IEN · Dorotheenstrasse 54 · 10117 Berlin

Bundesnetzagentur für Elektrizität, Gas,
Telekommunikation, Post und Eisenbahnen
Referat 116b
Tulpenfeld 4

53113 Bonn

Per Email an: 116-Postfach@bnetza.de

Anforderungskatalog nach § 113f TKG
Katalog von technischen Vorkehrungen und sonstigen Maßnahmen zur Umsetzung des Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten

Stellungnahme der Initiative Europäischer Netzbetreiber (IEN)

Berlin, den
30.06.2016

Sehr geehrte Damen und Herren,

die Bundesnetzagentur hat im Amtsblatt Nr. 9 den Entwurf des technischen Anforderungskatalogs nach § 113f TKG veröffentlicht. Interessierten Parteien wurde die Möglichkeit der Stellungnahme bis zum 30.06.2016 eingeräumt. Die Initiative Europäischer Netzbetreiber (IEN) nimmt die Gelegenheit zur Stellungnahme nachfolgend gerne wahr.

I. Allgemeine Anmerkungen

Die IEN möchte zunächst ausdrücklich betonen, dass sie das Vorgehen der BNetzA und des BSI grundsätzlich begrüßt, in Zusammenarbeit mit den betroffenen Marktbeteiligten die technischen Anforderungen an die Umsetzung des Gesetzes über die Festlegung einer Höchstspeicherfrist für Verkehrsdaten zu konkretisieren.

Allerdings ist die IEN auch der Auffassung, dass der vorgelegte Entwurf dieses Bemühen noch nicht hinreichend wiederspiegelt und deshalb noch grundlegend weiter entwickelt werden muss.

Festzuhalten ist, dass Konsens darüber besteht, dass die verlangten Systeme derzeit weder existieren, noch es in anderen Ländern vergleichbare Maßnahmenkataloge gibt. Die neuen Systeme, die von den Unternehmen für eine Implementierung der Sicherheitsanforderungen benötigt werden,

…

bedürfen zunächst der Entwicklung, so dass nach wie vor Zweifel an der tatsächlich gesetzten Umsetzungsfrist besteht. Es besteht eine erhebliche (Rechts-)Unsicherheit auf Seiten der verpflichteten Unternehmen, da die erforderlichen Eigenimplementierungen einen erheblichen Zeit- und Kostenaufwand mit sich bringen werden. Dies gilt umso mehr, als dass das dem Anforderungskatalog zugrundeliegende Gesetz bereits Gegenstand von gerichtlichen Verfahren ist.

Darüber hinaus lässt sich hinsichtlich der nunmehr vorgeschlagenen technischen Anforderungen festhalten, dass diese eine deutliche Steigerung jedweden bisher geschätzten Aufwands bei den betroffenen Unternehmen bedeuten. Die Art der Umsetzung sämtlicher Maßnahmen bedeutet für die Anbieter über Jahre hinweg eine dauerhafte, umfängliche finanzielle und personelle Belastung. Gerade das durchgehend vorgesehene Vier-Augen-Prinzip, die laufenden Sicherheitsüberprüfungen, anhaltende Generierung und Löschung der Schlüssel, die Protokollierung aller Arbeitsschritte etc. bedeuten einen erheblichen Aufwand. Die Umsetzung des Vier-Augen-Prinzips bei der Bearbeitung der Abfrage eines bestimmten, von der Behörde geforderten Datums, ist realitätsfremd und führt bei einer konsequenten Umsetzung unter Berücksichtigung von Krankheits- und Urlaubszeiten zu einer dauerhaften Mitarbeiterbefassung von mehr als zwei Mitarbeitern. Ressourcen werden belegt, die so nicht vorhanden sind und eigens beschäftigt werden müssten. Derartige Mehrbelastungen dürften vor allem für KMUs, nur schwer zu bewältigen sein. Die IEN hat in diesem Zusammenhang in ihren Stellungnahmen zum Gesetzentwurf bereits vielfach darauf hingewiesen, wie unverhältnismäßig sich dieser Aufwand darstellen dürfte. Die IEN plädiert hier auch für eine Rechtssicherheit schaffende Formulierung der Härtefallregelung nicht nur für die Investition in erforderliche Hardware sondern auch für den laufenden Betrieb. Dies gilt neben den KMUs für sämtliche Unternehmen, die lediglich eine geringe Kundenzahl (wie etwa nur große Geschäftskunden und Behörden) bedienen, da diese für eigene Kunden so gut wie keine Anfragen zu erwarten haben. Falls die berechtigten Stellen zu allen Anfragen im Rahmen der Auslandskopfüberwachung auch Verkehrsdaten nach § 113b TKG verlangen werden, was durchaus denkbar ist, dann kann sich die Zahl der Anfragen auch beträchtlich erhöhen. Auch hier ist eine Klarstellung erforderlich.

