Leistungsbeschreibung

WOBCOM DDos-Protection

1. Allgemeines

Die WOBCOM (im Folgenden Anbieter genannt) erbringt die nachfolgend beschriebene Dienstleistung auf Basis der Vereinbarungen im Angebot, dem vereinbarten Regelwerk (s. Abschnitt 3.1) und den Allgemeinen Geschäftsbedingungen (AGB) der WOBCOM GmbH. Der DDoS-Schutz ist eine kostenpflichtige Zusatzleistung zu einem Vertrag oder mehreren bestehenden Verträgen über Internetanbindungen.

2. DDoS-Schutz

2.1. Funktionsweise

Für einen wirksamen DDoS-Schutz werden im Backbone des Anbieters Verkehrs, Telemetrie- und Baselining-Daten erhoben. Auf Basis der erhobenen Daten und Muster kann der Anbieter verteilte (distributed) Denial-of-Service-Angriffe (DDoS-Angriffe) identifizieren. Wird ein DDoS-Angriff auf das angegebene Kunden-Netzwerk identifiziert, ergreift der Anbieter Maßnahmen, um den DDoS-Angriff abzuwehren oder abzuschwächen (s. Abschnitt 3.8).

2.2. Umfang des DDoS-Schutzes

Der Anbieter stellt dem Kunden im Rahmen seiner technischen und betrieblichen Möglichkeiten einen Schutz vor DDoS-Angriffen zur Verfügung. Im Rahmen des DDoS-Schutzes verwendet der Anbieter eine Technologie, die in seinem Backbone integriert ist. Diese Technologie identifiziert aktive DDoS Angriffe unter Berücksichtigung des mit dem Kunden abgestimmten Regelwerks (s. Abschnitt 3.1) und wehrt diese ab. Auf Wunsch des Kunden erfolgt ein regelmäßiges Reporting über DDoS Angriffe. Die Einrichtung oder Bereitstellung einer Internetanbindung ist nicht Bestandteil des DDoS-Schutzes.

2.3. Volumenangriffe

Der Anbieter behält sich vor, DDoS-Angriffe mit sehr hohem Datenvolumen (Volumenangriffe) durch den Einsatz von Blackholing (s. Abschnitt 3.8.3) oder durch Einbindung von Dienstleistungen Dritter abzuwehren. Das maximale Volumen bevor sich der Anbieter den Einsatz von Blackholing vorbehält, ergibt sich aus der Spezifikation der vom Kunden gebuchten Dienstleistung.

2.4. Wirkungsbereich des DDoS-Schutzes

Der DDoS-Schutz kann nur DDoS-Angriffe auf zuvor mit dem Kunden abgestimmten IP-Adressen abwehren. Der Wirkungsbereich des DDoS-Schutzes umfasst Schutz gegen DDoS-Angriffe, die sich auf OSI-Layer 3 (z.B. IP/ICMP) oder OSI-Layer 4 (z.B. TCP/UDP) beziehen. Der auf OSI-Layer 3 und 4 bezogene DDoS-Schutz umfasst die Identifikation und Abwehr des Angriffs im Rahmen der technischen Möglichkeiten und nach dem jeweiligen Stand der Technik sowie eine Information des Kunden über den Angriff. Der Anbieter erkennt nur solche DDoS-Angriffe, die über das Netzwerk des Anbieters zu den darin befindlichen IP-Adressen des Kunden geführt werden. Sollte der Kunde zusätzliche Anbindungen an das Internet von anderen Anbietern beziehen, sind diese nicht durch den DDoS-Schutz geschützt. Ebenso wenig umfasst der DDoS-Schutz einen Schutz vor neuartigen Ausprägungen von DDoS-Angriffen, die noch nicht im technischen Regelset für die Netzwerke des Kunden enthalten sind. Dieses Regelset wird fortlaufend durch neue Erkenntnisse von der WOBCOM oder auf Wunsch des Kunden aktualisiert, sodass neuartige Angriffsmethoden, nach einer

Anpassung des Regelset durch den Anbieter, ebenfalls erkannt werden. Der DDoS-Schutz dient nicht dem Schutz vor Hacker-Angriffen (Einbruchsversuche), Angriffen auf Sicherheitslücken (Hardware oder Software) oder anderen Gefahren aus dem Internet, wie zum Beispiel SPAM, Viren, Würmern oder Trojanern.

