# DDoS-Schutzdienste

Global IP Network | Servicebroschüre

# Eine Welt der Cyber-Unsicherheit

**Rekordzahlen von Verbrauchern gehen für Handel, Nachrichten und Videounterhaltung online; der Anstieg neuer Geschäftsfelder, wie das Internet der Dinge (IoT) und Virtualisation, sind die Trends, die wir heute sehen. Aber eine vernetztere Welt bedeutet natürlich auch mehr Möglichkeiten für Kriminelle und immer raffiniertere Cyberangriffe. Internet-zentrische Geschäfte und Unternehmen können es sich nicht leisten, in ihrer Wachsamkeit nachzulassen, denn solche Verstöße können zum möglichen Ausfall von Netzwerken führen und Millionen kosten. Den Schutz zu einem zentralen Merkmal bei der Einführung neuer Produkte und Dienstleistungen zu machen ist daher ein Muss – und eines der maßgeblichen Geschäftsanliegen.**

## DDoS-Angriffe

Am besorgniserregendsten sind heutzutage Distributed-Denial-of-Service (DDoS)-Angriffe. Diese sind zu einer regelmäßigen Bedrohung für die Online-Geschäftswelt geworden. Leider können diese jederzeit passieren und zu verheerenden Auswirkungen auf Ihr Netzwerk, Schäden an Vermögenswerten und großen Umsatzverlusten führen. Und sie nehmen an Größe, Häufigkeit und Komplexität zu – einige dieser Angriffe haben Hunderttausende von Geräten kompromittiert. Diese Angriffe auszumerzen, bevor sie wirklichen Schaden anrichten können, ist daher unerlässlich.

### Volumetrische Angriffe

Volumetrische Angriffe sind darauf ausgelegt, einen Host oder ein Netzwerk zu überwältigen, und somit unerreichbar zu machen. Diese Art von Angriffen kommt typischerweise von kompromittierten Geräten oder durch die Ausnutzung bestimmter Netzwerkprotokolle, was oft zu einer Art Kollateralschaden führt und das Netzwerk für mehr als nur das beabsichtigte Ziel unzugänglich macht.

- **TCP SYN-Überschwemmung**
- **UDP-Überschwemmung**
- **ICMP-Überschwemmung**
- **Reflexionsangriff**

### Angriffe auf Anwendungsebene

Angriffe auf Anwendungsebene sind gut ausgearbeitete Angriffe, die auf einen bestimmten Dienst des Host abzielen. Diese können schwer aufzuspüren sein, da sie wie eine legitime Verbindung aussehen, aber oft mit unwichtigen Anfragen gefüllt sind. Aufgrund der zahlreichen verfügbaren Tools, wie z. B. dem LOIC-Tool, sind diese Angriffe bei Hackern noch beliebter geworden.

- **HTTP-GET**
- **HTTP-POST**
- **SSL-Angriffe**

### Erschöpfungszustand-Angriffe

Diese Angriffe können volumetrischer Art sein und/oder auf Anwendungsebene erfolgen und werden häufig durch ein Slowloris-Angriffstool von HTTP-GET- oder SSL-Angriffen repräsentiert.

---

## Ein proaktiver Ansatz zur Netzwerksicherheit

Hier beim Global IP Network verstehen wir die Notwendigkeit, mit diesen zunehmend komplexen Bedrohungen Schritt zu halten. Unsere Vorgehensweise ist daher proaktiv – wir warten nicht, bis der Schaden schon angerichtet ist. Unsere Sicherheitsprodukte sind so ausgerichtet, dass sie mehrere Sicherheitsumgebungen unterstützen und wir bieten außerdem maßgeschneiderte Optionen an, so dass Sie selbst entscheiden können welchen Schutz Sie benötigen, und welcher am besten zur Cyberabwehrstrategie Ihres Unternehmens passt.

Wir helfen Ihnen, die richtige und beste Wahl zu treffen, wenn es um Ihre Sicherheits-Ansprüche geht. Wir sind hier, um Sie mit dem perfekten Team zu unterstützen: Unser engagiertes Netzwerksicherheitsteam (NST) verfügt über eine durchschnittliche Betriebszugehörigkeit von mehr als 10 Jahren und daher ein solides Fachwissen. In Kombination mit der Unterstützung unseres globalen Tier-1-IP-Backbone ist unser Sicherheitsangebot unübertroffen.

# Schutz vor DDoS-Angriffen (DPS, Distributed Denial of Service Protection Services)

Unsere DDoS-Schutzservices (DPS) bieten einen umfassenden, abgestuften Ansatz zur DDoS-Mitigation– je nach Art und Grades des von Ihnen gewünschten Schutzes. Diese Optionen geben Ihnen die Chance, die Schutzfunktion zu erhalten, die am besten zu Ihrer Verteidigungsstrategie passt. Unsere Dienste helfen, groß angelegte Angriffe abzuweisen, indem sie den Verkehr über unsere Minderungsplattform umleiten und bereinigen. Kontaktiern Sie uns noch heute und schützen Sie Ihre Anwendungen, bevor die Angreifer Ihre Andwendungen ausschalten können.

