VERBAND DER INTERNETWIRTSCHAFT E.V.

Stellungnahme zum Inception Impact Assessment der Europäischen Kommission „Revision of the NIS Directive“ (Ares(2020)3320999)

Berlin, 12. August 2020

Die NIS-Richtlinie stellt in ihrer derzeitigen Form ein zentrales Instrument für die Gestaltung der IT-Sicherheit in Europa und deren Regulierung dar. 2017 wurde sie noch einmal durch einen Durchsetzungsrechtsakt ergänzt. Zahlreiche EU-Mitgliedsstaaten haben die NIS-Richtlinie umgesetzt und auch eigene Regulierung auf ihrer Grundlage aufgesetzt. Der Cybersecurity Act von 2019 bezieht sich auch stark auf die in der NIS-Richtlinie ausgearbeitete Regulierung und die sektoralen Einteilungen der Verordnung.

Mit der vorliegenden Konsultation und dem hierzu gehörigen Inception Impact Assessment möchte die EU Kommission die vorgeschriebene Evaluierung der NIS-Richtlinie bereits vorwegnehmen und verschiedene Optionen für deren Weiterentwicklung erörtern. eco – Verband der Internetwirtschaft e.V. sieht in der NIS-Richtlinie und der daraus abgeleiteten bzw. der darauf aufbauenden Regulierung einen strikten, im Wesentlichen aber tauglichen Regulierungsrahmen für den Bereich der IT-Sicherheit. eco sieht die nachfolgenden Aspekte für die folgenden Evaluierungen und das vorgelegte Inception Impact Assessment als besonders relevant an.

I. Allgemeine Anmerkungen

Der Regulierungsrahmen für IT-Sicherheit hat in den vergangenen fünf Jahren enorm an Dynamik gewonnen. Dies ist nachvollziehbar, da moderne Informationstechnologien und Netze in wachsendem Maße in systemkritischen Bereichen eingesetzt werden. Neben den bereits genannten europäischen Regelungen wurden auch auf nationaler Ebene entsprechende Gesetze erlassen, in Deutschland das IT-Sicherheitsgesetz von 2015, sowie das NIS-Richtlinien-Umsetzungsgesetz von 2017. Ein weiteres IT-Sicherheitsgesetz wird derzeit diskutiert und befindet sich in der Vorstufe des Gesetzgebungsverfahrens.

Vor diesem Hintergrund sollte festgehalten werden, dass jede neue Regulierung für Unternehmen Umsetzungsaufwand darstellt, der mit Anpassungen der betrieblichen Abläufe und Systeme einhergeht und mit Kosten verbunden ist. Ein sich dynamisch entwickelndes Regelwerk für IT-Sicherheit sollte daher im Interesse von Unternehmen, die um Rechtskonformität bemüht sind, konsistente und nachvollziehbare Regeln anstreben, die die Anforderungen und den Anpassungsdruck neben den

ständig stattfindenden technischen Neuerungen und Verbesserungen überschaubar halten und in vernünftigen Zyklen erfolgen.

II. Zum Inception Impact Assessment im Einzelnen

- **Zu „Problem the initiative aims to tackle“**

Die EU-Kommission führt an, dass die NIS-Richtlinie mit ihrer Vorgabe zur Mindestharmonisierung zwar grundsätzlich erfolgreich war und eine breite Akzeptanz in den meisten EU-Mitgliedsstaaten erfuhr, weist aber auch darauf hin, dass zahlreiche Regelungen, die mit Bezug zur NIS-Richtlinie geschaffen wurden, immer noch einen starken Grad an nationaler Fragmentierung aufweisen, der weiterer Harmonisierung bedarf. Nach Ansicht des eco ist dieses Bestreben grundsätzlich begrüßenswert. eco erachtet die weitere Harmonisierung auch von Sicherheitsvorgaben im IT-Bereich für einen zentralen Aspekt der weiteren Ausgestaltung des europäischen digitalen Binnenmarkts. Gleichzeitig möchte eco auch darauf hinweisen, dass nationale Besonderheiten teilweise dem Regulierungsgefüge an anderer Stelle geschuldet sind; bspw. dem Rechtsrahmen für Telekommunikation, wo ein hohes Maß an nationaler Regulierungsdichte vorherrscht, dessen Harmonisierung nicht ohne weiteres mit neuer Regulierung begegnet werden sollte, da dies Unternehmen vor einen überkomplexen Anpassungsdruck stellen könnte. Im Übrigen werden bei der Auswertung der Kommission „wichtige“ Akteure aufgeführt, die in der Regulierung derzeit nicht erfasst sind. Hier stellt sich die Frage, inwieweit es sich tatsächlich um kritische Bereiche oder systemrelevante Akteure handelt. Nach Ansicht des eco wäre es daher zunächst erforderlich eine Konkretisierung durch die Kommission vorzunehmen, bevor weitere Schritte im Bereich der Rechtssetzung erfolgen.

- **Zu „Objectives and Policy Options“**

Die EU-Kommission sieht derzeit vier verschiedene Optionen für die weitere Gestaltung und Entwicklung der NIS-Richtlinie.

Die erste Option sieht die Beibehaltung des Status Quo vor und dürfte auf die derzeitige Situation damit die geringsten Auswirkungen haben. Unklar ist hierbei, inwieweit dieser bestehende Status Quo die jeweiligen nationalen Gesetzgeber dazu ermutigt oder herausfordert, eigene Regulierung über die NIS-Richtlinie hinaus zu erlassen, und damit der Fragmentierung des Regulierungsgefüges Vorschub leisten würde, dem auch eco skeptisch gegenübersteht. Inwieweit bestehende begleitende Maßnahmen wie best-practices sich als hilfreich bei der weiteren Harmonisierung erweisen, ist letzten Endes nicht sicher festzustellen.

