Verwaltungsvorschrift zur Umsetzung der NIS-2-Richtlinie in der Freien Hansestadt Bremen (VV NIS2Ums FHB)

Vom 14. Januar 2025

Inkrafttreten: 15.01.2025
Fundstelle: Brem.ABl. 2025, 42

Vom 14. Januar 2025

Der Senat der Freien Hansestadt Bremen erlässt zur Umsetzung der Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie) in der Freien Hansestadt Bremen folgende Verwaltungsvorschrift:

Präambel

Am 16. Januar 2023 ist die Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie) nach Veröffentlichung am 27. Dezember 2022 im Amtsblatt der Europäischen Union in Kraft getreten. Die Mitgliedstaaten müssen die Richtlinie bis zum 17. Oktober 2024 in nationales Recht umsetzen.

Die NIS-2-Richtlinie verfolgt das übergreifende Ziel, den europäischen Binnenmarkt resilienter gegenüber Bedrohungen aus dem Cyberraum zu machen. Große Unterschiede zwischen den Mitgliedstaaten sollen beseitigt werden, indem insbesondere Mindestvorschriften für einen funktionierenden und koordinierten Rechtsrahmen festgelegt werden, Mechanismen für die wirksame Zusammenarbeit zwischen den zuständigen Behörden in den einzelnen Mitgliedstaaten vorgesehen werden, die Liste der Sektoren und Tätigkeiten, die Pflichten im Hinblick auf die Cybersicherheit unterliegen, aktualisiert

wird und wirksame Abhilfemaßnahmen und Durchsetzungsmaßnahmen, die für die wirksame Durchsetzung dieser Verpflichtungen von entscheidender Bedeutung sind, eingeführt werden.

Durch die Richtlinie werden überwiegend Unternehmen adressiert. Aber auch die öffentliche Verwaltung ist betroffen. Ihr kommt eine Sonderrolle zu, da sie durch ihre staatlichen Dienste maßgeblichen Einfluss auf wirtschaftliche Tätigkeiten und damit die Funktionsfähigkeit des Binnenmarkts hat.

Die Umsetzung der NIS-2-Richtlinie erfolgt für den Mitgliedsstaat Deutschland im Wesentlichen durch das Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz). Gemäß der grundgesetzlichen Kompetenzordnung besitzt der Bund dabei die Regelungsbefugnis für den Bereich der Wirtschaft und für die Bundesverwaltung. Den Ländern obliegt hingegen die Umsetzung hinsichtlich der ihrer Hoheit unterliegenden Landesverwaltung. Hierbei verpflichtet die Richtlinie zur Identifizierung von Einrichtungen der öffentlichen Verwaltung auf regionaler Ebene, die nach einer risikobasierten Bewertung Dienste erbringen, deren Störung erhebliche Auswirkungen auf kritische gesellschaftliche oder wirtschaftliche Tätigkeiten haben könnte. Der regionalen Ebene sind insoweit die in den Ressorts zu verortenden Teile der unmittelbaren Landesverwaltung zuzuordnen. Diese werden durch die vorliegende Verwaltungsvorschrift angesprochen.

§ 1
Begriffsbestimmungen

(1) Im Sinne dieser Verwaltungsvorschrift ist oder sind

1. eine „kritische Einrichtung der Landesverwaltung“ eine organisatorisch hinreichend verselbstständigte Stelle der öffentlichen Verwaltung auf Ebene der unmittelbaren Landesverwaltung, die gemäß § 2 Absatz 2 innerhalb der Ressorts als kritisch ermittelt worden ist;

2. „Informationstechnik“ jedes technische Mittel zur Verarbeitung von Informationen;

3. „Sicherheit in der Informationstechnik“ die Gewährleistung der Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit mittels Informationstechnik verarbeiteter Daten oder mittels Informationstechnik angebotener oder zugänglicher Dienste auf einem bestimmten Vertrauensniveau;

4.

