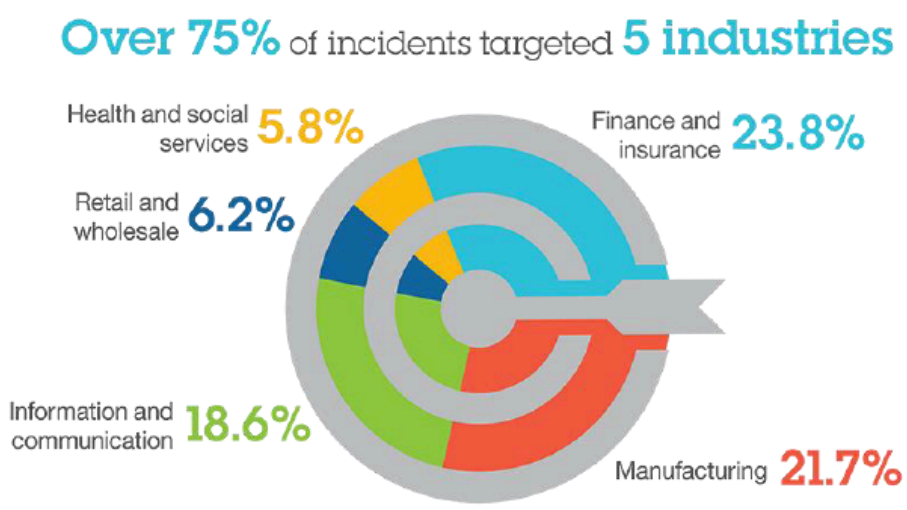
Cyber sécurité : Le Maroc doit bien s’armer



Cyber sécurité : Le Maroc doit bien s’armer

Le coût de la cybercriminalité dans le monde s'est chiffré en 2013 à 350 milliards de dollars*. Au-delà de l'enjeu économique colossal, la multiplication des cyber-attaques et de quelques cyber-guerres pose la question du «contrôle» de ce nouvel espace de souveraineté, créé par l'Homme.

Le Maroc classé 49e pays mondial à risque en matière de sécurité Internet et 3e au niveau africain dans le dernier rapport de Symantec (Symantec Corporation – Internet Security Threat Report 2013). Le risque d'une attaque virtuelle est bien réel, et les PME sont les premières cibles des cyberattaquants.
Au Maroc, le niveau des organisations marocaines par rapport à la norme ISO 27002 est encore trop faible. En effet, rares sont les entreprises marocaines ayant mis en place à ce jour une Politique de Sécurité des Systèmes d'Information (PSSI).
Pourtant la protection face aux cyber-menaces et leur évolution constante (globalisation, …) apparaît comme une initiative majeure : les attaques informatiques contre les infrastructures nationales représentent des menaces réelles. La prévention et la réaction aux attaques informatiques sont une priorité absolue des dispositifs de cyber-sécurité, en particulier les structures organisationnelles.

Aujourd'hui, les entreprises repensent leurs tactiques de cybersécurité
Selon l'étude IBM CISO (Chief Information Security Officer) parue en décembre 2014 qui visait à découvrir et à comprendre comment les entreprises se protègent actuellement contre les cyber-attaques. Elle révèle que 70% des responsables de la sécurité pensent avoir des technologies traditionnelles matures, qui mettent l'accent sur la prévention des intrusions réseau, la détection avancée des logiciels malveillants et l'analyse de la vulnérabilité du réseau.
Cependant, près de 50% reconnaissent que le déploiement de nouvelles technologies de sécurité est prioritaire pour leur entreprise. Ils ont identifié trois principaux domaines nécessitant un changement drastique : la prévention des fuites de données, la sécurité du Cloud et la sécurité des appareils et des mobiles.

