11873/AB
vom 14.11.2022 zu 12147/J (XXVII. GP)

Bundesministerium
Land- und Forstwirtschaft,
Regionen und Wasserwirtschaft

bml.gv.at

Mag. Norbert Totschnig, MSc
Bundesminister für Land- und Forstwirtschaft,
Regionen und Wasserwirtschaft

Herrn
Mag. Wolfgang Sobotka
Präsident des Nationalrats
Parlament
1017 Wien

Geschäftszahl: 2022-0.661.023

Ihr Zeichen: BKA - PDion
(PDion)12147/J-NR/2022

Wien, 14. November 2022

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Katharina Kucharowits, Kolleginnen und Kollegen haben am 14.09.2022 unter der Nr. **12147/J** an mich eine schriftliche parlamentarische Anfrage betreffend „Vorbereitung auf Cyberangriffe innerhalb der österreichischen Bundesverwaltung“ gerichtet.

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

Zur Frage 1:

- Gab es in Ihrem Ressort bereits Cyberangriffe?
  a. Falls ja, bitte um detaillierte Schilderung des Angriffs/der Angriffe, welche Schäden daraus resultierten und welche Gegenmaßnahmen ergriffen wurden?

Das Bundesministerium für Land- und Forstwirtschaft, Regionen und Wasserwirtschaft ist, so wie auch andere Ministerien und Unternehmen, kontinuierlichen Angriffsversuchen im Cyberraum ausgesetzt. Im Bundesministerium für Land- und Forstwirtschaft, Regionen und Wasserwirtschaft konnten bisher derartige Angriffsversuche sowie Schäden und Ausfälle erfolgreich von den eigenen Schutzsystemen abgewehrt werden. Aus Gründen der IT-Sicherheit des Ressorts können nähere Details nicht bekannt gegeben werden.

Zur Frage 2:

- Welche Rolle und welche konkreten Aufgaben fallen Ihrem Ressort in der gesamtstaatlichen Bekämpfung von Cyberkriminalität zu?

Die Aufgabenwahrnehmung zur Bekämpfung der Cyberkriminalität obliegt dem Bundesministerium für Inneres. Weiterführend darf in Bezug auf Cybersicherheit auf die Beantwortung der parlamentarischen Anfragen zu dieser Fragestellung durch das Bundeskanzleramt (Nr. 12156/J), das Bundesministerium für Inneres (Nr. 12157/J) und das Bundesministerium für Landesverteidigung (Nr. 12148/J) verwiesen werden.

Zur Frage 3:

- Ergreift Ihr Ressort aktiv konkrete Maßnahmen, um sich präventiv gegen Cyberattacken und Cyberkriminalität angemessen zu schützen?
  a. Falls ja, welche Maßnahmen sind das im Detail?
  b. Falls ja, wird in der Vorbereitung auf einen potenziellen Cyberangriff auch die Expertise externer Expert*innen, etwas Personen auf Wissenschaft oder Zivilgesellschaft, hinzugezogen?
  c. Falls nein, warum gibt es keine Pläne, sich für den Ernstfall eines potenziellen Cyberangriffs zu schützen?

Im Bundesministerium für Land- und Forstwirtschaft, Regionen und Wasserwirtschaft werden zur Erhöhung der Cybersicherheit Maßnahmen getroffen, um sich angemessen vor Cyberattacken und Cyberkriminalität zu schützen. Das Bundesministerium für Land- und Forstwirtschaft, Regionen und Wasserwirtschaft arbeitet dafür auch mit externen Fachleuten zusammen. Weiters fließen die Erkenntnisse aus dem gesamtstaatlichen Lagebildprozess mit ein und werden gemeinsam mit dem technischen Personal des Ressorts zeitnahe umgesetzt. Aus Gründen der IT-Sicherheit des Ressorts können nähere Details nicht bekannt gegeben werden.

