Leistungsbeschreibung
WiTCOM DDOS SCHUTZ

1. ALLGEMEINES

WiTCOM, Wiesbadener Informations- und Telekommunikations GmbH (im Folgenden WiTCOM), bietet auf der Grundlage der „Allgemeinen Geschäftsbedingungen der WiTCOM GmbH“ ihren Geschäftskunden den Service „WiTCOM DDOS SCHUTZ“ an.

2. STANDARDLEISTUNG

Ein DDoS-Angriff ist eine spezielle Art der Cyber-Kriminalität. Der Distributed-Denial-of-Service (DDoS) ist ein „verteilter“ Denial-of-Service (DoS), der wiederum eine Dienstblockade/ Dienstverweigerung auslösen soll. Diese liegt vor, wenn ein angefragter Dienst (z. B. ein Internetzugang, eine Serverinfrastruktur, eine Website, etc.) nicht mehr bzw. nur noch stark eingeschränkt verfügbar ist. Auslöser ist in den meisten Fällen eine Überlastung der IT-Infrastruktur, die durch einen Angriff herbeigeführt wird. Der WiTCOM DDOS SCHUTZ bietet im Falle eines DDOS-Angriffes auf Ihren WiTCOM INTERNETZUGANG eine Filterung des Datenverkehrs an. Dieser WiTCOM DDOS SCHUTZ dient sowohl dem Schutz des WiTCOM INTERNETZUGANGES, wie auch der Infrastruktur des Kunden, bevor der Angriff diesen erreicht. Die Lösung ist On-Demand, was bedeutet, dass im Falle eines Angriffes die Lösung automatisiert geschaltet wird. Durch permanentes Monitoring der WiTCOM Infrastruktur kann nach Feststellung einer Annomalie eine Filterung des Kunden Datenverkehrs erfolgen. Diese Filterung wird zur Abwehr des Angriffes bei signifikant höheren Datenraten, sowie bei speziellen Angriffsmustern als Maßnahme eingeleitet. Die dabei ermittelten Pakete werden verworfen (Bad-Traffic) und der Datenverkehr gereinigt (Clean-Traffic) dem Zielsystem (Kunden) zugestellt. Die Bereinigung kann dabei im Verantwortungsbereich der WiTCOM sowie in einem Rechenzentrum eines Partners in Deutschland erfolgen.

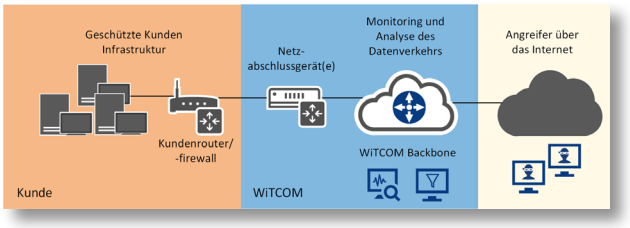
Bei Beauftragung von WiTCOM DDOS SCHUTZ wird die Subnetzgröße und die zu reinigende Bandbreite (Clean-Traffic) definiert. Während eines Angriffes wird die definierte und gereinigte Bandbreite dem Kunden wieder zugeführt. Ein möglicher Ausfall während des Angriffs oder durch den WiTCOM Infrastrukturschutz Blackholing (8.1 Blackholing / Sinkholing) wird umgangen und die Kundeninfrastruktur ist weiterhin, über den WiTCOM INTERNETZUGANG mit der gebuchten gereinigten Bandbreite, erreichbar. Der Schutz umfasst die ISO/OSI Schichten 3 (IP) und 4 (TCP, UDP) sowie verschiedene netzwerk-, und protokollbasierte DDoS-Angriffsarten, zum Beispiel gegen SYN/ACK/RST-Flood, ICMP-Flood, UDP-Fragmentation, UDP-Amplification via DNS, NTP, rcpbind, SSDP, LDAP usw..

Durch Anpassungen der Maßnahmen und der Reaktion auf Veränderungen während eines Angriffes, liefert WiTCOM DDOS SCHUTZ eine optimale und individuelle Lösung zur DDoS Abwehr.

WiTCOM speichert die zur Verfügung stehenden Protokolldaten der Schichten 3 und 4 des OSI-Schichtenmodells in folgendem Umfang zur Angriffserkennung, -analyse und -abwehr:

Eingehende Trafficpakete in mehreren Snippets zu gesamt 3 Sekunden je Minute. Hierüber lassen sich stochastische und heuristische Rückschlüsse auf den Gesamttraffic und ein eventuelles Angriffsverhalten ziehen. Eine Analyse auf Applikationsebene (OSI-Schicht 7) findet nicht statt. Die gespeicherten und analysierten Snippets werden nach erfolgter Analyse komplett verworfen.

