

Messagerie Lumen inc.: où vous en êtes, et quoi corriger en premier

Un bilan à portée fixe des cinq points que les attaquants testent en premier. En lecture seule, non intrusif, réalisé en deux semaines.

Organisation	Taille	Période	Préparé par
Messagerie Lumen inc. (fictive)	38 employés · 41 comptes	5 au 16 octobre 2026	Mikhaël Esterez

PORTRAIT GLOBAL

À corriger

Quatre problèmes à risque élevé offrent aujourd'hui à un attaquant une façon réaliste d'entrer. Les quatre peuvent être corrigés en moins d'un mois, dont trois en moins d'une journée. Rien n'indique une intrusion en cours.

4 Élevé : ce mois-ci

4 Moyen : ce trimestre

2 Faible : bonne pratique

LES CINQ VÉRIFICATIONS

VÉRIFICATION	RÉSULTAT	EN UNE LIGNE
Exposition sur Internet	ÉLEVÉ	Le Bureau à distance et un RPV désuet sont accessibles depuis Internet
Courriel et domaine	MOYEN	N'importe qui peut envoyer un courriel qui semble venir de votre domaine
Microsoft 365	ÉLEVÉ	6 comptes, dont un administrateur, n'ont pas de deuxième facteur
Mots de passe divulgués	ÉLEVÉ	3 mots de passe d'employés ont été volés par un logiciel malveillant
Mesures de base	MOYEN	3 des 13 contrôles de base nationaux respectés; sauvegardes jamais testées

LES TROIS RISQUES PRINCIPAUX

- 1 Votre serveur de bureau répond à n'importe qui sur Internet.** Un Bureau à distance exposé est une porte d'entrée courante des rançongiciels.
- 2 Un mot de passe volé suffit** pour 6 comptes Microsoft 365, dont un administrateur.
- 3 Trois mots de passe d'employés sont déjà entre des mains criminelles.** Traitez ces comptes et leurs ordinateurs comme compromis.

À FAIRE CE MOIS-CI

- ☐ Fermer le Bureau à distance à Internet; y accéder par le RPV avec un deuxième facteur
- ☐ Mettre à jour le micrologiciel du RPV
- ☐ Activer l'authentification multifacteur pour tous les comptes
- ☐ Réinitialiser les trois mots de passe exposés et vérifier ces ordinateurs

Liste complète des correctifs, par ordre, en page 5.

CE QUI VA BIEN

Microsoft Defender protège chaque portable, les portables se mettent à jour automatiquement, les sauvegardes s'exécutent chaque nuit, les clés USB sont bloquées et le site Web utilise HTTPS avec un certificat valide. Ce sont de bonnes bases.

Portée et façon de travailler

MESSAGERIE LUMEN INC.

CE QUI ÉTAIT INCLUS

ÉLÉMENT	PORTÉE
Domaine	lumen-courier.example et ses sous-domaines
Adresses Internet	203.0.113.10 à 203.0.113.24 (15 adresses, confirmées par le client)
Microsoft 365	Un environnement, 41 comptes (36 utilisateurs, 5 boîtes partagées), accès en lecture seule accordé pour le bilan
Entrevue	Une heure avec la directrice de bureau et le fournisseur informatique externe
Autorisation	Signée par le président le 3 octobre 2026 : vérifications non intrusives seulement, aucune exploitation

LES CINQ VÉRIFICATIONS

	VÉRIFICATION	CE QUE NOUS AVONS FAIT
01	Exposition sur Internet	Repéré tout ce qui est accessible depuis Internet (sous-domaines, adresses, services ouverts), puis vérifié les versions, le chiffrement et les vulnérabilités connues. Chaque résultat a été confirmé à la main.
02	Courriel et domaine	Vérifié les enregistrements qui empêchent d'envoyer des courriels en votre nom (SPF, DKIM, DMARC) et le chiffrement des courriels en transit (MTA-STS).
03	Microsoft 365	Comparé l'environnement à des références reconnues (CISA SCuBA, Microsoft Secure Score), puis revu l'authentification multifacteur, les rôles d'administration, les règles de transfert et le partage.
04	Mots de passe divulgués	Recherché les comptes de votre domaine dans les fuites de données et le renseignement sur les logiciels voleurs d'identifiants. Nous signalons les comptes et les dates; nous ne récupérons ni n'utilisons jamais les mots de passe.
05	Mesures de base	Entrevue fondée sur les contrôles de cybersécurité de base pour les petites et moyennes organisations du Centre canadien pour la cybersécurité.

