VERBAND DER INTERNETWIRTSCHAFT E.V.

Stellungnahme zum zweiten Entwurf einer Verordnung zur Änderung der BSI-Kritisverordnung

Berlin, 17. Mai 2021

Mit der BSI-Kritisverordnung (BSI-KRITISV) wurden im Jahr 2016 erstmals Schwellenwerte zur näheren Definition kritischer Infrastrukturen auf Grundlage des IT-Sicherheitsgesetzes festgeschrieben und im Jahr 2017 auf Grundlage der von der EU-Kommission vorgelegten NIS-Richtlinie überarbeitet. Mit der nunmehr erfolgten Überarbeitung des IT-Sicherheitsgesetzes steht eine weitere Anpassung der BSI-KRITISV an.

eco – Verband der Internetwirtschaft e.V. befürwortet die frühzeitige Diskussion um die KRITISV und die darin vorgesehene Anpassung der Schwellenwerte für kritische Infrastrukturen.

I. Vorbemerkung

Mit der fortschreitenden Digitalisierung und insbesondere einer stärkeren Vernetzung von Infrastrukturen und Endgeräten stellt sich die Frage nach einer Anpassung der Schwellenwerte für kritische Infrastrukturen – auch vor dem Hintergrund, dass immer häufiger wichtige Prozesse digital abgewickelt werden. Gleichzeitig gilt es auch zu berücksichtigen, dass die Regulierung von IT-Sicherheit kein rein nationales Unterfangen ist. Auf europäischer Ebene wird derzeit die Nachfolgerichtlinie der NIS-Richtlinie von 2016 verhandelt. Eine Verabschiedung der neuen Rahmenregelung für IT-Sicherheit wird für das kommende Jahr erwartet. Vor diesem Hintergrund stellt sich die Frage, inwieweit es sinnvoll ist, zum jetzigen Zeitpunkt die Schwellenwerte für kritische Infrastrukturen neu zu bestimmen, oder ob man zunächst abwartet bis die NIS-2 Richtlinie finalisiert worden ist, um dann klare Regeln zu erlassen und so Rechtssicherheit für Unternehmen und Betreiber herzustellen. Die Erfahrungen bei der Umsetzung der ersten NIS-Richtlinie im Jahr 2017 haben gezeigt, dass sich durch die europäische Regulierung oftmals noch weitere Anpassungsbedarfe ergeben, die dann ein erneutes legislatives Handeln erforderlich machen. Beispielsweise genannt seien Reparaturgesetze wie das NIS-Richtlinien-Umsetzungsgesetz und der damit einhergehenden Überarbeitung der BSI-KRITISV. eco plädiert daher dafür, neue Schwellenwerte erst festzulegen, wenn diese auch verbindlich und im Einklang mit europäischen Vorgaben festgesetzt werden können. Ein dringender Handlungsbedarf für die Anpassung oder Festlegung neuer Schwellenwerte ist derzeit nicht vorhanden. Insbesondere haben die bestehenden Regelungen weiterhin Bestand und dementsprechend werden bereits zahlreiche Unternehmen als kritische Infrastruktur erfasst. Daher wäre ein abgestimmter und harmonisierter Ansatz sinnvoll, damit

sichergestellt ist, dass die BSI-KRITISV mit der noch zu verabschiedenden NIS-2 Richtlinie in Einklang steht.

Darüber hinaus muss bei den Überlegungen zur Überarbeitung der KRITISV berücksichtigt werden, dass durch das kürzlich von Bundestag und Bundesrat verabschiedete IT-Sicherheitsgesetz 2.0 die Auflagen für KRITIS-Betreiber deutlich verschärft werden. Gleichzeitig den Betroffenenkreis auszuweiten und die Maßnahmen zu verschärfen wird insbesondere für die neu als KRITIS eingestuften Unternehmen und Betreiber eine Herausforderung bei der Umsetzung sein und mit erheblichem finanziellen und administrativen Aufwand verbunden sein. Es sollte daher für die verschärften Regeln des IT-SiG 2.0 zumindest eine angemessene Übergangsfrist vorgesehen werden, damit für die durch den erweiterten Anwendungsbereich einbezogenen Unternehmen die Möglichkeit besteht, erforderlichen Anpassungen und Änderungen vorzunehmen und damit den umfangreichen Anforderungen des IT-SiG 2.0 gerecht zu werden.

II. Zu den Regelungen der BSI-KRITISV im Einzelnen

Zu § 1 Punkt 1:

Die neu eingefügte Formulierung zur Rolle von Software und IT-Diensten sieht eco als eine nachvollziehbare und grundsätzlich positive Klarstellung, dass nicht nur die physische Infrastruktur selbst, sondern evtl. auch weitere Komponenten mit einzubeziehen sind. Die Ausweitung der entsprechenden Verantwortlichkeit sieht eco als sinnvollen Schritt zur Verbesserung der IT-Sicherheit. Dass durch die Hinzuziehung von IT-Diensten auch externe Services in die Regelung mit einbezogen werden, ist aus Sicht der Internetwirtschaft nachvollziehbar und entspricht den gängigen Praktiken im Markt. Allerdings muss darauf geachtet werden, dass die entsprechend hinzugezogenen Dienste über ihre Rolle und Funktion als kritische Infrastruktur informiert sind und sich dieser Rolle bewusst sind.

Nach Ansicht des eco ist die neu eingefügte Formulierung, nach der auch mehrere Anlagen, die in einem betriebstechnischen Zusammenhang verbunden sind als eine gemeinsame Anlage gelten sollen, nicht hinreichend präzise. Es sollte klargestellt sein, dass derselbe Dienst und derselbe Betreiber gemeint sind. Die momentane Formulierung lässt dies offen.