„Bedrohungen in der Informationstechnik“ alle möglichen Umstände, Ereignisse und Handlungen, die die Sicherheit in der Informationstechnik beeinträchtigen und dadurch Schäden oder andere negative Folgen verursachen können;

5. „erhebliche Bedrohungen in der Informationstechnik“ solche Bedrohungen in der Informationstechnik, die informationstechnischen Systeme einer Einrichtung oder der Nutzer solcher Systeme aufgrund ihrer technischen Merkmale erheblich beeinträchtigen können, indem sie erhebliche materielle oder immaterielle Schäden verursachen;

6. ein „Sicherheitsvorfall“ ein Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit mittels Informationstechnik verarbeiteter Daten oder mittels Informationstechnik angebotener oder zugänglicher Dienste beeinträchtigt;

7. ein „erheblicher Sicherheitsvorfall“ vorbehaltlich Absatz 2 ein Sicherheitsvorfall, der
   a) schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann, oder

   b) andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann;

8. ein „Beinahe-Vorfall“ ein Ereignis, das die Verfügbarkeit, Authentizität Integrität oder Vertraulichkeit mittels Informationstechnik verarbeiteter Daten oder mittels Informationstechnik angebotener oder zugänglicher Dienste beeinträchtigt haben könnte, dessen Eintritt jedoch erfolgreich verhindert worden oder aus anderen Gründen nicht erfolgt ist;

9. „Bewältigung von Sicherheitsvorfällen“ ein Oberbegriff für alle Maßnahmen und Verfahren zur Verhütung, Erkennung, Analyse und Eindämmung von Sicherheitsvorfällen oder die Reaktion darauf und die Erholung davon;

10. ein „Risiko“ das Potenzial für Verluste oder Störungen, die durch einen Sicherheitsvorfall verursacht werden, das als eine Kombination des Ausmaßes eines solchen Verlusts oder einer solchen Störung und der Wahrscheinlichkeit des Eintretens des Sicherheitsvorfalls zum Ausdruck gebracht wird;

11. ein „IKT-Produkt“ ein Element oder eine Gruppe von Elementen eines informationstechnischen Systems;

12.

ein „IKT-Dienst“ ein Dienst, der vollständig oder überwiegend aus der Übertragung, Speicherung, Abfrage oder Verarbeitung von Informationen mittels eines informationstechnischen Systems besteht;

13. ein „IKT-Prozess“ eine Bezeichnung für jegliche Tätigkeiten, mit denen ein ITK-Produkt oder -Dienst konzipiert, entwickelt, bereitgestellt oder gepflegt werden soll;

14. eine „Schwachstelle“ eine Schwäche, Anfälligkeit oder Fehlfunktion von IKT-Produkten oder IKT-Diensten, die ausgenutzt werden und so die Sicherheit in der Informationstechnik beeinträchtigen kann;

15. ein „Schwachstellenscan“ eine proaktive Überprüfung informationstechnischer Systeme auf Schwachstellen mit potenziell signifikanten Auswirkungen.

(2) Soweit die Europäische Kommission für kritische Einrichtungen der Landesverwaltung einen Durchführungsrechtsakt gemäß Artikel 23 Absatz 11 Unterabsatz 2 Satz 2 der NIS-2-Richtlinie erlässt, worin näher bestimmt wird, in welchen Fällen nach Absatz 1 Nummer 7 ein Sicherheitsvorfall als erheblich anzusehen ist, sind dessen Vorgaben zu beachten.

§ 2
Geltungsbereich

(1) Die nachfolgenden Bestimmungen gelten für alle kritischen Einrichtungen der Landesverwaltung soweit nicht ausdrücklich etwas anderes bestimmt ist.

