Cyberlink AG
Bellerivestrasse 241
CH-8008 Zürich

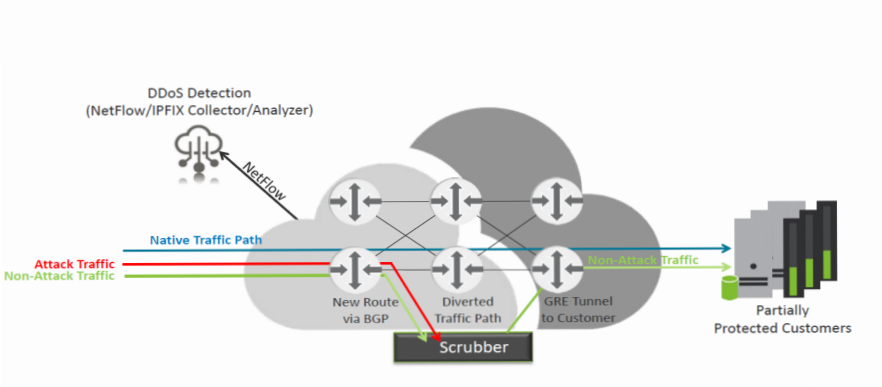
+41 44 287 29 92
info@cyberlink.ch
www.cyberlink.ch

cyberlink

Factsheet

DDoS Protection Service

Immer noch verbinden die meisten mit der Bezeichnung „DDoS“ automatische Angriffe mit nur einem Angriffsvektor, nämlich dem volumetrischen. Solche Angriffe, die eine enorme Bandbreite verbrauchen, sind leicht zu identifizieren und abzuwehren. Der DDoS-Schutz von Cyberlink schützt zusätzlich und zuverlässig, auch vor ausgefeilten mehrstufigen Attacken.



Schematische Darstellung des DDoS-Schutzes

Multi-Vektor-Angriffe und adaptive DDoS-Angriffstechniken etablieren sich

Analysen haben neben der steigenden Zahl von Brute-Force-Angriffen mit mehr als einem Angriffsvektor noch etwas anderes zu Tage gefördert. Hacker gehen demnach verstärkt dazu über, adaptive Techniken einzusetzen, die es ihnen erlauben, sich ein genaueres Bild von der jeweiligen Sicherheitsinfrastruktur zu machen. Mithilfe dieses Profils konzipieren sie dann eine massgeschneiderte zweite und dritte Attacke, bei denen sie die Sicherheitsebenen genau dieses Unternehmens gezielt umgehen. Auch wenn volumetrische Angriffe weiterhin die häufigste Form einer DDoS-Attacke sind, etablieren sich daneben gemischte und adaptive Angriffsformen.

DSub-Saturating-DDoS-Angriffe- das smartere DDoS

Neu sind intelligente DDoS-Angriffe, die quasi „chirurgisch“ arbeiten: 84 % der beobachteten Angriffe dauern weniger als 10 Minuten, 71,6 % davon sogar nur zwischen 0 und 5 Minuten, 93 % beanspruchen dabei weniger als 1 Gbit/s (Quelle: Corero Networks Inc). Dabei benutzen die Angreifer gerade genug Bandbreite, um ihr Ziel zu erreichen. Traditionelle Lösungen zur Abwehr von DDoS-Angriffen übersehen solche Attacken. Selbst wenn sie auf dem Radar als Angriffe erkannt werden, sind sie oft schon vorbei, bevor man etwas gegen sie tun kann. Dabei folgen die Angriffe oftmals einem ganz typischen Verlauf über die Zeit. Und sie bleiben nicht folgenlos.

Man braucht also beides. Die unmittelbare Einschätzung, ob tatsächlich eine Sicherheitsbedrohung vorliegt, genauso wie eine langfristige Analyse der Trends, um frühzeitig auf Entwicklungen reagieren zu können.

Die Lösung

Heutzutage können DDoS-Angriffe deutlich mehr als „nur“ Dienste zu unterbrechen oder dafür zu sorgen, dass Webseiten nicht mehr erreichbar sind. Seit längerem beobachten wir eine stark steigende Zahl von kurzzeitigen DDoS-Angriffen, die nur wenig Bandbreite für sich beanspruchen.

Davor schützen wir alle unsere Kunden mit unserem Basic-DDoS-Schutz. Für Attacken mit hohem Volumen oder Unterstützung bei der Analyse von Attacken bieten wir unseren Kunden mit dem Standard und Premium Service umfangreiche weitere Dienste an.

