

Cyberkriminalität: Der Druck auf Cloud-Anbieter nimmt zu **NETSCOUT veröffentlicht jährlichen weltweiten Sicherheitsbericht**

- DDoS-Angriffe auf Cloud-Anbieter steigen um 14 Prozent
- 95 Prozent aller Service Provider haben 2018 DDoS-Angriffe verzeichnet
- Politisch motivierte Attacken auf Regierungen nehmen zu - und werden auch für Unternehmen zu einer echten Bedrohung

Fast jeder zweite Cloud Service Provider hat Distributed-Denial-of-Service (DDoS)-Attacken im vergangenen Jahr registriert. Dies ist ein Plus von 14 Prozent gegenüber 2017. Geschäftskritische Unternehmensprozesse sind zunehmend von der Verfügbarkeit Cloud-basierter Dienste abhängig. Gleichzeitig sind Cloud-Angebote ein integraler Bestandteil im Portfolio vieler Anbieter. Daher haben erfolgreiche Cyberangriffe das Potenzial, sowohl den Anbietern als auch Nutzern erheblichen Schaden zuzufügen. Das sind Ergebnisse des jährlichen Worldwide Infrastructure Security Report (WISR). Dieser wird von NETSCOUT, ein Marktführer für Service-Assurance- und Cybersecurity-Lösungen, veröffentlicht. Die weiteren Zahlen zeigen im Vorjahresvergleich, 2017 bis 2018, einen klaren Trend zu gezielten Angriffen auf Anbieter und deren Cloud-Dienste.

Ziel der Angreifer, die DDoS-Attacken einsetzen, ist es, Internet-Services, IT-Komponenten oder die IT-Infrastruktur eines attackierten Unternehmens zu verlangsamen, gänzlich lahmzulegen oder zu schädigen. 2017 standen noch Finanzdienstleister, E-Commerce-Anbieter und Gaming-Plattformen im Fokus der Cyberkriminellen. Nun geraten insbesondere Regierungen und staatliche Organisationen ins Kreuzfeuer der Angreifer. Die Motivation hinter DDoS-Attacken verändert sich ebenfalls. Ging es im Vorjahr vor allem um Erpressungsversuche, steht nun politischer und ideologischer Hacktivismus im Vordergrund. Darüber hinaus professionalisieren Akteure sich und ihre Angriffsmethoden und vermieten diese. So können auch zunehmend Laien für geringes Geld, DDoS-Angriffe in Auftrag geben oder selbst starten. Da die politische Instabilität und Wahlmanipulationen weltweit zunehmen, erwartet NETSCOUT, dass DDoS-Angriffe sowohl als Form des Protestes als auch als Waffe in geopolitischen Streitigkeiten künftig vermehrt eingesetzt werden.

Insgesamt mussten 95 Prozent aller Service Provider DDoS-Angriffe im Jahr 2018 verzeichnen. Das entspricht einem Anstieg von 10 Prozent gegenüber dem Vorjahr. Die Attacken erreichten dabei eine Rekordgröße von 1,7 Terabit pro Sekunde. So geben 88 Prozent der befragten Service Provider an, dass DDoS-Angriffe daher aktuell ihre größten Sicherheitsbedenken sind.

„Die Cloud ist zu einem festen Bestandteil unseres privaten und geschäftlichen Alltags geworden. Es werden immer mehr Daten in der Cloud gelagert und zunehmend mehr Dienste darüber abgewickelt. So ist es nicht verwunderlich, dass Angreifer sich auf die dahinterliegenden Infrastrukturen fokussieren“, sagt Darren Anstee, NETSCOUT CTO für den Bereich Sicherheit. „Da hybride und Multi-Cloud-Umgebungen in Naher Zukunft zudem zum Regelfall werden, setzen Cyberkriminelle zunehmend auf komplexere Multi-Vektor-Angriffe. Professionelle Sicherheitsfunktionen und umfassende Transparenz in die eigene IT-Infrastruktur wird damit zum wesentlichen Faktor für Unternehmen und Organisationen.“

Über den Sicherheitsbericht:

Befragt wurden weltweit 231 Service Provider, Cloud- und Hosting Provider, Mobilfunkbetreiber, Unternehmen und andere Netzbetreiber. Bei zwei Drittel der Befragten handelt es sich um Sicherheits-, Netzwerk- oder IT-Spezialisten.

Die Umfrage deckt eine breite Palette von Themen ab – von DDoS-Angriffen über Trends in der Industrie bis hin zu Aspekten der Unternehmensorganisation wie das Testen und Trainieren von Notfallplänen (Rapid Response Plan) sowie die Personal- und Finanzausstattung. Der Fokus der Umfrage lag auf operativen Herausforderungen des Tagesgeschäfts und Strategien, mit denen Netzbetreiber diesen Herausforderungen begegnen und Cyberangriffe abwehren können.

###

Über NETSCOUT

NETSCOUT SYSTEMS, INC. (NASDAQ: NTCT) ist auf Business Assurance spezialisiert und unterstützt Unternehmen bei der unterbrechungsfreien Bereitstellung ihrer digitalen Dienste. Der Schwerpunkt der Lösungen liegt auf den Themen Verfügbarkeit, Performance und Sicherheit. Die Kombination aus patentierter intelligenter Datentechnologie und intelligenten Analysefunktionen machte das Unternehmen zum Markt- und Technologieführer. Wir bieten umfassende Transparenz in Echtzeit, detaillierte Einblicke und WLAN-Tools, die Kunden für die Beschleunigung und Sicherung ihrer digitalen Transformation benötigen. Unser Ansatz verändert die Art und Weise, wie Unternehmen und Organisationen Dienste und Anwendungen planen, bereitstellen, integrieren, testen und nutzen. Unsere Monitoring-Plattform nGenius ermöglicht eine kontextbezogene Echtzeitanalyse der Performance von Diensten, Netzwerken und Anwendungen. Die Sicherheitslösungen von Arbor schützen vor DDoS-Angriffen, die die Verfügbarkeit von Diensten gefährden, sowie vor komplexen Bedrohungen, die in Netzwerke eindringen, um strategische Unternehmensdaten zu entwenden. Weitere Informationen, wie Sie die Leistung von Diensten, Netzwerken und Anwendungen in physischen und virtuellen Rechenzentren bzw. in der Cloud optimieren können und wie die mit Service Intelligence (SI) ausgestatteten Performance- und Sicherheitslösungen von NETSCOUT dazu beitragen, dass

Sie gelassen in die Zukunft blicken können, finden Sie auf unserer Website www.netscout.com oder auf Twitter, Facebook oder LinkedIn, wenn Sie [@NETSCOUT](https://twitter.com/NETSCOUT) und [@ArborNetworks](https://twitter.com/ArborNetworks) folgen.

Pressekontakt

Carolin Nillert / Yannik Bartling

Oseon

netscout@oseon.com

+49-69-25 73 80 22 -16 / -15