(2) Kritische Einrichtungen der Landesverwaltung werden als wichtige Einrichtungen im Sinne des Artikel 3 Absatz 2 Satz 1 in Verbindung mit Nummer 10 Alternative 2 Anhang I der NIS-2-Richtlinie auf Grundlage von Artikel 2 Absatz 2 Buchstabe f Ziffer ii der NIS-2-Richtlinie gemäß dem vom IT-Planungsrat in seiner 42. Sitzung am 3. November 2023 beschlossene Identifizierungskonzept (Beschluss 2023/39) ermittelt. Die Senatskanzlei und die senatorischen Behörden gelten dabei als formal identifiziert. Sie wenden das Identifizierungskonzept für ihre jeweils nachgeordneten Einrichtungen der öffentlichen Verwaltung auf Ebene der unmittelbaren Landesverwaltung erstmals zum 17. Oktober 2024 und in der Folge alle zwei Jahre in eigener Verantwortung an und teilen die Ergebnisse der zuständigen Behörde gemäß § 3 Absatz 1 mit.

(3) Bestehende Regelungen zur Sicherheit in der Informationstechnik in der öffentlichen Verwaltung bleiben unberührt.

§ 3
Zuständigkeit und Aufgaben

(1) Die Zentralstelle Cybersicherheit (Zentralstelle) beim Senator für Inneres und Sport nimmt die Aufgaben als zuständige Behörde im Sinne des Artikel 8 Absatz 1 der NIS-2-Richtlinie war. Sie überwacht insbesondere die Einhaltung der nach dieser Verwaltungsvorschrift für kritische Einrichtungen der Landesverwaltung geltenden Verpflichtungen. Innerhalb der Zentralstelle wird die Position der oder des Chief Cyber Security Officer (CCSO) geschaffen. Maßnahmen nach § 12 Absatz 1 und 2 dürfen nur durch sie oder ihn angeordnet werden. Sie oder er handelt bei entsprechenden Anordnungen unabhängig. Sie oder er ist befugt bei Verstößen unmittelbar mit der Leitung der betroffenen kritischen Einrichtung der Landesverwaltung und erforderlichenfalls mit dem zuständigen Senatsmitglied in Kontakt zu treten und zu berichten.

(2) Die Zentralstelle nimmt die Aufgaben eines Computer Security Incident Response Team (CSIRT) im Sinne der Artikel 10 und 11 der NIS-2-Richtlinie für die kritischen Einrichtungen der Landesverwaltung wahr. Soweit dies für die jeweilige Aufgabe erforderlich ist, muss sie die dafür notwendigen technischen Fähigkeiten besitzen sowie insbesondere die Anforderungen des Artikel 11 Absatz 1 der NIS-2-Richtlinie einhalten. Die Zentralstelle kann zur Erfüllung ihrer Aufgaben Dritte beauftragen; ihre Verantwortlichkeit bleibt dabei bestehen. Die Aufgaben des CSIRT sind:

1. Überwachung und Analyse von Bedrohungen in der Informationstechnik, Schwachstellen und Sicherheitsvorfällen;

2. auf Ersuchen Bereitstellung von Unterstützung für betreffende kritische Einrichtungen der Landesverwaltung hinsichtlich der Überwachung ihrer Informationstechnik in Echtzeit oder nahezu in Echtzeit;

3. Ausgabe von Frühwarnungen und Alarmmeldungen sowie Bekanntmachung und Weitergabe von Informationen über Bedrohungen in der Informationstechnik, Schwachstellen und Sicherheitsvorfälle an die kritischen Einrichtungen der Landesverwaltung sowie an die zuständigen Behörden und andere einschlägige Interessenträger, möglichst echtzeitnah;

4. Reaktion auf Sicherheitsvorfälle und auf Ersuchen technische Unterstützung der betreffenden kritischen Einrichtungen der Landesverwaltung bei solchen;

5. Erhebung und Analyse forensischer Daten sowie dynamische Analyse von Risiken und Sicherheitsvorfällen sowie Lagebeurteilung im Hinblick auf die Cybersicherheit;

6. auf Ersuchen die Durchführung von Schwachstellenscans bei betreffenden kritischen Einrichtungen der Landesverwaltung;

7.

