VERBAND DER INTERNETWIRTSCHAFT E.V.

ENTWURF: Stellungnahme zum Kommissionsentwurf einer Richtlinie „On a high common level of cybersecurity across the Union repealing Directive (EU) 2016/1148"

Berlin, 4. Februar 2021

Mit der NIS-Richtlinie aus dem Jahr 2016 und dem EU-Cybersecurity Act aus dem Jahr 2019 hat die Europäische Union den Rahmen für die rechtliche und institutionelle Gestaltung der Regulierung von IT-Sicherheit für die EU und ihre Mitgliedsstaaten gesetzt. Für die NIS-Richtlinie stellte sie im Rahmen einer vorzeitigen Auswertung Anfang 2020 eine neue Regelung in Aussicht. Mit dem nun vorgelegten Richtlinienentwurf „On a high common level of cybersecurity across the Union repealing Directive (EU) 2016/1148" hat die Kommission dieser Ankündigung Rechnung getragen und eine Nachfolgerichtlinie (im Folgenden als NIS-2 bezeichnet) auf den Weg gebracht.

Mit dem nunmehr vorliegenden Richtlinienentwurf soll die alte NIS-Richtline abgelöst werden, ihr Regulierungsfeld an neue Herausforderungen angepasst werden. eco erkennt die Bemühungen der EU-Kommission zur Verbesserung und weiteren Harmonisierung der IT-Sicherheit in Europa an und weist darauf hin, dass die Bemühungen der Kommission den bisherigen Erfolgen der NIS-Richtlinie Rechnung tragen sollten.

eco sieht in der Richtlinie einen geeigneten Rahmen für die Ausgestaltung der Regulierung für IT-Sicherheit in Europa und verbindet damit auch die Hoffnung einer Stärkung des europäischen digitalen Binnenmarkts. eco erkennt an, dass der mit NIS-2 angestrebte Regulierungsrahmen robust ausgestaltet werden soll und in wesentlichen Punkten den Erfahrungen mit der bisherigen NIS-Richtlinie Rechnung trägt. Gleichzeitig möchte eco an einigen Stellen noch ergänzende Anmerkungen machen, um eine stärkere Orientierung auf den digitalen Binnenmarkt hin zu erreichen. Zuletzt sollte aus der Sicht von eco die Rolle und Bedeutung der so genannten „wichtigen Einrichtungen" weiter bestimmt und konkretisiert werden, so dass eine sinnvolle Abgrenzung von kritischen Infrastrukturen besser möglich ist.

Zum vorliegenden Richtlinienentwurf möchte eco nachfolgend erste Anmerkungen machen.

I. Allgemeine Anmerkungen:

- **Betroffenenkreis der „wichtigen Einrichtungen"**

Die NIS-2 Richtlinie schafft ein Regulierungsfeld aus „grundlegenden" und „wichtigen" Einrichtungen. Erstere knüpfen stark an das Regulierungsgefüge

der kritischen Infrastrukturen (KRITIS) an. Mit den „wichtigen Einrichtungen“ hingegen wird das Regulierungsfeld auf weitere Unternehmen ausgeweitet. Ein zentraler Erfolgsfaktor für die zukünftige Gestaltung von IT-Sicherheit wird sich um die Frage drehen, wie diese „wichtigen“ Einrichtungen reguliert werden. Der Kommissionsentwurf stellt hierfür ein ex-post Kontrollregime in Aussicht und umreißt Sektoren und Unternehmen, die als „wichtige Einrichtungen“ klassifiziert sind. Unklar bleibt indessen, wie sich die ex-post Kontrolle für „wichtige Einrichtungen“ aufstellt und inwieweit sich Maßgaben, Ziel- und Schwellenwerte von denen „grundlegender Einrichtungen“ konkret unterscheiden. Hier bedarf es aus Sicht der Internetwirtschaft mehr Klarheit, um die Regulierung von „grundlegenden“ und „wichtigen“ Einrichtungen besser zu differenzieren.

