Sécurité de l'information visant les tiers

Sécurité de l'information du CN – Lignes directrices

Objectif

Les présentes lignes directrices énoncent les exigences générales en matière de sécurité de l'information que les tiers devraient respecter afin de protéger les actifs informatiques et les informations du CN. Tous les tiers du CN doivent protéger la disponibilité, l'intégrité et la confidentialité de l'information confidentielle du CN. De plus, certains tiers peuvent avoir accès aux actifs informatiques du CN et, par conséquent, ils doivent respecter les politiques et les normes du CN pour prévenir les cyberattaques contre les actifs informatiques du CN. Le non-respect de ces politiques et de ces normes pourrait causer des dommages irréparables aux activités commerciales et d'exploitation, à la réputation et à la situation financière du CN.

Champ d'application

Les présentes lignes directrices s'appliquent à tous les tiers qui fournissent au CN des services informatiques, des services de technologies opérationnelles ou des services dans le cadre desquels ils hébergent ou stockent de l'information confidentielle du CN, ou y ont accès. De plus, lorsqu'ils accèdent aux actifs informatiques du CN, les tiers doivent appliquer les politiques et les mécanismes de contrôle de la sécurité de l'information de l'entreprise. Le CN mettra à jour périodiquement ses Lignes directrices en matière de sécurité de l'information à l'intention des tiers pour tenir compte de l'évolution de la technologie, des menaces et des normes de sécurité; on encourage les tiers à vérifier les lignes directrices de temps à autre. Le CN se réserve le droit de surveiller la performance de ses tiers et leur conformité aux normes de sécurité comprises dans les documents contractuels du CN.

Détails sur le document
Dates importantes

Publication le 9/3/2018

Propriétaire : InfoSec

Table des matières

Définitions

« **Information confidentielle** » désigne les renseignements protégés, comme les informations sur les infrastructures essentielles, les informations sensibles relatives à la sécurité ou tout renseignement qui est confidentiel par sa nature et qui, avec ou sans mention de confidentialité ou d'exclusivité, a été diffusé par le CN à un tiers, et que le CN demande au tiers de garder en toute confidentialité et de n'utiliser qu'aux fins de sa relation avec le CN. Voici des exemples d'information confidentielle :

- Renseignements commerciaux sensibles, de nature délicate face à la concurrence, exclusifs ou privés, notamment des renseignements de nature opérationnelle, commerciale, industrielle, scientifique, stratégique ou technique
- Formules, processus et mécanismes
- Données, plans et schémas, en particulier les plans opérationnels, commerciaux, financiers ou d'investissement
- Plans commerciaux et plans stratégiques d'exploitation
- Contrats et ententes
- Transactions, fusions et acquisitions d'entreprises
- Communications, notes de service et présentations internes
- Listes de fournisseurs
- Renseignements personnels d'identification des employés du CN
- Données classées CN-DISTRIBUTION INTERNE, CN-DISTRIBUTION CONFIDENTIELLE ou CN-DISTRIBUTION RESTREINTE, peu importe leur format, qu'il s'agisse d'un document papier ou électronique, d'une vidéo ou d'un enregistrement de la voix
- Propriété intellectuelle du CN
- Nouveaux produits, stratégies relatives à l'image de marque et au marketing, plans et prévision, alliances stratégiques, élaboration de nouveaux produits ou secteurs d'activité
- Listes des clients et coordonnées, besoins, historiques d'achat, taux, spécifications et préférences des clients
- Informations de nature juridique, notamment celles couvertes par le privilège juridique
- Renseignements sur la concurrence et le marché recueillis pour le CN
- Informations sur les systèmes, l'infrastructure et les activités de la TI du CN
- Données d'entreprise
- Renseignements personnels sur la santé des employés du CN

« **Tiers** » désigne les fournisseurs, les gouvernements, les organismes non gouvernementaux ou les autres entités (y compris leur personnel) avec qui le CN entretient une relation et à qui il pourrait transmettre de l'information confidentielle.

