AIG

Expertise sinistres AIG

Assurance Cyber : analyse des principales tendances

Les statistiques d'AIG EMEA (Europe, Moyen-Orient & Afrique) révèlent que les sinistres liés à la cyber-extorsion représentent la majorité des sinistres cyber et ce, quelle que soit la taille de l'organisation. Les interruptions de réseaux et les atteintes à la sécurité des données constituent les sinistres ayant les conséquences financières les plus importantes.

Les atteintes majeures à la sécurité des données et les attaques complexes par déni de service distribué (DDoS) via les objets connectés font les gros titres de l'actualité. Pourtant, les cas de cyber-extorsion et d'utilisation de ransomware augmentent de plus en plus, comme le montrent les chiffres d'AIG EMEA sur les cyber-risques de 2013 à septembre 2016.

Les cas d'extorsion par ransomware représentent 16 % des sinistres cyber déclarés sur la période, auxquels viennent s'ajouter les autres types de cyber-extorsion (4 %). L'année 2016 en particulier a été marquée par une multiplication des actes de cyber-extorsion. « Au cours des neuf premiers mois de l'année, beaucoup d'entreprises ont déclaré avoir été victimes d'attaques par ransomware, impliquant une tentative d'extorsion dans la quasi-totalité des cas, » déclare Kathy Avery, Financial Lines Major Loss Adjuster. « De nombreuses TPE-PME ont été touchées. »

Sinistres cyber déclarés à AIG EMEA (2013-2016) – par type

16%	Extorsion par logiciel de cryptage de type ransomware
14%	Atteintes à la sécurité des données par des hackers
10%	Autres types d'atteintes à la sécurité/accès non autorisés
10%	Autres types d'atteintes causées par des virus/malware
8%	Atteintes à la sécurité des données résultant de la négligence d'un salarié (p. ex. : envoi de données par erreur)
7%	Usurpations d'identité
6%	Attaques par déni de service
6%	Perte ou vol d'outils informatiques (p. ex. : perte d'ordinateur portable)
4%	Autres types de cyber-extorsion
4%	Actions en justice/poursuites administratives pour violation de la réglementation relative à la protection de la vie privée
4%	Panne de système
4%	Interruption d'activité
9%	Autre

Kathy Avery prend l'exemple d'une entreprise de vente en ligne d'articles de jardinage dont les dirigeants se sont rendus compte qu'un ransomware avait été introduit dans leur système et cryptait l'ensemble de leurs données. La PME n'avait que peu de données sensibles susceptibles d'être compromises, mais cette attaque l'empêchait de contacter ses clients et d'accéder à ses factures. Elle a donc décidé de verser la rançon demandée afin de pouvoir débloquer ses fichiers, et l'expert informatique d'AIG lui a apporté un appui durant tout le processus, en supervisant l'utilisation de la clé de décryptage.

Les cas d'extorsion et les attaques par déni de service (DoS) ou déni de service distribué (DDoS) peuvent se recouper. Ceux-ci impliquent fréquemment une tentative d'extorsion. Au cours des trois dernières années, 6 % des sinistres cyber déclarés à AIG EMEA ont été classés dans la catégorie des attaques par déni de service. « Certaines attaques par déni de service pourraient également être considérées comme des cas de cyber-extorsion, » précise Madame Avery. « Dans certains cas, les auteurs de ces attaques procèdent par injection SQL. Ils peuvent extraire des données et menacer de les publier si l'entreprise ne verse pas la rançon demandée. »

Malgré le développement de l'assurance cyber et, de ce fait, l'augmentation des déclarations des cas de cyber-extorsion, on pense que nombre d'entreprises ne signalent pas les rançons qu'elles ont eues à verser. « Les rançons sont généralement payées en Bitcoin. Dans certains cas, l'entreprise, de par son manque d'expérience, peut être victime d'une autre attaque alors qu'elle pense être en train de décrypter ses fichiers, » prévient Madame Avery. « Certaines personnes s'étonnent parfois du faible montant des rançons demandées. »

Pourtant, compte tenu de la fréquence de ces attaques, l'extorsion est un moyen lucratif et relativement simple d'obtenir rapidement de l'argent. Une étude réalisée par la Cyber Threat Alliance laisse apparaître que les auteurs de ce type d'attaques seraient parvenus à soutirer environ 325 millions de dollars à leurs victimes au cours des trois dernières années, grâce au code CryptoWall. Le gang Cryptolocker, quant à lui, aurait réussi à extorquer plus de 30 millions d'euros en 2015, au moyen d'un ransomware plutôt basique.

