Devolutions

# Comment les PME peuvent détecter, stopper et prévenir les attaques internes

JUILLET 2025

# RÉSUMÉ

Depuis plusieurs années, les organisations sont conseillées, incitées — et parfois même sommées — par les instances réglementaires et les compagnies d'assurance à se protéger activement contre les cybercriminels. Et si cette mise en garde reste d'actualité, un autre danger, souvent négligé, plane sur le champ de bataille de la cybersécurité : **les menaces internes**. Ces dernières peuvent s'avérer tout aussi coûteuses et perturbatrices que les attaques provenant de l'extérieur.

Dans ce document technique, nous examinons en profondeur « l'ennemi de l'intérieur » et abordons les points suivants :

- **La définition des menaces internes**
- **L'impact des attaques internes**
- **Les menaces internes et les petites et moyennes entreprises (PME)**
- **Les types d'attaques internes**
- **Les indicateurs d'attaques internes**
- **7 stratégies pour aider les PME à détecter, arrêter et prévenir les attaques internes**

# QUE SONT LES MENACES INTERNES?

TechTarget définit une menace interne comme une « **catégorie de risque posée par des personnes ayant accès aux actifs physiques ou numériques d'une organisation** ».

Il est important de préciser que le terme « personnes internes » ne désigne pas uniquement les employés actuels. **Il englobe également les stagiaires, les contractuels, les fournisseurs, les partenaires commerciaux, les anciens employés ou toute autre personne ayant (ou ayant eu) un accès autorisé aux systèmes et réseaux de l'organisation.**

Non, cela ne signifie pas que toutes ces personnes doivent immédiatement être considérées comme des suspects prêts à voler des données ou à commettre des vols d'identité ! Mais cela montre bien que la surface d'exposition potentielle aux menaces internes est immense — et bien plus vaste que ce que de nombreuses organisations imaginent. Nous explorerons de plus près ces coûts et conséquences potentiels dans la prochaine section.

# L'IMPACT DES ATTAQUES INTERNES

En matière de cybersécurité, de nombreuses organisations concentrent leurs efforts — à des degrés divers — sur la défense contre les pirates informatiques. Cet aspect est essentiel, mais il est loin d'être suffisant. **Il est tout aussi crucial de se prémunir activement contre les attaques internes.** Considérez les faits suivants :

- Les auteurs du Verizon Data Breach Investigations Report 2025 déclarent : « Nous avons observé de nombreux cas où des personnes internes ont abusé de leurs accès pendant des années avant d'être découvertes. »
- Selon le Cost of a Data Breach Report 2024 d'IBM, **le coût moyen d'une violation de données causée par un initié malveillant s'élève à 4,99 millions de dollars par incident.**

Le *Insider Threat Report 2024* publié par Cybersecurity Insiders révèle que **83% des organisations ont signalé au moins une attaque interne au cours de la dernière année.**

Par ailleurs, l'impact d'un risque lié aux menaces internes non géré dépasse largement le simple coût financier — parfois vertigineux. **Il peut aussi engendrer des sanctions réglementaires, compliquer les réclamations d'assurance, miner la confiance entre équipes et départements, nuire à la réputation de l'organisation sur le marché et affaiblir sa capacité de détection et de réponse.** Parmi toutes ces conséquences, la dernière est particulièrement préoccupante. En effet, une fois qu'un initié « ouvre la porte » à une compromission de comptes ou à une exfiltration de données, **il peut tracer un chemin que d'autres cybercriminels externes suivront par la suite — entraînant encore plus de pertes et de dommages.**

# MENACES INTERNES ET PME

Dans le **Portrait de la sécurité informatique chez les PME québécoises de Devolutions, 78% des PME ont déclaré être « préoccupées » par les menaces internes**. Il s'agit d'une augmentation de 45% par rapport à 2023, et d'un progrès certain puisque la sensibilisation est essentielle.

Cependant, l'enquête de Devolutions a également révélé que **82% des PME ne surveillent pas activement les risques liés aux menaces internes.** Plus inquiétant encore, **28% des PME n'ont aucun plan pour gérer ces menaces — ou ne les considèrent pas comme une priorité.**

L'implication est claire : bien que la **plupart des PME soient conscientes du problème, une grande majorité ne transforme pas cette compréhension en actions stratégiques concrètes.** Malheureusement, les menaces internes ne disparaîtront pas d'elles-mêmes. Au contraire, elles deviendront de plus en plus dangereuses et coûteuses à mesure que la valeur des données volées — qu'elles soient exploitées par des initiés malveillants ou revendues sur le dark web — augmentera.

