1.0 INTRODUCTION

Au besoin et le cas échéant, toutes les unités, tous les dispositifs spécifiés, ainsi que l'intégration des communications et des systèmes, doivent être conformes à l'ensemble des pratiques exemplaires et des normes de l'industrie. Les dispositifs de transmission de radiofréquence (RF), lorsqu'ils ne sont pas permis, doivent être complétés par des dispositifs qui ont des protocoles de communication sans fil limités ou inexistants. L'ensemble des recommandations/remplacements/environnements d'hébergement de données liés au dispositif doivent être approuvés avant l'intégration.

2.0 POSTES DE TRAVAIL SUR PLACE

2.1 Les postes de travail situés sur le site doivent avoir une sauvegarde disponible hors site qui doit être disponible rapidement en cas de panne.

2.2 Il faut appliquer régulièrement les correctifs et les mises à jour des logiciels des postes de travail, y compris le système d'exploitation, selon les recommandations des fournisseurs du logiciel.

2.3 Tous les ports USB des postes de travail doivent être désactivés.

3.0 GESTION DES DISPOSITIFS DE RÉSEAU DE TO

3.1 Les dispositifs de TO doivent être soigneusement sélectionnés auprès de fournisseurs réputés, utiliser des modèles normalisés et être configurés de façon sécuritaire pour assurer la fiabilité et la sécurité du réseau de TO. Les dispositifs de réseau de TO sur les sites des clients ne peuvent être installés sur les réseaux de TO par une personne ou un groupe, à moins d'avoir obtenu l'approbation de BGIS.

3.2 Il faut appliquer aux dispositifs de réseau de TO les mises à jour et les correctifs les plus récents en réponse à des vulnérabilités de sécurité, dès que possible et dans les 30 jours suivant leur publication.

3.3 Les configurations ou les modifications des dispositifs réseau de TO doivent être consignées, examinées, mises à l'essai et déployées conformément à la politique de gestion du changement en matière de TI.

3.4 La documentation relative aux réseaux TO et aux dispositifs réseau doit être classifiée, stockée et manipulée conformément aux pratiques exemplaires et aux normes de l'industrie.

3.5 Tous les documents de réseau de TO contenant des renseignements précis sur la configuration et l'adressage du réseau doivent être classés comme confidentiels et ne doivent être partagés avec nul autre que BGIS sans le consentement écrit de BGIS.

3.6 Les réseaux de TO doivent être disponibles pour une évaluation indépendante par des évaluateurs/vérificateurs internes/externes.

4.0 CONFIGURATION DES DISPOSITIFS RÉSEAU DE TO

4.1 Les dispositifs réseau de TO doivent se trouver sur une plateforme matérielle dédiée sur laquelle seuls les logiciels ou les services essentiels à l'exploitation du réseau sont installés et exécutés.

4.2 S'il y a lieu, les dispositifs réseau de TO doivent être conçus de manière à offrir une disponibilité élevée et des capacités de reprise après sinistre pour répondre aux exigences établies en matière de réseau et de niveau de service opérationnel.

4.3 Les dispositifs de réseau de TO ne doivent pas partager de ressources informatiques avec d'autres applications ou services, sauf pour permettre des contrôles de sécurité comme la surveillance et l'analyse de la sécurité.

4.4 Les appareils réseau de TO doivent prendre en charge des outils de surveillance de la circulation et de la sécurité qui sont conformes aux pratiques exemplaires de l'industrie comme Zabbix ou d'autres outils préapprouvés par BGIS.

4.5 Les mots de passe par défaut des dispositifs réseau de TO doivent être modifiés avant leur installation et leur déploiement. Le mot de passe doit compter au moins 30 caractères et comprendre au moins (1) lettre majuscule, (1) lettre minuscule, (1) chiffre et (1) caractère spécial.

4.6 Les dispositifs réseau de TO doivent conserver leur configuration, leurs paramètres de sécurité, ainsi que les contrôles d'accès après une réinitialisation ou un redémarrage ou à la suite d'un basculement vers un dispositif réseau de secours.

