurité?
- Comment les protégez-vous?

CSN

Quelques rappels

- La protection des renseignements personnels des membres d'un syndicat découle notamment du droit à la vie privée et est couverte par plusieurs lois avec des degrés divers de contrainte.
- Les syndicats ont des obligations qui découlent de la *Loi sur la protection des renseignements personnels dans le secteur privé (LPRPSP)* quant aux renseignements personnels de ses membres en sa possession.
- La loi s'applique, peu importe le médium ou le support sur lequel l'information est conservée ou détenue.

CSN

Quelques rappels

- L'accès aux renseignements personnels des membres doit être limité aux personnes pour qui ces renseignements sont nécessaires uniquement.
- Le syndicat doit prendre les mesures de sécurité nécessaires pour assurer la protection des renseignements personnels de leurs membres.
- Nécessité de se prémunir contre :
  - la perte,
  - le vol,
  - la communication,
  - la consultation,
  - la copie ou
  - la modification non autorisée de renseignements personnels.

CSN

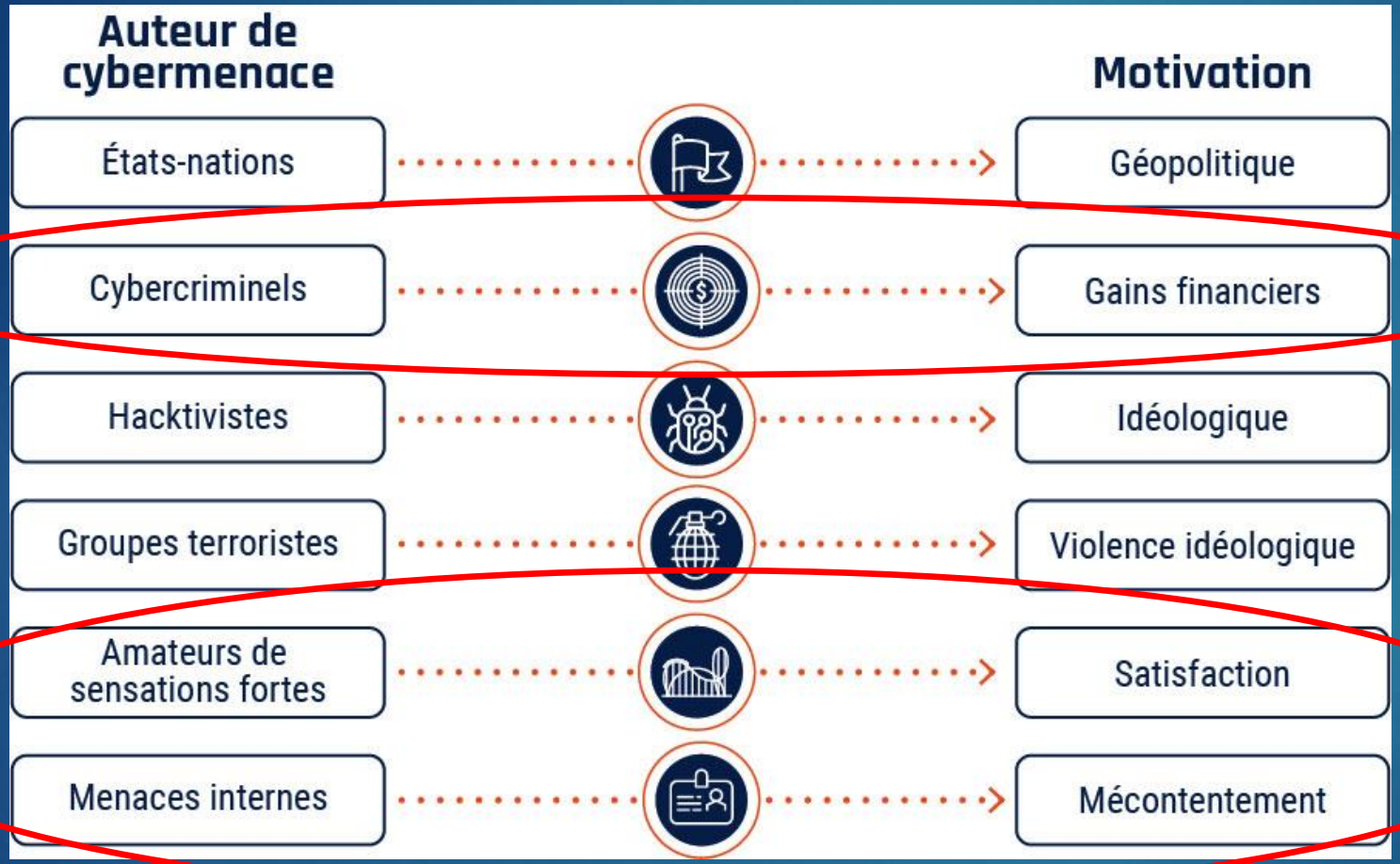
Définition d'une cybermenace

- Une cybermenace est une activité qui vise à compromettre la sécurité d'un système d'information en altérant la disponibilité, l'intégrité ou la confidentialité d'un système ou de l'information qu'il contient, ou à perturber le monde numérique en général.

Référence : introduction à l'environnement de cybermenace isbn 978-0-66045951-6

CSN

Les auteurs de cybermenace



Méthodes utilisées :

- **Piratage psychologique**
- **Exploitation des vulnérabilités**

Les plus probables pour les organisations syndicales

Référence : introduction à l'environnement de cybermenace isbn 978-0-66045951-6

CSN

Piratage psychologique

- Hameçonnage et harponnage
  - L'auteur conçoit un courriel ou message texte destiné à tromper la vigilance de l'utilisateur et tentant de lui soutirer des informations.
  - Vidéo d'information hameçonnage
- Mystification
  - L'auteur conçoit des sites web semblables à des sites web d'organisations connues permettant de saisir des informations personnelles.
- Compromission de courriel d'affaires
  - L'auteur conçoit un courriel au nom d'un responsable de l'organisation demandant un transfert d'argent au responsable financier.

Exploitation des vulnérabilités

- Programmes malveillants
