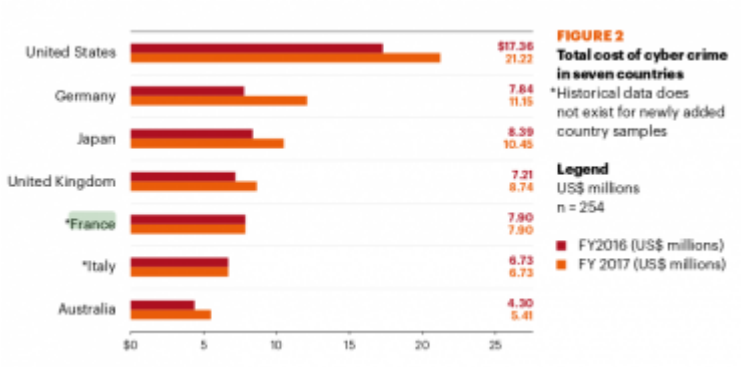
Cyberattaques : une facture annuelle de 11,7 millions de dollars par entreprise

Accenture publie l'enquête annuelle sur le coût de la cybercriminalité (« 2017 Cost of Cyber crime Study ») réalisée par le Ponemon Institute.

L'enquête a été menée auprès de 2182 répondants dans 254 entreprises sur sept pays : Allemagne, France, Italie, Royaume-Uni, États-Unis, Japon et Australie. Et la facture augmente.

Le coût moyen des cyberattaques devrait atteindre 11,7 millions de dollars par entreprise en 2017. Un chiffre en hausse de 22,7% par rapport à 2016. Il s'agit d'un « total ». Les coûts de détection, investigation, gestion, réponse à incident et reprise après sinistre sont inclus.

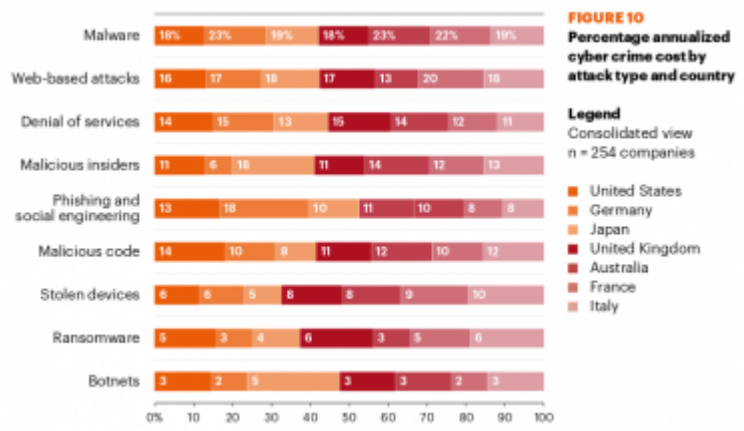
En matière de cybercrime, l'addition est bien plus salée aux États-Unis (21 M$ en 2017) que dans les autres pays étudiés, France incluse (7,9 M$).



Pour tous les pays étudiés, la hausse du coût annuel est directement liée à la multiplication des attaques, du déni de service aux ransomwares (WannaCry, Petya…).

Le rapport dénombre en moyenne 130 violations de sécurité (infiltration du SI et/ou du réseau) par entreprise. Une hausse de 27,4% par rapport à 2016 et de 62% en cinq ans !

Dans l'Hexagone, 22% du coût total est imputable aux logiciels malveillants (malwares), 20% proviennent du Web, 12% au déni de service (DoS), 12% aux attaques internes. Suivent le phishing et le code malicieux (10% respectivement), les terminaux volés (9%), les ransomwares (5%) et les Botnets (2%).



Les secteurs les plus touchés sont les services financiers et l'énergie. La situation est d'autant plus préoccupante que la durée moyenne pour résoudre une attaque par ransomware est de 23 jours. Et de 50 jours en cas d'attaque informatique interne.

Cybersécurité active

Pour mieux se protéger, les entreprises ont donc tout intérêt à prendre des mesures. Accenture met en avant les trois recommandations suivantes :

1. Bâtir une cybersécurité sur des fondations solides – notamment le renseignement de sécurité et la gestion avancée d'accès ;
2. Effectuer des tests de résistance extrême pour identifier les vulnérabilités ;
3. Investir dans des innovations de rupture, de l'analytique à l'intelligence artificielle.

Les entreprises n'ont pas d'autres alternatives que de tenter de *« résister à des attaques de plus en plus sophistiquées et extrêmement motivées »*, explique dans un communiqué Eric Boulay, directeur d'Accenture Security France et Benelux.

Pour ce faire, ajoute-t-il, *« les entreprises doivent adopter une stratégie de sécurité dynamique et agile, permettant de construire la résilience de l'intérieur vers l'extérieur. Avec une approche spécifique à l'activité pour protéger l'ensemble de la chaîne de valeur ».*

Lire également :

Le coût des cyberattaques ? Personne n'en sait rien, selon l'UE

Le vrai coût d'une cyberattaque… selon les assureurs