Baseline Sécurité

Microsoft 365

Guide pour PME — Microsoft Entra ID & Écosystème M365

> **i** Ce document est conçu pour des équipes avec peu de ressources IT. Chaque section indique clairement la priorité et l'effort attendu. Commencez par les éléments critiques car ils couvrent l'essentiel du risque. Ce guide est destiné à être partagé gratuitement.

Ce guide couvre :

01 - Identités et accès

C'est la porte d'entrée de tout votre environnement. Si un compte est compromis sans protection, tout le reste devient secondaire. Ces mesures doivent être mises en place avant tout le reste.

MFA obligatoire pour tous les utilisateurs

Activer le MFA sur 100 % des comptes, sans exception.

La méthode recommandée est d'utiliser une application telle que Microsoft Authenticator, Google Authenticator, Authy.

Le FIDO2 (clé physique) peut être envisagé pour les profils les plus exposés (ex. Administrateurs).

Accès conditionnel et configuration minimale

L'accès conditionnel permet de définir des règles précises sur qui peut se connecter, depuis où, et dans quelles conditions. À minima :

- Bloquer les connexions provenant de pays non autorisés
- Imposer le MFA pour tout accès depuis l'extérieur du réseau
- Imposer le MFA systématiquement sur les comptes administrateurs
- Désactiver les authentifications legacy (IMAP, POP, SMTP basic auth).

Comptes administrateurs

Les comptes admin sont des cibles prioritaires. Quelques règles importantes :

- Avoir au moins deux comptes administrateurs distincts, dont un compte “break-glass” non utilisé au quotidien
- Ne jamais utiliser un compte admin pour les tâches du quotidien, un compte séparé pour les responsables IT.
- Appliquer le principe de moindre privilège, chaque admin ne doit avoir que les droits strictement nécessaires à sa fonction
- MFA obligatoire + accès conditionnel renforcé sur tous les comptes admin

À configurer	Notes
☐ MFA sur 100% des comptes	
☐ Bloquer legacy authentication	
☐ Accès conditionnel (pays)	
☐ Compte break-glass	

02 - Protection des emails

La grande majorité des incidents commencent par un email. Phishing, pièce jointe malveillante, usurpation d'identité, etc. les emails restent le canal le plus exploité. Microsoft Defender for Office 365 couvre l'essentiel de ce risque.

Anti-phishing et anti-malware

- **Activer Safe Links** : les URL dans les emails sont vérifiées en temps réel avant l'ouverture
- **Activer Safe Attachments** : les pièces jointes sont analysées dans un environnement isolé avant distribution
- Mettre en place **SPF, DKIM et DMARC** sur votre domaine, ces trois mécanismes limitent fortement le spoofing

Paramètres à vérifier en plus

- Désactiver le forwarding automatique vers des adresses externes
- Configurer une alerte sur la création de règles inbox inhabituelles

À configurer	Notes
☐ Safe Links	
☐ Safe Attachments	
☐ SPF / DKIM / DMARC	
☐ Forwarding externe	

03 - Logs, audit et détection

Sans logs, il est impossible de savoir ce qui s'est passé après un incident. Ces paramètres doivent être activés dès le départ.

Activation des logs

- Activer l'Unified Audit Log dans le portail de conformité Microsoft
- Conserver les journaux sur une durée d'au moins 90 jours.

Ce qu'il faut surveiller

Ces événements méritent une alerte immédiate :

- Connexion depuis deux pays impossibles à atteindre dans le même délai
- Désactivation du MFA sur un compte
- Ajout ou modification d'un rôle administrateur
- Création d'une règle de transfert email suspecte
- Création de nouveaux comptes utilisateurs.

04 - Sécurité des endpoints

Un device non géré qui accède à vos données M365, c'est une surface d'attaque que vous ne contrôlez pas. Microsoft Intune permet de s'assurer que les devices connectés respectent vos exigences.

