Warum Frankfurt?

Frankfurt hat sich in den vergangenen Jahren zum größten Datenumschlagplatz der Welt entwickelt, noch vor Amsterdam und London. Das hat etwas mit dem Aufbau des Internets zu tun: Es besteht aus vielen einzelnen Netzwerken, die miteinander verbunden sind – über Knotenpunkte, von denen es mehr als 300 weltweit gibt. Einer ist in Frankfurt, er besteht aus mehreren Rechenzentren und heißt German Commercial Internet Exchange oder kurz: DE-CIX. Die Betreiberfirma ist eine Tochtergesellschaft des Internetverbandes ECO.

Über den DE-CIX läuft ein großer Teil des deutschen und internationalen Internetverkehrs. Eine App der Journalistenagentur OpenDataCity demonstriert die Bedeutung von DE-CIX, Sie sehen rechts einige Beispiele dafür: Egal, ob Sie Facebook oder Google aufrufen, und selbst wenn Ihr Computer ganz woanders in Deutschland steht, läuft die Anfrage, bis sie ihr Ziel erreicht hat, über mehrere Stationen – und unter anderem über Frankfurt.

„An einem Knotenpunkt laufen sehr, sehr viele Informationen zusammen", sagt Josef von Helden, Informatik-Professor an der Hochschule Hannover. „Deshalb lassen sich an einer so zentralen Stelle des Internets auch potenziell mehr interessante Informationen sammeln." Das ist eine Chance – und gleichzeitig eine Last, wie eine Zahl verdeutlicht: Über Frankfurt laufen in Spitzenzeiten ein bis zwei Terabit pro Sekunde, meldet der DE-CIX. Wären es nur E-Mails, wären es an einem Tag mehr als 21 Billionen. Es sind aber nicht nur elektronische Nachrichten.

„Der größte Teil der Daten im Internet sind Videos und Musik", sagt Peter Leppelt, Geschäftsführer der Datenschutzfirma Praemandatum. „Ich bekomme an einer solchen Schnittstelle wie einem Knotenpunkt also viel Überschuss, viel Müll, den ich aussortieren muss." Für einen Geheimdienst wäre es deshalb einfacher, direkt einen E-Mail-Provider wie Google Mail anzuzapfen als einen Internet-Knotenpunkt, meint Leppelt. „Die schiere Menge an Daten macht es unrentabel." Auch von Helden sieht dieses Problem. In den vergangenen Jahren seien aber „intelligente und effiziente Filtermechanismen" entwickelt worden. „Deshalb ist es möglich", meint der Informatik-Professor, dessen Schwerpunkt IT-Sicherheit ist. „Aber es ist eine gewaltige Herausforderung."

Direkt am Knotenpunkt

Am einfachsten wäre es, am Knotenpunkt selbst, also im Rechenzentrum die Daten mitzuschneiden. Aber wenn hier jemand ein Kabel anklemme und Geräte aufstelle, „müsste das dem Betreiber auffallen", sagt Josef von Helden, Informatik-Professor an der Hochschule Hannover. Und der Betreiber des Knotenpunktes dementiert vehement, dass die NSA oder andere Auslandsgeheimdienste auf die Datenleitungen zugreifen können. Die für eine Überwachung im großen Stil notwendigen Kabelstränge würden auffallen, sagte ein Sprecher des DE-CIX. Außerdem gebe es verschiedene technische Schutzvorrichtungen.

Ist es wirklich definitiv ausgeschlossen? Es wäre möglich, dass jemand von außen Schadprogramme ins Rechenzentrum einschleuse und die Kontrolle übernehme, sagt von Helden. „Diese Schadprogramme würden weitgehend unbemerkt arbeiten." Allerdings könne die Software niemals den gesamten Internet-Traffic umleiten. Deshalb müssten die Programme die Daten schon vor Ort filtern und heraussuchen, was von Interesse ist. „Trotzdem ist diese Variante eher ungeeignet, um sehr umfangreiche Datenmengen mitzulesen, wie es für Geheimdienste eher von Interesse sein dürfte", sagt der Informatik-Professor aus Hannover. „Deswegen halte ich sie für unwahrscheinlich."

Für deutsche Geheimdienste gilt das Dementi des DE-CIX übrigens nicht. Zwar äußert sich der Betreiber des German Commercial Internet Exchange dazu nicht. Er dementierte aber einen Spiegel-Bericht auch nicht. Demnach hat der Auslandsgeheimdienst „an den wichtigsten Knotenpunkten für den digitalen Verkehr durch Deutschland eigene technische Zugänge eingerichtet". In Frankfurt unterhalte der Dienst sogar „eigene Räume, um Zugriff auf die Daten zu haben".

