ayming

Operations performance

Operations Insight #15

Assurances : mais que fait votre police contre la cybercriminalité ?

Jean-Marc Sarter
Senior Consultant
Expertise Achats indirects
jmsarter@ayming.com

Une cyberattaque d'ampleur inédite a paralysé une partie du web vendredi 21 octobre aux États-Unis. Pour saturer les services de connexion et rendre des sites internet inaccessibles, les hackers ont organisé des vagues déferlantes de demandes de connexion en passant par des millions d'objets connectés. De quoi regarder son grille-pain avec suspicion ! Pour autant, 87% des entreprises ne croient pas qu'une cyberattaque puisse les viser et les mettre en péril. Et tout autant ne sécurisent pas suffisamment l'accès à leurs données. Or, la sous-estimation du risque représente un danger majeur et reste le principal atout des pirates !

Qu'est-ce qu'une cyberattaque ?

L'actualité nous fournit des exemples de cyberattaques au quotidien. Données volées et divulguées (mails d'Hillary Clinton, piratage de Sony), secrets technologiques ou militaires dévoilés (sous-marins DCNS), désinformation (attaque contre TV5 Europe), fonds détournés, espionnage industriel, etc.

Les auteurs de ces intrusions ont des profils divers : services de renseignements étrangers, groupes terroristes, organisations mafieuses mais aussi et surtout hackers, concurrents, collaborateurs mécontents ou toute personne aux intentions crapuleuses. Ne pas protéger ses données représente donc un risque réel.

L'ampleur des menaces

Les derniers chiffres fiables concernant le coût de la cybercriminalité datent de 2014[1]. Aux États-Unis, celle-ci a coûté 108 milliards de dollars soit 0,64% du PIB, pour 60 milliards en Chine (0,63% du PIB) et 59 milliards de dollars en Allemagne (1,6% du PIB). En France, ce coût serait de l'ordre de 3 milliards de dollars soit 0,11% du PIB. Un chiffre relativement faible, qui ne s'explique pas par une meilleure cybersécurité au plan national. Il semblerait plutôt que la France ne soit pas encore une cible prioritaire pour les cybercriminels. Nul doute que le rattrapage est en cours…

[1] Source : rapport du Center for Strategic and International Studies (CSIS)

Car la menace va croître, de manière exponentielle, et ce partout dans le monde, avec pour ligne de mire les cibles les plus lucratives et les moins protégées. Inga Beale, présidente des Lloyd's de Londres vient ainsi de lancer un cri d'alarme dénonçant la « nonchalance » des dirigeants d'entreprises face à ce qui n'est toujours pas perçu comme un péril vital.

Cette nonchalance présumée s'explique en grande partie par le fait que la plupart des dirigeants ont été rassurés par les conséquences limitées des attaques subies. Ainsi, fin 2014, lorsque des pirates ont obtenu les numéros de téléphone de 500 millions de clients Yahoo en organisant une fraude majeure, le grand public a été rassuré parce qu'il suffisait de consulter l'annuaire téléphonique pour obtenir le même résultat ! Une forme de réassurance par l'absurde et un sentiment général de déni, « tout cela n'est pas si grave », qui s'expliquent par une mauvaise compréhension de la menace.

La nature de la cybermenace

En fonction de l'intention du cyberpirate introduit dans le système, les dommages causés peuvent être considérables et menacer la survie même de l'entreprise.

Pour exemple, Aramco est une entreprise saoudienne qui extrait 10% de la production mondiale de pétrole. En juillet 2012, un collaborateur ouvre un e-mail piégé. Le 15 août suivant, une organisation se dénommant « le glaive tranchant de la justice » met hors d'état de fonctionnement 35 000 ordinateurs ainsi que les téléphones de l'entreprise qui fonctionnaient tous en VOIP[2] . Aramco n'a alors pas d'autre solution que de ressortir les machines à écrire et les fax analogiques des années 70 et d'affréter un avion pour aller chercher de nouveaux disques durs en Asie du sud-est ! La gestion des stocks, l'expédition, la facturation deviennent cauchemardesques et une bonne partie du pétrole livré les semaines suivantes n'a jamais été payée… Une compagnie moins solide qu'Aramco aurait probablement disparu.