Die zweite Option sieht ergänzend zur Beibehaltung des bestehenden Rechtsrahmens weitere vorgesetzliche Maßnahmen vor. Ähnlich wie im ersten Szenario stellt sich auch hier die Frage, inwieweit diese Guidelines und Durchführungsrechtsakten mit nationalem Recht harmonisieren oder dort auch Doppelregulierung auslösen und inwieweit sich jeweils Nationalstaaten daran gebunden sehen. Die grundlegende Problematik von Szenario 1 lässt sich mit ergänzenden Ausführungen zumindest teilweise adressieren, was die Entwicklung eines besseren gemeinsamen Verständnisses von IT-Sicherheit anbetrifft. Gleichzeitig bleibt unklar, welche regulatorischen Konsequenzen sich jeweils in den Mitgliedsstaaten in Bezug auf die Regulierung von IT-Sicherheit ergeben.

Die dritte Option sieht eine teilweise Überarbeitung und ggfs. Ergänzung der NIS-Richtlinie vor. eco versteht diesen Ansatz so, dass die bestehende Regulierung im Wesentlichen beibehalten würde, während einzelne Teile überarbeitet, weiter konkretisiert und ggfs. ergänzende neue Elemente von Relevanz für die Regulierung aufgenommen würden. Insbesondere die Erweiterung des Anwendungsbereichs auf neue Sektoren oder Dienste „von ähnlicher Bedeutung“ ist hier ein zentraler Aspekt. Die teilweise Anpassung der NIS-Richtlinie wäre, aufbauend auf der bestehenden Regulierung nachvollziehbar, wobei unklar ist, inwieweit sich die Ausweitung des Anwendungsbereichs als tatsächlich sinnvoll darstellen wird. Bisherige Überlegungen auf nationaler Ebene haben keine plausible Begründung für eine Ausweitung des Regulierungsfeldes geliefert.

Die vierte Option sieht einen gänzlich neuen Rechtssetzungsakt vor, der die bestehende NIS-Richtlinie ersetzen soll, und mit dem verbindliche einheitliche Regeln im Bereich der IT-Sicherheit geschaffen werden sollen. Auch in diesem Fall wäre eine Ausweitung des Anwendungsbereichs der NIS-Richtlinie bzw. deren Nachfolgeregelung die Konsequenz. Ähnlich wie bei Option 3 stellt sich auch hier die Frage, wie eine sinnvolle Erweiterung des NIS-Rechtsrahmens erfolgen kann. Gleichzeitig stellt sich die Frage, inwieweit durch eine mögliche striktere Vereinheitlichung des Rechtsrahmens auf bereits bestehende nationale Regulierung reagiert wird. Wie bereits eingangs beschrieben, existieren außerhalb der Regulierung von IT-Sicherheit bereits in zahlreichen Sektoren bereichsspezifische Regeln, die entsprechend ebenfalls berücksichtigt und in Konsequenz angepasst werden müssten.

- **Zu „Likely economic impacts“**

Neben den im Inception Impact Assessment beschriebenen positiven Aspekten, sollte auch berücksichtigt werden, dass die ständigen regulatorischen Anpassungen, Ergänzungen und Erweiterungen zum einen das Risiko einer zunehmenden und divergierenden Doppelregulierung für

Unternehmen nach sich ziehen, die insbesondere kleine und mittelständische Unternehmen einem weiteren kontinuierlichen Anpassungsdruck unterwerfen. eco begrüßt grundsätzlich ein solides und möglichst europaweit einheitliches und hohes Maß an IT-Sicherheit. Gleichzeitig weist eco darauf hin, dass zur Erreichung dieses Ziels für Unternehmen verlässliche, nachvollziehbare und erfüllbare Regeln gelten sollten und insbesondere der technische und organisatorische Anpassungsbedarf für diese handhabbar bleibt. Dies sollte insbesondere bei der weiteren Ausgestaltung von Melde- und Berichtspflichten berücksichtigt werden.

III. Zusammenfassung und Bewertung

Mit einer Überarbeitung der NIS-Richtlinie setzt sich die EU-Kommission in einem dynamischen Regulierungsumfeld das ambitionierte Ziel, die bestehende, grundsätzlich als erfolgreich eingestufte NIS-Richtlinie maßgeblich zu erweitern und deren Anwendung in den EU-Mitgliedsstaaten stärker zu vereinheitlichen. eco begrüßt das Ziel der Kommission und hält dieses für grundsätzlich unterstützenswert. Gleichzeitig weist eco darauf hin, dass Unternehmen bei einer etwaigen Anpassung neben der europäischen auch die jeweilige nationale Rechtslage zu berücksichtigen haben. Hinsichtlich einer möglichen Ausweitung des bestehenden NIS-Regimes auf neue Sektoren und Felder stellt sich die Frage, wie diese ausgestaltet sind und inwieweit die Regeln für diese Sektoren nachvollziehbar und verhältnismäßig sind. Hierbei sind auch weitergehenden rechtliche Fragestellungen zu berücksichtigen beispielsweise Auswirkungen und Vereinbarkeit mit der Informations- und Pressefreiheit. Nach Ansicht des eco gilt es, dies bei der Weiterentwicklung des Rahmens der NIS-Richtlinie zwingend zu berücksichtigen. Einer erfolgreichen Weiterentwicklung der IT-Sicherheitsregulierung wäre sicher eine weitere Harmonisierung von Vorschriften im Rahmen des digitalen Binnenmarkts von Vorteil.

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.