Der Anforderungskatalog lässt vollkommen außer Acht, dass im Gegenzug zu den extrem hohen Anforderungen ein finanzieller Ausgleich für die laufenden Betriebskosten im Gesetz fehlt. Vorgesehen ist dort lediglich die Entschädigung für einzelne Anfragen sowie eine Härtefallklausel für Implementierungskosten. Wenn jedoch schon keinerlei operative Kostenerstattungen für die Unternehmen vorgesehen sind, so ist es vollkommen unverhältnismäßig, wenn dann noch derart – über den bloßen Gesetzestext hinausgehende – Anforderungen, wie das nunmehr durchgängig vorgesehene Vier-Augen-Prinzip und weitere, extrem aufwändige, technische Vorgaben vorgeschrieben werden sollen.

Gerade im Hinblick auf KMUs und Geschäftskundenanbieter, die häufig weniger als 10.000 Kunden bedienen, gilt, dass diese in der Vergangenheit im Regelfall lediglich ein bis zwei Behördenanfragen pro Jahr erhalten haben. Angesichts des zu erwartenden (geringen) Nutzens der Datenvorhaltung bei diesen Unternehmen im Verhältnis zu dem immensen Aufwand, scheinen die Anforderungen noch weniger gerechtfertigt.

Die IEN möchte daher nochmals ausdrücklich ein abgestuftes Konzept im Anforderungskatalog anregen, welches auch die Verhältnismäßigkeit der Umsetzung bei den einzelnen Unternehmen berücksichtigt. Dies könnte etwa im Rahmen der Erstellung des Sicherheitskonzepts nach § 113 g TKG erfolgen. Andernfalls plädiert die IEN dafür, dass Anbieter, die weniger als 10.000 Kunden haben, grundsätzlich als Härtefälle eingestuft werden um zu gewährleisten, dass gerade kleinere Unternehmen und solche, bei denen der Aufwand und Nutzen bereits aufgrund der wenigen zu erwartenden Anfragen in einem Missverhältnis stehen, zumindest die Implementierungskoten erstattet bekommen.

Durch diese vorausschauende Vorgehensweise würde nicht nur schnell die dringend erforderliche Rechtssicherheit hergestellt werden können, sondern es könnten auch zeit- und kostenintensive Gerichtsverfahren zur Feststellung des individuellen Unterfallens eines Unternehmens unter die Härtefallklausel vermieden werden. Es muss dem Gesetzgeber und den umsetzenden Behörden bewusst sein, dass der angestrebte Grad an Datensicherheit und technischen Vorkehrungen bei der Datenvorhaltung den betroffenen Unternehmen im Wege der Härtefallklausel vergütet werden muss, um keinen enteignenden oder enteignungsgleichen Eingriff darzustellen. Die Diskussionen im politischen Raum sollten jedenfalls zu der Erkenntnis geführt haben, dass ein besonderes Maß an Sicherheit nicht ohne weitere Anstrengungen auf allen Seiten zu gewährleisten sein wird und entsprechende Investitionen auch auf Seiten des Gesetzgebers erforderlich macht.

