Vereinigung Österreichischer Elektrizitätswerke

Bundeskanzleramt
Ballhausplatz 2
1010, Wien

Ergeht per E-Mail an: nis@bka.gv.at

Graz, am 29. Oktober 2018
EW - 60 - TR/SI

Stellungnahme der Vereinigung Österreichischer Elektrizitätswerke (VÖEW) zum Begutachtungsentwurf des „Bundesgesetzes zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssicherheitsgesetz – NISG)“

Sehr geehrte Damen und Herren,

Als Vertreterin der 130 kleinen und mittelgroßen Elektrizitätsunternehmen in Österreich bedanken wir uns für die Gelegenheit, zum vorliegenden Begutachtungsentwurf, dem „Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssicherheitsgesetz – NISG)“ des Bundeskanzleramtes (BKA) Stellung nehmen zu dürfen.

Der vorliegende Begutachtungsentwurf wird von uns weitgehend als positiv beurteilt. Im vorliegenden Entwurf wird besonders die gesetzliche Grundlage für die Etablierung von sektorenspezifischen Computer-Notfallteams, sowie die Bestimmung, dass Betreiber wesentlicher Dienste gemeinsam mit ihren Sektorenverbänden sektorenspezifische Sicherheitsvorkehrungen vorschlagen können, begrüßt.

Seit über sechs Jahren wird in einer beispielgebenden Public-Private-Partnership (PPP) zwischen Energiebranche, Regulator und den sicherheitsrelevanten Behörden das Thema IKT-Sicherheit in einem risikobasierten Ansatz behandelt. Durch diese konstruktive Zusammenarbeit konnte auf beiden Seiten ein lösungsorientiertes Verständnis für das Thema erreicht werden. Mit dem gemeinsamen Aufbau eines brancheneigenen Austrian Energy Computer Emergency Response Teams und der Erstellung der IKT-Risikoanalyse wurde bereits frühzeitig das Bewusstsein und die Prävention im Energiesektor gestärkt. Die österreichische E-Wirtschaft ist durch ihre Aktivitäten national und EU-weit ein Vorreiter in Bezug auf IKT-Sicherheit.

Wir möchten jedoch darauf hinweisen, dass für die konkrete Umsetzung in den Unternehmen die noch zu erlassenden Verordnungen gemäß der § 14 (sektorenspezifische Regelungen bzw. Faktoren hinsichtlich der Ermittlung der Betreiber wesentlicher Dienste), § 15 (Abs. 4: Erfordernisse, die eine qualifizierte Stelle, welche die im Unternehmen getroffenen Sicherheitsmaßnahmen zertifizieren muss, erfüllen muss; Abs. 6: Festlegung von Sicherheitsvorkehrungen selbst) und § 16 (Parameter für das Vorliegen eines Sicherheitsvorfalles im Sinne von § 3 Z 6 NISG) wesentlich sind.

Vereinigung Österreichischer Elektrizitätswerke • Augasse 20 • 8020 Graz • T 0316.685787.0 • F 0316.685787.11 • sekretariat@voeew.at • www.voeew.at
Raiffeisenbank Graz-Andritz • KtoNr. 4.499 • BLZ 38.377 • UID ATU 49765507 • ZVR 759609579

Daher ist eine gesamthafte Beurteilung der Vorschriften im Zusammenhang mit der Umsetzung der Richtlinie (EU) 2016/1148 (NIS-Richtlinie) abschließend noch nicht möglich.

Vor dem Erlassen der Verordnungen sollte somit jedenfalls die Möglichkeit einer intensiven Abstimmung mit den betroffenen Betreibern wesentlicher Dienste bzw. deren Interessensvertretungen gegeben sein.

