

Checklist sécurité Microsoft 365

20 contrôles pour vérifier les identités, la messagerie, le partage et la capacité de réponse aux incidents.

Ressource liée : « Votre entreprise est peut-être déjà piratée. Et personne ne le sait. » sur sunitech.ch

FICHE D'ÉVALUATION

Organisation		Évaluateur	
Domaine principal		Évalué le	
Licence M365		Revue suivante	

Les cellules sur fond jaune pâle sont à compléter ; les résultats se saisissent dans l'onglet 01. La licence détermine les fonctionnalités et la durée des journaux.

INDICATEURS CLÉS

SCORE DE SÉCURITÉ	CONFORMES	NON CONFORMES	AVANCEMENT
n.d. Évaluation à démarrer Base : 0 contrôle(s) évalué(s)	0 sur 20 contrôles + 0 partiellement conforme(s)	0 dont 0 à priorité immédiate Échéances dépassées : 0	0% des 20 contrôles évalués Non applicables : 0

SCORE PAR DOMAINE

Domaine	Conformes	Partiels	Non conformes	Non évalués	Score
1 Identités et authentification	0	0	0	5	n.d.
2 Messagerie et Exchange Online	0	0	0	5	n.d.
3 Données et collaboration	0	0	0	5	n.d.
4 Surveillance et réponse aux incidents	0	0	0	5	n.d.
Ensemble	0	0	0	20	n.d.

ÉCARTS PAR PRIORITÉ

LECTURE DU SCORE

Priorité	Non conformes	Partiels	Score	Interprétation
● Immédiate	0	0	≥ 80 %	Bon niveau de maîtrise
● Court terme	0	0	50 à 79 %	Niveau à renforcer
● Moyen terme	0	0	< 50 %	Action prioritaire recommandée
Total	0	0	Score = (conformes + ½ × partiels) ÷ contrôles évalués, hors « Non applicable ».	

MODE D'EMPLOI

01

Contrôles M365

Vérifiez chaque point dans la console indiquée, puis choisissez : Conforme, Partiel, Non conforme ou Non applicable.

02

Plan d'amélioration

Pour chaque écart, notez le constat, l'action, le responsable et l'échéance, en commençant par les priorités immédiates.

03

Réponse à incident

En cas de suspicion de compromission, suivez les 10 étapes et tenez la chronologie à jour.

Cette liste constitue un point de départ pour une revue de sécurité. Elle ne remplace ni une investigation ni un audit complet. Les fonctionnalités et les durées de conservation dépendent des licences Microsoft 365.

Besoin d'un regard expert ? Sunitech réalise des audits de sécurité Microsoft 365 pour les PME romandes : sunitech.ch/contact

sunitech.ch · Suisse romande · Partenaire IT des PME


CHECKLIST SÉCURITÉ MICROSOFT 365
 01 - Contrôles Microsoft 365

01 20 CONTRÔLES DE SÉCURITÉ MICROSOFT 365

Score : à évaluer

Vérifiez chaque point dans la console indiquée, puis choisissez le résultat. Les écarts se suivent dans les colonnes Constat / action et Échéance.

