11869/AB
vom 14.11.2022 zu 12156/J (XXVII. GP)

Bundeskanzleramt

bundeskanzleramt.gv.at

Karl Nehammer
Bundeskanzler

Herrn
Mag. Wolfgang Sobotka
Präsident des Nationalrats
Parlament
1017 Wien

Geschäftszahl: 2022-0.660.251

Wien, am 14. November 2022

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Kucharowits, Kolleginnen und Kollegen haben am 14. September 2022 unter der Nr. **12156/J** eine schriftliche parlamentarische Anfrage betreffend „Vorbereitung auf Cyberangriffe innerhalb der österreichischen Bundesverwaltung“ an mich gerichtet.

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

Zu Frage 1:

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 Bundeskanzleramt sieht sich, wie auch andere Ministerien, Unternehmen und Bildungseinrichtungen kontinuierlichen Angriffsversuchen im Cyberraum ausgesetzt. Im Bundeskanzleramt 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 Innerer 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 die Beantwortung der parlamentarischen Anfrage Nr. 11854/J vom 8. Juli 2022 verweisen.

Zu Frage 2:

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

Hinsichtlich der Aufgabenwahrnehmung zur Bekämpfung der Cyberkriminalität darf ich auf die Beantwortung der parlamentarischen Anfragen Nr. 12150/J vom 14. September 2022 durch die Bundesministerin für Justiz und Nr. 12157/J vom 14. September 2022 durch den Bundesminister für Inneres verweisen.

Im Bundeskanzleramt ist die Abteilung I/8 für Cybersicherheit zuständig. Konkret liegen dort gemäß Geschäftseinteilung folgende Aufgabenwahrnehmungen:

- Angelegenheiten für strategische Kommunikations-, Netzwerk- und Informationssystemsicherheit,
- Koordination von nationalen und internationalen Cyberthemen,
- Führen des NIS Büros sowie Angelegenheiten der Umsetzung der NIS Richtlinie,
- Leitung des GOVCERTs,
- Koordination von gesamtstaatlichen Cyberübungen sowie Angelegenheiten des Ordnungspolitischen Rahmens für Cybersicherheit;
- Angelegenheiten des Cyber Stakeholdermanagements und Koordination der Cyber Security Steuerungsgruppe (CSS)
- Interne Cybersicherheit

Zu Frage 3:

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 Bundeskanzleramt 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 Bundeskanzleramt arbeitet hier auch mit externen Expertinnen und Experten zusammen. Erkenntnisse aus dem gesamtstaatlichen Lagebildprozess werden in Zusammenarbeit mit den Technikerinnen und Technikern des Ressorts zeitnahe umgesetzt.

Darüber hinaus muss von der detaillierten Auflistung der Maßnahmen zur Erhöhung bzw. dem Erhalt eines hohen IKT- Sicherheitsniveaus gemäß des Netz- und Informationssystemsicherheitsgesetz, 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.

Zu Frage 4:

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 Bundeskanzleramt wurde zum Zweck der systemischen Risikoanalyse ein Information Security Management System (ISMS) aufgebaut. Im Zuge der Umsetzung der NIS-RL (Richt-

linie (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.

Zu Frage 5:

5. *Gibt es eine Person oder einen Personenkreis in Ihrem Ressort, die dezidiert als „Cybersichterheitsbeauftrage(r)" fungiert/fungieren?*
   a. *Falls ja, über welche Expertise verfügt/verfügen diese Person(en)?*
   b. *Falls nein, warum gibt es keine(n) „Cybersicherheitsbeauftrage(n)" in Ihrem Ressort?*

Der Leiter der Abteilung Cybersicherheit nimmt die Rolle des Chief Information Security Officer (CISO) im Bundeskanzleramt wahr. Der CISO trägt als Durchführungsverantwortlicher des Informationssicherheitsmanagement-Prozesses die Gesamtverantwortung für das Qualitätsmanagement der IT-Sicherheit im Ressort.

Zu seinen Aufgaben gehören die Stärkung des Bewusstseins für IT-Sicherheit im Managementbereich, die Einbringung von IT-Sicherheits-Projektanträgen, die Gewährleistung der IT-Sicherheit im laufenden Betrieb sowie die Verwaltung der für den Informationssicherheitsmanagement -Prozess zur Verfügung stehenden Ressourcen.

