Checkliste: Fünf Empfehlungen für den Umgang mit DDoS-Angriffen

DDoS-Studie von CDNetworks belegt frappierende Selbstüberschätzung von Unternehmen in Bezug auf die IT-Sicherheit – es fehlen Sicherheitsanalysen und strategisches Vorgehen

London, 17. Oktober 2017 – Die letzte Woche vorgestellte Studie des Content-Delivery-Network und Cloud Security-Spezialisten CDNetworks zeigt eine große Diskrepanz zwischen Wirklichkeit und Selbsteinschätzung in Unternehmen hinsichtlich ihrer IT-Sicherheit. Der Großteil (83 %) der über 300 in der DACH-Region und in Großbritannien befragten Unternehmen war der Meinung, angemessen auf einen Angriff vorbereitet zu sein. Dass es sich hierbei um eine Fehleinschätzung handelt belegt die Tatsache, dass 54 Prozent dieser Unternehmen in den vergangenen 12 Monaten trotzdem Ziel eines erfolgreichen DDoS-Angriffs waren. Über 50 Angriffe wurden 2016 von 8 Prozent der Firmen verzeichnet. Im Durchschnitt lag der Wert bei 6 Angriffen pro Jahr – allerdings mit steigender Tendenz. Zudem wächst das Ausmaß der Angriffe, und die Datenübertragungsraten (bis zu 58,8Gbps) vervielfachen sich. Daher hat CDNetworks fünf wichtige Schritte zusammengefasst, die Unternehmen für den Umgang mit DDoS-Angriffen beachten sollten, um besser vorbereitet zu sein.

1. Sicherheitsanfälligkeit und Schweregrad der Problematik ermitteln

In einem ersten Schritt gilt es, den Sicherheitsstatus im Unternehmen zu prüfen. Dies erfordert eine umfassende Prüfung der Stärken und Schwächen des Netzwerks um festzustellen, wo System- und Netzwerkabwehr-Lücken bestehen und wie einfach diese ausgenutzt werden könnten. Letzteres kann anhand von Vulnerabilitätstests und DDoS-Test ermittelt werden. Danach sollte geprüft werden, ob vorhandene Lösungen zur DDoS-Minimierung ausreichend sind.

Empfehlenswert ist auch ein sogenannter Penetrationstest (Pentest) als IT-Gesundheitscheck. Dieser Sicherheitstest simuliert einen Angriff von innerhalb und außerhalb des Netzwerks auf die Schwachstellen, um festzustellen, ob ein unberechtigter Zugriff auf die Daten möglich ist. Dies ist weniger für DDoS-Angriffe relevant. Die Ergebnisse der aktuellen Studie haben jedoch gezeigt, dass 13 % der Befragten die Auffassung vertraten, dass es sich bei den DDoS-Angriffen, deren Opfer sie wurden, um vorsätzliche Manöver handelte, die von anderen böswilligen Angriffen (wie direkte Hacking-Angriffen auf das Netzwerk) ablenken sollten.

Die Testphase zeigt, wo die größten Schwachpunkte liegen. Daraus lässt sich ableiten, welche Dienstleistungen und Technologien erforderlich sind und wo individuelles Feintuning nötig ist.

2. Geeignete Lösungsstrategie finden

In den frühen 2000er Jahren, als DDoS-Angriffe noch selten und unkompliziert waren, boten Do-it-Yourself-Lösungen ausreichend Schutz. Heute entwickeln sich die Methoden der DDoS-Angriffe sowie deren Umfang so schnell weiter, dass einzelne IT-Teams und selbst entwickelte Abwehrsysteme nicht mithalten können. Die Methode zusätzliche Hardware vor Server und Router zu schalten ist nicht nur kostspielig, sie erfordert auch permanente Updates und Konfigurationen, um die zunehmend komplexeren DDoS-Angriffen abwehren zu können. Zudem sind die Systeme immer noch anfällig für eine gezielte Überlastung der Netzwerkkapazitäten. Fast alle Vulnerabilitätstests zeigen, dass einer der größten Schwachpunkte in den Kapazitätsgrenzen des eigenen Netzwerks liegt. Wird diese Grenze überschritten – sei es aufgrund harmloser Ursachen oder durch böswillige DDoS-Angriffe – kommt es zu einem Netzwerkausfall.