Zur Frage 4:

- Durch die unterschiedlichen Zuständigkeitsbereiche aller Ressorts der Bundesregierung ergeben sich auch unterschiedliche Risiken in Bezug auf Cyberangriffe, beispielsweise wird es im Bundesministerium für europäische und internationale Angelegenheiten aller Wahrscheinlichkeit nach andere Herausforderungen und Risiken in Bezug auf Cyberkriminalität geben als beispielweise im Bundesministerium für Justiz.

a. Gab es eine ressortspezifische Risikoanalyse in Ihrem Ressort?
    i. Falls nein, warum nicht?
b. Welche konkreten Maßnahmen setzen Sie, um den spezifischen Risiken Ihres Ressorts gerecht zu werden?

Das Bundesministerium für Land- und Forstwirtschaft, Regionen und Wasserwirtschaft betreibt ein Informations-Sicherheits-Management-System (ISMS) nach „best practice“ und führt in diesem Umfang Risikoanalysen und zyklisch eine Schutzbedarfsanalyse durch. Darüber hinaus darf auf die Beantwortung der Fragen 1 und 3 verwiesen werden.

Zur Frage 5:

- Gibt es eine Person oder einen Personenkreis in Ihrem Ressort, die dezidiert als „Cybersichterheitsbeauftrage(r)" fungiert/fungieren?
    a. Falls ja, wie viele Personen sind zum Zeitpunkt der Beantwortung dieser Anfrage im Bereich Cybersecurity in Ihrem Ressort beschäftigt?
    b. Falls ja, über welche Expertise verfügt/verfügen diese Person(en)?
    c. Falls nein, warum gibt es keine(n) „Cybersicherheitsbeauftrage(n)" in Ihrem Ressort?

Dezidiert steht für diese Funktion keine Person zur Verfügung. Innerhalb des Bundesministerium für Land- und Forstwirtschaft, Regionen und Wasserwirtschaft werden diese Agenden vom Abteilungsleiter der IKT-Abteilung und Chief-Information-Officer (CIO) in Kooperation mit dem Chief-Digital-Officer (CDO) des Ressorts wahrgenommen. Aus Gründen der Aufrechterhaltung eines hohen Schutzniveaus innerhalb des Ressort wird von einer näheren Beschreibung der Expertise Abstand genommen.

Zur Frage 6:

- Bietet Ihr Ressort spezielle Trainings, Webinare, Kurse etc. an, um alle Mitarbeiter*innen im Umgang mit potenziellen Cyberangriffen und der daraus resultierenden Gefahrenlage zu sensibilisieren?

Im Bundesministerium für Land- und Forstwirtschaft, Regionen und Wasserwirtschaft werden für Mitarbeiterinnen und Mitarbeiter zyklisch Awareness-Schulungen durchgeführt. Darüber hinaus werden aktuelle Informationen anlassbezogen über das Intranet des Bundesministeriums für Land- und Forstwirtschaft, Regionen und Wasserwirtschaft zum Thema Cybersicherheit bereitgestellt.

Zur Frage 7:

- Der Rechnungshofbericht bemängelt unter anderem, dass Krisen-, Kontinuitäts- und Einsatzpläne in Bezug auf Cybersicherheit gänzlich fehlen. Zum Zeitpunkt der Beantwortung dieser Anfrage, wurden diese von Ihrem Ressort mittlerweile erstellt?
  a. Falls ja, wurden zur Erstellung dieser Pläne auch externe Expert*innen hinzugezogen?
  b. Falls nein, wann ist mit der Fertigstellung dieser Pläne in Ihrem Ressort zu rechnen?

