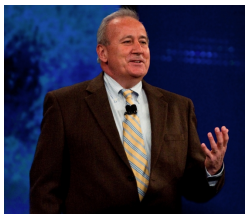

La célèbre phrase de Ken Olson me revient à l'esprit : « Il n'existe aucune raison pour que quiconque désire un ordinateur chez lui ». Donc, totalement conscient de la déraison de mon entreprise, je prends de nouveau ma plume (ou en l'occurrence mon clavier) pour partager certaines de mes idées sur 2013 et les présages pour 2014.2013 marque un tournant dans l'évolution des technologies informatiques (SaaS, IaaS, etc.)...:

IDC a bien décrit l'évolution de l'informatique au cours des 40 dernières années en trois ères ou plates-formes. Après les ères du mainframe et du client/serveur dans les années 70 et 90 est arrivée la troisième plate-forme, dont l'origine remonte à 2007 avec le lancement de l'iPhone. Au sein de cette troisième plate-forme, le cloud, les Big Data et le Web social constituent les environnements majeurs et les appareils mobiles les terminaux. Elle a donc vite gagné en maturité depuis sa naissance.

2013 n'échappe pas à la règle. Le modèle SaaS (Software as a Service) est de plus en plus adopté et cet essor poursuit son accélération. L'adoption du modèle IaaS (Infrastructure as a Service) suit une même courbe de croissance. Avec le développement du bureau virtuel, les entreprises exigent de plus en plus un accès à des applications métier sur des appareils mobiles.

... mais aussi dans l'évolution de la sécurité informatique (défis de la mobilité, révélations sur la NSA, etc.)

Toutefois, une récente étude internationale parrainée par EMC a révélé que deux des principaux problèmes de sécurité identifiés par les services informatiques concernent l'accès tiers aux applications de l'entreprise (43 %) et l'accès mobile aux réseaux (40 %), montrant le besoin de technologies plus sophistiquées et de solutions de sécurité intelligentes à l'ère de la troisième plate-forme.

Dans ce contexte, l'un des sujets majeurs et récurrents en 2013 était l'interaction de la sécurité et la confidentialité à la lumière des révélations sur la NSA.

A quoi s'attendre en 2014 ?

Je vais maintenant scruter ma boule de cristal et livrer mes cinq principaux pronostics pour 2014 :

1. Le BYOD a la une en 2013 - la nouveauté pour 2014 est le BYOI. L'une des tendances phares de la troisième plate-forme a été la consumérisation de l'informatique, les entreprises accordant plus de liberté aux employés dans l'accès à ses ressources et aux données via leurs appareils personnels (BYOD). La prochaine étape de cette tendance sera la consumérisation

de l'identité, les employés demandant de plus en plus un système d'identification plus simple et intégré pour tous les modes d'utilisation de leurs périphériques. L'identité sera moins confiée à des tiers et toujours plus étroitement détenue et gérée par les individus, qu'ils pourront gérer comme ils le font déjà avec leurs propres appareils. 2014 marquera le début du BYOI (Bring -and control - Your Own Identity).

2. Le retour de la menace interne – La menace interne est un problème dont l'acuité fait les montagnes russes dans notre conscience collective. Les évènements de l'an dernier ont de nouveau focalisé fortement l'attention sur ce problème. En 2014, nous allons voir les entreprises considérer plus soigneusement la menace interne et prendre des mesures pour se protéger contre le risque de dommages importants en termes de ventes, de marque, voire de continuité d'activité.

3. Le futur du cloud s'ennuage – Alors que les clouds publics ont présenté un intérêt grandissant pour certaines applications depuis quelques années, les révélations sur la NSA et les questions sur la sécurité de ces clouds pourraient changer la donne. Nous constatons que des entreprises repensent leurs stratégies de clouds publics et même que des États en Europe prônent la balkanisation de ces clouds afin qu'ils reflètent les frontières nationales. Il faut s'attendre à ce que les fournisseurs de clouds publics revoient résolument la sécurité de leurs clouds pour se démarquer des concurrents et éviter les risques pour leur activité. Les acteurs de la sécurité du cloud devraient connaître une année record en 2014.

4. 2014 va marquer un tournant dans le malware mobile – Les entreprises offrant un accès mobile élargi à leurs applications métier stratégiques ou leurs données sensibles et le grand public adoptant de plus en plus la banque mobile, il est évident que le malware mobile va gagner rapidement en sophistication et omniprésence en 2014. Nous avons déjà observé ce double renforcement au cours des derniers mois et, à nos yeux, il ne s'agit que du début d'une immense vague. Nous allons assister à des attaques d'envergure avant que les entreprises et le grand public ne réalisent le risque et ne prennent des mesures adéquates pour l'atténuer. Bien que certains organismes souhaitent relativiser les risques encourus, il est probablement judicieux de tout de même se préparer.

5. L'Internet des objets – Comme noté lors de Black Hat l'été dernier, la future cible du hacking n'est pas le PC ou même les appareils mobiles, mais bel et bien les objets connectés, c'est-à-dire le réseau grandissant de périphériques qui détectent et pilotent des systèmes réels. Des voitures aux appareils médicaux en passant par les réseaux électriques intelligents, nous allons constater un nombre croissant d'attaques plus sophistiquées ciblant l'Internet des objets. Ces attaques seront par ailleurs plus destructrices et ne se contenteront pas de perturber l'activité.

Il existe, bien entendu, de nombreuses autres tendances intéressantes – De l'émergence de nouveaux malwares, à l'engouement pour le Bitcoin et au partage accru d'informations sur les menaces entre les entreprises et les secteurs. Autant dire que 2014 sera une autre année clé en termes de sécurité. Alors que des défis majeurs nous attendent assurément, mes conversations avec des clients, partenaires et confrères me confortent plus que jamais dans ma confiance en notre capacité à les relever résolument. Au final, je pense et j'espère que

l'adoption croissante par les professionnels d'un modèle de sécurité intelligent, exploitant les Big Data, une analyse approfondie et des contrôles intégrés, dynamiques, pour fournir une sécurité contextuelle, va permettre aux entreprises de relever avec succès les défis qu'elles peuvent rencontrer à présent et ceux à venir. Nous allons créer ensemble un monde numérique de confiance.