IEN · Marienstr. 30 · 10117 Berlin

Bundesnetzagentur
Referat IS 17
An der Trift 40
66123 Saarbrücken

Per Email an: IS17.Postfach@Bundesnetzagentur.de

Berlin, den
17.04.2019

Eckpunkte der BNetzA zusätzlicher Sicherheitsanforderungen für Telekommunikationsnetze

Stellungnahme der Initiative Europäischer Netzbetreiber

Die Bundesnetzagentur überarbeitet derzeit im Einvernehmen mit dem Bundesamt für Informationstechnik (BSI) die Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten. Insbesondere für Betreiber von öffentlichen Telekommunikationsnetzen mit erhöhtem Gefährdungspotenzial sollen Sicherheitsanforderungen spezifiziert werden, die bei der Festlegung von angemessenen technischen Vorkehrungen oder sonstigen Maßnahmen zu beachten sein werden. Dazu hat die BNetzA im März 2019 Eckpunkte veröffentlicht und interessierten Parteien die Gelegenheit zur Stellungnahme eingeräumt.

Die IEN begrüßt grundsätzlich die Veröffentlichung der Eckpunkte im Vorfeld der Überarbeitung des Katalogs von Sicherheitsanforderungen gemäß § 109 Abs. 6 TKG und nimmt die Gelegenheit zur Stellungnahme gerne wahr.

I. Allgemeine Anmerkungen

1. Erforderlichkeit der Verschärfung fragwürdig

Die IEN als Verband international tätiger Anbieter von grenzüberschreitendenden Telekommunikationsdienstleistungen für große Unternehmenskunden und Behörden setzt sich bereits seit vielen Jahren für möglichst weitgehende Harmonisierung, insbesondere bei der Identifikation kritischer Infrastrukturen und Komponenten bei gleichzeitiger

…

INITIATIVE EUROPÄISCHER NETZBETREIBER

MITGLIEDER
Colt
Orange Business
Verizon
Vodafone

SITZ UND BÜRO
Marienstr. 30
10117 Berlin

GESCHÄFTSFÜHRUNG
RAin Malini Nanda

VORSTAND
Dr. Jutta Merkt
Dr. Andreas Peya
Christian Weber

KONTAKTE
Telefon +49 30 3253 8066
Telefax +49 30 3253 8067
info@ien-berlin.com
www.ien-berlin.com

Berücksichtigung der hohen Anforderungen, welche die Kunden der IEN-Mitgliedsunternehmen an die Dienstleister stellen, ein. Die IEN-Mitgliedsunternehmen haben bereits aufgrund ihres eigenen Geschäftsfokus ein erhebliches Interesse an der Sicherheit ihrer Infrastrukturen und räumen diesem Aspekt im Rahmen ihrer Aktivitäten und Strategien einen erheblichen Stellenwert ein.

Vor diesem Hintergrund erachtet die IEN die geplanten Änderungen des IT-SicherheitsG sowie die Überarbeitung des Katalogs gemäß § 109 Abs. 6 TKG hinsichtlich rein nationaler Aspekte als kritisch. Es sind aus Sicht der IEN keine belastbaren Tatsachen, die gegen die Vertrauenswürdigkeit eines oder mehrerer Hersteller sprächen, ersichtlich. Dies hat die BNetzA auch jüngst gerade hinsichtlich der Spionagevorwürfe gegen Huawei bestätigt.[1]

Zudem kam es zu keinen konkreten Sicherheitsvorfällen in den Netzen der Anbieter, welche eine Verschärfung der Maßnahmen erforderlich gemacht hätten. Darüber hinaus möchte die IEN bezweifeln, dass die geplanten Maßnahmen tatsächlich geeignet sind, ein signifikant höheres Sicherheitsniveau in der Netzstruktur zu schaffen.

