**Un quart des directeurs TI belges paieraient une rançon
pour éviter des amendes RGPD**

* *Les petites entreprises sont les dernières à envisager de payer leurs attaquants*
* *Les directeurs TI belges manquent de confiance quant à leur conformité au RGPD*
* *Près de la moitié des entreprises belges ont déménagé leurs données dans le cloud suite au RGPD*

**Bruxelles, le 23 novembre 2018 –** Une nouvelle étude commissionnée par Sophos, un leader dans la sécurité des réseaux et des terminaux, a révélé qu’un quart (24%) des directeurs TI belges, paieraient ‘sûrement’ une rançon à des hackers qui ont volé les données de leur société, plutôt que de rapporter une infraction aux autorités et de payer une amende plus élevée suite au RGPD (Règlement Général sur la Protection des Données) européen.

En outre, 42% des directeurs TI en Belgique prétendent qu’ils ‘pourraient’ envisager de payer la rançon aux criminels, si celle-ci est inférieure à l’amende éventuelle pour l’infraction. Presqu’un tiers (30%) des répondants excluaient fermement vouloir payer leurs assaillants.

**Les directeurs TI belges sont moins enclins à payer que leurs homologues français**

* Les résultats en Belgique ont révélé une plus grande volonté de se conformer aux règles du RGPD qu’en France, où 33% des directeurs TI répondaient qu’ils paieraient ‘sûrement’ une rançon pour éviter une plus grande amende des autorités.
* Dans les autres pays européens mentionnés dans l’étude, les directeurs TI du Royaume-Uni et des Pays-Bas étaient les plus enclins à payer la rançon : 47% des répondants britanniques et 38% des sondés néerlandais paieraient ‘sûrement’.
* En queue du peloton se trouvent les directeurs TI irlandais : 19% seulement d’entre eux répondent être prêts à payer leurs assaillants.

**L’envergure de l’entreprise influence la perspective de paiements de rançons**

* En Europe occidentale, les petites entreprises étaient les moins enclines à répondre positivement à une demande de paiement de rançon. Plus de la moitié des directeurs Ti (51%) de sociétés de moins de 250 travailleurs écartaient carrément la possibilité de payer leurs attaquants.
* Comparez ce chiffre à 20% des directeurs TI des sociétés de 250 à 499 travailleurs et seulement 13% de celles de 500 à 750 travailleurs.

Erik Farine, Regional Director Benelux chez Sophos, dit : *“Les entreprises qui paient la rançon pourraient regagner l’accès à leurs données, mais ce n’est pas certain et c’est également une fausse économie si elles le font pour éviter une amende. Elles doivent toujours communiquer l’infraction aux autorités et pourraient faire face à une amende nettement plus élevée si elles ne le faisaient pas sans délai. Il est surprenant que les plus grandes entreprises semblent vouloir payer la rançon plus rapidement. Or c’est une erreur de faire confiance aux hackers ou de penser que ces derniers vont tout simplement rendre les données. Quel est notre conseil ? Ne payez pas la rançon, avertissez les autorités rapidement et entreprenez les actions nécessaires pour minimiser les risques d’être attaqués à l’avenir. La meilleure façon d’éviter de payer est d’avoir de l’avance sur les cybercriminels. Les hackers ont tendance à compter sur l’hameçonnage, des logiciels non corrigés et des portails d’accès à distance pour s’infiltrer. Donc soyez vigilants pour repérer les signaux d’une éventuelle attaque. Corrigez vos logiciels vite et fréquemment et sécurisez les points d’accès à distance par des mots de passe appropriés et une identification multifactorielle. ”*

**Les directeurs TI belges n’ont pas confiance en leur conformité au RGPD**

* L’étude de Sophos a démontré que les directeurs TI en Belgique sont les moins confiants en Europe occidentale pour ce qui est de leurs préparations au RGPD
* 30% seulement des directeurs TI belges estiment que leur organisation est entièrement conforme aux règles du RGPD. Au Royaume-Uni ce taux s’élève à 46%, aux Pays-Bas à 44% et en France à 37%.
* 20% des directeurs TI en Belgique ont un outil qui prouve leur conformité s’ils sont victimes d’une infraction. Deux tiers (66%) ne disposent pas de ce genre d’outil et 14% ne savent pas s’ils en ont un.
* Un quart seulement (24%) des directeurs TI français prétendaient avoir les outils en place pour prouver qu’ils sont conformes en cas d’infraction. Seules les organisations néerlandaises (27%) sont mieux préparées.

**Presque la moitié des sociétés belges ont transféré leurs données dans le cloud suite au RGPD**

* 46% des répondants disaient avoir accru leur utilisation du nuage informatique entièrement suite au RGPD

**Méthodologie**

Dans le courant des mois d’août et de septembre 2018, l’étude de marché de la société Sapio Resarch a interviewé 906 directeurs et managers TI à propos de leurs expériences et leurs approches concernant la cybercriminalité. Les interviews ont été effectués en ligne, en premier lieu avec des preneurs de décision travaillant dans des compagnies comptant entre 240 en 750 travailleurs et situées en Belgique, en France, en Irlande, aux Pays-Bas et au Royaume-Uni.

**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 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