VERBAND DER INTERNETWIRTSCHAFT E.V.

Stellungnahme

zum Anforderungskatalog nach § 113f TKG der Bundesagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen

Berlin, 21. Juni 2016

Vorab ist darauf hinzuweisen, dass die Hersteller nach eigener Ankündigung die neuen Systeme, die von den Unternehmen für eine Implementierung der Sicherheitsanforderungen benötigt werden, zunächst nicht entwickeln werden. Sie wollen abwarten, bis Rechtssicherheit darüber besteht, ob diese Entwicklungen tatsächlich erforderlich sind oder – wie nach dem ersten Aufschlag zum Thema – die Vorratsdatenspeicherung wiederum für verfassungswidrig erklärt wird. Da die verlangten Systeme weder existieren noch es irgendwo im Ausland vergleichbare Maßnahmenkataloge gibt, wird dies ein nicht zu überwindendes praktisches Problem für die Anbieter und verpflichteten Unternehmen sein. Vor diesem Hintergrund ist die Umsetzung und Implementierung der Speicherpflichten für die verpflichteten Unternehmen innerhalb der gesetzlich vorgesehenen Umsetzungsfrist nach § 150 Abs. 13 („spätestens zum 1. Juli 2017“) deutlich zu kurz bemessen.

I. Allgemeine Anmerkungen

1. Aufwand für die Unternehmen bei der Umsetzung

Generell ist zu den nun vorliegenden technischen Anforderungen zu sagen, dass sie die schlimmsten Befürchtungen noch übertreffen. Die geforderte Umsetzung all dieser Maßnahmen wird in jedem Unternehmen eine permanente Beschäftigung mit dem Thema zur Folge haben. Fortwährende Sicherheitsüberprüfungen, Generierung und Löschung der Schlüssel, die Protokollierung aller Arbeitsschritte und vieles andere mehr machen einen vielfach höheren personellen und administrativen Arbeitsaufwand notwendig als anfangs zu vermuten war. Der zusätzliche Personalaufwand wird ebenfalls nicht mit der Umsetzung des Vier-Augen-Prinzips bei der Abfrage eines bestimmten, von der Behörde geforderten Datums sein Bewenden haben, sondern im Gegenteil täglich Aufwand verursachen und personelle Kapazitäten binden. Die in dem Katalog enthaltenen technischen Vorkehrungen und sonstigen Maßnahmen zur Umsetzung der Vorratsdatenspeicherung werden alle Unternehmen - unabhängig von Geschäftsmodell, Unternehmensgröße oder Kundenzahl - vor eine immense Herausforderung stellen. Dies betrifft sowohl kleinere und mittlere Netzbetreiber, aber auch große Netzbetreiber. Bei größeren Anbieter ist insbesondere die Komplexität der Netzinfrastruktur und die hohe Anzahl an verteilten Systemen und Netzkomponenten zu berücksichtigen, die für die Erfüllung der Speicherpflichten und Anforderungen nach § 113f TKG angepasst werden müssen. Eine solche Dauerbelastung ist vor allem für

kleine und mittlere Betreibe schlichtweg nicht zu leisten. Zudem ist sie auch vollkommen unnötig, wenn man in diese Rechnung einbezieht, wie oft kleinere Carrier oder im Geschäftskundensegment tätige Unternehmen realistischer Weise Anfragen der Behörden erhalten werden.

2. Einhaltung des Vier-Augen-Prinzips

Das zweite große Problem ist die in allen Bereichen vorgesehene Einhaltung des Vier-Augen-Prinzips. Aus dem Gesetzeswortlaut war bislang nur ersichtlich, dass bei einer konkreten Systemabfrage immer zwei Mitarbeiter des Unternehmens involviert sein sollen. Durch den Anforderungskatalog zieht sich das Vier-Augen-Prinzip nun jedoch wie ein roter Faden: Für nahezu alle Aktionen, die irgendwie mit dem Datenspeicher der Vorratsdaten in Zusammenhang stehen, ist die Beteiligung von zwei Personen vorgesehen. Das wird in der Praxis oft dazu führen, dass ein Mitarbeiter dem anderen „beim Arbeiten zusehen“ muss. Die Erfüllung dieser Vorgabe ist für eine hohe Anzahl kleiner und mittlerer Betriebe schlicht nicht leistbar. Erschwerend kommt hinzu, dass Lösungen, die diese Anforderung im Einzelfall etwas realistischer machen würde, ebenfalls nicht in Frage kommen. Etwa eine Fernwartung(-beteiligung), die sich für einige Betriebe als einzig praktikable Notlösung anbieten würde, ist technisch gar nicht möglich. Ein besserer Ansatz wäre demgegenüber auch für den Anforderungskatalog nach § 113f TKG auf das bereits bestehende und beim jeweiligen Netzbetreiber bereits implementierte Vorgehen nach § 113d TKG abzustellen, welches bereits im Sicherheitskonzept nach § 113g TKG der Unternehmen beschrieben und festgelegt ist.

