INITIATIVE EUROPÄISCHER NETZBETREIBER

IEN · Marienstr. 30 · 10117 Berlin

Bundesnetzagentur
Referat IS 17

An der Trift 40
66123 Saarbrücken

Per Email an: IS17.Postfach@Bundesnetzagentur.de

Berlin, den
07.06.2019

Überarbeitung des Katalogs von Sicherheitsanforderungen gemäß § 109 Abs. 6 TKG

Stellungnahme der Initiative Europäischer Netzbetreiber

Die Bundesnetzagentur überarbeitet derzeit im Einvernehmen mit dem Bundesamt für Informationstechnik (BSI) den Katalog von Sicherheitsanforderungen (§ 109 Abs. 6 TKG). 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 bereits im März 2019 Eckpunkte veröffentlicht und die IEN hat dazu Stellung genommen.

Anlässlich der Anhörung am 12.06.2019 nimmt die IEN erneut die Gelegenheit zur Darlegung ihrer Einschätzungen zu den Plänen der BNetzA wahr. Dabei sind die nachfolgenden Ausführungen ausdrücklich als Ergänzung zu der bislang eingereichten Stellungnahme zu verstehen, da die bislang vorgetragenen Aspekte weiterhin ihre Gültigkeit haben.

I. Allgemeine Anmerkungen

Wie bereits dargestellt, haben die IEN-Mitgliedsunternehmen als international tätige Anbieter von grenzüberschreitendenden Telekommunikationsdienstleistungen für große Unternehmenskunden und Behörden bereits aufgrund ihres eigenen Geschäftsfokus ein erhebliches Interesse an der Sicherheit und Integrität ihrer Infrastrukturen und räumen diesem Aspekt im Rahmen ihrer Aktivitäten und Strategien einen erheblichen Stellenwert ein.

Da ihre Dienstleistungen 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.

Vor diesem Hintergrund sollten sich jedwede regulatorischen Maßnahmen im Einklang mit internationalen Standards und europäischen Vorgaben von ENISA oder dem EU Cyber Security Act befinden. Dies gilt insbesondere im Hinblick auf Definitionen und Zertifizierungen. Aus Sicht der IEN besteht 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 Rechts- und Planungssicherheit zu sorgen.

1. Notwendige Konkretisierung von Begrifflichkeiten

Die IEN hat bereits darauf hingewiesen, dass eine detaillierte Kommentierung der Eckpunkte aufgrund ihrer (naturgemäßen) Oberflächlichkeit und insbesondere fehlender Definitionen nur schwer möglich ist.

Vor diesem Hintergrund begrüßt die IEN einerseits die Bestrebungen der BNetzA, durch gezielte Fragestellungen im Vorfeld der Anhörung auch Auffassungen der Marktbeteiligten für Vorgaben und Begrifflichkeiten einzuholen. Gleichzeitig ist diesbezüglich jedoch zu berücksichtigen, dass aufgrund unterschiedlichster Geschäftsmodelle nicht zu erwarten steht, dass es damit zu einheitlichen Vorschlägen und somit zu Klarstellungen kommt. Es bleibt Aufgabe der BNetzA, bzw. des BSI, hier Vorgaben auf der Basis von bestehenden internationalen und europäischen Standards und existierender Gremien zu entwickeln.

Es stellt andernfalls für die Anbieter grenzüberschreitender Kommunikationsdienstleistungen ein erhebliches Hemmnis ihrer Geschäftstätigkeit dar, wenn die Komponenten nicht international einheitlich bewertet werden.

2. Flexibilität für unterschiedliche Kundengruppen

Große, international agierende Geschäftskunden (als Kundengruppe der IEN-Mitgliedsunternehmen) verfügen über eigene IT-Abteilungen die die geforderten TK-Dienstleistungen regelmäßig mit konkreten Vorgaben an

die Leistungserbringung und die entsprechenden -komponenten ausschreiben. Sie geben den TK-Dienstleistern mithin auch vertragliche Bedingungen vor, nach denen sie bestimmte Leistungen erhalten wollen und in welcher Art sie über Beeinträchtigungen und Sicherheitsverletzungen, gleich welcher Art oder Verursachung, informiert werden wollen.

