

19. Wahlperiode

Schriftliche Anfrage

der Abgeordneten Gollaleh Ahmadi (GRÜNE)

vom 24. Februar 2025 (Eingang beim Abgeordnetenhaus am 24. Februar 2025)

zum Thema:

Umsetzung der NIS-2-Richtlinie und Informationssicherheit des Landes Berlin

und **Antwort** vom 6. März 2025 (Eingang beim Abgeordnetenhaus am 11. März 2025)

Frau Abgeordnete Gollaleh Ahmadi (Grüne)

über
die Präsidentin des Abgeordnetenhauses von Berlin

über Senatskanzlei - G Sen -

Antwort

auf die Schriftliche Anfrage Nr. 19/21732

vom 24. Februar 2025

über Umsetzung der NIS-2-Richtlinie und Informationssicherheit des Landes Berlin

Im Namen des Senats von Berlin beantworte ich Ihre Schriftliche Anfrage wie folgt:

1. Welche konkreten Schritte hat Berlin bisher unternommen um die Unternehmen in der Umsetzung der NIS-2-Richtlinie zu unterstützen? Bitte um Darstellung jedweder Maßnahmen bei Nennung der begünstigten Organisation.

Zu 1.:

Die Senatsverwaltung für Wirtschaft, Energie und Betriebe hat folgende Maßnahmen ergriffen, um Berliner Unternehmen bei der Umsetzung der NIS-2-Richtlinie zu unterstützen und die IT-Sicherheit in der Unternehmenslandschaft zu verbessern:

- Informationsangebot: Die DAB Digitalagentur Berlin GmbH wurde beauftragt, ein umfassendes Informationsangebot für die NIS-2-Richtlinie zu erstellen. Dieses Angebot wurde in Zusammenarbeit mit dem Netzwerk it's.BB e.V. entwickelt und richtet sich an alle Berliner Unternehmen. Es beinhaltet relevante Informationen zur Umsetzung der Richtlinie und ist über folgende Webseite abrufbar: <https://digitalagentur.berlin/angebote/it-sicherheit/nis-2-richtlinie/>
- Kostenfreie Beratung: Betroffene Unternehmen haben die Möglichkeit, sich jederzeit für eine kostenfreie Beratung an die DAB Digitalagentur oder den it's.BB e.V. zu

wenden. Diese Beratungen sollen den Unternehmen helfen, die spezifischen Anforderungen der NIS-2-Richtlinie zu verstehen und umzusetzen.

Zudem wurden seitens Berlin Partner für Wirtschaft und Technologie eine Informationsveranstaltung für die NIS-2-Richtlinie für Unternehmen durchgeführt und in einem Video dokumentiert: <https://youtu.be/3dW0TOnbHto>

Darüber hinausgehend vermittelt das im Rahmen des Masterplan Industriestadt Berlin geförderte Projekt it's.INBerlin (<https://itsinberlin.de/>) neben Informationen zur NIS-2 Richtlinie allgemeine IT-Sicherheitsrelevante Informationen für Unternehmen.“

2. Inwieweit gibt es spezifische Richtlinien oder Empfehlungen für private Betreiber kritischer Infrastrukturen in Berlin? Bitte um Darstellung.

Zu 2.:

Der Bundesgesetzgeber plant für den Bereich der Privatwirtschaft, die NIS-2-Richtlinie vor allem durch Anpassung des BSI-Gesetzes insofern umzusetzen, als dass weitere Unternehmen dem BSI-Gesetz unterfallen sollen. Die privaten Betreiber kritischer Infrastrukturen unterfallen bereits unmittelbar dem BSI-Gesetz in der aktuellen Fassung. Es existieren zahlreiche Handreichungen des BSI. Insofern sind landesspezifische Richtlinien oder Empfehlungen speziell für die Betreiber kritischer Infrastrukturen nicht zielführend und dementsprechend nicht vorhanden. Dass kein Bedarf besteht, wird auch im engen Austausch mit den Betreibern kritischer Infrastrukturen in der von der Senatsverwaltung für Inneres und Sport betriebenen KoSt KRITIS (Koordinierungsstelle Kritische Infrastrukturen) bestätigt.

3. In welchem Umfang werden Ressourcen auf Landesebene für die Umsetzung der NIS-2- Richtlinie bereitgestellt?

Zu 3.:

Die Senatsverwaltung für Inneres und Sport hat als die für die Koordinierung der Cybersicherheit zuständige Stelle mit den in der Arbeitsgruppe Cybersicherheit bestehenden Ressourcen den sich aus der NIS-2-Richtlinie ergebenden konkreten Umsetzungsbedarf für die Berliner Landesverwaltung aufgeschlüsselt.

