WIRTSCHAFTSKAMMER ÖSTERREICH

Herrn
Mag. Michael Böhm
Bundeskanzleramt
Ballhausplatz 2
1010 Wien

per E-Mail: recht@bka.gv.at
begutachtungsverfahren@parlament.gv.at

Wiedner Hauptstraße 63 | Postfach 195
1040 Wien
T +43 (0) 5 90 900DW | F +43 (0) 5 90 900243
E rp@wko.at
W http://wko.at/rp

Ihr Zeichen, Ihre Nachricht vom	Unser Zeichen/Sachbearbeiter	Durchwahl	Datum
BKA-180.310/0234-I/6/2018	Rp 487.0002/2018/WP/VR Dr. Winfried Pöcherstorfer	4002	22.10.2018

Entwurf – Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG) – Stellungnahme

Sehr geehrter Herr Mag. Böhm,

die Wirtschaftskammer Österreich bedankt sich für die Übermittlung des Entwurfes für ein Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG) und nimmt hiezu wie folgt Stellung:

A. Allgemeines

Der vorliegende Entwurf für ein NISG, der in Umsetzung der 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 (kurz: NIS-RL) ergeht, enthält eine Reihe von für zahlreiche Unternehmen neuartigen Verpflichtungen. Die Bereitschaft des federführenden Bundeskanzleramtes, die betroffenen Kreise mit den aus der neuartigen Sachmaterie resultierenden Verpflichtungen bereits in einem frühen Stadium vertraut zu machen und dabei die Bedürfnisse der Wirtschaft nach Möglichkeit zu berücksichtigen sind dabei ausdrücklich positiv hervorzuheben, ebenso wie auch der Umstand, dass nunmehr – anders als nach ursprünglichen Überlegungen - Gold Plating hinsichtlich des Adressatenkreises vermieden wird und sich das NISG nur an jene Wirtschaftsbranchen richtet, die auch in der NIS-RL als Adressaten genannt sind.

Die NIS-RL und das NISG sind wichtige Schritte, die zu einem allgemein hohen Sicherheitsniveau in den Bereichen Netz- und Informationssystemsicherheit in Österreich und Europa beitragen können. Wichtig ist dabei die sorgfältige Einbeziehung der betroffenen Unternehmen in den unterschiedlichen Sektoren. Denn einerseits betreiben die betroffenen Unternehmen (im Sinn des Gesetzes die „*Betreiber wesentlicher Dienste*“) in vielen Fällen bereits sehr ausgereifte Sicherheitssysteme. Vor diesem Hintergrund sollten Belastungen für Unternehmen also möglichst geringgehalten werden. Andererseits sind die Gegebenheiten und Anforderungen je nach Sektor

und Tätigkeit des Betreibers wesentlicher Dienste sehr spezifisch, weshalb maßgeschneiderte Lösungen notwendig sind. Das gilt für den Entwurf zum NISG ebenso wie für die noch zu erlassenden Verordnung und Bescheide.

Die betroffenen Betreiber wesentlicher Dienste sollen mittels Verordnung, deren zügige Erlassung im Interesse unserer Mitgliedsunternehmen steht, näher spezifiziert werden. Dazu sollen die Schwellenwerte, wie sie in den Branchengesprächen erarbeitet wurden, Anwendung finden. Wir gehen davon aus, dass die dort kommunizierten Schwellenwerte auch tatsächlich in die noch zu erlassende Verordnung Eingang finden werden und beschränken unsere Einschätzung daher allein auf den vorliegenden Gesetzesentwurf.

Anders als bei den Betreibern wesentlicher Dienste, die vom Bundeskanzleramt identifiziert und mit Bescheid festgestellt werden, müssen bestimmte Anbieter digitaler Dienste von sich aus feststellen, ob sie ein Anbieter digitaler Dienste im Sinne des NISG sind. Zu diesem Zwecke sind noch weitere Konkretisierungen in den Erläuterungen erforderlich. Zusätzlich zu den gesetzlichen Vorgaben verfügbar gemachtes Informationsmaterial wäre hier außerdem noch sehr hilfreich.

Darüber hinaus sollten die bestehenden Handlungsspielräume im Hinblick auf die bereits umfangreichen Pflichten, die durch die Umsetzung der DSGVO entstanden sind, derart gestaltet werden, dass Synergieeffekte im Rahmen der DSGVO-Umsetzung bestmöglich genutzt werden können.

Die nachfolgenden Überlegungen nehmen zunächst in allgemeiner Weise Bezug auf die einzelnen Bestimmungen des NISG. Im Anschluss daran werden branchenspezifische Überlegungen dargestellt.

B. Zu den einzelnen Bestimmungen des NISG

Zu § 3 – Begriffsdefinitionen:

Hinsichtlich der Begriffsdefinitionen und insbesondere zu § 3 Z 6 sollte so bald wie möglich eine klarstellende, die Bedürfnisse der Wirtschaft berücksichtigende Konkretisierung der dort angeführten Begrifflichkeiten im Verordnungswege erfolgen.

Zu § 9 - Befugnisse zur Vorbeugung von Sicherheitsvorfällen:

Zunächst ist anzumerken, dass der Einsatz technischer Einrichtungen nach § 9 Abs 1 und Abs 2 keinesfalls zu Störungen im Netzbetrieb führen darf, und zwar weder hinsichtlich Netzintegrität und Datensicherheit noch im Hinblick auf die Performance, Verfügbarkeit oder Ausfallsicherheit und weiterer Parameter.

