An das
Bundeskanzleramt
Sektion I – Präsidium
Abteilung I/C/8 – Cyber Security, GovCERT, NIS-Büro und ZAS

E-Mail: nis@bka.gv.at

Wien, am 25. März 2021

Sehr geehrter Herr Mag. Heußler,
Sehr geehrte Damen und Herren,

die ISPA bedankt sich für die Möglichkeit, auf die folgenden Punkte des Entwurfs einer Richtlinie über Maßnahmen für ein hohes gemeinsames Maß an Cybersicherheit in der gesamten Union („NIS-2-Richtlinie“) aufmerksam zu machen, und steht jederzeit für Rückfragen zur Verfügung:

- Ausweitung des Anwendungsbereichs auf sämtliche Anbieter von elektronischen Kommunikationsdiensten/-netzen (Art 2)

Anbieter von elektronischen Kommunikationsdiensten bzw. -netzen sind bereits seit jeher auch in ihrem eigenen Interesse daran bemüht, ein hohes Sicherheitsniveau zu gewährleisten. Denn ein solches ist eine Grundvoraussetzung dafür, dass Kundinnen und Kunden in die Dienste dieser Unternehmen vertrauen und diese nutzen. Die Unternehmen unterliegen zudem auch strikten Sicherheitsvorgaben in deren sektorspezifischen Rechtsrahmen, der erst vor kurzem durch den European Electronic Communications Code[1] erneuert wurde.

Dieser enthält in Art 40 u. 41 zwei Bestimmungen zur Gewährleistung der Sicherheit der Netze und Dienste, die derzeit gerade im Rahmen der nationalen Implementierung des EECCs – in Österreich etwa durch das TKG 2021 – umgesetzt werden. Darüber hinaus, wurden auch in der im vergangenen Jahr beschlossenen „5G-Toolbox“[2] der EU-Kommission zahlreiche neue Vorgaben geschaffen, die in Österreich in die Telekom-Netzsicherheitsverordnung[3] aufgenommen und von den betroffenen Unternehmen gerade erst umgesetzt werden.

[1] Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation
[2] Empfehlung (EU) 2019/534 der Kommission vom 26. März 2019 Cybersicherheit der 5G-Netze. (ABl. Nr. L 88 S. 42)
[3] Verordnung der Rundfunk und Telekom Regulierungs-GmbH (RTR-GmbH) über Verpflichtungen von Betreibern elektronischer Kommunikationsnetze und Anbietern elektronischer Kommunikationsdienste im Zusammenhang mit Mindestsicherheitsmaßnahmen unter Berücksichtigung von 5G-Netzen sowie mit Informationspflichten bei Sicherheitsvorfällen

Der Entwurf der NIS-2-Richtlinie sieht nun vor – anders als bislang die NIS-Richtlinie – sämtliche dieser Anbieter in den Anwendungsbereich aufzunehmen, noch dazu, ohne dabei Klein- und Kleinstunternehmen vom Anwendungsbereich der Richtlinie auszunehmen wir dies bei den anderen erfassten Sektoren der Fall ist. Dies hätte zu Folge, dass die betroffenen Unternehmen innerhalb kurzer Zeit erneut erhebliche zusätzliche Anforderungen erfüllen müssten, wobei der zusätzliche Nutzen im Sinne der Cybersicherheit fraglich erscheint.

Die ISPA anerkennt zwar die Beweggründe, ein einheitliches Cybersicherheitsniveau über sämtliche kritische Sektoren hinweg zu schaffen. Dabei wird jedoch übersehen, dass gerade der IKT-Sektor bereits ein sehr hohes Sicherheitsniveau gewährleistet, und die zusätzlichen Vorgaben daher einen hohen administrativen Aufwand bedeuten, ohne, dass hierdurch jedoch das Sicherheitsniveau signifikant erhöht werden würde.

Aus diesem Grund ersucht die ISPA, Anbieter von elektronischen Kommunikationsdiensten bzw. -netzen weiterhin, wie auch schon gemäß Art 1 Abs. 3 der NIS-Richtlinie vom Anwendungsbereich auszunehmen, und im Rahmen der Richtlinie klarzustellen, dass Art 40 EECC bereits ein angemessenes, gleichwertiges Sicherheitsniveau gewährleistet.