Gerade weil eine geänderte, akute Risikosituation oder sonstige Gefährdung ersichtlich ist, dürfen etwaige Anpassungen lediglich mit Augenmaß und unter Wahrung des Grundsatzes der Verhältnismäßigkeit durchgeführt werden.

2. Internationale Standards und Vorgaben berücksichtigen

Da die Dienstleistungen der IEN-Mitgliedsunternehmen überwiegend grenzüberschreitend stattfinden, haben diese Unternehmen insbesondere auch ein erhebliches Interesse daran, dass die internen Sicherheitsprozesse möglichst zentralisiert und länderübergreifend einheitlich durchgeführt werden und dass entsprechende regulatorische Vorgaben diesen Ansatz unterstützen.

[1] Vgl Heise-Mitteilung vom 15.04.2019: Regulierer: "Keine konkreten Hinweise gegen Huawei" abrufbar unter: https://www.heise.de/newsticker/meldung/Regulierer-Keine-konkreten-Hinweise-gegen-Huawei-4399689.html

Dies dient zudem auch dem Ziel der Erreichung größtmöglicher Harmonisierung im Binnenmarkt, welches erheblich beeinträchtigt würde, wenn die Mitgliedstaaten jeweils unterschiedliche Kriterien bei Identifikation der kritischen Infrastrukturen zugrunde legen würden. Dies kann aus Sicht der IEN nur durch ein effektives, transparentes und zentralisiertes Gesamtkonzept erreicht werden, welches gerade nicht nur Verpflichtungen für Netzbetreiber vorsieht, sondern als Ende-zu-Ende Konzept auch andere betroffene Marktbeteiligte und regulatorische Vorgaben (NIS Vorgaben) mitberücksichtigt. Daher wird insbesondere die Überarbeitung des Katalogs vor dem Hintergrund der ENISA-Empfehlungen im Grundsatz begrüßt und die stringente Orientierung an internationalen Standards anstelle von nationalen Sonderwegen gefordert.

Dies ist umso wichtiger gerade vor dem Hintergrund, dass sich die betreffenden TK-Infrastrukturanbieter, deren Dienstleistungen überwiegend grenzüberschreitend erbracht werden, im Fall der Festlegung von nationalen Einzelregelungen häufig unterschiedlichen Vorgaben für ein und dieselbe Dienstleistung für ein und denselben Kunden gegenübersehen. Deren Erfüllung dürfte häufig wegen konträrer Vorgaben, etwa zur Art der Meldung oder Schnittstelle, überhaupt nicht rechtskonform möglich sein, obgleich die TK-Unternehmen sich rechtstreu verhalten wollen und erheblichen Wert auf die Sicherheit ihrer Infrastrukturen legen.

Im Rahmen der damit einhergehenden Betrachtung der gegenwärtigen Marktgegebenheiten müssen TK-Infrastrukturanbieter bereits seit Jahren entsprechende grenzüberschreitende Vorkommnisse, die die Sicherheit der Infrastrukturen betreffen, an die zuständige europäische Behörde ENISA melden. Aus Sicht der IEN besteht jedoch weiterhin Bedarf, europaweit einheitliche Mindestregelungen, welche insbesondere auch internationalen Standards entsprechen, für die betroffenen Unternehmen in den Mitgliedstaaten unter der Beteiligung von ENISA festzulegen, um in der Branche verstärkt für harmonisierte Rechts- und Planungssicherheit zu sorgen.

Schließlich regt die IEN an, im Rahmen der Überarbeitung des Anforderungskatalogs auch noch einmal kritisch zu überprüfen, ob die derzeit in Deutschland verankerten Strukturen von Zuständigkeiten und Meldepflichten geeignet sind, für die notwendige Sicherheit am Markt zu sorgen.

II. Im Einzelnen zu den Eckpunkten

Die von der BNetzA vorgestellten Eckpunkte sehen unter anderem die folgenden Verpflichtungen vor:

- Der Netzverkehr muss regelmäßig und kontinuierlich auf Auffälligkeiten hin beobachtet werden und im Zweifelsfall sind geeignete Maßnahmen zum Schutz zu ergreifen.

