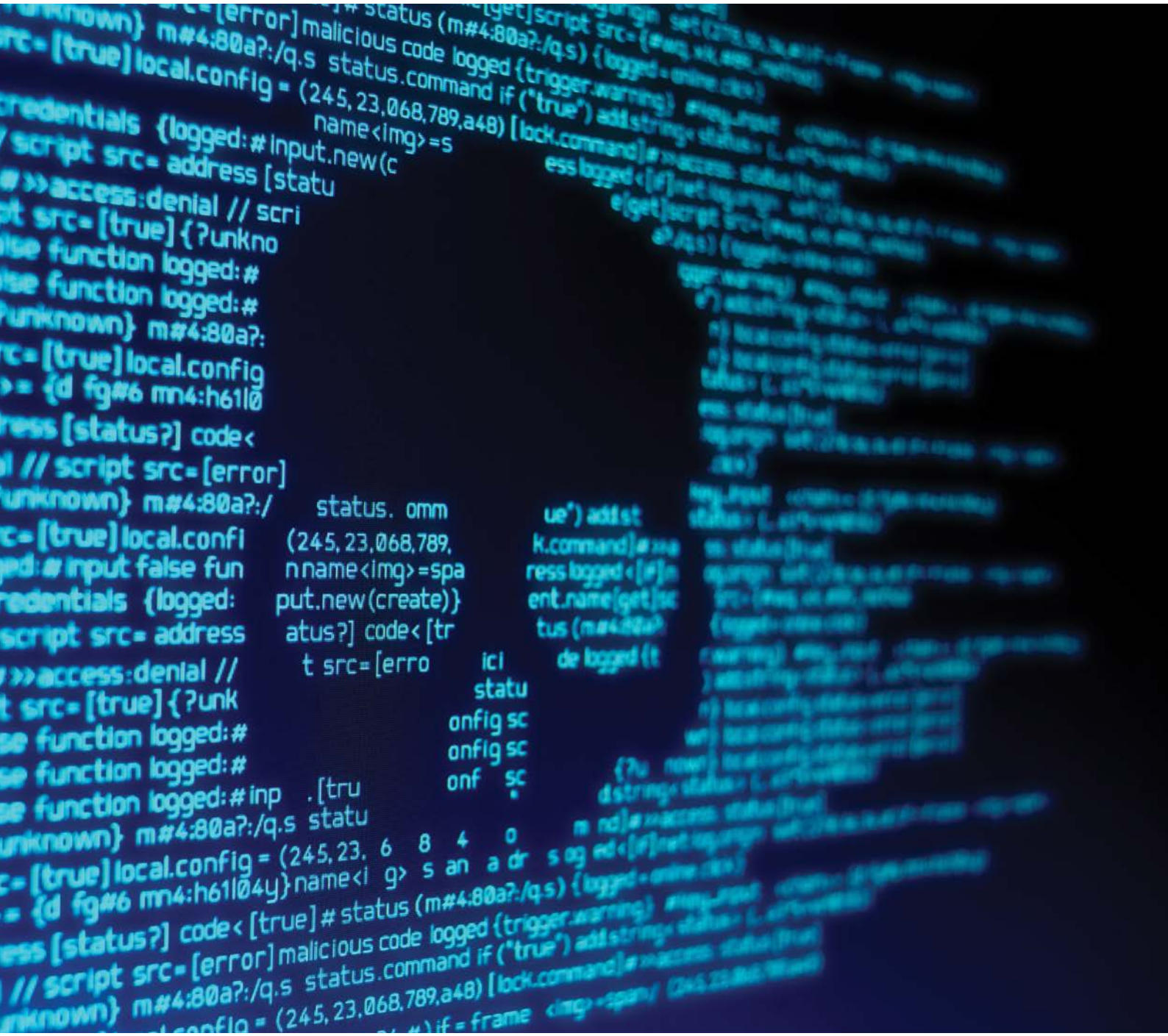


Sinistres Cybers :
les « ransomwares » perturbent l'activité

Les chiffres d'AIG en matière de sinistres cyber en 2017 traduisent la maturité croissante du portefeuille cyber ainsi qu'un environnement menaçant marqué, ces derniers mois, par une série d'attaques sophistiquées et systémiques, comprenant les programmes malveillants et *ransomwares* (logiciels de demandes de rançons) WannaCry et NotPetya. Alors que de nombreuses entreprises européennes ont été mises à mal par des interruptions d'activité ou de réseau, la majorité de celles-ci étaient sous assurées.

Comme l'avaient prédit les experts en sinistres cyber d'AIG, début 2016, les cas de cyber-extorsions et les interruptions d'activité après une attaque cyber se sont généralisés en 2017. Les chiffres d'AIG montrent que les *ransomwares* ont été la cause de plus d'un quart des sinistres cyber (26 %) déclarés en 2017. Une progression considérable par rapport aux 16 % des sinistres recensés entre 2013 et 2016.

« Le vol successif d'outils de la National Security Agency (NSA) et de ressources d'État a été le point de départ d'une menace systémique » explique Mark Camillo, Head of cyber for EMEA chez AIG. « L'attaque WannaCry qui a contaminé des centaines de milliers d'ordinateurs dans le monde aurait pu être pire si un chercheur britannique n'avait pas rapidement trouvé et activé le bouton d'arrêt d'urgence ».

