

Pressekonferenz auf der Systems

**Innere Sicherheit und Hightech**

24. Oktober 2007, München

**Prof. Dieter Kempf**

**Mitglied des Präsidiums**

**Bundesverband Informationswirtschaft, Telekommunikation und neue Medien**

- es gilt das gesprochene Wort -

Seite 2

Meine sehr geehrten Damen und Herren,

auch von mir ein herzliches Willkommen zu unserer Pressekonferenz zur Inneren Sicherheit. Seit Monaten wird das Thema leidenschaftlich diskutiert, vor allem wenn es um die Online-Durchsuchung geht. Es wird deutlich, dass Innere Sicherheit in vielen Bereichen nicht ohne die Beteiligung der ITK-Branche denkbar ist.

Deshalb wollen wir zunächst einen kurzen Überblick zu Markt und Technologie geben und zeigen, wo der Staat die Unterstützung der BITKOM-Branche in Anspruch nimmt. Die neuen Sicherheitsgesetze zur Vorratsdatenspeicherung und zur Online-Durchsuchung möchte ich dann etwas näher beleuchten.

Mit dem Thema Sicherheit hat unsere Branche in dreifacher Hinsicht zu tun – im Bereich der Sicherheitselektronik, bei der staatlichen Kommunikationsüberwachung und bei der individuellen IT-Sicherheit von privaten und geschäftlichen Anwendern. Für die Innere Sicherheit in Deutschland sind vor allem die ersten beiden Dimensionen wichtig. Bevor wir zu den aktuellen politischen Dauerbrennern kommen, lassen Sie uns einen Blick auf ausgewählte Märkte für Sicherheitselektronik werfen.

Nach den Anschlägen in New York und später in europäischen Hauptstädten ist zum Beispiel die Nachfrage nach **Videoüberwachung** gestiegen. Öffentliche und private Auftraggeber in Deutschland haben im vergangenen Jahr rund 185 Millionen Euro investiert. Das ist ein leichtes Plus von fünf Prozent gegenüber 2005. International gibt es gewaltige Unterschiede: So investiert das kleinere Großbritannien mehr als dreimal so viel in Videoüberwachung. Mehr Kameras allein reichen allerdings nicht. Es geht ja nicht nur darum, im Nachhinein Täter zu erkennen. Ziel muss sein, Angriffe zu verhindern. Hier helfen Systeme zur Bewegungsanalyse. Sie erkennen zum Beispiel, wenn ein herrenloser Koffer länger auf dem Bahnsteig steht.

Ein weltweiter Wachstumsmarkt ist auch die **Biometrie**, also Systeme, die biologische Merkmale registrieren und vergleichen können. Der Begriff ist aus den griechischen Wörtern für „Leben“ und „messen“ entstanden. Fingerabdrücke, Gesichter und Stimmen lassen sich mit solchen Systemen erkennen, und ich nenne Ihnen gleich ein paar Beispiele aus der Praxis. Hier zunächst die weltweite Umsatzprognose, von der wir heute ausgehen – der Markt wächst jährlich um gut ein Viertel.

In Deutschland kommen wir ebenfalls auf eine jährliche Wachstumsrate von 25 Prozent, und das über einen längeren Zeitraum gesehen. Der heimische Markt für Biometrie wird bis 2010 auf rund 300 Millionen Euro zulegen.

Die heute wichtigsten Technologien auf diesem Markt sind die Erkennung von Fingerabdrücken und Gesichtern. Vielleicht nutzen einige von Ihnen, meine Damen und Herren, ja auch ein biometrisches System. Zum Beispiel an Ihrem Laptop, wenn er über einen Fingerabdruck-Sensor verfügt. Auch zur Anmeldung in Firmennetzen und zur Zutrittskontrolle lässt sich die Technik verwenden, künftig sogar zum Bezahlen im Einzelhandel. Ein Edeka-Markt in Bayern hat es vorgemacht.