- 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. Kritische Kernkomponenten dürfen nur von vertrauenswürdigen Lieferanten/Herstellern bezogen werden. Dies schließt auch eine Zusicherung der Vertrauenswürdigkeit seitens der Lieferanten/ Hersteller ein.

- Sicherheitsrelevante Netz- und Systemkomponenten (kritische Kernkomponenten) dürfen nur nach einer geeigneten Abnahmeprüfung bei Zulieferung eingesetzt werden und müssen regelmäßig und kontinuierlich Sicherheitsprüfungen unterzogen werden. Die Definition der sicherheitsrelevanten Komponenten (kritische Kernkomponenten) erfolgt einvernehmlich zwischen BNetzA und BSI.

- In sicherheitsrelevanten Bereichen darf nur eingewiesenes Fachpersonal eingesetzt werden.

- 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.

- Bei Planung und Aufbau der Netze sollen „Monokulturen“ durch Einsatz von Netz- und Systemkomponenten unterschiedlicher Hersteller vermieden werden.

- Bei Auslagerung von sicherheitsrelevanten Aufgaben dürfen ausschließlich fachkompetente, zuverlässige und vertrauenswürdige Auftragnehmer berücksichtigt werden.

- Für kritische, sicherheitsrelevante Netz- und Systemkomponenten (kritische Kernkomponenten) müssen ausreichend Redundanzen vorgehalten werden.

…

1. Notwendige Konkretisierung von Begrifflichkeiten und Berücksichtigung internationaler Standards

Aus Sicht der IEN ist eine vollumfängliche, detaillierte Kommentierung der einzelnen Eckpunkte zum gegenwärtigen Zeitpunkt nur schwer möglich, da gewählte Begrifflichkeiten noch zu wenig Trennschärfe gewährleisten und Ausführungen darüber fehlen, wie die Eckpunkte im konkreten Fall tatsächlich in der Praxis gehandhabt werden sollen.

So ist übergreifend eine Klarstellung notwendig, welche Systemkomponenten konkret als „kritisch" eingestuft werden. Erst eine solche Festlegung ermöglicht es den betroffenen Unternehmen, eine detaillierte Prüfung der diesbezüglichen Vorgaben vorzunehmen. Da die Definition und Zertifizierung der Komponenten erst „im Benehmen zwischen BNetzA und BSI" stattfinden soll, möchte die IEN jedoch bereits gegenwärtig darauf hinweisen, dass eine Definition und insbesondere auch Zertifizierung von kritischen Kernkomponenten sich mindestens auf europäische, im Idealfall internationale, anerkannte Standards berufen und existierende Gremien weitestgehend berücksichtigen muss. Es stellt für die Anbieter grenzüberschreitender Kommunikationsdienstleistungen ein erhebliches Hemmnis ihrer Geschäftstätigkeit dar, wenn die Komponenten nicht international einheitlich bewertet werden. Darüber hinaus stellt sich die Frage, inwieweit Zertifizierungen in anderen europäischen Ländern nicht ebenfalls hinreichend sein können, um bürokratischen Aufwand für alle Betroffenen zu vermeiden.

Vor diesem Hintergrund müssen die Aktivitäten auf EU-Ebene zum „Cyber Security Act", der bereits im Trilog final abgestimmt und vom EU-Parlament am 12. März 2019 verabschiedet wurde, größtmögliche Berücksichtigung finden. Gerade die durch den Cyber Security Act beabsichtigte Stärkung von ENISA und die Erarbeitung des harmonisierten Zertifizierungskonzepts auf dieser Ebene dürfen durch konträre, nationale Vorgaben nicht unterlaufen werden, um grenzüberschreitende elektronische Kommunikationsdienstleistungen nicht zu behindern. Darüber hinaus sind Dopplungen in Hinsicht auf Melde- und Berichtspflichten zu vermeiden und einheitliche Standards einzuführen, um unnötigen bürokratischen Aufwand und damit einhergehende Kosten zu Lasten insbesondere der Anbieter grenzüberschreitender Telekommunikationsdienstleistungen einzudämmen.

