***80% des ressources financiÃ¨res de sÃ©curitÃ© sont dÃ©pensÃ©es Ã  mauvais escient***
**SÃ©curitÃ©**
PostÃ© par : JPilo
PubliÃ©e le : 2/10/2013 13:00:00

Depuis peu, les questions de sÃ©curitÃ© informatiques profitent dâ□□une popularitÃ© inÃ©dite. Malheureusement, ce succÃ¨s est surtout dÃ» Ã  lâ□□envolÃ©e du nombre dâ□□attaques, qui sâ□□accompagne en plus dâ□□une nuÃ©e de rumeurs et dâ□□informations erronÃ©es, incomplÃ¨tes ou exagÃ©rÃ©es participant Ã  la confusion gÃ©nÃ©rale. **Art Coviello**, PrÃ©sident exÃ©cutif de RSA nous en dit plus.

Pendant ce temps, les attaques les plus massives sont passÃ©es sous silence â□□ et encore, lorsquâ□□elles sont identifiÃ©es â□□ pendant des mois, si ce nâ□□est plus.

**Comment je le sais ?** Parce que jâ□□observe les rÃ©percussions tous les jours chez nos clients. Et parce jâ□□ai Ã©tÃ© dans cette position, lorsque RSA a Ã©tÃ© victime dâ□□une attaque il y a deux ans. Mais depuis, le phÃ©nomÃ¨ne nâ□□a fait que sâ□□aggraver.

Et pour cause : le terrain de jeu des cybercriminels sâ□□est Ã©tendu. Si au dÃ©but du millÃ©naire ils devaient encore se contenter de quelques points dâ□□entrÃ©es vers des pÃ©rimÃ¨tres spÃ©cifiques contrÃ´lÃ©s par firewall, ils ont aujourdâ□□hui face Ã  eux une infinitÃ© dâ□□appareils mobiles, dâ□□environnements virtualisÃ©s, de rÃ©seaux sociaux et dâ□□objets connectÃ©s pour la plupart ouverts.

***Nos ennemis sont aussi devenus plus forts.*** Au dÃ©part inexpÃ©rimentÃ©s, ils sont aujourdâ□□hui capable de camoufler et transformer leurs virus et logiciels espions pour quâ□□ils soient indÃ©tectables. Leurs cibles se multiplient et leurs mÃ©thodes se professionnalisent pendant que leurs attaques se font plus complexes et coordonnÃ©es.

Encore plus troublant, nous observons depuis peu une Ã©volution des attaques intrusive traditionnelles comme la fraude ou le vol dâ□□IP Ã  des attaques Ã  grande Ã©chelle qui ont pour

but de paralyser le systÃ¨me. Câ□□est le cas par exemple des attaques DDOS des derniers mois. Pour lâ□□instant, ces mÃ©thodes sont trÃ¨s difficiles Ã  utiliser sur Internet sans intervention manuelle. Mais lâ□□essor des appareils connectÃ©s et le passage vers le tout-IP vont largement faciliter les attaques informatiques entraÃ®nant des destructions physiques rÃ©elles.

Câ□□est pourquoi il devient urgent dâ□□agir pour amÃ©liorer la comprÃ©hension des enjeux de sÃ©curitÃ© informatique dans les organisations.

## Sans comprÃ©hension, pas de protection

En sÃ©curitÃ© informatique, 80% des ressources financiÃ¨res sont dÃ©pensÃ©es Ã  mauvais escient. Le plus souvent, elles sont consacrÃ©es Ã  la prÃ©vention des intrusions alors que nous nÃ©gligeons de dÃ©velopper notre capacitÃ© Ã  identifier et comprendre les attaques dans notre environnement. Quant Ã  la prÃ©vention des risques de pertes de donnÃ©es ou la rÃ©ponse Ã  y apporter, elle est la cinquiÃ¨me roue du carrosse.

Ironiquement, il est impossible dâ□□identifier et combler toutes les failles dâ□□une infrastructure. Essayer est donc une perte de temps et dâ□□argent.

En cas dâ□□attaque, si les informations dont nous disposons ne sont pas suffisantes ou pas pertinentes, il est impossible de comprendre le problÃ¨me et de le rÃ©gler. Au contraire, cela gÃ©nÃ¨re de lâ□□anxiÃ©tÃ© et un sentiment dâ□□impuissance contre-productifs.

***Pour adresser une menace efficacement***, il est essentiel de mettre en perspective trois Ã©lÃ©ments : le pÃ©rimÃ¨tre de lâ□□attaque, lâ□□environnement des menaces et les opportunitÃ©s de faire Ã©voluer la sÃ©curitÃ©. Pour faciliter le croisement dâ□□informations, nous faisons la promotion dâ□□un nouveau modÃ¨le de sÃ©curitÃ© intelligente.

Pour une efficacitÃ© optimale, il est important de pouvoir analyser des informations internes et externes. Comprendre les vulnÃ©rabilitÃ©s et Ã©valuer la probabilitÃ© dâ□□une attaque demandent une comprÃ©hension des enjeux et contraintes internes comme externes. Il est donc essentiel de mieux partager lâ□□information. Et aprÃ¨s ? Car câ□□est un premier pas essentiel, mais ce nâ□□est pas suffisant. Plus notre comprÃ©hension est Ã©tendue, plus il est facile dâ□□interprÃ©ter les signes et de limiter le nombre dâ□□inconnus, mais comment peut-on amÃ©liorer nos systÃ¨mes de sÃ©curitÃ©?

Il est Ã©vident quâ□□il nâ□□existe aucune protection parfait et infaillible, je fais ici rÃ©fÃ©rence a un modÃ¨le qui peut sâ□□adapter et apprendre au fur et Ã  mesure de lâ□□Ã©volution des processus, des technologies ou des menaces. Je fais rÃ©fÃ©rence Ã  un modÃ¨le qui nous permet de dÃ©tecter les attaques et dâ□□y rÃ©pondre rapidement. Je fais rÃ©fÃ©rence Ã  un modÃ¨le Big Data.

## Transformer les donnÃ©es en bouclier de protection

Les organisations doivent pouvoir jouir dâ□□une visibilitÃ© total de leurs donnÃ©es, quâ□□elles soient structurÃ©es ou non structurÃ©es. Les architectures Big Data seront suffisamment Ã©volutives pour que toutes les donnÃ©es puissent Ãªtre analysÃ©es, permettant aux entreprises de construire une mosaÃ¯que dâ□□informations spÃ©cifiques Ã  propos de leurs actifs numÃ©riques, des utilisateurs et de lâ□□infrastructure. Le systÃ¨me sera alors capable dâ□□identifier et de recouper les comportements anormaux dans un flux continu dâ□□informations.

Bien sÃ»r, le systÃ¨me ne sera pas pour autant inviolable mais cela permettra de maintenant un niveau acceptable de risque et de ne pas nous laisser distancer par lâ□□adversaire. Est-ce que ce sera difficile ? Oui, mais les technologies nÃ©cessaires pour y arriver sont dÃ©jÃ  entre nos mains.