Neueste Technik macht sogar Lichtleiter sicherheitskritisch

Glasfaserkabel nicht abhörsicher

Lange Zeit galten Glasfaserkabel als quasi abhörsicher. Doch die Zeiten ändern sich, und der alten Behauptung weichen neuere Erkenntnisse, dass auch die Lichtwellenleiter in höchstem Maße sicherheitskritisch und angreifbar sind.

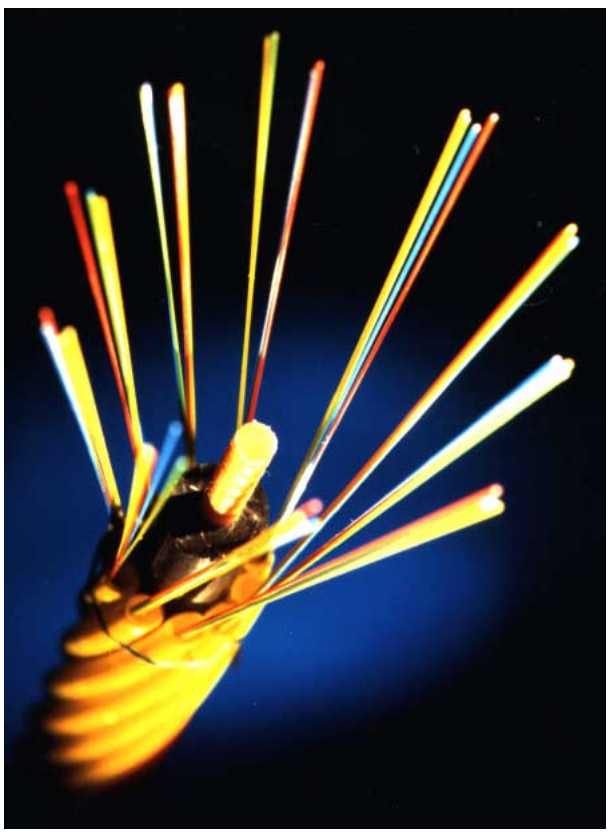
Das Abhören von Telefonaten durch die Nachrichtendienste hat lange Tradition. Zu Beginn der siebziger Jahre sollen die USA damit begonnen haben, mit einem ihrer U-Boote ein auf dem Meeresgrund vergrabenes Kabel der russischen Nordmeerflotte vor der Halbinsel Kamtschatka abzuhören. Die besten Lauschergebnisse hätten die Amerikaner an den Relaisstationen gehabt, die der Signalverstärkung dienten. Das erfolgreiche Lauschen ist per Induktion ziemlich simpel und ähnelt den Saugnapf-Mikrofonen der damaligen Zeit zum Mitzeichnen von Gesprächen in Büros direkt vom Telefon.

Die Spionagetechnologie wurde fortentwickelt und führte zu Methoden, bei denen die Gespräche bis zu einem Jahr durch Abhöreinrichtungen aufgezeichnet werden konnten. Die Spionage-U-Boote mussten die Aufnahmen dann nur noch regelmäßig abholen.

Ebenso gilt es als sicher, dass seit etwa 20 Jahren auch die Seekabel zwischen Europa und Afrika im Mittelmeer von den USA belauscht werden. Inzwischen sind jedoch die alten Kupferkoaxialkabel durch moderne Glasfaserkabel ersetzt worden und damit ist auch das Belauschen zumindest per Induktion hinfällig geworden.

Lauschen mit neuer Technik

Glasfaserkabel übermitteln Telefonate und Datenübertragungen mittels optischer Signale. Gerhard Schmid, der Verfasser des Berichtes über das Spionagesystem Echolon für das Europäische Parlament, hält in seinem Dossier nur die Glasfaserkabel der älteren Generation für angreifbar, weil sie noch mit induktiven Zwischenverstärkern arbeiten.



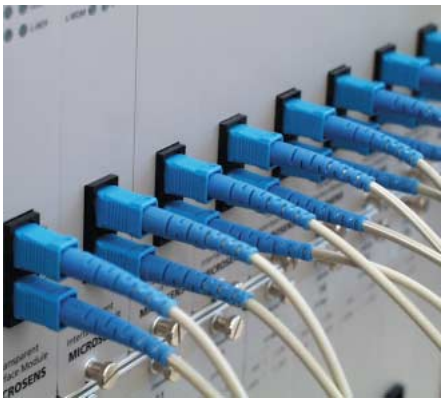
Die Leistungsfähigkeit ist enorm: Jede Glasfaser in diesem Kabel kann 41 Millionen Telefonate übertragen.