3. Finanzieller Ausgleich fehlt

Im Gegenzug zu diesen extrem hohen Anforderungen fehlt ein finanzieller Ausgleich für die laufenden Betriebskosten im Gesetz aber vollkommen. So ist zwar eine Entschädigung für einzelne Anfragen vorgesehen; auf die Implementierungskosten wird wenigstens mit einer allgemein formulierten Härtefallklausel eingegangen. Die operativen Kosten für die Unternehmen aber werden weder im Gesetz noch im Anforderungskatalog erwähnt. Auch die bisherigen Entschädigungssätze nach § 23 des Justizvergütungs- und -entschädigungsgesetz (JVEG) für die einzelnen Abfragen sind grundsätzlich viel zu knapp bemessen. In die Kalkulation hat anscheinend keinen Eingang gefunden, dass künftig immer das Vier-Augen-Prinzip gelten soll, also bei jeder Interaktion mit dem System immer zwei Mitarbeiter beschäftigt sein werden. Eine Anpassung des bestehenden Entschädigungsregimes an die veränderten Anforderungen bei den verpflichteten Unternehmen ist daher unumgänglich.

4. Keine Sicherheitsanforderungen für abfragende Behörden

Des Weiteren lässt der Anforderungskatalog bezüglich der Datensicherheit aber auch einige Fragen offen: Müssten die strengen Regeln, die die Unternehmen verpflichten, nicht auch für die Empfänger gelten? Wie soll

eine sichere Übermittlung stattfinden? Die erhobenen Daten müssten auch nach ihrer Ausleitung aus den Systemen der Anbieter noch als genauso sensibel gelten, deshalb ist nicht zu erklären, warum auch sogar Grundvorschriften für die Datensicherheit in den Behörden fehlen. Gerade weil ja auch hier nicht davon ausgegangen werden kann, dass nur einzelne Daten auf Anfrage versendet werden: Die bisherigen Erfahrungen vieler Anbieter mit den Behörden lassen eher befürchten, dass etwa wegen ungenauer zeitlicher Anfragen hunderte oder gar tausende dieser Datensätze weitestgehend ungesichert an die Behörden übermittelt werden, um dort nahezu vollkommen ungesichert abgespeichert zu werden. Vor diesem Hintergrund ist nicht nachvollziehbar, warum der Anforderungskatalog keinerlei Sicherheitsanforderungen für abfragende Behörden enthält. Denn erfahrungsgemäß wäre ein unberechtigter Zugriff auf die Daten der Vorratsdatenspeicherung an der schwächsten Stelle zu befürchten. Denn bekanntlich bestimmt das schwächste Glied das gesamte Sicherheitsniveau der Gesamtkette. Wenn es bei dem bisherigen Stand des Anforderungskatalogs bleiben sollte, und keine Sicherheitsanforderungen für und bei den abfragenden Behörden festgelegt werden, sind Sicherheitsmaßnahmen auf Seiten der verpflichteten Unternehmen nutzlos. Insofern wären die in dem Anforderungskatalog enthaltenen Sicherheitsmaßnahmen für die verpflichteten Unternehmen auch unverhältnismäßig.

II. Konkrete Anmerkungen

1. Datensicherheit und Datenqualität

Allgemein wird im Abschnitt 4.1 über die Anforderungen an die Datensicherheit und Datenqualität von falschen Voraussetzungen ausgegangen: Bestimmte Daten, die im Anforderungskatalog wie selbstverständlich als vorhanden vorausgesetzt werden, werden nicht von allen Carriern heute selbstverständlich erhoben. Alleine die Erhebung dieser zur Erfüllung der Speicherpflichten zusätzlichen Daten wird einen unverhältnismäßig hohen technischen Aufwand erfordern. Dass derartige Investitionen in das eigene Netz - sowohl in die Netzinfrastruktur als auch die eingesetzten Komponenten noch notwendig sein könnte, ist im Gesetzgebungsprozess und bei der Erarbeitung des Anforderungskatalog nach § 113f TKG schlichtweg übersehen und nicht berücksichtigt worden. Das ist darauf zurückzuführen, dass in allen Dokumenten vom „Stand der Technik“ die Rede ist; die nun vorgestellten Voraussetzungen gehen tatsächlich aber weit über diesen heute üblichen und bei den Anbietern implementierten „Stand der Technik“ hinaus.
Etwa bei Punkt 4.2. des Anforderungskatalogs werden „besonders hohe Standards der Qualität“ bei den speicherpflichtigen Verkehrsdaten vorgeschrieben. Damit soll die Richtigkeit und Aussagekraft der Daten sichergestellt und ungenaue oder unrichtige Ergebnisse nach Anfragen der Behörden vermieden werden. Zu diesem Zweck werden unter anderem Maßnahmen zur Sicherstellung der Genauigkeit zu speichernder Zeitangaben verlangt. Das bedeutet, dass diese Voraussetzungen im

