SÃ©curitÃ© : Big Data et la sÃ©curitÃ© informatique

SÃ©curitÃ©

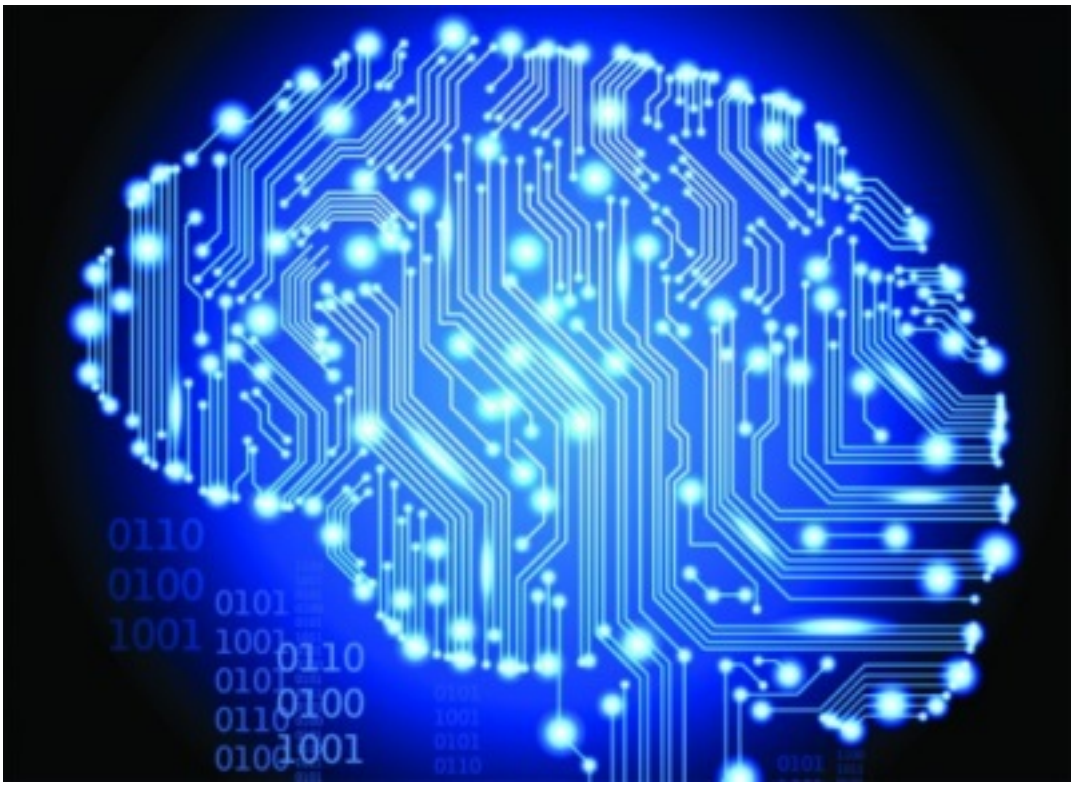
PostÃ© par : JPilo

PubliÃ©e le : 20/3/2014 13:30:00

Le cycle de vie de la sÃ©curitÃ© informatique repose aujourdâ□□hui sur deux Ã©tapes principales. Dans un premier temps, lâ□□entreprise se protÃ¨ge contre les menaces connues â□□ virus, malwares, etc. Ce premier niveau de sÃ©curitÃ© a Ã©tÃ© adoptÃ© par la totalitÃ© des entreprises aujourdâ□□hui. Il est mÃªme devenu une commoditÃ©.

Dans un second temps, lâ□□entreprise sâ□□efforce dâ□□identifier et de se protÃ©ger en temps rÃ©el contre des menaces inconnues, notamment via des technologies de Â« sandboxing Â». Celles-ci exÃ©cutent le code dans un environnement contrÃ´lÃ© afin de lâ□□interprÃ©ter et de dÃ©cider sâ□□il est malicieux ou lÃ©gitime. Ici encore, la plupart des entreprises commencent Ã sâ□□Ã©quiper.

Mais aujourdâ□□hui, la question nâ□□est plus de savoir si son entreprise va Ãªtre attaquÃ©e, mais de savoir quand et comment. Et de ce fait, ces deux Ã©tapes sont insuffisantes pour offrir une protection rÃ©ellement efficace... Une troisiÃ¨me Ã©tape consiste Ã Ã©valuer lâ□□impact que la menace dÃ©tectÃ©e a eu sur lâ□□infrastructure et implique donc que lâ□□entreprise ait la capacitÃ© de remonter le passÃ©.



