Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Qualifizierte DDoS-Mitigation Dienstleister

im Sinne § 3 BSIG

Stand: 03. Februar 2021

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582- 0
E-Mail: qdl@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhalt

1 Hintergrund

Das BSI hat gemäß § 3 BSIG die Aufgabe, Betreiber Kritischer Infrastrukturen auf deren Ersuchen bei der Sicherung ihrer Informationstechnik zu beraten und zu unterstützen. Hierzu kann auch auf qualifizierte Sicherheitsdienstleister verwiesen werden.

Angriffe auf Unternehmen nehmen in der letzten Zeit stark zu, sowohl in der Anzahl, als auch in der Intensität der Bedrohungen. Der Schaden, welcher dabei entsteht, verursacht bei den betroffenen Unternehmen nicht nur große wirtschaftliche Schäden, sondern auch einen Reputationsverlust, wenn Dienste nicht zur Verfügung stehen oder ein Datenabfluss zu verzeichnen war. Zur Verbesserung der Abwehr oder zur Bewältigung eines erfolgreichen Angriffs bedarf es vielfältig der Unterstützung externer Dienstleister, die in ihrem jeweiligen Tätigkeitsgebiet ein hohes Spezialwissen erlangt haben.

Mit der Benennung von themenspezifischen Qualitätskriterien und der Identifikation geeigneter Dienstleister möchte das BSI betroffenen Unternehmen eine Hilfestellung bei der Suche und Auswahl geeigneter Dienstleister bieten, um die Unternehmen im Ernstfall von einem eigenen zeitintensiven Rechercheaufwand zu entlasten. Gleichzeitig soll auf diese Weise ein gewisses Qualitätsniveau in der jeweiligen Branche etabliert werden.

Zur Identifikation von qualifizierten Sicherheitsdienstleistern für die Abwehr von DDoS-Angriffen hat das BSI Kriterien[1] veröffentlicht, die betroffene Betreiber Kritischer Infrastrukturen bei der Auswahl von geeigneten Dienstleistern unterstützen sollen.

Die Dienstleister, die anhand der Kriterien mit der Hilfe des in Kapitel 2 beschriebenen Verfahrens gefunden wurden, sind in diesem Dokument im Folgenden aufgelistet. Dazu gehören sowohl die Kontaktdaten in Kapitel 3 als auch die Gegenüberstellung der einzelnen Leistungsmerkmale in Kapitel 5. Die Leistungsmerkmale, welche sowohl die Kriterien beinhalten als auch weitere individuelle Unterschiede der Dienstleister darstellen, werden zuvor in Kapitel 4 genauer beschrieben.

[1] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Dienstleister-DDos-Mitigation.html

2 Verfahren

Um den Betreibern Kritischer Infrastrukturen eine leichtere Übersicht über den Markt der DDoS-Mitigation-Dienstleister zu bieten, wurde, basierend auf den Auswahlkriterien, ein Verfahren zur Identifizierung geeigneter Dienstleister durchgeführt.

Das Verfahren gliedert sich in die folgenden Schritte:

1. Überprüfung der vom Dienstleister bereitgestellten Dokumentation
   Der Dienstleister musste zunächst eine vollständige Dokumentation bereitstellen. Hierzu zählten sowohl Beschreibungen der Produkte und Dienstleistungen, als auch Erläuterungen in Bezug auf die Einhaltung der vom BSI aufgestellten Kriterien. Des Weiteren bestand die Möglichkeit, vorhandene Zertifizierungen von Rechenzentren oder dem Unternehmen selbst mitzuliefern.

2. Durchführung eines Fachinterviews
   In einem mehrstündigen Termin beim BSI musste der Dienstleister anhand fiktiver Szenarien zeigen, dass er in der Lage ist, die Situationen fach- und zielgerichtet zu bedienen. Dabei wurde sowohl auf das allgemeine Vorgehen des Dienstleisters, als auch auf gestellte Fragen und Verarbeitung der erhaltenen Informationen geachtet.

Weiteren interessierten Dienstleistern steht das Verfahren jederzeit offen, sie können sich für Informationen an das Funktionspostfach qdl@bsi.bund.de wenden.