- **Sicherstellung von IT-Sicherheit in Lieferketten**

Die Sicherstellung von IT-Sicherheit in Lieferketten wird vor dem Hintergrund des Ausbaus neuer Mobilfunknetze auf dem 5G-Standard sowohl in den Mitgliedsstaaten als auch auf europäischer Ebene diskutiert. Sie ist auch darüber hinaus wichtig, wenn es um die Frage geht, welche Hardware in IT-Systemen eingesetzt wird und in welchem Umfang Technologien Angriffen gegenüber besonders exponiert sind. Zwar fällt die konkrete Ausgestaltung entsprechender Maßgaben in den Verantwortungsbereich der Mitgliedsstaaten. Dennoch wäre es aus der Sicht von eco sinnvoll und unterstützenswert, im Sinne eines digitalen Binnenmarktes, auf eine stärkere Harmonisierung der verschiedenen nationalen Regelungen hinzuwirken. Dieser Gedanke wird teilweise in NIS-2 aufgegriffen, sollte jedoch insbesondere durch die NIS-Cooperation Group und durch stärkere Normierung und Standardisierung europäisch und international unterstützt werden.

- **Auflagen für Domain-Name-Systems müssen verhältnismäßig sein**

Die Auflagen, die NIS-2 für Registrare und Registries vorsieht, ist aus der Sicht von eco zu streng. Das Geschäft mit Domains ist in der Regel ein Massengeschäft, so dass das ständige und genaue Identifizieren und Verifizieren von Domaininhabern für Registrare und Registries einen enormen bürokratischen und finanziellen Aufwand darstellt, der sich letzten Endes auch auf Anwenderinnen und Nutzer auswirken wird. Dem stehen in der Regel nur begrenzte Vorteile gegenüber, so dass die Verhältnismäßigkeit der Regelungen in NIS-2 kritisch überprüft werden sollte. eco hatte sich in der Vergangenheit dafür ausgesprochen, auf Grundlage der erfolgten Zahlungen und der hinterlegten Zahlungsdaten im Bedarfsfall eine Identifizierung durchzuführen und so entsprechende Informationen beizutreiben. Ein solcher „Folge-den-Zahlungen“–Ansatz dürfte genauso

zielführend, weniger invasiv und von den betroffenen Unternehmen besser zu bewältigen sein.

II. Zu den Artikeln im Einzelnen

Zu Artikel 2: Scope

Der Entwurf für NIS-2 erfasst gemäß Artikel 2 (2) auch “public electronic communications networks or publicly available electronic communications services”. Dies entspricht im Wesentlichen dem Anwendungsbereich des Art. 40 des Europäischen Kodex für elektronische Kommunikation (EKEK). Unklar ist indessen, wie sich die beiden Regelungen zueinander verhalten. eco sieht in den hier getroffenen Regelungen das Risiko einer Doppelregulierung, wenn diese nicht umgekehrt im EKEK in einer genauso konsistenten Weise nachvollzogen werden. Hier wäre eine Klarstellung dahingehend wünschenswert, dass die Regelungen des EKEK aufgehoben sind und in die NIS-2 Richtlinie integriert werden, oder dass Unternehmen, die über den EKEK reguliert sind, von der NIS-2 Richtlinie ausgenommen sind. Da dies derzeit nicht vorgesehen ist, besteht nach Ansicht des eco Nachbesserungsbedarf.

Daneben wirft der Vorschlag zu Artikel 2 die Frage auf, inwieweit die Hersteller von Hard- und Software für die Betreiber kritischer Infrastrukturen in die Regelungen der NIS-2 mit einbezogen werden. Derzeit sieht NIS-2 insbesondere für Telekommunikationsunternehmen eine alleinige Verantwortung für den sicheren Betrieb ihrer Infrastrukturen und Lieferketten vor und schafft einen Vorbehalt zu deren weiterer Regulierung (vgl. Artikel 18 (3) und Artikel 19). Hier wäre es – auch im Sinne einer sachgerechten Verteilung von Verantwortlichkeiten für IT-Sicherheit – begrüßenswert, wenn in die Regelungen auch Zulieferer und Entwickler einbezogen werden können, so dass die Betreiber grundlegender und wichtiger Einrichtungen (essential und important entities) bei einer Compliance mit den entsprechenden Regelungen nicht das alleinige Risiko vertragsrechtlicher und wirtschaftlicher Nachteile tragen müssen.

