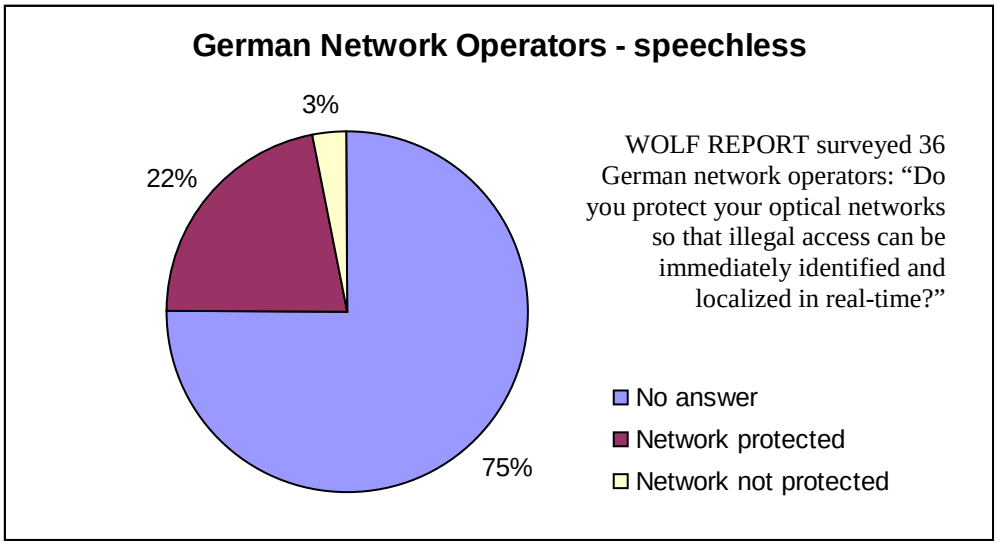
WOLF REPORT
executive facts

Top Story: Why businesses are inadequately protected from eavesdropping and data-theft.

March 2003, Wolfgang Müller-Scholz
[Original Article from the Wolf Report in German Language at www.wolf-report.com]

The Silent Conspiracy

Security. Discrete telephone calls, secret faxes and confidential emails are for easy prey for industrial spies – even in modern fiber optic networks. Deutsche Telekom, ARCOR and others, however, leave their customers in the dark.



Melbourne, Florida. This experiment applies to every decision-maker: In a secret U.S. electronics laboratory, the Head of Engineering, Bill Rock (name changed), demonstrates how simple it is to tap into an optical fiber: He clamps a fist-size tapping device to a cable running a live video conference. There is no tell-tale flicker or crackle on the display. The micro-bending tap – EXFO model FCD-10B – transmits the video conference in flawless quality on the spies' laptop. "Just a little light is enough to fully copy even the biggest volumes of data, such as live video, completely unnoticed.

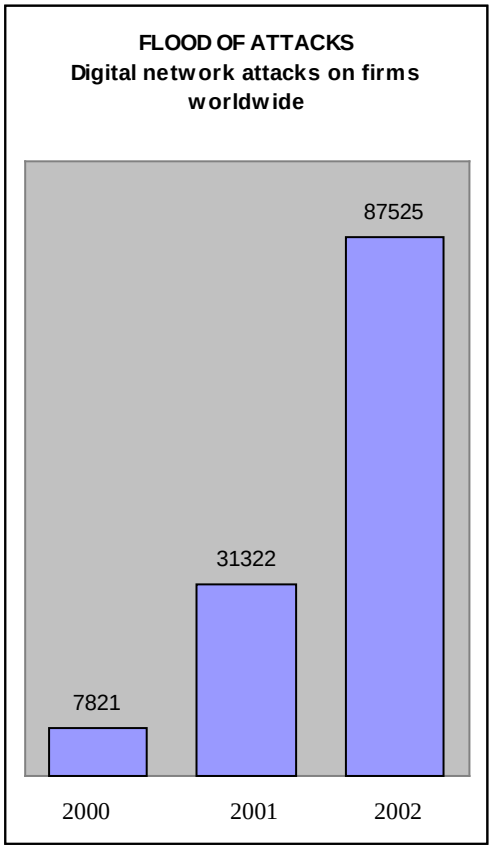
The eavesdropping of fiber optic cables, the primary telecommunication veins, is much easier than previously believed. It is even more easy for industrial spies to simply copy faxes containing secret figures or the telephone conversations of the Board of Directors than it is to steal data-intensive video: The perpetrator needs only the fax number, telephone number or Internet IP-address. The messages are filtered out and decoded by means of such

identifying numbers. Eavesdropping devices (from approximately $1300 on up) and software are widely available for purchase and optical cable routes are widely accessible. “Most transmissions are sent unencrypted and codes are breakable anyway”, explains Seth Page, CEO of Oyster Optics, Inc., a U.S. firm, which develops security electronics.

How secure are German fiber optic networks? WOLF REPORT surveyed 36 network operators – und came across a surprising silence: three-fourths didn’t answer the survey. “That would be too critical of us”, whimpered ARCOR as an example. Only one carrier showed courage and conceded under the condition of anonymity, that their network was poorly protected. Only eight regional network operators believed their cables to be adequately prepared against illegal attacks: Berlinkomm, Ewetel, Heag Medianet, Lambdanet, MDCC Magdeburg, Netkom, Netcologne as well as the Tropolys-Group. And what about Deutsche Telekom? Like most of the others they evaded a concrete answer to the security question, but conceded nonetheless: “The possibility of eavesdropping is not completely excluded”.

