eco Stellungnahme

zu den Eckpunkten Sicherheitsanforderungen für Telekommunikationsnetzbetreiber der Bundesnetzagentur, des BSI und des BfDI sowie

den entsprechend angekündigten Änderungen des TKG und BSIG des Bundesministeriums des Innern und des Bundesministeriums für Wirtschaft und Energie

Berlin, 04.05.2019

Die Bundesnetzagentur hat am 07.03.2019 bekannt gegeben, neue Sicherheitsanforderungen für Telekommunikationsnetzbetreiber aufzustellen. Diese erarbeitet sie gemeinsam mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und dem Beauftragten für Datenschutz und Informationsfreiheit des Bundes. Am selben Tag haben das Bundesministerium des Innern und das Bundesministerium für Wirtschaft und Energie entsprechende Pläne zur Änderung des Telekommunikationsgesetzes und des BSI-Gesetzes bekannt gegeben.
eco bedankt sich für diese frühe Gelegenheit, Stellung nehmen zu können und nimmt diese gerne wahr. Die IT-Sicherheit und die Integrität ihrer Netzinfrastrukturen und Komponenten ist unseren Mitgliedsunternehmen seit jeher ein wichtiges Anliegen.

eco sieht die angekündigten Verschärfungen des Sicherheitskataloges nach § 109 Absatz 6 TKG und die entsprechend angekündigten Änderungen des TKG und des BSI-Gesetzes kritisch. Wir halten sie in keiner Weise für erforderlich und können abseits einer politischen Diskussion keine Belege für deren Notwendigkeit erkennen. Es gibt keine Tatsachen für fehlende Vertrauenswürdigkeit oder konkrete Vorfälle in der Netz- oder IT-Struktur der TK-Netzbetreiber, welche die ankündigten Verschärfungen geboten erscheinen ließen. Teilweise wirken sich die avisierten Maßnahmen sogar kontraproduktiv auf die IT-Sicherheit aus. Das für 2025 gesetzte Ziel, einer flächendeckenden Gigabitversorgung in Deutschland wird mit diesen Verschärfungen unerreichbar.

I. Eckpunkte neue Sicherheitsanforderungen Bundesnetzagentur

- Keine Erforderlichkeit

In Deutschland gelten bereits sehr hohe Anforderungen an die Sicherheit in TK-Netzen, die in einem bewährten und konstruktiven Prozess zunächst

gemeinsam mit der Branche und der Bundesnetzagentur erarbeitet wurden. Letztere legt bereits jetzt im Einvernehmen mit dem BSI und dem BfDI den Sicherheitskatalog nach § 109 Abs. 6 TKG fest. Die Bundesnetzagentur kontrolliert im Rahmen der Überprüfung des Sicherheitskonzeptes auch die Einhaltung der Vorgaben aus dem Sicherheitskatalog. Dank der Vorgaben, deren Einhaltung durch die Netzbetreiber und der Kontrolle durch die BNetzA wird ein durchgängig hohes Sicherheitsniveau gewährleistet und demgemäß gab es keine nennenswerten Zwischenfälle in den TK-Netzen in Deutschland.

eco hält die angekündigten Verschärfungen vor diesem Hintergrund für nicht erforderlich. Es gibt bereits keinerlei belastbare Tatsachen, die gegen die Vertrauenswürdigkeit eines oder mehrerer Hersteller sprächen. Zwar besteht immer ein abstrakt-generelles Risiko für die Integrität von IT-Systemen und für Daten. Dies ist jedoch unabhängig vom Hersteller der Netzwerktechnik, über das Daten transportiert werden und unabhängig vom Herkunftsstaat der Hersteller. Es gibt keine Belege, dass sich dieses abstrakt-generelle Risiko in TK-Netzen verändert hätte oder gestiegen wäre.
Weiter gab es keine konkreten Sicherheitsvorfälle in den Netzen der deutschen TK-Betreiber, welche diese verschärften Maßnahmen notwendig machten. Diese vorgeschlagenen Maßnahmen sind außerdem nicht geeignet, tatsächlich ein deutlich höheres Sicherheitsniveau in der Netzstruktur zu schaffen, denn auch dadurch kann Abfluss von Daten nicht mit Sicherheit verhindert werden.
Wir bitten insoweit die Bundesnetzagentur, das BSI und den BfDI entsprechend um eine substanzielle und detaillierte Begründung für die jeweilige Erforderlichkeit der einzelnen vorgeschlagenen Eckpunkte, insbesondere warum mildere Mittel als nicht gleichermaßen wirksam angesehen werden, wie Verschlüsselung von Daten. Darüber hinaus mögen die Behörden bitte konkret darlegen, wie sich die vorgeschlagenen Maßnahmen zum Schutz von zu benennenden Gefahren bzw. Risiken eignen.

