**Kwart van de Belgische IT-directors zou losgeld betalen**

**om GDPR-boetes te ontlopen**

* *Kleine bedrijven overwegen het minst om hun aanvallers te betalen*
* *Belgische IT-directors missen het vertrouwen in hun naleving van GDPR*
* *Bijna de helft van de Belgische bedrijven heeft vanwege GDPR gegevens naar de cloud verplaatst*

**Brussel, 23 november 2018 –** Nieuw onderzoek dat in opdracht van Sophos is uitgevoerd, toont aan dat een kwart (24%) van de Belgische IT-directors 'absoluut' bereid zou zijn om losgeld te betalen aan hackers die hun bedrijfsgegevens hebben gestolen, in plaats van de overtreding bij de autoriteiten te rapporteren (en daarmee een hogere boete te omzeilen op grond van de algemene verordening van de gegevensbescherming van de EU (GDPR)).

Nog eens 42% van de Belgische IT-leiders zegt dat ze 'mogelijks' zouden overwegen het losgeld van de criminelen te betalen indien dit lager is dan de mogelijke straf voor een overtreding. Bijna een derde (30%) van de respondenten sluit het betalen aan hackers volledig uit.

**Belgische IT-directors betalen minder vaak dan hun tegenhangers in Frankrijk**

* De resultaten in België wijzen op een grotere bereidheid om te voldoen aan de GDPR-regels dan in Frankrijk, waar 33% van de IT-managers zegt dat ze 'absoluut' bereid zouden zijn om losgeld te betalen om een grotere boete met de autoriteiten te voorkomen
* In de bestudeerde West-Europese landen maken IT-directors in het VK en Nederland het meeste kans om losgeld te betalen, 47% van de ondervraagden in het VK en 38% in Nederland zegt 'absoluut' bereid te zijn om te betalen
* Slechts 19% van de ondervraagde Ierse IT-leiders zeggen dat ze 'absoluut' bereid zouden zijn hun aanvallers te betalen

**Bedrijfsgrootte beïnvloedt de vooruitzichten voor ransomware-betalingen**

* In heel West-Europa zijn kleine bedrijven het minst geneigd te overwegen om een ransomware-vraag te betalen. Meer dan de helft (51%) van IT-directors bij bedrijven met minder dan 250 werknemers sluit het betalen van hun aanvallers volledig uit
* Dit in vergelijking met 20% van IT-directors bij bedrijven met 250 - 499 werknemers en slechts 13% van degenen met 500 - 750 personeelsleden

Erik Farine, Regional Director Benelux bij Sophos: *“Bedrijven die losgeld betalen, krijgen misschien weer toegang tot hun gegevens, maar dat is niet gegarandeerd. Losgeld is overigens een verkeerd motief als ze het doen om ​​boetes te voorkomen. Ze dienen de overtreding nog steeds aan de autoriteiten te melden en krijgen een aanzienlijk hogere boete als ze dit niet meteen doen. Het is verrassend dat grotere bedrijven zouden overwegen om ​​losgeld te betalen. Het is een vergissing om hackers te vertrouwen of te verwachten dat ze de gegevens eenvoudigweg teruggeven. Ons advies? Betaal het losgeld niet, informeer de autoriteiten onmiddellijk en zorg ervoor dat er stappen worden ondernomen om in de toekomst geen slachtoffer meer te worden. De beste manier om betalingen te vermijden is om de cybercriminelen een stap voor te blijven. Hackers hebben de neiging om te vertrouwen op phishing e-mails, ongepatchte software en externe toegangspoorten om toegang te krijgen. Bedrijven doen er goed aan om ervoor te zorgen dat de systemen en mensen in staat zijn om de tekenen van aanvallen te herkennen. Maak een vroege patch en patch vaak, en beveilig externe endpoints met de juiste wachtwoorden en multi-factor authenticatie.”*

**Belgische IT-managers missen het vertrouwen in hun naleving van GDPR**

* Sophos’ onderzoek toont ook aan dat IT-directors in België het minst vertrouwen hebben in hun voorbereidingen voor GDPR, van alle West-Europese landen die werden bestudeerd
* Slechts 30% van de IT-directors in België is ervan overtuigd dat hun organisaties volledig aan de GDPR-regels voldoen. Dit in vergelijking met 46% van de IT-directors in het Verenigd Koninkrijk, 44% van die in Nederland en 37% van de respondenten in Frankrijk
* Slechts 20% van de Belgische IT-directors beschikt over een tool om compliance te bewijzen als ze het slachtoffer van een inbreuk zijn. Tweederde (66%) heeft geen dergelijke tool en nog eens 14% weet niet of ze een tool hebben
* Slechts een kwart (24%) van de Franse IT-directors zegt dat ze over tools beschikken om naleving te bewijzen in het geval van een inbreuk. Alleen organisaties in Nederland (27%) zijn in dit opzicht beter voorbereid

**Bijna de helft van de Belgische bedrijven heeft vanwege GDPR gegevens naar de cloud verplaatst**

* 46% van de respondenten zegt dat ze hun gebruik van cloud computing als een direct gevolg van GDPR hebben verhoogd

**Methodologie**

In augustus en september 2018 interviewde marktonderzoeksbureau Sapio Research 906 IT-directors en -managers over hun ervaringen met cybercriminaliteit en benaderingen van cyberbeveiliging. De interviews werden online afgenomen, voornamelijk met IT decision makers die werkzaam zijn in bedrijven met tussen 240 en 750 werknemers in België, Frankrijk, Ierland, Nederland, het Verenigd Koninkrijk en de Republiek Ierland.

**Neem voor meer informatie contact op met:**

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

**Over Sophos**

Meer dan 100 miljoen gebruikers in 150 landen rekenen op Sophos voor de beste bescherming tegen complexe bedreigingen en dataverlies. Sophos levert security- en databeschermingsoplossingen die eenvoudig in te zetten, te beheren en te gebruiken zijn. Zo biedt Sophos prijswinnende oplossingen aan voor endpoint security, web security, e-mail security, network security, mobile security en encryptie. Deze worden ondersteund door Sophos Labs, een wereldwijd netwerk van threat intelligence centra. Het hoofdkwartier van Sophos bevindt zich in Oxford (UK) en in Boston (VS). Meer informatie over Sophos op: [www.sophos.com](http://www.sophos.com).