Dans la suite de ce document technique, nous explorerons des méthodes éprouvées et pratiques permettant aux PME d'atténuer les risques de menaces internes. Commençons par examiner les différents types de menaces internes, ainsi que certains indicateurs de risque.

# TYPES D'ATTAQUES INTERNES

En général, les incidents liés aux attaques internes se classent dans l'une des quatre grandes catégories suivantes : **malveillantes, accidentelles, négligentes et collusoires.**

**Malveillantes :** Ces attaques sont menées par des personnes conscientes que leurs actions nuiront à l'organisation. Ces individus peuvent être motivés par différents facteurs, comme la cupidité ou des rancunes personnelles.

**Accidentelles:** Ces incidents résultent d'erreurs involontaires (bien que parfois extrêmement maladroites). Par exemple, un employé peut cliquer sur un lien dans un courriel qu'il croyait légitime, mais qui provenait en réalité de pirates dans le cadre d'une campagne d'hameçonnage. Ou encore, un fournisseur peut envoyer un document à un tiers sans se rendre compte qu'il s'agissait d'un fichier confidentiel. Bien qu'elles ne soient pas intentionnelles, les conséquences de ces erreurs accidentelles peuvent s'avérer extrêmement coûteuses.

**Négligentes:** Ces attaques découlent du non-respect délibéré d'une règle (ou de plusieurs), sans toutefois qu'il y ait intention de compromettre la sécurité. Par exemple, un employé peut choisir de contourner une politique en stockant des données sensibles de l'entreprise dans son compte personnel de stockage infonuagique (comme Google Drive, OneDrive ou DropBox), parce que cela lui semble plus pratique. Bien que cette conduite soit injustifiable — et puisse mener à un congédiement, voire à des poursuites — il est important de souligner que la personne impliquée, bien que négligente et imprudente, n'avait pas l'intention de nuire à l'organisation.

**Collusoires:** Ces attaques sont le fruit d'une collaboration entre un initié (ou un groupe d'initiés) et des cybercriminels externes, dans le but de commettre une fraude, un vol de propriété intellectuelle ou encore des actes d'espionnage. Il est crucial que les organisations ne considèrent pas ce type de menace comme « sensationnaliste » — c'est-à-dire que seules les grandes entreprises multinationales de renom (comme celles du classement Fortune 100) devraient s'en inquiéter, alors que les PME seraient à l'abri en raison de leur profil plus discret. En réalité, toutes les organisations, peu importe leur taille ou leur secteur, sont exposées à ce type de risque. Un sondage mené par Bravura Security révèle que 65% des cadres dirigeants ou de leurs employés ont été approchés par des pirates informatiques pour collaborer à des attaques par rançongiciel.

# TYPES D'INDICATEURS D'ATTAQUES INTERNES

Certaines cyberattaques sont évidentes. Par exemple, les victimes de rançongiciels n'ont pas à se demander si elles sont attaquées : les preuves sont claires (et terrifiantes), accompagnées d'une demande de paiement et d'un compte à rebours inquiétant.

**À l'inverse, les attaques menées par des initiés sont généralement beaucoup plus insidieuses et difficiles à détecter, car elles se déroulent en coulisses — parfois durant des mois, voire des années.** Voici quelques signes pouvant indiquer qu'une attaque interne est en cours ou imminente :

**Escalade de privilèges :** Un employé élève ses privilèges d'accès (s'il est capable de le faire lui-même), ou demande un accès accru sans justification d'affaires claire.

**Accès anormal aux systèmes :** Un employé accède à des ressources auxquelles il a techniquement droit (donc sans avoir besoin d'escalade de privilèges), mais sans raison évidente. Par exemple, un membre de l'équipe des ventes consulte des bases de données ou systèmes utilisés par l'équipe des finances. Bien que cela puisse être légitime, cela peut également signaler une activité suspecte ou préparatoire à une attaque.

