Virtualisation : les limites en termes de dÃ©tection et de prÃ©vention des intrusions.
SÃ©curitÃ©
PostÃ© par : JulieM
PubliÃ©e le : 10/9/2009 0:00:00

La vague de virtualisation des systÃ¨mes et rÃ©seaux dÃ©ferle sur nos systÃ¨mes dâ□□information. Les bÃ©nÃ©fices sont immenses et indÃ©niables. Il est toutefois important de prendre quelques prÃ©cautions pour Ã©viter que nos systÃ¨mes IPS/IDS ne deviennent complÃ¨tement aveugles et sourds voire inexploitables.

Le principe est simple et efficace, lâ□□hÃ©bergement des systÃ¨mes dâ□□exploitation et des services sur des environnements virtuels permet une flexibilitÃ© et une rÃ©activitÃ© aux besoins informatiques jusquâ□□ici inÃ©galÃ©es.

Pourquoi ces avantages gÃ©niaux que nous procurent les environnements virtuels poseraient-ils problÃ¨me Ã nos systÃ¨mes de prÃ©vention et de dÃ©tection des intrusions?

Tout dâ□□abord pour le caractÃ¨re flexible justement. Le problÃ¨me majeur de lâ□□IDS/IPS Ã©tant le faux positif, la configuration dâ□□un IPS doit reflÃ©ter exactement la couverture des vulnÃ©rabilitÃ©s prÃ©sentes dans le rÃ©seau afin de limiter les erreurs.

Si un service nouveau et diffÃ©rent des autres dÃ©marre (version diffÃ©rente / Ã©diteur diffÃ©rent), il est donc nÃ©cessaire de mettre un â□□coup de tournevisâ□□ sur lâ□□IPS afin de garantir le maintien du niveau de sÃ©curitÃ© et dâ□□Ã©viter le risque de faux positif.

Le recours aux environnements virtuels dynamise Ã©normÃ©ment le rÃ©seau ce qui alourdit fortement la tache des exploitants de lâ□□IPS.

Pour se prÃ©munir contre ce surcoÃ»t dâ□□exploitation de la sÃ©curitÃ©, il est recommandÃ© dâ□□utiliser un IPS dit â□□adaptatifâ□□ capable de cartographier le rÃ©seau en temps rÃ©el et dâ□□adapter son profil de protection en suivant le dynamisme du rÃ©seau. Lâ□□IPS â□□adaptatifâ□□ est capable de dÃ©couvrir en temps rÃ©el le dÃ©marrage dâ□□un service sur un environnement virtuel.

Plus ennuyeux encore, sâ□□il y a systÃ¨me virtuel, sâ□□il y a application virtuelle, il y a bien souvent

et de plus en plus un rÃ©seau virtuelâ¦ Au sein dâ□□un mÃªme environnement virtuel, les systÃ¨mes et applications peuvent communiquer entre eux/elles sans Ãªtre contrÃ´lÃ©s par les systÃ¨mes IPS qui sont trÃ¨s largement dÃ©ployÃ©s Ã lâ□□extÃ©rieur de lâ□□environnement virtuel et souvent hÃ©bergÃ©s sur un boÃ®tier appliance.

En bref, les IPS classiques sont sourds et aveugles devant les attaques rÃ©alisÃ©es au sein mÃªme de lâ□□environnement virtuel. De quoi nourrir lâ□□imagination des hackersâ¦

La solution sâ□□impose dâ□□elle mÃªme, sâ□□il y a rÃ©seau virtuel, il suffit de dÃ©ployer une sonde IDS virtuelle au sein mÃªme de lâ□□environnement afin dâ□□y contrÃ´ler le trafic et dâ□□y dÃ©tecter les attaques et anomalies qui nous intÃ©ressent dans le monde rÃ©el.

En bref, caractÃ¨re adaptatif de lâ□□IPS reste Ã©videmment intÃ©ressant.

En conclusion, un IPS classique uniquement basÃ© sur appliance fera mauvais mÃ©nage avec une politique forte de virtualisation. La dÃ©marche de virtualisation dâ□□une partie du SI nÃ©cessite une prise en compte particuliÃ¨re de ce sujet afin de contrÃ´ler les coÃ»ts dâ□□exploitation et dâ□□Ã©viter une dÃ©tÃ©rioration du niveau de dâ□□efficacitÃ© des IPS.

Les technologies Ã©voluent mais la logique de gestion des Ã©vÃ©nements de sÃ©curitÃ© reste inchangÃ©e.