****

**Wereldwijd onderzoek Sophos:**

**“Organisaties nooit meer dezelfde nadat ze getroffen zijn door ransomware”**

* *Vertrouwen van IT-managers en de aanpak van cyberaanvallen verschilt enorm tussen degenen die getroffen zijn door ransomware en zij die nog moeten;*
* *Nieuwe Ryuk ransomware-technieken onderstrepen hoe snel aanvallers schakelen*
* *Onderzoek gehouden onder 5.000 bedrijven*

**Oosterhout, 14 oktober 2020** – Sophos concludeert in zijn meest recente onderzoek [**Cybersecurity: The Human Challenge**](https://www.sophos.com/en-us/content/cybersecurity-the-human-challenge.aspx) dat organisaties nooit meer dezelfde zijn nadat ze door ransomware zijn getroffen. Met name het vertrouwen van IT-managers en hun aanpak om cyberaanvallen te bestrijden, verschillen aanzienlijk naargelang hun organisatie al dan niet is aangevallen door ransomware.

IT-managers van organisaties die door ransomware zijn getroffen, hebben bijvoorbeeld bijna drie keer zoveel kans om zich "aanzienlijk achtergesteld" te voelen als het gaat om het begrijpen van cyberdreigingen – dit in vergelijking met hun collega's in organisaties die niet werden getroffen (17% versus 6%).

Meer dan een derde (35%) van de slachtoffers van ransomware geeft aan dat het werven en behouden van bekwame IT-security professionals de grootste uitdaging vormt als het gaat om cyberbeveiliging (ter vergelijking: 19% van degenen die niet waren getroffen).

Wanneer het de security focus betreft, blijkt uit de enquête dat slachtoffers van ransomware verhoudingsgewijs minder tijd besteden aan het voorkomen van bedreigingen (42,6%) en meer tijd aan respons (27%), in vergelijking met degenen die niet zijn getroffen (respectievelijk 49% en 22%).

“Het verschil in personele prioriteiten zou erop kunnen wijzen dat slachtoffers van ransomware in het algemeen meer incidenten te verwerken krijgen. Het zou echter evengoed kunnen aangeven dat ze alerter zijn op de complexe, meerfasige aard van geavanceerde aanvallen en net daarom meer middelen inzetten voor het opsporen en reageren op de aanwijzingen dat een aanval op til is, ”aldus Chester Wisniewski, principal research scientist bij Sophos.

Het feit dat ransomware-aanvallers hun tactieken, technieken en procedures (TTP's) blijven ontwikkelen, draagt ​​bij aan de druk op IT-beveiligingsteams. Onlangs deconstrueerde Sophos in een artikel een recente aanval met Ryuk-ransomware waarbij werd ontdekt dat de aanvallers algemeen beschikbare en legitieme tools gebruikten om ransomware in te zetten. Dit ging gepaard met grote snelheid: binnen drie en een half uur nadat een medewerker een kwaadwillende phishing e-mailbijlage had geopend, waren de aanvallers al actief binnen het netwerk. Binnen 24 uur hadden de aanvallers toegang tot een domeincontroller en konden ze Ryuk lanceren.

“Ons onderzoek naar de recente Ryuk ransomware-aanval laat zien waar verdedigers mee te maken hebben. IT-beveiligingsteams moeten 24 uur per dag, zeven dagen per week volledig alert zijn en een volledig inzicht hebben in de nieuwste dreigingsinformatie over de tools en het gedrag van aanvallers. De bevindingen van het onderzoek illustreren duidelijk de impact van deze bijna onmogelijke eisen. Onder andere werd vastgesteld dat degenen die door ransomware werden getroffen, het vertrouwen in hun eigen cyberdreigingsbewustzijn ernstig hadden ondermijnd. Hun ransomware-ervaringen lijken hen echter ook een grotere waardering te hebben gegeven voor het belang van bekwame cyberbeveiligingsprofessionals, evenals een gevoel van urgentie bij het introduceren van door mensen geleide dreigingsjacht om het nieuwste gedrag van aanvallers beter te begrijpen en te identificeren”, aldus Wisniewski. "Wat de redenen ook zijn, het is duidelijk dat als het op beveiliging aankomt, een organisatie nooit meer dezelfde is na te zijn getroffen door ransomware."

**Over het onderzoek**

Het onderzoek **Cybersecurity: The Human Challenge** werd in januari en februari 2020 uitgevoerd en werden 5.000 IT-besluitvormers in 26 landen gesproken. Voor de Benelux werden er 200 bedrijven in Nederland en 100 in België geïnterviewd. Alle respondenten zijn afkomstig uit 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:**

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