**Exfiltration anormale de données :** Un employé commence soudainement à télécharger des données sensibles, un comportement incohérent avec ses activités passées ou celles de ses collègues occupant des fonctions similaires. Un exemple fréquent : un employé sur le départ copie des données confidentielles pour en tirer un avantage personnel ou les utiliser dans son prochain emploi (nous verrons plus loin comment gérer la désactivation des comptes lors d'un départ).

**Séquence d'activités douteuses :** Un employé effectue des actions qui, prises individuellement, ne sont pas nécessairement suspectes. Cependant, la séquence (et parfois la rapidité) de ces actions soulève des questions. Par exemple, un employé renomme un fichier, puis le télécharge sur un appareil personnel. Cela peut indiquer une tentative délibérée de contourner les règles pour s'approprier le fichier — même si son intention exacte demande à être clarifiée.

**Changements d'attitude :** Il s'agit du signe le moins « noir ou blanc » de cette liste, mais il peut s'avérer très révélateur. Un employé qui adopte soudainement un comportement secret et furtif — ou à l'autre extrême, menaçant et intimidant — pourrait être en train de mener une attaque interne. Il faut également garder à l'esprit que certaines personnes peuvent être contraintes ou manipulées par des cybercriminels, ce qui peut entraîner des changements de comportement inhabituels et imprévisibles.

Avant d'aborder ce que les PME peuvent faire pour réduire les risques liés aux menaces internes, il est important de souligner que, sauf dans les cas les plus flagrants (par exemple, un employé pris sur le fait à accéder à des comptes interdits ou à voler des données sensibles), ces signes ne sont que des indicateurs potentiels. Ils méritent une enquête rigoureuse, documentée et menée avec discrétion.

# 7 STRATÉGIES POUR AIDER LES PME À DÉTECTER, STOPPER ET PRÉVENIR LES ATTAQUES INTERNES

Jusqu'ici, nous avons examiné ce que sont les menaces internes, qui en sont les auteurs, et comment elles peuvent se manifester. Passons maintenant à sept stratégies concrètes qui peuvent aider les PME à réduire considérablement leur risque d'être victimes d'une attaque interne.

### 1. Mettre en place une stratégie complète de gestion des menaces internes

Comme mentionné précédemment, selon le sondage *État de la sécurité TI dans les PME 2024/25* de Devolutions, la sensibilisation aux menaces internes est passée de 33% à 78% en un an. Pourtant, durant la même période, **la proportion de PME disposant d'une stratégie complète pour gérer ces menaces n'a augmenté que de 15% à 20%.**

De nombreuses PME adoptent des outils qui renforcent leur posture de cybersécurité, comme la gestion des accès privilégiés (PAM) ou l'authentification multifacteur (MFA). **Cependant, sans intégrer ces outils dans une stratégie globale face aux menaces internes, l'organisation reste vulnérable.**

Les PME doivent combler l'écart entre sensibilisation et action, en harmonisant leurs politiques de sécurité avec leurs pratiques de surveillance et de gestion du cycle de vie des employés (recrutement/départ — un point que nous aborderons plus en détail dans la prochaine stratégie). Ces éléments doivent être intégrés dans les flux de gestion des accès et de formation, et inclus dans le plan global de réponse aux incidents. Chaque intervenant doit savoir quoi faire, quand agir et dans quel ordre en cas d'attaque — quelle qu'en soit l'origine. **Les PME sont averties : traiter les menaces internes comme des cas marginaux est une erreur.** Il est bien plus judicieux de les considérer comme inévitables, et d'être prêtes à y répondre efficacement — plutôt que de réagir dans la panique.

## 2. Révoquer les accès des employés quittant l'entreprise

Aujourd'hui, un employé changera en moyenne 12 fois de poste au cours de sa carrière — souvent davantage. Quel est le lien avec la prévention des menaces internes ? Ce chiffre en appelle un autre, plus inquiétant : un sondage de Beyond Identity révèle **qu'un ex-employé sur quatre conserve des accès à des comptes de ses anciens emplois — y compris d'anciens membres du personnel TI et des gestionnaires ayant eu accès à des comptes privilégiés.**

Certes, on peut supposer que la majorité de ces anciens employés ne représentent pas une menace. Mais il suffit d'un seul individu — motivé par la rancune, la cupidité ou victime de compromission — pour provoquer une attaque destructrice.