Viennent ensuite comme causes de sinistres, les atteintes à la sécurité des données par des hackers, les autres failles de sécurité/accès non autorisés et les usurpations d'identité. Si le pourcentage de sinistres causés par la négligence d'employés a légèrement reculé à 7 % en 2017, l'erreur humaine reste un facteur important dans la plupart des sinistres cyber.

En résumé

- AIG a reçu en 2017 autant de déclarations de sinistres qu'au cours de ces quatre dernières années cumulées, soit l'équivalent d'un sinistre par jour ouvrable.
- Les cyber-extorsions par *ransomware* restent en tête des causes de sinistres cyber (la principale conséquence étant la parte d'exploitation), preuve que ce type d'attaques a une incidence accrue au niveau mondial.
- Les sinistres cyber touchent principalement les services professionnels, et financiers et le commerce de détail, mais les incidents se répandent plus largement dans tout un éventail de secteurs, signe qu'aucune activité n'est à l'abri.

Fig 1 **Sinistres cybers déclarés à AIG EMEA (2017) – Par catégories d'incidents déclarés**

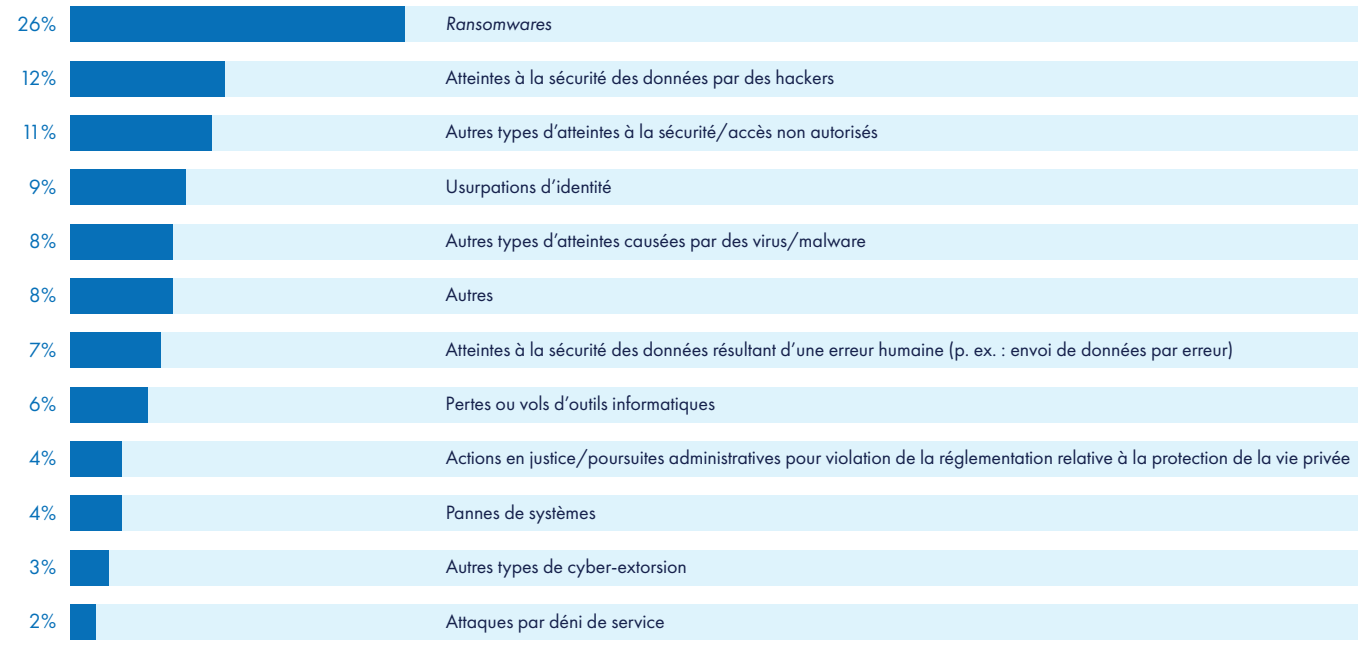
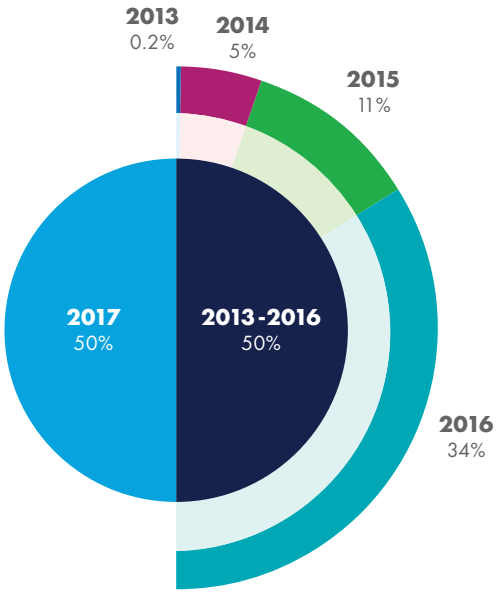


