2004/50 Inland

https://shop.jungle.world/artikel/2004/50/black-box-brd

Black Box BRD

Von **Carsten Schnober**

Der Staat hat die großen Internet-Provider verpflichtet, ihm ab 1. Januar die Überwachung ihrer Kunden zu erleichtern. von carsten schnober

Nach wie vor gilt das Internet als schwer kontrollierbar. Der große Lauschangriff stutzte das Post- und Fernmeldegeheimnis auf ein selbst für Otto Schily und Günther Beckstein erträgliches Maß zurecht, doch beim Überwachen der elektronischen Kommunikation tun sich die Behörden immer noch schwer. Das liegt weniger an juristischen Schranken als am erforderlichen technischen Aufwand. Doch eine Lösung ist in Sicht: Die Telekommunikationsüberwachungsverordnung (TKÜV) verpflichtet Internet-Provider ab 1. Januar dazu, die Hilfsgeräte zum lückenlosen Belauschen ihrer Kunden selbst bereitzustellen.

Einige Anbieter bitten ihre Kunden mit einer einmaligen Zusatzgebühr zur Kasse, um die Abhöreinrichtung zu finanzieren. Denn der Staat gibt sich nicht mit dem Billigsten zufrieden: Auf 10 000 bis 50 000 Euro beziffern Provider die Kosten für die Anschaffung und Installation einer Box, die das Abhören per Knopfdruck ermöglicht. Auch um die Wartung und Reparatur der Geräte sollen sie sich kümmern.

Anbieter von E-Mail oder anderen Kommunikationsdiensten im Internet kommen um diese Ausgabe nur herum, wenn sie weniger als 1 000 Kunden betreuen. Alle anderen müssen die Boxen bereitstellen, auch wenn nach dem Ende des Internet-Booms ihre Kassen meist nicht mehr so prall gefüllt sind. Die inzwischen hart umkämpften Kunden wollen sie nach Möglichkeit nicht mit Zusatzgebühren fürs Abhören verprellen.

Wie die elektronische Überwachung funktioniert? Die betroffenen Provider schließen die Abhörboxen an die Server an, auf denen die E-Mail-Konten oder andere private Daten ihrer Kunden liegen. Die Boxen bieten eine Schnittstelle, über die sich Ermittler via Internet direkt in den Datenverkehr einklinken können. Die Staatsschützer brauchen also ihr Büro nicht mehr zu verlassen, um auf die persönlichen Daten der meisten deutschen Internet-Benutzer zuzugreifen. Richterlicher Kontrolle unterliegen Verfassungsschutz, Bundesnachrichtendienst (BND) und Militärischer Abschirmdienst (MAD) dabei nicht: Den Behörden genügt ein »konkreter Anhaltspunkt«, der auf eine schwere Straftat oder deren Planung hindeutet, um eine Abhörmaßnahme eigenständig und legal durchführen zu dürfen.

Das ist zwar nicht neu, doch bislang müssen die Sicherheitsbehörden die Provider per Anordnung zur Mitarbeit anhalten. Künftig werden die Internet-Anbieter von einem Lauschangriff

genauso wenig erfahren wie die Abgehörten.

Neben Firmen mit weniger als 1 000 Kunden bleiben auch reine Internet-Zugangsanbieter verschont von der Abhörbox. Wer seine Kunden ausschließlich mit dem Internet verbindet, ohne ihnen Zusatzdienste wie E-Mail-Adressen zu vermitteln, leitet Daten lediglich weiter, ohne sie zu speichern. Solche Provider werden ebenso wie Telefonanbieter behandelt: Sie müssen zwar bei staatlichen Lauschaktionen kooperieren und die Kosten tragen, aber keine dauerhafte Abhörschnittstelle bereitstellen. Auch verpflichtet die TKÜV nur öffentliche Anbieter zur präventiven Mitarbeit. Firmen und Privatpersonen, die nur ihren Angestellten oder Freunden E-Mail-Konten zur Verfügung stellen, sind von der Pflicht befreit.