COMMENT LIRE LES RÉSULTATS

COTE	SIGNIFICATION	À CORRIGER
ÉLEVÉ	Façon réaliste d'entrer pour un attaquant, avec un impact sérieux	Ce mois-ci
MOYEN	Augmente la probabilité ou les dommages d'un incident	Ce trimestre
FAIBLE	Bonne pratique; risque limité à lui seul	Quand c'est possible

LIMITES Ce bilan est une photo à un moment précis, pas un test d'intrusion : rien n'a été exploité, le réseau interne n'a pas été balayé et les applications Web n'ont pas été testées. Un bon résultat dans un domaine ne garantit pas qu'il est sécuritaire. Les constats reflètent ce qui était visible du 5 au 16 octobre 2026.

Constats (1 de 2)

CLASSÉS PAR RISQUE

BS-01 Le Bureau à distance est accessible depuis Internet

ÉLEVÉ

CONSTAT

Le Bureau à distance (RDP) du serveur de fichiers répond à n'importe qui sur Internet.

203.0.113.14:3389 ouvert · Windows Server 2012 R2

POURQUOI C'EST IMPORTANT

Les attaquants balaient tout Internet à la recherche de RDP ouverts et essaient des mots de passe volés ou devinés. C'est une porte d'entrée courante des rançongiciels.

COMMENT CORRIGER

Bloquer le port 3389 au pare-feu. Les employés qui ont besoin du serveur passent par le RPV avec un deuxième facteur.

Effort : ~1 heure · fournisseur informatique

BS-02 Le micrologiciel du RPV a une vulnérabilité activement exploitée

ÉLEVÉ

CONSTAT

La page de connexion du RPV indique une version de FortiOS touchée par CVE-2024-21762, que la CISA répertorie comme exploitée.

vpn.lumen-courier.example · FortiOS 7.0.x

POURQUOI C'EST IMPORTANT

La faille peut permettre d'exécuter du code sur le RPV sans mot de passe, ce qui donne un point d'appui dans le réseau.

COMMENT CORRIGER

Installer la version corrigée du fabricant, puis vérifier les journaux du RPV pour des connexions inconnues depuis la publication de la faille.

Effort : ~2 heures · fournisseur informatique

BS-03 6 des 41 comptes Microsoft 365 n'ont pas de deuxième facteur

ÉLEVÉ

CONSTAT

L'authentification multifacteur n'est pas imposée. Six comptes n'ont jamais enregistré de deuxième facteur, dont un administrateur général.

6/41 sans AMF · 1 des 3 administrateurs généraux

POURQUOI C'EST IMPORTANT

Pour ces comptes, un mot de passe hameçonné ou divulgué suffit, et le compte administrateur contrôle tout l'environnement.

COMMENT CORRIGER

Imposer l'AMF à tous (paramètres de sécurité par défaut ou accès conditionnel). Donner aux administrateurs un compte distinct réservé à l'administration.

Effort : ~2 heures · fournisseur informatique

BS-04 3 mots de passe d'employés volés par un logiciel malveillant

ÉLEVÉ

CONSTAT

Trois comptes de l'entreprise figurent dans des journaux de logiciels voleurs d'identifiants recueillis entre juin et septembre 2026. Les noms d'utilisateur sont dans l'annexe confidentielle remise au président.

3 comptes · source : renseignement sur les voleurs d'identifiants

POURQUOI C'EST IMPORTANT

Ces logiciels copient aussi les sessions du navigateur : un attaquant peut entrer même sans le mot de passe. Les ordinateurs infectés peuvent encore l'être.

COMMENT CORRIGER

Réinitialiser les trois mots de passe, fermer toutes les sessions et vérifier ou réinstaller les ordinateurs utilisés. L'AMF (BS-03) limite les dégâts.

Effort : ~3 heures · fournisseur informatique et employés

BS-05 Votre domaine peut être usurpé par courriel

MOYEN

CONSTAT

DMARC est en mode surveillance seulement et SPF se termine par un échec souple : les serveurs de réception livrent les faux courriels.

