Cybersécurité : forte résistance au changement en France

En matière de politique de cybersécurité, la résistance au changement des entreprises est forte, même après une attaque informatique. C'est le principal enseignement du rapport de l'éditeur de logiciels CyberArk sur les menaces avancées.

Ce rapport (*Global Advanced Threat Landscape Report 2018*) est basé sur une enquête internationale menée par le cabinet Vanson Bourne. 1300 responsables de la sécurité informatique, décideurs métiers et développeurs ont été interrogés.

Globalement, 46 % des organisations concernées modifient rarement leur stratégie de sécurité de manière significative, même après avoir été la cible d'une cyberattaque. En France, ce taux est bien plus élevé : 61 %.

Par ailleurs, 46 % des répondants (57 % en France) jugent que leur organisation n'est pas en mesure d'empêcher chaque tentative d'intrusion dans les réseaux internes.

De plus, 50 % des professionnels interrogés (57 % en France toujours) pensent que les données ou informations personnelles identifiables de leurs clients peuvent être menacées. Et ce car les contrôles de sécurité n'excèdent pas les bases légales requises. Il reste à savoir si l'entrée en vigueur du Règlement général sur la protection des données (RGPD), en mai 2018, changera la donne…

Autre constat préoccupant : 36 % des répondants (53 % en France) indiquent que les identifiants administrateurs sont enregistrés dans des documents Word ou Excel sur les ordinateurs de l'entreprise.

Comptes à privilèges

Une majorité pense qu'une meilleure protection des comptes à privilèges (le coeur de métier de CyberArk) sur site, dans le cloud et sur terminaux est nécessaire. Toutefois, les décideurs IT et métiers interrogés sont encore peu nombreux à l'activer, selon le rapport.

Or, les répondants en France citent les attaques ciblées par hameçonnage (53 %), les comptes à privilèges non sécurisés (49 %) et les menaces internes (44 %) parmi les plus grandes menaces de sécurité auxquelles leurs organisations sont confrontées. Les données non sécurisées stockées dans le cloud (31 %), les ransomwares et d'autres logiciels malveillants (28 %) arrivent ensuite.

Pour CyberArk, une approche passive de la sécurité crée un cyber-risque « majeur » alors que les menaces se multiplient. Selon l'éditeur basé à Petah Tikva (Israël) et Newton (Etats-Unis), sortir de l'inertie dans ce domaine est une nécessité. Elle implique que les dirigeants diffusent une véritable culture de la sécurité informatique au sein de leur organisation.

Lire également :

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

Sécurité des réseaux : la France transpose la directive NIS

(crédit photo © Rawpixel.com / shutterstock)