4.7 Les dispositifs de pare-feu du réseau de TO doivent être configurés de manière à repérer les incidents de sécurité et à permettre l'amorce de procédures d'intervention en cas d'incident. BGIS doit être informée de tout événement de sécurité lié aux appareils du réseau de TO.

4.8 Les renseignements sur la configuration des dispositifs réseau de TO doivent être effacés de façon sécuritaire avant la mise hors service et l'élimination des dispositifs.

4.9 Les dispositifs réseau de TO doivent être renforcés pour veiller à ce que l'accès physique local nécessite une authentification (par exemple : veiller à ce que la connexion à la console nécessite un mot de passe et désactiver toute connexion auxiliaire comme les ports USB).

5.0 ACCÈS À LA GESTION DES DISPOSITIFS RÉSEAU DE TO

5.1 L'accès aux dispositifs réseau de TO doit être approuvé uniquement pour le personnel autorisé.

5.2 Les droits d'accès et les comptes utilisateur aux dispositifs réseau de TO doivent être certifiés au moins deux fois par an et les artéfacts de vérification doivent être stockés en toute sécurité.

5.3 L'accès aux dispositifs réseau de TO et aux systèmes de gestion de réseau doit être immédiatement révoqué lorsqu'un administrateur change de responsabilités de travail. Tous les mots de passe de l'administrateur réseau et des services doivent également être réinitialisés.

5.4 Nonobstant les comptes d'administrateur de service et de réseau, les comptes d'utilisateur des appareils réseau de TO et des systèmes de gestion de réseau doivent tous être des comptes d'utilisateur individuels particuliers; il ne doit y avoir aucun compte utilisateur générique ou partagé. L'accès aux dispositifs réseau de TO et aux systèmes de gestion de réseau doit être immédiatement révoqué lorsqu'un administrateur change de responsabilités de travail.

5.5 Dans la mesure du possible, l'accès de gestion des dispositifs réseau de TO doit utiliser l'authentification multifactorielle.

5.6 L'accès aux dispositifs réseau de TO et au système de gestion de réseau à l'aide de Telnet, FTP ou d'autres protocoles non chiffrés est interdit. Il faut créer des comptes distincts pour tous les utilisateurs. Les comptes d'accès général pour la configuration des dispositifs de réseau de TO sont interdits.

6.0 SÉCURITÉ DU PÉRIMÈTRE DE RÉSEAU DE TO

6.1 S'il y a lieu, les appareils réseau de TO doivent avoir des capacités de traitement intelligent des documents (IDP) (ou l'équivalent) et celles-ci doivent être activées pour tous les flux de trafic,

6.2 L'équipement réseau de TO installé aux sites des clients doit être disponible pour une évaluation indépendante par BGIS.

6.3 Le périmètre de réseau de TO doit veiller à ce que toute connexion en destination et en provenance d'Internet passe par des passerelles réseau approuvées. La passerelle de TO doit être la seule passerelle disponible entre les réseaux locaux de TO et les zones non sécurisées.

6.4 Le périmètre du réseau doit être configuré pour filtrer le trafic réseau à destination et en provenance d'Internet, en respectant les règles suivantes :

6.4.1 Règle implicite visant à tout refuser; tout le trafic du réseau de TO est interrompu, à moins que ce ne soit explicitement autorisé.

6.4.2 Toutes les règles relatives au pare-feu de TO doivent reposer sur le principe du moindre privilège (ne permettre que ce qui est nécessaire au fonctionnement de l'application).

6.4.3 Les règles du pare-feu de TO doivent être créées de manière à ne pas permettre aux applications tierces de contourner les principes ou les fonctionnalités de sécurité. Exemple : la politique relative à Internet sortant doit garantir que les applications de commande à distance (exemple : TeamViewer) ne permettent pas une connexion à distance non autorisée vers le système de TO.

6.4.4 Tout le trafic traversant le réseau d'OT (intrazone ou interzone) doit être chiffré, au minimum, au moyen du protocole TLS 1.2 ou IPSEC.

