FINANCIAL AND CONSUMER SERVICES COMMISSION

COMMISSION DES SERVICES FINANCIERS ET DES SERVICES AUX CONSOMMATEURS

Avis concernant les risques liés à la cybersécurité

Introduction

Les cybermenaces constituent un risque croissant pour les organisations des secteurs réglementés par la FCNB[1]. Il est de plus en plus important d'assurer une gestion proactive de ce risque afin de se protéger contre les attaques visant à compromettre ou à perturber les systèmes informatiques ou à voler des données et des renseignements stockés.

La FCNB dispose de ressources pour aider les organisations à renforcer leurs pratiques de gestion des risques et à mieux se préparer contre les cybermenaces.

Le présent avis contient des mesures de base importantes qui peuvent être prises dans ce sens.

La gestion des risques liés à la cybersécurité

Il existe un certain nombre de normes de pratiques exemplaires en matière de gestion des risques liés à la cybersécurité. Pour sa part, la FCNB utilise une version modifiée du cadre conçu par le National Institute of Standards and Technology[2] (NIST) pour gérer ces risques.

Bon nombre de ces normes de pratiques exemplaires proposent, étape par étape, des mesures importantes que les organisations doivent prendre pour gérer les risques sur différents plans.

Champ d'activités	Étapes de gestion des principaux risques
Planification en matière de cybersécurité	L'organisation a entrepris d'améliorer sa posture en matière de cybersécurité. Elle a mis en place du personnel compétent et affecté des ressources à la cybersécurité. Un plan a été établi pour déterminer les actifs et les risques qui guettent ces actifs et pour prendre des mesures correctives au besoin.
Sécurité des personnes	Les employés sont formés pour adopter des comportements prudents. Une culture de cybersécurité existe au sein de l'organisation. Tout le personnel sait ce qu'il a à faire pour assurer le maintien de la sécurité sur

[1] L'étude sur les coûts relatifs à la cybercriminalité 2019 de la société Accenture cerne des risques considérables et croissants en matière de cybersécurité pour les entreprises. Selon cette étude, les cybercriminels se concentrent de plus en plus sur le vol de renseignements et la perturbation des données et des systèmes centraux et utilisent des techniques plus agressives et évoluées pour cibler la « composante humaine » des entreprises, par l'intermédiaire de l'hameçonnage et d'attaques d'ingénierie sociale. Voir https://www.accenture.com/us-en/insights/security/cost-cybercrime-study (en anglais seulement).

[2] Le cadre de cybersécurité du NIST fournit aux entreprises une structure pour évaluer et améliorer leur capacité à cerner, à prévenir et à détecter les cyberincidents ainsi que leur capacité à intervenir dans de telles situations et à se rétablir. Voir https://www.nist.gov/cyberframework (en anglais seulement).

	le plan informatique. L'organisation a mis en place un processus solide d'entrée en fonction et de cessation d'emploi, et les employés ont uniquement accès aux ressources informatiques dont ils ont besoin pour accomplir leur travail.
Politiques organisationnelles	Des politiques ont été établies pour définir des pratiques exemplaires en ce qui concerne l'utilisation des ressources informatiques et la gestion des données.
Sécurité opérationnelle	L'organisation est sensibilisée aux menaces et aux vulnérabilités en matière de cybersécurité sur le plan des opérations et elle sait comment ses ressources informatiques et ses données sont utilisées et consultées. Elle peut prendre des mesures efficaces quand un risque se concrétise et des plans d'intervention en cas d'incident et de continuité des affaires sont en place. L'organisation tire des leçons de ses expériences.
Conception des logiciels	Les nouveaux logiciels font l'objet d'une évaluation des risques liés à la cybersécurité avant d'être utilisés. Les logiciels conçus à l'interne respectent les normes de sécurité appropriées et sont mis à l'essai avant d'être implantés.
Sécurité physique	Des systèmes et des processus sont en place pour empêcher les personnes non autorisées de pénétrer sur les lieux ou d'accéder physiquement aux biens de l'organisation. On maintient de bons registres de contrôle d'accès, s'il y a lieu.
Relations avec des tiers	L'organisation vérifie la posture en matière de cybersécurité des tiers qui pourraient avoir accès à ses systèmes informatiques et ses données. Elle obtient des garanties de ces tiers qu'ils la préviendront s'ils sont victimes d'une atteinte à leur cybersécurité.
Sécurité des réseaux	Le réseau de l'organisation est structuré de manière à être protégé contre les menaces externes. Des solutions pare-feu, configurations de serveurs et mécanismes de cryptage appropriés sont en place. Les mécanismes de contrôles peuvent gérer la connexion de dispositifs externes au réseau (comme des clés USB).
Sécurité des plateformes	Tous les systèmes d'exploitation des ordinateurs et des serveurs du réseau font l'objet de mises à jour et de mises à jour correctives au besoin. Des logiciels antivirus et antimaliciels appropriés sont installés sur tous les dispositifs connectés au réseau. Des mécanismes ont été établis pour s'assurer que tous les utilisateurs s'authentifient avant d'accéder au réseau et ont le droit d'y accéder. Les utilisateurs ont des mots de passe difficiles à deviner.

Sécurité des applications	Les applications des utilisateurs sont mises à l'essai avant d'être utilisées, afin de s'assurer qu'elles sont sécuritaires, et sont actualisées au besoin.

Par où commencer?

Tous les risques ne sont pas égaux. Certains sont plus menaçants que d'autres. Certains risques sont faciles à traiter, tandis que d'autres sont plus complexes à gérer. Une bonne stratégie consiste à cerner les risques les plus importants auxquels il est le plus facile de remédier.