MacAfee Labs, craignant que certains secteurs d'activités, tels que les services financiers et les collectivités locales, ne deviennent la cible des cybercriminels, a placé les ransomware en tête de sa liste des principales menaces en 2016. Les hôpitaux et cabinets médicaux sont également une cible privilégiée des cyber-criminels. « Dans les établissements de soins, les logiciels de cryptage de type « ransomware » peuvent avoir des effets immédiats sur les soins prodigués aux patients et entraîner une violation de l'obligation de confidentialité incombant à l'établissement, ce qui rend ce secteur particulièrement vulnérable à ce type d'attaques » explique David Ferbrache, directeur technique chez KPMG.

« Au cours des deux premiers mois de l'année, nous avons constaté une évolution importante et une multiplication des types de ransomware, avec l'émergence de familles et d'outils différents, ce qui laisse supposer que ce type d'attaque est devenu un véritable "business model", » poursuit-il. « Ce type d'outil s'est généralisé, et certains signes nous laissent penser que les groupes qui les utilisent se professionnalisent. »

Dans les cas de cyber-extorsion, la gravité du sinistre dépend du type d'organisation, de l'ampleur de l'interruption d'activité et de la nécessité de procéder à une enquête judiciaire et de mettre en œuvre des mesures de restauration des systèmes a posteriori. Les rançons demandées demeurent généralement peu élevées. Dans les cas d'attaque par déni de service ou par déni de service distribué, les coûts associés à la mise hors service des sites Web peuvent être particulièrement élevés, comme ce fut notamment le cas pour l'e-commerçant cité dans l'exemple ci-après.

« Les attaques par déni de service se sont également largement répandues, » explique Monsieur Ferbrache. « Il n'en coûte que 5 ou 10 dollars de l'heure aux cyber-criminels pour mettre en place une attaque par déni de service capable de perturber un site Web ouvert au public et générer un trafic important. »

« Mais ce sont surtout les attaques par déni de service distribué qui inquiètent en ce moment, » poursuit-il. « On voit désormais apparaître des réseaux d'objets connectés zombies : des enregistreurs numériques, des caméras de surveillance, ou encore des routeurs installés chez des particuliers, qui sont infectés et causent des perturbations particulièrement importantes. »

Les cyber-criminels auraient généré 325 millions de dollars de revenus au cours des trois dernières années grâce au code CryptoWall.

En octobre 2016, une attaque par déni de service distribué de grande ampleur a touché les serveurs de l'entreprise Dyn, fournisseur de DNS, entraînant des perturbations généralisées. Cette attaque a été menée au moyen d'un réseau de machines zombies constitué de plusieurs dizaines de millions d'objets connectés infectés par le malware Mirai, y compris des caméras de surveillance, des webcams, des thermostats intelligents, et même des écoute-bébés. Le nombre d'attaques de ce type augmente, au rythme de 138 % par an selon le dernier rapport d'Akamai, intitulé « State of the Internet/Security Report ».

Pour les entreprises touchées par une attaque par ransomware ou par déni de service, les pertes d'exploitation sont particulièrement élevées pendant les pics d'activité. La moitié des entreprises récemment interrogées dans le cadre d'une enquête ont admis qu'elles pourraient perdre plus de 100 000 USD par heure au cours des périodes les plus critiques. « Je me souviens d'une entreprise pour laquelle la rançon demandée s'élevait à 262 livres sterling, mais dont la perte d'exploitation causée par l'attaque se chiffrait en millions, » explique Stephen Tester, associé chez CMS Cameron McKenna. « Les cyber-criminels ont empêché l'accès à un site Web pendant un week-end entier. »

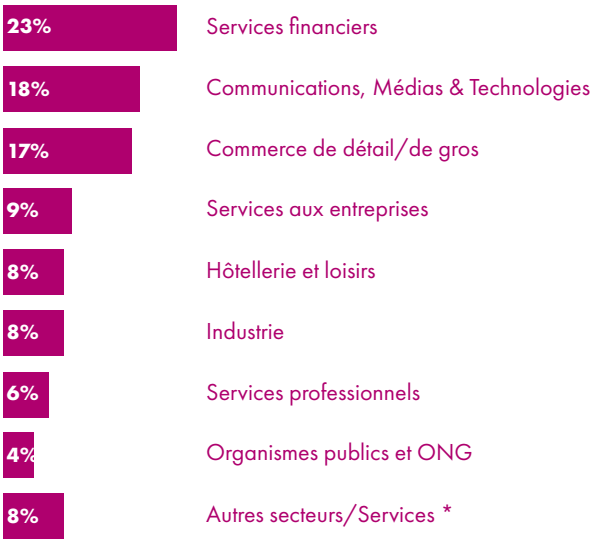
Si les pertes d'exploitation représentent actuellement seulement 4 % des sinistres cyber déclarés à AIG EMEA (auxquels viennent s'ajouter 4 % supplémentaires correspondant aux sinistres résultant d'une défaillance ou d'une panne de système), elles devraient gagner en ampleur et en fréquence à l'avenir. Une réaction rapide en cas d'attaque permet d'atténuer son impact potentiel.