Das in der Antwort zu Frage 1 beschriebene Informations- und Beratungsangebot zur NIS-2-Richtlinie wird im Rahmen der bestehenden institutionellen Zuwendung der Senatsverwaltung für Wirtschaft, Energie und Betriebe an die DAB Digitalagentur Berlin GmbH bereitgestellt.

Das Informationsangebot, das im Rahmen des Projekts it's.INBerlin entstanden ist, wird im Rahmen einer Projektförderung aus dem Masterplan Industriestadt Berlin der Senatsverwaltung für Wirtschaft, Energie und Betriebe finanziert.

Für den Sektor Öffentliche Verwaltung, der unter dem Gesichtspunkt der Informationssicherheit federführend von der Senatskanzlei verantwortet wird, werden auf Landesebene zusätzliche Ressourcen im Rahmen der Umsetzung erforderlich, die zum großen Teil im Wege von vertraglichen Anpassungen zu Leistungen des ITDZ bereitzustellen sind. Der Prozess zu den erforderlichen Vertragsanpassungen wird nach gesetzlicher Umsetzung der NIS-2-Richtlinie abgeschlossen.

4. Hat der Senat Anfragen von Berliner Unternehmen erhalten zur Unterstützung in der Umsetzung der NIS-2-Richtlinie? Wie wurde mit diesen Anfragen im konkreten Einzelfall verfahren?

Zu 4.:

Es sind keine entsprechenden Anfragen bekannt.

5. Welche Auswirkungen hat die Umsetzung der NIS-2-Richtlinie im Hinblick auf das Land Berlin als Bundeshauptstadt? Bitte um Darstellung jedweder Maßnahmen, z.B. Notwendigkeit weiterer Rechtssetzungsakte.

Zu 5.:

Die bundesgesetzliche Umsetzung der NIS-2-Richtlinie wird vor allem Auswirkungen auf private Unternehmen haben, die künftig dem BSI-Gesetz unterfallen. Diese Auswirkungen können valide nur vom Bundesgesetzgeber im Rahmen des noch ausstehenden Gesetzgebungsverfahrens abgeschätzt werden. Da der Bund keine Gesetzgebungskompetenz im Hinblick auf die Berliner Verwaltung hat, muss die NIS-2-Richtlinie insoweit im Land mittels Runderlass, Verordnung oder Gesetz im betroffenen Bereich umgesetzt werden, im Zuge dessen erst die konkreten Auswirkungen für die Landesverwaltung valide abgeschätzt werden können.

Für den Sektor Öffentliche Verwaltung im Land Berlin ergeben sich im Sinne der in der Richtlinie vorgegebenen einheitlichen Umsetzung Aufwände im vergleichbaren Rahmen zu anderen Bundesländern. Die Richtlinie enthält keine spezifischen Ausführungen zu Hauptstädten der Mitgliedstaaten und unterscheidet inhaltlich zwischen nationaler und regionaler Ebene.

6. Welche Kontrollmechanismen wurden eingeführt, um die Einhaltung der NIS-2-Vorgaben auf Landesebene zu überwachen? Inwiefern wird Berlin mit dem Bund zu dem Thema zusammenarbeiten?

Zu 6.:

Eine wesentliche Anforderung der NIS-2-Richtlinie ist die einheitliche Umsetzung. Diese erfolgt, sofern nicht unmittelbar in der Richtlinie reguliert, auf Landesebene für den Sektor öffentliche Verwaltung nach den im IT-Planungsrat gefassten Beschlüssen. Berlin ist als Bundesland Mitglied des IT-Planungsrates.

Dieser hat mit Beschluss vom 03.11.2023 (Beschluss 2023/39) ein risikobasiertes Identifizierungskonzept für wichtige Einrichtungen auf regionaler Ebene i. S. von Artikel 3 Abs. 2 Satz 1 i. V. m. Nr. 10 Alternative 2 Anhang I NIS-2-Richtlinie verabschiedet. Hierdurch wird eine einheitliche Umsetzung der NIS-2-Richtlinie in den Bundesländern sichergestellt.

Für den Sektor Öffentliche Verwaltung wird die Kontrolle der Umsetzung im Rahmen des Geltungsbereiches des EGovG Berlin in der IKT-Steuerung durch den Stab des Landesbeauftragten für Informationssicherheit als zuständige Behörde erfolgen.

Das Berliner EGovernment-Gesetz (EGovG Bln) enthält in den §§ 21 und 23 bereits Regelungen zur Informationssicherheit. So sind gemäß § 23 Absatz 1 EGovG Bln alle Behörden der Berliner Verwaltung verpflichtet, ein Informations-Sicherheits-Management-System gemäß den Standards des Bundesamtes für die Sicherheit in der Informationstechnik aufzubauen und weiterzuentwickeln.