Darüber hinaus schafft NIS-2 eine Unterscheidung von Anbietern digitaler Dienstleistungen (Digital Service Providers) und Rechenzentren. Die Kommission folgt damit der Kritik des in der alten NIS-Richtlinie oftmals als zu unpräzise gefassten Begriffs der Cloud-Diensteanbieter. eco befürwortet diese Klarstellung, möchte allerdings gleichzeitig darauf hinweisen, dass die jeweiligen Regelungen für Digital Services Providers und Data Centres nicht zu einander in Widerspruch stehen sollten. Um Doppelregulierung zu vermeiden, sollten sie aufeinander abgestimmt sein und ineinandergreifen.

Zu Artikel 3: Minimum harmonisation

Wie auch mit der Vorgängerregelung hat die Kommission den Weg einer Richtlinie gewählt. Dies ist mit Blick auf die Vorgaben zur Rechtsetzung der

Union nachvollziehbar. Positiv hervorzuheben ist, dass die Richtlinie harmonisiert ist und dadurch ein europaweiter Mindeststandard gesetzt wird. Wünschenswert wäre es darüber hinaus, wenn die Kommission und ENISA darauf hinarbeiteten, ein möglichst einheitliches Regulierungsregime europaweit umzusetzen und zu etablieren. Vor diesem Hintergrund schlägt eco vor, zu prüfen, welche Aspekte aus dem NIS-2 Richtlinienvorschlag im Rahmen einer Verordnung umgesetzt werden könnten, so dass zumindest für diese Bereiche eine Vollharmonisierung der IT-Sicherheitsregulierung realisiert werden könnte.

Zu Artikel 5: National cybersecurity strategy

eco befürwortet den Ansatz der Kommission, Mitgliedsstaaten auf Basis der Richtlinie aufzufordern, nationale Cybersicherheitsstrategien zu entwickeln. Diese können mit Hilfe der Vorgaben der NIS-2-Richtlinie konkrete und operationalisierbare Ziele erreichen. Entsprechende Strategien können technische, rechtliche und institutionelle Entwicklungspotentiale aufzeigen aber auch frühzeitig mögliche Divergenzen in den jeweiligen nationalen Regulierungsansätzen sichtbar machen. Daneben werden mit den nationalen Cybersicherheitsstrategien auch weitere Aspekte, wie die Sicherung von Lieferketten, angeführt. eco weist in diesem Kontext darauf hin, dass entsprechende nationale Initiativen eine starke Fragmentierung des IT-Marktes in Europa zur Folge haben können. Aspekte, die auf eine stärkere Fragmentierung des Binnenmarktes hinauslaufen könnten, sollten aus der Richtlinie entfernt werden. Stattdessen sollte verstärkte Kooperation und Harmonisierung über die NIS-Cooperation Group und die europäische Cybersicherheitsagentur angestrebt werden. Diese können dann zwar keine bindenden Vorgaben machen, erzeugen jedoch allgemeine normative Wirkung, die in allen Mitgliedsstaaten berücksichtigt werden.

Zu Artikel 6: Coordinated vulnerability disclosure and a European vulnerability registry

Der Ansatz, einen strukturierten und grenzübergreifenden Mechanismus für die Meldung von Sicherheitslücken einzuführen, ist nach Ansicht des eco begrüßenswert. Ebenso positiv zu bewerten ist der Ansatz, Hersteller von Informations- und Kommunikationstechnologie ebenfalls in die Melde-strukturen einzubeziehen, wie die von Sicherheitsvorfällen betroffenen Unternehmen. eco unterstützt den Ansatz der Kommission und sieht darin eine Möglichkeit zu einer deutlichen Verbesserung der bestehenden Meldestrukturen. Gleichzeitig sollte allerdings darauf geachtet werden, dass die Meldeprozesse möglichst effizient auszugestalten sind. Damit kann erreicht werden, dass Unternehmen im Stande sind, erhaltene Hinweise schnell und effizient umzusetzen und nicht durch überbordende

Informationspflichten beeinträchtigt werden. Vor diesem Hintergrund sollte auch der Umfang der Meldungen eindeutig bestimmt und festgelegt werden.

