Le risque cyber est-il systémique ?

En décembre 2016, AIG a interrogé des experts en cyber-sécurité et en gestion des risques afin de mieux comprendre leur point de vue concernant la probabilité d'une attaque cyber systémique et ses incidences.

Si la question « le risque cyber est-il systémique ? » semble en soi assez simple, nous pensons que les éléments de réponse sont en réalité beaucoup plus subtils. Une seule attaque peut-elle toucher des dizaines, des centaines voire des milliers d'entreprises en même temps ? L'ampleur d'une attaque est-elle inversement proportionnelle à la probabilité qu'elle se produise ? Certains secteurs sont-ils plus exposés à un risque systémique que d'autres ? Ces questions et d'autres dictent les travaux de recherche présentés dans ce rapport. Ces données peuvent se révéler utiles pour évaluer l'ampleur du risque cyber systémique et se préparer à l'éventualité d'attaques systémiques, des questions centrales pour toute entreprise évoluant dans l'écosystème de la cyber-sécurité. En outre, les éléments de réponse à ces questions fournissent aux assureurs de risques cyber des informations précieuses pour modéliser et gérer efficacement le risque lié à l'accumulation des données.

Si la question que nous étudions - « le risque cyber est-il systémique ? » - est en soi assez simple, nous pensons que les éléments de réponse sont en réalité beaucoup plus subtils.

Principales conclusions

Un oui catégorique : le risque cyber est bien de nature systémique

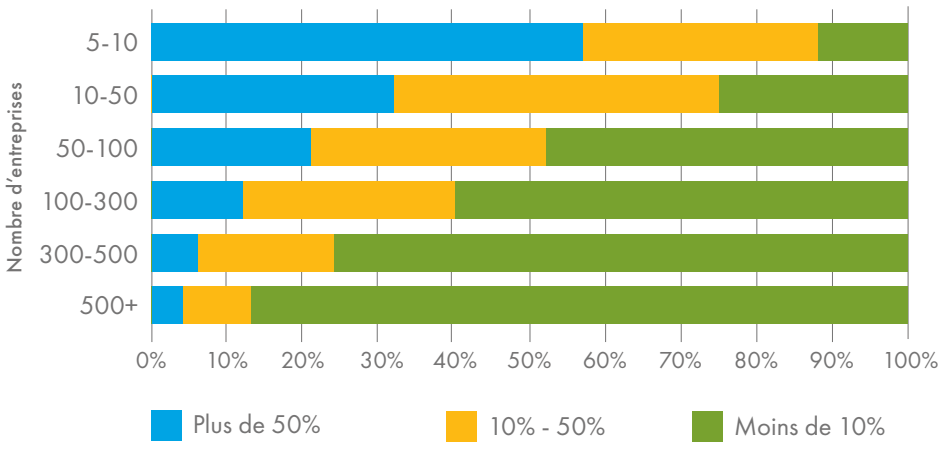
Plus de 90% des experts interrogés pensent que le risque cyber est de nature systémique, c'est-à-dire qu'il peut potentiellement affecter un grand nombre d'entreprises simultanément. Un constat lourd d'implications pour tout ce qui touche à la cyber-sécurité et à l'assurance, sans compter les pratiques en matière de gestion des risques. Entreprises, municipalités et particuliers doivent réfléchir autrement à leurs vulnérabilités en matière de cyber-sécurité car faire appel à des fournisseurs, transférer ses données dans le cloud et utiliser des machines et des dispositifs interconnectés peuvent profondément modifier leur profil de risque. Dans le même temps, assureurs, courtiers et prestataires de services doivent travailler de concert pour renforcer la protection physique, virtuelle et financière et le soutien apporté aux clients afin de limiter ce risque grandissant.

Plus de 90% des experts interrogés pensent que le risque cyber est de nature systémique, c'est-à-dire qu'il peut potentiellement affecter un grand nombre d'entreprises simultanément.