Beteiligung am CSIRTs-Netzwerk im Sinne des Artikel 15 der NIS- 2-Richtlinie und – im Rahmen ihrer Kapazitäten und Kompetenzen – auf Gegenseitigkeit beruhende Unterstützung anderer Mitglieder des CSIRTs-Netzwerks auf deren Ersuchen;

8. Beitrag zum Einsatz sicherer Instrumente für den Informationsaustausch gemäß Artikel 10 Absatz 3 der NIS-2-Richtlinie.

Die Zentralstelle darf auf Grundlage eines risikobasierten Ansatzes Aufgaben nach Satz 4 priorisieren. Für Leistungen nach Satz 4, die auf Ersuchen erbracht werden, kann die Zentralstelle Kosten erheben. Die Möglichkeit der Einbeziehung weiterer Einrichtungen außerhalb des Geltungsbereichs dieser Verwaltungsvorschrift in den Aufgabenkreis nach Satz 4 bleibt unberührt.

(3) Die Zentralstelle ist zur Erfüllung ihrer Aufgaben als zuständige Behörde und CSIRT mit angemessenen Ressourcen auszustatten. Dabei ist auch für eine angemessene Personalausstattung zu sorgen, damit das CSIRT seine technischen Fähigkeiten entwickeln kann.

(4) Die Zentralstelle arbeitet bei der Erfüllung ihrer Aufgaben nach Absatz 1 und Absatz 2 mit den anderen zuständigen Behörden und den CSIRTs des Bundes und der Länder, einschließlich des Bundesamtes für Sicherheit in der Informationstechnik als zentrale Anlaufstelle im Sinne des Artikel 8 Absatz 3 der NIS-2-Richtlinie sowie den Strafverfolgungsbehörden, den Datenschutzbehörden, den nationalen Behörden gemäß den Verordnungen (EG) Nr. 300/2008 und (EU) 2018/1139, den Aufsichtsstellen gemäß der Verordnung (EU) Nr. 910/2014, den gemäß der Verordnung (EU) 2022/2554 zuständigen Behörden, den nationalen Regulierungsbehörden gemäß der Richtlinie (EU) 2018/1972, den gemäß der Richtlinie (EU) 2022/2557 zuständigen Behörden sowie im Rahmen anderer sektorspezifischer Rechtsakte der Union innerhalb des jeweiligen Mitgliedstaats zuständiger Behörden zusammen.

§ 4
Liste kritischer Einrichtungen der Landesverwaltung

(1) Die Zentralstelle führt eine Liste der erfassten kritischen Einrichtungen der Landesverwaltung, die neben den Namen weitere relevante Informationen enthält. Zu diesem Zweck teilen die kritischen Einrichtungen der Landesverwaltung der Zentralstelle spätestens bis zum 17. Januar 2025 erstmals Folgendes mit:

1. ihre Anschriften;

2.

aktuelle Kontaktdaten, einschließlich E-Mail-Adressen und Telefonnummern, der Leitung und, sofern vorhanden, der oder des jeweiligen Informationssicherheitsbeauftragten;

3. ihre IP-Adressbereiche.

Werden infolge des Verfahrens nach § 2 Absatz 2 Satz 3 bisher nicht erfasste kritische Einrichtungen der Landesverwaltung ermittelt, teilen diese die Angaben nach Satz 2 innerhalb von drei Monaten nach ihrer Erfassung mit. Sind infolge des Verfahrens nach § 2 Absatz 2 Satz 3 bisher erfasste Einrichtungen nicht mehr als kritische Einrichtungen der Landesverwaltung zu bewerten, sind sie von der Liste zu entfernen und die Angaben nach Satz 2 zu löschen.

(2) Die kritischen Einrichtungen der Landesverwaltung teilen alle Änderungen der nach Absatz 1 Satz 2 übermittelten Angaben unverzüglich, spätestens jedoch innerhalb von zwei Wochen mit.

