Devolutions

# 7 ACTIONS RAPIDES POUR LA CYBERSÉCURITÉ DES PME

## EN 2025

19 MARS 2025

Les **petites et moyennes entreprises (PME) d'aujourd'hui sont la cible d'attaques incessantes** de la part des hackers, qui trouvent à la fois pratique et rentable de s'en prendre aux petites organisations plutôt qu'aux grandes. Voici quelques chiffres révélateurs:

- Selon une étude d'Accenture, **43% de l'ensemble des cyberattaques dans le monde visent désormais les PME.**

- Un rapport d'IBM et du Ponemon Institute indique que le **coût moyen d'une violation de données pour une PME a atteint 2,98 millions de dollars par incident.**

- L'enquête de Devolutions sur l'état de la sécurité informatique des PME en 2023 a révélé que **78% des PME sont plus préoccupées par la cybersécurité qu'il y a un an**, et que **69% d'entre elles ont subi au moins une cyberattaque au cours des 12 derniers mois**.

En effet, pour chaque violation de données touchant une grande entreprise et faisant les gros titres – comme l'attaque SolarWinds en 2019-2020 –, des milliers de cyberattaques sont menées contre des PME, avec des conséquences allant de lourdes pertes financières à des catastrophes totales. D'ailleurs, **60% des PME ferment définitivement leurs portes dans les six mois** suivant une violation de données.

# EFFICACE, ABORDABLE ET FACILE À GÉRER

Ce livre blanc présente sept actions rapides pour **aider les PME à renforcer leur posture en cybersécurité, à réduire leur surface d'attaque et à minimiser leurs risques d'être ciblées en 2025 et au-delà**. De plus, ces sept stratégies tiennent compte du fait que les PME ne disposent généralement ni des budgets conséquents ni des équipes spécialisées en cybersécurité que l'on trouve dans les grandes entreprises. Ainsi, les conseils et recommandations proposés ne sont pas seulement très efficaces, mais aussi **particulièrement abordables et faciles à mettre en œuvre pour les PME.**

## #1
## METTRE EN PLACE UNE GESTION DES ACCÈS À PRIVILÈGES (PAM)

La gestion des accès privilégiés (PAM) regroupe des solutions permettant de sécuriser, contrôler, gérer et surveiller l'accès aux comptes critiques – autrement dit, les « clés du royaume ». Ces comptes incluent notamment :

- Comptes administrateurs de domaine
- Comptes utilisateurs à privilèges
- Comptes administrateurs locaux
- Comptes d'accès d'urgence
- Comptes applicatifs
- Comptes système
- Comptes de service de domaine

Lorsqu'un de ces comptes est utilisé, une solution PAM enregistre la session et suit les actions effectuées, garantissant ainsi que seuls les utilisateurs autorisés accèdent aux bons comptes au bon moment.

**Pour choisir une solution PAM adaptée, les PME doivent éviter les offres coûteuses et complexes aux nombreuses fonctionnalités superflues. Il est préférable de privilégier une solution qui propose des fonctionnalités essentielles comme :**

- **Gestion polyvalente des comptes :** intégration d'Active Directory, Entra ID (anciennement Azure AD), des utilisateurs locaux SSH et des bases de données (MySQL, Oracle, Microsoft SQL).
- **Rotation et propagation des mots de passe :** mise à jour automatique des mots de passe sur l'ensemble des systèmes.
- **Contrôle d'accès granulaire basé sur les rôles :** application efficace du principe du moindre privilège (POLP) en définissant des rôles et leurs droits d'accès spécifiques. Ce principe sera détaillé plus loin dans ce livre blanc.
- **Élévation Juste-à-Temps (JAT) :** octroi temporaire de privilèges élevés dans Active Directory ou les groupes Azure pour une tâche ou une période définie.
- **Processus d'approbation personnalisables :** régulation des accès avec des exigences d'approbation et des destinataires paramétrables.

**Devolutions PAM** est une plateforme de sécurité essentielle conçue pour contrôler, surveiller et sécuriser les accès à privilèges des utilisateurs, comptes, processus et systèmes. Elle est particulièrement adaptée aux PME, qui disposent généralement de budgets de cybersécurité plus restreints et de moins de ressources internes spécialisées que les grandes entreprises. Devolutions PAM se distingue par son prix abordable, sa simplicité d'utilisation et sa capacité à évoluer avec les besoins des PME.