Sofern der europäische Gesetzgeber sich jedoch dazu entschließt diese Unternehmen in den Anwendungsbereich aufzunehmen, ersucht die ISPA, dass zumindest das Größenkriterium in Art 2 Abs. 1, wonach Klein- und Kleinstunternehmen generell vom Anwendungsbereich ausgenommen sind, auch für Anbieter von elektronischen Kommunikationsdiensten bzw. -netzen gilt. Denn es erscheint nicht sachgemäß, weshalb dieser Sektor anders behandelt werden sollte als andere kritische Infrastrukturen. Gleichzeitig würden diese Klein- und Kleinstunternehmen ohnehin weiterhin Art 40 EECC unterliegen und dadurch ein gleichermaßen hohes Sicherheitsniveau gewährleisten.

Würden sämtliche Unternehmen hingegen ohne Rücksicht auf deren Größe in den Anwendungsbereich aufgenommen werden, ist zu befürchten, dass zahlreiche kleine Unternehmen, die oftmals regional wichtige Infrastruktur betreiben und somit single-points of failure vermeiden, angesichts der hohen zusätzlichen Aufwände vom Markt verschwinden. Hierdurch würde der Cyberresilienz erheblich geschadet werden, ohne, dass durch die zusätzlichen Aufwendungen ein tatsächlicher Mehrwert geschaffen wird.

- <u>ENISA IT-Schwachstellenregister (Art 6 Abs. 2)</u>

Sofern ENISA in Hinkunft ein eigenes IT-Schwachstellenregister betreibt bzw. zur Verfügung stellt, ist es unabdingbar sicherzustellen, dass hierdurch nicht eine lückenhafte Parallelinfrastruktur geschaffen wird, die am Ende der Cybersicherheit eher schadet als nutzt. Das Register sollte daher laufend mit der bereits bestehenden MITRE Common Vulnerabilities and Exposures (CVE) Datenbank abgeglichen werden bzw. sollten die beiden Datenbanken synchronisiert und einheitliche Identifier den jeweiligen Schwachstellen zugeordnet werden um so de facto als backup füreinander zu bestehen.

- Mindestanforderungen an Cybersicherheits-Risikomanagementmaßnahmen (Art 18 Abs. 2)

Gemäß Art 18 Abs. 1 müssen die der Richtlinie unterworfenen Unternehmen geeignete und angemessene technische und organisatorische Maßnahmen ergreifen, um die Risiken für die Sicherheit von Netzwerk- und Informationssystemen, die diese Unternehmen bei der Erbringung ihrer Dienstleistungen verwenden, zu bewältigen. Die entsprechenden Maßnahmen sollen dem bestehenden Risiko gemäß angemessen sein. Diese Vorgabe entspricht im Wesentlichen Art 14 Abs. 1 der NIS-Richtlinie.

Art 18 Abs. 2 des Entwurfs präzisiert diese Vorgabe jedoch weiter, indem eine Reihe an konkreten Mindestanforderungen aufgelistet werden, welche von sämtlichen Unternehmen umzusetzen sind. Obwohl die in der Liste enthaltenen Maßnahmen einzeln betrachtet durchaus sinnvolle Sicherheitsmaßnahmen darstellen, erscheint es dem Grundsatz der Verhältnismäßigkeit der Maßnahmen in Abs. 1 zu widersprechen, sämtliche Unternehmen zu sämtlichen dieser Maßnahmen zu verpflichten. Manche der angeführten Maßnahmen, wie etwa die verpflichtende Nutzung von Verschlüsselung, sind aufgrund geltender technischer Standards für manche Kommunikationstechnologien zudem überhaupt nicht vorgesehen. Beispielsweise sehen die aktuellen 3GPP und GSMA Standards in Bezug auf 5G-Technolgie Verschlüsselung nicht zwingend bzw. nur optional vor). Darüber hinaus verbieten etwa auch internationale Roamingvereinbarungen, dass Kommunikationsinhalte verschlüsselt werden.

Art 18 Abs. 5, nach dem es der EU-Kommission ermöglicht werden soll Durchführungsrechtsakte zu erlassen, in denen technische und methodische Spezifikationen für die in Absatz 2 genannten Maßnahmen festgelegt werden könnten, würde die Möglichkeit, je nach Risiko und Art des Unternehmens und betroffenen Dienstes verhältnismäßige Maßnahmen zu ergreifen noch weiter beeinträchtigen.