De quelle ampleur parle-t-on ?

Identifier le risque d'une attaque systémique est un bon début. Encore faut-il en comprendre la probabilité et l'étendue. Invités à noter le risque d'attaques de différentes ampleurs au cours de ces douze prochains mois, une large majorité des experts interrogés pensent qu'une attaque cyber systémique qui affecterait entre cinq et dix entreprises à la fois est plus probable qu'une seule attaque qui toucherait une centaine voire un plus grand nombre d'entreprises. Pour autant, de récents incidents, comme par exemple, le « ransomware » qui s'est infiltré dans plusieurs bases de données MongoDB, l'attaque cyber massive contre Dyn par déni de service ou encore le piratage du protocole bancaire de transfert international SWIFT, mettent en lumière la menace bien réelle d'incidents systémiques d'une ampleur autrement plus importante. Dans le cas de l'attaque cyber contre Dyn, un gestionnaire de trafic Web, les hackers ont infiltré un service d'infrastructure sur Internet, occasionnant des retards ponctuels sur des sites internet à grand trafic affectant plusieurs secteurs d'activité.

Quelle est la probabilité qu'une attaque systémique affecte plusieurs entreprises dans les 12 prochains mois ? (n=68)



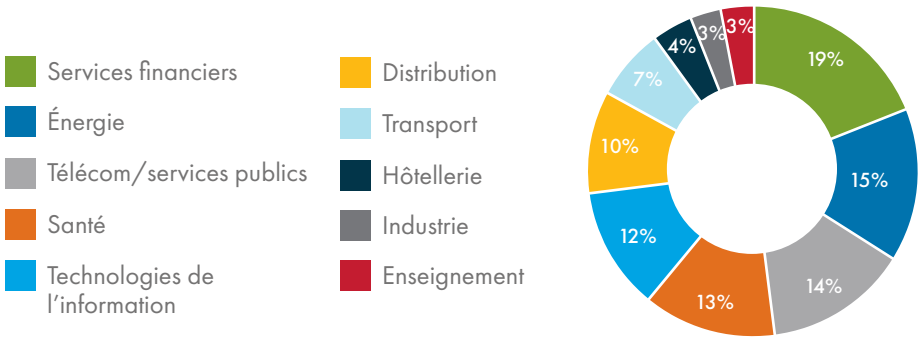
Fin 2016 et début 2017, des hackers ont rançonné les clients d'une plateforme de base de données open source largement utilisée, MongoDB. Ils ont apparemment attaqué des versions antérieures dont les paramètres de sécurité par défaut ont facilité l'accès, la visualisation, la modification ou la suppression de données. Selon des chercheurs en sécurité, entre 50 000 et 100 000 bases de données ont été exposées à l'échelle mondiale. Flashpoint, cabinet spécialiste de la cyber-sécurité, estime qu'au moins 20 000 bases de données ont peut-être été définitivement supprimées[1].

Selon un hacker éthique qui étudie le problème, l'attaque pourrait avoir affecté des entreprises de plusieurs secteurs d'activité, notamment la santé, les services financiers, l'éducation et le tourisme[2]. Quoique difficiles à quantifier, les répercussions de ces pertes de bases de données sont probablement assez importantes. Un établissement de santé de premier plan aurait perdu trois années de données de recherches suite à l'attaque qui a détruit sa base de données.