Unsere wesentlichen Kritikpunkte sind:

- Generell erlauben wir uns auf den aktuell unbefriedigenden Umstand hinzuweisen, dass Verpflichtungen aus anderen gesetzlichen Vorgaben der Intention von NIS-Richtlinie / NISG diametral entgegenlaufen. Als Beispiel ist das Telekommunikationsgesetz genannt, welches nach wie vor die verpflichtende Einmeldung der kritischen Infrastruktur auf Grund von kommerziellen Interessen vorschreibt.
- Wir erlauben uns davon ausgehen zu dürfen, dass die Kompetenz und Zuständigkeit für das NISG und den noch zu erlassenden Verordnungen ausschließlich bei den festgelegten NIS-Behörden verbleibt und keine Ausweitung auf andere Behörden erfolgt (Vermeidung einer doppelten Meldestruktur, Vorgabe von sektorspezifischen Regelungen / Monitoring nur durch die NIS-Behörde, etc.)
- §§ 9, 10 Die Teilnahme an technischen Einrichtungen des BMI muss unbedingt freiwillig sein. Aufnahme von Ergänzungen, dass die Entscheidung vom Betreiber wesentlicher Dienste nach den Erfordernissen des Betriebes und insbesondere hinsichtlich der Informationssicherheit getroffen werden.
- §§ 12, 13: Anerkennung des bereits bestehenden Austrian Energy Computer Emergency Response Team als ein sektorenspezifisches CSIRT/CERT.
- §§ 14-16: Im Begutachtungsentwurf ist festgelegt, dass mittels Verordnungen weitere sektorenspezifische Vorgaben definiert werden. Die Möglichkeit einer intensiven Abstimmung mit den betroffenen Betreibern bzw. deren Interessensvertretungen muss vorab gegeben sein.
- § 15: Verankerung der „Verhältnismäßigkeit und Angemessenheit der Sicherheitsvorkehrungen hinsichtlich des bestehenden Risikos“, entsprechend Art 14. Abs. 11 NIS-Richtlinie.
  Die generell verankerte unmittelbare „Einschau in die Netz- und Informationssysteme und diesbezügliche Unterlagen“ bei Unternehmen und qualifizierten Stellen durch das Ministerium stellt eine umfangreiche Generalvollmacht dar, die sachlich nicht gerechtfertigt ist und daher abgelehnt wird.
- Aufnahme von praxistauglichen Fristen und Übergangsfristen zur Erfüllung der Verpflichtungen.
- § 20: Konkretisierung dahingehend, dass eine freiwillige Meldung nicht dazu führen darf, dass der meldenden Einrichtung Pflichten auferlegt werden, die nicht für sie gegolten hätten, wenn sie den Vorfall nicht gemeldet hätte (entsprechend NIS-Richtlinie Art. 20).

Vereinigung Österreichischer Elektrizitätswerke

Zu den einzelnen Punkten des Begutachtungsentwurfes des BKA nehmen wir, wie folgt, Stellung:

Zu § 2 Abs. 1 (Gegenstand und Ziele des Gesetzes):
Betreiber wesentlicher Dienste werden in § 3 Z 8 definiert, welcher auf Einrichtungen verweist, die einen wesentlichen Dienst in einem der in § 2 Abs. 1 genannten Sektoren erbringen. § 2 enthält eine Aufzählung nur der Sektoren des Anhangs II der NIS-Richtlinie zählt jedoch nicht auch die Teilsektoren und die Arten der Einrichtungen auf, welche in diesem Anhang detailliert als Betreiber wesentlicher Dienste angeführt sind. Da die Richtlinie es den Mitgliedstaaten freistellt, die Liste der wesentlichen Dienste zu erweitern, wird im Sinne der erforderlichen gesetzlichen Determinierung und Klarstellung ersucht, die in Anhang II der NIS-Richtlinie angeführten Teilsektoren und Arten der Einrichtungen wesentlicher Dienste in den Gesetzesentwurf zu übernehmen. Dies dient der Rechtssicherheit für allfällig betroffene Unternehmen im Sinne des Vermeidens von „Golden-Plating".

Zu § 3 (Begriffsbestimmungen):
Zur Klarstellung, dass nur jene Netz- und Informationssysteme iS von Erwägungsgrund (22) der NIS- Richtlinie betroffen sind, die zum Betrieb eines als wesentlich geltenden Dienstes benötigt werden, könnte dieser Aspekt in die Legaldefinition der Z 1 übernommen werden.