Die ISPA schlägt daher vor, die Liste der Mindestanforderungen in Artikel 18 Absatz 2 zu streichen und den in Art 18 Abs. 1 vorgesehenen flexiblen Ansatz beizubehalten, der es Unternehmen ermöglicht, Maßnahmen zu ergreifen, die dem jeweiligen Risiko angemessen sind. Zumindest sollten die Mindestmaßnahmen in Abs. 2 jedoch in eine beispielhafte Aufzählung möglicher Maßnahmen umgewandelt werden.

- Pflicht zur Meldung von Cyberbedrohungen (Art 20)

Die in Art 20 vorgesehene Pflicht, in Hinkunft auch Cyberbedrohungen zu melden ist nach Ansicht der ISPA überschießend und im Sinne der Cybersicherheit kontraproduktiv. Nach der weitreichenden Definition in Art 2 Z 8 des Rechtsakts zur Cybersicherheit[4] handelt es sich bei einer Cyberbedrohung um jeden „möglichen Umstand, ein mögliches Ereignis oder eine mögliche Handlung, der/das/die Netz- und Informationssysteme, die Nutzer dieser Systeme und andere Personen schädigen, stören oder anderweitig beeinträchtigen könnte“. Auch wenn die ISPA das

[4] Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013

grundsätzliche Bestreben anerkennt, auch weitere Bedrohungsszenarien als bereits eingetretene Sicherheitsvorfälle zu erfassen, geht diese Definition aus dem Cybersicherheitsakt weit über das Ziel hinaus, da hierdurch de facto jegliches, grundsätzlich denkbares Bedrohungsszenario gemeldet werden müsste. Generell stellt sich die Frage, ob nicht bereits die erweiterte Definition eines „erheblichen Sicherheitsvorfalls“ in Art. 20 Abs. 3 ausreicht, die nun auch Sicherheitsvorfälle erfasst die das Potential haben, zu erheblichen Schäden führen können – und nicht nur solche, durch welche ein Schaden bereits eingetreten ist.

Würde an der weitreichenden Definition einer „Cyberbedrohung“ festgehalten werden, ist zu befürchten, dass es zu einem Überschuss an Meldungen an die zuständigen nationalen Behörden kommen würde. Denn in der Regel wird ein Chief Information Security Officer über eine lange Liste solcher Bedrohungsszenarien verfügen. Bei einer dauerhaften Auslastung des Meldesystems ist wiederum zu befürchten, dass wichtige Meldungen möglicherweise verspätet behandelt werden.

Des weiteren sieht der Richtlinienentwurf auch eine Meldepflicht von Cyberbedrohungen an die Empfänger des Dienstes vor. Der Mehrwert einer solchen Meldepflicht wird von Seiten der ISPA stark in Frage gestellt und ist vielmehr zu befürchten, dass es zu kontraproduktiven Auswirkungen kommen würde, da solche Meldungen dazu führen können, dass Bedrohungsszenarien von Personen mit entsprechenden Absichten für Angriffe missbraucht werden und gleichzeitig das Vertrauen der Nutzer in die jeweiligen Dienste untergraben wird. Hierdurch wird somit dem Grundgedanken der Cybersicherheit geradezu entgegengewirkt.

- <u>Zertifizierungssysteme für Cybersicherheit müssen freiwillig bleiben (Art 21)</u>

In Art 21 wird vorgesehen, dass Mitgliedstaaten die der Richtlinie unterworfenen Unternehmen zur Einholung eines Europäischen Cybersicherheits-Zertifikats iSd Art 49 Cybersecurity Act für bestimmte IKT-Produkte, IKT-Dienste und IKT-Prozesse verpflichten können.

Dabei ist darauf hinzuweisen, dass seit der Verabschiedung des Cybersecurity Acts im Jahr 2019 bislang noch kein Cybersecurity-Zertifizierungssystem formell im Rahmen eines Durchführungsakts gemäß Artikel 49 Abs. 7 Cybersecurity Act umgesetzt wurde. Daher erscheint die in Art 21 vorgesehene Möglichkeit verfrüht.

Darüber hinaus existieren im Bereich der Informationssicherheit bereits weitere international anerkannte Zertifizierungsnormen – zu nennen ist insbesondere ISO 27001 – durch die ein entsprechender Nachweis bereits erbracht werden könnte. Um zu verhindern, dass Unternehmen, die bereits eine solche Zertifizierung eingeholt haben in Hinkunft zu einer weiteren redundanten Zertifizierung verpflichtet werden, sollte in Art 21 klargestellt werden, dass neben einem Cybersicherheits-Zertifikat gem. Art 49 Cybersecurity Act auch gleichwertige, international anerkannte Zertifizierungen zum Nachweis über die Einhaltung der Vorgaben in Art 18 ausreichen.

