„State of the Internet“-Sicherheitsbericht

Zusammenfassender Bericht für das 4. Quartal 2017

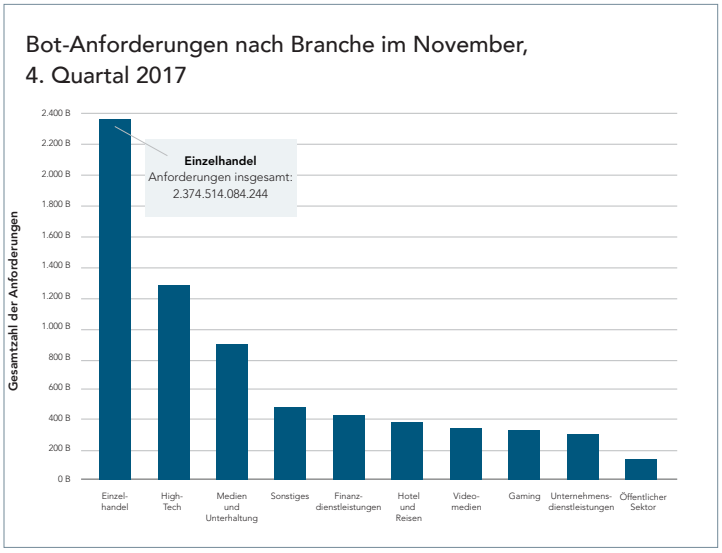
Akamai

Zusammenfassender Bericht / 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 erstellt, um Unternehmen und Behörden bessere strategische Entscheidungen durch die Nutzung dieser Daten und der darin enthaltenen Erkenntnisse zu ermöglichen. In jedem Quartal veröffentlicht Akamai einen *„State of the Internet"-Bericht* auf Basis dieser Daten, in dem es vorrangig um die Breitbandkonnektivität und Cloudsicherheit geht.

Auswirkungen auf Unternehmen / Einige der kostspieligsten und am meisten geschäftsschädigenden Angriffe im Jahr 2017 waren gravierende Sicherheitsverletzungen, die deutlich gemacht haben, wie wichtig Cybersicherheit für Unternehmen ist. Es sind die tückischen Hardwareschwachstellen, die es Spectre und Meltdown ermöglichten, Daten ohne Berechtigung über Schadprogramme aus dem Computerspeicher auszulesen. Solche weit verbreiteten und bedrohlichen Schwachstellen und das Chaos, das sie anrichten, sollten selbst das optimistischste Unternehmen aufhorchen lassen.

Viele der heutigen Angriffe nutzen weiterhin bekannte Schwachstellen aus, die bereits dokumentiert und gepatcht wurden und verhindert werden können. Es ist möglich, durch gemeinsame Anstrengungen einen grundlegenden Schutz aufzubauen – etwa durch sichere Codierungspraktiken, rechtzeitiges Patchen, die richtige Gerätekonfiguration und ein vernünftiges Passwortmanagement – auch wenn dies leichter gesagt als getan ist.

Die Sicherheitslage verändert sich kontinuierlich, da Kriminelle immer wieder neue Angriffsflächen ausnutzen. 2018 ist vor allem mit Angriffen auf Mobilgeräte, das Internet der Dinge und APIs zu rechnen. Zudem entwickeln sich die Angriffsstrategien stetig weiter. Tendenziell werden bei Angriffen auf Unternehmenssysteme heute nicht nur Daten, sondern auch Rechenressourcen gestohlen. Dies ist zum Teil auf den zunehmenden Einsatz von Kryptowährungen aber auch darauf zurückzuführen, dass sich mit diesen gestohlenen Ressourcen potenziell immer größere Vorteile erzielen lassen. Im *„State of the Internet"-Sicherheitsbericht* dieses Quartals werden darüber hinaus die Bereiche Netzwerkkonnektivität, Botnet-Traffic und der Missbrauch von Anmeldedaten beleuchtet. Es wird verdeutlicht, dass ein hoher Prozentsatz (43 %) der Anmeldeversuche bei Websites schädlich ist. Sich dieser Trends bewusst zu werden, ist heute ein Muss für jedes digital vernetzte Unternehmen.



Redaktionsübersicht / Der Jahresbeginn ist ein guter Zeitpunkt, um die im letzten Jahr gewonnenen Erkenntnisse Revue passieren zu lassen.

