INITIATIVE EUROPÄISCHER NETZBETREIBER

IEN · Marienstr. 30 · 10117 Berlin

Bundesnetzagentur für Elektrizität, Gas,
Telekommunikation, Post und Eisenbahnen
Referat IS17
An der Trift 40
66123 Saarbrücken

Per E-Mail: IS17.Postfach@bnetza.de

Berlin, den
22.11.2019

Überarbeitung des Katalogs von Sicherheitsanforderungen gemäß § 109 Abs. 6 TKG – Version 2.0

Stellungnahme der Initiative Europäischer Netzbetreiber

Die Bundesnetzagentur überarbeitet derzeit den Katalog von Sicherheitsanforderungen (§ 109 Abs. 6 TKG) und hat am 15.10.2019 einen Entwurf veröffentlicht.

Die nach § 109 Abs. 4 TKG verpflichteten Unternehmen sollen durch Festlegung von Sicherheitsanforderungen bei der Erfüllung ihrer Pflichten unterstützt werden. Die Bundesnetzagentur hat daher (im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit) den gegenständlichen Entwurf: „Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten als Grundlage für das Sicherheitskonzept nach §109 Abs. 4 TKG und für die zu treffenden technischen Vorkehrungen und sonstigen Maßnahmen nach §109 Abs 1 und 2 TKG“ erstellt.

Dabei ist die Beachtung der grundlegenden Sicherheitsanforderungen des ersten Kapitels für alle Unternehmen zwingend. Anlage 1 beschreibt geeignete technische und organisatorische Maßnahmen zu Anforderungen an TK-Anbieter mit IP-Infrastruktur. Die beschriebenen Maßnahmen richten sich daher an Internet-Service-Provider. Zusätzliche Sicherheitsanforderungen enthält die Anlage 2. Die zusätzlichen Sicherheitsanforderungen richten sich ausschließlich an Betreiber von Telekommunikationsnetzen mit erhöhtem Gefährdungspotential.

…

Interessierten Parteien wurde die Gelegenheit zur Stellungnahme bis zum 22.11.2019 eingeräumt.

1. Allgemeine Anmerkungen

Die IEN-Mitgliedsunternehmen als international tätige Anbieter von grenzüberschreitendenden Telekommunikationsdienstleistungen für große Unternehmenskunden und Behörden 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.

Da ihre Dienstleistungen überwiegend international erbracht werden, haben diese Unternehmen zudem auch ein essentielles Interesse daran, dass die internen Sicherheitsprozesse möglichst zentralisiert und länderübergreifend einheitlich durchgeführt werden und dass entsprechende regulatorische Vorgaben diesen Ansatz unterstützen. Gerade die Zunahme unterschiedlicher gesetzlicher Anforderungen weltweit, z.B. zu Verstoßmeldungen und Datenschutzanforderungen, häufig sowohl in branchenspezifischen als auch in horizontalen Rahmenbedingungen, verursachen bei den betroffenen Marktteilnehmern enorme Compliance-Belastungen, die Handel, Investitionen und Innovation beeinträchtigen. Dies gilt auch für kleinere Unternehmen, die versuchen, international zu expandieren.

Gerade auch vor dem Hintergrund des von der BNetzA im Entwurf ausdrücklich zitierten und zu berücksichtigenden Grundsatzes der Verhältnismäßigkeit sollten behördliche Sicherheitsvorgaben daher risikobasiert und flexibel sein, die Zusammenarbeit von Unternehmen begrüßen und innovationsfreundliche und technologieneutrale Lösungen fördern. Dabei sollten bestehende, interoperable und globale Best Practices sowie freiwillige Industriestandards und -zertifizierungen nicht unberücksichtigt bleiben, um die Sicherheit zu verbessern und gleichzeitig das Wachstum des internationalen Handels mit digitalen Mitteln zu ermöglichen.

In Bezug auf das Internet der Dinge (IoT-Dienste) ist festzuhalten, dass dieses eine Weiterentwicklung bestehender Dienste und Branchen ist und keine spezifischen Datenschutz- oder Sicherheitsbestimmungen erforderlich sind. An dieser Stelle ist von hervorzuheben, dass IoT-Dienste, die von Unternehmenskunden verwendet werden, im Gegensatz zu Verbraucherdiensten häufig keine personenbezogenen Daten enthalten. Infolgedessen sollten sie auch nicht wie Verbraucherdienstleistungen behandelt und geregelt werden. Aus Sicht der IEN können freiwillige und branchengeführte Zertifizierungs- und Standardisierungsregelungen nach wie vor dazu dazu beitragen, eine Sicherheitskultur rund um das Internet der Dinge aufzubau-

…

en und der Industrie die Möglichkeit zu geben, sich an neue Bedrohungen anzupassen, wenn sich Geräte und Dienste weiterentwickeln.

Jedwede Regelung sollte schließlich berücksichtigen, dass an zahlreichen Stellen im Online-Ökosystem Risiken bestehen, die von Geschäftsbenutzern, einzelnen Benutzern, Geräteherstellern, Geräteherstellern und Dienstanbietern ausgehen. Die Einbeziehung aller Akteure in das digitale Ökosystem ist für die Schaffung einer stabileren Cybersicherheitsumgebung von entscheidender Bedeutung.

Aus Sicht der IEN muss der gegenständliche Entwurf weiter dafür eintreten, 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.