Key Facts

- **Gratis DDoS-Schutz für alle Internetanschlüsse bis zu einem Attackenvolumen in der Höhe Ihrer Bandbreite**
- **Zusätzlicher DDoS-Schutz bis zu einem Attackenvolumen von mehreren TB**
- **Echtzeit- und vollautomatisierter Schutz**
- **forensische Analyse bereits erfolgter Angriffe**
- **Persönlicher Service rund um die Uhr, auch 7x24 Stunden**

Unsere DDoS-Protection-Lösungen im Überblick

	Basic	Standard	Premium
Maximale Attacken-Bandbreiten	Anschluss-bandbreite	max. Cyber-link Internet-kapazität	bis 1 TB
Verfügbarkeit	Alle Internet-anschlüsse	Alle Internet-anschlüsse	Dat[illegible]nter Internet
Funktionsumfang			
Schutz vor DDoS-Attacken	✓	✓	✓
Installationsverpflichtung		✓	✓
Personalisiertes Kundenportal mit Echtzeit-Auswertung		✓	✓
Forensische Analysen durch Cyberlink Fachpersonal		optional	optional
Aktion, wenn maximale Attacken-Bandbreite überschritten	Zugriff auf IP-Adresse wird gesperrt		Umleiten zu Cloud Service
Vertrag			
Mindestvertragsdauer	keine	keine	keine

Ab 2018

Mit dem vollautomatischen DDoSP Service schützt Cyberlink sowohl die eigenen Systeme als auch Kundenanschlüsse vor Überlast-Angriffen. Auf diese Weise kann Cyberlink sicherstellen, dass kein unerwünschter Datenverkehr in den Cyberlink Backbone oder zum Endkunden gelangt. Die Schutzsysteme sind in unseren Rechenzentren (EQ und IX) georedundant installiert und werden von Cyberlink ständig überwacht. Eingehender Internetverkehr wird überprüft und unerwünschte Datenpakete automatisch entfernt.

Basic DDoS Protection Service

Dieser Schutz ist für alle Cyberlink Anschlüsse implementiert und steht allen Kunden gratis zur Verfügung. Solange das Volumen einer DDoS-Attacke die Bandbreite eines Kundenanschlusses nicht übersteigt, wird der unerwünschte Datenverkehr automatisch gesäubert. Überschreitet das Volumen einer Attacke die Bandbreite eines Anschlusses, wird der Datenverkehr für 15 Minuten geblockt (Remote Triggered Blackholing, RTBH).

Standard DDoS Protection Service

Optional können Kunden von Cyberlink einen erweiterten DDoS-Schutz nutzen. In diesem Fall werden alle Attacken so lange gesäubert, solange die Gesamtkapazität des Cyberlink Perimeters zum Internet nicht überschritten wird. Überschreitet das DDoS-Attacken-Volumen die gesamte Internetkapazität von Cyberlink, erfolgt eine Blockierung der angegriffenen IP-Adresse (RTBH). Kunden die diesen Service beziehen, erhalten Zugriff auf ein Online-Portal in dem sowohl Echtzeit- als auch historische Informationen vorliegen und Attacken genau analysiert werden können.

Premium DDoS Protection Service

Zusätzlich zum Standard DDoS-Schutz wird beim Überschreiten der Gesamtkapazität von Cyberlink der Datenverkehr in ein externes Scrubbing Center eines spezialisierten DDoSP-Anbieters umgeleitet und gesäubert. Auf diese Weise können auch Terabit-Attacken abgewehrt werden. Es gilt zu beachten, dass solche Services die Daten u.U. im Ausland analysieren und säubern und es typischerweise zu Verzögerungen (Latenzzeit-Erhöhung) kommt.

Weitere Cyberlink-Angebote

Security

Schützen Sie Ihr Netzwerk vor Angriffen und ungewollten Zugriffen aus dem Internet. Unsere Sicherheitsexperten designen zusammen mit Ihnen den passenden Service für Ihr Unternehmen.

- Managed Firewall Onsite und Datacenter
- Zscaler Web Content Security

Datacenter

Hochmodernes Tier-3 Datacenter mit optimaler Klimatisierung, Notstromzufuhr und einem Sicherheitszutritts- und Brandschutz-System.

- Co-Location von 1/4 bis zu ganzen Rack
- Virtuelles Datacenter (VDC)

Über Cyberlink

Cyberlink beschäftigt rund 30 Mitarbeiter, welche tagtäglich ihr fundiertes Expertenwissen mit Leidenschaft für Technologie kombinieren und über 1´500 Geschäftskunden mit über 6´000 Anschlüssen in der ganzen Schweiz betreuen.

Einige unserer Kunden

BSI Business Systems Integration AG, Halter AG, Max Havelaar Stiftung (Schweiz), Brust-Zentrum AG, invest.ch, mhs internet AG, swiss IT-Factory AG, Post CH AG.