_dmarc : p=none · SPF : ~all · aucun MTA-STS

POURQUOI C'EST IMPORTANT

Les fausses factures ou demandes de changement de paiement qui semblent venir de votre équipe sont au départ de la plupart des fraudes.

COMMENT CORRIGER

Analyser les rapports DMARC pendant deux semaines, passer à p=quarantine, puis à p=reject. Changer SPF pour -all.

Effort : ~1 heure sur 4 semaines · fournisseur informatique

Constats (2 de 2)

CLASSÉS PAR RISQUE

BS-06 Deux boîtes transfèrent tous leurs courriels vers l'extérieur

MOYEN

CONSTAT

Deux boîtes ont des règles qui transfèrent chaque message vers des adresses Web personnelles. Le transfert externe est permis pour tout l'environnement.

2 règles · paramètre : transfert externe activé

POURQUOI C'EST IMPORTANT

Des renseignements de clients et de paiement sortent de l'entreprise sans protection. Les attaquants créent aussi de telles règles pour surveiller les factures.

COMMENT CORRIGER

Valider avec les deux utilisateurs, supprimer les règles et bloquer le transfert externe automatique pour tous.

Effort : ~30 minutes · fournisseur informatique

BS-07 Le serveur de fichiers utilise une version de Windows non soutenue

MOYEN

CONSTAT

Le serveur de fichiers fonctionne sous Windows Server 2012 R2, qui ne reçoit plus de mises à jour de sécurité depuis octobre 2023.

FS01 · Windows Server 2012 R2

POURQUOI C'EST IMPORTANT

Les nouvelles failles ne seront jamais corrigées, et il contient les fichiers partagés de l'entreprise.

COMMENT CORRIGER

Planifier son remplacement (serveur récent ou SharePoint). D'ici là, le garder hors d'Internet (BS-01) et limiter qui peut l'atteindre.

Effort : projet · direction et fournisseur informatique

BS-08 Sauvegardes jamais testées, sans copie hors ligne

MOYEN

CONSTAT

Les sauvegardes de nuit vont vers un appareil de stockage sur le même réseau. Personne ne se souvient d'un test de restauration.

Entrevue · NAS sur le réseau du bureau

POURQUOI C'EST IMPORTANT

Les rançongiciels chiffrent ou suppriment d'abord les sauvegardes accessibles. Une sauvegarde jamais testée peut ne pas fonctionner le jour venu.

COMMENT CORRIGER

Ajouter une copie hors ligne ou immuable dans le nuage. Tester une restauration chaque trimestre et noter le temps requis.

Effort : ~1 jour · fournisseur informatique

BS-09 Fichiers partagés avec « tout le monde », sans expiration

FAIBLE

CONSTAT

27 liens actifs vers des fichiers SharePoint et OneDrive fonctionnent pour quiconque les possède, et n'expirent jamais.

27 liens anonymes · aucune expiration

POURQUOI C'EST IMPORTANT

Un lien transféré ou divulgué expose le fichier à n'importe qui, sans trace de qui l'a ouvert.

COMMENT CORRIGER

Limiter le partage par défaut aux personnes de l'organisation; imposer une expiration (p.ex. 30 jours) aux liens externes; revoir les 27.

Effort : ~1 heure · fournisseur informatique

BS-10 Aucun plan écrit en cas de cyberincident

FAIBLE

CONSTAT

Il n'existe aucun plan d'intervention, et le personnel ne savait pas qui appeler ni quoi faire en premier.

Entrevue

POURQUOI C'EST IMPORTANT

La première heure détermine le coût d'un incident. Les assureurs demandent aussi un plan.

COMMENT CORRIGER

Rédiger un plan d'une page : qui décide, qui appeler (TI, assureur, avocat), ce qu'il ne faut pas toucher. La fiche gratuite « première heure » de Privateer est un bon point de départ.