Premier visé ? Le secteur des services financiers

Une majorité des experts interrogés (85 %) pensent que certains secteurs d'activité sont plus susceptibles d'être visés par des attaques systémiques que d'autres. Les services financiers (19 %), l'énergie (15 %), les télécommunications/ les services publics (14 %), la santé (13 %) et les technologies de l'information (12 %) sont les secteurs cités comme les plus susceptibles d'être impactés par une attaque systémique au cours des douze prochains mois. Ces chiffres donnent un aperçu des vastes attaques systémiques que l'on pourrait voir, comme la perturbation de réseaux financiers ou de systèmes de transactions, des infrastructures Internet, du réseau électrique, et du système des soins. Les sociétés spécialisées dans les technologies de l'information, y compris les fournisseurs de logiciels et de matériels qui forment l'ossature de notre économie numérique, sont également perçues comme des cibles privilégiées. Notre économie ultra-connectée repose sur des flux de données et des échanges électroniques sécurisés, efficaces et réguliers. La moindre perturbation dans ces flux et la moindre faille dans la sécurité des données peuvent avoir des effets en chaîne et nuire aux organisations qui travaillent avec ces données.

Vous avez 100 € à miser. Placez cette somme en fonction des secteurs qui seront victimes d'une attaque systémique au cours des 12 prochains mois (n=70) (montant total misé = 7 000 €)



[1]https://krebsonsecurity.com/2017/01/extortionists-wipe-thousands-of-databases-victims-who-pay-up-get-stiffed/#more-37597
[2]http://www.securityweek.com/33000-databases-fall-mongodb-massacre

La plus grande menace : les attaques massives DDoS

Invités à évaluer la probabilité du pire scénario (par exemple, une seule attaque touchant au moins 500 entreprises), les experts ont jugé qu'une attaque massive par déni de service distribué (DDoS) contre un important fournisseur de services Cloud pouvait constituer le méga-incident multisectoriel le plus probable. Une analyse particulièrement importante étant donné la croissance dynamique du Cloud computing et la prolifération des dispositifs IoT (Internet des objets) utilisés pour lancer des attaques massives DDoS. Il ressort également de ce classement que des attaques systémiques pouvant toucher les services financiers, la santé et la distribution sont jugées les plus probables. Des failles dans du matériel ou des logiciels largement utilisés dans un secteur arrivent en tête des craintes dans des scénarios de vol ou de destruction de données.

À l'inverse, les attaques d'infrastructures sensibles pouvant entraîner d'importantes pertes humaines et des préjudices corporels n'arrivent qu'en dernière position. Lancer une attaque de grande envergure sur des infrastructures (par exemple, des services publics, l'aviation ou les transports) exige de toute évidence un niveau élevé de sophistication, réduisant de ce fait le nombre de candidats compétents, bien que le spectre d'une telle menace plane.

Il semble plus probable de vivre une attaque DDoS qui touche 15 entreprises du secteur financier qu'une faille dans la tour de contrôle impactant 10 compagnies aériennes.

Classer les scénarios suivants du plus probable au moins probable au cours des 12 prochains mois. Plus probable = 1, moins probable = 10 (n=66)	Classement moyen
Services financiers. 15 entreprises touchées. Interruption massive d'activité. Attaque massive DDoS coordonnée dirigée contre des établissements financiers.	4.1
Santé. 10 entreprises touchées (par exemple, hôpital, pharmacie, mutuelle). Vol massif de données. Faille au niveau du logiciel couramment utilisé pour gérer les dossiers électroniques des patients.	4.1
Distribution/hôtellerie. 25 entreprises touchées . Vol massif de données. Faille au niveau du logiciel/matériel largement utilisé pour traiter les paiements.	4.3
Mutisecteur. 350 entreprises touchées . Interruption massive d'activité. Attaque massive DDoS dirigée contre un important fournisseur de services Cloud.	4.5
Services financiers. 15 entreprises touchées . Vol massif de données. Faille dans le système largement utilisé par les chambres de compensation.	4.7
Mutisecteur. 350 entreprises touchées . Interruption massive d'activité. Faille dans les logiciels couramment utilisés (par exemple, Plesk, BIND) sur les machines dont le système d'exploitation est Linux.	6.2
Mutisecteur. 350 entreprises touchées . Vol massif de données. Faille dans les logiciels couramment utilisés (par exemple, Plesk, BIND) sur les machines dont le système d'exploitation est Linux.	6.3
Services publics/électricité. 35 entreprises publiques touchées. Interruption massive d'activité. Faille dans le système de contrôle industriel couramment utilisé.	6.3
Services publics/électricité. 10 entreprises publiques touchées. Importants dégâts matériels, préjudices corporels, interruption d'activité. Faille dans le système de contrôle industriel couramment utilisé.	6.8
Aviation. 10 compagnies aériennes/aéroports touchés. Importants dégâts matériels, préjudices corporels, interruption d'activité. Faille dans la tour de contrôle et le logiciel de navigation à bord.	8.0

