CYBERATTAQUES
UNE VEILLE PERMANENTE

Toujours un coup d'avance. Indispensable aux échecs, cette stratégie est difficilement applicable à la lutte contre la cybercriminalité, tant les cyberattaques se caractérisent par une imprévisibilité et une diversité qui rendent délicates toutes anticipations. Voilà pourquoi la veille est primordiale pour réduire les risques.

Sébastien Viou
Directeur cybersécurité produit chez Stormshield
Crédit photo : DR

L'ÉVOLUTION DE LA MENACE

Plus 255% sur une année. Entre 2019 et 2020, les cyberattaques ont explosé (enquête ANSSI, Agence nationale de la sécurité des systèmes d'information, 2021). Ce chiffre illustre une menace omniprésente. À ce titre, Sébastien Viou, directeur cybersécurité produit chez Stormshield, fait remarquer que « malgré la grande médiatisation des attaques ciblant les établissements de santé, ces derniers sont loin d'être les seuls visés. Industrie, finance, administration, aucun domaine n'est épargné ». Pour cet expert, la fréquence des tentatives d'attaques et le profil des menaces sont relativement stables. « Ce qui a changé, c'est avant tout l'impact. Désormais, les conséquences sont beaucoup plus importantes. Cela tient au fait que la menace s'est professionnalisée. Aujourd'hui, les attaques sont plus ciblées, plus structurées et adaptées à chaque cible, là où il y a quelques années, les criminels procédaient massivement et de façon désorganisée. Ils s'insèrent dans les systèmes d'information et en prennent le contrôle pour lancer des ransomwares « chirurgicaux ». Autre spécificité nouvelle : les vulnérabilités sont exploitées sans attendre. À peine sorties, les cybercriminels profitent de la latence des mises à jour pour faire de nombreuses victimes, comme par exemple avec Log4Shell. Lorsque l'on ajoute à cela la surface d'attaque des entreprises qui s'étend – du fait de la multiplication de prestataires extérieurs ou de la généralisation du télétravail –, le cocktail devient détonnant. »

LE CUSTOMER SECURITY LAB, SIGNÉ STORMSHIELD

Pour prévenir les risques, Stormshield, entreprise française, fournit des solutions de cloisonnement, de sécurité réseau et de chiffrement. « Parmi elles, des firewalls, des concentrateurs VPN, de la gestion d'accès à distance, de l'IPS, des solutions de protections des flux industriels spécifiques et des postes de travail ou encore des solutions de chiffrement pour garantir la confidentialité et la conformité RGPD », explique Sébastien Viou. L'entreprise développe des outils de sécurisation adaptés à l'évolution des menaces que subissent ses clients.

Et côté veille, la société mise sur son Customer Security Lab. Cette entité a pour mission de suivre les évolutions des menaces et de mettre à jour le niveau de sécurité des solutions Stormshield afin de garantir une sécurité optimale à ses clients.

Elle collecte un maximum d'informations sur les menaces et vulnérabilités nouvellement découvertes les "0-Day", puis suit leur évolution. En son sein : une dizaine d'experts en cybersécurité et d'analystes capables de décortiquer un malware et de faire de l'ingénierie inversée pour en comprendre son fonctionnement. « Ils utilisent leurs connaissances en CTI (Cyber Threat Intelligence) pour définir la capacité des acteurs malveillants à exploiter les vulnérabilités d'un système. »

Pour cette activité, la multiplication des sources d'information est de mise. Le laboratoire est en veille constante auprès des organismes de gestion des vulnérabilités (NIST, CERT divers), des éditeurs (Microsoft en particulier via le partenariat MAPP) et bien sûr en veille sur les réseaux spécialisés via Twitter ou des forums. Des partenariats sont également noués dans la Communauté Européenne : avec des clients, via le Cybercampus notamment, ou des éditeurs comme Sekoia. « Le partage d'informations (?) est primordial », souligne Sébastien Viou. « Nous sommes efficaces si nous agissons groupés. La cybersécurité exige cet échange entre clients, partenaires et éditeurs. »

UNE RÉPONSE COLLECTIVE ET RAPIDE

Quand la menace est identifiée, le plan de riposte entre en action. Exemple, avec la récente alerte sécurité Spring4Shell. Une vulnérabilité de type « 0-Day » concernant le framework Java « Spring » a été identifiée et corrigée le 31 mars dernier. Son score : 9.8 de type RCE (Remote Code Execution). Très vite, un « Proof Of Concept » d'exploitation est mis en ligne, et les cybercriminels commencent à exploiter cette nouvelle faille. La liste des logiciels et des versions impactés est établie. Stormshield réagit alors en publiant une signature IPS sur son firewall, permettant de détecter et de bloquer les tentatives d'exploitation. L'ensemble des IoCs (indicateurs de compromissions) découverts est ensuite intégré à la base d'IP Réputation. En moins de 48h, le client se voit donc proposer une mise à jour qui le prémunira de l'attaque. « La réponse apportée est la combinaison de nos solutions propres (ici, les signatures IPS et l'IP Réputation), notre analyse de l'exploitation des vulnérabilités et des informations délivrées par l'éditeur attaqué ou par les organismes publics. »

Et pour améliorer encore la détection, la société est en cours de développement d'un projet apportant du machine learning dans ses « sandboxing ». Cette technique consiste à créer un environnement de test isolé, comme un bac à sable, dans lequel il est possible d'exécuter un fichier suspect pour observer son comportement et extraire des indicateurs de compromission. Le « sandboxing » doit être un environnement virtuel sécurisé. « Afin que notre « sandbox » classe automatiquement un fichier comme malveillant, nous la nourrissons d'échantillons bienveillants et malveillants pour affiner son apprentissage », décrit Sébastien Viou.

Toujours en alerte, Stormshield insiste sur l'intérêt d'une cybersécurité européenne pour contrer les risques représentés par les enjeux géopolitiques. « Maîtriser ses infrastructures est devenu un véritable enjeu de pouvoir et cela signifie également maîtriser les moyens de protection », conclut Sébastien Viou.

Carla BERNINI et **Marion BOIS**