NETRICS
HOSTED SOLUTIONS

BOLL
IT Security Distribution

NETRICS HOSTING SETZT AUF DDOS-DEFENSE-SYSTEM VON CORERO

ÜBERWACHUNG UND ABWEHR VON «MULTI LAYER DDOS»-ATTACKEN

DoS- und DDoS-Angriffe gehören laut zahlreichen Studien zu den grössten Gefahren für IT-Infrastrukturen und -Applikationen. Um entsprechende Angriffe zu erkennen und wirksam abzuwehren, setzt der Bieler Managed-Service-Anbieter netrics hosting ag auf ein hoch performantes DDoS-Defense-System (DDS) von Corero.

corero
NETWORK SECURITY

«Wo der Standard aufhört, beginnt unsere Leidenschaft.» Diesem Credo verpflichtet bietet der in Biel domizilierte Hosting- und Managed-Service-Provider netrics hosting seinen Kunden massgeschneiderte, den individuellen Bedürfnissen angepasste Lösungen für Dienstleistungen aus dem Datacenter. Das im Jahre 2002 gegründete Unternehmen betreibt in seinen Rechenzentren rund 600 Server (dedizierte Server-Plattformen für Endkunden sowie diverse virtuelle Plattformen). Zu den angebotenen Services gehören gehostete SaaS-Dienste (Software as a Service) wie Mail-Archivierung und -Verschlüsselung, Backup-Services mit Datenverschlüsselung, ERP- und CRM-Systeme sowie «Platform as a Service»-Dienste (PaaS). Dabei handelt es sich um physische und virtuelle Outsourcing-Services in Form einer «Private Cloud», in welchen sich die unterschiedlichsten Anforderungen an die IT-Infrastruktur ideal abbilden lassen. Darüber hinaus bietet netrics ihren Kunden mit Swiss-VDC (Swiss Virtual Datacenter) «klassische» IaaS-Dienste (Infrastructure as a Service) an.

LEBENSNERV SECURITY

netrics hosting hat sich im Laufe der Zeit zu einem bevorzugten Managed-Service-Partner für mehr als 1200 Kunden entwickelt. Diese betreiben in den netrics Rechenzentern in Biel businesskritische Anwendungen und Applikationen. Sie sind folglich auf eine stets verfügbare, hochgradig gesicherte IT-Infrastruktur angewiesen. Entsprechend vielschichtig präsentieren sich die von netrics getroffenen Basis-Sicherheitsvorkehrungen. Umfassend sind aber auch die angebotenen Security-Services, die Kunden on demand zur Verfügung stehen. Einen wichtigen Dreh- und Angelpunkt bildet dabei ein leistungsfähiges DDoS-Defense-System von Corero, mit dem sich «Distributed Denial of Service»-Attacken erkennen und wirksam abwehren lassen. Dazu Markus Blösch, CTO und Mitglied der Geschäftsleitung von netrics hosting: Seit rund zwei Jahren stellen wir eine markante Zunahme an DDoS-Attacken fest. Diese weisen oft eine derart hohe Bandbreite auf, dass auch leistungsfähige Firewalls und IPS-Systeme nicht in der Lage sind, die Angriffe abzuwehren. Vor diesem Hintergrund haben wir entschieden, in ein dediziertes DDoS-Defense-System zu investieren, um Kunden und Infrastrukturen gleichermassen zu schützen.»

ANGRIFFE WERDEN GEZIELTER UND AUSGEKLÜGELTER

Die von netrics festgestellte Zunahme an DoS/DDoS-Attacken deckt sich mit den Ergebnissen weltweit durchgeführter Studien, in denen auch Service- und Breitbandprovider befragt wurden. Gemäss diesen Reports zeichnen sich zwei primäre Trends ab. Zum einen erfolgen breit angelegte Angriffe in zunehmender Frequenz mit immer höherer Bandbreite. So sind Angriffe im Bereich von mehreren GBit/s alltäglich und Attacken, die die Bandbreite der angegriffenen Rechenzentren überschreiten, keine Seltenheit. Diese Entwicklung kommt für Blösch nicht unerwartet. «Die den einzelnen Usern zur Verfügung stehende Bandbreite hat sich in kurzer Zeit multipliziert. Zudem sind mobile Devices in immer grösserer Anzahl und mit steigenden Datenraten mit dem Internet verbunden. Dadurch stehen Angreifern – beispielsweise für Botnetz-Attacken – schier unbegrenzte Kapazitäten zur Verfügung. Dies präsentierte sich vor noch nicht allzu langer Zeit komplett anders. So wurden einzelne Kundenprojekte primär von wenigen Zombie-PCs attackiert. Entsprechende Angriffe konnten durch das Sperren einzelner IP-Adressen oder eines IP-Ranges gestoppt werden. Heute erfolgen Angriffe weltweit von Tausenden IP-Adressen aus. Dadurch ist selbst das Sperren geografischer Regionen keine wirksame Option mehr, um Angriffe zu blockieren.»