In § 9 wird die Möglichkeit für Betreiber wesentlicher Dienste (ua) angeführt, an vom BMI betriebenen technischen Einrichtungen teilzunehmen und festzulegen, welche Daten an den Bundesminister für Inneres übermittelt werden. Für die Teilnahme fallen entsprechende Kosten an, die dem BMI von den teilnehmenden Betreibern wesentlicher Dienste (ua) ersetzt werden sollen. Um Klarheit über den Charakter dieser Option zu schaffen, schlagen wir vor, folgenden Satz am Ende von § 9 Abs 1 zu ergänzen:

„Die Teilnahme an den vom Bundesminister für Inneres betriebenen technischen Einrichtungen erfolgt für die Betreiber wesentlicher Dienste, Anbieter digitaler Dienste und Einrichtungen des Bundes auf freiwilliger Basis und kann für diese nicht verpflichtend vorgeschrieben werden.“

Weiters schlagen wir folgende Konkretisierungen in den Erläuterungen vor (Seite 11):

„Sinkholes“ hingegen sind insbesondere für die Erkennung von Botnetzen erforderlich, von denen eine wesentliche Gefahr für die Netz- und Informationssystemsicherheit in Österreich ausgeht. Ein Botnetz ist ein Zusammenschluss von netzwerkfähigen Geräten, die mit Schadsoftware infiziert sind und über einen oder mehrere sogenannte „C2-Server“ (Command and Control Server) kontrolliert und missbräuchlich verwendet werden können. „Sinkholes“ stellen Maßnahmen dar, die dahingehend Abhilfe schaffen, dass sie den Datenverkehr zwischen infizierten netzwerkfähigen Geräten und C2-Servern analysieren. Sie bieten somit die Möglichkeit, Botnetze entsprechend zu untersuchen und die Kommunikation zwischen infizierten Geräten und C2-Servern so einzuschränken, dass kein Schaden verursacht werden kann. Im Gegensatz zu „Honeypots“ werden „Sinkholes“ nur insofern genutzt, als der Bundesminister für Inneres „Sinkholes“ nicht von sich aus physisch betreibt, sondern nur auf den Datenverkehr von bei Betreibern wesentlicher Dienste, Anbietern digitaler Dienste und Einrichtungen des Bundes installierten Sinkholes Zugriff,

unter Beachtung geltender anderer Sicherheitsregeln wie Safetyanforderungen und anderen gesetzlichen Vorgaben,

bekommt.

Zu § 10 – Datenverarbeitung:

Datenschutzrechtliche Klarstellungen erforderlich

Wir weisen darauf hin, dass aus Gründen der Verhältnismäßigkeit im Rahmen von Auskunftsersuchen erfragte Daten auf den erforderlichen Umfang zu beschränken sind, und regen an, einen klarstellenden Zusatz in diesem Sinne in § 10 voranzustellen. Weiters sei darauf hingewiesen, dass die nach § 10 Abs 2 abgefragten Daten Betriebs- und Geschäftsgeheimnisse der Betreiber sind und hier unbedingt besonders datensparsam und auf hohem Sicherheitsniveau agiert werden muss. Und nicht nur das: Diese Daten können sogar erstmalige Informationen über Schwachstellen der Netzarchitektur enthalten (siehe Erl zu § 9), die potentiellen Angreifern wesentliche Informationen liefern können und so per se ein Gefahrenpotential bergen.

§ 10 Abs 1 weist hinsichtlich der Datenverarbeitung des Bundeskanzlers und des Bundesministers für Inneres aus, dass diese nur die nach den §§ 4 und 5 NISG erforderlichen personenbezogenen Daten verarbeiten dürfen. Nach Abs 2 sind darüber hinaus weitergehende Verarbeitungsmöglichkeiten ausgewiesen. Es muss sichergestellt sein, dass auch hier Verhältnismäßigkeit und insbesondere eine Zweckbindung der Datenverarbeitung gewährleistet wird. Generell sollten die Verarbeitungsgrundsätze nach Art 5 DSGVO sichergestellt sein, weshalb zumindest in den Erläuterungen nochmals explizit darauf verwiesen werden sollte.

Betroffenenrechte, wie in § 11 Abs 2 aufgelistet, kommen laut DSGVO (Art 15-22) nur natürlichen Personen zu. Da sich das NISG allerdings hauptsächlich oder überwiegend an juristische Personen wendet, könnte der Eindruck entstehen, man würde hier den Anwendungsbereich der DSGVO ausdehnen wollen. Hier sollte in den Erläuterungen klargestellt sein, dass sich Absatz 2 an betroffene Personen, welche natürliche Personen sind, richtet. In § 11 NISG ist eine gemeinsame Datenverarbeitung von Bundeskanzler, Innenminister und Verteidigungsminister vorgesehen. Letztgenannter wird jedoch in § 10 nicht dazu ermächtigt, weshalb hier eine DSGVO-Konformität fraglich erscheint. Das gilt ebenso im Hinblick auf § 7.

Zu § 12 – Aufgaben der Computer-Notfallteams:

Zu § 12 (2) Z 6:

Hier wäre eine Klarstellung hinsichtlich des Austausches mit bzw dem Zugang für private und Unternehmens-CERTs im Sinne einer Integration in das AT CERT-Netzwerk wünschenswert.