Gerade in Deutschland ist die Struktur von administrativen Zuständigkeiten zu Cybersicherheitsthemen breit gesplittert, wie aus der beigefügten Grafik in der Anlage deutlich wird. Dies erschwert ein rechtskonformes Verhalten der betroffenen Marktbeteiligten und macht eine einheitliche Behandlung der Abfragen und Vorgaben seitens der Behörden unmöglich. Daher regt die IEN dringend an, im Rahmen der Umsetzung der EU-Vorgaben auch

…

die gesamte administrative Behandlung der Sicherheitsthemen und Zuständigkeiten auf den Prüfstand zu stellen.

Vor diesem Hintergrund möchte die IEN auch nochmals betonen, dass die Konzentration des Anwendungsbereichs des Katalogs für Sicherheitsanforderungen sicherstellen sollte, dass eine trennscharfe, streng am jeweiligen Ausfallrisiko orientierte Identifizierung der Infrastrukturen, Komponenten und der entsprechenden Vorgaben erfolgt.

Auch die Verwendung weiterer Begrifflichkeiten wird seitens der IEN kritisch gesehen. Dies gilt etwa für den Begriff des „vertrauenswürden Lieferanten/Herstellers“, bei welchem in keinster Weise dargelegt wird, nach welchen Maßgaben ein hinreichendes Maß an Vertrauenswürdigkeit erreicht wird. Die bisherigen Ausführungen und Verweise, nach welchen zumindest keinen nationalen Interessen zuwidergelaufen werden darf, sind gerade auch im Hinblick auf die internationalen Standards und die grenzüberschreitenden Kommunikationsdienstleistungen nicht sachgerecht.

Darüber hinaus bleibt offen, wie die BNetzA und das BSI etwa den Umgang mit Eilfällen, in welchen eine Sicherheitsstörung zur Vermeidung von Schäden den Einsatz neuer Hard- und/oder Software erfordert, die möglicherweise noch nicht zertifiziert wurde, erforderlich macht. Unklar bleibt auch die Frage der Kostentragung im Bereich der verpflichtenden Durchführung von Zertifizierungen.

2. Flexibilität für unterschiedliche Kundengruppen und Bestandsschutz

Wie bereits dargestellt, bedienen die IEN-Mitgliedsunternehmen große, international agierende Geschäftskunden mit elektronischen Kommunikationsdienstleistungen. Diese Kundengruppe verfügt über eigene IT-Abteilungen die die geforderten TK-Dienstleistungen regelmäßig mit konkreten Vorgaben an die Leistungserbringung und die entsprechenden -komponenten ausschreiben. Bei der Erbringung von TK-Dienstleistungen mit großen Unternehmenskunden gilt, dass diese Kunden vertraglich Bedingungen vereinbaren, nach denen sie über Beeinträchtigungen und Sicherheitsverletzungen, gleich welcher Art oder Verursachung, informiert werden wollen, was auch das Erfordernis des ständigen Monitorings der Infrastrukturen sowie gegebenenfalls die Verwendung bestimmter Hardware-Komponenten beinhaltet. Die Intention der Vereinheitlichung der Prozedere hinter dieser Vorschrift kann somit für die Anbieter zu Konflikten führen, da diese mit ihren Kunden stets Individualvereinbarungen nach den Vorgaben des Kunden und dessen IT-Beschaffungsabteilungen abschließen.

