DDoS Studie zeigt Selbstüberschätzung und mangelnde Vorbereitung von Unternehmen im Kampf mit Cyberkriminellen

Studie von CDNetworks über die Abwehrfähigkeit gegen DDoS-Angriffe in der DACH-Region und UK zeigt große Diskrepanzen zwischen Wirklichkeit und Selbsteinschätzung

London, 10. Oktober 2017 – Eine aktuelle Studie des Content-Delivery-Network und Cloud Security-Spezialisten CDNetworks untersuchte die Fähigkeit von mehr als 300 Organisationen in Großbritannien und der DACH-Region DDoS-Angriffe abzuwehren sowie deren Investitionen in Schutzmaßnahmen. Trotz rapide steigender Angriffszahlen und -volumen, zeigen die Ergebnisse der Untersuchung, dass die überwältigende Mehrheit der Unternehmen (83 %) der Meinung ist, angemessen auf einen Angriff vorbereitet zu sein. Dass es sich hierbei um eine Fehleinschätzung handelt, belegt die Rückmeldung, dass 54 Prozent dieser Unternehmen in den vergangenen 12 Monaten trotzdem Ziel eines erfolgreichen DDoS-Angriffs waren.

Die Zahl der DDoS-Angriffe steigt weiterhin rapide an: 2015 erhöhte sich die Zahl der Attacken gegenüber dem Vorjahr um ganze 200 Prozent. Seit 2016 zeichnete sich zudem ein deutlicher Trend in Richtung größerer Ausmaße der DDoS-Angriffe ab. In der ersten Hälfte des Jahres 2015 kam es beim größten aufgedeckten Angriff zu Datenübertragungsraten von 21Gbps, während 2016 im gleichen Zeitraum der größte Angriff mit Datenübertragungsraten von 58,8Gbps fast dreimal so groß war. Dabei handelt es sich nicht um ein Ausreißer-Phänomen. Bei 31 Prozent der Angriffe wurden Datenübertragungsraten von 50Gbps oder mehr gemessen, während im entsprechenden Vorjahreszeitraum keiner der Angriffe diesen Umfang erreichte. Im Jahr 2017 gab es bisher sowohl Attacken mit vielen, kleinen Angriffen bis hin zu besonders umfassenden, massiven Angriffen.

Die Ergebnisse der Studie, und deren Zusammenfassung in einer Infografik, stellen die Sicherheits-einschätzung der Verantwortlichen der Entwicklung von Angriffen und Investitionen gegenüber.

<u>Einschätzung vs. Zahl der Angriffe pro Jahr</u>

- **83 %** der befragten Unternehmen sind der Meinung, angemessen auf einen DDoS-Angriff vorbereitet zu sein.
- **54 %** von ihnen waren in den letzten 12 Monaten trotzdem Ziel eines <u>erfolgreichen</u> DDoS-Angriffs!
- Die Zahl der **DDoS-Angriffe insgesamt** (erfolgreich oder nicht) lag in den vergangenen 12 Monaten bei **86 %** – damit ergibt sich ein Durchschnitt von sechs Angriffe pro Jahr.
- **8 %** der Unternehmen erfassten sogar **mehr als 50 Angriffe!**

<u>Auswirkungen von DDoS-Angriffen</u>

Befragt man Verantwortliche zu den Folgen eines Angriffs, zeigt sich ein deutlicher Unterschied: Von den Firmen, die noch nicht von einer Attacke betroffen waren sind ein Drittel davon überzeugt, dass sie keinen langfristigen Imageschaden erleiden würden. Ein weiteres Drittel ist der Meinung, dass sie keine Kunden verlieren würden und ein Viertel ging davon aus, dass es nicht zu Umsatzeinbußen kommen würde. Diese Einschätzung ändert sich jedoch schlagartig sobald ein Unternehmen Opfer einer erfolgreichen Attacke wird:

- 46 % erwarten langfristige 47% kurzfristige Imageschäden
- 39 % befürchten Kundenverluste und 52% Verluste von Geschäftschancen
- 52 % rechnen mit Umsatzverlusten
- 49 % befürchten, dass die Reputation der IT-Leitung oder der gesamten IT-Funktion (48%) leidet
- 54 % befürchten hohe Kosten für die Problembehebung sowie die dazu nötige Umverteilung von Ressourcen des IT-Teams (59 %)

Investitionsentwicklung

Der anhaltende Hype um Cyber-Bedrohungen, in Verbindung mit spektakulären DDoS-Angriffen, wie dem massiven Dyn-Angriff, der zum Ausfall von Twitter und CNN führte, hat offenbar einen erheblichen Investitions-Trend ausgelöst:

