LLOYD'S

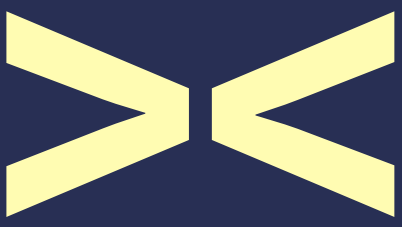
Anticiper les besoins

Assurer votre entreprise contre les menaces cyber en constante évolution

Juin 2017

Synthèse

En association avec
KPMG et DAC Beachcroft



KPMG

DAC beachcroft

Synthèse

1.1 Vue d'ensemble

Depuis quelques décennies, Internet a permis à de formidables innovations de voir le jour avec l'adoption de nouveaux modèles de fonctionnement, l'apparition d'entreprises qui ont transformé le monde et la création de millions d'emplois.

Toutefois, tous ces progrès ont eu un coût. Par leur nature, les systèmes numériques sont sensibles à des attaques cyber perpétrées par des individus ou des groupes malveillants et entraînent des répercussions de plus en plus graves pour les entreprises du monde entier. La nature des menaces évolue à un rythme si rapide qu'elles deviennent de plus en plus difficiles à contrer.

Pourtant, alors que les menaces cyber gagnent en complexité, les chefs d'entreprise sont nombreux à ne pas mesurer la pleine gravité de la situation. Une enquête récente du Lloyd's réalisée auprès de plus de 350 décideurs d'entreprises européennes a révélé que bien que 92 % des entreprises aient été victimes d'un incident cyber au cours des cinq dernières années, seulement 42 % d'entre elles craignaient qu'un nouvel incident ne se produise à l'avenir.

Ce rapport du Lloyd's, rédigé en association avec KPMG au Royaume-Uni, le cabinet d'avocats international DAC Beachcroft et les assureurs du Lloyd's, aide les entreprises à mieux appréhender la menace cyber.

La première partie du rapport offre un tour d'horizon unique, secteur par secteur (un exemple pour les services financiers est donné ici), des différentes menaces cyber auxquelles sont confrontées les entreprises aujourd'hui en proposant des pistes pour les atténuer. Elle fait également le bilan de l'ensemble des répercussions financières des violations de données et revient sur les coûts associés aux attaques cyber de forte notoriété qui se sont produites récemment.

La deuxième partie se penche sur quatre raisons pour lesquelles les entreprises doivent faire de réels efforts dans leur lutte contre les risques cyber et des conseils sont prodigués de la part d'assureurs du Lloyd's spécialisés dans ce domaine.

Risques du secteur des services financiers

- Cible principale
- Cible fréquente
- Cible occasionnelle
- Cible rare

(La taille des cercles de la même catégorie n'est pas indicative de leur fréquence relative.)

Pour consulter l'intégralité du bilan des menaces cyber auxquelles font face les entreprises aujourd'hui, voir lloyds.com/cyberriskinsight

Les secteurs concernés comprennent :
- Éducation
- Services financiers
- Soins de santé
- Hôtellerie
- Informatique
- Production
- Médias et divertissements
- Pétrole et gaz
- Services professionnels
- Secteur public
- Commerce de détail
- Télécommunications
- Transports
- Services publics

Pour en savoir plus sur ces menaces, vous pouvez consulter le rapport complet intitulé « Anticiper les besoins » à l'adresse lloyds.com/closingthegap

1.2 Principales constatations

Les types d'attaques cyber perpétrées contre les entreprises varient d'un secteur à l'autre et sont en constante évolution. Par exemple :

- Il s'est produit une hausse très nette des « attaques au président » (« CEO fraud » en anglais) dans les entreprises, qui ont entraîné des pertes financières importantes.
- Le secteur des services financiers se trouve certes au tout premier rang des attaques ciblées par la cyber-criminalité organisée, mais le commerce de détail est lui aussi de plus en plus visé.
- Les sociétés de services, comme les cabinets d'avocats et de comptables, sont de plus en plus ciblées comme passerelle d'accès afin de lancer des attaques contre leurs clients, qui sont souvent de grandes entreprises.
- Les entreprises font de plus en plus l'objet d'attaques par des rançongiciels et de déni de service distribué, les secteurs de la santé, des médias et des divertissements étant particulièrement ciblés.
- Le secteur public et le secteur des télécommunications sont très sensibles à des attaques cyber à des fins d'espionnage.