Zu § 12 (7):

Das Verhältnis zur DSGVO sollte hier klargestellt werden, um Unsicherheiten von vornherein zu vermeiden.

Zu §14 – Betreiber wesentlicher Dienste:

Wir gehen, wie eingangs bereits erwähnt, davon aus, dass bei der Ermittlung der Betreiber wesentlicher Dienste die in den Sektorengesprächen besprochenen Schwellenwerte maßgeblich sind, da diese in konstruktivem Diskurs zwischen den zuständigen Ministerien und den in den jeweiligen Sektoren betroffenen Unternehmen praxisnahe und realistisch behandelt wurden. Das sollte sich auch in den auszustellenden Bescheiden widerspiegeln.

Zu begrüßen ist, dass durch § 14 Abs (5) Z 1 NISG die Ermittlung von Betreibern wesentlicher Dienste einer regelmäßigen Evaluierung unterzogen werden und der Bescheid, mit dem ein Betreiber eines wesentlichen Dienstes ermittelt wird, bei Wegfall der Voraussetzung für die Ermittlung widerrufen werden muss. Wichtig ist, dass die gesetzlichen Regelungen im sicherheitspolitischen Interesse ausgewogen sind und nicht zu wettbewerbsverzerrenden Folgen zwischen den einzelnen Mitbewerbern führen.

Generell erscheint die Feststellung der Betreiber wesentlicher Dienste mittels Bescheid sinnvoll und bringt Rechtssicherheit. Für die Unternehmer wäre es hilfreich, wenn die Beschwerde aufschiebende Wirkung hätte. Wir regen an, dies in die Erläuterungen aufzunehmen.

Die Zeit zur Nennung eines Notfallteams nach Zustellung des Bescheides ist mit zwei Wochen sehr kurz bemessen. Hier geeignete Personen zu finden kann länger dauern. Auch beträgt die Beschwerdefrist 4 Wochen gemäß § 7 Abs 4 VwGVG. Daher sollte die Frist in Abs 3 zumindest auf 4 Wochen erweitert werden.

Vor §§ 15 ff - Nachweis- und Berichtspflichten:

Unternehmen haben ein Eigeninteresse daran, sowohl ihre Mitarbeiter, die Umwelt sowie die Anlagen bzw Systeme als auch ihre Aktivitäten vor Angriffen von außen zu schützen. Sie investieren zunehmend, um ihre Sicherheitsstandards wahren zu können. Neben gesetzlichen Vorgaben und international anerkannten Standards ziehen sie auch entsprechende Konzern- bzw Branchenstandards heran. In diesem Zusammenhang ist es zu begrüßen, dass der Entwurf zum NISG, Unternehmen die Flexibilität einräumt, ihre technischen und organisatorischen Sicherheitsmaßnahmen zur Risikobewältigung als solche nachzuweisen.

Zu § 15 – Sicherheitsvorkehrungen für Betreiber wesentlicher Dienste:

Zu § 15 Abs 1 NISG Intensität der Sicherheitsvorkehrungen:

Gemäß Art 14 (1) NIS-RL sind „geeignete und verhältnismäßige“ […] Maßnahmen zu ergreifen, um die Risiken […] zu bewältigen. Diese Maßnahmen müssen unter Berücksichtigung des Stands der Technik ein Sicherheitsniveau […] gewährleisten, das dem bestehenden Risiko angemessen ist.“

Das Wort „verhältnismäßig“ in der NIS-RL bezieht sich auf das erforderliche Schutzniveau des jeweiligen wesentlichen Dienstes. Dieses Schutzniveau ist je nach Art des Dienstes unterschiedlich

hoch. Um diesem Sachverhalt Rechnung zu tragen, sollte zum einen der Begriff „verhältnismäßig“ auch in den Gesetzestext (§ 15 Abs 1) aufgenommen werden. Ergänzend sollte auch die Fügung „dem bestehenden Risiko angemessene [Maßnahmen]“ Aufnahme in den Gesetzestext finden. Anderenfalls drohen finanzielle Ausgaben zur IKT-Sicherheit weit über das erforderliche Maß hinaus.

Textvorschlag zu § 15 Abs 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 NIS (§ 3 Z 2) zu treffen“

Zu § 15 Abs 3 - Fristen:

Diese Bestimmung enthält die Umsetzungsfrist für die Sicherheitsvorkehrungen, die die Betreiber wesentlicher Dienste zu gewährleisten haben. Entgegen unserem Verständnis aus den bisherigen Diskussionen beträgt diese nunmehr insgesamt lediglich ein Jahr, dh es können entsprechende Nachweise bereits ab einem Jahr(!) nach Zustellung des Bescheids gemäß § 14 NISG abverlangt werden (§ 15 Abs 3). Dies ist kürzer als von den Branchen erhofft und wird die Betreiber wesentlicher Dienste vermutlich vor große Herausforderungen stellen. Weder sind die „geeigneten, dem Stand der Technik entsprechenden Sicherheitsvorkehrungen“ gem § 15 Abs 1 Z 1 NISG ausreichend definiert, noch sind „sektorenspezifische Sicherheitsvorkehrungen“ gemäß Z 2 absehbar. Gleiches gilt für die Entwürfe der konkretisierenden Verordnung. Beides ist einer effektiven Umsetzung abträglich.