Les technologies en place aujourdâ□□hui nâ□□offrent quâ□□une vision parcellaire, alors que les entreprises ont besoin de disposer dâ□□une visibilitÃ© complÃ¨te et exacte sur tout ce qui transite dans leurs rÃ©seaux. Et câ□□est ici que les big data interviennent.

Una analogie aide Ã mieux comprendre le principe. Un policier arrive sur une scÃ¨ne de crime. Il nâ□□y a pas de tÃ©moin.

Il cherche donc si dans le quartier, une camÃ©ra de vidÃ©oprotection nâ□□aurait pas enregistrÃ© les faits. Sâ□□il en trouve une, il devient capable de visionner la scÃ¨ne de crime et dâ□□accumuler les preuves afin de confondre le ou les auteur(s).

Câ□□est exactement ce dont ont besoin les entreprises en matiÃ¨re de sÃ©curitÃ© informatique : enregistrer le trafic qui transite par leurs rÃ©seaux pour traquer le cheminement de la menace quâ□□on vient de repÃ©rer et dÃ©velopper des mesures en consÃ©quence.

Au-delÃ de la capacitÃ© Ã rejouer des scÃ¨nes antÃ©rieures, que lâ□□on appellera Â« sÃ©curitÃ© analytique Â», le systÃ¨me permet parallÃ¨lement de confirmer la conformitÃ© du systÃ¨me dâ□□information.

Par exemple, lâ□□entreprise est lÃ©galement tenue dâ□□empÃªcher la fuite de numÃ©ros de cartes bleues, elle doit donc savoir si des informations ont dÃ©jÃ fuitÃ© et Ãªtre capable de rÃ©aliser ce type dâ□□analyse post-mortem.

Mais la collecte et le stockage dâ□□un tel volume de donnÃ©es nâ□□est pas si simple. Lâ□□entreprise doit dans un premier temps fixer les rÃ¨gles de collecte et de conservation, puis analyser ces Ã©normes volumes de donnÃ©es pour comprendre ce qui sâ□□est passÃ© de maniÃ¨re explicite, câ□□est-Ã -dire en reconstruisant les sessions et les fichiers concernÃ©s.

La difficultÃ© consiste Ã©galement Ã analyser les volumes massifs de donnÃ©es ainsi collectÃ©s. Lâ□□entreprise a besoin de corrÃ©ler des sources extrÃªmement variÃ©es dâ□□informations, internes comme externes. Et surtout elle doit savoir quelles questions se poser. Si elles ne sont Ã©videmment pas une fin en soi, les big data vont aider lâ□□entreprise Ã renforcer ses trois niveaux de protection.

Leur intÃ©gration dans lâ□□architecture globale de sÃ©curitÃ© va permettre non seulement de remonter Ã la source de la menace et de faire en sorte quâ□□elle ne puisse pas frapper Ã nouveau, mais Ã©galement de rapprocher les diffÃ©rentes Ã©quipes en charge des trois niveaux de protection dont nous parlions plus haut, tout en disposant dâ□□un vue globale des risques auxquels lâ□□entreprise est confrontÃ©e.

Les entreprises ont dÃ©sormais pris conscience que quelles que soient les technologies quâ□□elles utilisent et leur degrÃ© de sophistication, elles seront un jour attaquÃ©es. Elles sont conscientes en outre que la sÃ©curitÃ© ne doit pas Ãªtre un frein mais un accÃ©lÃ©rateur de productivitÃ©.

PlutÃ´t que de chercher Ã Ã©viter Ã tout prix ce type dâ□□attaque en plaÃ§ant des barriÃ¨res gÃ©nÃ©riques qui au final perturbent leur activitÃ©, elles devraient investir dans un systÃ¨me leur permettant de comprendre comment elles ont Ã©tÃ© attaquÃ© et ce qui a Ã©tÃ© volÃ©.

Cette technologie existe aujourdâ□□hui. Elle permet de capturer le trafic, de stocker les donnÃ©es, puis les analyser et reconstruire les sessions comme elles Ã©taient lors de lâ□□attaque Ã partir dâ□□une question, par exemple : qui a utilisÃ© tel ou tel fichier ?

A lâ□□heure oÃ¹ absolument aucune entreprise ne doit se sentir protÃ©gÃ©e complÃ¨tement contre les attaques, la sÃ©curitÃ© analytique est absolument critique. Mais elle nâ□□est pleinement efficace quâ□□Ã la condition quâ□□elle soit intÃ©grÃ©e avec les solutions assurant les deux premiers niveaux de protection. Il est fondamental quâ□□elles puissent communiquer afin de sâ□□enrichir mutuellement, confirme Dominique Loiselet, Directeur GÃ©nÃ©ral France Blue Coat.