La réglementation, un facteur déterminant

Les atteintes à la sécurité des données enregistrées par AIG EMEA se divisent en deux catégories distinctes : celles qui sont causées par des hackers et celles qui résultent de fautes commises par des employés. Ensemble, elles représentent plus d'un cinquième des sinistres cyber (22 %) déclarés au cours des trois dernières années (voir p. 2). Le coût croissant des atteintes à la sécurité des données, les atteintes associées à la réputation et l'augmentation des obligations déclaratives devraient peser sur la fréquence et la gravité de ces sinistres.

Il n'est peut-être pas étonnant de constater que la majorité des sinistres cyber sont déclarés par des entreprises soumises à l'obligation d'informer leurs clients en cas d'atteinte à la sécurité de leurs données sensibles. Ainsi, les entreprises du secteur des services financiers sont à l'origine de près du quart des déclarations de sinistres cyber reçues par AIG EMEA au cours des trois dernières années. Suivent les entreprises du secteur de la communication, des médias et des technologies(18%), comprenant notamment les entreprises de télécommunications.

Sinistres cyber déclarés à AIG EMEA (2013-2016) - Par secteur



*Construction, agroalimentaire, services d'information, autres services, transport, agriculture et pêche, énergie et immobilier

Remarque : les chiffres ayant été arrondis, leur somme peut ne pas correspondre à 100%.

En vertu du règlement général sur la protection des données, les entreprises basées dans l'UE et les entreprises basées hors de l'UE qui traitent des données émanant de ressortissants de l'UE devront notifier toute atteinte à la sécurité des données dans les 72 heures suivant leur survenance - dans la mesure du possible. Les entreprises qui ne mettent pas en œuvre des moyens de protection des données suffisants se verront imposer des amendes significatives. Une entreprise peut être condamnée à verser jusqu'à 2 % de son chiffre d'affaires annuel si ses archives ne sont pas en ordre, ou si elle s'abstient d'informer les autorités compétentes de toute atteinte à la sécurité de ses données ou de réaliser des évaluations d'impact. Dans certains cas les plus graves, l'amende peut aller jusqu'à 4 % du chiffre d'affaires.

Sinistres cyber déclarés à AIG EMEA (2013-2016) - Volume

Les nouvelles règles sur la protection des données et la médiatisation de certaines affaires continueront à nourrir la demande en matière d'assurance cyber, ce qui contribuera par la suite à la hausse du nombre de déclarations de sinistres. José Martínez, VP Financial Lines Major Loss Claims, observe que le nombre de déclarations de sinistres cyber en vertu de contrats d'assurance dédiés est passé de deux en 2013 à 170 en 2016.

Le coût total moyen d'une atteinte à la sécurité des données s'élève désormais à 4 millions de dollars, soit une hausse de 29 % depuis 2013, selon une étude menée par Ponemon et IBM. Malgré cette augmentation, une réaction rapide et professionnelle peut contribuer à atténuer la gravité de certains sinistres, explique Madame Avery. « Tel qu'il est conçu, le contrat nous permet de contenir un nombre important d'incidents dans les premières 48 heures. »

« Avec l'arrivée des nouvelles réglementations européennes sur la protection des données, les amendes devraient être moins importantes si l'entreprise peut apporter la preuve qu'elle a correctement géré la situation et qu'elle a mis des systèmes efficaces en place, » ajoute-t-elle.

Globalement, le coût total moyen d'une atteinte à la sécurité des données s'élève désormais à 4 millions de dollars, soit une augmentation de 29 % depuis 2013

Très souvent, les sinistres cyber ont une dimension humaine, résultant d'une simple erreur ou d'agissements délibérés d'un employé ou d'un ancien employé mécontent. Le risque de phishing ou d'envoi de données par erreur peut être réduit grâce à des formations et à la mise en place de contrôles et de systèmes efficaces. La perte et le vol d'ordinateurs portables, de clés USB ou de disques durs représentent 6 % des sinistres cyber déclarés à AIG EMEA entre 2013 et 2016.

