Abgeschirmte Messkabine
„Das Spionagerisiko steigt“

COMPUTER

Datendiebstahl aus der Luft

Jeder Monitor ist ein Sender: Auch moderne Bildschirme von Laptops lassen sich ohne großen Aufwand belauschen.

Von außen wirkt die Szene unauffällig. Ein roter VW-Bus steht am Straßenrand im Industriegebiet von Diepholz, geparkt vor dem Büro eines mittelständischen Betriebs. Die Autoscheiben sind getönt. Im Auto starrt Lars Friedrichs, 29, auf einen Schwarzweißmonitor. „Gleich hab ich ihn“, flüstert der blonde Mann mit dem jungenhaften Aussehen.

Er hat eine Antenne auf das Büro gegenüber gerichtet. Feinfühlig wie ein Harfenist bedient er mit dem rechten Zeigefinger die Schalter, die aus einem nackten Platinenbausatz ragen – das experimentelle Steuerungsmodul für seinen Empfänger. Plötzlich, bei 618,7 Megahertz, erscheint das Abbild einer Benutzeroberfläche auf dem Schirm vor ihm, schwarzweiß und leicht verwaschen wie ein Bild von Gerhard Richter. Eine lange Excel-Preistabelle flimmert auf, die wie von Geisterhand um weitere Einträge ergänzt wird. Wort für Wort kann Friedrichs mitlesen, was im Büro gegenüber getippt wird.

Die Spionageattacke ist nur eine Demonstration dessen, was möglich ist. Friedrichs arbeitet für die Computersicherheitsfirma GBS seines Vaters.

Der Besitzer des bespitzelten Rechners staunt nicht schlecht, als Friedrichs ihm den Datenklau vorführt. Auch Uwe Claaßen hat dabei zugesehen: Er ist beim Verfassungsschutz Niedersachsen für das Thema Wirtschaftsspionage zuständig.

„Es gibt keine zuverlässigen Zahlen, wie viele Firmen mit dieser Methode ausspioniert werden“, berichtet Claaßen, „denn im Gegensatz zu Einbrechern oder Computerviren hinterlassen diese Angriffe keine Spuren. Wer kann schon sagen, ob letzte Woche vielleicht ein unauffälliger Lieferwagen vor der Tür geparkt war?“

„Tempest“ – so nennen Fachleute die Ausnutzung dieser Lücke in der Datensicherheit: Kaum ein Computernutzer weiß, dass jeder Bildschirm wie eine Antenne wirkt und elektromagnetische Pulse ausstrahlt. Wer diese Abstrahlung mit einer Antenne aus der Luft fischt und am Computer wieder zusammenpuzzelt, kann den Spitzelfunk nutzen, um sich in Ruhe mit vertraulichen Daten berieseln zu lassen.

Je nachdem wie viele störende Signale dazwischenfunken, könnte ein Bildschirmspion noch aus hundert Meter Entfernung durch die Scheiben eines Hochhausturms hindurch verfolgen, welche Firmenstrategie etwa ein Vorstandsvorsitzender gerade diktiert hat. Die Reichweite hängt dabei von vielen Faktoren ab, unter anderem von der Luftfeuchtigkeit. „Schwülwarme Sommertage sind ideal, weil die Luft dann gut leitet“, sagt Friedrichs.

Eigentlich ist Tempest (was so viel wie Sturm bedeutet) nichts Neues. Schon in den achtziger Jahren streunte der niederländische Wissenschaftler Wim van Eck mit einem von ihm entwickelten Spezialgerät durch Londoner Büroviertel, um den tückischen Sendereffekt öffentlichkeitswirksam zu beweisen.

Fieberhaft rüsteten daraufhin Militärs, Geheimdienste und Diplomaten ihre Büros auf, um die verräterische Streustrahlung zu blockieren – oder sie selbst für Spionagezwecke zu nutzen. Bald boomte eine ganze Tempest-Industrie mit schätzungsweise über einer Milliarde Dollar Jahresumsatz bereits im Jahr 1990.

Doch dann ließ das Interesse nach. Das Problem schien sich erledigt zu haben, weil neue Flachbild-Displays die strahlungsintensiven Kathodenstrahlröhren ersetzten. Doch nun zeigt sich: Das war ein Irrtum. „Auch Notebooks lassen sich sehr gut abhören“, sagt Friedrichs. Denn die Kabel, vor allem die von der Platine zum Bildschirm, wirken wie leistungsfähige Sender.

Rund tausend Euro verlangt Friedrichs dafür, einen Bildschirm abhörsicher zu machen. Bislang kamen seine Kunden vor allem aus dem militärischen Bereich; doch neuerdings wollen auch immer mehr Privatfirmen ihre Rechner härten lassen. In einer strahlungsisolierten Messkabine, die mit schweren Ferrit-Kacheln tapeziert ist, bastelt er so lange herum, bis der ungewollte Sender verstummt.

„Das Spionagerisiko steigt schon deshalb, weil die Bauteile und die Software billiger werden“, sagt der Computerwissenschaftler Markus Kuhn, der an der Universität Cambridge als Dozent lehrt. „Was früher so teuer war, dass es sich nur Geheimdienste leisten konnten, kann man heutzutage für ein paar tausend Euro zusammenbauen.“

Der gebürtige Münchner berät Friedrichs und hat auch die Steuerelektronik für sein Spitzelgerät gebaut. Immer wieder scheucht Kuhn die Fachwelt mit neuen Aufsätzen zum Thema auf. Derzeit erforscht er beispielsweise, wie sich auch Chip-Karten abhören lassen, wenn ihre Datensätze etwa am Geldautomaten auf die Straße hinausgepustet werden. Im Herbst will er seine Ergebnisse vorstellen.

Derlei Szenarien sind gut für Friedrichs' Geschäfte – er lebt von der Angst seiner Kunden. Die Firmen stehen Schlange: 6000 Geräte soll er innerhalb des kommenden Jahres abhörsicher machen.

HILMAR SCHMUNDT

JÖRG OBERHEIDE

Computerexperte Friedrichs: *Lauschangriff im VW-Bus*