COMMENT PROTÉGER VOTRE ORGANISATION CONTRE LES MENACES INTERNES

FEVRIER 2020

ITSAP.10.003

Le présent document porte essentiellement sur les enjeux de TI qui concernent les menaces internes. On entend d'une *menace interne* toute personne qui connaît l'infrastructure ou l'information de votre organisation, ou qui y a accès, et qui utilise ses connaissances ou son accès d'une façon malveillante ou involontaire pour nuire à l'organisation. Les menaces internes peuvent poser des risques contre vos employés, vos clients, vos actifs, votre réputation et vos intérêts. Sachez que vous pouvez toutefois adopter des mécanismes de sécurité afin de réduire les risques connexes.

MENACE INTERNE MALVEILLANTE OU INVOLONTAIRE?

Un employé peut porter préjudice à l'infrastructure ou à l'information de votre organisation sans le savoir, par exemple dans les cas suivants :

- s'il perd un dispositif mobile ou un support amovible;
- s'il permet à des employés d'accéder à de l'information sensible qu'ils n'ont pas l'autorisation de consulter;
- s'il gère mal l'information sensible en la laissant à découvert ou en oubliant d'appliquer les permissions requises.

Dans les cas de menace interne malveillante, une personne se sert délibérément de votre infrastructure ou de votre information pour nuire à votre organisation. Pour ce faire, elle accède de façon non autorisée à des comptes privilégiés ou à des comptes généraux ou, encore, utilise ces comptes à mauvais escient. Parmi les facteurs qui motivent les menaces à accéder de façon non autorisée à ces types de comptes ou à mener des activités interdites, notons les raisons suivantes :

- elles cherchent à se venger (p. ex. aucun avancement professionnel, licenciement [menace d'un ancien employé, selon le plan de départ en place au sein de l'organisation]);
- elles sont victimes de menaces ou de chantage;
- elles souhaitent obtenir un gain personnel ou financier.

Une personne autorisée à accéder à votre infrastructure ou à votre information peut en réalité représenter une menace interne (p. ex. des employés, des entrepreneurs, des tierces parties ou des partenaires). Cette personne peut tenter de camoufler ses activités en modifiant les programmes de détection ou en supprimant les enregistrements de vérification. Le personnel qui détient inutilement des privilèges d'accès élevés peut représenter une grave menace pour votre organisation. Vous devez donc vous assurer que les employés ont uniquement les accès dont ils ont besoin pour accomplir leurs tâches (c.-à-d. appliquer le principe des droits d'accès minimaux).

CONSÉQUENCES POSSIBLES

En l'occurrence, une personne pourrait exposer l'information sensible ou personnelle à laquelle elle aurait accédé sans autorisation. Des violations de données et des atteintes à la vie privée risquent par ailleurs de nuire à votre organisation, car elles pourraient engendrer des conséquences financières, ternir la réputation de votre organisation et entraîner une perte de confiance du public envers votre organisation.

MESURES À PRENDRE CONTRE UNE MENACE INTERNE

Si une menace interne réussit à accéder sans autorisation aux réseaux, aux systèmes et à l'information de votre organisation ou, encore, à mener des activités interdites, vous devez prendre les mesures minimales suivantes :

- gérer les contrôles d'accès (c.-à-d. restreindre les privilèges afin de minimiser les dommages);
- localiser et surveiller tous les points terminaux (p. ex. une menace interne peut menacer des organisations à distance);
- vérifier les journaux de vérification pour relever tout comportement suspect;
- informer les fournisseurs de services tiers si les activités de la menace interne risquaient de s'étendre à leurs systèmes ou si elles provenaient de leur côté;
- collaborer avec la haute direction pour élaborer un plan de communication en cas d'incident;
- miser sur l'expérience acquise pour sensibiliser le personnel et offrir de la formation adaptée.

SÉRIE SENSIBILISATION

MESURES À PRENDRE POUR PRÉVENIR ET RÉDUIRE LES DOMMAGES

Les menaces internes sont difficiles à détecter. Vous pouvez toutefois gérer les risques connexes en adoptant les contrôles de sécurité suivants : mise en place de politiques et de procédures, de contrôles d'accès, de mesures de prévention de la perte de données de même que de vérifications.