Certaines faiblesses, comme les erreurs humaines et/ou une bonne connaissance des rouages internes de l'organisation, sont souvent exploitées dans le cadre des « arnaques du vendredi après-midi », qui ciblent fréquemment les cabinets d'avocats et sont bien souvent découvertes le lundi suivant. Les criminels trouvent chaque jour des moyens plus complexes pour convaincre les entreprises de leur communiquer certaines données sensibles, en utilisant notamment des informations relatives à des opérations authentiques pour se donner une apparente légitimité.

Dans le cas de l'arnaque au faux président, un collaborateur, travaillant généralement au service comptabilité, est contacté, le plus souvent par téléphone et par e-mail, par une personne se présentant comme un cadre dirigeant de l'entreprise et lui demandant de procéder à un paiement urgent. Les pertes résultant de la compromission d'une adresse e-mail professionnelle (« business email compromise » aux États-Unis), ont explosé de 1 300 % selon l'Internet Crime Complaint Center du FBI, pour atteindre 3,1 milliards de dollars en mai 2016.

« Ce n'est que la partie émergée de l'iceberg, car ces données correspondent uniquement aux cas survenus aux États-Unis et à certains cas survenus ailleurs et déclarés au FBI, » juge Monsieur Ferbrache, de KPMG. « Le problème est majeur. Parfois, les auteurs de ces escroqueries peuvent commencer par s'attaquer à un cabinet d'avocats ou d'experts-comptables, qu'ils utilisent ensuite pour envoyer des e-mails frauduleux et attaquer l'organisation visée. »

« Le montant moyen de ce type d'escroquerie s'élève à l'heure actuelle à 160 000 dollars, » ajoute-t-il. « Et pour le cas le plus important signalé en Europe, il s'est élevé à 40 millions d'euros. Mais je ne saurais dire s'il s'agit de cyber-crimes ou de simples cas d'abus de confiance particulièrement bien organisés. »

En pratique : études de cas

Les cas cités ci-après, tous réels, illustrent bien l'étendue des sinistres couverts par la garantie CyberEdge® d'AIG. Ils montrent également que personne n'est à l'abri et que le problème concerne toutes les entreprises, quelle que soit leur taille.

Attaque par ransomware visant une entreprise de broderie en ligne

En 2015, peu avant Noël, une entreprise de broderie en ligne basée au Royaume-Uni a subi une attaque par ransomware. L'auteur de cette attaque a créé deux comptes utilisateurs et a tenté de crypter et de supprimer les données clients de l'entreprise, ainsi que d'autres informations concernant ses commandes, ses stocks et ses comptes. Il a ensuite envoyé une demande de rançon dans laquelle il donnait pour instruction à l'assuré d'envoyer un message à l'adresse e-mail communiquée.

L'auteur de l'attaque n'est pas parvenu à crypter les données, mais il a réussi à supprimer de nombreux fichiers et à déplacer certaines données. Ne pouvant plus se fier aux données déplacées, l'assuré se trouvait dans l'incapacité d'exercer son activité via le système. La dernière sauvegarde de données datait de quatre jours avant l'incident, de sorte que l'ensemble des données de la semaine précédente étaient également perdues.

Suite à cette attaque, l'assuré a reçu les conseils d'experts juridiques et informatiques. Les données de tiers ne semblaient pas avoir été compromises. Il fut donc conseillé à l'assuré de ne pas déclarer l'incident aux autorités en charge de la protection des données.

Les consultants informatiques de l'assuré lui ont proposé des solutions pour atténuer les conséquences de l'incident et l'ont conseillé sur les précautions à prendre pour éviter qu'il se reproduise. Ils lui ont notamment conseillé de sauvegarder les données contenues dans le serveur touché afin de déterminer l'origine de l'incident et de revoir son plan de reprise d'activité après sinistre.

Cryptage de fichiers contenus sur le serveur interne d'un intermédiaire en assurance

L'un des ordinateurs de l'assuré a été contaminé par le malware CryptoWall, qui a crypté certains fichiers qui y étaient stockés ainsi que le serveur interne. Les fichiers ont été renommés « help_your_files.png » et une rançon a été demandée en échange de l'accès aux données.

L'assuré, basé au Royaume-Uni, pensait que les fichiers cryptés contenaient certaines données clients, comme des noms et des adresses, mais pas d'autres données à caractère personnel ni d'informations financières. Aucune preuve ne laissait suggérer que les données contenues dans les fichiers cryptés avaient été consultées ou exportées, ou que des données avaient pu être perdues, en raison des sauvegardes régulières prévues par le système informatique de l'assuré.

L'assuré a reçu les conseils d'un expert juridique concernant l'étendue de ses obligations déclaratives au Lloyd's et à la FCA. Des consultants externes en informatique ont également proposé certaines mesures d'urgence destinées à contenir l'incident (restriction du partage de fichiers entre utilisateurs, notamment) et ont proposé des mesures préventives destinées à éviter qu'un tel incident se reproduise.