« **Personnel** » désigne, le cas échéant, les employés, les mandataires, les consultants, les sous-traitants ou les représentants des tiers, qui participent à la prestation des Services.

« **Actifs informatiques du CN** » désigne les technologies de l'information, les technologies et les environnements opérationnels, les réseaux, le matériel, les ordinateurs, les systèmes, les appareils, les serveurs, les applications, les logiciels, les services, les installations et les infrastructures.

1. Certifications, cadres et normes de sécurité de l'information

1.1. Les tiers doivent adopter une approche globale et structurée de la protection de l'information confidentielle du CN. Leur approche devrait englober un programme de sécurité de l'information qui comprend des politiques, des normes, des méthodes et des mécanismes de contrôle relatifs à la sécurité. Les programmes de sécurité de l'information des tiers devraient être conformes à un ou plusieurs des éléments suivants, ou être certifiés par ceux-ci ou en adopter les versions actuelles :

- Normes ou certifications de sécurité de l'information de la série ISO/IEC 27000
- Cadre de cybersécurité du National Institute of Standards and Technology (NIST)
- Certification FedRAMP du gouvernement américain
- Certification STAR de la Cloud Security Alliance (CSA)
- Rapports SOC 1 de type 2 de la norme SSAE 16 de l'American Institute of CPAs (AICPA)
- Attestation SOC 2 de type 2 ou norme SSAE 18 de l'AICPA
- Norme d'assurance ISAE 3402 appliquée à la sécurité de l'information
- Norme canadienne de missions de certification (NCMC) 3416 (équivalent canadien de l'attestation SOC 2 de l'AICPA)

1.2. Les tiers devraient évaluer leur exposition aux risques pour la sécurité et aux autres menaces et prendre des mesures appropriées pour faire face aux risques connexes auxquels sont exposés leurs installations, leurs actifs informatiques, ainsi que l'information confidentielle du CN.

1.3. Les tiers devraient consulter le document intitulé AAR Rail Information Security Committee Cyber Security Effective Practices for Information Technology Procurement. Ce document se trouve sur la page https://www.aar.org/data/cyber-security-effective-practices-for-information-technology-procurements/. Il contient un ensemble de pratiques recommandées pour assurer la protection des systèmes ferroviaires.

1.4. Les tiers devraient officialiser et documenter leur programme et leurs mécanismes de contrôle de la sécurité de l'information dans des politiques, des normes et des méthodes qui pourront, sur demande, être mises à la disposition du CN.

2. Programmes et méthodes de gestion des risques

2.1. Les tiers devraient adopter une approche globale et structurée de la gestion des risques qui permet de cerner et de diminuer les risques associés à leurs actifs informatiques et à leur programme de sécurité de l'information. Cette approche peut être fondée sur l'un des éléments suivants :

- Norme ISO/IEC 27005
- Cadre COBIT 5 de l'ISACA
- Publication spéciale 800-30 du NIST
- Méthode IRAM 2 de l'Information Security Forum
- Cadre FAIR (factor analysis of information risks)

2.2. Les tiers devraient évaluer leur exposition aux risques et aux menaces liés à la sécurité de l'information en procédant à des examens réguliers. Ils devraient également prendre des mesures appropriées pour faire face aux risques connexes auxquels sont exposés leurs actifs informatiques et l'information confidentielle du CN. Les résultats de ces examens doivent être mis à la disposition du CN lorsqu'il le demande.