Pour les experts interrogés, une attaque massive par déni de service distribué (DDoS) contre un important fournisseur de services cloud est le méga-incident multisectoriel le plus probable.

Conclusion

Les avancées technologiques font progresser les sociétés. Vaccination, électricité, transports en commun, chimie de pointe, toutes ces avancées fondamentales ont fait de notre monde un monde meilleur. Mais à chaque avancée, son lot de risques et la tentation de s'écarter des normes et des exigences établies. Bien plus que tout autre facteur social, le commerce électronique influence le profil de risque de notre économie moderne.

Mais, comme les précédents exemples le montrent, le risque reste gérable puisque la majorité des experts interrogés s'accordent à reconnaître qu'il est possible de limiter l'exposition au risque d'une attaque cyber systémique grâce à des investissements avisés dans la cyber-sécurité. Outre les logiciels et matériels de sécurité, ces investissements devraient englober le contrôle rigoureux et la gestion prudente des fournisseurs, la formation aux bonnes pratiques en matière de sécurité (par exemple, sauvegardes des données essentielles à l'activité) et la souscription d'une police d'assurance pour limiter l'incidence d'une attaque cyber systémique. Tandis que les menaces cyber continueront de se perfectionner et de se multiplier, les stratégies de défense doivent suivre le même rythme.

Dans les pires scénarios, industriels et pays entrent en cyber-guerre

Les experts interrogés ont été invités à désigner, parmi un large choix de scénarios, ceux qui « les effraient le plus », des jeux de guerre virtuels aux attaques mortelles dirigées contre des infrastructures vitales. Voici quelques exemples de scénarios retenus :

- Attaque d'un réseau électrique en période de tension du système ayant d'énormes répercussions sur la population.
- Jeux offensifs virtuels du chat et de la souris, représailles et escalade pouvant aller jusqu'au conflit armé entre des nations puissantes.
- Attaque significative dirigée contre des infrastructures de télécommunications et de services publics ayant de vastes répercussions sur des services fondamentaux.
- Piratages visant à manipuler ou à détruire des données (plutôt que de les dérober ou une attaque DDoS). Des dossiers médicaux, d'usagers des services publics ou financiers sont corrompus de telle sorte que les utilisateurs du système ne peuvent plus se fier à ces informations.
- Exploitation de failles de sécurité dans les dispositifs IoT largement utilisés dans les infrastructures critiques entraînant des interruptions de services de grande ampleur ou des préjudices corporels.

Méthodologie

Afin de recueillir ces données pour les besoins de cette étude, AIG a envoyé, en décembre 2016, des enquêtes électroniques à plus d'une centaine de professionnels de la cyber-sécurité, des technologies et de l'assurance aux États-Unis, au Royaume-Uni et en Europe continentale. Parmi les destinataires figuraient des responsables en sécurité de l'information, des experts en technologies et des enquêteurs scientifiques ainsi que des chercheurs en cyber-sécurité, des universitaires, des courtiers en assurance, des souscripteurs et des spécialistes de la modélisation des risques.

Contact

Pour plus d'informations sur la souscription des couvertures AIG contre les risques cyber :

Sophie Parisot
Responsable Produit Cyber
sophie.parisot@aig.com

www.aig.com/fr

AIG Prêts pour demain®

FL00002081 06/17 - FR DMC 008 Cyber systemic 072017