3 Qualifizierte DDoS-Mitigation-Dienstleister

Im Folgenden werden die bisher identifizierten qualifizierten DDoS-Mitigation-Dienstleister mit den entsprechenden Kontaktdaten in alphabetischer Reihenfolge aufgelistet.

3.1 Akamai Technologies GmbH

Homepage	https://www.akamai.com/de/de/about/stop-ddos-attacks.jsp
Kontakt-Telefonnummer	+49 (0)89 94 00 63 08
Kontakt-E-Mail-Adresse	ddos-assistance@akamai.com

3.2 Cloudflare GmbH

Homepage	https://www.cloudflare.com
Kontakt-Telefonnummer	+49 (0)89 26204574
Kontakt-E-Mail-Adresse	ddos-support@cloudflare.com

3.3 Deutsche Telekom AG

Homepage	https://geschaeftskunden.telekom.de/security/netzwerksicherheit/ddos-protection https://public.t-systems.de/it-tk-portfolio/security/network-security/ddos-protection/abwehr-von-cyber-angriffen-403444 https://globalcarrier.telekom.com/business-areas/internet-content/ddos-defense
Kontakt-Telefonnummer	IP Transit Anschlüsse: +49 (0)69 20060 5575 Company Connect und Deutschland LAN Connect IP Anschlüsse: +49 (0)800 5231323

3.4 EWE

Homepage	https://www.ewe.de/unternehmen/telekommunikation/security/ddos
Kontakt-Telefonnummer	+49 (0)800 1393835
Kontakt-E-Mail-Adresse	business@ewe.de

3.5 F5 Networks

Homepage	https://f5.com https://www.f5.com/products/security/silverline
Kontakt-Telefonnummer	+49 (0)800 7000 5050 +1 (206) 272-7969
Kontakt-E-Mail-Adresse	SilverlineSales@f5.com

3.6 Link11

Homepage	https://www.link11.com	
Kontakt-Telefonnummer	Mobile Home Office:	+49 (0)172 3855186
	Zentrale:	+49 (0)69 264929777
	Durchwahl Büro:	+49 (0)69 2649297763
Kontakt-E-Mail-Adresse	m.hempe@link11.com support@link11.com	

3.7 Myra Security GmbH

Homepage	https://www.myrasecurity.com
Kontakt-Telefonnummer	+49 (0)89 414141 345
Kontakt-E-Mail-Adresse	info@myrasecurity.com

3.8 Netscout

Homepage	https://www.netscout.com/Arbor
Kontakt-Telefonnummer	+49 (0)30 782 9685
Kontakt-E-Mail-Adresse	Klaus.Kreye@netscout.com

3.9 Radware GmbH

Homepage	https://www.radware.com
Kontakt-Telefonnummer	+49 (0)6103 70657 0
Kontakt-E-Mail-Adresse	michaelt@radware.com

3.10 Vodafone GmbH

Homepage	https://www.vodafone.de
Kontakt-Telefonnummer	+49 (0)800 444063 3000
Kontakt-E-Mail-Adresse	cloud.hosting@vodafone.com

4 Leistungsmerkmale

4.1 Dienstangebot

4.1.1 Dienstleistung auch für Nicht-Bestandskunden

Werden die angebotenen Dienstleistungen und Produkte auch Unternehmen zur Verfügung gestellt, welche keine weiteren Leistungen des qualifizierten Dienstleisters (zum Beispiel Internet-Leitung) beziehen?

4.1.2 24x7 Erreichbarkeit

Ist der DDoS-Mitigation-Dienstleister rund um die Uhr bei Angriffen oder Problemen erreichbar?

4.1.3 Dienstleister SPOC (für RIPE- und/oder Provider-Kontakte) oder Unterstützung bei Kontaktaufnahme und Kommunikation

Für die Umleitung des Netzwerkverkehrs vom KRITIS-Unternehmen über den DDoS-Mitigation-Dienstleister müssen je nach Größe des umzuleitenden Netzes verschiedene Voraussetzungen und Absprachen zum Beispiel mit dem Provider des KRITIS-Unternehmens getroffen werden. Hierbei sollte der Dienstleister den Kunden unterstützen können.

4.2 Allgemeines zum Dienstleister

4.2.1 ISO27001-Zertifizierung der RZ-Standorte

Sind die Rechenzentren des DDoS-Mitigation-Dienstleisters ISO27001 zertifiziert?

