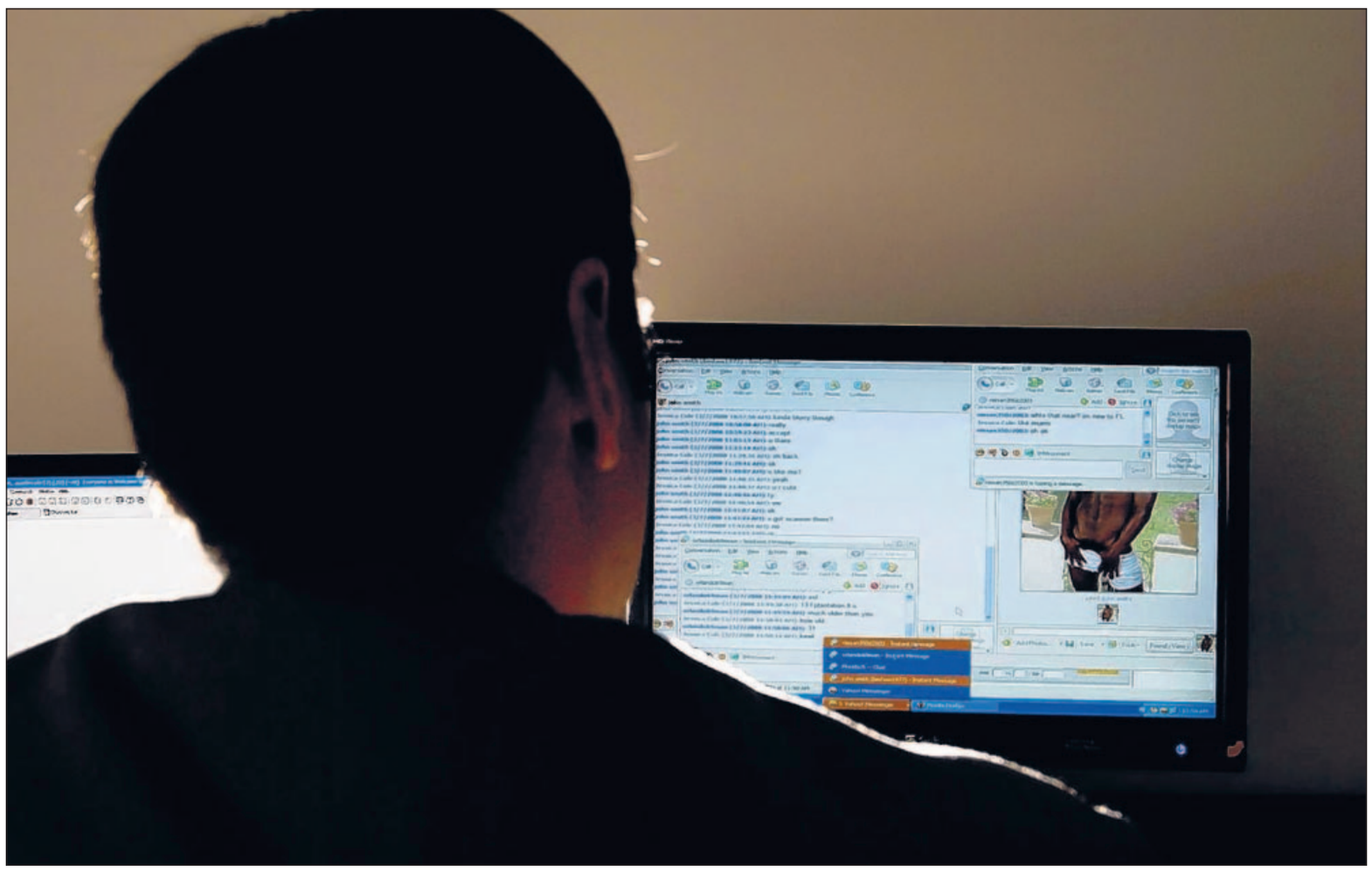
Sperren schaffen Kinderpornos nicht aus der Welt

Heute wollen Familienministerin von der Leyen und eine Reihe von Internetprovidern einen Vertrag unterzeichnen. Damit verpflichten sich die Dienstleister, Seiten mit kinderpornografischem Inhalt zu sperren. Dass das funktioniert, bezweifeln Experten: Abgesehen davon, dass im weltweiten Netz nichts verloren geht, ist eine Sperrung von Seiten mit der geplanten Methode sinnlos.

VON MARCO KALINKE



Ermittler sind im Internet Pädophilen weltweit auf der Spur. FOTO: AFP

Internetseiten mit kinderpornografischem Inhalt so zu sperren, wie es Familienministerin Ursula von der Leyen fordert, funktioniert nicht. Darin sind sich Experten einig wie Michael Rotert, Vorstandsvorsitzender des Verbandes Deutscher Internetwirtschaft, oder der Chaos Computer Club, ein Forum der Hackerszene. Im Gespräch ist eine DNS-Sperre, und allein der Begriff Sperre ist schon irreführend. Gesperrt wird nämlich nichts, lediglich der Zugang wird etwas schwieriger.

