Combattre le crime économique — et vaincre ensemble

Contrer les menaces en combinant nos forces en matière de fraude, de crimes financiers et de cybersécurité

KPMG au Canada

home.kpmg/ca/fr/

Avant-propos

En raison de différences culturelles et organisationnelles ancrées de longue date, les équipes de lutte contre la fraude et les crimes financiers et les spécialistes en cybersécurité travaillent souvent en vase clos. Pourtant, la ligne de démarcation entre crime économique et cybercrime est en train de s'estomper, une réalité qu'ont déjà comprise les auteurs des attaques.

Les innovations numériques, l'évolution des besoins des entreprises et des clients et le raffinement croissant des méthodes utilisées par les réseaux criminels ont fait naître de nouveaux dangers pour la société et l'économie. La situation exige que nous unissions nos forces autour d'une approche globale pour lutter contre la prolifération des menaces dans ce nouveau monde.

Points saillants

- Il est essentiel de conjuguer les efforts en matière de fraude, de crimes financiers et de cybersécurité pour combattre efficacement le crime économique dans notre nouvelle réalité.
- Les communications la collaboration doivent se faire dans un esprit d'ouverture et de transparence.
- Les approches relatives à la gouvernance des risques et à l'évaluation des menaces sont de plus en plus intégrées.
- L'efficacité passe par l'unification des contrôles des processus et des outils.
- L'adoption d'une approche commune de réponse aux incidents s'impose.

Table des matières

Forger de nouvelles alliances efficaces pour lutter contre le crime économique 04

Des équipes innovantes avec des plans de match gagnants 06

Défendre activement son écosystème 14

Se préparer à affronter de nouvelles menaces plus complexes 16

Comment KPMG peut aider 17

Forger de nouvelles alliances efficaces pour lutter contre le crime économique

L'accès à la technologie numérique a fourni aux criminels une panoplie de nouveaux moyens pour perpétrer des crimes économiques, qu'il s'agisse de crimes financiers, de fraudes, de blanchiment d'argent ou de corruption. Une nouvelle réalité s'est installée dans la société, crime économique et crime technologique étant devenus indissociables. Comment faire face à cette situation? Pour les experts en criminalité économique, il n'existe qu'une solution : harmoniser les capacités opérationnelles et les mesures d'intervention.

Pour combattre le crime économique, les entreprises doivent revoir les bases actuelles du cadre de gouvernance lié aux crimes financiers, à la fraude et à la cybersécurité pour adopter une approche rigoureuse, efficace et résiliente, mais surtout plus globale et mieux intégrée. Il est également essentiel que leur système de défense puisse évoluer, car les criminels ne manquent pas d'imagination pour ce qui est de trouver de nouveaux stratagèmes de fraude.

Points communs

Si les équipes de cybersécurité, et celles chargées de la lutte contre la fraude et les crimes financiers ont évolué séparément en fonction des nouveaux défis qu'elles devaient relever, leurs différences tendent à s'estomper à l'ère numérique. Les spécialistes de la cybersécurité veillent à la sécurité de l'information, à la résilience des technologies et, dans une certaine mesure, aux contrôles de protection des renseignements personnels. Aujourd'hui, les équipes engagées dans la lutte contre les crimes financiers se concentrent principalement sur les activités liées au blanchiment d'argent, à la corruption, à l'évasion fiscale et à la surveillance du risque d'exposition à des sanctions. Quant aux équipes de lutte contre la fraude, elles s'intéressent aux menaces internes et aux fraudes financières telles que le piratage psychologique, la fraude par carte de crédit ou de débit et l'utilisation de passeurs d'argent. Chacune de ces équipes vise le même but : combattre le crime organisé qui cherche à tirer profit d'activités illégales perpétrées au moyen d'intrusions informatiques, de vols de données et de la manipulation de personnes vulnérables.