De plus, ces anciens employés peuvent eux-mêmes être victimes d'attaques. Leurs identifiants, s'ils sont stockés dans un fichier Excel, dans un navigateur ou dans un gestionnaire de mots de passe peu sécurisé, peuvent être subtilisés par des cybercriminels.

Le message pour les PME est clair : **comblez cette lacune en mettant en place un processus normalisé de gestion des départs.** Ce processus devrait inclure au minimum les étapes suivantes :

- **Changer immédiatement les mots de passe** de l'employé afin de bloquer toute tentative de connexion. S'il existe une raison légitime pour qu'il accède encore à certains éléments, une demande officielle pourra être soumise.

- **Désactiver ou verrouiller tous les comptes.** La désactivation est préférable, puisqu'elle empêche tout accès futur. Toutefois, il peut être nécessaire de verrouiller certains comptes temporairement, le temps d'archiver les données ailleurs — après quoi les comptes devraient être désactivés.

- **Modifier les mots de passe de tous les comptes privilégiés partagés**, tels que les comptes administrateurs de domaine, les comptes administrateurs locaux, les comptes d'accès d'urgence, les comptes d'application, les comptes système et les comptes de service. Selon des recherches de Forrester, 74% des violations de données impliquent des identifiants privilégiés compromis.

### 3. Appliquer le principe du moindre privilège (POLP)

Une méthode éprouvée et pragmatique pour aider les PME à réduire leur exposition aux menaces internes (ainsi qu'aux menaces externes) consiste à appliquer le principe du moindre privilège (POLP). Cette politique vise à n'accorder à chaque utilisateur — employé, contractuel, stagiaire ou toute autre personne nécessitant un accès légitime — que les privilèges strictement nécessaires à l'exécution de ses tâches.

**Pour instaurer et appliquer le principe, les PME devraient :**

- **Faire du moindre privilège le point de départ par défaut**, puis ajouter les accès de niveau supérieur en fonction des besoins, après analyse et en concertation avec les utilisateurs.
- **Utiliser des identifiants à usage unique** lorsqu'un accès privilégié temporaire est nécessaire. Ceux-ci doivent être fournis au dernier moment, puis immédiatement révoqués après usage. Cette approche, appelée « *privilege bracketing* », s'applique autant aux utilisateurs individuels qu'aux processus et systèmes.
- **Séparer les comptes administrateurs des comptes standards.**
- **Séparer les fonctions systèmes de haut niveau de celles de bas niveau.**
- **Consigner automatiquement toutes les tentatives de connexion** (y compris les échecs) et les activités. Il est essentiel d'avoir une visibilité complète sur ce que font les utilisateurs.
- **Auditer régulièrement les privilèges des utilisateurs** afin de s'assurer que les accès sont toujours appropriés.
- **Prévoir la possibilité de révoquer automatiquement les privilèges d'un utilisateur** en cas d'urgence.

**ASTUCE BONUS :** Avec Devolutions Hub Business, les PME peuvent centraliser la gestion des accès tout en appliquant le POLP — sans nuire à l'agilité des équipes. De plus, Remote Desktop Manager et Devolutions PAM permettent de configurer des contrôles d'accès granulaires parfaitement adaptés au POLP.

## 4. Établir un cadre de sécurité de type *Zero Trust*

Le principe fondateur du modèle Zero Trust est : **« ne jamais faire confiance, toujours vérifier »**. Cela signifie que chaque utilisateur, appareil et application doit être authentifié et autorisé avant de pouvoir accéder à des ressources — peu importe sa localisation physique. Cette approche limite considérablement la capacité des initiés malveillants à obtenir et maintenir un accès non autorisé aux systèmes et réseaux sensibles.

