Sécurité : 175 jours pour détecter une cyberattaque en Europe

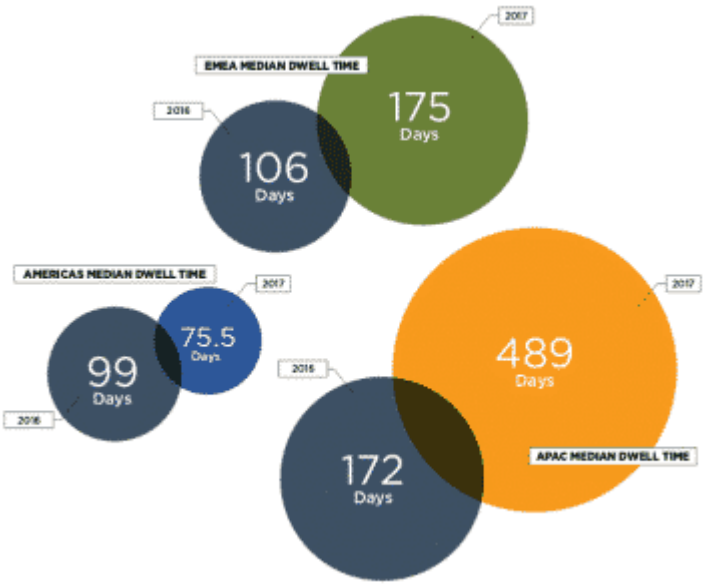
FireEye a publié la 9e édition de son rapport M-Trends. Il est alimenté par les résultats d'enquêtes menées par Mandiant, sa filiale, lors d'interventions sur incidents.

Dans la région Europe, Moyen-Orient, Afrique (EMEA), le temps de détection d'une cyberattaque par les entreprises a augmenté de près de 10 semaines en un an, selon la firme.

Le délai médian entre une attaque informatique et sa découverte est ainsi passé de 106 jours en 2016 à 175 jours en 2017 dans la zone EMEA. 6 mois sont donc nécessaires entre un assaut et son identification. Un délai bien supérieur à la **médiane mondiale** restée pratiquement stable sur la période (101 jours en 2017, contre 99 jours l'année précédente).

FireEye explique qu'en Europe davantage d'attaques anciennes ont été déclarées dans le cadre de programmes nationaux de notifications d'incident de sécurité. Une tendance confortée cette année par la transposition de la directive NIS, par exemple.

La région Asie-Pacifique est la plus mal lotie, selon le rapport. Ses entreprises mettent désormais plus d'un an pour identifier les attaques informatiques (489 jours en 2017, contre 172 jours en 2016). À l'inverse, la région des Amériques réduit les délais (75,5 jours l'an dernier pour détecter une cyberattaque, contre 99 jours en 2016).



Autre enseignement du rapport : la finance est à nouveau le secteur le plus touché (24% des investigations Mandiant menées dans la zone EMEA). Elle devance ainsi l'administration publique (18%) et les services aux entreprises (12%).

Dans le monde, dans 62% des cas (56% en EMEA), ce sont les organisations elles-mêmes qui constatent que leurs réseaux et systèmes d'information ont été compromis. *« Le délai médian mondial de détection en interne d'attaques a baissé de plus de trois semaines, passant de 80 jours en 2016 à 57,5 jours en 2017 (voire à 24,5 jours dans la zone EMEA) »*, observe FireEye.

Guerre des talents

Malgré tout, les entreprises sont encore nombreuses (44% dans la région EMEA, 38% dans le monde) à ignorer qu'elles ont été la cible d'une attaque IT, sans alerte d'un tiers : agence gouvernementale, chercheur en sécurité ou autre source externe à l'entreprise.

De surcroît, les organisations qui ont déjà été la cible d'une cyberattaque sont susceptibles d'être ciblées de nouveau par le même groupe d'attaquants ou ayant les mêmes motivations. Ainsi 56% des clients des services managés de détection (*managed detection and response*) de FireEye, auparavant clients de Mandiant, ont été la cible d'au moins une nouvelle cyberattaque significative dans les 18 mois suivant la précédente.

La situation est préoccupante. Or, la demande de compétences en cybersécurité est encore supérieure à l'offre. Une tendance qui se serait aggravée ces cinq dernières années, selon l'éditeur américain. La guerre des talents devrait se poursuivre avec l'entrée en vigueur, en mai 2018, du Règlement général sur la protection des données (RGPD).

Lire également :

Cybersécurité : forte résistance au changement en France

Cybersécurité : les RSSI parient sur l'automatisation et l'IA

(crédit photo de une © shutterstock.com)