(3) Die Zentralstelle überprüft regelmäßig, mindestens jedoch alle zwei Jahre, die Aktualität und Vollständigkeit der Liste sowie die Durchführung des Verfahrens nach § 2 Absatz 2 Satz 3.

(4) Die Liste ist gemäß der Verschlusssachenanweisung für das Land Bremen zu klassifizieren.

(5) Die Zentralstelle übermittelt dem Bundesamt für Sicherheit in der Informationstechnik in seiner Funktion als zentrale Anlaufstelle im Sinne des Artikel 8 Absatz 3 der NIS-2-Richtlinie erstmalig zum 27. März 2025 und danach alle zwei Jahre die Anzahl der erfassten kritischen Einrichtungen der Landesverwaltung.

§ 5
Risikomanagementmaßnahmen

(1) Kritische Einrichtungen der Landesverwaltung sind verpflichtet, geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen zu ergreifen, um die Risiken für die Informationstechnik, die sie für die Erbringung ihrer Dienste nutzen, zu beherrschen und die Auswirkungen von Sicherheitsvorfällen auf ihre oder andere Dienste zu verhindern oder möglichst gering zu halten. Bei der Bewertung der Verhältnismäßigkeit nach Satz 1 sind das Ausmaß der Risikoexposition der Einrichtung, die Größe der Einrichtung, die Umsetzungskosten und die Eintrittswahrscheinlichkeit und Schwere von Sicherheitsvorfällen sowie ihre gesellschaftlichen und wirtschaftlichen Auswirkungen zu berücksichtigen. Die Einhaltung der Verpflichtung nach Satz 1 ist durch die Einrichtungen zu dokumentieren.

(2) Maßnahmen nach Absatz 1 sollen den Stand der Technik einhalten, die einschlägigen europäischen und internationalen Normen berücksichtigen und müssen auf einem gefahrenübergreifenden Ansatz beruhen. Die Maßnahmen müssen zumindest Folgendes umfassen:

1. Konzepte in Bezug auf die Risikoanalyse und auf die Sicherheit in der Informationstechnik,

2. Bewältigung von Sicherheitsvorfällen,

3. Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement,

4. Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern,

5. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, einschließlich Management und Offenlegung von Schwachstellen,

6. Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen zur Sicherheit in der Informationstechnik,

7. grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen zur Sicherheit in der Informationstechnik,

8. Konzepte und Verfahren für den Einsatz von Kryptografie und Verschlüsselung,

9. Sicherheit des Personals, Konzepte für die Zugriffskontrolle und für das Management von Anlagen,

10. Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

(3) Bei der Erwägung geeigneter Maßnahmen nach Absatz 2 Nummer 4 berücksichtigen die kritischen Einrichtungen der Landesverwaltung

1. die spezifischen Schwachstellen der einzelnen unmittelbaren Anbieter und Diensteanbieter sowie die Gesamtqualität der Produkte und der

Cybersicherheitspraxis ihrer Anbieter und Diensteanbieter, einschließlich der Sicherheit ihrer Entwicklungsprozesse, und

2. die Ergebnisse der gemäß Artikel 22 Absatz 1 der NIS-2-Richtlinie durchgeführten koordinierten Risikobewertungen kritischer Lieferketten.

(4) Soweit die Europäische Kommission für kritische Einrichtungen der Landesverwaltung einen Durchführungsrechtsakt gemäß Artikel 21 Absatz 5 Unterabsatz 2 der NIS-2-Richtlinie erlässt, in dem die technischen und methodischen Anforderungen sowie erforderlichenfalls die sektoralen Anforderungen der in Absatz 2 genannten Maßnahmen festgelegt werden, sind dessen Vorgaben zu beachten.

