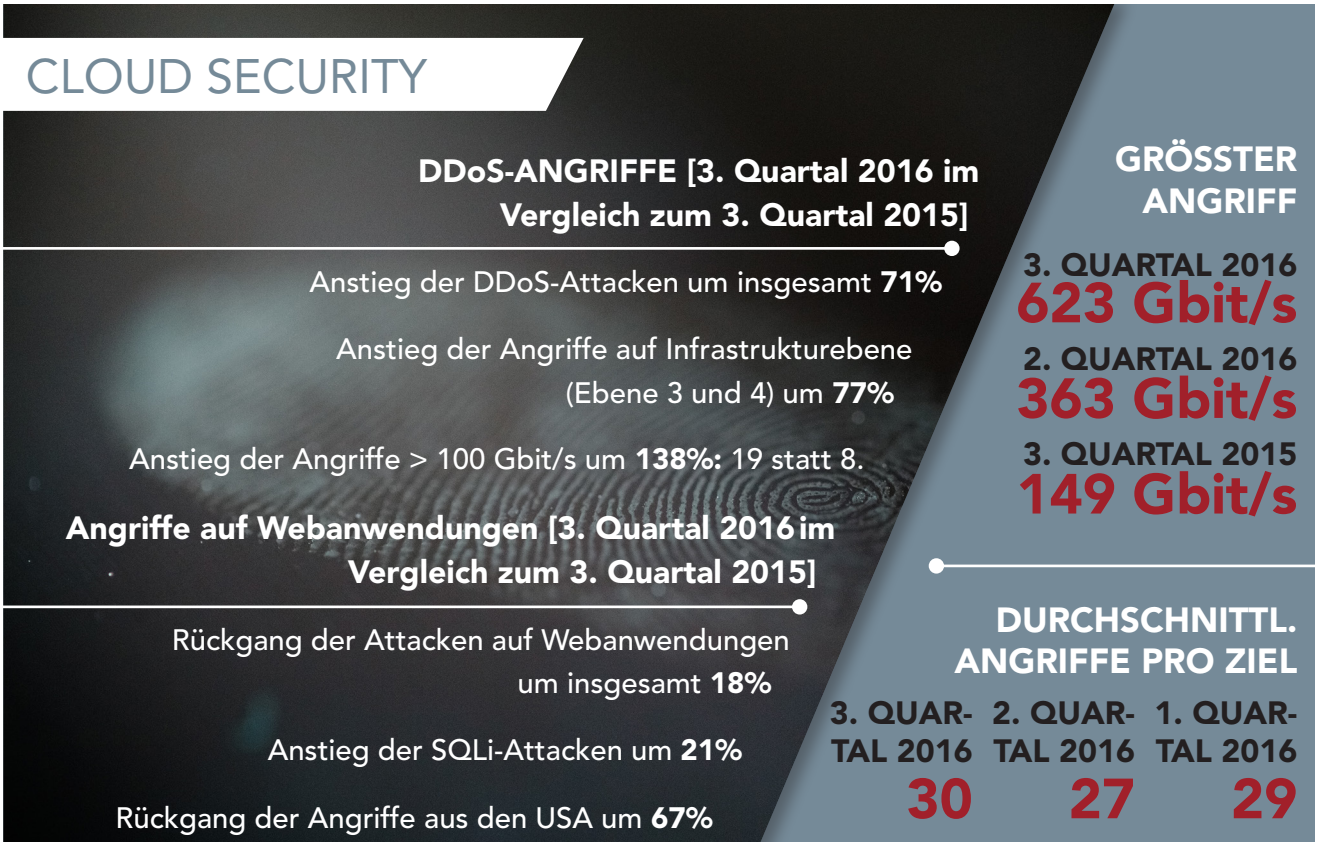
[State of the Internet] / Sicherheit von Akamai

Zusammenfassender Bericht für das 3. Quartal 2016

Informationen zum Bericht / Akamai, der führende Anbieter von Content Delivery Networks (***CDN***), verarbeitet auf seiner global verteilten Intelligent Platform™ täglich mehrere Billionen Webtransaktionen. Somit erfasst Akamai riesige Datenmengen in Bezug auf Kennzahlen zur Breitbandkonnektivität, Cloud Security und Medienbereitstellung. Mit unserem Programm *State of the Internet* möchten wir diese Daten gezielt einsetzen und es Unternehmen und Regierungen dadurch erleichtern, intelligente und strategische Entscheidungen zu treffen. In jedem Quartal veröffentlicht Akamai auf Basis dieser Daten Berichte im *State of the Internet*-Programm, in denen es vorrangig um Breitbandkonnektivität und Cloud Security geht.



