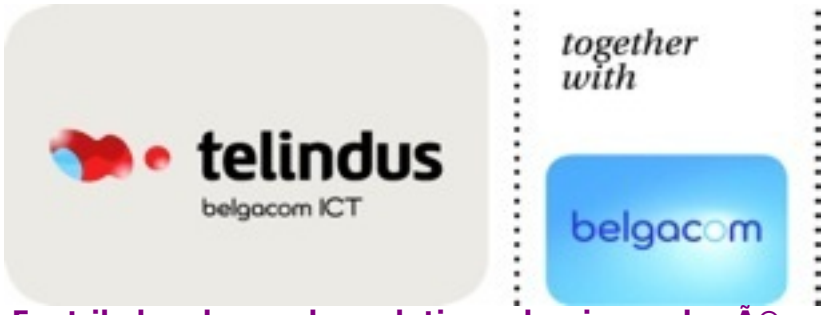
Cyber-attaques : quels types de solutions mettre en place ?
Internet
PostÃ© par : JPilo
PubliÃ©e le : 6/11/2012 13:00:00

Terrorisme, espionnage industriel, vols de donnÃ©es critiques, monÃ©tisation de lâ□□information, **les opportunitÃ©s dâ□□attaques se multiplient et Ã©voluent** au fur et Ã mesure oÃ¹ le cyber-espace se dÃ©veloppe. De nouveaux attaquants font leur apparition, ils sont plus nombreux, mieux organisÃ©s, plus compÃ©tents.

Cette Ã©volution sâ□□observe dans la complexitÃ© des malwares analysÃ©s jusquâ□□Ã prÃ©sent tels que STUXNET en 2010 qui reste toutefois 20 fois moins sophistiquÃ© que FLAME identifiÃ© Ã peine deux ans plus tard en juin 2012. **NoÃ«l Chazotte** et **Nicolas Leseur**, Marketing et Innovation SÃ©curitÃ©, Telindus France nous en disent un peu plus.

Avec lâ□□ouverture du systÃ¨me dâ□□information (SI) des entreprises , lâ□□exposition au risque provenant dâ□□Internet ne cesse dâ□□augmenter. Or, les attaques qui se multiplient le prouvent, les entreprises ne sont pas Ã©quipÃ©es pour y faire face. Lâ□□Ã©tude Â« Growing Risk of Advanced Threats Â» menÃ©e en 2010 par Ponemon Institute rÃ©vÃ¨le que 83% des entreprises pensent quâ□□elles ont Ã©tÃ© victimes dâ□□attaques avancÃ©es et 65 % dâ□□entre elles pensent quâ□□elles nâ□□ont pas les ressources pour sâ□□en prÃ©munir. Trop dâ□□entreprises ne sont dotÃ©es que dâ□□une protection passive, qui leur permet Ã©ventuellement dâ□□agir en cas dâ□□attaques mais elles doivent aujourdâ□□hui Ã©voluer vers une protection proactive pour crÃ©er toujours plus dâ□□obstacles sur la route des cyber-criminels.



Faut-il abandonner les solutions classiques de sÃ©curitÃ© et de protections ?

Les outils de sÃ©curitÃ© pÃ©rimÃ©trique et interne Ã lâ□□entreprise ont Ã©voluÃ© pour atteindre un trÃ¨s bon niveau de maturitÃ© (stabilitÃ©, efficacitÃ©). Ceci conduit Ã pouvoir bloquer la majoritÃ© des attaques provenant dâ□□Internet.

De plus, si effectivement les outils de sÃ©curitÃ© traditionnels nâ□□ont pas la capacitÃ© Ã arrÃªter les attaques avancÃ©es, ils vont pouvoir Ãªtre utiles poursurveiller les flux lÃ©gitimes, dÃ©tecter certains comportements anormaux (signaux faibles) et Ã©ventuellement, prendre part au processus de rÃ©action (remÃ©diation, correctionâ□¦). Ces outils resteront donc Ã la base dâ□□un systÃ¨me de sÃ©curitÃ©.

Les technologies actuelles sont donc toujours nÃ©cessaires, mais plus suffisantes.