Der Begriff DNS hat in diesem Fall nichts mit dem Erbgut zu tun, sondern bezeichnet einen Dienst, der Anfragen im Internet beantwortet, das Domain Name System. Wer beispielsweise die Zeitungsberichte der RHEINPFALZ im Internet lesen will, muss die Adresse www.rheinpfalz.de in die Adressleiste seines Browsers eingeben. Browser sind Programme zum Ansehen von Internetseiten, gängig sind etwa der „Internet Explorer“ oder „Firefox“. Der Browser an sich weiß nicht, wo die Seiten der RHEINPFALZ abgelegt sind. Deshalb sendet er eine Anfrage an einen DNS-Server. Das ist ein Rechner, auf dem die genaue Adresse hinterlegt ist, und in der Regel ist das der Rechner des Anbieters, bei dem der Kunde einen Internet-Vertrag abgeschlossen hat. Das kann etwa die Telekom sein oder 1&1.

Der DNS-Server schickt nun die Adresse an den Browser zurück, der sich mit der gewünschten Adresse verbindet. Diese Vorgehensweise ist nötig, weil eine Internetadresse nicht aus Namen besteht, sondern aus einer Nummer. Diese wird IP-Adresse (Stichwort) genannt. Für den Nutzer ist es natürlich einfacher, sich einen Namen zu merken als eine Zahl mit bis zu zwölf Ziffern. Deshalb gibt er rheinpfalz.de in seinen Browser ein und nicht die Zahlen. Der DNS-Server schaut dann nach, welche Nummer zu dem gewünschten Namen gehört. Er ist im Prinzip ein Telefonbuch für Internetadressen.

> Gesperrt wird gar nichts – nur der Zugang wird etwas schwieriger.

Und das ist schon der erste Haken an der DNS-Sperre. Soll eine unerwünschte Seite gesperrt werden, wird einfach der Eintrag aus dem Telefonbuch genommen, die Seite bleibt unangetastet und steht weiter zur Verfügung. Wer die Nummer kennt, gibt einfach die in den Browser ein, statt des Namens. Das kann jeder ausprobieren, indem er die folgende Nummer mit den Punkten dazwischen eingibt. Und zwar sonst nichts. Kein www oder http. Er wird bei der Suchmaschine Google landen, so als ob er den Namen eingegeben hätte. Die IP-Adresse zur Domäne „www.google.com“ lautet 209.85.227.103.

Der zweite Pferdefuß an der DNS-Sperre: Der Nutzer ist nicht auf den DNS-Server des Anbieters angewiesen. Ähnlich wie beim Telefonieren kann er sagen: Gut, wenn die Nummer nicht im Örtlichen drin steht, schau ich halt mal bei den Gelben Seiten nach. Übertragen heißt das, der Nutzer stellt seinen Router auf einen DNS-Server in Timbuktu oder Kasachstan ein, der vielleicht keine Adressen aus seiner Liste sperrt. Wie das ganz einfach geht, beschreibt der Chaos Computer Club auf seinen Internetseiten für verschiedene Betriebssysteme. (http://www.ccc.de/censorship/dns-howto/).

Schutz vor Kinderpornografie oder eine Möglichkeit, den Handel im Internet damit nur ansatzweise zu unterbinden, bietet die DNS-Sperre nach Meinung von Michael Rotert nicht. Zumal der Handel ganz anders funktioniere. Beispielsweise kann ein Buch zum Verkauf angeboten werden, der Käufer bekommt aber kein Buch geschickt, sondern eine Adresse, unter der er sich 100 Bilder oder ein Video herunterladen kann. „Die Szene hantiert mit Zahlen, auf die stößt Otto-Normalnutzer nie“, sagt Rotert. Und selbst wenn sich jemand mal vertippt und auf einer solchen Seite landet, würde die DNS-Sperre nicht greifen. Denn der DNS-Server schaut nur nach dem ersten Teil der Domäne, also nach www.abc.de. Wer mit illegalen Inhalten handelt, wird die aber sehr gut verstecken. Beispielsweise unter www.abc.de/efg/x/y/z. Eine DNS-Sperre müsste also ganz tief im Datenpaket suchen, eventuell gar auf Inhalte untersuchen.

Macht sie das nicht und sperrt die gesamte Domäne, kann es passieren, dass die legalen Firmen efg, x und y plötzlich abgeschnitten sind, nur weil z einen illegalen Dienst betreibt. Wenn eine Sperre aber bei jeder Anfrage derart tief in ein Datenpaket eindringen muss, kostet das Zeit. Das Internet würde nach Meinung Roterts ganz schnell in die Knie gehen: „Statt Breitband haben wir dann wieder ein Schmalband.“

Dass es eine Diskussion um Kinderpornografie im Netz gibt, findet Rotert absolut nicht schlecht, fürchtet aber, dass sich durch die DNS-Sperren, das Phänomen der Ekelseiten von „Rotten“ wiederholt. Die Internetseite stellte Perversionen und Schrecklichkeiten aller Art dar. Nachdem das Thema in den Medien hochkochte, seien die Bilder kurz darauf auf allen Schulhöfen getauscht worden. Ähnliches könnte sich mit den Adressen der gesperrten Seiten wiederholen. Denn mit einem einfachen Befehl kann sich ein Nutzer sämtliche Adressen eines DNS-Servers auflisten lassen, auch die gesperrten, sagt Rotert. „Was ist dann los? Das macht doch erst recht neugierig. Im Internet gibt es solche Listen bereits, und die Leute werden erst recht drauf gestoßen.“

