Bundesministerium
Klimaschutz, Umwelt,
Energie, Mobilität,
Innovation und Technologie

bmk.gv.at

Leonore Gewessler, BA
Bundesministerin

leonore.gewessler@bmk.gv.at
+43 1 711 62-658000
Radetzkystraße 2, 1030 Wien
Österreich

An den
Präsident des Nationalrates
Mag. Wolfgang Sobotka
Parlament
1017 W i e n

Geschäftszahl: 2022-0.660.912

. November 2022

Sehr geehrter Herr Präsident!

Die Abgeordneten zum Nationalrat Kucharowits, Genossinnen und Genossen haben am 14. September 2022 unter der **Nr. 12149/J** an mich eine schriftliche parlamentarische Anfrage betreffend Vorbereitung auf Cyberangriffe innerhalb der österreichischen Bundesverwaltung gerichtet.

Diese Anfrage beantworte ich 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?*

Es gab in den letzten Jahren laufend Angriffe und Angriffsversuche auf die in meinem Ressort eingesetzten Computersysteme. Es ist meinem Ressort auf Basis der umgesetzten Sicherheitsvorkehrungen bisher jedoch immer gelungen, nennenswerte Schäden durch solche Angriffe abzuwehren.

Zu Frage 2:

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

Die Wahrnehmung gesamtstaatlicher Aufgaben im Bereich der Cyberkriminalität obliegen dem Bundesministerium für Inneres (BMI) und dem Bundesministerium für Justiz (BMJ).

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

Um die Informations- und Kommunikationstechnik (IKT) Systeme des Ressorts präventiv vor und gegen Cyberattacken und Cyberkriminalität zu schützen, setzt mein Ressort mehrere spezifische Sicherheitsvorkehrungen ein. Diese Sicherheitsvorkehrungen sollen die IKT-Sicherheitsrisiken minimieren und so die IKT-Systeme des Ressorts schützen. Bei der Planung und Umsetzung der Sicherheitsvorkehrungen werden auch externe Expert:innen hinzugezogen. Ich ersuche aber um Verständnis, dass gerade im Hinblick auf die Effektivität dieser Maßnahmen es nicht möglich ist, die Sicherheitsvorkehrungen im Detail öffentlich mitzuteilen.

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?*

IKT-Sicherheit und damit auch die Cybersicherheit werden als fortlaufender und umfassender Prozess verstanden. Dementsprechend werden im risikobasierten Ansatz kontinuierlich Anpassungen an der IKT-Sicherheitsstruktur und den dahinterliegenden Prozessen vorgenommen. Dies betrifft sowohl die Beschaffung von State of the Art-IKT-Sicherheitsinfrastruktur, als auch die permanente Evaluierung und Anpassung der Prozesse.

Weiters werden basierend auf den aktuellen Bedrohungslagen Maßnahmen zur Hebung der Awareness durchgeführt. Erkenntnisse aus dem gesamtstaatlichen Lagebildprozess werden in Zusammenarbeit mit den Techniker:innen meines Ressorts zeitnahe umgesetzt.

Bezüglich der Bekanntgabe der IKT-Sicherheitsmaßnahmen ersuche ich um Verständnis, dass im Hinblick auf die Sicherung der Effektivität der Schutzmaßnahmen von einer detaillierten Auflistung der Sicherheitsmaßnahmen Abstand genommen werden muss.

Zu Frage 5:

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

Wie oben ausgeführt werden die IKT-Sicherheit und damit auch die Cybersicherheit als fortlaufender und umfassender Prozess verstanden, der mehrere Bereiche des Ressorts betrifft. An der Planung und Umsetzung von Cybersicherheitsmaßnahmen sind daher, abhängig von der aktuellen Lage und den aktuellen Herausforderungen mehrere Personen, mit jeweils unterschiedlichen Expertisen, beteiligt. Jedenfalls werden im Rahmen der Chief Information Officer (CIO)-Tätigkeiten auch Agenden bezüglich Cybersicherheit wahrgenommen.

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?*

Die Verwaltungsakademie des Bundes (VAB) (Aus- und Weiterbildungsinstitut für Mitarbeiter:innen im Bundesdienst) bietet diverse Seminare zum Thema Datenschutz und Datensicherheit für Mitarbeiter:innen und Führungskräfte an, zu welchen sich die Mitarbeiter:innen meines Ressorts anmelden können. Die Mitarbeiter:innen meines Ressorts werden regelmäßig auf die Möglichkeit des Besuchs von Seminaren an der Verwaltungsakademie hingewiesen. Im Bedarfsfall sind darüberhinausgehende anlassbezogene Weiterbildungen möglich.

Seitens der IKT-Abteilung werden anlassbezogene Sensibilisierungsaktionen durchgeführt. Im Portal Austria werden Schulungs-Anwendung bezüglich Informationssicherheit und Datenschutz bereitgestellt.

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?*

IKT-Sicherheit wird als fortlaufender und umfassender Prozess verstanden. Dabei wird ein risikobasierter Ansatz verfolgt und abhängig von den konkreten Systemen und ihren Sicherheitsanforderungen werden entsprechende Sicherheitsmaßnahmen ergriffen. Diese Sicher-

heitsmaßnahmen beinhalten auch entsprechende Vorkehrungen, um Systemausfälle und Krisen bewältigen zu können. Für die Bewältigung großer katastrophaler Ereignisse steht meinem Ressort ein Ausweich-Rechenzentrum zur Verfügung.

Ein permanent verfügbares Cyber-Einsatzteam, ein Cyber-Lagezentrum oder regelmäßig erstellte Cyber-Lagebilder fallen nicht in den Zuständigkeitsbereich meines Ressorts. Für diese Themen darf auf die Beantwortung des Bundesministeriums für Inneres (BMI) oder die des Bundesministeriums für Landesverteidigung (BMLV) verwiesen werden.

Leonore Gewessler, BA

REPUBLIK ÖSTERREICH
BUNDESMINISTERIUM FÜR KLIMASCHUTZ, UMWELT, ENERGIE, MOBILITÄT, INNOVATION UND TECHNOLOGIE
AMTSSIGNATUR

Hinweis	Dieses Dokument wurde amtssigniert.
Datum	2022-11-08T09:17:00+01:00
Seriennummer	1871969199
Aussteller-Zertifikat	CN=a-sign-corporate-05,OU=a-sign-corporate-05,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at/

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2022-11-08T09:19:37+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.	