Fig 2 **Sinistres cybers déclarés à AIG EMEA (2013-2017) – En volume**

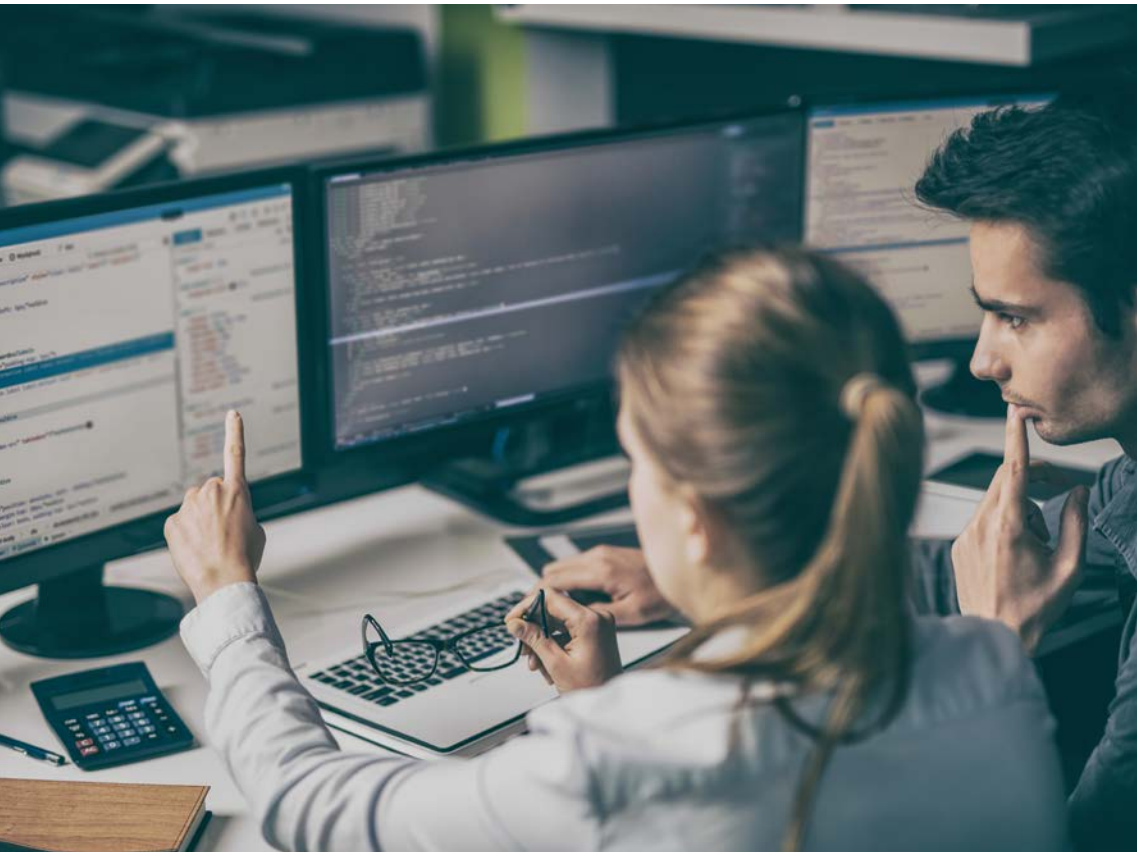


La fréquence des sinistres a encore augmenté l'année dernière. En 2017, les spécialistes en sinistres cyber chez AIG ont traité l'équivalent d'un sinistre par jour ouvrable. Cette augmentation traduit une tendance plus générale d'augmentation des pertes dues à une attaque cyber.

La couverture contre les risques cyber devenant un réflexe plus courant pour de nombreuses organisations, les acheteurs ont désormais une meilleure connaissance du produit. Ils perçoivent mieux l'étendue de la couverture et les incidents pouvant et devant être déclarés à leur assureur.

La souscription de produits d'assurances cyber a considérablement augmenté suite à la série d'attaques systémiques par *ransomwares* et déni de service distribué (DDoS). Un phénomène qui risque d'accroître encore la fréquence des sinistres. « Les acheteurs non traditionnels se montrent de plus en plus intéressés par les produits d'assurances cyber. Le nombre de sinistres devrait donc augmenter d'une année sur l'autre, simplement par la croissance du portefeuille », constate Mark Camillo.

« L'attaque WannaCry qui a contaminé des centaines de milliers d'ordinateurs dans le monde aurait pu être pire ». Mark Camillo

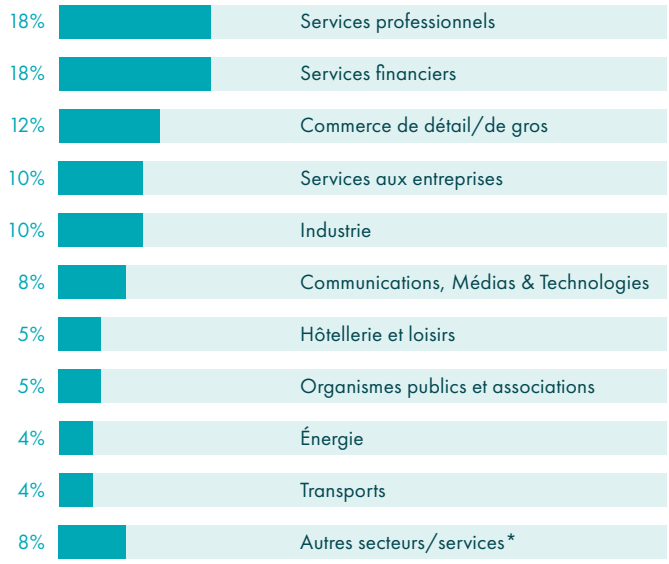


Tous les secteurs sont menacés

Les chiffres d'AIG indiquent qu'aucun secteur n'est à l'abri d'une attaque cyber. En 2017, des sinistres cybers ont été déclarés dans huit secteurs d'activité jusqu'alors jamais recensés par AIG dans ses statistiques sur ce type d'incidents. Une tendance qui se confirme, un nombre croissant de sinistres déclarés chaque année provenant d'un ensemble plus large de secteurs tels que l'énergie et les transports, en plus des secteurs traditionnellement exposés aux risques cyber.