Des Weiteren schlagen wir vor, folgende Begriffsdefinition aufzunehmen:
Neu: „qualifizierte Stelle" eine Stelle, die den Anforderungen gemäß § 15 Abs. 4 entspricht, mittels Bescheid als qualifiziert identifiziert wurde und daher geeignet ist Sicherheitsvorkehrungen (§§ 18 und 19) zu überprüfen.

Zu § 3 Abs. 1 Z 2 (Begriffsbestimmungen „Netz und Informationssicherheit (NIS)"):
Aus Gründen der Vollständigkeit schlagen wir vor, in die Definition neben den genannten Funktionen auch das Erkennen von Sicherheitsvorfällen aufzunehmen**.**

Zu § 3 Abs. 1 Z 8 (Begriffsbestimmungen, „Betreiber wesentlicher Dienste"):
Es wird aus grundsätzlichen und pragmatischen Erwägungen angeregt, im Gesetz eine Möglichkeit für zentrale Ansprechpartner bei Unternehmen mit Konzernstruktur explizit vorzusehen.

Zu § 4 (Aufgaben des Bundeskanzlers):
Wir begrüßen, dass auf die Österreichische Strategie für Cyber Security (ÖSCS) aufgebaut und gleichzeitig die öffentlich-private Zusammenarbeit PPP explizit angesprochen wird.

Zu § 5 Z 3 (Aufgaben des Bundesministers für Inneres):
Für die Erstellung des Lagebildes sind auch freiwillige Meldungen von „Beinahe-Ereignissen" relevant. Es muss aber sichergestellt werden, dass freiwillige Meldungen über nicht meldepflichtige Ereignisse oder Sachverhalte zu keinem Nachteil für den meldenden Betreiber wesentlicher Dienste führen. Daher muss sichergestellt sein, dass die **Vertraulichkeit und die Anonymität des Melders in jedem Fall sichergestellt** sind.

Zu § 5 Z 7 (Aufgaben des Bundesministers für Inneres):

Die Anbindung des Cyberkrisenmanagements an das generelle staatliche Krisen- und Katastrophenmanagement wird ausdrücklich begrüßt.

Zu § 9 (Befugnisse zur Vorbeugung von Sicherheitsvorfällen):
Aus unserer Sicht sollten bei § 9 noch Ergänzungen hinsichtlich der Verantwortung der Betreiber wesentlicher Dienste erfolgen, damit klar ist, dass letztlich die Entscheidung vom Betreiber nach den Erfordernissen des Betriebes und insbesondere hinsichtlich der Informationssicherheit getroffen werden kann.

Zu § 9 (Befugnisse zur Vorbeugung von Sicherheitsvorfällen):
Betreiber wesentlicher Dienste können an vom Bundesministerium für Inneres betriebenen technischen Einrichtungen (CSC) teilnehmen. Die Teilnahme an einer solchen technischen Einrichtung des BMI muss, so wie derzeit geplant, unbedingt freiwillig sein. Teilnahmeverpflichtungen für Betreiber oder Nutzungsrechte von Betreibereinrichtungen durch das BMI wären in jedem Fall abzulehnen.

Als Ergänzung wird daher in Abs. 1 und 2 vorgeschlagen:
Zu § 9 Abs. 1 (Befugnisse zur Vorbeugung von Sicherheitsvorfällen):
„(1)…übermittelt werden. ***Betreiber wesentlicher Dienste sind berechtigt, die konkreten technischen Einrichtungen zu evaluieren und bei Sicherheitsbedenken abzulehnen. Freiwillig teilnehmende Organisationen haben jedenfalls das Recht, umfassend, zeitnahe und unentgeltlich über sie betreffende Erkenntnisse informiert zu werden.*** *Für die Teilnahme…“*

Zu § 9 Abs. 2 (Befugnisse zur Vorbeugung von Sicherheitsvorfällen):
„(2) Der Bundesminister für Inneres…Einrichtungen ***eines Betreibers wesentlicher Dienste*** *nutzen, um die Muster von Angriffen auf Netz- und Informationssysteme zu erkennen,* ***soweit es nicht zu einer Gefährdung der Anlagen oder des Betriebes von Betreibern wesentlicher Dienste führt. An diesen Betreiber ist ebenfalls ein dem § 9 Abs. 1 entsprechender Pauschalbetrag zu leisten.“***

Die Erläuterungen zu § 9 sehen vor, dass die Teilnahme und das Ausmaß der Datenverarbeitung über Rahmenverträge geregelt werden. Hier wäre es 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.

