Litecom
stark verbunden

Servicebeschreibung

Dienst **DDoS-Schutz (Basis-/Vollschutz)**
Version / Datum 1.2 vom 27. September 2023

Inhaltsverzeichnis

Litecom AG
Entfelderstrasse 2 | CH-5000 Aarau
T +41 62 562 62 62 | www.litecom.ch

1. Servicebeschreibung – DDoS Schutz

Cyberangriffe mittels Distributed Denial of Service (DDoS) nehmen stetig zu und beinträchtigen gesamte Web-Dienste und IT-Plattformen. Das führt zu grossen Herausforderungen bei Organisationen, die geschäftskritische Internetdienste betreiben.

1.1. Wie funktioniert eine DDoS Attacke?

Eine Distributed Denial of Service Attacke beinhaltet den Einsatz vieler IT-Geräte (Bots), die am Internet angeschlossen sind. Dabei werden Geräte im Internet mit Sicherheitslücken mit Schadsoftware infiziert. Die Bots werden durch die Schadsoftware zentral von einem «Command and Control» Server gesteuert. Dabei wir ein spezifisches Internetziel ausgewählt und alle infizierten Bots über dieses Ziel informiert. Danach senden die Bots zeitgleich viele Anfragen an das Zielsystem, dass unter der hohen Anfragelast zusammenbricht.
Das Mirai Botnet hat im Jahr 2016 durch seine bisher unübertroffene Grösse und Kapazität Berühmtheit erlangt. Mirai verfügte über rund 300'000 Bots die Angriffe mit insgesamt 1Tbps Schlagkraft durchführen konnte.

Ein DDoS Angriff wird nicht ausschliesslich zur Lahmlegung von Internetdiensten eingesetzt. Ein DDoS Angriff kann als Ablenkungsmanöver für einen parallelen Cyberangriff eingesetzt werden. Die Angreifer fokussieren sich dabei auf andere Ziele des Unternehmens wie zum Beispiel dem Datenklau von geschäftskritischen Unternehmensdaten.
DDoS Attacken werden meist im Darknet zu immer günstigeren Preisen angeboten. Die Angebotsvielfalt und Qualität nimmt stetig zu und ermöglicht es somit auch Laien einen wirkungsvollen DDoS Angriff zu organisieren.

1.2. DDoS in der Schweiz

2016 wurden Digitec, Migros und Coop Opfer von DDoS Attacken. Dabei wurden die Unternehmen einige Tage vor der Attacke von den Angreifern erpresst. Die Unternehmen haben sich nicht erpressen lassen, was auch der Empfehlung vom Bund entspricht. Als Folge davon, dauerten die Angriffe rund eine Woche wobei in dieser Zeit nur vereinzelt Bestellungen in den Online-Shops getätigt werden konnte. Auch bereits bestellte Waren konnten nur vereinzelt ausgeliefert werden. Die Umsatzeinbussen der Unternehmen durch den Angriff wurden nicht bekannt. IT-Sicherheitsexperten gehen von einem zweistelligen Millionenbetrag aus.

Durch die vermehrte Nutzung von Homeoffice und dem daraus resultierenden erhöhten Bedürfnis nach Kommunikation und Kollaboration wurden Teile der Betriebs IT über Nacht businessrelevant. Gleichzeitig mit der Zunahme von Home Office wird laufend eine Zunahme der DDoS Angriffe verzeichnet.

