An das
Bundeskanzleramt
Büro für strategische Netz- und Informationssystemsicherheit
Ballhausplatz 2
1010 Wien

E-Mail: nis@bka.gv.at, begutachtungsverfahren@parlament.gv.at

Wien, am 29. Oktober 2018

BETREFF: ISPA STELLUNGNAHME ZUM ENTWURF EINES BUNDESGESETZES ZUR GEWÄHRLEISTUNG EINES HOHEN SICHERHEITSNIVEAUS VON NETZ- UND INFORMATIONSSYSTEMEN (NETZ- UND INFORMATIONSSYSTEMSICHERHEITSGESETZ – NISG)

Sehr geehrte Damen und Herren,

die ISPA erlaubt sich, im Zusammenhang mit der öffentlichen Konsultation des Bundeskanzleramtes betreffend den Entwurf des Bundesgesetzes zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen – NISG wie folgt Stellung zu nehmen:

Einleitend weist die ISPA auf den Umstand hin, dass sich viele Unklarheiten in Zusammenhang mit dem vorliegenden Entwurf des NISG daraus ergeben, dass die für die Praxis am relevantesten Informationen erst in separaten Verordnungen geregelt werden und somit derzeit nicht in die Einschätzung aufgenommen werden können. Es handelt sich hierbei unter anderem um die Fragen, welche Unternehmen als Betreiber wesentlicher Dienste identifiziert und wie die konkretisierten Vorschriften zu Sicherheitsvorkehrungen und zu Meldepflichten ausgestaltet werden. Hierdurch verbleibt Raum für Spekulationen und Mutmaßungen, was eine rechtssichere und transparente Nachvollziehbarkeit dieses Gesetzesvorhabens deutlich erschwert. Aufgrund ihrer beträchtlichen Praxisrelevanz sowie im Sinne eines demokratischen und transparenten Gesetzgebungsprozesses ist es aus Sicht der ISPA unabdingbar, dass auch die Verordnungen nach diesem Gesetzesentwurf, insbesondere diese gemäß § 4 Abs. 1 Z 4 und Z 7 sowie gemäß § 14 Abs. 4, § 15 Abs. 4 und § 16 Abs. 7 NISG einer öffentlichen Begutachtung unterzogen werden, bevor diese in Kraft treten.

Zusammengefasst betont die ISPA, dass das österreichische NISG dem risikobasierten Ansatz der NIS-RL hinsichtlich der Sicherheitsvorkehrungen von Betreiber wesentlicher Dienste entsprechen

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

soll. Die Ermächtigungen und Befugnisse der Behörden nach dem NISG müssen den verfassungs- und datenschutzrechtlichen Prinzipien u.a. der Zweckbindung sowie der Datensparsamkeit Rechnung tragen. Die ISPA merkt an, dass die DSGVO-konforme Datenverarbeitung nach dem NISG durch das Bundesministerium für Landesverteidigung zu hinterfragen ist. Ferner lehnt die ISPA den Einsatz von technischen Einrichtungen des BMI im Rahmen der Betreibernetze strikt ab, da hierdurch die Integrität der Systeme von IKT-Betreibern oder die Vertraulichkeit der dadurch transportierten Kundendaten kompromittiert werden könnten. Die ISPA fordert Kostenersatz für die Mitwirkung der Betreiber wesentlicher Dienste an die Frühwarnsysteme des BMI sowie beim Einsatz von „Honeypots“ und „Sinkholes“, da dieser eine Inpflichtnahme von privaten Betreibern bei der Mitwirkung an staatlichen Aufgaben darstellt und somit auch verfassungsrechtlich geboten ist. Aus Sicht der ISPA ist für die Übermittlung von allfälligen personenbezogenen Daten im Rahmen freiwilliger Meldungen von Sicherheitsvorfällen eine hinreichende Rechtsgrundlage erforderlich. Im Sinne einer korrekten Umsetzung der NIS-RL fordert die ISPA eine ausdrückliche Ausnahme für Telekombetreiber vom Anwendungsbereich des NISG, wie dies bereits in die NIS-RL vorgesehen ist. Ferner merkt die ISPA an, dass redundante Meldungen und Meldestrukturen nach dem TKG 2003 und NISG hintanzuhalten sind und betont, dass die Ausnahme für kleine und mittelgroße Anbieter digitaler Dienste präzisiert werden soll.

