Landtag Brandenburg **Drucksache 8/00000**
8. Wahlperiode

Antwort
der Landesregierung

auf die Kleine Anfrage Nr. 530
des Abgeordneten Corrado Gursch (CDU-Fraktion)
Drucksache 8/1425

Stand der Cybersicherheitsstrategie des Landes Brandenburg

Namens der Landesregierung beantwortet der Minister der Justiz und für Digitalisierung die Kleine Anfrage wie folgt:

Vorbemerkung des Fragestellers:

Die Gefährdungslage durch Cyberangriffe auf öffentliche Einrichtungen, kritische Infrastrukturen und Unternehmen hat sich in den letzten Jahren erheblich verschärft. Auch die Bundesregierung, das Bundesamt für Sicherheit in der Informationstechnik (BSI) sowie zahlreiche Fachverbände warnen vor zunehmenden Bedrohungen durch staatlich gesteuerte oder organisierte Angreifer.

Das Land Brandenburg hat in der Vergangenheit immer wieder betont, dass es auf eine umfassende Strategie zur Cybersicherheit setzt. Gleichzeitig sind jedoch bisher nur wenige öffentlich zugängliche Informationen über den aktuellen Stand der Cybersicherheitsstrategie verfügbar. Gerade vor dem Hintergrund der steigenden Risiken ist es von besonderem öffentlichen Interesse, welche konkreten Maßnahmen die Landesregierung in den Jahren 2024 und 2025 ergriffen hat und in welchem Umfang die personellen und organisatorischen Ressourcen für die Cybersicherheit zur Verfügung stehen.

Ich frage die Landesregierung:

1. Gibt es aktuell eine verbindliche Landesstrategie für Cybersicherheit und in welchem Umfang ist diese öffentlich einsehbar?

2. Wann wurde diese Strategie zuletzt fortgeschrieben oder aktualisiert?

7. Welche zentralen strategischen Ziele verfolgt die Landesregierung mit der Cybersicherheitsstrategie, insbesondere in Bezug auf kritische Infrastrukturen und die digitale Verwaltung?

8. Welche Gremien oder Steuerungskreise auf Landesebene sind mit der Koordination der Cybersicherheitsstrategie befasst, und wie oft tagen diese?

9. Wie erfolgt die Erfolgskontrolle und Evaluation der Wirksamkeit der Cybersicherheits-strategie und der daraus abgeleiteten Maßnahmen?

Eingegangen: tt.mm.jjjj / Ausgegeben: tt.mm.jjjj

Die Fragen 1, 2, 7, 8 und 9 werden wegen des Sachzusammenhangs gemeinsam beantwortet:

Mit § 1 der Brandenburgischen NIS-2-Umsetzungsverordnung (BbgNIS2UmsV) vom 14. Juli 2025 (GVBl. II Nr. 53) wird erstmalig die zuständige Behörde für eine verbindliche Cybersicherheitsstrategie des Landes Brandenburg geregelt. Auf dieser Grundlage wurde im Ministerium der Justiz und für Digitalisierung der Entwurf einer Cybersicherheitsstrategie erstellt, die nunmehr in der Landesregierung abzustimmen ist.

Die Leitlinie für die Informationssicherheit in der Landesverwaltung Brandenburg und der Justiz (Informationssicherheitsleitlinie) wurde zuletzt im Jahr 2024 von der Landesregierung grundlegend novelliert und trat am 25. Juni 2024 in Kraft. Sie dient der Organisation der Informationssicherheit und ist ein Grundsatzdokument zum Stellenwert, zu den verbindlichen Prinzipien und dem anzustrebenden Niveau der Informationssicherheit der unmittelbaren Landesverwaltung und Justiz. Die Informationssicherheitsleitlinie setzt dabei bereits einige Vorgaben der sog. NIS-2-Richtlinie (Richtlinie (EU) 2022/2555), die einen einheitlichen Rechtsrahmen für die Aufrechterhaltung der Cybersicherheit bezweckt, um. Aufbauend auf die Informationssicherheitsleitlinie erarbeitete das Ministerium der Justiz und für Digitalisierung den Entwurf einer Cybersicherheitsstrategie, welcher nunmehr in der Landesregierung abgestimmt wird. Die Informationssicherheitslinie ist im Amtsblatt für Brandenburg (ABl./24, [Nr. 30], S. 574) öffentlich einsehbar.

3. Welche konkreten Umsetzungsmaßnahmen im Bereich der Cybersicherheit wurden im Land Brandenburg in den Jahren 2024 und 2025 begonnen oder abgeschlossen?

Zu Frage 3: Im Jahr 2024 gab es keine spezifische Cybersicherheitsstrategie. Mit der in der Antwort zur Frage 1 bereits erwähnten Verordnung ist das Land seinen rechtlichen Verpflichtungen aus der NIS 2 Richtlinie der Europäischen Union (Richtlinie (EU) 2022/2555) nachgekommen. Insbesondere werden mit der Verordnung im Land eine zuständige Behörde für die Kontrolle der Einhaltung der Richtlinienvorgaben und ein Computer Notfallteam für präventive und Unterstützungszwecke bei Cybervorfällen eingerichtet.

