18764/J
vom 05.06.2024 (XXVII. GP)

Anfrage

der Abgeordneten Douglas Hoyos-Trauttmansdorff, Kolleginnen und Kollegen

an die Bundesministerin für Landesverteidigung

betreffend Wie steht es um die Cyber Defence?

Nach dem Cyberangriff auf das BMEIA im Jahr 2020 wurde ein NEOS-Antrag auf die Einrichtung eines Cyberstabes im BMLV zuerst vertagt, dann nach Wiederaufnahme im Oktober 2022 abgelehnt. Die Bundesministerin argumentierte, wie auch die Regierungsparteien im Ausschuss in der Begründung für ihre Ablehnung, der Aufbau einer Cyber Defence sei bereits weit fortgeschritten und bedürfe keiner weiteren Handlungsempfehlungen durch den Nationalrat.

Just in diesem Zeitraum – August bis November 2022 – prüfte der Rechnungshof die Koordinierung der Cyber Defence und fand deutliche Schwächen. Ebenso in diesem Zeitraum berichtete die internationale Beratungsfirma KPMG, dass sich die Anzahl der Cyberangriffe in Österreich innerhalb eines Jahres verdreifacht hatte, und dass Angriffe vermehrt von staatlichen oder staatsnahen Akteuren verübt werden.

Ein Problem ist die Koordinierung. Cyber Defence ist in Österreich eine Querschnittmaterie. Das BMI koordiniert die Abwehr von Cyberkrisen. Sobald die Attacke sich in eine souveränitätsgefährdende Gefahr ausweitet, ist das BMLV mit der Verteidigung betraut. Dafür muss das Verteidigungsministerium eine ständige Bereitschaft erhalten und die nötigen personellen und materiellen Voraussetzungen zur Abwehr bereitstellen können. Der RH fordert zwei Einsatzteams. Weiters verlangen die Prüfer:innen die Umsetzung zweier bestehender Vorhaben: ein Security Operation Center; und eine Cyber-Plattform als Trainingszentrum (eine militärische Cyber-Range).

Der Rechnungshof kommt zum Schluss, dass das BMLV für seine Cyber-Defence Aufgaben nicht ausreichend gerüstet ist. So hat das BMLV noch keine konkreten Szenarien und Kriterien erarbeitet um festlegen zu können, ob und wann eine Souveränitätsgefährdung vorliegt und damit der Übergang von der Cyberkrise zum Cyber-Defense Fall zu vollziehen ist. Auch fehlen laut RH gesamtstaatliche Konzepte zur Konkretisierung von Schritten, um die Kommunikation und Aktivitäten von staatlichen Stellen und Körperschaften zu gewährleisten.

Als einen Grund für die mangelnden Fortschritte bei der Aufbau einer robusten Cyber Defence sieht der RH die Zentralstellenreform. Die Direktion 6 (IKT & Cyber) war noch nicht durch Erlass verfügt, Bedienstete waren teilweise zugeteilt, die Aufstockung des Personals kommt wegen der Probleme bei der Finalisierung der Reform nicht vom Fleck. Aber auch andere Probleme behindern eine effektive Cyberabwehr. So z.B. gibt es keine schriftliche Festlegung der Prozesse zwischen den beiden militärischen Nachrichtendiensten und der Direktion 6. Für einen reibungslosen und vorhersehbaren Ablauf des Austausches und er Planung wäre ein klar definierter Prozess, unabhängig von den gerade dort arbeitenden Personen, aber unabdingbar.

Die unterfertigten Abgeordneten stellen daher folgende

Anfrage:

1. In Anbetracht der Gefährdungssituation und Häufigkeit von Cyberattacken, auch durch staatliche oder staatsnahe Akteure, ist Cyber Defence noch weiter ins Zentrum der Verteidigungsfähigkeit gerückt als noch zur Zeit der Prüfung durch den Rechnungshof. Welche spezifischen Maßnahmen hat das BMLV seit dem Rechnungshofbericht gesetzt, um die im Bericht aufgezeigten Schwächen zu beseitigen?
    a. Welche Maßnahmen wurden gesetzt, um die Cyber Defence während der durch die sich weiterhin verzögernde Zentralstellenreform geschaffenen Übergangszeit lückenlos zu gewährleisten?
    b. Ist die durch die Zentralstellenreform neu geschaffene Direktion 6 (IKT & Cyber) bereits arbeitsfähig? Wenn nein, wie und in welcher Abteilung wird Cyber Defence derzeit gewährleistet?
    c. Sind die leitenden Positionen der Direktion 6 vom BMKÖS bewertet und permanent besetzt?
    d. Wer bzw. welche Abteilung ist für die Beurteilung eines Cyber-Defence Falles zurzeit verantwortlich?
    e. Welche Ressourcen stellt das BMLV dieser Abteilung zur Verfügung?
2. In Erwartung der neuen Direktion 6 (IT & Cyber), wer koordiniert(e) in der Zeit, in der die Direktion noch nicht arbeitsfähig war bzw. ist die Arbeit des BMLV mit dem BMI und den anderen Sicherheitsministerien?
3. Gibt es bereits das vom Rechnungshof geforderte gesamtstaatliche Cyber-Krisenmanagement Konzept (CKM 2019) zwischen den Sicherheitsressorts BMI, BMEIA und BMLV sowie dem Bundeskanzleramt?
    a. Wenn nein, für wann ist dieses Konzept zu erwarten? Wer ist für die Ausarbeitung verantwortlich?
    b. Wenn ja, wie wurden die Verantwortlichkeiten zwischen den drei Sicherheitsministerien und dem BKA geregelt? Welche Kommunikationskanäle wurden eingerichtet?
4. Das BMLV muss für den Fall des Eintritts einer souveränitätsgefährdende Gefahr eine ständige Bereitschaft aufrecht erhalten. Ohne Cyberstab und ohne Direktion 6, wie wird die konstante Abwehrfähigkeit im BMLV aufrecht erhalten?
    a. Wer kommandiert die Cyberabwehr bis zur Ernennung der neuen Leitung der neuen Direktion 6?
5. Der RH kritisiert, dass das BMLV noch keine konkreten Szenarien und Kriterien erarbeitet hat um zu bestimmen, ob ein Angriff zur Souveränitätsgefährdung wurde. Wurden derartige Szenarien und Kriterien mittlerweile erstellt?
    a. Wurden seit Erscheinen des RH-Berichts Kriterien erarbeitet, die einen militärischen Einsatz rechtfertigen bzw. notwendig werden lassen?
    b. Wurden seit Erscheinen des RH-Berichts Kriterien erarbeitet, die den Übergang von Cyberkrise zu Cyber Defence konkretisieren? Gibt es in diesem Zusammenhang einen Plan zur Übergabe der Verantwortung vom BMI an das BMLV?