1. Das österreichische NISG muss dem risikobasierten Ansatz der NIS-RL entsprechen

Der Gesetzesentwurf lässt den Verhältnismäßigkeitsansatz der NIS-RL[1] hinsichtlich der geforderten technischen und organisatorischen Maßnahmen missen, welche von Betreibern wesentlicher Dienste ergriffen werden müssen, um die Risiken für ihre Netz- und Informationssystemen zu bewältigen. Laut der NIS-RL müssen derartige Maßnahmen einerseits dem Stand der Technik entsprechen anderseits aber auch verhältnismäßig und dem bestehenden Risiko angemessen sein.[2] Diesem risikobasieren Ansatz wurde jedoch in der österreichischen Umsetzung der NIS-Richtlinie nur zum Teil, nur hinsichtlich Anbieter digitaler Dienste in § 18 NISG, Rechnung getragen. In § 15 Abs. 1 NISG wird gefordert, dass die Sicherheitsvorkehrungen dem Stand der Technik entsprechen müssen, unabhängig davon, ob dieser u.U. für die gegebenen Sicherheitsrisiken überschießend oder dem bestehenden Risiko unangemessen und somit unverhältnismäßig wäre.

Daher spricht sich die ISPA dafür aus, dass der Gesetzesentwurf dem von der NIS-RL vorgegebenen Verhältnismäßigkeitsansatz auch für Betreiber wesentlicher Dienste Rechnung trägt und mit der Klarstellung ergänzt wird, dass die Sicherheitsvorkehrungen der Betreiber wesentlicher Dienste, unter Berücksichtigung des Stands der Technik, verhältnismäßig und dem bestehenden Risiko angemessen sein müssen.

[1] Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, ABl. L 194/l.
[2] Art. 14 Abs. 1 NIS-RL.

ISPA Vorschlag Gesetzestext:

Sicherheitsvorkehrungen für Betreiber wesentlicher Dienste

§ 15. (1) Die Betreiber wesentlicher Dienste haben in Hinblick auf die von ihnen betriebenen wesentlichen Dienste (§ 14 Abs. 2) geeignete und verhältnismäßige~~, dem Stand der Technik entsprechende~~ Sicherheitsvorkehrungen zur Gewährleistung der Netz- und Informationssysteme (§ 3 Z 2) zu treffen. Diese Sicherheitsvorkehrungen müssen unter Berücksichtigung des Stands der Technik ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, das dem bestehenden Risiko angemessen ist.

Erläuterungen zu § 15, Seite 17:

„In Umsetzung des Art. 14 Abs. 1 NIS-RL wird den Betreibern wesentlicher Dienste vorgeschrieben, geeignete und verhältnismäßige, dem Stand der Technik entsprechende Sicherheitsvorkehrungen zu treffen. Sicherheitsvorkehrungen sind nicht angemessen, wenn der erforderliche Aufwand unverhältnismäßig zu den Folgen eines Ausfalls oder einer wesentlichen Beeinträchtigung der betroffenen kritischen Infrastruktur steht. Sie können sowohl technischer als auch […]*“*

2. Die Ermächtigungen der Behörden müssen den verfassungs- und datenschutzrechtlichen Prinzipien Rechnung tragen

Laut § 10 Abs. 3 NISG sind die NIS Büros im Bundeskanzleramt (BKA) sowie im Bundesministerium für Inneres (BMI) berechtigt, von Betreibern wesentlicher Dienste und Anbietern digitaler Dienste jene Auskunft zu verlangen, welche sie als wesentliche Voraussetzung zur Erfüllung ihrer Aufgaben benötigen. Dabei sind die ersuchten Stellen zur unverzüglichen Auskunftserteilung verpflichtet.

Aus Sicht der ISPA ist diese Bestimmung überschießend und sollte daher konkretisiert werden. Den Hinweis in den Erläuterungen, dass es sich dabei etwa „[…] *um Informationen, die für die umfassende Beurteilung eines Sicherheitsvorfalls notwendig sind*“[3] handelt, ist einleuchtend aber unzureichend, um sicherzustellen, dass eine ausufernde Datenabfrage hintangehalten wird.

Diese Rechtsvorschrift sollte dahingehend, idealer Weise in Form von fix definierten Use Cases, insofern konkretisiert werden, dass die Auskunftspflicht nur auf jene taxativ aufgeführten Daten zu beschränken ist, welche unmittelbar und unbedingt in Zusammenhang mit einem konkreten, bereits gemeldeten Sicherheitsvorfall stehen und unbedingt zur Aufklärung dieses Sicherheitsvorfalles erforderlich sind. Hierbei ist sowohl dem Einsatz des gelindesten Mittels als

[3] Erläuterungen zum § 10 Entwurf NISG, S. 12 2. Absatz.