## DPS Control

DPS Control ist unser Einstiegsservice. Mit diesem Service können Kunden permanente Zugangskontrolllisten (ACLs) definieren, um das Netz für bestimmte, vom Kunden festgelegte, Verkehrsarten zu sperren. Wenn Sie also keine vollständige Unterstützung bei der Schadensbegrenzung benötigen, aber dennoch einen robusten Service wünschen, auf den Sie sich verlassen können, könnte dies die richtige Option für Sie sein. Dieser Service bietet die folgenden Funktionen:

### Permanente ACL-Unterstützung

- Unterstützung für ACLs bis zu 50 Zeilen
- Unterstützung von Standard- und Notfall-ACL-Änderungen

### ACL-Reaktionszeit Service-Level-Vereinbarung

- 30 Minuten Reaktionszeit SLA für Notfall-ACL-Anfragen
- 1 Werktag Reaktionszeit SLA für Standard-ACL-Anfragen

## DPS Core

Unsere nächste Schutzstufe ist DPS Core. Neben einer Reihe von Zusatzfunktionen bietet diese Sicherheitslösung mit Hilfe unseres Netzwerksicherheitsteam (NST) – das gleiche Team, das auch das Global IP Network vor Angriffen verteidigt – eine zusätzliche Sicherheitsstufe. Mit modernster Technologie in Reaktion auf eine Anfrage zur Schadensbegrenzung kann unser Team einen Angriff schnell analysieren und alle erforderlichen Gegenmaßnahmen ergreifen, um den Angriff zu vereiteln – wie z. B. die Identifizierung der wichtigsten Angriffsvektoren, die Filterung des Datenverkehrs und die Umleitung zu unserer Schadensbegrenzungsplattform zur Säuberung. Wählen Sie diese Option, wenn Sie eine schnelle, effektive Reaktion auf böswillige DDoS-Aktivitäten wünschen. Zusätzlich zu den Basisfunktionen in DPS Control umfasst dieser Service:

### Zugang zum Netzwerksicherheitsteam

- DPS-Core-Abonnenten haben direkten Zugang zu unserem hochkompetenten Netzwerksicherheitsteam, das Sie während der Schadensbegrenzung auf dem Laufenden hält

### Service-Level-Vereinbarung zur Verkürzung der Reaktionszeit

- 15 Minuten Reaktionszeit für Anfragen über das DPS-Portal
- 30 Minuten für Anfragen per E-Mail, Telefon oder über das Kundenportal

### Abschwächung von Angriffen

- Unser NST verwendet einen vielschichtigen Ansatz zur Abschwächung von Angriffen und setzt eine Vielzahl von Tools und Techniken ein, einschließlich der Säuberung des Angriffsverkehrs durch unsere Abschwächungsplattform

### Portal und Berichterstattung

- Unser exklusives DPS-Portal bietet Zugang zu Berichten über Abschwächungen und den relevanten Verlauf

## DPS Detect

Wünschen Sie ein noch höheres, gründlicheres Maß an Unterstützung? DPS Detect könnte die Antwort sein. Zusätzlich zu all den Funktionen, die DPS Core bietet, werden Dienstleistungen wie Erkennungsfunktionen zur Benachrichtigung der Kunden über potenzielle Angriffe und vom Kunden initiierte Abwehrmaßnahmen auf Knopfdruck über das DPS-Portal hinzugefügt. Kunden können auch ihren Erkennungsverlauf und frühere Schadensminderungsberichte einsehen und Konfigurationsänderungen anfordern. Wenn Sie also einen vollständigen Service für den DDoS-Schutz wünschen, der alle Grundlagen abdeckt, sollten Sie sich DPS Detect besorgen. Die folgenden Funktionen sind nur in DPS Detect enthalten:

### Erkennung von Angriffen

- Mit Hilfe von kundendefinierten Schwellenwerten werden DPS Detect-Kunden über das DPS-Portal und optional per E-Mail oder Syslog vor potenziellen Angriffen gewarnt

### Selbstinitiierte Schadensbegrenzung

- Im DPS-Portal können Kunden auf der Grundlage eines aktiven Erkennungsalarms oder durch Angabe der Ziel-IP-Adresse eine Abschwächung einleiten

## DPS Max

Das umfassendste Angebot für den DDoS-Schutz für Kunden ist DPS Max. Dieser Dienst nutzt eine Kombination aus NTT Ressourcen, Fachwissen und Eindämmungsstrategien zum Schutz von Kunden, die von DDoS-Angriffen betroffen sind - einschließlich Angriffserkennung und automatischer Eindämmung. Der Dienst wird von unserem NST unterstützt, das auch für die Verteidigung des Global IP Network gegen Angriffe zuständig ist.

### Auto-Mitigation

- Sobald die Plattform über einen möglichen DDoS-Angriff benachrichtigt wird, startet sie automatisch die Schadensbegrenzung. Wird ein Angriff erkannt, wird der Datenverkehr zu unserer Schadensbegrenzungsplattform umgeleitet und stoppt die Schadensbegrenzung, sobald der Angriff beendet ist.

**Für weitere Informationen und Updates zum Global IP Network:**

Kontaktieren Sie uns: gin@ntt.net
www.gin.ntt.net

Folgen Sie uns auf Twitter
@GinNTTnet
#globalipnetwork #AS2914


v202101DEdps