3 à 6 mois pour détecter une attaque dans la Finance et le Retail

Arbor Networks a commandé deux études auprès de l'Institut Ponemon sur la détection des menaces avancées au sein des entreprises avec un focus sur deux secteurs : **la finance et la distribution**. Plusieurs centaines de spécialistes de la sécurité de ces différentes activités dans 14 pays ont été interrogés et les résultats reflètent un fossé entre la réalité des attaques et les réponses apportées pour les trouver et y remédier. Selon la méthodologie de l'étude, les menaces avancées en question sont celles qui réussissent à contourner les firewalls, les systèmes anti-intrusion (IDS) ou les anti-malwares.

Les chiffres les plus marquants concernent la durée de détection et de résolution des incidents. Pour le secteur financier prend en moyenne 98 jours (plus de 3 mois) pour la découverte de l'anomalie et prend 26 jours de plus pour la contenir, soit un total de **124 jours (un peu plus de 4 mois)**. Le secteur de la distribution explose les compteurs avec une découverte d'incident en 197 jours en moyenne auxquels il faut ajouter 39 jours pour le fixer, soit un total de **236 jours (presque 8 mois)**. Sur les deux secteurs on peut aller du simple au double, même si la durée de détection et de réparation reste longue dans les deux cas.

Une pratique des menaces et des méthodes à professionnaliser

Comment expliquer ces différences ? Les services financiers ont une pratique plus intense des menaces. L'étude montre que chaque mois les équipes de sécurité traitent **226 incidents de sécurité par mois**. En comparaison, dans la distribution les niveaux sont plus faibles avec **81 incidents de sécurité par mois**. La distribution est surtout en train de prendre conscience des risques à travers quelques affaires retentissantes comme Target ou Home Depot.

Cette montée en puissance des menaces ne s'accompagnent cependant pas par des changements de mentalité et des investissements supplémentaires. Ainsi dans la distribution, la méthode la plus utilisée (38% des répondants) pour identifier des attaques est **« l'intime conviction »**. Une approche toute personnelle, mais aussi toute relative quant à son efficacité.

Le secteur de la finance reste fidèle aux méthodes traditionnelles d'enquête, de traçage des signatures, d'intelligence partagée et seulement 20% des répondants se basent sur leur propre conviction. Pour le spécialiste des attaques DDoS, il est urgent d'investir dans les moyens de détection des attaques et de renforcer les moyens humains pour cela.

A lire aussi :

L'Anssi met son nez dans la sécurité des grandes entreprises

SOC : le must de la sécurité opérationnelle ? Pas si sûr…

Crédit Photo : Andrei Lishnesky- Shutterstock