Positionspapier

BITKOM-Positionspapier zu
Abhörmaßnahmen der Geheimdienste und Sicherheitsbehörden,
Datenschutz und Datensicherheit
31. Oktober 2013

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. vertritt mehr als 2.000 Unternehmen, davon über 1.200 Direktmitglieder mit etwa 140 Milliarden Euro Umsatz und 700.000 Beschäftigten. Hierzu zählen Anbieter von Software & IT-Services, Telekommunikations- und Internetdiensten, Hersteller von Hardware und Consumer Electronics sowie Unternehmen der digitalen Medien. Der BITKOM setzt sich insbesondere für eine Modernisierung des Bildungssystems, eine innovative Wirtschaftspolitik und eine zukunftsorientierte Netzpolitik ein.

Bundesverband
Informationswirtschaft,
Telekommunikation und
neue Medien e.V.

Albrechtstraße 10 A
10117 Berlin-Mitte
Tel.: +49.30.27576-0
Fax: +49.30.27576-400
bitkom@bitkom.org
www.bitkom.org

Präsident
Prof. Dieter Kempf

Hauptgeschäftsführer
Dr. Bernhard Rohleder

Vorbemerkung

Die BITKOM-Branche betrachtet alle Abhörmaßnahmen von Behörden gleich welchen Landes mit großer Sorge, die die informationelle Selbstbestimmung verletzen oder der Wirtschaftsspionage dienen, die Vertrauen in neue Technologien beschädigen, die unverhältnismäßig sind oder gar gegen geltendes Recht verstoßen.

Nach allem was derzeit bekannt ist, sind es nicht die deutschen Sicherheitsbehörden, die Grad und Maß bei der Abwägung zwischen Freiheit und Sicherheit aus den Augen verloren haben. In Deutschland gibt es einen klaren, für jeden nachlesbaren und aus Sicht des BITKOM ausgewogenen Rechtsrahmen für das Sammeln und Auswerten von Daten zu nachrichtendienstlichen Zwecken.

Der latente Verdacht einer umfassenden Überwachung hat schwerwiegende Folgen: Ausgelöst durch die Medienberichterstattung über Abhörmaßnahmen der Geheimdienste aus den USA und Großbritannien ist ein erheblicher Vertrauensverlust in der Bevölkerung bereits feststellbar.

Es steht zu befürchten, dass sich dies nachteilig auf die Nutzung neuer Technologien auswirkt und damit Schaden für Wirtschaft und Gesellschaft entsteht, zumindest die Potentiale neuer Technologien nicht umfassend erschlossen werden.

Gleichzeitig führt die aktuelle Diskussion dazu, dass die notwendige Aufmerksamkeit für reale und unmittelbare Bedrohungen durch die im Internet oder über das Internet organisierte Kriminalität, den Terrorismus und staatlich sanktionierte Wirtschaftsspionage verloren geht.

Die wirtschaftlichen und gesellschaftlichen Chancen der Digitalisierung für Deutschland dürfen nicht gefährdet werden. Digitalisierung schafft Wohlstand, ist für die Lösung der großen gesellschaftlichen Herausforderungen unverzichtbar und ermöglicht Teilhabe. Allein die Modernisierung der öffentlichen Infrastruktur birgt volkswirtschaftliche Potenziale in Höhe von 350 Milliarden Euro bis 2020. (vgl.: BITKOM Gesamtwirtschaftliche Potenziale intelligenter Netze in Deutsch-

land, 2012). Medizinischer Fortschritt, sichere und effiziente Verkehrsführung, die Energiewende, neue Bildungschancen und eine moderne Verwaltung brauchen digitale Technologien und Vernetzung. Mit Industrie 4.0 können der Technologiestandort Deutschland ausgebaut, die Wettbewerbsfähigkeit verbessert und zusätzliche Arbeitsplätze geschaffen werden.

Die Nutzung von IT- und Internettechnologien basiert in starkem Maße auf dem Vertrauen in deren Integrität und Sicherheit. BITKOM hat sich intensiv mit den Auswirkungen der Debatte über behördliche Abhörmaßnahmen befasst und bezieht hierzu im Folgenden Stellung.

