bmi.gv.at

Bundesministerium
Inneres

Mag. Gerhard Karner
Bundesminister

Herrn
Präsidenten des Nationalrates
Mag. Wolfgang Sobotka
Parlament
1017 Wien

Geschäftszahl: 2022-0.719.490

Wien, am 14. November 2022

Sehr geehrter Herr Präsident!

Die Abgeordnete zum Nationalrat Katharina Kucharowits, Genossinnen und Genossen haben am 14. September 2022 unter der Nr. PA 12157/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?*

Angriffsversuche und Angriffe selbst können aufgrund der dynamischen Bedrohungslage nie ausgeschlossen werden. Aufgrund vorhandener präventiver und reaktiver Sicherheitsmaßnahmen (siehe Antwort zu Frage 3) konnten bislang keine erfolgreichen Angriffe mit daraus entstandener Schadenswirkung festgestellt werden.

Zur Frage 2:

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

Die Bekämpfung der Cyberkriminalität fällt BMI-intern in kriminalpolizeilichen Angelegenheiten in den Zuständigkeitsbereich des Cybercrime Competence Centers (C4) im Bundeskriminalamt, dessen Kernkompetenz eben darin besteht. Das C4 wurde 2011 als eigene Einheit innerhalb der Abteilung 5 Kriminalpolizeiliche Assistenzdienste des Bundeskriminalamts etabliert und als bundesweite Zentralstelle konzipiert. Es ist zugleich nationale und internationale Koordinierungs-, Ermittlungs- und Meldestelle im Zusammenhang mit Cybercrime im engeren Sinn sowie für die elektronische Beweismittelsicherung und deren Auswertung zuständig. Das C4 dient aber auch allen Polizeidienststellen als wichtige Drehscheibe und Koordinationspunkt bei landesweiten und international auftretenden Phänomenen und hiermit zusammenhängenden Ermittlungen. Es gliedert sich mit seinen Schnittstellen zur Direktion Staatsschutz und Nachrichtendienst (DSN) als wesentlicher Bestandteil in die Strategie des Bundeskanzleramtes ein. In diesem Zusammenhang ist das C4 Teil des Inneren Kreises der operativen Koordinierungsstrukturen (IKDOK). Weiterführende Informationen zur Cybersicherheit können unter https://www.bundeskanzleramt.gv.at/themen/cyber-sicherheit-egovernment.html gefunden werden. Darüber hinaus bestehen Strukturen ebenso auf Landesebene (eigener Assistenzbereich IT-Beweissicherung der Landeskriminalämter) und in den Bezirken (Bezirks IT-Ermittler).

Die Direktion Staatsschutz und Nachrichtendienst spielt im Rahmen der Aufgabenerfüllung nach §§ 6 Abs 2 und 3 SNG (vorbeugender Schutz vor verfassungsgefährdenden Angriffen), sowie im Sicherheitspolizeigesetz und der Strafprozessordnung bei rechtswidriger Verwirklichung eines Tatbestandes nach §§ 118a, 119, 119a, 126a, 126b oder 126c StGB gegen verfassungsmäßige Einrichtungen und ihre Handlungsfähigkeit (§ 22 Abs. 1 Z 2 SPG) oder kritische Infrastrukturen (§ 22 Abs. 1 Z 6 SPG) eine zentrale Rolle. Den Organisationseinheiten des Verfassungsschutzes obliegt außerdem zur Vorbeugung verfassungsgefährdender Angriffe, insbesondere auf dem Gebiet der Cybersicherheit, die Förderung der Bereitschaft und Fähigkeit des Einzelnen, sich über eine Bedrohung seiner Rechtsgüter Kenntnis zu verschaffen und Angriffen entsprechend vorzubeugen. Weiters nimmt die Direktion Staatsschutz und Nachrichtendienst regelmäßig an innerstaatlichen bzw. interministeriellen Treffen (etwa im Rahmen des IKDOK) teil und steht darüber hinaus im regelmäßigem Austausch mit den anderen Ministerien.

Seitens der operativen NIS-Behörde im BMI wird Cyberkriminalität im Bereich der Prävention, auf Grundlage des NISG, im Rahmen von Sensibilisierungsgesprächen, Präventionsveranstaltungen und Publikationen ebenfalls laufend thematisiert und behandelt.