Auch ist in Hinblick auf die Umsetzungsfrist zu berücksichtigen, dass die in Absatz 3 genannten Zertifizierungen nicht innerhalb einiger weniger Monate abgeschlossen werden können. Zertifizierungen dieser Art nehmen erfahrungsgemäß bis zu einem Jahr in Anspruch und können erst dann zielführend begonnen werden, wenn die Umsetzung von Sicherheitsvorkehrungen bereits relativ weit fortgeschritten ist.

Fraglich ist auch, ob die in Abs 3 bzw 4 genannten „qualifizierten Stellen“ binnen der oben genannten Frist eingerichtet bzw in ausreichendem Umfang zur Verfügung stehen werden. Wenig wünschenswert wäre – dies hat schon die Umsetzung der DSGVO in den Unternehmen gezeigt – , wenn eine bloß überschaubare Anzahl qualifizierter Stellen einer großen Zahl an nachfragenden Betreibern gegenübersteht.

Um Engpässe zu vermeiden, ersuchen wir, dass die Umsetzungsfrist gemäß § 15 Abs 3 NISG angemessen verlängert wird. Dies stünde nach Expertenmeinung auch nicht in Widerspruch zu den Vorgaben der NIS-RL.

§ 15 Abs 3 – Textvorschlag:

Wir schlagen folgende Konkretisierungen im Gesetzestext vor:

(3) Die Betreiber wesentlicher Dienste haben […] die Erfüllung der Anforderungen nach Abs 1 […] nachzuweisen. Dieser Nachweis kann zwei Jahre nach Zustellung des Bescheids gemäß § 14 Abs 5 Z 1 jederzeit verlangt werden. Zu diesem Zweck übermitteln die Betreiber wesentlicher Dienste eine Aufstellung der vorhandenen Sicherheitsvorkehrungen,

nach den Vorgaben der Sicherheitsvorkehrungsmaßnahmen des jeweiligen Sektors. Diese können durch den Nachweis von Zertifizierungen oder durchgeführten Überprüfungen durch qualifizierte Stellen (Abs 4), einschließlich der dabei aufgedeckten Sicherheitsmängel, erbracht werden.

Der Bundesminister für Inneres kann zur Kontrolle der Einhaltung der Anforderungen nach Abs 1

Einschau, unter Beachtung geltender anderer Sicherheitsregeln wie Safetyanforderungen und anderen gesetzlichen Vorgaben,

in die Netz- und Informationssysteme und diesbezügliche Unterlagen nehmen. Zur Herstellung der Anforderungen nach Abs 1 ist der Bundesminister für Inneres ermächtigt, Empfehlungen auszusprechen, für deren Befolgung und entsprechenden Nachweis erforderlichenfalls eine angemessene Frist zu setzen ist, widrigenfalls die Befolgung bescheidmäßig angeordnet wird.

Zu § 15 Abs 3 – Sicherheitsüberprüfung:

Die Sicherheitsüberprüfung durch qualifizierte Stellen soll sich darauf beziehen, ob Betreiber wesentlicher Dienste die Sicherheitsvorkehrungen umgesetzt haben. Organisatorische Sicherheitsvorkehrungen (zB die regelmäßige Durchführung von Risikoanalysen oder die Schaffung und Umsetzung einer betriebsinternen Informationssicherheitsrichtlinie) sollen auf deren Vorhandensein geprüft werden. Wie Betreiber wesentlicher Dienste diese geforderten Sicherheitsvorkehrungen umsetzen können, soll aber nicht von qualifizierten Stellen vorgegeben werden.

Weiters ist unklar, warum zusätzlich der Bundesminister für Inneres zur Kontrolle Einschau in die Netz- und Informationssysteme von Betreibern wesentlicher Dienste nehmen kann. Hier müsste der Nachweis von durchgeführten Sicherheitsüberprüfungen durch qualifizierte Stellen genügen. Denn gemäß Art 15 Abs 2 NIS-RL muss die zuständige Behörde (also der Innenminister) nur die erforderlichen Informationen (lit a) sowie die Nachweise für die wirksame Umsetzung der Sicherheitsmaßnahmen (lit b) zur Verfügung gestellt bekommen. Zwar kann der Nachweis auch durch eine Sicherheitsüberprüfung durch die zuständige Behörde selbst erfolgen, aber eben auch bzw „oder“ alternativ durch einen qualifizierten Prüfer.

Da gemäß § 15 Abs 3 des Gesetzesentwurfes die Sicherheitsüberprüfung durch qualifizierte Stellen vorgesehen wird, sollte nicht parallel auch der Bundesminister für Inneres Einschau in die Netz- und Informationssysteme erhalten. Dies würde unseres Erachtens über die Anforderungen der NIS-RL hinausgehen und der Satz „Der Bundesminister für Inneres kann … nehmen“ sollte daher entfallen oder zumindest eingeschränkt werden.

Zudem sieht Art 15 Abs 2 NIS-RL letzter Satz vor, dass die zuständige Behörde bei der Anforderung der Informationen und Nachweise den Zweck und die konkret verlangten Informationen anzugeben hat. Diese Vorgabe sollte sich auch im NISG wiederfinden.

