Nine Internet Solutions AG
Badenerstrasse 47
CH-8004 Zürich

Postmortem: DDoS-Angriff auf unser Netzwerk, 11. bis 13. August 2026

Zusammenfassung

Am Abend des 11. August 2026 richtete sich ein grosser DDoS-Angriff gegen das Netzwerk eines unserer Kunden, für den wir die Anbindung zum Internet bereitstellen. Aufgrund des zeitlichen Ablaufs und des Angriffsmusters gehen wir davon aus, dass dieser Kunde das primäre Ziel war, können aber nicht vollständig ausschliessen, dass auch andere Kunden angegriffen wurden. Der dadurch entstandene Traffic beeinträchtigte auch unser eigenes Netzwerk. Wenige Stunden später richtete sich der Angriff zusätzlich direkt gegen unsere eigenen Dienste.

- *Dauer:* Dienstag, 11. August, ca. 19:15 Uhr, bis Donnerstag, 13. August, ca. 12:51 Uhr
- *Betroffene Systeme:* sämtliche Applikationen auf deplo.io, unsere Website, das Cockpit und unser Ticketsystem
- *Muster:* kein durchgehender Ausfall, sondern eine Reihe wiederkehrender Unterbrüche (den vollständigen Ablauf findest du auf unserer Statusseite)
- *Spitzenvolumen:* geschätzte 500 bis 600 Gbit/s im Aggregat, ein Mehrfaches unserer Uplink-Kapazität; zwei Upstream-Provider haben einen Traffic von 260 Gbit/s gemessen

Es gab keinen unbefugten Zugriff auf Daten und keine kompromittierten Systeme. Der Angriff war ausschliesslich darauf ausgelegt, eine Überlastung zu verursachen.

Dabei sind auch Lücken in unseren eigenen Schutzmassnahmen sichtbar geworden, die wir weiter unten im Detail beschreiben. Wenn du eigene Apps auf deplo.io betreibst, enthält der letzte Abschnitt konkrete Handlungsempfehlungen.

Ablauf der Ereignisse

Zeitraum	Ereignisse
Di, 11. August, ab ca. 19:15 Uhr	Die erste Welle trifft eine Kunden-IP und überlastet unsere Uplinks. Wir wehren sie mit einer Blackhole-Route bei unseren Upstream-Providern ab. Weitere Wellen folgen über die Nacht, unter anderem gegen unsere Website.
Mi, 12. August, ab ca. 07:10 Uhr	Weitere Wellen folgen, wobei die Ziele laufend wechseln. Wir stellen unsere exponierten Applikationen hinter ein CDN mit DDoS-Schutz und leiten die betroffenen Netze nur noch über Routen, auf denen unsere Abwehrmassnahmen greifen. Gegen 19:15 Uhr stoppt der Angriff, bestätigt durch die Messungen eines Upstream-Providers.
Do, 13. August, bis ca. 12:51 Uhr	Wir bauen die Abwehrmassnahmen kontrolliert ab. Alle Applikationen und Dienste sind wieder im Normalbetrieb.

Nine Internet Solutions AG
Badenerstrasse 47
CH-8004 Zürich

Wie der Angriff funktionierte und wie wir ihn abgewehrt haben

Der Angreifer nutzte UDP-Amplification, sendete kleine Anfragen an offene Dienste im Internet und trug dabei die IP-Adresse des Ziels als Absender ein. Die Antworten gehen damit an das Ziel und sind um ein Vielfaches grösser als die Anfragen. Wenig Bandbreite erzeugt so ein sehr grosses Angriffsvolumen. Die CISA beschreibt die Methode ausführlich unter UDP-Based Amplification Attacks.

Sobald der Uplink voll ist, greift eine Filterung innerhalb des eigenen Netzwerks nicht mehr. Zu diesem Zeitpunkt werden legitime Pakete bereits verworfen, weil der Uplink überlastet ist. Ein Angriff dieser Art lässt sich nur weiter ausserhalb abwehren, bei den Upstream-Providern. Das Mittel dort ist Blackholing: Der Provider verwirft Traffic, der an eine bestimmte IP-Adresse gerichtet ist, statt ihn an uns auszuliefern. Das schützt das Netzwerk und alle anderen Kunden, betrifft aber auch den legitimen Traffic zu dieser IP-Adresse. Als Konsequenz waren betroffene IP-Adressen während des aktiven Blackholings bewusst nicht erreichbar, auch für legitimen Traffic. Wir haben die Verfügbarkeit einzelner Ziele vorübergehend aufgegeben, um das Netzwerk für alle anderen stabil zu halten.

Nachdem wir unsere Website auf eine neue IP-Adresse verschoben hatten, wurde auch diese Adresse innerhalb von Minuten angegriffen. Der Angriff war nicht nur eine Frage der Bandbreite. Auch die Anzahl der Anfragen war hoch genug, um einzelne Dienste zu überlasten. Blackholing schützte zwar das Netzwerk vor weiterer Überlastung, konnte die angegriffenen Dienste aber nicht verfügbar halten, weil es sämtlichen Traffic zur betroffenen IP-Adresse blockiert. Es brauchte deshalb andere Ansätze, damit Angriffsverkehr von legitimen Anfragen unterschieden werden konnte.