But the huge Deutsche Telekom network is exactly the one most suffering from network attacks: For years the STASI snooped around the Berlin-Bonn fiber optic route. At the beginning of 2000 the Supervisory Board of Deutsche Telekom was busy with the security of the high-tech network at the Frankfurt Airport after culprits gained access to the three main fiber trunk lines. The former monopoly knows the explosiveness of the situation: In 1999 they had already secured European patent number EP 0915356 A1, which enables the eavesdropping of optical fibers without even the diversion of light. This simplified the localization of network problems for their maintenance technicians. Criminals can utilize the technology just as well, however, for undetectable eavesdropping.

The threat has become critical: eavesdropping of data and telephone communications of businesses increased 10-fold in the past two years. In 2002 a solid 5,300 cases in Germany alone were registered by the London-based market research institute *mi2g*. That means that worldwide Germany ranks number fourth place after the U.S.A (first place with 32,434 cases), Brazil and Great Britain.



The economic damage is immense: Every data attack costs firms between $150,000 to $400,000 according to a study by the F.B.I. and the American Society for Industrial Security. The German Office for Security of Information Technologies (BSI) currently calculates a more conservative €25,000 per case.

That is theory. In reality it is swarming with multiple attacks where the aggregate damage per company per year is up to $50 million according to the F.B.I.

Secret service organizations also intervene: French agents were thus able to obtain the bid numbers from the network of a U.S. aircraft manufacturer and pass it along to the competition at home. In turn they underbid the U.S. offer by a hair and won the billion dollar contract. “In particular bids for Request-for-Proposals (RFP’s) are intensively tapped”,

knows Roland Bopp, Executive Vice President of Hochtief Inc. in New York, and an ex-Manager at both Mannesmann and Deutsche Telekom.

Even cruder money theft through network attacks is on the rise: In the summer of 2002 unknown persons diverted more than $1 million into their accounts online from a New York Bank; at the same time at the network manufacturer Cisco, two accountants broke into the corporate computer and transferred stock worth over $8 million to their private accounts.

Market traders proceed even more brazenly in order to tap into insider-information: Recently security forces in the U.S. discovered an illegally installed eavesdropping device in Verizon's optical network. It was placed at a mutual fund company – shortly before the release of their quarterly numbers. Investigators speculate that terrorist seeking to fill their pockets with stock market profits may be the culprit.

Most of the time culprits clamp their fiber-bending-tap directly onto the optical lines of a firm. From all the flowing data and voice packets, special software such as E-Sniff makes unnoticed copies based on the desired recipient's known identification number. Unencrypted packets such as telephone calls, emails or faxes are read immediately. High-tech computers break most encrypted data within a few hours anyhow. More stringent protective-barriers are often countered by the intruder with even better attack techniques. "The ever increasing race between the cat and the mouse", remarks Bernd Schmidbauer, ex-Secret-Service Coordinator of the German National Government.

How business can help themselves: Encrypt the data with especially long codes – if possible use an asymmetrical 1024-bit key. Ever more secure are physical methods, which change the light signals and at the same time identify illegal attacks (For example: U.S. Patent # 6,469,816). Such protection has its price however: Some network integration is around 5 to 15 percent more expensive.

Network Checklist for Decision-Makers

1. Ask your provider of communications services if their optical network is protected against illegal access: with across-the-board physical protection (approximately 80 cm underground, coated, protected routes) in addition to electronic alarms.

2. Dig deep to find out if technologies are in place that "identify and localize in real-time unauthorized access everywhere in the network, at-any-time and immediately". Only if the provider guarantees this in writing can you be relatively sure that telephone calls, faxes and computer data can't be illegally tapped.

3. Let your telecommunications carrier certify in writing that they meet the required Paragraph 87 of the German Telecommunications Law (TKG) for suitable technical precautions or other measures for the protection of the telecommunications and data processing systems against unauthorized access and outside attacks. Thereby the telco must take the state-of-the-art technical developments into consideration – such as patents EP 0915356 A1, US 6,469,816 B1 and US 6,476,952 B1. They should also have appointed a security representative and developed a security plan.

4. If your network operator isn't prepared to take such steps then one must fear that no such protections exist. You should contact competitive, more regional providers. They operate more

manageable systems and are more trusted with higher security standards such as banks. (Further details on this subject – formulated in an applicable and consistent manner – are available to subscribers for free at www.wolf-report.com)

Wolf K. Müller Scholz is known in business journalism as a distinguished aficionado of the global high-tech industry. For many years he covered this area – amongst others as long-term department head, columnist and U.S.A.-correspondent for the business magazine *Capital*.

Wolf K. Müller Scholz is author of the bestseller "Inside Silicon Valley" – the only non-American book worldwide about the industry, research and financing branches of the business-center of the American West. In additional he is a sought-after lecturer, moderator and discussion partner at business events on both sides of the Atlantic.

Wolf K. Müller Scholz was born in 1957 in Hamelt. He studied economics, sociology and communications and finished his M.A. in Marburg with honors. As a business journalist Wolf K. Müller Scholz worked from 1985-1989 on the corporate magazine *Nord-Handwerk* in Hamburg. Between 1989-2002 he was active with *Capital Magazine*, including five years as department head in Cologne. From 1997 to 2002 he reported for *Capital* from the U.S.A. Since March 2003 he is the publisher and chief-editor of the WOLF REPORT.