# Das Internet der Dinge wird zur Waffe

Das Jahr 2016 war ein gutes Jahr für Cyberkriminelle – und ein schlechtes für ihre Opfer. Sie mussten die bisher stärksten DDoS-Attacken erdulden. Angriffe, die nun nicht mehr in Gigabit, sondern in Terabit pro Sekunde gemessen werden. Autor: Coen Kaat

Auf seinem Blog warnt der US-amerikanische Journalist Brian Krebs regelmässig vor den aktuellen Gefahren rund um Internetkriminalität. Er zeigt der Welt die Gesichter hinter den Skimasken, die man aus den unzähligen Symbolbildern zu Cybercrime und Hackern kennt. Ende September 2016 war sein Blog jedoch still. Statt sich über IT-Sicherheit informieren zu können, fanden Besucher lediglich eine Fehlermeldung vor. Eine DDoS-Attacke hatte den Blog regelrecht aus dem Netz gefegt. Eine DDoS-Attacke von einer noch nie dagewesenen Stärke. Um diese zu erreichen, änderten die Cyberkriminellen ihre üblichen Methoden.

Die Abkürzung DDoS steht für Distributed Denial of Service – zu Deutsch etwa «Verteilte Dienstverweigerung». Derartige Attacken zielen darauf ab, Server oder andere Netzwerkkomponenten zu überlasten. Cyberkriminelle überhäufen dabei ein System mit mehr Anfragen, als es verarbeiten kann. Die Folge: Die angegriffene Infrastruktur kann legitime Anfragen entweder nicht mehr oder nur noch sehr langsam verarbeiten. Die Website ist effektiv nicht mehr verfügbar.

Jede dritte DDoS-Attacke im DACH-Raum läuft über gemietete Cloud-Server. Bild: Shutterstock

## Das geheime Doppelleben eines PCs

Die enorme Masse an Anfragen generieren Cyberkriminelle in der Regel mit einem sogenannten Botnetz – zuweilen auch als Zombiearmee bezeichnet. Der Begriff beschreibt eine Gruppe von Computern, die ein Cyberkrimineller zu einem Netzwerk gebündelt hat. Zuoberst im Netzwerk steht der Command-and-Control-Server. Dieser kontrolliert alle Bots im Netz. Die betroffenen Benutzer bekommen das oft gar nicht mit.

Die Bots verteilen anschliessend Spam und Malware. Ein Cyberkrimineller kann seine Bots jedoch auch auffordern, gleichzeitig dieselbe Website aufzurufen. Je grösser das Botnetz, desto wahrscheinlicher ist, dass die Infrastruktur hinter der Website die Anzahl der Anfragen nicht bewältigen kann.

## Bots mieten bei AWS

In der Regel werden die Computer über Malware infiziert und dem Master-Server untergeordnet. Die Bots verteilen die Malware anschliessend weiter. So infizieren sie noch mehr Rechner. Der deutsche Sicherheitsanbieter Link-11 stellte jedoch fest, dass gewisse Cyberkriminelle einen deutlich leichteren Weg gefunden hatten. Das Unternehmen untersuchte im Juni 2016 DDoS-Attacken, die es auf Ziele im DACH-Raum abgesehen hatten. Fast ein Drittel davon lief über Cloud-Server. Ein deutlicher Anstieg im Vergleich zum Jahresanfang.

Die Sicherheitsexperten von Link-11 schliessen daraus, dass Cyberkriminelle die benötigte Rechenleistung zunehmend bei Cloud-Anbietern mieten und sie mit ge-

fälschten Kreditkarten bezahlen. Dass dies in den AGBs ausdrücklich untersagt werde, halte niemanden davon ab. Laut dem Bericht von Link-11 kann man etwa bei AWS rasch 200 Server pro Account mieten. Mit diesen 200 Cloud-Servern können die Cyberkriminellen Angriffsbandbreiten von mehr als 100 Gigabit pro Sekunde erreichen. Mehr als genug, um eine gewöhnliche Website lahmzulegen.

