INDUSTRIELLEN VEREINIGUNG
Infrastruktur | Transport | Ressourcen | Energie

Bundeskanzleramt
BKA - I/6 (Rechts- und Vergabeangelegenheiten)
Ballhausplatz 2
1011 Wien

per eMail: nis@bka.gv.at
begutachtungsverfahren@parlament.gv.at

Wien, am 31. Oktober 2018
GZ: BKA-180.310/0234-I/6/2018

Betrifft: Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz und Informationssystemsicherheitsgesetz - NISG); Stellungnahme Industriellenvereinigung (IV)

Sehr geehrte Damen und Herren!

Die Industriellenvereinigung (IV) dankt dem Bundeskanzleramt für die Übermittlung des oben zitierten Gesetzesentwurfes und nimmt wie folgt dazu Stellung:

1. Grundsätzliches

Im Kontext der Globalisierung nehmen die Anforderungen an die Sicherheit der heimischen Industrie seit Jahren an Komplexität zu. Die Gewährleistung eines hohen Sicherheitsniveaus der Netz- und Informationssysteme liegt daher im ureigenen Interesse der Industrie. Eine sichere Wirtschaft leistet auch einen Beitrag zu sozialer Sicherheit und gesellschaftlicher Stabilität unseres Landes. Wirtschaftsschutz ist damit sowohl Wettbewerbsvorteil als auch Zukunftssicherung. Österreichs Industrie ist bereit und willens, Verantwortung zu tragen und die notwendigen Schritte für mehr Cybersicherheit aktiv und in enger Abstimmung mit den Behörden voran zu treiben. Der Entwurf zum NISG ist ein wichtiger Schritt, diesen Entwicklungen Rechnung zu tragen und kann zu einem allgemein hohen Sicherheitsniveau in Österreich und Europa beitragen.

Die betroffenen Unternehmen betreiben in vielen Fällen bereits sehr ausgereifte Sicherheitssysteme. Der Erfüllungsaufwand der Gesetzesinitiative für Unternehmen sollte daher möglichst gering gehalten werden. Auch sind die Gegebenheiten und Anforderungen je nach Sektor und Tätigkeit der Betreiber wesentlicher Dienste sehr spezifisch, weshalb maßgeschneiderte Lösungen notwendig sind. Das gilt für den Entwurf zum NISG ebenso wie für die noch auszustellenden Bescheide und Verordnungen.

2. Details zum NISG-Entwurf

Zu § 3 Begriffsbestimmungen
Hier sollte eine Klarstellung getroffen werden, dass nur jene Netz- und Informationssysteme iSd ErwGr 22 der NIS-RL betroffen sind, die zum Betrieb eines wesentlich geltenden

Dienstes benötigt werden. Dieser Aspekt könnte in die Legaldefinition NIS-G § 3 Z1 übernommen werden.

Zu § 9 Befugnisse Vorbeugung von Sicherheitsvorfällen
Es wird die Möglichkeit für u.a. Betreiber wesentlicher Dienste angeführt, an den vom BMI betriebenen technischen Einrichtungen teilzunehmen und festzulegen, welche Daten an den Bundesminister für Inneres übermittelt werden. Um Klarheit über den Charakter dieser Option zu schaffen, wird angeregt § 9 Abs. 1 wie folgt zu ergänzen: *„Die Teilnahme an dem 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."*

Zusätzlich wird angeregt, in den Erläuterungen zu § 9 festzuhalten, dass auch die Schnittstelle zwischen dem System des Teilnehmers und dem CSC (Cyber Security Center) mittels Rahmenvertrag geregelt werden kann.

