3397/J XXVI. GP

Eingelangt am 24.04.2019

Anfrage

der Abgeordneten Claudia Gamon, MSc (WU), Douglas Hoyos-Trauttmansdorff, Kolleginnen und Kollegen

an den Bundesminister für Inneres

betreffend Schutz der kritischen Infrastruktur Österreichs

Im März 2019 wurde der größte Aluminium-Hersteller der Welt, die norwegische Firma Norsk Hydro, Opfer eines Cyberangriffs. Es handelte sich um eine sogenannte Ransomware-Attacke, bei der wertvolle Daten verschlüsselt werden. Teile der Produktion standen in der Folge still. Die Angreifer forderten Lösegeld. Als Folge der Attacke stieg der Aluminium-Preis. Norsk Hydro wäre nach der Kategorisierung des NIS-Gesetzes nicht Teil der kritischen Infrastruktur, ist aber – wie die Ereignisse nach dem Angriff zeigen – ein Unternehmen von größter Bedeutung.

Durch das 2018 beschlossene NIS-Gesetz wurde die Netz- und Informationssystem-Richtlinie der Europäischen Union endlich umgesetzt.

Durch diese sollen 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 (NIS) zu erreichen, nationale Behörden und Computer-Notfallteams benannt werden und bestimmte, für das Gemeinwohl wichtige private und öffentliche Anbieterinnen/Anbieter (Betreiberinnen/Betreiber wesentlicher Dienste und digitale Diensteanbieter) zu angemessenen Sicherheitsmaßnahmen und Meldung erheblicher Störfälle verpflichtet werden.

Betreiberinnen/Betreiber eines wesentlichen Dienstes sollen einen Dienst der im Anhang II der Netz- und Informationssystem-Richtlinie genannten und im Folgenden aufgelisteten Sektoren zur Verfügung stellen: Energie (Elektrizität, Erdöl, Erdgas), Verkehr (Luftverkehr, Schienenverkehr, Schifffahrt, Straßenverkehr), Bankwesen (Kreditinstitute), Finanzmarktinfrastrukturen (Betreiberinnen/Betreiber von Handelsplätzen, zentrale Gegenparteien), Gesundheitswesen (Einrichtungen der medizinischen Versorgung, einschließlich Krankenhäuser und Privatkliniken), Trinkwasserlieferung und -versorgung (Lieferantinnen/Lieferanten von 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 Diensteanbieterin-

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

Gemäß NIS-Gesetz ist der Bundeskanzler dazu verpflichtet, die Betreiber wesentlicher Dienste zu ermitteln und eine laufend aktualisierte Liste dieser zu führen, Sicherheitsvorkehrungen für diese festzulegen und diese per Bescheid zu informieren. Es ist anzunehmen, dass das Bundeskanzleramt diese Dinge in Kooperation mit dem Innenministerium erledigt.

Der Innenminister ist hingegen dazu verpflichtet eine zentrale Anlaufstelle (SPOC) für die Sicherheit von Netz- und Informationssystemen einzurichten und für die grenzüberschreitende Zusammenarbeit mit zuständigen Stellen anderer Mitgliedstaaten der Union bzw. Kooperationsgruppe und CSIRT-Netzwerk zu nutzen.

Nur Unternehmen, die Betreiber wesentlicher Dienste sind, sind bei Cyberattacken meldepflichtig und nur diese werden durch das BVT unterstützt. Nun umfasst die Liste jener Betreiber, die in diesem Zusammenhang als kritische Infrastruktur gelten, zwar vieles, allerdings nicht alles, was de facto zur kritischen Infrastruktur Österreichs zählt. So ist etwa die Trinkwasserversorgung erfasst, Abwassersysteme aber nicht. Ebenso fällt die Versorgung mit Nahrungsmitteln nicht grundsätzlich unter jene Betreiber, die durch das NIS-Gesetz gedeckt sind.

Unternehmen haben 3 Jahre Zeit, sich NIS-fit zu machen.

Eine zügige Verbesserung der Sicherheitsvorkehrungen gegen Angriffe auf die kritische Infrastruktur Österreichs sollte im Interesse der Versorgung der Bürgerinnen und Bürger mit lebenswichtigen Diensten Priorität haben.

Die unterfertigten Abgeordneten stellen daher folgende

Anfrage:

1. Hat Ihr Ressort seine Empfehlungen für die Liste von Betreibern kritischer Infrastruktur bereits an das BKA übermittelt?
   a) Wenn ja, wann?
   b) Wenn ja, wie viele Unternehmen enthielt diese Liste österreichweit? Bitte um Aufschlüsselung nach Bundesländern.
   c) Wenn nein, warum nicht?
2. Nach welchen Kriterien gehen Sie bei der Ermittlung von kritischer Infrastruktur vor?
   a) Wie argumentieren Sie, dass die Lebensmittelversorgung der Bevölkerung grundsätzlich nicht darunter fällt?
   b) Wie argumentieren Sie, dass Systeme zur Abwasser- und Müllentsorgung nicht darunter fallen?
3. Ist das BVT bereits ausreichend darauf vorbereitet, eine größere Anzahl von Unternehmen österreichweit beim Schutz ihrer Netzwerke zu unterstützen?
   a) Wenn ja, wie wird das gewährleistet?
   b) Wenn nein, warum nicht?

4. Haben Sie bereits eine zentrale Anlaufstelle (SPOC) für die Sicherheit von Netz- und Informationssystemen eingerichtet und ist diese bereits zum Austausch von Informationen mit anderen Mitgliedstaaten bereit?
   a) Wenn ja, seit wann?
   b) Wenn nein, warum nicht? Wann wir diese Einsatzbereit sein?
5. Wie ermittelten Sie die festgelegte Dauer der Übergangsfrist für Unternehmen? Während Unternehmen sicherlich einige Zeit brauchen, um sich umzustellen, tun Sie dies doch in ihrem eigenen Sicherheitsinteresse. Öffnet diese sehr lange Übergangsfrist Ihrer Analyse nicht zwischenzeitlich Sicherheitsrisiken Tür und Tor, die bei schnellerer Umsetzung vermeidbar wären?