2.5. Beeinträchtigung der Qualität der Internet-Anbindung
Führt der Anbieter Gegenmaßnahmen (s. Abschnitt 3.8) zur Abwehr eines DDoS-Angriffes durch, kann es zu einer Beeinträchtigung der Qualität der Internetanbindung des Kunden kommen, zum Beispiel in Form von Paketverlusten oder Latenzerhöhungen. Solche Beeinträchtigung stellen keine durch den Anbieter verursachte Störung der Internetanbindung dar, sondern sind eine unvermeidliche Folge des DDoS-Schutzes.

2.6. Kein Mindestniveau der Dienstqualität
Die in dieser Leistungsbeschreibung beschriebenen Dienstleistungen umfassen keine Mindestniveaus der Dienstqualität.

3. Basisleistungen
Der DDoS-Schutz besteht aus den Leistungen des vom Kunden gebuchten Dienstleistungspakets. Bestandteil des DDoS-Schutzes ist ein Regelwerk, auf dessen Basis aktive DDoS-Angriffe identifiziert werden können. Der DDoS-Schutz beinhaltet die Identifikation von DDoS-Angriffen sowie die Abwehr dieser Angriffe. Der Anbieter übernimmt die Konfiguration, das Management und die Wartung der eingesetzten Technologie.

3.1. Vor-Abstimmung und Review-Meeting
Vor dem Beginn der Bereitstellung wird eine Abstimmung mit dem Kunden durchgeführt. Diese Vorabstimmung findet ausschließlich als Video- oder Telefonkonferenz statt. Auf Wunsch des Kunden kann binnen einer Frist von sechs Monaten nach Vertragsstart ein Review-Meeting stattfinden, mit dem Ziel, das zu dem Zeitpunkt aktive Regelwerk zu besprechen und gegebenenfalls Änderungen an diesem zu vereinbaren, etwa wegen einer Veränderung der zu schützenden Infrastruktur oder der darauf ausgeführten Dienste. Über die Art und Weise der Durchführung des Reviews-Meetings werden sich die Parteien vorab gemeinsam verständigen. Je nach der gebuchten Dienstleistung des Kunden kann dieser in regelmäßigen Abständen weitere Review-Meetings in Anspruch nehmen oder während eines Angriffs eine adaptive Anpassung des Regelwerks mit einem Mitarbeitenden des Anbieters in Anspruch nehmen.

3.2. Bereitstellung
Der Anbieter informiert den Kunden über die Bereitstellung des DDoS-Schutzes.

3.3. Management
Im Rahmen des Managements des DDoS-Schutzes übernimmt der Anbieter im Hinblick auf die hierfür bei ihm verwendeten Technologie die Funktionsüberwachung, das Backup der Konfiguration sowie die Software- und Hardwarepflege wie zum Beispiel das Einspielen von Patches oder die Durchführung von Reparaturen.

3.4. Meldung von DDoS-Angriffen

Im Rahmen des DDoS-Schutzes werden DDoS-Angriffe identifiziert und gemeldet. Die Meldung eines DDoS-Angriffs kann auf zwei Wegen erfolgen.

3.4.1. Meldung von DDoS-Angriffen durch den Anbieter

Das für die Identifikation von DDoS-Angriffen betriebene System erkennt einen DDoS-Angriff und meldet diesen über einen abgestimmten Benachrichtigungsweg (E-Mail, Push Notification) an das Network Operation Center des Anbieters.

