**An das Bundeskanzleramt**

Per Mail an nis@bka.gv.at

**An das Präsidium des Nationalrats**

Per Mail an begutachtungsverfahren@parlament.gv.at

**Stellungnahme der Austrian Power Grid AG zum Entwurf eines Bundesgesetzes zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG)**

Austrian Power Grid AG bedankt sich für die Möglichkeit zur Stellungnahme zum Entwurf eines Bundesgesetzes zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG) und übermittelt nachstehende Anmerkungen:

**Generelle Anmerkungen:**

Austrian Power Grid AG begrüßt die Umsetzung der NIS-Richtlinie und die mit dem Gesetzesvorschlag einhergehende Weiterentwicklung und Koordination einer neuen Strategie für die Sicherheit von Netz- und Informationssystemen. Als Übertragungsnetzbetreiber ist Austrian Power Grid AG einer der der wichtigsten Betreiber kritischer Infrastruktur in Österreich. In dieser Rolle sind wir selbstverständlich massiv an einem hohen Sicherheitsniveau von Netz- und Informationssystemen interessiert und dafür bereit einen konstruktiven Beitrag zu leisten.

Der vorliegende Entwurf wird weitgehend als positiv beurteilt. Besonders erfreulich ist, dass der Gesetzgeber von der Möglichkeit Gebrauch gemacht hat, die Einrichtung **sektorenspezifischer** Computer-Notfallteams vorzusehen. Noch verbesserungsfähig sind aus unserer Sicht mancherorts missverständliche Formulierungen. Auch die Bestimmung, wonach bereits mit Rechtskraft des Bescheides, mit dem ein Betreiber eines wesentlichen Dienstes festgestellt wird, die Sicherheitsvorkehrungen iSd § 15 erfüllt werden müssen, ist kritisch zu hinterfragen, würde das die Betreiber wesentlicher Dienste doch vor eine in der Praxis wohl kaum durchführbare Aufgabe stellen.

**Konkrete Anmerkungen:**

**Zu § 3 (Begriffsbestimmungen)**

Zur Klarstellung, dass nur jene Netz- und Informationssysteme iSd ErwGr 22 der NIS-RL betroffen sind, die zum Betrieb eines wesentlich geltenden Dienstes benötigt werden, könnte dieser Aspekt in die Legaldefinition der Z1 übernommen werden.

**Zu § 9 (Befugnisse zur Vorbeugung von Sicherheitsvorfällen)**

Betreiber wesentlicher Dienste können an vom Bundesminister für Inneres betriebenen technischen Einrichtungen (CSC) teilnehmen. Die Erläuterungen zu § 9 sehen vor, dass die Teilnahme und das Ausmaß der Datenverarbeitung über Rahmenverträge geregelt werden. Hier wäre wünschenswert, dass in den Erläuterungen zu § 9 klargestellt wird, dass auch die Schnittstelle zwischen dem System des Teilnehmers und dem CSC mittels Rahmenvertrag geregelt werden kann.

**Zu § 10 (Datenverarbeitung)**

Gem § 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 um Informationen, die für die umfassende Beurteilung eines Sicherheitsvorfalls notwendig sind. Das Kriterium der Unverzüglichkeit steht 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. Daher schlagen wir vor das Wort „unverzüglich“ in § 10 Abs 3 zu streichen und durch „ehestmöglich“ oder ähnliches zu ersetzen.

§ 10 Abs 4 ist unseres Erachtens missverständlich formuliert. Es kann nicht entnommen werden, wen die dreijährige Aufbewahrungspflicht trifft. Wir ersuchen daher um Kenntlichmachung und Klarstellung, 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 (Aufgaben der Computer-Notfallteams)**

Die Möglichkeit der Einrichtung sektorenspezifischer Computer-Notfallteams wird ausdrücklich begrüßt. Jedoch ist weder dem Gesetz noch den Erläuterungen zu entnehmen, ob sektorenspezifische Computer-Notfallteams eine gewisse Rechtsform aufweisen müssen. Hier wären weitergehende Erläuterungen wünschenswert.

**Zu § 15 (Sicherheitsvorkehrungen für Betreiber westlicher Dienste)**

Es ist zu befürchten, dass § 15 Abs 1 so interpretiert wird, dass Betreiber wesentlicher Dienste sofort ab Rechtskraft eines Bescheides gem § 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 von der Behörde verlangt werden. Die sofortige Verpflichtung zur Erfüllung gewisser durch Verordnung festgestellter Sicherheitsvorkehrungen ist aus unserer Sicht nicht praxistauglich. Nachdem die zeitliche Abfolge bzw. Dauer zwischen Verordnungs- und Bescheiderlassung nicht 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. Um den Normunterworfenen eine realistische Möglichkeit zur zeitgerechten Herstellung eines rechtskonformen Zustands zu geben, ist dringend der **Einbau einer Übergangsfrist** in § 15 Abs 1 zu empfehlen. Aufgrund der Tatsache, dass der Nachweis von Sicherheitsvorkehrungen nach Ablauf des ersten Jahres verlangt werden kann, wäre auch der Einbau einer einjährigen Frist in § 15 Abs 1 im Sinne der Praxistauglichkeit der Bestimmung wünschenswert.

Positiv hervorzuheben ist § 15 Abs 2: Gem dieser Bestimmung 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 Austrian Power Grid AG ausdrücklich begrüßt.

Bezüglich der zu erwartenden Verordnung iSd § 15 Abs 6 wäre es ratsam, dass dem Erlass der Verordnung ein Begutachtungsverfahren vorausgeht. Dies würde den betroffenen Betreibern wesentlicher Dienste die Möglichkeit geben, aus Sicht der Praxis, einen konstruktiven Beitrag zur Ausgestaltung der Verordnung iSd § 15 Abs 6 zu leisten.

**Zu § 20 (Freiwillige Meldung)**

Um die freiwillige Meldung als Instrument der Prävention zu stärken, empfehlen wir in die Norm aufzunehmen, dass eine freiwillige Meldung zu keinerlei Nachteilen für den meldenden Betreiber wesentlicher Dienste führen darf.

**Kontakt:**
Austrian Power Grid AG
Wagramer Starße 19, IZD-Tower
1220 Wien

Wien, im Oktober 2018