# #2

## UTILISER UN GESTIONNAIRE DE MOTS DE PASSE POUR APPLIQUER DES POLITIQUES STRICTES

Selon une étude de LastPass, **81% des violations de sécurité confirmées sont causées par des mots de passe faibles, réutilisés ou volés**. Et en matière de mots de passe faibles, le classement 2024 des 200 mots de passe les plus courants, publié par NordPass en collaboration avec NordStellar, révèle que **«123456»** occupe encore une fois la première position. **La majorité des mots de passe de cette liste peuvent être piratés en moins d'une seconde**. Les cybercriminels sont bien conscients de cette vulnérabilité et l'exploitent sans difficulté.

Malgré cette menace, de nombreuses PME ne font pas le nécessaire pour assurer une visibilité complète sur les mots de passe utilisés, alors que cela est essentiel pour appliquer des règles d'accès, surveiller la conformité et garantir une gouvernance efficace. L'enquête de Devolutions sur l'état de la sécurité informatique des PME en 2023 a révélé que **moins de 60 % des PME utilisent un gestionnaire de mots de passe**, pourtant une mesure de cybersécurité essentielle.

Une solution robuste de gestion des mots de passe permet aux PME d'avoir une visibilité complète sur les pratiques des utilisateurs tout en leur facilitant la création de mots de passe complexes et uniques, pratiquement impossibles à pirater.

De plus, les utilisateurs n'ont plus à mémoriser plusieurs mots de passe longs et complexes. Ils peuvent stocker toutes leurs informations d'identification (ainsi que d'autres données sensibles comme des codes d'alarme et des clés de licence logicielle) dans des coffres-forts sécurisés, accessibles uniquement en cas de besoin.

**Lors de la sélection d'un gestionnaire de mots de passe, les PME doivent s'assurer que la solution inclut les fonctionnalités suivantes :**

- **Sécurité renforcée des mots de passe :** création, stockage, partage et gestion des mots de passe sans risque de fuite ou de piratage.
- **Protection de niveau entreprise :** chiffrement AES 256 bits et respect des meilleures pratiques en matière de sécurité des données (notamment pour les solutions basées sur le cloud).
- **Outils avancés :** générateur de mots de passe forts, accès par navigateur avec injection automatique des identifiants et analyse de la sécurité des mots de passe.
- **Rapports complets :** génération rapide de rapports pour la conformité, la gouvernance et l'audit, incluant journaux d'activité, rapports d'utilisation et suivis administratifs.

**Devolutions Hub Business** garantit une hygiène stricte des mots de passe grâce à une gestion centralisée et hautement sécurisée dans le cloud. Cette solution utilise un chiffrement robuste, ainsi que des algorithmes surpassant ceux de nombreux autres gestionnaires de mots de passe basés sur le cloud. Comme toutes les solutions **Devolutions, Hub Business** est abordable pour les PME, offrant une gestion des mots de passe de niveau entreprise sans nécessiter un budget de cybersécurité équivalent.

# #3

# FONDER SA CYBERSÉCURITÉ SUR LE PRINCIPE DU MOINDRE PRIVILÈGE ET LE ZERO TRUST

Le principe du moindre privilège repose sur l'attribution aux utilisateurs uniquement des accès dont ils ont besoin pour accomplir leur travail. Quant au Zero Trust, son principe fondamental est «ne jamais faire confiance, toujours vérifier» : chaque utilisateur, appareil et application, quel que soit son emplacement, doit être authentifié et autorisé avant d'accéder aux ressources. **Ces deux approches sont complémentaires et constituent une base solide pour une cybersécurité efficace.**

**Mise en place et application du principe du moindre privilège**
Pour établir et appliquer le principe, les PME doivent :

- **Adopter le moindre privilège comme point de départ**, puis accorder des accès supplémentaires uniquement après analyse et concertation avec les utilisateurs.
- **Expliquer aux employés l'objectif du principe**, en insistant sur le fait qu'il ne vise pas à limiter leur productivité, mais à protéger l'organisation.
- **Utiliser des identifiants temporaires à usage unique** pour les accès privilégiés ponctuels. Cette approche, appelée **«privilege bracketing»,** consiste à accorder des accès au dernier moment, puis à les révoquer immédiatement après utilisation. Elle s'applique aussi bien aux utilisateurs qu'aux processus et systèmes.
- **Séparer les comptes administrateurs des comptes standards.**
- **Distinguer les fonctions critiques des fonctions de moindre importance** au sein des systèmes.
- **Suivre automatiquement toutes les tentatives de connexion** (réussies ou non) et les activités des utilisateurs pour une visibilité totale sur qui fait quoi et quand.

