Cyberattaques – les bons réflexes juridiques

publié le **20/05/2014**, vu **3614 fois**, Auteur : Me Henri de la Motte Rouge

Face à une attaque informatique d'un pirate, l'entreprise doit réagir efficacement. A défaut, elle risque d'engager sa responsabilité pour ne pas avoir pris les précautions utiles pour préserver la sécurité des données. Envisager une action judiciaire peut être un moyen de réparer le préjudice et de prévenir la récidive.

Les attaques informatiques sont en hausse. Il s'agit le plus souvent de pratiques ayant pour seul but de nuire, à un particulier, à une institution ou une entreprise commerciale. La plus courante reste l'attaque par « déni de service » qui vise à rendre inaccessible un serveur à ses utilisateurs légitimes en le surchargeant de requêtes.

Les personnes et *a fortiori* les entreprises victimes de ces attaques subissent un réel préjudice.

Lorsque l'activité de la société est dépendante de ses serveurs, celle-ci est suspendue tant que l'attaque perdure. Il peut résulter de ces attaques des pertes financières conséquentes.

Au delà de la baisse d'activité, l'indisponibilité des serveurs du fait d'une attaque par déni de service est souvent synonyme d'une perte de crédibilité, essentielle dans un marché ou l'aptitude de la société à assurer la sécurité informatique de ses données est un critère de choix pour le client.

Par ailleurs, garantir la sécurité des données est devenu une obligation légale (article 34 Loi informatique et libertés) contrôlée par la CNIL et appliquée de plus en plus strictement par les tribunaux. Au-delà du risque civil, des sanctions pénales peuvent être prononcées, jusqu'à cinq ans d'emprisonnement et de 300 000 € d'amende (article 226-17 du code pénal).

Ainsi la victime qui n'aurait pas pris toutes les « *précautions utiles* » pour préserver « *la sécurité des données* » peut, indépendamment de son dommage, se voir reconnaître partiellement responsable ... C'est d'ailleurs le premier moyen invoqué dans la défense du hacker pour l'exonérer totalement ou partiellement de sa responsabilité civile.

Dès lors, pour les entreprises victimes, la première réaction face à une attaque est évidement de mettre en place les mesures logiques et physiques nécessaires à la sécurité informatique. Ces

actions sont également indispensables pour se conformer aux obligations légales de sécurité.

Attention, en cas de violation des données personnelles, l'entreprise responsable de traitement devra également avertir sans délai la CNIL, selon l'article 34 bis de la Loi informatique et libertés.

Opter pour la mise en place de mesures de sécurité informatique est donc une réaction indispensable. Toutefois elle ne répare en rien le préjudice subi. Il convient pour cela d'envisager une action judiciaire.

Si pour l'administrateur du serveur prouver l'attaque est aisé, identifier qui en est l'auteur est plus complexe. Tout au plus, des adresses IP peuvent être collectées, mais l'entreprise ne dispose pas des moyens d'identifier formellement l'auteur de l'attaque qui procédera la plupart du temps anonymement.

Dans ce cas, il est possible de déposer une requête en identification devant le Président du Tribunal de grande instance (article 145 ou 812 al 2 du Code de procédure civile), lequel pourra ordonner au Fournisseur d'Accès à Internet (qui a une obligation légale de conservation des données) de communiquer l'identité précise du détenteur de l'adresse IP. Une fois l'auteur identifié, ce dernier pourra être directement cité devant le Tribunal de Grande Instance.

Si la requête en identification ne donne pas de résultats significatifs ou face à des hackers organisés (IP anonyme ou usurpé), il est recommandé de procéder par la voie pénale. Les attaques par déni de service, phénomène apparu au début des années 2000, sont punies de cinq ans d'emprisonnement et 75 000€ d'amende (article 323-2 du code pénal).

Un dépôt de plainte suivi d'une plainte avec constitution de partie civile a pour effet de saisir un juge d'instruction de l'affaire. Ce dernier dispose des moyens matériels et juridiques de remonter à la source de l'attaque pour identifier l'IP de l'auteur puis son identité précise. Les juges d'instruction diligentent ce genre de commissions rogatoires assistés de services de polices et de gendarmeries spécialisé en cybercriminalité dotés de moyens d'investigations efficaces.

La voie pénale, bien qu'elle soit souvent longue et ardue reste la voie privilégiée lorsque la société n'a pas la possibilité de procéder elle-même à des investigations, et qu'elle souhaite obtenir une condamnation dissuasive de l'auteur et la réparation de son préjudice.

Henri de la Motte Rouge

ww.tlmr-avocats.com

lamotterouge@tlmr-avocats.com

Le Cabinet TOUATI - LA MOTTE ROUGE Avocats est référencé parmis les meilleurs cabinets d'avocats français en IP/IT