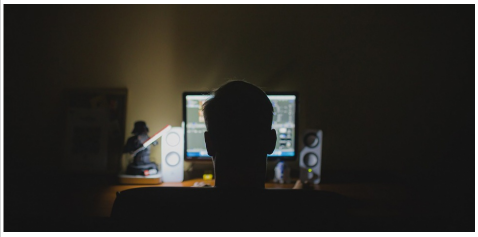
Dirigeants, êtes-vous prêts à réagir en cas de cyberattaque?

Dirigeants, êtes-vous prêts à réagir en cas de cyberattaque?

Pour Nicolas Reys de la société de conseil en gestion des risques Control Risks, la question doit être soulevée en conseil d'administration.



L'ancien directeur du FBI Robert Mueller déclarait en 2014: « il y a seulement deux types d'entreprises: celles qui ont été piratés et celles qui le seront un jour. » Ce message devient de plus en plus réel. L'attaque récente sur le principal fournisseur de services de messagerie de paiements pour les institutions financières SWIFT nous rappelle que même les organisations considérées les plus sûres ne sont pas infaillibles et que maintenant les cyberattaques font désormais partie intégrante du paysage du risque des entreprises modernes. Selon une étude récente, 1.673 brèches de données ont exposé plus de 707 millions de données diverses au cours de l'année 2015, à travers le monde. Une autre étude relève que 90% des grandes entreprises et 74% des petites et moyennes entreprises dans le monde ont subi une brèche de sécurité.

Peut être très coûteux

De nombreux dirigeants considèrent toujours la réponse à une cyberattaque comme un problème purement technique et non stratégique. Pourtant la fréquence et l'ampleur croissante des cyberattaques, ainsi que l'intérêt grandissant que les partenaires commerciaux et les autorités portent à la cybersécurité, exigent d'élever le problème au rang des conseils d'administration. Certes, le lexique associé aux cyberattaques peut être intimidant pour les chefs d'entreprises, des termes tels que « centre de commandement et de contrôle », « numéro de port TCP » et « injection SQL » peuvent laisser entendre qu'une cyber intrusion est un problème informatique et donc ne concernant pas le comité de direction. Toutefois, quel qu'en soit sa nature, ce type d'événement peut être très coûteux et une réponse mal gérée est susceptible d'augmenter de manière significative son impact commercial et opérationnel. L'Institut Ponemon estime que le coût moyen d'une fuite de données est de 3,79 millions de dollars par entreprise victime; en augmentation de 23% depuis 2013.

Préjudice de réputation

A l'extrémité de ce spectre, le distributeur américain Target, qui a subi une énorme perte de données clients en 2013, estime que le coût total de cette attaque s'est élevé à 162 millions de dollars. Un montant supplémentaire de 90 millions ayant par ailleurs été couvert par les assureurs du détaillant. Mais surtout, la marque a subi un préjudice de réputation considérable et Target a vu son rythme de croissance ralentir suite à cette crise. Il est donc possible que l'impact total sur l'entreprise sera encore plus significatif à moyen terme. D'ailleurs le PDG et le responsable de la sécurité des systèmes d'information (RSSI) de Target ont été licenciés à la suite de cet événement. Bien que comprendre les dimensions techniques de ce type de crise reste crucial pour les résoudre, il faut absolument prendre en compte les implications opérationnelles et commerciales associées aux cyberattaques.
Les gestionnaires de crise au sein de l'entreprise doivent s'interroger sur au moins trois points : « quel est l'impact opérationnel immédiat sur l'entreprise de cette attaque et avec quelle rapidité pouvons-nous revenir en ligne? Quelle est notre responsabilité juridique? Avons-nous un plan de communication en place? ». Le département informatique d'une entreprise est normalement en mesure de répondre à l'incident technique et de fournir les informations sur les accès ouverts, ce qui a été volé et ce qu'il faudra faire pour reconnecter les systèmes. Mais les informaticiens ont rarement l'expérience ou le mandat pour répondre aux questions de gestion opérationnelle qu'une cyberattaque suscite.

Brèches souvent détectées par des tiers

D'autant que, les « cyberattaques » peuvent rapidement prendre des proportions médiatiques mal maîtrisées puisque Mandiant relève que 53% des brèches de sécurité informatique sont détectées par des tiers plutôt que par les victimes.
Comment se protéger? D'abord en comprenant les capacités et motivations des acteurs prenant pour cible votre entreprise afin de formuler un plan de gestion de crise adapté et proportionné, envisageant les scénarios de crises les plus probables ainsi que les plus dangereux pour votre entreprise. Il est ainsi souhaitable d'établir avant une cyberattaque, un plan de gestion de crise et des procédures bien documenté. Assurez-vous que la réponse à l'incident technique soit complète et s'accompagne d'un plan de gestion commerciale et opérationnelle. Vérifiez donc que tous les acteurs principaux de l'entreprise connaissent ce plan et qu'ils peuvent rapidement l'actionner. Testez son fonctionnement en vous exerçant dans des conditions réelles, et posez-vous les questions suivantes: Tout le monde peut-il être contacté? Connaissent-ils leurs rôles et responsabilités face à une telle crise? Enfin soyez prêts, à vous procurer le soutien de spécialiste en gestion de crise pour vous aider si vous ne disposez pas des capacités techniques, juridiques, de communications, ou de gestion de crises nécessaires en interne.
Les attaques cybercriminelles ont doublé entre 2014 et 2015, il n'est donc plus possible d'ignorer la menace. Même si vous êtes une entreprise bien protégée, une cyberattaque a toute les chances de vous affecter dans un futur proche. La question n'est déjà plus « quand aura lieu une attaque? », mais plutôt « êtes-vous prêts à réagir? »
Nicolas Reys de la société de conseil en gestion des risques Control Risks.

Article original de Challenges.fr

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Dirigeants, êtes-vous prêts à réagir en cas de cyberattaque?