■ Colonnes à compléter

ID	Contrôle	Où vérifier	Critère de conformité	Risque si absent	Priorité	Résultat	Vérifié le	Responsable	Constat / action corrective	Échéance	Doc.
1 IDENTITÉS ET AUTHENTIFICATION											
M01	Les comptes utilisateurs disposent d'une authentification multifactor adaptée.	Entra > Méthodes d'authentification > Détails d'inscription des utilisateurs (User registration details) ; Entra > Accès conditionnel > Stratégies (ou paramètres de sécurité par défaut).	100 % des utilisateurs inscrits au MFA ; une stratégie impose le MFA à tous les comptes, sans exclusion non justifiée. Application Authenticator ou passkeys privilégiés plutôt que SMS ou appel.	Prise de contrôle du compte par phishing ou mot de passe réutilisé (credential stuffing).	Immédiate	Non évalué					Ouvrir
M02	Les comptes administrateurs bénéficient de protections renforcées.	Entra > Rôles et administrateurs ; Accès conditionnel > stratégie dédiée aux rôles d'administration (force d'authentification).	Comptes d'administration dédiés, sans messagerie ; MFA résistant au phishing (FIDO2 / passkey) exigé ; deux comptes d'accès d'urgence protégés et surveillés.	Contrôle total du tenant : création de comptes, désactivation des protections, exfiltration massive.	Immédiate	Non évalué					Ouvrir
M03	Les méthodes d'authentification enregistrées sont contrôlées.	Entra > Méthodes d'authentification > Stratégies et Activité ; journaux d'audit Entra (événement « User registered security info »).	Méthodes faibles (SMS, appel) désactivées lorsque c'est possible ; enregistrement des informations de sécurité protégé par l'accès conditionnel ; tout ajout de méthode inconnue est détecté et vérifié.	L'attaquant enregistre sa propre méthode MFA et conserve l'accès après un changement de mot de passe.	Immédiate	Non évalué					Ouvrir
M04	Les comptes inactifs sont identifiés et traités.	Entra > Utilisateurs (activité de connexion, dernière connexion) ; Centre d'administration Microsoft 365 > Rapports > Utilisation.	Aucun compte actif sans connexion depuis plus de 90 jours sans justification ; comptes des départs bloqués le jour même ; licences récupérées.	Compte oublié utilisé par un attaquant sans que personne ne remarque d'anomalie.	Immédiate	Non évalué					Ouvrir
M05	Les permissions privilégiées sont limitées et revues régulièrement.	Entra > Rôles et administrateurs > Affectations ; Privileged Identity Management (Entra ID P2) ; revues d'accès.	Entre 2 et 4 administrateurs généraux ; rôles spécifiques (Exchange, utilisateurs...) plutôt que globaux ; revue documentée au moins trimestrielle.	Abus ou détournement de privilèges excessifs, surface d'attaque élargie.	Immédiate	Non évalué					Ouvrir
2 MESSAGERIE ET EXCHANGE ONLINE											
M06	Les transferts automatiques externes sont encadrés.	Microsoft Defender > Stratégies de menace > Stratégie de courrier indésirable sortant (règles de transfert automatique) ; PowerShell : Get-Mailbox ? {\$_.ForwardingSmtpAddress}.	Transfert automatique externe désactivé par défaut ; exceptions nominatives, justifiées et documentées ; aucune redirection inconnue au niveau des boîtes aux lettres.	Fuite silencieuse de messages vers une adresse externe, préparation d'une fraude au paiement (BEC).	Immédiate	Non évalué					Ouvrir
M07	Les règles de boîte de réception suspectes peuvent être identifiées.	Exchange Online PowerShell : Get-InboxRule -Mailbox <utilisateur> -IncludeHidden ; Defender > Stratégies d'alerte (transfert ou règle suspecte) ; audit Purview (New-InboxRule).	Procédure de revue des règles (transfert, redirection, suppression, déplacement vers des dossiers peu visibles) ; alertes correspondantes actives et traitées.	Messages détournés ou masqués à l'utilisateur pendant que l'attaquant suit les échanges.	Immédiate	Non évalué					Ouvrir
M08	Les délégations de messagerie font l'objet de contrôles.	Centre d'administration Exchange > Boîtes aux lettres ; Délégation ; PowerShell : Get-MailboxPermission, Get-RecipientPermission.	Droits « Accès total », « Envoyer en tant que » et « Envoyer de la part de » justifiés et nominatifs ; revue au moins semestrielle ; droits des départs retirés.	Lecture ou envoi de messages au nom d'un collaborateur, persistance après remédiation.	Court terme	Non évalué					Ouvrir
M09	Les protections anti-phishing et anti-usurpation sont configurées.	Microsoft Defender > Stratégies de menace > Stratégies de sécurité prédéfinies, Anti-hameçonnage, Liens fiables, Pièces jointes fiables ; Analyseur de configuration.	Stratégie prédéfinie Standard ou Stricte appliquée à tous ; protection contre l'emprunt d'identité pour la direction et la comptabilité ; Liens et Pièces jointes fiables actifs (Defender for Office 365).	Phishing et usurpation de dirigeants ou de fournisseurs non bloqués.	Court terme	Non évalué					Ouvrir
M10	Les domaines de messagerie disposent de configurations SPF, DKIM et DMARC adaptées.	Microsoft Defender > Stratégies de menace > Paramètres d'authentification des e-mails (DKIM) ; DNS : Resolve-DnsName -Type TXT _dmarc.votredomaine.ch.	Un seul enregistrement SPF (≤ 10 recherches DNS) ; DKIM activé pour chaque domaine personnalisé ; DMARC en p=quarantine ou p=reject avec rapports ; domaines inutilisés verrouillés.	Usurpation de votre domaine pour tromper clients et fournisseurs, délivrabilité dégradée.	Court terme	Non évalué					Ouvrir

