18235/J XXVII. GP

Eingelangt am 27.03.2024

Anfrage

der Abgeordneten Dr. Helmut Brandstätter, Douglas Hoyos-Trauttmansdorff, Kolleginnen und Kollegen

an die Bundesministerin für Landesverteidigung

betreffend Frequenz von Cyberattacken und Gegenmaßnahmen

In den medialen Debatten über die Aufrüstung des Bundesheers mit konventionellen Waffen kommt die Gefahr subkonventioneller, hybrider Kriegführung oft zu kurz. In den Medien finden sich zwar tagtäglich Berichte über Cyberangriffe auf Unternehmen wie auch Behörden. So wurden etwa die Stadtgemeinde Korneuburg, die Therme Laa und das Wifi Niederösterreich innerhalb weniger Tage im Februar 2024 Opfer von Angriffen. Diese Attacken sind Anzeichen einer breiteren Bedrohung der nationalen Sicherheit und müssen auch derart eingeordnet werden.

Die mediale Aufmerksamkeit über die Gefahren im Cyberraum täuscht nicht. Das renommierte Consulting-Unternehmen KPMG berichtet in *Cybersecurity Österreich 2023* von einer Verdreifachung der Anzahl der Angriffe innerhalb eines Jahres, mit einer zehnprozentigen Erfolgsquote.[1] KPMG befragte 903 Unternehmen, von denen alle (!) zumindest einen Angriff im Untersuchungsjahr meldeten. Während ein Angriff für ein Unternehmen existenzbedrohend sein kann, mehren sich auch Angriffe auf die kritische Infrastruktur und werden laufend zielgerichteter und komplexer. Krankenhäuser, Windparks zur Stromerzeugung, Supermärkte und Handelsketten, aber auch IT-Dienstleister sind laut Studie immer häufiger von Ransomware-Attacken betroffen. Die Auswirkungen gehen in diesen Fällen über die einzelnen Unternehmen hinaus und sind gesamtstaatlich relevant.

Besonders bedrohlich ist, dass diese Angriffe nicht ausschließlich von Kriminellen, sondern vermehrt von Staaten initiiert werden. So schreibt KPMG:

> *"Befeuert hat diesen Negativtrend noch der Krieg in Europa: Jedes dritte Unternehmen (33 Prozent) hat bereits einen Zusammenhang zwischen dem russischen Angriffskrieg auf die Ukraine und Cyberangriffen auf das eigene Unternehmen festgestellt. Besorgniserregend ist dabei vor allem das zunehmende Interesse der Angreifer:innen an der kritischen Infrastruktur."*

KPMG kommt zum Schluss, dass es "*um der Gefahr von Cyberangriffen nachhaltig entgegenwirken zu können*" einer "*stärkere Zusammenarbeit zwischen den Unternehmen und öffentlichen Stellen, auch über die Landesgrenzen hinweg*" bedürfe. „*Wir müssen und werden uns mit der Frage der digitalen Souveränität in*

Europa auseinandersetzen. Die Chancen für österreichische bzw. europäische Lösungen sind gerade beim Thema Cybersicherheit sehr groß. Die Anstrengung, hier gemeinsam tragfähige Wege und Lösungen zu finden, wird sich lohnen“, so Michael Höllerer, Präsident des Kompetenzzentrum Sicheres Österreich (KSÖ), in der Studie.

In Österreich ist Cyberabwehr eine Querschnittsmaterie, die sich BKA, BMLV, BMI und BMEIA aufteilen. Laut BMLV obliegt dem Bundeskanzleramt die Planung und Koordinierung; dem BMI unterliegen die Bereiche Cybersecurity und Cybercrime. Das BMEIA ist für Cyberdiplomacy verantwortlich. Das BMLV bewerkstelligt Cyberdefence. Ein Problem bei dieser Unterteilung entsteht aus unklaren Definitionen. Wenn die Trennung zwischen Cybercrime und Cyberdefense unklar ist, entstehen Grauzonen zwischen den Ministerien und deren Kompetenzen, die entweder zu Überschneidungen in den Aufgaben führen können, oder aber aufgrund unklarer Kompetenzverteilung von niemandem zeitgerecht bearbeitet werden.

