Leistungsbeschreibung

der EWE TEL GmbH für EWE Managed Security: DDoS-Schutz

1 Allgemeines

Die EWE TEL GmbH (im Folgenden Anbieter genannt) erbringt die nachfolgend beschriebene Dienstleistung EWE Managed Security: DDoS-Schutz (im Folgenden DDoS-Schutz genannt) auf Basis der Vereinbarungen im Auftragsformular, dem vereinbarten Regelwerk (s. Abschnitt 2.1) und den *Allgemeinen Geschäftsbedingungen (AGB) der EWE TEL GmbH für Telekommunikations-, Online- und Datendienstleistungen*. Der DDoS-Schutz ist eine kostenpflichtige Zusatzleistung zu einem Vertrag oder mehreren bestehenden Verträgen über Internetanbindungen aus den Produktfamilien EWE Proline, EWE Multi Connect und EWE Colocate.

1.1 Funktionsweise des DDoS-Schutzes

Für einen wirksamen DDoS-Schutz werden im Backbone des Anbieters Telemetrie- und Baselining-Daten erhoben. Auf Basis der erhobenen Daten und Muster kann der Anbieter aktive Distributed Denial of Service (DDoS)-Angriffe identifizieren. Wird ein aktiver DDoS-Angriff auf den Kunden identifiziert, ergreift der Anbieter Maßnahmen, um den DDoS-Angriff abzuwehren (s. Abschnitt 2.7).

1.2 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 2.1) und wehrt diese ab. Auf Kundenwunsch wird ein zyklisches DDoS-Reporting aktiviert. Die Einrichtung oder Bereitstellung einer Internetanbindung ist nicht Bestandteil des DDoS-Schutzes.

1.3 Volumenangriffe

Der Anbieter behält sich vor, DDoS-Angriffe mit sehr hohem Datenvolumen (Volumenangriffe) durch den Einsatz von Blackholing (s. Abschnitt 2.8.2) abzuwehren.

1.4 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. DDoS-Angriffe auf OSI-Layer 5 bis 7 können höchstens nach einer manuellen Identifikation, zum Beispiel auf Basis einer Meldung des Kunden, abgewehrt werden. 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 in der Signaturen-Datenbank der eingesetzten Technologie enthalten sind. Diese Datenbank wird jedoch fortlaufend – auf Basis von weltweiten Analysen – aktualisiert, sodass neuartige Ausprägungen, nach einem Update 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.

1.5 Beeinträchtigung der Qualität der Internet-Anbindung

Führt der Anbieter Gegenmaßnahmen (s. Abschnitt 2.8) 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 Basisleistungen

Der DDoS-Schutz besteht aus einer Basisleistung und weiteren kostenpflichtigen optionalen Leistungen (s. Abschnitt 3). Bestandteil des DDoS-Schutzes ist ein mit dem Kunden abgestimmtes 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.

2.1 Regelwerk; Consulting-Termin; Review-Meeting

Der Anbieter führt gemeinsam mit dem Kunden einen Consulting-Termin durch. Soweit nicht ausdrücklich anders vereinbart, findet der Termin telefonisch statt. In diesem Termin werden die gewünschten Regeln sowie die gewünschte Konfiguration des DDoS-Schutzes festgelegt und in einem Regelwerk elektronisch dokumentiert. Als Vorbereitung für den Consulting-Termin definiert der Kunde seine Kommunikationsbeziehungen, die durch den DDoS-Schutz geschützt werden sollen. Der Anbieter wird den DDoS-Schutz auf Basis des mit dem Kunden abgestimmten Regelwerks in Form eines (einzigen) Managed Objects konfigurieren. In komplexen Umgebungen kann der Kunde ein kostenpflichtiges, erweitertes Regelwerk mit zusätzlichen Managed Objects erhalten (s. Abschnitt 3.1).

Auf Wunsch des Kunden kann in einem Intervall von sechs Monate 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.

