Inhalt des Live-Webcasts

Wie DDoS-Schutz Ihre Geschäftskontinuität sicherstellt (inkl. Live-Demo)

Datum und Uhrzeit: **25. Oktober 2022, 11:00 Uhr**
Dauer: **ca. 60 Minuten**

Distributed-Denial-of-Service (DDoS) Angriffe werden immer häufiger und vielschichtiger und können Ihrem Unternehmen enormen Schaden zufügen. Mit der wachsenden Online-Verfügbarkeit von Angriffs-Tools sind die Varianten möglicher Angriffe heute größer denn je. In diesem Webcast erfahren Sie, welche Lösungen es gibt, um sich vor DDoS-Angriffen effektiv zu schützen und entsprechend vorbereitet zu sein – inklusive einer Demo!

Die Erreichbarkeit Ihrer Applikationen und Dienste ist essenziell für Unternehmen – sie sind Umsatzbringer, Informationsquelle und wichtige Plattform für die Interaktion mit Kunden und Partnern. Sie müssen immer „online“ sein, um die Geschäftskontinuität nicht einzuschränken. Ausfälle oder Einschränkungen der Erreichbarkeit haben gravierende Folgen, wie beispielsweise Umsatzverlust oder gar Imageschäden. Das Ziel von DDoS-Angriffen ist aber, genau die ständige Verfügbarkeit massiv zu beeinträchtigen. Es ist gerade in diesen Zeiten offensichtlich, dass kaum ein Unternehmen oder Organisation von dieser Bedrohung ausgenommen ist.

Viele Firmen setzen wie selbstverständlich Schutzmechanismen wie Firewalls ein, auch Web Application Firewalls (WAF) sind allgegenwärtig. Dem Thema Schutz gegenüber DDoS-Angriffen wird aber nicht selten eine niedrigere Priorität eingeräumt oder es wird erst angegangen, wenn bereits eine Attacke erfolgt ist. Um Netzwerke und Applikationen wirksam und zuverlässig zu schützen, muss DDoS-Schutz ein essenzieller Bestandteil Ihrer Sicherheitsstrategie sein. Als Beispiel seien die sogenannten Flood-Attacken genannt: Diese attackieren gezielt verschiedenste Systeme in Ihrem Netzwerk, um die Erreichbarkeit eben jener einzuschränken. Dadurch wird die „User Experience“ negativ beeinflusst, was natürlich auch das Ziel des Angriffs gewesen sein kann. Des Weiteren kann auch die sogenannte “Carpet Bombing” Attacke ihre Infrastruktur überlasten und zu Ausfällen führen.

In diesem Webcast erläutern Alexander Flossdorf und Markus Link von Radware, wie DDoS-Angriffe Ihre Netzwerke und Applikationen beinträchtigen können und welche Möglichkeiten es gibt die Verfügbarkeit Ihrer IT-Infrastruktur sicherzustellen. Sie erläutern, wie mithilfe spezialisierter Angriffscharakterisierung selbst sogenannte Zero-Day-Angriffe erfolgreich abgewehrt werden können.
In einer Demo wird als Beispiel dargestellt, wie mit Hilfe eines cloudbasierten DDoS-Schutzes der Kunde gegenüber DDoS-Angriffen geschützt ist und gleichzeitig die volle Übersicht über die aktuelle Situation behält.

Moderiert wird der Webcast von Sebastian Gerstl von Heise Business Services.

Sprecher:

Alexander Floßdorf, Systems Engineer, Radware GmbH

Alexander Floßdorf ist Systems Engineer für DACH bei Radware, einem der führenden Anbieter von Lösungen im Bereich Cyber Security. Alexander Floßdorf begann seine Laufbahn in der IT-Sicherheit vor mehr als 25 Jahren als Trainer und Systems Engineer, zunächst bei einem Distributor. Vor seinem Wechsel zu Radware war er neun Jahre lang Trainer bei Enterasys (heute Teil von Extreme Networks). Seit 2015 ist Alexander Floßdorf nun bei Radware tätig. Dort umfasst sein Aufgabengebiet unter anderem die Beratung und Lösungserstellung im Bereich der Applikations- und Netzwerksicherheit. Dazu gehören die Themen DDoS, WAF und Bot-Management.

Markus Link, Sales Engineer DACH, Radware GmbH

Markus Link ist Systems Engineer für DACH bei Radware, einem der führenden Anbieter von Lösungen im Bereich Cybersecurity. Vor mehr als 20 Jahren startete er seine Karriere in der Informationstechnik zu Beginn als Techniker bei einem mittelständischen Systemintegrator mit Fokus auf Webfilter-Lösungen. Nach weiteren Stationen als Systems Engineer bei Net Optics und IXIA ist er seit 2019 für Radware tätig. Sein Aufgabengebiet umfasst unter anderem die Beratung und Lösungserstellung im Bereich der Applikations- und Netzwerksicherheit. Dazu gehören die Themen DDoS, WAF und Bot-Management.

Sebastian Gerstl, Heise Business Services

Sebastian Gerstl war mehrere Jahre lang IT-Redakteur beim Computermagazin Chip, wo er sich schwerpunktmäßig mit Themen rund um Betriebssysteme wie Windows, Linux oder Android, aber auch Netzwerke, Single-Board-Computer sowie Smartphones und Tablets befasste. Ab 2015 arbeitete er als Fachredakteur für Embedded Systeme und Software Engineering beim Elektronik-Fachmagazin ELEKTRONIKPRAXIS, wo er neben seiner redaktionellen Tätigkeit auch Webinare und Kongresse koordinierte, gestaltete und moderierte. Seit Juli 2022 ist Sebastien Gerstl Projektmanager bei den Heise Business Services.