- Verstoß gg. Übermaßverbot - Mangelnde Differenzierung

Die vorgesehenen Auflagen dürften ob ihrer bisherigen Undifferenziertheit hinsichtlich Größe, Umsatz und Kundenzahl bei Netzbetreibern gegen das Übermaßverbot verstoßen. Sie stellen wegen der hohen Kosten und Haftungsrisiken ein ernstzunehmendes Hemmnis sowohl bei laufenden Kreditverhandlungen als auch bei bestehenden Finanzierungen von TK-Netzbetreibern dar. Allein die undifferenzierte Ankündigung deutlich verschärfter Sicherheitsauflagen hat zu entsprechenden Unsicherheiten

geführt. Kreditgeber könnten sich veranlasst sehen, dass Kreditrisiko erneut zu bewerten, da der Staat nun bekannt gemacht hat, Sicherheitsauflagen deutlich zu erhöhen. In der Konsequenz sind die avisierten Auflagen überaus geeignet, kleine Netzbetreiber vom Markt zu drängen, da sie sehr wahrscheinlich schwerer Kredite erhalten werden. Die Folge ist die Einschränkung des Wettbewerbs mit Verringerung von Innovationen und steigenden Preisen.

Deshalb fordern wir eine sachgerechte Differenzierung, wie bei der Kundendatenauskunftsverordnung (KDAV) oder der Telekommunikationsüberwachungsverordnung (TKÜV), die besonders kostenintensive Anforderungen erst ab einer festgelegten, größeren Kundenzahl vorschreibt. Alternativ sind denkbar auf Umsatz bezogene Festlegungen, im Sinne von § 267 HGB oder entsprechend der Empfehlung der EU-Kommission 2003/361/EG (L 124/36 v. 20.05.2003), welche zusätzlich zum Umsatz die Mitarbeiterzahl miteinbezieht.

▪ Gefährdung der IT-Sicherheit durch Verzögerung
Eckpunkt BNetzA: „*Sicherheitsrelevante Netz- und Systemkomponenten (kritische Kernkomponenten) dürfen nur eingesetzt werden, wenn sie von einer vom BSI anerkannten Prüfstelle auf IT-Sicherheit überprüft und vom BSI zertifiziert wurden.*

- Sicherheitsrelevante Netz- und Systemkomponenten (kritische Kernkomponenten) dürfen nur nach einer geeigneten Abnahmeprüfung bei Zulieferung eingesetzt werden und müssen regelmäßig Sicherheitsprüfungen unterzogen werden. Sollten bei den Prüfungen Abweichungen gegenüber den Leistungsvorgaben der Netzbetreiber oder Erbringer auftreten, sind diese zu dokumentieren und einem Risikobehandlungsprozess zuzuführen. Bei Abweichungen, die zu erheblichen Beeinträchtigungen von Telekommunikationsnetzen und -diensten führen können, sind die BNetzA und das BSI über die zur Minderung des Risikos ergriffenen Maßnahmen umgehend zu informieren.“

Zu bedenken ist, dass bei einem konkreten Sicherheitsvorfall in einem TK-Netz die unverzügliche Behebung bei einer kritischen Kernkomponente massiv verzögert werden würde. Diese Verzögerungen entstünden durch die Prüfung durch die anerkannte Prüfstelle, danach wegen der Zertifizierung durch das BSI und schließlich durch die geeignete Abnahmeprüfung vor dem Einbau. Sollte eine daraus resultierende Verzögerung zu einem Schaden

führen, der ohne dieses langwierige staatliche Prüfverfahren nicht eingetreten wäre, wirft das auch Haftungsfragen auf.

