

Le monde du travail veut apprendre à sécuriser ses données mobiles

La quantité de données produites par l'Homme a doublé en l'espace de deux ans seulement. Une grande partie de cette masse d'information, aussi riche soit-elle, finit invariablement par tomber dans l'oubli, ou même dans de mauvaises mains.

On a longtemps cru que des « experts » allaient surgir sur le marché du travail pour assurer la sécurité de nos données, mais ce sont les entreprises qui ont finalement pris l'initiative d'aborder le problème et sensibiliser leurs équipes. La protection des données est donc devenue une culture d'entreprise plutôt qu'une affaire de spécialistes.

Un rapport nouveau sur ses données personnelles

Le succès retentissant du mobile a entraîné un changement culturel majeur dans l'espace professionnel : les utilisateurs ont développé une connaissance approfondie des risques en matière de sécurité. Tout le monde sait qu'il faut mettre un mot de passe pour verrouiller son terminal - même si certains prennent le risque de s'en passer - et que chaque application installe une copie des données. Données qui potentiellement peuvent intéresser de nombreux tiers, dont certains mal intentionnés. Les utilisateurs sont également devenus proactifs puisqu'ils peuvent effectuer les mises à jour de l'OS de leurs terminaux mobiles eux-mêmes.

Conséquence directe : les entreprises doivent s'adapter, et très vite. Comment assurer à la fois la sécurité des données de l'entreprise, celle de ses collaborateurs et ne pas les empêcher d'utiliser des systèmes de sécurité trop contraignants ?

Les entreprises recherchent-elles des experts à tout prix ?

Des spécialistes en sécurité des données, il en existe peu voire quasiment pas sur le marché du travail. Est-ce réellement un handicap pour la protection des données d'entreprise ? Non, car les entreprises ont davantage besoin d'adaptabilité que de spécialistes. Mieux vaut connaître ses outils technologiques sur le bout des doigts et l'architecture de ses réseaux pour mieux cibler une faille ou renforcer la sécurité de ceux-ci. Au-delà de la seule sécurité des données, la problématique est encore plus grande : comprendre les besoins des utilisateurs, comprendre comment fonctionne une application pour mieux la sécuriser.

Chez les usagers comme chez les développeurs, on passe de l'ordinateur au mobile

Jusqu'à présent, les équipes des services informatiques se devaient être

spécialisées dans la sécurité des ordinateurs. D'ailleurs, chaque collaborateur possède un smartphone, voire une tablette. Des terminaux qui sont souvent autant voire plus utilisés pour consulter, accéder et partager des données internes ou externes à l'entreprise. L'attention des équipes IT s'est donc logiquement portée vers la sécurité de ces terminaux. C'est pourquoi les profils de spécialistes en sécurité mobile sont d'ailleurs la priorité du recrutement des équipes IT.

Une pénurie de formations tournées vers la sécurité de données

Mais alors comment attirer les bons talents, les meilleurs experts en la matière ? Bien sûr, il y a les écoles d'ingénieurs à l'informatique. Mais ces établissements ne créent pas (encore) de profils de spécialistes de la datasécurité. Aux Etats-Unis, par exemple, il n'existe pas de filière qui formerait ce type d'expert. En revanche, il existe déjà des formations et des spécialistes du développement d'applications. Et c'est vers ce type de profils que les entreprises se tournent à l'heure actuelle. Si on sait développer, coder, il sera bien plus facile de sécuriser ses données : voici comment les entreprises s'adaptent. Les écoles ont bien compris et les cours de code informatique ou de développement sont désormais l'option dans tous les cursus scolaires outre-Atlantique. Il reste maintenant à l'Europe à rattraper son retard en la matière.

L'émulation entre employés...

Comment stimuler les équipes à la recherche des failles ou lacunes liées à la sécurité des données dans ses propres services ? Certaines ont choisi d'opter pour la compétition interne : les équipes informatiques se lancent ainsi un défi, une partie s'attaquant aux failles, l'autre étant consacrée à les résoudre ou à renforcer cette sécurité. Avec un objectif commun : consolider ses propres outils internes. C'est notamment le cas de NeXP, société de conseil en informatique, qui a mis en place ce type de « duels » au sein de ses équipes. Un exercice qui permet à ces « hackers » d'entreprises d'être ensuite rugieusement chassés par de grands groupes grâce à leur expertise.

À l'let la concurrence entre entreprises

Le recrutement de ce type de profils reste très complexe. Car en raison du manque flagrant de forces en présence sur le marché du travail, les entreprises font face à une concurrence externe particulièrement rude. Avec très peu de profils d'ingénieurs à la sécurité des mobiles, le turnover est plus important dans ce secteur que dans n'importe quel autre corps de métier. Pour parer à la perte de leurs meilleurs éléments, les entreprises ont massivement adopté la solution des formations, que ce soit en interne ou par un organisme externe. Mais si la formation est un usage populaire en France, elle se consacre le plus souvent à des fonctions liées au management, rarement à la sécurité informatique. Et c'est ce que les entreprises vont devoir corriger dans les mois et années à venir, sous peine de ne pouvoir assurer la sécurité de leurs propres données.