Nach dem G-10-Gesetz über Eingriffe in das Brief-, Post- und Fernmeldegeheimnis darf der BND bis zu 20 Prozent der Kommunikation zwischen der Bundesrepublik und dem Ausland auf verdächtige Inhalte prüfen. Das Ausmaß ist in den vergangenen Jahren aber kleiner geworden: 2009 waren es etwa 6,8 Millionen Überwachungsvorgänge, 2011 zirka 2,9 Millionen 2011 und 2012 rund 800 000. Dem US-Geheimdienst NSA wäre ein Mitschneiden des Datenverkehrs dagegen untersagt, wie Bundesinnenminister Hans-Peter Friedrich sagte. „Wenn ein ausländischer Dienst den Internetknoten in Frankfurt anzapfen würde, wäre das eine Verletzung unserer Souveränitätsrechte."

Vor dem Knotenpunkt

Wahrscheinlich laufen die Daten über Glasfaserkabel zum Knotenpunkt in Frankfurt – und nicht über Kupferkabel. Deshalb sind zwei Möglichkeiten denkbar, wie sich der Internetverkehr abfangen lasse, erklären Fachleute: Zum einen könne das Glasfaserkabel aufgeschnitten und ein Splitter eingesetzt werden, sagt Josef von Helden, Informatik-Professor an der Hochschule Hannover. „Dann wird der Datenstrom durch das eigene Gerät geleitet und dabei kopiert", ergänzt Marko Schuba, Professor für Elektrotechnik und Informationstechnik an der Fachhochschule Aachen. Zwar wäre der Datenstrom kurz unterbrochen, während der Splitter eingebaut würde. „Trotzdem muss das Rechenzentrum nicht unbedingt etwas davon mitbekommen, weil kleinere Störungen nicht unüblich sind."

Denkbar wäre auch, das Glasfaserkabel zu biegen, erläutert Schuba. Das Licht folgt zwar größtenteils der Biegung, aber ein Teil strahlt über die Faser hinaus. Mit feinen Sensoren könne dieses Licht aufgefangen werden – und damit ein Teil des Datenstroms. Den Empfänger erreicht trotzdem noch ein ausreichend starkes Signal, so dass er nichts bemerkt. Laut einem Bericht im Fachmagazin KES können die dafür notwendigen Biegekoppler für rund 1000 US-Dollar legal über das Internet bestellt werden.

Allerdings müssten die gesammelten Daten dann direkt gespeichert oder weggtransportiert werden. „Deshalb müssen Sie entweder vor Ort einen Rechner mit einer Festplatte aufbauen", sagt Schuba, „oder ein Kabel verlegen – zu einem eigenen Rechenzentrum in der Nähe. Das wäre wahrscheinlich sinnvoller."

Hinter dem Knotenpunkt

Durch den Aufbau des Internets ist eine dritte Möglichkeit denkbar: Da es aus vielen einzelnen Netzwerken besteht, also aus Leitungen und Rechenzentren, die nicht den Nationalstaaten, sondern vielen verschiedenen Unternehmen gehören, läuft der weltweite Internetverkehr über die Kabel privater Firmen. Allein am DE-CIX in Frankfurt sind mehr als 500 sogenannte Internet Service Provider angeschlossen. Darunter sind zum Beispiel Telekommunikationsfirmen, Betreiber von Breitbandnetzen und Anbieter von Cloud-Diensten.

Würde nun eines der Unternehmen mit dem US-Geheimdienst NSA zusammenarbeiten, könne die National Security Agency unbemerkt die Daten abfangen, die durch die Leitungen der Firma fließen, erklärt Peter Leppelt, Geschäftsführer der Datenschutzfirma Praemandataum. „Dann kann ich als Geheimdienst die Daten kopieren, und niemand bekommt es mit." Deshalb hält auch Josef von Helden, Informatik-Professor an der Hochschule Hannover, diese Variante für „am wahrscheinlichsten". Zwar würden über die Leitungen des Internet Service Providers nur ein Teil der Daten laufen. „Unter Umständen aber ein signifikanter Teil."

Die Betreiber des DE-CIX schließen diese Möglichkeit nicht aus. Im Gespräch mit der Leipziger Volkszeitung hatte Geschäftsführer Harald Summa in der vergangenen Woche an die mehr als 500 Unternehmen erinnert, die mit ihren Leitungen an den Knotenpunkt angeschlossen sind. „Irgendwo hier wird vermutlich auch die NSA zugreifen, denn die Attraktivität für den Dienst liegt auf der Hand."