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

Das Bundesministerium für Inneres ist zur Abwehr von Cyberattacken durch technische und organisatorische Sicherheitsmaßnahmen in den Bereichen Prävention, Absicherung, Erkennung und Incident Response auf dem Stand der Technik vorbereitet.

Das Bundesministerium für Inneres steht in enger Abstimmung mit Personen aus der Wissenschaft und der Zivilgesellschaft, um deren Expertise einfließen zu lassen. Erkenntnisse aus dem gesamtstaatlichen Lagebildprozess werden in Zusammenarbeit mit den 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, oder aber auch der Auflistung einzelner im Einsatz befindlichen Produkte, im Hinblick auf die Sicherung der Effektivität der Schutzmaßnahmen von einer detaillierten Bekanntgabe dieser eingesetzten Produkte 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 anderen 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?

Ja. Das kontinuierliche Risikomanagement definiert die im Bundesministerium für Inneres kritischen Prozesse und Dienste. Für diese ist ein Betriebskontinuitätsmanagement eingerichtet. Dementsprechend werden dem risikobasierten Ansatz nach, laufend Anpassungen an der IKT-Sicherheitsstruktur und der dahinterliegenden Prozesse vorgenommen. Dies betrifft sowohl die Beschaffung von State-of-the-Art IKT-Sicherheitsinfrastruktur als auch die permanente Evaluierung und Anpassung der Prozesse. Zusätzlich werden basierend auf den aktuellen Bedrohungslagen Maßnahmen zur Hebung der Awareness durchgeführt.

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, oder aber auch der Auflistung einzelner im Einsatz befindlicher Produkte im Hinblick auf die Sicherung der Effektivität der Schutzmaßnahmen Abstand genommen werden.

Zur Frage 5:

- *Gibt es eine Person oder einen Personenkreis in Ihrem Ressort, die dezidiert als „Cybersicherheitsbeauftragte(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?*

Im Bundesministerium für Inneres ist die Funktion des Chief Information Security Officer (CISO) eingerichtet, der die Agenden eines „Cybersicherheitsbeauftragten“ innehat: Der Chief Information Security Officer 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.

Der CISO verfügt über ein abgeschlossenes Hochschulmasterstudium mit Fokus IT-Security und eine langjährige Berufserfahrung im Bereich IKT-Sicherheit. Darüber hinaus sorgt eine

kontinuierliche berufsbegleitende Weiterbildung für das notwendige Expertenwissen, um gegen die ständig steigende Bedrohung durch Cyberangriffe entsprechend vorbereitet zu sein.

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.

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 Inneres sind Krisen- und Notfallmanagementprozesse etabliert. Diese werden im Sinne eines kontinuierlichen Verbesserungsprozesses laufend aktualisiert und weiterentwickelt.

Im Rahmen des IKDOK (Innerer Kreis der operativen Koordinierungsstruktur) sind zur Umsetzung der Rechnungshofempfehlung Standard Operating Procedures (SOPs) für das gesamtstaatliche Cyberkrisenmanagement in Ausarbeitung. Die Expertise des nationalen Computernotfallteams (CERT.at) sowie Erkenntnisse aus europäischer Zusammenarbeit im Rahmen des europäischen Netzwerks von Computernotfallteams (CSIRTs-Network) und des sich etablierenden europäischen Cyber Crisis Liaison Organisations Network (CyCLONe) fließen in die Erstellung ein. Mit einer Fertigstellung ist aus derzeitiger Sicht im Jahre 2023 zu rechnen.

Zur Frage 8:

- *Der Rechnungshof sah zudem die Etablierung eines permanent verfügbaren CyberEinsatzteam („Rapid Response Team") sowie die Schaffung eines ebenso permanenten Cyberlagezentrums zur Bearbeitung von Notfällen als essenziell. 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?

Derzeit werden Räumlichkeiten im Raumverbund mit der operativen NIS-Behörde adaptiert und mit Infrastruktur ausgestattet. Ab 2023 sollen diese als Cyberlagezentrum dienen.

Bezüglich Cyber-Einsatzteams wird auf die Beantwortung des Bundesministeriums für Landesverteidigung verwiesen.

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?*

Lagebilder zum Thema Cybersicherheit werden ressortübergreifend im IKDOK seit Jänner 2018 auf der österreichischen Strategie für Cybersicherheit bzw. seit dessen Inkrafttreten auf Basis des Netz- und Informationssystemsicherheitsgesetzes (NISG) monatlich erstellt; bereits zuvor erfolgte eine anlassbezogene Lagebilderstellung. Zusätzlich wurden bzw. werden Sonderlagebilder anlassbezogen zum Thema Cybersicherheit produziert.