Zur forensischen Analyse speichert WiTCOM auf Wunsch des Kunden lediglich statistische Daten über Trafficmengen und Paketarten im Rahmen der Flowdaten-Analyse. Inhaltlich werden keine Datenpakete erhoben oder für weitere Verwendungen verarbeitet.



2.1 Bandbreite

Der WiTCOM DDOS SCHUTZ wehrt Angriffe mit bis zu 2 Tbit/s Abwehrbandbreite ab. Unter der Abwehrbandbreite ist die Bandbreite zu verstehen, welche den Kunden vor dem Angriffsvolumen schützt.

Damit der Kunde trotz des Angriffes erreichbar bleibt, führt WiTCOM dem Kunden eine zuvor vereinbarte bereinigte Bandbreite (Clean-Traffic) zu, über welche das Zielsystem (Kunde) weiterhin erreichbar ist. Eine Erhöhung dieser bereinigten Bandbreite ist während der Vertragslaufzeit nicht vorgesehen.

2.3 IPv4 und IPv6

Der Zuwachs von IPv6 Adressen und der damit einhergehende vergrößerte Adressraum, sorgt zunehmend für Sichereheitsrisiken. Angriffe durch IPv4 lassen sich inzwischen auch durch IPv6 umsetzten, mit häufig verstärkter Intensität. Mit Dualstack wird Ihnen der Datenaustausch sowohl mit IPv4 als auch mit IPv6 Adressen sichergestellt.

2.4 E-Mail Support

Für allgemeine Fragen im Zusammenhang mit dem beauftragten Service oder für sonstige Standard-Unterstützung, steht dem Kunden der WiTCOM Support während der Öffnungszeiten zwischen Montag und Freitag von 8 bis 17 Uhr (ausgenommen Feiertage in Hessen) per E-Mail (technik@witcom.de) zur Verfügung.

2.5 Monitoring und Reporting

Für die frühzeitige Erkennung von Angriffen analysiert WiTCOM permanent den Datenverkehr im WiTCOM Backbone (Flow Monitoring). Mögliche Angriffe sollen damit frühestmöglich erkannt und Gegenmaßnahmen eingeleitet werden. Nach Abwehr eines DDoS-Angriffes erstellt WiTCOM ein Reporting mit verschiedenen Informationen des Angriffes, welches dem Kunden an Werktagen innerhalb von 48 Stunden zur Verfügung gestellt wird. Im Reporting werden Informationen zum Zeitraum des abgewehrten Angriffs sowie zur Anzahl der Anfragen (Requests), die während des Angriffs die betroffene IP-Adresse angesprochen haben, präsentiert. Der Typ des Angriffes, Daten über die Peak-Bandbreiten und die Peak-Paketrate sind tabellarisch und grafisch dargestellt.

2.6 Testumschaltung

Nach Bereitstellung des WiTCOM DDOS SCHUTZ wird das neu geschützte Kundennetz durch eine Testumschaltung (BGP Schwenk) umgeroutet. Dies geschieht händisch oder durch einen simulierten Angriff. Die Testumschaltung nimmt nur einen kurzen Zeitraum (i. d. R. 30 Minuten) in Anspruch und wird zwischen dem

Kunden und der WiTCOM abgesprochen (Zeitfenster). Dieser Service ist in den Produktkosten inkludiert. Es kann während der Testumschaltung zu kurzen minimalen Einschränkungen kommen, die den laufenden Betrieb nicht langfristig beeinflussen. Der Test ist Abschluss der Bereitstellung und ermöglicht WiTCOM alle Konfigurationen zu prüfen und den legitimen Traffic des Kunden nachzuvollziehen, um Anomalien früher und besser zu erkennen.

3. BUCHBARE ZUSATZLEISTUNGEN (ENTFÄLLT)

4. BEREITSTELLUNG

Die Bereitstellung des WiTCOM DDOS SCHUTZ liegt ausschließlich im Verantwortungsbereich der WiTCOM. WiTCOM stimmt die Einzelheiten der Realisierung mit dem Kunden ab. Der verbindliche Bereitstellungstermin wird dem Kunden per E-Mail mitgeteilt.

