La cyber-vulnérabilité des entreprises marocaines sous la loupe de Kaspersky Lab

La vulnérabilité des entreprises marocaines en matière de cyber-sécurité était au cœur d'une récente étude menée par le leader mondial Kaspersky Lab, en partenariat avec le cabinet d'études Averty. Si les premiers résultats font état d'une réelle prise de conscience face aux menaces informatiques, il apparait également que le facteur comportemental peut lourdement aggraver les risques encourus par les entreprises marocaines.

Spécialiste mondial dans la sécurité des systèmes d'information, Kaspersky Lab a dévoilé - en fin novembre 2017, les résultats de cette étude qui diagnostique les comportements et attitudes des professionnels marocains en matière de sécurité informatique.

En vidéo, les principales conclusions de Kaspersky :

0:00 / 0:50

Première constatation, les entrepreneurs marocains sont pleinement conscients des cyber-menaces. Les sondés identifient les virus (63%), les logiciels malveillants (21,4%) et la perte de données (16,9%) comme étant les trois principaux risques informatiques guettant leur activité. Qui plus est, 21% d'entre eux - soit plus d'une entreprise sur cinq, affirment avoir déjà fait les frais de ces menaces.

Face à cette situation, 78% des professionnels marocains ayant participé à cette étude sont convaincus de l'importance des outils de sécurité informatique dans la protection des données professionnelles. Toutefois, 20% des sondés n'y ont pas recours, estimant ne pas en avoir besoin. Il n'en demeure pas moins que l'antivirus représente, pour 84,6% d'entre eux, l'outil de protection informatique le plus fréquemment utilisé.

Les facteurs comportementaux aggravent le risque

En présence d'une faille de sécurité informatique, l'on pourrait penser que le premier réflexe serait d'alerter le département informatique de l'entreprise. Or, l'étude de Kaspersky Lab révèle qu'étonnamment, ce département n'est sollicité que dans 50 % des cas avérés. Ce qui rend encore plus difficile la possibilité de circonscrire ces menaces informatiques.
L'élément humain figure en bonne place dans la liste des facteurs de cyber-vulnérabilité. 40% des professionnels interrogés déclarent avoir déjà connecté des clés USB inconnues, là où 33% affirment avoir déjà cliqué sur des pièces jointes qu'ils n'attendaient pas ou incluses dans des mails envoyés par des inconnus.
Près de 46% des répondants affirment aussi ne pas changer de mot de passe, renforçant ainsi les risques de piratage et d'intrusion de compte. Enfin, encore près de 30% des interrogés ont confié outrepasser ou négliger les règles de sécurité (retarder les mises à jours, utiliser des softwares non autorisés,...).

Toujours dans la liste des comportements à risque, un peu plus que la moitié des professionnels interrogées (53,5%) ont déjà essayé d'outrepasser les règles de sécurité IT : 23,8% le font rarement, 13,4% assez souvent, tandis que 16,2% le font toujours.

L'urgence d'un changement d'approche

Paradoxalement, si cette étude met en évidence un certain nombre de comportements à risque, elle révèle également que le tiers des sondés se sentent tout de même préoccupés par les dernières cyber-attaques telles que Wanacry et Petya - 78,8% d'entre eux estimant pouvoir être victime un jour de crypto-malwares similaires. D'où la nécessité de mettre en place des outils efficaces de sécurité informatique, compte tenu de l'importance des enjeux.

En effet, on peut lire dans le dernier rapport mondial 'Corporate IT Security Risk Survey 2016' – initié par Kaspersky Lab, que les conséquences d'une infection par un crypto-malware peuvent aller jusqu'à l'interruption totale d'activité, avec des dommages pouvant atteindre 99.000 dollars par entreprise !

S'il n'y avait qu'une chose à retenir de l'étude de Kaspersky Lab, c'est bien l'urgence d'un changement d'approche – aussi bien technologique que comportemental, face à l'ampleur des risques encourus. « La dématérialisation des contenus n'induit pas, pour autant, la dématérialisation des risques, et lutter efficacement contre la cybercriminalité ne pourra se faire sans le rôle essentiel de l'éducation et de la formation. Internet étant maintenant devenu un pilier de nos existences, la cyber-sécurité doit faire partie intégrante de l'éducation tout au long de nos vies, autant d'un point de vue personnel que professionnel » souligne Julien Pulvirenti, Responsable des ventes pour l'Afrique du Nord.