3396/AB
vom 24.06.2019 zu 3397/J (XXVI.GP)

Bundesministerium
Inneres

bmi.gv.at

Dr. Wolfgang Peschorn
Bundesminister

Herrn
Präsidenten des Nationalrates
Mag. Wolfgang Sobotka
Parlament
1017 Wien

Geschäftszahl: BMI-LR2220/0331-II/2019

Wien, am 21. Juni 2019

Sehr geehrter Herr Präsident,

die Nationalräte Claudia Gamon, MSc (WU), Douglas Hoyos-Trauttmansdorff, Kolleginnen und Kollegen haben am 24. April 2019 unter der Nr. **3397/J** an den Herrn Bundesminister Herbert Kickl eine schriftliche parlamentarische Anfrage betreffend „Schutz der kritischen Infrastruktur Österreichs" gerichtet.

Diese Anfrage beantworte ich nach den mir vorliegenden Informationen wie folgt:

Zur Frage 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?*

Es besteht ein terminologischer und rechtlicher Unterschied zwischen den Betreibern kritischer Infrastruktur, deren Legaldefinition sich zum Beispiel in § 22 Abs. 1 Z 6 Sicherheitspolizeigesetz findet, und den Betreibern wesentlicher Dienste, deren Rahmen durch die NIS-Richtlinie bzw. das Netz- und Informationssystemsicherheitsgesetz (NISG) vorgegeben werden.

Aufbauend auf den österreichischen Programmen zum Schutz kritischer Infrastruktur (APCIP – Austrian Program for Critical Infrastructure Protection) wurde in den Jahren von 2008 und 2014 eine Liste von kritischen Infrastrukturen in Österreich durch das Bundeskanzleramt und das Bundesministerium für Inneres erstellt. Diese Liste dient dem Bundeskanzleramt als Rahmen zur Ermittlung der Betreiber wesentlicher Dienste nach dem Netz- und Informationssystemsicherheitsgesetz. Die Schwellenwerte zur Ermittlung der Betreiber wesentlicher Dienste wurden durch das Bundeskanzleramt gemeinsam mit dem Bundesministerium für Inneres und weiteren zuständigen Bundesministerien sowie unter Einbeziehung von Branchenexperten ermittelt und werden durch die NIS-Verordnung des zuständigen obersten Organs im Einvernehmen mit dem Bundesminister für Inneres festgelegt werden.

Die ACI (Austrian Critical Infrastructure) Liste enthält aktuell 377 Unternehmen, die als Betreiber kritischer Infrastruktur eingeordnet wurden.

Anzahl der Unternehmen, aufgeschlüsselt nach Bundesländern	
Burgenland	19
Kärnten	17
Niederösterreich	38
Oberösterreich	57
Salzburg	22
Steiermark	31
Tirol	22
Vorarlberg	13
Wien	158

Zur Frage 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?*

Bei der Einordnung von Unternehmen als Betreiber kritischer Infrastruktur wird auf die gesamtstaatliche oder regionale Bedeutung für die Daseinsvorsorge abgestellt. Dabei werden Kriterien wie die Zeit, in der sich ein Ausfall oder eine Störung eines Unternehmens auf die

Bevölkerung auswirkt, die Art der potenziellen Auswirkungen, das Ausmaß der Auswirkungen sowie bestehende Redundanzen miteinbezogen.

Sowohl die Lebensmittelversorgung als auch die Abwasser- und Müllentsorgung sind Teil der kritischen Infrastruktur und somit vom gesetzlichen Auftrag der zuständigen Organisationseinheiten umfasst.

Aus unionsrechtlicher Sicht ist derzeit jedoch nicht vorgesehen, diese Bereiche im Rahmen der NIS-Richtlinie zu adressieren. Auch das Netz- und Informationssystemsicherheitsgesetz als Umsetzung der NIS-Richtlinie sieht die Einbeziehung der beiden Bereiche nicht vor.

Zur Frage 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?*

Der vorbeugende Schutz kritischer Infrastruktur ist im Sicherheitspolizeigesetz normiert und wird nochmals im Polizeilichen Staatsschutzgesetz für den Bereich der Cybersicherheit besonders hervorgehoben. Dieser umfasst alle Betreiber kritischer Infrastruktur und daher grundsätzlich bereits die Betreiber wesentlicher Dienste. Zu diesem Zweck wurde im Bundesamt für Verfassungsschutz und Terrorismusbekämpfung das Cyber Security Center etabliert.