Etwas besser als einfache DNS-Sperren sind die Hybrid-Sperren, die die Britische Telekom einsetzt. Dort werden Name und Nummer überprüft. Wenn an einer Adresse mehrere Kunden dranhängen, wird genauer hingeschaut, welcher gemeint ist. „Aber das ist relativ teuer, und nur die Britische Telekom benutzt es. Kleine Anbieter können sich das gar nicht leisten. Außerdem braucht es ein bis zwei Jahre, bis das System aufgesetzt ist. Für den Wahlkampf reicht das nicht mehr“, stellt Rotert fest.

Um eine DNS-Sperre aufzubauen, sind vorgeschaltete Rechner nötig, neue Namens-Server müssen eingerichtet und Logbücher geführt werden, in denen steht, wer wann wohin wollte. Außerdem müssen die entsprechenden Programme entwickelt werden, denn von Hand kann das niemand leisten. Je nachdem wie viele Kunden ein Anbieter verwaltet, schätzt Rotert die Kosten zwischen 100.000 Euro und einstelligen Millionenbeträgen. „Aber die Kosten sind nicht das Problem, sondern dass die ganze Idee nicht durchdacht ist.“

Viel sinnvoller findet Rotert den Einsatz von Filtern auf Benutzerseite, also im PC oder den Anschlusskomponenten. Denn diese sind nicht auf das Sperren – um bei dem Vergleich zu bleiben – des Telefonbuches beschränkt, sondern könnten zusätzlich IP Adressen, also die Telefonnummern, oder gar Inhalte wie Bilder sperren. Sinnvoll ist der Einsatz von Filtern, um Kinder vor Seiten zu schützen, die nicht für sie gedacht sind. Hier sieht Rotert alle gefordert: Die Anbieter von Internetzugängen, die ihre Router standardmäßig mit Filtern ausrüsten könnten und auch die Anbieter von Browsern oder Softwareprogrammen.

Dem Pädophilen, der gezielt nach kinderpornografischen Seiten sucht, machen die Filter das Leben jedoch nicht schwerer. Denn der sperrt sich ja nicht selbst. Die Alternative wäre, dass Anbieter die Nummern in ihren Routern sperren. Doch was passiert, wenn unter einer Nummer eine illegale Seite und neun legale liegen? Ein Schuhhändler seine Schuhe plötzlich nicht mehr über das Netz verkaufen kann oder ein Reisebüro nicht mehr erreichbar ist? Dann kommt ganz schnell das Thema Schadensersatz zur Sprache. In der Verantwortung wären die Anbieter. Es sei denn, die Bundesregierung findet einen anderen Dummen.

STICHWORT

IP-Adresse

Die IP-Adresse ist eine eindeutige Nummer, die jedem Teilnehmer (Rechner) zugeordnet wird, der mit dem Internet verbunden ist, sozusagen die Postadresse. Anhand der Adresse wissen die Router – die Poststellen – wohin sie Datenpakete schicken müssen. Domänen wie beispielsweise www.google.de haben eine feste IP-Adresse. Anbieter von Internetzugängen, die Provider, haben einen ganzen Pool voller Adressen. Wenn sich nun ein Kunde ins Internet einwählt, wird ihm eine freie Adresse aus diesem Pool zugeordnet. Verlässt der Kunde das Internet, ist die Adresse wieder frei. Eine IP-Adresse besteht aus vier Zahlen zwischen 0 und 255, die durch einen Punkt getrennt sind. (mco)

Zur Sache: Benutzerautonome Filter

Einen benutzerautonomen Filter, der direkt in den Router integriert ist, bietet in Deutschland – nach eigenen Angaben – nur die Mainzer Cybits AG zusammen mit dem Unternehmen D-Link an. Der Filter überprüft beim Verbindungsaufbau, ob die IP-Adresse, also die „Telefonnummer“ erlaubt ist. Ist sie das nicht, kommt keine Verbindung zustande. Eine DNS-Sperre hingegen zeigt dem Nutzer lediglich die „Telefonnummer“ nicht an. Besorgt er sich die über einen anderen Weg, ist die DNS-Sperre nutzlos.

Die Cybits-Filter arbeiten mit Negativ- und Positivlisten. Eltern können den Router so einstellen, dass ihre Kinder nur Internetseiten besuchen können, deren Inhalt auf der Positivliste steht. Oder sie dürfen alles sehen, außer den Seiten der Negativliste. Die Listen werden von Medienpädagogen per Hand erstellt und in regelmäßigen Abständen über das Internet auf dem Router aktualisiert. Nach Angaben des Unternehmens können die Eltern die Listen nach eigenen Wünschen ändern, also Seiten von der Negativliste auf die Positivliste verschieben und umgekehrt. (mco)