Zu den Fragen 10, 11 und 11a bis 11d:

- *Der Rechnungshof bemängelt weiters, dass zum Ende des Untersuchungszeitraums Ende Mai 2021 das „NIS-Meldeanalysesystem", dass im Netz- und lnformationssystemsicherheitsgesetz (NISG) bereits 2018 beschlossen wurde und im Bundesministerium für Inneres angesiedelt sein soll, noch nicht in Betrieb ist. Das Meldesammelsystem ist zwar seit dem dritten Quartal 2021 etabliert, dabei handle es sich aber nur um eine Vorstufe zum Meldeanalysesystem. Zum Zeitpunkt der Beantwortung dieser parlamentarischen Anfrage, ist das finale Cyber-Meldeanalysesystem bereits im Einsatz?*
  - *a. Falls ja, seit wann ist das finale Meldeanalysesystem im Einsatz?*

   b. *Falls nein, warum nicht und ab wann wird das Meldeanalysesystem im Einsatz sein?*
- *Wer - welche Stellen der öffentlichen Verwaltung, welche privatwirtschaftlichen Unternehmen, Organisationen etc. waren an der Konzipierung und Ausarbeitung der in Frage 10 erwähnten Meldesammel- bzw. Meldeanalysesysteme beteiligt?*
- *Welche(s) Unternehmen, Organisationen etc. wurde(n) mit der Konzipierung und Ausarbeitung der Meldesammel- bzw. Meldeanalysesysteme betraut? Weshalb wurde(n) diese(s) Unternehmen gewählt?*
- *Wie hoch waren die Kosten für die Konzipierung und Ausarbeitung der Meldesammel- bzw. Meldeanalysesysteme?*
- *Wie hoch sind (werden) die laufenden Betriebskosten der Meldesammel- bzw. Meldeanalysesystem (sein)?*
- *Gab es eine öffentliche Ausschreibung für die Konzipierung und Ausarbeitung dieser Systeme?*
    i. *Falls ja, wie viele Unternehmen, Organisationen etc. haben sie für diese Ausschreibung beworben?*
    ii. *Falls nein, warum gab es keine öffentliche Ausschreibung dazu?*

Die Konzeption und Umsetzung der Meldesammelstelle erfolgte zur Gänze innerhalb des BMI und der zuständigen Abteilung. Der Betrieb des Meldesammelsystems erfolgt mit Standardsystemen innerhalb des BMI und verursachen keine zusätzlichen laufenden Kosten.

Zur Umsetzung des Meldeanalysesytems wurde im Jahr 2019 im Rahmen des Europäischen Förderprogramms „Connection Europe Facility“ (CEF) im Detailprogramm „ICT 2020: Leading the Digital Age“ das Projekt „AWAKE“ gemeinsam mit dem Bundeskanzleramt, dem nationalen Computernotfallteam (CERT.at) und dem Austrian Institute of Technology (AIT) eingereicht. Das Projekt erhielt 2020 den Zuschlag und befindet sich derzeit in Umsetzung. Mit einer Fertigstellung ist 2024 zu rechnen.

Das Gesamtvolumen des Projekts beläuft sich auf EUR 1.767.569,38, wobei das Bundesministerium für Inneres einen Eigenanteil von EUR 21.400 zu tragen hat. Weitere laufende Aufwendungen fallen zum aktuellen Zeitpunkt nicht an.

Zur Frage 11e:

- *Welche Stellen der öffentlichen Verwaltung, Zivilgesellschaft etc. nehmen zum Zeitpunkt der Beantwortung dieser parlamentarischen Anfrage bereits am*

Meldesammel- bzw. Meldeanalysesystems teil? Gibt es Pläne, auch noch andere Stellen miteinzubinden?

Das Meldesammel- bzw. in weiterer Folge Meldeanalysesystem betrifft die Adressaten des Netz- und Informationssystemsicherheitsgesetzes (NISG) und wird aktuell mit Informationen aufgrund abgegebener freiwilliger und Pflichtmeldungen nach dem NISG gespeist.