ID	Contrôle	Où vérifier	Critère de conformité	Risque si absent	Priorité	Résultat	Vérifié le	Responsable	Constat / action corrective	Échéance	Doc.
3 DONNÉES ET COLLABORATION											
M11	Les politiques de partage SharePoint sont documentées.	Centre d'administration SharePoint › Stratégies › Partage (niveau de partage externe, type de lien par défaut, expiration des liens).	Politique écrite et validée ; lien par défaut « Personnes spécifiques » ; liens « Tout le monde » désactivés ou avec expiration ; sites sensibles plus restrictifs.	Documents confidentiels accessibles via des liens anonymes ou trop larges.	Moyen terme	Non évalué					Ouvrir
M12	Les accès invités sont révisés périodiquement.	Entra › Utilisateurs (filtre Type d'utilisateur = Invité) ; Identités externes › Paramètres de collaboration externe ; revues d'accès (Entra ID P2).	Revue au moins semestrielle ; invités inactifs ou sans propriétaire supprimés ; invitations limitées aux rôles autorisés ; expiration des accès invités SharePoint activée.	Partenaires ou anciens prestataires conservant l'accès à des équipes et documents.	Moyen terme	Non évalué					Ouvrir
M13	Les permissions OneDrive sont cohérentes avec les usages.	Centre d'administration SharePoint › Stratégies › Partage (niveau OneDrive) ; rapports d'activité de partage ; Paramètres › Rétention OneDrive.	Partage externe OneDrive au plus égal à celui de SharePoint ; partages externes de fichiers sensibles revus ; OneDrive des départs transféré au responsable puis supprimé selon la rétention.	Fichiers de travail partagés hors contrôle, données perdues au départ d'un collaborateur.	Moyen terme	Non évalué					Ouvrir
M14	Les applications connectées et leurs autorisations sont contrôlées.	Entra › Applications d'entreprise › Consentement et autorisations ; liste des applications et des autorisations accordées (Mail.Read, Files.ReadWrite.All...).	Consentement utilisateur limité aux éditeurs vérifiés et autorisations à faible risque, ou désactivé ; workflow de consentement administrateur ; revue trimestrielle ; applications inconnues révoquées.	Accès persistant via un consentement OAuth malveillant, non révoqué par un changement de mot de passe.	Immédiate	Non évalué					Ouvrir
M15	Les données critiques disposent d'une stratégie de protection et de restauration adaptée.	Solution de sauvegarde Microsoft 365 (Microsoft 365 Backup ou outil tiers) ; Microsoft Purview › Gestion du cycle de vie des données ; rapports de tests de restauration.	Exchange, OneDrive et SharePoint sauvegardés au-delà des seules corbeilles ; rétention définie ; test de restauration documenté depuis moins de 12 mois.	Perte définitive de données après suppression malveillante, ransomware ou erreur.	Immédiate	Non évalué					Ouvrir
4 SURVEILLANCE ET RÉPONSE AUX INCIDENTS											
M16	Les journaux de connexion sont accessibles pour la période nécessaire.	Entra › Surveillance › Journaux de connexion ; Microsoft Purview › Audit ; PowerShell : Get-AdminAuditLogConfig fl UnifiedAuditLogIngestionEnabled.	Audit unifié activé ; durée de conservation connue selon la licence (voir onglet Références) ; export vers un stockage ou un SIEM si l'historique nécessaire est plus long.	Impossible de reconstituer une intrusion découverte tardivement.	Court terme	Non évalué					Ouvrir
M17	Les alertes critiques sont envoyées aux personnes responsables.	Microsoft Defender › Stratégies d'alerte (destinataires) ; Paramètres › Microsoft Defender XDR › Notifications par e-mail ; notifications Entra ID Protection (P2).	Destinataires nominatifs et boîte surveillée, pas uniquement l'administrateur par défaut ; envoi testé ; suppléant défini pendant les absences.	Alertes générées mais jamais lues ; l'attaque se poursuit malgré la détection.	Court terme	Non évalué					Ouvrir
M18	Les événements suspects font l'objet d'une procédure de traitement.	Procédure interne ou contrat de supervision (prestataire, MDR, SOC) ; file d'incidents Microsoft Defender.	Rôles définis (qui qualifie, qui décide, qui intervient), délais de prise en charge, escalade et registre des alertes traitées.	Réaction tardive ou improvisée, signaux faibles ignorés.	Court terme	Non évalué					Ouvrir
M19	Une procédure de compromission de compte est documentée et testée.	Onglet « Réponse à incident » de ce classeur ; procédure interne ; compte rendu du dernier exercice.	Procédure écrite couvrant confinement, investigation, communication et annonces ; contacts d'urgence à jour ; exercice réalisé depuis moins de 12 mois.	Perte de temps et de preuves au moment critique, obligations d'annonce manquées.	Court terme	Non évalué					Ouvrir
M20	Les résultats des contrôles sont suivis dans un plan d'amélioration.	Microsoft Defender › Microsoft Secure Score (Degré de sécurisation) ; colonnes « Constat / action » et « Échéance » de ce classeur.	Écarts priorisés avec responsable et échéance ; Secure Score suivi dans le temps ; revue au moins trimestrielle avec la direction.	Constats non suivis ; les mêmes faiblesses persistent d'une revue à l'autre.	Moyen terme	Non évalué					Ouvrir