Les organisations bien établies tendent à intégrer leurs activités de prévention des crimes financiers (généralement liées à la réglementation), de lutte contre la fraude (gérées par l'entreprise et concentrées sur les pertes financières et la sécurité des clients) et de cybersécurité, les données, les analyses, les connaissances et les technologies étant largement partagées afin de permettre aux équipes de lutter ensemble contre les principales menaces.

L'évolution de l'écosystème

La gouvernance de la cybersécurité couvre tout ce qui touche à la fraude et aux crimes financiers. S'inspirant des règlements sur le blanchiment d'argent, la corruption et la subordination, les organismes de réglementation tiennent maintenant les organisations responsables de leur performance en matière de cybersécurité et de protection des données relatives à leur chaîne d'approvisionnement et à leur réseau croissant de partenaires.

La fraude et la cybersécurité, quant à elles, s'attaquent à des menaces similaires et évoluent dans le même sens. Dans ces deux domaines, les autorités, en particulier dans le secteur financier, imposent de plus en plus aux organisations l'obligation de protéger de manière adéquate les finances des clients et d'offrir un accès sûr aux applications financières et de commerce électronique.

Dans ces trois domaines, les frontières entre la gestion des risques d'entreprise et des risques liés aux fournisseurs s'estompent à mesure que les réseaux des fournisseurs deviennent plus complexes et interdépendants. Et comme les attentes des consommateurs en matière de sécurité augmentent, toutes les fonctions ont un rôle à jouer dans la protection de la marque et de la réputation.

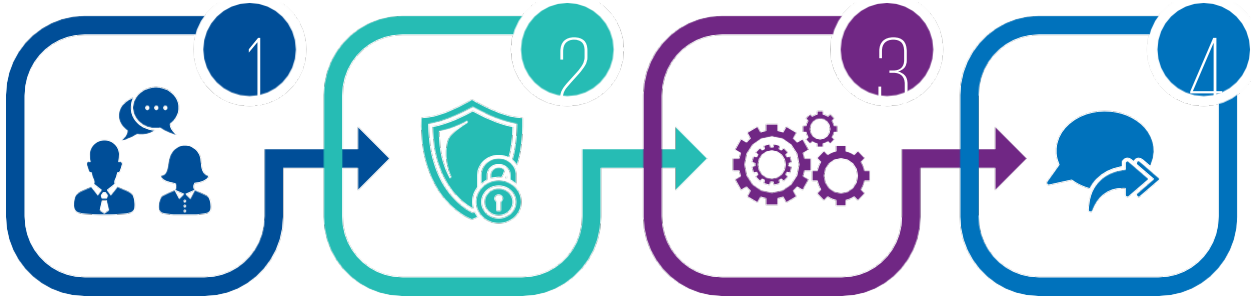
Des équipes innovantes avec des plans de match gagnants

Dans le cas de la fraude et des crimes financiers, certaines institutions financières ont innové en faisant participer leurs équipes de cybersécurité aux opérations. Grâce à l'intégration des outils d'analyse prédictive de la fraude et des renseignements sur la cybersécurité, une banque a réussi, en scrutant les adresses IP et les habitudes de paiement, à repérer les comptes des passeurs et à prévenir le blanchiment d'argent.

Dans un autre cas, les adresses IP ont été utilisées pour traquer un réseau qui exploitait des plateformes de commerce électronique pour tester des cartes de crédit et des portefeuilles électroniques volés. L'enquête qui a permis de le démasquer réunissait des équipes de lutte contre la fraude, les crimes financiers, le blanchiment d'argent et les cybercrimes.

Ces cas illustrent l'évolution vers une stratégie axée sur les données et la technologie, qui intègre la cybersécurité aux efforts qui visent à contrer la fraude et les crimes financiers dans le but d'améliorer l'efficacité de la détection et de la répression des crimes économiques.