Zu Artikel 10: Requirements and tasks of CSIRTs

Die im Entwurf zu Artikel 10 (2) Punkt e NIS-2 vorgesehene Möglichkeit proaktiver Maßnahmen durch CSIRTs (Computer Security Incident Response Team), zum Scannen von Netzwerken und Technologien, ist in der vorliegenden Form sehr unspezifisch, da jegliche Einrichtung dazu berechtigt scheint, von den CSIRTs entsprechende Maßnahmen zu verlangen. Netzwerk- und Portscans stellen tiefgreifende Eingriffe in IT-Systeme und Netze dar, die unter Umständen schädliche Auswirkungen nach sich ziehen können, und sollten daher nur von den jeweils betroffenen Netzbetreibern bzw. Einrichtungen oder in deren Auftrag durchgeführt werden dürfen. Nach Ansicht des eco müssen aufgrund der Eingriffstiefe und der Auswirkungen auf die Infrastrukturen hier eindeutig und abschließend die Befugnisse und die Reichweite für die Regelungen und den Befugnissen der CSIRT festgelegt und bestimmt werden.

Zu Artikel 17: Governance

eco begrüßt die Bemühungen der EU-Kommission, eine harmonisierte Umsetzung von NIS-2 anzustreben. Ebenso ist es unterstützenswert, dass neben den grundlegenden Einrichtungen (KRITIS) auch die so genannten wichtigen Einrichtungen stärker kontrolliert werden sollten. Vor diesem Hintergrund bewertet eco die angestrebten Regelungen zur Governance grundsätzlich positiv. Allerdings sieht eco in den Vorgaben zum „Training“ von Mitgliedern des Managements entsprechender Einrichtungen eine unverhältnismäßige Regelung, die administrativen Aufwand erzeugt, ohne, dass dem ein erkennbarer Mehrwert entgegensteht. Es ist grundsätzlich davon auszugehen, dass grundlegende und wichtige Einrichtungen spezialisierte Teams für die Sicherung ihrer IT-Systeme einsetzen und verfügbar haben, die die individuell erforderlichen konkreten Maßnahmen umsetzen. Darüber hinausgehende Verpflichtungen und die vorgeschlagenen „Trainings für das Management“ sind in diesem Kontext nicht zielführend.

Zu Artikel 18: Cybersecurity risk management measures

Um Cybersicherheit effektiv regulieren und überwachen zu können, müssen die zuständigen nationalen Behörden entsprechende Regelungen erlassen. Vor diesem Hintergrund bewertet eco die Regelungen und Anforderungen in Artikel 18 als grundsätzlich sachgerecht. Gleichwohl gilt es zu bedenken,

dass die jeweiligen Regelungen den unterschiedlichen Anforderungen an grundlegende und wichtige Einrichtungen jeweils gerecht werden müssen. Die im Richtlinienentwurf gesetzten Maßstäbe hierfür erscheinen allerdings vor diesem Hintergrund noch nicht differenziert genug. Zudem möchte eco darauf hinweisen, dass Regelungen zu Versorgungsketten grundsätzlich möglichst auf europäischer Ebene adressiert werden sollten, um mit Blick auf den digitalen Binnenmarkt eine Fragmentierung zu vermeiden.

Hinsichtlich der Regelungen zum Einsatz von Verschlüsselung sollte ergänzend festgehalten werden, dass diese auch die Hersteller von Endgeräten und Software mit einbeziehen sollten und nicht nur die grundlegenden und die wichtigen Einrichtungen, da insbesondere Ende-zu-Ende Verschlüsselung nur mit deren Unterstützung effektiv realisiert werden kann.

Zu Artikel 19: EU coordinated risk assessments of critical supply chains

Die Koordinierung bei der Bewertung von Risiken in Lieferketten ist nach Ansicht des eco ein wichtiges Element für die Gestaltung der IT-Sicherheit in Europa und trägt dem digitalen Binnenmarkt angemessen Rechnung. Vor diesem Hintergrund bewertet eco es als positiv, dass auf europäischer Ebene eine koordinierte Regelung als Möglichkeit ausdrücklich angeführt wird. Nach Ansicht des eco wäre es daher auch notwendig und erforderlich, dem mit der Regelung vorgeschlagenen koordinierten Ansatz mehr Bedeutung beizumessen.

