Canadian Institute of Actuaries / Institut canadien des actuaires

Cybersécurité : Le paysage de la menace financière et d'assurance

JESSE JORDAN

Expert-conseil principal, FireEye Mandiant

Cet article fait partie d'une collection d'articles portant sur la gestion du risque d'entreprise (GRE) de l'Institut canadien des actuaires (ICA). Ces articles ont été rédigés par des experts en la matière, actuaires et non-actuaires, qui nous donnent leurs propres opinions et nous font part de leurs expériences professionnelles. Ils mettent ainsi en lumière des questions nouvelles et émergentes dans le monde actuel de la gestion des risques. Lisez tous les articles à **cia-ica.ca/gre**.

Les cyberattaques continuent d'évoluer. Les organisations de toutes tailles sont ciblées par divers cybercriminels qui recourent à une vaste gamme de tactiques et de techniques. Les incidents d'extorsion sont en hausse et les attaques contre les services infonuagiques ont augmenté en raison d'une plus grande utilisation de l'infonuagique par les organisations dans le cadre de stratégies TI globales.

Bien que des cyberattaques contre tous les secteurs d'activité soient signalées, les institutions financières demeurent principalement visées. Parmi les incidents auxquels la division d'expertise-conseil Mandiant de FireEye (une firme de cybersécurité) a répondu en 2018, 23 % ont touché l'industrie des services financiers.

Portrait des menaces visant les industries des services financiers et de l'assurance

Les auteurs de menaces commandités par l'État continuent de poser un risque élevé pour les industries des services financiers et de l'assurance, qui ont toutes deux accès à un éventail de renseignements de nature délicate sur leurs clients. En ce qui concerne les assurances, les courtiers examinent les risques potentiels auxquels leurs clients sont exposés dans le cadre du processus de souscription. L'information recueillie, qui comprend des profils complets de vulnérabilité liés à des actifs de grande valeur, peut être utilisée par les auteurs de menaces pour déterminer les failles potentielles. Les auteurs de menaces commandités par l'État peuvent également faire bénéficier les intérêts commerciaux d'une nation en obtenant des renseignements économiques provenant de négociations commerciales avec des entités étrangères.

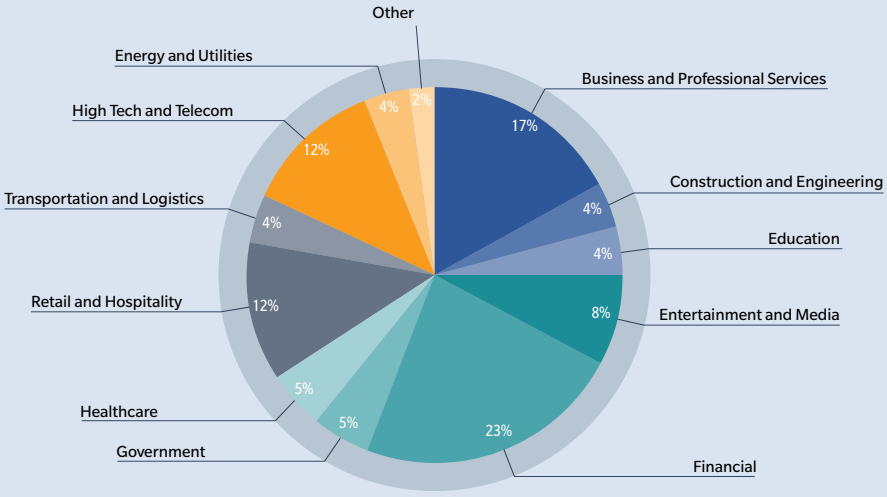
En 2018, la Corée du Nord, la Russie, la Chine et l'Iran ont été responsables du plus grand nombre d'attaques de cyberespionnage dans le monde. Nous avons constaté une complexité accrue des attaques d'auteurs nord-coréens ciblant des institutions financières par l'exploitation de vulnérabilités non déclarées auparavant (zero-day vulnerabilities), des attaques d'hameçonnage ciblées contre des chefs de la direction et des chefs des services financiers, et des attaques de chaîne d'approvisionnement motivées par un gain financier. Des attaques visant une chaîne d'approvisionnement peuvent survenir lorsque des pirates réussissent à infiltrer une organisation par l'entremise d'un fournisseur de produits ou services par le biais d'un code ou d'une infrastructure partagés en recourant à des modes de distribution fiables. Ces attaques sont particulièrement efficaces, car un seul élément compromis dans la chaîne d'approvisionnement peut faire un grand nombre de victimes. Mandiant a relevé des exemples récents où des auteurs de menaces ont été en mesure d'insérer un code malveillant dans des ressources logicielles collaboratives, dans certains cas par l'entremise de personnes malveillantes en interne, ou ont expédié à des clients des dispositifs renfermant un logiciel malveillant préinstallé. Si la rupture de la chaîne d'approvisionnement est suffisamment importante, les auteurs de menaces commandités par l'État passent essentiellement inaperçus.

