11872/AB
vom 14.11.2022 zu 12150/J (XXVII. GP)

Bundesministerium
Justiz

bmj.gv.at

Dr.in Alma Zadić, LL.M.
Bundesministerin für Justiz

Herrn
Mag. Wolfgang Sobotka
Präsident des Nationalrats
Parlament
1017 Wien

Geschäftszahl: 2022-0.660.663

Ihr Zeichen: BKA - PDion (PDion)12150/J-NR/2022

Wien, am 14. November 2022

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Katharina Kucharowits, Kolleginnen und Kollegen haben am 14. September 2022 unter der Nr. **12150/J-NR/2022** 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 Justiz (BMJ) sieht sich - wie andere Ministerien, Unternehmen und Bildungseinrichtungen auch – kontinuierlichen Angriffsversuchen im Cyberraum ausgesetzt. Im BMJ konnten bisher derartige Angriffsversuche abgewehrt sowie Schäden und Ausfälle hintangehalten werden. Die IKT-Sicherheit wird im Bund als fortlaufender Prozess verstanden. Dementsprechend werden, unterstützt durch die Bundesrechenzentrum GmbH, Governmental Computer Emergency Response Team (GovCERT) und den Innerer Kreis der operativen Koordinierungsstruktur (IKDOK),

kontinuierlich Anpassungen der IKT-Sicherheitsstruktur vorgenommen, um auch auf sich ändernde Bedrohungen reagieren zu können.

Zur Frage 2:

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

Den Gerichten und Staatsanwaltschaften obliegt gemeinsam mit dem BMI die Strafverfolgung bei Cyberkriminalitätsdelikten. Dem BMJ kommt die Zuständigkeit für die Legistik der gerichtlichen Straftatbestände iZm Cyberkriminalität und der korrespondierenden Strafverfolgung zu.

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 BMJ werden zur Erhöhung der Cybersicherheit Maßnahmen auf strategischer, operativer und technischer Ebene in den Bereichen Prävention, Absicherung, Erkennung und Incident Response auf dem Stand der Technik ergriffen. Das BMJ arbeitet hier auch mit externen Expert:innen zusammen. Erkenntnisse aus dem gesamtstaatlichen Lagebildprozess werden in Zusammenarbeit mit Bundesrechenzentrum zeitnahe umgesetzt.

Darüber hinaus muss von der detaillierten Auflistung der Maßnahmen zur Erhöhung bzw. dem Erhalt eines hohen IKT- Sicherheitsniveaus gemäß des Netz- und Informationssystemsicherheits-gesetz, BGBl. I Nr. 111/2018 (NISG), oder aber auch der Auflistung einzelner im Einsatz befindlicher Cybersicherheitsprodukte im Hinblick auf die Sicherung der Effektivität der Schutzmaßnahmen Abstand genommen 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?

Im Zuge der Umsetzung der NIS RL (Richtlinie (EU) 2016/1148, über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystem) durch das NISG (Netz- und Informationssystemsicherheitsgesetz, BGBl. I Nr. 111/2018) wurden die kritischen Dienste identifiziert und mit entsprechenden Prozessen zur Aufrechterhaltung bzw. zur Weiterführung der Kernaufgaben nach Systemausfällen hinterlegt.

Darüber hinaus wird auf die Beantwortung der Fragen 1 und 3 verwiesen.

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?

Im Bundesministerium für Justiz trägt der Chief Information Security Officer (CISO) trägt als Durchführungsverantwortlicher des Informationssicherheitsmanagement-Prozesses die Gesamtverantwortung für die IT-Sicherheit im Ressort. Zu seinen Aufgaben gehören die Stärkung des Bewusstseins für IT-Sicherheit im Managementbereich, die Einbringung von IT-Sicherheits-Projektanträgen sowie die Gewährleistung der IT-Sicherheit im laufenden Betrieb.

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?*

Ja, im BMJ werden allen Mitarbeiter:innen im Wege des Serviceportals Schulungen zum Thema der „IKT-Benutzungsrichtlinien“ zur Verfügung gestellt, im Rahmen derer insbesondere auch IT-Sicherheitsthemen adressiert werden.

Zu den Fragen 7 und 8:

- *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?*
- *8. Der Rechnungshof sah zudem die Etablierung eines permanent verfügbaren Cyber-Einsatzteam („Rapid Response Team") sowie die Schaffung eines ebenso permanenten Cyberlagezentrums 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?*

Die Erstellung von Krisen-, Kontinuitäts- und Einsatzplänen für das Cyber-Krisenmanagement fällt in die Zuständigkeit des BKA; diesbezüglich darf auf den Bericht „Österreichische Strategie für Cybersicherheit - Bundeskanzleramt Österreich (ÖSCS 2021)“, der den strategischen Rahmen für die nationale Cybersicherheitspolitik bildet, verwiesen werden. Fragen zum Rapid Response Team fallen in die Zuständigkeit des BMLV, solche zum Cyberlagezentrum in die des BMI.

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 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 Vertreter:innen des Bundeskanzlers, des Bundesministers für Inneres, des Bundesministers für Landesverteidigung und des Bundesministers für Europa, Integration und Äußeres.

Der IKDOK tritt regulär wöchentlich zusammen und erstellt seit 2018 monatlich das gesamtstaatliche IKDOK-Lagebild, welches den Ministerien und den obersten Organen zur Verfügung gestellt wird. Das daraus abgeleitete OPKOORD-Lagebild (Operative Koordinierungsstruktur) wird den gemäß Netz- und Informationssystemsicherheitsgesetz (NISG) bescheideten Stellen übermittelt. Zusätzlich werden Sonderlagebilder anlassbezogen zum Thema Cybersicherheit produziert und distribuiert.

Dr.in Alma Zadić, LL.M.

REPUBLIK ÖSTERREICH BMJ SIGNATUR	**Datum/Zeit**	2022-11-14T14:30:24+01:00
	Hinweis	Dieses Dokument wurde elektronisch signiert. Auch ein Ausdruck dieses Dokuments hat die Beweiskraft einer öffentlichen Urkunde.
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: www.signaturpruefung.gv.at Informationen zur Prüfung des Ausdrucks finden Sie unter: www.justiz.gv.at/amtssignatur

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2022-11-14T14:37:22+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.	