§ 6
Verwendung zertifizierter IKT-Produkte, -Dienste und -Prozesse

(1) Die Zentralstelle kann im Benehmen mit der oder dem Informationssicherheitsbeauftragten des Landes Empfehlungen aussprechen, welche von kritischen Einrichtungen der Landesverwaltung eingesetzten IKT-Produkte, - Dienste oder -Prozesse über eine Cybersicherheitszertifizierung gemäß europäischer Schemata nach Artikel 49 der Verordnung (EU) 2019/881 verfügen sollten, da sie für die Erbringung der kritischen Dienste der Einrichtung maßgeblich sind und Art und Ausmaß des Risikos eine verpflichtende Verwendung erforderlich machen. Die Verwendung solcher Produkte, Dienste und Prozesse dient auch dem Nachweis der Erfüllung bestimmter in § 5 genannter Anforderungen. Die Entscheidungskompetenzen innerhalb der Ressorts bleiben unberührt.

(2) Soweit die Europäische Kommission für kritische Einrichtungen der Landesverwaltung einen Durchführungsrechtsakt gemäß Artikel 24 Absatz 2 der NIS-2-Richtlinie erlässt, sind dessen Vorgaben zur verpflichtenden Verwendung bestimmter zertifizierter IKT-Produkte, -Dienste und -Prozesse zu beachten.

§ 7
Leitungsverantwortung und Schulungen

(1) Die Leitung einer kritischen Einrichtung der Landesverwaltung ist verpflichtet, die von ihrer Einrichtung nach § 5 zu ergreifenden Risikomanagementmaßnahmen zu billigen und ihre Umsetzung zu überwachen. Die Haftungsregeln des öffentlichen Dienstrechts und der Amtshaftung bleiben unberührt.

(2) Die Leitung einer kritischen Einrichtung der Landesverwaltung muss regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Risikomanagementpraktiken im Bereich der Sicherheit in

der Informationstechnik und deren Auswirkungen auf die von ihrer Einrichtung erbrachten Dienste zu erwerben. Sie stellen sicher, dass zu diesem Zweck auch ihren sonstigen Mitarbeiterinnen und Mitarbeitern die Teilnahme an entsprechenden Schulungen ermöglicht wird.

§ 8
Meldung erheblicher Sicherheitsvorfälle

(1) Kritische Einrichtungen der Landesverwaltung sind verpflichtet bei sie betreffenden erheblichen Sicherheitsvorfällen an die Zentralstelle über den von ihr festgelegten Informationsweg folgende Meldungen zu machen:

1. unverzüglich, spätestens jedoch innerhalb von 24 Stunden nach Kenntniserlangung, eine frühe Erstmeldung, in der angegeben wird, ob der Verdacht besteht, dass der erhebliche Sicherheitsvorfall auf rechtswidrige oder böswillige Handlungen zurückzuführen ist oder grenzüberschreitende Auswirkungen haben könnte;

2. unverzüglich, spätestens jedoch innerhalb von 72 Stunden nach Kenntniserlangung, eine Meldung, die die in Nummer 1 genannten Informationen bestätigt oder aktualisiert und eine erste Bewertung des erheblichen Sicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen enthält; soweit möglich sind die Kompromittierungsindikatoren anzugeben;

3. auf Ersuchen der Zentralstelle eine Zwischenmeldung über relevante Statusaktualisierungen;

4. vorbehaltlich Absatz 2 spätestens einen Monat nach Meldung gemäß Nummer 2 eine Abschlussmeldung, die Folgendes enthält:
   a) eine ausführliche Beschreibung des Sicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen;

   b) Angaben zur Art der Bedrohung beziehungsweise zugrundeliegenden Ursache, die wahrscheinlich den Sicherheitsvorfall ausgelöst hat;

   c) Angaben zu den getroffenen und laufenden Abhilfemaßnahmen;

   d) soweit möglich die grenzüberschreitenden Auswirkungen des Sicherheitsvorfalls.

(2) Dauert der erhebliche Sicherheitsvorfall zum in Absatz 1 Nummer 4 genannten Zeitpunkt noch an, legt die betroffene Einrichtung statt einer Abschlussmeldung zu diesem

Zeitpunkt eine Fortschrittsmeldung und eine Abschlussmeldung innerhalb eines Monats nach Abschluss der Bearbeitung des erheblichen Sicherheitsvorfalls vor.