Les auteurs de menaces considèrent les attaques de la chaîne d'approvisionnement comme un moyen efficace de contourner des années d'investissement dans des moyens de défense périmétriques par des organisations matures en termes de cyberdéfense. Ces dernières années, Mandiant a noté une importante augmentation de ces types d'attaques.

L'augmentation du nombre d'attaques de la chaîne d'approvisionnement à motivation financière par des auteurs de menaces commandités par l'État peut être attribuée en partie à des sanctions accrues contre certains des États-nations cités précédemment, lorsque l'obtention de fonds par tous les moyens est jugée nécessaire. Par exemple, dans le cadre d'opérations menées à l'échelle mondiale, des pirates nord-coréens ont tenté de voler plus de 1,1 milliard de dollars US à des sociétés financières en exploitant des transferts entre banques sur une période de deux années.

Les cybercriminels continuent également de cibler les entreprises dans les industries des services financiers et de l'assurance en tirant parti de l'ingénierie sociale et des attaques d'hameçonnage pour expédier des rançongiciels dans le but d'extorquer des organisations pour en tirer un gain financier. Les cybercriminels utilisent des méthodes semblables pour voler des renseignements de nature délicate à la fois aux assureurs et à leurs clients, en conservant ces renseignements sous la menace d'une divulgation publique si l'organisation ne répond pas à certaines demandes financières. Les cybercriminels tirent également parti des informations échangées dans le cadre de la souscription d'une police d'assurance par un client pour

Graphique 1 : Rapport M-Trends 2019 de FireEye Mandiant – Industries étudiées



Source : FireEye Mandiant, 2019. Reproduit avec permission. Disponible en anglais seulement.

recueillir des renseignements sensibles et les vendre ensuite sur les marchés clandestins pour le vol d'identité, l'extorsion et la fraude.

Mandiant prévoit que la cybercriminalité, en particulier la cyberfraude, continuera de progresser en 2019. La hausse des attaques contre des sites Web financiers, où des « cloneurs » virtuels sont utilisés pour voler des renseignements personnels, des numéros de cartes de paiement et des codes CVC de cartes de crédit, se poursuivra. En 2018, les auteurs de menaces financières ont eu recours à des techniques avancées pour contourner les processus d'enregistrement des comptes par l'entremise de portails en ligne afin d'avoir accès aux comptes, de transférer des fonds, de commander des chèques et de modifier les destinations des transactions.

Bien qu'ils posent un risque relativement faible pour les industries des services financiers et de l'assurance, les pirates informatiques activistes continuent de causer des perturbations sous forme d'attaques à motifs idéologiques, dont l'objectif consiste souvent à porter atteinte à la réputation d'une organisation, ce qui entraîne des pertes de parts de marché, soit en exposant des renseignements de nature délicate sur les clients, en volant des renseignements stratégiques ou en tentant de causer des interruptions d'affaires en effectuant des attaques par déni de service contre des sites Web destinés aux clients ou d'autres systèmes critiques.

La détection et l'intervention précoces sont essentielles

Les organisations des Amériques détectent plus rapidement les menaces à leur environnement. Le temps d'arrêt médian, qui correspond au temps pendant lequel les auteurs de menaces sont demeurés dans les réseaux de victimes, de la première preuve de compromission à la détection de l'intrusion, a diminué, passant de 99 jours en 2016 à 71 jours deux ans plus tard (voir le graphique 2). Cette diminution est en grande partie attribuable aux organisations qui travaillent à améliorer continuellement leur capacité de détecter rapidement les menaces – soit en créant des unités internes de surveillance des menaces, soit en mettant au point une capacité accrue de détection et d'intervention en matière de réseau, de point d'accès et d'infonuagique.