Les quatre étapes vers l'harmonisation des efforts en matière de fraude, de crimes financiers et de cybersécurité



Améliorer la communication et la collaboration

Relier et harmoniser les approches en matière de gestion des risques et d'évaluation des menaces

Unifier les données, les contrôles et les outils associés aux processus

Établir une approche commune d'intervention en cas d'incident

À un niveau plus élevé, les organisations devraient réfléchir aux mesures qu'elles peuvent prendre pour s'associer et collaborer avec leurs pairs afin de défendre activement leur écosystème contre un ensemble de plus en plus convergent de fraudes économiques et de cybercrimes.

1re étape : Améliorer les communications et la collaboration

Améliorer la connaissance mutuelle de la terminologie et des cadres commerciaux et réglementaires propres à chaque groupe

Les équipes qui luttent contre les crimes financiers et la fraude communiquent en utilisant un jargon qui peut sembler étranger à l'équipe de cybersécurité, dont le propre langage technique sur les logiciels malveillants et les vecteurs d'attaque trouvent peu d'écho chez les enquêteurs sur les fraudes. C'est pourquoi ces équipes doivent trouver un langage commun, car elles combattent en fin de compte les mêmes réseaux criminels. Le transfert de connaissances entre les équipes peut combler certaines lacunes terminologiques et faire en sorte que chaque équipe comprenne bien les motivations et le contexte commercial des autres équipes.

Établir des points de contact diversifiés dans chaque équipe

Qu'elle soit affectée aux crimes financiers, à la prévention de la fraude ou à la cybersécurité, chaque équipe doit comprendre au moins un membre possédant une solide connaissance des autres domaines. Il est donc important d'exiger des compétences pluridisciplinaires lors du recrutement et d'améliorer les compétences du personnel en place par des programmes d'affectation et de rotation.

Tenir des réunions d'équipe conjointes et assister ensemble à des conférences

Les équipes chargées de la cybersécurité, et celles affectées aux crimes financiers et à la fraude devraient tenir des réunions conjointes pour discuter des défis, des pressions réglementaires et des facteurs opérationnels qui les touchent toutes et chercher des causes communes à différents aspects des crimes économiques. Les équipes de cybersécurité et de prévention de la fraude doivent par ailleurs veiller à ce que leurs représentants respectifs assistent aux conférences pertinentes sur la sécurité ou la fraude afin de mieux comprendre les divers types de menaces.

Briser la mentalité de cloisonnement et développer des méthodes de travail interfonctionnelles

Les organisations devraient permettre au personnel de passer d'une équipe à l'autre afin de briser le cloisonnement et favoriser la collaboration entre les équipes d'enquête en sélectionnant le personnel possédant les compétences et l'expérience appropriées.

Développer des méthodes de travail interfonctionnelles qui font appel à une conception des choses et à un savoir-faire permettant de travailler dans les différents domaines.

2e étape : Relier et harmoniser les approches en matière de gestion des risques et d'évaluation des menaces

Cartographier les meilleures pratiques, normes et règlements sectoriels

Les équipes de cybersécurité appliquent les meilleures pratiques découlant d'une série de normes de sécurité et de cadres d'application qui se reflètent aujourd'hui dans la législation sur l'audit financier, la réglementation sur la protection de la vie privée de nombreux territoires et la réglementation sur la résilience des infrastructures critiques. Les équipes chargées de la lutte contre la fraude et les crimes financiers appliquent les meilleures pratiques et les normes sectorielles à leurs cadres opérationnels. Le temps est venu de relier toutes les normes pertinentes au sein d'un cadre d'évaluation des risques mieux adapté aux nouveaux modèles, comportements et modus operandi des criminels. Ainsi, les équipes pourraient cartographier les règlements pertinents et les mesures prises pour prévenir, détecter et contrer les cybermenaces en les faisant correspondre aux pratiques de cybersécurité, comme le cadre de cybersécurité du NIST, dans le but de créer une norme commune d'audit interne et d'évaluation des risques.