4.1 Voraussetzung

Voraussetzung ist, dass der Kunde über einen von WiTCOM betriebenen Internetzugang verfügt. Für die Bereitstellung muss die Subnetzgröße und die zu bereinigende Bandbreite durch den Kunden festegelegt werden. WiTCOM empfiehlt eine bereinigte Bandbreite von 20 % der originär über WiTCOM bezogenen Bandbreite des Internetzugangs des Kunden.

4.2 Realisierung

Zur Realisierung des WiTCOM DDOS SCHUTZ muss ein technisch geklärter Auftrag vorliegen.

Ein Auftrag für einen WiTCOM DDOS SCHUTZ gilt als technisch geklärt, wenn die oben genannten Voraussetzungen erfüllt sind und eine Prüfung der verfügbaren Infrastrukturressourcen mit positivem Ergebnis seitens WiTCOM abgeschlossen wurde. Hierzu erfolgt gegebenenfalls seitens WiTCOM eine Ortsbegehung.

4.3 Standardinstallation

Nach abgeschlossener Installation meldet WiTCOM dem Kunden schriftlich (per E-Mail) die Betriebsbereitschaft und fordert ihn zur Abnahme des Services auf.

Die Abnahme gilt als stillschweigend erklärt, wenn der Kunde spätestens fünf (5) Arbeitstage nach der Mitteilung der Betriebsbereitschaft keine erheblichen Mängel anzeigt oder die Abnahme ausdrücklich verweigert.

Bei Beginn dieser Frist weist WiTCOM den Kunden nochmals besonders darauf hin, dass eine unterbliebene Mängelanzeige bzw. die ausdrückliche Abnahmeverweigerung mit Fristablauf als Abnahme gilt.

Das Produkt WiTCOM DDOS SCHUTZ ist nur in Kombination mit einem WiTCOM INTERNETZUGANG buchbar. Dadurch liegen WiTCOM die benötigten Netzwerkinformationen zur Installation bereit.

5. SERVICELEISTUNGEN

WiTCOM beseitigt Störungen ihrer technischen Einrichtungen im Rahmen der technischen und betrieblichen Möglichkeiten. Hierbei erbringt WiTCOM insbesondere folgende Leistungen:

5.1 Verfügbarkeit

Unter „Verfügbarkeit eines Services“ versteht man den prozentualen Anteil eines Kalenderjahres, währenddessen der Service nicht von Störungen betroffen ist.

Die Verfügbarkeit errechnet sich nach folgender Formel:

$$\text{Verfügbarkeit} = 100\% - \frac{\text{kumulierte Entstörzeiten im Kalenderjahr in Stunden x } 100\%}{\text{Kalenderjahr in Stunden}}$$

Die Verfügbarkeit (% p. a.) wird für den gesamten Service ermittelt, wobei die Störungen jeweils mit ihren gemäß 5.4 gemessenen Entstörzeiten berücksichtigt werden.

Die Serviceverfügbarkeit des WiTCOM DDOS SCHUTZ beträgt i. d. R.mindestens 99,5 % p. a..

5.2 Störungsmeldung

WiTCOM nimmt Störungsmeldungen täglich von 0 Uhr bis 24 Uhr unter der Technischen-Hotline-Nummer 08000-948266 (08000-WiTCOM) entgegen. Bei der Störungsmeldung ist es wichtig das WiTCOM folgende Informationen vorliegen: Service-ID, Firmenname, Ansprechpartner, ggf. der Standort (falls es mehrere Lokationen gibt) und die Details der Störung.

5.3 Servicebereitschaft

Die Servicebereitschaft besteht bei WiTCOM DDOS SCHUTZ täglich von 0 bis 24 Uhr.

5.4 Entstörzeit

Entstörzeit ist die Zeit vom Eingang der Störungsmeldung, jedoch nicht vor Beginn der Servicebereitschaft, bis zu der Zeit in der WiTCOM einen Service wiederherstellt. Sie beinhaltet die Reaktionszeit. WiTCOM garantiert im Standardfall eine maximale Entstörzeit von vier (4) Stunden.

Die Fristen gelten als eingehalten, wenn innerhalb der Entstörzeiten die vollständige Wiederherstellung des vertraglich vereinbarten Leistungsumfanges abgeschlossen wird und die Rückmeldung gem. 5.7 erfolgte.