Wenn überhaupt, wäre eine Eilfall-Regelung dringend geboten, welche die Behebung einer erheblichen, konkreten Gefährdung der IT-Sicherheit schnellstmöglich zulässt und Kontrollen im Nachgang vorsieht. In Fällen von hoher Kritikalität bzgl. der Gefahr für besondere Rechtsgüter und/oder in zeitlicher Hinsicht ist häufig eine rasche Lösung innerhalb von mehreren Stunden oder wenigen Tagen notwendig. Bei strikter Einhaltung des dreistufigen Prüfprozesses ist dies unmöglich. Dieser Prüfprozess wird Wochen andauern, ein undenkbarer Zeitraum bei einer kritischen Lücke. Wird letztere bekannt, steigt außerdem das Risiko des Ausnutzens durch Angreifer erheblich an und gebietet umso mehr das eilige Schließen der Lücke. Das Offenbleiben dieser Lücke wird erst recht andauern, wenn die Abnahmeprüfung auch von behördlicher Seite aus erfolgen soll.
Um nicht sinnvolle Doppelprüfungen zu vermeiden, sind Inhalt und Form der Abnahmeprüfungen und die Prüfungsinhalte der BSI-Zertifizierung aufeinander abzustimmen, sodass bei der Abnahme nur Punkte zu kontrollieren sind, die nicht bereits bei der Zertifizierung überprüft worden sind.

- Vertrauenswürdiger Hersteller

Auszug Eckpunkt BNetzA*: „Kritische Kernkomponenten dürfen nur von solchen Lieferanten/Herstellern bezogen werden, die in geeigneter Weise ihre Vertrauenswürdigkeit zusichern. Die Verpflichtung soll für die gesamte Lieferkette gelten und Voraussetzung für die notwendige Zertifizierung der Komponenten sein. Diese Vorgaben werden im Katalog weiter konkretisiert werden. Die hierfür zugrundeliegenden Standards werden vom BSI im Benehmen mit der BNetzA veröffentlicht.*“

Diese Vorgabe ist in hohem Maße unbestimmt und deshalb geeignet Rechtsunsicherheit zu erzeugen. Der Verweis auf § 9 BSIG in den Pressemitteilungen des BMWi und des BMI lässt sogar darauf schließen, dass die Anwendbarkeit der angestrebten Regelung im Sinne von § 9 Abs. 4 Nr. 2 BSIG nur eingeschränkt gerichtlicher Kontrolle unterläge. Der umgekehrt eröffnete Beurteilungsspielraum, ob vage sicherheitspolitische Belange der BRD gegen die Vertrauenswürdigkeit eines oder mehrerer Hersteller sprechen, würde sich somit nicht originär an der IT-Sicherheit der kritischen Kernkomponenten orientieren, sondern von einer lediglich politischen Einschätzung abhängig gemacht. Das dient weder der IT-Sicherheit von Staat, Gesellschaft und Unternehmen noch der Rechts- und

Planungssicherheit der TK-Netzbetreiber, TK-Diensteanbieter und TK-Hersteller.

Zudem halten wir diese Verschärfung für nicht erforderlich und für unangemessen im rechtlichen Sinne. Es ist vollkommen ausreichend, wenn die noch näher festzulegenden „kritischen Kernkomponenten“ in TK-Netzen von einer anerkannten Prüfstelle und danach vom BSI zu zertifizieren sind. Damit ist die Vertrauenswürdigkeit nach unserer Auffassung ausreichend dargelegt.

▪ Anlasslose Beobachtung des Netzverkehres
Eckpunkt BNetzA: „*Der Netzverkehr muss ständig auf Auffälligkeiten hin beobachtet werden und im Zweifelsfall sind geeignete Maßnahmen zum Schutz zu ergreifen (z.B. Netzverkehr unterbinden, Verkehr zu Störern einschränken oder unterbinden). Die Detektionsmaßnahmen müssen dem Stand der Technik entsprechen.*“

Dieser Eckpunkt ist nach unserer Auffassung unter mehreren Gesichtspunkten unverhältnismäßig.

