SÃ©curisation de lâ□□Internet des objets, des systÃ¨mes dâ□□exploitation mobiles et du Cloud

Internet

PostÃ© par : JPilo
PubliÃ©e le : 15/1/2014 11:00:00

AprÃ¨s une annÃ©e riche en cyber-attaques et en scandales dâ□□espionnage, LogRhythm, fournisseur de solutions de dÃ©tection, de dÃ©fense et de rÃ©action face aux cyber-menaces, fait aujourdâ□□hui lâ□□Ã©tat des lieux de ce qui attend les entreprises en matiÃ¨re de cyber-menaces en 2014 et des grands dÃ©fis quâ□□elles devront relever.

2014 sera marquÃ©e par un intÃ©rÃªt croissant pour lâ□□exfiltration de donnÃ©es sur le rÃ©seau, le plus souvent Ã des fins commerciales, en raison de la disponibilitÃ© des donnÃ©es stockÃ©es dans le cloud mais aussi du web profond (partie du web non-indexÃ©e par les moteurs de recherche). Dans cet environnement, lâ□□exfiltration de donnÃ©es deviendra presque imperceptible et des analyses comportementales bien plus avancÃ©es seront nÃ©cessaires pour pouvoir les dÃ©tecter.

Internet des objets et systÃ¨mes dâ□□exploitation mobiles : des cibles grandissantes

Si lâ□□Internet des objets est en plein essor avec de plus en plus de terminaux connectÃ©s tels que les tÃ©lÃ©visions intelligentes ou autres appareils utilisÃ©s au quotidien, ce phÃ©nomÃ¨ne soulÃ¨ve une vÃ©ritable problÃ©matique en matiÃ¨re de sÃ©curitÃ©.

En effet, les hackers sont susceptibles de prendre le contrÃ´le de ces objets et sâ□□introduire sur le rÃ©seau en ciblant ces systÃ¨mes. Par ailleurs, Microsoft ayant mis fin au support Windows XP, il faut Ã©galement sâ□□attendre Ã des attaques massives sur ce systÃ¨me dâ□□exploitation puisquâ□□il ne bÃ©nÃ©ficiera bientÃ´t plus dâ□□aucune mise Ã jour que ce soit en termes dâ□□ergonomie ou bien de sÃ©curitÃ©.

2014 sera en outre une annÃ©e riche pour les systÃ¨mes dâ□□exploitation mobiles. Alors quâ□□AndroÃ¯d a dominÃ© le marchÃ© en 2013, Windows Mobile de Microsoft enregistre une demande croissante, tout comme dâ□□autres plateformes open source telle que Tizen, Boot-to-Gecko de Mozilla et Ubuntu, qui devraient reprendre des parts de marchÃ© Ã AndroÃ¯d.

Cette guerre entre les systÃ¨mes dâ□□exploitation mobiles va prendre de lâ□□ampleur et, en raison de la rapiditÃ© de dÃ©veloppement â□□ essentielle sur ce marchÃ©, pourrait gÃ©nÃ©rer certaines vulnÃ©rabilitÃ©s au sein des OS et des applications en mesure de se rÃ©pandre trÃ¨s rapidement, laissant ainsi la porte grande ouverte aux hackers.

RÃ¨glementation plus stricte et conformitÃ© : prioritÃ© du gouvernement et des entreprises

Cette annÃ©e, lâ□□Etat et les organismes en charge de la rÃ©gulation des normes relatives Ã la sÃ©curitÃ© informatique interviendront de plus en plus. En 2013, nous avons dÃ©jÃ vu certains gouvernements pratiquer la politique de la carotte et du bÃ¢ton pour garantir le respect de la rÃ©glementation.

Les Etats-Unis par exemple ont vu augmenter les sanctions pour le non-respect de la loi rÃ©gissant la cyber-sÃ©curitÃ©. Il devrait en Ãªtre de mÃªme en 2014 puisque le nombre de brÃ¨ches de sÃ©curitÃ© Ã travers le monde menaÃ§ant les donnÃ©es personnelles des consommateurs, des patients ou encore celles des cartes de crÃ©dit pour nâ□□en citer que quelques-unes, ne va pas rÃ©duire.

Lâ□□Europe nâ□□est, quant Ã elle, pas encore habilitÃ©e Ã appliquer de telles mesures mais elle y travaille puisque lâ□□obligation de signalement de cyber-attaques et la mise en place de sanctions dans le cadre de la rÃ©glementation europÃ©enne sont toujours en cours de discussion au Parlement europÃ©en.

En 2014, la crÃ©ation de motivations financiÃ¨res pour sensibiliser les entreprises et les gouvernements devrait sâ□□accÃ©lÃ©rer, dans la mesure oÃ¹ les gouvernements et les organismes de rÃ©gulation sont dÃ©cidÃ©s Ã se montrer rÃ©actifs face Ã ces problÃ©matiques de sÃ©curitÃ©.

En ce qui concerne la conformitÃ©, elle ne se pourra plus se limiter Ã un systÃ¨me de cases Ã cocher pour les entreprises. Elles vont devoir se conformer Ã un certain nombre de rÃ¨gles beaucoup plus strictes en matiÃ¨re de sÃ©curitÃ©. En ce dÃ©but dâ□□annÃ©e, les recommandations, telles que lâ□□adoption de la version 3.0 de la norme de sÃ©curitÃ© des donnÃ©es PCI DSS, sont nombreuses et les organisations devront adopter une attitude beaucoup plus proactive pour faire face aux cyber-menaces.

Â« *La faÃ§on dont les entreprises perÃ§oivent la conformitÃ© va changer : elle sera plus considÃ©rÃ©e comme un effort nÃ©cessaire quotidien et permanent plutÃ´t quâ□□une simple obligation. Lâ□□anticipation des attaques est aujourdâ□□hui essentielle car il sâ□□agit de savoir "quand", et non plus "si", les organisations sont ciblÃ©es par des attaques, mÃªme si elles sont "conformes" sur le papier,* Â» dÃ©clare **Jean-Pierre Carlin**, Directeur Europe du Sud chez **LogRhythm**.

Impact de lâ□□Ã©volution du cloud sur la sÃ©curitÃ©

Alors que les utilisateurs du Cloud se sont dâ□□abord focalisÃ©s sur lâ□□accessibilitÃ© et la productivitÃ© des services, la sÃ©curitÃ© dans le Cloud va devenir une question prioritaire cette annÃ©e.

Ce qui signifie notamment pour les entreprises dâ□□avoir une meilleure visibilitÃ© des API pour contrÃ´ler les activitÃ©s et les Ã©vÃ©nements, comme par exemple le service Amazon CloudWatch qui offre une surveillance pour les ressources du Cloud Amazon Web Service ainsi que sur les applications utilisÃ©es par les clients.

Approche hybride de la gestion de la sÃ©curitÃ© dans les entreprises

Enfin, en 2014, les Services de SÃ©curitÃ© ManagÃ©s (MSS) continueront de se dÃ©velopper mais il sâ□□agira dâ□□une croissance progressive. En effet, les clients sont en train dâ□□apprÃ©hender la faÃ§on dont ils peuvent tirer profit de ces offres externes tout en conservant une partie de la gestion de la sÃ©curitÃ© en interne.

Les entreprises vont donc adopter une approche MSS hybride, entre partenaire de services managÃ©s et ressources propres, basÃ©e sur les besoins en termes de sÃ©curitÃ© et la capacitÃ© dâ□□investissement.