Cybersécurité : les RSSI parient sur l'automatisation et l'IA

L'équipementier réseau américain Cisco publie son rapport annuel sur la cybersécurité.

L'édition 2018 fait la synthèse de recherches menées par ou pour la multinationale et ses partenaires technologiques (Anomali, Lumeta, Qualys, Radware, SAINT Corporation et TrapX) ces 18 derniers mois. Elle est complétée d'une enquête réalisée auprès de **3600 RSSI** (responsables de la sécurité des systèmes d'information) dans 26 pays.

Premier constat : fin octobre 2017, 50 % du trafic internet mondial était chiffré. Un taux en croissance de 12 points par rapport à novembre 2016, relève Cisco dans son rapport.

Le chiffrement permet d'améliorer la sécurité des internautes et des organisations. Mais il peut aussi servir d'outil puissant pour masquer une activité malveillante, voire une prise de contrôle à distance non autorisée de systèmes et réseaux ciblés.

Pour réduire le temps d'action dont les cyber-attaquants disposent et limiter les dégâts infligés, 39 % des RSSI misent sur l'automatisation. 34 % sur l'apprentissage automatique (machine learning) et 32% sur d'autres applications d'intelligence artificielle (IA).

Par ailleurs, 92 % des RSSI jugent efficaces (44 %) ou très efficaces (48 %) les outils d'analyse du comportement des utilisateurs pour identifier les menaces potentielles.

La protection doit couvrir un périmètre étendu : terminaux, réseaux, cloud, environnement virtualisé, capteurs et autres objets connectés (IoT)…

Dans ce contexte, les RSSI utilisent des solutions de différents fournisseurs pour prévenir et répondre aux cyber-attaques. 25 % d'entre eux travaillaient avec 11 à 20 fournisseurs de solutions de cybersécurité différents en 2017. Un taux en hausse de 7 points par rapport à 2016.

RSSI de tous secteurs…

Le rapport 2018 de Cisco révèle d'autres points sensibles, dont le coût des cyberattaques.

D'après les répondants, plus de la moitié des attaques informatiques rapportées au cours des 12 derniers mois ont entraîné des dommages financiers supérieurs à 500 000 dollars.

Les cyber-attaques sont de plus en plus complexes et étendues. Tous les secteurs sont concernés. Et la logistique n'est pas épargnée, insiste Cisco.

En 2017, plusieurs cas ont été dénombrés. Le programme qui a infecté CCleaner et les rançongiciels et malwares destructeurs Expetr/NotPetya (Nyetya), par exemple, ont fait des dégâts dans les chaînes d'approvisionnement.

Lire également :

Cybersécurité : les prévisions de Sophos pour 2018

Sécurité : la logistique fortement menacée en 2018, selon Kaspersky

(crédit photo © Cisco)