Im Bundesministerium für Land- und Forstwirtschaft, Regionen und Wasserwirtschaft werden sowohl technische als auch organisatorische Vorkehrungen getroffen, um alle gesetzlichen Rahmenbedingungen zu erfüllen und die Aufrechterhaltung des ordentlichen Betriebes zu gewährleisten. Darüber hinaus darf auf die Beantwortung der parlamentarischen Anfragen zu dieser Frage durch das Bundeskanzleramt (Nr. 12156/J), Bundesministerium für Inneres (Nr. 12157/J), Bundesministerium für europäische und internationale Angelegenheiten (Nr. 12154/J) und Bundesministerium für Landesverteidigung (Nr. 12148/J) verwiesen werden.

Zur Frage 8:

- Der Rechnungshof sah zudem die Etablierung eines permanent verfügbaren Cyber-Einsatzteam („Rapid Response Team") sowie die Schaffung eines ebenso permanenten Cyber-Lagezentrums zur Bearbeitung von Notfällen als essentiell. Wurden dieses Einsatzteam und das Lagezentrum zum Zeitpunkt der Beantwortung dieser Anfrage bereits geschaffen?
  a. Falls ja, in welchem Ressort sind diese Strukturen angesiedelt und der Zuständigkeit welcher/welchen Bundesministerin/Bundesministers unterliegen diese?

Für das Rapid Response Team darf auf die Beantwortung der parlamentarischen Anfrage Nr. 12148/J durch das Bundesministerium für Landesverteidigung und hinsichtlich des Cyberlagezentrums auf die Beantwortung durch das Bundesministerium für Inneres (Nr. 12157/J) verwiesen werden.

Zur Frage 9:

- Zudem forderte der Rechnungshof ein regelmäßig zu erstellendes Cyber-Lagebild, um laufende Bedrohungen und potentielle Gefahrenquellen schneller und effektiver zu identifizieren. Wird ein solches Cyberlagebild in Ihrem Ressort zum Zeitpunkt der Beantwortung dieser Anfrage bereits regelmäßig erstellt?
  a. Falls ja, seit wann wird ein solches Lagebild in Ihrem Ressort erstellt und in welchen Abständen findet das statt?
  b. Falls nein, warum wird bisher kein Cyber-Lagebild in Ihrem Ressort erstellt und ab wann planen Sie, ein solches regelmäßig zu erstellen?

In Österreich erstellt der mit der Österreichischen Strategie für Cybersicherheit 2013 eingesetzte und mit dem NISG festgeschriebene Innere Kreis der Operativen Koordinierungsstruktur (IKDOK) das gesamtstaatliche Cyberlagebild. Der IKDOK ist eine interministerielle Struktur zur Koordination auf der operativen Ebene im Bereich der Sicherheit von Netz- und Informationssystemen, bestehend aus Vertretern des Bundeskanzlers, des Bundesministers für Inneres, der Bundesministerin für Landesverteidigung und des Bundesministers für Europa, Integration und Äußeres. Er tritt regulär wöchentlich zusammen und erstellt seit 2018 monatlich das gesamtstaatliche IKDOK-Lagebild, welches allen Bundesministerien und den obersten Organen zur Verfügung gestellt wird. Das daraus abgeleitete OPKOORD-Lagebild (Operative Koordinierungsstruktur) wird den gemäß NISG bescheideten Stellen übermittelt. Zusätzlich werden Sonderlagebilder anlassbezogen zum Thema Cybersicherheit produziert und distribuiert.

Mag. Norbert Totschnig, MSc

REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR LAND- UND FORSTWIRTSCHAFT, REGIONEN UND WASSERWIRTSCHAFT @ AMTSSIGNATUR	Unterzeichner	Bundesministerium für Land- und Forstwirtschaft, Regionen und Wasserwirtschaft
	Datum/Zeit	2022-11-14T14:34:31+01:00
	Aussteller-Zertifikat	CN=a-sign-corporate-07,OU=a-sign-corporate-07,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	1921487807
Hinweis	Dieses Dokument wurde amtssigniert.	
Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur und des Ausdrucks finden Sie unter: http://www.lebensministerium.at/amtssignatur	

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2022-11-14T14:37:32+01:00
	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.	