(3) Die Zentralstelle übermittelt der betroffenen kritischen Einrichtung der Landesverwaltung unverzüglich, jedoch möglichst innerhalb von 24 Stunden nach Eingang der frühen Erstmeldung im Sinne von Absatz 1 Nummer 1 eine Antwort, einschließlich einer ersten Rückmeldung zu dem erheblichen Sicherheitsvorfall und, auf Ersuchen der Einrichtung, Orientierungshilfen oder operativer Beratung für die Durchführung möglicher Abhilfemaßnahmen. Auf Ersuchen leistet die Zentralstelle in ihrer Funktion als CSIRT zusätzliche technische Unterstützung. Wird bei dem erheblichen Sicherheitsvorfall ein krimineller Hintergrund vermutet, sollen die betroffenen kritischen Einrichtungen der Landesverwaltung die zuständigen Strafverfolgungsbehörden informieren. Die Zentralstelle gibt dafür Orientierungshilfen.

(4) Die Zentralstelle übermittelt dem Bundesamt für Sicherheit in der Informationstechnik in dessen Funktion als zentrale Anlaufstelle im Sinne des Artikel 8 Absatz 3 der NIS-2-Richtlinie

1. im Fall eines grenz- oder sektorenübergreifenden erheblichen Sicherheitsvorfalls im Sinne von Artikel 21 Absatz 1 Unterabsatz 3 der NIS-2-Richtlinie unverzüglich die nach Absatz 1 und Absatz 2 gemeldeten einschlägigen Informationen;

2. zum Zwecke der Erstellung eines zusammenfassenden Berichts nach Artikel 23 Absatz 9 der NIS-2-Richtlinie erstmalig zum 5. April 2025 und danach alle drei Monate anonymisierte und aggregierte Daten zu nach diesem Paragraphen gemeldeten erheblichen Sicherheitsvorfällen.

(5) Soweit die Europäische Kommission für kritische Einrichtungen der Landesverwaltung einen Durchführungsrechtsakt gemäß Artikel 23 Absatz 11 Unterabsatz 1 der NIS-2-Richtlinie erlässt, in dem die Art der Angaben, das Format oder das Verfahren der Meldungen nach diesem Paragraphen festgelegt werden, sind dessen Vorgaben einzuhalten.

§ 9
Freiwillige Meldungen und Mitteilungen

(1) Kritische Einrichtungen der Landesverwaltung können über ihre Verpflichtungen nach § 8 hinaus der Zentralstelle auch freiwillig Meldung über sie betreffende sonstige Sicherheitsvorfälle oder Beinahe-Vorfälle machen. Für das Meldeverfahren gilt § 8 Absatz 1 bis 3 entsprechend. Pflichtmeldungen sollen vorrangig vor freiwilligen Meldungen bearbeitet werden.

(2) Sonstige die Cyber- und Informationssicherheit betreffende Informationen, insbesondere zu Bedrohungen in der Informationstechnik, nimmt die Zentralstelle im Rahmen ihrer allgemeinen Aufgaben und als CSIRT jederzeit und von jeder Einrichtung oder Person entgegen.

(3) Unbeschadet der Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten dürfen die freiwilligen Meldungen und Mitteilungen nach Absatz 1 und 2 nicht dazu führen, dass der meldenden Einrichtung zusätzliche Verpflichtungen auferlegt werden, die nicht für sie gegolten hätten, wenn die Meldung oder Mitteilung nicht erfolgt wäre.

(4) § 8 Absatz 4 und Absatz 5 findet für freiwillige Meldungen und Mitteilungen nach Absatz 1 und 2 mit folgenden Maßgaben entsprechend Anwendung:

1. § 8 Absatz 4 Nummer 1 betrifft nur grenz- oder sektorenübergreifende Sicherheitsvorfälle;

2. § 8 Absatz 4 Nummer 2 betrifft nur Daten zu erheblichen Beinahe-Vorfälle und erheblichen Bedrohungen in der Informationstechnik.