7. Welche spezifischen Herausforderungen wurden in der öffentlichen Verwaltung Berlins im Zusammenhang mit der Umsetzung der NIS-2-Richtlinie identifiziert?

Zu 7.:

Für den Sektor Öffentliche Verwaltung im Land Berlin ergeben sich vergleichbare Herausforderungen wie für Landesverwaltungen anderer Bundesländer. Spezifisch ist, dass durch das Prinzip der Einheitsgemeinde auch alle kommunalen Verwaltungssachverhalte der Anwendung der NIS-2-Richtlinie und damit deren Zielstellung unterliegen und entsprechend umzusetzen sind.

Die schon bestehenden Regelungen des EGovG Berlin werden durch weitere Umsetzungsmaßnahmen zu ergänzen sein. Diese werden derzeit vorbereitet.

8. Inwieweit werden bestehende IT-Sicherheitsmaßnahmen in der Berliner Verwaltung an die Anforderungen der NIS-2-Richtlinie angepasst?

Wenn ja, welche konkreten Schritte hat Berlin bisher unternommen, um die Anforderungen der NIS-2-Richtlinie umzusetzen?

Wenn nein, basierend auf welchen Analysen/Bewertungen hat Berlin die Entscheidung getroffen den Informationssicherheitsstandard nicht an die NIS-2-Richtlinie anzuheben?

Zu 8.:

Die Fortschreibung der Informationssicherheitsarchitektur ist Teil der Prozesse des strategischen Informationssicherheitsmanagements, die als kontinuierlicher Verbesserungsprozess zu gestalten sind. Diese Prozesse werden durch die Vorgaben aus der NIS-2-Richtlinie gestärkt und begonnene bzw. geplante Maßnahmen gestärkt. Im Fokus stehen dabei hinsichtlich des Managements und der Nutzenden Maßnahmen gemäß den Anforderungen zur Informationssicherheitssensibilisierung, aus organisatorischer Sicht verstärkter Anstrengungen zur Verbesserung der ISMS-Ressourcen der öffentlichen Verwaltung, sowie auf technischer Seite Prozesse der Absicherung der genutzten Infrastrukturen, insbesondere des Berliner Landesnetzes.

9. In welchem Rhythmus wird die IT-Sicherheit und Informationssicherheit des Landes Berlin geprüft und erneuert?

Zu 9.:

Das nach dem EGovG zu etablierende Informationssicherheitsmanagementsystem (ISMS) beinhaltet einen kontinuierlichen Verbesserungsprozess und folgt keinem festen Rhythmus. Neben regelmäßigen und anlassbezogenen Anpassungen organisatorischer Regelungen (beispielsweise Zugriffsberechtigungen, Zuständigkeiten, zulässiger Einsatz, etc.) werden auf technischer Seite verschiedenste Maßnahmen umgesetzt. Hierzu zählen u.a. die permanente Überwachung der IKT-Systeme, die regelmäßige Überprüfung auf das Vorliegen von Aktualisierungen für die IKT-Systeme zur Schließung von Schwachstellen, die Auswertung von Meldungen zu Schwachstellen und die regelmäßige oder anlassbezogene Prüfung der IKT-Systeme auf bekannte Schwachstellen mit entsprechenden Hilfsmitteln. Das ITDZ Berlin als IT-Dienstleister der Berliner Verwaltung ist zertifiziert nach ISO 27001 auf der Basis von IT-Grundschutz und wird jährlich unabhängig auditiert. Begleitet wird dieses Vorgehen mittels regelmäßiger Prozesse zum Controlling. Die Prozesse beinhalten neben dem jährlichen Bericht zu Informationssicherheit, jährliche Berichte zu Inhalten des Umsetzungsplanes zur Informationssicherheitsleitlinie des IT-Planungsrates und nach den gesetzlichen Vorgaben aus dem OZG zur IT-Sicherheitsverordnung Portalverbund.

10. Welche Maßnahmen werden ergriffen, um Mitarbeitende in der öffentlichen Verwaltung Berlins zu kontinuierlich zur Informationssicherheit zu schulen? Wie oft finden solche Schulungen statt?