Établir un cadre global d'évaluation des risques

Les équipes de cybersécurité, et celles chargées de la lutte contre la fraude et les crimes financiers adoptent différentes approches pour cerner, documenter et évaluer différents types de risques. Dans les secteurs réglementés tels que la finance, les organisations sont tenues de mettre en place des cadres formels à cette fin. Ceux-ci portent sur les clients, les canaux de distribution, les transactions, les tiers, le personnel, et les secteurs d'activité ou les territoires. De nombreuses organisations se sont dotées de cadres exigeant que les risques opérationnels soient évalués indépendamment pour chaque fonction.

Une approche opérationnelle plus globale de détection des menaces permettrait aux organisations d'acquérir une vue d'ensemble des risques liés à la fraude et à la cybersécurité, ainsi qu'à certains aspects de la protection des renseignements personnels, tout en demeurant centrées sur leur objectif principal, la lutte contre les crimes financiers. Les équipes devraient élaborer un cadre de contrôle unifié qui permette de détecter et de gérer efficacement les risques communs.

Former des groupes de travail conjoints et définir des IPC relatifs aux menaces communes

Tout en demeurant assujetties à des règles différentes en matière de gouvernance, les équipes devraient élaborer des mesures communes pour détecter et contrer les menaces qui pèsent sur l'ensemble de l'organisation. En plus de favoriser l'harmonisation des pratiques de travail, la création de groupes de travail opérationnels conjoints stimulerait l'effort collectif à l'égard des défis communs à relever.

2e étape : Relier et harmoniser les approches en matière de gestion des risques et d'évaluation des menaces (suite)

Unifier l'évaluation des menaces et partager les résultats de l'analyse des perspectives réglementaires

Les crimes financiers, les fraudes externes et les cyberattaques sont souvent perpétrés par le crime organisé au moyen de réseaux criminels à grande échelle. Quant aux fraudes internes et aux menaces à la sécurité provenant de l'intérieur de l'organisation, elles sont souvent le fait du même groupe de personnes. Ainsi, les changements dans le mode opératoire des réseaux criminels et dans le cadre de réglementation peuvent avoir des incidences sur le contrôle technique exercé par les trois équipes concernées.

Les équipes de cybersécurité et de lutte contre la fraude et les crimes financiers pourraient organiser des ateliers d'évaluation des menaces avec les unités opérationnelles en vue de cerner les menaces communes, de partager les données et les sources de renseignement, et de stocker l'information pertinente dans un seul et même référentiel. Chaque équipe devrait également veiller à partager les résultats de l'analyse des perspectives réglementaires.

3e étape : Unifier les données, les contrôles et les outils associés aux processus

Exploiter les contrôles prédictifs des risques de fraude basés sur les données dans une optique de cybersécurité

Certains secteurs d'activité et territoires sont plus exposés aux risques de blanchiment d'argent, de subordination et de corruption liés aux transactions, aux responsables en place et aux fournisseurs. Une bonne pratique à cet égard consiste à établir une liste des territoires et des secteurs à haut risque. Outre l'évaluation et la catégorisation des risques effectuées à l'interne, les organisations peuvent consulter des sources externes, y compris les évaluations nationales des risques et des menaces, et les listes publiées par des ONG, notamment l'Indice de perception de la corruption (Corruption Perceptions Index) de Transparency International. Ces informations seront également utiles pour mettre en œuvre une approche des contrôles de sécurité fondée sur le risque ou prévoir l'exposition aux crimes technologiques lorsqu'une entreprise projette de faire affaire dans certains territoires.

Les équipes de cybersécurité qui veulent agir proactivement devraient explorer de nouvelles façons d'optimiser les outils de surveillance, les autorisations d'accès et les exigences de sécurité des applications, à la lumière des indicateurs de risque de fraude et de crimes financiers. Elles pourraient également étudier la possibilité d'intégrer à ce cadre de contrôle renforcé les transactions financières provenant de fournisseurs, d'employés ou d'adresses IP.

Déceler les possibilités d'unifier les outils en matière de prévention et de détection des fraudes

Les équipes de cybersécurité utilisent un éventail d'outils de surveillance des données réservées aux utilisateurs privilégiés, de prévention des pertes de données, de surveillance du Web invisible, de gestion de l'information et des événements de sécurité (SIEM) et de détection des logiciels malveillants.

