CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Comment protéger votre organisation contre les menaces internes

Mai 2024 ITSAP.10.003

On entend, par **menace interne**, toute personne qui connaît les réseaux, les systèmes ou les données de votre organisation, ou qui y a accès. Ces menaces peuvent être intentionnelles, dans la mesure où l'objectif est de causer des dommages, ou non intentionnelles, comme dans le cas de la négligence d'une ou un employé et d'accidents. Les menaces internes peuvent mettre à risque les membres de votre personnel, votre clientèle, vos actifs, votre réputation et vos intérêts. Il y a toutefois des mécanismes de sécurité que vous pouvez mettre en place afin de réduire ces risques.

Menace interne non intentionnelle

Une ou un employé peut accidentellement porter préjudice à l'infrastructure ou à l'information de votre organisation comme, par exemple, dans les cas suivants :

- s'il perd un dispositif mobile ou un support amovible;
- s'il permet à d'autres employées ou employés d'accéder à de l'information sensible qu'ils n'ont pas l'autorisation de consulter;
- s'il fait une mauvaise gestion de l'information sensible en la laissant à découvert ou en oubliant d'appliquer les autorisations requises.

Menace interne malveillante

Une menace interne malveillante survient lorsqu'une personne utilise sciemment l'infrastructure et l'information de votre organisation pour causer du tort. Elle peut obtenir un accès non autorisé à des comptes généraux ou privilégiés ou utiliser de tels accès de façon abusive. Parmi les facteurs qui motivent la menace interne à accéder de façon non autorisée à ces types de comptes ou à mener des activités interdites, citons les raisons suivantes :

- elle cherche à se venger si elle éprouve des difficultés ou se heurte à un problème en milieu de travail;
- elle est victime de menaces ou d'extorsion;
- elle souhaite obtenir un gain personnel ou financier.

Quiconque est autorisé à accéder à votre infrastructure ou à votre information peut en réalité représenter une menace interne. Il pourrait s'agir, entre autres, de membres du personnel, d'entrepreneures et entrepreneurs ou de partenaires. Ces personnes pourraient tenter de camoufler leurs activités en modifiant les programmes de détection ou en supprimant les dossiers 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 employées et employés ont uniquement les accès dont ils ont besoin pour accomplir leurs tâches, ce qu'on appelle le **principe de droit d'accès minimal**.

Conséquences possibles

Une personne pourrait exposer l'information sensible ou personnelle à laquelle elle aurait accédé sans autorisation. Les menaces internes peuvent donner lieu à d'importantes entorses à la confidentialité, à l'intégrité et à la disponibilité des processus opérationnels et de l'information de votre organisation.

SÉRIE SENSIBILISATION

No de cat. D97-1/10-003-2024F-PDF
ISBN 978-0-660-71500-1

Mesures à prendre contre une menace interne

Si une menace interne réussit à accéder sans autorisation aux réseaux, aux systèmes ou à l'information de votre organisation ou à mener des activités interdites, activez votre plan d'intervention en cas d'incident :

- gérez les contrôles d'accès et limitez l'accès aux comptes administratifs et privilégiés pour prévenir de plus amples dommages;
- localisez et surveillez tous les points terminaux et les dispositifs mobiles, puisqu'une menace interne peut agir à distance;
- vérifiez les journaux de vérification pour relever tout comportement suspect;
- informez les fournisseurs de services tiers si l'activité malveillante risque de s'étendre à leurs systèmes ou si elle provient de leurs systèmes;
- misez sur l'expérience acquise pour sensibiliser le personnel et offrir de la formation adaptée.

Assurez-vous de suivre les lignes directrices en matière de communication indiquées dans votre plan pour informer les parties prenantes. Si vous n'avez pas encore mis en place un plan d'intervention en cas d'incident, consultez l'ITSAP.40.003, *Élaborer un plan d'intervention en cas d'incident*.

