Directive du Bureau du Chef de l'Information : TI 10.05	Publié : 04/2019
Chapitre : Sécurité des réseaux	Dernière révision : 01/2024
Objet : **Détection d'intrusion dans un réseau**	

1 DIRECTIVE

1.01 Un processus systématique sera en place pour surveiller les réseaux du GNB afin de détecter les tentatives d'accès non autorisées. Cette surveillance utilisera les meilleurs matériels et logiciels de l'industrie qui consignent les tentatives d'accéder au réseau sans autorisation et qui analysent les journaux d'accès au réseau et les scénarios de connexion pour repérer et consigner les accès non autorisés possibles afin d'approfondir leur examen.

2 OBJET

2.01 La présente directive a pour objet d'améliorer le niveau de sécurité en recherchant de manière proactive les signes d'intrusions non autorisées dans le réseau.

3 PORTÉE

3.01 La présente directive s'applique à la totalité des systèmes hôtes, des serveurs et des appareils informatiques fournis par le GNB (parties I à IV).

4 RESPONSABILITÉ

4.01 L'équipe de la cybersécurité du Conseil du Trésor travaille en étroite collaboration avec les équipes de sécurité et de soutien de la TI des fournisseurs de services. Ces équipes assument ensemble la responsabilité de l'évaluation et de la mise en œuvre des outils de détection des intrusions dans le matériel informatique et les logiciels du réseau.

4.02 Opérations de la TI a les responsabilités ci-dessous :

a) surveiller les systèmes et les réseaux pour détecter les signes de tentatives infructueuses et d'intrusions réussies;

b) faire le suivi de toutes les preuves de tentatives d'intrusion et les tenir;

c) signaler les incidents d'intrusion dans le réseau à **[Sécurité de la TI]**;

d) prendre immédiatement des mesures visant à minimiser les dommages créés par les intrusions réussies.

4.03 Le chef de la sécurité de l'information (CSI) et Soutien technique de la TI sont responsables de la suite à donner aux tentatives d'intrusion détectées ou signalées et de la recommandation de changements à mettre en œuvre pour empêcher qu'elles se reproduisent.

5 DÉFINITIONS

5.01 Le **« TCP »** (**Transmission Control Protocol/Protocole de contrôle de**

transmissions) est un protocole de communication qui représente la partie du protocole TCP/IP qui sert à transmettre des données sous la forme d'unités individuelles ou de paquets de données dans Internet. Le protocole TCP est chargé de créer l'ensemble de paquets, d'effectuer le suivi de tous les paquets et d'assurer leur arrivée à destination en toute sécurité, puis leur assemblage selon la séquence correcte.

5.02 L'**« UDP »** (**User Datagram Protocol/Protocole de datagramme utilisateur**) est un protocole moins fiable que le protocole TCP et qui, comme lui, se superpose aux réseaux IP. Il offre très peu de services de reprise sur erreur, mais permet d'envoyer et de recevoir directement des données sur un réseau IP. Alors que le protocole TCP est utilisé pour des données qui doivent arriver en parfait état, le protocole UDP ne permet que d'envoyer des paquets de données sans prévoir le temps de renvoyer les paquets de données éliminés ou de rectifier ceux qui sont erronés en temps réel. On l'utilise principalement pour diffuser en temps réel des données sur un réseau pour le contenu multimédia, VoIP et les vidéoconférences.

6 DIRECTIVE CONNEXES

BCI TI 10.01 – Connexion au réseau par matériel externe

BCI TI 10.03 – Accès à distance

BCI TI 10.04 – Réseau sans fil

BCI TI Chapitre 13 –Responsabilités de l'utilisateur