Pour instaurer un cadre *Zero Trust*, les PME devraient :

- **Remplacer les services et systèmes hérités non authentifiés par des technologies infonuagiques.** Cela facilite notamment l'adoption de méthodes d'authentification sans mot de passe, comme les passkeys (voir l'astuce bonus ci-dessous).
- **Concevoir l'architecture *Zero Trust* selon la manière dont les données circulent dans le réseau**, et la façon dont les utilisateurs et les applications accèdent à l'information sensible.
- **Vérifier les droits d'accès en temps réel** à l'aide de l'authentification multifacteur (MFA).
- **Étendre les contrôles d'identité aux points d'extrémité** afin de reconnaître et valider tous les appareils.
- **Organiser les utilisateurs par groupes ou rôles** pour faciliter l'application des politiques de gestion des appareils.
- **Automatiser la désactivation des accès**, et prévoir la capacité d'effacer, verrouiller ou désinscrire les appareils perdus ou volés.
- **Mettre à jour régulièrement les droits des utilisateurs**, en fonction de l'évolution de leurs rôles, des politiques de sécurité en vigueur ou des exigences de conformité.

**ASTUCE BONUS :** Chez **Devolutions**, nous avons adopté les passkeys en les intégrant à nos produits et services. L'extension de navigateur **Devolutions Workspace** permet aux utilisateurs d'enregistrer leurs clés d'accès dans **Devolutions Hub Business** (infogéré), ou dans des sources de données avancées auto-hébergées comme **Devolutions Server** et **Devolutions Hub Personal**.

### 5. Mettre en œuvre des solutions de surveillance avancées

Comme mentionné précédemment, les attaques internes sont souvent plus difficiles à détecter que les attaques externes. **Les solutions de surveillance avancées offrent donc un avantage considérable aux PME.** Par exemple, les outils d'analyse du comportement des utilisateurs et des entités (User and Entity Behavior Analytics – UEBA) utilisent des algorithmes d'apprentissage automatique et des analyses comportementales pour surveiller l'activité des utilisateurs et signaler automatiquement les anomalies pouvant indiquer une menace interne potentielle.

### 6. Réaliser régulièrement des audits de sécurité

Les audits de sécurité permettent de vérifier si les pratiques et solutions en place sont réellement efficaces pour atténuer les risques liés aux menaces internes. **Ces évaluations doivent être approfondies, et non superficielles.** Elles doivent couvrir des aspects tels que les politiques de sécurité, les autorisations et les contrôles d'accès.

Il est également essentiel de réviser le plan de réponse aux incidents — qui, comme mentionné plus tôt, devrait intégrer une procédure spécifique pour les menaces internes — et de le mettre à jour au besoin.

### 7. Offrir de la formation aux employés

Selon le *Insider Threat Report 2024 de* **Cybersecurity Ventures**, 32% des répondants ont indiqué qu'un manque de formation et de sensibilisation était un facteur majeur contribuant aux attaques internes. Et cela ne concerne pas uniquement les incidents dus à la négligence ou à des erreurs.

Une formation continue en cybersécurité contribue à instaurer une **culture de sécurité. Lorsque les employés savent que l'organisation accorde une importance sérieuse à la sécurité des TI, ils sont plus enclins à faire preuve de rigueur — et moins susceptibles d'enfreindre les règles, que ce soit volontairement ou accidentellement.**

# LE MOT DE LA FIN

Le paysage des cybermenaces ne se limite pas à la défense contre les pirates externes. **Tout comme les grandes entreprises, les PME doivent également prendre en compte les menaces internes — qu'elles soient causées par des erreurs, de la négligence ou des intentions malveillantes** — et mettre en place des mesures pour les atténuer.

Adopter une posture proactive et mettre en œuvre les stratégies présentées dans ce rapport pourrait faire toute la différence entre une trajectoire stable et fructueuse, ou un parcours chaotique et coûteux pour les PME.

# DEVOLUTIONS: À VOS CÔTÉS, DANS VOTRE ÉQUIPE

**Chez Devolutions, nous proposons plusieurs solutions — dont certaines ont été mises en avant dans ce document technique — pour aider les PME à protéger leurs données, leurs actifs et leur réputation contre les dommages causés par les attaques internes.**

**Nos solutions sont faciles à utiliser, évolutives, abordables, et conçues spécialement pour les PME qui souhaitent renforcer leur cybersécurité sans nuire à l'efficacité ni à la productivité.**

**Pour en savoir plus, communiquez avec notre équipe à sales@devolutions.net. Découvrez comment nous pouvons vous aider à lutter efficacement contre les menaces internes, tout en consolidant votre posture globale en cybersécurité.**