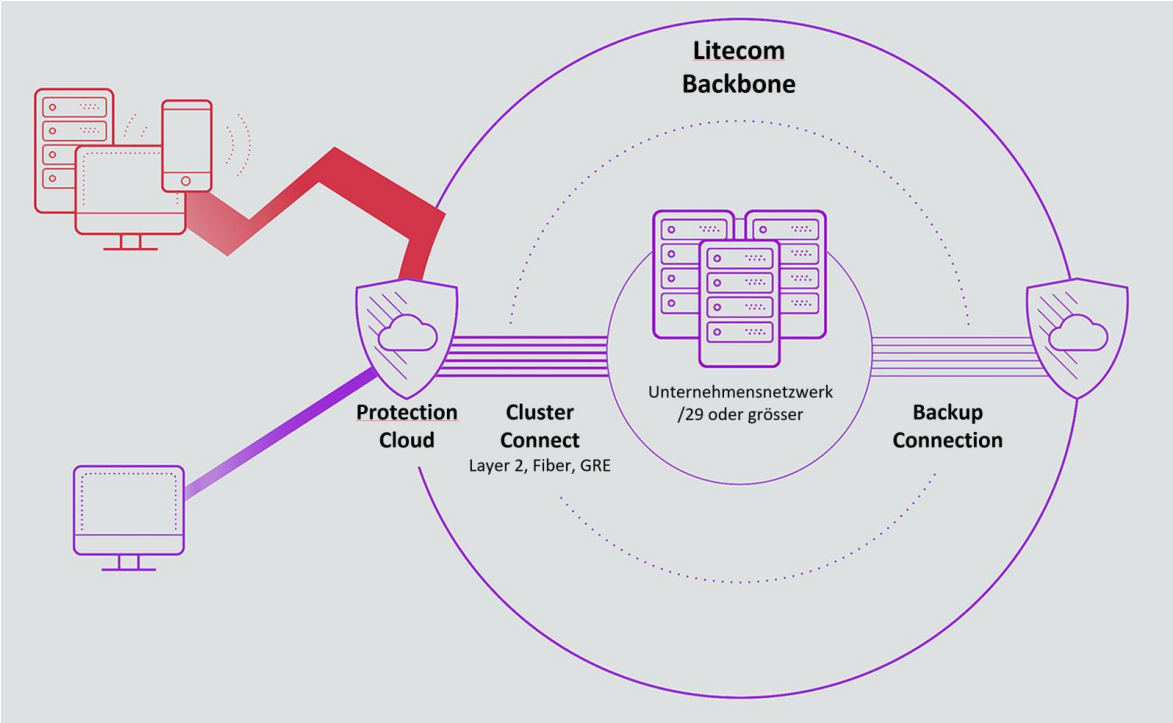
1.3. Generelle Beschreibung

Litecom bietet mit dem DDoS-Basisschutz Firmen einen cloudbasierten Service, in Zusammenarbeit mit einem DDoS-Spezialisten als Technologiepartner, an. Litecom verfügt über eine direkte dedizierte Anbindung an den Filter-Cluster (Datacenterstandort Zürich) des Technologiepartners. Diese Anbindung bis zum Filter-Cluster wird von Litecom betrieben und gewartet. Gegenüber einer cloudbasierten Lösung mit einer Overlay-Anbindung resultiert in der Litecom-Lösung keine Verkleinerung der MTU-Size.

Darüber hinaus betreibt und wartet unser Technologiepartner den Filter-Cluster (Scrubbingcenter) und übernimmt die Mitigation von DDoS Attacken. Durch den DDoS Service von Litecom kann der Kunde Investitionen in hochspezifische Fachkräfte, hochbandbreitige Internet Uplinks und in eine eigene DDoS-Lösung vermeiden.

DDoS-Attacken sind Angriffe auf IT-Ressourcen und Netzwerke mit dem erklärten Ziel, diese zu überlasten und ausser Kraft zu setzen. Der cloudbasierte DDoS-Schutz von Litecom hat das Ziel, möglichst viele dieser bösartigen Anfragen möglichst früh herauszufiltern, sodass das angegriffene Ziel diensttauglich bleibt. Demnach werden legitime Nutzeranfragen vom schädlichen DDoS-Verkehr des Angreifers bewahrt. Die Services bleiben somit für Kunden und Mitarbeiter des Unternehmens auch während eines laufenden Angriffes verfügbar.

Litecom als renommierter Anbieter für Netzwerklösungen hat die Bedrohungslage durch DDoS Angriffe erkannt und bietet gemeinsam mit Partnern verschiedene DDoS-Lösungen an. Die vielfältigen Lösungskonzepte bieten unseren Kunden den passenden Schutz für den entsprechenden Bedarf.



2. Lösungsübersicht DDoS

Die DDoS-Lösung kann entweder als Basisschutz oder Vollschutz bestellt werden. Je nachdem welche Bedürfnisse Sie haben. Wir finden für Sie die passende Lösung.