Les équipes de lutte contre la fraude et les crimes financiers pourraient partager les renseignements qu'elles détiennent afin d'améliorer les techniques d'analyse des risques de l'équipe de cybersécurité, qui comprennent la surveillance des utilisateurs à haut risque et des activités connexes. Le groupe de lutte contre la fraude pourrait-il fournir des données permettant de mieux configurer les systèmes de défense (filtrage du courrier électronique et du Web, contrôles de prévention des pertes de données, etc.)? Les analystes qui examinent les alertes pourraient-ils être mieux formés sur les processus financiers utilisés pour commettre des fraudes?

Il est en outre important que les équipes de cybersécurité comprennent le fonctionnement des systèmes d'analyse de la fraude fondée sur les données et l'utilisation optimale qu'on peut en faire pour gérer le risque de fraude et de menaces internes. Tout en contribuant à prévenir la fraude et les cybercrimes, l'unification des outils permettrait de réduire le nombre d'enquêtes juricomptables et la nécessité de déployer des plans d'intervention.

3e étape : Unifier les données, les contrôles et les outils associés aux processus (suite)

Concevoir une architecture de prestation unifiée pour tous les produits et canaux de distribution

Les entreprises offrent généralement une multitude de services numériques par le biais de divers circuits de vente comportant chacun leurs propres exigences en matière d'adhésion, de sécurité de base et de prévention de la fraude. Il est difficile pour les organisations du secteur des services financiers d'obtenir une vue unique du client, ce que vient aggraver le manque de cohésion des méthodes d'exploitation, de surveillance et de sécurisation de chaque service ou circuit.

La création d'une vue unique et intégrée des interactions clients pour l'ensemble des circuits d'accès aux produits, qui repose sur une approche fondée sur les données, peut simplifier le développement de produits de consommation et fournir des informations cohérentes et globales aux équipes de cybersécurité et de lutte contre la fraude et les crimes financiers chargées d'en gérer les risques.

Intégrer des contrôles relatifs à la fraude et aux crimes financiers dans un processus DevOps sécurisé

Il est important que les équipes de cybersécurité qui s'efforcent d'accroître l'agilité du processus de développement sécurisé de logiciels et d'applications (DevOps) soient conscientes qu'il est également possible d'inclure dans ce processus des contrôles relatifs à la fraude et aux crimes financiers.

Alors que les attentes des clients quant à la sécurité des applications et des transactions financières augmentent, promouvoir une approche de prévention de la fraude et des crimes financiers axée sur la « fiabilité et la sécurité planifiées » peut favoriser la fidélisation de la clientèle et l'établissement de partenariats au sein de l'entreprise.

Intégrer des contrôles à toutes les étapes du cycle de gestion de la relation client

Même si certains consommateurs estiment que les contrôles financiers et de sécurité appliqués aux produits et services sont trop intrusifs, la réputation de la marque et la fidélisation de la clientèle d'une organisation dépendent de plus en plus de l'efficacité des mesures de défense contre la fraude, les crimes financiers et les cyberattaques.

Les trois équipes devraient jouer des rôles de premier plan au sein de l'entreprise et auprès des clients en intégrant aux produits et services des mécanismes d'authentification et de vérification de l'identité qui ont un impact minimal sur l'expérience client. Il peut s'agir de méthodes d'authentification comportementale fondées sur le risque et de technologies de reconnaissance alimentées par l'apprentissage automatique. Il y aurait également lieu d'intégrer les indicateurs clés de performance (ICP) liés aux contrôles de sécurité des clients aux ICP établis en matière de fraude et de crimes financiers.

