11864/AB
vom 14.11.2022 zu 12154/J (XXVII. GP)

Bundesministerium
Europäische und internationale
Angelegenheiten

bmeia.gv.at

Mag. Alexander Schallenberg
Bundesminister
Minoritenplatz 8, 1010 Wien, Österreich

Herrn
Präsidenten des Nationalrates
Mag. Wolfgang Sobotka
Parlament
1017 Wien

Wien, am 14. November 2022

GZ. BMEIA-2022-0.667.208

Sehr geehrter Herr Präsident!

Die Abgeordneten zum Nationalrat Katharina Kucharowits, Kolleginnen und Kollegen haben am 14. September 2022 unter der Zl**.** 12154/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:

Zu den Fragen 1 bis 7:

- *Gab es in Ihrem Ressort bereits Cyberangriffe?*
  Falls ja, bitte um detaillierte Schilderung des Angriffs/der Angriffe, welche Schäden daraus resultierten und welche Gegenmaßnahmen ergriffen wurden?
- *Welche Rolle und welche konkreten Aufgaben fallen Ihrem Ressort in der gesamtstaatlichen Bekämpfung von Cyberkriminalität zu?*
- *Ergreift Ihr Ressort aktiv konkrete Maßnahmen, um sich präventiv gegen Cyberattacken und Cyberkriminalität angemessen zu schützen?*
  Falls ja, welche Maßnahmen sind das im Detail?
  *Falls ja, wird in der Vorbereitung auf einen potenziellen Cyberangriff auch die Expertise externer Expert*innen, etwas Personen auf Wissenschaft oder Zivilgesellschaft, hinzugezogen?*
  Falls nein, warum gibt es keine Pläne, sich für den Ernstfall eines potenziellen Cyberangriffs zu schützen?

- *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.*
  Gab es eine ressortspezifische Risikoanalyse in Ihrem Ressort?
  Falls nein, warum nicht?
  Welche konkreten Maßnahmen setzen Sie, um den spezifischen Risiken Ihres Ressorts gerecht zu werden?
- *Gibt es eine Person oder einen Personenkreis in Ihrem Ressort, die dezidiert als „Cybersichterheitsbeauftrage(r)" fungiert/fungieren?*
  Falls ja, wie viele Personen sind zum Zeitpunkt der Beantwortung dieser Anfrage im Bereich Cybersecurity in Ihrem Ressort beschäftigt?
  Falls ja, über welche Expertise verfügt/verfügen diese Person(en)?
  Falls nein, warum gibt es keine(n) „Cybersicherheitsbeauftrage(n)" in Ihrem Ressort?
- *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?*
- *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?*
  Falls ja, wurden zur Erstellung dieser Pläne auch externe Expert innen hinzugezogen?*
  Falls nein, wann ist mit der Fertigstellung dieser Pläne in Ihrem Ressort zu rechnen?

Ich verweise auf meine Beantwortung der parlamentarischen Anfrage Zl. 12044/J-NR/2022 vom 24. August 2022.

Zu 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?*
  Falls ja, in welchem Ressort sind diese Strukturen angesiedelt und der Zuständigkeit welcher/welchen Bundesministerin/Bundesministers unterliegen diese?

Die Beantwortung diese Fragen fällt nicht in die Vollziehung meines Ressorts. Betreffend das Rapid Response Team darf ich auf die Anfragebeantwortung des Bundesministeriums für Landesverteidigung (BMLV) verweisen, betreffend das Cyberlagezentrum auf jene des Bundesministeriums für Inneres (BMI).

Zu 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?*
  Falls ja, seit wann wird ein solches Lagebild in Ihrem Ressort erstellt und in welchen Abständen findet das statt?
  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 Netz- und Informationssystemsicherheitsgesetz (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 Vertreterinnen und Vertretern des Bundeskanzleramtes, des Bundesministeriums für Inneres, des Bundesministeriums für Landesverteidigung, sowie meines Ressorts. Er tritt regulär wöchentlich zusammen und erstellt seit 2018 monatlich das gesamtstaatliche IKDOK-Lagebild, das den Ministerien und den obersten Organen zur Verfügung gestellt wird. Das daraus abgeleitete Lagebild der Operativen Koordinierungsstruktur wird den im NISG angeführten Stellen übermittelt. Zusätzlich werden Sonderlagebilder anlassbezogen zum Thema Cybersicherheit produziert und verteilt.

Mag. Alexander Schallenberg

REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR EUROPÄISCHE UND INTERNATIONALE ANGELEGENHEITEN @ AMTSSIGNATUR	Unterzeichner	Bundesministerium für europäische und internationale Angelegenheiten
	Datum/Zeit	2022-11-14T09:38:53+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.	789818819
Hinweis	Dieses Dokument wurde amtssigniert.	
Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: http://www.signaturpruefung.gv.at Informationen zur Prüfung des Ausdrucks finden Sie unter: http://www.bmeia.gv.at/verifizierung	

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2022-11-14T09:43:23+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.	