****

**Sophos:**

**‘Losgeld betalen verdubbelt kosten van een ransomware-aanval’**

* *Internationaal Sophos-onderzoek toont aan dat de gemiddelde kosten van herstel €1,3 miljoen zijn wanneer organisaties losgeld betalen (en €675.000 als ze dat niet doen)*
* *In België is 59% van de ondervraagden het afgelopen jaar aangevallen door ransomware; maar liefst een derde (32%) ging over tot het betalen van losgeld wanneer hun data werd versleuteld; Belgische herstelkosten bedragen gemiddeld €340.000*
* *Publieke sector wordt minst getroffen door ransomware*

OXFORD, 12 mei 2020 – **Sophos laat in het rapport** [**The State of Ransomware 2020**](https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/?url=%2fen-us%2fmedialibrary%2fGated-Assets%2fwhite-papers%2fsophos-the-state-of-ransomware-2020-wp.pdf) **weten dat het betalen van losgeld voor een ransomware-aanval de kosten voor een herstel na een aanval bijna verdubbelt. Het onderzoek, gehouden onder 5.000 IT-beslissers in organisaties in 26 landen in Europa, Amerika, Azië-Pacific en Centraal-Azië, het Midden-Oosten en Afrika, wijst ook uit dat de publieke sector het minst wordt getroffen door ransomware.**

Meer dan de helft (51%) van de organisaties heeft de afgelopen twaalf maanden een aanzienlijke ransomware-aanval ervaren; in 2017 was dit nog 54%. Data werden in bijna driekwart (73%) van de aanvallen versleuteld. De gemiddelde kosten om de impact van een dergelijke aanval aan te pakken – inclusief bedrijfsonderbreking, verloren bestellingen, operationele kosten en losgeld – bedroegen meer dan €675.000. Deze gemiddelde kosten stegen tot 1,3 miljoen euro, bijna twee keer zoveel bij organisaties die losgeld betaalden. Meer dan een kwart (27%) van de door ransomware getroffen organisaties gaf toe het losgeld te hebben betaald.

Op wereldwijd niveau kregen de categorieën media, ontspanning en entertainment de grootste klappen: 60% van de respondenten heeft ransomware-aanvallen aangegeven. De publieke sector werd het minst getroffen; slechts 45% van de ondervraagde organisaties gaf aan slachtoffer te zijn geweest van een aanval.

“Organisaties voelen mogelijk grote druk en betalen hierdoor losgeld om zo schadelijke ‘downtime’ te voorkomen”, zegt Chester Wisniewski, principal research scientist Sophos. “Op het eerste gezicht lijkt het betalen van losgeld een effectieve manier om data terug te krijgen, maar dit is een illusie. Uit onze bevindingen blijkt dat betalen voor tijd en kosten weinig uitmaakt voor de moeite die men erin moet steken om gegevens terug te krijgen. Dit kan zijn omdat het onwaarschijnlijk is dat één enkele decoderingssleutel alles is wat nodig is om volledig te herstellen. Aanvallers kunnen verschillende sleutels hebben. Het gebruik hiervan kan een complexe en tijdrovende aangelegenheid zijn.”

Meer dan de helft (56%) van de ondervraagde IT-managers kon de data van back-ups herstellen zonder losgeld te betalen. Slechts bij 1% leidde het betalen van losgeld niet tot herstel van gegevens. Dit cijfer steeg tot 5% voor overheidsorganisaties. In feite slaagde 13% van de ondervraagde overheidsorganisaties er nooit in om hun versleutelde gegevens te herstellen, vergeleken met 6% in het algemeen.

**Ransomware: de Belgische situatie**

Aan het onderzoek The State of Ransomware 2020 namen 100 Belgische bedrijven deel: 59% van de ondervraagden heeft hierbij aangegeven in het afgelopen jaar slachtoffer te zijn geworden van een ransomware-aanval. Van deze groep was 23% in staat een aanval af te slaan voordat data kon worden versleuteld. Maar liefst een derde (32%) van wie de data werd versleuteld, ging over tot het betalen van losgeld. In België bedroegen de gemiddelde herstelkosten zo’n €340.000. Als laatste werd er aan de Belgische ondervraagden gevraagd of zij verzekerd zijn tegen cybersecurity: 81% gaf in het onderzoek aan hiervoor verzekerd te zijn. Van deze groep heeft 69% ook een verzekering tegen ransomware.