4e étape : Établir une approche commune d'intervention en cas d'incident

Mettre en place un bureau de service centralisé pour améliorer la gestion des incidents dans toutes les fonctions

L'absence d'un bureau de service centralisé complique souvent la coordination des interventions en cas d'incident. La surveillance et le signalement des incidents (perte de données, fraudes, crimes financiers, cyberattaques et problèmes informatiques) sont-ils assurés par des systèmes séparés au sein de votre organisation? Utilisez-vous des canaux distincts pour les incidents internes, les incidents externes et ceux liés aux clients, même si les événements sont étroitement liés? Les cas de fraude, de fuite de données ou d'intrusion de maliciels sont-ils assujettis à des processus indépendants de recours hiérarchique, même lorsque tous les éléments concernent une même attaque?

Les organisations devraient envisager d'intégrer tous les bureaux de service pour harmoniser la gestion des parties prenantes et des ressources, des délais de réponse et de la production de données en temps réel, et pour veiller à ce que les incidents soient étudiés dans leur intégralité, du point de déclenchement au niveau du client ou de l'employé jusqu'à leur signalement dans le système SIEM et leur résolution éventuelle.

Harmoniser les carnets tactiques de l'équipe de cybersécurité, et des équipes chargées de la lutte contre la fraude et les crimes financiers

Les carnets tactiques des cyberincidents exposent en détail la façon dont les équipes des centres opérationnels de la sécurité des systèmes d'information répondent à des cas d'utilisation spécifiques, tels que les attaques par déni de service distribué (DDoS), les rançongiciels, l'abus de privilèges et la perte de données.

Les évaluations des équipes de lutte contre la fraude et les crimes financiers portent sur des menaces ciblées et prioritaires. Si l'on pouvait combiner l'expertise acquise et les renseignements tirés des carnets tactiques et des évaluations pour rationaliser l'approche et élargir la portée de l'évaluation, il serait possible d'améliorer les étapes du tri, du traitement, de l'investigation et de la gestion des perturbations liées à certaines menaces. Cela permettrait également de mieux définir les exigences en matière d'indemnisation des clients et de notification réglementaire.

Travailler en collaboration avec l'équipe rouge ou pourpre

Les équipes de cybersécurité font appel à des tiers pour mener des exercices de simulation de cyberattaque, dans lesquels les outils de détection des incidents, les carnets tactiques et les activités de sécurité interne (l'équipe « bleue ») sont testés par un acteur de la menace simulée (l'équipe « rouge ») dans un contexte d'opposition.

Les équipes de lutte contre la fraude et les crimes financiers pourraient collaborer avec l'équipe rouge ou pourpre, afin de tester les carnets tactiques sur les incidents, et d'évaluer l'efficacité des outils de détection des fraudes et des processus d'intervention.

4e étape : Établir une approche commune d'intervention en cas d'incident (suite)

Inviter toutes les équipes à participer à l'analyse du bilan d'après-incident

L'un des défis de la réponse aux incidents est de comprendre la séquence complète des événements qui ont permis à un intrus de compromettre un réseau ou de déjouer les contrôles de prévention. Il est essentiel de s'assurer que les équipes en contact avec la clientèle, et celles chargées des fraudes internes et de la sécurité de l'information participent à l'analyse du bilan d'après-incident afin de dégager une vue globale claire de l'incident.

Que pouvez-vous apprendre des autres équipes? Peut-être ont-elles une visibilité sur des angles du cadre de contrôle qui vous échappent? Une meilleure vue d'ensemble du scénario de compromission peut aider les équipes à apporter des correctifs ciblés et efficaces aux lacunes du contrôle.

Défendre activement son écosystème

Pour mettre en œuvre ces innovations, les dirigeants doivent faire preuve de vision et de leadership, être déterminés à expérimenter de nouvelles façons de travailler et adopter une approche qui permettra de dégager rapidement des avantages concrets de la lutte contre la criminalité.

Il faut toutefois se rappeler que les cyberattaques et les crimes économiques sont des problèmes systémiques qui nécessitent une action concertée à l'échelle sectorielle. L'intégration des activités de cybersécurité, et de lutte contre la fraude et les crimes financiers à l'intérieur d'un écosystème élargi – comprenant les fournisseurs, les partenaires, les organismes de réglementation, les concurrents, etc. – est une étape importante pour renforcer la confiance et lutter efficacement contre la criminalité.