Cloud-Sicherheit / Im *State of the Internet-Sicherheitsbericht für das 3. Quartal 2016* werden DDoS-Angriffsdaten (Distributed Denial-of-Service) auf dem gerouteten Netzwerk mit Webanwendungs- und DDoS-Angriffsdaten der Akamai Intelligent Platform™ kombiniert.

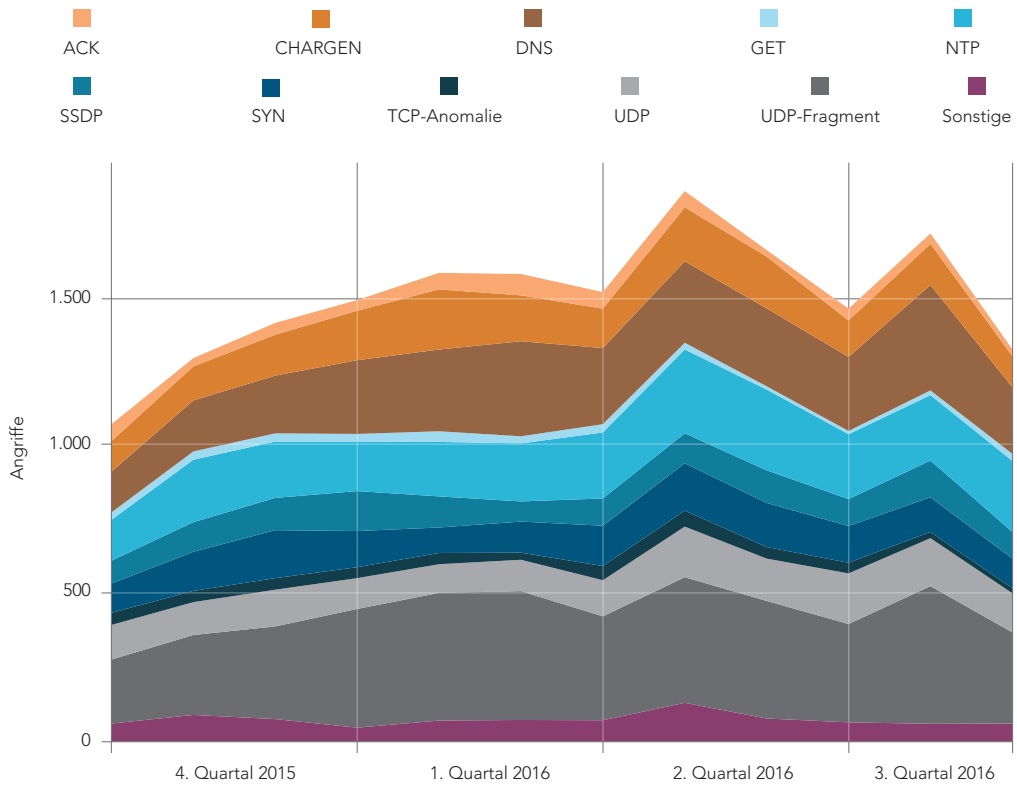
DDoS-Update / Die Größe der größten Angriffe hat sich in diesem Quartal fast verdoppelt. Es traten zwei DDoS-Angriffe mit neuen Spitzenwerten von 623 Gbit/s (Gigabit pro Sekunde) und 555 Gbit/s auf. Dies stellt eine deutliche Steigerung im Vergleich zum bisherigen Spitzenwert von 363 Gbit/s dar. Beide Angriffe zielten auf den Autor und Blogger Brian Krebs (www.krebsonsecurity.com) ab, der sich mit Cybersicherheit befasst. Nach einem kürzlich veröffentlichten Artikel verwandelte sein Blog sich in einen Blitzableiter für das Mirai-Botnet. Der Angriff mit 555 Gbit/s umfasste ACK-Floods und NTP-Reflection, doch die Quelle des Angriffs mit 623 Gbit/s war ungewöhnlich: Sie bestand aus einem Malware-basierten Botnet namens Mirai, das sich auf infizierte internetfähige Geräte stützt.

