Pour les RSSI, les solutions de cybersécurité ne sont pas satisfaisantes

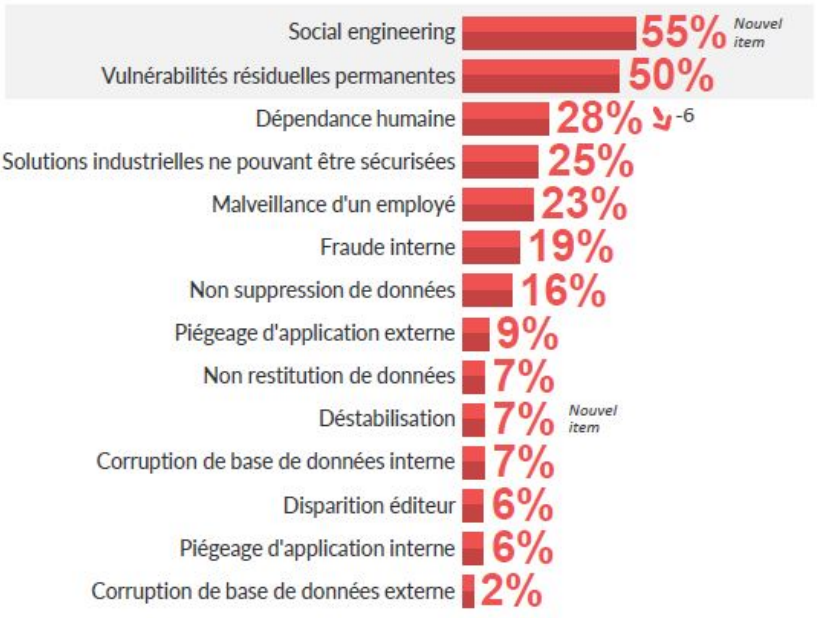
Les cyber-attaques se multiplient, mais les solutions pour y faire face manquent de pertinence. C'est un des principaux enseignements du baromètre réalisé par OpinionWay, pour le Cesin (Club des experts de la sécurité de l'information et du numérique), auprès de 141 RSSI français. 46 % d'entre eux constatent une augmentation des cyberattaques par rapport à l'année dernière, alors que seulement 1 % des responsables interrogés décèlent une baisse. Sans surprise, cette recrudescence des menaces est avant tout marquée par le phénomène des ransomwares, ces malwares qui chiffrent les données des utilisateurs et demandent une rançon pour en restituer l'accès.

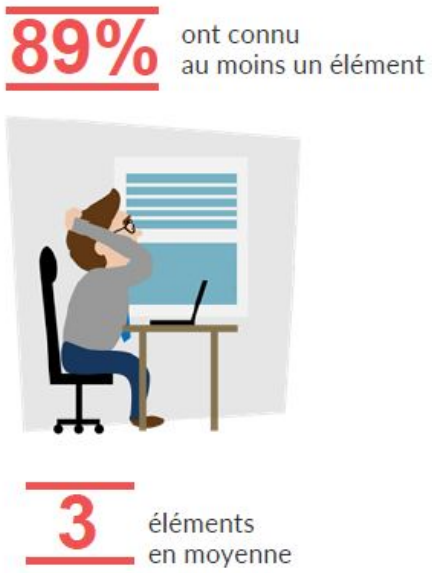
« *Pour les petites entreprises, lutter contre cette menace nécessite des moyens élevés*, relève Olivier Ligneul, le vice-président du Cesin, une association de RSSI, et par ailleurs lui-même responsable de la sécurité des systèmes d'information d'EDF. *Les grandes entreprises parviennent souvent à contenir ce type d'attaques et à nettoyer les postes touchés. Même si on craint toujours une infection massive qui parviendrait à toucher des milliers de machines, car les cybercriminels font évoluer le comportement de ces malwares pour contourner nos défenses.* » Derrière les ransomwares, on retrouve les classiques DDoS et attaques virales. Mais des menaces plus pernicieuses, comme la fraude externe, le vol d'informations ou de données personnelles, figurent également en bonne place dans le tableau dressé par le Cesin.

