8ack CASESTUDY

DDoS Stresstest

Active Defense for Datacenters

IT-Dienstleister ennit optimiert Sicherheits- und Abwehr-Maßnahmen mit DDoS-Stresstests von 8ack

„DDoS-Stresstests sind Maßnahmen, die wir zur Überprüfung von Funktionen und Workflows empfehlen können."

Uwe Kastens, Mitglied der Geschäftsführung

Herausforderung

Der Kunde wünschte Unterstützung für die Überprüfung eines Anti-DDoS-Setups. Es sollte sich um legale, einfache und skalierbare Angriffs-Simulationen handeln.

Lösung

Der Kunden nutzte unsere dedizierte DDoS-Plattform, um Anti-DDoS-Setups, Maßnahmen und Prozesse auf unterschiedliche Angriffsarten zunächst in einer Test-Umgebung und später in einer Live-Umgebung zu testen.

Benefits

- Verbesserte DDoS-Protection
- Kürzere Reaktionszeit durch eingespielte Notfall-Prozesse
- Sicherstellung Business Continuity

Über den Kunden

Der Kieler IT-Dienstleister ennit betreibt Rechenzentren, Netze und Internet-Services für nationale und internationale Kunden. ennit agiert damit sowohl als Internet-Service-Provider und als Hosting-Provider. Für einen Premiumkunden wurde eine DDoS-Lösung konzipiert und implementiert, um die Netze des Kunden vor diesen Cyber-Angriffen nachhaltig zu schützen.
Es kommt dabei eine Lösung zum Einsatz, die bis zu einer Bandbreite von mehreren hundert Gbit/s den Angriff bereinigen kann.

Die Herausforderung

Im Zuge der Implementierung der Anti-DDoS-Lösung mussten bestehende Prozesse und Alarmierungswege getestet und optimiert werden. Weiterhin sollte die Funktion der Lösung überprüft werden. Dafür wurde zunächst eine Testumgebung gewählt, die einer tatsächlichen Kundenumgebung am nächsten kam, um somit

- das Setup (z.B. Filtereinstellung) zu prüfen,
- Notfall-Prozesse unter Krisenfallumständen zu trainieren und zu optimieren,
- die Effektivität des Gesamtkonstruktes zu validieren.

Die Lösung

Das Team entschied sich für die DDoS-Stresstests der **8ack** GmbH, da diese verschiedene Arten von Angriffen ausführen können, eine kontrollierte Umgebung gewährleisten und garantieren, dass durch umfangreiche Monitoring-Maßnahmen die Tests sofort abgebrochen werden, falls es zu ungeplanten Ausfällen kommt. Die Stresstests können verschiedene Arten von Angriffen durchführen und damit Lösungen und Workflows bei unterschiedlichen Bedingungen testen: Flood (langsam ansteigender Traffic) oder Tsunami (von 0 auf 100 in einer Sekunde), einige wenige Angreifer mit viel Traffic bis hin zu tausenden Angreifern mit geringem Traffic; mit

Version 1.4 - 5512edc8decff892ef2368e131d20cdb

diesem vielfältigen Setup ist 8ack in der Lage, unterschiedliche Angriffsszenarien abzubilden und das Funktionieren der Anti-DDoS-Lösung zu testen.
8ack berät die zu testenden Organisationen, um einerseits Schäden für die IT-Infrastruktur zu vermeiden, andererseits aber die Stresstests mit notwendiger Stärke und Setup durchzuführen; die Tester halten laufend Kontakt während der Testphase, um die Angriffe jederzeit bei ungewollten Störungen abbrechen zu können.
Es wurden insgesamt 4 Tests mit ansteigendem Volumen vereinbart, um im ersten Schritt die Workflows und danach die Filter der eingesetzten Appliance zu testen und zu adjustieren.
Das Admin-Team war über die Durchführung der Tests nicht informiert, um reale Bedingungen zu erhalten. Lediglich ein gesonderter IP-Bereich wurde benannt und bereitgestellt.

Das Resultat

Mit den ersten beiden Tests wurden die internen Workflows dermaßen optimiert, dass nach dem 2. Test die Reaktionszeit des Teams auf wenige Minuten gebracht und damit signifikant verbessert werden konnte.
Während der 3. und 4. Testphase wurde erreicht, dass die Anti-DDoS-Lösung weiter optimiert und die Lösung in einer existierenden Kundenumgebung getestet werden konnte.
Ein finaler Test unter härtesten Bedingungen brachte für das Team die Gewissheit, dass die internen Prozesse optimal eingestellt waren und die Anti-DDoS-Appliance wie erwartet funktioniert.
Das Team wird die Tests im regelmäßigen Turnus wiederholen, um die gewonnene Routine in der Abwehr von DDoS-Angriffen zu bewahren.

1 http://www.funkschau.de/telekommunikation/artikel/101832/2/

Version 1.4 - 5512edc8decff892ef2368e131d20cdb