Die Rolle der Netzwirtschaft

In wohl jedem Land der Welt sind die Unternehmen der Netzwirtschaft zur Kooperation mit Sicherheitsbehörden gesetzlich verpflichtet. Weder für Anlass noch für Umfang oder prozedurale Ausgestaltung von Abhörmaßnahmen sind die Unternehmen verantwortlich. Welche Daten unter welchen Bedingungen wo und wie erhoben, gesammelt, verarbeitet und gespeichert werden, entscheiden allein die hierfür zuständigen staatlichen Stellen und der Gesetzgeber. Es gibt bisher keinen Anlass daran zu zweifeln, das nach Aussagen der Unternehmen nur im Rahmen des gesetzlich vorgeschriebenen Maßes mit den Behörden zusammengearbeitet wird.

Die Unternehmen der Netzwirtschaft haben keinerlei Interesse daran, sich an der Ausspähung ihrer Kunden oder anderer Internetnutzer zu beteiligen. Die Unternehmen haben das alleinige Interesse, ihren Kunden sichere und hoch vertrauenswürdige Dienste anbieten zu können. Dabei sind sie bestrebt, den Schutz von Daten und Kommunikation und die Unversehrtheit der Privatsphäre jederzeit sicherzustellen und Angriffe und Zugriffe von außen zu verhindern. In die Sicherheit der Daten ihrer Kunden investieren die Unternehmen der Netzwirtschaft jährlich weltweit einen zweistelligen Milliardenbetrag.

Die Rolle von Staat und Politik

Besorgniserregend ist der Umgang befreundeter Staaten miteinander. Wenn sich Regierungen von Partnerländern gegenseitig ausspähen, so ist dies mehr als befremdlich. Sollte aber darüber hinaus das nicht nur in Deutschland verfassungsrechtlich verankerte Fernmeldegeheimnis faktisch durch ein kollusives Zusammenwirken verschiedener nationaler Nachrichtendienste ausgehebelt werden, so rührt dies an den Grundwerten des gesellschaftlichen Zusammenlebens und dem gesetzlich definierten Verhältnis des Staats zu seinen Bürgern. Hier sind Behörden und parlamentarische Kontrollinstanzen aufgefordert, die nachrichtendienstliche Praxis umgehend zu überprüfen und im Bedarfsfall an die verfassungsrechtlichen Vorgaben sowie die EU-Menschenrechtskonvention anzupassen.

BITKOM hat im Folgenden einige weitere Vorschläge zusammengetragen, die helfen können, Sicherheit und Schutz von Daten international zu verbessern und eine gemeinsame Basis für jene nachrichtendienstlichen Aktivitäten zu schaffen, die allgemein als unverzichtbar angesehen werden. Nachrichtendienstliche Tätigkeiten müssen sich dabei auf den gut begründeten Einzelfall beschränken

und dürfen nicht zum Regelfall werden – nicht in Deutschland und in keinem anderen Land der Welt.

1 Transparenz: Schnellstmögliche und umfassende Aufklärung

Transparenz ist die erste und wichtigste Maßnahme, um verloren gegangenes Vertrauen zurückzugewinnen. Die Schaffung von Transparenz ist zunächst Aufgabe der Politik. Denn nur die Regierungen, die Kontrollgremien der Parlamente und die zuständigen Aufsichtsbehörden können wissen, wie Geheimdienste und Sicherheitsbehörden jeweils agieren und in welchem Umfang entsprechende Maßnahmen getroffen werden.

Folgende Maßnahmen zur Schaffung von Transparenz sollten zunächst ergriffen werden:

1. Die Bundesregierung sollte in aggregierter Form schnellstmöglich über den Umfang der tatsächlichen Abhörmaßnahmen der Geheimdienste aufklären und umfassend und im Detail darlegen, auf welcher Rechtsgrundlage in den jeweiligen Ländern Abhörmaßnahmen durchgeführt werden, in welcher Form die rechtlichen Vorgaben jeweils in die Praxis umgesetzt werden und welche Kontrollmechanismen greifen, um das behördliche Vorgehen jeweils zuverlässig zu überprüfen und im Bedarfsfall einzuschränken.

