Sécurité des données : attention aux mythes…

Selon Victor S. Wheatman,

managing vice-president du cabinet d'études Gartner, la donne a changé : « *Les principales questions soulevées aujourd'hui en matière de sécurité ont évolué. Elles concernent désormais le développement d'une infrastructure souple et efficace qui soit, en outre, gérable. Elles visent également à maintenir un bureau standard en garantissant un niveau égal de performance au niveau des applications, le tout en améliorant le coût de possession global des actifs informatiques*« . Dans ce contexte, les outils d'amélioration de la sécurité sont passés du premier rang en 2002-2003 au troisième rang cette année. Pourquoi un tel recul ? Peut-être parce que les préoccupations des entreprises ont évolué. Celles-ci recherchent en premier lieu à éviter toute interruption de leur activité pouvant provenir d'une faille de sécurité. Mais ce sont ensuite les coûts opérationnels qui sont dans la ligne de mire, suivis par la protection des données et la garantie du caractère privé de ces dernières. **Ce que disait Bill Gates, en mars dernier…** Autrement dit, il ne s'agit plus de crier au loup mais de travailler en étant conscient des risques et des enjeux. C'est ce qui disait Bill Gates, interrogé à l'occasion du symposium ITxpo de SAN Diego en mars dernier: « *Je pense que d'ici deux ans, la sécurité sortira du hit parade des cinq principales préoccupations des entreprises. Passé ce délai, nous devrions disposer de systèmes quasi automatiques de mise en quarantaine des éléments douteux. Par ailleurs, tout un chacun sera suffisamment éduqué et toutes les entreprises disposeront d'outils d'audit sophistiqués*« … Après avoir concerné les PC, puis les réseaux locaux, le client/serveur, Internet, Java, le sans fil, le champ d'action de la sécurité s'est déplacé vers les services Web. Mais pour qu'un certain équilibre soit respecté et que la sécurité du système d'information soit optimale, il convient de détruire une fois pour toutes quelques mythes tenaces qui sapent le crédit des politiques sécuritaires auprès des directions administratives et financières. **Premier mythe:** ***on peut toujours investir plus en matière de sécurité tout en continuant à investir sur le reste*** Hélas, non, l'investissement sécuritaire n'est pas un tonneau des Danaïdes. D'ailleurs, lorsque l'on scrute le secteur industriel, on s'aperçoit que la part d'investissement qui lui est dédiée n'excède pas 3 à 5 % du budget informatique global (chiffres 2004) – il s'agit ici d'entreprises sensibilisées au sujet, celles qui savent apprécier et gérer le niveau de risques, et qui ne connaissent pas de problèmes majeurs. Cette proportion n'inclut toutefois ni les salaires versés aux équipes ni les services acquis. **Deuxième mythe:** ***la sécurité est un voyage, pas une destination*** En réalité, sans objectifs précis, contrairement à de nombreux responsables sécurité qui courent après le dernier IDS ou la toute nouvelle technologie biométrique, il n'y pas de sécurité efficace. Il existe de vrais problèmes en matière de sécurité, mais il se présente aussi et surtout une foule de faux problèmes tenant plus à des phénomènes de mode qu'à autre chose. **Troisième mythe:** ***il est normal qu'un logiciel soit bogué*** Et bien non. C'est tout sauf normal! Est-ce qu'on admet qu'un produit blanc ou brun présente des défectuosités ? Non ! Il devrait en être de même, de plus en plus, en matière d'informatique. Le système des mises à jour permanentes est d'ailleurs le premier pas vers ce zéro défaut (ou zéro faille). **Quatrième mythe:** ***l'année prochaine sera l'année de…*** Qui n'a pas entendu de tels propos ? C'est ainsi que certaines technologies, considérées comme prometteuses, sont tout simplement devenues obsolètes avant même de s'être répandues dans les entreprises. Il en est ainsi des systèmes de détection d'intrusion. D'autres

technologies n'atteindront apparemment leur maturité que dans deux à cinq ans. C'est le cas notamment du filtrage des 'spams', de l'inspection fouillée des paquets de données par les coupe-feux, des outils de conformité, des MSSP, de la gestion des droits numériques dans l'entreprise, de la gestion des identités et des opérations nécessitant des clés publiques… D'autres technologies ne seront pas mûres avant une dizaine d'années. Ainsi des groupements de confiance en matière informatique, idem de la biométrie. **Cinquième mythe:** ***les réglementations n'ont pas d'importance, les comptables si!*** Il n'empêche que la plupart des entreprises font dorénavant tout pour se mettre en conformité avec la réglementation financière américaine Sarbanes-Oxley et que c'est le branle-bas de combat dans le Landerneau financier avec la prochaine prise en compte de la réglementation Bâle II. De toute façon, les entreprises ont besoin de sécurité. Mais ce que veulent désormais vraiment les sociétés, c'est l'avénement d'une plate-forme unifiée de sécurité qui soit directement intégrée dans le système d'exploitation de leur architecture informatique. L'idéal serait une plate-forme qui s'occupe aussi bien de l'utilisateur interne que du nomade, et qui puisse communiquer avec les plates-formes de sécurité des autres partenaires de l'entreprise étendue - fournisseurs et clients. Une plate-forme qui gère les antivirus, assume l'administration des 'patchs', gère les coupe-feux des postes clients tout en délimitant un périmètre de sécurité et en assurant des fonctionnalités de réseau privé virtuel. **En conclusion: une question de bon sens!** Bref, tout est d'abord une question de bon sens (ce qui manque, hélas, le plus). Dans la plupart des cas, il n'est nul besoin de signatures électroniques individuelles, de clés quantiques pour les échanges, de détection d'intrusion passive, de biométrie, de gestion des droits numériques au niveau du groupe (en dehors de groupes de travail), de procédures tenant sur un demi-millier de pages, de mots de passe par défaut… pour ne citer que quelques « tartes à la crème » parmi les plus répandues. En revanche, sur les réseaux sans fil, on se hâtera d'implanter le 802.1X, d'assurer la quarantaine et le confinement des documents douteux, de gérer les vulnérabilités, de disposer d'un système de cryptage standardisé et sophistiqué, d'avoir un portail SSL/TLS, de gérer automatiquement les mots de passe, d'éliminer tout le 'spam' possible et de disposer d'un plan de continuité d'activité. Faites le test et cochez parmi ces deux listes ce que vous avez mis (ou non) en oeuvre. Certains seront surpris du résultat. On ne saurait conclure une telle démystification sans un minimum dde précautions. Nous retiendrons **six recommandations**: 1? si possible, achetez des produits déjà sécurisés 2? n'ouvrez pas grande la porte de l'entreprise à des individus auxquels vous ne pouvez pas vous fier (autrement dit, n'embauchez pas n'importe qui!) 3? arrêtez de compter les attaques et commencez à boucher les trous 4? virez les solutions de sécurité qui se sont avérées passables et remplacez-les par des solutions qui ont fait leurs preuves chez d'autres, avant de consacrer le moindre budget au tout dernier 'gimmick' 5? pensez aussi à protéger vos clients ou partenaires: à leur tour ils feront tout pour protéger votre activité 6? enfin et surtout, consolidez vos investissements sécurité pour ne retenir que l'essentiel, que ce qui s'avère vraiment efficace!