Servicebeschreibung

Thema **DDoS-Protection (DDoS-BP Backbone-Protection & DDoS-Protection)**
Version 1.4 vom 13. September 2024

Inhaltsverzeichnis

Litecom AG
Obere Vorstadt 40 | CH-5000 Aarau
T +41 62 562 62 62 | www.litecom.ch

1. Servicebeschreibung – DDoS-Protection

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, das 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. Weitere Fälle sind bekannt.

Ein DDoS Angriff wird nicht ausschliesslich zur Lahmlegung von Internetdiensten eingesetzt. Ein DDoS Angriff kann als Ablenkungsmanöver für einen parallelen Cyberangriff eingesetzt werden oder aber auch als Türöffner für ein weiters eindringen in die Systeme eines Unternehmens. 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 konnten. 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 Homeoffice wird laufend eine Zunahme der DDoS Angriffe verzeichnet.

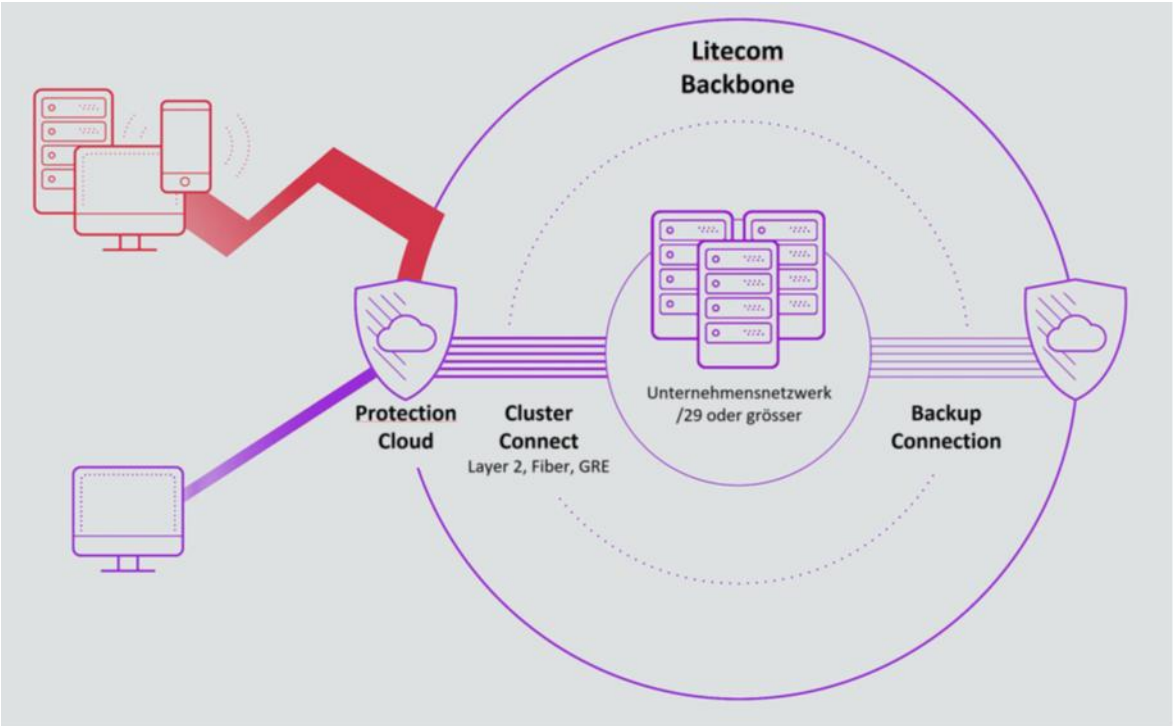
1.3. Generelle Beschreibung

Litecom bietet mit dem DDoS-Schutz einen cloudbasierten Service an, dies in Zusammenarbeit mit einem DDoS-Spezialisten als Technologiepartner. 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 cloudbasier-ten 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 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 vielfäl-tigen Lösungskonzepte bieten unseren Kunden den passenden Schutz für den entsprechenden Bedarf.



