Fusion-Acquisition : bien encadrer la sécurité des données de l'entreprise acquise est primordial

Le piratage du groupe hôtelier Marriott a mis en avant la question du risque lié aux données dans le cadre des fusions-acquisitions. Lorsqu'ils acquièrent les données d'une autre entreprise, les dirigeants et les membres du conseil d'administration doivent comprendre l'étendue des risques encourus. Quand Marriott a intégré les systèmes et les données de Starwood dans son réseau, cet oubli lui a coûté cher (fuite de données de plus de 500 millions de clients et une amende de 111 millions d'euros infligée dans le cadre du Règlement Général sur la Protection des Données).

Lors de fusions-acquisitions, les entreprises négligent généralement les données. Or, le rachat d'une entreprise implique aussi de récupérer l'héritage de toutes les menaces qui pèsent sur sa sécurité et ses données. Les activités de fusion et d'acquisition impliquent bien souvent l'intégration de milliers, voire de millions, de fichiers.

Généralement, qu'il s'agisse d'informations sensibles sur les employés et les clients, de données financières, de propriété intellectuelle, etc., les risques numériques associés à ces fichiers ne sont pas vérifiés. Dans une entreprise moyenne, environ un fichier sur cinq est accessible à l'ensemble du personnel. Ce libre accès au contenu sensible est à l'origine de fuites majeures et d'autres incidents.

Plus les données sont exposées, plus le risque de piratage augmente.

Les entreprises qui ne savent pas où se trouvent leurs informations sensibles (aussi bien sur site que dans le Cloud), ni qui y a accès, risquent de rencontrer des difficultés avec les autorités de réglementation. L'ignorance n'est pas une excuse et ne tient pas la route face à des réglementations récentes sur la confidentialité des données telles que le RGPD (ou le CCPA – California Consumer Privacy Act – aux Etats-Unis).

Désigner des boucs émissaires n'aide pas non plus les entreprises à échapper à des amendes de plusieurs millions de dollars. Marriott, en l'occurrence, ne pouvait pas se justifier en rejetant la faute du piratage sur Starwood.

Les entreprises vont devoir intégrer les systèmes et les données de futures acquisitions

Il est essentiel qu'elles puissent évaluer et quantifier pleinement les risques. Une opération certes difficile, mais pas impossible. Il vaut mieux s'assurer que les systèmes et les données sont

verrouillés et surveillés avant de les intégrer dans son réseau lors d'une fusion. Une simple évaluation des risques, en recensant les données et en déterminant où elles sont exposées, représente une première étape importante.

Prenons le cas de cet établissement de santé qui, à la suite d'une fusion, a décidé de migrer ses données vers le Cloud. Il ne s'attendait cependant pas à trouver six millions de dossiers accessibles à l'ensemble des employés, et près de 30 000 fichiers contenant des données sensibles, dont des informations d'identification personnelle dont la protection est de plus réglementées. Sans parler des milliers de comptes utilisateur obsolètes, mais toujours actifs.

La bonne nouvelle est que les réglementations sur la confidentialité des données telles que le RGPD et le CCPA, ont un réel effet et forcent les entreprises à mettre en place de meilleurs contrôles, ou du moins certains contrôles, autour des informations d'identification personnelle. Les entreprises prennent très au sérieux l'incident dont Marriott a été victime. L'évaluation des risques liés aux données devient une composante de plus en plus courante du processus de vérification préalable à une opération de fusion-acquisition.

Le groupe Marriott a fait les gros titres à deux reprises : une première fois à l'annonce du piratage, et une seconde fois lorsqu'il a été condamné à verser une amende pour non-respect de la confidentialité des données en vertu du RGPD. S'il est à espérer que d'autres entreprises tireront la leçon de l'affaire Marriott, une attaque similaire pourrait très probablement se reproduire dans l'année à venir. Trop de données sont accessibles à un trop grand nombre de personnes.