Seite 3

Eine erfolgreiche Biometrie-Anwendung ist der **elektronische Reisepass**, den heute schon mehr als 4,3 Millionen Deutsche besitzen. Bisher ist auf dem Chip ein Foto gespeichert, ab November kommen Fingerabdrücke dazu – mit einem speziellen Datenschutzmechanismus. Das dient auch der Fälschungssicherheit. Beim E-Pass sind wir europaweit Vorreiter, und die nötigen Technologien sind hierzulande entstanden. Hier hat Deutschland eine Führungsrolle in einem Schlüsselbereich moderner Hightech. Nächster Schritt ist der elektronische Personalausweis, der die Nutzung staatlicher Online-Dienste erleichtert und bei Einkäufen im Netz helfen wird.

Hier macht IT das Leben der Menschen nicht nur sicherer, sondern auch einfacher. Das ist sinnvoller, praktischer und alltagstauglicher Fortschritt, mithin eine echte Innovation. Wir sind auf dem besten Weg, hier große Zukunftsmärkte zu schaffen.

Wenn wir über Innere Sicherheit reden, geht es aber nicht nur um Technologien zum Anfassen. Aktuell wird vor allem das diskutiert, was im Alltag nicht sichtbar ist: Die Speicherung von Daten und der Zugriff von Ermittlern auf diese Daten. Da müssen wir zwei Dinge unterscheiden: Zuerst einmal die Speicherung von Verbindungsdaten, also die Protokollierung, wer wann mit wem telefoniert hat. Und dann das Abhören und Speichern von Inhalten der Kommunikation. Wir möchten Ihnen einen kurzen Überblick geben und dann unsere Position zu den geplanten Gesetzen erklären.

In dieser Tabelle sehen Sie, was sich Anfang 2008 mit der **Vorratsdatenspeicherung** ändert. Bisher gab es keine generelle Speicherpflicht für die Verbindungsdaten. Die Telekommunikations- und Internet-Anbieter dürfen die Daten zwar bis zu sechs Monaten speichern, aber nur im Zusammenhang mit der Rechnung. Bei erheblichen Straftaten können Ermittler diese Daten schon jetzt bei den Netzbetreibern und Providern abfragen. Aus der Praxis eines Mobilfunk-Anbieters kann Ihnen Herr Haas dazu nachher berichten.

Künftig sind sechs Monate Speicherung eine generelle Pflicht. Außerdem wird die Datenspeicherung ausgedehnt, sowohl bei Festnetz- und Handygesprächen als auch bei E-Mails und Internet-Telefonie. Im Detail müssen nun zum Beispiel auch Handy-Standortdaten und die IP-Adressen von Internetnutzern gespeichert werden.

Meine Damen und Herren,

wenn dadurch eine Reihe schwerer Straftaten aufgeklärt werden kann, wenn vielleicht Terroranschläge mit diesen Maßnahmen verhindert werden können, dann wollen wir sie nicht grundsätzlich ablehnen. Die Netzbetreiber und Provider wollen hier im Interesse der ganzen Gesellschaft ein verlässlicher Partner sein, und Sie sind das seit jeher. Ohne Mithilfe der Hightech-Branche ist Innere Sicherheit heute nicht möglich. Im Übrigen gibt es, das sollten wir bei der nationalen Diskussion nicht vergessen, zur Vorratsdatenspeicherung eine EU-Vorgabe.

Deshalb müssen wir zusehen, dass diese Regelung praxisgerecht ausgestaltet wird. Unsere Maxime ist: So viel Sicherheitsaufwand wie nötig, so viel Privatsphäre wie möglich. Es kann nicht darum gehen, möglichst viele Daten möglichst lange zu

speichern. Im Großen und Ganzen hält sich die Bundesregierung mit Ihrem Gesetzentwurf an die EU-Richtlinie, aber in einigen wenigen Punkten geht sie darüber hinaus. Hier wünschen wir uns, dass der Gesetzgeber genau prüft, was einen echten Gewinn bringt für die Verhinderung oder Verfolgung schwerer Straftaten. Lassen Sie mich einen Punkt herausgreifen: Nach dem aktuellen Entwurf könnten die Daten auch dazu verwendet werden können, Beleidigungsdelikte im Internet zu verfolgen. Das hat mit der öffentlichen Sicherheit wenig zu tun.

