[State of the Internet] / Sicherheit von Akamai

Zusammenfassender Bericht für das 4. Quartal 2016

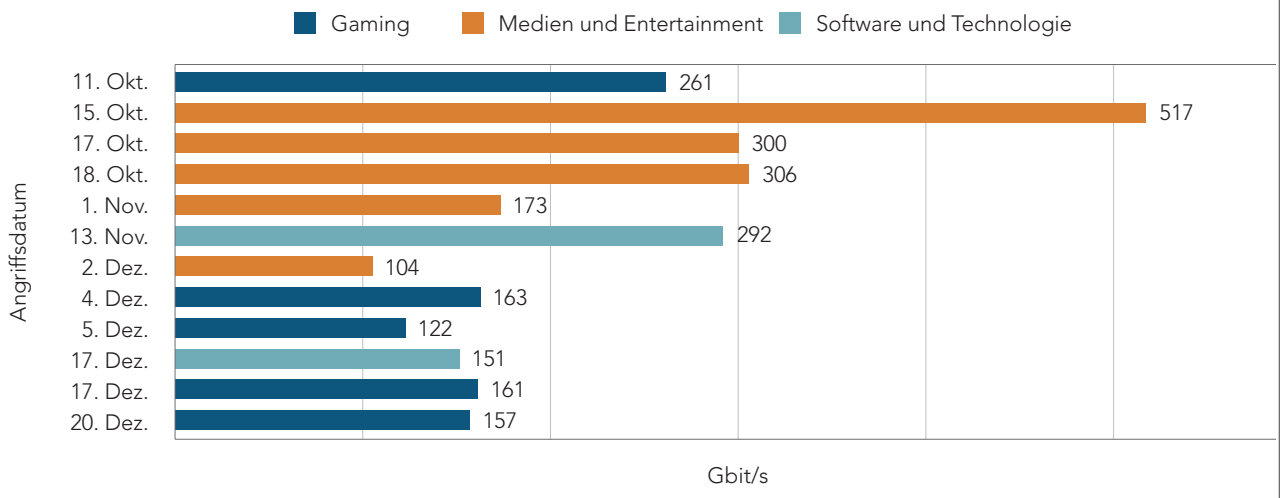
Informationen zum Bericht / Akamai, der führende Anbieter von Content Delivery Networks (***CDN***), verarbeitet auf seiner global verteilten Intelligent Platform™ täglich mehrere Billionen Webtransaktionen. Somit erfasst Akamai riesige Datenmengen in Bezug auf Kennzahlen zur Breitbandkonnektivität, Cloud Security und Medienbereitstellung. Mit dem *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*, in denen es vorrangig um Breitbandkonnektivität und Cloudsicherheit geht.

Berichtsübersicht / Im *State of the Internet-Sicherheitsbericht für das 4. Quartal 2016* werden DDoS-Angriffsdaten (Distributed Denial-of-Service) im gerouteten Netzwerk mit Webanwendungs- und DDoS-Angriffsdaten der Akamai Intelligent Platform™ kombiniert.

DDoS-Update / Unsichere IoT-Geräte (Internet of Things) stellten weiterhin eine große Quelle von DDoS-Angriffstraffic dar. Die schnelle Verbreitung solcher Geräte sorgt somit auch für einen rapiden Anstieg an Angriffsressourcen, der durch die Entdeckung neuer Schwachstellen und anfälliger Systeme weiter verstärkt wird. Die Geräte, die im dritten Quartal an Mirai-Angriffen beteiligt waren, stellten nur einen Bruchteil aller mit dem Internet verbundener IoT-Geräte dar. Hauptsächlich handelt es sich hierbei um IP-fähige Kameras und Router. Je mehr anfällige Geräte zu den IoT-basierten Botnets hinzukommen, desto stärker steigen Funktions- bzw. Angriffsumfang von Botnets und DDoS-Attacken.

Es lässt sich jedoch ein gewisser Gegentrend feststellen: Die Federal Trade Commission (FTC) ist nun in Kalifornien gegen einen Hersteller drahtloser Router vor Gericht gegangen. Der Hersteller gefährde seine Kunden, indem er fehlerhafte und unsichere Software für ihre Systeme entwickle. Und dies ist nicht der erste Fall, in dem die FTC gegen Hersteller unsicherer Software vorgeht. Diese Bemühungen sollten von anderen Unternehmen als Warnung verstanden werden, auf die Sicherheit ihrer Systeme zu achten.