Teil des Verhältnismäßigkeitsgrundsatzes als auch den datenschutzrechtlichen Prinzipien der Zweckbindung und der Datenminimierung Rechnung zu tragen.

Gleichermaßen besorgniserregend ist auch die weitreichende und ausgesprochen unpräzise formulierte Ermächtigung des Bundesministeriums für Inneres in § 10 Abs. 2 NISG jene personenbezogenen Daten zu verarbeiten, die zur Wahrnehmung sämtlicher Aufgaben gemäß § 5 und § 9 NISG erforderlich sind. Dabei handelt es sich um Daten u.a. zur Vorbeugung von Sicherheitsvorfällen, zur Überprüfung von Sicherheitsvorkehrungen sowie zum Betreiben von technischen Einrichtungen wie „Honeypots“ und „Sinkholes“, um die Muster von Angriffen auf Netz- und Informationssysteme zu erkennen.

Die Erläuterungen enthalten diesbezüglich eine Vielzahl an Datenkategorien wie u.a. IP-Adressen der zugreifenden Systeme bzw. Personen, verwendete Ports und IP-Adressen von Angriffszielen, Host-Namen, URL, Ports, Domainnamen, Whois-Informationen, Zugangsdaten, Log-Files sowie Metadaten, aber auch Informationen, die das Verhalten bzw. das Muster eines Angriffs abbilden. Auch in Zusammenhang mit dieser Bestimmung betont die ISPA daher, dass die datenschutzrechtlichen Prinzipien und der Grundsatz der Verhältnismäßigkeit berücksichtigt werden müssen, um Missbrauchsgefahren wie beispielsweise überschießende Datenabfrage bzw. -verarbeitung hintanzuhalten, und gleichzeitig eine zielgerichtete, verhältnismäßige und präzise Datenabfrage und sparsame Datenverarbeitung durch die NIS-Behörden zu gewährleisten.

Grundsätzlich ist aus Sicht der ISPA erforderlich, dass die Verarbeitungsprinzipien des Art 5 DSGVO ihren Niederschlag in § 10 Abs. 2 und 3 finden und regt an, eine diesbezügliche Klarstellung in den Erläuterungen aufzunehmen, um dadurch klare gesetzliche Schranken für Auskunftsanfragen sowie für Datenverarbeitungsermächtigungen der NIS-Behörden aufzustellen und somit überschießende Amtshandlungen hintanzuhalten.

§ 10 Abs. 3 ISPA Vorschlag Gesetzestext:

Datenverarbeitung

> ***§ 10.*** *(3) Jedes NIS-Büro darf von dem anderen NIS-Büro, den Computer-Notfallteams und den Betreibern wesentlicher Dienste und Anbietern digitaler Dienste jene Auskünfte verlangen, die sie als wesentliche und unabdingbare Voraussetzung zur Erfüllung ihrer Aufgaben benötigt. Die ersuchten Stellen sind verpflichtet, unverzüglich Auskunft zu erteilen.*

ISPA Vorschlag für die Erläuterungen:

Zu § 10 Abs. 3, Seite 12:

> „[…] *Dabei handelt es sich etwa um Informationen, die für die ~~umfassende~~ Beurteilung eines Sicherheitsvorfalls notwendig sind. Daher ist diese Auskunftspflicht nur auf jene Daten zu beschränken, welche unmittelbar und unbedingt in Zusammenhang mit einem konkreten, bereits gemeldeten Sicherheitsvorfall stehen und unbedingt zur Aufklärung dieses Sicherheitsvorfalles erforderlich sind. Hierbei ist sowohl dem Einsatz des gelindesten Mittels als Teil des Verhältnismäßigkeitsgrundsatzes als auch den datenschutzrechtlichen Prinzipien der Zweckbindung*

und der Datenminimierung sowie den in Art. 5 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 verankerten Grundsätzen Rechnung zu tragen […].