In diesem Zusammenhang möchte ich auch an die Bundesregierung appellieren, ihre Pläne nicht über die Köpfe ihrer Kooperationspartner hinweg zu schmieden. Unsere Branche kann die erweiterte Datenspeicherung nicht von heute auf morgen umsetzen. In dem Gesetz brauchen wir eine Übergangsregelung bis 2009, damit die Unternehmen technisch und personell aufstocken können.

Und, meine Damen und Herren, die Netzbetreiber dürfen auf ihren Ausgaben nicht sitzen bleiben. Innere Sicherheit ist eine genuine Staatsaufgabe. Auch wenn die Unternehmen gerne ihren Teil zu einer sicheren Gesellschaft beitragen, muss die öffentliche Hand die Kosten tragen. Allein für die Vorratsdatenspeicherung muss die ITK-Branche bis zu 75 Millionen Euro in Technik investieren. Hinzu kommen jährlich Betriebskosten in zweistelliger Millionenhöhe. Deshalb ist es nur recht und billig, dass zeitgleich mit der Vorratsdatenspeicherung auch eine **Entschädigungsregelung** greift. Seit Jahren warten die Anbieter darauf. Bisher bekommen sie nur einen Bruchteil ihrer Kosten erstattet.

Lassen Sie uns nun einen Blick werfen auf die Fälle, in denen Ermittler die Inhalte von **Kommunikation überwachen**. Die Zahlen der Bundesnetzagentur zeigen, dass zur **Strafverfolgung** überwiegend Handy-Gespräche mitgehört werden. Hier gab es im vergangenen Jahr ein leichtes Plus. Nur in Ausnahmefällen waren Telefonate per Internet betroffen, steigend sind die Zahlen bei Internetzugängen und E-Mails. Straftaten, die eine Überwachung rechtfertigen, sind etwa Mord und Totschlag, sexueller Missbrauch, organisierte Kriminalität, auch Geldwäsche und Drogendelikte.

Zeitgleich mit der Vorratsdatenspeicherung soll es auch hier Änderungen geben. Einige Straftaten kommen hinzu, etwa Korruption, schwere Steuerdelikte, Menschenhandel und Doping. Es bleibt dabei, dass ein Richter zustimmen muss; bei Gefahr im Verzug darf es auch der Staatsanwalt.

Das besonders intensiv diskutierte Thema ist in diesem Zusammenhang aber die **Online-Durchsuchung**, die Sie ebenfalls in dieser Übersicht sehen. Bisher gibt es nur einen Gesetzentwurf mit informellem Status. Im BKA-Gesetz soll der Online-Zugriff auf Computer geregelt werden. Nach diesem Entwurf sind prinzipiell alle Computersysteme ein mögliches Ziel, auch mobile Endgeräte und die Zentralrechner von E-Mail-Anbietern, die von einem Verdächtigen genutzt werden. Die rechtlichen Voraussetzungen sind hier nicht so klar definiert wie bei der Telefonüberwachung. Bei der Online-Durchsuchung soll es aber nicht um die Strafverfolgung gehen, sondern um die Abwehr „dringender Gefahren“ und terroristischer Aktivitäten.

Seite 5

Zum Vergleich haben wir auch die Voraussetzungen für den Großen Lauschangriff angeführt, also das Abhören von Gesprächen innerhalb von Wohnungen. Hier gelten besonders hohe gesetzliche Hürden.

Wir sind der Meinung, dass die Leitlinien des Bundesverfassungsgerichts zum Großen Lauschangriff auch eine Orientierung geben können bei der Online-Durchsuchung. Die Vielfalt der Daten, auch sehr privater Daten, die Sie auf einer Festplatte finden können, ist ähnlich umfang- und facettenreich wie die Kommunikation innerhalb von Wohnungen. Deshalb liegt es auf der Hand, dass auch hier besonders enge Voraussetzungen gelten müssen. Das muss im Gesetzentwurf deutlicher werden.