Es ist mithin für die betreffenden Anbieter essenziell, dass sie neben dem unbedingt rechtskonformen Verhalten noch hinreichende Flexibilität erhalten, auch den Kundenvorgaben nachkommen zu können. Die IEN fordert daher dringend die Gewährleistung von hinreichend flexiblen Vorgaben, die gegebenenfalls eine Unterscheidung nach Kundengruppen ermöglicht. Die IEN möchte daher etwa auf die gefundenen Lösungsansätze im Rahmen der Entwicklung der Transparenz-VO verweisen, in welcher man sich ausdrücklich darauf geeinigt hat, Ausnahmeregelungen zuzulassen, soweit der Anbieter mit Kunden eine Individualvereinbarung getroffen hat.

In diesem Zusammenhang möchte die IEN schließlich auch darauf hinweisen, dass die bislang veröffentlichten Eckpunkte vermissen lassen, wie die BNetzA bestehende Sicherheitskonzepte von Kunden behandeln möchte. Die Anbieter haben für ihre Kunden in Ansehung der bestehenden regulatorischen Vorgaben bereits umfangreiche Sicherheitskonzepte erstellt und umgesetzt, welche von der BNetzA auch regelmäßig auditiert wurden und werden. Um diesem Aufwand Rechnung zu tragen, fordert die IEN, dass hinsichtlich dieser Konzepte ein Bestandsschutz zu gewähren ist.

3. Zur Vermeidung von Monokulturen

Soweit die BNetzA erreichen möchte, dass bei Planung und Aufbau der Netze „Monokulturen" durch den Einsatz von Netz- und Systemkomponenten unterschiedlicher Hersteller vermieden werden, ist dies aus Sicht der IEN zu begrüßen.

Die IEN-Mitgliedsunternehmen sind diesbezüglich bereits gegenwärtig an unterschiedliche Kundenvorgaben gebunden, um bei diesen entsprechende Kompatibilitäten gewährleisten zu können. Insofern existiert bereits heute eine „Multi-Vendor"-Handhabung. Allerdings weist die IEN in diesem Zusammenhang auch darauf hin, dass allein die Vielzahl nicht geeignet ist, zu mehr Sicherheit zu führen. So muss auch diese Regelung für die betroffenen Anbieter einen hinreichenden Ansatz der Flexibilität gewährleisten, um sicherheitsbasierten Anforderungen von Unternehmenskunden hinreichend gerecht werden zu können.

4. Zur Vorhaltung von Redundanzen

Hinsichtlich der weiteren Forderung, für kritische, sicherheitsrelevante Netz- und Systemkomponenten (kritische Kernkomponenten) ausreichend

…

Redundanzen vorhalten zu müssen – die als besonders kritisch wahrgenommene Netzkomponenten wie u. a. Home Location Register, Core Network, Backbone und Portierungsserver umfassen soll – wird seitens der IEN als ein zu tiefgreifender und verfehlter Eingriff in die Netzplanungs- und Einkaufsstrategie der Anbieter eingeordnet und daher abgelehnt. Dabei ist zu berücksichtigen, dass eine solche Maßnahme nicht zwangsläufig zu mehr Sicherheit, aber garantiert zu erheblichen Mehrkosten für die Anbieter und damit in letzter Konsequenz auch zu steigenden Endkundenpreisen führt.

Darüber hinaus gefährdet die Redundanzanforderung letztlich die Aufrechterhaltung eines regulatorischen Level Playing Field, da es aufgrund der Skalenvorteile der großen Anbieter im Markt hinsichtlich der Beschaffung redundanter Komponenten zu einer Wettbewerbsverzerrung zu Lasten kleinerer Anbieter kommen wird, was wiederum den regulatorischen Zielen des TKG zuwiderlaufen dürfte.