6.5 L'accès à distance à partir d'Internet ou d'autres réseaux externes doit être considéré comme non fiable et doit être authentifié, au minimum, par une adresse IP source reconnue et confirmée. Ce type de connectivité ne doit être utilisé que par le trafic d'applications. Le trafic d'accès à distance doit provenir du Canada.

6.6 L'authentification multifactorielle doit être utilisée lors de la connexion à distance de l'ordinateur d'un utilisateur final à un réseau de TO.

6.6.1 Les sources de trafic des sites Internet et des adresses IP reconnues pour héberger ou lancer des attaques et des malwares ou pour soutenir des pourriels, des logiciels malveillants, des attaques par déni de service, des plateformes d'attaque réseau, du matériel offensant ou d'autres risques technologiques pour l'équipement et les systèmes du client doivent être bloquées.

6.6.2 Les réseaux internes du réseau de TO doivent être séparés, le cas échéant. (P. ex., les dispositifs de TO ne doivent pas se trouver sur le même sous-réseau que les utilisateurs d'entreprise.)

6.7 Tous les accès à distance d'utilisateur passant par des dispositifs non sécurisés doivent réussir une vérification du profil d'information d'hôte (HIP) avant de pouvoir se connecter au RPV de TO. (Exemple : L'ordinateur de l'utilisateur doit utiliser Windows 11 avec les correctifs Windows les plus récents).

6.7.1 Le cas échéant, les réseaux de TO doivent avoir un contrôle d'accès réseau (CAR) couche 2 au minimum.

7.0 ACCÈS AU RÉSEAU SANS FIL

7.1 Les réseaux de TO utilisent souvent des protocoles d'authentification de base comme WEP ou WPA. Il s'agit d'une mesure acceptable si ces réseaux suivent le principe de moindre privilège et ségrégation réseau.

7.2 Les réseaux sans fil de TO doivent être masqués.

7.3 Les réseaux sans fil de TO doivent être consacrés exclusivement à la fonctionnalité du système de TO. Par exemple, les utilisateurs du réseau sans fil pour invités ne doivent pas avoir accès au réseau sans fil de TO.

7.4 Les utilisateurs locaux des réseaux sans fil doivent avoir une authentification au niveau de l'utilisateur (exemple : RADIUS).

8.0 ADMINISTRATION DES TO

8.1 Pour chaque réseau de TO, il doit y avoir un utilisateur désigné responsable de l'approbation et de l'autorisation de toute demande liée à son réseau de TO. Si un réseau de TO n'a pas d'administrateur désigné, il faut en nommer un avant le traitement de tout changement.

8.2 L'accès des utilisateurs au réseau de TO doit être entièrement authentifié (avec une autorisation à deux facteurs) et utiliser un répertoire des utilisateurs qui peut être audité et examiné.

9.0 SERVICES INFONUAGIQUES

9.1 Tous les services infonuagiques doivent satisfaire aux exigences minimales suivantes :

9.1.1 Les données doivent être stockées au Canada.

9.1.2 Toutes les données doivent être détruites (lettre de certification signée par le représentant autorisé de l'entreprise) à la résiliation du contrat après le transfert au service de stockage privilégié du client.

9.1.3 BGIS se réserve le droit d'effectuer une évaluation des vulnérabilités de sécurité de toute plateforme infonuagique suggérée et désignée comme pouvant être utilisée. Dans le cadre de cette évaluation, fournisseur devra fournir les renseignements suivants (sans toutefois s'y limiter) avant l'attribution du contrat ou à tout autre moment pendant la durée du contrat :

a) Contrat de licence d'utilisateur final (CLUF)

b) Déclarations/politiques en matière de confidentialité

c) Politiques sur la résidence et la destruction des données

10.0 EXIGENCES DE BGIS EN MATIÈRE DE PARE-FEU

10.1 Les systèmes et les dispositifs de TO des fournisseurs tiers seront connectés au moyen d'un pare-feu, conformément à l'architecture suivante.