Si les services financiers continuent de contribuer dans une large mesure aux sinistres déclarés, ils sont néanmoins en léger recul en 2017, à 18 % contre 23 % sur la période 2013-2016. La nature même de l'activité bancaire et assurantielle, le fait que les établissements financiers recueillent et conservent d'importants volumes de données et soient soumis à des réglementations strictes (et potentiellement à de lourdes amendes) expliquent que les services financiers ont toujours eu besoin d'une approche robuste face aux risques cyber.

Fig 3 **Sinistres cyber déclarés à AIG EMEA (2017) – Par secteur**



*Agroalimentaire, Construction, Immobilier, Agriculture, Services d'informations

Note: Les pourcentages ont été arrondis.

Néanmoins, le fléchissement du nombre de sinistres déclarés par des établissements financiers pourrait simplement refléter la croissance régulière des incidents déclarés par les autres secteurs, conséquence de maturité croissante du portefeuille cyber d'AIG dans la région EMEA. D'après Mark Camillo, « historiquement, les services financiers ont toujours figuré parmi les secteurs les plus importants d'AIG, mais, depuis l'année dernière, de nombreux autres secteurs souscrivent nos produits. Les incidents survenus durant l'été dernier ont été particulièrement déterminants ».

« Les récentes attaques par *ransomwares* ont, pour la plupart, touché indistinctement les secteurs d'activité », poursuit-il. « Il suffit que les utilisateurs d'un logiciel ciblé présentent une faille particulière pour être victimes à leur tour d'attaques à l'aveugle comme celles observées en 2017. Il faudra vérifier si le nombre d'attaques ciblées augmente en 2018, en particulier dans le contexte politique actuel favorable au cyber terrorisme étatique ».

Le nombre de sinistres a général a considérablement augmenté dans le secteur des services professionnels, à 18 % contre 6 % sur la période 2013-2016, tandis que les autres secteurs plus couramment associés aux sinistres cyber ont reculé dans le classement. « Les services professionnels deviennent davantage une cible en raison des données qu'ils détiennent », explique Kathy Avery, Financial lines major loss adjuster, chez AIG. « Les cabinets d'avocats et de comptables, avec des bases de données clients conséquentes, sont une une proie de choix pour les cyber-criminels attirés par la qualité des données qu'ils détiennent et leur vulnérabilité aux attaques cyber qui ciblent des transactions financières classiques ».

« Les dirigeants de ces cabinets pensent encore que cela n'arrive qu'aux autres ou qu'ils ne seront pas visés, jugeant leurs données sans intérêt. Et même si elle ne détient aucune donnée intéressante, n'importe quelle société peut toujours être victime d'extorsion par *ransomware*. Sans fichier accessible, aucune entreprise n'est en état de fonctionner », ajoute-t-elle.

« Les entreprises de services professionnels, parmi lesquelles les avocats et les comptables, deviennent davantage une cible en raison des données qu'ils détiennent ». Kathy Avery

Vers une banalisation des *ransomwares*

Les entreprises ont été visées par des attaques systémiques majeures dans plusieurs pays européens l'année dernière. WannaCry a exploité une vulnérabilité de Windows pour propager un programme malveillant à des centaines de milliers d'ordinateurs dans plus de 150 pays. Le virus a contaminé des entreprises dans de nombreux secteurs, dont la santé, les services financiers, la logistique, l'enseignement et l'industrie manufacturière.

Au cours des 24 derniers mois, les *ransomwares* se sont banalisés, les auteurs des variantes plus récentes proposant même à leurs « associés » des accords de partage de revenus. Rien ne garantit aux assurés qu'ils récupèreront leurs données, même en payant la rançon. Le « professionnalisme » des précédentes attaques par *ransomware* avec de véritables centres d'appels mis en place par les hackers enjoignant aux victimes d'accéder aux Bitcoins pour payer la rançon et restaurer les données compromises a presque disparu aujourd'hui.

Pour autant, les entreprises restent toujours menacées par le « Ransomware-as-a-Service ». Les entreprises ne pensent pas forcément que les données qu'elles détiennent sont importantes ou susceptibles d'être compromises. Toutefois, d'après les antécédents de sinistres en 2017, les attaques par ransomwares sont dans une large mesure lancées sans distinction et peuvent toucher des entreprises de tout secteur et de toute taille. AIG anticipe la tendance à l'automatisation et à la banalisation des ransomwares, qui devrait se confirmer, un nombre croissant d'attaquants s'en prenant aux entreprises comme aux particuliers.

Le « cryptojacking »[1]. devrait également gagner en importance. Courant 2017, le marché des cryptomonnaies a progressé de plus de 1 200 %[2]. Toutefois, les monnaies électroniques qui gagnent en valeur aiguisent l'appétit des cyber-criminels qui inondent les réseaux de programmes malveillants pour détourner de la cryptomonnaie.

