DDoS-Angriffe im Cyberraum

Einführung

Wenn Dienste, die eigentlich über das Internet erreichbar sein sollten, nicht verfügbar sind, spricht man von einem **Denial of Service (DoS)**.

Ein DoS (Denial of Service) kann verschiedene Gründe haben. Physische nicht-Erreichbarkeit ist ebenso eine mögliche Ursache, wie eine ungewollte Überlastung des Systems oder aber ein mutwilliger Angriff.

Eine mutwillige Überlastung wird meist unter Zuhilfenahme eines Botnetzes hervorgerufen. Dabei werden vom Täter vorher gekaperte IT-Systeme zusammengeschlossen und zeitgleich auf das Ziel losgelassen. Sollte es sich bei dem Ziel um einen Host handeln, so verursacht die große Menge von Anfragen eine sehr langsame Reaktionszeit. Die Dienste oder Webseiten des Hostes sind in diesem Falle für legitime Nutzer - wenn überhaupt - nur mit starken Verzögerungen erreichbar. Dies bezeichnet man als **DDoS (Distributed Denial of Service)**.

In einigen Fällen setzen Angreifer nicht nur auf die schiere Masse von Anfragen, sondern versuchen gezielt Programmfehler im Zielsystem auszunutzen. So werden die Ziele nicht nur verlangsamt sondern können Fehlverhalten bis hin zu Abstürzen erleiden.

Dokumente und Informationen

Im Folgenden finden Sie verschiedene Informationen und Hilfestellungen des Bundesamtes für Sicherheit in der Informationstechnik und der Allianz für Cyber-Sicherheit zum Thema, die sowohl bei der Vermeidung als auch bei der Reaktion im Falle eines Vorfalls helfen können. Bitte beachten Sie, dass einige dieser Dokumente nicht öffentlich zugänglich sind, sondern einen Login für den internen Bereich der Webseite der Allianz für Cyber-Sicherheit erfordern.

Qualifizierte Dienstleister

Bei Cyberangriffen kann sowohl bei der Prävention als auch nach einem akuten Sicherheitsvorfall die Einbindung eines qualifizierten Dienstleisters sinnvoll sein.
Hier finden Sie die **> Übersichtsliste der Dienstleister** sowie die Auswahlkriterien für qualifizierte DDoS-Mitigation-Dienstleister. Wenn Sie Interesse haben als qualifizierter Dienstleister tätig zu werden, finden Sie auf der Seite auch die Verfahrensbeschreibung und Kontaktinformationen.

Publikationen des BSI

- **Download Industrial Control System Security: Top 10 Bedrohungen und Gegenmaßnahmen 2022 [Deutsch] v1.5 (PDF)**
- **Download Prävention von DDoS-Angriffen v2.0 (PDF)**
- **Download Abwehr von DDoS - Angriffen v2.0 (PDF)**
- **Download Anti-DDoS-Maßnahmen v2.0 (PDF)**
- **Download Zunahme von DDoS-Angriffen durch DNS-Reflection v2.0 (PDF)**
- **Download Maßnahmen gegen Reflection Angriffe v1.1 (PDF)**

Zusätzliche Informationen für registrierte Teilnehmer der ACS

- **Gefährdungen durch Webserverkompromittierung [TLP-Amber] v2.0**
- **Erkennung und Abwehr von DDoS-Angriffen im Internet [TLP-Amber]**

Zusätzliche Informationen für INSI-Teilnehmer der ACS

- **Download Kurzübersicht DDoS-Angriffsverfahren [TLP-Amber] (PDF)**

Ähnliche Themen

Ransomware | Social Engineering | APT | Malware

Zurück zu Cyber-Sicherheitsempfehlungen nach Gefährdungen

Seite drucken

THEMEN
Verbraucherinnen und Verbraucher
Unternehmen und Organisationen
Staat und Verwaltung
KRITIS und regulierte Unternehmen

KARRIERE
Arbeiten im BSI
Stellenangebote
Studium und Ausbildung

IT-SICHERHEITSVORFALL
IT-Sicherheitsvorfall

FOLGEN SIE UNS

DAS BSI
Leitbild
Organisation und Aufbau
BSI Standorte
Auftrag
Kontakt

Impressum Datenschutz Nutzungsbedingungen Barrierefreiheit