Im Zuge der rechtlichen Umsetzung wurden entsprechend den Anforderungen der NIS-2-Richlinie zudem wichtige Einrichtungen in der Landesverwaltung Brandenburg, die den Sicherheitsanforderungen der Richtlinie unterliegen, identifiziert.

4. Wie ist die personelle Ausstattung im Ministerium der Justiz und für Digitalisierung sowie in weiteren zuständigen Behörden des Landes für den Bereich Cybersicherheit strukturiert (bitte nach Anzahl der Vollzeitäquivalente und Aufgabenbereichen aufschlüsseln)?

Zu Frage 4: Im MdJD werden die Aufgaben nach der BbgNIS2UmsV und der Informationssicherheitsleitlinie derzeit mit 2,2 VZÄ im MdJD veranschlagt. Für den nachgeordneten Bereich des MdJD ohne den ZIT-BB beträgt die personelle Ausstattung 7,33 VZÄ.

.

Für die Gewährleistung der Informationssicherheit sind beim ZIT-BB das IT-Sicherheitsmanagement für die IT-Infrastruktur der Landesverwaltung und ein Computersicherheits-Ereignis- und Reaktionsteam (CERT) eingerichtet. Hierfür sind 12 VZÄ beim ZIT-BB vorgesehen.

Darüber hinaus liegen beim ZIT-BB die in § 2 BbgNIS2UmsV beschriebenen Aufgaben.

Daneben besteht das Informationssicherheitsmanagement – Team (ISMT), das aus allen Informationssicherheitsbeauftragten der obersten Behörden der Landesregierung besteht.

Für Angelegenheiten zur Abwehr von Cyberspionage, Bekämpfung von Cyberkriminalität sowie BSI-Kontaktstelle in Bezug auf Kritische Infrastrukturen liegt die Zuständigkeit beim MIK. Im Geschäftsbereich des MIK werden für die Bewältigung dieser Aufgaben weitere Strukturen vorgehalten.

5. Welche Kooperationen bestehen derzeit mit dem Bund, dem BSI, dem Bundeskriminalamt, anderen Ländern oder privaten Akteuren im Bereich der Cybersicherheit?

Zu Frage 5: Nachdem das MIK Brandenburg und das BSI eine Absichtserklärung zur vertieften Kooperation im Bereich der Cyber- und IT-Sicherheit gezeichnet haben, befindet sich gegenwärtig der Entwurf dieser beabsichtigten Kooperationsvereinbarung in Abstimmung beim BSI.

Darüber hinaus kooperieren Vertreter der Landesverwaltung im VerwaltungsCERTVerbund (VCV), in der AG InfoSic des IT-Planungsrates sowie in der Länderarbeitsgruppe Cybersicherheit der Innenministerkonferenz. Die Koordinierungsstelle KRITIS im MIK ist zentrale Kontaktstelle des Landes Brandenburg nach § 8b Absatz 2 Nr. 4c BSIG. Private Akteure werden als Unterstützungsleistungen über entsprechende Dienstleistungsverträge gebunden.

6. Welche Betreiber kritischer Infrastrukturen (KRITIS) werden aktuell durch Landesbehörden betreut, beraten oder überwacht und in welchem Umfang erfolgen diese Unterstützungsmaßnahmen?

Zu Frage 6: Der Verfassungsschutz Brandenburg steht mit den Betreibern kritischer Infrastrukturen im Land in einem kontinuierlichen Austausch – sowohl über Fragen des politischen Extremismus als auch zu Themen wie Sabotage- und Cyberabwehr. Dabei unterstützt der Verfassungsschutz Brandenburg KRITIS-Einrichtungen bei Bedarf mit geeigneten Maßnahmen zur Gefahren- und Cyberabwehr und zur Stärkung der (Cyber-)Resilienz. Umfang und Art der Zusammenarbeit richten sich nach den jeweiligen Erfordernissen und erfolgen im Rahmen bestehender Zuständigkeiten.

Darüber hinaus besteht zwischen der Koordinierungsstelle KRITIS im MIK sowie dem MWAEK mit für das Land Brandenburg besonders wichtigen Betreibern aus den Branchen Gas und Elektrizität ein regelmäßiger Austausch, um unterschiedliche Lageerkenntnisse über konkrete und abstrakte Gefahren für die Versorgungssicherheit und die Sicherheit der

kritischen Infrastrukturen auszutauschen, um so die Versorgungssicherheit fortlaufend zu gewährleisten und den Schutz kritischer Infrastrukturen kontinuierlich zu verbessern.

10. Wie bewertet die Landesregierung die Cybersicherheitslage in Brandenburg insgesamt im Vergleich zur Lage in anderen ostdeutschen Flächenländern?

Zu Frage 10: Der aktuelle BSI-Lagebericht sowie das Bundeslagebild Cybercrime des BKA schätzt die Bedrohungslage durch Cyberkriminalität in Deutschland als abstrakt hoch ein. Dies gilt auch für Brandenburg sowie die anderen ostdeutschen Flächenländer. Laut Einschätzung des BKA stehen dabei vor allem öffentlichen Verwaltungen und Behörden im Fokus von sich stetig professionalisierenden Angreifern (Cybercrime-as-a-Service).