S'élever au-dessus du « seuil de pauvreté en matière de cybersécurité »

Les auteurs de cybermenaces, les fraudeurs et les bandes organisées sont souvent liés et interdépendants. Ces groupes criminels évitent généralement les entreprises dotées d'un programme de cybersécurité, de contrôles antifraude et de processus d'intervention solides pour se concentrer sur les organisations moins bien outillées qui se situent sous ce que le Centre de cybersécurité du Forum économique mondial appelle le « seuil de pauvreté en matière de cybersécurité ».

Les organisations disposant de solides capacités, les gouvernements et les forces de l'ordre ont mutuellement avantage à unir leurs efforts pour combattre activement les auteurs de menaces, plutôt que de simplement réagir aux agressions.

Les organisations bien établies qui ont été victimes de cyberattaques recueillent des renseignements techniques sur les fraudeurs, les auteurs de cybermenaces et les bandes organisées, renseignements qu'ils utilisent pour aider les services de police à démanteler ces groupes, et à identifier et arrêter les suspects. Les organisations doivent également travailler avec leurs partenaires de la chaîne d'approvisionnement, y compris les intervenants de première ligne et les centres opérationnels de sécurité afin de recueillir des données essentielles sur les auteurs des menaces.

Collaboration sectorielle

Des partenariats public-privé ont été créés dans certains territoires pour lutter contre les crimes économiques, mais également contre le cybercrime. Il faudrait intensifier ces efforts et élaborer des protocoles détaillés pour faciliter l'échange de renseignements et la collaboration entre les équipes chargées de la détection des menaces, ainsi qu'une certaine coordination avec les services de police et les regroupements sectoriels. La collaboration entre les pairs du secteur est essentielle pour lutter efficacement contre les problèmes sociaux qu'entraînent la cybercriminalité, la fraude et les autres crimes financiers.

Cette nouvelle façon de travailler en collaboration et en partenariat exige une transparence accrue entre les organisations et les services de police, ainsi que le soutien des organismes de réglementation et des entreprises concurrentes. Ce n'est qu'ensemble que toutes les parties concernées réussiront à combattre les attaques de grande envergure visant les industries et les chaînes d'approvisionnement, des attaques que les petites organisations sont incapables de repousser seules. Les gouvernements ont également un rôle clé à jouer dans la création d'un cadre juridique et opérationnel qui favorise la coopération et protège la vie privée des citoyens tout en luttant contre la criminalité.

Des techniques de défense active, allant de la détection préventive à la riposte offensive et à la perturbation, sont de plus en plus présentes dans le cyberespace depuis dix ans. Dans de nombreux cas, les partenariats entre les organisations privées et les organismes publics ont été essentiels à leur succès.

Rupture des réseaux zombis (botnets)

Un important fournisseur de technologie a collaboré avec le US Cyber Command pour fournir de fausses informations à des groupes de rançonneurs connus dans le but de provoquer une rupture de réseaux zombis[1].

Contamination d'un réseau anonyme

Un établissement d'enseignement américain a travaillé avec les forces de l'ordre pour contaminer le réseau de navigation anonyme Tor et démasquer les utilisateurs d'un marché bien connu du Web invisible[2].

Utilisation de données fournies par un partenaire

INTERPOL a utilisé les données recueillies par un partenaire du secteur privé pour identifier une souche de logiciels malveillants utilisés pour infecter des sites de commerce électronique dans le but de voler des renseignements relatifs à des cartes de paiement et des données personnelles. Les renseignements recueillis ont été diffusés aux pays concernés et ont permis l'arrestation de trois cybercriminels en Indonésie[3].