Zu § 10 Abs. 2, Seite 12

„[…] *Zu den Daten bzw. zweckentsprechenden Informationen, die gemäß § 9 Abs. 1 und 2 gewonnen werden, zählen insbesondere technische personenbezogene Daten […], aber auch Informationen, die das Verhalten bzw. das Muster eines Angriffs abbilden (z.B. welche Dateien liegen im Fokus des Angreifers). Sämtliche Datenverarbeitungsermächtigungen gemäß § 10 Abs. 2 müssen den datenschutzrechtlichen Prinzipien der Zweckbindung und der Datenminimierung sowie den in Art. 5 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 verankerten Grundsätzen Rechnung tragen.* […]“

3. Die DSGVO-konforme Datenverarbeitung nach dem NISG durch das Bundesministerium für Landesverteidigung ist zu hinterfragen

Das Bundesministerium für Landesverteidigung (BMLV) ist in § 11 NISG als gemeinsam Verantwortliche im Sinne von Art. 26 DSGVO zusammen mit BKA und BMI vorgesehen. Dadurch soll diese zur Verarbeitung von personenbezogenen Daten nach dem NISG ermächtigt werden.

Das BMLV ist allerdings in der einschlägigen Bestimmung - nämlich § 10 NISG, welche eine explizite gesetzliche Ermächtigung für die Datenverarbeitung iSv Art. 6 DSGVO nach dem NISG darstellt, nicht neben BKA und BMI angeführt.

Aus Sicht der ISPA ist zu hinterfragen, ob die Einstufung des BMLV als gemeinsam Verantwortliche in § 11 NISG als eine ausreichende Rechtsgrundlage bewertet werden kann, um eine DSGVO-konforme Datenverarbeitung im Sinne von Art. 6 DSGVO durch das BMLV zu gewährleisten. Sollte vom Gesetzgeber erwünscht sein, dass dem BMLV die datenschutzkonforme Datenverarbeitung nach dem NISG ermöglicht wird, ist aus Sicht der ISPA neben dem BKA und dem BMI auch die Aufnahme des BMLV in § 10 NISG erforderlich, welche eine explizite gesetzliche Ermächtigung für die Datenverarbeitung iSv Art. 6 DSGVO nach dem NISG darstellt. Daher weist die ISPA darauf hin, dass die Bestimmung in diesem Sinne neu überdacht werden sollte.

Darüber hinaus sind die Betroffenenrechte, wie in § 11 Abs. 2 NISG aufgelistet, gemäß DSGVO (Art 15 bis Art. 22) nur natürlichen Personen vorbehalten. Da sich das NISG allerdings hauptsächlich auf juristische Personen bezieht, könnte der Eindruck entstehen, dass hier die Ausdehnung des Anwendungsbereichs der DSGVO angestrebt worden wäre.

Daher ist aus Sicht der ISPA erforderlich, dass in den Erläuterungen klargestellt wird, dass § 11 Abs. 2 NISG sich ausschließlich an betroffene Personen, welche natürliche Personen sind, richtet.

4. Der Einsatz von technischen Einrichtungen des BMI innerhalb der Betreibernetze ist strikt abzulehnen

In § 9 Abs. 1 und Abs. 2 NISG ist vorgesehen, dass das BMI zur Erfüllung ihrer Aufgabe gemäß § 5 Z 4 NISG, nämlich präventive Kompetenzen zur Vorbeugung von Sicherheitsvorfällen durch Erstellung und Weitergabe von Informationen zur Gewährleistung der Sicherheit von Netz- und Informationssystemen, ermächtigt ist, technische Einrichtungen zu betreiben, um einerseits Störungen oder Unregelmäßigkeiten von Netz- und Informationssystemen frühzeitig zu erkennen und anderseits die Muster von Angriffen auf Netz- und Informationssystemen zu eruieren. Diese Befugnis umfasst sowohl den Einsatz eines Frühwarnsystems (§ 9 Abs. 1) als auch den Betrieb von „Honeypots" und „Sinkholes" (§ 9 Abs. 2).

§ 9 Abs. 1 NISG ist als eine „kann" Vorschrift formuliert, daher sollen Betreiber wesentlicher Dienste und Anbieter digitaler Dienste scheinbar nicht zur Teilnahme an den vom BMI betriebenen technischen Einrichtungen verpflichtet werden. Das in den Erläuterungen bereits ausführlich vorgegebene Kooperationsregime lässt jedoch Zweifel hinsichtlich der beabsichtigten Freiwilligkeit dieser Bestimmung aufkommen.

Obwohl das dahinterliegende Ansinnen des Gesetzgebers nachvollziehbar ist, lehnt die ISPA den Einsatz jeglicher technischer Einrichtungen des BMI in den Netzen von Betreibern wesentlicher Dienste, welche die Integrität der Systeme von IKT-Betreibern oder die Vertraulichkeit der dadurch transportierten Kundendaten kompromittieren könnten, strikt ab und fordert eine diesbezügliche Klarstellung im Gesetzesentwurf.

