**Persbericht**

**“Gemiddelde herstelkosten ransomware binnen een jaar verdubbeld naar iets meer dan 1,5 miljoen euro”**

* *Sophos-rapport ‘State of Ransomware 2021’ onthult dat slechts 8% van de bedrijven die losgeld betalen, al hun data terugkrijgt*
* *54% zegt dat cyberaanvallen te geavanceerd zijn om door eigen IT-teams te worden afgehandeld*

Oosterhout, 27 april 2021 – **Sophos heeft in zijn onderzoek 'The State of Ransomware 2021' bekendgemaakt dat de gemiddelde herstelkosten na een ransomware-aanval in een jaar tijd meer dan verdubbeld zijn, van € 631.000 in 2020 tot € 1.540.000 in 2021. Het gemiddelde losgeldbedrag dat werd betaald bedroeg € 141.000. De bevindingen van dit wereldwijde onderzoek tonen ook aan dat slechts 8% van de organisaties erin slaagt al hun data terug te krijgen na betaling van losgeld, terwijl 29% niet meer dan de helft van hun gegevens terugkrijgt.**

De 5.400 respondenten zijn IT-besluitvormers in middelgrote organisaties in 30 landen in Amerika, Azië-Pacific en Centraal-Azië, het Midden-Oosten, Afrika en Europa. Voor de Benelux waren er 250 deelnemers.

Hoewel het aantal organisaties in het onderzoek dat een ransomware-aanval heeft meegemaakt is gedaald (51% in 2020 tot 37% in 2021) en minder organisaties te kampen hebben met dataencryptie als gevolg van een aanval (54% in 2021 vergeleken met 73% in 2020) tonen de onderzoeksgegevens een aantal zorgwekkende trends, en met name over de impact van ransomware-aanvallen.

"De schijnbare afname van het aantal organisaties dat wordt getroffen door ransomware is goed nieuws, maar wordt getemperd door het feit dat dit waarschijnlijk, althans gedeeltelijk, veranderingen in het gedrag van aanvallers weerspiegelt", aldus Chester Wisniewski, principal research scientist bij Sophos. "We hebben gezien dat aanvallers zijn overgestapt van grootschalige, generieke, geautomatiseerde aanvallen naar meer gerichte aanvallen, waaronder menselijke *hands-on-keyboard* hacking. Hoewel het totale aantal aanvallen daardoor lager is, leert de ervaring helaas dat de kans op schade door deze meer geavanceerde en gerichte aanvallen veel groter is. Dergelijke aanvallen zijn ook moeilijker te herstellen, en we zien dit in de enquête in de verdubbeling van de totale herstelkosten terug.”

De belangrijkste bevindingen van het rapport:

* Het aantal organisaties dat losgeld betaalde, steeg van 26% in 2020 naar 33% in 2021, hoewel minder dan een op de tien (8%) erin slaagde al hun gegevens terug te krijgen;
* Het gemiddeld betaalde losgeld was € 141.000. De meest voorkomende betaling was € 8.300, met als hoogste € 2,7 miljoen. Tien organisaties betaalden losgeld van € 690.000 of meer;
* De gemiddelde kosten voor het aanpakken van de impact van een ransomware-aanval zijn de afgelopen twaalf maanden meer dan verdubbeld. De herstel- en overige kosten, waaronder downtime van het bedrijf, verloren bestellingen en operationele kosten stegen van gemiddeld € 631.000 in 2020 tot € 1.540.000 in 2021. Dit betekent dat de gemiddelde kosten tien keer hoger zijn dan de gemiddelde losgeldbetaling.

"De bevindingen in het onderzoek bevestigen de harde waarheid dat het niet loont om te betalen in het geval van een ransomware-aanval. Ondanks dat meer organisaties ervoor kozen om losgeld te betalen, kreeg slechts een kleine minderheid van degenen die betaalden al hun data terug ”, vervolgt Wisniewski. “Dit kan gedeeltelijk zijn omdat het gebruik van decoderingssleutels gecompliceerd kan zijn. Bovendien is er geen garantie voor succes. Zoals we onlangs hebben gezien met de DearCry- en Black Kingdom-ransomware kunnen aanvallen die worden gestart met lage kwaliteit of snel samengestelde code en technieken het herstel van data moeilijk, of zelfs onmogelijk maken.”

* Meer dan de helft (54%) van de respondenten is van mening dat cyberaanvallen op dit moment te geavanceerd zijn om door hun IT-team alleen te worden afgehandeld
* Afpersing zonder encryptie neemt toe. Een kleine maar belangrijke 7% zei dat hun gegevens niet waren versleuteld maar dat ze toch afgeperst werden om te betalen. Mogelijk omdat de aanvallers erin waren geslaagd informatie te stelen. In 2020 was dit nog 3%.

"Het herstel na een ransomware-aanval kan jaren duren en gaat over zoveel meer dan alleen het decoderen en dataherstel", vervolgt Wisniewski. “Hele systemen moeten van de grond af aan opnieuw worden opgebouwd. En vergeet ook niet de operationele downtime, de impact op de klant, etc. Verder evolueert de definitie van wat een ‘ransomware-aanval is’. Voor een kleine maar aanzienlijke minderheid van de respondenten betroffen de aanvallen betalingsverzoeken zonder dataencryptie. Dit kan zijn omdat ze anti-ransomware-technologieën hadden om de encryptiefase te blokkeren of omdat de aanvallers er simpelweg voor kozen om de gegevens niet te versleutelen. Het is waarschijnlijk dat aanvallers betaling eisten om geen gestolen informatie online te publiceren. Het is belangrijker dan ooit om je te beschermen voordat aanvallers de kans krijgen om hun steeds veelzijdiger aanvallen uit te rollen. Wanneer organisaties worden aangevallen, hoeven ze deze uitdaging gelukkig niet alleen aan te gaan. Ondersteuning is 24 uur per dag, 7 dagen per week beschikbaar in de vorm van externe beveiligingscentra, door *threat hunters* en incident responsteams."

**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:**

Sandra Van Hauwaert, Square Egg Communications, [sandra@square-egg.be](mailto:sandra@square-egg.be), GSM 0497 251816.