2. Lösungsübersicht DDoS

Die DDoS-Lösung kann entweder als DDoS-Backbone-Protection oder DDoS-Protection (dies ist der Schutz der einzelnen Kunden) bestellt werden.

2.1. DDoS-Backbone-Protection

Die DDoS-Backbone-Protection von Litecom bietet Hostern und Carriern die Möglichkeit die eigene Infrastruktur zu schützen. In den unter Schutz stehenden IP-Ranges wird eine fixe Bandbreitenlimitierung per IP-Adresse eingerichtet.
Die DDoS-Backbone-Protection verhindert, dass die Internetanbindung ihres Backbones komplett mit Angriffsverkehr überflutet wird. Somit wird sichergestellt, dass die vom Angriff nicht betroffenen IP-Adressen nach wie vor erreichbar bleiben. Für den Backbone Schutz benötigen Sie somit mindestens ein /24 öffentliches IP-Subnetz und ist damit für Carrier, Reseller, Hoster und Gross-kunden interessant die ihre eigene Backbone-Infrastruktur schützen möchten. Der Verkehr der an-gegriffenen IP-Adresse wird bezüglich Bandbreite limitiert oder gelöscht, sodass der Backbone wie auch der Zugriff ins Internet für alle übrigen Adressen weiterhin verfügbar ist.
Dabei sind von Kundenseite keine Kenntnisse zu DDoS-Angriffen und Vektoren notwendig. Der DDoS-Schutz-Cluster analysiert den Netzwerkverkehr auf bestimmte Muster und wertet diese anonymisiert aus. Die Inhalte der Datenpakete werden nicht gespeichert (DSGVO konforme Datenverarbeitung).

2.2. DDoS-Protection

Die DDoS-Protection (dies ist der Schutz der einzelnen Kunden) bietet einen umfassenden Schutz für Internet-Anschlüsse bzw. der öffentlichen IP-Adressen des Anschlusses. Gemeinsam mit unserem Technologiepartner, wird der gesamte Netzwerkverkehr fortlaufend analysiert und im Angriffsfall aussortiert und gefiltert. Ziel ist es, den schädlichen 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 benötigen, bietet der Vollschutz eine optimale Lösung, um Sicherheitsrisiken und Auswirkungen durch DDoS-Angriffe stark zu minimieren.
Unter anderem überwacht eine KI den Verkehr und lernt anhand der Nutzung, um so jederzeit und so schnell wie möglich auf Angriffe reagieren zu können. Dabei sind von Kundenseite keine Kenntnisse zu DDoS-Angriffen notwendig. Der DDoS-Schutz-Cluster analysiert den Netzwerkverkehr 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.
Diese Lösung basierend auf der Backbone-Protection, hat den Vorteil, dass auch Kunden mit kleineren IP-Adressbereichen als /24 von einer DDoS-Protection profitieren können.

3. Service Level Agreement

3.1. Beschreibung der Service Level Parameter

3.1.1. Verfügbarkeit

Die Verfügbarkeit ist definiert als die Summe der Zeit, in welcher der Dienst für eine Verbindung oder einen Anschluss in einem Betrachtungszeitintervall von einem Kalenderjahr (365 Tage) dem Kunden garantiert zur Verfügung steht.

Ein Dienst gilt von dem Zeitpunkt an als nicht verfügbar, ab welchem der Kunde bei der Litecom Störungsannahmestelle eine Störung platziert hat. Ausnahmen dabei bilden Dienste, welche mit der Zusatzoption „proaktive Überwachung“ bezogen werden. In diesem Fall gilt der effektive Ausfall-Zeitpunkt des Dienstes als Beginn des Ausfalls.