****

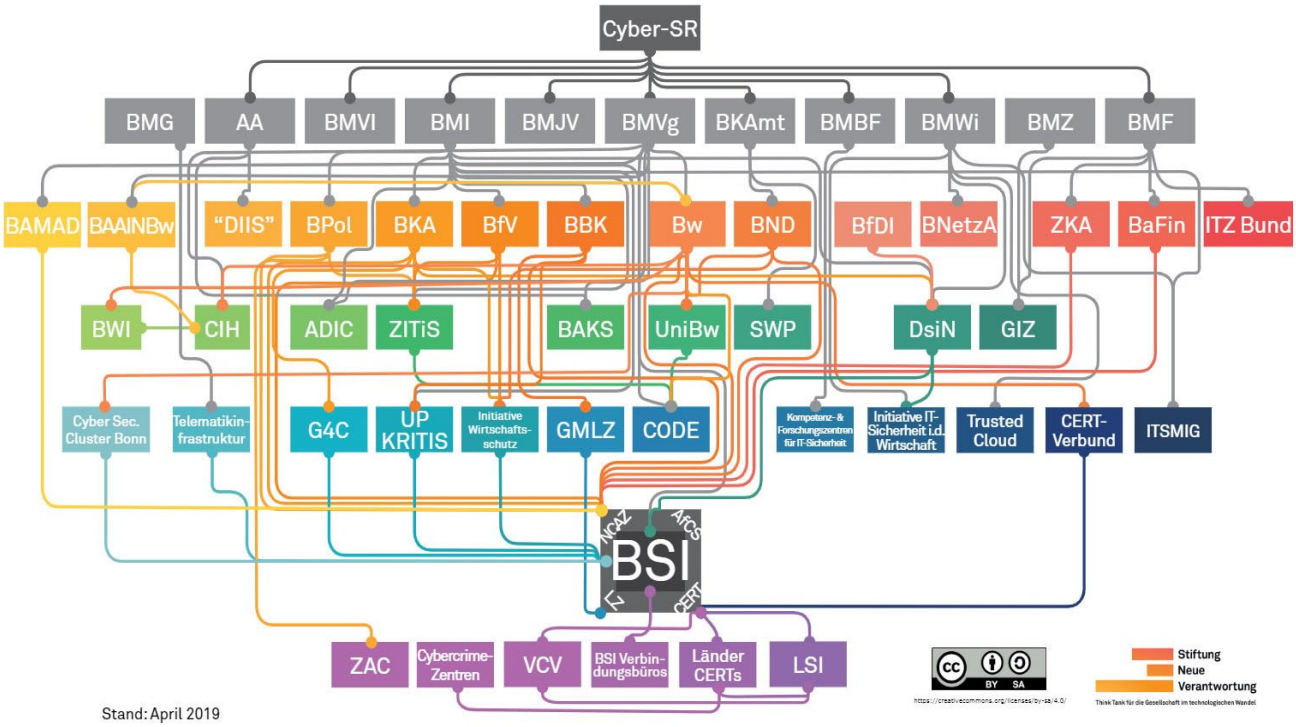
In Ansehung der aktuellen und anhaltenden Diskussionen und Veröffentlichungen zum Thema IT Sicherheit sowie auch hinsichtlich des Entwurfs eines überarbeiteten IT-SicherheitsG möchte die IEN darauf hinweisen, dass sie die gegenständliche Stellungnahme noch nicht als abschließend erachtet und zudem auch gerne in den weiteren Austausch mit der BNetzA und dem BSI zu diesem Thema treten möchte. Selbstverständlich stehen die IEN-Mitgliedsunternehmen sowie die Unterzeichnerin auch für Rückfragen gern zur Verfügung.

Diese Stellungnahme enthält keine Betriebs- und Geschäftsgeheimnisse.

Malini Nanda, Rechtsanwältin
Geschäftsführerin der IEN

Anlage: Grafik

Staatliche Cybersicherheitsarchitektur



Stand: April 2019

https://creativecommons.org/licenses/by-sa/4.0/

Stiftung Neue Verantwortung
Think Tank für die Gesellschaft im technologischen Wandel