Ferner merkt die ISPA an, dass die technischen Ausführungen hinsichtlich des Einsatzes von „[…] *entsprechend konfigurierte[n] und vor den Netzwerken der Teilnehmer platzierte[n] technische[n] Einrichtungen* […]"[4] durch das BMI in den Erläuterungen bedauerlicherweise unschlüssig sind und kein klares Bild ergeben, wie bzw. wo diese Einrichtungen eingebracht werden, und welche allfälligen Auswirkungen diese auf die Teilnehmernetzwerke bzw. auf die dadurch passierenden Daten haben könnten.

ISPA Vorschlag für den Gesetzestext:

Befugnisse zur Vorbeugung von Sicherheitsvorfällen

> ***§ 9.*** *(1) Der Bundesminister für Inneres ist zur Erfüllung der Aufgabe gemäß § 5 Z 4 ermächtigt, technische Einrichtungen zu betreiben, die Unregelmäßigkeiten oder Störungen von Netz- und Informationssystemen frühzeitig erkennen. Betreiber wesentlicher Dienste, Anbieter digitaler Dienste und Einrichtungen des Bundes können an den vom Bundesminister für Inneres betriebenen technischen Einrichtungen freiwillig teilnehmen und festlegen, welche Daten an den Bundesminister für Inneres übermittelt werden. Für die Teilnahme an den technischen Einrichtungen gebührt dem Bund als Ersatz ein Pauschalbetrag, der nach Maßgabe der durchschnittlichen Kosten mit Verordnung des Bundesministers für Inneres festgelegt wird.*

[4] Erläuterungen zum § 9 Abs. 1 Entwurf NISG, Seite 10 erster Absatz.

(2) Der Bundesminister für Inneres ist zur Erfüllung der Aufgabe gemäß § 5 Z 4 ermächtigt, technische Einrichtungen zu betreiben oder zu nutzen, um die Muster von Angriffen auf Netz- und Informationssysteme zu erkennen. Diese Einrichtungen werden außerhalb des Netzwerkes des betroffenen Unternehmens angebracht und lassen weder eine Analyse von Daten innerhalb des Netzwerkes des betroffenen Unternehmens, noch die Überwachung des Netzwerks zu.

5. Der Kostenersatz für die Inpflichtnahme von privaten Betreibern bei der Mitwirkung an staatlichen Aufgaben ist verfassungsrechtlich geboten

Darüber hinaus stellt aus Sicht der ISPA jegliche Mitwirkung der Betreiber, freiwillig oder nicht, an einem Frühwarnsystem des BMI oder beim Einsatz von „Honeypots" und „Sinkholes" eine Inpflichtnahme privater Betreiber für die Mitwirkung an einer staatlichen Aufgabe dar. Aus dem Verhältnismäßigkeitsgrundsatz ist es ableitbar, und daher auch verfassungsrechtlich geboten, dass die Kostentragung für diese Mitwirkung von privaten Betreibern dem Staat obliegt. Diese Auffassung vertritt auch der Verfassungsgerichtshof im Rahmen seiner Judikatur über die Verpflichtung zur Bereitstellung von Einrichtungen zur Überwachung des Fernmeldeverkehrs durch Telekombetreiber.[5]

Aus diesem Grund betont die ISPA, dass sofern ein Betreiber wesentlicher Dienste gemäß § 9 Abs. 1 NISG am Frühwarnsystem des BMI teilnehmen sollte, diesem im Sinne der VfGH Rechtsprechung ein Kostenersatz gebühren muss. Der Gesetzesentwurf spricht derzeit Kostenersatz nur dem Bund zu. Umso mehr gilt diese Forderung für die Mitwirkung der Betreiber beim Einsatz von „Honeypots" und „Sinkholes" durch das BMI gemäß § 9 Abs. 2 NISG, da diese Bestimmung u.U. zu einer verpflichtenden Teilnahme seitens der Betreiber wesentlicher Dienste oder Anbieter digitaler Dienste führen könnte.

Darüber hinaus fordert die ISPA die unentgeltliche Zurverfügungstellung der Daten, welche im Rahmen des Betriebs dieser technischen Einrichtungen durch das BMI gewonnen werden, um eine umfassendere Abwehr von DDoS Attacken und sonstigen Angriffen durch die IKT-Branche sicherstellen zu können.