Immer häufiger treten DDoS-Angriffe mit über 300 Gbit/s auf. Sieben der bisher zehn von Akamai festgestellten DDoS-Angriffe mit mehr als 300 Gbit/s fanden 2016 statt, drei davon im vierten Quartal. Im Vergleich zum vierten Quartal 2015 nahm die Anzahl der Angriffe mit mehr als 100 Gbit/s um 140 Prozent zu. Von den zwölf Mega-Angriffen im vierten Quartal 2016 wurden zwei auf Software- und Technologieunternehmen verübt, während fünf der Angriffe auf Gaming-Organisationen abzielten. Auch Medien- und Unterhaltungsanbieter wurden in fünf Fällen Opfer einer solchen Mega-Attacke – drei dieser Angriffe erreichten oder überschritten sogar 300 Gbit/s.

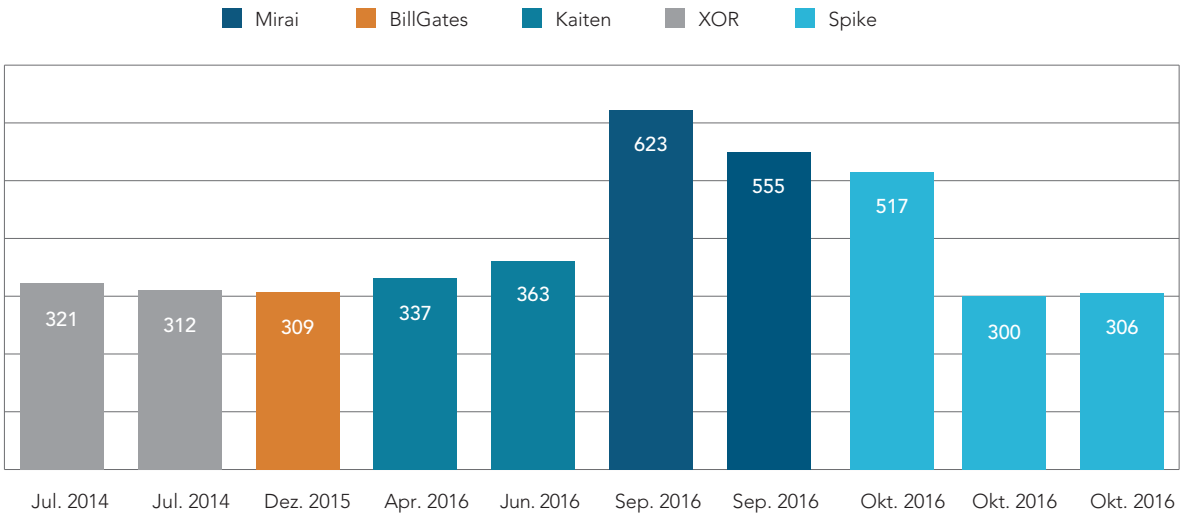


Im vierten Quartal 2016 überschritten zwölf DDoS-Attacken die 100 Gbit/s, fünf von ihnen sogar die Marke von 200 Gbit/s.

Obwohl Nachrichten zu Mirai und IoT-Botnets seit dem dritten Quartal an der Tagesordnung sind, wurde für den mit 517 Gbit/s bisher größten Angriff des Quartals eine andere Quelle eingesetzt: das DDoS-Toolkit „Spike“. Diese Malware wird für gewöhnlich eher mit x86-basierter Linux-Malware in Verbindung gebracht, wie z. B. XOR oder BillGates. Als das Security Intelligence Response Team (SIRT) von Akamai im September 2014 einen Ratgeber zu Spike veröffentlichte, umfasste der bis dato größte Angriff 215 Gbit/s, also weniger als die Hälfte der diesjährigen Spike-Attacke mit 517 Gbit/s.

DDoS-Angriffe mit mehr als 300 Gbit/s sind zwar ein neues Phänomen, jedoch kamen sie wenig überraschend. Sehen wir uns einmal die Entwicklung der Botnets an, aus denen die größten Mega-Angriffe stammten: XOR trat Mitte 2014, BillGates Ende 2015, Kaiten (Mirais Vorgänger) im ersten Halbjahr 2016, Mirai im September und Spike im vierten Quartal in Erscheinung. Die Hälfte der bisher festgestellten Angriffe mit mehr als 300 Gbit/s wurde 2016 zwischen September und Dezember verübt.