Eine Grauzone eröffnet die TKÜV bezüglich der 1 000-Kunden-Grenze, da die Wiederverkäufer, die so genannten Reseller, nicht genau definiert sind. Zwar setzt die Verordnung natürliche und juristische Personen gleich, doch ergibt sich aus dem Text nicht, ob auch die Kunden der Kunden mitzählen. Wäre dem nicht so, könnte eine solche Situation entstehen: Ein großer Anbieter versorgt einige hundert Reseller. Diese verkaufen die Internet-Dienste wiederum jeweils an einige hundert Kunden; das Spiel lässt sich beliebig weitertreiben. Hätte keiner der einzelnen Zwischenhändler mehr als 1 000 Kunden, kämen sie allesamt ohne Abhörbox durch.

Wenig Klarheit bringt das Telekommunikationsgesetz (TKG), auf dem die TKÜV hauptsächlich fußt, in dieser Angelegenheit. Es definiert Teilnehmeranschlüsse als physische Verbindungen in die Räume des Kunden. Das würde allerdings bedeuten, dass Wiederverkäufer, die einen Server in den Räumen ihres Anbieters angemietet haben, mitsamt ihren Kunden grundsätzlich nicht mitzählten. Ob solche Spitzfindigkeiten vor Gericht bestehen können, wird aber erst ein rechtskräftiges Urteil endgültig klären, und nur wenige Anbieter dürften eine Verurteilung riskieren. Denn eine Geldbuße von 500 000 Euro droht Providern, wenn sie bis zum 1. Januar 2005 keine Abhörbox vorweisen können, obwohl sie dazu verpflichtet wären.

Es wird Internet-Anbieter und -Nutzer kaum trösten, dass die Verpflichtung, Abhörgeräte zu installieren, seit fast drei Jahren bekannt ist. Bereits Anfang 2002 trat die TKÜV in Kraft, gewährte den Providern aber eine Frist, um die Technik einzurichten. Diese Schonfrist endet mit Beginn des kommenden Jahres.

Bereits seit 1998 legt das Telekommunikationsgesetz (TKG) die Finanzierung staatlicher Überwachungen in die Hände der Anbieter. Die TKÜV sollte lediglich die praktische Umsetzung definieren, die Abhörboxen stellte die Regierung infolgedessen als technisches Detail dar.

Doch erst durch sie entsteht eine flächendeckende Infrastruktur, die fast alle Internet-Provider Deutschlands dauerhaft unter staatliche Überwachung stellt. Die Behörden kommen damit buchstäblich per Knopfdruck an die E-Mail-Konten innerhalb ihres Hoheitsgebiets. Wie wenig Gehalt die erforderlichen »konkreten Anhaltspunkte« in der Praxis häufig bieten, zeigten schlecht begründete Abhöraktionen in der Vergangenheit oft genug. In die Verlegenheit, solche Maßnahmen zu rechtfertigen, dürften Ermittler wegen der geringen Kontrollmöglichkeiten künftig jedoch noch seltener kommen.

Angesichts immer autoritärer agierender Sicherheitsbehörden bietet die neue Dimension der E-Mail-Überwachung beängstigende Möglichkeiten. Wenn die Infrastruktur bereits besteht, könnte ein Argument lauten: Warum sollte man sie dann nur zur Aufklärung der festgelegten schweren Straftaten verwenden? Spektakuläre Fälle, die eine Ausweitung der Überwachungsmaßnahmen

rechtfertigen, finden sich üblicherweise schnell. Schon heute gibt es immer wieder Diskussionen um die Grenzen des Lauschangriffs.

Wer sich ob der weitgehenden technischen Möglichkeiten trotz oder wegen der gesetzlichen Bestimmungen bereits jetzt beobachtet fühlt, dem bleibt der Griff zu Verschlüsselungsprogrammen wie PGP (»Pretty Good Privacy«) oder dessen auf freier Software basierenden Abkömmling GnuPG (»Gnu Privacy Guard«). Mathematiker halten die zugrunde liegenden Algorithmen für nicht zu knacken. Auch spricht nichts dagegen, sich einen außerhalb Deutschlands liegenden E-Mail-Provider zu suchen, der deutschen Sicherheitsbehörden natürlich keine dauerhafte Abhörschnittstelle bietet. In diesem Fall bliebe Ermittlern nur, die private Internet-Verbindung anzuzapfen, wenn sie nicht gleich eine internationale Abhöraktion auslösen möchten.