2. Grundsätzlich sind gesetzliche Pflichten für Unternehmen zur „Geheimhaltung“ zu überprüfen. Vielmehr sollten auch Unternehmen die Möglichkeit erhalten, in aggregierter Form regelmäßig über einschlägige Maßnahmen zu berichten.

2 Rechtssicherheit: Internationale Übereinkunft zur Zusammenarbeit von Unternehmen mit Sicherheitsbehörden und Datenschutz

Europa braucht einheitliche Gesetze und Regelungen für die Speicherung von Daten sowie den Zugriff von Sicherheitsbehörden auf diese. Probleme entstehen, wenn etwa die Weitergabe von Daten an Behörden in einigen Ländern untersagt wird, eine solche grenzüberschreitende Weitergabe von Daten in anderen Ländern gleichzeitig aber verpflichtend vorgesehen ist. International aktive Unternehmen dürfen nicht der Unsicherheit ausgesetzt werden, sich zwischen widersprechenden Anforderungen an die Herausgabe von Daten entscheiden zu müssen und damit zwangsläufig gegen die eine oder andere Rechtsordnung zu verstoßen.

BITKOM fordert die Bundesregierung und die Mitgliedstaaten der Europäischen Union deshalb auf, innerhalb der EU und mit wichtigen Partnerländern wie den USA eine internationale Übereinkunft darüber zu erzielen, welche Auskunftsersuchen von wem und unter welchen Umständen zulässig sind und nach welchen international zu standardisierenden Verfahren Datenweitergaben erfolgen müssen – und wann sie zu unterbleiben haben.

Die geplante EU-Datenschutzverordnung ist wichtig, um einen einheitlichen Rechtsraum in Europa zu schaffen und damit auch Europas internationale Verhandlungsposition zu stärken. Die Bundesregierung soll darauf hinwirken,

dass die Verhandlungen über die Datenschutz-Grundverordnung unverzüglich zum Abschluss gebracht werden.

BITKOM setzt sich hierbei für einen modernen, auf einem hohen Niveau harmonisierten Datenschutz in Europa und der Welt ein. Ohne Vorliegen eines entsprechenden Abkommens sollte die Herausgabe von Daten europäischer Nutzer unzulässig sein. Etwaige Auskunftsersuchen müssen dabei im Wege eines Amtshilfeersuchens gegenüber Staaten und nicht direkt gegenüber Unternehmen erfolgen. Die Politik ist dringend aufgefordert, hier für Rechtssicherheit zu sorgen. Wir erwarten, dass sich die Bundesregierung darüber hinaus für die Neuverhandlung und nachhaltige Verbesserung des Safe Harbour Agreements und dessen Vollzug in den USA einsetzt.

Darüber hinaus ermutigt der BITKOM die Bundesregierung, bei den Verhandlungen zur Datenschutzgrundverordnung, zur Transatlantischen Handels- und Investitionspartnerschaft und zum Datenschutzrahmenabkommen zwischen der USA und der Europäischen Union die Belange des Datenschutzes und des Datenmanagements zu berücksichtigen. Nach Abschluss dieser Verhandlungen sollten bestehende Vereinbarungen dahingehend geprüft werden, ob sie eventuell entbehrlich sind.

In der aktuellen Überwachungs-Debatte geht es im Kern um die Kontrolle der Nachrichtendienste. Die Datenschutzgrundverordnung kann deswegen die durch PRISM sichtbar gewordenen Probleme nicht alleine lösen. Denn die Verordnung regelt nicht das Handeln der staatlichen Stellen, sondern nur das der Unternehmen. Es muss auf internationaler Ebene so schnell wie möglich Verhandlungen für ein Antispy-Abkommen geben.

3 EU-Bürger: Europaweiter Schutz vor Ausspähung

In der Regel dürfen Geheimdienste die Daten der Staatsangehörigen ihres Landes nicht ohne konkreten Anlass ausspähen oder verwenden. Gleichzeitig ist ihnen die Ausspähung von Ausländern erlaubt. In einem vereinten Europa ist dieses Prinzip ein Anachronismus.