Zu § 10 Datenverarbeitung
Gemäß § 10 Abs. 3 sind ersuchte Stellen, das können auch Betreiber wesentlicher Dienste sein, dazu verpflichtet, unverzüglich Auskunft zu erteilen. Bei dieser Auskunft handelt es sich etwa um Informationen, die für die umfassende Beurteilung eines Sicherheitsvorfalls notwendig sind (siehe dazu § 10 in den Erläuterungen). Das Kriterium der Unverzüglichkeit steht aus Sicht der Industrie in einem gewissen Widerspruch mit § 14 Abs. 3, nach dem ein Betreiber wesentlicher Dienste sicherzustellen hat, dass er über eine Kontaktstelle jedenfalls in jenem Zeitraum erreichbar ist, in dem er einen wesentlichen Dienst zur Verfügung stellt. Eine Kontaktstelle wird jedoch regelmäßig nicht über die nötige Expertise verfügen, um die in § 10 Abs. 3 normierte unverzügliche Auskunft zu erteilen. Die Verpflichtung zur Erteilung einer unverzüglichen Auskunft wäre daher mit einem äußerst hohen Aufwand verbunden. Es wird daher angeregt, diese Regelung zu überprüfen und entsprechend zu adaptieren.

§ 10 Abs. 4 erscheint zudem missverständlich formuliert. Es ist nicht klar ersichtlich, wen die dreijährige Aufbewahrungspflicht trifft. Es wird daher um Kenntlichmachung und Klarstellung ersucht, dass lediglich die Behörden, bei denen NIS-Büros eingerichtet sind, von der Verpflichtung zur Aufbewahrung erfasst sind. Sollten in § 10 Abs. 4 jedoch auch Betreiber wesentlicher Dienste mitumfasst sein, empfehlen wir in den Erläuterungen festzuhalten, dass es sich bei den Protokollaufzeichnungen lediglich um ein Mindestmaß an Daten, die einzig dem Zweck der Protokollierung einer Abfrage, Übermittlung und Änderung dienen, handeln soll. Eine dreijährige Aufbewahrungspflicht von IP-Adressen und Log-Files für Betreiber wesentlicher Dienste sollte in den Erläuterungen zu § 10 jedenfalls ausgeschlossen werden.

Zu § 12 Computer-Notfallteams
Die Möglichkeit sektorenspezifische Computer-Notfallteams einzurichten, wird ausdrücklich begrüßt. Wir regen an, zusätzlich festzuhalten, ob sektorenspezifische Computer-Notfallteams eine bestimmte Rechtsform aufweisen müssen, weitergehende Erläuterungen wären wünschenswert.

Zu § 14 Ermittlung Betreiber wesentlicher Dienste
Bei der Ermittlung der Betreiber wesentlicher Dienste sollten die in den Sektorengesprächen besprochenen Schwellenwerte für das BKA eingehalten werden, da diese in konstruktivem Diskurs zwischen den zuständigen Ministerien und den in den jeweiligen Sektoren betroffenen Unternehmen praxisnah und realistisch festgelegt wurden.

Zu § 15 Sicherheitsvorkehrungen für Betreiber wesentlicher Dienste
§ 15 Abs. 1 könnte so interpretiert werden, dass Betreiber wesentlicher Dienste sofort ab Rechtskraft eines Bescheides gemäß § 14 Abs. 5 Z 1 Sicherheitsvorkehrungen iSd § 15 implementiert haben müssen. Der Nachweis des Vorliegens solcher Sicherheitsvorkehrungen kann jedoch erst ab einem Jahr nach Zustellung des Bescheids

iv

von der Behörde verlangt werden. Die sofortige Verpflichtung zur Erfüllung gewisser durch Verordnung festgestellter Sicherheitsvorkehrungen ist somit in der Praxis nicht umsetzbar. Nachdem die zeitliche Abfolge bzw. Dauer zwischen Verordnungs- und Bescheiderlassung schwer abschätzbar ist, kann bei einem engen Zeitabstand nicht erwartet werden, dass im Moment der Rechtskraft des Bescheides, die in der Verordnung genannten Sicherheitsvorkehrungen bereits getroffen sind.

In Hinblick auf die Umsetzungsfrist ist ebenfalls zu berücksichtigen, dass die in Abs. 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.