Zu § 15 Abs 4:

Generell sind gesonderte Überprüfungen und Auditierungen durch externe Prüfer oder Behörden aus Kosten-, Zeit- und Aufwandsgründen kritisch zu sehen. Die im Gesetzesentwurf vorgesehen Möglichkeit, sich als Unternehmen als sogenannte „qualifizierte Stelle“ zu registrieren (§15 Abs 4 bzw Erl, S 17 f), kann diesen Aufwand reduzieren und wird grundsätzlich als positiv erachtet.

Zu § 16 - Meldepflichten für Betreiber wesentlicher Dienste:

Die in § 16 Abs 1 normierte Meldepflicht im Falle eines Sicherheitsvorfalles wird – sofern personenbezogene Daten iSd Art 4 Z 1 DSGVO betroffen sind – wohl zu Überschneidungen mit der Meldepflicht nach Art 33 f DSGVO (Data Breach Notification) führen. Wären bei einem derartigen Sicherheitsvorfall personenbezogene Daten betroffen, so müsste eine Meldung sowohl nach § 16 Abs 1 NISG als auch nach Art 33 f DSGVO erfolgen. Diese Mehrfachverpflichtung führt nicht nur zu einem erheblichen Mehraufwand für die betroffenen Betriebe, sondern bringt bei einer fehlerhaften Meldung auch die Gefahr einer Bestrafung nach § 23 NISG bzw nach Art 83 Abs 4 DSGVO mit sich.

Dieser Zusammenhang wurde auch in ErwG 63 der NIS-RL erkannt und es wurde eine Zusammenarbeit der zuständigen Behörden mit den jeweiligen Datenschutzbehörden angeregt. In diesem Sinne sollte unbedingt eine Lösung gefunden werden, die keine unnötigen, weil redundanten, Meldepflichten schafft.

§ 16 Abs 4 ist missverständlich formuliert: *„(4) Nimmt ein Betreiber wesentlicher Dienste die Dienste eines Anbieters digitaler Dienste in Anspruch, so ist jede erhebliche Auswirkung auf die Verfügbarkeit der wesentlichen Dienste, die von einem den Anbieter digitaler Dienste beeinträchtigenden Sicherheitsvorfall verursacht wurde, von diesem Betreiber wesentlicher Dienste zu melden.“*

Aus unserer Sicht lässt diese Formulierung zumindest zwei Lesarten zu: Entweder würde das bedeuten, dass eine erhebliche Auswirkung auf die wesentlichen Dienste vorliegt, die ohnehin nach §16 zu melden ist. In diesem Fall ist dieser Absatz redundant und kann somit gänzlich gestrichen werden.

Oder dieser Absatz ist dahingehend zu deuten, dass ein Betreiber wesentlicher Dienste eine Meldung machen muss, die sich auf den Sicherheitsvorfall beim Anbieter digitaler Dienste bezieht. In diesem Fall handelt es sich für den Betreiber wesentlicher Dienste um eine „doppelte Meldepflicht“, die sachlich nicht gerechtfertigt ist, da der Anbieter digitaler Dienste diese Meldung ohnehin nach § 18 machen muss. Außerdem ist seitens des Betreibers wesentlicher Dienste gar nicht zu beeinflussen, ob für eine etwaige Meldung überhaupt Daten über den Sicherheitsvorfall in ausreichender Qualität vorliegen. Dann handelt es sich um eine Mehrbelastung für Betreiber wesentlicher Dienste, die aus unserer Sicht nicht gerechtfertigt ist.

In beiden Fällen sprechen wir uns für eine Streichung von § 16 Abs 4 aus. Sollten beide Interpretationen nicht der Intention des Gesetzgebers entsprechen, so sollte eine eindeutige Formulierung gesucht werden.

Auch hier gehen wir davon aus, dass sich die in § 16 Abs 7 genannte Verordnung bei der Festlegung der Parameter des Sicherheitsvorfalls (siehe § 3 Abs 6 lit a bis d) ebenfalls auf die in den Sektorengesprächen erzielten Ergebnisse stützt, um eine praxisnahe Umsetzung und praktikable Anwendung zu gewährleisten.

Abschließend wäre es wünschenswert, wenn zumindest in die Erläuterungen zu § 16 Abs 6 die Interessenabwägung des ErwG 59 der RL zwischen dem Interesse der Öffentlichkeit, über Bedrohungen informiert zu werden, und einem möglichen wirtschaftlichen Schaden bzw Image-schaden übernommen werden könnte.

Zu § 18 – Sicherheitsvorkehrungen und Meldepflicht für Anbieter digitaler Dienste:

Nach ErwG 49 der NIS-RL ist das Risiko für Betreiber wesentlicher Dienste höher als das Risiko für den Anbieter digitaler Dienste. Daher sollten die an Anbieter digitaler Dienste gestellten Sicherheitsanforderungen dementsprechend geringer sein. Anbietern digitaler Dienste sollte es freigestellt sein, solche Maßnahmen zu ergreifen, die sie für die Bewältigung der Risiken für die Sicherheit der Netz- und Informationssystem für angemessen halten.

Diesem Umstand wurde uE weder in § 18 noch in den Erläuterungen hinreichend Rechnung getragen. Daher sollte - zumindest in den Erläuterungen – ausdrücklich festgehalten werden, dass Anbieter digitaler Dienste geringere Sicherheitsanforderungen zu erfüllen haben, wobei außerdem auch ein Verweis auf den entsprechenden Durchführungsrechtsakt der Kommission hier hilfreich wäre.