Unterbrechungen aus betrieblichen Gründen haben bei der Kalkulation der Dienstverfügbarkeit keine Relevanz und gelten nicht als Unterbruch im Sinne der garantierten Verfügbarkeit.

Die für einen Dienst garantierte Verfügbarkeit wird über die Service Level Stufe definiert.

3.1.2. Supportzeit

Die Zeit, in welcher der Kunde Anrecht auf die Behebung einer Störung hat und in welcher er je nach Service Level Stufe garantierte Fristen für Reaktions- und Interventionszeit hat gilt als Supportzeit. Diese kann entweder rund um die Uhr (7x24x365) oder zeitlich eingeschränkt auf bestimmte Zeitfenster, wie z.B. Bürozeiten 08.00 bis 17.00 Uhr, sein. Die für einen Service garantierte Supportzeit ist mit der Service Level Stufe definiert.

3.1.3. Reaktionszeit (Response Time)

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. Fällt die Reaktionszeit auf einen Zeitpunkt ausserhalb der Supportzeit, beginnt diese erst mit dem Beginn des nächsten Supportzeitfensters zu laufen. Die für einen Service garantierte Reaktionszeit ist mit der Service Level Stufe definiert.

3.1.4. Interventionszeit (Onsite Troubleshooting Response Time)

Die Zeit zwischen Eingang der Störungsmeldung und Beginn der Intervention auf die Störung vor Ort oder remote ist definiert als Interventionszeit. Die Interventionszeit wird bei Beendigung des Supportzeitfensters bis zum Beginn des nächsten Supportzeitfensters unterbrochen. Die für einen Service garantierte Interventionszeit ist mit der Service Level Stufe definiert.

3.1.5. Typische Wiederherstellungszeit (MTRS/MTTR)

Die durchschnittliche Zeit, die benötigt wird, um einen Dienst nach einer Störung wiederherzustellen. Gemessen vom Zeitpunkt der Störungsmeldung durch den Kunden oder mit der Zusatzoption „proaktive Überwachung“ beim effektiven Ausfallzeitpunkt.

3.2. Service Levels

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

* siehe Kapitel 3.1.4 Interventionszeit.

Die Service Level Stufe für einen Dienst ist jeweils im entsprechenden Objektvertrag respektive Preisblatt definiert. Die einzelnen Parameter sind oben unter 3.1 beschrieben.

Die typische Wiederherstellungszeit eines Dienstes hängt von der Priorität der Störung ab, welche sich wiederum aus der Dringlichkeit und dem Ausmass der Störung ableitet:

Priorität	MTRS
P1	8 h
P2	16 h
P3	48 h

4.1. Unterbrechung der Dienste für Wartungsarbeiten

4.1.1. Geplante Arbeiten / Ordentliche Wartungsfenster

Um Telekom-Dienste auf hohem Sicherheits- und Qualitätsniveau anbieten zu können, muss das entsprechende Netzwerk systematisch gewartet und aktualisiert werden. Solche Unterhaltsarbeiten sind leider nicht immer unterbruchsfrei durchführbar. Selbstverständlich ist die Litecom als Anbieter bemüht, wartungsbedingte Unterbrechungen auf ein Minimum zu beschränken.

Sind aus betrieblichen Gründen Unterbrechungen der Dienste notwendig, so können diese in einem **ordentlichen Wartungsfenster** durchgeführt werden. Das ordentliche Wartungsfenster findet zum Zeitpunkt des Vertragsabschlusses jede Woche von **Montag auf Dienstag zwischen 01:00 und 06:00 Uhr** statt. Änderungen an der Zeitdauer oder am Zeitpunkt des Wartungsfensters werden dem Kunden schriftlich mitgeteilt. Der Kunde wird über bevorstehende Unterbrechungen von Diensten in einem ordentlichen Wartungsfenster nicht einzeln informiert.

