„State of the Internet“-Sicherheitsbericht

Zusammenfassender Bericht für das
3. Quartal 2017

Akamai

Akamai verarbeitet auf seiner global verteilten Intelligent Platform™ – der weltweit größten und bekanntesten Plattform für die Cloudbereitstellung – täglich mehrere Billionen Webtransaktionen. Somit erfassen wir bei Akamai riesige Datenmengen in Bezug auf Kennzahlen zur Breitbandkonnektivität, Cloudsicherheit und Medienbereitstellung. Der *„State of the Internet"-Bericht* wurde entwickelt, um Unternehmen und Regierungen mithilfe der hierbei erfassten Daten die Informationen zu bieten, die sie für strategische Entscheidungen benötigen. In jedem Quartal veröffentlicht Akamai auf Basis dieser Daten einen „State of the Internet"-Bericht, in dem es vorrangig um Breitbandkonnektivität und Cloudsicherheit geht.

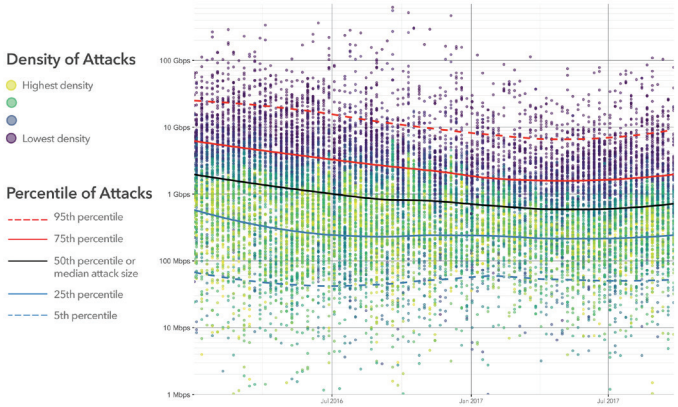
Der *„State of the Internet"-Sicherheitsbericht* für das 3. Quartal 2017 kombiniert Angriffsdaten aus der globalen Infrastruktur von Akamai und spiegelt die Forschung verschiedenster Teams im gesamten Unternehmen wider.

Geschäftliche Auswirkungen / In diesem Quartal wurden die Schlagzeilen von schwerwiegenden finanziellen und anderen geschäftlichen Schäden für Unternehmen unterschiedlicher Branchen beherrscht. Unsere Daten lassen erkennen, dass die Angriffe angesichts der bevorstehenden Feiertage weiter zunehmen werden. Eines ist also klar: Wer die Cybersicherheit ignoriert, setzt sich und sein Unternehmen großer Gefahr aus. Genau das sagt auch unser Gastautor des aktuellen Berichts, CTO Chris Wysopal, der schon seit zwei Jahrzehnten versucht, Menschen vor diesen Gefahren zu warnen.

Um grundlegende Sicherheit zu schaffen, müssen Unternehmen Soft- und Firmware immer auf dem neuesten Stand halten und Sicherheitslücken umgehend patchen. Darüber hinaus sollten bei den Vorbereitungen auf die Feiertage auch Maßnahmen zur DDoS-Abwehr getroffen werden. Die ständige Analyse der Bedrohungen, denen sich Unternehmen gegenübersehen, ist unerlässlich. Denn wir müssen verstehen, wie sich die Strategien der Angreifer entwickeln, um zuverlässigere Verteidigungen aufbauen zu können. Der diesjährige „State of the Internet"-Sicherheitsbericht behandelt das neue Android-basierte Botnet „WireX" und enthält zusätzliche Forschungsergebnisse zu Fast-Flux-Netzwerken, die von Botnets verwendet werden, um schädliche Aktivitäten sowie die CnC-Kommunikation (Command and Control) zu verbergen und so die Erkennung zu erschweren.

Redaktionsübersicht / In jüngster Vergangenheit haben es einige der bisher weitreichendsten Sicherheitsvorfälle in die Schlagzeilen geschafft: von der Offenlegung von drei Milliarden Yahoo-Konten bis hin zum Equifax-Angriff, bei dem vertrauliche Daten von 146 Millionen US-Amerikanern gestohlen wurden. Zur gleichen Zeit begannen die schweren finanziellen Auswirkungen der NotPetya-Malware im zweiten Quartal. Durch die Ransomware erlitten viele Unternehmen Schäden in dreistelliger Millionenhöhe.

Angriffsdichte und -trends
Januar 2017 bis September 2017



Zwar wurden die Schlagzeilen von diesen Vorfällen beherrscht, jedoch reichen schon „normale" DDoS-Attacken und Angriffe auf Webanwendungen aus, um den Geschäftsbetrieb zu stören. Die Häufigkeit solcher Angriffe nimmt ständig zu – bei Unternehmen jeder Größe und über alle Branchen hinweg. Im dritten Quartal verzeichnete Akamai erneut einen Anstieg der DDoS-Angriffe (8 Prozent) und Attacken auf Webanwendungen (30 Prozent). Auch der durchschnittliche Umfang der Angriffe sowie die Häufigkeit der Attacken pro Ziel sind gestiegen.