Vous trouverez ci-dessous une liste de vérification de base en matière de cybersécurité pour les organisations qui n'ont pas encore de plan ou de stratégie dans ce domaine. Elle n'est pas exhaustive et ne couvre pas tous les risques possibles. Toutefois, elle devrait vous aider à cerner et à contrer les risques les plus évidents.

Les organisations qui prendront les mesures recommandées dans la liste amélioreront considérablement leur posture en matière de cybersécurité et leur état de préparation aux cybermenaces.

Elles sont également encouragées à élaborer un plan de cybersécurité plus vaste, qui couvre davantage de secteurs de risque, dans un cadre de travail concret, en plus de mettre en œuvre les mesures de la liste. Pour obtenir d'autres ressources et des renseignements sur la façon d'élaborer un plan de cybersécurité global, consultez le site Web de la FCNB.

En passant la liste en revue une première fois, vous devriez déjà être en mesure de cerner certaines lacunes. Attaquez-vous à ces lacunes en premier, en fonction du risque qu'elles posent et des ressources disponibles, et confiez-les à une personne en particulier, afin qu'elle y remédie dans un délai prescrit.

Liste de vérification

- ☐ Affecter une ou plusieurs personnes à la gestion des risques liés à la cybersécurité de l'organisation.
- ☐ Faire l'inventaire de tous les dispositifs informatiques de l'organisation et déterminer pour chacun d'eux :
    - le type de dispositif (téléphone intelligent, tablette, ordinateur de bureau, ordinateur portatif, serveur, etc.) et le numéro de modèle;
    - le numéro de série consigné ou qui se trouve sur le dispositif;
    - l'utilisateur responsable de l'appareil;
    - le système d'exploitation et les applications utiles du dispositif;
    - si le dispositif est crypté ou non.

- Faire une liste de tous les types de dossiers et de données électroniques conservés sur les systèmes informatiques (les « biens électroniques ») de l'organisation et déterminer où ils sont stockés.
- Classer les biens électroniques selon qu'ils contiennent ou non ce qui suit :
    - renseignements d'identification;
    - renseignements exclusifs;
    - information financière sensible (p. ex. : numéro de carte de crédit);
    - données sur les opérations.
- Déterminer quels dossiers et données électroniques sur la liste sont essentiels au fonctionnement de l'organisation.
- Établir une topologie des réseaux de l'organisation (p. ex. : comment les ordinateurs et les autres appareils informatiques sont connectés; quels serveurs et appareils de stockage sont connectés au réseau, comment le réseau est connecté à Internet).
- Mener une analyse des risques auxquels sont exposés les appareils informatiques, les biens électroniques et la topologie de réseau en déterminant :
    - quels risques et biens sont des cibles faciles;
    - quels vecteurs d'attaque pourraient permettre d'accéder à ces appareils et biens;
    - qui pourrait vouloir attaquer l'organisation;
    - quels sont les risques d'atteinte à la sécurité par l'intermédiaire d'un vecteur d'attaque;
    - quelles seraient les répercussions d'une telle atteinte à la sécurité;
    - comment atténuer ou même éliminer les risques d'atteinte à la sécurité.
- Envisager la possibilité de se doter d'un outil de gestion à distance afin de contrôler les dispositifs informatiques de l'organisation utilisés à l'extérieur des bureaux.
- Passer en revue la liste de personnes qui ont accès aux biens électroniques de l'organisation et accorder à ces personnes un droit d'accès minimal[3].
- Vérifier, mettre à jour et mettre à l'essai les processus de secours et de rétablissement pour les dossiers et les données électroniques.
- Offrir de la formation sur la sensibilisation à la cybersécurité au personnel, préférablement de façon continue.
- Créer des politiques clés en matière de cybersécurité pour l'organisation ou réviser celles en place :
    - Pratiques exemplaires en matière de cybersécurité
        - Authentification
        - Mots de passe
        - Bureau propre
        - Utilisation des dispositifs informatiques à l'extérieur du bureau, etc.
    - Utilisation appropriée des ressources informatiques

[3] Les employés ont uniquement accès à l'information dont ils ont besoin pour accomplir leur travail et à rien de plus.

- Entrée en poste et cessation d'emploi
- Tiers et fournisseurs de TI

- Évaluer la posture de l'organisation sur le plan de la sécurité physique. S'assurer que des contrôles appropriés sont en place pour limiter l'accès aux installations de l'organisation et permettre uniquement aux employés appropriés de pénétrer sur les lieux.
  - Cartes d'accès
  - Cartes d'identité
  - Règles d'accès des visiteurs
- Vérifier que les processus d'aliénation des biens (équipement désuet, dossiers papier, etc.) prévoient la destruction ou le déchiquetage approprié de tous les dossiers importants en fin de vie.
- Examiner l'architecture du réseau de l'organisation. Des solutions pare-feu, configurations de serveurs et mécanismes de cryptage appropriés sont-ils en place?
- Vérifier les systèmes d'exploitation et les applications d'activation de réseau pour s'assurer qu'ils sont à jour, que les corrections appropriées ont été apportées et qu'un calendrier de mises à jour convenable est en place et est respecté.
- Veiller à ce que des logiciels antivirus et antimaliciels soient installés sur tous les dispositifs qui permettent d'accéder aux biens électroniques.
- Élaborer un plan d'intervention en cas d'atteinte à la cybersécurité et le mettre à l'essai.
- Élaborer un plan de continuité des affaires et le mettre à l'essai.