Zu § 20 – Freiwillige Meldungen:

Nachdem eine freiwillige Meldung praktisch keine Vorteile für den Meldenden bietet, steht zu befürchten, dass die Bestimmung des § 20 totes Recht werden wird. Ausgehend von Art 20 NIS-RL sollte zumindest ausdrücklich klargestellt werden, dass „

[…] der meldenden Einrichtung nicht Pflichten auferlegt werden, die nicht für sie gegolten hätten, wenn sie den Vorfall nicht gemeldet hätte.“

Zu § 23 - Verwaltungsstrafbestimmungen:

Der Strafrahmen des § 23 reicht weit und gerade im Falle von Formalverstößen oder einfachen Verletzungen von Meldepflichten scheinen die möglichen Sanktionen doch überzogen.
Aufgrund der neuen Qualität des NISG und der damit verbundenen Meldepflichten wäre es aus unserer Sicht im Sinn des Funktionierens des Systems förderlich, wenn vor einer allfälligen Geldstrafe zunächst Abhilfemaßnahmen seitens der Verwaltungsbehörde (zB Beratung, Aufforderungen zur Beseitigung der Verwaltungsübertretung, etc.) ergriffen würden, wenn diese eine Übertretung gemäß § 23 Abs 1 Z 1 - 6 feststellt. Wie eingangs erwähnt liegt die Gewährleistung der Sicherheit von Netz- und Informationssystemen im ureigenen Interesse von Betreibern wesentlicher Dienste. Deshalb und aufgrund der gegenseitigen Vernetzung von Betreibern wesentlicher Dienste, Anbietern digitaler Dienste und Behörden haben alle Akteure ein Interesse am Funktionieren dieser Sicherheitsvorkehrungen. Ein sofortiges Strafen steht diesem gemeinsamen Interesse entgegen. Wir ersuchen daher, dass im Rahmen der vorgesehenen Verwaltungsstrafen dem Prinzip „Beraten statt Strafen“ der Vorrang eingeräumt wird und dass Verwaltungsstrafen erst nach entsprechenden Mängelbehebungsaufträgen einschließlich angemessener Umsetzungsfrist ausgesprochen werden.
Zudem ist die Höhe der vorgesehenen Geldstrafen unverhältnismäßig hoch und sollten auf *„bis zu 25.000 Euro, im Wiederholungsfall bis zu 50.000 Euro“* halbiert werden.

Weitere Anmerkungen:

Das Format für jene Meldungen, die im Falle eines Sicherheitsvorfalls laut § 16 von den Betreibern wesentlicher Dienste zu erfolgen haben, sollte standardisiert sein, um eine einheitliche Qualität der Meldungen zu gewährleisten. Die Meldung sollte auf einfache Weise abgegeben werden können und für den Fall von Systemausfällen sollte für alternative Möglichkeiten Sorge getragen werden. Der (Zeit-) Aufwand für eine Meldung sollte jedenfalls so gering wie möglich gehalten werden, damit der Betreiber wesentlicher Dienste möglichst alle Ressourcen für die Behebung/Bearbeitung des Sicherheitsvorfalls verwenden kann.

C. Anmerkungen aus den Branchen:

a) Telekommunikation

Regelungszweck des NISG durch das TKG bereits erfasst

Das Regelungsziel des NISG ist für die Telekommunikationsbranche nicht neu: ein sicherer und störungsfreier Betrieb von Kommunikationsnetzen und –diensten ist seit jeher das Kerngeschäft dieser Branche. Er ist Voraussetzung für das Erbringen performanter Leistungen im In- und Ausland und wäre ohne international abgestimmte technische Normen und Übertragungsprotokolle gar nicht möglich.

Im Laufe der Zeit wurden Aspekte der Netzintegrität und der Datensicherheit auch im sektorspezifischen Recht adressiert. So findet sich eine grundlegende, auf EU-Rahmenrecht zurückgehende Bestimmung zB in § 16a TKG:

§ 16a
(1) Betreiber öffentlicher Kommunikationsnetze haben geeignete Maßnahmen zur Gewährleistung der Integrität ihrer Netze zu ergreifen und die fortlaufende Verfügbarkeit der über diese Netze erbrachten Dienste sicher zu stellen.

(2) Betreiber öffentlicher Kommunikationsnetze oder -dienste haben unter Berücksichtigung des Standes der Technik durch angemessene technische und organisatorische Maßnahmen ein Sicherheitsniveau zu gewährleisten, das zur Beherrschung der Risiken für die Netzsicherheit geeignet ist. Die Maßnahmen müssen insbesondere geeignet sein, Auswirkungen von Sicherheitsverletzungen für Nutzer und zusammengeschaltete Netze zu vermeiden bzw. so gering wie möglich zu halten.

In den weiteren Absätzen des § 16a TKG sind dann Kontrollrechte der Regulierungsbehörde, Meldepflichten der Betreiber bei Störungen festgehalten und auch die internationale Kooperation der Regulierungsbehörden mit der ENISA ist dort angesprochen.

