Ministres des Finances et des gouverneurs des banques centrales du Groupe des Sept (G7)
Prochaines étapes pour renforcer la cyberrésilience du secteur financier
à l'échelle internationale
Document de référence
Octobre 2018

L'amélioration de la cyberrésilience du secteur financier demeure une priorité pour les pays du G7. Le groupe d'experts cybernétiques (GEC) du G7 continue d'appuyer les efforts des ministres des Finances et des gouverneurs des banques centrales du G7 visant à faciliter la coordination entre les membres et à élaborer des pratiques efficaces en matière de cyberrésilience dans le secteur financier.

L'an dernier, les ministres des Finances et les gouverneurs des banques centrales du G7 ont publié les *Éléments fondamentaux pour l'évaluation efficace de la cybersécurité dans le secteur financier*, qui ont fourni aux entités un ensemble de résultats démontrant de bonnes pratiques en matière de cybersécurité, ainsi qu'un ensemble d'éléments de haut niveau non prescriptifs et non juridiquement contraignants pouvant être utilisés pour évaluer leur niveau de cybersécurité. Ces éléments fondamentaux peuvent être utiles aux entités publiques et privées lorsqu'elles envisagent des pratiques efficaces pour les essais de pénétration fondés sur les menaces et la gestion des risques cybernétiques de tiers dans le secteur financier.

Aujourd'hui, nous publions deux nouveaux ensembles d'éléments fondamentaux : les *Éléments fondamentaux pour les tests de pénétration fondés sur les menaces* et les *Éléments fondamentaux pour la gestion des risques cybernétiques liés à des tiers dans le secteur financier*.

Les *Éléments fondamentaux pour les tests de pénétration fondés sur les menaces* fournissent aux organisations un guide pour évaluer leur résilience face aux cyberincidents au moyen d'événements simulés. Les *Éléments fondamentaux pour les tests de pénétration fondés sur les menaces* énoncent six (6) éléments de base que les entités et les autorités peuvent utiliser lorsqu'elles conçoivent, mettent en œuvre et gèrent ces essais. Ces éléments sont les suivants : (1) définition du champ d'application du test et gestion des risques; (2) ressources; (3) renseignements relatifs aux menaces; (4) tests de pénétration; (5) clôture et actions correctrices; (6) données thématiques.

Les *Éléments fondamentaux pour la gestion des risques cybernétiques liés à des tiers dans le secteur financier* fournissent des pratiques exemplaires pour gérer les risques cybernétiques posés par des tiers aux entités privées et publiques du secteur financier et ils proposent aux organisations des éléments de haut niveau à utiliser dans le cadre de leurs pratiques de gestion des risques cybernétiques par des tiers. Elles énoncent six éléments fondamentaux pour les entités et les autorités chargées de gérer les risques cybernétiques liés aux tiers, notamment : (1) gouvernance; (2) processus de gestion des risques concernant les risques cybernétiques liés à des tiers; (3) intervention en cas d'incident; (4) plan de contingence; (5) surveillance des risques pouvant avoir des conséquences systémiques; (6) coordination entre les secteurs.

Pour ce qui est de l'avenir, le groupe d'experts cybernétiques continuera d'appuyer les ministres des Finances et les gouverneurs des banques centrales en entreprenant des activités visant à

promouvoir la cyberrésilience dans le secteur financier. Cela comprend d'autres travaux visant à améliorer la connaissance de la situation et la coordination des interventions en cas de cyberincidents au moyen d'un exercice transfrontalier de simulation cybernétique auquel participeront les autorités financières du G7, ainsi qu'un engagement accru des autorités financières du G7 et des intervenants du secteur privé.