Aus unserer Sicht ist auch eine Datenminderung sinnvoll. Unser Vorschlag lautet:
„(3) Die technischen Einrichtungen laut Abs. 1 und 2 sind so zu installieren, dass sie möglichst nur den für die Erfüllung des Zweckes unbedingt nötigen Datenverkehr erfassen. Die gewonnenen personenbezogenen Daten dürfen ausschließlich für die Erfüllung der Aufgabe gemäß § 5 Z 4 verwendet werden.“

Zu § 10 Abs. 2 (Datenverarbeitung):
Alle Entscheidungen müssen vom Betreiber wesentlicher Dienste nach den Erfordernissen des Betriebes und insbesondere hinsichtlich der Informationssicherheit getroffen werden.
Wir gehen somit davon aus, dass nur organisatorische Sicherheitsmängel an die NIS Behörde übermittelt werden müssen - also keine technischen Details oder Meldung von Systemschwachstellen, bevor diese behoben werden konnten.

Zur Klarstellung sollte eine Ergänzung wie folgt vorgenommen werden:
„(2)…die Daten gemäß § 9 Abs. 1 und 2 sowie Verwaltungsdaten ***unter Gewährleistung der Informationssicherheit*** *zu verarbeiten.“*

Zu § 10 Abs. 3 (Datenverarbeitung):
Gem. § 10 Abs. 3 sind ersuchte Stellen, das können auch Betreiber wesentlicher Dienste sein, dazu verpflichtet, unverzüglich Auskunft zu erteilen. Die Vorgabe, dass Auskünfte „unverzüglich“ zu erfolgen haben, ist nicht praxistauglich, weil komplexere Auskünfte Recherchearbeit und – punktuell – durchaus Expertenwissen erfordern können. Für eine „unverzügliche“ Antwort wäre ein weit höherer Aufwand erforderlich als ihn die – gem. § 14 Abs. 3 – einzurichtende Kontaktstelle leisten kann.
Wir empfehlen daher das Wort *„unverzüglich“* im Gesetzestext zu streichen oder gegebenenfalls durch ***„zeitnah“*** oder ähnliches zu ersetzen (vgl. auch § 23 Abs. 1 Z. 1). Die Aufnahme einer Definition des Begriffes wäre zielführend.
Die Auskunftspflicht der Betreiber, der Computer-Notfallteams sowie der qualifizierten Stellen gegenüber der NIS-Behörde soll jedenfalls auf jenen Umfang eingeschränkt sein, der unmittelbar für die NIS relevant ist (Systeme und Services, die unmittelbar für die Erbringung der wesentlichen Dienste erforderlich sind) und nicht darüber hinaus gehen. Eine Konkretisierung ist vorzunehmen.

Zu § 10 Abs. 4 (Datenverarbeitung):
Dieser Absatz ist unseres Erachtens missverständlich formuliert. Es kann nicht entnommen werden, wen die dreijährige Aufbewahrungspflicht trifft. Wir ersuchen daher um 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.

Angeregt wird auch eine ergänzende Regelung in § 10, wonach die, den Behörden zugehenden Daten und Unterlagen (z.B. auch jene nach § 15 Abs. 3 zu übermittelnden Unterlagen) einer strikten Geheimhaltung unterliegen und auch besonders zu schützen sind.

Zu §§ 12, 13 (Computer Notfallteams):
Die gesetzliche Grundlage für sektorenspezifische Computer-Notfallteams wird von uns ausdrücklich begrüßt, jedoch wären weitergehende Erläuterungen in Bezug auf die Rechtsnatur bzw. Rechtsform der sektorenspezifischen Computer-Notfallteams wünschenswert. Innerhalb des Energiesektors wurden hier bereits substantielle Vorarbeiten erbracht.
Folglich soll das bereits bestehende Austrian Energy Computer Emergency Response Team als ein sektorenspezifisches CSIRT/CERT anerkannt werden. Gleiches gilt auch für das bisherige nationale CERT, CERT.at, für die Rolle des nationalen Computer-Notfallteam.

