Fusion-Acquisition : Dirigeants, quand avez-vous parlé à votre RSSI pour la dernière fois ?

En 2018, il y a eu un total de 52 224 acquisitions dans le monde, équivalant à un montant total de 3 600 milliards d'euros (IMAA, 2018). Dans 52 % des cas, des cyber problèmes ont été découverts à postériori.

Aujourd'hui, la croissance des entreprises repose en partie sur la croissance externe, soit sur la fusion et l'acquisition d'entreprises, ce qui permet de diversifier son portefeuille produits et/ou de conquérir de nouvelles parts de marché.

Le coût moyen d'une faille s'élevant à 3,86 millions de dollars (Ponemon, 2018), membres du conseil d'administration et comité exécutif ne devraient pas prendre la cybersécurité à la légère.

Depuis 3 ans, nous observons une évolution de la prise en compte des risques cyber lors de la fusion et l'acquisition d'entreprises. En effet, suite au piratage de Yahoo en 2016, qui a affecté Verizon son acquéreur et qui lui aurait coûté 4,8 millions de dollars :

Les RSSI ont été sensibilisés et formés à la gestion des risques inhérents à ces acquisitions,
Les audits de cybersécurité sont devenus monnaie courante,
Les clauses stipulent généralement que l'entreprise subira une dévaluation, si faille il y a dans l'année qui suit.

Cependant, le manque de communication entre le département IT et le reste de l'entreprise est un problème persistant. Dans une étude du Ponemon Institute, il est mis en lumière que 63 % des dirigeants des départements IT n'ont pas la possibilité d'échanger régulièrement et de remonter des informations aux membres du conseil d'administration, et 40 % pas du tout.

Fusion et Acquisition, quelles sont les menaces ?

Lors de la fusion-acquisition, la question de la cybersécurité est soulevée lorsqu'il faut intégrer les deux réseaux d'entreprise. Il faut pour cela avoir une bonne compréhension des flux et pour cela, il faut avoir une bonne visibilité sur lesdits flux réseau.

Il y a plusieurs défis critiques en matière de cybersécurité à surmonter et à gérer au cours d'une fusion-acquisition :

Une surface d'attaque plus large - Les vecteurs d'attaque potentiels qu'un attaquant pourrait exploiter augmentent et laissent les réseaux des entreprises acquéreuses et des entreprises cibles exposés et vulnérables.
Des menaces héritées ou importées - L'introduction d'une nouvelle organisation dans son réseau peut imposer une menace importante sans visibilité sur les attaquants cachés.
Des menaces internes - pendant les fusions, les menaces internes potentielles augmentent pour diverses raisons, préoccupations et incertitudes liées à l'emploi ou à la mauvaise connaissance des

usages de la nouvelle entreprise.

Des menaces tierces - Les consultants commerciaux et techniques qui sont couramment employés pendant les fusions-acquisitions peuvent, sciemment ou non, devenir des pions dans le procédé d'une cyberattaque.

Une charge importante pesant sur les équipes IT - Pendant toute la durée des fusions-acquisitions, les équipes informatiques et de sécurité des sociétés acquéreuses et cibles sont généralement très dispersées.

Il est important de dissiper ces risques, afin de ne pas souffrir une détérioration de l'image de marque, une dévaluation de l'entreprise ainsi que de charges importantes liées à la perte de données.

Dirigeants, que pouvez-vous faire à votre niveau ?

La cybersécurité ne s'appréhende pas en silo, c'est une discipline transverse à laquelle tous les collaborateurs et les cadres dirigeants doivent être sensibilisés. Tout particulièrement lors d'une acquisition, la surface d'attaque étant brusquement élargie. Doivent être mis dans la balance le temps et les charges nécessaires pour sensibiliser et former les nouveaux collaborateurs, mais également le coût potentiel d'une faille si aucune mesure n'est prise. Les coûts de la prévention des risques sont minimes comparés aux risques financiers (dévaluation en bourse), aux risques pour la réputation de l'entreprise, aux coûts informatiques, etc. Soyez-en sûr(e)s.

Dans un premier temps, programmez une réunion avec le RSSI de votre entreprise. Il pourra vous éclairer sur les risques encourus pour les systèmes informatiques de l'entreprise.

Suite à cela, plusieurs démarches peuvent être mises en place (incluant, mais ne s'y limitant pas) :

Un audit - analyse de la cyberhygiène de l'entreprise absorbée (le concept anglo-saxon Due diligence, ou audit préalable)

Une analyse des flux réseau.

Une formation rapide des nouveaux collaborateurs aux nouveaux protocoles de cybersécurité.

La mise en place d'outils de détection de menaces internes.

La notion d'intégration et de formation des nouveaux collaborateurs est tout aussi importante que les solutions de cybersécurité mises en place.

Lors d'une fusion, la gestion des cyberrisques ne devrait pas se cantonner à un paragraphe du contrat annonçant la dévaluation de l'entreprise absorbée, si attaque il y a. Il existe des moyens de se prémunir contre ces attaques pouvant engendrer de graves conséquences, un plan d'action peut être mis en place si les décideurs et le département IT de l'entreprise travaillent de concert, en complément de l'indispensable Due diligence informatique, permettant de vérifier la cyberhygiène de l'entreprise acquise. Même s'il n'existe pas de risque zéro, dirigeants, l'élaboration d'un plan est nécessaire pour réduire au minimum les risques encourus. Pour éviter une chute vertigineuse de la valeur de vos actifs en bourse, misez sur la prudence !

Du côté de l'entreprise absorbée

Les cybercriminels poursuivants généralement des objectifs pécuniaires, l'annonce de la fusion peut appâter les cybercriminels plus que d'ordinaire. En effet, en infiltrant le réseau de l'entreprise absorbée, ils pourront éventuellement réaliser une intrusion sur le réseau de la nouvelle entité et avoir accès à des données de plus grande valeur.

Les entreprises acquéreuses en sont bien conscientes. De ce fait, en mettant en place de bonnes pratiques en termes de cyberhygiène, vous sécurisez l'achat et la valeur de l'entreprise.