Gestion des appareils professionnels

- Enrôler tous les appareils professionnels dans Intune
- Exiger le chiffrement du disque (BitLocker pour Windows, FileVault pour Mac)
- Exiger un code PIN ou une authentification biométrique à l'écran de verrouillage
- Bloquer l'accès aux ressources M365 depuis des appareils non conformes

Gestion des appareils personnels (BYOD)

Pour les collaborateurs qui utilisent leur propre matériel, la Mobile App Management (MAM) permet d'isoler les données professionnelles sans toucher à leur vie privée :

- Cloisonner les données professionnelles dans Outlook et Teams
- Interdire le copier-coller entre les applications professionnelles et les apps personnelles
- Conserver la capacité d'effectuer un wipe sélectif (données pro uniquement) à distance en cas de perte ou de départ

05 - Données et collaboration

SharePoint et OneDrive sont pratiques et souvent surexposés par défaut. Quelques paramètres simples permettent de limiter significativement les risques de fuite.

SharePoint et OneDrive

- Limiter le partage externe : privilégier une whitelist de domaines ou une validation explicite
- Configurer une expiration automatique sur les liens de partage
- Auditer régulièrement les fichiers et dossiers accessibles publiquement

Sensibilité et protection des données

- Mettre en place des labels de sensibilité si votre licence le permet. Ils permettent de classer et de protéger les documents automatiquement
- Bloquer le téléchargement depuis des appareils non conformes pour les contenus sensibles

06 - Configuration globale du tenant

Ces paramètres de base sont souvent laissés à leur valeur par défaut, alors qu'ils peuvent représenter une exposition significative.

- Désactiver ou encadrer strictement les comptes invités non contrôlés
- Restreindre la possibilité pour les utilisateurs d'enregistrer eux-mêmes des applications OAuth
- Auditer régulièrement les permissions accordées aux applications tierces
- Désactiver tous les protocoles d'authentification legacy restants

07 - Facteur humain

La technique ne suffit pas. Les attaques les plus efficaces ciblent les comportements, pas les systèmes. Une organisation qui forme ses équipes réduit considérablement son exposition réelle.

- Formation au phishing au minimum une fois par an. (https://phishingquiz.withgoogle.com/ donne certaines bases)
- Simulations de phishing régulières pour mesurer concrètement le niveau de vigilance
- Procédure simple et claire pour signaler un email suspect.

08 - Sauvegarde et résilience

⚠ M365 n'est pas une solution de backup. Microsoft garantit la disponibilité de la plateforme, pas la récupération de vos données supprimées ou chiffrées par un ransomware. Une sauvegarde externe est indispensable.

- Mettre en place une solution de backup externe couvrant emails, SharePoint et OneDrive au minimum.
- Tester la restauration régulièrement,un backup qu'on n'a jamais testé n'est pas un backup
- Vérifier les durées de rétention configurées dans M365 pour éviter les mauvaises surprises

09 - Réponse à incident

Ces capacités doivent être documentées et testées avant d'en avoir besoin.

Scénarios à préparer

- Compte compromis : qui prend la décision, qui exécute, dans quel délai
- Phishing interne : comment identifier la portée, comment alerter les destinataires

Capacités techniques à avoir en main

- Réinitialisation de mot de passe en moins de 5 minutes
- Révocation de toutes les sessions actives d'un utilisateur
- Forçage du MFA sur un compte spécifique

10 - Quick Wins
Ce que vous pouvez faire en une journée

ℹ Priorité absolue si vous démarrez de zéro. Ces cinq actions couvrent la majorité du risque avec un effort minimal.
Si vous ne faites qu'une chose, faites ça.

- **MFA activé sur tous les comptes sans exception**
- **Legacy authentication bloquée**
- **Safe Links et Safe Attachments activés**
- **Forwarding automatique externe désactivé**
- **Deux comptes administrateurs sécurisés avec MFA strict**

Repère de maturité

Où en est votre organisation ? Ce tableau permet de situer rapidement votre niveau actuel et d'identifier les prochaines étapes.

Niveau	Ce qui est en place
🟡 **Basique**	MFA activé sur tous les comptes + politique anti-phishing configurée
🟠 **Intermédiaire**	Accès conditionnel opérationnel + endpoints gérés avec Intune
🟢 **Avancé**	Approche Zero Trust + détection automatisée + monitoring continu

ℹ N'hésitez pas à nous contacter pour aller plus loin, former vos équipes, ou mettre en place des solutions adaptées à votre activité. Nous sommes labellisés par la Région Wallonne dans le cadre des **Chèques-Entreprises "Cybersécurité".**

La cybersécurité n'est pas un luxe. C'est une hygiène numérique, aussi essentielle que de verrouiller la porte de votre bureau.

justin.mccarthy@cyberinit.be