Pour repenser lâ□□axe stratÃ©gique de dÃ©fense du SI il faut prendre en compte 3 piliers :

1) Surveiller

Le problÃ¨me des nouvelles attaques est que leurs flux se prÃ©sentent comme des flux licites (exploitant desprotocoles standards), Ã©ventuellement chiffrÃ©s, et dont les donnÃ©es utiles sont fractionnÃ©es (le code actif ou l'extraction de donnÃ©es est dÃ©coupÃ© en de multiples Ã©lÃ©ments a priori anodins).

Les systÃ¨mes de surveillance peuvent protÃ©ger et surveiller tout ou partie des couches du SI, en distinguant notamment, les couches d'infrastructures, des applications, et des donnÃ©es.

On peut citer et regrouper les principales technologies suivantes :

filtrage rÃ©seaux (FW) ;

application des signatures (AV, IPS) ;

analyse comportementale (Anti-malware) ;

protections des applications (WAF) ;

surveillance de l'accÃ¨s aux donnÃ©es sensibles (usage rÃ©el, droits d'accÃ¨sâ¦) ;

DLP.

2) DÃ©tecter

La principale caractÃ©ristique des nouvelles attaques est leur furtivitÃ©, en effet, elles parviennent Ã faire passer du code (vers le SI) ou extraire des donnÃ©es (depuis le SI), de maniÃ¨re silencieuse. Cette furtivitÃ© est donc associÃ©e aux signaux que ces attaques s'efforcent de minimiser : ce sont les Â« signaux faibles Â». Lâ□□un des enjeux techniques sera donc de parvenir Ã dÃ©tecter ces signaux parmi la multitude dâ□□Ã©vÃ¨nements normaux ou anormaux (Facteur technique liÃ©s Ã lâ□□infrastructure du SI, dÃ©tection dâ□□un changement de rÃ©putation Â« Ã©lectronique Â» de lâ□□entreprise, etc., facteur humain comme des plaintes venant des clients, utilisateurs, administrateurs et le facteur Environnemental, hors cadre du domaine informatique).

Les solutions de dÃ©tection vont venir en renfort des briques de sÃ©curitÃ© traditionnelles afin de couvrir les zones non couvertes par celles-ci, tout en apportant les moyens nÃ©cessaires pour gagner en proactivitÃ© et capacitÃ© de rÃ©action.

3) RÃ©agir

La rÃ©action face Ã un incident est gÃ©nÃ©ralement constituÃ©e de deux phases :

la phase d'enrichissement : prise en compte de toutes les informations possibles associÃ©es Ã l'Ã©vÃ¨nement ;

la phase de remÃ©diation en tant que telle qui s'appuie sur une procÃ©dure liant le traitement technique et organisationnel de lâ□□incident.

Un IPS ou un antivirus permettent par exemple d'avoir une rÃ©action automatique sur

reconnaissance d'un Ã©vÃ¨nement malveillant clairement identifiÃ©. En revanche, ces outils sont limitÃ©s pour de nouveaux types dâ□□attaques.

Quels types de solutions mettre en place ?

Les nouvelles solutions permettent de couvrir une ou plusieurs de ces Ã©tapes capitales pour assurer la protection de son SI. On parlera ici de nouvelles technologies autour de trois axes principaux :

- Protection avancÃ©e contre les malwares :

Parmi les solutions disponibles nous retrouvons celles basÃ©es sur un systÃ¨me de prÃ©vention contre les programmes malveillants qui exploitent une technologie de pointe pour dÃ©tecter et empÃªcher l'exÃ©cution de code malveillant, le vol de donnÃ©es et la prolifÃ©ration des botnet.

Ce type de technologies dÃ©tecte les Â« maliciels Â» et les machines Â« botnet Â» en utilisant la technologie de Machine Virtuelle (VM) en Â« sandbox Â». De plus, lâ□□interaction avec une plate-forme mondiale dâ□□Ã©changes dâ□□informations dÃ©diÃ©es aux logiciels malveillants amÃ©liore lâ□□efficacitÃ© des analyses locales et permet dâ□□identifier, de comprendre et dâ□□arrÃªter plus rapidement et plus prÃ©cisÃ©ment les attaques (connues ou inconnues) de logiciels malveillants venant du Web et de rÃ©seaux de Â« zombies Â». Cette solution ne permet pas forcÃ©ment dâ□□empÃªcher un code malveillant de pÃ©nÃ©trer le systÃ¨me dâ□□information, nÃ©anmoins la dÃ©tection peut Ãªtre rapide afin de mettre en place les contre-mesures spÃ©cifiques avant que lâ□□attaque ne puisse rÃ©ellement Ãªtre mise en Å□uvre.