Jedes Jahr zeigen die Statistiken, dass sowohl DDoS- als auch Webanwendungsangriffe weiter zunehmen und Kriminelle nach wie vor altbewährte Angriffsvektoren effektiv nutzen. Ein klarer Hinweis dafür, dass grundlegende Best Practices zur Sicherheit dringend befolgt werden müssen. Dazu gehören beispielsweise das korrekte Konfigurieren und Patchen internetfähiger Geräte und die Einhaltung sicherer Codierungsrichtlinien wie die Bereinigung eingehender Daten.

Im 4. Quartal 2017 erlebten wir die anhaltenden Auswirkungen und Weiterentwicklungen des Mirai-Botnets. Im *„State of the Internet"-Sicherheitsbericht* dieses Quartals werden die Aktivität von Mirai und dessen Weiterentwicklung im vergangenen Jahr beleuchtet und es wird erläutert, wie Sie sich auf diese Bedrohung vorbereiten können. Das Akamai-SIRT-Mitglied Larry Cashdollar gibt einen tiefen Einblick in CVEs, auf die Sie vorbereitet sein sollten. Die beleuchteten Schwachstellen sind besonders gefährlich, da sie eine Ausführung auf dem System ohne Authentifizierung ermöglichen. Wir hatten in diesem Quartal ebenfalls die Möglichkeit, uns zwei Bereiche anzusehen, die bis dato noch nicht im *„State of the Internet"-Sicherheitsbericht* aufgeführt wurden: die Analyse von Bot-Traffic und die Analyse von Versuchen, Anmeldedaten zu missbrauchen.

DDoS-ANGRIFFE [4. Quartal 2017 im Vergleich zum 3. Quartal 2017]

- Abnahme der DDoS-Angriffe insgesamt um weniger als 1 %
- Abnahme der Angriffe auf Infrastrukturebene (Ebene 3 und 4) um 1 %
- Abnahme der Reflection-Angriffe um 3 %
- Anstieg der Angriffe auf Anwendungsebene um 115 %

Und nicht zuletzt ist damit zu rechnen, dass Kryptowährungen die Schlagzeilen im Jahr 2018 stärker dominieren werden. Sie spielen möglicherweise eine Rolle, wenn Unternehmenscomputer zum Zwecke der Abschöpfung von Rechenressourcen infiltriert werden. Kryptowährungen scheinen auch in vielen anderen Bereichen maßgeblich an der fortlaufenden Weiterentwicklung von Hackerstrategien beteiligt zu sein.

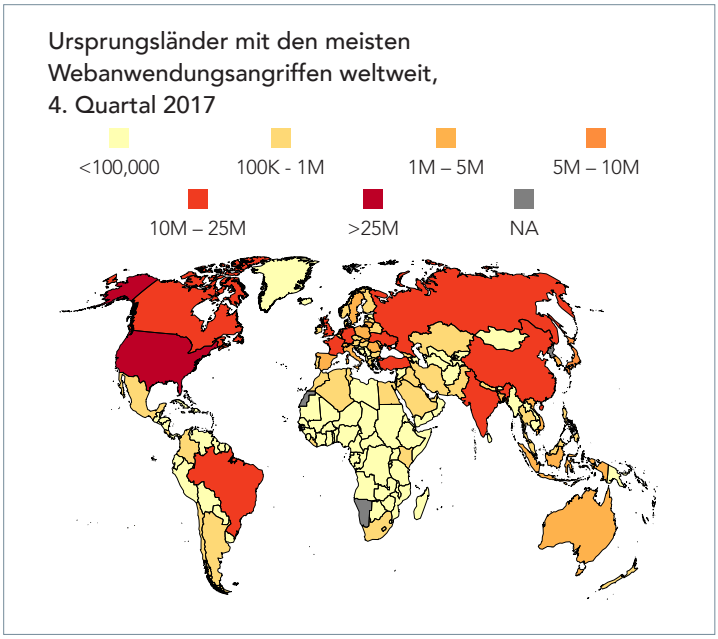
DDoS-Update / DDoS-Angriffe können Websites zum Erliegen bringen, den Geschäftsbetrieb unterbrechen und Ressourcen umleiten. Manchmal finden unter ihrem Deckmantel sogar noch bedrohlichere Daten- und Systemverletzungen statt. DDoS-Angriffe nahmen in den vergangenen Quartalen stetig zu. Im vierten Quartal 2017 gingen sie allerdings im Vergleich zum dritten Quartal leicht zurück (um weniger als 1 %). Es sind vor allem Attacken auf Anwendungsebene, die im Quartalsvergleich um ganze 115 % zunahmen, doch sie machen weiterhin lediglich 1 % der DDoS-Angriffe insgesamt aus. DDoS-Angriffe nahmen im Vergleich zum vierten Quartal 2016 um 14 % zu, was auf einen langfristigen Anstieg hindeutet.