2.2 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.

2.3 Abnahme

Nachdem der Anbieter den DDoS-Schutz in Betrieb genommen hat, stellt er dem Kunden das Regelwerk elektronisch zur Verfügung und fordert den Kunden zur Abnahme des vom Anbieter eingerichteten DDoS-Schutzes auf. Der Kunde hat die Abnahme in Textform zu erklären. Die Abnahme kann nicht auf Grund unwesentlicher Mängel verweigert werden. Der Abnahme steht es gleich, wenn der Kunde den DDoS-Schutz nicht binnen einer Frist von 10 Werktragen abgenommen hat, obwohl er dazu verpflichtet ist. Das bereitgestellte DDoS-Schutz-Regelwerk bildet die Basis für den Betrieb des DDoS-Schutzes. Stellt der Kunde innerhalb von 10 Werktagen nach Inbetriebnahme des DDoS-Schutzes fest, dass die im Rahmen des Consulting-Termins (Abschnitt 2.1) ermittelten Regeln unvollständig oder fehlerhaft sind, wird der Anbieter die Regeln entsprechend erweitern oder korrigieren. Die vorgesehene Frist von 10 Werktagen zur Abnahme verlängert sich hierdurch nicht.

2.4 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.

2.4.1 Meldung von DDoS-Angriffen durch den Anbieter

Das für die Identifikation von DDoS-Angriffen betriebene System erkennt einen DDoS-Angriff und meldet diesen über ein Netzwerkmanagementsystem an das Network Operation Center des Anbieters.

Stand: 03/19 LB_GK_DDoS_e_02_010319

2.4.2 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 und unter Mitteilung des im Regelwerk definierten Passworts an den Anbieter weiterzugeben.

2.4.3 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 (s. Abschnitt 2.7). 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.

2.5 Manuelle Abwehr von DDoS-Angriffen

Im Falle eines aktiven DDoS-Angriffs steht dem Kunden telefonisch ein Mitarbeiter des Anbieters zur Verfügung (s. Abschnitt 2.7), 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.

2.5.1 Statusmeldung

Im Falle eines aktiven DDoS-Angriffs erfolgt in regelmäßigen Abständen, spätestens aber nach 2 Stunden, oder nach Absprache mit dem Kunden, eine Statusmeldung. Im Falle einer Änderung des Status informiert der Anbieter den fachlichen Ansprechpartner des Kunden unmittelbar.

2.5.2 Reporting

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

2.6 Automatische Abwehr von DDoS-Angriffen

Auf ausdrücklichen Wunsch des Kunden richtet der Anbieter eine automatische Erkennung und Abwehr von DDoS-Angriffen durch die verwendete Technologie ein. In diesem Fall beruht die Erkennung eines DDoS-Angriffs ausschließlich auf festen, vorab vorgegebenen Parametern. Eine manuelle Qualifizierung von DDoS-Angriffen durch den Anbieter entfällt. Aus diesen Gründen erhöht sich die Gefahr einer fehlerhaften Erkennung (false positives). Die automatische Abwehr von DDoS-Angriffen sollte nur nach sorgfältigen Tests und in enger Absprache zwischen Anbieter und Kunden erfolgen.

2.7 Reaktionszeit

Die Reaktionszeit zwischen einem von dem Kunden oder der eingesetzten Technologie gemeldeten DDoS-Angriff und dem Beginn der in Abschnitt 2.4.3 beschriebenen Aktivitäten beträgt

- während der Regelarbeitszeit (an Werktagen, montags bis freitags 7.00 bis 17.00 Uhr) eine Stunde und
- außerhalb der Regelarbeitszeit zwei Stunden.

