

Art Coviello, PrÃ©sident de RSA, partage ses prÃ©dictions pour 2014

Internet

PostÃ© par : JPilo

PubliÃ©e le : 23/1/2014 11:00:00

La cÃ©lÃ©bre phrase de Ken Olson me revient Ã l'esprit : « *Il n'existe aucune raison pour que quiconque dÃ©sire un ordinateur chez lui* ». Donc, totalement conscient de la dÃ©raison de mon entreprise, je prends de nouveau ma plume (ou en l'occurrence mon clavier) pour partager certaines de mes idÃ©es sur 2013 et les prÃ©visions pour 2014.

2013 marque un tournant dans l'Ã©volution des technologies informatiques (SaaS, IaaS, etc.)

IDC a bien dÃ©crit l'Ã©volution de l'informatique au cours des 40 derniÃ©res annÃ©es en trois Ã©tapes ou plates-formes. AprÃ©s les Ã©tapes du mainframe et du client/serveur dans les annÃ©es 70 et 90 est arrivÃ©e la troisiÃ©me plate-forme, dont l'origine remonte Ã 2007 avec le lancement de l'iPhone.

Au sein de cette troisiÃ©me 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 gagnÃ© en maturitÃ© depuis sa naissance.

2013 n'Ã©chappe pas Ã la rÃ©gle. Le modÃ©le SaaS (Software as a Service) est de plus en plus adoptÃ© et cet essor poursuit son accÃ©lÃ©ration. L'adoption du modÃ©le IaaS (Infrastructure as a Service) suit une mÃªme courbe de croissance.

Avec le dÃ©veloppement du bureau virtuel, les entreprises exigent de plus en plus un accÃ©s Ã des applications mÃ©tier sur des appareils mobiles.

â mais aussi dans l'Ã©volution de la sÃ©curitÃ© informatique (dÃ©fis de la mobilitÃ©, rÃ©vÃ©lations sur la NSA, etc.)



Toutefois, une rÃ©cente Ã©tude internationale parrainÃ©e par EMC a rÃ©vÃ©lÃ© que deux des principaux problÃ©mes de sÃ©curitÃ© identifiÃ©s par les services informatiques concernent l'accÃ©s tiers aux applications de l'entreprise (43 %) et l'accÃ©s mobile aux rÃ©seaux (40 %), montrant le besoin de technologies plus sophistiquÃ©es et de solutions de sÃ©curitÃ© intelligentes Ã© l'Ã©chelle de la troisiÃ©me plate-forme.

Dans ce contexte, l'un des sujets majeurs et rÃ©currents en 2013 Ã©tait l'interaction de la sÃ©curitÃ© et la confidentialitÃ© Ã© la lumiÃ©re des rÃ©vÃ©lations 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 nouveautÃ© pour 2014 est le BYOI. L'une des tendances phares de la troisiÃ©me plate-forme a Ã©tÃ© la consommation de l'informatique, les entreprises accordant plus de libertÃ© aux employÃ©s dans l'accÃ©s Ã© leurs ressources et aux donnÃ©es via leurs appareils personnels (BYOD).

La prochaine Ã©tape de cette tendance sera la consommation de l'identitÃ©, les employÃ©s demandant de plus en plus un systÃ©me d'identification plus simple et intÃ©grÃ© pour tous les modes d'utilisation de leurs pÃ©riphÃ©riques.

L'identitÃ© sera moins confiÃ©e Ã© des tiers et toujours plus Ã©troitement dÃ©tenue et gÃ©rÃ©e par les individus, qu'ils pourront gÃ©rer comme ils le font d'Ã©jÃ© avec leurs propres appareils. 2014 marquera le dÃ©but du BYOI (Bring -and control - Your Own Identity).

2. Le retour de la menace interne â La menace interne est un problÃ©me dont l'acuitÃ© fait les montagnes russes dans notre conscience collective. Les Ã©vÃ©nements de l'annÃ©e derniÃ©re ont de nouveau focalisÃ© fortement l'attention sur ce problÃ©me.

En 2014, nous allons voir les entreprises considÃ©rer plus soigneusement la menace interne et prendre des mesures pour se protÃ©ger contre le risque de dommages importants en termes de ventes, de marque, voire de continuitÃ© d'activitÃ©.

3. Le futur du cloud s'ennuige â Alors que les clouds publics ont prÃ©sentÃ© un intÃ©rÃ©t grandissant pour certaines applications depuis quelques annÃ©es, les rÃ©vÃ©lations sur la NSA et les questions sur la sÃ©curitÃ© de ces clouds pourraient changer la donne.

Nous constatons que des entreprises repensent leurs stratÃ©gies de clouds publics et mÃªme que des Ã©tats en Europe prÃ©nent la balkanisation de ces Clouds afin qu'ils reflÃ©tent les frontiÃ©res nationales. Il faut s'attendre Ã© ce que les fournisseurs de clouds publics revoient rÃ©solument la sÃ©curitÃ© de leurs clouds pour se dÃ©marquer des concurrents et Ã©viter les risques pour leur activitÃ©. Les acteurs de la sÃ©curitÃ© du Cloud devraient connaÃ©tre une annÃ©e record en 2014.

4. 2014 va marquer un tournant dans le malware mobile â Les entreprises offrant un accÃ©s mobile Ã© leurs applications mÃ©tier stratÃ©giques ou leurs donnÃ©es sensibles et le grand public adoptant de plus en plus la banque mobile, il est Ã©vident que le malware mobile va gagner rapidement en sophistication et omniprÃ©sence en 2014.

Nous avons d'Ã©jÃ© observÃ© ce double renforcement au cours des derniers mois et, Ã© nos yeux, il ne s'agit que du dÃ©but d'une immense vague. Nous allons assister Ã© des attaques d'envergure avant que les entreprises et le grand public ne rÃ©alisent le risque et ne prennent des mesures adÃ©quates pour l'attÃ©nuer. Bien que certains organismes souhaitent relativiser les risques encourus, il est probablement judicieux de tout de mÃªme se prÃ©parer.

5. L'Internet des objets Comme noté lors de Black Hat l'année dernière, 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.

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.

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 intelligents, dynamiques, pour fournir une sécurité contextuelle, va permettre aux entreprises de relever avec succès les défis qu'elles peuvent rencontrer présent et ceux à venir. Nous allons créer ensemble un monde numérique de confiance.

À