Zum einen ist eine anlasslose, regelmäßige, kontinuierliche und tiefgehende Überwachung des Netzverkehrs eine unangemessene Belastung für die Netzbetreiber. Sie verletzt das dem Netzbetrieb innewohnende Regel-Ausnahme-Verhältnis. Bei Auffälligkeiten sollte ein Netzbetreiber prüfen, ob ein Sicherheitsvorfall vorliegt; er sollte hingegen nicht alles überwachen müssen, um Auffälligkeiten zu finden. Außerdem ist diese Pflicht im Hinblick auf den entstehenden finanziellen, personellen und zeitlichen Aufwand für die TK-Netzbetreiber unverhältnismäßig.

Zudem sind die Begriffe unbestimmt. Im Sinne einer Rechtmäßigkeit und Planungssicherheit sind jedenfalls bei einer solchen Regelung der Anwendungsbereich der Netzanalyse und die Prüfungstiefe des Netzverkehrs stark erläuterungsbedürftig und sollte daher seitens der BNetzA noch deutlich konkreter beschrieben werden. So wäre bspw. die Bedeutung des Wortes „ständig“ unter Beachtung der Verhältnismäßigkeit zu präzisieren und es wäre zu erläutern, auf welche neuen Auffälligkeiten die Netzbetreiber nun weiteres Augenmerk legen sollen.

Wir gehen insoweit davon aus, dass alleine eine systematische Beobachtung aller Netzverkehre der kritischen Kernkomponenten auf Auffälligkeiten gemeint ist, nicht ein Screening und eine Beobachtung aller Netzverkehre

inklusive der Kundenverkehre. Vorstellbar wäre eine systematische Untersuchung der reinen Managementverkehre der Netzkomponenten. Diese wäre ohne größere Schwierigkeiten umsetzbar.
Hier können auch "übliche" Verkehrsmuster angelernt und automatisch mit den aktuellen Mustern verglichen werden.

Außerdem sind die Vorgaben der TSM-VO zur Netzneutralität sowie die Vorgaben der DSGVO und des TKG zum Datenschutz dringend zu beachten. Demnach ist eine Beobachtung von Kundenverkehren aus Sicht des Verbandes als überbordend und nicht mit den Vorgaben der Vertraulichkeit der Kommunikation zu vereinbaren anzusehen. Dies gilt selbst dann, wenn eine Untersuchung alleine auf Verbindungsdaten und nicht auf Inhaltsdaten zu beziehen wäre, für welche nach unserer Auffassung ein identisches Schutzniveau zu gewährleisten ist.

▪ Kritische Kernkomponenten
Aus den Eckpunkten der BNetzA: „*Sicherheitsrelevante Netz- und Systemkomponenten (kritische Kernkomponenten) dürfen nur eingesetzt werden, wenn sie von einer vom BSI anerkannten Prüfstelle auf IT-Sicherheit überprüft und vom BSI zertifiziert wurden.*

- Um die Verbindlichkeit der Anforderungen sicherzustellen und konkrete Anforderungen wie etwa die Zertifizierungspflicht rechtlich eindeutig abzusichern, planen die zuständigen Ministerien entsprechende gesetzliche Absicherungen, insbesondere im Rahmen der laufenden großen Novelle des Telekommunikationsgesetzes.

- Die Festlegung der sicherheitsrelevanten Netz- und Systemkomponenten (kritische Kernkomponenten) erfolgt einvernehmlich zwischen BSI und BNetzA.“

eco und seine betroffenen Mitgliedsunternehmen sind der Ansicht, dass auf Grund der unverändert gebliebenen Risikolage in TK-Netzen nur wenige Netz- und Systemkomponenten als sicherheitsrelevant (kritische Kernkomponenten) angesehen werden können, diese nur in wenigen TK-Netzen eingesetzt werden und dort jeweils auch nicht sehr häufig. Gegenüber den gegenwärtigen Mobilfunknetzen 2G, 3G und 4G und anderen bestehenden TK-Netzen dürfte es bis auf wenige Ausnahmen nur wenige neue Komponenten geben, über die wesentlich sensiblere bzw. schützenswertere Daten als bisher transportiert werden. Dieses angeblich gesteigerte Risiko im Vergleich zu den bestehenden Netzen, in welchen die Technik vorgeblich unzuverlässiger Hersteller bereits vielfach eingesetzt

wurde und wird, und insbesondere den Nachweis dieses Risikos, sehen wir als zwingende Voraussetzung einer substanziell anderen Behandlung mit erheblichen Mehrbelastungen im Vergleich zu vorher.