Zur Frage 12:

- *Neben dem Meldeanalysesystem soll es ein Frühwarnsystem geben, ebenfalls im Bundesministerium für Inneres angesiedelt. Laut Rechnungshofbericht war dieses Frühwarnsystem 2021 erst in einer ersten Konzipierungsphase, obwohl bereits 2019 Investitionen und 2020 auch schon Betriebskosten dafür veranschlagt wurden.*
  a. *Zum Zeitpunkt der Beantwortung dieser parlamentarischen Anfrage, ab wann wird das genannte Frühwarnsystem zum Einsatz kommen?*
  b. *Wieso wurden gemäß Rechnungshofbericht und wirkungsorientierter Folgenabschätzung zum NISG - bereits Investitionen bzw. Betriebskosten für ein System veranschlagt, das erst in der ersten Phase der Konzipierung ist?*
  c. *Welche(s) Unternehmen, Organisationen etc. wurde(n) mit der Konzipierung und Ausarbeitung des Frühwarnsystems betraut? Weshalb wurde(n) diese(s) Unternehmen gewählt?*
  d. *Wie hoch waren die bisherigen Kosten für Konzipierung und Ausarbeitung des Frühwarnsystems? Wie hoch werden die weiteren Kosten für Konzipierung und Ausarbeitung des Frühwarnsystems bis zu Fertigstellung geschätzt sein?*
  e. *Wie hoch sind (werden) die laufenden Betriebskosten des Frühwarnsystems (sein)?*
  f. *Gab es eine öffentliche Ausschreibung für die Konzipierung und Ausarbeitung des Frühwarnsystems?*
     i. *Falls ja, wie viele Unternehmen, Organisationen etc. haben sie für diese Ausschreibung beworben?*
     ii. *Falls nein, warum gab es keine öffentliche Ausschreibung dazu?*
  g. *Sofern das Frühwarnsystem bereits im Einsatz ist: Welche Stellen der öffentlichen Verwaltung, Zivilgesellschaft etc. nehmen zum Zeitpunkt der Beantwortung dieser parlamentarischen Anfrage bereits am Frühwarnsystem teil? Gibt es Pläne, auch noch andere Stellen miteinzubinden?*

Ein öffentliches Vergabeverfahren zur Konzeption des Frühwarnsystems ist zum Zeitpunkt der Antworterstellung im Laufen.

Bis dato fielen keine laufenden Kosten für das Frühwarnsystem an. Weiterführende Antworten zu Betriebskosten können zum derzeitigen Zeitpunkt nicht gegeben werden, da diese in weiterer Folge vom Ergebnis der Konzeption des Frühwarnsystems abhängen werden. Eine Veranschlagung von Kosten das Frühwarnsystem betreffend war aus damaliger Sicht aufgrund der vorzunehmenden haushaltsrechtlichen wirkungsorientierten Folgenabschätzung zum NISG erforderlich.

Zur Frage 13:

- *Schließlich sieht der Rechnungshof bei den „Personalressourcen, um die Cyber-Sicherheit aufrecht zu erhalten" konkret im Bundesministerium für Inneres großen Aufholbedarf.*
  - *a. Zum Ende des vom Rechnungshof überprüften Zeitraums, nämlich Mai 2021, wie viele Personen waren im Bundesministerium für Inneres dezidiert im Bereich Cybersicherheit tätig?*
  - *b. Wurde zum Zeitpunkt der Beantwortung dieser Anfrage bereits zusätzliches Personal im Bereich der Cybersicherheit im Bundesministerium für Inneres aufgenommen?*
    - *i. Falls ja, wie viele Personen sind zum Zeitpunkt der Beantwortung dieser Anfrage im Bundesministerium für Inneres im Bereich Cybersicherheit tätig?*
    - *ii. Falls nein, wann planen Sie, mehr Personen für den Bereich Cybersicherheit im Bundesministerium für Inneres einzustellen?*

Die Gewährleistung von Cybersicherheit sowie die damit einhergehende Bekämpfung von Cyberkriminalität wurde in meinem Ressort als oberste Priorität erkannt, weshalb eine Personalzufuhr in diesem hochsensiblen Bereich laufend erfolgt. Von einer ausführlichen Beantwortung dieser Fragen muss jedoch aufgrund der Verpflichtung zur Wahrung der Amtsverschwiegenheit, insbesondere 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.

Gerhard Karner

REPUBLIK ÖSTERREICH AMTSSIGNATUR	Datum/Zeit	2022-11-14T14:56:43+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.	148769640
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	2022-11-14T15:01:12+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.	