Shadow IT, danger au centre névralgique des données par Steve Zagnoli – 25 oct. 2016

Alors non, nous ne vous apprenons rien : la sécurité de vos données doit faire face à de nombreuses menaces. **Mais encore ?**

Dans l'ère du numérique telle que nous la connaissons, craindre pour ses données personnelles est légitime, mais est-ce le seul volet du problème ? Aujourd'hui, les entreprises font elles aussi face à des problèmes de sécurité parfois liés à leur structure interne, d'autres fois en raison des méthodes d'organisation et de traitement de ces mêmes données. On en vient donc à parler de ***Shadow IT***, une problématique de plus en plus récurrente dès lors qu'il est question de protection d'informations sensibles.

Les cas de Shadow IT se multiplient et touchent des structures de plus en plus importantes, en passant même par de grandes organisations. Si l'on se penche sur **le vol massif des données de 112 000 policiers à la Mutuelle Générale de la Police par un ancien collaborateur** (à retrouver ici) survenu dans le courant de juin de cette année, on comprend clairement que le Shadow IT représente une réelle menace pour les données, qu'elles soient personnelles ou non. Un cas représentatif pour un nombre conséquent d'entreprises dont les services informatiques ne sont pas toujours au courant des pratiques de leurs collaborateurs eux-mêmes (78 % seulement, selon une étude explicitée dans l'article un paragraphe plus haut). Ce type d'incident doit permettre aux individus faisant face au phénomène du Shadow IT de prendre conscience de l'ampleur de la chose et des répercussions qu'il peut avoir en cas de faille sécuritaire.

À titre d'exemple, les applications de messagerie et de stockage de data tels que Yahoo ou Dropbox ont subi cette année de gros revers en terme de protection des données avec des milliers (voire millions pour ces gros groupes) d'emails et de mots de passe dérobés permettant l'accès aux documents. Si la réactivité fait partie de vos qualités, un simple changement de vos identifiants suffira. Entendez par là **les identifiants de tous vos comptes**, car, soyons honnêtes, nous avons en grande majorité la fâcheuse habitude de réutiliser le même mot de passe sur différentes applications web. Généraliser ce processus est d'autant plus dangereux qu'il peut être source de problèmes s'il s'étend aux frontières du domaine professionnel.

Ce type de service est d'ailleurs extrêmement sensible au *hacking*, pratique ne faisant quasiment aucune différence entre usage personnel et professionnel. Tendance naissante mais terriblement insidieuse, les *ransomwares* peuvent occasionner des dommages considérables et placer les entreprises en position défavorable. Pour rappel, **ces virus sous forme de logiciel prennent littéralement en otage vos données**, l'objectif du larcin étant par la suite de forcer le malheureux à payer une rançon pour récupérer le contrôle de celles-ci (dans l'éventualité que l'interlocuteur soit « honnête »). Même si de nouveaux outils sont

proposés pour contrer leur effet parfois catastrophique, il aujourd'hui impossible d'affirmer qu'ils en deviennent inoffensifs.

Au-delà des informations personnelles, qui étaient il y a quelques années la cible prioritaire à 99 %, **les données professionnelles sont en passe de devenir les informations les plus prisées par les pirates informatiques** (avec un stupéfiant **43 %**) selon un rapport commandé plus tôt cette année par Laurent Heslault, directeur des stratégies de sécurité chez Symantec, l'éditeur américain de l'antivirus Norton.

Les solutions pouvant aider à la réduction des risques relèvent simplement en grande partie du bon sens humain : garder à l'esprit que les intérêts sécuritaires des entreprises doivent prévaloir sur les habitudes individuelles est essentiel. De son côté, la direction doit s'assurer de fournir à ses collaborateurs les outils nécessaires afin de favoriser l'efficacité des processus et de garantir l'intégrité des informations relatives à la compagnie. Si l'on peut aussi mêler à l'ensemble ergonomie, réduction des coûts et adaptabilité des modules d'application, c'est toujours mieux. **À bon entendeur !**