Stellungnahme der VERBUND AG

zum Entwurf des Bundesgesetzes zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG)

Hauptanliegen von VERBUND:

- Sicherheitsvorkehrungen sollen risikoorientiert entschieden werden und somit der Höhe des potenziellen Risikos angemessen sein.
- Das bereits bestehende Austrian Energy CERT soll als ein sektorenspezifisches CSIRT/CERT anerkannt werden.
- Kein unmittelbares Einsichtsrecht des BMI in Daten von erfassten Betreibern wesentlicher Dienste – weder bei diesen selbst noch bei den qualifizierten Stellen.

VERBUND bedankt sich für die Möglichkeit zur Stellungnahme und übermittelt folgende Anmerkungen zum Vorschlag des Bundeskanzleramtes für ein Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG).

Generelle Anmerkungen:

VERBUND begrüßt die nun von der Bundesregierung gefassten Schritte zur Umsetzung der NIS-Richtlinie der Europäischen Union und teilt die Intention des Gesetzgebers, bestehende Koordinationsstrukturen im Bereich der Sicherheit von Netz- und Informationssystemen weiter zu verbessern.

VERBUND, als führendes Unternehmen der Elektrizitätsbranche in Österreich, wird in konstruktiver Weise zur weiteren Verbesserung der Sicherheitsniveaus seinen Beitrag leisten. VERBUND war bereits in der Vergangenheit in der Risikoanalyse aktiv und beteiligte sich am Aufbau der ECERT.

Auch wenn der vorliegende Entwurf über weite Strecken positiv eingeschätzt wird, gibt es unseres Erachtens noch die eine oder andere Verbesserungsmöglichkeit. Insbesondere weisen wir darauf hin, dass auch bei den Sicherheitsvorkehrungen für Betreiber wesentlicher Dienste (§15) auf die Risikoadäquanz abgestellt werden sollte, so wie dies bei den Betreibern digitaler Dienste bereits vorgesehen ist. Darüber hinaus erscheinen die Möglichkeiten des Innenministers dort unangemessen, wo er direkt in Netz- und Informationssysteme Einsicht nehmen kann.

Konkrete Anmerkungen:

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 Bundekanzlers)

VERBUND begrüßt, dass auf die Österreichische Strategie für Cyber Security (ÖSCS) aufgebaut und gleichzeitig die öffentlich-private Zusammenarbeit explizit angesprochen wird.

Zu § 5 (Aufgaben des Bundesministers für Inneres)

Z 3: 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 ist.

Z 7: Die Anbindung des Cyberkrisenmanagement an das generelle staatliche Krisen- und Katastrophenmanagement wird ausdrücklich begrüßt.

Zu § 9 (Befugnisse zur Vorbeugung von Sicherheitsvorfällen)

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.

Zu §10 (Datenverarbeitung)

In § 10 Abs. 3 wird die Auskunftspflicht gegenüber den NIS Büros normiert. 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 eine 24/7 erreichbare Kontaktstelle, die gem. § 14 Abs. 3 einzurichten ist, leisten kann. Wie empfehlen daher das Wort „unverzüglich" im Gesetzestext zu streichen oder gegebenenfalls durch „zeitnah" oder ähnliches zu ersetzen. Die Auskunftspflicht sowohl der Betreiber als auch der Computer-Notfallteams als auch 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.

Zu §§ 12, 13 (Computer Notfallteams)

Die gesetzliche Grundlage für sektorenspezifische Computer-Notfallteams wird von VERBUND ausdrücklich begrüßt. Innerhalb des Energiesektors wurden hier bereits substantielle Vorarbeiten erbracht. Folglich soll das bereits bestehende Austrian Energy CERT als ein sektorenspezifisches CSIRT/CERT anerkannt werden.

Zu § 14 (Ermittlung der Betreiber wesentlicher Dienste)

Abs. 3: 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. Wie empfehlen eine Streckung der Frist auf 30 Tage.

Wie schon in der Anmerkung zu § 3 Abs. 1 Z 8 ausgeführt, regen wir aus grundsätzlichen und pragmatischen Erwägungen an, im Gesetz eine Möglichkeit für zentrale Ansprechpartner bei Unternehmen mit Konzernstruktur explizit vorzusehen.

Abs. 4: Konkretisierungen (insbes. Schwellenwerte) werden mittels Verordnung erfolgen. Wir empfehlen diese Verordnung einer Begutachtung zu unterziehen, an der sich die betroffenen Betreiber bzw. deren Interessensvertretungen beteiligen können.

Zu §15 (Sicherheitsvorkehrungen für Betreiber wesentlicher Dienste)

Abs. 1: Wir weisen wir darauf hin, dass auch bei den Sicherheitsvorkehrungen für Betreiber wesentlicher Dienste zusätzlich zum Stand der Technik auch auf die Risikoadäquanz abzustellen ist, so wie dies bei den Betreibern digitaler Dienste bereits vorgesehen ist (§18 Abs. 1). Das Sicherheitsniveau soll im Verhältnis zur Höhe des Risikos dem Grundsatz der Angemessenheit folgen, das, wird auch die Akzeptanz in der Praxis erhöhen und eine sachlich ungerechtfertigte Differenzierung vermeiden helfen.

Abs. 2: Es wird begrüßt, dass Sektorenverbände sektorenspezifische Sicherheits-vorkehrungen vorschlagen und diese auf Antrag mittels Bescheid als geeignet festgestellt werden können.

Abs. 3: Die Frist für den Nachweis von Sicherheitsvorkehrungen ist mit einem Jahr ab Zustellung des Bescheids festgesetzt. Die ist aus VERBUND Sicht durchaus praxistauglich. Aus Gründen der Rechtssicherheit sollte zusätzlich einer Klarstellung erfolgen, dass dann auch die Sicherheitsvorkehrungen spätestens erfolgt sein müssen.

Abs. 3 und 5: Die Formulierung „*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 nachvollziehbar 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 und des gesamten Abs. 5. Sollte dies nicht erfolgen, so wird eine Konkretisierung der Möglichkeiten des BMI angeregt, im Besonderen insofern, als ein Datenzugriff des BMI ohne Zustimmung nicht möglich sein darf.
In Abs. 5 sollte zudem 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.

§ 20 Freiwillige Meldungen

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 oder seine Mitarbeiter und Führungskräfte führen. Daher muss normiert werden, dass die Vertraulichkeit und die Anonymität des Melders in jedem Fall gewährleistet ist.

Kontakt:

Wien, im Oktober 2018

VERBUND AG
Mag. Roland Langthaler
Am Hof 6a, 1010 Wien
Tel: +43 (0)50313-53116
e-mail: roland.langthaler@verbund.com
www.verbund.com