Mirai-Botnets verbreiten sich wie ein Wurm über Telnet und Standard-Nutzernamen/-Kennwörter, um Geräte zu infizieren. Diese Geräte reagieren dann auf Angriffsbefehle und scannen nach weiteren angreifbaren Geräten. Die Angriffe setzten sich unter anderem aus UDP-, GRE-, ACK-, SYN-, DNS-, Valve Engine- und HTTP-Floods zusammen.

Im 1. Quartal traten die bisher häufigsten Angriffe mit Spitzenwerten von mehr als 100 Gbit/s auf. Das 3. Quartal stand dem mit 19 weiteren Mega-Angriffen in nichts nach. Die Gesamtzahl der Attacken fiel in diesem Quartal zwar um 8%, doch die Anzahl und Größe großer Angriffe nahm zu. Von den 19 Mega-Angriffen richteten sich 13 gegen die Medien- und Entertainmentbranche, 4 gegen Gaming-Unternehmen und 2 gegen Unternehmen aus dem Bereich Software und Technologie.

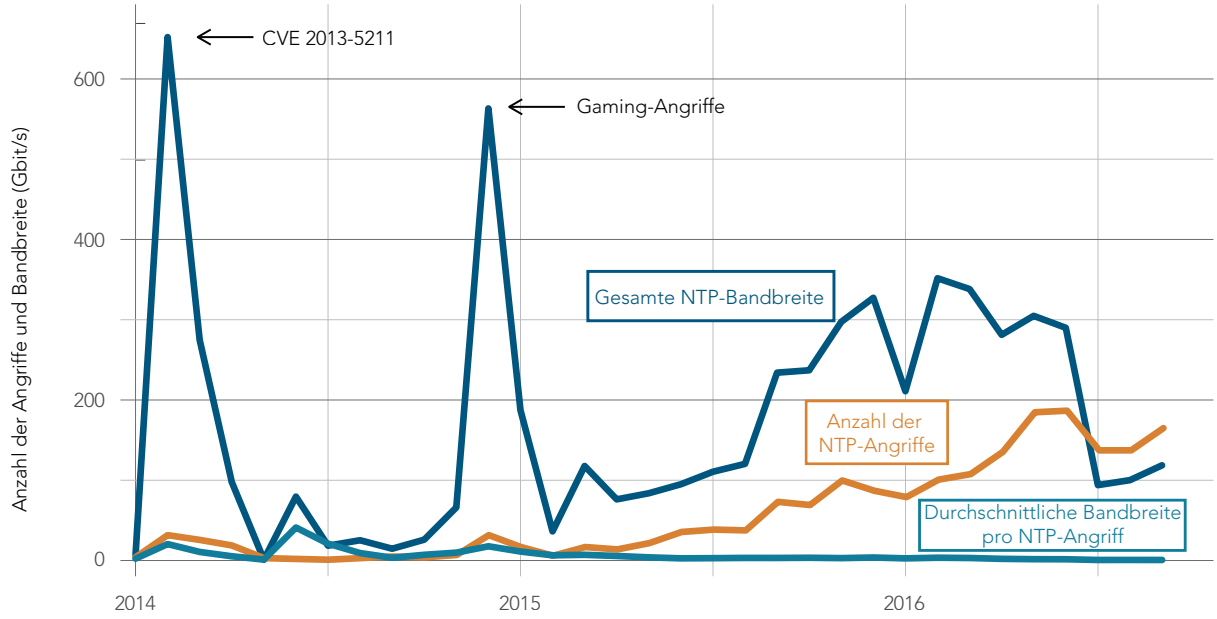
Insgesamt verzeichneten wir 4.556 DDoS-Angriffe auf dem gerouteten Netzwerk. Im Vergleich zum 3. Quartal des Vorjahres entspricht dies einer Zunahme von 71%. Vergleicht man den Wert mit dem des vorherigen Quartals, ist ein Rückgang von 8% erkennbar. Auch wenn es beruhigend ist, dass die Gesamtzahl der Angriffe abgenommen hat, wird sich dieser Trend aller Wahrscheinlichkeit nach nicht fortsetzen. Traditionell ist in der Wintersaison ein Anstieg der DDoS-Angriffe zu erwarten. Zudem steht Angreifern jetzt ein neues Werkzeug zur Verfügung, nämlich Botnets aus infizierten internetfähigen Geräten. Es ist davon auszugehen, dass dieses Werkzeug in Zukunft erneut zum Einsatz kommt.