Zu § 12 Abs. 2 Z 1 (Computer Notfallteams):
In Z 1 ist nicht weiter spezifiziert, welcher Inhalt der Meldungen weitergegeben wird. Die Referenz auf Z 1 beinhaltet auch freiwillige Meldungen laut § 20. Wir gehen davon aus, dass freiwillige Meldungen nur anonymisiert und inhaltlich zusammengefasst weitergegeben werden.

Zu § 12 Abs. 5 (Computer Notfallteams):
Es ergibt sich auch aus der NIS-RL, dass alle sektoralen Computer-Nofallteams Mitglieder im CSIRTs Network sind. Wir halten es daher für sinnvoll den Abs. 5 mit
„Das GovCert, das nationale und alle sektorspezifischen Computer-Notfallteams sind Mitglied des europäischen CSIRT-Netzwerks." einzuleiten.

Zu § 14 Abs. 2 lit a bis f und Abs. 4 (Ermittlung der Betreiber wesentlicher Dienste):
In Abs. 2 werden die Faktoren definiert, die eine Einteilung zu einem wesentlichen Dienst vorgeben und somit den Anwendungsbereich des NISG festlegen. Aus Abs. 4 ergibt sich die Möglichkeit, weitere sektorenspezifische Faktoren mittels Verordnungen festzulegen. Um diese näheren Regelungen und weiteren Faktoren sowie die Schwellenwerte für Meldepflichten und geforderte Sicherheitsvorkehrungen, welche mittels Verordnungen definiert werden, bewerten zu können und sich entsprechend darauf vorzubereiten, **muss die Möglichkeit einer intensiven Abstimmung mit den betroffenen Betreibern bzw. deren Interessensvertretungen vorab gegeben sein.** Dies vor allem in Hinblick auf § 28 Abs. 4 mit der Möglichkeit eines Inkrafttretens der Verordnung rückwirkend mit 9. Mai 2018.

Zur Klarstellung sollte in Abs. 4 weiters eine Ergänzung wie folgt vorgenommen werden:
„(4)…Sicherheitsniveau für Netz- und Informationssysteme ***im jeweiligen Sektor*** *gewährleisten…"*

Zu § 14 Abs. 3 (Ermittlung der Betreiber wesentlicher Dienste):
Die Frist von zwei Wochen ab Zustellung des Bescheids zur Nennung einer Kontaktstelle ist äußerst kurz angesetzt – vor allem, wenn noch formelle Beschlüsse beim Betreiber gefasst werden müssen. Da gegenwärtig weiters noch nicht festgelegt ist, welche Anforderungen die erwähnte Kontaktstelle im Hinblick auf deren Erreichbarkeit bzw. die Qualifikation der entsprechenden Mitarbeiter zu erfüllen hat, sollte die vorgesehene Frist von zwei Wochen auf mindestens vier Wochen erstreckt werden. Im Übrigen sind die Kommunikationsstrukturen, über die der Informationsaustausch mit den Betreibern wesentlicher Dienste erfolgt, zu definieren und es sind konkrete Reaktionszeiten festzulegen.

Zu § 15 Abs. 1 (Sicherheitsvorkehrungen für Betreiber wesentlicher Dienste):
Wir sehen hier aufgrund der **fehlenden Verankerung** des in der NIS-Richtlinie Art. 14. Abs. 1 angeführten Verweises **auf Verhältnismäßigkeit und Angemessenheit der Sicherheitsvorkehrungen hinsichtlich des bestehenden Risikos, einen wesentlichen Ergänzungsbedarf im vorliegenden Entwurf NISG.**
Dies führt dazu, dass laut Gesetzesentwurf alle wesentlichen Dienste und im Geltungsbereich liegenden Netz- und Informationssysteme mittels des Standes der Technik entsprechenden Sicherheitsvorkehrungen zu schützen sind. Wird kein risikobasierter Ansatz ermöglicht, könnte

dies dazu führen, dass die Sicherheitsvorkehrungen der Betriebssicherheit entgegenwirken und damit die Erbringung des wesentlichen Dienstes beeinträchtigt werden könnte.