Sur le plan stratégique, le Centre national de cybersécurité du Royaume-Uni (NCSC) a mis en œuvre un programme de cyberdéfense active afin de réduire l'impact des cyberattaques les plus répandues sur les marchés britanniques. D'autres modèles de défense active sont également mis en œuvre pour combattre certaines formes de crimes économiques, avec des PPP combinant information et capacités pour accroître l'efficacité de la réponse.

Dans le secteur des services financiers britannique, la Joint Money Laundering Intelligence Taskforce (JMLIT), née d'un partenariat entre les organismes de réglementation, les services de police et le secteur financier, a remporté des succès significatifs depuis sa création en 2015 et est considérée à l'échelle internationale comme un exemple de pratique exemplaire. En tant que professionnels en matière de fraude, de crimes financiers et de cybersécurité, nous devons nous efforcer de trouver des moyens d'étendre les modèles de défense efficaces à un plus grand nombre de groupes et de stratagèmes criminels.

Se préparer à affronter de nouvelles menaces plus complexes

Une stratégie de défense active est essentielle pour contrer les menaces actuelles et éliminer à long terme certains des groupes responsables des campagnes de cybercriminalité et de fraude. Il faut toutefois s'attendre à ce que les cyberattaques et les fraudes se multiplient à mesure qu'elles s'adaptent à l'évolution des capacités technologiques. Les cybermenaces et les fraudes qui seront perpétrées dans la prochaine décennie tireront profit des nouvelles technologies et se propageront par le biais de chaînes d'approvisionnement et de modèles de travail complexes.

Pour relever le défi, les organisations doivent rassembler leurs forces en matière de cybersécurité, de fraude et de crimes financiers, et élargir leur stratégie relative aux données. Pour faire face aux nouveaux dangers qui menacent l'écosystème, il faudra investir davantage dans une réponse sectorielle coordonnée afin de cibler et de démanteler les réseaux de criminalité grave et organisée.

Comment KPMG peut aider

Présente à l'échelle mondiale, KPMG compte dans ses rangs de nombreux professionnels en matière de cybersécurité, de crimes financiers et de juricomptabilité qui vous offrent une vision multidisciplinaire des risques. Nous vous aidons à protéger votre organisation en vous donnant les moyens d'anticiper l'avenir, d'accélérer la cadence et de prendre de l'avance grâce à une technologie sûre et fiable.

Forte d'une excellente connaissance du marché et d'une solide expertise technique, notre équipe de professionnels créatifs saura vous guider pour accroître la résilience et l'agilité de votre cadre de gouvernance en matière de cybersécurité, de fraude et de crimes financiers. Ensemble, créons un monde numérique fiable, pour que vous puissiez repousser les limites du possible.

Communiquez avec nous

Les professionnels des Services-conseils – Gestion des risques de KPMG aident les organisations à transformer le risque en un avantage concurrentiel durable, et à venir à bout des problèmes les plus complexes. Pour obtenir un complément d'information, communiquez avec l'un de nos professionnels des Services-conseils – Gestion des risques.

Doron Telem
Leader national Services-conseils – Gestion des risques
KPMG au Canada
416-777-3815
dorontelem@kpmg.ca

Stéphan Drolet
Leader national Juricomptabilité
KPMG au Canada
514-840-2202
sdrolet@kpmg.ca

Hartaj Nijjar
Leader national Cybersécurité
KPMG au Canada
416-228-7007
hnijjar@kpmg.ca

Région du Grand Toronto

Enzo Carlucci
Associé Juricomptabilité
KPMG au Canada
416-777-3383
ecarlucci@kpmg.ca

Québec

Stéphan Drolet
Leader national Juricomptabilité
KPMG au Canada
514-840-2202
sdrolet@kpmg.ca

Ouest du Canada

Shelley Hayes
Associée Juricomptabilité
KPMG au Canada
403-691-8467
shelleyhayes@kpmg.ca

Est du Canada

Kas Rehman
Associé Juricomptabilité
KPMG au Canada
613-212-3689
kasrehman@kpmg.ca

Conception par Evalueserve.
Titre de la publication : Battling economic crime — and winning together Numéroi de publication : 137178-G