Es ist demzufolge für die betreffenden Anbieter essenziell, dass sie auch im Rahmen von Prüfungen, Zertifizierungen, etc. neben dem unbedingt rechtskonformen Verhalten dennoch eine hinreichende (Mindest-)Flexibilität erhalten, um auch den Kundenvorgaben nachkommen zu können.

Dies gilt umso mehr im Rahmen der gängigen Praxis der Leistungserbringung, da die betreffenden Anbieter ständig Korrekturen und Fehlerbehebungen innerhalb kürzester Zeit zur Gewährleistung der Sicherheit und Integrität ihrer Netze vornehmen müssen. Eine entsprechende Anforderung an Prüfung und Zulassung von jedweden Patches oder sonstigen Maßnahmen lässt sich in der Praxis nicht realisieren. Zudem sind häufig gerade bei Aktualisierung von Software eine Vielzahl von Parteien beteiligt, die einen derartigen Prüf-Prozess im Rahmen der Notwendigkeit einer schnellen Realisierung kaum möglich machen. Auch hier gilt, dass die Anbieter bereits selbst ein erhebliches Eigeninteresse an der Gewährleistung der Sicherheit und Integrität ihrer Netze haben, welcher beim Erlass entsprechender Regulierung zu berücksichtigen ist.

Gleiches gilt auch im Rahmen der Vorgabe zur Vermeidung von Monokulturen. Wie bereits in der vorherigen Stellungnahme dargestellt, gewährleisten die Anbieter von TK-Dienstleistungen bereits heute eine erhebliche Diversität bei dem Einsatz von Netz- und Systemkomponenten, um wirtschaftliche Abhängigkeiten zu vermeiden. Allerdings müssen sie gleichzeitig auch über einen Ermessensspielraum verfügen, um ohne erheblichen und unangemessenen Aufwand von Tests und Entwicklung ein ausgewogenes Netz und maßgeschneiderte Angebote nach den Vorgaben großer Unternehmenskunden anbieten zu können.

3. Bürokratischen Aufwand für sämtliche Marktbeteiligte vermeiden

Im Rahmen der geplanten Vorgaben sollen u.a. zum Schutz des eigenen Netzes der Netzverkehr ständig hinsichtlich etwaiger Auffälligkeiten beobachtet werden. Diesbezüglich die obigen Ausführungen hinsichtlich der Vorgaben großer Unternehmenskunden über Monitoring und Meldungen. Gerade vor dem Hintergrund der datenschutzrechtlichen Vorgaben zu Datensparsamkeit sollte hier ein übermäßiger bürokratischer Aufwand, welcher möglicherweise auch im Konflikt mit anderen gesetzlichen Vorgaben stehen könnte, vermieden werden.

Gleiches gilt hinsichtlich etwaiger Meldepflichten. TK-Infrastrukturanbieter müssen bereits seit Jahren entsprechende grenzüberschreitende Vorkommnisse, die die Sicherheit der Infrastrukturen betreffen, an die zuständige europäische Behörde ENISA melden. Auch hier sind unnötige Doppelmeldungen zu vermeiden.

Soweit die neuen Vorgaben den Einsatz von „eingewiesenem Fachpersonal“ und die Auslagerung von systembezogenen Prozessen nur an „fachkompetente, zuverlässige und vertrauenswürdige Auftragnehmer“ vorsehen, stellt sich ebenso die Fragestellung, was die BNetzA mit diesen Vorgaben anderes als die Gewährleistung von Selbstverständlichkeiten bezwecken möchte. Die bei den TK-Anbietern mit der Thematik betrauten Mitarbeiter sind stets in der Materie fachlich kompetent und bereits aus Eigeninteresse wird keine Auslagerung an unzuverlässige Drittanbieter vorgenommen. Auch hier sind konkrete Klarstellungen notwendig.

4. Bestandsschutz gewährleisten

Schließlich ist erneut darauf hinzuweisen, dass die TK-Anbieter auch in der Vergangenheit bereits mit hohem Aufwand kundenindividuelle Sicherheitskonzepte erstellt und von der BNetzA haben auditieren lassen. Für diese muss ein Bestandsschutz gelten, um unnötige Kosten für erneute Prüfungen zu vermeiden.