4.2.2 ISO27001-Zertifizierung der Institution

Besitzt der DDoS-Mitigation-Dienstleister eine ISO27001 Zertifizierung für die Institution?

4.2.3 Räumliche Verteilung der RZ

Falls der DDoS-Mitigation-Dienstleister über mehrere Rechenzentren verfügt, ist es sinnvoll, dass diese in einem ausreichend großen Abstand zueinanderstehen. Nur so kann gewährleistet werden, dass regionale Probleme, zum Beispiel bei der Netzanbindung, nicht alle Standorte betreffen.

Des Weiteren bietet eine großflächige Verteilung der Rechenzentren den Vorteil, dass der Netzverkehr in der Nähe des Ursprungs gefiltert werden kann.

4.2.4 Beschränkung auf RZ in Deutschland möglich

Bietet der DDoS-Mitigation-Dienstleister an, dass umgeleiteter Verkehr ausschließlich in Rechenzentren in Deutschland verarbeitet wird?

4.2.5 Berücksichtigung des BDSG

Der Netzwerkverkehr fließt zumindest im Falle einer Mitigation über die Rechenzentren des DDoS-Mitigation-Dienstleisters. Dabei werden unter Umständen auch die Transportverschlüsselungen terminiert, sodass der Dienstleister prinzipiell den gesamten Verkehr inklusive aller Eingaben sehen könnte.

Das deutsche Datenschutzgesetz sieht dabei zahlreiche Pflichten vor, welche jedoch nur gelten, wenn sich der Dienstleister an das BDSG halten muss. Dies ist dann der Fall, wenn die Rechenzentren in Deutschland stehen.

4.2.6 Redundante Internet-Anbindung

Verfügen die DDoS-Mitigation-Dienstleister über eine redundante Internet-Anbindung? Die redundante Anbindung ist notwendig, damit auch beim Ausfall einer Anbindung weiterhin eine Erreichbarkeit und ein Schutz der Anwendungen von KRITIS-Unternehmen gewährleistet werden kann.

4.3 Angriff

4.3.1 Verkehrsumleitung mittels DNS / BGP

Im Falle eines Angriffs muss der gesamte Netzwerkverkehr über den DDoS-Mitigation-Dienstleister umgeleitet werden, damit dieser den Verkehr filtern kann. Eine Umleitung kann dabei für größere Netzbereiche über das Border Gateway Protocol oder bei wenigen IP-Adressen über DNS-Einstellungen erfolgen. Dabei unterstützt nicht jeder Dienstleister unbedingt beide Varianten.

4.3.2 Optionale Umleitung im Angriffsfall

Besteht die Umleitung des Netzwerkverkehrs über die Rechenzentren des DDoS-Mitigation-Dienstleisters dauerhaft, also auch zu Zeiten, wo kein DDoS-Angriff stattfindet, oder besteht die Möglichkeit, den Netzwerkverkehr ausschließlich im Angriffsfall umzuleiten?

4.3.3 Mitigation im Angriffsfall automatisch aktiv

Falls ein Angriff erkannt wird, greift der DDoS-Mitigation-Dienstleister automatisiert ein oder muss erst ein manueller Start der Mitigation oder eine Anweisung durch das KRITIS-Unternehmen erfolgen?

4.3.4 Unterstützung von IPv4 / IPv6

Werden Verbindungen über die Protokolle IPv4 und/oder IPv6 unterstützt?

4.3.5 Handling verschlüsselter Verbindungen

Kann der DDoS-Mitigation-Dienstleister mit verschlüsselten Verbindungen (HTTPS) umgehen? Dazu muss zum Beispiel der private Schlüssel zu einem TLS-Zertifikat des KRITIS-Unternehmens bereitgestellt werden können, womit auch die Dateneingabe von Kunden eingesehen werden können.

4.4 Filtermöglichkeiten

4.4.1 DDoS-Filter zum Schutz gängiger Dienste

DDoS-Angriffe erfolgen auf unterschiedliche Arten und haben die verschiedensten Dienste als Ziel. Je nach Dienst ist dabei eine unterschiedliche Handhabung notwendig, sodass der DDoS-Mitigation-Dienstleister für alle gängigen Dienste (Web, E-Mail, VPN, DNS) Filter parat haben sollte.