Les entreprises devraient être conscientes du coût total d'une attaque cyber, surtout sur la durée (on parle de « slow-burn ») : il s'agit du coût des impacts à long terme d'une attaque cyber, tels que la perte d'un avantage concurrentiel et la perte de clients. Ils peuvent augmenter de beaucoup le montant des coûts immédiats (en frais juridiques, frais d'investigations ou de reconstitution des données).

Quatre facteurs contribuent à aggraver les dommages causés par les attaques cyber : il est donc plus important que jamais que les entreprises fassent tout pour se prémunir des risques cyber et améliorent leur cyber-sécurité :

- Des sanctions plus lourdes pour les entreprises qui enfreignent les règles de cyber-sécurité telles que stipulées dans la législation européenne à venir.
- Une volonté accrue de la part des victimes de cyber-criminalité à poursuivre en justice les entreprises qui ont perdu leurs données.
- Une responsabilité renforcée vis-à-vis de la cyber-sécurité dans la chaîne d'approvisionnement.
- Une vulnérabilité accrue due à l'utilisation croissante d'appareils connectés (l'internet des objets).

1.3 Marche à suivre

Le Lloyd's regroupe plus de 70 assureurs qui offrent une couverture d'assurance cyber. En s'appuyant sur la perspective unique qu'apportent les experts du marché du Lloyd's, le rapport met en évidence quatre pistes à suivre par les entreprises pour se préparer à une menace cyber et s'en prémunir :

1. Comprendre les menaces spécifiques pour votre entreprise, tant en termes de coûts immédiats qu'en termes de durée, qu'il s'agisse de réputation telle que perçue par les clients ou de valeur des données détenues, des failles au sein de la chaîne d'approvisionnement et des profils des dirigeants d'entreprises.

2. Apprécier les menaces actuelles et futures : les souscripteurs tiennent compte des deux pour vous offrir la couverture d'assurance la mieux adaptée à vos besoins.

3. S'assurer que tous les salariés, y compris la direction, comprennent bien les menaces cyber auxquelles votre entreprise est confrontée, et favoriser une culture de gestion des risques cyber.

4. Demander de l'aide à des experts lorsqu'il s'agit de souscrire des assurances cyber pour veiller à la bonne prise en charge de vos risques.

1.4 Conclusion

Alors que les menaces cyber évoluent au quotidien, les entreprises doivent mieux se préparer aux conséquences d'un incident cyber. En plus de l'accroissement des coûts que la nouvelle législation européenne devrait entraîner, les entreprises font aussi face à des risques qui se multiplient.

Bien qu'il ne soit pas possible de se protéger à 100 % d'une attaque cyber, les entreprises peuvent néanmoins prendre plusieurs mesures pour s'en prémunir, veiller à en minimiser les conséquences et se rétablir plus rapidement en cas de violation de données.

L'assurance fait partie intégrante de cette solution. Tous les jours, les souscripteurs du Lloyd's spécialisés dans les risques cyber accompagnent au quotidien des milliers d'entreprises du monde entier, des multinationales aux PME, pour mieux appréhender leurs risques en leur offrant les avis d'experts et la couverture d'assurance dont elles ont besoin.

Pour lire le rapport complet « Anticiper les besoins » du Lloyd's, voir **lloyds.com/closingthegap**

Pour savoir comment les assureurs du Lloyd's peuvent vous aider, voir **lloyds.com/cybercover**