In Anlehnung an § 18 Abs. 1 NISG bzw. Art. 14 Abs. 1 NIS-Richtlinie könnte daher § 15 Abs. 1 wie folgt geändert werden:
(1) Die Betreiber wesentlicher Dienste haben in Hinblick auf die von ihnen betriebenen wesentlichen Dienste (§ 14 Abs. 2) geeignete ***und verhältnismäßige*** *Sicherheitsvorkehrungen zur Gewährleistung der NIS (§ 3 Z 2) zu treffen.* ***Diese Vorkehrungen müssen unter Berücksichtigung des Stands der Technik ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, das dem bestehenden Risiko angemessen ist.***

In den Erläuterungen zu § 15 wäre weiters entsprechend zu ändern/ergänzen: „In Umsetzung des Art. 14 Abs. 1 NIS-RL wird den Betreibern wesentlicher Dienste vorgeschrieben, geeignete und ***verhältnismäßige*** *Sicherheitsvorkehrungen zu treffen.* ***Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer wesentlichen Beeinträchtigung der betroffenen kritischen Infrastruktur steht.*** *Sie können sowohl…“*

Abs. 1 kann weiters so interpretiert werden, dass die 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 implementiert sind. Um den Normunterworfenen eine realistische Möglichkeit zur zeitgerechten Herstellung eines rechtskonformen Zustands zu geben, wird dringend die Aufnahme einer Übergangsfrist in § 15 Abs. 1 empfohlen. Aufgrund der Tatsache, dass der Nachweis von Sicherheitsvorkehrungen nach Ablauf des ersten Jahres verlangt werden kann, wäre auch die **Aufnahme einer einjährigen Frist in § 15 Abs. 1** im Sinne der Praxistauglichkeit der Bestimmung wünschenswert.

Zu § 15 Abs. 2 (Sicherheitsvorkehrungen für Betreiber wesentlicher Dienste):
Positiv hervorzuheben ist § 15 Abs. 2. Entsprechend 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 ausdrücklich begrüßt.

Ähnlich wie in § 16 Abs. 3 geregelt, sind die wesentlichen Inhalte einer Antragstellung aber noch näher zu spezifizieren.

Zu § 15 Abs. 3 (Sicherheitsvorkehrungen für Betreiber wesentlicher Dienste):
Bei § 15 Abs. 3 weisen wir darauf hin, dass die vom NISG vorgesehene Frist von einem Jahr ab Zustellung zu kurz bemessen ist. Angesichts der Komplexität der Thematik erscheint eine

Verlängerung auf 24 Monate sachlich geboten. Das **Verlangen des Nachweises der Erfüllung aller Sicherheitsmaßnahmen** durch den Bundesminister für Inneres bereits ein Jahr nach Zustellung des Bescheides gemäß § 14 Abs. 5 Z 1 könnte dazu führen, dass wiederum mit erheblichem wirtschaftlichen Aufwand innerhalb kürzester Zeit ohne Gesamtsicht auf den wesentlichen Dienst die Maßnahmen zur Erfüllung der Verpflichtung umgesetzt werden. Dies würde auch dazu führen, dass alle Betreiber wesentlicher Dienste in einem engen zeitlichen Rahmen ihre Nachweise der Erfüllung der Sicherheitsmaßnahmen prüfen lassen und an die Behörde übermitteln würden und in weiterer Folge drei Jahre später die nächste Abgabewelle eintreten würde.