Die Gaming-Branche war am häufigsten betroffen: IM 4. Quartal fanden hier 79 % der DDoS-Angriffe statt. Die am zweitstärksten betroffene Branche ist der Finanzdienstleistungssektor, der im vierten Quartal einen deutlichen Anstieg von bis zu 45 Angriffen pro Woche zu beklagen hatte. Die Häufigkeit dieser Angriffe unterstreicht, wie notwendig eine leistungsstarke DDoS-Abwehrlösung ist. Sie schützt nicht nur vor Geschäftsunterbrechungen, sondern auch vor mehrstufigen Angriffen, die DDoS-Kampagnen als Deckmantel für weitaus bedrohlichere Systemverletzungen nutzen.

ANGRIFFE AUF WEBANWENDUNGEN [4. Quartal 2017 im Vergleich zum 3. Quartal 2017]

- Rückgang der Attacken auf Webanwendungen um insgesamt 9 %
- Rückgang der Angriffe aus den USA um 29 %
- Rückgang der SQLi-Attacken um 9 %

Webanwendungsangriffe / Im Gegensatz zu DDoS-Angriffen zielen Webanwendungsangriffe in der Regel auf Anwendungsschwachstellen ab, um Daten zu stehlen oder das zugrunde liegende System auf irgendeine andere Art lahmzulegen. Webanwendungsangriffe sind weitaus häufiger als DDoS-Angriffe. Die Angreifer scannen dabei einfach das Internet auf Schwachstellen, die sie ausnutzen können. Nach einer starken Zunahme von 30 % vom zweiten zum dritten Quartal nahm die Zahl der Webanwendungsangriffe im vierten Quartal leicht ab. Im Vergleich zu 2017 zeigt sich aber insgesamt ein starker Zuwachs und für 2018 wird eine Fortsetzung dieses Trends erwartet.



Der wichtigste Angriffsvektor bleibt SQL-Injection. 50 % der Webanwendungsangriffe waren im vierten Quartal darauf zurückzuführen, verglichen mit 47 % im dritten Quartal. Diese Arten von Angriffen sind leicht automatisierbar und skalierbar und bleiben so lange effektiv, bis Unternehmen angemessene Sicherheitsmaßnahmen ergreifen, beispielsweise die Überprüfung von Benutzereingaben in den Code.

Die USA bleiben bei den von Akamai beobachteten Webanwendungsangriffen Spitzenreiter – sowohl als Ursprungsland als auch als Angriffsziel. In den USA gab es im vierten Quartal 238 Millionen Webanwendungsangriffe. Das sind weniger als die 323 Millionen Angriffe im dritten Quartal, aber immer noch zehnmal so viele wie in Brasilien. 132 Millionen Angriffe wurden im vierten Quartal von den USA aus gestartet. An zweiter Stelle stehen die Niederlande mit 47 Millionen Angriffen.

Weitere Analysen und Forschungsergebnisse finden Sie im vollständigen Bericht.

Der *„State of the Internet"-Sicherheitsbericht* für das 4. Quartal 2017 kombiniert Angriffsdaten aus der globalen Infrastruktur von Akamai und spiegelt die Forschung verschiedenster Teams im gesamten Unternehmen wider.

„State of the Internet"-Sicherheitsbericht

***State of the Internet / Sicherheit* – Das Team**
Jose Arteaga, Akamai SIRT Lead, Data Wrangler – Attack Spotlight
Dave Lewis, Global Security Advocate – DDoS Activity, Web Application Attack Activity
Chad Seaman, Akamai SIRT – Attack Spotlight
Wilber Mejia, Akamai SIRT – Attack Spotlight
Alexandre Laplume, Akamai SIRT – Attack Spotlight
Larry Cashdollar, Akamai SIRT, Sr. Engineer – Web Vulnerabilities to Watch
Richard Willey, Sr. Data Scientist – How to Make Sense of a Planetary Scale Network
Elad Shuster, Security Data Analyst, Threat Research Unit
Jon Thompson, Custom Analytics

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

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

Vollständigen Bericht herunterladen

Vollständiger „State of the Internet"-Sicherheitsbericht für das 4. Quartal 2017