Kurzum: Es besteht hinsichtlich des für die TK-Branche allenfalls einschlägigen Sektors „digitale Infrastruktur“ kein Bedarf, neue materielle Regelungen zu schaffen. Der Rechtsbestand umfasst bereits alle Maßnahmen im Sinne des NISG. Er geht sogar weit darüber hinaus, weil er nicht bloß die drei in Anhang II zur NIS-RL genannten Einrichtungen betrifft, sondern das gesamte Kommunikationsnetz der Betreiber.

Daher kommt hier ErwG 9 der NIS-RL zum Tragen, der für diesen Fall vorsieht:

„Wann immer solche Unionsrechtsakte Bestimmungen enthalten, mit denen Anforderungen in Bezug auf die Sicherheit von Netz- und Informationssystemen oder die Meldung von Sicherheitsvorfällen auferlegt werden, sollten diese Bestimmungen gelten, wenn sie Anforderungen vorsehen, die hinsichtlich ihrer Wirkung den in dieser Richtlinie enthaltenen Verpflichtungen mindestens gleichwertig sind.“

Branchenrisikoanalyse der Regulierungsbehörde

Welches hohe Sicherheitsniveau der Infrastruktur- und Dienstebetrieb der Telekommunikations-Branche erreicht hat, belegt der Bericht eines 2017 ins Leben gerufen Projekts der Regulierungs-behörde, in dessen Rahmen Risiken der Telekommunikationsbrache komplex analysiert und auf Basis der gewonnenen Erkenntnisse Empfehlungen für Betreiber von Netzen und Diensten sowie für die öffentliche Verwaltung gegeben wurden. Diese „IKT Branchen Risikoanalyse“ deckt alle Aspekte des NISG hinreichend ab und sollte daher auch die Basis für Bewertungen nach dem NISG sein.

Meldelinien für Betreiber nicht ausweiten

Gerade in einem Krisenfall, wenn alles von den Betreibern daran gesetzt werden muss, die Funktionsfähigkeit des Netzbetriebes aufrecht zu erhalten, sind zusätzliche Meldelinien für Störungen nicht sinnvoll. In solchen Krisenlagen gilt es, redundante Prozeduren zu vermeiden und alle Kapazitäten auf die Aufrechterhaltung des Betriebes zu lenken. Daher sollten hier die Betreiber neben den Meldungen nach TKG nicht auch noch selber nach dem NISG Meldungen vornehmen müssen. Es ist völlig ausreichend, wenn die Informationen von der RTR an die zuständigen Stellen nach dem NISG weitergeleitet werden. Hier laufen bereits alle Meldungen zusammen.

Es bedarf allerdings im NISG einer Ergänzung um sicherzustellen, dass die RTR an sie gemeldete Daten an das Bundeskanzleramt bzw das Innenministerium weitergeben darf. Hier bietet sich eine § 17 Absatz 2 nachgebildete Regelung in einem Folgeabsatz an, die wie folgt lauten könnte:

(2) Die Telekom-Regulierungsbehörde hat *die zu diesem Zweck erforderlichen* Meldungen nach § 16a TKG von Betreibern öffentlicher Kommunikationsnetze unverzüglich an den Bundesminister für Inneres zu übermitteln.

Vorbeugung von Sicherheitsvorfällen

Unter der Überschrift „Befugnisse zur Vorbeugung von Sicherheitsvorfällen" findet sich eine an das BMI adressierte Ermächtigung zum Betrieb von Störungen erkennenden Systemen, an denen die Adressaten des Gesetzes freiwillig mitwirken dürfen. Hier ist anzumerken, dass in den Erläuterungen schon von einem umfassend geplanten Kooperationsmodell die Rede zu sein scheint, was angesichts des freiwilligen Charakters dieser Zusammenarbeit zu diesem Zeitpunkt etwas verwundert. Wir schlagen daher vor und bieten zugleich an, für diese geplante Zusammenarbeit mit Unternehmen der Branche beispielsweise die bereits bestehende „Plattform Telekommunikationsüberwachung" zur Verfügung zu stellen, ein vom Fachverband Telekom-Rundfunk der Wirtschaftskammer etablierter und organisierter Arbeitskreis aus Betreibern und Vertretern des BMI und Ermittlungsbeamten des BKA.

b) Banken

Zu § 14:

Hinsichtlich § 14 NISG-E (Ermittlung der Betreiber wesentlicher Dienste) scheint eine Klarstellung sinnvoll, ob im Falle einer Unternehmensgruppe (Beteiligungen >50%) in Österreich, der durch den Bundeskanzler an Betreiber wesentlicher Dienste ausgestellte Bescheid nur für die Mutter oder auch diesbezügliche Beteiligungen, die den NISG-wesentlichen Dienst erbringen, gilt.

c) Industrie (Mineralölwirtschaft und Gasversorgungsunternehmen):

Generelle Anmerkungen:

Der Schutz der Anlagen vor Bedrohungen von außen – seien es physische oder virtuelle Angriffe – ist nicht nur Voraussetzung für eine stabile und sichere Energieversorgung, sondern liegt auch im ureigenen Interesse der Mineralölindustrie und ihrer gesetzlichen Interessenvertretung. Ein Interesse, welches in den letzten Jahren zunehmend an Bedeutung gewonnen hat, die weltweit steigenden Investitionen der Unternehmen in die IT-Sicherheit dokumentieren dies.