Comment gérer les risques posés par les menaces internes

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

Politiques et procédures

Mettez en place des politiques et des procédures pour établir clairement les exigences de votre organisation en matière de sécurité. Vos politiques et procédures devraient définir le comportement attendu de l'ensemble des utilisatrices et utilisateurs lorsqu'ils utilisent des réseaux, des systèmes ou de l'information de l'organisation. Pour prévenir les menaces internes, vos politiques doivent mettre de l'avant les sujets suivants :

- Présélection des employées et employés
  - procédez aux évaluations de l'intégrité et aux vérifications des antécédents initiales et périodiques des membres du personnel qui traitent de l'information sensible;
  - mettez en œuvre des plans de mutation interne et de départ, comme procéder à des entrevues de fin d'emploi;
- Formation et sensibilisation obligatoires en matière de cybersécurité
  - abordez des sujets tels que les courriels d'hameçonnage, l'exposition aux maliciels et les risques associés aux médias sociaux;
  - adaptez les séances de formation de manière à ce qu'elles portent sur les menaces et les contrôles de sécurité propres à l'organisation;
  - offrez des formations d'appoint et de sensibilisation à la sécurité;
- Ententes sur la sécurité avec les partenaires et les parties prenantes
  - assurez-vous que les données de l'organisation sont conservées en sol canadien pour renforcer la protection des données en vertu des pouvoirs juridiques du Canada;
  - surveillez et consignez les activités en assurant le suivi des personnes qui accèdent aux données et les moments où elles y accèdent;
  - déterminez la fiabilité des partenaires et établissez des relations de confiance à long terme avec ces derniers.

Pour en savoir plus

- *Les 10 mesures de sécurité des TI : No 6, Miser sur une formation sur mesure en matière de cybersécurité* (ITSM 10.093)
- *Gestion de l'identité des justificatifs d'identité et de l'accès (GIJIA)* (ITSAP.30.018)

Contrôle de l'accès

Le contrôle de l'accès permet de restreindre de manière sélective l'accès d'une utilisatrice ou un utilisateur à des réseaux, à des systèmes et à des données grâce à l'adoption de mécanismes d'authentification et d'autorisation. Les employées et 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 de droit d'accès minimal** dans l'attribution de privilèges d'administrateur et d'accès aux comptes;
- mettre en place des méthodes d'authentification multifacteur conformément aux *Étapes à suivre pour déployer efficacement l'authentification multifacteur* (ITSAP.00.105);
- assurer la **règle d'intégrité par deux personnes** (TPI pour *Two-Person Integrity*);
    - la TPI est un système selon lequel deux personnes autorisées sont requises pour effectuer une tâche, interdisant ainsi toute activité individuelle;
    - elle peut aider votre organisation à sécuriser le matériel ou les opérations critiques;
- révoquer les accès aux comptes et les privilèges d'administrateur qui ne sont plus requis comme, par exemple, si une utilisatrice ou 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;
- établir des listes d'applications autorisées et interdites pour protéger l'information.

Pour en savoir plus

- *Les 10 mesures de sécurité des TI : No 3 – Gestion et contrôle des privilèges d'administrateur* (ITSM.10.094)
- *L'organisation bénévole et l'accès sécurisé* (ITSM.30.010)

Vérifications

La vérification vous permet de recueillir, d'analyser et de conserver les données et les journaux qui sont associés aux activités que mènent les utilisatrices et utilisateurs sur les systèmes d'information. Vous pouvez entre autres utiliser les journaux de vérification pour gérer les risques associés aux menaces internes d'une des manières suivantes :

- surveiller les activités et les consigner en détail afin de détecter tout comportement inhabituel;
- consigner les activités et les événements, puis inscrire l'heure et la date qui leur sont associées;
- passer régulièrement en revue les changements administratifs;
- faire le suivi des dispositifs mobiles appartenant à l'organisation;
- adopter des stratégies de gestion des informations et des événements de sécurité (GIES).

Pour de plus amples renseignements, prière de consulter l'ITSAP.80.086, *Vérification de la sécurité des réseaux.*

Prévention de la perte de données

Un logiciel de prévention de la perte de données permet à votre organisation de détecter et de prévenir 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 utilisatrices et utilisateurs de communiquer des données sensibles de façon involontaire ou malveillante.

Selon le 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. Prière de consulter le *Catalogue des contrôles de sécurité* (ITSG-33) pour en apprendre plus sur la sélection des contrôles de sécurité et protéger vos systèmes d'information.