ISPA Vorschlag für die Erläuterungen zu § 9 Abs. 2, Seite 10:

„[…] *Sowohl bei „Honeypots" als auch bei „Sinkholes" ist die Aufzeichnung und Verarbeitung zweckentsprechender Informationen erforderlich, um Angriffsquellen und Angriffsziele zu erkennen und analysieren zu können (§ 10 Abs. 2 letzter Satz). Für allfällige Kosten, welche durch den Einsatz von „Honeypots" und „Sinkholes" den Unternehmen entstehen könnten, gebührt ihnen ein Kostenersatz sowohl für jegliche Investitions- als auch Wartungs- bzw. Instandhaltungskosten im Sinne der VfGH Rechtsprechung vom 27.02.2003 zu GZ 37/02 ua. Die im Rahmen des Betriebs der*

[5] VfGH vom 27.02.2003 zu GZ 37/02 ua.

technischen Einrichtungen durch das BMI gewonnenen Daten, sind den Unternehmen unentgeltlich zur Verfügung zu stellen.“

6. Für die freiwillige Meldung von Sicherheitsvorfällen ist eine hinreichende Rechtsgrundlage erforderlich

Der Gesetzentwurf hält in § 20 NISG fest, dass Einrichtungen, welche nicht ausdrücklich im Anwendungsbereich des NISG fallen, dennoch das Auftreten von Sicherheitsvorfällen auf freiwilliger Basis melden können. Die ISPA unterstützt die Intention dieser Bestimmung.

Aus Sicht der ISPA schafft diese Bestimmung jedoch leider keine ausreichende und verlässliche gesetzliche Rechtsgrundlage, um den betroffenen Betreibern die freiwillige Übermittlung der unter Umständen erforderlichen personenbezogenen Daten zur Aufklärung eines Sicherheitsvorfalles zu ermöglichen, da es aus der gegenständlichen Fassung des § 20 NISG nicht deutlich hervorgeht, auf welche der in Art. 6 DSGVO verankerten Zulässigkeitstatbestände die Übermittlung von personenbezogener Daten an die NIS -Behörden, anlässlich der freiwilligen Meldung eines Sicherheitsvorfalles gestützt werden könnte. Dieser Umstand schafft Rechtsunsicherheit und würde dem § 20 NISG jegliche Praxisrelevanz absprechen, da aufgrund der unsicheren Rechtslage und der Aussicht auf exorbitant hohen Geldstrafen nach der DSGVO zu befürchten stünde, dass freiwillige Meldungen in der Praxis kaum durchgeführt würden. Daher fordert die ISPA, dass die Ausgestaltung der Bestimmung über die freiwilligen Meldungen von Sicherheitsvorfällen diesbezüglich adaptiert wird und in den Erläuterungen klar eingeführt wird, dass die freiwillige Meldung eines Sicherheitsvorfalles im öffentlichen Interesse iSv Art. 6 Abs. 1 lit e) DSGVO erfolgt.

ISPA Vorschlag für den Gesetzestext:

Freiwillige Meldungen

§ 20. *Störungen, die kein Sicherheitsvorfall (§ 3 Z 6) sind oder die Betreiber von nicht wesentlichen Diensten betreffen, können an das Computer-Notfallteam gemeldet werden, das die Meldungen zusammengefasst an den Bundesminister für Inneres weiterleitet; die Nennung der meldenden Einrichtung kann dabei auf ihr Verlangen entfallen. Die freiwillige Meldung kann Angaben zur Störung sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache, der betroffenen Informationstechnik, der Art der betroffenen Einrichtung oder Anlage sowie zum Sektor des Betreibers enthalten. Sollten von der freiwilligen Meldung nach dieser Bestimmung personenbezogene Daten im Sinne von § 10 NISG betroffen sein, dann sind die Grundsätze der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zu beachten.*

Vorschlag in den Erläuterungen zu § 20, Seite 20:

„[…] Art. 20 NIS-RL sieht diesen Fall der freiwilligen Meldungen explizit vor. Die freiwilligen Meldungen erfolgen im öffentlichen Interesse im Sinne von Art. 6 Abs. 1 lit e) der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016.

