Poulo TI · Audit Flash Microsoft 365

Rapport d'évaluation de la sécurité

Cabinet Démo CPA — Exemple fictif

Données recueillies le 18 novembre 2026

Exemple fictif — Données simulées

Préparé par Daouda Sow, Poulo TI, daouda.sow@pouloti.com · 418 814-2001
Exemple fictif préparé à partir d'un environnement simulé à des fins de démonstration uniquement.
Aucune organisation réelle ni aucune donnée de client n'y figure.

Résumé pour la direction

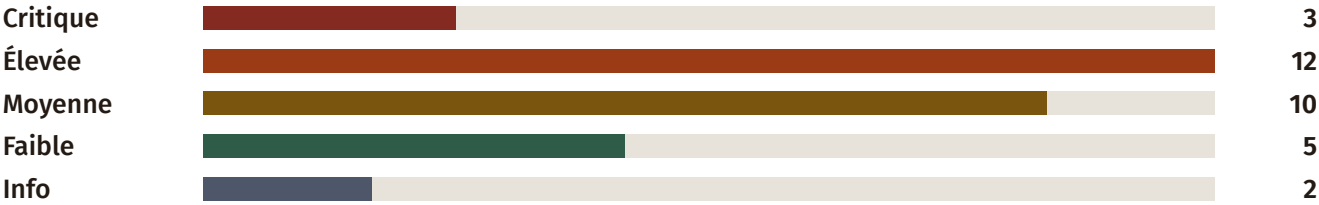
Ce qui a été vérifié : comptes et accès, courriel, appareils de votre environnement Microsoft 365, en lecture seule. 1 point(s) n'ont pas pu être vérifiés (voir l'annexe).



contrôles clés en place

sur les 7 que les assureurs vérifient le plus souvent. Oui = 1 point, Partiel = ½ point ; le détail est à la section « Questions habituelles des assureurs ».

Constats par gravité



Les trois risques principaux

1. 2 comptes administrateurs n'ont pas de vérification en deux étapes. Critique

Un seul mot de passe volé donne le contrôle complet : courriels, fichiers, comptes. Les assureurs refusent souvent de couvrir un incident dans ce cas.

2. 1 compte actif n'ont aucune vérification en deux étapes (MFA). Critique

Un mot de passe volé par hameçonnage suffit pour entrer dans la messagerie et les fichiers de l'entreprise. C'est la cause la plus fréquente des fraudes par courriel déclarées aux assureurs.

3. 1 règle cachent ou suppriment des courriels, par exemple ceux qui contiennent « facture » ou « virement », ou les déplacent vers un dossier que personne ne consulte. Critique

C'est la signature d'une fraude en cours : l'attaquant cache les réponses pendant qu'il détourne des paiements.

Les cinq priorités

Classées par gravité. L'effort estimé est à compléter avec votre équipe ou votre fournisseur TI.

1

Critique Réf. ENTRA-ROLE-03

2 comptes administrateurs n'ont pas de vérification en deux étapes.

POURQUOI C'EST UN RISQUE

Un seul mot de passe volé donne le contrôle complet : courriels, fichiers, comptes. Les assureurs refusent souvent de couvrir un incident dans ce cas.

CORRECTIF

Exiger immédiatement la vérification en deux étapes sur tous les comptes administrateurs.

EFFORT ESTIMÉ

_____

2

Critique Réf. ENTRA-MFA-01

1 compte actif n'ont aucune vérification en deux étapes (MFA).

POURQUOI C'EST UN RISQUE

Un mot de passe volé par hameçonnage suffit pour entrer dans la messagerie et les fichiers de l'entreprise. C'est la cause la plus fréquente des fraudes par courriel déclarées aux assureurs.

CORRECTIF

Inscrire tous les employés à l'application d'authentification et rendre la vérification en deux étapes obligatoire.

EFFORT ESTIMÉ

_____

3

Critique Réf. MSG-RULE-02

1 règle cachent ou suppriment des courriels, par exemple ceux qui contiennent « facture » ou « virement », ou les déplacent vers un dossier que personne ne consulte.

POURQUOI C'EST UN RISQUE

C'est la signature d'une fraude en cours : l'attaquant cache les réponses pendant qu'il détourne des paiements.

CORRECTIF

Traiter immédiatement comme un incident les règles qui cachent des courriels : sécuriser le compte, vérifier les paiements récents, consigner l'incident.

EFFORT ESTIMÉ

4

Élevée Réf. ENTRA-ROLE-06

1 compte externe ont des droits d'administration.