Les formes plus traditionnelles d'extorsion devraient poser problème et être plus ciblées à l'avenir lors de violations de données. Une tendance déjà observée aux États-Unis, ce qui généré des pertes pour des entreprises européennes présentes sur le marché américain. Le règlement général européen sur la protection des données personnelles (RGPD) va certainement devenir un nouvel outil de pression pour les extorqueurs tentés de menacer les données d'une entreprise à moins de recevoir une rançon, en sachant que les conséquences seront plus importantes avec ce nouveau réglement.

Interruption des systèmes informatiques : une lourde peine

D'après les chiffres, les pertes d'exploitation suite à une attaque cyber, principale cause de sinistres, ont reculé en un an par rapport à la période 2013-2016, malgré les témoignages de nombreuses entreprises européennes en 2017 pour lesquelles les interruptions de réseaux ont été un problème majeur. Tandis que les interruptions de réseaux ont été l'une des multiples causes de sinistres, elles ne sont pas toujours citées comme cause principale et sont donc sous-représentées dans les statistiques des sinistres.

« Assez souvent, les assurés n'ont pas conscience, à la première alerte, de l'ampleur du problème qui les attend », explique Martin Overton, Cyber specialist EMEA chez AIG. « Ils pensent à un code malveillant ou à une tentative d'extorsion. Ce n'est qu'après avoir dépêché une équipe d'experts et après une analyse approfondie du problème, qu'ils comprennent que l'attaque va impacter leur activité, car ils sont privés d'accès à leurs données ou leur système n'est plus opérationnel ».

[1] https://www.forbes.com/sites/jasonbloomberg/2018/03/04/top-cyberthreat-of-2018-illicit-cryptomining/#48b90c4d5ae8

[2] https://www.forbes.com/sites/cbovaird/2017/11/17/why-the-crypto-market-has-appreciated-more-than-1200-this-year/#53e14c226eed

De nombreuses entreprises n'ont pas de couverture cyber pouvant les dédommager en cas d'interruption des systèmes informatiques. La plupart des attaques par *ransomwares* survenues l'année dernière se sont soldées notamment par des pertes d'exploitation au bilan (voir encadré).

Sur les sinistres déclarés en 2017, les pertes d'exploitation dues à une interruption de réseau ont été plus ou moins graves selon la durée de l'incident, la taille et le secteur de l'entreprise. En 2017, AIG Europe a ainsi indemnisé entre 3 250 et 5,2 millions USD de pertes d'exploitation suite à une interruption de réseau.

Les assurés sans protection efficace contre les attaques cyber et/ou sauvegardes de leurs données s'exposent au risque de subir une interruption de réseau suite à une attaque par *ransomwares*, indique José Martinez, Vice president of financial lines major loss claims EMEA chez AIG. « Les PME sont particulièrement vulnérables car leur système n'est pas aussi robuste et les sauvegardes ne sont pas régulières », explique-t-il.

« En règle générale, les entreprises possédant des sauvegardes ne sont pas disposées, dans la quasi-totalité des cas, à payer une rançon », poursuit-il. « Pour autant, l'année dernière, faute de sauvegardes de bonne qualité, un certain nombre d'entreprises se sont réellement trouvées en grand danger. Elles ont dû céder au chantage afin de récupérer leurs données ».

« Dans ce type de cas, plus le chantage dure, plus les pertes financières sont lourdes », ajoute-t-il. « Sans mesure commune avec les années précédentes, en 2017, nos assurés ont sollicité notre partenaire expert, KPMG, pour les aider à gérer des demandes de rançon, tenter de décrypter les données ou récupérer des sauvegardes antérieures. Outre l'assistance de nos experts, certains ont commencé à chercher à être dédommagés des pertes consécutives dues à l'impossibilité d'accéder à leurs systèmes et données, à l'obligation de renvoyer le personnel chez lui, etc. ».

« L'année dernière, faute de sauvegardes suffisantes, un certain nombre d'entreprises se sont réellement retrouvées en grand danger ». José Martinez

L'interruption des systèmes informatiques demeure sous-assurée

En 2017, la plupart des pertes d'exploitation provoquées par des logiciels de rançon qui codent les données et d'autres attaques qui déconnectent les systèmes n'étaient pas assurées. Les attaques par *ransomwares* qui ont fait la une des journaux n'étaient pas nécessairement motivées par l'appât du gain, mais par le désir de paralyser des services étatiques.

Ces attaques ont été d'une grande ampleur et auraient pu être bien pires si WannaCry n'avait pas été neutralisé. Alors que les paiements de rançons ont généré moins de 150 000 USD, le montant total des pertes économiques associées à WannaCry s'élèverait à 8 milliards USD[3], dont 500 millions en coûts directs et interruptions d'activité indirectes[4].

Avec la sophistication des programmes malveillants et des ransomwares, les interruptions d'activité devraient provoquer plus de dommages.
Pour autant, aussi graves que puissent être les conséquences pour les entreprises, l'interruption des systèmes informatiques ne suscite pas l'attention qu'elle mérite.

« Lorsque que je m'entretiens avec les assureurs ou les courtiers à ce sujet, les assurés ne semblent pas, la plupart du temps, particulièrement concernés par l'interruption des systèmes informatiques. Curieux alors que c'est le plus gros problème pour une majorité d'entreprises aujourd'hui », déclare Martin Overton, Cyber specialist EMEA chez AIG.