Zu Artikel 20: Reporting obligations

eco sieht in Meldeverfahren und dem Austausch über Sicherheitslücken einen wichtigen Beitrag zur Gewährleistung von IT-Sicherheit. Die Verpflichtung, Nutzer über etwaige Störungen bei Diensten nach Möglichkeit zu unterrichten ist in der vorgeschlagenen Ausgestaltung jedoch problematisch, da durch eine entsprechende Unterrichtungsverpflichtung auch die Möglichkeiten zur Eindämmung und Verfolgung entsprechender Angriffe eingeschränkt und untergraben werden. eco plädiert dafür, die Unterrichtungspflicht für Anwender und Nutzer als freiwillig auszugestalten. Eine verpflichtende Meldung sollte nur im Fall eines etwaigen Datenabflusses oder der Erforderlichkeit eines Nutzereingriffes (z.B. einer Passwortänderung) vorgesehen werden.

Darüber hinaus sind die in Artikel 20 dargelegten Meldepflichten für grundlegende und wichtige Einrichtungen nach Ansicht des eco nicht praktikabel. Das auf Grundlage von Artikel 20 (4) etablierte mehrstufige Meldeverfahren ist unpraktikabel, mit erheblichem administrativem Aufwand

verbunden und bindet daher unnötig Ressourcen, die besser für die Bewältigung des Sicherheitsvorfalls eingesetzt werden könnten. Die vorgeschlagene Frist von 24 Stunden für die Erstmeldung ist zu starr und für die tatsächliche Bewältigung des IT-Sicherheitsvorfalls nicht zielführend. Hier wäre begrüßenswert, wenn an das aus der bestehenden NIS-Richtlinie etablierte Meldesystem angeknüpft werden könnte. Demnach sollten Meldungen unverzüglich (ohne schuldhaftes Verzögern) erfolgen. Damit könnte ein verhältnismäßiges und gleichzeitig funktionierendes Melderegime etabliert und die Anzahl regelmäßig aktualisierter Zwischenmeldungen deutlich reduziert werden.

Zu Artikel 21: Use of European cybersecurity certification schemes

Gütesiegel im Bereich der Cybersicherheit können einen sinnvollen Beitrag zur Verbesserung der IT-Sicherheit liefern, indem sie Anwendern und Nutzern eine strukturierte Marktübersicht gewähren. Allerdings sollte bei der Entwicklung entsprechender Gütesiegel beachtet werden, dass diese primär auf die Konformität mit bestimmten Sicherheitsauflagen und die Einhaltung von Prozeduren und Standards abzielen, um ihre Glaubwürdigkeit nicht zu untergraben und den Mehrwert, den entsprechende Zertifizierungsstrukturen bieten nicht zu konterkarieren.

Zu Artikel 23: Databases of domain names and registration data

Die Verpflichtung zur Bereitstellung regelmäßig aktualisierter Informationen über die Betreiber von Domains für Registrare und Registries sind aus der Sicht von eco unverhältnismäßig und stellen für die betroffenen Unternehmen eine erhebliche administrative und finanzielle Belastung dar. Unklar ist zudem, inwieweit sich durch diese Maßnahme die Sicherheit von IT-Systemen tatsächlich verbessert, bspw. wenn eine Domain umgeleitet oder eine entsprechend auf der Domain hinterlegte Website gehackt wurde. Vor diesem Hintergrund sieht eco diese Verpflichtung als unverhältnismäßig an und fordert den Gesetzgeber auf, die Auflagen für Registrare und Registries von Domains noch einmal kritisch zu überprüfen und auf ihren Mehrwert für die Sicherheit zu hinterfragen.

Zu Artikel 24: Jurisdiction and territoriality

Die Klarstellung zur Regelung für die in Artikel 24 (1) benannten Unternehmen ist grundsätzlich begrüßenswert. Darüber hinaus sieht eco jedoch die Notwendigkeit, klarzustellen, inwieweit die Regelungen zur Regulierung insbesondere von Clouddiensten, die europaweit angeboten werden, angewandt werden. Es sollte dringend vermieden werden, dass

diese unter unklare Aufsichtsstrukturen fallen. Daher wäre eine weitere Konkretisierung dahingehend, ob der Hauptsitz eines Konzerns oder der Hauptsitz für die Legaleinheit eines Konzerns ausschlaggebend ist, die den entsprechenden Dienst anbietet, zu begrüßen.

