

S'ASSURER CONTRE LA CYBERCRIMINALITÉ

« 75% des entreprises ont été l'objet d'une cyberattaque lors des 12 derniers mois », c'est le constat inquiétant dressé par le groupe Symantec à la suite d'un sondage réalisé auprès de plus de 2000 entreprises dans 27 pays. La cybercriminalité concerne donc tous les types de sociétés, depuis le grand groupe international jusqu'à la TPE, pour autant qu'elles utilisent l'outil informatique.

En matière de cyberattaque, les moyens utilisés et les objectifs sont multiples et changeants. Une seule chose les rassemble, la finalité du projet : gagner de l'argent à vos dépens. L'image du jeune hacker qui opère dans son grenier ne correspond pas du tout à la réalité des menaces qui pèsent les entreprises. En effet, sauf certains « hacktivistes » qui s'attaquent parfois de très grandes entreprises, le domaine économique est réservé à des groupes organisés, de caractère souvent mafieux, qui mobilisent des ressources massives dans un but purement vénal. Il suffit pour le comprendre de connaître les types de dommages les plus fréquemment cités : le vol de données personnelles sur les usagers et clients, notamment les informations bancaires, et le vol de propriété intellectuelle. Pour les victimes, les répercussions en sont rapides et souvent importantes.

L'exemple récent du piratage de Sony vient le prouver. En plus des 100 millions d'euros que pourraient lui coûter cette faille dans son système de protection, l'entreprise voit s'évanouir un capital confiance qu'elle mettra longtemps à retrouver.

A ces deux éléments peut venir s'ajouter une baisse de compétitivité, dans le cas où les infrastructures sont victimes d'une attaque de type « déni de service », qui sature les serveurs et les rend inutilisables pour un certain temps.

Les risques sont d'autant plus grands que l'interconnexion des appareils est aujourd'hui plus forte que jamais : même les imprimantes et les téléphones portables sont reliés à l'internet et constituent ainsi, au même titre que les supports mobiles tels que les USB, des vecteurs de contagion. Le virus Stuxnet qui a récemment ciblé Siemens a notamment circulé sur des clés USB et des smartphones.



En plus d'être un enjeu direct pour l'activité de l'entreprise, toute faille dans le système de protection représente un sérieux risque juridique. En effet, selon l'article 226-17 du Code Pénal : «Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 34 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende». De plus, l'article 34 de la loi Informatique et Libertés explique que « le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.[...]». De ces dispositions découle une obligation de sécurité qui pèse sur le responsable du traitement des données. Cette obligation vaut autant pour les risques informatiques (intrusions, cheval de Troie, etc.), que pour les risques matériels (incendies, vol physique de données, etc.).

Malgré cela, les habitudes des entreprises françaises changent peu, ou trop peu. Selon la dernière étude du Clusif, plus de la moitié des sociétés dans les secteurs à risque que sont l'industrie et le commerce consacrent des budgets constants à la sécurité malgré les menaces croissantes.

En plus des nécessaires protections

informatiques (anti-virus, firewall,...) à mettre en place et à actualiser en permanence, existe-t-il des assurances qui couvrent efficacement les risques matériels à côté des risques classiques comme le bris ou le vol ? A priori, la première difficulté d'une telle police est son coût, car les dommages causés par une attaque informatique efficace peuvent être supérieurs à ceux d'une destruction matérielle, comme vient le prouver l'exemple de Sony. Le deuxième obstacle est l'établissement de la preuve et de la responsabilité, qui amène certaines compagnies à adresser des questionnaires très techniques et des demandes de preuves particulièrement complexes à leurs clients.

Pour toutes ces raisons, voici quelques points à déterminer dans le choix d'une telle police :

- Tous les supports sont-ils couverts (périphériques,...)?
- Quels types de dommages sont couverts : dommages au système informatique de tiers, gestion de crise, réputation, ... ?
- Quelle technique pour établir la preuve? Quelques assureurs proposent une solution efficace sous la forme d'un périphérique capable de déterminer avec certitude l'origine extérieure et malveillante de la perte de données.

Quelques références dans ce domaine

- Ace Europe
- Chartis
- NASSAU HDI Gerling
- Hiscox
- Chubb Assurance