10 häufigste Angriffsvektoren nach Quartal



Während die Anzahl der Angriffe im August stark anstieg, lag die Gesamtzahl der Angriffe im 3. Quartal im Vergleich zum 2. Quartal 2016 niedriger.

Im letzten Quartal meldeten wir einen Anstieg der NTP-Angriffe um 276% im Vergleich zum 2. Quartal 2015. Unsere Analyse in diesem Quartal hat ergeben, dass die Anzahl der Angriffe zwar hoch war, die von jedem Angriff generierte Menge an Traffic jedoch abgenommen hat. Dies lag daran, dass die Anzahl der nicht durch Patches geschützten NTP-Server, die für eine schädliche Nutzung anfällig sind, weiterhin rückläufig ist. Während der Vorweihnachtszeit 2014 generierte eine durchschnittliche NTP-Flood-Attacke Traffic von über 40 Gbit/s. In diesem Quartal erreichte ein durchschnittlicher NTP-Angriff jedoch kaum mehr als 700 Mbit/s (Millionen Bit pro Sekunde). Dies entspricht einer Abnahme der Bandbreite um 98%.

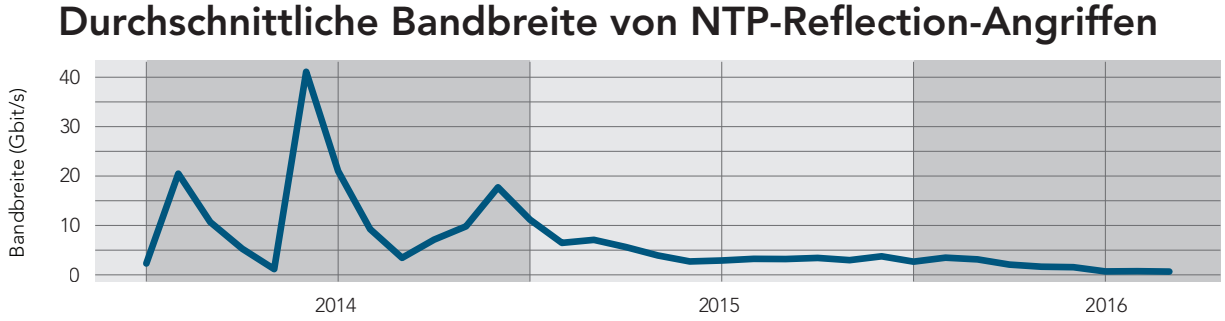


Die NTP-Schwachstelle „monlist" führte zu einem starken Anstieg des NTP-Angriffs-Traffic, gefolgt von einem konzentrierten Angriff auf Spieleunternehmen im Dezember 2014.

Obwohl das Mirai-Botnet im 3. Quartal vermehrt GRE-Floods (Generic Routing Encapsulation) einsetzte, bleibt GRE auch weiterhin ein eher geringfügiger Aspekt der allgemeinen Bedrohungslage. Es ist jedoch wahrscheinlich, dass die Beliebtheit von GRE-Floods aufgrund der Aufmerksamkeit, die die kürzlich erfolgten Angriffe erregten, in Zukunft zunimmt. Im Gegensatz zu Reflection-basierten Angriffen machen sich GRE-Floods die Fähigkeiten der Botnet-Nodes zunutze, ohne dass dabei der Angriffs-Traffic verstärkt würde.

