



2008/35 Lifestyle

<https://jungle.world/artikel/2008/35/great-firewall-china>

Internetzensur in China

Great Firewall of China

Von **Carsten Schnober**

Während der Olympischen Spiele wurde viel über die »Great Chinese Firewall« geredet. Aber wie funktioniert die Internetzensur in China, und wie kann man sie umgehen?

»Wir sind Idealisten. Idealismus ist etwas, das mit Naivität verbunden ist«, erklärte Jacques Rogge, Präsident des Internationalen Olympischen Komitees (IOC), zu Beginn der Olympischen Spiele in Peking. Damit rechtfertigte er das Vertrauen, mit dem er der chinesischen Regierung ihr Versprechen abgenommen hatte, während der Spiele ihre Internet-Filter auszuschalten. Politische Naivität will man dem IOC-Vorsitzenden gewiss nicht absprechen, aber dass er tatsächlich davon überrascht war, dass Journalisten und IOC-Offizielle an Ort und Stelle ein gefiltertes Internet vorfanden, erscheint dennoch fraglich.

Von der chinesischen Internet-Zensur wurde während der Olympischen Spiele viel gesprochen. Zugleich weiß man wenig darüber, wie das System funktioniert, das viele Millionen chinesische Internet-Nutzer automatisch von kritischen Inhalten fernhalten soll. Weder die chinesischen Behörden noch Internet-Anbieter geben darüber Auskünfte. Die über die große Firewall bekannten Informationen haben internationale Experten in zahlreichen Versuchen zusammengetragen, wie beispielsweise ein britisches Forscherteam an der Universität Cambridge.

Die automatische Internet-Zensur profitiert davon, dass der gesamte Datenverkehr zwischen China und dem Internet eine überschaubare Anzahl von Knotenpunkten passiert. An diesen Schnittstellen verbinden Router die chinesischen Teilnetze mit dem Rest der Welt. Intrusion-Detection-Systeme (IDS), die eigentlich Angriffe auf Internet-Computer und -Teilnetze abwehren sollen, überwachen dort, ob Daten, die den Zensurregeln zuwiderlaufen, zwischen Internet und chinesischen Rechnern weitergeleitet werden. Was für ein System dabei genau zum Einsatz kommt, ist unbekannt. Die chinesischen Behörden besitzen das »Secure Intrusion Detection System« der Firma Cisco, das auf einem Filter basiert, der angeforderte Homepages danach untersucht, ob sie bestimmte Stichwörter enthalten. Sobald der Filter ein unerwünschtes Wort findet, unterbricht das System die

Verbindung. Dabei wird ein spezielles Datenpaket (Reset-Paket) sowohl an den Server als auch an den Computer geschickt, der die Anfrage gestellt hat. Normalerweise interpretieren dann beide Rechner die Verbindung als von der Gegenseite zurückgesetzt und beenden die Kommunikation.

Außer dem Wortfilter existieren Listen von Seiten, die prinzipiell blockiert werden. Darunter fallen beispielsweise Angebote wie Youtube, Wikipedia und die Seiten vieler US-amerikanischer, britischer und anderer westlicher Zeitungen sowie Fernsehsender. Allerdings gibt es in den chinesischen Provinzen Unterschiede, und von Zeit zu Zeit werden Sperrungen aufgehoben oder neu eingerichtet. Das erklärt, weshalb Internet-Nutzer im olympischen Pressezentrum mehr westliche Seiten erreichen konnten, als es in China üblich ist. Der Filter wurde allerdings auch für die dort anwesenden Journalisten nicht gänzlich abgeschaltet, wie es beispielsweise in der chinesischen Sonderverwaltungszone und Wirtschaftsmetropole Hongkong der Fall ist. Constanze Kurz, Sprecherin des Chaos Computer Clubs (CCC), schätzt, dass in der chinesischen Zensurbehörde etwa 30 000 Personen die Wort- und Seitenlisten ständig aktualisieren. Andere gehen sogar von 50 000 Mitarbeitern aus, aber offizielle Angaben gibt es nicht. Die Internet-Zensoren sorgen dafür, dass sich das Filtersystem trotz seiner statischen Funktionsweise ständig anpasst.

Der chinesische Internet-Filter gilt zwar als einer der ausgefeiltesten der Welt, lässt sich aber mit vergleichsweise einfachen Mitteln austricksen. Erkennt das Filtersystem bei einer Anfrage Wörter, die gefiltert werden sollen, reicht es aus, wenn der Server und der anfragende Rechner die von der Zensur-Firewall versandten Reset-Pakete ignorieren, um ihre Kommunikation fortzusetzen. Das erfordert die Installation einer speziellen Software, sowohl auf dem Server als auch auf dem Client-Computer. Ein solches Programm zu installieren, setzt keine besonders große Fachkenntnis voraus, dafür aber die aktive Kooperation des betreffenden Servers. Zudem lässt sich die Verbindung unabhängig davon zurückverfolgen; für die chinesischen Web-Surfer besteht deshalb die Gefahr, entdeckt und von der bekanntermaßen nicht eben milden Justiz der Volksrepublik belangt zu werden.