II. Im Einzelnen

Vor dem Hintergrund der obigen Ausführungen möchte die IEN im Folgenden darlegen, zu welchen Themen und Begriffen aus ihrer Sicht weitere Erläuterungen, Konkretisierungen oder Definitionen notwendig sind.

1. Systeme dürfen nur von vertrauenswürdigen Lieferanten bezogen werden, deren Einhaltung der nationalen Sicherheitsvorschriften und Bestimmungen über das Fernmeldegeheimnis und den Datenschutz gewährleistet ist.

Zu diesem Eckpunkt sind aus Sicht der IEN insbesondere folgende Fragen zu klären:

- Was sind die Kriterien, um eine Quelle als "vertrauenswürdig" zu bestimmen?

- Welche Bestimmungen sollen genau von den "nationalen Sicherheitsbestimmungen" umfasst sein?

- Welche Kriterien werden für "Bestimmungen über das Fernmeldegeheimnis und Datenschutz" herangezogen?

Sollte die BNetzA an den Vorgaben in dieser Form festhalten wollen, würde es aus Sicht der IEN mehr Rechts- und Planungssicherheit geben, wenn die BNetzA/das BSI eine Liste von Anbietern bereitstellen würde, welche die vorgegebenen Kriterien erfüllen, anstatt jedes Unternehmen den bürokratischen (Prüf- und Kontroll-)Mehraufwand erledigen zu lassen, da sämtliche Anbieter wiederholt die gleichen Prüfungen vornehmen müssten. Ein konstruktiverer und praxistauglicherer Ansatz wäre daher, dass die Behörden die Lieferanten auf die oben genannten Kriterien überprüfen und eine Liste dieser positiv bewerteten Lieferanten veröffentlichen, die von den TK-Dienstleistern angefragt werden können. Soweit ein Anbieter einen Lieferanten beauftragen will, welcher nicht auf dieser Liste steht, obliegt ihm die Überprüfungspflicht und Nachweispflicht gegenüber den Behörden (soweit erforderlich).

Darüber hinaus weist die IEN darauf hin, dass diese Vorgaben für die älteren Geräte fast unmöglich zu bestimmen sein werden. Diesbezüglich ist unbedingt zu vermeiden, dass die neuen Vorgaben dazu führen, die Anschaffung neuer Geräte zu erzwingen. Vielmehr sind diesbezüglich Bestandsschutz zu gewähren und Ausnahmeregelungen zu erlassen, die für Rechts- und Planungssicherheit sorgen.

2. Der Netzwerkverkehr muss regelmäßig und kontinuierlich auf Anomalien überwacht werden, und wenn Anlass zur Sorge besteht, müssen geeignete Schutzmaßnahmen getroffen werden.

Wie bereits in den allgemeinen Ausführungen dargelegt, ist dies eine gängige Praxis der TK-Anbieter. Gerade große Unternehmenskunden verlangen entsprechende Funktionalitäten, so dass die IEN-Mitgliedsunternehmen bereits entsprechende Mechanismen zur Überwachung ihrer Netzwerke implementiert haben.

Zur Wahrung der Rechtssicherheit ist zudem zu erläutern, wie die BNetzA den Begriff „Anomalie" definiert.

3. 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 solchen Lieferanten/Herstellern bezogen werden, die in geeigneter Weise ihre Vertrauenswürdigkeit zusichern. Die Verpflichtung soll für die gesamte Lieferkette gelten und Voraussetzung für die not-wendige 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. 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 Telekommunikations-gesetzes

Auch bezüglich dieses Eckpunkts sieht die IEN erheblichen Klarstellungsbedarf:

-Wie lautet die Definition von "kritischen Kernkomponenten"?

- Welche Komponenten fallen genau unter den Begriff der "sicherheitsrelevanten" Netzwerk- und Systemkomponenten?

- Wie wird der Prüf- und Zertifizierungsprozess aussehen? Werden die Auditoren/zugelassenen Prüfstellen die Implementierungen testen wollen oder sollen bereits Tests an Geräten durchgeführt werden, die vom BSI/den Prüfstellen vorab selbst beschaffen werden?

