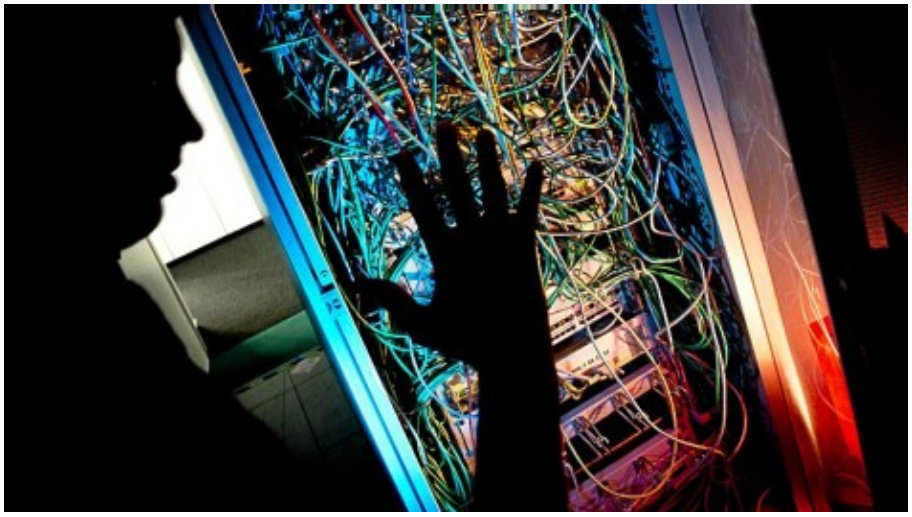
BRAUNSCHWEIGER ZEITUNG

05.07.2013 - 22:21 Uhr

Wer das Kabel biegt, kann Daten abzapfen

Der Ausspähungs-Skandal wirft Fragen nach der Sicherheit im Internet auf. Wir erklären, wie Internet-Nutzer sich gegen Spionage schützen können und wie der Datentransfer überwacht werden kann.



Unser Leser Uwe Rosenkranz aus Braunschweig fragt:

Wie kann es überhaupt gelingen, die Leitungen anzuzapfen, die unsere Telekommunikation übertragen?

Die Antworten recherchierte **Philipp Engel**

Unsere Telekommunikation wird heutzutage zum Großteil über Glasfaserkabel übertragen. Diese können – wie im Fall des britischen Geheimdienstes geschehen – angezapft werden. Dabei ist es aber zunächst wichtig, die Funktionsweise der Kabel zu verstehen:

Unsere Daten liegen auf Computern zumeist als elektrisches Signal vor. Um es per Glasfaserkabel über eine längere Distanz zu transportieren, wird das elektrische Signal mittels einer Lichtquelle, etwa einer Leuchtdiode (LED), umgewandelt. Das Signal breitet sich im Kabel mit Lichtgeschwindigkeit aus und tritt am Ende wieder aus. Hier wird es durch einen Fototransistor registriert und zu einem elektrischen Signal zurückgewandelt.

Alexander Strahl, Physiker der TU Braunschweig, zeigt den Vorgang. Mit einem Laserpointer leuchtet er in ein mehrfach gebogenes Glasfaserkabel, dabei leuchten die Fasern auch am anderen Ende auf. Computer- und Telekommunikationsdaten sind in Glasfaserkabeln eine Abfolge von Lichtblitzen. Die Informationen setzen sich dabei aus zwei Zuständen zusammen: Licht an und Licht aus. Licht an steht für eine eins, Licht aus für eine null. Eine Eins oder Null entspricht einem Bit. Acht Bit stellen ein Byte dar, welches einem Zeichen auf dem Computer entspricht.

Glasfaserkabel bieten die Möglichkeit, mehrere Signale gleichzeitig zu transportieren, denn grob vereinfacht lassen sich verschiedene Wellenlängen gleichzeitig benutzen. Ein Glasfaserkabel kann also vereinfacht dargestellt das Licht eines roten und eines grünen Lasers gleichzeitig übertragen – beide beeinflussen sich nicht gegenseitig.

Allerdings findet auch bei Glasfaserkabeln ein Verlust der Signalstärke statt, denn die Lichtteilchen kollidieren im Faserkern mit kleinsten Unregelmäßigkeiten des Glases. Hier streut das Licht, ein Teil tritt aus – ein Lauschangriff könnte stattfinden.

Theoretisch wäre dafür nur eine lichtempfindliche Manschette nötig, die um die Faser gelegt wird und austretendes Licht ausliest. Dazu müsste ein Angreifer allerdings zuvor das Kabel freilegen, so dass nur die Faser sichtbar bleibt – ein ziemlich filigranes und kompliziertes Vorhaben. Denn die Kabel sind im Erdreich vergraben und mehrere Schutzschichten umgeben die Glasfaser, die üblicherweise so dick wie ein menschlichen Haar ist.

Einen solchen Angriff von außen kann ein Betreiber zudem sicher erkennen, sagt Thomas Gehrke, Physiker und Produktmanager für Glasfasertechnik beim Kabelhersteller Dätwyler aus Augsburg, unserer Zeitung.

„Bei der Inbetriebnahme einer Faserleitung gibt es immer eine Prüfungsmessung. Greift jemand die Leitung an, dann entsteht eine messbare Dämpfung,“, sagt Gehrke. Betreiber könnten die Störstelle sogar auf wenige Meter eingrenzen. Das komme aber eher zur Anwendung, wenn eine Leitung beschädigt werde. „Das kann ein Erdrutsch oder auch ein Haibiss sein“, sagt Gehrke. Dann ist die Eingrenzung wichtig, um nicht kilometerweise Unterseekabel absuchen zu müssen.