Zu Artikel 25: Registry for essential and important entities

Die in Artikel 25 vorgesehenen Regelungen zur Registrierung grundlegender und wichtiger Einrichtungen sehen eine Meldepflicht für die betroffenen Unternehmen und Einrichtungen vor. Gleichzeitig sind auch die nationalen Aufsichtsbehörden dazu verpflichtet, entsprechende Kontakte zu Ansprechpartnern vorzuhalten. eco sieht in der Regelung für Artikel 25 das Risiko einer doppelten Registrierungspflicht, die er als zu bürokratisch ablehnt. Anstelle dessen wäre es sinnvoller, wenn die Registrierung grundlegender und wichtiger Einrichtungen entweder in den jeweiligen Mitgliedsstaaten oder direkt bei ENISA erfolgen würde und dann jeweils an die andere korrespondierende Einrichtung weitergegeben werden könnte.

Zu Artikel 29: Supervision and enforcement for essential entities

eco erachtet die in Artikel 29 dargelegten Möglichkeiten zur Aufsicht über die Anbieter grundlegender Einrichtungen als zu weitgehend. Der Anspruch für Behörden, entsprechende Informationen von Betreibern grundlegender Einrichtungen zu erhalten, muss mit hinreichenden Auflagen für deren Weiterverwendung verbunden sein, da es sich dabei oft um betriebliche Informationen und auch um Geschäftsgeheimnisse handeln könnte. Vor diesem Hintergrund ist es nach Ansicht des eco erforderlich, dass entsprechende Auflagen für die Anbieter grundlegender Einrichtungen auch mit korrespondierenden Verpflichtungen für die anfragenden Behörden einhergehen.

Besonders tiefgreifend und einschneidend sind darüber hinaus die Auflagen aus Artikel 29 (2) Punkte c und d, die in Verbindung mit Artikel 10 auch simulierte oder tatsächliche Angriffe auf IT-Systeme entsprechender Einrichtungen umfassen können, die den Betrieb der Einrichtung nachhaltig beeinträchtigen und darüber hinaus schwere wirtschaftliche Schäden verursachen können. Vor diesem Hintergrund sind entsprechende Regelungen dringend einzuschränken und auf das zwingend notwendige Maß zu beschränken.

Zudem sind die in Artikel 29 (5) enthaltenen Regelungen zur Sanktionierung einzelner Personen aus grundlegenden und wichtigen Einrichtungen unverhältnismäßig. Die vorgeschlagenen Regelungen gehen deutlich über das übliche Maß von Organisationshaftung hinaus und greifen in das Recht der freien Berufsausübung ein. Nach Ansicht des eco sind diese Regelungen

nicht mit den Maßgaben von Artikel 15 der europäischen Grundrechtecharta vereinbar.

Zu Artikel 30: Supervision and enforcement for important entities

eco befürwortet den von der Kommission gewählten Ansatz eine ex-post Kontrolle für wichtige Einrichtungen zu etablieren. Diese kann Grundlage für eine nachvollziehbare und verhältnismäßige Regulierung von IT-Sicherheit für zentrale Akteure unterhalb der KRITIS-Schwelle darstellen. Gleichzeitig sieht eco die Herausforderung darin, die Auflagen für wichtige Einrichtungen angemessen von denen kritischer Infrastrukturen zu differenzieren. Vor diesem Hintergrund wären weitere Ausführungen und eine Konkretisierung zur Kontrolle wichtiger Einrichtungen und dem für sie angestrebten Regulierungsrahmen sinnvoll.