ISPA – Internet Service Providers Austria
Währingerstrasse 3/18, 1090 Wien, Austria
☎ +43 1 409 55 76
✉ office@ispa.at
www.ispa.at

UniCredit Bank Austria AG
Konto-Nr.: 00660 491 705, **BLZ:** 12000
BIC: BKAUATWW
IBAN: AT59 1200 0006 6049 1705

UID-Nr.: ATU 54397807
ZVR-Zahl: 551223675

- Datenbanken für Domainregistrierungsdaten (Art 23)

Nach Ansicht der ISPA ist es fraglich inwieweit die in Art 23 vorgesehene Pflicht für Registries bzw. Registrars zur Erhebung und Überprüfung der Registrierungsdaten von Domainnameinhabern tatsächlich zu einem höheren Maß an Cybersicherheit beitragen würde. Aktuelle Berichte, wie etwa der ENISA Threat Landscape Report 2020 zeigen deutlich, dass fehlerhafte Domainname-Registrierungsdaten keine Rolle bei der Gefährdung der Cybersicherheit spielen. Auch für die Sicherheit des DNS im engeren Sinn spielen falsche Registrierungsdaten keine bzw. nur eine untergeordnete Rolle. Hierfür kommt es vielmehr darauf an, dass Zugangsdaten sicher aufbewahrt werden oder DNS-Server vor unautorisierten Zugriffen geschützt werden. Falsche Registrierungsdaten gefährden an sich hingegen nicht die Sicherheit des DNS.

Die vorgesehenen Registrierungspflichten gehen auch deutlich über die Vorgaben aus dem ICANN Registrar Accreditation Agreement (RAA) hinaus, das im Rahmen des globalen ICANN-Multistakeholder-Prozesses ausgehandelt wurde. Dieses sieht bereits Maßnahmen vor, um die Richtigkeit der Domainregistrierungsdaten zu gewährleisten, wie etwa eine jährliche Erinnerungspflicht an den Registranten seine Daten zu überprüfen bzw. eine Pflicht zur Korrektur von Daten, wenn Beweise für deren Ungenauigkeiten vorgelegt werden. Von einer absoluten Pflicht zur Gewährleistung der Richtigkeit der Daten hat man jedoch Abstand genommen, da eine solche in der Praxis de facto nicht zu erfüllen ist, mangels etwa einheitlicher Adressanforderungen oder Datenbanken, um die Adressen zu überprüfen. Darüber hinaus gibt es auch keine Möglichkeit sich zu vergewissern, dass nicht Informationen einer anderen Person angegeben werden. Da die Domainregistrierung de facto ein Massenmarkt ist, würde das Erfordernis, jede einzelne Registrierung individuell zu überprüfen zudem einen erheblichen zusätzlichen bürokratischen und finanziellen Aufwand für die betroffenen Registrare verursachen, der die allermeisten Unternehmen vor erhebliche Probleme stellen würde.

Nach Ansicht der ISPA ist die Verhältnismäßigkeit dieser Bestimmung daher klar in Frage zu stellen, insbesondere aber deren Rechtfertigung im Rahmen der NIS-2-RL, da die Bedeutung zur Gewährleistung der Cybersicherheit verschwindend gering erscheint und auch in der Richtlinie selbst nicht näher erläutert wird. Sowohl die Betreiber TLD name registries und DNS service provider unterliegen jedoch ohnehin den weiteren Sicherheitsanforderungen der Richtlinie – insbesondere Art 18 – und gewährleisten bereits aufgrund dessen die Sicherheit des DNS. Aus diesem Grund sollte Art 23 ersatzlos gestrichen werden.

- Aufweichung von Verschlüsselungsstandards (ErwGr 54)

Die Ausführungen in ErwGr 54 wonach die Verwendung von end-to-end Verschlüsselung mit nationalen Sicherheitsinteressen in Einklang gebracht werden muss und darüber hinaus, eine Lösung für den Zugang zu diesen Informationen durch Strafverfolgungsbehörden geschaffen werden soll, ist nach Ansicht der ISPA heftig zu hinterfragen.