DDoS-Angriffe mit mehr als 300 Gbit/s nach Botnet, Juli 2014 bis Dezember 2016



Von Juli 2014 bis Dezember 2016 generierten vier Botnets zehn DDoS-Angriffe mit jeweils mehr als 300 Gbit/s. Von diesen zehn traten sieben im Jahr 2016 auf.

Insgesamt konnten wir in diesem Quartal 25 DDoS-Angriffsvektoren feststellen; am häufigsten wurden dabei UDP-Fragmentierung (27 %), DNS (21 %) und NTP (15 %) eingesetzt. Im Gegensatz zu IoT-Ressourcen, die immer mehr zunehmen, nimmt die Anzahl von NTP-Ressourcen für DDoS-Angriffe ab, da aktive Server gepatcht und ältere Server ausgetauscht werden. Bei CHARGEN, dem viertbeliebtesten Angriffsvektor, handelt es sich um ein von Druckern verwendetes Test- und Messprotokoll. Das wirft die Frage auf, warum der Service so anfällig und nicht besser nach außen hin geschützt ist.

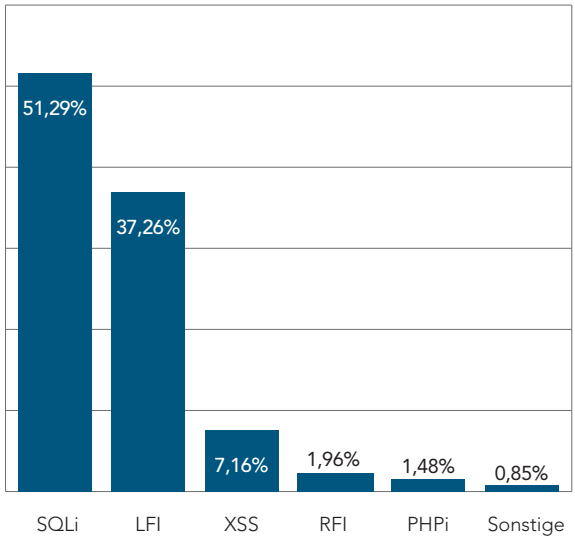
Im letzten Quartal konnten wir einen weiteren Reflection-DDoS-Angriffsvektor feststellen: Connectionless Lightweight Directory Access Protocol (CLDAP). Angreifer nutzen das CLDAP aus, um den DDoS-Traffic zu verstärken. CLDAP wird in Windows-Netzwerken bereitgestellt, um auf Authentifizierungsinformationen für die Netzwerkanmeldung zuzugreifen.

Am häufigsten stammten DDoS-Angriffe aus den USA (24 %), dem Vereinigten Königreich (10 %) und aus Deutschland (7 %). Diese Tatsache ist ungewöhnlich und lässt sich in Teilen durch das Mirai-Botnet erklären. Im vergangenen Jahr führte China die Top-10-Liste der Länder an, die als Angriffsquelle dienten. Im vierten Quartal 2016 belegte China mit 6 % des gesamten Angriffstraffics nur noch den vierten Platz. Kanada war an elfter Stelle – auch hier ein deutlicher Anstieg gegenüber den vorherigen Quartalen.

Die durchschnittliche Anzahl von DDoS-Angriffen lag in diesem Quartal bei ca. 30 pro Ziel. Diese Zahl zeigt, dass Unternehmen nach einem ersten Angriff mit hoher Wahrscheinlichkeit weitere Angriffe erdulden müssen. Einige Unternehmen werden nahezu durchgehend attackiert: Bei den Spitzenreitern der am meisten angegriffenen Unternehmen kam es zu drei bis fünf Attacken *pro Tag*.

Statistiken zu Angriffen auf Webanwendungen / Drei Vektoren machten in diesem Quartal 95 Prozent der Angriffe auf Webanwendungen aus: SQL-Injection (SQLi), Local File Inclusion (LFI) und Cross-Site-Scripting (XSS). Zwar wurden sie insgesamt ähnlich oft verwendet wie im dritten Quartal, jedoch stieg der Anteil von SQLi von 44 (Q2) über 49 (Q3) auf 51 Prozent (Q4) – das ist ein Anstieg von insgesamt 44 Prozent seit dem vierten Quartal 2015. Gleichzeitig wurde LFI weniger oft eingesetzt und fiel so von 45 (Q2) über 40 (Q3) auf 37 Prozent (Q4).