Mit diesem Quartal setzt China sich ein volles Jahr lang an die Spitze der DDoS-Angriffsländer. Im 3. Quartal stammten 30% des DDoS-Angriffs-Traffics aus China. Positiv ist jedoch anzumerken, dass die Menge des Traffics aus China um 56% abgenommen hat, was zum Rückgang der Angriffe insgesamt um 8% beiträgt. Zu den fünf führenden Ursprungsländern von Angriffen zählen zudem die USA, Großbritannien, Frankreich und Brasilien.

Die durchschnittliche Anzahl der DDoS-Angriffe pro Ziel erhöhte sich in diesem Quartal auf 30. Dies deutet darauf hin, dass ein Unternehmen nach einem ersten Angriff mit weiteren Angriffen rechnen muss. Einige Unternehmen stehen sogar fast fortlaufend unter Beschuss. Die beliebtesten Ziele mussten drei bis fünf Angriffe pro Tag abwehren. Für die betroffenen Unternehmen kann dies mehrere kurze Ausfälle täglich bedeuten, die sich in einer schwerwiegenden Rufschädigung niederschlagen.

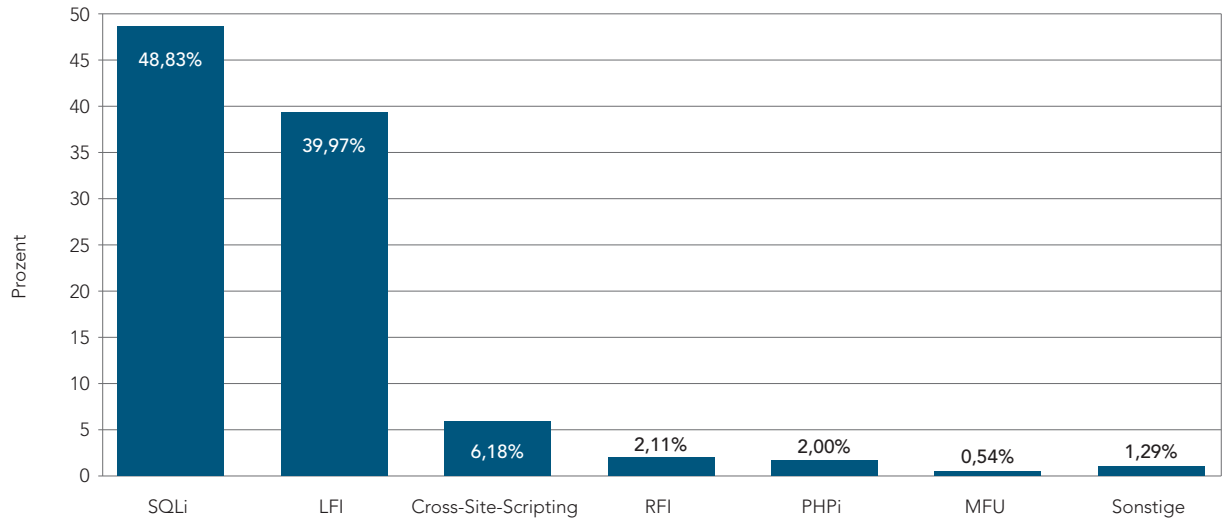


Bis Juni 2016 nahm die Bandbreite von NTP-Reflection-Angriffen so weit ab, dass Botnet-Betreiber sich anderen Protokollen zuwandten.

Statistiken zu Angriffen auf Webanwendungen / Trotz eines Rückgangs der Angriffe auf Webanwendungen aus den USA um 13% konnte das Land den Spitzenplatz unter den Ursprungsländern von Angriffs-Traffic zurückgewinnen. Brasilien, der Spitzenreiter des vergangenen Quartals, rangierte hinter den Niederlanden und Russland auf Platz 4. Den überraschenden 2. Platz erreichten mit 18% der Angriffe die Niederlande. Angreifer verschleiern die Quelle eines Angriffs auf Webanwendungen häufig mithilfe von Proxyservern. Diese Länder stellten die Ursprünge der IP-Adressen des letzten beobachteten Netzwerk-Hops dar.