Obwohl traditionelle Angriffsvektoren und -plattformen weiterhin beliebt sind und effektiv eingesetzt werden können, erweitern immer mehr Cyberkriminelle ihr Arsenal. Auch in diesem Quartal wurde weiter die Mirai-Malware verwendet, die IoT-Geräte (Internet of Things) nutzt. Gleichzeitig wurde WireX eingeführt, das die Kontrolle über Android-Geräte übernimmt. Beide Bedrohungen zeigen das unglaubliche Potenzial, das solche neuen Quellen für Botnet-Armeen Cyberkriminellen bieten.

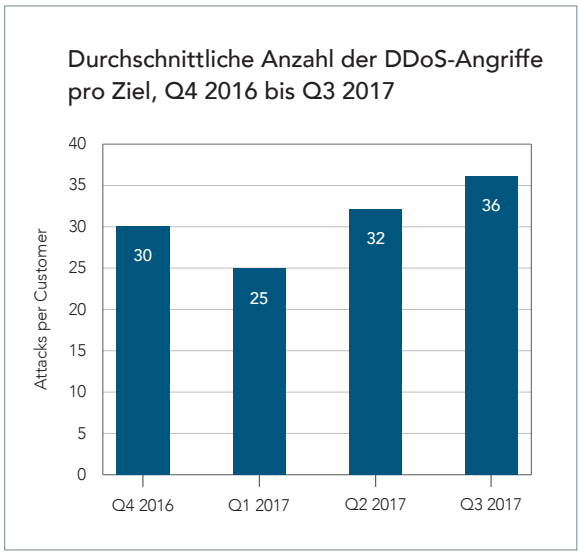
DDoS-Angriffe / DDoS-Angriffe (Distributed Denial of Service) verursachen hohe Kosten und können ganze Sites vom Netz nehmen, den Geschäftsbetrieb lahmlegen oder Ressourcen auslasten. Sie können auch als Ablenkung für einen tiefer gehenden Angriff auf Daten oder Systeme dienen. Im dritten Quartal setzte sich der Aufwärtstrend der DDoS-Attacken aus dem zweiten Quartal fort und verursachte eine Steigerung von acht Prozent. Auch die durchschnittliche Anzahl von DDoS-Angriffen pro angegriffenem Kunden stieg auf das neue Hoch von 36 – also alle drei Tage eine neue Attacke. Bei den Extremfällen liegt diese Zahl jedoch deutlich höher: Ein Gaming-Kunde erlebte allein im dritten Quartal 612 DDoS-Angriffe. Das entspricht fast sieben Angriffen pro Tag dieses Quartals.

DDoS-ANGRIFFE [Q3 2017 gegenüber Q2 2017]

- Anstieg der DDoS-Angriffe insgesamt um 8 %
- Anstieg der Angriffe auf Infrastrukturebene (L3 und L4) um 8 %
- Anstieg der Reflection-Angriffe um 4 %
- Anstieg der durchschnittlichen Angriffe pro Ziel um 13 %

Die DDoS-Attacken des dritten Quartals beinhalteten bekannte Angriffsvektoren. Die Mirai-Malwarevariante nutzte Unmengen von IoT-Geräten, um einige der bisher umfangreichsten DDoS-Angriffe durchzuführen. Die größte von Akamai verzeichnete Attacke erreichte 623 Gbit/s. Obwohl das Botnet mittlerweile weniger aktiv ist, stellt Mirai auch weiterhin eine Bedrohung dar und war im dritten Quartal erneut für den größten verzeichneten Angriff verantwortlich – mit einem Spitzenwert von 109 Gbit/s.

Im dritten Quartal trat auch WireX auf den Plan, eines der ersten großen Android-basierten Botnets mit einer bemerkenswerten Art der Verbreitung: Verbraucher auf der ganzen Welt luden sich die Malware arglos aus dem Play Store herunter, wo sie sich in legitim wirkenden, aber infizierten Apps versteckte. Obwohl sich WireX schnell verbreitete, konnte die Bedrohung durch die Zusammenarbeit mehrerer Unternehmen, darunter auch Akamai, schon früh nach ihrem ersten Auftreten aufgehalten werden. Dieses gemeinschaftliche Projekt zeigt, was sich durch branchenübergreifende Zusammenarbeit im Bereich der Cyberbedrohungen erreichen lässt. Ganz wie bei Mirai müssen wir jedoch auch bei WireX damit rechnen, dass die Bedrohung weiterentwickelt und erneut eingesetzt wird. Unternehmen müssen sich darauf vorbereiten, dass mit neuen kriminellen Techniken DDoS-Angriffe jederzeit auftreten können – mit bisher ungeahntem Umfang.



