Zusätzliche Bedingungen und Preise DDoS-Defence.

1 Vertragspartner

Vertragspartner sind die Telekom Deutschland GmbH (im Folgenden Telekom genannt), Landgrabenweg 151, 53227 Bonn (Amtsgericht Bonn HRB 5919) und der Kunde, der kein Verbraucher im Sinne von § 13 BGB ist.

2 Allgemeines

Mit DDoS-Defence bietet die Telekom ihren Kunden mit einer Internet-Anbindung (z. B. CompanyConnect) eine zubuchbare Serviceleistung für professionelle IT-Security zur reaktiven Abwehr von Internet-Attacken, d.h. bei volumenabhängigen DoS- (Denial of Service) und DDoS (Distributed Denial of Service) -Angriffen.
DDoS-Defence ist nur für Angriffsverkehr anwendbar, welcher über das Backbone-Netz der Telekom zum Netz des Kunden übertragen wird.
Voraussetzung für die Nutzung von DDoS-Defence ist ein bestehendes oder gleichzeitig abzuschließendes Vertragsverhältnis über ein InternetConnect aus dem Business Premium Access Portfolio oder DeutschlandLAN Connect IP-Produkt der Telekom.

3 Leistungsumfang

Die Telekom stellt im Rahmen der bestehenden technischen und betrieblichen Möglichkeiten für DDoS-Defence ein Team von Spezialisten bereit, dass bei einem vom Kunden gemeldeten DoS-Angriff Gegenmaßnahmen ergreift.
Die Telekom versucht innerhalb einer gewissen Zeitspanne (ggf. wenige Stunden) nach Beginn der Gegenmaßnahmen eine zumindest eingeschränkte Wiederherstellung der betroffenen Dienste zu erreichen. Die Telekom kann auf Grund der Komplexität der möglichen Angriffe für die Abwehr des Angriffs keine Zeitspanne zusichern.
Die Mechanismen von DDoS-Defence sind nicht für die Abwehr von Angriffen der nachfolgenden Arten geeignet:

- Einbruchsversuche in Computersysteme oder Netzwerkstrukturen (Hacker Angriffe).
- Angriffe auf Sicherheitslücken in Hard- oder Software.
- Spam-Mails.
- Schadsoftware, wie z.B. Viren, Würmer, Trojaner, etc.

3.1 Störungsmeldung

Der Servicedesk der Telekom nimmt täglich von 0.00 bis 24.00 Uhr Meldungen über Angriffe von den benannten Ansprechpartnern unter einer speziellen Service-Telefonnummer entgegen.
Der Servicedesk der Telekom authentifiziert den Kunden durch Rückruf des vom Kunden benannten Ansprechpartners mit der hinterlegten Rufnummer. Erst nach erfolgreicher Authentifizierung kann die Störung bearbeitet werden.
Der Ansprechpartner hat auf Nachfrage Angaben zu Art und Umfang des Angriffs den Kräften der Telekom zu liefern, um geeignete Gegenmaßnahmen schnellstmöglich einleiten zu können.

3.2 Reaktionszeit

Die Reaktionszeit zwischen einer qualifizierten Meldung eines DoS-Angriffs durch den Kunden und der Rückmeldung über den Beginn der Aktivitäten beträgt

- während der Regelarbeitszeit (an Werktagen – montags bis freitags 7.00 bis 20.00 Uhr und samstags 7.00 bis 14.00 Uhr –) eine Stunde und
- außerhalb der Regelarbeitszeit zwei Stunden.

3.3 Statusmeldungen

Während der Dauer des gemeldeten Angriffs wird der Kunde kontinuierlich über den Fortgang der Aktivitäten informiert. Eine Statusmeldung durch die Telekom erfolgt in der Regel alle zwei Stunden bzw. in Absprache mit dem Ansprechpartner des Kunden sowie bei Statusänderungen.

3.4 Gegenmaßnahmen und Abwehrmechanismen

Im Falle eines vom Kunden gemeldeten Angriffs werden von der Telekom im IP-Backbone geeignete Gegenmaßnahmen ergriffen, soweit dies technisch möglich ist.
Durch die Gegenmaßnahmen wird versucht, den Angriff soweit abzumildern, dass der Internetzugang des Kunden wieder erreichbar ist. Abhängig von der Art des Angriffs kann es aber weiterhin zu einer Beeinträchtigung der betroffenen Dienste des Kunden kommen.
Die Telekom wird in Abstimmung mit dem Ansprechpartner des Kunden die bestmögliche Lösung (Abwehrmechanismen) ermitteln und anwenden. Hiermit soll erreicht werden, dass die kundeneigenen Sicherheitsmechanismen wieder greifen können.
Die Telekom setzt hierbei u. a. verschiedene Standard Abwehrmechanismen ein.