Häufigkeit von Angriffen auf Webanwendungen, 4. Quartal 2016

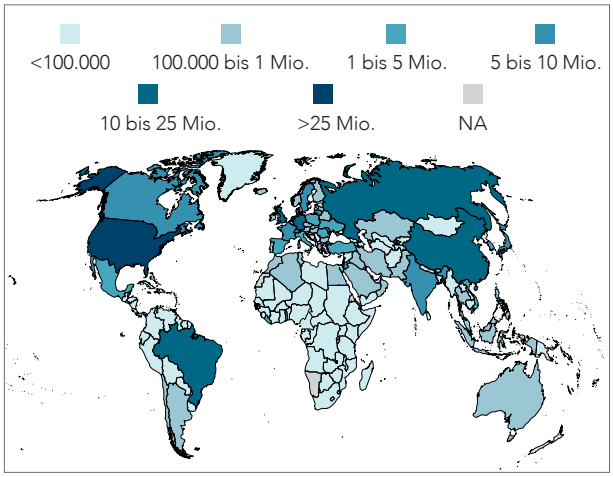


Zusammengenommen wurden SQLi und LFI bei 88 Prozent der festgestellten Angriffe auf Webanwendungen eingesetzt.

Während der Thanksgiving-Feiertage in den USA, also vom 22. bis zum 29. November, erreichte der von Akamai überwachte Traffic Spitzenwerte von 33 Tbit/s. In dieser Zeit wurden vier Branchen des Einzelhandels Opfer schwerwiegender Angriffe auf ihre Webanwendungen – pünktlich zum Feiertagsshopping. Zu den angegriffenen Unternehmen zählten Bekleidungs- und Schuhhändler, regionale Websites eines Kundenportal-Betreibers, Anbieter von Haushaltselektronik sowie Medien- und Unterhaltungsunternehmen.

Nach den Mirai-Angriffen im dritten Quartal führte Akamai eine rückwirkende Analyse durch, bei der die Ports 23 und 2323 untersucht wurden. Mirai nutzt diese Ports, um sich bei ungeschützten digitalen Videorekordern (DVR) und IP-fähigen Videoüberwachungssystemen anzumelden. Die ursprünglichen Versionen von Mirai griffen möglicherweise bereits am 13. Mai 2016 die ersten Systeme an. Ab diesem Zeitpunkt ließen sich deutliche Anstiege des entsprechenden Traffics feststellen. Ende Juli war ein zweiter Anstieg des Traffics festzustellen, der möglicherweise durch die endgültige Veröffentlichung des Mirai-Codes verursacht wurde.

Quellländer von Angriffen auf Webanwendungen weltweit, 4. Quartal 2016



Land	Angriffe aus Quelle	Prozent
USA	97.918.896	28%
Niederlande	61.499.919	17%
Deutschland	32.384.205	9,2%
Brasilien	19.379.729	5,5%
Russland	16.643.150	4,7%
China	14.275.358	4,0%
Großbritannien	11.908.055	3,4%
Litauen	9.793.507	2,8%
Frankreich	8.772.176	2,5%
Indien	8.638.666	2,4%

Angriffe auf Webanwendungen haben ihren Ursprung überall auf der Welt, das führende Quellland sind jedoch die USA.

Die USA und die Niederlande führten das zweite Quartal in Folge die Liste der führenden Quellen von Angriffen auf Webanwendungen an, gefolgt von Deutschland auf Platz 3. Durch die Analyse der Quellendaten nach Region gewinnen wir zusätzliche Erkenntnisse. Auf dem amerikanischen Kontinent waren die drei am häufigsten genutzten Quellen von Angriffen auf Webanwendungen die USA, Brasilien und Kanada. Im europäischen Raum waren die wichtigsten Quellen die Niederlande, Deutschland und Russland. In der Region Asien-Pazifik waren es China, Indien und Japan.

Ressourcen / Werfen Sie einen Blick auf folgende Akamai-Ressourcen zum Thema Cybersicherheit für das 4. Quartal 2016:

1. Bedrohungsratgeber zum Mirai-Botnet / Angriffe und Erkenntnisse vor Veröffentlichung des Mirai-Codes und danach folgende Angriffe
2. Bedrohungsratgeber zu mDNS Reflection / Die Ausnutzung des mDNS-Protokolls (Multicast Domain Name System) für Angriffe auf die Gaming-, Software- und Technologiebranchen
3. State of the Dark Web 2016 / Neue Kryptowährungen, Schwarzmärkte und Produktangebote, Datenschutzservices und -richtlinien und Bemühungen der Strafverfolgungsbehörden

[State of the Internet] / Sicherheit

***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 zum 4. 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.com/locations aufgeführt.