4.4.2 Filtermöglichkeiten

Die Filterung kann auf Basis verschiedenster Ansätze geschehen. Um dabei möglichst alle Angriffe erfolgreich erkennen und abwehren zu können, sollte der DDoS-Mitigation-Dienstleister in der Lage sein, eine Filterung auf Protokoll-Ebene, mit der Hilfe verschiedener Techniken, wie zum Beispiel TCP-Flags, Quell- und Ziel-IPs sowie Rate-Limiting oder regulären Ausdrücken, durchzuführen können. Des Weiteren können Filterungen auch auf Layer-7-Ebene möglich sein.

4.4.3 Unterstützung des Kunden beim Erstellen eigener Definitionen

Kann der Kunde eigene Definitionen für die Filterung des Netzwerkverkehrs einbringen? Dazu können zum Beispiel IP-Bereiche gehören, die immer freigeschaltet (Allowlisting) oder welche dauerhaft geblockt werden sollen, zum Beispiel Geo-Blocking. Auch allgemeine Profile des erlaubten Verkehrs anhand regulärer Ausdrücke können durch den DDoS-Mitigation-Dienstleister ermöglicht werden.

4.4.4 Automatische Ableitung der Filter-Definition aus Angriffsmustern

Unterstützt der DDoS-Mitigation-Dienstleister eine Verbesserung seiner Filter durch eine automatische Analyse der Angriffe?

4.4.5 Erkennung menschlicher Benutzer / Captcha-Einsatz

Angriffe erfolgen zumeist durch Botnetze und sind dabei automatisiert. Bei der Filterung gegen diese Angriffe ist es potentiell möglich, dass auch normalen Benutzern der Zugang zur Seite verwehrt wird.

Bei diesem Leistungsmerkmal wird abgefragt, ob der Dienstleister die Option bietet, gesperrten Benutzern ein Captcha anzuzeigen, sodass sie durch das Lösen der Aufgabe nachweisen können, dass es sich bei ihnen um reguläre menschliche Benutzer handelt.

4.4.6 Benutzer-Plattform

Die Bereitstellung von Informationen durch den DDoS-Mitigation-Dienstleister geschieht für die Kunden häufig durch eine Benutzer-Plattform. Diese kann auf der einen Seite rein passiv sein und lediglich Statistiken bereitstellen. Auf der anderen Seite besteht aber auch oftmals die Möglichkeit für den Kunden, eigene Definitionen zur Filterung des Netzwerkverkehrs einzubringen.

Des Weiteren wird bei diesem Leistungsmerkmal abgefragt, wie der Zugang zur Plattform gesichert ist (TLS-geschützt, 2-Faktor-Authentifizierung) und ob Rollen/Rechte-Konzepte vorgesehen sind, sodass nicht jeder Mitarbeiter des KRITIS-Unternehmen, welcher Zugang zur Benutzer-Plattform erhalten soll, Zugriff auf alle Funktionsmöglichkeiten erhalten muss.

5 Gegenüberstellung der Leistungsmerkmale der einzelnen DDoS-Mitigation-Dienstleister

Die folgende Tabelle liefert eine grobe Gegenüberstellung einzelner Leistungsmerkmale der DDoS-Mitigation-Dienstleister und soll einen ersten Ansatzpunkt für die Auswahl eines geeigneten Dienstleisters darstellen. Genauere Informationen können nur im Gespräch mit potentiell geeigneten Kandidaten erörtert werden.

Leistungsmerkmale	Akamai Technologies GmbH	Cloudflare GmbH	Deutsche Telekom AG	EWE	F5 Networks	Link11	Myra Security GmbH	Netscout	Radware GmbH	Vodafone GmbH
4.1 Dienstangebot										
4.1.1 Dienstleistung auch für Nicht-Bestandskunden	✓	✓	✓	✗	✓	✓	✓	✓	✓	✗
4.1.2 24x7 Erreichbarkeit	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
4.1.3 Dienstleister SPOC (für RIPE- und/oder Provider-Kontakte) oder Unterstützung bei Kontaktaufnahme und Kommunikation	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗
4.2 Allgemeines zum Dienstleister										
4.2.1 ISO27001-Zertifizierung der RZ-Standorte	✓	✗ [2]	✓	✓	✓	✓	✓	✓	✓	✓