Um den Normunterworfenen eine realistische Möglichkeit zur zeitgerechten Herstellung eines rechtskonformen Zustands zu geben, ist dringend der Einbau einer angemessenen Übergangsfrist in § 15 Abs. 1 zu empfehlen. Aufgrund der Tatsache, dass der Nachweis von Sicherheitsvorkehrungen nach Ablauf des ersten Jahres verlangt werden kann, wird die Aufnahme einer einjährigen Frist in § 15 Abs. 1 im Sinne der Praxistauglichkeit der Bestimmung angeregt.

Positiv hervorzuheben ist § 15 Abs. 2: demnach können Betreiber wesentlicher Dienste gemeinsam mit ihren Sektorenverbänden sektorenspezifische Sicherheitsvorkehrungen vorschlagen. Diese können auf Antrag mittels Bescheid als geeignet festgestellt werden. Diese Möglichkeit wird der Diversität der verschiedenen Sektoren gerecht und wird von der Industriellenvereinigung ausdrücklich begrüßt.

Zu § 16 Meldepflicht für Betreiber wesentlicher Dienste

§ 16 Abs. 4 erscheint missverständlich formuliert und könnte eine doppelte Meldepflicht bedeuten:

„(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“.

Obige Formulierung lässt folgende Interpretationen zu:

1) Liegt eine erhebliche Auswirkung auf die wesentlichen Dienste vor, ist diese ohnehin nach § 16 zu melden. Somit wäre dieser Absatz redundant und könnte gestrichen werden.
2) Oder ein Betreiber wesentlicher Dienste muss einen Sicherheitsvorfall melden, der sich auf einen Anbieter digitaler Dienste bezieht. Da der Anbieter digitaler Dienste einen Sicherheitsvorfall nach § 18 melden muss, würde es sich hierbei um eine doppelte Meldepflicht handeln, was sachlich nicht gerechtfertigt wäre. Außerdem ist seitens der Betreiber wesentlicher Dienste nicht beeinflussbar, ob für die geforderte Meldung Daten in ausreichender Qualität vorliegen.

Beide Interpretationen würden eine Mehrbelastung für Betreiber wesentlicher Dienste darstellen, welcher durch eine eindeutigere Formulierung Abhilfe geschaffen werden sollte.

Die in § 16 Abs. 7 genannt Verordnung sollte sich bei der Festlegung der Parameter des Sicherheitsvorfalls (siehe § 3 Abs. 6 lit. a bis d) ebenfalls auf die in den Sektorengesprächen erzielten Ergebnisse stützen, um eine praxisnahe Umsetzung und praktikable Anwendung zu gewährleisten.

iv

Zu § 20 Freiwillige Meldung
Um die freiwillige Meldung als Instrument der Prävention zu stärken, wird empfohlen in die Norm aufzunehmen, dass eine freiwillige Meldung zu keinerlei Nachteilen für den meldenden Betreiber wesentlicher Dienste und Anbieter digitaler Dienste führt.

§ 23 Verwaltungsbestimmungen
Aufgrund der neuen Qualität des NISG und der damit verbundenen Meldepflichten ist es aus Sicht der Industrie im Sinne des Funktionierens des Systems förderlich, wenn im Rahmen der vorgesehenen Verwaltungsstrafen seitens der Behörden bei Feststellung einer Übertretung gemäß § 23 Abs. 1, 1. – 6. dem Prinzip „Belehren statt Strafen“ Vorrang eingeräumt wird bzw. Verwaltungsstrafen erst nach entsprechenden Mängelbehebungsaufträgen einschließlich angemessener Umsetzungsfrist ausgesprochen werden.

Wir bedanken uns für die Möglichkeit zur Stellungnahme und ersuchen um Berücksichtigung der genannten Anregungen.

Mit freundlichen Grüßen
Industriellenvereinigung

Mag. Monika Schuh e.h.
Geschäftsführerin des Infrastrukturausschusses