Weiterhin verweist die IEN auf absehbare Unklarheiten im Zusammenhang mit der sich ebenfalls in der Diskussion befindlichen Novellierung der TKÜV. Dort wird in § 2 zum Auskunftsbegehren nach 96 und 113b TKG Bezug genommen. Demnach dürfen berechtige Stellen Auskünfte nach §§ 96 und 113b TKG stellen. Dies bedeutet aus Sicht der IEN, dass die Auskunftserteilung aus § 113b TKG nach der geänderten Kundenauskunftsverordnung erfolgen soll. Dann stellt sich die Frage, weshalb dann die – für die betroffenen Unternehmen als erheblich einzustufenden - gesonderten Anforderungen im neuen Anforderungskatalog zu § 113b TKG gestellt werden.

Schließlich möchte die IEN noch darauf hinweisen, dass der Entwurf des Anforderungskatalogs bislang noch die Fragen des Umgangs mit den Daten seitens der Behörden unberücksichtigt lässt. Auch nach der Ausleitung der georderten Daten aus den Systemen der Unternehmen handelt es sich um sensible Daten, die auch seitens der Behörden entsprechend zu behandeln sind, was Themen der sicheren Bearbeitung und Speicherung betrifft. So

haben mehrere Untersuchungen in den vergangenen Monaten zum Datenschutz in Polizeisystemen ergeben, dass häufig zu lax mit den Datenschutzbestimmungen umgegangen wird[1].

II. Im Einzelnen

1. Datensicherheit

Die IEN bemängelt zunächst die in Ziffer 4.1 vorgesehenen Anforderungen an die Datensicherheit und Datenqualität.

Zunächst gilt, dass die im Anforderungskatalog als vorhanden vorausgesetzten Daten nicht von allen betroffenen Anbietern auch erhoben werden. So bedeutet bereits die Erhebung dieser – zusätzlichen - Daten einen unverhältnismäßig hohen technischen Aufwand.

Diskussionen im Vorfeld des Gesetzes, etwa im Rahmen der Erörterung im Normenkontrollrat im Juni 2015 über die Frage, was der vorgesehene „Stand der Technik“ bedeuten soll, haben bereits seinerzeit deutlich gemacht, dass sich der tatsächliche Aufwand weder damals als auch heute unter den nunmehr bekannten Rahmenanforderungen noch nicht vollends konkret beziffern lässt. Deutlich ist jedoch, dass die nun vorgesehenen Voraussetzungen weit über den heute üblichen und bei den Anbietern implementierten Stand der Technik hinausgehen sollen.

In Ziffer 4.2.1 des Anforderungskatalogs werden beispielsweise „besonders hohe Standards der Qualität“ bei den speicherpflichtigen Verkehrsdaten festgelegt, um die Richtigkeit und Aussagekraft der Daten sicherzustellen. Dazu ist unter anderem vorgesehen, dass „Maßnahmen zur Sicherstellung der Genauigkeit zu speichernder Zeitangaben“ implementiert werden. Für die betroffenen Unternehmen hat dies zur Folge dass diese Voraussetzungen im gesamten (eigenen) Netz vorhanden sein müssen. Diese Vorgaben sind nicht standardmäßig in sämtlichen Netzen der Anbieter vorhanden sondern müssen implementiert werden. Dies verursacht nicht nur Kosten, sondern verlängert auch die Umsetzungsdauer der Anforderungen.