[2] Einige Rechenzentren sind ISO zertifiziert

Leistungsmerkmale	Akamai Technologies GmbH	Cloudflare GmbH	Deutsche Telekom AG	EWE	F5 Networks	Link11	Myra Security GmbH	Netscout	Radware GmbH	Vodafone GmbH
4.2.2 ISO27001-Zertifizierung der Institution	✗	✓	✓	✓	✓	✗[3]	✓	✗	✓	✓
4.2.3 Räumliche Verteilung der RZ	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
4.2.4 Beschränkung auf RZ in Deutschland möglich	✗[4]	✗	✓	✓	✗[4]	✓	✓	✓	✓	✓
4.2.5 Berücksichtigung des BDSG	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
4.2.6 Redundante Internet-Anbindung	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
4.3 Angriff										
4.3.1 Verkehrsumleitung mittels DNS / BGP	✓/✓	✓/✓	✓/✓	✗/✓	✓/✓	✓/✓	✓/✓	✓/✓	✓/✓	✗/✓
4.3.2 Optionale Umleitung im Angriffsfall	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓
4.3.3 Mitigation im Angriffsfall automatisch aktiv	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓
4.3.4 Unterstützung von IPv4 / IPv6	✓/✓	✓/✓	✓/✓	✓/✓	✓/✓	✓/✓	✓/✓	✓/✓	✓/✓	✓/✗

[3] In Erstellung
[4] Beschränkung auf EU möglich

Leistungsmerkmale	Akamai Technologies GmbH	Cloudflare GmbH	Deutsche Telekom AG	EWE	F5 Networks	Link11	Myra Security GmbH	Netscout	Radware GmbH	Vodafone GmbH
4.3.5 Handling verschlüsselter Verbindungen	✓	✓	✓	✗ [5]	✓	✓	✓	✓	✓	✗
4.4 Filtermöglichkeiten										
4.4.1 DDoS-Filter zum Schutz gängiger Dienste										
Web	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
E-Mail	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
VPN	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
DNS	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
4.4.2 Filtermöglichkeiten										
Layer 7	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Protokoll	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

[5] Handling verschlüsselter Verbindungen nur aufgrund der TLS-Header-Informationen möglich

Leistungsmerkmale	Akamai Technologies GmbH	Cloudflare GmbH	Deutsche Telekom AG	EWE	F5 Networks	Link11	Myra Security GmbH	Netscout	Radware GmbH	Vodafone GmbH
TCP-Flags	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Quell- und Ziel-IP	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Rate-Limiting	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Reguläre Ausdrücke	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓
4.4.3 Unterstützung des Kunden beim Erstellen eigener Definitionen										
Zulässige oder spezielle IP-Bereiche	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Zulässige oder spezielle Regionen (GEO-IP)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Profile des erlaubten Verkehrs	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
4.4.4 Automatische Ableitung der Filter-Definition aus Angriffsmustern	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
4.4.5 Erkennung menschlicher Benutzer / Captcha-Einsatz	✗/✗	✓/✓	✓/✓	✗/✗	✓/✓	✓/✓	✓/✓[6]	✗/✗	✓/✗	✓/✗

[6] Auf Wunsch möglich

Leistungsmerkmale	Akamai Technologies GmbH	Cloudflare GmbH	Deutsche Telekom AG	EWE	F5 Networks	Link11	Myra Security GmbH	Netscout	Radware GmbH	Vodafone GmbH
4.4.6 Benutzer-Plattform										
TLS-geschützt	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓
2-Faktor-Authentifizierung	✓	✓	✗	✓	✓	✓	✓	✓	✓	✗
Verschiedene Rollen/Rechte-Konzepte möglich	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓
Statistiken	✓	✓	✓[7]	✓	✓	✓	✓	✓	✓	✓
Möglichkeit zur Eingabe eigener Definitionen	✓	✓	✗	✓	✓	✓[8]	✓[8]	✓	✗	✓[9]

[7] Statistik-Report wird automatisch per E-Mail verschickt; Plattform existiert nicht.
[8] Allow- und Denylisting von IP-Adressen und Bereichen, Angabe individueller Fehlerseiten, DNS-Editor, …
[9] Allowlisting von IP-Adressen