

# Bericht

## des Ausschusses für innere Angelegenheiten

**über die Regierungsvorlage (369 der Beilagen): Bundesgesetz, mit dem das Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemssicherheitsgesetz – NISG) erlassen und das Telekommunikationsgesetz 2003 geändert wird**

Mit 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 (im Folgenden: NIS-RL), die am 8. August 2016 in Kraft getreten ist, soll EU-weit ein hohes Sicherheitsniveau der Netz- und Informationssysteme erreicht werden. Vor diesem Hintergrund soll(en) unter anderem die Zusammenarbeit zwischen den Mitgliedstaaten in strategischer und operationeller Hinsicht gestärkt werden, Mitgliedstaaten eine nationale NIS-Strategie erarbeiten, die strategische Ziele, Prioritäten und Maßnahmen enthalten soll, um in den einzelnen Mitgliedstaaten ein hohes Sicherheitslevel der Netz- und Informationssysteme zu erreichen, nationale Behörden und Computer-Notfallteams benannt werden und bestimmte, für das Gemeinwohl wichtige private und öffentliche Anbieter (Betreiber wesentlicher Dienste und digitale Diensteanbieter) zu angemessenen Sicherheitsmaßnahmen und Meldung erheblicher Störfälle verpflichtet werden.

Betreiber eines wesentlichen Dienstes stellen einen Dienst der in Anhang II der NIS-RL genannten und im Folgenden aufgelisteten Sektoren zur Verfügung: Energie (Elektrizität, Erdöl, Erdgas), Verkehr (Luftverkehr, Schienenverkehr, Schifffahrt, Straßenverkehr), Bankwesen (Kreditinstitute), Finanzmarktinfrastrukturen (Betreiber von Handelsplätzen, zentrale Gegenparteien), Gesundheitswesen (Einrichtungen der medizinischen Versorgung, einschließlich Krankenhäuser und Privatkliniken), Trinkwasserlieferung und -versorgung (Lieferanten von und Unternehmen der Versorgung mit „Wasser für den menschlichen Gebrauch“), Digitale Infrastruktur (Internet Exchange Points, DNS-Diensteanbieter, TLD-Name-Registries). Ferner sollen (ohne entsprechende RL-Vorgabe) bestimmte Einrichtungen des Bundes im Rahmen der österreichischen Umsetzung berücksichtigt werden.

Digitale Diensteanbieter sind – ab einer gewissen Größe – sämtliche Anbieter eines Online-Marktplatzes, einer Online-Suchmaschine oder eines Cloud-Computing-Dienstes.

In Österreich wird die NIS-RL mit dem vorliegenden Bundesgesetz (Netz- und Informationssystemssicherheitsgesetz – NISG) umgesetzt. Dabei sollen Aufgaben, die sich aus der NIS-RL ergeben, bereits bestehenden Strukturen übertragen werden. Der Bundeskanzler wird die strategischen Aufgaben und der Bundesminister für Inneres die operativen Aufgaben wahrnehmen.

Um ein hohes Sicherheitsniveau von Netz- und Informationssystemen zu erreichen, werden in diesem Bundesgesetz Maßnahmen vorgesehen. Neben den Verpflichtungen, die Betreiber wesentlicher Dienste, Anbieter digitaler Dienste sowie Einrichtungen des Bundes treffen, werden eine nationale Strategie für die Sicherheit von Netz- und Informationssystemen, Behördenzuständigkeiten und -befugnisse sowie Koordinationsstrukturen für den Bereich der Netz- und Informationssystemssicherheit und die Aufgaben und Anforderungen der Computer-Notfallteams festgelegt.

**Die Hauptgesichtspunkte sind im Einzelnen:**

- die Festlegung von Aufgaben und Behördenzuständigkeiten sowie Befugnissen zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen;
- die Festlegung einer nationalen Strategie für die Sicherheit von Netz- und Informationssystemen;
- die Ermittlung der vom Anwendungsbereich konkret erfassten Betreiber wesentlicher Dienste anhand der in einer Verordnung noch näher zu definierenden Teilsektoren und Faktoren;
- die Regelung von Verpflichtungen für die ermittelten Betreiber wesentlicher Dienste, die digitalen Diensteanbieter sowie Einrichtungen des Bundes. Diese haben einerseits angemessene Sicherheitsvorkehrungen für ihre Netz- und Informationssysteme vorzusehen und andererseits Sicherheitsvorfälle an die zuständigen Stellen zu melden;
- die Überprüfung geeigneter Sicherheitsvorkehrungen und der Einhaltung der Meldepflicht;
- die Einrichtung von Computer-Notfallteams und Festlegung der Aufgaben, die diesen zukommen sollen;
- die Regelung von Strukturen und Aufgaben im Falle der Cyberkrise;
- die Festlegung von Sanktionen bei Nichteinhaltung der nach diesem Bundesgesetz einzuhaltenden Pflichten.

Der Ausschuss für innere Angelegenheiten hat die gegenständliche Regierungsvorlage in seiner Sitzung am 29. November 2018 in Verhandlung genommen. An der Debatte beteiligten sich im Anschluss an die Ausführungen des Berichterstatters Abgeordneten Nikolaus **Prinz** die Abgeordneten Ing. Maurice **Androsch**, Eva-Maria **Himmelbauer**, BSc, Dr. Stephanie **Krisper** sowie der Bundesminister für Inneres Herbert **Kickl**.

Im Zuge der Debatte haben die Abgeordneten Werner **Amon**, MBA, Dr. Walter **Rosenkranz**, Angela **Lueger**, Kolleginnen und Kollegen einen Abänderungsantrag eingebracht, der wie folgt begründet war:

„Redaktionelles Versehen.“

Bei der Abstimmung wurde der in der Regierungsvorlage enthaltene Gesetzentwurf unter Berücksichtigung des oben erwähnten Abänderungsantrages der Abgeordneten Werner **Amon**, MBA, Dr. Walter **Rosenkranz**, Angela **Lueger**, Kolleginnen und Kollegen einstimmig beschlossen.

Als Ergebnis seiner Beratungen stellt der Ausschuss für innere Angelegenheiten somit den **Antrag**, der Nationalrat wolle dem **angeschlossenen Gesetzentwurf** die verfassungsmäßige Zustimmung erteilen.

Wien, 2018 11 29

**Nikolaus Prinz**

Berichterstatter

**Angela Lueger**

Obfrau