7. Eine ausdrückliche Ausnahme für Telekombetreiber vom Anwendungsbereich des NISG ist im Sinne einer korrekten Umsetzung der NIS-RL unabdingbar

Die NIS-RL sieht in Art. 1 Abs. 3, ebenso wie Recital 7, eine ausdrückliche Ausnahme von ihrem Anwendungsbereich für Unternehmen, welche bereits den Anforderungen der Art. 13 und Art. 13a der Rahmenrichtlinie[6] unterliegen. Eine diesbezügliche ausdrückliche Klarstellung dieses Umstandes wurde jedoch in den Entwurf des NISG nicht aufgenommen. Während eine derartige Klarstellung für den Bereich der Telekom-Wirtschaft bedauerlicherweise unterblieben ist, wurde in § 17 NISG sehr wohl eine (vergleichbare) sektorspezifische Ausnahme aufgenommen, welche sich auf Art. 1 Abs. 7 NIS-RL bezieht und Zahlungsdienstleister klar ausnimmt.

Aus diesem Grund fordert die ISPA erneut die Aufnahme eines eindeutigen Hinweises in den Erläuterungen, dass Anbieter, welche den Sicherheitsanforderungen und den Meldepflichten gemäß Art. 13a und 13b Rahmenrichtlinie unterliegen, vom Anwendungsbereich des NISG ausgenommen werden sollen, wie dies bereits in Art. 1 Abs. 3 sowie ErwG 7 NIS-Richtlinie vorgesehen ist.

ISPA Vorschlag für die Erläuterungen zu § 17, Seite 19:

„[…] Unternehmen, die öffentliche Kommunikationsnetze oder öffentlich zugängliche elektronische Kommunikationsdienste im Sinne des § 3 Z 3 und Z 4 TKG 2003 bereitstellen und die den besonderen Sicherheits- und Integritätsanforderungen des § 16a TKG 2003 unterliegen, sind nicht vom gegenständlichen Gesetz erfasst.

8. Redundante Meldungen und Meldestrukturen nach dem TKG 2003 und NISG sind hintanzuhalten

§ 16a Abs. 5 TKG 2003 verpflichtet IKT-Betreiber Sicherheitsverletzungen oder den Verlust der Integrität ihrer Netze der Regulierungsbehörde zu melden. Zusätzlichen Meldepflichten für IKT-Betreiber aufgrund des NISG würden daher eine redundante und obsolete Meldeverpflichtung darstellen, welche nur zusätzlichen Aufwand und Kosten für die Betreiber mit sich bringen würde.

[6] Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste (Rahmenrichtlinie).

Die ISPA weist darauf hin, dass sofern eine Sicherheitsverletzung oder der Verlust der Netzintegrität durch einen Betreiber an die Regulierungsbehörde gemäß § 16a Abs. 5 TKG 2003 gemeldet wird und vom Gesetzgeber erwünscht ist, dass diese Meldung ihren Niederschlag in einem gesamtösterreichischen Lagebild findet, es der Aufnahme einer entsprechenden Rechtsgrundlage für die Datenweitergabe der RTR-GmbH an das BMI bedarf.

Eine derartige Ermächtigung war im Ministerialentwurf der TKG Novelle 2018[7] enthalten, wurde jedoch von der Regierungsvorlage[8] gestrichen. Generell wäre im Sinne der Kosteneffizienz und einer sparsamen Verwaltung sinnvoll, wenn die Meldungen eines Telekombetreibers, sofern dieser als Betreiber eines DNS-Resolvers dem NISG unterliegen sollte, für den Ausfall dieser DNS-Service auch an die RTR-GmbH ergehen sollen und von dieser abgewickelt werden.

Die ISPA wiederholt, dass redundante Meldungen sowohl an die RTR-GmbH als auch an die nach dem NISG zuständigen Behörden durch die IKT-Betreiber strikt abgelehnt werden. Daher spricht sich die ISPA für die Aufnahme einer diesbezüglichen gesetzlichen Ermächtigung für die RTR-GmbH vorzugsweise in das TKG 2003 aus. Sofern eine derartige gesetzliche Ermächtigung im Rahmen der TKG-Novelle 2018 nicht umgesetzt wird, fordert die ISPA, dass diese im Entwurf des NISG verankert wird.