Im Hinblick auf die Festlegung der kritischen Kernkomponenten ist sicherzustellen, dass diese praktikabel und eindeutig zu identifizieren sind. Wir halten es für sehr sinnvoll, unter Federführung der BNetzA und Einbeziehung der Anbieter von TK-Diensten und TK-Netzbetreiber sowie anderer Behörden in einem Arbeitskreis die Festlegungen gemeinsam zu erarbeiten. Dabei ist auf sinnvolle Bezugsgrößen zu achten, d. h. es könnte die Menge der durch die kritischen Kernkomponenten geflossenen Kundendaten maßgeblich sein oder bei einem Ausfall eine festgelegte Mindestanzahl betroffener Kunden.

▪ Nachweispflicht Hardware und Quellcode
Eckpunkt BNetzA: *„Es ist nachzuweisen, dass die für ausgewählte, sicherheitsrelevante Komponenten geprüfte Hardware und der Quellcode am Ende der Lieferkette tatsächlich in den verwendeten Produkten zum Einsatz kommen.“*

Unklar ist, wer der Adressat dieser Verpflichtung sein soll; dies wäre klarzustellen. Außerdem ist detailliert darzulegen, wie diese Prüfung durchzuführen ist, wie der entsprechende Nachweis erfolgreich erbracht werden kann und wem gegenüber dieser Nachweis zu erbringen wäre.

Angesichts der Vielzahl an Netz- und Systemkomponenten und deren komplexen Aufbaus, der noch größeren Menge an Software und der hohen Dynamik in diesem Bereich bestehen erhebliche Bedenken an der Angemessenheit dieser Vorgabe und ihrer Erfüllbarkeit. Das gilt insbesondere für etwaige Kontrollen in diesem Kontext durch BSI und BNetzA. Veranschaulicht sei das hier durch individuelle Betriebssoftware, welche häufig in Netz- und Systemkomponenten eingesetzt wird. Diese individuelle Betriebssoftware ist funktional auf das für den Einsatz beim jeweiligen Netzbetreiber Nötige reduziert. Diese Reduzierung erhöht gerade die Sicherheit, indem ungenutzte Module wegfallen. Allerdings stellt sich nun konkret die Frage, was in diesem Fall genau zertifiziert werden soll. Ist dann eine Art "Bauartprüfung" ohne Betrachtung des konkreten Modells, gleichsam individuelle Betriebssoftware, angedacht?

Offen lassen die Eckpunkte auch, was für Anbieter von öffentlich zugänglichen Telekommunikationsdiensten gilt. Oft verwenden diese

OpenSource oder selbstentwickelte Software. Durch die Offenlegung von Quelltext in der Öffentlichkeit (OpenSource) ist es erheblich erschwert, gezielt einzelne Unternehmen zu sabotieren. Zudem ist in diesen Fällen gut nachvollziehbar, wie eine etwaige Lücke genutzt wurde und/oder die Arbeitsweise der Angriffssoftware. Eine Zertifizierung ist überflüssig.

Selbstentwickelte Software kann die IT-Sicherheit der Komponenten erhöhen, da Standard-Malware für einen erfolgreichen Angriff ungeeignet ist. Darüber hinaus sind bei TK-Diensteanbietern, welche OpenSource oder selbstentwickelte Software verwenden, der Adressat der Zertifizierungspflicht und deren Gegenstand völlig unklar.

Es erscheint kaum realistisch, dass seitens des BSI jede Version jeder Betriebssoftware nebst jedem Update jedes Netzbetreibers (nicht Hersteller) immer individuell zertifiziert wird. Wenn aber dies nicht alles geprüft werden kann, ist jedoch eine Prüfung auf angebliche Hintertüren bereits im Ansatz gescheitert, da ein Auffinden derselben beliebig und dem Zufall überlassen wird.

- Kostentragung

In den Eckpunkten gibt keinerlei Aussage zu den mit einer Zertifizierung verbundenen Kosten oder der Attribuierung derselben an einen "Verursacher".
Unklar ist, wer beispielsweise für eine individuelle Prüfung von Systemsoftware aufkommen soll oder wer eine Prüfung von beliebten, in kritischen Bereichen eingesetzten Softwaren wie Linux, Bind, NHD, Sendmail, Postfix, MariaDB oder ähnlichem bezahlen soll und für originäre oder durch Updates verursachte weitere Prüfkosten aufkommen soll. Nach unserer Ansicht hat die öffentliche Hand diese Kosten zu tragen.