3. Mécanismes de contrôle de la sécurité

3.1. Les tiers devraient mettre en place des mécanismes de contrôle de la sécurité qui doivent comprendre minimalement les éléments suivants :

- Des processus robustes et documentés de contrôle des changements, dont des cycles de gestion des nouvelles versions, qui, de préférence, sont conformes à des pratiques connues comme l'ITIL.
- La gestion de la vulnérabilité, les rustines de sécurité et les changements apportés aux actifs informatiques doivent être contrôlés et respecter les méthodes normalisées de gestion des changements et les plages horaires approuvées pour les changements opérationnels qui, le cas échéant, peuvent faire l'objet d'une entente entre le CN et les tiers.
- Des environnements de développement, d'essai, de production ou de sauvegarde qui sont séparés physiquement et logiquement afin de réduire le risque d'accès ou de changements non autorisés aux environnements de production.
- Des contrôles pour prévenir le changement, le copiage ou l'altération des codes appartenant au CN sans autorisation écrite préalable.

- Des politiques de sauvegarde et de conservation qui définissent la fréquence des cycles de sauvegarde et de conservation pour toutes les données et tous les environnements pour permettre la prestation de leurs services conformément à toute entente relative à ces services.
- La détection et la prévention des intrusions et des contrôles de reprise qui protègent contre les codes malveillants et tiennent à jour et maintiennent en service les logiciels antivirus et les signatures afin qu'ils détectent et éliminent les logiciels malveillants.
- Des outils de détection qui empêchent les utilisateurs de télécharger des programmes ou d'autre matériel dans Internet ou d'utiliser des supports d'information amovibles (clés USB, CD, DVD, etc.) dans des actifs informatiques des tiers qui stockent ou traitent de l'information confidentielle du CN, ou y ont accès, à moins qu'on ait vérifié qu'ils proviennent d'une source sûre et qu'ils ont été analysés pour détecter les virus.
- Des normes de complexité des mots de passe pour atténuer les menaces liées aux mots de passe faibles.
- La sécurité du réseau et du périmètre physique.
- Des pratiques sécuritaires de développement de logiciels (couramment appelées S-SDLC).

4. Gestion des registres d'exploitation et de sécurité et accès

4.1. Les actifs informatiques des tiers devraient être configurés de façon à comprendre des capacités de gestion des registres qui :

- font le suivi des événements liés à la sécurité et à l'exploitation, des incidents, des activités, des accès à l'information et aux programmes, des événements systèmes comme les alertes, les messages de consoles et les erreurs système, et les mécanismes de contrôle de la détection, de la prévention et de la reprise, en ce qui concerne tous les aspects de la relation avec le CN et des services gérés par les tiers;
- gèrent les cycles de vie des registres et les conservent après la prestation de services ou la relation, ou plus longtemps lorsque cela est spécifié dans l'entente pertinente ou lorsque l'exige la loi ou les règlements applicables aux services ou à la relation des tiers;
- sont protégées contre les altérations et les accès non autorisés.

4.2. On pourrait demander aux tiers de mettre des renseignements pertinents des registres à la disposition du CN de façon régulière ou sur demande aux fins de vérification et d'archivage.

5. Droits de vérification

5.1. Si un préavis raisonnable a été donné, les tiers doivent permettre au CN ou à ses partenaires (y compris les organismes de réglementations gouvernementaux qui demandent des inspections du CN) d'accéder à l'information confidentielle du CN qui est hébergée, stockée ou traitée dans les actifs informatiques des tiers, ou à laquelle on accède à partir de ces actifs, afin qu'il procède à des évaluations de la sécurité. Les évaluations de la sécurité doivent comprendre, selon les cas :

- des évaluations de la vulnérabilité du réseau;
- un examen de la conception globale et de la topologie des services de sécurité de l'information;
- un examen des fichiers de configuration pour les actifs informatiques;
- un examen des mécanismes de contrôle technique et de sécurité dans le centre de traitement de l'information et les activités de TI associées;
- des enquêtes judiciaires sur les incidents de cybersécurité.