Die Regierungen der EU-Mitgliedstaaten müssen einen gemeinsamen Ansatz für die Aktivitäten ihrer Geheimdienste entwickeln. Alle EU-Bürger müssen in den EU-Mitgliedstaaten unter entsprechenden Aspekten als Inländer gelten, womit die strengeren Regeln z.B. des Verfassungsschutzes für ihre Überwachung zur Anwendung zu bringen sind. Ein kollusives Zusammenwirken der nationalen Behörden untereinander und damit eine faktische Aushebelung des verfassungsrechtlich garantierten Fernmeldegeheimnisses und des Rechts auf informationelle Selbstbestimmung darf es nicht geben. Dies widerspricht den Grundsätzen der Union.

4 Legitimation und Umfang nachrichtendienstlicher Überwachung

Sicherheitsbehörden agieren im Spannungsfeld aus Freiheit und Sicherheit. Es gibt legitime Interessen wie etwa Strafverfolgung und Gefahrenabwehr, die ein Informationsbedürfnis staatlicher Stellen grundsätzlich rechtfertigen können. Diese Rechtfertigung staatlicher Überwachung gilt aber nicht schrankenlos.

Insoweit ist es originäre Aufgabe der Politik, eine Balance zwischen der Sicherheit auf der einen und Freiheit des Einzelnen sowie der Berufsausübungsfreiheit der betroffenen Unternehmen auf der anderen Seite zu finden. Die aktuellen Medienberichte legen nahe, dass hier in Bezug auf die Aktivitäten der Nachrichtendienste befreundeter Staaten dringender Handlungsbedarf besteht.

Ziel der Bundesregierung sollte es sein, sich auf internationaler Ebene für angemessene Regelungen nachrichtendienstlicher Tätigkeiten einzusetzen, um elementare Grundrechte zu schützen und das Vertrauen in die digitale Welt zu stärken. Dazu ist weitest mögliche Transparenz unerlässlich, etwa indem den Unternehmen gestattet wird, über die Häufigkeit ihrer Inanspruchnahme für nachrichtendienstliche Vorgänge anonymisiert zu berichten.

5 Routing: Beitrag zu Datenschutz und –sicherheit prüfen

Es ist zu prüfen, welche Beiträge zu mehr Datenschutz und Datensicherheit Maßnahmen im Bereich des Routings grundsätzlich leisten können. Im Besonderen ist dabei zu untersuchen, welche entsprechenden Beiträge von einem nationalen Routing oder einem Routing im Schengen-Raum ausgehen können.

6 Nationaler Rat: Verhältnis von Freiheit und Sicherheit, von Anonymität und Verantwortung

Die aktuelle Diskussion macht deutlich, dass über das Verhältnis von Freiheit und Sicherheit, von Anonymität und Verantwortung für das eigene Handeln im Internet unterschiedliche Auffassungen vertreten werden. Es ist unklar, in welcher digitalen Welt wir leben und arbeiten wollen. Besonders durch die großen Volksparteien zieht sich in diesen Fragen ein Riss, der vornehmlich Netzpolitiker einerseits und Innen- bzw. Rechtspolitiker andererseits voneinander trennt.

BITKOM regt an, ähnlich dem Nationalen Ethikrat einen Kreis von Persönlichkeiten einzurichten, der in der Lage ist, Orientierungshilfe bei der Weiterentwicklung der digitalen Welt und der Ausformulierung des entsprechenden Rechtsrahmens und seiner Umsetzung zu geben.

7 Wirtschaftsspionage: Schutz von Unternehmensgeheimnissen

Es ist zu befürchten, dass bei einem unkontrollierten Zugriff auf elektronische Informationen durch ausländische Behörden auch auf Unternehmensgeheimnisse zugegriffen wird. Die Wettbewerbsfähigkeit deutscher Unternehmen könnte so signifikant geschwächt werden.
Dass der unkontrollierte Zugriff auf elektronische Informationen durch Nachrichtendienste auch den Zugriff auf Unternehmensgeheimnisse einschließt, ist in Einzelfällen nachweisbar, wobei von einer hohen Dunkelziffer auszugehen ist.
Die nachhaltige Wettbewerbsfähigkeit deutscher Unternehmen ist ohne die Sicherheit der Innovations- und Kommunikationsdaten nicht zu gewährleisten, - hier wird eine volkswirtschaftliche Dimension erreicht. Insbesondere die Klein- und Mittelbetriebe (KMU), die i.d.R. über keine eigenen IT-Abteilungen verfügen, aber auch international eine hohe Wettbewerbsfähigkeit erreicht haben, gilt es in diesem Zusammenhang zu schützen und zu unterstützen.

