Sécurité informatiques : les hackers de plus en plus patients

Il n'y a pas si longtemps, pour réussir une attaque, il fallait opérer le plus rapidement possible. Les hackers identifiaient un ou plusieurs points faibles (vulnérabilités) dans les mécanismes de défense de leurs cibles et ils s'en servaient comme vecteur d'attaque, la plupart du temps sous la forme de campagnes de dénis de service.

Le temps que les ressources de l'organisation s'organisent pour mettre au point une défense, le mal était fait. Si la phase de reconnaissance pouvait durer plusieurs jours ou semaines, l'attaque en elle-même et l'extorsion d'information prenaient quelques minutes seulement en moyenne.

A mesure que le marché de la sécurité a gagné en maturité et que des contre-mesures plus sophistiquées ont été déployées, une nouvelle méthodologie d'attaque est apparue, qui dépendait beaucoup moins cette fois du critère de lsquo;rapidité'. En effet, contrairement aux stratégies suivies jusque-là, les attaques de nouvelle génération s'étendent sur de plus longues périodes, l'idée étant qu'en procédant très lentement sur plusieurs semaines ou plusieurs mois, le trafic réseau paraîtrait normal et aucune alarme ne se déclencherait.

A présent, les changements intervenus au niveau des types et des flux des données font qu'il est plus compliqué encore de détecter ces attaques. Avec le Big Data, l'Internet des objets et autres réseaux virtualisés, l'efficacité d'une solution de sécurité dépend de sa capacité à passer au crible d'énormes quantités de données structurées et non structurées. Il faut aussi qu'elle piste les flux de données sur de longues périodes pour déceler les « signaux faibles» élaborées pour tromper les produits de sécurité ponctuels. Sachant qu'une voiture de Formule 1 typique embarque 240 capteurs qui génèrent 25 mégaoctets de données par tour, qu'un téléchargement de film HD fait entre 3 et 4,5 Go et qu'un salarié envoie et reçoit plus de 250 e-mails avec pièce jointe par jour en moyenne, il n'est pas surprenant qu'il soit aussi compliqué de repérer une attaque préparée sur des semaines ou des mois que de trouver une aiguille dans une botte de foin.

Les solutions de sécurité les plus efficaces aujourd'hui suivent une approche différente. En déployant des capteurs en plusieurs points du réseau distribué, il est possible de capturer les données en différentes positions et examiner les flux en circulation d'où que viennent les données et où qu'elles aillent. Des techniques avancées de corrélation de ces flux de données disparates aident à atténuer l'ampleur de la tâche ; la botte de foin est réduite à une poignée de brins, si bien que l'administrateur peut auditer plus facilement les données. Selon le type de violation détecté, il est possible de créer des règles de hiérarchisation des niveaux de réaction, bloquer le trafic nuisible, ou simplement déclencher une alarme. Le fait d'observer les données sur de longues périodes et en différents points permet aussi d'accélérer l'identification et de lutter plus efficacement contre ces attaques qui font des ravages dans les entreprises.

Nous avons longtemps pensé qu'un niveau minimum de sécurité « faisait l'affaire ». En compliquant la tâche au hacker, on le dissuadait de perpétrer une attaque qui lui prendrait trop de temps et d'énergie. Mais le hacker est bien plus patient aujourd'hui. S'il convoite quelque chose qui vous appartient, il ou elle prendra le temps qu'il faut pour contourner ou tromper votre ligne de défense. Il devient alors aussi difficile de le bloquer que de trouver cette fameuse aiguille dans une botte de foin. Par contre, si vous vous équipez d'outils de corrélation et analytiques avancés, vous pourrez

réduire la taille de cette botte de foin de façon à analyser les attaques les plus virulentes.