Rétablissement des systèmes, conclusions de l'enquête et lignes directrices en matière de conformité *(27 août 2025)*

Surveillance et confirmation du rétablissement des systèmes

Nous avons mis à l'essai nos systèmes durant la fin de semaine dernière en levant temporairement nos mesures de rétention chaque jour et en surveillant très attentivement toutes les activités. Nous avons testé et validé les accès à nos systèmes. Ni l'OCRI ni les équipes de sécurité de CrowdStrike n'ont détecté d'activité suspecte. Le trafic du réseau entrant et sortant était conforme à nos attentes.

En ce qui concerne le rétablissement des services, nous prioriserons les systèmes qu'utilisent les membres pour remplir leurs obligations de déclaration ainsi que ceux diffusant de l'information publique, notamment :

- Services de l'OCRI;
- Système d'enregistrement des plaintes et des règlements (ComSet);
- Système de suivi et de rapport de la formation continue (SSRFC);
- Site réservé aux courtiers membres en épargne collective;
- SDE;
- Système d'établissement de relevés des opérations sur le marché (SEROM);
- Rapport *Info-conseiller;*
- Information sur les titres de créance privés et publics.

Nous vous rappelons que les fonctions critiques comme la surveillance des marchés ont continué d'être exercées efficacement depuis le début de l'incident, grâce à des solutions de contournement et à l'infrastructure qui n'a pas été touchée ou désactivée dans le cadre de l'enquête et qui a été jugée sécuritaire.

Conformité avec les obligations de déclaration

Nous nous attendons à ce que les sociétés s'acquittent de leurs obligations de déclaration lorsque les systèmes seront de nouveau accessibles en ligne.

- En ce qui concerne les rapports dont l'échéance tombait durant la période d'interruption des systèmes (et ce, jusqu'au lundi 1er septembre inclusivement), les sociétés pourront les soumettre dans les cinq (5) jours ouvrables suivant la date de l'avis confirmant le rétablissement des systèmes.
- Pour ce qui est des rapports devant être soumis le mardi 2 septembre ou après cette date, les sociétés devront les soumettre à temps, conformément à leurs obligations.

Constatations confirmées par notre enquête

Comme vous le savez déjà, l'OCRI a immédiatement activé ses protocoles d'intervention en cas d'incident et engagé les experts techniques de CrowdStrike. Ensemble, nous avons mené une enquête approfondie et pris des mesures correctives pour assurer l'intégrité, la confidentialité et l'accessibilité de nos systèmes et services.

Nous pouvons confirmer ce qui suit :

- Aucune menace active n'a été détectée dans l'environnement de l'OCRI depuis l'interruption des systèmes le 11 août.
- Le point d'entrée et l'ampleur de l'attaque ont été déterminés et confirmés par notre enquête et des artéfacts judiciaires, y compris des fichiers journaux.
- L'OCRI ainsi que les logiciels de détection et de réponse des terminaux (EDR) et les logiciels judiciaires de CrowdStrike n'ont trouvé aucune preuve attestant le déploiement d'un maliciel ou d'un logiciel de chiffrement.
- Les données de nos systèmes n'ont pas été manipulées ni supprimées.

Mesures correctives techniques prises

Nous avons aussi pris des mesures correctives techniques. Par exemple :

- Tous les systèmes et services touchés ont fait l'objet d'examens complets de la sécurité et d'une validation technique. Les appareils touchés par l'incident ont été remplacés.
- Les comptes d'utilisateur et les logiciels touchés par l'incident ont été supprimés.
- Des logiciels de sécurité supplémentaires ont été déployés dans tous les appareils afin de nous protéger contre les menaces connues et d'y réagir de façon proactive.
- L'isolation et l'intégrité de nos systèmes de secours ont été confirmées.
- Tous les renseignements de connexion et d'accès du personnel de l'OCRI et des fournisseurs de services ont été réinitialisés dans l'ensemble de l'environnement.
- Un service de surveillance du Web clandestin a été activé, et rien n'indique que les renseignements copiés durant cet incident ont été vendus ou communiqués.