Bei der Störungsbehebung hat der Kunde WiTCOM im Rahmen seiner Möglichkeiten bei der Lokalisierung des Fehlers zu unterstützen und gegebenenfalls Zugang zu seinen Standorten zu gewähren.

Besondere Bedingungen des Störungsmanagements mit einer näheren Beschreibung des Prozesses können in einer gesonderten Vereinbarung als Ergänzung des Vertrags geregelt werden.

Als Entstörzeiten gelten nicht:

- Zeiten, in denen der Kunde für WiTCOM nicht erreichbar ist.
- Zeitanteile, die aus einer fehlenden oder unzureichenden Mitwirkung des Kunden bei der Störungsbeseitigung resultieren. Insbesondere gilt dieses für vom Kunden zu vertretende Wartezeiten des WiTCOM-Servicetechnikers beim Zugang zu den Räumlichkeiten, in denen sich möglicherweise betroffene technische Einrichtungen befinden.
- Zeiten, die durch Umstände außerhalb des Einflussbereiches der WiTCOM hervorgerufen worden sind, z. B. in oder durch Einrichtungen des Kunden oder anderer Netzbetreiber.
- Zeiten, die aufgrund höherer Gewalt entstehen, z. B. bei Naturkatastrophen (vgl. § 11 AGB).

- Ereignisse / Ursachen, die WiTCOM nicht zu vertreten hat (insbesondere durch Fremdeinwirkung in Form einer mechanischen oder andersartigen Beschädigung / Zerstörung der aktiven Komponenten und / oder passiven Kabeltrassen).
- ausdrückliche Ablehnungen der Störungsbehebung seitens des Kunden vor Ort.
- Störungen / Fehler außerhalb des Zuständigkeitsbereichs von WiTCOM und ihrer Zulieferer (z. B. Inhouseverkabelung, Stromversorgungsanlagen und Kundenausrüstungen).

5.5 Reaktionszeit

Die Reaktionszeit beträgt maximal 30 Minuten ab Eingang der Störungsmeldung.

Die Reaktion kann auch durch Antritt des Servicetechnikers vor Ort beim Kunden erfolgen.

5.6 Zwischenmeldung

WiTCOM informiert den Kunden auf Wunsch alle zwei (2) Stunden nach Ablauf der Reaktionszeit oder nach Absprache über den Bearbeitungsstand und den Ausblick auf weitere Maßnahmen.

5.7 Rückmeldung

WiTCOM informiert den Kunden nach Beendigung der Entstörung. Wird der Kunde beim erstmaligen Versuch nicht erreicht, gilt die Entstörungszeit nach Punkt 5.4 als eingehalten. Weitere Versuche zur Rückmeldung werden regelmäßig durchgeführt.

5.8 Wartung

WiTCOM wird den Kunden von erforderlichen geplanten Wartungsmaßnahmen, die Betriebsunterbrechungen verursachen, mindestens 10 Arbeitstage (ausgenommen Feiertage in Hessen) im voraus informieren. Auf Wunsch kann der Kunde in begründeten Einzelfällen um eine Aufschiebung oder Terminänderung für Wartungsarbeiten bitten / erfragen. Die Arbeiten finden zu Zeiten statt, in denen in der Regel eine geringe Nutzung der Services erfolgt. Die Zeiten für Wartungsmaßnahmen werden bei der Ermittlung von Verfügbarkeiten nicht berücksichtigt.

5.9 Terminvereinbarung

WiTCOM vereinbart mit dem Kunden, soweit erforderlich, einen Termin für den Besuch eines Servicetechnikers. Dieser Termin wird mit einer maximalen Zeitspanne von zwei (2) Stunden angegeben (z. B. „Zwischen 10 Uhr und 12 Uhr“).

Ist die Leistungserbringung im vereinbarten Zeitraum aus von dem Kunden zu vertretenden Gründen nicht möglich, wird ein neuer Termin vereinbart und eine gegebenenfalls zusätzlich erforderliche Anfahrt berechnet.

5.10 Sonstige Störungsmeldungen

Soweit die Störung vom Kunden zu vertreten ist (hervorgerufen z. B. in oder durch Einrichtungen des Kunden oder durch eine vom Kunden veranlasste Störungsfalschmeldung) hat WiTCOM Anspruch auf Ersatz der dadurch entstandenen Kosten.

Dieser Fall wird entsprechend des Aufwandes nach internen Stundensätzen abgerechnet.