2.1. DDoS Basisschutz

Der DDoS Basisschutz von Litecom bietet Hostern und Carriern die Möglichkeit die eigene Infrastruktur zu schützen. Eine fixe Bandbreitenlimitierung per IP wird für die Kundenetzwerke bei Hostern oder für den Backbone bei Carriern eingerichtet. Bei einem DDoS-Angriff wird ausschliesslich der Bandbreite in Höhe des gebuchten Internetanschlusses zum Ziel weitergereicht.
Der DDoS-Basisschutz verhindert, dass die Internetanbindung ihres Backbones komplett mit Angriffsverkehr überflutet wird. Somit wird sichergestellt, dass die vom Angriff nicht betroffenen IPs nach wie vor erreichbar bleiben. Für den Basisschutz benötigen Sie somit mindestens ein /24 IP-Netz und ist somit für Carrier, Reseller, Hoster und Grosskunden interessant die ihre eigene Backbone-Infrastruktur schützen möchten. Der Verkehr der angegriffenen IP-Adresse wird bezüglich Bandbreite limitiert und der Rest des Verkehrsverworfen, sodass der Backbone wie auch der Zugriff ins Internet für alle übrigen Adressen weiterhin in vollem Umfang verfügbar ist.
Dabei sind von Kundenseite keine Kenntnisse zu DDoS-Angriffen und Vektoren nötig. Das DDoS-Schutz-Cluster analysiert den Datentransfer auf bestimmte Muster und wertet diese anonymisiert aus. Die Inhalte der Datenpakete werden nicht gespeichert.

2.2. DDoS Vollschutz

Der DDoS-Vollschutz bietet einen umfassenden Schutz für ganze Netzwerksegmente. Gemeinsam mit unserem Technologiepartner, wird der gesamte Netzwerkverkehr fortlaufend analysiert und im Angriffsfall aussortiert und gefiltert. Ziel ist es, den schädlichen Netzwerkverkehr von legitimem Netzwerkverkehr zu unterscheiden und nur den legitimen Verkehr an das Ziel weiterzuleiten. Unternehmen die geschäftskritische Internetdienste anbieten, Mitarbeiter von unterwegs Zugriff auf Ressourcen im Firmennetzwerk oder Datacenter oder auch darauf angewiesen sind via Internet zu kommunizieren, bietet der Vollschutz eine optimale Lösung, um Sicherheitsrisiken und Auswirkungen durch DDoS-Angriffe stark zu minimieren.
Unter anderem überwacht eine KI und lernt anhand des Nutzerverhaltens, um so jederzeit und so schnell wie möglich auf Angriffe reagieren zu können. Dabei sind von Kundenseite keine Kenntnisse zu DDoS-Angriffen und Vektoren nötig. Das DDoS-Schutz-Cluster analysiert den Datentransfer auf bestimmte Muster und wertet diese anonymisiert aus. Die Inhalte der Datenpakete werden nicht gespeichert.
Für die Säuberung der DDoS-Attacken und Anbindung am Filter-Cluster wurde ein DDoS-Scrubbing Center in Zürich errichtet. Weitere DDoS-Filter-Cluster im Backbone des Technologiepartner sind weltweit im Einsatz und mitigieren Angriffe frühzeitig, sodass diese bereits an der Quelle beseitigt werden. Damit sorgt der Service für einen performanten, hochverfügbaren und stark skalierbaren DDoS-Schutz für Kundennetzwerke.
Bei der Kombination aus Basis- und Vollschutz resultiert der Vorteil, dass auch Kunden mit kleineren IP-Adressbereichen als /24 von einem Vollschutz profitieren können.

3. Serviceverfügbarkeit

Vorfälle, die die Dienste der Litecom beeinträchtigen und von Dritten verursacht werden (wie zum Beispiel Störungen durch andere Netzbetreiber, IP-Traffic-Knoten oder von Dritten kontrollierte Energieanlagen), liegen ausserhalb der Verantwortung von Litecom. Ausfallzeiten, die auf solche Vorfälle zurückzuführen sind, fallen nicht unter die Verfügbarkeit.

Die Verfügbarkeit ist definiert als die Summe der Zeit, in welcher der DDoS-Schutz Dienst in einem Betrachtungszeitintervall von einem Kalenderjahr (365 Tage) dem Kunden garantiert zur Verfügung steht. Die für einen Dienst garantierte Verfügbarkeit wird über die Service Level Stufe definiert. Die Verfügbarkeit der Anschlusstechnologie an den DDoS-Schutz sind nicht Bestandteil der Verfügbarkeitsbetrachtung und deshalb ausgeschlossen. Die Verfügbarkeiten können der unteren Tabelle entnommen werden.

Stufe	Verfügbarkeit	Supportzeit	Reaktionszeit	Interventionszeit	Penalty
Premium	>99.9%	7x24 h	30 Min.	4 h*	Ja
PremiumPlus	>99.95%	7x24 h	30 Min.	4 h*	Ja

* siehe Kapitel 3.2.3 Interventionszeit.

