La cybersécurité innove !

Les nouvelles menaces imposent une approche innovante. Le secteur de la cybersécurité emprunte dès lors de nouvelles pistes en s'intéressant aux big data, à l'intelligence artificielle et à d'autres idées originales.

Guy Kindermans

Au-delà des produits existants et connus en sécurité, plusieurs start-up ont développé ces dernières années des stratégies alternatives pour sécuriser les environnements d'information commerciaux et industriels. Plusieurs d'entre elles étaient présentes à la 20e édition de NetEvents dans la Silicon Valley.

IA CONTESTÉE

La plus visible était Cylance, une société de sécurité d'Irvine (Ca.) qui applique l'intelligence artificielle, l'approche algorithmique et l'apprentissage machine à la sécurisation des systèmes pour utilisateurs finaux. Ce faisant, elle affirme pouvoir protéger les systèmes sans mise à jour (ou en tout cas minimale), même contre les attaques de type zero day (basées donc sur des vulnérabilités pas encore connues). Cylance a 'calculé' en l'occurrence le risque potentiel d'un élément (code, fichier, etc.) sur la base d'un grand nombre de caractéristiques. Cofondée par Stuart McClure, co-auteur du livre 'Hacking exposed', Cylance affirme que son produit a permis de détecter une fuite de données sur 21,5 millions de militaires et personnel de la sécurité nationale de l'administration américaine.

Toujours à NetEvents, la canadienne Wedge Networks (Calgary, Alberta) a annoncé avoir pris une licence sur la technologie de Cylance afin d'intégrer aux réseaux un 'advanced malware block'. Ce faisant, les systèmes non-Windows sont également protégés, y compris les appareils personnels (BYOD), tout en ouvrant des portes sur l'Internet des objets (IoT).

Cela dit, Cylance se lance également dans les produits de sécurité 'de nouvelle génération.' Ainsi, les éditeurs d'antivirus classiques font état du refus de Cylance de participer à des tests comparatifs de produits réputés, alors que des tests comparatifs informels ne démontrent nullement la supériorité de Cylance par rapport aux produits AV classiques, que du contraire.

TROMPERIE ET ISOLEMENT

Pour sa part, l'israélienne Javelin Networks adopte une autre approche pour découvrir très rapidement les 'intrus' ou les collaborateurs internes malveillants. Ainsi, Javelin inonde une entreprise d'un grand nombre de 'faux' systèmes, avec des données apparemment vraies notamment. Après l'attaque, le pirate se met à analyser l'environnement système et dès qu'il pénètre un 'faux' système, il révèle du même coup sa présence. Après quoi les services de sécurité de l'entreprise peuvent le poursuivre (notamment à des fins de forensics) et au final le neutraliser. Javelin se positionne comme une alternative aux systèmes de détection d'intrusion et de 'deep packet inspection'.

De son côté, Menlo Security (Menlo Park, Ca.) mise avec son Isolation Platform sur un usage sécurisé de l'Internet grâce à une protection contre les sites dangereux et les attaques d'hameçonnage. En l'occurrence, l'entreprise considère simplement tous les éléments extérieurs (fichiers, courriels, etc.) comme 'mauvais' et les contrôle dans le cadre d'un isolement rigoureux sur des dizaines de caractéristiques suspectes. L'utilisateur n'a qu'une image sécurisée de cet élément, tandis que l'interaction peut éventuellement être bloquée par un réglage 'read only'.

Cela dit, NetEvents n'a pas fait l'impasse sur les produits établis. Ainsi, le spécialiste de la gestion de réseau Netscout – optimisation de services par une vue big data sur le trafic réseau, notamment pour les communications unifiées – a acquis notamment Arbor Networks suite au rachat récent de Danaher Communications. Au départ conçu pour se protéger contre les attaques DDos, Arbor propose désormais aussi – en associant les informations des produits Netscout et sa propre 'threat intelligence' – des possibilités de protection proactive contre les attaques grâce à ses propres technologies Atlas (corrélation de données) et Asert (analyse de données et réponse).