Bereits 2020 nach dem Angriff auf das BMEIA wurde ein NEOS Antrag zur Gründung eines spezifischen Cyberstabes zur besseren Koordinierung der österreichischen Cybersicherheit vertagt, nach Wiederaufnahme 2022 in Zuge der vermehrten Cyberangriffe nach dem russischen Angriff auf die Ukraine wurde er abgelehnt. Die Cybersicherheit hat sich seit diesen negativen Entscheidungen aber offensichtlich verschlechtert.

1. https://kpmg.com/at/de/home/media/press-releases/2023/05/kpmg-studie-anzahl-der-cyberattacken-innerhalb-eines-jahres-verdreifacht.html

Die unterfertigten Abgeordneten stellen daher folgende

Anfrage:

1. Laut KPMG hat sich die Anzahl der Cyberangriffe 2023 verdreifacht. Diese Schätzung beruht auf Anfragen bei Unternehmen. Wie stellt sich die Zahl der Cyberangriffe aus Sicht der Nachrichtendienste dar? Entspricht eine Verdreifachung der Angriffe den Erkenntnissen der Dienste?
2. Wie hat sich die Anzahl der Cyberangriffe seit Beginn der russischen Drohungen gegen und des Angriffs auf die Ukraine entwickelt? Bitte um Auflistung der Anzahl der Angriffe für 2020, 2021, 2022 und 2023.
3. Welcher Anteil der Cyberangriffe in den in Frage 2 abgefragten Jahren ist staatlich initiiert, gelenkt oder unterstützt, bzw. kann auf staatliche Entitäten, Institutionen oder Finanzierung zurückgeführt werden?
4. Welcher Anteil der staatlich initiierten, gelenkten oder unterstützten Cyberangriffe kann nach Russland zurückverfolgt werden?
    a. In absoluten Zahlen, bitte um Aufschlüsselung der staatlich initiierten, gelenkten oder unterstützten Cyberangriffe auf Österreich nach Ursprungsland für die Jahre 2020 bis 2023.
5. Welche Maßnahmen hat das BMLV aufgrund des erhöhten Risikos durch den russischen Krieg und die erhöhte Zahl der Angriffe ergriffen?
6. Die Anwerbung von Cyberexpert:innen ist für das BMLV, wie den Staatsdienst generell, kompliziert. Besonders das Gehaltsschema im öffentlichen Dienst

stellt für die Anwerbung von Top-Talent eine große Herausforderung dar. Welche Gesetzesnovellen – finanzieller Natur und andere – wären nötig, um die notwendige Quantität und Qualität anzuwerben und im Dienst zu halten?

7. Ein Antrag auf Schaffung einer zentralen Stelle für Cyberverteidigung wurde im Landesverteidigungsausschuss des Nationalrats mehrheitlich vertagt, dann abgelehnt. Wie steht das BMLV heute, zum Zeitpunkt der Anfragebeantwortung, der Schaffung einer zentralen Stelle zur Koordinierung der österreichischen Cybersicherheit gegenüber?
    a. Welche Vor- und Nachteile hätte die zentrale Koordinierung der österreichischen Cybersicherheit in einem koordinierenden Ministerium? Wäre das BMLV aufgrund seiner Expertise für diese Rolle geeignet?
8. Welche Maßnahmen setzt das BMLV auf europäischer Ebene, um die Cybersicherheit in Österreich zu verbessern?
    a. Welche "gemeinsame Wege oder Lösungen" wie im KPMG Report gefordert werden auf europäischer Ebene gegangen bzw. gefunden?
    b. An welchen europäischen Koordinationsmaßnahmen beteiligt sich Österreich wie?
9. Welche Budgetmittel stehen dem BMLV spezifisch für Cyberdefense zur Verfügung? Bitte um Vergleichszahlen für die Jahre 2020 bis 2023 sowie für den Finanzrahmen.