[3] https://uk.reuters.com/article/uk-cyber-lloyds-report/global-cyber-attack-could-spur-53-billion-in-losses-lloyds-of-london-idUKKBN1A20AH

[4] https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/risk/downloads/crs-cyber-risk-outlook-2018.pdf

La RGPD en tête des tendances liées aux violations de données

Avec l'entrée en vigueur du RGPD, le 25 mai 2018, le nombre de sinistres liés aux violations de données et autres failles de sécurité devrait bondir. Les entreprises seront plus enclines à signaler les failles informatiques, avec comme impact une hausse des sinistres cyber identique à celle ayant suivi l'entrée en vigueur aux États-Unis des lois fédérales sur la notification de violations de données.

« Il est conseillé à un grand nombre de petits assurés de signaler une violation alors que rien ne les y oblige en vertu du droit actuel », observe Kathy Avery. « Avec l'entrée en vigueur de la RGPD en mai, la notification ne sera plus une option. Nous anticipons une augmentation des déclarations après cette date ».

Les données personnelles ne sont plus perçues de la même manière depuis la révélation du scandale qui éclabousse Cambridge Analytica et Facebook, constate-t-elle, avec des incidences au niveau des sinistres qui seront déclarés en 2018, les consommateurs tolérant de moins en moins la violation de leurs données personnelles.

« Nous avons dernièrement traité un sinistre après l'attaque d'une université », explique-t-elle. « L'université a notifié les personnes concernées comme si le règlement RGPD était déjà en vigueur. L'incident s'est avéré relativement coûteux et difficile à gérer en termes d'image. Notifier 100 000 personnes n'est pas une mince affaire. Imaginez la contrariété que ce type de courrier peut provoquer, alors que vous pensez être prudent ».

L'issue du recours collectif déposé à l'encontre du géant des chaînes de supermarchés, Morrisons, au Royaume-Uni, par ses employés aura valeur de test quant aux dédommagements que pourraient imposer les tribunaux pour les personnes dont les données ont été compromises. Les employés demandent à être dédommagés de la « contrariété et du désarroi » provoqués par le vol de données personnelles de près de 100 000 d'entre eux en 2015.

L'introduction du RGPD pourrait inciter davantage d'actionnaires à poursuivre leurs entreprises et leurs dirigeants à l'avenir. Depuis plusieurs années, les États-Unis imposent des exigences strictes en matière de notification, et presque toutes les fuites de données de grande ampleur donnent au moins lieu à un recours collectif en justice.

Si un tel niveau de procédures et de mécanismes de recours collectifs n'existe pas encore en Europe, le verdict dans l'affaire Morrisons pourrait faire jurisprudence. « Si, dans l'affaire Morrisons, des dommages et intérêts sont ordonnés sur la base de la détresse émotionnelle provoquée par la perte de données, les conséquences pourraient être considérables et créer un précédent intéressant », affirme Mark Camillo. « Les recours de ce type pourraient se multiplier à l'encontre des entreprises qui auront informé le public d'une fuite de données ».

[5] https://www.independent.co.uk/news/business/news/morrisons-data-leak-staff-payout-details-sensitive-data-personal-online-hack-a8086521.html

« La plupart des assurances responsabilité des dirigeants n'intègreront aucune exclusion en cas de poursuites intentées par les actionnaires suite à un piratage de données informatique. Ces polices d'assurance vont donc pouvoir fonctionner dans le cadre ce type de sinistres », poursuit-il.

Le RGPD prévoit deux types d'amendes à l'encontre des entreprises n'ayant pas mis en place les systèmes et les mesures de sécurité nécessaires pour protéger les données de tiers. La première va jusqu'à 10 millions d'euros, ou 2 % du chiffre d'affaires annuel de l'année précédente, le montant le plus élevé s'appliquant. La seconde va jusqu'à 20 millions d'euros, ou 4 % du chiffre d'affaires annuel de l'année précédente, le montant le plus élevé s'appliquant.

« L'année 2018 nous en dira plus long sur l'assurabilité de ces amendes et ces sanctions », indique Mark Camillo. « Certains pays européens l'interdisent, mais d'autres, comme le Royaume-Uni, restent évasifs. Le gouvernement a suggéré que les assureurs pourraient éventuellement couvrir davantage d'amendes ou de sanctions administratives ».

« Nous savons que des armées de botnets sont en préparation sans aucun signe d'accalmie à l'horizon ». Martin Overton

Les entreprises négligent de se protéger contre les attaques DDoS

Deux ans après l'attaque du botnet Mirai qui a terrassé Dyn, fournisseur de serveurs DSN, les vulnérabilités aux attaques DDoS sont toujours une menace, et les entreprises ne protègent pas suffisamment leurs réseaux contre ce type d'attaques.

Reaper est la toute dernière version de ces programmes malveillants. Comme Mirai, il se compose d'un grand nombre d'appareils domestiques non sécurisés qui forment l'Internet des objets (IoT), comme les routeurs domestiques, les caméras IP et les babyphones.

« Le botnet Reaper est principalement composé d'objets connectés pouvant potentiellement générer 1,6 térabits par seconde, soit un volume phénoménal de données », observe Martin Overton. « Nous savons que des armées de botnets sont en préparation sans aucun signe d'accalmie à l'horizon. Or, un grand nombre d'entreprises n'adoptent pas les défenses nécessaires ».

Si des solutions garantissant le fonctionnement des systèmes en cas d'attaques sont aujourd'hui disponibles sur le marché, les entreprises ne prennent pas les dispositions nécessaires pour se protéger contre les DDoS, et les PME sont vraisemblablement dissuadées par les coûts d'une telle protection.

Conclusion : l'heure du cyber-check-up ?