Darüber hinaus sieht der Entwurf folgende Regelung vor:

---

[1] Vgl. Berichte auf heise.de vom 20.06.2016 und bei CT in Ausgabe 2016-13, abrufbar unter: http://www.heise.de/newsticker/meldung/Datenschutz-in-Polizeisystemen-haeufig-nicht-eingehalten-3242089.html; http://www.heise.de/ct/ausgabe/2016-13-Fragwuerdiger-Datenschutz-in-Polizeisystemen-3227333.html

"... Nach dieser Einrichtung, stehen dem Unternehmen Verkehrsdaten zur Verfügung, die nach §§ 96 ff. TKG gespeichert werden dürfen (nicht Gegenstand dieses Anforderungskatalogs) und Verkehrsdaten, die nach § 113b TKG gespeichert werden müssen. Die letztgenannten, speicherpflichtigen Verkehrsdaten werden dem VDS-System zugeführt..." (Ziffer 4.1 S. 7 des Entwurfs)

Diesbezüglich ist anzumerken, dass die in § 113b genannten Daten sich zum Teil mit den in §§ 96 ff. genannten Daten decken. Eine Filterung in nicht nach dem Katalog zu speichernden Daten nach §§ 96 ff. und zu speichernden Daten nach § 113b TKG wird mithin ad absurdum geführt. Zudem ist davon auszugehen, dass die berechtigten Stellen Daten nach beiden Paragraphen anfordern werden.

Dieser Konflikt wird auch an anderer Stelle noch einmal deutlich in Ziffer 5.2.3 (S. 16 des Entwurfs):

"Im Datenspeicher des VDS-Systems, auch in einer virtuellen Umsetzung, dürfen darüber hinaus neben den Verkehrsdaten nach § 113b TKG und den notwendigen Systemdateien keine sonstigen Daten gespeichert werden, insbesondere keine Daten für die in § 96 TKG genannten Zwecke. Eine Vermischung der nach § 113b gespeicherten Daten mit sonstigen Daten ist aus Gründen der Datensicherheit und zur Vermeidung der Entstehung komplexer Systeme unzulässig."

Zudem ist aus Sicht der IEN unklar, ob nur dann eine Speicherung in Deutschland im VDS-System zu erfolgen hat, wenn es eine konkrete Aufforderung einer berechtigten Stelle gibt oder ob anlasslos alle Daten nach §§ 113b ff von den Systemen nach §§ 96 ff "gespiegelt" werden müssen. In letzterem Fall können sich Konflikte mit dem Datenschutzrecht einzelner Länder, in denen die Quelldaten ggf. gespeichert werden, ergeben. Dies würde wiederum mittelbar dazu führen, dass Anbieter gezwungen wären, ihre Verkehrsdatensysteme ins Inland zurückzuverlegen – was einen unzulässigen Eingriff in die unternehmerische Freiheit der Anbieter bei der Gestaltung der Netz- und Systemtopologie bedeuten würde, insbesondere bei den Mitgliedsunternehmen, bei denen es sich ausnahmslos um international agierende Telekommunikationsanbieter handelt.

Weiterhin unklar ist auch die Vorgabe nach Ziffer 4.2.1*:*

"Um die Genauigkeit der zu speichernden Zeitangaben zu gewährleisten, ist die jeweilige Uhrzeit von Zeitservern zu beziehen, die auf der amtlichen Zeit basieren..." (Seite 8 des Entwurfs).

Hier vertreten die Mitglieder die Ansicht, dass die Qualitätssicherung jedes Anbieters, welche durch ein jährliches Sachverständigengutachten nach § 45g Abs. 2 TKG („Gutachten zur Abrechnungsgenauigkeit und Entgeltrichtigkeit bei der Verbindungspreisberechnung“) überprüft wird, ausreichend

ist, den angestrebten Zweck zu erreichen. Es bedarf daher keiner weiteren, eigenständigen Regelung.

In Ziffer 4.2.2 werden zudem automatisierte Plausibilitätsprüfungen verlangt:

„Vor der Einspeicherung in die Speichereinrichtung sollen die speicherpflichtigen Verkehrsdaten automatisiert gegen die erwarteten Formate geprüft werden, um eine grundsätzliche Plausibilitätskontrolle durchzuführen…“ (Seite 9 des Entwurfs).