POURQUOI C'EST UN RISQUE

L'entreprise ne contrôle ni le mot de passe ni le départ de ces personnes : un fournisseur compromis devient votre incident.

CORRECTIF

Retirer les droits d'administration des comptes externes et passer par un accès délégué, encadré et limité dans le temps.

EFFORT ESTIMÉ

5

Élevée Réf. ENTRA-APP-01

1 application externe peuvent lire des courriels, des fichiers ou l'annuaire.

POURQUOI C'EST UN RISQUE

Ces applications gardent leur accès même après un changement de mot de passe. Ce sont des sous-traitants à inscrire à l'inventaire exigé par les lois sur les renseignements personnels.

CORRECTIF

Revoir chaque application externe qui a accès aux données et retirer celles qui ne sont pas nécessaires.

EFFORT ESTIMÉ

PROCHAINE ÉTAPE

Pack Durcissement M365

Les priorités de ce rapport sont corrigées pour vous, dans l'ordre, avec un prix fixe convenu avant de commencer. Un nouvel audit à la fin documente l'avant et l'après, prêt à joindre au questionnaire de votre assureur.

Délai	Prix	Preuves
30 jours	**à partir de 5 500 $, taxes en sus**	**Nouvel audit à la fin**

Questions habituelles des assureurs

Réponses déduites de l'état technique observé le 18 novembre 2026. Elles aident à remplir un questionnaire de cyberassurance ; validez-les avant de le signer.

QUESTION	RÉPONSE	SUR QUOI REPOSE LA RÉPONSE
La vérification en deux étapes (MFA) est-elle exigée pour tous les utilisateurs ?	✕ Non	Aucune règle ne l'impose à tous, et 1 compte actif n'y est pas inscrit.
Les comptes administrateurs sont-ils protégés par la MFA ?	✕ Non	2 comptes administrateurs sans MFA.
Les administrateurs utilisent-ils des comptes distincts pour l'administration ?	◐ Partiel	1 administrateur général sur 2 sert aussi au travail courant.
L'authentification héritée (anciens protocoles) est-elle bloquée ?	✕ Non	Aucune règle active ne la bloque.
Les postes de travail sont-ils chiffrés ?	◐ Partiel	1 poste actif sur 3 n'est pas chiffré.
Un journal d'activité est-il conservé (qui a fait quoi, quand) ?	✕ Non	Le journal d'audit unifié de Microsoft 365 est désactivé.
Votre domaine est-il protégé contre l'usurpation (SPF, DKIM, DMARC) ?	◐ Partiel	Protection en place, mais : DMARC en surveillance sur 1 domaine ; DKIM absent sur 1 domaine.

✓ Oui : en place partout. ◐ Partiel : en place, mais pas partout ou pas imposé. ✕ Non : absent. ? Non vérifié : l'audit n'a pas pu lire l'information ; ce n'est pas un « non ».

Questions que l'audit ne peut pas vérifier

Les assureurs les posent presque toujours. Elles ne se voient pas dans Microsoft 365 : la réponse vient de vous.

QUESTION	RÉPONSE	CE QU'IL FAUT POUVOIR MONTRER
Les données (courriels, fichiers, postes) sont-elles sauvegardées, hors ligne ou hors du compte Microsoft 365, et la restauration a-t-elle été testée ?	ⓘ À confirmer	Le nom de la solution de sauvegarde, la date du dernier test de restauration.
Un antivirus ou une solution de détection et réponse (EDR) est-il actif sur tous les postes ?	ⓘ À confirmer	Le nom de la solution et le nombre de postes couverts.
Les employés suivent-ils une formation contre l'hameçonnage ?	ⓘ À confirmer	La fréquence de la formation et la date de la dernière séance.
Existe-t-il un plan d'intervention en cas d'incident de sécurité ?	ⓘ À confirmer	Le document, son responsable et sa date de mise à jour.

Feuille de route

Les correctifs regroupés en trois phases. Les budgets sont à compléter.