Zu Frage 6:

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 Bundeskanzleramt werden allen Mitarbeiterinnen und Mitarbeiter im Wege des Serviceportals Schulungen zum Thema „Cybersicherheit Awareness" zur Verfügung gestellt. Darüber hinaus informiert die Abteilung I/8 routinemäßig und proaktiv zu Cybersicherheitsthemen inklusive konkreter Handlungsanleitungen.

Zu Frage 7:

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?*

Das Bundeskanzleramt wird im Rahmen seiner Zuständigkeit als vorsitzführende Stelle der Cyber Sicherheit Steuerungsgruppe (CSS) nach Vorliegen der in Zusammenhang mit der Empfehlung zur Erarbeitung von Krisen-, Kontinuitäts- und Einsatzplänen für das Cyber-Krisenmanagement stehenden und derzeit im Rahmen der IKDOK unter Federführung des Bundesministeriums für Inneres in Ausarbeitung befindlichen Standard Operating Procedures entsprechende koordinierende Schritte setzen.

Zu Frage 8:

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 ich auf die Beantwortung der Anfrage Nr. 12148/J vom 14. September 2022 durch die Bundesministerin für Landesverteidigung, für das Cyberlagezentrum auf die Beantwortung der parlamentarischen Anfrage Nr. 12157/J vom 14. September 2022 durch den Bundesminister für Inneres verweisen.

Zu Frage 9:

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 Vertretern des Bundeskanzleramts, des Bundesministeriums für Inneres, des Bundesministeriums für Landesverteidigung und des Bundesministeriums für europäische und internationale Angelegenheiten.

Er 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 NISG zuständigen Stellen übermittelt. Zusätzlich werden Sonderlagebilder anlassbezogen zum Thema Cybersicherheit produziert und distribuiert.

Zu Frage 10:

10. Schließlich sieht der Rechnungshof bei den „Personalressourcen, um die Cyber-Sicherheit aufrecht zu erhalten" konkret im Bundeskanzleramt großen Aufholbedarf.

a. Zum Ende des vom Rechnungshof überprüften Zeitraums, nämlich Mai 2021, wie viele Personen waren im Bundeskanzleramt dezidiert im Bereich Cybersicherheit tätig?

b. Wurde zum Zeitpunkt der Beantwortung dieser Anfrage bereits zusätzliches Personal im Bereich der Cybersicherheit im Bundeskanzleramt aufgenommen?

i. Falls ja, wie viele Personen sind zum Zeitpunkt der Beantwortung dieser Anfrage im Bundeskanzleramt im Bereich Cybersicherheit tätig?

ii. Falls nein, wann planen Sie, mehr Personen für den Bereich Cybersicherheit im Bundeskanzleramt einzustellen?

Im Bundeskanzleramt ist die Abteilung I/8 für den Bereich Cybersicherheit zuständig. Mit Ende der Prüfung durch den Rechnungshof wurde kein zusätzliches Personal im Bereich Cybersicherheit aufgenommen. Auf EU-Ebene werden weitere den Cyberbereich betreffende Richtlinien ausgearbeitet, welche in weiterer Folge zusätzliche Aufnahmen erforderlich machen werden.

Von einer ausführlichen Beantwortung dieser Fragen über die dargestellten Sachverhalte hinaus muss aufgrund der Verpflichtung zur Wahrung der Amtsverschwiegenheit, insbeson-

dere aufgrund des Interesses der Aufrechterhaltung der öffentlichen Ordnung und Sicherheit Abstand genommen werden. Durch die Bekanntgabe von Personalzahlen im Bereich der Cybersicherheit meines Ressorts, könnten konkrete Rückschlüsse auf die Leistungsfähigkeit in diesem sensiblen Tätigkeitsfeld gezogen und die damit in Verbindung stehende Aufgabenerfüllung wesentlich erschwert bzw. in gewissen Bereichen unmöglich gemacht werden.

Karl Nehammer

REPUBLIK ÖSTERREICH BUNDESKANZLERAMT AMTSSIGNATUR	Unterzeichner	serialNumber=932783133,CN=Bundeskanzleramt,C=AT
	Datum/Zeit	2022-11-14T10:27:44+01:00
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at Informationen zur Prüfung des Ausdrucks finden Sie unter: https://www.bundeskanzleramt.gv.at/verifizierung
	Hinweis	Dieses Dokument wurde amtssigniert.

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2022-11-14T10:37:45+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.	