- Protection des donnÃ©es :

Une autre solution pour se prÃ©munir des malwares visant Ã compromettre ou voler les donnÃ©es de lâ□□entreprise, consiste justement Ã identifier les risques pour protÃ©ger lâ□□accÃ¨s aux donnÃ©es sensibles. On parle alors dâ□□outils de gouvernance de la donnÃ©e.

Lâ□□augmentation du volume de donnÃ©es est un fait, mais la difficultÃ© rÃ©side dans la dissÃ©mination de ces donnÃ©es dans le SI et la gestion des droits dâ□□accÃ¨s Ã ces donnÃ©es. Les donnÃ©es sont rÃ©parties majoritairement sur des serveurs de fichiers, et il est souvent difficile dâ□□identifier les propriÃ©taires des donnÃ©es et encore plus dâ□□identifier qui accÃ¨de rÃ©ellement Ã ces donnÃ©es, afin de savoir sâ□□ils ont les habilitations. Il existe pourtant des systÃ¨mes de classification des donnÃ©es qui sont sensÃ©s rÃ©pondre Ã ce besoin, nÃ©anmoins sur le volume on ne peut jamais Ãªtre sÃ»r que le systÃ¨me de classification a Ã©tÃ© respectÃ© et surtout, si les droits dâ□□accÃ¨s ont bien Ã©tÃ© appliquÃ©s en fonction de la sensibilitÃ© des donnÃ©es.

Aujourdâ□□hui, des solutions techniques permettent de rÃ©pondre Ã ce challenge en donnant une vue exhaustive de lâ□□accÃ¨s aux donnÃ©es permettant de mettre en Ã©vidence des points Ã corriger. On aura par exemple la possibilitÃ© de visualiser des donnÃ©es qui sont sur des serveurs de fichiers et qui ne sont pas accÃ©dÃ©es, ces donnÃ©es vont alors pouvoir Ãªtre archivÃ©es.

- VisibilitÃ© exhaustive des flux de donnÃ©es

Devant la complexitÃ© et la multitude de flux de donnÃ©es dans un systÃ¨me dâ□□information, il devient difficile voire impossible de dÃ©terminer quels sont les usages illicites ou anormaux parmi le flot dâ□□usages lÃ©gitimes. Lorsquâ□□on a un doute sur une intrusion possible ou mÃªme tout simplement lorsque lâ□□attaque est avÃ©rÃ©e (parfois les entreprises lâ□□apprennent par la presse !), il est important de pouvoir comprendre quel a Ã©tÃ© le vecteur de lâ□□attaque et surtout quels sont les dÃ©gÃ¢ts rÃ©ellement causÃ©s.

Lâ□□objectif de ce nouveau type de solution est dâ□□effectuer une capture complÃ¨te de toutes les sessions utilisateurs en permettant de suivre et ainsi de donner une visibilitÃ© exhaustive sur lâ□□activitÃ© rÃ©seau et le comportement des utilisateurs (de la couche rÃ©seau Ã la couche applicative). Tout cela, en ayant la capacitÃ© de remonter sur des Ã©vÃ¨nements passÃ©s. Il va sans dire quâ□□une telle masse dâ□□informations nâ□□a de sens que si lâ□□outil permet de crÃ©er des meta-donnÃ©es suffisamment complÃ¨tes et avancÃ©es pour gÃ©rer finement les recherches Ã travers une interface utilisateur simple et efficace.

Au final, mÃªme si ces nouvelles solutions donnent les moyens dâ□□agir face aux nouvelles menaces, les technologies ne sont que des outils au service dâ□□une nouvelle approche de la sÃ©curitÃ© qui doit Ãªtre crÃ©Ã©e au sein de lâ□□entreprise.