2.8. Gegenmaßnahmen

Dem Anbieter stehen verschiedene Gegenmaßnahmen zur Abwehr von DDoS-Angriffen zu Verfügung. Die Gegenmaßnahmen werden ausschließlich in dem Backbone des Anbieters und auf seiner Hardware durchgeführt; sie führen nicht dazu, dass Datenverkehr des Kunden zu Dritten geführt wird. 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 mit dem Ansprechpartner des Kunden die bestmögliche Lösung zur Abwehr des DDoS-Angriffs ermitteln. Der Anbieter kann nicht sicherstellen, dass durch die Abwehr des DDoS-Angriffs regulärer, nicht durch den DDoS-Angriff verursachter Traffic, gefiltert wird.

2.8.1 DDoS-Mitigation

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. 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.

2.8.2 Destination Based Blackholing

Bei der Gegenmaßnahme Destination Based Blackholing (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.

2.9 Ende eines Angriffs

Ein DDoS-Angriff gilt als beendet, wenn der Datenverkehr zur im Regelwerk des Kunden definierten IP-Adresse eine normale Verkehrscharakteristik aufweist. Der Anbieter nimmt in diesem Fall Kontakt zum fachlichen Ansprechpartner des Kunden auf und stellt die getroffenen Gegenmaßnahmen nach Rücksprache mit dem fachlichen Ansprechpartner ein.

3 Optionale Leistungen

Der Anbieter bietet optionale Leistungen für die Einrichtung und den Betrieb des DDoS-Schutzes an. Die optionalen Leistungen sind bei oder nach Beauftragung des DDoS-Schutzes buchbar und gemäß der jeweils gültigen Preisliste oder, wenn die Leistung in der Preisliste nicht vorgesehen ist, entsprechend des individuellen Angebots zu vergüten. Der Anbieter richtet beauftragte optionale Leistungen nach Vorgabe des Kunden und abhängig von den technischen Möglichkeiten ein. Nachfolgende optionale Leistungen stehen hierbei zur Verfügung:

- Erweitertes Regelwerk (Abschnitt 3.1),
- Konfigurations- und Regelwerksänderungen (Abschnitt 3.2).

3.1 Erweitertes Regelwerk

Das erweiterte Regelwerk bietet in komplexen Umgebungen die Möglichkeit, über das in Abschnitt 2.1 definierte Limit von einem Managed Object hinaus, jeweils ein weiteres Managed Object zu beauftragen.

3.2 Konfigurations- und Regelwerksänderungen

Der Kunde kann den Anbieter damit beauftragen, Änderungen an dem Regelwerk und der Konfiguration des DDoS-Schutzes vorzunehmen. Über das hierbei einzuhaltende Verfahren informiert der Anbieter den Kunden. Der Anbieter nimmt Änderungen an Konfiguration oder Regelwerk nur dann vor, wenn sie von den im Regelwerk aufgeführten autorisierten Personen und mit allen erforderlichen Angaben beauftragt wurden.

Der Anbieter führt vereinbarte Änderungen an Konfiguration oder Regelwerk innerhalb von zwei Werktagen durch, sofern keine Rücksprache mit dem Kunden notwendig ist; solche Änderungen stellen keine Wartung dar. Der Kunde hat die Durchführung der Änderung an Konfiguration oder Regelwerk gemäß der jeweils gültigen Preisliste oder, wenn die Leistung in der Preisliste nicht vorgesehen ist, nach Aufwand zu vergüten.

4 Zusätzliche Leistungen

Erbringt der Anbieter vereinbarungemäß 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 des Auftragsformulars 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 des DDoS-Schutzes

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

6.1 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 nicht angerechnet

6.2 Behebung von Störungen

Eine Störung gilt als behoben, wenn der Anbieter sie gegenüber dem Kunden abgemeldet hat oder wenn die Funktionalität wiederhergestellt ist und der Kunde diese vertragliche Dienstleistung wieder nutzen kann.

6.3 Eigenverschulden

Hat der Kunde die Störung zu vertreten oder liegt eine vom Kunden gemeldete 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 6.1),
- 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.

Stand: 01.03.2019

LB_GK_DDoS_e_02_010319

Stand: 03/19