ISPA Vorschlag für das TKG 2003 § 16a:

> *Nach § 16a Abs. 5 wird folgender Abs. 5a eingefügt:*
>
> *„(5a) Die Regulierungsbehörde hat eine erfolgte Mitteilung nach Abs. 5 unverzüglich an den Bundesminister für Inneres weiterzuleiten. Dieser hat die darin enthaltenen Informationen in das gemäß § 5 Z 3 Netz- und Informationssystemsicherheitsgesetz (NISG), BGBl. I Nr. X/2018, zu erstellende Lagebild aufzunehmen, das im Rahmen der Operativen Koordinierungsstruktur (OpKoord, § 3 Z 5 NISG) zu erörtern ist.“*

Oder nach § 11 Abs. 4 NISG wird folgender Abs. 4a eingefügt:

> *Die Rundfunk und Telekom Regulierungs-GmbH hat eine erfolgte Mitteilung nach § 16a Abs. 5 TKG 2003 unverzüglich an den Bundesminister für Inneres weiterzuleiten. Dieser hat die darin enthaltenen Informationen in das gemäß § 5 Z 3 Netz- und Informationssystemsicherheitsgesetz (NISG), BGBl. I Nr. X/2018, zu erstellende Lagebild aufzunehmen, das im Rahmen der Operativen Koordinierungsstruktur (OpKoord, § 3 Z 5 NISG) zu erörtern ist.*

[7] Ministerialentwurf TKG-Novelle 2018, Pkt. 32, § 16a Abs. 5, S. 6, https://www.parlament.gv.at/PAKT/VHG/XXVI/ME/ME_00063/imfname_701825.pdf (16.10.2018)
[8] Regierungsvorlage TKG-Novelle 2018, https://www.parlament.gv.at/PAKT/VHG/XXVI/I/I_00257/fname_708777.pdf (16.10.2018).

9. Die Ausnahme für kleine und mittelgroße Anbieter digitaler Dienste soll präzisiert werden

Der Entwurf sieht in § 3 Z 10 NISG eine Ausnahme vom Anwendungsbereich des NISG für kleine und mittelgroße Anbieter digitaler Dienste im Sinne von Art 1 Abs. 2 und Abs. 3 der Empfehlung der EU-Kommission 2003/361/EG[9] vor. Aus der Definition digitaler Dienste in § 3 Z 9 NISG sowie aus der Definition des Cloud-Computing-Diensts in § 3 Z 14 NISG ist jedoch schwer zu entnehmen, wie diese Ausnahme zu verstehen ist, wenn beispielsweise ein Cloud-Dienst im Rahmen eines IKT-Unternehmens betrieben wird, welches u.U. als Betreiber wesentlicher Dienste identifiziert wird. Sofern die Ausnahme für die kleinen und mittelgroßen Anbieter digitaler Dienste an die Rechtspersönlichkeit geknüpft werden sollte, ist in den Erläuterungen anhand Beispielen klarzustellen, dass z.B. sofern keine selbstständige Rechtspersönlichkeit wie z.B. ein Tochterunternehmen für den Clouddienst gegründet wird, die Richtsätze der Empfehlung der EU-Kommission 2003/361/EG bezüglich Mitarbeiteranzahl und Umsätzen auf die Muttergesellschaft anzuwenden sind. Eine diesbezügliche Präzisierung ist aus Sicht der ISPA erforderlich, um eine rechtsichere und anwenderfreundliche Ausgestaltung des Gesetzesentwurfs zu gewährleisten.

Ferner ist es in den Erläuterungen eindeutig klarzustellen, unter welchen Umständen der Abschluss eines Kaufvertrages im Internet dazu führen würde, dass eine Plattform als Online-Marktplatz eingestuft wird. Darüber hinaus ist hervorzuheben, dass der direkte Erwerb von Endgeräten von Betreibern zu keiner Einstufung der Online-Präsenz derselben als Online-Marktplatz im Sinne des NISG führt.

Die ISPA ersucht um die Berücksichtigung ihrer Bedenken und Anregungen bei der Gestaltung des Gesetzesentwurfs.

Mit freundlichen Grüßen,
ISPA - Internet Service Providers Austria

Dr. Maximilian Schubert
Generalsekretär

Die ISPA – Internet Service Providers Austria – ist der Dachverband der österreichischen Internet Service-Anbieter und wurde im Jahr 1997 als eingetragener Verein gegründet. Ziel des Verbandes ist die Förderung des Internets in Österreich und die Unterstützung der Anliegen und Interessen von über 200 Mitgliedern gegenüber Regierung, Behörden und anderen Institutionen, Verbänden und Gremien. Die ISPA vertritt Mitglieder aus Bereichen wie Access, Content und Services und fördert die Kommunikation der Marktteilnehmerinnen und Marktteilnehmer untereinander.

[9] Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen, ABl L 124/36.