Netzsperren in Österreich

Werner illsinger

Seit Donnerstag 2.10.2014 gibt es in Österreich Netzsperren. Der Verein für Antipiraterie in Österreich (VAP) hat über ein Gerichtsverfahren erreicht, dass Internet Seiten von den Internet-Providern auf Zuruf (ohne weiteres Gerichtsverfahren und ohne Anordnung eines Richters) gesperrt werden müssen.

Die Internet-Provider sind mit diesem Zustand sehr unzufrieden, denn sie werden zu Hilfssheriffs ernannt, die selbst Recht sprechen müssen. Sie müssen beurteilen, ob die behauptete Rechteverletzung tatsächlich vorliegt – und dann eine Seite sperren. Dies kann natürlich auch nach hinten losgehen, denn wenn der Provider eine Seite sperrt, könnte ein Kunde den Provider verklagen, weil er seine Verträge nicht erfüllt.

Ich muss auch vorausschicken, dass ich grundsätzlich Verständnis für das Urheberrecht habe – ich habe meine Brötchen auch schon mit Softwareentwicklung verdient und ich verstehe, dass ein Urheber (in meinem Fall Programmierer) mit seiner Arbeit Geld verdienen möchte. Wir müssen uns als Gesellschaft überlegen, wie wir das Problem lösen können. Der derzeit eingeschlagene Weg ist aus meiner Sicht aber der falsche.

Zudem ist es aus meiner Sicht auch fragwürdig, ob Seiten wie kinox.to oder andere derartige Seiten überhaupt selbst Urheberrechtsverletzungen begehen. Zumeist sind auf solchen Seiten selbst keine urheberrechtlich geschützten Werke gespeichert. Die Filme liegen nicht auf dem betroffenen Server selbst, sondern sind meist übers Internet verstreut auf unterschiedlichen File Sharing Plattformen gespeichert. Die Seite beinhaltet nur eine „Suchmaschine“ und Links auf die Werke. Man müsste eigentlich also bei den Plattformen ansetzen, die die Werke tatsächlich zum Download anbieten. Das ist jedoch schwierig, weil es derer sehr viele gibt. Zum anderen bieten diese Plattformen auch legale Inhalte an (je nachdem was die Benutzer eben auf diese Server laden).

Ich selbst finde kinox.to auch nicht sehr sympathisch und sehr mühsam. Die dort angebotenen Filme können nur schlecht gefunden und gestreamt werden – man wird mit Werbepopups und teilweise auch Malware überschüttet – und die Wahrscheinlichkeit, dass man sich Adware und andere Dinge auf den PC holt, ist größer, als dass man einen annehmbaren Filmgenuss hat. Der Hintergrund ist, dass Seiten wie kinox.to viel Geld mit Werbung verdienen – die ihre Seite zupflastert. Der Gratis-Download von Filmen ist gar nicht so gratis und die Portalbetreiber verdienen nicht schlecht damit. Betreiber kino.to (Vorläufer von kinox.to) Kim Schulz (aka Kim Dotcom) war immerhin einer der reichsten Neuseeländer. Das ist unfair, denn das Geld wäre nicht diesem Typen sondern den Urhebern der Filme zugestanden.

Die Implementierung der Netzsperren erfolgt über eine Falscheintragung im DNS Server des betroffenen Providers. DNS Server sind jene Server die einen Namen (kinox.to) auf eine vom Computer verständliche IP Adresse (91.202.61.170) umsetzen. Wenn man also im Browser http://kinox.to eintippt landet man eigentlich auf http://91.202.61.170.

Wenn nun der Provider eine „Netzsperre“ vornimmt, dann gibt der DNS Server eine falsche Antwort. Im Normalfall wird man auf eine Web Seite des Providers umgelenkt, die einem mitteilt, warum man die Seite nicht erreichen kann.

Die betroffenen Provider sind Tele2, A1, UPC und 3. Wenn man also Kunde von einem dieser Provider ist, deren DNS Server nutzt und kinox.to ansurft, gelangt man auf eine Website die einem mitteilt dass man das nicht darf.