POLITIQUES ET PROCÉDURES

Vous devez mettre en place des politiques et des procédures qui définissent clairement les exigences de sécurité de votre organisation et le comportement auquel on s'attend de toutes les personnes (employés, partenaires, tierces parties) qui utilisent les réseaux, les systèmes et l'information de l'organisation. Pour prévenir les menaces internes, vos politiques doivent mettre de l'avant les enjeux suivants :

- réaliser des enquêtes de sécurité sur le personnel qui traite de l'information sensible (p. ex. vérifier leurs antécédents);
  - mettre en œuvre des plans de mutation interne et de départ (p. ex. des plans de fin d'emploi);
- offrir des séances de formation obligatoires et des activités de sensibilisation;
  - aborder des sujets tels que les courriels d'hameçonnage, l'exposition aux maliciels et les risques associés aux médias sociaux;
  - adapter les séances de formation pour qu'elles portent sur les menaces et les contrôles de sécurité propres à l'organisation;
- mettre en œuvre des ententes axées sur la sécurité avec les partenaires de l'organisation et des tierces parties;
  - s'assurer que les données de l'organisation sont conservées au Canada (protection des données en vertu des pouvoirs juridiques du Canada);
  - surveiller et consigner les activités (c.-à-d. faire le suivi des personnes qui accèdent aux données et les moments où elles y accèdent);
  - établir des relations de confiance à long terme avec des partenaires (p. ex. déterminer leur fiabilité).

CONTRÔLES D'ACCÈS

Le contrôle des accès permet de restreindre de manière sélective l'accès d'un utilisateur à des réseaux, à des systèmes et à des données grâce à l'adoption de mécanismes d'authentification et d'autorisation. Les employés devraient uniquement détenir les accès dont ils ont besoin pour accomplir leurs tâches. Afin de contrôler les accès, vous devriez envisager les mesures suivantes :

- appliquer le principe des droits d'accès minimaux dans l'attribution de privilèges d'administrateur et d'accès aux comptes;
- mettre en œuvre des mécanismes d'authentification à deux facteurs ou à facteurs multiples (p. ex. des mots de passe et des jetons cryptographiques matériels pour accéder à des données sensibles);
- appliquer la règle relative à l'intégrité assurée par deux personnes afin de sécuriser les opérations ou le matériel de nature essentielle;
- révoquer les accès aux comptes et les privilèges d'administrateur qui ne sont plus requis (p. ex. si un utilisateur quitte l'organisation ou change d'équipe);
- veiller à la compréhension et à la mise en œuvre du concept de séparation entre les rôles d'administrateur et d'utilisateur sur le réseau de votre organisation.

Pour en savoir plus sur le contrôle des accès liés aux privilèges d'administrateur, consulter le document ITSM.10.094 – *Les principales mesures de sécurité : Gestion et contrôle des privilèges d'administrateur* que vous trouverez sur notre site Web.

VÉRIFICATIONS

En vérifiant les activités, vous pouvez recueillir, analyser et conserver des données et des journaux qui sont associés aux activités que mènent les utilisateurs sur les systèmes d'information. Vous pouvez entre autres recourir aux journaux de vérification pour gérer les risques associés aux menaces internes dans les cas suivants :

- surveiller les activités et les consigner en détail afin de détecter tout comportement inhabituel (p. ex. faire le suivi des changements apportés dans un système ou des caractéristiques comportementales inhabituelles);
- consigner les activités et les événements, puis inscrire l'heure et la date qui leur sont associées;
- vérifier les changements administratifs (p. ex. les moments où ont été ajoutés ou retirés des comptes);
- faire le suivi des dispositifs mobiles appartenant à l'organisation (p. ex. consigner toutes les activités menées sur les dispositifs ayant servi à accéder à l'infrastructure et à l'information de l'organisation à distance).

PRÉVENTION DE LA PERTE DE DONNÉES

Un logiciel de prévention de la perte de données permet à votre organisation de détecter et d'empêcher toute perte de contrôle de ses données. Ce type de logiciel a recours à des alertes, à du chiffrement et à d'autres mesures de protection pour empêcher les utilisateurs de communiquer de façon involontaire ou malveillante des données sensibles.

En fonction du budget en cybersécurité de votre organisation, nous recommandons la mise en place d'un profil de contrôle de sécurité si votre organisation traite de l'information de nature très sensible. Pour en savoir plus sur les profils de contrôle de sécurité, consulter le document ITSG-33 — *La gestion des risques liés à la sécurité des TI : une méthode axée sur le cycle de vie* sur notre site Web.

Vous avez des questions ou vous avez besoin d'aide? Vous voulez en savoir plus sur les questions de cybersécurité? Consultez le site Web du Centre canadien pour la cybersécurité (CCC) à **cyber.gc.ca**.