3.4.2. Meldung von DDoS-Angriffen durch den Kunden

Für den Fall, dass der Kunde einen DDoS-Angriff erkennt oder vermutet, steht ihm eine Notfall-Hotline zur Verfügung, die er 24 Stunden am Tag, 7 Tage die Woche, kontaktieren kann. Meldungen über einen DDoS-Angriff sind ausschließlich von den benannten Ansprechpartnern des Kunden über die angegebenen Rufnummern und E-Mail-Adressen an den Anbieter weiterzugeben.

3.4.3. Bearbeitung von gemeldeten Angriffen

Nach Meldung des DDoS-Angriffs durch die Technologie des Anbieters oder den Kunden nimmt der Anbieter die Qualifizierung des DDoS-Angriffs vor und bewertet, ob es sich um einen aktiven DDoS-Angriff handelt oder nicht. Der Anbieter nimmt im Falle eines aktiven DDoS-Angriffs Kontakt mit dem festgelegten fachlichen Ansprechpartner des Kunden auf. In Abstimmung mit dem Kunden werden geeignete Gegenmaßnahmen zur Abwehr des DDoS-Angriffs eingeleitet.

3.5. Manuelle Abwehr von DDoS-Angriffen

Im Falle eines aktiven DDoS-Angriffs steht dem Kunden telefonisch ein Mitarbeiter des Anbieters zur Verfügung (s. Abschnitt 3.7), der Gegenmaßnahmen zur Abwehr des DDoS-Angriffs vornimmt, der zudem mit dem fachlichen Ansprechpartner des Kunden telefonisch in Kontakt steht und diesen über den Status der Abwehrmaßnahmen informiert.

3.5.1. Statusmeldung

Im Falle eines aktiven DDoS-Angriffs erfolgt in regelmäßigen Abständen oder nach Absprache mit dem Kunden, eine Statusmeldung. Im Falle einer Änderung des Status informiert der Anbieter den fachlichen Ansprechpartner des Kunden unmittelbar.

3.5.2. Reporting

Nach Abschluss eines DDoS-Angriffs wird auf Wunsch des Kunden ein Report mit Informationen über den erfolgten Angriff generiert und via E-Mail an den Kunden versendet.

3.6. Automatische Abwehr von DDoS-Angriffen

Der Anbieter richtet standardmäßig eine automatische Erkennung und Abwehr von DDoS-Angriffen (Auto Mitigation) durch die verwendete Technologie ein. In diesem Fall beruht die Erkennung eines DDoS-Angriffs ausschließlich auf festen, vorab vorgegebenen Parametern. In diesem Fall entfällt eine manuelle Qualifizierung von

DDoS-Angriffen durch den Anbieter. Auf ausdrücklichen Wunsch des Kunden kann der Anbieter die automatische Erkennung und Abwehr von DDoS-Angriffen (Auto Mitigation) deaktivieren.

3.7. Reaktionszeit

Falls die in Abschnitt 3.6 beschriebene automatische Erkennung und Abwehr von DDoS-Angriffen (Auto Mitigation) deaktiviert ist, beträgt die Reaktionszeit zwischen einem von dem Kunden oder manuell gemeldeten DDoS-Angriff und dem Beginn der in Abschnitt 3.4.3 beschriebenen Aktivitäten

• während der Regelarbeitszeit (montags bis freitags 7:00 bis 17:00 Uhr) eine Stunde und

• außerhalb der Regelarbeitszeit zwei Stunden.

3.8. Gegenmaßnahmen

Dem Anbieter stehen verschiedene Gegenmaßnahmen zur Abwehr von DDoS-Angriffen zu Verfügung. Die nachfolgend beschriebenen Gegenmaßnahmen haben zum Ziel, die im Regelwerk des Kunden definierten IP-Netze und die damit verbundenen Services erreichbar zu halten. Abhängig von der Art des DDoS-Angriffs kann es jedoch weiterhin zu einer Beeinträchtigung der betroffenen IP-Adressen des Kunden kommen. Der Anbieter wird im Falle eines Angriffs die bestmögliche Lösung zur Abwehr des DDoS-Angriffs ermitteln. Der Anbieter kann nicht sicherstellen, dass durch die Abwehr des DDoSAngriffs regulärer, nicht durch den DDoS-Angriff verursachter Traffic, gefiltert wird. Es können auch unterschiedliche Gegenmaßnahmen miteinander kombiniert werden.