Der Absatz sollte folgendermaßen adaptiert werden:
(3)…gegenüber dem Bundesminister für Inneres nachzuweisen. ***Dieser Nachweis kann frühestens 24 Monate nach Rechtskraft des Bescheides gemäß § 14 Abs. 5 Z 1 jederzeit verlangt werden. Die Betreiber wesentlicher Dienste haben binnen dieser Frist*** *eine Aufstellung der vorhandenen Sicherheitsvorkehrungen durch den Nachweis von Zertifizierungen oder durchgeführten Überprüfungen durch qualifizierte Stellen (Abs. 4), einschließlich der dabei aufgedeckten Sicherheitsmängel* ***nachzuweisen****. Der Bundesminister für Inneres kann …“*

Die Formulierung *„(3)…Der Bundesminister für Inneres kann zur Kontrolle der Einhaltung der Anforderungen nach Abs. 1* ***Einschau in die Netz- und Informationssysteme und diesbezügliche Unterlagen nehmen“*** **stellt eine umfangreiche Generalvollmacht dar, die sachlich nicht begründbar ist**. Insbesondere, weil eigentlich vorgesehen ist, dass die Überprüfung durch *„qualifizierte Stellen“* zu erfolgen hat. Diese qualifizierten Stellen werden vorher durch die Behörde zugelassen. Ein darüber hinaus gehender Datenzugriff ist aus Gründen der Datensicherheit und des notwendigen Schutzes von Geschäfts- und Betriebsgeheimnissen nicht wünschenswert. Wir empfehlen daher die Streichung der zitierten Stelle in Abs. 3.

Zu § 15 Abs. 5 (Sicherheitsvorkehrungen für Betreiber wesentlicher Dienste):
In Abs. 5 sollte sichergestellt werden, dass bei der *„Einschau“* in die Netz- und Informationssysteme einer qualifizierten Stelle zwar die Qualifikation dieser qualifizierten Stelle überprüft werden darf, dass aber keine Daten von geprüften Betreibern offengelegt werden dürfen.

Zu § 15 Abs. 6 (Sicherheitsvorkehrungen für Betreiber wesentlicher Dienste):
Da manche Betreiber Zertifizierungen entsprechend der ISO/IEC 27001 (Informationssicherheit) anstreben bzw. schon über eine solche verfügen, wäre sicherzustellen, dass bei einer entsprechenden Zertifizierung die dafür erforderlichen Sicherheitsvorkehrungen auch dem vom NISG geforderten Standard genügen. Die gemäß § 15 Abs. 6 noch zu erlassende Verordnung sollte diesbezüglich entsprechende Festlegungen enthalten.
Weiters muss **vor dem Erlassen der Verordnung die Möglichkeit einer intensiven Abstimmung mit den betroffenen Betreibern bzw. deren Interessensvertretungen gegeben sein.**

Zu §16 Abs. 1 und 3 (Meldepflicht für Betreiber wesentlicher Dienste)
Es wird empfohlen, die Möglichkeit vorzusehen, mit einer unverzüglichen Meldung nur Erstinformationen zu übermitteln und diese Erstmeldung, durch spätere Ergänzungen zu konkretisieren bzw. zu stornieren, falls sich der Verdacht auf einen Sicherheitsvorfall nicht bestätigt hat.

Zu § 16 Abs. 3 (Meldepflicht für Betreiber wesentlicher Dienste):
Die Meldepflicht sollte sich nur auf relevante Angaben zum Sicherheitsvorfall erstrecken. Dazu wird vorgeschlagen, den Begriff *„sämtliche“* durch ***„relevante“*** zu ersetzen. Weiters kann in der Meldung nur die ***„bekannte** betroffene Informationstechnik“* angeführt werden.

Zu § 16 Abs. 6 (Meldepflicht für Betreiber wesentlicher Dienste):
Die vorgesehene Möglichkeit, dass die Behörde vom Betreiber die Übernahme der Unterrichtungsverpflichtung verlangen kann, wird abgelehnt. Daher soll der letzte Satz von § 16 Abs. 6 *„Die zuständige Behörde kann verlangen, dass der Betreiber wesentlicher Dienste dies übernimmt.“* ersatzlos gestrichen werden.

Wenn die zuständige Behörde entscheidet, die Öffentlichkeit zu informieren, so sollte dies in Abstimmung mit den betroffenen Betreibern erfolgen, damit diese auf den dadurch zu erwartenden Kommunikationsbedarf vorbereitet sind und reagieren können.