> «Jenseits üblicher Standards beginnt der Erfolg. Diesem Leitspruch verpflichtet adressieren wir mit unseren Dienstleistungen die individuellen Bedürfnisse unserer Kunden.»
>
> **MARKUS BLÖSCH**
> CTO, netrics hosting ag

Als zweiten Trend nennen Studien eine zunehmende Komplexität von DDoS-Angriffen. Mehrschichtige bzw. Multivektor-Angriffe und Attacken auf Applikationsebene sind alltäglich geworden. Diese «langsamen» und «leistungsschwachen» Angriffe sind wesentlich smarter als breit angelegte Attacken. Die Angreifer benötigen vergleichsweise bescheidene Ressourcen, operieren im Verborgenen, lassen sich für die Infizierung der angegriffenen Systeme teils Wochen oder Monate Zeit und sind nur schwer als Gefahr zu erkennen. Zudem werden die den Hackern zur Verfügung stehenden Werkzeuge immer ausgeklügelter und einfacher handhabbar. Dazu Markus Blösch: «Server und Applikationen sind vermehrt mit perfiden DDoS-Attacken konfrontiert, die anfänglich nicht als solche erkannt werden. Dazu gehören beispielsweise Angriffe auf Anwendungsebene (Application Layer DDoS). Dabei werden reguläre TCP-Verbindungen aufgebaut, um an das attackierte System kontinuierlich

CORERO – DDOS-ATTACKEN VERHINDERN

Die leistungsstarken DDoS-Defense-Systeme (DDS) des Netzwerk-Security-Spezialisten Corero leisten sowohl auf Kundenseite (on premise) als auch bei ISPs und Cloud-Anbietern wertvolle Dienste. Sie ermöglichen die nahtlose Überwachung und Abwehr von DDoS-Angriffen – von volumenbasierten Layer-3-Angriffen bis hin zu intelligenten Layer-7-Attacken, die keinen merkbar gesteigerten Netzwerkverkehr verursachen.

- Effektiver Schutz vor heimtückischen «Low Bandwith»-DDoS-Attacken auf Protokollebene sowie vor traditionellen Network Layer «High Volume Floods»
- Verhaltensbasierte Reputations-DDoS-Engine mit Scoring-System
- Sicherstellung maximaler Verfügbarkeit und Performance der geschützten Dienste und Infrastrukturen
- Geolocation Filtering
- Tiefste Latenz und höchster Durchsatz – auch unter Attacken
- Sehr hohe Ausfallsicherheit durch redundante 1-Höheneinheit-(HE-)Hardware ohne Chip Fans mit Solid State Design
- Lösung mit patentierten DDoS-Schutz-Algorithmen

Requests zu übermitteln, bis der Service nicht mehr aufrechterhalten werden kann. Ein einfaches Beispiel dazu ist das Downloaden grosser PDF-Dateien. Werden in kürzester Zeit Tausende Requests übertragen, kann dies zum Totalausfall des entsprechenden Dienstes führen.»
Blösch macht ferner auf das vermehrte Auftreten von DNS-Attacken (DNS Amplification Attack) aufmerksam, bei denen unter Missbrauch des Domain-Name-Systems grosse Datenströme auf den Internetanschluss des attackierten Servers gelenkt werden. Diese sind in der Lage, bei eingeschränkten Ressourcen einen grossen Datenverkehr zu generieren. Auch DNS-basierte Angriffe lassen sich aufgrund ihrer Mehrebenen-Architektur kaum nachverfolgen und ohne dedizierte DDoS-Defense-Systeme nicht abwehren.

ANGRIFFE ERKENNEN UND ABWEHREN

DoS/DDoS-Attacken haben eine enorme Zerstörungskraft. Sie können komplette Systemausfälle verursachen und Unternehmen und Organisationen immensen Schaden zufügen. Aber auch Teilausfälle oder markante Beeinträchtigungen des Betriebs reichen oft aus, um Umsatzeinbrüche, Imageverlust und sinkende Kundenzufriedenheit zu bewirken. Um dies zu verhindern, hat sich netrics hosting für die Evaluation und Installation eines leistungsfähigen DDoS-Defense-Systems (DDS) des Netzwerk-Security-Spezialisten Corero entschieden. «Damit wollen wir sicherstellen, dass guter Traffic ohne Performanceeinbussen übertragen wird, schlechter Code jedoch als solcher erkannt und gebannt wird.»