Einfacher ist es, den Wortfilter gar nicht erst zum Zuge kommen zu lassen, indem man verschlüsselt kommuniziert und somit keinerlei Einblick in die ausgetauschten Informationen gewährt. Auch dazu ist es allerdings notwendig, dass der angesteuerte Webserver mitspielt und das https-Protokoll unterstützt – die verschlüsselte Variante des im WWW normalerweise verwendeten Protokolls. Auf dem Rechner des Surfers ist dann jedoch keine Modifikation notwendig.

Beim Zugriff auf nicht entsprechend präparierte Webserver hilft ein Proxy. Er funktioniert als Zwischenstation und nimmt Anfragen entgegen, um sie an das eigentliche Ziel weiterzuleiten. Die Antwort gelangt auf demselben Weg zurück. Dazu muss lediglich die Verbindung zwischen dem hinter der chinesischen Firewall befindlichen Server und dem irgendwo im Ausland stationierten Proxy verschlüsselt ablaufen, um den Wortfilter zu umgehen.

Verschlüsselte Verbindungen funktionieren aber nur mit Webservern, die nicht durch die zweite Komponente des chinesischen Filters blockiert werden, die nach dem Server-Namen oder der numerischen Internet-Adresse siebt. Auch Proxy-Server können auf diese Weise nutzlos werden. Wer die Internet-Mauer durchbrechen möchte, benötigt deshalb

immer wieder neue Proxys, weil sie nach und nach auf der schwarzen Liste landen.

Schwieriger zu verhindern ist für die Zensur der Einsatz des Anonymisierungsdienstes Tor («The Onion Router»). Dabei läuft die Verbindung zwischen einem Rechner und dem Server immer über unterschiedliche Stationen ab, wobei sich dank der eingesetzten Verschlüsselung Start und Ziel der Kommunikation einander nicht mehr zuordnen lassen. Der Chaos Computer Club hat für den einfachen Einsatz von Tor nicht nur in China einen so genannten Freedom-USB-Stick entwickelt. Das Speichermedium enthält die Tor-Software und einen entsprechend voreingestellten Web-Browser. Schließt man ihn an einen beliebigen Windows-Rechner an, kann man direkt anonym und verschlüsselt surfen. Es existieren zahlreiche weitere Methoden, um Informationen am chinesischen Internet-Filter vorbeizuschleusen. Er ist also ganz und gar nicht perfekt, und man kann davon ausgehen, dass viele Chinesen mit entsprechendem Bildungsstand über die nötige Fachkenntnis verfügen, um ihn regelmäßig zu umgehen. Das setzt allerdings voraus, dass überhaupt Interesse daran besteht – die große Mehrheit der chinesischen Surfer kommt mit dem Internet außerhalb Chinas gar nicht erst in Kontakt.

Chinesische Webseiten enthalten normalerweise keine Links auf ausländische Homepages. Die chinesischen Varianten der großen Suchmaschinen von Google, Yahoo und Microsoft liefern ebenfalls keine Ergebnisse, die die chinesischen Behörden nicht abgesegnet haben. Weil Querverweise ins Netz außerhalb des chinesischen Einflussbereichs fehlen, müssen Surfer also von sich aus auf die Idee kommen, Server im restlichen Internet aufzusuchen. Der automatische Internet-Filter funktioniert vor allem bei den Surfern, die eher versehentlich auf unliebsame Seiten geraten. Er reduziert die Zahl der Besucher ausländischer Seiten damit auf eine leichter überschaubare Personenzahl, bei der man von aktivem Interesse ausgehen kann. Diese Surfer verlieren damit den Schutz der Masse und werden pauschal verdächtigt, politische Dissidenten oder Kriminelle im Sinn des chinesischen Strafrechts zu sein; denn nicht nur politische, sondern auch pornografische und andere in China illegale Inhalte werden gefiltert.

Auch andere Staaten könnten vergleichbare Filtersysteme einsetzen, um unliebsame Inhalte auszusperren, obwohl bislang in erster Linie Listen eingesetzt werden, um einzelne Seiten statisch vollständig zu sperren, beispielsweise auf Druck der Landesregierung auch durch nordrhein-westfälische Internet-Anbieter. Dienste wie Tor verleihen Internet-Nutzern aber überall Anonymität und damit Schutz vor politischer und strafrechtlicher Verfolgung. Die vollkommene Kontrolle des Internets wird keiner Regierung möglich sein, aber aus ihrer Perspektive besteht ein Erfolg bereits darin, den »verdächtigen« Personenkreis einzuschränken, sodass die Kontrolle einfacher wird.