6. VERTRAGSBEDINGUNGEN

Es gelten die Allgemeinen Geschäftsbedingungen der WiTCOM GmbH (AGB). Bei Abweichungen haben die Regelungen dieser Leistungsbeschreibung Vorrang vor den AGB.

6.1 Vertragslaufzeit

Die Vertragslaufzeit richtet sich grundsätzlich nach der Laufzeit des beauftragten WiTCOM INTERNETZUGANGES und wird individuell mit dem Kunden vereinbart. In begründeten Ausnahmefällen kann WiTCOM eine Mindestvertragslaufzeit festlegen, die die Restlaufzeit des WiTCOM INTERNETZUGANGES überschreiten kann. Der Vertrag ist erstmals mit der Frist von drei (3) Monaten zum Ende der festgelegten Mindestvertragslaufzeit oder der Frist des WiTCOM INTERNETZUGANGES kündbar. Ohne Kündigung verlängert sich der Vertrag im Anschluss auf unbestimmte Zeit und ist mit einem (1) Monat kündbar. Jede Kündigung kann frühestens zum Ablauf der vereinbarten Laufzeit erfolgen, soweit keine anderweitigen Regelungen getroffen wurden.

6.2 Zahlungsbedingungen

Für die Überlassung von WiTCOM DDOS SCHUTZ zahlt der Kunde an WiTCOM ein Entgelt, das sich aus den Abrechnungspositionen „einmaliges Bereitstellungsentgelt“ und „monatliches Entgelt“ ergibt.

Das monatliche Entgelt ist grundsätzlich nutzungsunabhängig und als solches im Voraus zur Zahlung fällig.

6.3 Rückgabebedingungen (CPE)

Die dem Kunden für die Vertragsdauer leihweise überlassene technische Einrichtung (CPE – Customer-Premises-Equipment) verbleit im Eigentum der WiTCOM. Bei Vertragsbeendigung ist der Kunde verpflichtet die von WiTCOM gestellte technische Einrichtung vollständig innerhalb von 14 Tagen nach Auslaufen des Vertrages an WiTCOM zurückzusenden. Die technische Einrichtung ist in einwandfreien Zustand und innerhalb der Rückgabefrist zurückzugeben, andernfalls kann WiTCOM Schadensersatz verlangen. Durch Versand entstehende Kosten sind vom Kunden zu tragen. Alternativ zum Versand können separate Abkommen mit WiTCOM per E-Mail getroffen werden.

7. HAFTUNG

Das Netzabschlussgerät verbleibt im Eigentum der WiTCOM. Bei Kündigung des Vertrages ist das Netzabschlussgerät in der Originalkonfiguration an WiTCOM zu übergeben. Der Kunde haftet für jede von ihm oder von Dritten, für die er einzustehen hat, verschuldete Beschädigung des Netzabschlussgerätes.

8. SONSTIGE LEISTUNGEN

8.1 Blackholing / Sinkholing

Blackholing und Sinkholing sind von WiTCOM bereitgestellte Verfahren, die nicht erwünschten Traffic im Netz unterbinden. Bei Blackholing werden alle Anfragen (gewünschte und unerwünschte) an Domains oder IP-Adressen statt in das eigene Netz ins „Nichts“ geleitet. Mit dem Einsatz von Sinkholing werden die Anfragen auf DNS-Server umg eleitet auf welchen zuständige Domain-Registrierungsstellen die schädlichen Domainnamen analysieren und protokollieren. Zum Schutz unserer Kunden und zum Schutz der eigenen Infrastruktur, hält sich WiTCOM vor, auf Angriffe von

außen mit den beschriebenen Methoden zu reagieren. Diese Methoden schützen den Kunden bzw. die WiTCOM Infrastruktur, indem Quell-Adressen (Angriffsquelle) ausgeschlossen werden oder Ziel-Adressen (Kunde) nicht mehr erreichbar sind. Hierbei wird die Attacke unterbunden und der Zugriff aus / auf diesem(n) IP-Bereich verwehrt. Als Folge der Methoden sind die Ziel- aber auch Quelladressen nicht mehr erreichbar. Alternativ dazu bietet WiTCOM das Produkt WiTCOM DDOS SCHUTZ, mit welchem der Kunde auch bei Angriffen weiterhin erreichbar ist. Kunden können WiTCOM direkt auf übermäßig hohen Verkehr zu deren Netz hinweisen. WiTCOM informiert den Kunden, sollte dieser durch die entsprechenden Maßnahmen nicht mehr erreichbar sein.