Wie bereits vorstehend festgestellt, sollte die durch jährliches Gutachten bestätigte Qualitätssicherung hinsichtlich der Anforderungen an die Abrechnungsgenauigkeit und Entgeltrichtigkeit eine automatisierte Plausibilitätskontrolle überflüssig machen bzw. in das Ermessen der Anbieter gestellt werden.

2. Richtigkeit und Vollständigkeit von Drittdaten

Gemäß Ziffer 5.1.1 Abs. 3 S. 3 ist „Bei Verkehrsdaten, die aus der Signalisierung oder Abrechnung von Interconnection-Partnern stammen, […] deren Richtigkeit und Vollständigkeit durch regelmäßige Prüfungen sicherzustellen“ (Seite 11 des Entwurfs). Die Mitgliedsunternehmen unterhalten Zusammenschaltungsverträge mit einer Vielzahl anderer Anbieter, die ihrerseits den originären Verpflichtungen des Anforderungskataloges hinsichtlich der Speicherung ihrer Verkehrsdaten unterliegen. Diese Verpflichtungen muss jeder Anbieter für sich selbst erfüllen – weder dürfen sie hierbei von anderen Anbietern einer Überprüfung unterzogen werden – die eine originäre hoheitliche Aufgabe der Bundesnetzagentur darstellt – noch dürfen anderen Anbieter diese Überprüfungspflichten auferlegt werden. Ferner ist auch der personelle und finanzielle Aufwand, der für derartige Regelüberprüfungen zu betreiben wäre, nicht unerheblich. Ein dementsprechender Eingriff in die Vertragsautonomie der Anbieter bedarf stets einer gesetzlichen Grundlage, keinesfalls genügt hierfür ein bloßer Anforderungskatalog.

Zudem mangelt es der Regelung an Bestimmtheit, da weder Umfang noch Regelmäßigkeit der Prüfungen näher definiert werden. Darüber hinaus ist unklar, welche rechtlichen Folgen eine unterlassene, unregelmäßige oder nicht sorgfältig durchgeführte Überprüfung hätte. Die Anforderung ist daher insgesamt zu streichen.

3. Unverzüglichkeit der Auskunft

Unklarheiten ergeben sich auch im Hinblick auf die Vorgabe der Unverzüglichkeit der Auskunft. So wird in Ziffer 5.1.3 vorgegeben:

*"Nach § 113b Abs. 7 TKG hat die Speicherung der Verkehrsdaten so zu erfolgen, dass Auskunftsersuchen der berechtigten Stellen unverzüglich beantwortet werden können." (*S. 12 des Entwurfs)

Es stellt sich an dieser Stelle insbesondere die Frage, inwieweit etwa Ausnahmen von der 24/7 Regelung nach TKÜV (im Rahmen der Erstellung der TKÜV-Änderungsverordnung nunmehr als Entwurf der „Kundendaten-Auskunftsverordnung“ bezeichnet) beantragt werden können.

Wie bereits in den allgemeinen Anmerkungen dargelegt, erachtet die IEN insgesamt eine Klärung der Verhältnisse von der sich ebenfalls in der Diskussion befindlichen Kundendaten-AuskunftsVO und dem hier gegenständlichen Anforderungskatalog für zwingend geboten. Im Rahmen dieser Novelle der TKÜV wird gerade die Ausnahmeregel von der 24/7 Regelung höchst unklar und schwammig gestaltet. Eine Ausnahme ist weiterhin für KMUs unbedingt erforderlich und darf keinesfalls aufgeweicht werden.

4. Löschung der Daten

In Ziffer 5.2.5 werden die technischen Vorgaben der besonders sicheren Methode der Löschung von Daten aus persistenten Speichern dahingehend beschrieben, dass zunächst eine geeignete Verschlüsselung der Daten vorzunehmen und anschließend die verwendeten Schlüssel zu löschen sind. Auch an dieser Stelle wird der erhebliche Aufwand für die Unternehmen deutlich, da diese Vorgaben mit dem gegenwärtigen Stand der Technik nichts gemein haben und entsprechende Systeme erst entwickelt und implementiert werden müssen.