Doch auch die modernen Kabel mit einem Erbiumlaser zur Verstärkung sind nach neuen Erkenntnissen ein Sicherheitsrisiko. Aufgeschreckt wurden viele Sicherheitsexperten erst durch die vom „Wall Street Journal“ verbreitete Nachricht, dass der amerikanische Geheimdienst National Security Agency [1] einmal mehr mit Hilfe von U-Booten nun auch Glasfaserkabel anzapfen möchte. Funktionieren soll das mit dem Atom-U-Boot „USS Jimmy Carter“.

Angeblich soll das bald unter Milliardenaufwand aufgerüstete U-Boot sogar in der Lage sein, Glasfaserkabel zu durchtrennen, um Gespräche mitzuschneiden, ohne dass dies den Betreibern auffallen würde. Das klingt selbst für Experten der Materie sehr unwahrscheinlich, eher nach Science-Fiction.

Dauer-Datenverlust

Bekannt und bewiesen ist dagegen eine andere Methode,



Anschlussleiste für Glasfaserverbindungen Quelle: Microsens

Glasfaserkabel ganz ohne mechanisches Zutun anzuzapfen. Wird ein Glasfaserkabel gebogen, geht ein Teil der optischen Informationen verloren. Die Daten verlassen zu geringen Teilen ganz unfreiwillig ihren vorbestimmten Weg, weil sie nicht vollständig der Biegung folgen können. Und selbst bei einem ideal verlegten Kabel strahlt ein geringer Teil der optischen Informationen nach außen. Dies hat physikalische Ursachen und beruht auf dem Dämpfungsmechanismus der so genannten Rayleigh-Streuung, die sich wegen im Glas enthaltener mikroskopischer Dichteschwankungen entwickeln kann. Vor allem aus Gründen der Thermodynamik lassen sie sich nicht vollständig elimieren.

Das nach außen tretende Licht kann mit Hilfe von Sensoren aufgefangen, verstärkt und anschließend mitgelesen und ausgewertet werden.

Die Deutsche Telekom AG [2] hat inzwischen beim Europäischen Patentamt [3] ein Verfahren angemeldet (EP 09153566A1), das auf die-

Kabelmuffe in einem Stadtnetz der Colt Telecom. Hier laufen sämtliche Glasfaserkabel zusammen. Quelle: Colt Telecom

ser Erkenntnis beruht und mit dem sich „Signale aus einer Glasfaser“ auffangen lassen, ganz ohne jeden Nachweis für den Empfänger und ohne Schwächung des Signals. Wer etwas Bestimmtes sucht, hat es also auch nicht viel schwerer als zu Zeiten des Kupferkabels. Die Daten werden im heutigen Zeitalter vergleichbar einer E-Mail mit einem „Header“ zur Identifikation gesendet.

Anzapfen an Land bevorzugt

Insider halten das Anzapfen per U-Boot für übermäßig aufwändig, da die Unterseekabel alle gut geschützt sind, weniger wegen möglicher Lauschangriffe als vielmehr vor natürlichen „Angriffen“ der Natur.

An Land gibt es allerdings einen ganz einfachen Zugang. Überall sind zwischen die Kabel-Verbindungspunkte Koppler und Verstärker geschaltet, die als besonders angreifbar gelten. Die Grundausrüstung dafür gibt es für etwa 1.000 Euro bei der Canadian Instrumentation & Reserch Ltd. [4] zu kaufen. Und der Weg zum nächsten Glasfaserkabel ist nun wirklich nicht weit. In öffentlichen Gebäuden laufen sie in Kellern zusammen, man findet sie in U-Bahnschächten großer Städte und mitunter sogar in stillgelegten Gasleitungen. Meist verfügen die Netzschaltpunkte auch über keine speziellen Sicherungssysteme. Man braucht nur einen Vierkantschlüssel.

Licht ins Dunkel möglicher Abhörversuche bringen die Netzbetreiber nicht, sind sie doch daran interessiert, dass derartige Fälle nicht publik werden. Ganz im Gegenteil: Schweigen ist Gold. Die Studie „Computerspionage – Risiken und Prävention“ von Karl-Friedrich Fecht, Walter Opfermann, Wolfgang Scheiterle, alles Mitarbeiter des Landesamtes für Verfassungsschutz Baden-Württemberg, kommt zu dem Schluss, dass die Angriffe zumeist unbemerkt erfolgen, „d. h. es ist von einer sehr hohen Dunkelziffer (ca. 85 %) auszugehen. [...] Die Sicherheit in öffentlichen Netzen ist vor allem durch Abhörangriffe, Manipulationen von Daten und Systemen, Wiederholen, Verzögern oder Verändern von Informationen, Vortäuschen falscher Kommunikationsverbindungen oder Partner sowie durch physische Angriffe auf die Verbindungen und Kommunikationseinrichtungen selbst erheblich gefährdet.“

Hier laufen alle Glasfaserkabel der Hansenet zusammen. Ein Anzapfen der Leitungen für Fremde ist an dieser Stelle allerdings nicht möglich.