3.8.1. DDoS-Mitigation über Flowspec im Backbone des Anbieters

Bei der Gegenmaßnahme Flowspec an BGP-Routern wird eine Erweiterung des Routingprotokolls BGP (Flowspec) verwendet, um im Angriffsfall Flowspec basierte Filter an den BGP-Routern zu verteilen. Diese Filter sorgen dafür, dass identifizierte Datenpakete, die Teil des Angriffs sind, bereits an den Routern gefiltert werden können.

3.8.2. DDoS-Mitigation über Umleitung von Datenverkehr

Bei der Gegenmaßnahme DDoS-Mitigation wird der Datenverkehr zu den angegriffenen IP-Adressen des Kunden im Backbone des Anbieters über ein dediziertes System im Rechenzentrum des Anbieters geleitet. Der Anbieter behält sich vor, DDoS-Angriffe mit sehr hohem Datenvolumen (Volumenangriffe) durch den Einsatz von Dienstleistungen Dritter (außerhalb des Rechenzentrums des Anbieters) abzuwehren. Die DDoS-Mitigation hat zum Ziel, den durch den DDoS-Angriff verursachten Datenverkehr vom regulären Datenverkehr zu trennen. Der reguläre Datenverkehr wird im Rahmen der technischen Möglichkeiten an die ursprünglichen IP-Adressen des Kunden weitergeleitet.

3.8.3. Destination Based Blackholing

Bei der Gegenmaßnahme Destination Based Blackholing wird der gesamte Datenverkehr zu der angegriffenen IP-Adresse des Kunden zwischen Internet und Backbone des Anbieters verworfen. Dadurch ist die betroffene IP-Adresse im Internet nicht mehr erreichbar. Die Internetanbindung des Kunden steht für die nicht betroffenen IP-Adressen jedoch weiterhin zur Verfügung. Der Anbieter behält sich vor, bei sehr großen DDoS-Angriffen auch die vorgeschalteten Internet

Service Provider oder Peering Partner darum zu bitten, den betroffenen Datenverkehr ebenfalls zu verwerfen.

3.9. Ende eines Angriffs
Ein DDoS-Angriff gilt als beendet, wenn der Datenverkehr zur im Regelwerk des Kunden definierten IP-Adresse eine normale Verkehrscharakteristik aufweist. Im Falle von automatisiert ausgerollten Filtern werden diese automatisch zurückgezogen. Im Falle einer manuellen Mitigation des DDoS-Angriffs nimmt der Anbieter Kontakt zum fachlichen Ansprechpartner des Kunden auf und stellt die getroffenen Gegenmaßnahmen nach Rücksprache mit dem fachlichen Ansprechpartner ein.

4. Zusätzliche Leistungen
Erbringt der Anbieter vereinbarungsgemäß neben den vertraglich geschuldeten Leistungen weitere Leistungen, so sind diese vom Kunden gemäß der jeweils gültigen Preisliste oder, wenn die Leistung in der Preisliste nicht vorgesehen ist, nach Aufwand zu vergüten, falls nicht ausdrücklich eine entgegenstehende Vereinbarung getroffen worden ist.