In diesem Zusammenhang wird ein weiteres Manko des Anforderungskatalogs deutlich: die eingeforderten Vorgaben stehen bislang isoliert und sind nicht mit bereits existierenden Vorgaben oder Standards kompatibel. Ohne einen technischen Mehrwert zu bringen, erfordern die Vorgaben mithin die bereits eingangs beschriebenen Eigenentwicklungen, die weit über den Stand der Technik hinausgehen.

Für den Fall der Löschung von Daten bedeutet dies konkret Folgendes: Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist die zentrale, unabhängige und neutrale Stelle für Fragen zur IT-Sicherheit. Es hat selber im November 2013 eine Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten entwickelt[2]. Die Leitlinie wurde von der Secorvo Security Consulting GmbH erstellt. Sie ist das Ergebnis des Projekts "Datenschutzkonformes Löschkonzept - Standardisierungsmöglichkeiten für einen Best-Practice-Ansatz" für das DIN e.V. und wurde im Rahmen des Programms "Innovation mit Normen und Standards" vom Bundesministerium für Wirtschaft und Technologie gefördert.

---

2 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Extern/Leitlinie_zur_Entwicklung_eines_Loeschkonzepts.html

Die Leitlinie definiert einige zentrale Begriffe und beschreibt, wie Löschregeln effizient festgelegt werden können. Sie gibt außerdem Hinweise für die Steuerung der Umsetzung von Löschregeln und zu den Pflegeaufgaben im Löschkonzept.

Der vorliegende Anforderungskatalog scheint jedoch in keiner Weise an diesen Leitlinien orientiert zu sein. Vielmehr das Gegenteil scheint der Fall zu sein:

Auf Seite 13 der Leitlinie wird zum Löschen von Daten festgestellt:

> *Löschen wird z. B. durch das physische Überschreiben von Datenobjekten erreicht.*
>
> *Datenobjekte können auch gelöscht werden, indem der Datenträger, auf dem sie enthalten sind, geeignet zerstört oder vernichtet wird.*
>
> *Gegebenenfalls können die Datenobjekte auch anonymisiert werden, statt sie zu löschen. Denn wenn kein Personenbezug mehr hergestellt werden kann, unterliegen sie nicht mehr den datenschutzrechtlichen Löschregeln. Daten richtig zu anonymisieren ist allerdings oft sehr schwierig.* ***Es wird dringend empfohlen, der Löschung von Daten den Vorrang zu geben.***
> *[Hervorhebung nur hier]*

Die Leitlinien referenzieren auch andere international gebräuchliche Standards, die ebenfalls eine andere Form des Löschens als bisher im Anforderungskatalog vorgesehen, nahelegen.

So diskutieren die in der Leitlinie in Bezug genommenen „Guidelines for Media Sanitization“ (NIST Special Publication 800 – 88 Revision 1[3]) das Thema „Cryptographic Erase“ durchaus kritisch[4] und legen nahe, nur unter bestimmten engen Voraussetzungen überhaupt einen „Cryptographic Erase“ zuzulassen.

Es ist nicht ersichtlich, dass der aktuelle Anforderungskatalog überhaupt mit bestehenden Leitlinien synchronisiert ist oder bestehende Empfehlungen wie die „Guidelines for Media Sanitization“ vollumfänglich umsetzt. Vielmehr stehen die bislang aufgestellten Anforderungen isoliert für sich und verursachen technisch und finanziell einen unverhältnismäßigen Implementierungsaufwand auf Seiten der Provider, ohne tatsächlich einen Mehrwert an (Daten-)Sicherheit zu generieren.

---

[3] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf.

[4] Abschnitt 2.6, S. 9 ff. des Dokuments.

Entsprechendes gilt auch für die Anforderungen an die Software und die Protokolldaten.