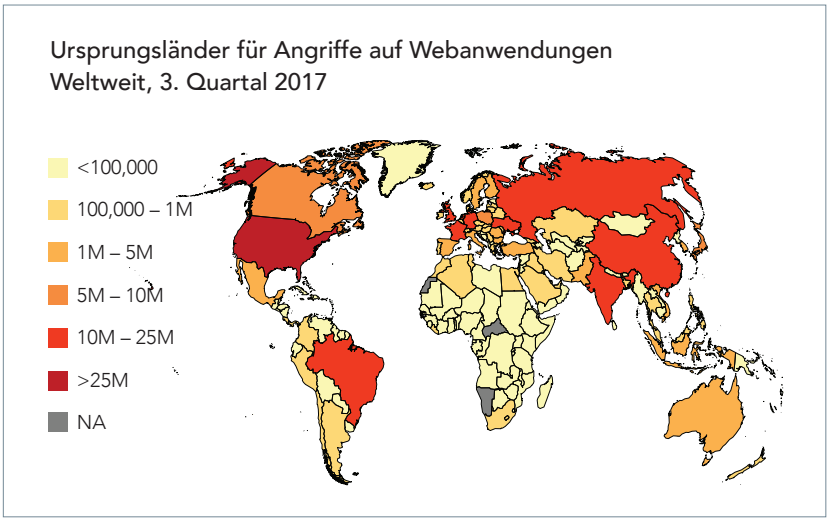
Angriffe auf Webanwendungen / Im Gegensatz zu DDoS-Attacken zielen Angriffe auf Webanwendungen meist auf Anwendungsschwachstellen ab, anstatt eine Website überlasten zu wollen. Ziel solcher Attacken ist es, Daten zu stehlen oder das zugrunde liegende System anderweitig zu beeinträchtigen. Angriffe auf Webanwendungen kommen deutlich häufiger vor als DDoS-Angriffe und können so potenziell größere Schäden verursachen. Durch diese Häufigkeit tendieren außerdem viele Unternehmen dazu, das Problem zu ignorieren. Leider nimmt die Anzahl solcher Attacken mit jedem Quartal zu. Im dritten Quartal stieg die Häufigkeit um 30 Prozent an. 85 Prozent der Angriffe nutzten entweder SQL-Injection oder Local File Inclusion, die beiden beliebtesten Angriffsvektoren.

ANGRIFFE AUF WEBANWENDUNGEN [Q3 2017 gegenüber Q2 2017]

- Anstieg der Angriffe auf Webanwendungen insgesamt um 30 %
- Anstieg der Angriffe aus den USA (führendes Ursprungsland) um 48 %
- Anstieg der SQLi-Attacken um 19 %

Die Vereinigten Staaten belegen weiterhin mit Abstand den ersten Platz als Quelle und Ziel des von Akamai verzeichneten Traffics aus Angriffen auf Webanwendungen. Im dritten Quartal erfolgten in den USA mehr als 300 Millionen Attacken auf Webanwendungen, also ca. fünfmal so viel wie beim Zweitplatzierten Russland.

Weitere Analysen und Forschungsergebnisse finden Sie im vollständigen Bericht.



„State of the Internet"-Sicherheitsbericht

***State of the Internet / Sicherheit* – Das Team**
Jose Arteaga, Leiter Akamai SIRT, Data Wrangler – Angriffe im Fokus
Dave Lewis, Global Security Advocate – DDoS-Aktivität, Angriffe auf Webanwendungen
Chad Seaman, Akamai SIRT – Angriffe im Fokus, Mirai-CnC-Cluster (Command and Control)
Wilber Mejia, Akamai SIRT – Angriffe im Fokus
Alexandre Laplume, Akamai SIRT – Angriffe im Fokus
Elad Shuster, Security Data Analyst, Threat Research Unit
Or Katz, Principal Lead and Security Researcher – Domain Generation Algorithm (DGA)
Jon Thompson, Custom Analytics
Shrijita Bhattacharya, Praktikant – Mirai-CnC-Cluster

Redaktionsteam
Martin McKeay, Senior Security Advocate, Senior Editor
Amanda Fakhreddine, Senior Technical Writer, Editor

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

Kontakt
sotisecurity@akamai.com
Twitter: *@akamai_soti* / *@AkamaiDACH* / *@akamai*
www.akamai.com/stateoftheinternet-security

Vollständigen Bericht herunterladen

„State of the Internet"-Sicherheitsbericht
Vollständiger Sicherheitsbericht für
das 3. Quartal 2017