Ich habe mittlerweile in diesem Text bereits zwei Methoden dargestellt, wie man diese Netzsperren umgehen kann:

- Wenn man die IP Adresse des Servers kennt, benötigt man den DNS Server gar nicht. Mittels http://91.202.61.170. landet man auch auf kinox.to – der DNS Server wird nicht gefragt – daher funktioniert das auch bei den betroffenen Providern.
- Wenn man einen anderen DNS Server als den des Providers verwendet.
  Die bekanntesten „freien“ DNS Server sind die von Google: 8.8.8.8 und 8.8.4.4. Trägt man diese beiden Server unter den Einstellungen der Netzwerkkarte im IPv4 Protokoll als Name Server ein – funktioniert die Sperre der Seiten auch nicht.

Es gibt noch weitere Möglichkeiten:

- Kinox.to hat sofort reagiert und ist nun auch unter http://kinox.tv und http://kinox.me erreichbar. Da ein anderer Name verwendet wird, müssen die Provider auch diese sperren. Das wird wieder einige Zeit dauern – und irgendwann werden auch diese Seiten gesperrt werden.
- VPN
  Virtuelle Private Netzwerke verwenden sogenannte Tunnelprotokolle. Wenn ich mich von zu Hause mit einem VPN-Server verbinde, dann sieht es für den Rest der Welt so aus, als ob ich das Internet aus dem Blickpunkt des VPN-Servers verwenden würde. Ich sitze also sozusagen zum Surfen im Netzwerk des VPN-Servers. Wenn der VPN-Server im Ausland steht, dann haben Österreichische Sperrvorschriften keinen Einfluss auf diesen Server. Man kann daher das Internet verwenden wie es dieses Land / dieser VPN Provider zulässt.
- TOR
  TOR ist ein „Verschleierungsnetzwerk“ – Es macht es schwieriger nachzuvollziehen, wer von wo, welche Seiten ansurft. Auch die Verwendung von TOR würde die Sperrlisten unwirksam machen.

Die VAP sagt nun, dass sie die bestehenden Sperrmaßnahmen für die Seiten für unzureichend hält. Man verlangt nun von den Providern weitergehende Sperren als die Seite nur im DNS-Server zu blocken. Man legt nahe, dass man Sperren gewisser IP Adressen wünscht.

Die VAP übersieht dabei, dass auch diese Sperren leicht zu umgehen sind. VNP oder TOR ist auch die IP-Adresssperre egal. Da man mit VPN sozusagen von einem anderen Land aus surft, sind Sperren des eigenen Providers irrelevant.

Was kommt dann als Nächstes?

Sperre von VPN Zugängen. Natürlich könnten die Provider auch alle VPN-Zugänge aus ihrem Netz blockieren. VPN ist aber eine Technologie, die vor allem von Unternehmenskunden verwendet wird. In Unternehmen werden VPNs dazu verwendet, dass ein Mitarbeiter von zu Hause oder von unterwegs sicher auf Unternehmensdaten zugreifen kann. Eine Sperre der VPN -Technologie würde also dazu führen, dass Unternehmen die Netzwerke der betroffenen Provider nicht mehr nutzen können.

Da VPNs also voraussichtlich nicht verboten werden können – müsste man noch einen „Sittenwächter“ neben jeden Benutzer stellen. Das wäre die einzige Möglichkeit, flächendeckend sicherzustellen, dass der Benutzer nicht „böse“ Seiten ansurft. Da das vermutlich zu teuer wäre, könnte man die Internet Provider dazu verpflichten, Benutzer zu „vernadern“ – und dann erst die „Sittenwächter“ losschicken, um die bösen Benutzer zur Rechenschaft zu ziehen.

Kommt Euch dieses Szenario bekannt vor?

Mir auch. Und mir läuft ein kalter Schauer über den Rücken. Solche Systeme gab es schon einmal in der Geschichte und nein, sie haben nicht nur dazu gedient Urheberrechtsverletzungen zu verfolgen. Wenn die Mechanismen einmal da sind, kann man sie natürlich auch anders verwenden. In so einem System will ich nicht leben.