Wenn das gelingt, müssen wir nicht mehr davon ausgehen, dass uns eine breit angelegte Überwachung von PCs und Festplatten droht. Das Bundeskriminalamt spricht inzwischen von lediglich fünf bis zehn Fällen pro Jahr. Wenn in solchen Einzelfällen tatsächlich terroristische Gefahren vermieden werden können, meine Damen und Herren, dann können wir das Instrument nicht prinzipiell ablehnen. Was wir aber brauchen, sind genauere Informationen über die Pläne des Innenministeriums – und eine klare Definition der juristischen Voraussetzungen von Online-Durchsuchungen. An beidem fehlt es bisher.

In der Diskussion um die Technik der Online-Durchsuchung sind vor allem zwei Aspekte zu beachten. Schon mehrfach wurde debattiert, ob in Deutschland tätige Anbieter von Sicherheitssoftware standardisierte Hintertüren für den Staat einbauen müssen – damit ein so genannter **Bundestrojaner** Durchlass findet. Aus unserer Sicht bringt das wenig und schadet viel: In Zeiten des Internets können die Anbieter jederzeit auf ausländische Anbieter von Firewalls und Virenscannern ausweichen. Eine rein deutsche Gesetzgebung wäre in diesem Punkt zum Scheitern verurteilt. Außerdem müssten die Unternehmen auf dem deutschen Markt Nachteile befürchten, weil eine Sicherheitssoftware mit offizieller Hintertür nun mal wenig attraktiv ist. Das kann ich auch als Chef eines Unternehmens sagen, das selbst Sicherheitslösungen anbietet. Wenn es nur um eine niedrige zweistellige Zahl an Durchsuchungen geht, dann ist die Online-Durchsuchung ein Fall für qualifizierte Spezialisten der Ermittlungsbehörden, nicht für eine generelle Software-Schnittstelle. Problematisch ist aus unserer Sicht auch der Zugriff auf die Server von E-Mail-Providern. Auch hier ist ein nationaler Ansatz wenig sinnvoll, denn Nutzer können ohne die geringsten Probleme über ausländische Anbieter ihren Email-Verkehr abwickeln.

Meine Damen und Herren,

es gibt auch zu anderen technischen und rechtlichen Aspekten noch offene Fragen. Kommt das Überwachungsprogramm als Trojaner, der im Hintergrund Daten ausspäht und an die Ermittler weiterleitet? Oder als Key-Logger, der Tastatur-Anschläge protokolliert? Wie erfolgt die Installation? Diese technischen Details wird das Bundeskriminalamt sicher nicht öffentlich diskutieren, aus verständlichen Gründen. Wir möchten nur zeigen, dass es hier mehrere denkbare Varianten gibt.

Seite 6

In jedem Fall müssten die Kriminalisten Firewalls und Virens Scanner umgehen, und sie müssen dafür sorgen, dass ihr Programm nicht irrtümlich auf weitere Rechner gelangt. Eine Online-Durchsuchung ist weit komplexer, als ein Telefon abzuhören.

Juristisch relevant ist die Frage, ob für Festplatten ähnliche Schutzkriterien wie für Wohnräume gelten. Hier sind sich die Experten noch nicht einig. Unter anderem wird die Frage aufkommen, ob Erkenntnisse aus der Gefahrenabwehr anschließend in Strafprozessen genutzt werden dürfen.

All diese Fragen müssen noch beantwortet werden, um eine vernünftige und sachdienliche Regelung mit Augenmaß zu entwickeln.

Auch in unseren Nachbarländern Österreich und Schweiz wird aktuell über die Online-Durchsuchung diskutiert. Die unterschiedlichen Ansätze sehen Sie auf diesem Chart, und wir haben ein weiteres Beispiel aus den USA angefügt.

Meine Damen und Herren,

Wir müssen diese Diskussionen sicher schnell führen, aber wir dürfen sie nicht überhastet führen. Und wir brauchen dafür fachlichen Sachverstand, den der BITKOM gerne allen Beteiligten zur Verfügung stellt.

Herzlichen Dank.