Toujours selon l'étude IBM CISO :
La sécurité du Cloud reste en tête de l'ordre du jour : bien que la préoccupation liée à la sécurité du Cloud reste forte, près de 90% des personnes interrogées ont adopté le Cloud ou sont actuellement en train de mettre en place des initiatives en la matière. Dans ce groupe, 75% des responsables s'attendent à voir leur budget dédié à la sécurité du Cloud augmenter, voire de manière significative dans les 3 à 5 ans à venir.
La sécurité intelligente basée sur l'analyse des données est prioritaire : plus de 70% des responsables de la sécurité déclarent que les renseignements de sécurité en temps réel sont de plus en plus importants pour leur entreprise. Malgré cette constatation, l'étude révèle que des domaines tels que la classification et la découverte des données ainsi que l'analyse des renseignements de sécurité sont relativement peu matures (54%) et ont fortement besoin d'être améliorés ou transformés.
Les besoins dans la sécurité mobile restent importants : malgré une main-d'oeuvre de plus en plus mobile, seulement 45% des responsables de la sécurité déclarent qu'ils ont une approche efficace de la gestion des terminaux mobiles. En fait, selon l'étude, lorsque l'on adresse le sujet de la maturité, la sécurité des mobiles et des appareils arrive en fin de liste (51%).

Au Maroc, les structures organisationnelles s'organisent
La nouvelle stratégie "Maroc Numeric 2020" que le ministère de l'Industrie, du commerce, de l'investissement et de l'économie numérique, est en train de préparer, devra continuer à positionner le Maroc comme un hub technologique régional, en réalisant des progrès en termes de "transformation sociale" et d'accompagnement de l'entreprise et des différents chantiers de l'E-gouvernement. Surtout ce dernier, s'inscrit dans la poursuite des progrès réalisés depuis des années en matière des technologies de l'information, de sécurité en continuant à positionner le Maroc comme hub régional et à fournir des services aussi bien au citoyen qu'à l'entreprise, particulièrement la Petite et Moyenne.

Les PME, cible privilégiée et pourtant…
Paradoxalement alors que le Maroc est 3,5 fois plus vulnérable aux logiciels malveillants que la moyenne mondiale**, les PMEs, 1er tissu économique marocain, la cyber-criminalité, les défaillances techniques ou informatiques sont peu préoccupantes et donc peu prises en compte.

IBM a bien compris les enjeux de la sécurité des données en entreprise : « ces nouvelles offres sont conçues pour protéger les données et applications vitales de l'entreprise grâce à des techniques analytiques avancées, développées au sein même de l'entreprise, dans les clouds publics et privés, et dans les terminaux mobiles. » Actuellement, 75% des failles de sécurité nécessitent plusieurs jours, semaines voire mois pour être détectées, ce qui peut causer d'importants dommages.

Une gestion proactive de la sécurité par IBM
Les solutions proposées par IBM devraient permettre d'apporter une vue d'ensemble de l'état de la sécurité informatique, pour savoir qui utilise le cloud et de quelle façon. Les nouveaux outils peuvent être déployés dans le cloud ou sur site, pour s'adapter aux environnements informatiques des entreprises. Par ailleurs, les éventuelles menaces peuvent être identifiées en temps réel, grâce aux données d'analyse mises à disposition par IBM, appuyées sur 20 milliards d'événements quotidiens repérés dans plus de 130 pays***

Les offres de sécurité IBM apportent la sécurité intelligente pour aider les organisations à protéger les personnes, les données, les applications et les infrastructures. Les solutions IBM couvrent la gestion des identités et des accès, le SIEM (Security Information and Event Management), la sécurité des données, la sécurité des applications, la gestion du risque, la gestion des terminaux, la nouvelle génération de protection contre les intrusions, la lutte contre la fraude financière avec le rachat de Trusteer et d'autres sujets. IBM dispose d'une des plus importantes organisations de recherche et développement et de mise en oeuvre dans le domaine de la sécurité.

La cybercriminalité reste la deuxième forme la plus répandue de criminalité économique selon PwC;
La cyber-criminalité coûterait **327 milliards d'euros** par an. Selon un rapport publié par le « Center for Strategic and International Studies »;
 65% des utilisateurs d'internet ont été victimes d'une cyberattaque (virus, fraude à la carte de crédit en ligne, vol d'identité)- Soit 1.5 millions de personnes par jour (Mashable); Aux Etats-Unis, 40 millions de personnes ont été victimes de vols de données personnelles.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://lobservateurdumaroc.info/2014/12/23/cyber-securite-le-maroc-doit-bien-sarmer/
* (Le coût des failles informatiques selon l'étude menée pour le compte de Microsoft en 2013, par l'observatoire IDC (International Data Corporation)
** Source Microsoft
*** Source http://ibm.com/fr/security