Um die Verfügbarkeit wiederherzustellen, haben wir deshalb eine zusätzliche Abwehrebene eingeführt. Am 12. August haben wir unsere exponierten Applikationen hinter ein CDN mit DDoS-Schutz gestellt und die Migration am Folgetag abgeschlossen. Auch unser Kunde hat auf seiner Seite zusätzliche Abwehrmassnahmen geprüft und umgesetzt. Der Angriffsverkehr endet nun beim Schutzanbieter, während legitime Anfragen unsere Applikationen erreichen. Weil wir unser eigenes Netzwerk selbst betreiben, konnten wir Routing-Änderungen direkt während des laufenden Angriffs vornehmen und die zusätzlichen Abwehrmassnahmen koordinieren, ohne auf Anpassungen an einer darunterliegenden Netzwerkinfrastruktur angewiesen zu sein. Deshalb wurde aus einem Angriff von 500 bis 600 Gbit/s kein vollständiger Ausfall.

Wo unsere Schutzmassnahmen nicht ausgereicht haben

Unsere Erkennung deckte nicht alle Netzwerke ab, die wir betreiben. Sie war auf unsere eigenen Adressen beschränkt. Kundeneigene Netze, die wir in deren Auftrag announcen, waren nicht eingeschlossen. Die erste Welle traf genau ein solches Netz und musste manuell abgewehrt werden, was rund 90 Minuten kostete. Diese Lücke haben wir noch in derselben Nacht geschlossen.

Die Wirksamkeit des Blackholings wurde nicht pro Route überprüft. Das funktioniert nur für Peers, mit denen Blackholing vorher explizit vereinbart wurde, oder für Traffic, der über die Routeserver eines Internet Exchange läuft. An den Internet Exchanges, an denen wir angeschlossen sind, bestand mit keinem unserer direkten Peers eine solche Vereinbarung, wodurch Blackholing dort nur Traffic über die Routeserver abdeckte, nicht direkt ausgetauschten Traffic. Es gab weder eine regelmässige Überprüfung pro Route noch eine Alarmierung. Ein Ausweichen über andere Routen war keine Option: Ein einzelnes Netz gegenüber einem einzelnen Provider zurückzuhalten, war nicht vorgesehen. Diese Fähigkeit haben wir während des Angriffs unter Volllast entwickelt und in Betrieb genommen, ebenso wie den CDN-Schutz. Beide Massnahmen haben funktioniert, waren aber langsamer und riskanter als nötig.

Der Angriff hat unbeteiligte Kunden und unsere Kontaktkanäle getroffen. Wir betreiben unsere Website auf deplo.io, auf derselben Plattform wie unsere Kunden. Der Angriff darauf betraf deshalb auch Applikationen, die dieselbe Plattform nutzen. Das Cockpit und das Ticketsystem laufen auf separater Infrastruktur, wurden zu einem späteren Zeitpunkt aber ebenfalls direkt angegriffen. Daraus ergab sich die unangenehmste Folge des Vorfalls: Kunden verloren vorübergehend gleichzeitig ihre Applikation, deren Verwaltung und einen Teil ihres Kommunikationswegs zu uns.

Unsere Massnahmen

Jedes Kundennetz, das wir announcen, ist von unserer automatisierten Angriffserkennung abgedeckt; die Aufnahme ist Teil des Standardprozesses. Unsere exponierten Applikationen stehen hinter einem CDN mit DDoS-Schutz, und die Migration weiterer Dienste steht als vorbereitetes Verfahren bereit. Wir überwachen die Wirksamkeit unserer Abwehrmassnahmen über alle Links hinweg und arbeiten dabei eng mit unseren Upstream-Providern zusammen. Ziel ist es, Angriffe abzuwehren, ohne die Verfügbarkeit des Ziels aufzugeben.

Wir betreiben unsere eigenen Dienste weiterhin auf deplo.io, auf derselben Plattform, die wir unseren Kunden anbieten. Statt sie davon abzuziehen, härten wir die Plattform: Wir entwickeln die deplo.io-Architektur weiter, um die Abhängigkeit einzelner Applikationen von gemeinsam genutzten Adressen zu reduzieren. Zusätzlich sind das Cockpit und das Ticketsystem besser geschützt, damit du uns während eines Angriffs erreichen kannst. Das Szenario dieses Vorfalls ist Teil unserer regelmässigen Übungen.

Unsere Empfehlung: dynamische DNS-Record-Typen verwenden

Verwende einen CNAME- oder ALIAS-Record. Ein A-Record bindet deine App an eine bestimmte IP-Adresse auf unserer Plattform. Damit entfällt die Möglichkeit, kurzfristig auf eine andere Route zu wechseln, und genau darauf kam es an: Wo wir die Adresse ändern konnten, liess sich die Verfügbarkeit wiederherstellen. Zudem sind über dieselbe Adresse weitere Applikationen erreichbar. Dieses architektonische Problem liegt bei uns, und wir arbeiten daran. Bis dahin ist ein CNAME/ALIAS die wirksamste Massnahme, die du selbst umsetzen kannst.

Nine Internet Solutions AG
Badenerstrasse 47
CH-8004 Zürich

Stelle ein CDN mit DDoS-Schutz davor. Bei uns war es das, was die Verfügbarkeit wiederhergestellt hat. Für die meisten Applikationen ist der Aufwand minimal und die laufenden Kosten sind gering.

Wenn du nicht sicher bist, welche Option zu deiner Applikation passt, wende dich an support@nine.ch. Wir gehen das gerne gemeinsam mit dir durch.

Angriffe dieser Grössenordnung lassen sich nicht verhindern. Beeinflussen können wir, wie schnell wir reagieren und wie viele Unbeteiligte unsere Abwehrmassnahmen treffen. Daran arbeiten wir. Wir entschuldigen uns für allfällige Unannehmlichkeiten und danken dir für dein Verständnis sowie deine Geduld während der Störung.