Les lourdes conséquences financières liées aux interruptions d'activité/de réseau vont continuer à se faire sentir en 2018, stimulant la demande en couvertures et la croissance continue du marché de l'assurance cyber en Europe. L'activité s'intensifiant, les sinistres devraient augmenter en termes de fréquence, mais aussi en termes de gravité.

Banalisation des *ransomwares*, hausse attendue des sinistres liées aux violations de données dans le courant de l'année en raison de l'application du RGPD et ascendant des pouvoirs publics dans un contexte de fragilité accrue et d'incertitude politique vont encore peser sur les tendances au cours des 12 prochains mois. La cyber-extorsion traditionnelle et l'usurpation d'identité sont certainement à surveiller, et les employés restent la première ligne de défense contre ces attaques.

Quel que soient leur taille ou leur secteur, les entreprises évoluant dans un monde interconnecté et de plus en plus numérisé n'ont jamais été plus vulnérables aux attaques et à leurs conséquences financières potentiellement catastrophiques. Selon AIG, les attaques systémiques par *ransomwares* observées en 2017 ne sont que la partie émergée de l'iceberg, et des difficultés plus grandes encore sont à craindre à l'avenir.

S'il vaut mieux prévenir que guérir, les entreprises doivent se préparer à l'inévitable : leurs systèmes et leurs réseaux seront, à un moment ou à un autre, attaqués. Les entreprises cyber-résistantes sont prêtes et s'entrainent à réagir. Ce sont celles qui ont mis en place une solide stratégie de prévention du risque cyber et s'assurent d'être dédommagées de tous les risques cyber possibles, y compris l'interruption de réseau.

Principaux risques cyber pour les entreprises

D'après notre expérience en gestion des sinistres, les premiers risques cyber auxquels les entreprises s'exposent en termes de faille de sécurité sont les suivants :

- **Des serveurs externes accessibles à distance avec des mots de passe faiblement sécurisés.** Ces failles permettent aux programmes malveillants et autres logiciels de rançon de s'introduire dans le système. Les accès à distance devraient faire l'objet d'un contrôle plus rigoureux.
- **Des utilisateurs pas assez sensibilisés permettant le piratage par phishing de mots de passe.** L'utilisateur ouvre la pièce jointe d'un email de hameçonnage et est renvoyé vers une page de connexion factice où sont détournés ses identifiants pour permettre aux hackers d'accéder à son compte. L'utilisateur devrait toujours se demander s'il fait confiance à l'expéditeur d'un email. Toute demande d'identifiants de connexion doit alerter l'utilisateur d'une tentative de phishing.
- **La faiblesse des protocoles de connexion.** Le risque de phishing est éliminé avec l'activation de deux facteurs d'authentification, en exigeant un second code de connexion au compte. Les dirigeants et associés de l'entreprise ainsi que les employés intervenant dans les opérations de paiement devraient au minimum adopter ce principe.

Exemples de sinistres

Une entreprise de fabrication touchée par une interruption d'activité après une attaque par *ransomware*

L'assuré conçoit et fabrique des grues, des pelleteuses et des équipements de levage de charges lourdes et spécialisés.

Le 1er décembre, l'assuré découvre qu'il a été victime d'une attaque par *ransomware*. Jusqu'à 85 % de ses dossiers et documents ont été cryptés. L'assuré contacte la ligne d'assistance CyberEdge d'AIG et bénéficie des services d'intervention d'urgence d'experts informatiques. Suivant les conseils de cette société, l'assuré a décidé de restaurer ses données grâce aux sauvegardes. La restauration s'est achevée le 3 décembre.

Suite à la panne du système informatique, les employés de différents services n'ont pas pu travailler les 1er et 2 décembre faute de pouvoir accéder au serveur. L'assuré emploie aujourd'hui près de 300 ingénieurs et personnels de production. Sa principale activité consiste à gérer des projets clé en main ou des projets de génie civil dans lesquels l'outil informatique est essentiel pour la conduite des travaux.

L'équipe d'ingénieurs sauvegarde les données sur le serveur de l'entreprise afin de pouvoir les partager à l'ensemble des employés. Le personnel ingénieur facture directement le nombre d'heures travaillées sur un projet donné. L'incapacité de travailler durant ces deux jours s'est donc répercutée sur le nombre d'heures que l'entreprise pouvait facturer. Il a été difficile de récupérer ces heures à un stade ultérieur compte tenu des délais à tenir sur les divers projets de l'assuré, un non-respect des dates de livraison autorisant les clients à invoquer des pénalités contractuelles.

Les frais additionnels du personnel ingénieur ont été pris en charge afin de garantir la continuité de l'activité et l'achèvement des projets dans les délais.

Un établissement financier menacé par une attaque DDoS et une tentative d'extorsion

L'assuré a reçu un email de demande de rançon exigeant le paiement d'un bitcoin pour éviter une attaque par DDoS. Si l'assuré refusait de payer la rançon, les hackers l'ont également menacé d'augmenter le montant à dix bitcoins.

Avec l'aide d'AIG, l'assuré a engagé un prestataire spécialisé dans la protection contre les DDoS afin d'atténuer les conséquences d'une attaque et a informé son fournisseur de services Internet d'une possible attaque, au lieu de chercher à gérer la situation seul avec des ressources inadaptées comme les pare-feu.