> «Mit dem DDoS-Defense-System von Corero bieten wir unseren Kunden einen wichtigen Service zur Maximierung von Verfügbarkeit und Sicherheit ihrer Applikationen und Infrastrukturen.»
>
> **MARKUS BLÖSCH**
> **CTO**, netrics hosting ag

Die dedizierten Appliances von Corero ermöglichen die nahtlose Überwachung und Vermeidung von DoS- und DDoS-Angriffen auf allen Ebenen – von der Anwendungs- über DNS- und HTTP- bis hin zur Protokollebene. Sie blockieren gefährliche IP-Adressen und ungewollten Datenverkehr aus geografischen Regionen, limitieren die Anzahl Requests und Verbindungen, stoppen Protokollmissbrauch und -verletzungen, verhindern «Advanced Evasion»-Techniken (AET), blockieren unberechtigte Zugriffe (Intrusion Prevention), verhindern Buffer Overflows und Exploits und blockieren das Einschleusen von ausführbarem Code (Code Injection). Mit diesen und weiteren Massnahmen leisten die DDoS-Defense-Systeme von Corero einen wichtigen Beitrag zu maximaler Verfügbarkeit und hoher Performance der geschützten Dienste und Infrastrukturen.

CORERO – WAHL MIT WEITSICHT

Dass sich netrics hosting für ein DDoS-Defense-System von Corero entschied, hat laut Markus Blösch viele Gründe. «Im Rahmen einer Teststellung wurde schnell klar, dass sämtliche von uns definierten Anforderungen erfüllt – oft gar übertroffen wurden. Bereits die Installation erwies sich als ausgesprochen positive Erfahrung. So war die am Gateway transparent eingebundene Appliance aufgrund vordefinierter Rule-Sets sofort einsetzbar. Auch die Bedienung zeigte sich als vorbildlich intuitiv und die vom System erstellten granularen Logs verschaffen ein transparentes Bild über Gefahren, erfolgte Angriffe und Abwehrmassnahmen.»
Ergänzend dazu betont Blösch das unerreichte Preis-Leistungs-Verhältnis des gewählten DDoS-Defense-Systems von Corero und macht ferner auf die umfangreichen Leistungen des Service-Packages aufmerksam. Dieses beinhaltet nebst automatischen Updates auch das zeitnahe Einspielen neuer Signaturen. Dadurch werden u. a. wechselnde sowie anonymisierte und verborgene IP-Adressen sowie befallene Computer, die Teil eines Botnetzes sind, erkannt und automatisch gesperrt – ohne Zutun des Betreibers. «Mit Corero sind wir in der Lage, unseren Kunden einen einzigartigen, für die Verfügbarkeit und Sicherheit ihrer Applikationen zentralen Service zu bieten. Corero leistet somit einen wichtigen Beitrag, damit wir unser Versprechen für massgeschneiderte Dienstleistungen auch im Bereich der Security einhalten können.»

NX1 – NEUES HIGH DENSITY DATACENTER

Der kontinuierliche Erfolg von netrics hosting hat Konsequenzen: Das bisherige Rechenzentrum in Biel sowie das geografisch dezentralisierte Back-up-Datacenter stossen an ihre Grenzen. Vor diesem Hintergrund hat netrics entschieden, ein neues, hochmodernes «High Performance Computing»-Datacenter aufzubauen. Standort des per 2014/2015 realisierten Neubaus ist das Bözingenfeld. Dieses befindet sich in unmittelbarer Nähe zu den «Stades de Bienne» vor den Toren Biels. Das neue Datacenter zählt zu den innovativsten Rechenzentren Europas und nimmt eine wichtige Rolle im Bereich «Computing as a Service» ein. Mit seinem 100-Gbit-Internet-Access (Backbone) bietet es eine deutliche Antwort auf die wachsenden Bandbreiten-Bedürfnisse.

NETRICS HOSTING AG

Die in Biel/Bienne (BE) domizilierte netrics hosting ag wurde 2002 gegründet. Das Unternehmen, das seit 2010 eine Niederlassung in Zürich betreibt, beschäftigt 16 Mitarbeitende und befindet sich zu 100 Prozent im Besitz des Verwaltungsrates. Das serviceorientierte Unternehmen bietet Dienstleistungen im Bereich Hosting- und IT-Outsourcing an. Zum Angebot gehören Dienste wie SaaS (Software as a Service), IaaS (Infrastructure as a Service) und diverse Cloud-Services. Weit mehr als 1200 Kunden setzen auf das breit gefächerte Angebot von netrics.

NETRICS HOSTED SOLUTIONS

BOLL IT Security Distribution

STARKE PARTNER

KUNDE

netrics hosting ag
2500 Biel
www.netrics.ch

DISTRIBUTION

Boll Engineering AG
5430 Wettingen
www.boll.ch