Zu § 5:

Durch die Neuformulierung von Punkt 5 werden die Regeln für KRITIS klargestellt. Die hier verwendeten Formulierungen vermeiden Zirkelschlüsse, so dass die hier vorgeschlagene Regelung in Verbindung mit Anhang 4 im Sinne einer Klarstellung zu begrüßen ist.

Zu Anhang 4 Teil 1 Punkt 2:

Die Überarbeitung der Definition für IXPs erweitert den Bereich der unter diese Regelung fallenden Anlagen und Einrichtungen deutlich. Nach Ansicht des eco stellt sich hier die Frage, in welchem Umfang diese Erweiterung auch solche Dienste und Einrichtungen erfasst, die bislang nicht durch die KRITISV abgedeckt waren. Aufgrund der unzureichenden Definition fallen nun auch beispielsweise auch Transit Provider und Lichtwellen-Leiter Anbieter unter den Begriff IXP. Somit werden nun auch Anlagen und Einrichtungen erfasst, die nicht originär der Definition eines IXP im industrietypischen Sinn unterfallen. Wenn neue Klassen von Unternehmen (z.B. Transit Provider oder Lichtwellen-Leiter Anbieter) erfasst werden sollen, dann empfiehlt es sich, dies nicht unter dem Begriff IXPs zu tun, sondern dafür einen neuen Bereich zu definieren.

Weiterhin bleibt es abzuwarten, inwieweit die Absenkung des Schwellwertes von 300 auf 100 ASNs eine Ausweitung darstellt, die sich nachteilig auf die Anzahl und das Angebot von IXPs in Deutschland auswirken wird. Gerade für kleinere und nicht kommerziell betriebene IXPs könnte dies den wirtschaftlichen Betrieb in Frage stellen und auch eine hohe Marktzutrittsbarriere darstellen. Die Stabilität des Internets in Deutschland hängt auch von einer Vielzahl von kleineren und nicht kommerziellen IXPs, die unabhänigig von einander betrieben werden. Die Absenkung des Schwellwertes könnte einen inversen Effekt haben und die Stabilität des Internets in Deutschland nicht stärken, sondern sogar schwächen.

Darüber hinaus ist die Definition eines IXP insoweit unklar, dass der Verordnungsentwurf von der Verbindung von mindestens zwei Autonomen Systemen (ASN) die Rede ist, damit aber vermutlich öffentliche ASN gemeint sind, da teilweise auch Organisationsintern für Routingzwecke ASN miteinander verbunden werden. eco plädiert an dieser Stelle für eine Klarstellung dahingehend, dass die Definition von IXP auf öffentliche ASN bezogen ist.

Zudem sollte auch hier darauf geachtet werden, dass die hier geschaffenen Anforderungen und Definitionen die europäische NIS-2 Richtlinie angemessen aufgreifen und einbeziehen.

Neu aufgenommen werden sollen erstmalig Betreiber von TLDs. Die Verordnung trägt damit auch den Plänen der EU-Kommission, diese zukünftig im Rahmen von NIS-2 strenger zu regulieren, Rechnung. Inwieweit diese Regelung sinnvoll ist, bleibt abzuwarten. Die durch NIS-2 vorgesehenen Regelungen für TLD-Betreiber stuft eco als zu granular und für diese nicht handhabbar ein. eco befürwortet daher hier eine vorsichtigere Herangehensweise.

Zu Anhang 4 Teil 3

- IXPs

Nach Ansicht des eco ist die unter 1.3.1. angeführte Anpassung des Schwellenwertes von 300 auf 100 angeschlossene autonome Systeme nicht nachvollziehbar. In Verbindung mit der unklaren Definition dürfte sich der Bereich der betroffenen Unternehmen deutlich ausweiten. Auch ist nicht nachvollziehbar, warum einerseits die Anzahl der angeschlossenen Systeme herabgesetzt und andererseits der bisherige Schutzanspruch von 500.000 Personen unverändert in die neue KRITISV überführt worden ist. Die angeführte Formel zeigt eine deutliche Reduzierung der autonomen Systeme von 50.000 auf 20.000 auf. Woraus diese abgeleitet ist, wird nicht ersichtlich.

- Rechenzentren

Die in 2.1.1 vorgenommene Absenkung des Schwellenwerts auf eine vertraglich vereinbarte Leistung von 5 MW auf 3,5 MW ist nicht nachvollziehbar. Damit einher geht eine erhebliche Ausweitung des Kreises der betroffenen und zukünftig erfassten Unternehmen. Ein derart niedrig angesetzter Schwellenwert dürfte einen erheblichen Anteil der Rechenzentren in Deutschland erfassen. eco ist der Auffassung, dass die geplante Herabsetzung des Schwellenwertes einer kritischen Überprüfung unterzogen werden muss. Insbesondere die damit verbundenen Auswirkungen auf die Verfügbarkeit und das Angebot von Rechenzentrums-Dienstleistungen und die Attraktivität des Rechenzentrums-Standortes Deutschland muss in die Überlegungen einbezogenen werden.

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, schafft Rahmenbedingungen und vertritt die Interessen seiner Mitglieder gegenüber der Politik und in internationalen Gremien. Die Zuverlässigkeit und Stärkung der digitalen Infrastruktur, IT-Sicherheit und Vertrauen sowie eine ethisch orientierte Digitalisierung bilden Schwerpunkte der Verbandsarbeit. eco setzt sich für ein freies, technikneutrales und leistungsstarkes Internet ein.