Kein sicheres Wolkenschloss

Sophos-Umfrage: Cyber-Sicherheitsvorfälle in der Public Cloud bei fast drei Viertel der Unternehmen weltweit

- *Weltweit 70 Prozent der Organisationen betroffen*
- *Die Vorfälle durch Ransom- und andere Malware, ungeschützte Daten, kompromittierte Konten und Cryptojacking*
- *EU-DSGVO zeigt Wirkung, Europa weniger betroffen*

Wiesbaden, 9. Juli 2020 Sophos gibt weitere Ergebnisse aus seiner weltweiten Umfrage The State of Cloud Security 2020 bekannt. Demnach erlebten fast drei Viertel (70 Prozent) der Unternehmen im letzten Jahr einen Public Cloud-Sicherheitsvorfall – dazu zählten Ransomware und andere Malware (50 Prozent), ungeschützte Daten (29 Prozent), kompromittierte Konten (25 Prozent) und Cryptojacking (17 Prozent). Bei Organisationen mit Multi-Cloud-Umgebungen zeigt sich dabei eine um mehr als 50 Prozent höhere Wahrscheinlichkeit einen Cloud-Sicherheitsvorfall zu erleiden als bei Organisationen, die eine einzelne Cloud betreiben. Deutsche Unternehmen waren zu 61 Prozent von Vorfällen betroffen.

EU-DSGVO zeigt Wirkung

Mit viel Aufwand und unter hoher Kritik eingeführt, scheint die europäische Datenschutzgrundverordnung im weltweiten Vergleich eine positive Wirkung zu zeigen. Unternehmen in Europa hatten laut der Umfrage den niedrigsten Prozentsatz an Sicherheitsvorfällen in der Cloud zu verzeichnen – ein Indikator dafür, dass die Einhaltung der Richtlinien der EU-DSGVO dazu beiträgt, Organisationen vor einer Kompromittierung zu schützen. Am schlimmsten traf es dagegen Indien, wo 93 Prozent der Organisationen im vergangenen Jahr von einem Cyberangriff auf Daten in einer öffentlichen Cloud betroffen waren.

Daten in Public Clouds geraten besonders häufig in Geiselhaft

„Ransomware ist, was nicht überrascht, einer der meist gemeldeten Cybercrime-Vorfälle in der öffentlichen Cloud“, sagt Chester Wisniewski, Principal Research Scientist bei Sophos. „Schon unser Report State of Ransomware 2020 hat gezeigt, dass Lösegeld-Angriffe auf Daten in der öffentlichen Cloud zu den erfolgreichsten Attacken zählen.“ Die Angreifer ändern zudem stetig ihre Methoden, um Cloud-Umgebungen ins Visier zu nehmen, notwendige Infrastrukturen lahm zu legen und den Druck auf Unternehmen zu erhöhen, um Lösegeldzahlungen zu kassieren.

Home-Office als zusätzliche Verlockung für Cloud-Angreifer

„Die jüngste Zunahme von Remote-Arbeitsplätzen stellt eine zusätzliche Motivation dar, Cloud-Infrastrukturen, auf die man sich mehr denn je verlässt, zu attackieren und zu deaktivieren,“ so Chester Wisniewski weiter. „Es ist vor diesem Hintergrund beunruhigend, dass sich viele Unternehmen ihrer Verantwortung für die Sicherheit von Cloud-Daten und -Workloads noch immer nicht bewusst sind. Cloud-Sicherheit ist eine Aufgabe, die Unternehmen und Cloud Provider gemeinsam wahrnehmen. Organisationen müssen daher unbedingt ihren Part der Verantwortung übernehmen und ihre Cloud-Umgebungen sorgfältig verwalten und überwachen, um entschlossenen Angreifern immer einen Schritt voraus zu sein.“