c. Wurden seit Erscheinen des RH-Berichts Kriterien für die Einbeziehung von und Kommunikation mit verschiedenen Körperschaften im Krisenfall ausgearbeitet?

d. Wurden Kriterien hinsichtlich der Bedeutung einzelner kritischer Infrastrukturen bei einer Verletzung der Souveränität Österreichs ausgearbeitet?

6. Wie viele Übungen wurden seit Erscheinen des RH-Berichts abgehalten zu:

   a. Feststellung einer Souveränitätsgefährdung und damit einhergehend eines Militäreinsatzes? (Bitte um Daten und teilnehmende Abteilungen/Organisationen.)

   b. Übergang von Cyberbedrohung oder Angriff (BMI) zu Cyber-Defence-Einsatz (BMLV)? (Bitte um Daten und teilnehmende Abteilungen/Organisationen.)

   c. Kooperation und Kommunikation mit verschiedenen Körperschaften? (Bitte um Daten und teilnehmende Abteilungen/Organisationen/Körperschaften.)

   d. Schutz kritischer Infrastrukturen im Falle einer souveränitätsbedrohenden Cybergefahr? (Bitte um Daten und teilnehmende Abteilungen/Organisationen.)

   e. Cyberabwehr Assistenzleistungen? (Bitte um Daten und teilnehmende Abteilungen/Organisationen/Ministerien/Körperschaften.)

7. Wurde die vom Rechnungshof geforderte schriftliche Festlegung des Austauschs mit den Cyberverantwortlichen im BMLV und den beiden militärischen Diensten ausgearbeitet und verfügt?

8. Wurde das seit langem in Planung befindliche Security Operation Center umgesetzt? In welchem Stadium befindet es sich?

9. Wurde das Vorhaben, eine Cyber-Plattform für Trainingszwecke zu errichten, umgesetzt? In welchem Stadium befindet sie sich?

10. Welche finanziellen Mittel stehen in den Budgets 2023 und 2024 sowie im derzeit geltenden Finanzrahmen für die Cyberabwehr zur Verfügung?

    a. Wurden bzw. werden diese Mittel ausgeschöpft? Welche Anschaffungen wurden trotz des Fehlens des Direktorats 6 bereits getätigt, welche sind unter Vertrag?

11. Welche Mittel sind im Aufbauplan ÖBH 2032+ für Cyberabwehr vorgesehen? Bitte um Auflistung der /geplanten und bereits getätigten) Anschaffungen und der Personalpläne bis 2032 oder, wo bereits bekannt, darüber hinaus.

12. Wurden die vom Rechnungshof geforderten zwei Einsatzteams aufgestellt? Sind diese jederzeit und voll einsatzbereit?

    a. Wo sind sie angesiedelt?

13. Welche Aufgaben wird die Miliz in der Cyber Defence spielen?

14. Nachdem bereits 2020 und 2022 bei der Ablehnung der Cyberstab-Anträge von großem Fortschritt bei der Cyber Defence gesprochen wurde, welche Fortschritte wurden zwischen 2020 und dem ersten Quartal 2024 gemacht?

Bitte um Auflistung von Anschaffungen, Personalaufstockungen und Planungsdokumenten.

15. Außenminister Schallenberg besuchte am 23. April das neue Kommando Cyber der Schweizer Armee. Hat Ministerin Tanner sich über den Besuch und die Gründe der Schweiz, ein solches Zentrum einzurichten, beim Außenminister erkundigt? Gab es direkte Kontakte mit der Schweiz bezüglich der Gründe für die Errichtung eines solchen Zentrums und den Erfahrungen mit der Errichtung?

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2024-06-06T11:53:04+02:00
Prüfinformation	Dieses Dokument wurde elektronisch besiegelt. Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel	