Le nouveau visage de McAfee

Thierry Evangelista, responsable des partenaires à valeur ajoutée, et auteur de l'ouvrage « Les IDS », s'est prêté à nos questions.

Un changement de nom Etait-ce pour redorer son image? Network Associates s'est rebaptisé du nom de sa célèbre suite de solutions antivirus, McAfee. La raison principale ? « *Le nom McAfee semblait bien plus populaire que NAI. Par ailleurs, McAfee véhiculait une image liée à la protection antivirale et donc à la sécurité, tandis que Network Associates avait sans doute une consonance majeure pour les solutions réseau*« . **Les acquisitions** Au cours des deux années écoulées McAfee s'est résolument concentré sur le domaine de la sécurité et plus particulièrement sur la prévention d'intrusion, avec l'acquisition de bon nombre de sociétés spécialisées dans le domaine. Côté prévention d'intrusion, l'acquisition d'Intruvert a permis de bénéficier d'une solution de prévention réseau de type NIPS tandis que Entercept offrait une solution système de type HIPS. McAfee a par ailleurs renforcé sa gamme de solutions de protection de messagerie électronique avec l'acquisition de Deersoft il y a 18 mois, à l'origine de Spamassassin. Plus récemment McAfee s'est offert la prestigieuse société de conseil Foundstone reconnue essentiellement pour ses compétences en conseils et aussi pour sa solution de gestion de vulnérabilités Foundscan. **L'abandon des divisions non orientées sécurité** Le problème de McAfee était le suivant: mis à part sa gamme de solutions antivirus, les autres produits du portfolio allaient du 'Sniffer' pour l'analyse de trafic réseau au système de Help Desk pour la gestion des incidents. Difficile ainsi pour la firme de s'affirmer sur le marché de la sécurité et de se positionner contre les autres géants de l'industrie tels que Symantec. Mis à part les différentes acquisitions signées ces dernières années, McAfee avait besoin de se séparer d'une partie des anciens produits que la firme traînait dernière elle et qui n'étaient généralement pas liés directement à la sécurité. En 2002, PGP, la solution de chiffrement asymétrique est redevenue une entité à part qui a repris son nom d'origine PGP Inc. (http://www.pgp.com). Plus récemment, la solution Sniffer (http://www.sniffer.com), dédiée à l'analyse de trafic réseau a pris son indépendance, à son tour, en empruntant le nom de Network General (rappelons que Network Associates était issue de la fusion de McAfee et de Network General en 1997?). Magic Help Desk, la solution de gestion d'incidents a été cédée à BMC Software pour compléter son produit Remedy. **La prévention d'intrusion** L'année passée, McAfee s'est offer coup sur coup des sociétés leaders dans les domaines de la prévention système et réseau. Intruvert et Entercept sont désormais intégrées dans le catalogue de la firme et permettent d'adresser un marché en pleine expansion, là où beaucoup d'éditeur d'IDS avaient échoué. La solution Entercept permet ainsi de proposer une protection système (HIPS) sur l'ensemble des serveurs. Le mécanisme est simple, considérant que la plupart des attaques applicatives exploitent des vulnérabilités telles que des « buffers overflows » qui permettent d'accéder au noyau au travers d'appels systèmes. La solution Entercept permet de cloisonner l'espace du processus et d'effectuer un contrôle sur l'ensemble des primitives système. Un contrôle de l'intégrité sur les fichiers est parallèlement effectué. La solution Entercept se décline au travers d'une gamme allant du serveur Web jusqu'à la base de données et propose une protection pour les systèmes Windows comme pour certains Unix (Solaris, HP-UX et bientôt Linux). Pour ce qui est de la prévention d'intrusions réseau (NIPS) la solution de McAfee porte le nom de IntruShield et permet via une architecture en ligne d'autoriser ou nom les requêtes de connexions vers les systèmes cibles. IntruShield exploite un moteur de détection propriétaire basé