De onderzoekers van SophosLabs hebben met [Maze Ransomware: Victorting Extenders Victims for 1 Year and Counting](https://news.sophos.com/en-us/2020/05/12/maze-ransomware-1-year-counting/), een rapport gepubliceerd waarin de tools, technieken en procedures worden bekeken waarin data-encryptie wordt gecombineerd met informatiediefstal en de dreiging van het openbaar maken van data. Deze aanpak die volgens Sophos-onderzoekers ook is gebruikt door andere ransomwarefamilies (zoals LockBit) is bedoeld om de druk op slachtoffers om losgeld te betalen, te vergroten. Het nieuwe Sophos-rapport zal beveiligingsprofessionals helpen het veranderende gedrag van aanvallers van ransomware beter te begrijpen, erop te anticiperen en hun organisaties te beschermen.

"Een effectief back-upsysteem waarmee organisaties versleutelde data kunnen herstellen zonder de aanvallers te betalen, is bedrijfskritisch. Er zijn echter nog andere belangrijke zaken om bedrijven resistent te maken tegen ransomware", voegt Wisniewski eraan toe. "Geavanceerde tegenstanders zoals de operators achter de Maze-ransomware coderen niet alleen bestanden, ze stelen gegevens voor mogelijke blootstelling of afpersingsdoeleinden. Sommige aanvallers proberen ook back-ups te verwijderen of te saboteren om het voor slachtoffers moeilijker te maken data te herstellen en de druk op hen te verhogen. Het offline bewaren van back-ups is de manier om deze kwaadaardige manoeuvres aan te pakken. Ook het gebruik van multi-layered beveiligingsoplossingen behoort tot de oplossingen.”

**Over het onderzoek**

De State of Ransomware 2020-enquête werd uitgevoerd door Vanson Bourne, een onafhankelijke specialist in marktonderzoek, in januari en februari 2020. Onderzoekers interviewden 5.000 IT-besluitvormers in 26 landen: de VS, Canada, Brazilië, Colombia, Mexico, Frankrijk, Duitsland, het VK, Italië, Nederland, België, Spanje, Zweden, Polen, Tsjechië, Turkije, India, Nigeria, Zuid-Afrika, Australië, China, Japan, Singapore, Maleisië, de Filippijnen en de UAE. Alle respondenten waren afkomstig van organisaties met tussen de 100 en 5.000 werknemers.

**Over Sophos**

Als een wereldwijde leider in *next-gen* cybersecurity beschermt Sophos meer dan 400.000 organisaties, ongeacht bedrijfsgrootte, in meer dan 150 landen tegen de meest geavanceerde cyberdreigingen van vandaag. Aangedreven door SophosLabs, een wereldwijd team gespecialiseerd in bedreiginginformatie en wetenschappelijke data, beveiligen Sophos’ cloud-native en AI-verbeterde oplossingen endpoints (laptops, servers en mobiele apparaten) en netwerken tegen immer evoluerende cybercriminele tactieken en technieken. Hieronder vallen onder meer geautomatiseerde en actieve, vijandige inbreuken, ransomware, malware, exploits, data-exfiltration, phishing en meer. Het cloudgebaseerde Sophos Central-platform integreert Sophos’ gehele portfolio - van Intercept X-endpointoplossing tot XG Firewall - in een enkel systeem: Synchronized Security.

Sophos-producten zijn exclusief verkrijgbaar via een wereldwijd kanaal van meer dan 53.000 partners en Managed Service Providers. Sophos stelt zijn innovatieve commerciële technologieën ook beschikbaar aan consumenten via Sophos Home. Het bedrijf is gevestigd in Oxford, Verenigd Koninkrijk. Meer informatie: [www.sophos.com](http://www.sophos.com).

**Voor meer informatie, interviewmogelijkheden of beeldmateriaal:**

Square Egg Communications, Sandra Van Hauwaert, sandra@square-egg.be, GSM 0497251816.