*Sophos présente l’enquête « Les secrets des Pare-Feu Réseau »*

**‘Des entreprises en danger à cause d'un trafic réseau non identifié’**

* Les responsables informatiques ne peuvent pas identifier 45% du trafic réseau au sein de leur entreprise.
* 84% des entreprises s'accordent à dire que le manque de visibilité sur les applications est un sérieux problème de sécurité.
* 52% des entreprises sont également préoccupées par la perte de productivité due à des applications non désirées ou inutiles qu'elles ne détectent pas sur leur réseau.

Bruxelles, 18 avril 2018 **-** [**Sophos**](http://www.sophos.fr/) **(LSE: SOPH), leader mondial de la sécurité des réseaux et des systèmes endpoint, a présenté aujourd'hui les résultats de son enquête mondiale, Les Secrets des Pare-Feu Réseau, qui révèle que les responsables informatiques n’arrivent pas à identifier 45% du trafic réseau au sein de leur entreprise. En fait, près d'un responsable sur quatre ne parvient pas à identifier 70% de son trafic réseau. Le manque de visibilité implique des défis importants en matière de sécurité pour les entreprises actuelles, et pénalise une gestion efficace du réseau. L'enquête a interrogé plus de 2 700 responsables informatiques de PME, dans 10 pays, dont les États-Unis, le Canada, le Mexique, la France, l'Allemagne, le Royaume-Uni, l'Australie, le Japon, l'Inde et l'Afrique du Sud.**

Compte tenu de l'impact, parfois catastrophique, que les cyberattaques peuvent avoir sur une entreprise, il n'est pas surprenant que 84% des personnes interrogées reconnaissent que le manque de visibilité sur les applications est un sérieux problème en matière de sécurité. Sans la possibilité d'identifier les activités réelles sur leur réseau, les responsables informatiques ne parviennent pas à détecter les ransomwares, les malwares inconnus, d’éventuelles violations de données, des menaces avancées, ainsi que des applications potentiellement malveillantes et des utilisateurs sans scrupules. Les pare-feu réseau avec une détection basée sur les signatures ne sont pas en mesure de fournir une visibilité adéquate sur le trafic des applications, du fait de divers facteurs tels que l'utilisation croissante du chiffrement, l'émulation de navigateur et les techniques d'évasion avancées.

« Si vous ne pouvez avoir une vue globale sur votre réseau, vous ne pourrez jamais être certain que votre entreprise soit correctement protégée contre les menaces. Les professionnels de l'informatique ‘volent à vue’ depuis bien trop longtemps et les cybercriminels en profitent », a déclaré Dan Schiappa, senior vice president & general manager produits chez Sophos. « Avec les gouvernements du monde entier qui imposent des pénalités plus sévères pour la violation et la perte de données, le fait de savoir ‘quoi’ et ‘qui’ est sur votre réseau devient de plus en plus important. Ce type de secret ne peut plus être ignoré ».

En moyenne, les entreprises passent sept jours à réparer 16 machines infectées par mois. Les petites entreprises (100-1 000 utilisateurs) consacrent en moyenne cinq jours à la remédiation de 13 ordinateurs, tandis que les grandes entreprises (1 001 à 5 000 utilisateurs) consacrent en moyenne 10 jours à la remédiation de 20 machines par mois.

« Une unique faille au sein de votre réseau affecte souvent plusieurs ordinateurs. Ainsi, plus vite vous pourrez empêcher la propagation de l'infection, plus vous limiterez les dommages et le temps nécessaire pour nettoyer », a déclaré Schiappa. « Les entreprises sont à la recherche d’une solution Next-Gen intégrée, protégeant à la fois le réseau et les systèmes endpoint, afin de stopper les menaces avancées et empêcher qu'un incident isolé ne se transforme en une épidémie généralisée. Des exploits sophistiqués tels que MimiKatz et EternalBlue ont rappelé à tout le monde que la protection du réseau est essentielle à la sécurité des systèmes endpoint et vice versa. Seul le partage direct d’informations entre ces deux éléments peut révéler la vraie nature du ‘quoi’ et ‘qui’ se trouvent réellement sur votre réseau ».

Les responsables informatiques sont conscients que les pare-feu ont besoin d'une protection renforcée. En fait, l'enquête a révélé que 79% des responsables informatiques interrogés veulent une meilleure protection de la part de leur pare-feu actuel. 99% souhaitent une technologie de pare-feu capable d'isoler automatiquement les ordinateurs infectés, et 97% souhaitent une protection des systèmes endpoint et un pare-feu en provenance du même éditeur, permettant ainsi un partage direct d’informations sur l'état de la sécurité.

**La sécurité n'est pas le seul défi pour les entreprises**

Après les risques de sécurité, la perte de productivité a été citée comme une source de préoccupation pour 52% des personnes interrogées, concernant le manque de visibilité sur le réseau. La productivité des entreprises peut être affectée de manière négative si le service informatique ne peut pas prioriser la bande passante pour les applications critiques.

Pour les secteurs d’activité qui utilisent des logiciels personnalisés pour répondre à des besoins métier spécifiques, l'impossibilité de prioriser ces applications critiques face à un trafic moins important peut s'avérer coûteuse. 50% des professionnels de l'informatique qui avaient investi dans des applications personnalisées ont admis que leur pare-feu ne pouvait pas identifier le trafic et ils étaient donc incapables d’optimiser leur retour sur investissement. Le manque de visibilité génère également une sorte d’angle mort concernant le transfert potentiel de contenu illégal ou inapproprié au niveau des réseaux des entreprises, rendant ainsi ces dernières vulnérables vis-à-vis de litiges et de problèmes de conformité.

« Les entreprises ont besoin d'un pare-feu qui protège leur investissement dans les applications stratégiques et personnalisées en permettant aux employés d'avoir un accès priorisé aux applications dont ils ont besoin », a déclaré M. Schiappa. « Augmenter la visibilité sur le réseau nécessite une approche radicalement différente. En permettant au pare-feu de recevoir des informations directement à partir de la sécurité des systèmes endpoint, il peut maintenant véritablement identifier toutes les applications, même les applications dissimulées ou personnalisées ».

Les résultats de l’enquête sur Les Secrets des Pare-Feu Réseau sont disponibles dans ce rapport PDF.

L'enquête sur Les Secrets des Pare-Feu Réseau a été menée par Vanson Bourne, spécialiste indépendant en études de marché, en octobre et novembre 2017. Cette enquête s’est focalisée sur 2700 décideurs informatiques dans 10 pays, et sur cinq continents, dont les États-Unis, le Canada, le Mexique, la France, l’Allemagne, le Royaume-Uni, l’Australie, le Japon, l’Inde et l’Afrique du Sud. Toutes les personnes interrogées provenaient d'entreprises comptant entre 100 et 5 000 utilisateurs.

**Au sujet 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 26 000 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).

**Informations presse:**

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