Zu Artikel 31: General conditions for imposing administrative fines on essential and important entities

Die in der Richtlinie vorgesehenen Bußgeldrahmen von 2 Prozent des Jahresumsatzes oder 10 Mio. Euro sind nach Ansicht des eco deutlich zu hoch bemessen. Sie orientieren sich an den Bußgeldregeln der Datenschutzgrundverordnung, die einen maßgeblichen Eingriff in die Privatsphäre von Bürgerinnen und Bürgern annehmen, was im Falle eines IT-Sicherheitsvorfalls zwar theoretisch auch auftreten kann, jedoch nicht zwingend damit verbunden sein muss. Inwieweit die hier dargelegten Bußgelder sich darüber hinaus auch mit eventuellen weiteren Bußgeldern für Datenschutzverstöße kumulieren, bleibt unklar, ist jedoch anzunehmen. eco plädiert entsprechend dafür, einen geeigneteren und deutlich niedrigeren Ansatz für die Bußgelder zu wählen.

Zu Artikel 32: Infringements entailing a personal data breach

Die vorgesehene Meldepflicht für Datenverlust mit Auswirkung auf die Datenschutzgrundverordnung (DSGVO) ist nachvollziehbar. Nach Ansicht des eco besteht allerdings die Problematik, dass durch das Auseinanderfallen von Datenschutzaufsicht und Aufsicht über IT-Sicherheit, sich folglich die Meldepflichten und Meldewege oft doppeln. Daher wäre es begrüßenswert, die Anzahl der Meldungen im Falle eines bekannt gewordenen Sicherheitsproblems möglichst effizient und effektiv auszugestalten. Hierdurch wäre gewährleistet, dass in einer kritischen und schwierigen Situation Ressourcen effizient und effektiv für die Behebung des Sicherheitsvorfalls eingesetzt werden können. eco spricht sich daher dafür aus, die Meldewege und Meldeketten effizient und effektiv auszugestalten,

Doppelmeldungen von vornherein zu verhindern und Zuständigkeiten zu bündeln.

Fazit:

Der Entwurf der NIS-2-Richtlinie der Europäischen Kommission bildet grundsätzlich ein sinnvolles und solides Regulierungsgefüge, das auf bestehenden Strukturen und Verfahren aufsetzt. Nach Ansicht des eco ist dies positiv zu bewerten. Nachvollziehbar ist auch, dass zahlreiche in der Richtlinie berührte Aspekte der nationalen Gesetzgebung vorbehalten sind und durch europäische Gesetzgebung nicht ohne weiteres reguliert werden können. Gleichwohl möchte eco darauf hinweisen, dass eine stringentere Regulierung mit Blick auf den digitalen Binnenmarkt ein zentrales Element der NIS-2-Richtlinie werden muss, wenn diese letzten Endes erfolgreich sein soll. Andernfalls besteht durch die geplante Ausweitung des Anwendungsbereichs auf so genannte „wichtige Einrichtungen“ sonst die Gefahr einer weiteren Fragmentierung und einer wachsenden Unübersichtlichkeit für die europäische Internetwirtschaft. eco spricht sich daher für eine Stärkung entsprechender Bemühungen zur Institutionalisierung der IT-Sicherheitsregulierung auf europäischer Ebene aus. Dabei muss darauf geachtet werden, die Potentiale und Kapazitäten der bestehenden Einrichtungen, wie der NIS-Cooperation Group oder entsprechenden Normierungs- und Standardisierungsgremien, voll auszuschöpfen. Nur so kann ein überkomplexes Institutionengefüge vermieden werden. Zudem muss auch darauf geachtet werden, dass bei der Ausweitung des Anwendungsbereichs von NIS-2 keine Doppel- oder Mehrfachregulierung entsteht. Dementsprechend sollte auf den bereits spezialgesetzlich regulierten Telekommunikationssektor ein besonderes Augenmerk gelegt werden. Kritisch hinterfragt und einer Überprüfung unterzogen müssen im weiteren Gesetzgebungsverfahren die vorgesehenen weitreichenden Befugnisse für nationale Aufsichtsbehörden und dazu gehörige CSIRTs, die tiefgreifende Eingriffe in Infrastrukturen und IT-Systeme implizieren und deren Funktionsfähigkeit beeinträchtigen können. Außerdem sollte bei den Maßnahmen der NIS-2 und den damit verbundenen potentiellen Eingriffen die Vereinbarkeit mit der EU-Grundrechtecharta kritisch geprüft und rechtssicher ausgestaltet 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.