Eine praxistaugliche Lösung ist beispielsweise eine cloudbasierte DDoS-Abwehr. Cloud Security-Anbieter können auf Netzwerk-Kapazitäten zurückgreifen, die die eines einzelnen Rechenzentrums bei weitem übersteigen. Daher können sie auch bei sehr umfangreichen Angriffen einen verlässlichen Schutz bieten. Zudem arbeiten hier viele Experten-Teams permanent daran mit der Weiterentwicklung der DDoS-Strategien mitzuhalten. Gleichzeitig können sie den Traffic bereinigen, um zu gewährleisten, dass nur „legitimer“ Datenverkehr durchkommt. Ressourcen wie das Open Web Application Securitiy Project (OWASP) können zusätzlich bei der DDoS-Abwehrplanung helfen.

3. Auf das Schlimmste vorbereitet sein, um die Geschäftskontinuität sicherzustellen

Die aktuellen Studienergebnisse belegen, dass Unternehmen, die noch nicht Ziel einer erfolgreichen Sicherheits-Attacke geworden sind, die Schwere von Angriffen unterschätzen. Die erhobenen Daten zeigen jedoch überdeutlich die negativen Auswirkungen finanzieller, rechtlicher, regulatorischer und/oder auf das Markenimage bezogener Natur.

Das Sicherstellen der Geschäftskontinuität sollte daher ein wichtiges Element jeder DDoS-Planung sein. Das betrifft einerseits die technischen Anforderungen, wie die Duplizierung von Informationen und die Gewähr, dass Zielvorgaben im Zusammenhang mit den Recovery Time und Recovery Point Objectives (RTOs und RPOs) mit Geschäftsanforderungen vereinbar sind. Aber auch die vielfältigen prozessbezogenen Anforderungen sollten nicht außer Acht gelassen werden. Ganz oben auf der Checkliste steht dabei, ein Krisenteam für den Eintritt eines Notfalls zu identifizieren.

Dabei sollte auch festgehalten werden, wer der Notfallkontakt bei/m und für Sicherheitspartner/n ist, wie er/sie kontaktiert werden kann/können, wer wofür verantwortlich ist und wer intern und extern informiert werden muss. Dabei muss berücksichtigt werden, dass gängige Kommunikationskanäle (E-Mail, Chat, Blogs, Intranet, etc.) durch den Angriff ausfallen könnten. Eine große Zahl von Mitarbeitern, Partnern und Kunden muss also gegebenenfalls über alternative Systeme informiert werden.

4. Unternehmenspolitik für Lösegeld-Forderungen

Es gibt Cyberkriminelle, die eine Art Lösegeld fordern, um einen DDos-Angriff zu beenden und die Ressourcen wieder freizugeben. In diesen Fällen empfehlen Experten nicht zu zahlen: Zum einen gibt es keine Garantie, dass der Angreifer seine Verpflichtung nach der Zahlung des Lösegelds einlöst. Außerdem erhöht sich das Risiko, nachdem einmal eine Zahlung erfolgt ist, dass derselbe Angreifer erneut Forderungen stellt – wie bei der organisierten Kriminalität und „Schutzgeldzahlungen“.

Daher sollten Unternehmensrichtlinien stattdessen vorsehen die Rechtsabteilung über den Angriff und die Lösegeldforderung zu informieren. In einigen Fällen werden Lösegeldforderungen sogar vor Beginn einer Attacke versendet, sodass unklar ist, ob diese stattfindet oder erfolgreich sein wird. Sollte es zu einer schwerwiegenden Attacke kommen, so wie bei der Ransomware Wannacry im Mai 2017, sollten Organisationen den Angriff so schnell wie möglich melden, um andere Firmen zu warnen.

5. Versicherung gegen Folgen von Cyber-Angriffe

Der Kampf zwischen Unternehmen und Cyberkriminellen ist schon fast zu einem Wettrüsten geworden – und einige dieser Kämpfe werden die Cyberkriminellen gewinnen. Um dieser Tatsache Rechnung zu tragen, entscheiden sich manche Unternehmen heute dazu Versicherungen gegen Datenmissbrauch und andere Auswirkungen von Cyber-Angriffen abzuschließen. Bei der Wahl einer solche Versicherung sollten sie beachten, dass die Police nicht nur die unmittelbaren, konkreten Auswirkungen abdeckt, sondern auch mögliche Geldstrafen (z.B. für gestohlene Kundendaten).

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

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 / Laura Lehmann
wibke@gcpr.net
+49.89.360.363-40 / -52