Bundesministerium
Soziales, Gesundheit, Pflege
und Konsumentenschutz

sozialministerium.at

Johannes Rauch
Bundesminister

Herrn
Mag. Wolfgang Sobotka
Präsident des Nationalrates
Parlament
1017 Wien

Geschäftszahl: 2022-0.660.119

Wien, 11.11.2022

Sehr geehrter Herr Präsident!

Ich beantworte die an mich gerichtete schriftliche parlamentarische **Anfrage Nr. 12146/J der Abgeordneten Kucharowits, Genossinnen und Genossen betreffend Vorbereitung auf Cyberangriffe innerhalb der österreichischen Bundesverwaltung** wie folgt:

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 BMSGPK sieht sich, wie auch andere Ministerien, Unternehmen und Bildungseinrichtungen, kontinuierlichen Angriffsversuchen im Cyberraum ausgesetzt. Im BMSGPK konnten bisher derartige Angriffsversuche abgewehrt sowie Schäden und Ausfälle 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.

Auf die Beantwortung der Anfrage Nr. 11861/J darf verwiesen werden.

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 BMI und BMJ sowie für Cybersicherheit dem BKA. Es darf daher auf die diesbezüglichen Beantwortungen der Anfragen durch den Bundesminister für Inneres, die Bundesministerin für Justiz sowie den Herrn Bundeskanzler verwiesen werden.

Bezüglich Cybersicherheit im Gesundheitswesen ist das BMSGPK für Vorgaben zuständig. Das BMSGPK nimmt konkret folgende Aufgaben wahr:

- Angelegenheiten für strategische Kommunikations-, Netzwerk- und Informationssystemsicherheit im Gesundheitswesen,
- Koordination von nationalen und internationalen Cybersicherheitsthemen im Gesundheitswesen,
- Aufbau des HealthCERT,
- Koordination von gesamtstaatlichen Cyberübungen sowie Angelegenheiten des Ordnungspolitischen Rahmens für Cybersicherheit im Gesundheitswesen;
- Angelegenheiten des Cyber Stakeholdermanagements und Koordination des CSAeH
- Interne Cybersicherheit

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?*

Im BMSGPK 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 BMSGPK 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 des Netz- und Informationssystemsicherheitsgesetzes, 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.

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 BMSGPK wurde zum Zweck der systemischen Risikoanalyse ein ISMS 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 auf die Beantwortung der Fragen 1 und 3 verwiesen werden.

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?

Ja, wobei das BMSGPK die Bezeichnung „IT-Sicherheitsbeauftragte/r“ verwendet 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 wesentlich erschwert bzw. in gewissen Bereichen unmöglich gemacht wird.

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, im BMSGPK werden allen Mitarbeiter:innen diesbezüglich geschult, sowohl in Präsenz als auch online über E-Learnings. Über das ressorteigene elektronische Bildungsmanagement werden aktuell zwei E-Learnings (IT-Sicherheit, Umgang mit klassifizierten Informationen) sowie zwei Lehrvideos (IT-Sicherheit: Cyber Crime, Security Awareness Training) angeboten, um die Mitarbeiter:innen für das Thema zu sensibilisieren und niederschwellig Informationsangebote bereitzustellen. Betreffend Absolvierung der E-Learnings finden regelmäßig Erhebungen über das Bildungscontrolling statt. Die Vorgesetzten sind aufgefordert, die Mitarbeiter:innen auf die Absolvierung dieser Angebote ausdrücklich hinzuweisen.

Ziel ist es, dass diese Weiterbildungen möglichst umfassend von allen Mitarbeiter:innen absolviert werden. Für neu eintretende Mitarbeiter:innen ist dies im Onboarding innerhalb der ersten sechs Monate verpflichtend vorgesehen. Für die Zielgruppe Lehrlinge wird das Thema IT-Sicherheit gezielt im Rahmen der ELAK-Schulungen behandelt.

Auch erfolgen laufend Informationen über die verschiedensten Kanäle (Mails, Intranet, Mitarbeiter:innen-Zeitung, Online- und Präsenztrainings und Informationsveranstaltungen etc.). Auf eine hohe Awareness der Mitarbeiter:innen wird großer Wert gelegt, zu den Awarenessmaßnahmen gibt es auch Audits.

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 CyberEinsatzteam („Rapid Response Team") sowie die Schaffung eines ebenso permanenten Cyberlagezentrums 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?

Es darf auf die Beantwortungen der Anfragen durch den Herrn Bundeskanzler, den Bundesminister für Inneres und die Bundesministerin für Landesverteidigung verwiesen werden, etwa für das Rapid Response Team auf die Beantwortung durch die BMLV, für das Cyberlagezentrum auf die des BMI, für das Cyberlagebild, welches auch im BMSPGK verwendet wird, auf die Beantwortung des BKA.

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

Mit freundlichen Grüßen

Johannes Rauch

REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR SOZIALES, GESUNDHEIT, PFLEGE UND KONSUMENTENSCHUTZ @ AMTSSIGNATUR	Unterzeichner	Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz
	Datum/Zeit	2022-11-11T14:51:25+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.	2098721075
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: https://www.sozialministerium.at/site/Ministerium/Willkommen_im_Ministerium/Amtssignatur/Amtssignatur	

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2022-11-11T14:55:17+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.	