Im Angriffsfall können mindestens 100Gbps geschützt werden. Angriffe grösser als 100Gbps wird im Idealfall ebenfalls geschützt, trotzdem behalten wir uns das Recht vor, Verkehr der die 100Gbps übersteigt, zu blackholen, also zu löschen.
Der Demarkationspunkt für das SLA und deren Messung ist das Scrubbing Center. Ausgeschlossen von diesem SLA ist die Connectivity zum Scrubbing Center.

3.1. Schadensbegrenzungszeit

Bestimmte Arten von DDoS-Angriffen haben eine sogenannte Schadensbegrenzungszeit (Time to Mitigate, TTM). Die TTM beschreibt den Zeitraum zwischen dem Beginn eines Angriffs und dem Abschluss der Abwehralgorithmen mit dem Ergebnis, dass nahezu 99% des bösartigen Verkehrs blockiert werden.
Das SLA gilt nur für den Fall, dass der Datenverkehr im «Always-On» Betrieb über den Technologiepartner geleitet wird und der Vollschutz für das entsprechende Netzwerk gebucht wurde. Für eine Standby-Implementierung gelten die TTM-Werte in der folgenden Tabelle erst ab dem Zeitpunkt der Aktivierung des DDoS-Schutzes.

Angriffstyp	**TTM DPI (Always-on)**	**TTM DPI (Standby)**
Fragmentierung	sofort	sofort
TCP-Anomalien	sofort	sofort
UDP-Anomalien	sofort	sofort
IP-Anomalien	sofort	sofort
TCP/UDP-Reflection/Amplification-Angriffe	<10 Sekunden	<10 Sekunden
TCP-SYN-Floods	<10 Sekunden	<10 Sekunden
ICMP-Floods	<10 Sekunden	<10 Sekunden

Botnet-basierte UDP-Floods	<10 Sekunden	<10 Sekunden
Botnet-basierte TCP-Floods	<10 Sekunden	<10 Sekunden
Abwehr basierend auf künstlicher Intelligenz/maschinellem Lernen	<9 Sekunden	keine Angabe

3.2. Support und Störungen

Wir können rund um die Uhr auf das Security Operation Center unseres Technologiepartners zugreifen. Im Falle einer Störung oder eines Ausfalls wenden Sie sich bitte an unseren Servicedesk unter 0800 342 000 oder in weniger dringenden Fällen auch über unser Formular unter https://www.litecom.ch/Servicedesk.htm. Alle SLA relevanten Störungen müssen zwingend zusätzlich über das Servicedesk per Telefon gemeldet werden.

3.2.1. Supportzeiten

Die Supportzeit ist die Zeit, in welcher der Kunde ein Anrecht auf die Behebung einer Störung hat und welche durch das SLA gedeckt ist. Für den DDoS-Schutz beträgt die Supportzeit 7/24 während 365 Tagen im Jahr und ist zeitlich nicht eingeschränkt.

3.2.2. Reaktionszeiten

Die Zeit zwischen Eingang der Störungsmeldung durch den Kunden auf der Störungsnummer der Litecom und der Aufnahme der Bearbeitung des Störungsfalles ist definiert als Reaktionszeit.

Level	**Beispiel**	**Reaktionszeit**
P3 (low)	• Ausfälle, bei denen redundante Alternativen existieren • Backbone Connect mit Failover • andere Fehler, die die Nutzung des Link11-Dienstes oder den Zugriff auf ein wesentliches Merkmal des Services nicht einschränken	30 Minuten
P2 (high)	• Ausfälle mit Service Impact • kritische Störungen von Services oder Servicemerkmalen	30 Minuten
P1 (critical)	• Störungen/Ausfälle im Core-Netz, nicht absehbare Lösungszeit	30 Minuten

Die Reaktionszeit definiert, dass ein erster Kontakt zu einem Störungsmanager hergestellt worden ist und ein Ticket im Ticketsystem erstellt wurde.

3.2.3. Interventionszeit

Die Interventionszeit ist die Zeit zwischen Eingang der Störung und Beginn der Intervention auf die Störung.