Effort : ~2 heures · direction

Vos 10 correctifs, dans l'ordre

IMPACT D'ABORD, PUIS EFFORT

LE PLAN

	CORRECTIF	CONSTAT	EFFORT	QUI	QUAND
01	Bloquer le Bureau à distance depuis Internet	BS-01	1 h	Fournisseur TI	Semaine 1
02	Réinitialiser les 3 comptes exposés, fermer les sessions, vérifier leurs ordinateurs	BS-04	3 h	TI et employés	Semaine 1
03	Imposer l'AMF à tous; comptes d'administration distincts	BS-03	2 h	Fournisseur TI	Semaine 1
04	Mettre à jour le RPV et vérifier ses journaux	BS-02	2 h	Fournisseur TI	Semaine 1
05	Supprimer les 2 règles de transfert; bloquer le transfert externe	BS-06	30 min	Fournisseur TI	Semaine 2
06	Passer DMARC à quarantaine, puis reject; SPF à -all	BS-05	1 h	Fournisseur TI	Mois 1
07	Ajouter une copie hors ligne et tester une restauration	BS-08	1 jour	Fournisseur TI	Mois 1
08	Limitier les liens « tout le monde » et imposer une expiration	BS-09	1 h	Fournisseur TI	Mois 1
09	Rédiger un plan d'intervention d'une page	BS-10	2 h	Direction	Mois 1
10	Planifier le remplacement du serveur de fichiers	BS-07	Projet	Direction et TI	Trimestre

SEMAINE 1 Les correctifs 1 à 4 demandent environ **8 heures de travail informatique** au total et règlent les quatre problèmes à risque élevé. La plupart des petits fournisseurs informatiques peuvent les faire en une visite.

APRÈS LES CORRECTIFS

Contre-vérification (facultative). Une fois les correctifs de la semaine 1 faits, une courte vérification confirme qu'ils fonctionnent et met ce rapport à jour.

Votre assureur et vos clients. La page 1 peut être transmise à votre assureur ou à un client qui s'informe de votre sécurité. Les pages 3 à 5 sont à garder à l'interne.

Aller plus loin. Pour savoir ce qu'un attaquant pourrait réellement faire avec ces constats, un test d'intrusion est la prochaine étape. Les clients du bilan obtiennent 10 % de rabais s'il est réservé dans les 60 jours.

Mesures de base : contrôles nationaux

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

BILAN · 3 RESPECTÉS · 7 PARTIELS · 3 NON RESPECTÉS

	CONTRÔLE	ÉTAT	CE QUE NOUS AVONS VU
01	Plan d'intervention en cas d'incident	NON	Aucun plan écrit (BS-10)
02	Correctifs automatiques	PARTIEL	Portables mis à jour automatiquement; RPV et serveur non (BS-02, BS-07)
03	Logiciel de sécurité	OUI	Microsoft Defender actif sur tous les portables
04	Configuration sécuritaire	PARTIEL	Paramètres surtout renforcés; RDP exposé (BS-01)
05	Authentification forte	NON	AMF non imposée (BS-03)
06	Sensibilisation	PARTIEL	Abordée à l'accueil seulement
07	Sauvegarde et chiffrement	PARTIEL	Sauvegardes présentes; aucune copie hors ligne, jamais testées (BS-08)
08	Mobilité sécuritaire	PARTIEL	Téléphones protégés par NIP; non gérés centralement
09	Défenses du périmètre	NON	RDP et RPV vulnérable accessibles (BS-01, BS-02)
10	Infonuagique et TI impartie	PARTIEL	Le contrat du fournisseur TI n'a aucune clause de sécurité
11	Sites Web sécuritaires	OUI	Site en HTTPS avec certificat valide
12	Contrôle d'accès	PARTIEL	Compte administrateur utilisé au quotidien
13	Supports amovibles	OUI	Clés USB bloquées par politique

ANNEXE · OUTILS ET TERMES

Outils utilisés : journaux de transparence des certificats, subfinder, httpx, nmap (adresses autorisées seulement), nuclei, testssl.sh, checkdmrc, CISA ScubaGear, Microsoft Secure Score, renseignement sur les fuites et les voleurs d'identifiants. Tous les résultats ont été confirmés à la main.

AMF : deuxième preuve d'identité après le mot de passe. **DMARC :** indique aux serveurs quoi faire des faux courriels. **RDP :** accès à distance à un ordinateur Windows. **Voleur d'identifiants :** logiciel malveillant qui copie les mots de passe et les sessions du navigateur.

Un bilan pour votre organisation?

Prix fixe, en lecture seule, rapport en deux semaines. En français ou en anglais.