Die unbeabsichtigt offene Tür: Wie Angreifer einbrechen
Nach wie vor werden Organisationen durch eigene Fehler, quasi aus Versehen, zu Opfern von Daten-Angriffen. Wie im SophosLabs 2020 Threat Report bereits ausführlich beschrieben, sind Fehlkonfigurationen – nicht zuletzt angesichts der Komplexität des Cloud Managements – die Ursache für die Mehrzahl der Vorfälle: 66 Prozent der gemeldeten Angriffe entfallen auf Fehlkonfigurationen. Darüber hinaus geben 33 Prozent der befragten Unternehmen an, dass Cyberkriminelle sich Zugriff auf gestohlene Zugangsdaten von Cloud-Providern verschafft haben. Interessant dabei: Trotz dieser Zahl gibt nur ein Viertel der befragten Organisationen an, dass die Verwaltung des Zugriffs auf Cloud-Konten für sie ein Top-Thema für die IT-Sicherheit ist. Daten von Sophos Cloud Optix (Data from Sophos Cloud Optix), einem Tool zur Verwaltung der Sicherheitslage in der Cloud, zeigen außerdem, dass 91 Prozent der Accounts über privilegierte Identitäts- und Zugriffsverwaltungsfunktionen verfügen, aber 98 Prozent die Multi-Faktor-Authentifizierung in ihren Cloud-Provider-Accounts gar nicht nutzen und deaktiviert haben.

Der Silberstreifen am Datensicherheits-Horizont
Nahezu alle Befragten (96 Prozent) geben zu, dass sie sich Sorgen über ihr derzeitiges Sicherheitsniveau in der Cloud machen, ein ermutigendes Zeichen dafür, dass dies von höchster Bedeutung ist. Dementsprechend stehen „Datenlecks“ für fast die Hälfte der Befragten (44 Prozent) ganz oben auf der Liste der Sicherheitsbedenken, an zweiter Stelle steht die Identifizierung und Reaktion auf Sicherheitsvorfälle (41 Prozent). Ungeachtet dieses Silberstreifens ist nur einer von vier Befragten der Ansicht, dass mangelnde Fachkenntnisse des Personals zu den größten Sorgen gehören.

Über die Umfrage
Der Report „State of Cloud Security 2020“ wurde von Vanson Bourne im Auftrag von Sophos unter mehr als 3.500 IT-Managern in 26 Ländern in Europa, Nord- und Südamerika, im Asien-Pazifik-Raum, im Nahen Osten und in Afrika durchgeführt, deren Unternehmen Daten und Workloads in der öffentlichen Cloud hosten.

Der vollständige Bericht ist zusammen mit einer detaillierten Liste von Empfehlungen zur Sicherheit in der Cloud unter The State of Cloud Security 2020

Über Sophos
Als ein weltweit führender Anbieter von Next-Generation-Cybersicherheit schützt Sophos mehr als 400.000 Unternehmen jeder Größe in über 150 Ländern vor den neuesten Cyberbedrohungen. Mit den SophosLabs und seinem globalen Team für Bedrohungs- und Datenanalyse schützen die Cloud- und KI-gestützten Sophos-Lösungen Endpoints (Laptops, Server und mobile Geräte) sowie Netzwerke vor sich ständig verändernden Cyberangriffen, einschließlich Ransomware, Malware, Exploits, Datenexfiltration, individuellen Hackervorstößen, Phishing und mehr. Die cloud-basierte Plattform Sophos Central integriert über APIs das gesamte Next Generation Sophos-Portfolio, von der Intercept X Endpoint-Lösung bis zur XG Firewall, in einem einzigen Synchronized-Security-System. Sophos treibt die Entwicklung zur Next Generation Cybersicherheit voran und setzt fortschrittliche Technologien, beispielsweise aus den Bereichen Cloud, Machine Learning, APIs, Automatisierung oder Managed Threat Response ein, um Unternehmen jeder Größe Schutz der Enterprise-Klasse zu bieten. Sophos vertreibt Produkte und Services exklusiv über einen globalen Channel mit mehr als 53.000 Partnern und Managed Service Providern (MSP). Sophos stellt seine innovativen, gewerblichen Technologien auch Privatanwendern via Sophos Home zur Verfügung. Das Unternehmen hat seinen Hauptsitz in Oxford, Großbritannien. Weitere Informationen unter www.sophos.de.

Pressekontakt:

Sophos
Jörg Schindler, PR Manager CEEMEA
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de