Après enquête, les supposés hackers auraient opéré depuis la Lettonie. Ils se sont réclamés du groupe « XMR Squad » connu pour avoir lancé des attaques DDoS contre plusieurs entreprises les semaines précédentes, donnant ainsi du crédit à la menace. Néanmoins, d'après les renseignements reçus de la Bank of England, l'email proviendrait a priori d'un copycat et non de l'organisation officielle.

Rien ne permettait de confirmer que le supposé attaquant ait obtenu l'accès aux données personnelles sous le contrôle de l'assuré. Finalement, la menace n'a pas été mise à exécution, et ni la confidentialité, l'intégrité ou la disponibilité des données de l'assuré n'ont été compromises.

Le site Web et la plateforme numérique de l'assuré sont restés en ligne et opérationnels, avec toutefois la mise en place d'une surveillance et d'une analyse du trafic renforcées et continues. L'établissement financier n'a subi aucune perte financière sérieuse excepté les frais du consultant tiers et des autres intervenants en gestion de crise en rapport avec l'incident, et le temps considérable passé à enquêter et à régler l'incident. AIG a pris en charge les frais d'intervention d'urgence.

Une entreprise du secteur du luxe ciblée par une attaque de phishing

L'entreprise assurée a été victime d'une escroquerie au phishing au moyen d'un email ayant d'abord ciblé ses employés puis ses clients.

Les premières vérifications ont révélé qu'un employé avait suivi un lien dans un email frauduleux neuf mois avant que l'assuré ne s'aperçoive de l'incident, ayant ainsi permis aux malfaiteurs d'accéder à sa boîte de messagerie. Les boîtes de réception d'au moins deux autres employés ont été infiltrées selon le même procédé. Les malfaiteurs auraient obtenu les coordonnées de clients en accédant à ces trois boîtes de réception.

Par la suite, en l'espace de 12 mois, et à une fréquence croissante, l'assuré a reçu des plaintes de clients trompés par des emails supposés venir de l'assuré alors qu'ils étaient en réalité envoyés par les fraudeurs. Ces emails, à l'instar de ceux reçus initialement par les trois employés, invitaient les clients à suivre un faux lien leur demandant leurs identifiants de connexion, leur numéro de carte de crédit et d'autres informations personnelles, soi-disant pour aider l'assuré dans sa démarche visant à mieux « connaître le client ».

Plusieurs clients ayant signalé l'email frauduleux figuraient dans un tableur archivé dans la boîte de réception de l'un des employés. Ce tableau contenait une liste centrale de clients avec près de 21 000 adresses email.

Les experts informatiques engagés sur les conseils d'AIG ont bloqué l'accès à l'URL suspecte et ont passé au crible les boîtes de réception infectées pour identifier les données détournées. Après une analyse minutieuse des données, le méfait a été réduit à moins de 1 000 fichiers de données. Grâce à cette intervention, l'assuré a pu adresser une réponse personnelle aux clients affectés, parmi lesquels beaucoup de grandes fortunes.

LE SINISTRE, NOTRE PRIORITÉ

Méthodologie

En mars 2018, AIG Europe a analysé plus de 600 sinistres cyber déclarés dans le cadre de ses polices d'assurance cyber entre 2013 et décembre 2017.

www.aig.com

Sophie Parisot
Souscripteur Responsabilité Civile et Cyber
Responsable Produit Cyber
sophie.parisot@aig.com

Laurence Raguideau
Responsable Unité de Souscription Transactionnelle
RC Professionnelle / Cyber
laurence.raguideau@aig.com

Pour toute question concernant la couverture CyberEdge, il convient de demander un exemplaire de la police pour une présentation des conditions d'application et des limites de garantie.

American International Group, Inc. (AIG) est l'un des leaders mondiaux de l'assurance. Fondée en 1919, AIG offre aujourd'hui un large choix de solutions d'assurance dommages et responsabilité, d'assurance-vie et de retraite, ainsi que d'autres services financiers dans plus de 80 pays et territoires. Ces divers produits et services aident les entreprises et les particuliers à protéger leur patrimoine, à gérer les risques et à s'assurer des revenus de retraite. AIG est cotée à la bourse de New York et à la bourse de Tokyo. Pour en savoir plus sur AIG, rendez-vous sur www.aig.com et www.aig.com/strategyupdate | YouTube: www.youtube.com/aig | Twitter: @AIGinsurance | LinkedIn: www.linkedin.com/company/aig.

AIG est le nom commercial du réseau mondial d'assurances dommages et responsabilité, d'assurances de personnes et d'assurances vie-retraite-prévoyance d'American International Group Inc. Pour obtenir des informations complémentaires, veuillez consulter notre site internet www.aig.com. Nos produits et services sont fournis par des filiales ou des entités affiliées d'American International Group, Inc. et peuvent ne pas être disponibles dans tous les pays. L'étendue et les conditions d'application des garanties sont assujetties aux dispositions du contrat d'assurance. Certains produits ou services hors assurance peuvent être fournis par des tiers indépendants.

AIG Europe Limited est une société de droit anglais (numéro d'immatriculation : 1486260), dont le siège social est sis : The AIG Building, 58 Fenchurch Street, London, EC3M 4AB. AIG Europe Limited est agréée par la Prudential Regulation Authority et est régie par la Financial Conduct Authority et la Prudential Regulation Authority (numéro FRN 202628). Ces informations peuvent être vérifiées auprès de la FCA (www.fca.gov.uk/register).

FL00002800 06/18 - FRDMC 008.Cyber claims.0618