5. Verschlüsselung der Daten

Kritisch zu bewerten ist aus Sicht der IEN auch die Formulierung zur Verschlüsselung der Daten nach 5.2.2:

"Als besonders sicher werden nur solche Verschlüsselungsverfahren anerkannt, deren Überwindung für Unberechtigte einen unverhältnismäßig großen Aufwand erfordern würde." (S. 14 des Entwurfs)

So bleibt an dieser Stelle vollkommen unklar, was ist ein unverhältnismäßiger Aufwand tatsächlich sein soll, da der „Unberechtigte“ vollkommen unterschiedliche technische Hilfsmittel zur Verfügung haben kann.

Zu begrüßen ist aus Sicht der IEN an dieser Stelle aber, dass eine "Auslagerung an Dritte" vorgesehen ist (vgl. S. 14 des Entwurfs).

Hinzuweisen ist jedoch im Weiteren auf die bestehenden Unsicherheiten hinsichtlich der – grundsätzlich konsensfähigen Feststellung, dass „viele Unternehmen Daten zunächst in ihren Billing-Systemen sammeln, bevor sie in die VDS-Speicherinfrastruktur gelangen“ (S.15). Es ist nach wie vor nicht hinreichend klar, welche Daten genau „gespiegelt“ werden müssen und auch wann - etwa nur nach konkreter Anfrage der berechtigten Stellen oder permanent.

6. Speicherung der Daten

Weitere unklare Begrifflichkeiten finden sich schließlich auch in Ziffer 5.2.3, wonach eine „geeignete sichere Konfiguration der Systembestandteile zu gewährleisten“ ist. Hier stellt sich bereits die Frage, was als „geeignet“ gilt, was in diesem Zusammenhang eine „geeignete sichere Konfiguration“ sein soll und welche „Systembestandteile“ überhaupt betroffen sein sollen.

7. Vier-Augen-Prinzip

Die IEN kritisiert ausdrücklich die im Rahmen des Anforderungskatalogs vorgenommene Ausweitung des Vier-Augen-Prinzips. Wie bereits angesprochen führt dies zu einer personellen Belastung, die von kleinen und mittleren Unternehmen nicht zu leisten ist. Nach § 113d Ziffer 5 TKG ist das Vier-Augen-Prinzip grundsätzlich dann vorzusehen, wenn ein „Zugriff auf die Daten“ erfolgt. Die nunmehr vorgesehenen Vorgaben zum Vier-Augen-Prinzip gehen jedoch weit über eine konkrete Systemabfrage hinaus.

So enthält bereits das Rollenkonzept nach Ziffer 5.2.6.1 des Anforderungskatalogs weitreichende Vorgaben zu den personellen Anforderungen, die auch bereits in Fragen der Wartung der Firewalls, administrativer Aufgaben

ein Vier-Augen-Prinzip vorsehen. Auch der Zugang nach Ziffer 5.2.6.2 sieht im Rahmen der physischen Absicherung der Speichersysteme durchgängig die Anwendung des Vier-Augen-Prinzips vor.

Die IEN wertet dies als verzichtbare „Arbeitsbeschaffungsmaßnahme“. Was sich auch aus folgendem Zitat ergibt:

"Zum einen gibt es ermächtigte Mitarbeiter, die Anfragen berechtigter Stellen entgegen nehmen, prüfen, die Suchanfrage im Datenspeicher initiieren und die Ergebnisse an die berechtigten Stellen versenden oder aus anderen Gründen auf Verkehrsdaten zugreifen dürfen."
*"Zum anderen gibt es ermächtigte Mitarbeiter, die für die hardware- und softwaretechnische Wartung des VDS-Systems zuständig sind." (*S. 19f des Entwurfs)

An dieser Stelle wurde nach Auffassung der IEN unklar formuliert. Es ist eine Klarstellung erforderlich, wie viele verschiedene Personen minimal notwendig sein sollen für die Beauskunftung und den betrieblichen Zugriff. Wenn das Vier-Augen-Prinzip gelten soll stellt sich dennoch die Frage, wie viele Personen insgesamt betroffen sind – insbesondere auch im Hinblick auf Personen vom Hersteller mittels Fernzugriff. Gerade ein Fernzugriff sollte ausdrücklich erlaubt werden.