- Diversitätsvorgabe

Eckpunkt BNetzA: *„Bei Planung und Aufbau der Netze ist eine ausreichende Diversität durch Einsatz von Netz- und Systemkomponenten unterschiedlicher Hersteller sicherzustellen. Diese Vorgabe wird von der BNetzA konkretisiert und kann etwa für das Core- bzw. Access-Network unterschiedlich ausfallen.“*

eco geht davon aus, dass diese Vorgabe ausschließlich für kritische Kernkomponenten oder einen Teil dieser kritischen Kernkomponenten gelten soll, hingegen nicht für alle Netz- und Systemkomponenten zum Betreiben

von öffentlichen Telekommunikationsnetzen und öffentlich zugänglichen Telekommunikationsdiensten.

Zu beachten ist, dass diese Anforderung, wenn sie eher allgemein ausformuliert wird, bereits der gängigen Praxis der Netzbetreiber entspricht. Dies folgt aus den eigenen Erfahrungen der TK-Netzbetreiber hinsichtlich technischer, elektronischer und softwarebezogener Kompatibilität von Netz- und Systemkomponenten zur Erhöhung der IT-Sicherheit. Nach unserer Ausfassung sind all diese Umstände einer abstrakt-generellen Regelung kaum sinnvoll zugänglich.

Fällt diese Pflicht hingegen zu konkret aus, schafft sie selbst mehrere Sicherheitsrisiken. Denn zu konkrete Vorgaben zur Diversität für alle Netzbetreiber machen die konkreten Netztopologien vorhersehbar. Dies könnten sich auch Angreifer zu Nutze machen. Des Weiteren steigert eine Mehr-Lieferanten-/ Herstellerstrategie die Komplexität und kann auch zusätzliche Schwachstellen schaffen.

Die bisherigen Erfahrungen belegen, dass die internationale Normierung, auch aufgrund der durch Hersteller selbst durchgeführten Implementierung, für sich genommen keine Garantie für einen sicheren Betrieb bei herstellerübergreifenden Netz- und Systemkomponenten ist.

Die Vorgabe der Diversität ist mit der Anforderung nach Redundanz abzustimmen, um dem Angemessenheitsgrundsatz des TKG noch zu entsprechen.

▪ Ausgewiesenes Fachpersonal
Eckpunkt BNetzA: „*In sicherheitsrelevanten Bereichen darf nur eingewiesenes Fachpersonal mit vertieften Systemkenntnissen zur Bewertung von Gefährdungen und Schutzmaßnahmen eingesetzt werden. Dieses Personal ist in ausreichendem Umfang vorzuhalten.*“
eco sieht als klärungsbedürftig an, was jeweils unter den Begriffen „sicherheitsrelevante Bereiche“ und „vertiefte Systemkenntnisse“ zu verstehen ist. Ebenfalls ist zu konkretisieren, welches Fachpersonal bei welcher Tätigkeit hier gemeint ist.
Jedenfalls schließen wir aus der inhärenten Einschränkung bzgl. „Bereiche“, dass nicht alle Bereiche des TK-Netzes als sicherheitsrelevant angesehen werden.

▪ Auslagerung
Eckpunkt BNetzA: „*Die Netzbetreiber und Erbringer müssen bei Auslagerung von systemrelevanten Prozessen sicherstellen, dass unabhängige, fachkompetente und zuverlässige Auftragnehmer ausgewählt werden und die Einhaltung von gesetzlichen Vorgaben gewährleistet bleibt. Sie haben dies nachzuweisen.*“
Welche Art von systemrelevanten Prozessen im Fokus dieser Anforderung steht und wie diese mit den kritischen Kernkomponenten zusammenhängt, ist unklar. Diese ist deutlich konkreter zu beschreiben.

Zu präzisieren ist auch, hinsichtlich welcher gesetzlichen Vorgaben eine Nachweispflicht besteht, wer deren Adressat ist, wer die Nachweise vorzuhalten hat und wem gegenüber er den Nachweis zu führen hat.