sur une combinaison de 3 méthodes d'analyse : – Une base de signature d'exploits reposant sur une technologie de pattern-matching, – Un moteur de détection d'anomalies qui permet de détecter des évênements suspects liés à certains protocoles ou environnements applicatifs (non-conformité des flux aux normes, tentatives d'éxécution de shellcodes?) – Un auto-apprentissage permettant une analyse statistique des flux, ce qui permet de détecter rapidement des comportements suspects ou certaines attaques par déni de services Il faut noter que ces 3 moteurs sont corrélés entre eux et s'appuient sur un système de scoring, ce qui permet une réduction drastique des faux-positifs. En Juillet 2004, 3100 signatures étaient recensées dans la base avec près de 1000 taggées CVE (environ 650 sont taggées Bugtraq ID ou BID). Cote mises à jour, celles-ci sont régulières (tous les 15 jours environ, hors mises à jour suite à des alertes critiques). **La gestion des vulnérabilités et l'analyse de risque** Pour continuer dans sa lancée et combler la brique manquante de la gestion de vulnérabilités et de la mesure de risque, McAfee a acquis dernièrement l'un des leaders du domaine, en l'occurrence Foundstone. Le marché de la gestion de vulnérabilités pour l'entreprise a connu une croissance phénoménale au cours des dernières années et semble offrir davantage de perspectives d'évolutions. Ironie du sort, McAfee disposait il y a quelques années d'une solution d'analyse de vulnérabilités jugée excellente pour l'époque et qui tenait tête à ISS Internet Scanner. La solution avait été abandonnée par défaut de demande. L'intégration de la solution Foundscan, n'a pas encore été totalement effectuée au sein de l'offre de McAfee. Aussi la centaine de consultants sécurité Foundstone devrait rejoindre l'équipe de services professionnels de McAfee. Un capital de savoir-faire reconnu qui apportera sans doute une crédibilité très forte de la firme. Ces équipes ne viendront pas se substituer aux VARs existants mais interviendront sur des problématiques très spécifiques qui dépassent le cadre d'expertise du VAR. **Les intégrations avec des tiers** En ce qui concerne les intégrations avec des solutions tierces McAfee s'est comme beaucoup d'autres penché essentiellement sur les SIM (Security Information Management), et travaille en partenariat avec des sociétés comme ArcSight, Netforensics, Network Intelligence, Tivoli, Tenable Network Security ou encore Exaprotect (spécifiquement sur la France). Aussi, il n'est pas impossible que la prochaine acquisition de McAfee se fasse dans ce domaine. George Samenuk, CEO, lors d'un passage en France il y a quelques mois, disait: « *Il n'est pas exclu que nous procédions à une acquisition dans ce domaine*« . Bien évidemment, il faudra tenir compte de l'évolution de ce nouveau marché ainsi que du degré de maturité des technologies. **Norman Girard pour Vulnerabilite.com**

Une offre multiforme

Aujourd'hui, le coeur de compétence de McAfee repose sur les domaines suivants: – les antivirus sous toutes leurs formes avec McAfee VirusScan (windows, linux, Mac, messagerie, passerelle, PDA…) – la détection/prévention des intrusions avec IntruShield (Réseau) et Entercept (Système) – le Firewall au poste de travail au travers de McAfee Desktop Firewall, – l'antispam pour la protection de la messagerie électronique avec WebShield, – le management centralise de l'ensemble des solutions de sécurité avec ePO (déploiement, monitoring, détection des systèmes interdits, inventaires des patches déployés…) – la gestion des risques avec l'offre Foundstone. Ces solutions couvrent aussi bien les aspects identification des vulnérabilités (Vulnerability Assessment) que estimation de l'impact de celles-ci et mises en place de contre-mesures quand cela est possible. Autant dire que la firme a su s'affirmer dans le domaine de la sécurité et plus spécifiquement dans celui de la prévention d'intrusion. La nouveauté, ce sont des solutions résolument tournées entreprise, comme: HIPS/NIPS, de gestion de vulnérabilité et de mesure de risque.