Avis d'expert : « Sécurité adaptative : juste du bon sens ! »

La plupart des grandes sociétés qui ont été attaquées très sérieusement lors des deux dernières années étaient protégées par des outils de prévention d'intrusions (IPS) sérieux et robustes.

Pire encore, les éditeurs d'IPS avaient, dans la quasi-totalité des cas, déjà publié une règle de protection pour stopper l'exploit dont elles ont été victimes… Seulement, la règle de protection n'était pas activée au bon endroit et au bon moment.

L'arbre qui cache la forêt

Depuis toujours, les éditeurs ont pointé du doigt et cristallisé notre attention sur la menace et son évolution constante. Les hackers vont vite, très vite. Il faut donc que les éditeurs fassent d'énormes efforts pour suivre la menace qui est en perpétuel mouvement.

Nous le savons tous, un antivirus ou un IPS qui n'est pas mis à jour ne sert pas à grand-chose… Nous mettons donc à jour quasiment quotidiennement. Seulement, dans 90 % des cas, la politique mise à jour est la politique par défaut du constructeur.

Politique par défaut

Définition : une politique par défaut est une politique créée pour fonctionner sans effets de bord (faux positif) chez tout le monde, mais qui ne fait finalement de la sécurité chez personne.

Il est important de noter qu'un « faux positif » n'est pas généré par une règle mal écrite – il est généré par une règle utilisée dans un contexte inapproprié (par exemple, l'activation de règles Apache sera potentiellement génératrice de « faux positifs » si elle est réalisée dans un environnement qui utilise exclusivement des serveurs web IIS).

Afin d'éviter de rejeter du trafic licite, les constructeurs d'IPS proposent tous une politique par défaut « garantie » sans faux positifs. Elle s'applique aux systèmes et services les plus courants et les plus utilisés (le plus grand dénominateur commun de nos réseaux). En effet, le risque de faux positif étant fort dans un contexte inadapté, il s'agit de normaliser la politique autour d'un pseudo contexte commun.

Cette politique contient généralement entre 1000 et 3000 règles. Pourtant, il existe aujourd'hui plus de 25 000 règles IDS/IPS différentes.

Nos réseaux sont tous différents

Même si nos serveurs de fichiers, nos infrastructures et nos stations de travail sont peu différents d'un réseau à l'autre, nos applications métiers sont clairement toutes différentes en fonction de nos secteurs d'activité ; mais elles ont un point commun, elles correspondent au plus fort besoin de

sécurisation dans l'entreprise – elles sont nos ressources critiques.

Les politiques par défaut ne sont clairement pas adaptées pour gérer le risque lié à ces ressources critiques. Il faut réaliser une personnalisation précise pour garantir une protection complète en fonction des vulnérabilités présentes.

Le changement c'est maintenant

Supposons que nous ayons réalisé ce « tuning » précis nécessaire pour réellement tirer un bénéfice de l'outil de sécurité qui protège nos environnements critiques.

Nous sommes alors pour quelques heures en mesure de gérer et de contrôler le risque sur cette zone, et ce jusqu'à ce qu'un changement intervienne dans le réseau (nouveau service, nouvelle version, démarrage de machine virtuelle, nouvelles vulnérabilités découvertes).

Dans le réseau d'une grande entreprise, ce changement intervient quasi quotidiennement. Il faut donc « tuner » continuellement pour conserver un niveau de sécurité acceptable. Impossible…

Tous les éditeurs insistent sur les mises à jour nécessaires pour se protéger contre les nouvelles menaces extérieures. Qu'en est-il des changements à l'intérieur du réseau ?

Il est aujourd'hui admis par les spécialistes du domaine que sans adaptabilité ou « tuning » régulier, la protection d'un IPS contre des attaques ciblées est quasi nulle.

Sécurité adaptative ou NGIPS

Ainsi, la sécurité doit être adaptative. Un IPS adaptatif (qui intègre des modules intelligents de découverte du réseau protégé), permet d'avoir une connaissance des OS/Services/Applications/utilisateurs à protéger et ainsi connaître les vulnérabilités potentielles présentes sur les machines tout en sélectionnant pour vous les règles qui doivent être appliquées dans votre environnement, et ce dans une base de 25 000 règles disponibles.

Chaque entreprise doit disposer d'une politique IPS spécifique à son environnement, garantissant une protection exhaustive et limitant donc le taux de « faux positifs » au minimum possible.

Dans ce cadre, si une règle doit être déployée devant vos ressources à protéger, elle le sera.

Voir aussi

Silicon.fr étend son site dédié à l'emploi IT
Silicon.fr en direct sur les smartphones et tablettes