**Onderzoek Sophos: “68% van de Belgische organisaties slachtoffer van cyberincidenten in de public cloud”**

*Ransomware en malware, blootgestelde data, besmette accounts en cryptojacking als hoofdschuldigen; AVG is veelbelovend waardoor Europeanen het minst lijden*

**Oosterhout**, **8 juli 2020** - Volgens [The State of Cloud Security 2020](https://secure2.sophos.com/en-us/content/state-of-cloud-security.aspx), een wereldwijd onderzoek dat door Sophos is gehouden, heeft 68% van de organisaties in België het afgelopen jaar een beveiligingsincident in de public cloud ervaren. Hierbij waren onder meer ransomware en andere malware (66%), cryptojacking (26%), blootgestelde data (21%) en gecompromitteerde accounts (21%) de voornaamste boosdoeners. Organisaties met meerdere cloudomgevingen hebben meer dan 50% kans op een cloudbeveiligingsincident dan organisaties met slechts een enkele cloudomgeving.

Europeanen hebben het laagste percentage beveiligingsincidenten in de cloud meegemaakt. Het geeft aan dat de richtlijnen van de General Data Protection Regulation (‘AVG’) helpen te voorkomen dat ze in gevaar komen. India deed het daarentegen het slechtst: 93% van de organisaties werd het afgelopen jaar getroffen door een aanval.

Chester Wisniewski, principal research scientist bij Sophos: “Ransomware is, niet verrassend, een van de meest gerapporteerde cybercriminaliteiten in de public cloud. De meest succesvolle ransomware-aanvallen omvatten data in de openbare cloud, aldus het rapport. Aanvallers verleggen hun methoden naar cloud-aanvallen die de noodzakelijke infrastructuur verlammen en de kans op een betaling vergroten. De recente toename van remote werken zorgt voor extra motivatie om de cloudinfrastructuur, waarop meer dan ooit wordt vertrouwd, uit te schakelen. Je mag het gerust zorgwekkend noemen dat veel organisaties hun verantwoordelijkheid bij het beveiligen van cloudgegevens nog steeds niet begrijpen. Cloudbeveiliging is een gedeelde verantwoordelijkheid en organisaties moeten cloudomgevingen zorgvuldig beheren en bewaken om aanvallers een stap voor te blijven.”

**Hoe aanvallers binnenkomen**

Blootstelling blijft organisaties plagen, met verkeerde configuraties die in 58% van de gemelde aanvallen in België worden uitgebuit. In het [SophosLabs 2020 Threat Report](https://www.sophos.com/en-us/labs/security-threat-report.aspx) wordt vermeld dat verkeerde configuraties tot de meeste incidenten leiden, en komen ze maar al te vaak voor, gezien de complexiteit van cloudbeheer.

Bovendien meldt 35% van de organisaties dat cybercriminelen toegang verkrijgen via gestolen inloggegevens van cloudproviders. Desondanks is slechts een kwart van de organisaties van mening dat het beheren van de toegang tot cloudaccounts een belangrijk punt van zorg is. Uit gegevens van [Sophos Cloud Optix](https://news.sophos.com/en-us/2020/07/08/cloud-security-best-practices/), een tool voor het beheer van houdingen in de cloudbeveiliging, blijkt verder dat 91% van de accounts een overmachtige rol voor identiteits- en toegangsbeheer heeft en dat 98% multi-factor authenticatie op hun cloudprovideraccounts heeft uitgeschakeld.

**‘Silver Lining’**

Bijna alle Belgische respondenten (85%) geven toe bezorgd te zijn over het huidige niveau van hun cloudbeveiliging. Passend genoeg staan ​​‘datalekken’ voor een derde van de respondenten bovenaan de lijst met beveiligingsproblemen (36%). Het identificeren van en reageren op beveiligingsincidenten staat met 30% op de tweede plaats. Ondanks deze ‘Silver Lining’ ziet slechts 1 op de 4 respondenten het gebrek aan deskundigheid van gedegen personeel als topprioriteit.

**Methodologie**

De State of Cloud Security 2020-studie is het resultaat van een onafhankelijk onderzoek door Vanson Bourne van meer dan 3.500 IT-managers in 26 landen in Europa, Amerika, Azië-Pacific, het Midden-Oosten en Afrika, wiens bedrijf momenteel gegevens en applicaties host in de openbare cloud.

De volledige studie, samen met een gedetailleerde lijst met aanbevelingen voor cloudbeveiliging, is beschikbaar op https://secure2.sophos.com/en-us/content/state-of-Cloud-security.aspx

**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 0497251816