Wesentlich ist auch hier, dass das BSI zur Gewährleistung der Planungs- und Rechtssicherheit eine Liste der zertifizierten Komponenten veröffentlichen sowie eine Liste der abgelehnten Komponenten (sowie die Gründe für die Ablehnung) führen sollte. Zudem sollte ein Mechanismus für die Einreichung von Komponenten vorgesehen werden, die nicht auf einer der oben genannten Listen stehen.

- Darüber hinaus stellt sich die Frage, wie die "Vertrauenswürdigkeit“ der Lieferanten/Hersteller zugesichert werden soll.

4. 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.

- Wie soll eine "geeignete Abnahmeprüfung" aussehen?

- Wird ein Verfahren für "laufende" Sicherheitsprüfungen vorgesehen?

Hinsichtlich der Informationspflichten verweist die IEN auf die obigen Ausführungen unter I.3.

5. 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

Es muss definiert werden, was "eingewiesenes Fachpersonal" gegenüber dem, wie oben bereits dargestellten, mit der Materie vertrauten und vom TK-Anbieter für diesen Zweck eingesetzte Personal, unterscheiden soll. Darüber hinaus ist zu klären, was die BNetzA/BSI unter „ausreichendem Umfang“ versteht.

6. Es ist nachzuweisen, dass die für die ausgewählten, sicherheitsrelevanten Komponenten getestete Hardware und der Quellcode am Ende der Lieferkette tatsächlich in den Produkten eingesetzt werden.

- Welchen Nachweis erachten BNetzA/BSI für diese Anforderung als ausreichend?

- Ist es erforderlich, für jedes einzelne Gerät diesen Nachweis zu erbringen? Soweit dies vorgesehen ist, stellt sich die Folgefrage nach dem Informationsprozess hinsichtlich Art und Anzahl der Ausrüstung.

In Abhängigkeit von der Art der erforderlichen Nachweise und Elemente möchte die IEN bereits gegenwärtig darauf hinweisen, dass diese Vorgabe zu unangemessener Härte aufgrund erheblichen bürokratischen Aufwands für die Anbieter führen dürfte. Die Anbieter sind bereits aufgrund der übrigen Angaben zur Verwendung von nur zugelassenen Komponenten verpflichtet. Weshalb vorliegend eine weitergehende Nachweispflicht vorgesehen ist, bedarf nach unserer Auffassung näherer Erläuterung.

7. 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.

Auch bezüglich dieser Regelung ist zunächst darauf hinzuweisen, dass es sich bei diesen Vorgaben um eine gängige Praxis handelt, welche die Unternehmen bereits gegenwärtig im eigenen Interesse erfüllen.

- Soweit an den Vorgaben festgehalten wird, ist eine Definition von "fachlich kompetent, zuverlässig und vertrauenswürdig" notwendig.

- Zudem ist zu konkretisieren, welche "systembezogene Prozesse" umfasst sein sollen.

- Unklar bleibt schließlich auch, bei welchem Prozedere genau die „Auslagerung“ vorliegen soll. Beginnt dies bereits bei direkten Auftragnehmern, die im Unternehmen arbeiten oder bei externen Geschäftspartnern, die vor Ort tätig sind?

8. Für kritische, sicherheitsrelevante Netz- und Systemkomponenten (kritische Kernkomponenten) müssen ausreichend Redundanzen vorgehalten werden. Hierfür wird eine Liste besonders kritischer Netzkomponenten (z.B. Home Location Register, Core Network, Backbone, Portierungsserver) erstellt.

Soweit eine Liste „besonders kritischer Netzkomponenten“ erstellt werden soll, bleibt unklar, inwieweit diese Liste dann die „sicherheitsrelevanten Netz- und Systemkomponenten“, bzw. „kritische Kernkomponenten“ abschließend und rechtssicher definiert.

****

Diese Stellungnahme enthält keine Betriebs- und Geschäftsgeheimnisse. Für Rückfragen stehen die IEN-Mitgliedsunternehmen sowie die Unterzeichnerin gern zur Verfügung.

Malini Nanda, Rechtsanwältin
Geschäftsführerin der IEN