

«Les entreprises marocaines sont de plus en plus **conscientes des risques cyber**»

La première déclinaison marocaine de l'étude du cabinet de conseil et d'audit PwC « The Global State of Information Security Survey », lève le voile sur la cybersécurité au Maroc. Les détails avec Nabil Kettani. PROPOS RECUEILLIS PAR ADAMA SYLLA.

Challenge : La cybersécurité est-elle un enjeu majeur pour les entreprises au Maroc ?

Nabil Kettani : Dans un contexte marqué par une transformation digitale de plus en plus prégnante, la sécurisation des données et la cybersécurité sont bien évidemment des préoccupations majeures pour les entreprises, dans le monde entier. Au Maroc, la question de la cybersécurité est désormais un enjeu important. Nous avons constaté que les entreprises marocaines sont de plus en plus conscientes des risques cyber. Celles-ci doivent faire face à de nouveaux challenges et à une pression importante. Une pression qui est notamment liée aux multiples chantiers de digitalisation, des chantiers qui regorgent de hauts risques au niveau de la sécurité des données. Par ailleurs, le Maroc est l'un des pays les plus réactifs en matière de cybersécurité sur le continent africain. Il nous semblait donc essentiel de dresser un état des lieux des enjeux et perspectives de la cybersécurité au Maroc. C'est une première, pour cette étude «The Global State of Information Security® Survey 2018», que nous menons chaque année depuis 20 ans.

Qu'est-ce qui motive ces entreprises marocaines à renforcer leurs dispositifs en matière de protection des données ?

Nous avons constaté que la digitalisation et la réglementation de certains secteurs et directives nationales sont les facteurs qui motivent aujourd'hui les entreprises marocaines à renforcer leurs dispositifs en matière de cybersécurité. Notre enquête a d'ailleurs révélé que la conformité réglementaire reste l'élément moteur majeur qui stimule les entreprises à investir en matière de cybersécurité, devant la transformation digitale des organisations. C'est aussi par souci de laisser et de sécuriser une trace des opérations effectuées, ainsi que suite aux constats de vol d'informations clients et employés que les entreprises prennent la décision d'investir dans la cybersécurité.



Pour autant, ces entreprises sont-elles enclines à dépenser pour faire face aux menaces ?

Les entreprises marocaines sont désormais conscientes du risque cyber et de la nécessité d'investir pour se prémunir contre ces risques. Les entreprises marocaines ont consacré en 2017 des budgets en hausse significative par rapport à 2016. Ces budgets sont largement supérieurs par rapport au panel mondial (11% du budget IT au Maroc contre 4% dans le monde). Néanmoins, malgré un budget sécurité paraissant relativement significatif par rapport au budget IT, la multiplicité des sujets adressés dans un timing court induit cette perception de budget insuffisant, ce qu'affirment 72% des entreprises lors de notre enquête.

En fait, d'où proviennent ces menaces ?

Au Maroc, il s'avère que l'utilisation de logiciels malveillants est le vecteur principal des cyberattaques au sein des entreprises. 25% des entreprises, sondées dans notre étude, estiment que celles-ci sont à l'origine des incidents de sécurité subis en 2017, et près de 30% des cyberattaques sont d'origine interne

SON PARCOURS

Associé PwC en charge des offres Digital, Technology & Experience pour le Maroc et l'Afrique Francophone, Nabil Kettani capitalise 20 ans d'expérience. Il a rejoint PwC en 2011, après des expériences chez Arthur Andersen et Mazars, et la création d'AYEL, cabinet de conseil en Organisation et Systèmes d'Information, absorbé par PwC en 2011. Nabil, titulaire d'un BBA/Major en Management des SI, a mené plusieurs grands projets de transformation, autour du digital et des systèmes d'information, au niveau de plusieurs secteurs d'activité.

SON ACTU

Le cabinet de conseil et d'audit PwC vient de rendre publique la première déclinaison marocaine de son rapport «The Global State of Information Security Survey», une étude mondiale qui dresse l'état des lieux des enjeux de cybersécurité au Maroc.

à l'entreprise. Mais si le nombre d'incidents détectés au Maroc est moins important que dans le reste du monde, c'est parce que les entreprises ne détectent pas toujours les attaques dont elles sont victimes. En effet, 89% d'entre elles reconnaissent ne pas être en mesure de chiffrer leurs pertes et 39% d'entre elles ne savent pas identifier l'origine de ces incidents. Pour conclure, on peut également noter l'organisation des entreprises marocaines et pour la majorité d'entre elles, l'absence de RSSI (Responsable de la sécurité des systèmes d'information) au board, qui peut constituer un frein à la lutte contre ces menaces. Les dispositifs de lutte mis en place sont réactives post incidents ou post audit, et encore trop rarement proactives. Ceci souligne la nécessité d'intégrer la Cyber sécurité comme une priorité au niveau stratégique des organisations. ■