5. Besondere Pflichten und Obliegenheiten des Kunden
Dem Kunden obliegen gegenüber dem Anbieter insbesondere die im Folgenden beschriebenen Pflichten: Der Kunde hat dem Anbieter mindestens einen fachlich kompetenten Ansprechpartner mit Namen, Rufnummer, E-Mail-Adresse und Erreichbarkeitszeit entsprechend zu benennen. Der oder die Ansprechpartner stehen dem Anbieter als Kontakt für die Einrichtung des DDoS-Schutzes (Regelwerk) und während der Abwehr eines Angriffs zur Verfügung. Bei einer Änderung des Ansprechpartners hat der Kunde dies dem Anbieter unverzüglich mitzuteilen.

6. Störungen
Unbeschadet etwaiger Pflichten aus § 58 Telekommunikationsgesetz (Entstörung) gelten im Falle einer Störung der vertragsgegenständlichen Dienstleistungen die nachfolgenden Vereinbarungen in diesem Abschnitt 6.

6.1. Meldung der Störung
Treten im Betrieb des DDoS-Schutzes Störungen auf, obliegt es dem Kunden, dem Anbieter diese Störungen unverzüglich mitzuteilen.

6.2. Entstörfrist
Die Frist zur Entstörung des DDoS-Schutzes beträgt 16 Stunden nach Meldung der Störung durch den Kunden, soweit Hardware des Anbieters betroffen ist. Für Störungen des DDoS-Schutzes, die nicht auf Hardwareschäden des Anbieters zurückzuführen sind, gilt eine Entstörfrist von 8 Stunden nach Meldung der Störung durch den Kunden. Im Fall höherer Gewalt oder bei Störungen, die von Zulieferern des Anbieters verursacht werden, kann die Entstörfrist überschritten werden. Verzögerungen durch mangelnde Mitwirkung des Kunden werden auf die Entstörfrist angerechnet.

6.3. Behebung von Störungen

Eine Störung gilt als behoben, wenn die Funktionalität wiederhergestellt ist und der Kunde diese vertragliche Dienstleistung wieder nutzen kann.

6.4. Eigenverschulden
Hat der Kunde die Störung zu vertreten oder liegt eine vom Kunden gemeldet Störung nicht vor, ist der Anbieter berechtigt, dem Kunden die ihm durch die Entstörung bzw. den Entstörversuch entstandenen Kosten gemäß der jeweils gültigen Preisliste oder, wenn die Leistung in der Preisliste nicht vorgesehen ist, nach Aufwand in Rechnung zu stellen.

7. Wartungsarbeiten
Wartungsarbeiten des Anbieters können eine geplante Unterbrechung der vertraglichen Dienstleistung bewirken. Der Anbieter wird den Kunden rechtzeitig im Voraus über Wartungsarbeiten informieren. In dringenden Fällen kann eine ungeplante Wartung ohne vorherige Information des Kunden notwendig sein.

8. Verfügbarkeit
Der DDoS-Schutz-Service hat eine Verfügbarkeit von 99,5% im Jahresmittel. Folgende Zeiten und Ausfälle werden in der Verfügbarkeitsrechnung nicht berücksichtigt:
• Die Entstörfrist (s. Abschnitt 6.2),
• Ausfälle durch Fehler, die im Verantwortungsbereich des Kunden liegen,
• unvermeidliche Unterbrechungen auf Grund von Änderungswünschen des Kunden,
• Ausfälle, die durch höhere Gewalt verursacht wurden,
• Ausfälle in Folge des ausdrücklichen Wunsches des Kunden, die Störung nicht zu beheben,
• Ausfälle auf Grund geplanter oder vereinbarter Unterbrechungen in Folge von Wartungsarbeiten des Anbieters oder des Kunden und
• Zeitverluste, die nicht vom Anbieter verschuldet sind.

9. Sicherheit der Daten

Der Anbieter unternimmt alle angemessenen und zumutbaren Schritte, um größtmögliche Datensicherheit zu gewährleisten und den Zugriff von unberechtigten Dritten zu unterbinden, soweit es im Rahmen der gängigen Methoden technisch möglich ist. Der Anbieter kann jedoch nicht für Fehler haftbar gemacht werden, die vom Kunden oder von Dritten verursacht wurden.