gesamten (eigenen) Netz vorhanden sein müssen. Dies entspricht nicht dem Stand der Technik. Der überwiegende Teil der Carrier brauchen für eigene Zwecke diese besonders hohe Datenqualität nicht, weswegen sie in den Systemen auch nicht vorhanden ist. Das wiederum bedeutet gerade, dass die Voraussetzungen und Anforderungen für die Speicherung der Daten in dieser Qualität erst überall geschaffen und neu implementiert werden müssten. Dies ist ein zusätzlicher Kostentreiber. Auch wird diese Anforderung die Implementierungs- und Umsetzungszeit erheblich verlängern.
Auch das auf Seite 14 des Katalogs abgedruckte Umsetzungsbeispiel der VDS-Grundstruktur zeigt eindrücklich, wie weit die Annahme unrichtiger Voraussetzungen geht: Das Beispiel beschreibt im Grunde ausschließlich die Architektur im Bereich der Telefonie. Bei vielen Internet-Carriern, hauptsächlich den kleineren Unternehmen, sind Logdateiensysteme und Abfrage-Clients überhaupt nicht vorhanden. Diese müssen bisher auch nicht vorgehalten werden.

2. Technische Vorkehrungen für die Umsetzung

Bei der Lektüre von Abschnitt 5 des Anforderungskatalogs, der die technischen Vorkehrungen regelt, wird deutlich, was für ein ungeheuer hoher Aufwand die Anbieter treffen wird. Dieser ist durch die Vergütung, die die Provider für eine manuelle Datenabfrage gemäß § 113 TKG erhalten sollen, nicht im Ansatz gedeckt.

Randnummer 5.2.5 sieht eine besonders sichere Methode der Löschung von Daten aus persistenten Speichern darin, zunächst eine geeignete Verschlüsselung der Daten vorzunehmen und anschließend die verwendeten Schlüssel zu löschen. Eine solche Vorgehensweise ist technisch sicherlich möglich, aber ebenfalls nicht Stand der Technik. Das bedeutet, dass auch hier erst neue Systeme gebaut werden müssen, die diese Anforderung abbilden. Dies wiederum ist aufwendig und teuer. Damit ist das Problem der sicheren Löschung aber noch nicht gelöst: Es wird lediglich auf die Löschung der Schlüssel verlagert. Diese zu löschen ist genauso effizient oder sicher, wie die Daten selbst zu löschen. Die vorgeschlagenen Methoden sind aber sämtlich wenig praxistauglich.

Die gleichen Ausführungen gelten entsprechend für die Anforderungen an die Software und die Protokolldaten. Auch hier müssen komplett neue Systeme entwickelt werden, die nichts mit dem heutigen Stand der Technik zu tun haben.

Ein weiterer zu kritisierender Punkt ist die vorgesehene Beschränkung des Zutritts zu den Datenverarbeitungsanlagen gemäß § 113 d Satz 2 Nr. 4 TKG in Randnummer 5.2.6. Hiernach soll die Zutrittsbeschränkung insbesondere personell, organisatorisch und technisch erfolgen. Unter anderem soll es ein „Rollenkonzept“ der „verschiedenen ermächtigten Mitarbeiter“ geben, also sollen die unterschiedlichen Mitarbeiter unterschiedliche Aufgaben erfüllen. Außerdem werden dann getrennte Sicherheitsbereiche verlangt, konkret soll

„der Teil des Rechenzentrums, in dem die Hardware-Komponenten des VDS-Systems untergebracht sind, (...) als geschlossener Sicherheitsbereich konzipiert“ sein. Diese Komponenten müssen durch hochwertige Zutritts-kontrollmechanismen vor unbefugtem Zutritt geschützt werden. Ein Zugang zu Wartungszwecken etwa soll erst nach einer Identifikation und einer Zwei-Faktor-Authentisierung unter Anwendung des Vier-Augen-Prinzips möglich sein. Das bedeutet, dass die Unternehmen einen eigenen Raum zur Vorhaltung der neuen Systeme einrichten müssen – und diesen auf höchstem Niveau sichern müssen und immer nur zwei Mitarbeiter gleichzeitig diesen gemeinsam betreten dürfen.