2. Zu den allgemeinen Vorgaben

Die IEN begrüßt zunächst das Bestreben der BNetzA, durch die Abstufung der Anwendungsbereiche nach Art der Bestreiber, bzw. Kritikalität der Netze und Dienste, verhältnismäßige Regelungen zu schaffen, die die betroffenen Unternehmen nicht über das gebotene Maß hinaus belasten. Dies ist aus Sicht der IEN jedoch noch nicht hinreichend konsequent umgesetzt – insbesondere unter Berücksichtigung der in den Allgemeinen Anmerkungen dargestellten Aspekte.

Insbesondere wird sich weiterhin unbestimmter Rechtsbegriffe bedient, welche zu Rechtsunsicherheiten hinsichtlich der Einordnung von Netzen und Diensten führen dürfte. Dies gilt etwa für die Einordnung in die Bereiche gehobener Kritikalität und erhöhter Kritikalität. Unter Abschnitt 5.1.3 knüpfen sowohl die „gehobene“ als auch die „erhöhte“ Kritikalität an die Teilnehmerzahl des § 1 Abs. 1 Nr. 2 PSTG an - dies ist jedoch das einzig konkrete Kriterium. Ein Konkretisierungsbedarf ergibt sich umso mehr hinsichtlich der Begriffe des „Gemeinwohl“ oder „Bestand der Bundesrepublik Deutschland als Industrie- und Technologiestandort“.

Im Rahmen der geplanten Vorgaben soll zum Schutz des eigenen Netzes der Netzverkehr ständig hinsichtlich etwaiger Auffälligkeiten beobachtet werden. Diesbezüglich gelten die obigen Ausführungen hinsichtlich der Vorgaben großer Unternehmenskunden über die Einhaltung ihrer eigenen Sicherheitsvorgaben und Meldepflichten. 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 grenzüber-

schreitende Vorkommnisse, die die Sicherheit der Infrastrukturen betreffen, an die zuständige europäische Behörde ENISA melden. Auch hier sind unnötige Doppelmeldungen zu vermeiden.

Soweit die Vorgaben den Einsatz in Abschnitt 3.1.3 sowie 3.2 von „vertrauenswürdigen“ Personen/Dritten 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.

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.

3. Zu den Vorgaben der Anlage 1

In Bezug auf die Vorgaben der Anlage 1 ist aus Sicht der IEN kritisch, dass einige Vorgaben erheblich ins Detail gehen und somit den betreffenden Unternehmen wenig Möglichkeiten geben, etwaigen, potentiellen Sicherheitsbedrohungen nach etablierten und funktionierenden, internationalen Prozessen zu begegnen. Beispielsweise werden in Abschnitt 2.1.2.2 bestimmte Hinweise zu IETF-Methoden für IP-Spoofing vorgenommen oder in 3.4.3 Vorgaben bezüglich der DNSSEC-Signaturen gemacht.

Darüber hinaus scheinen nach Auffassung der IEN eine Reihe von Anforderungen in diesem Abschnitt erheblich weiter zu gehen, als es von einem Katalog von Sicherheitsanforderungen – insbesondere unter Berücksichtigung der Maßstäbe des Grundsatzes der Verhältnismäßigkeit - zu erwarten wäre. So wird in Abschnitt 2.1.3 die "Gleichbehandlung" von Datenpaketen behandelt. Die Umsetzung dieser Vorgaben bedeutet aus Sicht der IEN jedoch, dass es sich hier letztlich um Vorgaben zur Netzneutralität handelt. An dieser Stelle ist zwingend darauf zu achten, dass gerade B2B-Anbieter in Deutschland nicht über die in den vergangenen Jahren gefundenen Kompromisse hinaus im Rahmen dieses Katalogs belastet werden. Darüber hinaus wäre die Umsetzung der Vorgaben für einige DDOS-Präventions- / Minderungslösungen nicht praktikabel.

Entsprechend zu weit geht aus Sicht der IEN auch der Zwang zum Erkennen von Botnetzen in Abschnitt 2.1.2.5. Zunächst sieht die Regelung erneut keine Ausnahmen für kleinere Provider vor. Darüber hinaus fehlt es an einer Definition eines Botnetzes und es offenbleibt, was die tatsächliche

…

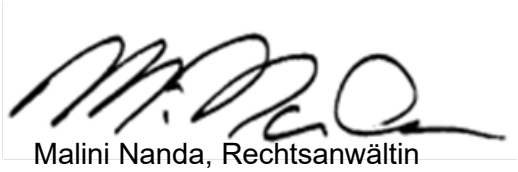
Konsequenz der Erkennung sein soll. Allein durch die Erkennung von Botnetzen ergibt sich keine erhöhte Sicherheit. Vielmehr wird hier eine Überwachungsmaßnahme implementiert, die faktisch den Aufbau einer Überwachungs- und insbesondere einer Sperrinfrastruktur vonnöten macht. Ob diese Vorgabe im Rahmen einer bloßen Katalogregelung zulässig ist, ist nach Auffassung der IEN kritisch zu bewerten.

Im Hinblick auf die Berücksichtigung der internationalen Standards wird in Abschnitt 3.4 auf DNS eingegangen. Derartige Vorgaben sollten jedoch in der NIS-Richtlinie behandelt werden.

Weit über den Rahmen der Kataloganforderungen hinaus geht aus Sicht der IEN auch die Einbeziehung der TK-Anbieter, die mit Anti-Malware-Herstellern zusammenarbeiten sollen, indem sie ihnen Malware-Beispiele zur Verfügung stellen.

****

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