CHECKLIST SÉCURITÉ MICROSOFT 365

02 · Réponse à incident

02 PROCÉDURE EN CAS DE COMPTE COMPROMIS

Étapes réalisées : 0 / 10

À suivre dès qu'une compromission est suspectée : contenir l'incident tout en préservant les éléments nécessaires à l'analyse.

■ Colonnes à compléter

N°	Étape	Actions clés	Statut	Date / heure	Par	Notes / preuves
01	Alerter le responsable sécurité IT	Prévenir immédiatement l'équipe IT ou le prestataire. Ne plus échanger d'informations sensibles depuis le compte suspect ; utiliser un canal indépendant (téléphone, autre messagerie).	À faire			
02	Contenir les accès suspects	Bloquer la connexion du compte, révoquer les sessions actives (Entra › Utilisateur › Révoquer les sessions) et suspendre les applications concernées. Compromission confirmée : désactiver le compte pendant l'investigation.	À faire			
03	Sécuriser l'authentification	Réinitialiser le mot de passe, vérifier et retirer les méthodes MFA inconnues, contrôler que le poste de l'utilisateur n'est pas lui-même compromis.	À faire			
04	Rechercher les mécanismes de persistance	Règles et transferts Outlook (Get-InboxRule -IncludeHidden), délégations de boîte, consentements OAuth, modifications de privilèges, méthodes d'authentification, comptes ou applications récemment créés.	À faire			
05	Analyser les accès aux données	Journaux Entra et Purview : messages consultés, fichiers SharePoint / OneDrive téléchargés ou partagés, liens externes créés pendant la période suspecte.	À faire			
06	Rechercher une compromission plus large	Vérifier les connexions et activités similaires sur d'autres comptes, administrateurs et systèmes ; rechercher les messages frauduleux envoyés depuis le compte.	À faire			
07	Documenter l'incident	Tenir la chronologie : journaux exportés, messages frauduleux, modifications constatées, actions réalisées et décisions prises (utile pour l'assureur et les autorités).	À faire			
08	Organiser la communication	Informar selon l'impact les collaborateurs, clients, fournisseurs ou partenaires. Fraude au paiement suspectée : contacter la banque sans délai pour tenter un blocage ou une récupération des fonds.	À faire			
09	Évaluer les obligations d'annonce	Données personnelles exposées ? Annonce au PFPDT en cas de risque élevé (art. 24 LPD) et information des personnes concernées si nécessaire. Infrastructures critiques soumises à la LSI : signalement à l'OFCS sous 24 h.	À faire			
10	Corriger et vérifier le retour à la normale	Confirmer la suppression des accès malveillants, traiter la cause (MFA, transferts, consentements...), renforcer les contrôles concernés. Ne pas clore l'incident sur un simple changement de mot de passe.	À faire			

