

# DTS

## DDOS MULTILAYER PROTECTION

# DDOS MULTILAYER PROTECTION

Beinahe jedes Unternehmen ist stark auf webbasierte Systeme, Anwendungen und Dienste angewiesen. Mit einer derartigen Abhängigkeit erhöht sich jedoch auch der potentielle Schaden durch DDoS-Angriffe. DDoS beschreibt eine „verbreitete Verweigerung des Dienstes“ und wird vom BSI als eine der Hauptgefahren im Bereich Cyberangriffe eingestuft. Bei einer DDoS-Attacke werden die Ressourcen eines Netzwerks, Dienstes oder einer Anwendung durch konzentrierte Angriffe überlastet. Die Absicht ist das Schädigen, Ausschalten, Infiltrieren oder gar Erpressen des Ziels. Ein zusätzliches Problem ist die sich immer weiter vergrößern Angriffsfläche durch veraltete Technologien, den Breitbandausbau und die verstärkte Nutzung von digitalisierten Geschäftsprozessen sowie dem Internet generell. Als DTS ermöglichen wir Ihnen mit unserer marktführenden Lösung einen kontinuierlichen Schutz vor DDoS-Angriffen als Managed Service.

- Auf BSI-Zertifizierung basierender, mehrstufiger Schutz gegen DDoS-Angriffe
- Marktführende Technologien & Schutzmechanismen
- Abwehr von hochvolumigen Angriffen
- Kundenindividuelle Service-Bausteine & Pakete
- Wunschweise über ein DTS Datacenter, On-Premises, Cloud oder als hybride Kombination
- DTS Managed Services

DDoS-Attacken können sehr unterschiedlich erfolgen. Das Spektrum reicht von hochvolumigen bis hin zu subtilen, schwer zu erkennenden Angriffen. Dabei werden IT-Infrastrukturgeräte, Applikationen, Sicherheitskomponenten oder schlicht die gesamte Bandbreitenkapazität angegriffen. Immer häufiger sind jedoch Kombinationen verschiedener Angriffstypen zu beobachten. Generell nehmen die Angriffshäufigkeit und Aggressivität massiv zu. Verliefe eine Attacke bereits erfolgreich, ist eine Anfälligkeit offenbart. Dann ist mit weiteren Attacken zu rechnen.

## MEHRSTUFIGER SCHUTZ GEGEN ALLE GEFAHREN

Erst nach dem Erkennen einer DDoS-Attacke ist der eigentliche Schutz möglich. Als Lösung bieten wir Ihnen einen mehrstufigen Multi Layer Schutz. Dieser basiert auf zwei Cloud Scrubbing Centern in der EU sowie dem DTS-eigenen Scrubbing Center. Die somit zur Verfügung stehenden 2,5 Tbps Mitigationskapazität schützen auch vor hochvolumigen Angriffen. Darüber hinaus können global bis zu 14 Cloud Scrubbing Center genutzt werden, für eine noch höhere Traffic-Kapazität. Dabei werden modernste Schutzmechanismen angewendet: Behavioral Protection, Real-Time Signature Generation, Challenge & Response.

Bei der Behavioral Protection werden spezielle Verhaltensanalysen zur Erkennung von Mustern und Attacken angewendet, auch zielgerichtet für kundenspezifische Anwendungen. Der Schutz gilt auch für kurze, wiederkehrende Burst-DDoS-Attacken. Dabei werden False-Positives bei der Abwehr von Attacken zuverlässig vermieden. Das Real-Time Signature Generation ist ein Schutz vor neuartigen und wechselnden Angriffstypen über Signaturen. Diese basieren auf dem Vergleich mit dem Verhalten von normalem Datenverkehr. Die automatische Erstellung der Signaturen, zzgl. anschließender Verfeinerung zur Fehlervermeidung, erfolgt in wenigen Sekunden beinahe sofort. Das Challenge & Response ist eine zusätzliche Überprüfung von verdächtigem Verkehr pro Abfragetyp vor dem Blocken.

Zusätzlich vervollständigen u. a. eine spezielle Engine als Mitigationsplattform gegen unbekannte Angriffe, automatische Security Updates mit Signaturen für bekannte Angriffe, eine Identifizierung und Blockierung von IP-Adressen bekannter Angreifer sowie Geo-Blocking feindlicher Ursprünge den mehrschichtigen Schutz zu einer ganzheitlichen Abwehr.

## SERVICE-BAUSTEINE

Zum einen ermöglichen wir den DDoS-Schutz anhand von drei Standard Datacenter Services. Diese gelten für nahezu alle Kunden in unseren DTS Rechenzentren mit schützenswerter IT-Infrastruktur:

- DTS Light DDoS Multilayer Protection: Basis-Schutz im DTS Scrubbing Center nach „Best Effort“
- DTS Basic DDoS Multilayer Protection: Basis-Schutz im DTS Scrubbing Center, inkl. Abwehr großvolumiger Angriffe in den Cloud Scrubbing Centern nach „Best Effort“
- DTS Advanced DDoS Multilayer Protection: Dedizierter Schutz, inkl. Abwehr großvolumiger Angriffe in den Cloud Scrubbing Centern mit skalierbaren, legitimen Traffic-Größen

Zum anderen ermöglichen wir den DDoS-Schutz anhand von On-Premises & Cloud Services. Diese gelten für Kunden mit eigener schützenswerter IT-Infrastruktur vor Ort, oder in hybriden Umgebungen beim Kunden bzw. in den DTS Rechenzentren:

- DTS Hybrid DDoS Multilayer Protection: Schutz mit eigener Scrubbing Lösung vor Ort im Service der DTS mit individuellen Regelwerken & Leserechten, inkl. Cloud Scrubbing Centern mit skalierbaren, legitimen Traffic-Größen
- DTS Always On DDoS Multilayer Protection: Permanenter Schutz durch Cloud Scrubbing Center zur Abwehr großvolumiger Angriffe, mit skalierbaren, legitimen Traffic-Größen