VALÉRIE LAFARGE-SARKOZY ET ALINE BOURCEREAU
Avocats, cabinet De Gaulle Fleurance et Associés

Le cybervandalisme, fusée à plusieurs étages

L'imagination sans limites des cyber-délinquants, et leurs tristement célèbres méfaits, concernent toutes les entreprises, quelle que soit leur taille. Il s'agit là d'un effet pervers de l'utilisation exponentielle de solutions informatiques, avec des chaînes de prestataires worldwide et des équipements nomades, qui augmentent le risque de perte de contrôle des données privées, confidentielles et/ou stratégiques. Les sociétés de services en ligne font de parfaites cibles, ce que la récente attaque du site de rencontres extra-conjugales AshleyMadison.com confirme, avec le vol de données (très personnelles) de près de 37 millions d'utilisateurs.

Parmi les risques immatériels liés à la cybercriminalité, le cybervandalisme, qui consiste notamment à piller les données d'une entreprise soit pour les revendre, soit pour opérer un chantage, est sans conteste le plus dévastateur : en termes d'image, de risques juridiques (recours civils), de baisse du chiffre d'affaires liée à la perte de confiance immédiate, de frais de restauration et de sécurisation… Or à l'inverse, la revente de données bancaires piratées générerait quelque 200.000 euros par mois, et la cybercriminalité en général 1.000 milliards de dollars par an dans le monde au profit des délinquants. Voilà qui laisse rêveur…

Il est donc plus que temps de prendre ce sujet au sérieux, car le cybervandalisme pourrait bien, dans certaines circonstances, coûter aux entreprises jusqu'à leur survie.

Ainsi cette PME de Bressuire qui serait aujourd'hui proche de la cessation des paiements (44 employés) à la suite d'une fraude au président. Ce mauvais scénario de série B lui aurait coûté sa trésorerie (près de 1,6 million d'euros).

Il est vrai que certains de ces risques peuvent être assurés, mais les assureurs doivent de leur côté relever un défi macroéconomique majeur : celui de l'assurabilité d'un nouveau risque dont la mutualisation est particulièrement difficile.

Quoi qu'il en soit, les entreprises ne doivent pas se contenter de cette possibilité. La prévention constitue pour elles l'enjeu majeur pour réduire leur exposition aux risques et combattre ces crimes. En outre, la toute récente décision des hautes autorités judiciaires américaines d'autoriser la Federal Trade Commission à poursuivre les entreprises américaines qui n'auraient pas mis en place une protection suffisante des données personnelles de leurs consommateurs pourrait à terme inspirer nos propres autorités, soucieuses elles aussi de préserver la richesse immatérielle des entreprises françaises.

Vandalisées par des délinquants hyperspécialisés et performants, bientôt sanctionnées par des autorités exigeantes tout en étant pourvues d'outils le plus souvent dépassés, les entreprises françaises doivent donc très rapidement investir le domaine de la cybersécurité. Le hacking éthique, un secteur d'avenir ? ■