Fuite de données : cours de bourse altérés et pertes de clients

Si les conséquences financières d'une attaque informatique pour une entreprise sont régulièrement évaluées par les cabinets d'études, assureurs et autres sociétés de sécurité, celles de la perte de confiance des consommateurs sont déjà moins fréquentes. Pourtant, le regard que portent les utilisateurs d'un service sur l'entreprise qui le propose peut peser de manière non négligeable sur l'économie d'une organisation.

Les entreprises qui ont rendu publique une attaque informatique accompagnée d'un vol de données ont vu leur valeur boursière reculer de 5% dans les heures qui ont suivi l'annonce. Et, en moyenne, il leur a fallu 45 jours pour retrouver leur valeur précédant l'événement. Avec des variations. Celles qui traitent rapidement le problème de la fuite des données voient leur valorisation remonter dans les 7 jours contre 90 jours pour celles qui donnent le sentiment de négliger les conséquences de l'attaque.

Jusqu'à 7% de clients perdus

C'est du moins ce qui ressort d'une étude du Ponemon Institute qui, à la demande du fournisseur de services d'identification et de solutions de sécurité Centrify, a évalué l'évolution de la valeur boursière de 113 compagnies britanniques dans 16 secteurs industriels qui ont subi une fuite de données comparées à celles qui n'en ont pas subi sur la même période (entre 30 jours avant l'annonce publique et jusqu'à 90 jours après). Il ressort également de l'enquête que les entreprises concernées ont perdu entre 2% et 7% de leurs clients suite à l'annonce de l'attaque. Au final, ces désagréments se traduisent par des pertes annuelles comprises entre 2,7 et 4 millions de dollars, selon le Ponemon. Notons que l'étude a été réalisée avant la vague d'attaque WannaCry.

L'institut d'études a également interrogé les consommateurs ainsi que les responsables IT et marketing sur les risques de pertes de données. On constate un décalage significatif entre les attentes des clients et la vision des professionnels. Quand près de 8 clients sur 10 (79%) considèrent que les entreprises devraient avoir une obligation de prendre des mesures nécessaires pour protéger les données, seuls 66% des responsables IT et 64% des responsables marketing partagent cet avis. Et si 73% des consommateurs estiment que l'entreprise devrait contrôler qui accède à leurs informations personnelles, moins de 44% de l'IT et moins de 46% du marketing voient cet aspect comme une nécessité pour l'activité. La préoccupation principale des responsables IT en cas de fuites de données est avant tout le risque de perdre leur emploi (63% des répondants), devant la mauvaise réputation que l'affaire peut entraîner (43%) et la perte de productivité (41%).

Le comportement paradoxal des utilisateurs

Néanmoins, le comportement des utilisateurs a de quoi interroger. Si une majorité d'entre eux (52%) considèrent que la sécurité et la vie privée sont importants quand ils utilisent un réseau

social, ils ne sont que 19% à accorder leur confiance aux fournisseurs de ces plates-formes. Une confiance qui reste néanmoins plus élevée que celle recueillie pour les compagnies d'aviation (11%) et des fournisseurs de services publics (*utilities*, 8%).

Autre paradoxe, les entreprises du secteur de la santé sont considérées comme dignes de confiance pour protéger les données personnelle par 68% des répondants. Juste derrière les banques (77%). Pourtant, les organisations médicales regroupent 34% des attaques avec fuites de données. Contre 4,8% pour les banques et instituts financiers. On notera enfin que, toujours selon l'étude, seuls 51% des utilisateurs déclarent avoir été informés d'un vol de données les concernant.

Lire également
Attaques DDoS : une facture moyenne de 2,5 M$ pour les entreprises
Face aux botnets IoT, les opérateurs vont devoir collaborer
Le coût des cyberattaques ? Personne n'en sait rien, selon l'UE

Crédit Photo : Tamidichi-Shutterstock