### DDoS-Rekorde fallen immer schneller

Die Attacke auf Krebsonsecurity, den Blog von Brian Krebs, erfolgte jedoch weder über infizierte PCs noch über gemietete Cloud-Server. Die Angreifer zapften das Internet der Dinge an. Die meisten Nutzer denken nicht daran, die Standardeinstellungen ihrer Router zu ändern oder den Zugriff auf ihre Netzwerkkameras zu beschränken. Der gewiefte Kriminelle findet schnell eine Vielzahl an Geräten, die er ohne grosse Mühen zu einem Botnetz verknüpfen kann. Gewisse Suchmaschinen haben sich sogar darauf spezialisiert, diese Geräte zu finden.

Die Angriffsbandbreiten auf Krebs' Blog waren entsprechend hoch: zwischen 620 und 665 Gigabit pro Sekunde. Das sei ein Vielfaches mehr, als ein Angreifer brauche, um eine Website lahmzulegen, schreibt Krebs im Nachhinein über die Attacke. Zudem haben die Angreifer den bisherigen Rekordwert fast verdoppelt. Dieser lag bei 363 Gigabit pro Sekunde und wurde erst im zweiten Quartal 2016 aufgestellt.

Auch Krebs' Rekord währte nicht lange. Gerade einmal eine Woche nach der Attacke auf den Blog meldete sich Octave Klaba auf Twitter zu Wort. Klaba ist Geschäftsführer des französischen Hosters OVH. Sein Unternehmen musste gleich zwei Cyberattacken erdulden. Eine mit einer Angriffsbandbreite von 901 Gigabit pro Sekunde. Die zweite mit knapp 1,2 Terabit pro Sekunde.

### DDoS wird Open Source

Mitte Oktober 2016 folgte die grosse Überraschung: Auf der Programmiererplattform Github veröffentlichte ein Nutzer den Quellcode für ein Tool namens Mirai. Das Tool steckte hinter den Attacken auf Krebs und OVH. Es ermöglicht dem Nutzer, ein massives Botnetz aus einer Vielzahl an vernetzten Geräten aufzubauen.

Sicherheitsforschern bot die Veröffentlichung von Mirai einen interessanten Einblick in die Angriffe – leider galt dies auch für Cyberkriminelle in spe. Noch im selben Monat wurde der US-amerikanische DNS-Serverbetreiber Dyn ebenfalls ein Opfer eines Mirai-Botnetzes. Die DDoS-Attacke hatte erneut eine rekordverdächtige Bandbreite von rund 1,2 Terabit pro Sekunde. Auch grosse Dienstleister und Unternehmen wie Amazon, Github, Netflix, Paypal, Reddit, Spotify, Tumblr und Twitter waren zeitweise nicht verfügbar.

### Jede Information lässt sich verkaufen

Nicht jeder Cyberkriminelle, der eine Website oder eine Dienstleistung mit einer DDoS-Attacke lahmlegt, gibt sich damit zufrieden. Für manche Cyberkriminelle sind DDoS-Angriffe nur Mittel zum Zweck. Ein Angriff kann aber auch verschleiern, dass ein Hacker eingedrungen ist und Daten gestohlen hat. Es gibt keine Information, die sich nicht irgendwo verkaufen lässt. Aber die Opfer zu erpressen, ist noch um einiges lukrativer. Die Kriminellen sind dadurch nicht mehr von einem Käufer abhängig. Zudem können sie ihren Opfern genau vorschreiben, welche Summe in welcher Währung wohin geschickt werden soll. Die Melde- und Analysestelle Informationssicherung (Melani) geht daher davon aus, dass die Anzahl Erpressungen weiter zunehmen werde. Dies geht aus dem ersten Halbjahresbericht 2016 hervor.

Im Bericht warnt Melani noch vor einer weiteren Taktik: Ransomware. Die Malware dringt in ein System ein und verschlüsselt Dateien oder ganze Festplatten. Der Benutzer sieht nur noch einen Sperrbildschirm mit der Aufforderung, ein Lösegeld zu zahlen.

Diese Erpressungstrojaner sind zwar keine neue Erfindung. Die ersten Gehversuche gehen bis in die 1980er-Jahre zurück. 2016 kann man jedoch eine inflationäre Zunahme feststellen. Ende 2015 konstatierte Sicherheitsanbieter Trend Micro etwa 29 verschiedene Ransomware-Familien. Ein halbes Jahr später waren es bereits 79. Da Unternehmen oft keine andere Wahl bleibt, als zu zahlen, wird diese Zahl wohl noch steigen.

**Für manche Cyberkriminelle sind DDoS-Angriffe nur Mittel zum Zweck.**