En outre, il importe d'assurer la participation de la sécurité aux pratiques de GRE au moyen d'une stratégie de gestion des risques clairement définie en ce qui a trait aux cybermenaces. Les organisations devraient adopter une vision structurée, incluant la mesure des risques, pour la sécurité et prévoir des stratégies claires d'atténuation et de correction.

Des processus détaillés de quantification, de classement, de propriété, de suivi et d'atténuation devraient être élaborés pour garantir l'application d'une approche uniforme et exhaustive. Des solutions centralisées de gestion des risques peuvent être mises en œuvre pour faciliter un suivi normalisé des risques de cybersécurité et des processus afférents.

Lors du suivi des risques, il convient de tenir compte des fournisseurs susceptibles d'exposer l'organisation dans les cas où ils seraient victimes d'une attaque. Il convient par le fait même d'implanter des contrôles connexes, comme la gestion d'un nombre réduit de fournisseurs et l'imposition d'exigences strictes de contrôle et d'attestation des fournisseurs, tout en veillant à ce que les changements non autorisés apportés aux logiciels soient décelés au moyen de processus établis.

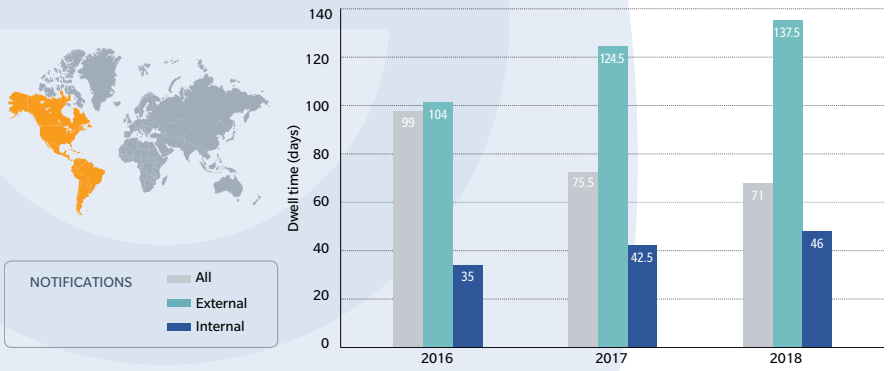
Les organisations doivent également assurer la mise en place d'un cadre et d'une méthodologie cohérents et systématiques de détection des incidents de cybersécurité, en plus de définir un processus d'analyse, de priorisation, de confinement et d'intervention.

Des exercices de simulation pour mesurer l'efficacité des interventions, combinés à des évaluations régulières de l'équipe d'intervention pour évaluer les capacités de détection et d'intervention de l'organisation, peuvent être utilisés pour rationaliser et améliorer davantage les capacités. Les tests de pénétration internes et externes constituent également un moyen efficace de détecter les vulnérabilités et les problèmes de configuration que les auteurs de menaces utilisent pour exploiter les environnements et obtenir davantage d'accès.

La formation du personnel sur la façon de repérer et de signaler un courriel d'hameçonnage, en particulier ceux qui demandent à l'utilisateur de prendre une mesure particulière, est également un facteur important pour empêcher les auteurs de menaces d'accéder initialement à un compte. Les simulations régulières d'hameçonnage représentent un moyen éprouvé de tester les messages de sensibilisation et l'efficacité globale des programmes.

Les atteintes à la sécurité sont inévitables, mais grâce à de solides pratiques de gouvernance de la sécurité et à une approche définie de gestion des incidents combinée à des mesures préventives, les organisations peuvent réduire leur impact global.

Graphique 2 : M-Trends 2019 de FireEye Mandiant – Temps d'arrêt médians dans les Amériques



Source : FireEye Mandiant, 2019. Reproduit avec permission. Disponible en anglais seulement.

Sources

[Mandiant] FireEye Mandiant Services. *M-Trends 2019: FireEye Mandiant Services|Special Report, FireEye*, Milpitas, 2019. https://content.fireeye.com/m-trends