Kriterien für qualifizierte Dienstleister

DDoS-Mitigation-Dienstleister

Die Auswirkungen von Distributed Denial-of-Service (DDoS) Angriffen können beträchtlich sein, für die betroffenen Institutionen einen großen wirtschaftlichen Schaden auslösen und auch einen Reputationsverlust nach sich ziehen.

Mit diesem Dokument möchte das BSI Hilfestellungen bei der Auswahl eines geeigneten DDoS-Mitigation-Dienstleisters geben.

1 Varianten

Prinzipiell stehen drei Varianten zur Mitigation von DDoS-Angriffen zur Verfügung:

1. Betrieb einer DDoS-Mitigation Appliance
2. Content Delivery Networks
3. DDoS-Mitigation as a Service

1.1 Betrieb einer DDoS-Mitigation Appliance

Der Betrieb einer Appliance zur DDoS-Mitigation erfolgt typischerweise „on premise" - also direkt im Rechenzentrum. Eine solche Appliance lässt sich in der Regel sehr genau an die eigenen Bedürfnisse anpassen. Allerdings wird der Angriffsverkehr bei dieser Variante bis ins Rechenzentrum weitergeleitet. Bei Angriffen mit hohen Bandbreiten wird in der Regel die Kapazität des Internetanschlusses übertroffen. Der Betrieb einer Appliance ist daher nur dann sinnvoll, wenn eine der folgenden Bedingungen greift:

1. Es ist nur mit geringen Angriffsbandbreiten auf Anwendungsebene zu rechnen oder
2. die Appliance ergänzt eine DDoS-Mitigation as a Service Lösung oder
3. die Appliance wird beim Upstream-Provider betrieben.

1.2 Content Delivery Network

Content Delivery Networks (CDN) sind Netze oder Overlay-Netze mit Instanzen an mehreren Standorten. Die abrufbaren Inhalte werden auf mehrere Instanzen gespiegelt und der Inhalt damit „näher zum Kunden" gebracht wird. So werden Anfragen regionalisiert, was zur Folge hat, dass die Last pro Instanz geringer ist und Zugriffszeiten geringer sind. CDNs eignen sich insbesondere zum Schutz von Webangeboten mit geringem dynamischen Anteil, da sich diese besonders gut spiegeln lassen. CDNs verfügen in der Regel über eine große Gesamtkapazität, so dass viele DDoS-Angriffe abgewehrt werden können. Zudem lässt sich in vielen Fällen Angriffsverkehr filtern.

1.3 DDoS-Mitigation as a Service

Einige Dienstleister bieten explizit DDoS-Mitigation an. Diese wird in der Regel über ein Scrubbing-Center realisiert. Der Datenverkehr kann in dieses Scrubbing-Center umgeleitet werden, wird dort bereinigt und der gesäuberte Verkehr wird an den eigentlichen

Server weitergeleitet. Mit diese Technik lassen sich zusätzlich zu Web auch weitere Dienste vor Angriffen schützen. Die Umleitung ins Scrubbing-Center kann entweder für einzelne Dienste über DNS oder für ganze IP-Adressbereiche über BGP erfolgen.

2 Kriterien

DDoS-Mitigation-Dienstleister müssen die folgenden Kategorien erfüllen:

- Der Anbieter verfügt eine redundante Internet-Anbindung.
- Es stehen DDoS-Filter für gängige Dienste (Web, Mail, VPN) zur Verfügung.
- Folgende Filtermöglichkeiten müssen mindestens zur Verfügung stehen
  - Protokoll (TCP, UDP, ICMP, etc.)
  - TCP-Flags, ICMP-Typ
  - Quell- und Ziel-IP
  - Rate-Limit pro IP bzw. Netzbereich
- Die Umleitung des Verkehrs ist auf Basis DNS und/oder BGP möglich.
- Es besteht die Option, den Verkehr nur im Angriffsfall umzuleiten.
- Es besteht die Option, die Mitigation im Angriffsfall automatisch aktivieren zu lassen.
- Es werden IPv4 und IPv6 unterstützt.
- Es lassen sich Inhalte einbetten, die es ermöglichen menschliche Benutzer zu erkennen.
- Der Dienstleister bietet eine 24x7 Erreichbarkeit
- Der Dienstleister kann mit verschlüsselten Verbindungen (TLS) umgehen.
- Der Kunde kann eigene Definitionen einbringen:
  - zulässige oder spezielle IP-Bereiche
  - zulässige oder spezielle Regionen (Geo-IP)
  - Profile des erlaubten Verkehrs
- Der Dienstleister sollte dem Kunden beim Erstellen solcher Definitionen unterstützen.
- Definitionen der Filter werden automatisch aus dem Angriffsmuster abgeleitet.
- Der Dienstleister erfüllt die gleichen Datenschutzbestimmungen wie der Kunde.
- Der Zugang zur Konfigurationsplattform ist TLS-geschützt.

3 Weiterführende Informationen

Die BSI-Empfehlung „Prävention von DDoS-Angriffen“[1] behandelt Ansätze zur Vorbeugung gegen Angriffe. Neben technischen Möglichkeiten sind auch organisatorische Maßnahmen wesentliche Bestandteile eines effektiven Schutzes vor DDoS-Angriffen.

Die BSI-Empfehlung „Abwehr von DDoS-Angriffen“[2] behandelt Maßnahmen zur Reaktion bei akuten Angriffen. Durch diese Maßnahmen besteht die Möglichkeit, die Folgen eines DDoS-Angriffs auch dann noch abzumildern, wenn keine präventiven Vorkehrungen getroffen wurden oder sich diese als ineffektiv erwiesen haben.

1 https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_025.html
2 https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_002.html