Nouvelles menaces, vieilles solutions

Notons que ces attaques exploitent des vecteurs assez classiques. Au premier rang desquels – évidemment, serait-on tenté d'écrire – on trouve le spearphishing : 55 % des RSSI interrogés affirment avoir été confrontés à ces mails ciblés visant à tromper leur destinataire et à introduire une menace dans l'entreprise (par exemple via une fausse facture). C'est notamment par ce biais que les ransomwares se propagent la plupart du temps, mais c'est aussi un vecteur classique pour des attaques ciblées, plus pernicieuses visant à dérober des informations sur la durée. Derrière le spearphishing, on retrouve un autre classique : les vulnérabilités résiduelles, autrement dit les failles connues non corrigées. Un problème connu de longue date mais demeure une épine dans le pied de bien des entreprises.

Q6BIS. Parmi les éléments suivants liés à la cyber-sécurité, quels sont ceux auxquels votre entreprise a été concrètement confrontée au cours des 12 derniers mois ?
Base : ensemble (141 répondants) / Plusieurs réponses possibles





Face à cet environnement de plus en plus menaçant, les solutions techniques déployées restent des plus classiques. Outre les incontournables antivirus et pare-feu, on retrouve des solutions traditionnelles comme les VPN, le filtrage Web ou les outils antispam. Si les solutions de SSO et de gestion des log sont déployées dans plus de 6 entreprises sur dix, les résultats sont plus mitigés pour l'authentification forte, la double authentification ou des outils censés contrer des attaques élaborées ou ciblant l'extraction de données (sandboxing, bastion d'autorisations, chiffrement de bases de données ou anti-APT). En moyenne, chaque entreprise sondée a installé 11 solutions complémentaires.

Big Data, IoT : des solutions inadaptées

Mais, globalement, l'efficacité des solutions reste discutée. Si les pare-feu et les VPN sont plébiscités, les autres outils sont critiqués par les RSSI. « *Ce sont avant tout des outils technico-techniques*, assure Olivier Ligneul. *Nous n'avons pas la capacité à disposer d'une analyse fine des cyberattaques. Nous avons besoin d'outils plus intelligents, embarquant de l'IA et capables de se baser sur les impératifs de protection des données et des processus de l'entreprise. Les outils devraient embarquer l'analyse d'impact.* » Autrement dit, face au flot d'attaques, les outils devraient davantage aiguiller les équipes vers celles qui comptent vraiment. 40 % des RSSI interrogés estiment que l'offre du marché n'est plutôt pas ou pas du tout adaptée aux menaces actuelles. Et près de 60 % d'entre eux affirment que ce portefeuille de solutions ne répond pas aux attentes imposées par la transformation numérique (Big Data, IoT notamment). Un verdict assez sévère pour les offreurs de solutions.

Assurance cyber : 1 entreprise sur 4

Malgré ces lacunes, le niveau de préparation des entreprises aux risques en matière de cybersécurité apparaît en progrès. Elles sont 65 % (+ 6 points en un an) à penser que leurs salariés sont sensibilisés à ces questions. Et 57 % des RSSI sondés affirment avoir mis en place des procédures pour tester la bonne application des recommandations. Les budgets semblent suivre, puisque plus d'un responsable de la sécurité sur deux affirme que son entreprise va augmenter son budget cybersécurité dans les 12 mois qui viennent. 84 % des sociétés sondées prévoient d'acheter de nouvelles solutions de protection sur la même période. Autre signe de cette maturité grandissante du sujet cybersécurité : la montée en puissance de l'assurance des risques cyber. 26 % des entreprises interrogées ont souscrit un contrat de ce type, une progression de 7 points en un an. Et 17 % supplémentaires l'envisagent sous un an.

Pour des RSSI dont le rôle s'est affirmé, l'enjeu de l'année qui vient consiste à placer le pilotage des

sujets cybersécurité au bon niveau dans l'entreprise, autrement dit d'impliquer la direction générale. Selon Olivier Ligneul, cette évolution est en cours : « *de plus en plus, les RSSI sont appelés par les comités de direction des entreprises qui veulent comprendre les enjeux en matière de cybersécurité.* » Il est vrai que l'actualité récente permet de moins en moins aux dirigeants de faire mine de regarder ailleurs.

A lire aussi :

Ransomware : les cybercriminels font maintenant la tournée des hôtels

Les antivirus, un poison pour l'écosystème logiciel

Mikko Hypponen : « Le hacking des élections américaines ? Oui, ce sont bien les Russes »

crédit photo : © Nikuwka – shutterstock