BSI rät: Verschlüsseln!

Beim Bundesamt für Sicherheit in der Informationstechnik [5] bezweifelt auch Pressesprecher Michael Dickopf nicht, dass sich Lichtwellenleiter prinzipiell anzapfen lassen, allerdings ist das nur „mit sehr hohem technischen Aufwand möglich und keineswegs unauffällig. Man müsste schon mit ein paar Koffern vorfahren, denn gerade die Auswertung der ungeheuren Datenmenge von etwa 1 Gigabyte Durchsatz pro Sekunde lässt sich nur schwer bewältigen.“ Ein System zur Absicherung von Leitungen ist nach seinem Kenntnisstand bisher noch nirgendwo im Einsatz, und daher empfiehlt er trotz des geringen Risikos eine Verschlüsselung. Auch die Bundesverwaltung nutze eine solche im „Informationsverbund Bonn–Berlin“, um ganz sicher zu gehen.

Bei der Deutschen Telekom möchte man die Möglichkeit zum Abhören ebenfalls nicht vollständig ausschließen, aber keine näheren Angaben machen, abgesehen davon, dass die eigene Infrastruktur durch spezielle Schließsysteme an den Netzschaltpunkten gesichert sei und das eigene Netzwerk regelmäßig überprüft werde.

Ebenfalls sehr zurückhaltend äußert sich Volker Isenmann, Pressesprecher der konkurrierenden Colt Telcom [6]. Fälle von Abhörversuchen der eigenen Netze seien nicht bekannt, aber über Details und Sicherheitskonzeptionen möchte man keine Auskunft geben, nur soviel: „Grundsätzlich sind alle unverschlüsselt übertragenen Signale abhörbar, egal, ob es sich um Glasfaser, Kupferkabel, Mobilfunk oder alle anderen Arten von Funkwellen handelt. Das Abhören einer Glasfaserverbindung ist technisch und logistisch aber enorm aufwändig und nur unter bestimmten Voraussetzungen möglich, die bei Colt Telecom nicht gegeben sind.“

Auch die Studie „Computerspionage – Risiken und Prävention“ kommt zu dem Schluss, dass einzig die Verschlüsselungstechnik heute sicheren Schutz vor unbefugtem Mitlesen bietet: „Neben standardisierten Netzsicherheitskonzepten auch in öffentlichen Netzen, die zumindest einen Grundschutz für alle Teilnehmer gewährleisten, müssen die eigenen Kommunikationseinrichtungen für den Anschluss an Netze gegen Sabotage und Spionage gesichert werden. Die Informationen selbst können nach dem Stand der Technik nur durch Verschlüsselung vor unbefugtem Mitlesen geschützt werden.“

Niels Gründel

Tipps: Sicher verkabeln

Wer Glasfaserkabel im eigenen Gebäude verlegt und sichergehen will, dass es niemandem besonders leicht gemacht wird mitzulesen, sollte nachfolgende Schutzmaßnahmen beachten.

- Glasfaserkabel sollten so verlegt werden, dass keine abhörbaren Schlaufen entstehen und Zugriffe erkennbar werden, daher nur eine Verlegung in abgeschlossenen Verlegesystemen bei regelmäßigen Kontrollen vornehmen, keine Stecker verwenden, keine Abzweigungen vornehmen, keine anderen Anschlüsse als die betriebsnotwendig vorhandenen einrichten.
- Anfang und Ende des Lichtwellenleiters in geschützten Sicherheitsbereichen platzieren.
- Verlegesysteme (Kabelkanäle) sollten gesichert, also abschließbar und verplombt, in nicht leicht zugänglichen Bereichen wie einer abgehängten Flurdecke oder in leicht zu kontrollierenden Bereichen wie Büros eingesetzt werden.
- Aktive Netzkomponenten sind gegen unbefugten Zugriff besonders zu schützen und immer in gesicherten Räumen unterzubringen.

Zum Weiterlesen

[1] National Security Agency, www.nsa.gov

[2] Deutsche Telekom AG, www.dtag.de

[3] Europäisches Patentamt, www.europarl.de

[4] Canadian Instrumentation & Reserch Ltd., www.cirl.com

[5] Bundesamt für Sicherheit in der Informationstechnik, www.bsi.bund.de

[6] Colt Telcom, www.colt.de