Eine andere Methode wäre die komplette Durchtrennung des Kabels. „Da könnte man

einen halbdurchlässigen Spiegel zwischenschalten, der einen Teil des Lichts reflektiert“, sagt Strahl. Das ursprüngliche Signal laufe normal weiter, während ein Teil davon auf einen anderen Weg geschickt wird. Das allerdings würde einem Netzbetreiber wohl erst recht auffallen – und es wäre technisch noch schwerer umsetzbar.

Es ist ohnehin unwahrscheinlich, dass der britische Geheimdienst mit U-Boot und Tauchern am Meeresboden die transatlantischen Datenkabel angezapft hat. „Am einfachsten wäre es, an die Messbuchse zu gehen, die an Land steht“, erklärt Gehrke. Denn dort laufe ja auch der komplette Datenverkehr hindurch. „Wer im Raum, in dem das aktive Equipment steht, die Messbuchse anzapft, könnte das Signal duplizieren und dann weiterleiten.“

Das bliebe zwar nicht unbemerkt, aber wenn die US-Behörde NSA Konzerne wie Google und Facebook dazu zwingen kann, Daten herauszugeben, dann ist es denkbar, dass die Briten mit dem Wissen der Netzbetreiber Daten saugen, mutmaßt Gehrke.

Vorstellbar wäre auch ein Angriff an einer anderen Stelle, etwa in der Nähe der Koppelstelle des Kabels, so der Experte. Alle Landverbindungen münden letztendlich in eines der Unterseekabel – und zwar noch an Land. Wer hier das Hauptkabel anzapft, hat ebenfalls Zugriff auf den kompletten Datenstrom – ohne komplizierte Tauchgänge.

Unser Leser Christopher Pfeiffer aus Braunschweig fragt:

Ist es für normale Nutzer möglich, im Internet und per Mail zu kommunizieren, ohne dass Geheimdienste mitlesen können? Wie kann man sich dem entziehen?

Wer seine Privatsphäre im Internet schützen will, der ist bei Hacker-Vereinen (Selbstbezeichnung: Hackerspace) an der richtigen Adresse. „Hacken“ meint ursprünglich nichts Illegales, sondern bezeichnet das Probieren und Verbessern von Technik im gesetzlichen Rahmen.

Vincent Breitmoser, Vorsitzender des Braunschweiger Vereins, erklärt die Problematik bei der Telekommunikation: „Das liegt in der Struktur des Netzes begründet: Ist eine Daten-Autobahn voll, dann nehmen die Datenpakete einen anderen Weg.“ So könne eine Verbindung von Wolfsburg nach München über Server im Ausland geleitet werden – wo dortige Geheimdienste zugreifen könnten.

Das Anzapfen der transatlantischen Kabel befähigt die Geheimdienste sogar dazu, schlicht jedes Datenpaket abzugreifen, das über eine bestimmte Leitung läuft.

Absolute Sicherheit gibt es laut Experten nicht. Selbst viele Verschlüsselungen sind unsicher. Breitmoser nennt Skype als Beispiel, ein Programm, mit dem Nutzer im Internet telefonieren und Nachrichten austauschen können. „Dort ist im

Nachrichtenfenster ein kleines Schloss-Symbol zu sehen. Das bedeutet, dass die Daten verschlüsselt gesendet werden“, sagt Breitmoser.

Problem: Der Absender schickt ein Datenpaket an den Server von Skype. Dort werden die Daten entschlüsselt und neu verschlüsselt an den Empfänger weitergesendet. „Skype kann die Klardaten also einsehen – trotz Verschlüsselung“, sagt Breitmoser.

Zwar geschehe das nur auf dem Server des Unternehmens, aber Skype gehört zu Microsoft – und Microsoft gibt laut Whistleblower Edward Snowden Daten an den US-Geheimdienst NSA weiter. Theoretisch kann also die NSA mitlesen – trotz Verschlüsselung. Das Szenario lässt sich auf diverse Internet-Dienste ausweiten.

Größtmögliche Privatsphäre ist bei E-Mails gegeben, wenn die Mail beim Absender verschlüsselt und erst beim Empfänger wieder entschlüsselt wird – und keine Zwischenstation die Daten einsehen kann. Dafür nennt Breitmoser verschiedene Methoden. Am geläufigsten sei die symmetrische Verschlüsselung: Der Absender erstellt ein Passwort und nur damit kann die Mail entschlüsselt werden. Bleibt die Frage, wie das Passwort sicher übermittelt werden kann. „Am sichersten ist, sich zu treffen und das Passwort ins Ohr zu flüstern“, schmunzelt Breitmoser.

Sicherer ist laut dem Experten die asymmetrische Verschlüsselung, bei der zwei zueinander passende Schlüssel eingesetzt sind. Das Problem mit der sicheren Schlüsselweitergabe entfällt.

Damit die Verschlüsselung lückenlos ist, muss das E-Mail-Programm auf dem heimischen Computer installiert sein. Gängige Programme dafür heißen Outlook oder Mozilla Thunderbird.

Viele der Programme, die wir rund um das Internet benutzen, gelten als unsicher. Eine Übersicht von als sicher geltenden Alternativen gibt es unter: http://prism-break.org/#de.

http://www.braunschweiger-zeitung.de/debatte/antworten/wer-das-kabel-biegt-kann-daten-abzapfen-id1070288.html