- **Auditer régulièrement les privilèges des utilisateurs** pour s'assurer qu'ils sont toujours appropriés.
- **Mettre en place un processus de suppression des accès pour les employés quittant l'entreprise.** Une enquête Beyond Identity a révélé que 1 ancien employé sur 4 pouvait encore accéder aux comptes de son ancien poste, y compris des ex-membres de l'IT et des managers ayant des accès privilégiés.
- **Pouvoir révoquer automatiquement les accès privilégiés en cas d'urgence.**

### Mise en place et application du Zero Trust

Pour instaurer une architecture Zero Trust, les PME doivent :

- **Remplacer progressivement les services et systèmes obsolètes non authentifiés** par des technologies cloud sécurisées.
- **Concevoir une architecture Zero Trust en fonction des flux de données** et des interactions entre utilisateurs, applications et informations sensibles.
- **Exiger une authentification multifactorielle (MFA) en temps réel** pour valider l'accès aux ressources réseau.
- **Étendre les contrôles d'identité aux appareils** pour vérifier et authentifier non seulement les utilisateurs, mais aussi les terminaux.
- **Organiser les utilisateurs en groupes ou rôles** pour faciliter l'application des politiques d'accès aux appareils.
- **Automatiser la révocation des accès** et permettre l'effacement, le verrouillage ou la désinscription des appareils perdus ou volés.
- **Mettre à jour régulièrement les droits des utilisateurs** en fonction de l'évolution de leurs rôles et des exigences de sécurité.

**Devolutions Remote Desktop Manager** et **Devolutions PAM** permettent aux PME de configurer et d'appliquer des contrôles d'accès granulaire, alignés sur les principes du POLP et du Zero Trust. Ces solutions sont faciles à utiliser, évolutives et abordables, offrant aux PME une cybersécurité robuste sans compromettre l'efficacité ni la productivité.

# #4

# AUTOMATISER LA DÉTECTION DES MENACES GRÂCE À L'IA

Les outils de sécurité basés sur l'**intelligence artificielle (IA)** révolutionnent la cybersécurité des PME en permettant une **détection et une réponse aux menaces en temps réel**. Ces solutions réduisent la nécessité d'une supervision manuelle tout en renforçant la capacité à identifier et neutraliser les incidents. Voici quelques-unes de leurs applications les plus importantes et impressionnantes :

**Apprentissage adaptatif :** utilisation de modèles d'apprentissage automatique pour améliorer en continu la détection des menaces.

**Reconnaissance avancée des schémas :** analyse rapide de volumes massifs de données pour identifier des modèles d'attaque et détecter des anomalies, y compris les signes subtils d'activités malveillantes.

**Réponses automatisées :** activation immédiate de mesures d'atténuation et de confinement des menaces.

**Analyse prédictive :** identification proactive des menaces futures en étudiant les tendances et les comportements suspects.

**Réduction des faux positifs :** évaluation plus précise des activités afin de mieux distinguer les actions sûres des activités malveillantes.

Chez Devolutions, nous travaillons actuellement à l'intégration d'analyses basées sur l'IA dans nos outils, afin d'aider les PME à protéger leurs actifs de manière proactive, sans nécessiter une équipe IT importante.

# #5

# ENVOYER DES INFORMATIONS SENSIBLES VIA UNE PLATEFORME DE MESSAGERIE SÉCURISÉE

De nombreuses PME utilisent des applications de messagerie instantanée gratuites comme Slack, Microsoft Teams ou Facebook Messenger pour la communication et la collaboration. Cependant, bon nombre de ces applications ne chiffrent pas les messages, ce qui permet aux hackers de les intercepter discrètement. La solution est simple : **les PME doivent impérativement utiliser un service de messagerie chiffré** pour **toutes les communications et transferts de fichiers privés, confidentiels et sensibles.**

**Une solution de messagerie sécurisée doit répondre aux exigences suivantes :**

- **Chiffrement robuste et autonome :** utilisation du protocole XChaCha20Poly1305 avec des nonces aléatoires. Le chiffrement doit s'effectuer directement dans le navigateur via un programme Rust sécurisé en mémoire compilé en WASM (WebAssembly). De plus, les données doivent être chiffrées au repos et en transit avec TLS 1.2+ via un chiffrement renforcé, et l'UUID v4 doit être utilisé uniquement pour garantir l'unicité des liens.
- **Transfert de fichiers sécurisé :** capacité à chiffrer et envoyer des fichiers, y compris de grande taille (10 Mo ou plus).
- **Sécurité renforcée :** possibilité pour l'expéditeur d'ajouter une couche de protection supplémentaire avec une phrase secrète. Seuls ceux qui connaissent cette phrase peuvent accéder au lien, empêchant ainsi son partage non autorisé.
- **Personnalisation des messages :** option permettant à l'expéditeur de définir la durée de vie du message chiffré. Si le destinataire ne le récupère pas avant expiration, il est automatiquement et définitivement supprimé. En outre, les destinataires doivent pouvoir supprimer les messages après lecture, sauf si l'expéditeur choisit de désactiver cette option.