Die Maßnahmen zum vorbeugenden Schutz kritischer Infrastruktur umfassen unter anderem

- *Beratung und Awareness-Veranstaltungen bei Betreibern kritischer Infrastruktur;*
- *Bereitstellen von Lageinformationen;*
- *Aussenden von Frühwarnungen;*
- *technische Expertise (IT Forensik, Reverse Engineering) sowie*
- *Vernetzung mit den IT-Sicherheitsbeauftragten*

Zudem erfolgt eine enge Zusammenarbeit mit dem Referat Schutz kritischer Infrastruktur (SKI), welches auch neben dem Cyber Security Center Betreiber kritischer Infrastruktur in sicherheitsrelevanten Fragen betreut und unterstützt.

Auf Basis der Österreichischen Strategie für Cyber Sicherheit wurde der Innere Kreis der Operativen Koordinierungsstruktur (IKDOK) ins Leben gerufen und im Netz- und Informationssystemsicherheitsgesetz rechtlich normiert. Im Rahmen des IKDOK können Vorfälle koordiniert und von den Experten mehrerer Ressorts gemeinsam auf technischer und

operativer Ebene abgearbeitet werden. Diese Zusammenarbeit wird regelmäßig in realitätsnahen Planspielen gemeinsam mit Betreibern kritischer Infrastruktur beübt. Auch auf Ebene der strategischen Entscheidungsträger finden regelmäßig Planspiele statt.

Die Zusammenarbeit mit den sektorspezifischen Computer-Notfallteams innerhalb der Operativen Koordinierungsstruktur (OpKoord), sowie die Zusammenarbeit zwischen IKDOK und OpKoord, welche im Rahmen des staatlichen Cyberkrisenmanagements als technisch-operative Berater für strategische Entscheidungsträger auftreten, wurden durch das Netz- und Informationssystemsicherheitsgesetz auf rechtliche Grundlagen gestellt.

Zudem ist ein weiterer Ausbau des Cyber Security Centers vorgesehen.

Zur Frage 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 wird diese einsatzbereit sein?*

Ja. Die spezifischen Kontaktdaten der zentralen Anlaufstelle wurden vom Bundeskanzleramt am 18. Februar 2019 an die Europäische Kommission übermittelt. Durch Journaldienste und Rufbereitschaften ist neben der Erreichbarkeit während der Regeldienstzeit gewährleistet, dass der Single Point of Contact (SPOC) jederzeit einsatzbereit ist.

Zur Frage 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 zwischenzeitliche Sicherheitsrisiken Tür und Tor, die bei schnellerer Umsetzung vermeidbar wären?*

Eine Übergangsfrist ist im Netz- und Informationssystemsicherheitsgesetz nicht vorgesehen. Gemäß § 17 Abs. 3 Netz- und Informationssystemsicherheitsgesetz haben alle Betreiber wesentlicher Dienste mindestens alle drei Jahre nach Zustellung des Bescheids, mit dem diese als Betreiber wesentlicher Dienste ermittelt wurden den Nachweis, dass spezifische Sicherheitsvorkehrungen getroffen wurden, zu erbringen. Dieser dreijährige Prüfungszyklus ist eine Maximalfrist, die auch von den Betreibern wesentlicher Dienste unterschritten werden kann.

Ein Kausalzusammenhang zwischen der Länge des Prüfungszyklus und der Vermeidbarkeit von Sicherheitsrisiken ist nicht erkennbar. Das Auftreten von Sicherheitsrisiken ist dynamisch und nicht vorhersehbar. Das Thema Cybersicherheit nimmt bei Betreibern kritischer Infrastruktur bzw. potentiellen Betreibern wesentlicher Dienste einen hohen Stellenwert ein. Neben der bisherigen Selbstverpflichtung der Unternehmen im Bereich der Cybersicherheit wird nun durch das Netz- und Informationssystemsicherheitsgesetz eine gesetzliche Pflicht geschaffen.

Der im Netz- und Informationssystemsicherheitsgesetz gewählte Prüfungszyklus deckt sich zudem mit branchenüblichen Zertifizierungszyklen (z.B. ISO-Zertifizierungen).

Dr. Wolfgang Peschorn

REPUBLIK ÖSTERREICH AMTSSIGNATUR	Datum/Zeit	2019-06-24T11:37:35+02:00
	Aussteller-Zertifikat	CN=a-sign-corporate-light-02,OU=a-sign-corporate-light-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	1710479
Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at. Eine Verifizierung des Ausdruckes kann bei der ausstellenden Behörde/Dienststelle erfolgen.	
Hinweis	Dieses Dokument wurde amtssigniert.	

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2019-06-24T11:41:21+02:00
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel
Hinweis	Dieses Dokument wurde elektronisch besiegelt.	