1

PHASE 1 · 30 JOURS

Fermer les portes ouvertes

14 action(s) · Budget : _____

Exiger immédiatement la vérification en deux étapes sur tous les comptes administrateurs. ENTRA-ROLE-03

Traiter immédiatement comme un incident les règles qui cachent des courriels : sécuriser le compte, vérifier les paiements récents, consigner l'incident. MSG-RULE-02

Exiger l'approbation d'un administrateur pour toute nouvelle application. ENTRA-APP-03

Bloquer l'authentification héritée par une règle d'accès conditionnel. ENTRA-CA-02

Valider chaque règle d'organisation qui envoie du courriel vers l'extérieur et retirer celles qui ne sont pas justifiées. MSG-TR-01

Vérifier avec son titulaire chaque règle de boîte qui transfère vers l'extérieur ; une règle inconnue est traitée comme un incident. MSG-RULE-01

Activer le chiffrement sur tous les postes, avec sauvegarde des clés de récupération. INT-ENC-01

Inscrire tous les employés à l'application d'authentification et rendre la vérification en deux étapes obligatoire. ENTRA-MFA-01

Retirer les droits d'administration des comptes externes et passer par un accès délégué, encadré et limité dans le temps. ENTRA-ROLE-06

Activer une règle qui exige la vérification en deux étapes pour tous les utilisateurs et toutes les applications. ENTRA-CA-01

Activer le journal d'audit unifié (aucun coût, quelques minutes). MSG-LOG-01

Bloquer le transfert automatique externe et autoriser les exceptions au cas par cas. MSG-FWD-03

Valider avec la direction chaque transfert automatique vers l'extérieur et supprimer ceux qui ne sont pas justifiés. MSG-FWD-01

Faire considérer comme non conformes les appareils qui n'ont reçu aucune règle de sécurité. INT-CMP-03

2

PHASE 2 · 90 JOURS

Consolider

11 action(s) · Budget : _____

Revoir chaque application externe qui a accès aux données et retirer celles qui ne sont pas nécessaires. ENTRA-APP-01

Ajouter la vérification du pare-feu aux règles de conformité. INT-FW-01

Créer des comptes d'administration distincts, sans boîte courriel, réservés à l'administration. ENTRA-ROLE-04

Bloquer la connexion des boîtes partagées et des ressources, et restreindre les comptes de service. ENTRA-MFA-04

Désactiver l'envoi SMTP par mot de passe seul et ne l'autoriser que pour les appareils qui en ont besoin, comme les imprimantes. MSG-SMTP-01

Activer la signature DKIM dans Microsoft 365. MSG-DNS-06

Mettre à jour les postes dont Windows n'est plus supporté, ou remplacer le matériel incompatible. INT-OS-01

Corriger les appareils non conformes, puis leur bloquer l'accès aux données. INT-CMP-01

Faire passer les comptes qui n'utilisent que le texto à l'application d'authentification. ENTRA-MFA-02

Retirer les exceptions au filtrage antipourriel ou les restreindre au strict nécessaire. MSG-TR-02

Passer DMARC en mode quarantaine, puis rejet. MSG-DNS-02

3

PHASE 3 · 6 MOIS

Mettre de l'ordre et maintenir

5 action(s) · Budget : _____

Récupérer ou retirer les appareils inactifs et mettre l'inventaire à jour. INT-INV-02

Faire valider par la direction ou les TI chaque application autorisée par un employé. ENTRA-APP-02

Passer SPF en mode strict une fois les expéditeurs confirmés. MSG-DNS-05

Réserver aux personnes désignées l'invitation de personnes externes. ENTRA-INV-01

