Et si l'on parlait de Lâ□□avÃ¨nement de la Security Intelligence

SÃ©curitÃ©

PostÃ© par : JerryG
PubliÃ©e le : 30/6/2014 15:00:00

Selon une Ã©tude rÃ©cente du cabinet dâ□□analyse IDC, les entreprises franÃ§aises sont de plus en plus prÃ©occupÃ©es par les menaces de sÃ©curitÃ© et comptent bien investir dans ce sens au cours des prochaines annÃ©es.

Les attaques rÃ©centes portÃ©es Ã lâ□□encontre de grandes entreprises telles quâ□□Orange ou Dominoâ□□s Pizza ne font quâ□□accentuer la prise en considÃ©ration des risques liÃ©s au vol de donnÃ©es personnelles : non seulement dâ□□un point de vue financier, mais aussi en raison de lâ□□impact sur la rÃ©putation de lâ□□entreprise.

Cette Ã©tude indique toutefois un certain dÃ©calage entre les craintes des RSSI et les politiques de sÃ©curitÃ© appliquÃ©es. Si la mobilitÃ© reprÃ©sente un risque pour 91% des entreprises interrogÃ©es, seules 75% disposent dâ□□une solution de sÃ©curitÃ© dÃ©diÃ©e.

En ce qui concerne les nouvelles tendances liÃ©es aux rÃ©seaux sociaux par exemple, dâ□□autres contradictions apparaissent : 72% des entreprises considÃ¨rent toujours les rÃ©seaux sociaux comme risquÃ©s, mais seulement 60% dâ□□entre elles disposent dâ□□outils de filtrage et 34% dispensent des formations de sensibilisation auprÃ¨s des employÃ©s.

Pour rÃ©pondre Ã des besoins prÃ©cis de sÃ©curitÃ© en matiÃ¨re de mobilitÃ©, dâ□□accÃ¨s aux rÃ©seaux, de transfert de donnÃ©es, etc., les organisations disposent de nombreuses solutions dÃ©diÃ©es. Cependant, dans un contexte oÃ¹ les cyber-attaques deviennent plus sophistiquÃ©es et les hackers plus expÃ©rimentÃ©s, câ□□est une stratÃ©gie globale consacrÃ©e Ã la sÃ©curitÃ© des donnÃ©es qui doit impÃ©rativement Ãªtre mise en place au sein de chaque organisation.

Mais chaque entreprise est diffÃ©rente et ses besoins en matiÃ¨re de sÃ©curitÃ© varient en fonction des infrastructures, voire de lâ□□activitÃ© mÃªme de lâ□□entreprise. Dâ□□aprÃ¨s IDC, une nouvelle alternative en matiÃ¨re de protection de donnÃ©es se prÃ©sente : le Big Data et lâ□□analytique.

Jean-Pierre Carlin, Directeur Europe du Sud chez LogRhythm, a fait les commentaires suivants :

Â« *Les entreprises savent aujourdâ□□hui dÃ©tecter et empÃªcher les attaques les plus basiques, cependant, les hackers font preuve dâ□□autant de dynamisme pour sâ□□introduire par tous les moyens sur les rÃ©seaux dâ□□entreprise, que les Ã©diteurs pour dÃ©tecter et parer ces attaques. Nous savons que la question nâ□□est plus de savoir "si" une menace pourra passer outre les systÃ¨mes de sÃ©curitÃ©, mais "quand". Et câ□□est Ã ce moment que lâ□□analytique entre en jeu.*

Si les mÃ©thodes de dÃ©tection traditionnelles ont prouvÃ© leurs limites, la combinaison des rapports dâ□□analyses de lâ□□ensemble des donnÃ©es de lâ□□entreprise permet une visibilitÃ© accrue de lâ□□activitÃ© sur les rÃ©seaux.

En termes de solution, le SIEM â□□ qui collecte la totalitÃ© des logs et journaux dâ□□activitÃ©s du systÃ¨me dâ□□information â□□ apporte une rÃ©ponse concrÃ¨te aux problÃ©matiques globales de sÃ©curitÃ© : grÃ¢ce Ã la collecte des logs en temps rÃ©el, aux analyses comportementales et Ã la corrÃ©lation des donnÃ©es, toute anomalie est repÃ©rÃ©e afin dâ□□Ãªtre aussitÃ´t contrÃ´lÃ©e. Ainsi, chaque incident peut-Ãªtre vÃ©rifiÃ© en temps rÃ©el et permettre une rÃ©ponse immÃ©diate en cas de vÃ©ritable menace.

Cette mÃ©thode de dÃ©tection automatisÃ©e et en temps rÃ©el peut Ãªtre dÃ©finie comme de la Security Intelligence, un concept qui tend vers des solutions dotÃ©e dâ□□intelligence artificielle, basÃ© sur les solutions SIEM de nouvelle gÃ©nÃ©ration. GrÃ¢ce aux Ã©volutions constantes dans ce domaine, notamment en termes de fonctionnalitÃ©s et de facultÃ©s dâ□□analyse automatique, nous pouvons espÃ©rer que les entreprises puissent enfin Ãªtre Ã lâ□□abri des cyber-attaques les plus avancÃ©es. Â»