4.1.2. Ausserordentliche Arbeiten / Ausserordentliche Wartungsfenster

Sind aus betrieblichen Gründen Unterbrechungen der Dienste notwendig, welche nicht innerhalb des regulären Wartungsfensters durchführbar sind, so können diese in einem ausserordentlichen Wartungsfenster durchgeführt werden. Der Kunde wird in diesem Fall mindestens 10 Arbeitstage im Voraus per E-Mail darüber informiert. Nach Möglichkeit werden seine Interessen berücksichtigt. Der Kunde kann im Zusammenhang mit betrieblich notwendigen Unterbrechungen keine Pönale geltend machen.

4.2. Penalty

Pro angebrochene 0.1% (8.75 Stunden) Unterschreiten der garantierten Verfügbarkeit, bezogen auf ein Betrachtungszeitintervall von einem Kalenderjahr (365 Tage), erstattet Litecom dem Kunden 10% des monatlich wiederkehrenden Betrages des betroffenen Dienstes zurück, maximal jedoch 100% des monatlich wiederkehrenden Betrages des betroffenen Dienstes pro Kalenderjahr. Ausfälle verschuldet durch höhere Gewalt oder durch den Kunden selbst sind davon ausgenommen.
Die für die Rückerstattung relevante Ausfallzeit berechnet sich ab dem Eingang der Störungsmeldung bei der Störungsannahmestelle.

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 DDoS-Schutz-Cluster. Ausgeschlossen von diesem SLA ist die Connectivity zum DDoS-Schutz-Cluster.

4.3. Schadensbegrenzungszeit

Bestimmte Arten von DDoS-Angriffen haben eine sogenannte Schadensbegrenzungszeit (Time to Mitigate, TTM). Die TTM beschreibt den Zeitraum zwischen dem detektieren des Starts 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 die DDoS-Protection (Kap. 2.2) Schutz für das entsprechende Netzwerk gebucht wurde. Für eine Standby-Implementierung gelten die TTM-Werte in der folgenden Tabelle erst ab dem Zeitpunkt, bis das entsprechende IP-Adresssegment via Technologiepartner geroutet wird. Dieses Re-Routing erfolgt nach Überschreiten der Grenzwerte automatisch. Die Zeitspanne bis der Verkehr via DDoS Technologiepartner geroutet wird, ist abhängig von den Konvergenzzeiten des Internets, dies wird typischerweise 1-60 Sekunden dauern.

Angriffstyp	TTM DPI (Always-on)	TTM DPI (Standby)
Fragmentierung	sofort	sofort + typ. 1-60 Sekunden
TCP-Anomalien	sofort	sofort + typ. 1-60 Sekunden
UDP-Anomalien	sofort	sofort + typ. 1-60 Sekunden
IP-Anomalien	sofort	sofort + typ. 1-60 Sekunden
TCP/UDP-Reflection/ Amplification-Angriffe	<10 Sekunden	<10 Sekunden + typ. 1-60 Sekunden
TCP-SYN-Floods	<10 Sekunden	<10 Sekunden + typ. 1-60 Sekunden
ICMP-Floods	<10 Sekunden	<10 Sekunden + typ. 1-60 Sekunden
Botnet-basierte UDP-Floods	<10 Sekunden	<10 Sekunden + typ. 1-60 Sekunden
Botnet-basierte TCP-Floods	<10 Sekunden	<10 Sekunden + typ. 1-60 Sekunden
Abwehr basierend auf künstlicher Intelligenz/maschinellem Lernen	<9 Sekunden	Nach re-routing von typ. 1-60 Sekun-den benötigt das Scrubbing Center ca. 15k gültige Transaktionen

5. Reports

5.1. DDoS-Report

Der Kunde erhält auf Anfrage einen DDoS-Report mit weiteren Angaben zu einem erfolgten DDoS-Angriff. Kunden mit einem öffentlichen /24 IP-Range oder grösser erhalten, auf Anfrage, einen Portalzugang.