BITKOM setzt sich dafür ein, dass ein unbefugter Zugriff auf Unternehmensgeheimnisse in der Datenverarbeitung und -übertragung als strafrechtlicher Tatbestand auch international konsequent verfolgt und mit angemessenen Schadensersatzansprüchen unterlegt wird – auch gegenüber staatlichen Stellen. Ziel sollte hier auch eine Erweiterung der vorhandenen Bündnisse um einen gegenseitigen Verzicht auf Staats- und Wirtschaftsspionage sowie Sabotage von kritischen Infrastrukturen und IT-Systemen sein.

Darüber hinaus sollte sich die Bundesregierung dafür stark machen, dass Wirtschaftsspionage international geächtet und ein Abkommen verabschiedet wird, dessen Unterzeichnerstaaten verbindlich erklären, zumindest untereinander künftig auf jedwede Wirtschaftsspionage zu verzichten und sich bei der grenzüberschreitenden Strafverfolgung einschlägiger Tatbestände gegenseitig bestmöglich zu unterstützen. Ungeachtet dessen bleibt jedes einzelne Unternehmen in der Pflicht, für seine Sicherheit auch im IT-Bereich selbst Sorge zu tragen.

Die Nutzung von zeitgemäßer IT-Sicherheitstechnologie und deren qualifizierter Einsatz müssen in Unternehmen zum Normalfall werden. Dazu gehört auch die Sicherung von Nischenbereichen wie etwa der mobilen Kommunikation via Smartphone, um sensible Daten zu schützen.

8 Sicherheitsbewusstsein: Befähigung zum Selbstschutz

BITKOM setzt sich u.a. mit der Allianz für Cybersicherheit und dem Verein Deutschland Sicher im Netz für eine Stärkung der Sicherheitskultur in Deutschland ein und leistet Beiträge, alle privaten und geschäftlichen IT-Nutzer zum Selbstschutz zu befähigen.

Der Schutz der eigenen und der Kundendaten ist eine der zentralen Aufgaben für Unternehmen der IT-Wirtschaft. Die Unternehmen in Deutschland und in Europa müssen jederzeit im Stande sein, ihre kritischen Daten und die Daten ihrer Kunden in der Art zu schützen, dass das Vertrauen in die IT-Wirtschaft nicht beschädigt wird und idealer Weise ausgebaut werden kann. Sinnvolle Mittel dazu können z.B. die Nutzung von verschlüsseltem Datenverkehr oder die Ablage von Daten nur in geschützten Bereichen sowie Data Leakage Prevention sein.

Auch Verbraucher können ihre Daten besser schützen. Eine weitere Sensibilisierung, Medienkompetenz, öffentliche und private Initiativen zur Erhöhung der Sicherheit begrüßt BITKOM ausdrücklich.

Gleichwohl: Technische Sicherheitslösungen können nicht vor gesetzlichen Eingriffsermächtigungen durch Behörden schützen und daher eine politische und rechtsstaatliche Lösung nicht ersetzen.

Aus diesem Grund werden auch Schulungen oder ähnliche Weiterbildungsmaßnahmen unterstützt, die Unternehmensmitarbeiter und Bürger in die Lage versetzen, mit sensiblen Daten richtig umzugehen und auch etwa bei der Datenspeicherung oder deren Bekanntgabe über mögliche Folgen informiert sind.

9 Technologiestandort Deutschland: IT-Strategie

Die neu gebildete Bundesregierung sollte gemeinsam mit der BITKOM-Branche eine Strategie zur Stärkung des IT-Standorts Deutschland entwickeln und umsetzen. Damit sollen die enormen Chancen, die sich mit der Digitalisierung für den Standort Deutschland verbinden, betont und genutzt werden.