LogRhythm : En matiÃ¨re de sÃ©curitÃ© informatique pour l'annÃ©e 2013
Info
PostÃ© par : JulieM
PubliÃ©e le : 20/11/2012 11:30:00

Anticiper les menaces cybercriminelles de lâ□□annÃ©e prochaine â□□ prÃ©dictions de LogRhythm

Lâ□□annÃ©e 2012 nâ□□a hÃ©las pas marquÃ© la fin de la crise de la violation des donnÃ©es, et les entreprises ne parviennent toujours pas Ã prÃ©server lâ□□intÃ©gritÃ© des donnÃ©es qui leur ont Ã©tÃ© confiÃ©es. On peut citer par exemple les cas dâ□□intrusion chez Yahoo et LinkedIn. Jean-Pierre Carlin, directeur lâ□□Europe du Sud et Benelux chez LogRhythm, donne ses prÃ©dictions pour 2013, et Ã©voque deux menaces qui sâ□□annoncent inÃ©vitables : la sÃ©curitÃ© des grands volumes de donnÃ©es â□□ Â« Big Data Â» â□□ et les attaques dâ□□infrastructures nationales critiques.

SÃ©curitÃ© du Â« Big Data Â»

Â« *Les grosses quantitÃ©s de donnÃ©es resteront sans aucun doute lâ□□un des principaux dÃ©fis des entreprises au cours de lâ□□annÃ©e Ã venir. Dâ□□un point de vue sÃ©curitaire, le seul moyen permettant dâ□□identifier immÃ©diatement la totalitÃ© des cyber-menaces au sein de nos rÃ©seaux IT de plus en plus complexes est dâ□□avoir une visibilitÃ© Ã 360 degrÃ©s de chaque donnÃ©e gÃ©nÃ©rÃ©e. Les tendances technologiques actuelles favorisant largement la croissance des flux de donnÃ©es, jamais le besoin dâ□□une visibilitÃ© proactive, continue et granulaire de toute lâ□□activitÃ© nâ□□a Ã©tÃ© aussi marquÃ©* . Â»

Â« *En effet, ceci permet aux organisations de mieux dÃ©finir leur activitÃ© IT normale et quotidienne, aux diffÃ©rents niveaux de leur structure IT, et leur permet de dÃ©tecter en temps rÃ©el toute activitÃ© anormale par rapport Ã leur comportement de base. Bref, au lieu de fuir la tÃ¢che consistant Ã analyser les gros volumes de donnÃ©es, les organisations doivent d'abord comprendre les avantages de sÃ©curitÃ© que cette intelligence peut fournir et reconnaÃ®tre que l'automatisation est la seule faÃ§on de naviguer efficacement dans ce labyrinthe de donnÃ©es et de sÃ©curiser les rÃ©seaux IT les plus vastes et les plus complexes.* Â»

Attaques dâ□□infrastructures nationales critiques

Â« *Au cours de lâ□□annÃ©e derniÃ¨re, les cyber-attaques, qui consistaient auparavant Ã voler des informations et des donnÃ©es financiÃ¨res, ont pris une tournure inquiÃ©tante en visant Ã prÃ©sent des systÃ¨mes critiques dans le but de causer de vÃ©ritables prÃ©judices mondiaux. Les cyber-attaques Ã©tant toujours plus frÃ©quentes et sophistiquÃ©es, alors que notre monde devient de plus en plus dÃ©pendant de la technologie (Internet rÃ©gissant par exemple de nombreux aspects de la vie quotidienne, des systÃ¨mes de navigation aux distributeurs dâ□□argent, en passant par les compteurs intelligents et autres infrastructures), lâ□□annÃ©e Ã venir verra ces vulnÃ©rabilitÃ©s augmenter.* Â»

Â« *La plupart des infrastructures nationales existantes ayant Ã©tÃ© dÃ©veloppÃ©es avant lâ□□avÃ¨nement de lâ□□Internet, leur systÃ¨me de sÃ©curitÃ© se limite souvent aux actifs physiques. Câ□□est pour cette raison que les organisations doivent adopter des plateformes de sÃ©curitÃ© intelligentes, capables dâ□□assurer une corrÃ©lation continue des Ã©vÃ¨nements pour la dÃ©tection prÃ©coce des menaces, dâ□□effectuer des analyses poussÃ©es pour comprendre l'impact et l'origine des attaques, et de dÃ©tecter les intrusions ou les anomalies les plus discrÃ¨tes avant que celles-ci ne deviennent un plus gros problÃ¨me. AprÃ¨s tout, vous ne*

pouvez combattre que ce que vous voyez. Câ□□est la seule faÃ§on de rÃ©agir et de contrer rapidement et intelligemment tout risque potentiel en temps rÃ©el. Â»