Während 20% der Angriffe auf Webanwendungen aus den USA stammten, war das Land gleichzeitig auch Ziel von 66% der Angriffe.

Häufigkeit von Angriffen auf Webanwendungen, 3. Quartal 2016



SQLi machte fast 50% der beobachteten Webangriffe aus.

Drei Vektoren machten in diesem Quartal 95% der Angriffe aus: SQL-Injection (SQLi), Local File Inclusion (LFI) und Cross-Site-Scripting (XSS). Remote File Inclusion (RFI), PHP Injection (PHPi) und Malicious File Upload (MFU) beliefen sich jeweils auf 2% oder weniger.

Aus reiner Neugier warfen wir einen Blick auf den Zusammenhang zwischen großen Sportereignissen und der Anzahl der Angriffe auf Webanwendungen. Wir kamen zu dem Schluss, dass Angriffe aus Frankreich und Portugal während des Endspiels der Europameisterschaft im Vergleich zum Folgemonat um 68% bzw. 95% niedriger lagen. Dieser Trend wurde auch bei den Sommerspielen in Rio deutlich. Aus Brasilien stammende Angriffe fielen im Vergleich zum gleichen 17-tägigen Zeitraum im Vormonat während der Sommerspiele von 7,3 Millionen auf nur 1 Million. Auch wenn dieser Trend interessant ist, empfehlen wir Ihnen dennoch, Ihre Firewall bei derartigen Veranstaltungen eingeschaltet zu lassen.

Ressourcen / Werfen Sie einen Blick auf folgende Ressourcen zum Thema Cybersicherheit für das 3. Quartal von Akamai:

1. Bedrohungsratgeber zu Kaiten-/STD-Router-DDoS-Malware
2. Bedrohungsratgeber zu SSHowDowN: Exploit von internetfähigen Geräten zur Durchführung groß angelegter Angriffskampagnen

***State of the Internet / Sicherheit* – Das Team**
Martin McKeay, Senior Security Advocate, Senior Editor
Jose Arteaga, Akamai SIRT
Amanda Fakhreddine, Editor
Dave Lewis, Security Advocate
Larry Cashdollar, Akamai SIRT
Chad Seaman, Akamai SIRT
Jon Thompson, Custom Analytics
Ryan Barnett, Threat Research Unit
Ezra Caltum, Threat Research Unit

Entwurf
Shawn Doughty, Creative Direction
Brendan O'Hara, Art Direction/Design

Kontakt
SOTIsecurity@akamai.com
Twitter: *@akamai_soti* / *@akamai*
www.akamai.de/StateOfTheInternet

Vollständigen Bericht herunterladen

[State of the Internet]-Sicherheitsbericht
3. Quartal 2016

Akamai FASTER FORWARD

Akamai ist der führende Anbieter von Content-Delivery-Network (CDN)-Services, die das Internet schnell, zuverlässig und sicher machen. Die leistungsstarken Lösungen von Akamai auf den Gebieten Web Performance, Mobile Performance, Cloud Security und Media Delivery revolutionieren die Art und Weise, wie Unternehmen das Nutzererlebnis von Webseiten, Web-Applikationen und Unterhaltungsangeboten für Privat- und Geschäftskunden optimieren können. Weitere Informationen zu den Akamai-Lösungen und wie das Team von Internetexperten Unternehmen dabei unterstützt, Innovationen schneller voranzutreiben, gibt es unter ***http://www.akamai.de***, im Blog ***blogs.akamai.com*** oder auf Twitter unter ***@AkamaiDACH*** sowie @Akamai.

Akamai hat seinen Hauptsitz im US-amerikanischen Cambridge, Massachusetts und betreibt mehr als 57 Niederlassungen weltweit. Unser Serviceangebot und eine erstklassige Kundenbetreuung ermöglichen es Unternehmen, ihren Kunden ein bisher unerreichtes Interneterlebnis zu bieten. Die Anschriften, Telefonnummern und Kontaktdaten aller Standorte sind unter ***www.akamai.de/locations*** aufgeführt.