Besonders Cyber-Angriffe gehören mittlerweile zum Alltag von Unternehmen und müssen ganzheitlich in deren Sicherheitsstrategien berücksichtigt werden. In Zeiten täglicher Wirtschaftsaktivität über nationale Grenzen hinaus wird eine intensive Kooperation zwischen den Mitgliedstaaten immer wichtiger, um kritische Infrastruktur vor solchen virtuellen Angriffen zu schützen. Der Beschluss der EU-Richtlinie zur Harmonisierung des Sicherheitsniveaus von Netz- und Informationssystemen (NIS) ist daher ein wichtiger Schritt für die Förderung von Systemsicherheit in Informationstechnologie- (IT) und Operationstechnologie (OT) gemäß dem Stand der Technik.

Neben den wirtschaftlichen und gesellschaftlichen Aspekten ist auch die Prozesssicherheit (SEVESO III) als oberstes Cybersicherheitsschutzziel zu berücksichtigen.

Es ist allerdings wesentlich, dass die nationale Umsetzung der NIS-RL im Netz- und Informationssystemsicherheitsgesetz (NISG) ausgewogen ist, keine exzessiven zusätzlichen

bürokratischen Hürden für Unternehmen darstellt und für die betroffene Industrie möglichst kostenneutral umgesetzt wird.

Ein umfassender Schutz von kritischer Infrastruktur ist ein kontinuierlicher Prozess. Besonders im Bereich der Cyber-Sicherheit werden immer neue Wege gefunden, Sicherheitslücken auszunutzen. Um einen bestmöglichen Schutz gewährleisten zu können, braucht es einen integrierten Ansatz, welcher durch Prävention, Reaktion und Geschäftskontinuität („business continuity“) die Verletzbarkeit und Kritikalität von Energieinfrastruktur mindert.

Definitionen von Anlagen und Dienstleistungen

Beim Schutz von kritischer Infrastruktur gilt es die gleichen Definitionen und Kriterien für die Einstufung in kritisch und nicht kritisch heranzuziehen. Im Sinne der Konsistenz sollten diese auf alle Regularien Anwendung finden, die einen Bezug zu kritischer Infrastruktur haben – ungeachtet dessen, ob sie von physischen oder virtuellen Angriffen betroffen sind.

Darüber hinaus ist in Bezug auf das NISG der gewählte anlagen- bzw. dienstleistungsspezifische Ansatz zu hinterfragen. Gerade die Energiewirtschaft ist ein stark systembasierter und vernetzter Sektor – von der Erzeugung, über die Verarbeitung und Verteilung bis hin zur Speicherung von Energie. Auch im Hinblick auf die fortschreitende Digitalisierung von Wirtschaft und Industrie wäre daher ein systembasierter Ansatz für eine gesetzliche Regelung sinnvoll.

Zu § 17:

Wir begrüßen, dass der vorliegende Entwurf zum NISG (§ 17 Abs 1) die Bedenken der Energiewirtschaft ernst nimmt und dementsprechend Ausnahmen von Verpflichtungen für Betreiber wesentlicher Dienste vorsieht, sofern es für diese anderwärtigen Vorschriften zu Sicherheitsvorkehrungen und Meldepflicht gibt. Gerade für den Bereich der Energiewirtschaft gibt es solche bereits im Rahmen diverser Gesetze (zB Gas Security of Supply Verordnung, Verordnung über die Integrität und Transparenz des Energiegroßhandelsmarktes, Energiegroßhandelsdaten-Verordnung, Seveso III Richtlinie), wodurch Unternehmen dazu verpflichtet sind, eine erhebliche Anzahl an überwiegend sensiblen Daten an den jeweiligen Regulator – sowohl auf nationaler als auch auf europäischer Ebene (E-Control und ACER) – zu melden.

D. Resümee

Der vorliegende Gesetzesentwurf zur Umsetzung der NIS-RL enthält für ein Reihe von betroffenen Unternehmen neuartige Verpflichtungen, wobei das Hintanhalten von Bedrohungen der Cybersicherheit im ureigenen Interesse aller Unternehmen steht. Einzelne Anpassungen im Gesetz sollten, wie oben ausgeführt, jedenfalls noch vorgenommen werden, wobei in einigen Fällen die Übernahme von Formulierungen der Richtlinienvorgabe sinnvoll und zielführend erscheint. Speziell für Anbieter digitaler Dienste wird die Verfügbarkeit von weiterführender Information von großer Bedeutung sein. Gerne stehen wir hier für die Fortführung des konstruktiven Dialogs der letzten Monate zur Verfügung, um die für den Wirtschaftsstandort so wichtige Cybersicherheit bestmöglich auf kooperative Weise sicherzustellen.

Wir ersuchen um Berücksichtigung unserer Überlegungen und verbleiben

mit freundlichen Grüßen

Dr. Harald Mahrer
Präsident

Karlheinz Kopf
Generalsekretär

WIRTSCHAFTSKAMMER ÖSTERREICH WKO ELEKTRONISCHE SIGNATUR	**Unterzeichner**	**Wirtschaftskammer Österreich**
	Datum/Zeit-UTC	**2018-10-30T16:44:02Z**
	Aussteller-Zertifikat	**CN=a-sign-corporate-light-02,OU=a-sign-corporate-light-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT**
	Serien-Nr.	**1716778599**
	Hinweis	**Dieses Dokument wurde amtssigniert.**
	Prüfinformation	**Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter https://www.signaturpruefung.gv.at/.**