Dave Merkel, FireEye : « Contre les menaces persistantes, il faut des technologies mais aussi des hommes »

Ex-directeur technique de Mandiant, société américaine spécialisée dans la réponse aux incidents de sécurité, Dave Merkel est désormais le directeur technique de FireEye, la société qui a racheté son ancien employeur pour 1 milliard de dollars. Entrée en bourse en 2013, le spécialiste des environnements virtuels de détection de menaces est engagé dans une **stratégie d'internationalisation** (l'international pèse aujourd'hui 30 % de son CA) et de **diversification de son portefeuille d'offres**, visant à offrir une réponse plus globale aux problématiques de sécurité IT des entreprises. L'éditeur américain va ainsi faire son entrée sur le marché des appliances de détection d'intrusion (IPS, *intrusion prevention systems*), concurrençant des spécialistes du domaine comme Cisco ou Palo Alto Networks. La firme annonce le lancement de ses premiers produits d'IPS, les MVX-IPS, pour le milieu de l'année 2014.

De passage en France, pour tenter de séduire de nouveaux clients (FireEye en compte 20 dans l'Hexagone pour l'instant), le directeur technique se penche sur les grandes évolutions des cyberattaques et décortique les stratégies de sa société pour grandir à l'international.

***Silicon.fr* : FireEye vient de publier un rapport sur l'évolution des menaces avancées (Advanced Threat Report). Quels en sont les principaux enseignements ?**

Dave Merkel : Le premier est que le niveau d'activités en provenance des assaillants spécialistes de ces techniques est en nette augmentation. Sur l'ensemble de notre réseau de clients, nous avons détecté une attaque avancée toutes les 1,5 secondes en 2013. Soit une fréquence doublée par rapport à 2012. Par ailleurs, on observe une internationalisation de ces attaques. Partout dans le monde, on retrouve les mêmes types d'attaques, les mêmes schémas d'intrusion. Ceci n'est finalement pas une surprise, car où qu'elles se trouvent, les entreprises ont le même type d'actifs à protéger.

En Europe, la France est au quatrième rang en matière d'activité des assaillants, derrière le Royaume-Uni, l'Allemagne et la Suisse, très attaquée en raison du poids de son industrie financière. Même si notre base installée en France est limitée, on y retrouve les mêmes schémas d'attaque qu'ailleurs. Au total, nous avons détecté 19 APT (*Advanced Persistent Threat*) en France en 2013.

Quel est le profil type des assaillants ?

Au sommet, on retrouve les groupes les plus organisés, ceux qui sont sponsorisés par des Etats. Ils s'intéressent aux secrets diplomatiques ou aux informations d'autres Etats, mais également à la propriété intellectuelle des entreprises : les négociations de contrats, les tarifications, la R&D, etc. Il ne fait plus aucun doute aujourd'hui que des Etats financent des opérations contre des cibles industrielles étrangères, à des fins d'espionnage. Ce type d'assaillants se moque d'être découvert et ne va pas hésiter à revenir même après avoir vu son attaque dévoilée.

L'autre grand vecteur d'infections provient du cyber-crime organisé, essentiellement originaire d'Europe de l'Est. Leurs cibles sont très nombreuses : schématiquement, n'importe quelle organisation à partir de laquelle il est possible de se faire de l'argent. Ces assaillants vont continuer à se servir tant qu'ils ne sont pas découverts. Mais, une fois leur présence mise au jour, ils ne vont plus réapparaître. Dans ces deux univers, chacun apprend des techniques des autres et on n'hésite pas à se copier.

Enfin, on trouve les attaques menées par les hacktivistes. Avec ces assaillants, la difficulté réside dans le fait qu'il est impossible de prévoir à l'avance quelles seront leurs motivations. Par contre, ils sont moins organisés que les deux autres types d'assaillants.

Et peut-on imaginer également des entreprises finançant des groupes de hackers pour dérober des informations chez des concurrents ?

En la matière, on ne peut pas citer d'exemple connu à ce jour. Mais c'est tout à fait possible. Pourquoi certaines entreprises ne le feraient-elles pas ?

Quelle est la logique du rachat de Mandiant par FireEye ?

Avant tout, le rachat de Mandiant répond à une volonté claire : rester le plus près possible de la faille. Dans le détail, trois éléments montrent clairement les atouts de ce rapprochement. D'abord Primo, FireEye ne disposait d'aucun produit de détection 'endpoint', ce que lui a amené Mandiant. Un élément clef au moment où FireEye est en train de bâtir une suite complète de sécurité. Secundo, Mandiant amène une importante activité de services, dans la réponse aux incidents. Or les clients FireEye lui demandaient souvent d'analyser les origines de l'attaque. Pour lutter contre les APT, vous avez besoin à la fois de technologies et d'hommes. Via ce rapprochement nous offrons désormais des services de défense managée, allant jusqu'à la réponse aux incidents. Et nous sommes en train d'internationaliser cette offre. Tertio, rapprocher FireEye et Mandiant permet d'améliorer la connaissance des menaces au sein du nouvel ensemble.

En Europe, allez-vous amener cette offre couplant détection et réponse aux incidents sous la seule étiquette FireEye ou via des partenaires ?

Nous allons mixer les deux approches. Certaines entreprises européennes se posent des questions concernant les entreprises américaines, questions sur la législation américaine, l'accès aux données sensibles, etc. Nous allons donc continuer à travailler avec des partenaires locaux. Depuis le rachat de Mandiant, aucun partenaire n'a d'ailleurs été écarté par FireEye.

Justement, un des points clefs de votre offre réside dans l'utilisation du Cloud pour mutualiser la connaissance des intrusions. Un élément qui peut déranger certains clients non américains. Prévoyez-vous des Cloud locaux, par exemple en Europe, afin de tranquilliser les entreprises sur ce point ?

Cette préoccupation existe et nous sommes en train d'étudier les différentes options envisageables en 2014. Il faut toutefois noter qu'il est déjà possible d'utiliser la solution FireEye sans activer la connexion au Cloud. Mais les entreprises doivent comprendre l'intérêt qu'elles ont à appartenir à une communauté de défense.

Voir aussi

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