  - Programmes permettant d'exploiter les vulnérabilités des dispositifs (ordinateurs et logiciels) en installant un logiciel à risque compromettant le système informatique.

Actions possibles :

- ❑ *Bloquer l'accès à l'information (ransomware)*
- ❑ *Installation de logiciels nuisibles et indésirables*
- ❑ *Obtenir discrètement des informations (logiciel espion)*
- ❑ *Perturber la fonctionnalité du système*

Exploitation des vulnérabilités (autres)

- Attaque de déni de service
- Attaque de l'intercepteur
- Injection SQL
- Exploit du jour zéro

CSN

Meilleures pratiques de sécurité (volet administratif)

- Nommer un responsable de la sécurité et identifier les actifs informationnels
- Créer un plan de réponse aux incidents de sécurité incluant un registre des incidents
- Sensibiliser et former les utilisateurs en matière de sécurité informatique
  - Gestion des mots de passe appropriés Vidéo gestion des mots de passe
  - Vigilance en lien avec les risques d'hameçonnage
- Attribuer judicieusement les droits d'accès aux systèmes informatisés

CSN

Meilleures pratiques de sécurité (volet technique)

- Avoir un mot de passe sécuritaire sur son ordinateur
- Sécuriser le réseau sans fil
- Gestion des correctifs et de mise à jours des systèmes de façon régulière
- Utilisation de l'authentification à deux facteurs
- Utilisation de logiciel de protection (anti-virus, anti-malware, anti-spam, EDR, Encryption, pare-feux, etc …)
- Mettre en place une solution de sauvegarde des données hors site

CSN

Outil de gestion de membres Sentinelle-CSN (partenariat)

- La CSN fournit aussi un logiciel de gestion de membres aux syndicats affiliés.
- Logiciel sécurisé sur le web dans les centres de données Microsoft du Canada. Un endroit sécurisé pour vos données syndicales.
- Le logiciel permet d'établir les accès aux données des membres selon le profil des utilisateurs en lien avec leur besoin d'accès à l'information.
- l'authentification à deux facteurs, backup complet journalier, connexion encrypté, mécanisme de blocage après 5 tentatives d'accès sans succès, notification et journalisation des extractions de données.
- Lien de référence sur le site web CSN: https://www.csn.qc.ca/mouvement/services/sentinelle/

CSN

Références utiles

- Trousse hameçonnage de cyber eco (vidéo, affiche, quiz, etc)
- Guide de gestion des incidents PME de Cyber eco
- https://cyber.gc.ca/fr/orientation/introduction-lenvironnement-de-cybermenaces
- Inventaire actif informationnel