Attaque par déni de service distribué visant un e-commerçant

Le site Web de l'assuré a subi une attaque par déni de service distribué, qui l'a rendu indisponible ou en a limité l'accès. Avant l'attaque, l'assuré a reçu un message en ligne lui indiquant que le niveau de protection de son site Web était extrêmement faible et que celui-ci serait mis hors ligne s'il ne versait pas 3 000 livres sterling. D'autres messages demandant des rançons de 500 livres sterling ont été reçus pendant l'attaque.

L'assuré a probablement subi une perte de chiffre d'affaires du fait de l'indisponibilité de son site Web, mais il était impossible de déterminer le montant du préjudice. L'assuré pensait qu'aucune donnée n'avait été consultée ou extraite durant l'attaque. Il a été informé qu'il n'était pas juridiquement tenu de déclarer cette attaque aux autorités.

Toutefois, l'assuré faisait face à plusieurs problèmes, informatiques, d'une part, et d'image d'autre part. L'assuré a été informé qu'il pouvait non seulement faire appel à des consultants en informatique, mais aussi à des consultants spécialisés dans les relations publiques, qui pourraient l'aider à gérer les conséquences de l'indisponibilité temporaire de son site Web.

Envoi non autorisé d'e-mails par une société de recouvrement

L'assuré a été victime d'envois d'e-mails non autorisés suite à l'erreur d'une plate-forme logicielle tierce. Un tiers a réclamé 11 275 livres sterling à l'assuré en rémunération de prestations réalisées du fait de cet envoi. L'assuré cherchait à obtenir cette somme auprès du fournisseur de plate-forme, mais il risquait de devoir la payer lui-même.

Cet incident soulevait plusieurs interrogations. L'assuré a bénéficié de conseils d'ordre juridique relativement au contrat conclu avec le fournisseur de plate-forme, et à la possibilité pour l'assuré de recouvrer les sommes réclamées auprès du fournisseur. Il a également reçu des conseils en matière de protection des données, bien qu'aucune donnée personnelle n'ait, semble-t-il, été perdue, divulguée, compromise ou corrompue du fait de cet incident.

Des consultants informatiques externes ont conseillé l'assuré et recueilli des informations afin de démontrer que l'incident n'avait pas été causé par une défaillance de ses propres systèmes ou de ses collaborateurs. Enfin, certains destinataires des e-mails ainsi envoyés ayant formulé des réclamations, il a été conseillé à l'assuré de consulter ses propres spécialistes des questions de relations publiques ou des conseillers externes, afin de déterminer la suite à donner à l'incident à ce niveau.

Les questions clés à poser à un assureur des cyber-risques ?

1. *L'assureur a-t-il déjà géré et indemnisé des sinistres cyber ?*

2. *L'assureur cherche-t-il continuellement à trouver de nouveaux moyens pour aider les assurés à se prémunir contre les nouveaux risques ?*

3. *L'assureur sera-t-il en mesure d'intervenir au niveau mondial ?*

4. *L'assureur dispose-t-il d'un réseau de professionnels agréés, composé d'experts informatiques et juridiques et de consultants en relations publiques ?*

5. *L'assureur a-t-il une approche globale de son métier de souscripteur et de gestionnaire sinistres, en d'autres termes, propose-t-il des prestations en amont et des conseils destinés à atténuer le risque en cas de sinistre ?*

6. *L'assureur assure-t-il la gestion des sinistres par le biais d'un prestataire externe, ou dispose-t-il en interne d'une équipe d'experts spécialisés, afin de garantir un dialogue constant entre gestionnaires de sinistres et souscripteurs ?*

Les auteurs :
Kathy Avery est Financial Lines Major Loss Adjuster chez AIG Europe Ltd. Elle est spécialisée dans les sinistres professionnels de grande ampleur et les cyber-risques au Royaume-Uni et dans le reste du monde. José Martínez est VP Financial Lines Major Loss Claims pour la région EMEA.

Méthodologie

En octobre 2016, AIG Europe a analysé 221 sinistres cyber déclarés en vertu de ses polices d'assurance des cyber-risques entre 2013 et septembre 2016.

Contacts

AIG a des équipes spécialisées dans la souscription et la gestion des sinistres cyber dans toute l'Europe. Chaque année, notre équipe d'experts traite un grand nombre de sinistres cyber. Pour en savoir plus, contactez votre représentant AIG au niveau local.

www.aig.com/fr

AIG Prêts pour demain®