**Devolutions Send** répond à toutes ces exigences et constitue la solution idéale pour les PME souhaitant partager des informations sensibles et fichiers en toute sécurité. Facile à utiliser, **Devolutions Send** est entièrement gratuit et disponible sous forme de service web autonome, ainsi qu'intégrée dans plusieurs solutions Devolutions, dont **Remote Desktop Manager**, **Devolutions Server**, **Devolutions Hub Business** et **Devolutions Workspace**.

# #6

# MAINTENIR LES MISES À JOUR DES SYSTÈMES ET LA GESTION DES CORRECTIFS

Un logiciel non mis à jour est une porte ouverte aux hackers. Une enquête menée par Sophos en 2024 a révélé que **32% des attaques par ransomware contre les entreprises interrogées au cours de l'année précédente avaient commencé par l'exploitation d'une vulnérabilité**. Plus globalement, **60% des violations de sécurité sont dues à des failles non corrigées**, et **50% des vulnérabilités restent non résolues après 50 jours**, laissant aux cybercriminels tout le temps nécessaire pour infiltrer les réseaux de leurs victimes.

**Différents outils permettent aux PME de gérer efficacement les mises à jour et les correctifs :**

- **Les outils les plus simples** envoient des notifications push lorsqu'une mise à jour ou un correctif est disponible. Toutefois, ces solutions nécessitent une intervention manuelle pour appliquer les mises à jour.
- **Les solutions plus avancées** (et généralement plus coûteuses) analysent proactivement les systèmes et logiciels pour détecter les mises à jour disponibles. Elles peuvent être configurées pour télécharger et installer automatiquement les correctifs à des dates et heures planifiées.

**Devolutions Remote Desktop Manager** permet aux PME de suivre les versions logicielles et d'automatiser l'application des mises à jour et correctifs. Cette approche proactive garantit que l'infrastructure reste résistante face aux nouvelles menaces et aux dernières vulnérabilités exploitées.

# #7

# FORMER RÉGULIÈREMENT LES UTILISATEURS À LA CYBERSÉCURITÉ

Les utilisateurs peuvent renforcer ou compromettre la cybersécurité d'une entreprise. Dans de nombreux cas, les incidents de sécurité ne sont pas intentionnels. En effet, selon le rapport 2023 de Verizon sur les violations de données, **74% des failles sont causées par des erreurs humaines**, comme le fait de cliquer sur un lien de phishing dans un e-mail. Autrement dit, former régulièrement les employés à la cybersécurité est essentiel.

Il n'existe pas de programme de formation universel, car les menaces évoluent constamment. Toutefois, toute formation — qu'elle soit **en ligne, en présentiel ou hybride** — devrait au minimum inclure :

- Contrôle des accès
- Bring Your Own Device (BYOD)
- Services cloud
- Fuites de données
- Usurpation d'identité
- Signalement des incidents
- Propriété intellectuelle

- Logiciels malveillants (malware)
- Sécurité des appareils mobiles
- Risques liés aux réseaux Wi-Fi publics
- Gestion des mots de passe
- Phishing (y compris l'émergence des attaques deepfake basées sur l'IA)
- Sécurité physique
- Protection des données personnelles
- Sécurisation des paiements par carte bancaire
- Ransomware
- Utilisation responsable d'Internet
- Ingénierie sociale
- Réseaux sociaux
- Sécurité en déplacement

Devolutions collabore avec les PME pour intégrer des programmes de formation adaptés à leur environnement, afin que leurs employés deviennent **des acteurs clés d'une cybersécurité fiable et robuste**.

## L'ESSENTIEL À RETENIR

En adoptant ces stratégies **à faible coût et à fort impact**, les PME peuvent efficacement faire face à l'évolution des menaces en 2025 et au-delà. Rappelez-vous : **la cybersécurité n'a pas besoin d'être compliquée** — des actions simples comme celles-ci peuvent faire une réelle différence!

# Besoin d'actions rapides pour sécuriser votre PME? DEVOLUTIONS PEUT VOUS AIDER!

Chez **Devolutions**, nous aidons les PME à relever les défis de la cybersécurité grâce à **des solutions abordables** qui simplifient la gestion des menaces et offrent **des résultats concrets** en matière de **sécurité, conformité et productivité**.

**Contactez-nous dès aujourd'hui à l'adresse** sales@devolutions.net **ou essayez nos solutions gratuitement pendant 30 jours !**