Confirmer chaque destinataire de transfert interne. MSG-FWD-02

Annexe

Tous les constats

GRAVITÉ	DOMAINE	CONSTAT	NOMBRE	RÉF.
Critique	Comptes	2 comptes administrateurs n'ont pas de vérification en deux étapes.	2	ENTRA-ROLE-03
Critique	Comptes	1 compte actif n'ont aucune vérification en deux étapes (MFA).	1	ENTRA-MFA-01
Critique	Courriel	1 règle cachent ou suppriment des courriels, par exemple ceux qui contiennent « facture » ou « virement », ou les déplacent vers un dossier que personne ne consulte.	1	MSG-RULE-02
Élevée	Comptes	1 compte externe ont des droits d'administration.	1	ENTRA-ROLE-06
Élevée	Comptes	1 application externe peuvent lire des courriels, des fichiers ou l'annuaire.	1	ENTRA-APP-01
Élevée	Comptes	Tout employé peut donner à une application externe l'accès à sa boîte courriel.	1	ENTRA-APP-03
Élevée	Comptes	Aucune règle n'oblige tous les utilisateurs à confirmer leur identité en deux étapes.	1	ENTRA-CA-01
Élevée	Comptes	Les anciens modes de connexion, qui ignorent la vérification en deux étapes, ne sont pas bloqués.	1	ENTRA-CA-02
Élevée	Courriel	Le journal d'activité de Microsoft 365 est désactivé.	1	MSG-LOG-01
Élevée	Courriel	1 règle de l'organisation copient ou redirigent du courriel vers l'extérieur.	1	MSG-TR-01
Élevée	Courriel	Le transfert automatique de courriels vers l'extérieur est permis.	1	MSG-FWD-03
Élevée	Courriel	1 règle de boîte courriel renvoient des messages vers l'extérieur.	1	MSG-RULE-01
Élevée	Courriel	1 boîte courriel envoient automatiquement une copie de tout leur courrier à l'extérieur.	1	MSG-FWD-01
Élevée	Appareils	1 poste ne sont pas chiffrés.	1	INT-ENC-01
Élevée	Appareils	1 poste utilisent une version de Windows qui ne reçoit plus de correctifs de sécurité.	1	INT-OS-01
Moyenne	Appareils	L'état du pare-feu n'est vérifié sur aucun poste (3 postes concernés).	3	INT-FW-01
Moyenne	Appareils	1 appareil ne respectent pas les règles de sécurité de l'entreprise.	1	INT-CMP-01
Moyenne	Appareils	Les appareils sans règle de sécurité sont considérés comme sûrs par défaut.	1	INT-CMP-03
Moyenne	Comptes	1 administrateur utilisent le même compte pour le travail quotidien et pour l'administration.	1	ENTRA-ROLE-04
Moyenne	Comptes	1 compte n'utilisent que le texto ou l'appel comme deuxième étape.	1	ENTRA-MFA-02
Moyenne	Comptes	1 compte actif sans licence (boîtes partagées, salles, comptes de service) n'ont aucune vérification en deux étapes.	1	ENTRA-MFA-04
Moyenne	Courriel	1 règle font éviter le filtrage antipourriel à certains messages.	1	MSG-TR-02

GRAVITÉ	DOMAINE	CONSTAT	NOMBRE	RÉF.
Moyenne	Courriel	Un ancien mode d'envoi de courriel, par mot de passe seul, est permis pour toute l'organisation.	1	MSG-SMTP-01
Moyenne	Courriel	1 domaine observent l'usurpation sans la bloquer (DMARC en surveillance).	1	MSG-DNS-02
Moyenne	Courriel	1 domaine ne signent pas leurs courriels (DKIM).	1	MSG-DNS-06
Faible	Appareils	1 appareil n'ont pas donné de nouvelles depuis plus de 30 jours.	1	INT-INV-02
Faible	Comptes	Tout le monde peut inviter des personnes externes dans l'environnement.	1	ENTRA-INV-01
Faible	Comptes	1 application externe ont été autorisées par des employés, sans validation.	1	ENTRA-APP-02
Faible	Courriel	1 boîte transfèrent leurs courriels vers un destinataire à vérifier.	1	MSG-FWD-02
Faible	Courriel	1 domaine ont leur liste de serveurs autorisés (SPF) en mode souple.	1	MSG-DNS-05
Info	Appareils	1 appareil personnel accèdent aux données de l'entreprise.	1	INT-INV-03
Info	Comptes	1 règle de sécurité sont en mode test et ne protègent pas encore.	1	ENTRA-CA-03

Limites de cet audit

- **Appareils — Support Windows** : 1 poste(s) ont une version absente de la table de fin de support du script. Builds : 28000 (1). Vérifier sur la page du cycle de vie de Microsoft et compléter la table.

Hors périmètre : sauvegardes, antivirus ou EDR, SharePoint et OneDrive, postes non inscrits dans la gestion centralisée, réseau local, attributions de rôles admissibles (PIM).

Fichiers de preuve

Remis séparément. Ils contiennent le détail nominatif (comptes, appareils, règles) et des renseignements personnels : à conserver chiffrés.

- constats-EntraID.json
- constats-Intune.json
- constats-Messagerie.json
- constats.csv
- entra-acces-conditionnel.csv
- entra-applications.csv
- entra-contexte.json
- entra-roles-admin.csv
- entra-utilisateurs-mfa.csv
- intune-appareils.csv
- intune-politiques-conformite.csv
- messagerie-dns.csv
- messagerie-politiques.csv
- messagerie-regles-boites.csv
- messagerie-regles-transport.csv
- messagerie-transferts-boites.csv
- Synthese.md

Ce rapport est une évaluation technique, pas un avis juridique.