Startups : le risque cyber est de plus en plus regardé par les investisseurs

67 % des entreprises françaises déclarent avoir subi au moins une cyberattaque en 2019 selon le rapport Hiscox sur la gestion des cyber-risques. Une tendance orientée à la hausse depuis de nombreuses années et ce, malgré une prise de conscience des acteurs économiques quant au coût moyen engendré par l'ensemble des cyber-incidents sur leurs activités, estimé en moyenne à 110 000 euros pour l'année 2019 selon Hiscox.

PME, ETI, mastodonte du CAC 40, quelle que soit la dimension ou le secteur d'activité, les entreprises françaises sont encore loin d'être préparées à la cybercriminalité. C'est en tous cas le message porté par l'ensemble des intervenants de la conférence « Cyber d'attaque, le jour d'après » lors de la troisième édition de la Maddy Keynote le 31 Janvier dernier.

Les petites entreprises sont aussi victimes de la cybercriminalité

Trop petit pour être attaqué, mon activité n'intéresse pas les hackers… Autant d'idées reçues détricotées dans le rapport Hiscox sur la gestion des cyber-risques qui estime à 47% le nombre de petites entreprises touchées par un cyber-incident en 2019, soit une croissance de 42 % en variation annuelle ! Thibault Carre, Manager Cyber–sécurité chez Inquest *« La question aujourd'hui n'est plus si on va être attaqué mais quand ».* Dans les faits, une majorité de cyber–attaques à destination des entreprises repose sur l'envoi de logiciels malveillants à un grand nombre de cibles indifférenciées. Plus le panel visé est large, plus il y a de chance qu'une entreprise morde à l'hameçon. Les principales cyber-attaques identifiées contre les entreprises sont le ransomware, un programme rendant inaccessible les documents de l'entreprise en les chiffrant, il est généralement succédé d'une demande de rançon pour lever le blocage, le phishing dont l'objectif est de soutirer des informations confidentielles tel que les identifiants et les mots de passe et l'attaque DDoS dont l'objectif est d'inonder de requêtes le serveur web du site afin de paralyser l'activité de l'entreprise.

La méconnaissance des risques encourus par les petites entreprises en termes de cyber-attaque les conduit à moins de vigilance, à moins d'investissement dans la cyber-sécurité se contentant généralement d'anti-virus et de pare-feux pour protéger leurs plateformes. En 2019, seul 8,3% du budget informatique des TPE a été alloué à la gestion des cyber risques et ce, malgré un coût moyen des cyber-incidents estimés à 14 000 € pour une petite entreprise. Outre les enjeux financiers liés notamment à l'arrêt de l'activité ou la perte de donnée, la difficulté à gérer les litiges qui s'ensuivent avec les fournisseurs ou les clients et l'impact négatif sur la réputation, sont autant de risques en cas de cyber-incident, comme le déplore Frédéric Rousseau, directeur technique de la souscription chez Hiscox « *Une cyberattaque peut tuer votre TPE* ».

Cyberattaque : agir en amont

La cyber-sécurité est un enjeu croissant pour les petites entreprises et constitue, pour nombre d'entre elles, une priorité majeure pour les années à venir. En effet, il est important de rappeler que le risque cyber est une donnée de plus en plus regardée par les investisseurs. Cette prise de conscience se matérialise par une volonté des PME de réorienter à la hausse les dépenses liées à la cyber-sécurité avec, en premier lieu, un investissement dans de nouvelles technologies de sécurité. Toutefois, il serait naïf de croire que la dépense technologique est suffisante à l'heure où 80% des cyber-incidents font suite à une erreur humaine selon l'assureur Hiscox. Comme le soulignait

ironiquement le philosophe allemand Klaus Klages « *La plupart des problèmes informatiques se trouvent entre le clavier et la chaise* ». La formation des salariés représente donc une urgence pour les petites entreprises tant le facteur humain est majeur dans les cyber-incidents. Dans ce contexte, la mise en place d'un responsable dédié à la cyber-sécurité au sein de la PME peut s'avérer extrêmement pertinent. En effet, une planification stratégique de long-terme dans ce domaine entraînera, de fait, une plus grande réactivité de l'entreprise en cas de d'attaque.

La souscription d'une cyber-assurance permet également de minimiser le risque financier en cas de hacking. Outre la prise en charge financière de l'incident (allant de la perte de revenu consécutive à l'interruption de l'activité aux dédommagements des clients de l'entreprise attaquée) la cyber-assurance permet en amont d'évaluer le niveau de risque de l'entreprise. En septembre dernier, l'assureur Hiscox a lancé en France le premier calculateur en ligne d'exposition au risque cyber afin d'estimer l'impact financier potentiel d'une cyberattaque « *On fait souvent appel à nous après un premier incident. Or une action en amont permettrait de mieux définir sa stratégie en cas de cyber-attaque et de bien définir son programme d'assurance. Par ailleurs, s'assurer est un élément de crédibilité vis-à-vis des investisseurs et des clients* » souligne Frédéric Rousseau.

Cyber-attaque : le jour d'après

Une fois la cyber-attaque intervenue, une véritable course contre la montre s'engage pour l'entreprise quant à la gestion de l'incident. Elle doit avant tout investiguer sur l'origine du hacking via un expert en cyber-sécurité qui travaillera étroitement avec le DSI de la structure. Une fois l'incident identifié, l'entreprise a tout intérêt à mettre en place une stratégie de gestion de l'attaque. Elle peut être soutenue pour cela par un avocat spécialisé. Une fois l'incident identifié et traité, il peut être obligatoire pour le dirigeant de l'entreprise de le relater à la CNIL (régulateur chargé de veiller à la protection des données personnelle des entreprises), en vertu de la loi RGPD et cela dans les 72H succédant l'attaque. La mise en place d'un plan de communication de crise peut également être essentiel pour protéger la réputation de l'entreprise. En effet, il est important pour la structure, quelle que soit sa taille, de disposer d'éléments de langage lui permettant de rassurer ses clients quant à l'attaque survenue et aux dommages causés. La capacité de gestion de ce type d'incidents est essentielle pour une entreprise, à l'heure ou la cybercriminalité est vouée à s'intensifier. Parmi les cyber-attaques les plus courante, le cryptage contre demande de rançon, illustre bien cette nécessité d'être préparé.

En lien avec la pérennisation de l'entreprise, un investisseur sera sensible à

tout ce qui dénote de la maturité du management en général et en particulier à la prise en compte et la bonne gestion des risques, dont cyber fait bien entendu partie.

Maddyness, partenaire média d'Hiscox.

Article écrit par MADDYNESS, AVEC HISCOX