Zu § 18 Abs. 4 (Sicherheitsvorkehrungen und Meldepflicht für Anbieter digitaler Dienste)
Die Wortfolge *„(4)…wenn ihm Umstände bekannt werden…“* könnte wohl auch dahingehend ausgelegt werden, dass der – beispielsweise – von einem Konkurrenten erhobene, nicht substantielle Verdacht für eine *„Einschau“* beim Anbieter digitaler Dienste ausreichen würde. Hier sollten nach unserem Dafürhalten objektive und nachvollziehbare Umstände normiert werden.

Zu § 20 (Freiwillige Meldung):
Die vertrauensvolle Meldung von nicht meldepflichtigen Vorfällen oder Beinahe-Vorfällen an das (sektorenspezifische) Computer-Notfallteam ist ein wichtiger Faktor für dessen Wirksamkeit (z.B. im Hinblick auf die Beobachtung und Analyse von Risiken und die Ausgabe von Frühwarnungen und Handlungsempfehlungen an die Mitgliedsunternehmen).
Es muss daher sichergestellt sein, dass freiwillige Meldungen an das Computer-Notfallteam zu keinerlei Nachteilen für den meldenden Betreiber, seinen Mitarbeitern oder Führungskräften führen. Daher muss **normiert werden, dass die Vertraulichkeit und die Anonymität des Melders in jedem Fall gewährleistet sind und eine Auskunftspflicht nach § 10 Abs. 3 nicht kompromittiert werden kann.**

Aus diesem Grund wird vorgeschlagen, dass die Nennung der meldenden Einrichtung automatisch entfallen sollte und § 20 wie folgt adaptiert wird:
***„Risiken und** Störungen, die kein Sicherheitsvorfall (§ 3 Z 6) sind oder die Betreiber von nicht wesentlichen Diensten betreffen, können an das **jeweils zuständige sektorenspezifische oder an das nationale** Computer-Notfallteam gemeldet werden, das die Meldungen **anonymisiert und inhaltlich** zusammengefasst an den Bundesminister für Inneres weiterleitet; …“*

Relevante Informationen in Form von freiwilligen Meldungen (ohne Nennung der meldenden Einrichtung) werden schon jetzt vom Austrian Energy Computer Emergency Response Team entsprechend dem Code of Conduct an das Ministerium weitergeleitet.

Zu § 23 Abs. 4 (Verwaltungsstrafbestimmungen):
Dieser Absatz sollte gestrichen werden. Auf jeden Fall sollte ein Risikotransfer durchgeführt werden müssen und die NIS-Behörde muss für das Risiko der *„Einschau“* auch haften. Technische Audits stellen immer ein betriebliches Risiko dar.
Generell muss dem Prinzip „Belehren statt Strafen“ Vorrang eingeräumt werden bzw. sollen Verwaltungsstrafen erst nach nicht erfolgten entsprechenden Mängelbehebungsaufträgen einschließlich angemessener Umsetzungsfrist ausgesprochen werden.

Erläuterungen:
Zu § 2, Abs. 3 letzter Satz
Anhand der Erläuterungen zu § 2 könnte der Eindruck entstehen, dass die Funktionsfähigkeit der staatlichen Einrichtungen alleinig von der Dienstleistung der Energieversorger abhängt. Wir schlagen daher folgende geänderte Formulierung vor, welche die tatsächliche Situation besser wiedergibt: *„Die Funktionsfähigkeit staatlicher Einrichtungen kann auch insbesondere dann gefährdet sein, wenn ein Sicherheitsvorfall nicht bei der staatlichen Einrichtung selbst, sondern bei einem **Betreiber wesentlicher Dienste** auftritt, von dessen Dienst die betroffene Einrichtung bei der Erbringung der eigenen Leistung abhängig ist.“*

Wir danken für die Möglichkeit eine Stellungnahme abgeben zu dürfen und bitten um Berücksichtigung unserer Ausführungen.

Für etwaige Rückfragen stehen wir Ihnen jederzeit gerne zur Verfügung.

Mit freundlichen Grüßen
VEREINIGUNG ÖSTERREICHISCHER ELEKTRIZITÄTSWERKE

Mag. Roland Tropper
Geschäftsführer