CHECKLIST SÉCURITÉ

Comment sécuriser Microsoft 365 dans votre entreprise

Microsoft 365 est aujourd'hui l'un des socles critiques des PME : e-mails, fichiers, Teams, collaboration, données clients et accès aux applications métiers. Lorsqu'il est mal configuré, il peut devenir un point de vulnérabilité majeur, avec des conséquences immédiates : interruption d'activité, perte de confiance, exposition de données sensibles et coûts de remédiation élevés.

Microsoft 365 intègre déjà de nombreuses fonctions de sécurité, mais leur efficacité dépend de la qualité du paramétrage, du suivi et de l'adoption par les utilisateurs. Cette checklist permet aux dirigeants et responsables IT d'identifier les priorités à traiter, de réduire les angles morts et de sécuriser progressivement leur environnement, en particulier dans un contexte de PME suisses.

UN RISQUE OPÉRATIONNEL, PAS SEULEMENT TECHNIQUE

La migration vers le cloud apporte flexibilité, mobilité et efficacité. Mais elle ouvre aussi de nouveaux accès à protéger : connexions à distance, appareils personnels, partages externes, comptes invités et applications tierces. Le sujet n'est donc pas uniquement informatique ; il concerne directement la capacité de l'entreprise à fonctionner, servir ses clients et protéger ses informations sensibles.

Pour un attaquant, compromettre un compte Microsoft 365 peut donner accès à des e-mails, documents confidentiels, contrats, données clients, conversations Teams et outils métiers. Dans la majorité des cas, les attaques exploitent moins la plateforme Microsoft elle-même que les comptes insuffisamment protégés, les configurations trop permissives ou les habitudes utilisateurs à risque.

DES RÉGLAGES PAR DÉFAUT INSUFFISANTS POUR UNE PME EXPOSÉE

Disposer des bonnes licences Microsoft ne garantit pas automatiquement un bon niveau de sécurité. Une entreprise peut rester exposée si la MFA n'est pas appliquée partout, si les accès externes sont trop ouverts, si les appareils ne sont pas maîtrisés ou si les utilisateurs ne savent pas reconnaître une tentative de phishing.

La sécurité Microsoft 365 doit être pilotée comme une démarche continue : cadrer les priorités, corriger les faiblesses, mesurer les progrès et accompagner les équipes. L'objectif n'est pas d'ajouter de la complexité, mais de réduire les risques tout en conservant une expérience de travail simple et fluide.

CHECKLIST DÉCISIONNELLE : LES MESURES À PRIORISER

01

Activer l'authentification multifacteur pour tous les utilisateurs

L'authentification multifacteur ajoute une étape de vérification lors de la connexion, par exemple via l'application Microsoft Authenticator ou une méthode sans mot de passe. C'est l'une des mesures les plus efficaces pour limiter les compromissions de comptes.

02

Mettre en place des règles d'accès conditionnel

Les règles d'accès conditionnel permettent d'adapter la sécurité selon le contexte : utilisateur, appareil, localisation, niveau de risque ou application utilisée. Elles aident à bloquer les connexions suspectes tout en conservant une expérience fluide pour les usages légitimes.

03

Bloquer les protocoles d'authentification obsolètes

Certains anciens protocoles, comme POP, IMAP ou SMTP Auth, peuvent contourner les protections modernes telles que la MFA. Les désactiver réduit fortement les possibilités d'attaque par vol d'identifiants.

04

Protéger les informations sensibles

Microsoft Purview et les fonctionnalités de protection de l'information permettent d'identifier, classifier et protéger les données sensibles dans les documents et les e-mails. Cette étape est particulièrement importante pour les entreprises manipulant des données clients, financières, RH ou réglementées.

05

Gérer les appareils avec Microsoft Intune ou une solution MDM

La gestion des appareils permet d'appliquer des règles de sécurité aux ordinateurs, smartphones et tablettes utilisés pour accéder à Microsoft 365. Elle facilite aussi l'effacement sélectif des données professionnelles en cas de perte, de vol ou de départ d'un collaborateur.

06

Renforcer la sécurité des e-mails

Les e-mails restent l'un des principaux vecteurs d'attaque. Il est recommandé d'activer les protections anti-phishing, l'analyse des pièces jointes et des liens, ainsi que les mécanismes SPF, DKIM et DMARC pour limiter l'usurpation d'identité.

07

Contrôler les partages externes

SharePoint, OneDrive et Teams facilitent le partage de fichiers avec des partenaires ou clients. Ces usages doivent être encadrés afin d'éviter que des documents sensibles restent accessibles trop largement ou trop longtemps.

08

Suivre régulièrement le Microsoft Secure Score

Le Secure Score donne une indication du niveau de sécurité de l'environnement Microsoft 365. Il permet d'identifier les faiblesses, de prioriser les actions et de suivre l'amélioration de la posture de sécurité dans le temps.

09

Sensibiliser régulièrement les utilisateurs

La technologie ne suffit pas. Les collaborateurs doivent savoir reconnaître un e-mail suspect, réagir face à une demande inhabituelle, signaler un incident et adopter les bons réflexes au quotidien. La formation et la sensibilisation restent des piliers essentiels de la cybersécurité.

UNE DÉMARCHE INDISPENSABLE POUR LES PME SUISSES

Pour les PME suisses, sécuriser Microsoft 365 n'est pas seulement une bonne pratique IT. C'est une mesure de gouvernance qui protège la continuité d'activité, les données clients, la réputation de l'entreprise et la conformité aux exigences de protection des données.

Une configuration adaptée permet de réduire le risque de compromission, de limiter l'impact d'un incident et de démontrer, auprès des clients comme des partenaires, que la sécurité est pilotée de manière sérieuse et proactive.

BESOIN D'ÉVALUER VOTRE ENVIRONNEMENT MICROSOFT 365 ?

Un audit de sécurité Microsoft 365 permet d'obtenir une vision claire et exploitable des risques prioritaires : comptes à risque, accès trop ouverts, absence de MFA, règles de partage mal maîtrisées, protections e-mail insuffisantes ou paramètres de conformité incomplets. L'enjeu n'est pas seulement de détecter les faiblesses, mais de savoir quelles actions mener en premier.

Chez AWSMTECH, nous aidons les PME à passer d'une configuration Microsoft 365 simplement fonctionnelle à un environnement sécurisé, lisible et pilotable. Notre approche combine analyse technique, lecture des risques pour la direction et plan d'action priorisé, afin de renforcer la protection sans complexifier le quotidien des équipes.

Vous souhaitez savoir si votre environnement Microsoft 365 protège réellement votre entreprise ?

AWSMTECH peut réaliser un diagnostic clair de votre configuration et vous fournir un plan d'action priorisé, lisible et directement exploitable.

DEMANDER UN DIAGNOSTIC