Erheblichen Aufwand bedeutet in diesem Zusammenhang auch das vorgesehene Raumkonzept. Verlangt werden getrennte Sicherheitsbereiche, wobei „der Teil des Rechenzentrums, in dem die Hardware-Komponenten des VDS-Systems untergebracht sind, (...) als geschlossener Sicherheitsbereich konzipiert“ sein muss. Diese Komponenten müssen durch hochwertige Zutrittskontrollmechanismen vor unbefugtem Zutritt geschützt werden. Der Zugang zu Wartungszwecken etwa soll erst nach einer Identifikation und einer Zwei-Faktor-Authentisierung unter Anwendung des Vier-Augen-Prinzips erfolgen dürfen, was die Bereitstellung eines Raums zur Vorhaltung der neuen Systeme bedeutet und welcher nur von zwei Mitarbeitern gemeinsam betreten werden darf.

Derartige Anforderungen gehen erneut vollkommen fehl, da sie die aktuell in Rechenzentren bereits zur Anwendungen kommenden Sicherheitsstandards außer Acht lassen und erneut isolierte Anforderungen aufstellen, die nur „am grünen Tisch“ ersonnen scheinen. Die angestrebten Anforderungen bringen jedenfalls erneut keinen sicherheitstechnischen Mehrwert, sondern erfordern allein kostenintensive bauliche Umgestaltungen innerhalb der Rechenzentren. Die bestehenden Sicherheitsmaßnahmen rund um den Zutritt zu einem Rechenzentrum erlauben auch heute bereits eine lückenlose Zutrittskontrolle. Externe haben realistischer Weise keine Zutrittsmöglichkeiten und selbst innerhalb der betroffenen Unternehmen wird der Zugang zu einzelnen technischen Bereichen bereits heute auf einer reinen „need to know“ Basis erteilt. Der BNetzA sind diese Sicherheitsmaßnahmen bereits aus den

schon jetzt zu erstellenden Sicherheitskonzepten der Provider gem. § 109 Abs. 4 TKG bekannt.

Auch hier zeigt sich einmal mehr, dass der Anforderungskatalog nicht mit den bereits bestehenden Anforderungen an die TK-Branche abgeglichen, sondern isoliert aufgestellt wurde.

Außer den bereits zuvor beschriebenen Mehrkosten ergibt sich hieraus aber kein sicherheitstechnischer Mehrwert.

Mit dem angestrebten Vorgehen des Anforderungskatalogs werden zudem auch die technisch ohne Probleme umsetzbaren Möglichkeiten einer Fernwartung o.ä. ausgeschlossen und den betroffenen Unternehmen jedwede Möglichkeit genommen, auf gegebene Prozesse und Arbeitsabläufe Einfluss zu nehmen und diese effizient an die gesetzlichen Vorgaben anzupassen.

Diese weitreichenden Vorgaben über den Gesetzeszweck hinaus bedeuten einen unverhältnismäßigen personellen Aufwand für die betroffenen Anbieter. Dies gilt umso mehr für die pan-Europäisch tätigen Mitgliedsunternehmen der IEN. Der Anforderungskatalog ist mithin immer auch an den Vorgaben des europäischen Rechts zu messen. Dies scheint bislang noch gar nicht der Fall gewesen zu sein.

****

Für Rückfragen stehen die Vertreter der Mitgliedsunternehmen der IEN sowie ich selbst jederzeit gern zur Verfügung. Die Stellungnahme enthält keine Betriebs- und Geschäftsgeheimnisse.

Mit freundlichen Grüßen

Malini Nanda, Rechtsanwältin
Geschäftsführerin der IEN