Derartige Vorgaben sind insbesondere für kleine und mittlere Betriebe nicht einzuhalten. Die damit verbundenen finanziellen, räumlichen, personellen und administrativen Aufwendungen sind utopisch. An diesem Beispiel lässt sich besonders deutlich zeigen, wie wenig Rücksicht auf die tatsächlich gegebenen Prozesse und Arbeitsabläufe der Unternehmen genommen wird. Die bestimmende Leitlinie und einziges maßgebliches Kriterium bei der Ausgestaltung der gesetzlichen Anforderungen und des Anforderungs-katalogs nach § 113f TKG scheint zu sein, die Sicherheitsvorkehrungen so hoch anzusetzen, dass sie vor einem Bundesgericht Bestand haben. Welche wirtschaftlichen Auswirkungen dies für die verpflichteten Unternehmen und die praktische Umsetzung und Implementierung der Vorgaben bedeutet, wurde nicht berücksichtigt.

III. Auswirkungen auf kleine und mittlere Unternehmen

Da es keine Marginalgrenze gibt, also keine Unternehmen ausgenommen sind, werden insbesondere kleine und mittlere Unternehmen darauf angewiesen sein, die Härtefallklausel in Anspruch zu nehmen. Da aber vollkommen unklar ist, wer unter diese Klausel fällt und nicht anzunehmen ist, dass eine entsprechende Prüfung oder gar Übernahme der Kosten durch den Staat vor Umsetzung erfolgen wird, müssen auch diese Betriebe bei Implementierung der Systeme in Vorleistung gehen. Schon das werden sich einige nicht leisten können, für viele Mittelständler wird dies die Insolvenz bedeuten. In keiner Relation demgegenüber steht der zu erwartende Beitrag, der dann von diesen Firmen für die Aufklärung von Schwerkriminalität zu erwarten ist. Anbieter mit weniger als 10.000 Kunden sowie Unternehmen die im Geschäftskundensegment tätig sind bekommen eine Behörden-anfrage in drei Jahren, der Durchschnitt liegt hier wohl bei ca. zwei im Jahr.

Insgesamt lässt sich feststellen, dass es sich um einen „Wunschkatalog“ der Politik handelt: Daten sollen in Gänze vorhanden, jederzeit abrufbar und dabei hochgesichert sein. Eine entsprechende Umsetzung ist sicher denkbar und erfüllbar, aber heute in den Systemen der Betreiber keinesfalls Standard. Derartige Systeme müssen vollkommen neu designed und aufgesetzt werden; außerdem werden fortlaufend manuelle Eingriffe von Nöten sein. Dies wird alle verpflichteten Unternehmen - unabhängig von Geschäftsmodell, Unternehmensgröße und Kundenzahl - vor eine erhebliche

Herausforderung bei der Erfüllung der Anforderungen stellen und mit einem immensen finanziellen Aufwand für die Implementierung verbunden sein. Wenn man bedenkt, dass absolut dieselben Daten wahrscheinlich eine ganze Zeit in den normalen Systemen der Carrier parallel vorhanden sein werden, ohne diese Sicherheitsvorkehrungen unterworfen zu sein (und auch ohne bisher überlieferte Zwischenfälle) wird die ganze Absurdität des Vorhabens sehr deutlich. Und wenn man den zu erwartenden Nutzen der Daten im Verhältnis zu diesem immensen Aufwand betrachtet, scheinen die Anforderungen noch weniger gerechtfertigt.

Zumindest die existenzbedrohenden Auswirkungen für kleinere und mittlere Unternehmen ließen sich mit etwas politischen Willen deutlich abschwächen. Es ist nicht nachvollziehbar, warum es in dem Anforderungskatalog kein abgestuftes Konzept gibt, wie es etwa bei den Anforderungen an die technischen Schutzmaßnahmen nach § 109 TKG vorgesehen ist: Hier wird bei der Umsetzung der Anforderungen auch die Wirtschaftlichkeit bzw. die Leistungsfähigkeit des einzelnen Unternehmens mitberücksichtigt. Die Vorratsdatenspeicherung bildet damit eine gesetzliche Ausnahme, auch der kleinste Mittelständler wird durch den enormen Umsetzungs- und Betriebsaufwand getroffen. Wenn ein solch abgestuftes Konzept aber nicht gewollt ist, böte es sich an, Anbieter, die weniger als 10.000 Kunden haben, grundsätzlich als Härtefälle einzustufen. So wäre wenigstens gewährleistet, dass der Staat die Kosten (zumindest der Implementierung) für die Betriebe immer übernehmen muss.

Über eco

eco - Verband der Internetwirtschaft e.V. ist Interessenvertreter und Förderer aller Unternehmen, die mit oder im Internet wirtschaftliche Wertschöpfung betreiben. Der Verband vertritt derzeit mehr als 900 Mitgliedsunternehmen. Hierzu zählen unter anderem ISP (Internet Service Provider), Carrier, Hard- und Softwarelieferanten, Content- und Service-Anbieter sowie Kommunikationsunternehmen. eco ist der größte nationale Internet Service Provider-Verband Europas.