Zu 10.:

Die grundlegenden Ziele, Anforderungen und die Strategie der Informationssicherheit sind in der Leitlinie zur Informationssicherheit der Landesverwaltung des Landes Berlin definiert. Ein Grundsatz der Leitlinie ist dabei die Einbindung aller Beschäftigten in den Sicherheitsmanagementprozess durch regelmäßige Schulungen und Sensibilisierung hinsichtlich der Informationssicherheit. Nach den umzusetzenden Standards des BSI liegt die Verantwortung für Informationssicherheit der Behörden und Einrichtungen bei den jeweiligen Leitungen. In Bezug auf die landesweite Sensibilisierung der Beschäftigten für Informationssicherheit ist ein Sensibilisierungs- und Schulungskonzept im Bereich Informationssicherheit für die Berliner Verwaltung in Erarbeitung. Das Awareness-Konzept zielt darauf ab, den Beschäftigten der Berliner Verwaltung ein solides Grundlagenwissen zur Informationssicherheit zu vermitteln. Zudem soll das Konzept den verantwortlichen Stellen in den Behörden eine konkrete Handlungsanweisung und Hilfestellung geben, wie sie Schulungen und Sensibilisierungen planen, durchführen und etablieren müssen, um das Informationssicherheitsniveau im Land Berlin aufrecht zu erhalten. Im Jahr 2024 wurde ein Entwurf für ein landesweites, zielgruppenspezifisches Informationssicherheits-sensibilisierungskonzept (Information Security Awareness-Konzept) zur Sensibilisierung der Beschäftigten für Informationssicherheit erstellt. Der Konzeptentwurf wird in 2025 finalisiert und den für Informationssicherheit verantwortlichen Stellen in den Behörden und Einrichtungen des Landes Berlin zur Verfügung gestellt. Erste landesweite Maßnahmen wurden mit der Verwaltungsakademie Berlin umgesetzt und sind nach Festsetzung des landesweiten Konzeptes in Vorbereitung. Damit wird die Umsetzung der bestehenden gesetzlichen Verpflichtung für die Behörden der Berliner Landesverwaltung, mindestens einmal jährlich ihre Beschäftigten zu schulen sowie eine übergreifende IT-Sicherheitsübung durchzuführen durch landesweite Maßnahmen unterstützt. Zur Unterstützung der Stellen wird eine Instanz des Behörden-IT-Sicherheitstrainings (BITS) [<https://bits.berlin-cert.verwalt-berlin.de/>] durch das Berlin-CERT im Intranet zur freien Nutzung bereitgestellt. Daneben finden in den Behörden verschiedene spezifische und zielgruppenorientierte Schulungen zur Informationssicherheit statt. In den Behörden werden auch ausgewählte Meldungen des Berlin-CERT aufbereitet und an die Beschäftigten kommuniziert.

11. Wie bewertet das Land Berlin die Zusammenarbeit zwischen dem CERT-Bund sowie den CERTs der anderen Bundesländer und dem CERT-Berlin? Gibt es einen automatisierten Austausch oder wird dieser manuell geteilt?

Zu 11.:

Die Zusammenarbeit des Berlin-CERT mit den CERTs der anderen Länder und dem CERT Bund erfolgt auf der Basis des vom IT-Planungsrat beschlossenen Mindeststandards CERT (https://www.it-planungsrat.de/fileadmin/beschluesse/2022/Beschluss2022-08_Mindeststandard_CERT.pdf). Im Mindeststandard sind die Aufgaben und Formen der Zusammenarbeit beschrieben. Sie beinhalten automatisierten Austausch über Plattformen ebenso wie anlass- bzw. ereignisbezogenen manuellen Dialog. Zur Umsetzung des Mindeststandards wird im Rahmen der Umsetzung der Informationssicherheitsleitlinie des IT-Planungsrates jährlich berichtet. Die verpflichtenden Anforderungen des Mindeststandards werden vom Berlin-CERT vollständig erfüllt.

12. Wurde ein Kooperationsvertrag zwischen dem Land Berlin und dem BSI abgeschlossen? Wenn nein, bis wann ist dies geplant?

Zu 12.:

Die Wahrung der Cyber- und Informationssicherheit und die Verteidigung gegen Cyber-Angriffe sind eine gesamtstaatliche Aufgabe, die nur gemeinsam von Bund und Ländern zu bewältigen ist. Im Rahmen der Bund-Länder-Zusammenarbeit beabsichtigt das Land Berlin den Abschluss einer Kooperationsvereinbarung im Bereich Cyber- und Informationssicherheit zwischen dem BSI und dem Land Berlin. In Vorbereitung des geplanten Abschlusses wurde von der Stabsstelle des Landesbevollmächtigten für Informationssicherheit im Jahr 2024 ein fachlicher Austausch mit dem BSI initiiert. Hierbei wurde die Auswahl sowie die konkrete Ausgestaltung von möglichen Kooperationsfeldern zwischen den künftigen Kooperationspartnern besprochen. Für das Jahr 2025 ist nach der finalen Auswahl der Kooperationsfelder und Festlegung der Inhalte der Abschluss der Kooperationsvereinbarung geplant.

Berlin, den 6. März 2025

In Vertretung

Christian Hochgrebe
Senatsverwaltung für Inneres und Sport