**Communiqué de presse**

**Enquête mondiale menée par Sophos :**

**« Les responsables informatiques sont submergés par les cyberattaques »**

Bruxelles - 11 juillet 2019 - **Sophos présente aujourd'hui les résultats de son enquête mondiale intitulée** [**The Impossible Puzzle of Cybersecurity**](https://secure2.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-impossible-puzzle-of-cybersecurity-wp.pdf) **(L’impossible défi de la cybersécurité). Cette dernière révèle que les responsables informatiques sont submergés par les cyberattaques et ont du mal à y faire face en raison d’un manque d’expertise en sécurité, de budget et de technologie à jour. L’enquête a été réalisée auprès de 3 100 décideurs informatiques au sein d’entreprises de taille moyenne en France, au Royaume Uni, en Allemagne aux États-Unis, au Canada, au Mexique, en Colombie, au Brésil, en Australie, au Japon, en Inde et en Afrique du Sud.**

**Les cybercriminels utilisent plusieurs méthodes d'attaque et de charges virales afin d’avoir un impact maximal**

L’enquête montre comment les techniques d’attaque varient et se déroulent, souvent en plusieurs étapes, rendant ainsi la protection des réseaux très complexe. Un responsable informatique sur cinq interrogé ne sait pas comment une telle attaque a pu avoir lieu au sein de son système, et la diversité des méthodes d’attaque signifie qu’aucune stratégie de défense unique ne peut apporter une solution miracle.

*« Les cybercriminels développent leurs méthodes d’attaque et utilisent souvent plusieurs charges virales pour maximiser leurs profits. Les exploits logiciels ont été le point d'entrée initial dans 23% des incidents, mais ils ont également été utilisés d'une manière ou d'une autre dans 35% des attaques, démontrant ainsi comment ils ont eu un effet à plusieurs étapes de la chaîne d'attaque »*, a déclaré Chester Wisniewski, chercheur principal chez Sophos. *« Les entreprises qui ne font qu'appliquer des correctifs externes au niveau des serveurs à haut risque restent vulnérables en interne et les cybercriminels profitent de cette situation ainsi que d'autres failles de sécurité ».*

Le large éventail, les multiples étapes et l’ampleur des attaques actuelles se révèlent être très efficaces. Par exemple, 53% des personnes victimes d'une cyberattaque ont reçu un email de phishing et 30% ont été pris pour cible par un ransomware. 41% des personnes interrogées ont déclaré avoir été victimes d'une violation de données.

**Les maillons faibles au niveau de la sécurité favorisent de plus en plus la compromission de la chaîne logistique**

Sur la base des 300 responsables informatiques français interrogés, les exploits logiciels (20,5%) et le phishing (17%) sont considérés comme des risques majeurs pour la sécurité. De manière alarmante, seulement 4,3% des responsables informatiques français considèrent la chaîne logistique comme un risque majeur pour la sécurité, offrant ainsi une faiblesse supplémentaire que les cybercriminels utiliseront probablement comme un nouveau vecteur d'attaque.

**Manque d'expertise en matière de sécurité, de budget et de technologie à jour**

Selon l’enquête menée par Sophos, 37% des responsables informatiques français ont déclaré consacrer en moyenne 20 à 30 % du temps de leur équipe à la gestion de la sécurité. Pourtant, 52,37% estiment que les compétences en matière de sécurité pourraient être améliorées et 48,7% souhaitent la mise en place d'une équipe plus solide pour détecter, investiguer et réagir face aux incidents de sécurité. Le recrutement de talents est également un problème. En effet, 79% d'entre eux déclarent qu'il est difficile de recruter des personnes possédant les compétences en cybersécurité dont ils ont besoin.

Concernant le budget, 42% ont déclaré que le budget consacré à la cybersécurité au sein de leur entreprise (incluant personnel et technologie) est inférieur à leur besoin. Disposer d’une technologie à jour est un autre problème, 43,7% des personnes interrogées ont confirmé que conserver une technologie de cybersécurité à jour était un véritable défi pour leur entreprise. Ce manque d’expertise en matière de sécurité, de budget et de technologie à jour indique que les responsables informatiques ont du mal à réagir efficacement face aux cyberattaques, pénalisant ainsi la planification et la gestion proactive des activités à venir.

**Synchronized Security résout « l'impossible défi de la cybersécurité »**

Avec les cybermenaces provenant d’attaques au niveau de la chaîne logistique, d’emails de phishing, d’exploits logiciels, de vulnérabilités, de réseaux sans fil non sécurisés, et bien plus encore, les entreprises ont besoin d’une solution de sécurité qui aide à éliminer leurs points faibles et à mieux identifier les menaces jusque-là inconnues. Sophos Synchronized Security, un système intégré unique, fournit cette visibilité indispensable sur les menaces. Il intègre les produits endpoint, network, mobile, Wi-Fi et chiffrement de Sophos pour partager des informations en temps réel et réagir automatiquement face aux incidents. Plus d'informations sur Synchronized Security sont disponibles sur le site Sophos.com.

**L’enquête**L'enquête intitulée « Impossible Puzzle of Cybersecurity » a été réalisée par Vanson Bourne, spécialiste indépendant des études de marché, en décembre 2018 et janvier 2019. Durant cette enquête 3 100 décideurs informatiques ont été interrogés dans 12 pays et sur six continents, aux États-Unis, au Canada, au Mexique, en Colombie, au Brésil, au Royaume-Uni, en France, en Allemagne, en Australie, au Japon, en Inde et en Afrique du Sud. Toutes les personnes interrogées provenaient d'entreprises qui comptaient entre 100 et 5 000 employés.

**À propos de Sophos**Sophos est un leader dans la sécurité Next-Generation des systèmes Endpoint et des réseaux. En tant que pionnier en matière de sécurité synchronisée, Sophos développe son offre innovante qui comprend des solutions pour les systèmes Endpoint, les réseaux, le chiffrement, le web, les emails et les mobiles, afin de mieux travailler ensemble. Plus de 100 millions d’utilisateurs dans 150 pays font confiance à Sophos, et considèrent sa gamme complète de produits de sécurité informatique comme la meilleure solution pour se protéger contre les menaces complexes et la perte de données. Les produits Sophos sont disponibles exclusivement via un réseau mondial de plus de 39 000 partenaires enregistrés. Le siège social de Sophos se situe à Oxford (Royaume-Uni), et Sophos a été introduit à la bourse de Londres sous le nom SOPH. Plus d’informations sont disponibles sur [www.sophos.com](http://www.sophos.com).

**Contacts Presse :**Sandra Van Hauwaert, Square Egg, sandra@square-egg.be, GSM 0497 251816