a) Filterlisten
   Die Filterlisten ermöglichen ein Filtern von IP-Verkehr anhand bestimmter Eigenschaften der IP-Pakete. Filterlisten werden manuell konfiguriert.
b) Blackholing
   Blackholing wird verwendet, wenn IP-Adressen angegriffen werden, die vom Kunden nicht verwendet oder benötigt werden, da der gesamte Datenverkehr zu diesen IP-Adressen verworfen wird. Die IP-Adressen sind im Internet nicht mehr erreichbar.
c) Rate-Limits
   Beschränkung der Bandbreite (Bandbreitendrosselung) zu einem Service. Im Falle eines Angriffs ist der betroffene Dienst nur eingeschränkt erreichbar und nur ein Teil der IP-Pakete wird zur Zieladresse übertragen.
d) Mitigation-Device
   Filtern und Verwerfen von anormalen IP-Paketen durch ein Mitigation-Device.
   Hierbei wird der Datenverkehr einzelner Adressen oder des gesamten IP-Adressbereiches des Kunden über ein Mitigation-Device mit automatischer Filterung umgeleitet.

Die Telekom richtet in Absprache mit dem Ansprechpartner des Kunden weitere Gegenmaßnahmen nach den aktuellen technischen Möglichkeiten und der spezifischen Situation während eines Angriffs aus.
Durch die Anwendung der Abwehrmaßnahmen kann nicht sichergestellt werden, dass auch gewollter Verkehr von den angewendeten Maßnahmen betroffen ist.

3.5 Beeinträchtigungen der Qualität der Internet-Anbindung

Für die Dauer der Anwendung der Abwehrmaßnahmen kann es zu Beeinträchtigungen der Qualität an der Internet-Anbindung des Kunden kommen (z. B. Paketverlust, Laufzeitverlängerung). Die von der Telekom für die jeweilige Internet-Anbindung vereinbarten Qualitätsparameter gelten daher für die Dauer der Abwehrmaßnahmen nicht.

3.6 Ein Angriff gilt als beendet, wenn das Datenvolumen wieder die für die jeweilige Internet-Anbindung übliche Verkehrscharakteristik aufweist. In diesem Fall werden nach Rücksprache mit dem Kunden die Abwehrmaßnahmen eingestellt und der Regelzustand der Plattform wiederhergestellt.

4 Besondere Pflichten und Obliegenheiten des Kunden

Der Kunde hat insbesondere folgende Pflichten:

a) Der Kunde hat der Telekom mindestens einen fachlich kompetenten Ansprechpartner mit Rufnummer und E-Mail-Adresse zu benennen, der als Ansprechpartner während der Abwehr eines Angriffs zur Verfügung steht.
   Bei einer Änderung des Ansprechpartners hat der Kunde dies der Telekom unverzüglich mitzuteilen.
   Wurde der Betrieb des Kundennetzes an die Telekom übertragen, kann die Rolle des Ansprechpartners auch von Kräften der Telekom übernommen werden.
b) Meldungen über einen Angriff sind ausschließlich von den benannten Ansprechpartnern des Kunden über die speziellen Rufnummern und E-Mail-Adressen an die Telekom weiterzugeben.
c) Der Kunde hat durch eigene geeignete Maßnahmen (z. B. Firewall, Virenschutz, Software-Updates) seine Infrastruktur vor Angriffen zu schützen und diese auf einen aktuellen Sicherheitsstand zu halten.

5 Vertragslaufzeit/Kündigung

5.1 DDoS-Defence wird jeweils mit einer Mindestvertragslaufzeit von drei Monaten überlassen. Die Vertragslaufzeit beginnt mit dem Tag der vereinbarten Leistungsaufnahme (Bereitstellung) für DDoS-Defence.
Das Vertragsverhältnis kann von beiden Vertragspartnern frühestens zum Ablauf der vereinbarten Mindestvertragslaufzeit mit einer Frist von einem Monat schriftlich gekündigt werden.

Wird nicht fristgerecht gekündigt, so verlängert sich die Vertragslaufzeit um jeweils einen Monat.

4.2 Mit Kündigung des Vertrages über die zugrundeliegende Internet-Anbindung endet auch automatisch das Vertragsverhältnis über DDoS-Defence.

6 Datenschutz

Im Rahmen der Maßnahmen zur Abwehr eines Angriffs kann es erforderlich sein, dass durch Kräfte der Telekom manuell in den Datenverkehr der Internet-Anbindung des Kunden eingegriffen werden muss. Alle Mitarbeiter der Telekom sind schriftlich auf die Einhaltung des Datengeheimnisses nach der Datenschutz-Grundverordnung (DSGVO) und des Fernmeldegeheimnisses nach § 88 Telekommunikationsgesetz verpflichtet. Diese Verpflichtungen werden regelmäßig wiederholt.

7 Preise

Die angegebenen Preise sind Preise ohne Umsatzsteuer (USt); die USt wird in der gesetzlich vorgeschriebenen Höhe zusätzlich berechnet. In der Rechnung werden für die Abrechnung der in Anspruch genommenen Leistungen die Preise ohne USt angegeben. Diese Preise ohne USt werden aufsummiert und sind Grundlage für die Berechnung des Umsatzsteuerbetrages.

	Preise
Überlassung von DDoS-Defence, je Anbindung, monatlich	auf Anfrage
Bereitstellung von DDoS-Defence	auf Anfrage