6. Respect des politiques du CN

6.1. Lorsque des tiers accèdent aux actifs informatiques du CN, les politiques, les normes et les méthodes liées à la sécurité de l'information d'entreprise du CN s'appliquent. Les tiers doivent les respecter, ainsi que toute instruction particulière fournie par le CN relativement à un engagement, un mandat, une entente, un accès ou un énoncé des travaux en particulier. Plus précisément, il est interdit aux tiers :

- de tenter de contourner ou de neutraliser les mécanismes de contrôle de la sécurité du CN;
- d'agir d'une manière qui constitue une violation des lois criminelles;
- de participer à des hameçonnages, ou à d'autres stratagèmes d'accès ou de divulgation non autorisés;
- d'accéder ou de tenter d'accéder sans autorisation aux actifs informatiques du CN, ou de porter atteinte à l'intégrité de ceux-ci;
- de transmettre des virus informatiques intentionnellement ou par insouciance;
- de supprimer ou d'altérer des mesures de protection, des mécanismes de contrôle ou des systèmes de sécurité mis en place ou configurés par le CN;
- de détruire, de modifier ou de crypter de l'information confidentielle du CN par inadvertance ou dans le but de la rendre inaccessible au CN;
- d'intercepter, d'écouter ou de brouiller les communications vocales, les transmissions de données ou les autres communications électroniques du CN;
- d'utiliser les actifs informatiques du CN à une fin autre que celle à laquelle ils sont destinés ou que le mandat ou les services des tiers. Il est notamment interdit aux tiers d'exploiter une entreprise personnelle ou d'effectuer des

transactions commerciales sans rapport avec l'exécution de leurs tâches pour le CN.

6.2. Les actifs informatiques du CN qui sont mis à la disposition des tiers demeurent la propriété exclusive du CN. Les tiers ne doivent pas s'attendre au respect de leur vie privée lorsqu'ils utilisent les actifs informatiques du CN ni s'attendre à ce que les données stockées dans les actifs informatiques du CN ou reçues et envoyées au moyen de ceux-ci soient considérées comme la propriété privée des tiers. Particulièrement, le CN peut, de temps à autre et sans préavis, surveiller, vérifier, intercepter, modifier ou supprimer des fichiers ou des communications stockés dans les actifs informatiques du CN ou échangés au moyen de ceux-ci, ou accéder à ces fichiers ou ces communications, y compris l'information qui n'est pas liée à ses activités.

7. Personnel

7.1. Les tiers sont responsables des actes et des omissions des membres de leur personnel. Par conséquent, ils doivent accomplir les actions suivantes pour tous les membres de leur personnel qui pourraient avoir accès aux actifs informatiques des tiers, ou avoir accès aux actifs informatiques, aux installations ou à l'information confidentielle du CN, ou en avoir la garde :

- Procéder à des vérifications adéquates des antécédents et des références.
- Fournir de la formation appropriée sur la sécurité de l'information et un programme de sensibilisation à la sécurité de l'information.
- Gérer la performance des membres de leur personnel relativement à la sécurité des actifs informatiques et de l'information confidentielle du CN.

8. Politiques et procédures sur l'échange d'information

8.1. Les tiers doivent adopter des pratiques exemplaires pour l'échange d'information. Par exemple, ils doivent avoir recours à des services de transfert de fichiers sécuritaires et gérés ou à des outils de courriel sécuritaires lorsqu'ils partagent ou échangent de l'information confidentielle du CN avec le CN ou d'autres tiers.

9. Conséquences du non-respect des politiques de sécurité de l'information du CN

9.1. Lorsqu'un tiers enfreint les politiques sur la sécurité de l'information du CN, cela pourrait mettre fin à la relation ou au contrat entre le CN et le tiers.

9.2. Le CN peut, à son entière discrétion, retirer l'accès d'un tiers à de l'information confidentielle du CN ou à certains actifs informatiques.

9.3. Si le comportement du tiers contrevient aux lois applicables, il pourrait également faire l'objet de mesures d'application de la loi, de poursuites criminelles ou de toute autre action en justice.