11880/AB
vom 14.11.2022 zu 12155/J (XXVII. GP)

Bundesministerium
Kunst, Kultur,
öffentlicher Dienst und Sport

bmkoes.gv.at

Mag. Werner Kogler
Vizekanzler
Bundesminister für Kunst, Kultur,
öffentlichen Dienst und Sport

Herrn
Präsidenten des Nationalrates
Mag. Wolfgang Sobotka
Parlament
1017 Wien

Geschäftszahl: 2022-0.678.860

Wien, am 14. November 2022

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Katharina Kucharowits, Genossinnen und Genossen haben am 14. September 2022 unter der Nr. **12155/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:

Zu 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 Kunst, Kultur, öffentlichen Dienst und Sport (BMKÖS) sieht sich, wie auch andere Ministerien, Unternehmen und Bildungseinrichtungen kontinuierlichen Angriffsversuchen im Cyberraum ausgesetzt. Im BMKÖS konnten bisher derartige Angriffsversuche abgewehrt sowie Schäden und Ausfälle weitgehend hintangehalten werden.

Die IKT-Sicherheit wird im Bund als fortlaufender Prozess verstanden. Dementsprechend werden, unterstützt durch das Governmental Computer Emergency Response Team (GovCERT) und den Inneren Kreis der operativen Koordinierungsstruktur (IKDOK), kontinuierlich Anpassungen der IKT-Sicherheitsstruktur vorgenommen um auch auf sich ändernde Bedrohungen reagieren zu können.

Darüber hinaus darf ich auf meine Ausführungen zu der an mich gerichteten parlamentarischen Anfrage Nr. 11857/J vom 8. Juli 2022 verweisen.

Zu Frage 2:

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

Die Aufgabenwahrnehmung zur gesamtstaatlichen Bekämpfung der Cyberkriminalität obliegt dem Bundesministerium für Inneres und dem Bundesministerium für Justiz sowie für Cybersicherheit dem Bundeskanzleramt. Ich darf daher auf die diesbezüglichen Beantwortungen der parlamentarischen Anfragen durch den Herrn Bundesminister für Inneres (Nr. 12157/J), die Frau Bundesministerin für Justiz (Nr. 12150/J) und den Herrn Bundeskanzler (Nr. 12156/J) verweisen.

Zu 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, etwa Personen aus Wissenschaft oder Zivilgesellschaft, hinzugezogen?*
    c. *Falls nein, warum gibt es keine Pläne, sich für den Ernstfall eines potenziellen Cyberangriffs zu schützen?*

Im BMKÖS 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 BMKÖS arbeitet hier auch mit externen Expert:innen zusammen. Erkenntnisse aus dem gesamtstaatlichen Lagebildprozess werden in Zusammenarbeit mit den Techniker:innen des Ressorts zeitnahe umgesetzt.

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

Zu 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 BMKÖS wurde zum Zweck der systemischen Risikoanalyse ein ISMS (Information Security Management System) aufgebaut. 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 darf ich auf meine Ausführungen zu den Fragen 1 und 3 verweisen.

Zu 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?*

Ja, wobei im BMKÖS die Bezeichnung „IT-Sicherheitsbeauftragte/r“ verwendet wird und dabei auch die Zuständigkeit für Cybersicherheit mitumfasst ist. Die erforderliche Expertise und Qualifikation ist gegeben. Darüber hinaus sind auch sämtliche IT-Mitarbeiter:innen für Cybersicherheit zuständig.

Es wird um Verständnis gebeten, dass von einer detaillierteren Bekanntgabe von Informationen zu diesem Personenkreis Abstand genommen wird, damit daraus keine konkreten Rückschlüsse auf die Leistungsfähigkeit in diesem sensiblen Tätigkeitsfeld gezogen werden können und die damit in Verbindung stehende Aufgabenerfüllung nicht erschwert bzw. in gewissen Bereichen unmöglich gemacht wird.

Zu 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 BMKÖS werden alle Mitarbeiter:innen diesbezüglich geschult, sowohl in Präsenz als auch online und über E-Learning. Auch erfolgen laufend Informationen über die verschiedensten Kanäle (E-Mails, Intranet, Online- und Präsenztrainings, Informationsveranstaltungen etc.). Auf hohe Awareness der Mitarbeiter:innen wird großer Wert gelegt, zu den Awarenessmaßnahmen gibt es auch Audits.

Zu den Fragen 7 bis 9:

- *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?*
- *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?*

- *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?*

Zu diesen Fragen darf, was das Cyberlagebild betrifft, auf die Beantwortung des Herrn Bundeskanzlers zur parlamentarischen Anfrage Nr. 12156/J, hinsichtlich des Cyberlagezentrums auf die Ausführungen des Herrn Bundesministers für Inneres zur parlamentarischen Anfrage Nr. 12157/J und hinsichtlich des Rapid Response Teams auf die Beantwortung der Frau Bundesministerin für Landesverteidigung zu der an sie gerichteten parlamentarischen Anfrage Nr. 12148/J verwiesen werden.

Ergänzend dazu darf mitgeteilt werden, dass im BMKÖS Notfallpläne für Anwendungen und Notfallpläne für bestimmte Cyberangriffe unter Beiziehung externer Expert:innen erstellt wurden.

Mag. Werner Kogler

REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR KUNST, KULTUR, ÖFFENTLICHEN DIENST UND SPORT @ AMTSSIGNATUR	Unterzeichner	Bundesministerium für Kunst, Kultur, öffentlichen Dienst und Sport
	Datum/Zeit	2022-11-14T19:43:46+01:00
	Aussteller-Zertifikat	CN=a-sign-corporate-05,OU=a-sign-corporate-05,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	2099471880
	Hinweis	Dieses Dokument wurde amtssigniert.
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: http://www.signaturpruefung.gv.at

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2022-11-15T10:00:10+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.	