Ainsi, outre le délit d'intrusion initial, le cyber hacking produit toute une série de crimes et délits des plus classiques (détournements de fonds, extorsions, usurpations d'identité) aux plus innovants. Parmi ces derniers, le vol de données critiques, y compris celles confiées par les clients. Et plus le caractère des données volées est sensible (données personnelles, médicales, financières, stratégiques, intimes…), plus les conséquences sont lourdes. Pertes sèches, couverture médiatique dévastatrice et déficit d'image à la clef.

[2] « Voice over IP » est une technologie permettant de communiquer via la voix au travers d'internet ou n'importe quel réseau basé sur le protocole TCP/IP.

Outre le vol de données, une cyberattaque peut également engendrer un déni de service. Une fois bloquée, l'entreprise ne fonctionne plus et subit une perte d'exploitation. Ce fut le cas, douze heures durant, le vendredi 21 octobre dernier, pour Amazon, Airbnb, Paypal, CNN, le New York Times et Twitter, entre autres.

Enfin, ultime risque à ne pas prendre à la légère, et non des moindres, celui des amendes encourues par les entreprises en cas de manquement. La protection des données est un sujet sensible et les pouvoirs publics renforcent la législation partout dans le monde. En découle des amendes de plus en plus lourdes. La législation européenne prévoit ainsi des amendes jusqu'à 4% du CA mondial en cas de manquement grave de la part des entreprises, et jusqu'à 20 M€ pour les autres organismes !

Le rôle de l'assureur face à la cybercriminalité

Dans ce monde menaçant et lucratif du piratage informatique, l'assureur adapte en permanence sa réponse.

D'une part, il encourage la prévention par une sécurisation des systèmes et des contrôles d'accès et la mise en place d'un plan d'urgence. Comme pour tout risque, l'issue finale ne dépend pas tant de la survenance que de la réaction suite à la survenance. En cas de cyberattaque, les assureurs disposent de véritables équipes d'intervention à disposition des clients : informaticiens, juristes et communicants à même de gérer la violation.

D'autre part, il finance le risque, ce qui est le cœur du métier d'assureur. Les polices cyber-risques prennent en charge les coûts générés par une atteinte à la disponibilité des systèmes et des données, leur intégrité et leur confidentialité. L'entreprise assurée sera indemnisée par rapport à la valeur de ses actifs en cas de détournement de fonds ou de rançon, pour ses pertes d'exploitation et surcoût de fonctionnement en cas d'attaque de type déni de service, pour les frais de notification de pertes de données à la CNIL, et aux clients en cas de vol de données, et pour les réclamations liées aux préjudices causés aux tiers.

La nature évolutive des risques fait que nul aujourd'hui ne peut connaître le prix réel du risque. Faire appel à des consultants pour adapter les contrats d'assurances aux besoins du client tout en respectant les réglementations européennes ou pour l'évaluation des risques IT, la stratégie de transformation et l'accompagnement (privacy, gestion de crise, cyberdéfense) peut s'avérer utile.

Avec plus de 3 milliards d'individus ayant accès à internet dans le monde, ne pas être assuré contre les attaques cyberattaques devrait paraître aujourd'hui aussi saugrenu que de ne pas l'être contre le risque d'incendie. À l'image des menaces, les réponses apportées par les assureurs sont très évolutives, mais le marché se structure et la garantie est aujourd'hui disponible pour un prix moyen de l'ordre de 350€ par million d'euros de CA. Car les entreprises ne sont pas seulement exposées à de lourdes pertes en cas d'attaque mais également à l'obligation d'indemniser leurs clients pour les préjudices subis et au paiement de fortes amendes. De quoi se pencher sérieusement sur ce risque de moins en moins virtuel !

A propos de l'auteur :
Senior Consultant Assurances chez Ayming, Jean-Marc compte plus de 25 années d'expérience en souscription des risques au sein de compagnies d'assurance et de réassurance.

operationsperformance@ayming.com
Ayming - 185 avenue des Grésillons - 92622 Gennevilliers Cedex
Tél. : 01 41 49 64 00 - Fax : 01 41 49 64 01