Level	Beispiel	Interventions-zeit
P3 (low)	• Ausfälle, bei denen redundante Alternativen existieren • Backbone Connect mit Failover • andere Fehler, die die Nutzung des Dienstes oder den Zugriff auf ein wesentliches Merkmal des Services nicht einschränken	4 Stunden
P2 (high)	• Ausfälle mit Service Impact • kritische Störungen von Services oder Servicemerkmalen	2 Stunden
P1 (critical)	• Störungen/Ausfälle im Core-Netz, nicht absehbare Lösungszeit	2 Stunden

3.2.4. Störungen bei Dritten

Vorfälle, die die Dienste des Technologiepartners beeinträchtigen und von Dritten verursacht werden (wie zum Beispiel Störungen durch andere Netzbetreiber, IP-Traffic-Knoten oder von Dritten kontrollierte Energieanlagen), liegen außerhalb der Verantwortung der Litecom AG. Ausfallzeiten, die auf solche Vorfälle zurückzuführen sind, fallen nicht unter die Verfügbarkeitsgarantie.

3.2.5. Penalty

Wenn die Verfügbarkeit in einer Abrechnungsperiode unter die Verfügbarkeit fällt, hat der Kunde am Ende der Abrechnungsperiode Anspruch auf eine einmalige Gutschrift, die mit der Gebühr für die nächste Abrechnungsperiode verrechnet wird. Die Dauer der Nichtverfügbarkeit berechnet sich, indem alle Zeiten während des Abrechnungszeitraums, in denen der Litecom-Dienst nicht verfügbar, addiert werden (unter Berücksichtigung der dienstspezifischen Berechnungsweisen). Die Gutschrift erfolgt auf Basis der letzten vom Kunden gezahlten regulären Gebühr.
Pro angebrochene 0.1% (8.75 Stunden) welche die garantierte Verfügbarkeit unterschreiten, bezogen auf ein Betrachtungszeitintervall von einem Kalenderjahr (365 Tage), erstattet Litecom dem Kunden 5% des monatlichen wiederkehrenden Betrags des betroffenen Dienstes zurück, maximal jedoch 90% des monatlich wiederkehrenden Betrages des betroffenen Dienstes pro Kalenderjahr. Ausfälle verschuldet durch höhere Gewalt, durch den Kunden selbst, oder andere im EULA und SLA aufgeführten Gründe sind von der SLA-Messung ausgenommen.

4. Wartungsfenster

Störungen aufgrund höherer Gewalt wie im EULA beschrieben und Wartungen sind von der Verfügbarkeitsgarantie ausgeschlossen, d.h. die SLA-Messung wird ausgesetzt. Wartungsarbeiten werden in der Regel zwischen 0:00 Uhr und 6:00 Uhr MEZ/MESZ durchgeführt, zu anderen Zeiten kündigt Litecom diese Wartungen im Vorfeld an. Sofern der Service weniger als 5 Minuten unterbrochen wird, hat Litecom jede Woche von Montag auf Dienstag zwischen 1 Uhr und 6 Uhr ein ordentliches Wartungsfenster, welches nicht angekündigt wird und für Änderungen verwendet werden kann.

4.1. Geplante Wartungsfenster

Wartungsarbeiten werden in der Regel zwischen 0:00 Uhr und 6:00 Uhr MEZ/MESZ durchgeführt werden – sie kann aber ebenfalls zu anderen Zeiten erfolgen.

4.2. Ungeplante Wartungsfenster

Sofern u.a. die Sicherheit der Plattform in Gefahr ist, z.B. aufgrund von Sicherheitslücken, Bugs oder anderen kritischen Fehlern – sofern der sichere Betrieb von einzelnen Teilen der Plattform nicht mehr gewährleistet werden kann oder ganze Standorte vom Netz genommen werden müssen, kann eine ungeplante Wartung jederzeit und ohne Ankündigung vorgenommen werden.

5. Reports

5.1. SLA-Report

Ausfallzeiten, welche durch die Litecom AG oder durch unseren Technologiepartner entstanden sind, werden durch einen Reason for Outage (RFO) dokumentiert, um die Rückverfolgbarkeit zu gewährleisten und zukünftige Ausfallzeiten zu vermeiden. Der RFO wird auf Anfrage zur Verfügung gestellt. Im RFO wird ein Ereignisprotokoll, eine Zeitliste, die Ursachenforschung und mögliche Lösungswege beschrieben.

5.2. DDoS-Report

Der Kunde erhält auf Anfrage einen DDoS-Report mit weiteren Angaben zu einem erfolgten DDoS-Angriff.