▪ Übergangsfristen
Wie im TKG bei anderen Themen, bspw. Vorgaben zur Technik bei der Telekommunikationsüberwachung sind angemessene und ausreichende Übergangszeiträume zur Erfüllung durch die TK-Netzbetreiber vorzusehen (vgl. § 110 Absatz 5 Satz 1 TKG).

▪ Rechte sind zugleich Pflichten der Behörden
Die angekündigten Kontrollbefugnisse der Bundesnetzagentur und des BSI, u. a. die Festlegung und die Kontrolle der sicherheitsrelevanten Netz- und Systemkomponenten sind dann nicht nur Rechte beider Bundesoberbehörden, sondern zugleich auch deren Pflichten, die sie zu erfüllen haben. Zur Erfüllung dieser Pflichten müssen beide Häuser dann sowohl sachlich als auch personell in der Lage sein. Erfolgen keine umfangreichen Budgetbewilligungen für die materielle Ausstattung und Personal vorgenommen, ist die praktische Fähigkeit zur Erfüllung der Pflichten mehr als fraglich. Dies ist im Sinne der IT-Sicherheit geboten, insbesondere in einer konkreten Bedrohungslage, bei der unverzügliches Handeln erforderlich und geboten ist. Die unausweichlichen Verzögerungen durch die geplanten mehrstufigen und langwierigen Prozesse stehen außerdem politisch gewünschten flächenendeckenden Ausbau von gigabitfähigen Netzen bis 2025 entgegen (s. o.).

Der bereits bewilligte Stellenzuwachs beim BSI von 350 Mitarbeitern ist gänzlich für andere Aufgaben verplant. Letztere sind gesetzlich vorgesehenen Aufgaben, werden nicht entfallen, und können nicht ohne weiteres zurückgestellt oder umgewidmet werden. Über die fehlenden Budgets hinaus ist absehbar, dass die Suche nach geeigneten – und

gewillten – Fachkräften erhebliche Schwierigkeiten bereiten wird. Letztere bestehen bereits heute bei
der Deckung des Bedarfs an kompetenten Informatikern, Software-Programmierern und an anderen technischen Berufen. Das liegt nicht nur an dem hohen Bedarf der Industrie und Wirtschaft an solchem Personal und dem dem generellen Mangel an solchem Personal, sondern auch und insbesondere an der kaum konkurrenzfähigen Besoldung/Gehältern im öffentlichen Dienst.

- Kein nationaler Alleingang

eco lehnt einen nationalen Alleingang Deutschlands ab. Insbesondere für unsere Mitglieder, die in mehreren EU-Staaten agieren, ist ein harmonisierter Ansatz von großer Bedeutung. Ein nationaler Flickenteppich widerspricht auch dem Konzept eines gemeinsamen digitalen Binnenmarktes.

Erste Anzeichen für europäisches Vorgehen sieht eco grundsätzlich positiv. So hat der Europäische Rat am 22.03.2019 festgestellt, dass er einen EU-weiten Ansatz zur Gewährleistung der Sicherheit von 5G Netzen positiv sieht. Am 26.03.2019 empfahl die EU-Kommission u. a., dass die Mitgliedsstaaten (MS) bis Mitte Juli 2019 eine eigene Risikoanalyse der 5G-Infrastrukturen vornehmen und an die Agentur der Europäischen Union für Cybersicherheit (ENISA) senden sollen. Parallel dazu will die EU-Kommission mit den MS Koordinierungsarbeiten innerhalb der NIS-Kooperationsgruppe aufnehmen.
Die ENISA soll einen Bericht über die 5G-Bedrohungslage abschließen, auf dessen Grundlage die Mitgliedstaaten bis zum 1. Oktober 2019 die EU-weite Risikobewertung vornehmen werden. Bis zum 31. Dezember 2019 sollte sich die NIS-Kooperationsgruppe dann auf Risikominderungsmaßnahmen einigen, mit denen auf die festgestellten Cybersicherheitsrisiken auf nationaler und EU-Ebene reagiert werden soll.
Sobald der Cybersecurity-Act in Kraft tritt, werden die Kommission und die ENISA den EU-weiten Zertifizierungsrahmen aufstellen. Die MS sind aufgerufen, mit der Kommission und der ENISA zusammenzuarbeiten, damit das Zertifizierungssystem für 5G-Netze und -Ausrüstungen vorrangig eingerichtet wird.
Der letztgenannte Aufruf stellt nach Ansicht des eco klar, dass sich die Mitgliedsstaaten bzgl. Sicherheitsvorgaben auf 5G konzentrieren sollten, unabhängig vom Hersteller, sowohl zeitlich als auch sachlich. Darüber hinaus sieht EU-Kommission in dieser Empfehlung keinen Anlass für generelle Verschärfungen der Sicherheitsanforderungen für alle TK-Netzbetreiber.