Die österreichische ISP-Branche investiert jährliche hohe Summen in Cybersicherheitsmaßnahmen, um ihre Systeme und Netze vor nicht autorisierten Zugriffen bzw. Angriffen zu schützen und

beispielsweise den Missbrauch von Kundendaten zu verhindern. End-to-end Verschlüsselung ist dabei eine der effektivsten Maßnahmen, um die Sicherheit der Nutzerinnen und Nutzer zu gewährleisten. Diesen Schutz nun im Namen der Strafverfolgung aufzuweichen, indem etwa Unternehmen verpflichtet werden, Zugriffsmöglichkeiten in Form von backdoors in ihre Software einzubauen, kann daher nicht im Interesse der EU in ein hohes Cybersicherheitsniveau sein. Darüber hinaus sind durch eine solche Schwächung des Cybersicherheitsniveaus auch direkte wirtschaftliche Nachteile für den europäischen Binnenmarkt zu erwarten, da, wie auch die Kommission selbst in ErwGr 3 ausführt, Sicherheitsvorfälle die Ausübung wirtschaftlicher Aktivitäten im Binnenmarkt behindern, finanzielle Verluste verursachen, und auch das Vertrauen der Nutzerinnen und Nutzer untergraben, die entsprechenden Dienste zu nutzen.

Die Diskussion, dass end-to-end Verschlüsselung auch von Kriminellen ausgenutzt werden kann, besteht bereits seit langer Zeit. Dennoch haben Sicherheitsexperten seit jeher darauf verwiesen, dass der Schaden, der durch ein Aufweichen dieser Verschlüsselungsstandards entsteht, um ein Vielfaches größer wäre als der Nutzen, welcher der Strafverfolgung daraus erwächst. Denn sogenannte „NOBUS“ (Nobody but us) Exploits, also Sicherheitslücken welche ausschließlich von Strafverfolgungsbehörden genutzt werden können, sind auf Dauer in der Praxis unerreichbar, da niemals gesichert sein kann, dass diese nicht durch Dritte ebenfalls aufgedeckt werden, sei es durch Zufall, einen Leak oder den Zugriff auf staatliche Computersysteme. Der daraus potentiell resultierende Schaden wurde bereits in der Vergangenheit deutlich, als durch Geheimdienste bewusst offengelassene Sicherheitslücken von Kriminellen für das Aufspielen von Erpressungstrojanern (Ransomware) missbraucht wurden und erheblicher Schaden angerichtet wurde.

Die Gewährleistung eines hohen Sicherheitsniveaus ist mit der Forderung nach einer Abschwächung von Kryptografie bzw. dem Eingriff in Kommunikations- und Datenflüsse daher schlichtweg nicht vereinbar. Aus diesen Gründen sollten die entsprechenden Ausführungen, wonach die Verwendung von End-to-End-Verschlüsselung mit nationalen Sicherheitsinteressen in Einklang gebracht werden soll, in einer Richtlinie die eigentlich der Stärkung der Cyberresilienz dienen soll, ersatzlos gestrichen werden.

- <u>Verhältnis zur Richtlinie über die Resilienz kritischer Einrichtungen</u>

Gemeinsam mit dem Vorschlag der NIS-2-Richtlinie wurde vom europäischen Gesetzgeber auch der Entwurf einer Richtlinie über die Resilienz kritischer Einrichtungen präsentiert. Nach Ansicht der ISPA ist es essentiell sicherzustellen, dass die Anwendungsbereiche dieser beiden Richtlinien klar getrennt und überschneidende bzw. inkohärente Bestimmungen in den beiden Rechtsinstrumenten vermieden werden.

Während aus Erwägungsgrund 8 und 14 der Richtlinie über die Resilienz kritischer Einrichtungen bereits deutlich hervorgeht, dass der Sektor der digitalen Infrastruktur von beinahe sämtlichen Bestimmungen der Richtlinie ausgenommen ist, insbesondere den Risikomanagementmaßnahmen und Berichtspflichten, wird dies aus dem Richtlinientext selbst nicht ausreichend deutlich. Anstelle der vage formulierten Ausnahmebestimmung in Art 1 Abs. 2 der Richtlinie über die Resilienz

kritischer Einrichtungen sollte darin daher vielmehr der Wortlaut aus ErwGr 14 übernommen werden, wonach der Sektor digitale Infrastruktur zur Gänze von der Anwendung der Kapitel III – VI ausgenommen ist.