FICHE INCIDENT			
Compte(s) concerné(s)		Détecté le	
Détecté par		Coordinateur	

CONTACTS D'URGENCE			
Rôle	Nom / organisation	Téléphone	E-mail / lien
Responsable sécurité IT / prestataire			
Direction			
Banque (fraude au paiement)			
Assureur cyber			
PFPDT : annonce de violation (art. 24 LPD)	Préposé fédéral à la protection des données et à la transparence		https://www.edoeb.admin.ch/fr/databreach-2
OFCS : signalement (infrastructures critiques, LSI)	Office fédéral de la cybersécurité		https://www.bacs.admin.ch/fr/information-sur-lobligation-de-signaler

03 RÉFÉRENCES & CONSERVATION DES JOURNAUX

Durées documentées par Microsoft, à titre indicatif : elles dépendent des licences et de la configuration (source : article Sunitech, octobre 2026).

Source de journaux	Conservation native indicative	Remarque
Microsoft Entra ID Free : connexions	7 jours	Journaux de connexion Entra.
Microsoft Entra ID P1 / P2 : connexions	30 jours	Entra ID P1 est inclus notamment dans Microsoft 365 Business Premium.
Microsoft Purview Audit (Standard)	180 jours	Journal d'audit unifié Microsoft 365.
Microsoft Purview Audit (Premium)	1 an par défaut	Pour les événements Entra ID, Exchange, OneDrive et SharePoint couverts ; autres activités : 180 jours. Licences requises, extensions possibles.

Les journaux Entra ID et le journal d'audit unifié restent des sources distinctes. Une nouvelle licence ne permet pas de récupérer des journaux déjà expirés : pour un historique plus long, prévoir un export vers un stockage ou un SIEM.

SOURCES OFFICIELLES		
Document	Éditeur	Lien
Votre entreprise est peut-être déjà piratée. Et personne ne le sait.	Sunitech	https://sunitech.ch/actualites/entreprise-deja-piratee-signes-microsoft-365/
Répondre à un compte de messagerie Microsoft 365 compromis	Microsoft Learn	https://learn.microsoft.com/fr-fr/defender-office-365/responding-to-a-compromised-email-account
Techniques d'attaque contre les identités, AiTM et consentement OAuth	Microsoft Security	https://www.microsoft.com/en-us/security/blog/2025/05/29/defending-against-evolving-identity-attack-techniques/
Passkeys (FIDO2) et résistance au phishing dans Entra ID	Microsoft Learn	https://learn.microsoft.com/fr-fr/entra/identity/authentication/concept-authentication-passkeys-fido2
Détecter et corriger les consentements d'application illicites	Microsoft Learn	https://learn.microsoft.com/fr-fr/defender-office-365/detect-and-remediate-illicit-consent-grants
Contrôler le transfert automatique externe des e-mails	Microsoft Learn	https://learn.microsoft.com/fr-fr/defender-office-365/outbound-spam-policies-external-email-forwarding
Durées de conservation des données Microsoft Entra	Microsoft Learn	https://learn.microsoft.com/fr-fr/entra/identity/monitoring-health/reference-reports-data-retention
Solutions d'audit Microsoft Purview (Standard et Premium)	Microsoft Learn	https://learn.microsoft.com/fr-fr/purview/audit-solutions-overview
Questions de sécurité sur Microsoft 365 Business Premium	Microsoft Learn	https://learn.microsoft.com/fr-fr/microsoft-365/admin/security-and-compliance/m365bp-security-faq
Violations de la sécurité des données : guide relatif à l'art. 24 LPD	PFPDT	https://www.edoeb.admin.ch/fr/databreach-2
Obligation de signaler les cyberattaques (infrastructures critiques)	OFCS	https://www.bacs.admin.ch/fr/information-sur-lobligation-de-signaler