II. Vorläufiges Fazit

In Deutschland weisen die TK-Netze bereits jetzt ein sehr hohes Sicherheitsniveau auf. Belastbare Tatsachen für Zweifel an der Integrität von Herstellern oder konkrete Sicherheitsvorfälle, die eine Notwendigkeit der Verschärfung der Sicherheitsanforderungen gegenüber den bisher geltenden aufzeigen, liegen nicht vor. Wären die Änderungen aber bei unveränderter Sachlage erforderlich, also vor der gegenwärtigen Debatte, dann wäre das ein Beleg, dass die agierenden Behörden bisher ihren Aufgaben nicht genügend nachgekommen wären und die IT-Sicherheit der TK-Netze vernachlässigt hätten. Für einen nur gefühlten Sicherheitsgewinn, nicht aber tatsächlichen, schafft man übereilt neue Auflagen.

Das Risiko eines Abflusses von Daten ist nie zu 100% auszuschließen. Ein weitaus sinnvolleres Mittel zum Schutz von Daten ist deren Verschlüsselung, die bei einer Vielzahl von Datenarten rechtlich vorgeschrieben ist (Datenschutz, Finanzsektor, usw.). Sicher ist hingegen, dass eine Umsetzung der vorgeschlagenen Maßnahmen alle betroffenen Unternehmen finanziell und personell erheblich belasten würde. Diese Belastungen sind unserer Ansicht nach von der öffentlichen Hand zu tragen. Zudem sind zur Wahrung der Verhältnismäßigkeit, sachgerechte und nachvollziehbare Differenzierungskriterien unternehmensbezogen vorzusehen, bspw. nach Risiko gemessen an Kundenzahl und Unternehmensgröße.

Nach unserer Auffassung gefährdet der skizzierte dreistufige Prüfungsprozess die IT-Sicherheit der TK-Netze wegen der offensichtlich daraus folgenden Verzögerungen konkret und generell, besonders aber im Eilfall. Dabei riskiert man das erneute Brechen eines Versprechens bei der Breitbandversorgung und nimmt höhere Preise für alle Endnutzer in Kauf. Dafür steigt im Gegenzug weder das Sicherheitsniveau tatsächlich und signifikant noch erhalten die Endnutzer für die höheren Preise qualitativ bessere Leistungen. Folglich hemmt man so die eigene Wirtschafts- und Industriepolitik und gefährdet die Wettbewerbsfähigkeit Deutschlands.

eco sieht dringenden Bedarf für einen harmonisierten Ansatz, in der Art wie von der EU-Kommission empfohlen. Das ist auch im Sinne eines europäischen digitalen Binnenmarktes und somit auch im Interesse der betroffenen Unternehmen. Letztere legen großen Wert auf die IT-Sicherheit und die Wahrung der Integrität ihrer Netze und auf den Schutz der Daten, insbesondere ihrer Kundendaten.

Für Gespräche stehen wir jederzeit gerne zur Verfügung.

Über eco: Mit über 1.100 Mitgliedsunternehmen ist eco der größte Verband der Internetwirtschaft in Europa. Seit 1995 gestaltet eco maßgeblich das Internet, fördert neue Technologien, formt Rahmenbedingungen und vertritt die Interessen seiner Mitglieder gegenüber der Politik und in internationalen Gremien. Leitthemen sind Zuverlässigkeit und Stärkung der digitalen Infrastruktur, IT-Sicherheit und Vertrauen sowie Ethik und Selbstregulierung. Deshalb setzt sich eco für ein freies, technikneutrales und leistungsstarkes Internet ein.