- Die Ausgaben für die Abwehr von DDoS-Angriffen liegen im Durchschnitt bei 26.300 EUR pro Jahr.
- Mehr als ein Fünftel aller Befragten investieren jedoch mehr als 44.000 EUR
- 49 % der Befragten haben in den zwei vergangenen Jahren erstmals in DDoS-Abwehr investiert
- 64 % planen in den kommenden 12 Monaten weitere Investitionen
- 44 % der Befragten befürchten, dass ihre Infrastrukturen aufgrund einer zu geringen Investition weiterhin gefährdet bleiben

Diese Entwicklung scheint zu einem außergewöhnlichen Vertrauen in den derzeitigen Aufbau der DDoS-Abwehrsysteme geführt zu haben. 83 Prozent der Befragten zeigten sich sowohl im Hinblick auf ihre derzeitigen Vorkehrungen zur DDoS-Abwehr, als auch im Hinblick auf die daraus resultierende Widerstandsfähigkeit auf eine Sicht von zwei Jahren zuversichtlich bzw. sehr zuversichtlich. Dabei stufen 79 % die Wahrscheinlichkeit eines Angriffs auf ihre Infrastruktur als wahrscheinlich oder fast sicher ein. Beängstigender Weise handelte es sich dabei überwiegend um gezielte vorsätzliche Angriffe. Die häufigste Hypothese sind böswillige Angriffe von Konkurrenten, gefolgt von Erpressung, hassmotivierten Verbrechen und ideologisch bedingten Konflikten.

„Da fast 80 Prozent der Unternehmen die Wahrscheinlichkeit eines Angriffs als fast sicher einstufen und dabei auch mehrheitlich von gezielten und vorsätzlichen Attacken ausgehen, erscheint das übersteigerte Selbstvertrauen der IT-Teams und ihre unzureichende Abwehrbereitschaft umso erstaunlicher. Vor allem da sich zeigt, dass 54 Prozent trotz ihrer Zuversicht Opfer einer erfolgreichen Attacke waren“, erklärt Alex Nam, Managing Director CDNetworks EMEA. Er empfiehlt Unternehmen daher die Durchführung eines DDoS-Tests zur Ermittlung der Schwachstellen sowie der erforderlichen Technologien oder Dienstleistungen.

Das DDoS-Wettrüsten mit den Cyberkriminellen zu gewinnen ist für die meisten Unternehmen im Alleingang nahezu unmöglich. Fast alle Vulnerabilitätstests zeigen, dass einer der deutlichsten Schwachpunkte in den Kapazitätsgrenze des eignen Netzwerks liegt. Sobald diese Grenze überschritten wird – sei es aufgrund harmloser Ursachen oder durch böswillige DDoS-Angriffe – kommt es zu einem Ausfall des Netzwerks. Die Kapazität, die cloudbasierte Anbieter von DDoS-Schutzlösungen nutzen können, ist erheblich größer als die eines einzelnen Unternehmens und kann Angriffe daher wesentlich besser abfedern. Spezialisierte Anbieter verfügen zudem in einer sich wandelnden DDoS-Landschaft über Mitarbeiter und die entsprechende Expertise zur Überwachung der Netzwerke und Aktualisierung der Abwehrsysteme von Kunden. Gleichzeitig können sie alle Daten bereinigen, um zu gewährleisten, dass nur „echter“ Datenverkehr durchkommt. Diese Ressourcen können Unternehmen allein kaum aufbringen.

Weitere Informationen und Ressourcen: https://www.cdnetworks.com/de/ddos-schutz

Über CDNetworks

CDNetworks ist ein globales Content Delivery Network (CDN) mit vollständig integrierter Cloud-Security-Lösung. CDNetworks garantiert Geschwindigkeit, Sicherheit und Zuverlässigkeit für die Bereitstellung von Web-Inhalten, auf allen Gerätetypen, Browsern und Netzen. Wir sorgen dafür, dass alle Nutzer weltweit ein schnelles und sicheres Web-Erlebnis haben - unabhängig davon, ob es sich um den B2B oder B2C-Bereich, mobile Mitarbeiter oder Niederlassungen im Ausland handelt.

CDNetworks bietet Web-Performance und Sicherheit für Websites und Anwendungen über ein strategisch aufgebautes Netzwerk von weltweit verteilten Präsenzpunkten (PoPs). Wir sind Spezialisten für die Regionen, in denen es besonders schwierig ist, Web-Inhalte zugänglich zu machen: Festlandchina, Russland, Südostasien und der Mittlere Osten. Seit 2000 bieten wir unseren

Kunden über unsere kompetenten und spezialisierten Techniker-Teams überall auf der Welt ausgezeichneten Kundenservice und Support.

CDNetworks hat Niederlassungen in China, Deutschland, Japan, Singapur, Südkorea, den USA und im Vereinigten Königreich. Weitere Informationen finden Sie auf https://emea.cdnetworks.com/de

Pressekontakt
GlobalCom PR Network
Wibke Sonderkamp / Martin Uffmann
wibke@gcpr.net
+49.89.360.363-40 / -41