(5) Gemäß der Informationssicherheitsleitlinie der Freien Hansestadt Bremen bestehende Melde- und Mitteilungspflichten bleiben unberührt.

§ 10
Unterrichtung betroffener Kreise und der Öffentlichkeit

(1) Soweit ein erheblicher Sicherheitsvorfall die Erbringung von Diensten durch die betroffene kritische Einrichtung der Landesverwaltung beeinträchtigen könnte, unterrichtet die Einrichtung die Empfänger der jeweiligen Dienste unverzüglich über diesen erheblichen Sicherheitsvorfall. Dies kann auch durch eine Veröffentlichung im Internet erfolgen.

(2) Soweit von einem mittels Informationstechnik angebotenen oder zugänglichen Dienst einer kritischen Einrichtung der Landesverwaltung eine erhebliche Bedrohung in der Informationstechnik für die Empfänger dieses Dienstes ausgeht, teilt die Einrichtung den potenziell betroffenen Empfängern alle Maßnahmen oder Abhilfemaßnahmen mit, die sie als Reaktion auf diese Bedrohung ergreifen können. Soweit die Europäische Kommission für kritische Einrichtungen der Landesverwaltung einen Durchführungsrechtsakt gemäß Artikel 23 Absatz 11 Unterabsatz 1 der NIS-2-Richtlinie erlässt, in dem die Art der Angaben, das Format oder das Verfahren der Mitteilungen nach diesem Absatz festgelegt ist, sind dessen Vorgaben einzuhalten.

(3) Soweit eine Sensibilisierung der Öffentlichkeit erforderlich ist, um einen erheblichen Sicherheitsvorfall zu verhindern oder einen laufenden erheblichen Sicherheitsvorfall zu bewältigen, oder soweit das öffentliche Interesse an der Offenlegung des erheblichen Sicherheitsvorfalls sonst überwiegt, kann die Zentralstelle nach Anhörung der betroffenen kritischen Einrichtung der Landesverwaltung die Öffentlichkeit über den erheblichen Sicherheitsvorfall informieren oder die Einrichtung verpflichten, dies zu tun.

§ 11
Nicht intrusive Überprüfungen bei öffentlich zugänglichen Systemen

Um von kritischen Einrichtungen der Landesverwaltung genutzte anfällige oder unsicher konfigurierte informationstechnische Systeme, Schwachstellen und andere Sicherheitsrisiken, zu ermitteln, kann die Zentralstelle an den öffentlich zugänglichen Schnittstellen dieser Systeme proaktive nicht intrusive Überprüfungen durchführen. Sie unterrichtet die für den Betrieb des Systems verantwortliche Stelle, die zuständigen Informationssicherheitsbeauftragten der betroffenen Einrichtung und Ressorts sowie die Informationssicherheitsbeauftragte oder den Informationssicherheitsbeauftragten des Landes über die Ergebnisse. Soweit ein unmittelbares Tätigwerden erforderlich ist, kann auch der mit dem Betrieb beauftragte Dienstleister direkt informiert werden. Die Überprüfungen dürfen keinerlei nachteilige Auswirkung auf die Arbeits- und Funktionsfähigkeit der betroffenen Einrichtungen haben.

§ 12
Kontrolle und Aufsicht

(1) Um die Einhaltung der Maßnahmen nach § 5 zu überprüfen, kann die Zentralstelle in ihrer Funktion als zuständige Behörde gemäß § 3 Absatz 1 ab dem 17. Oktober 2026 von den kritischen Einrichtungen der Landesverwaltung diese Maßnahmen betreffende Auskünfte sowie die Überlassung von entsprechender Unterlagen verlangen. Rechtfertigen Tatsachen die Annahme, dass die Maßnahmen nach § 5 nicht oder nicht hinreichend umgesetzt sind, informiert die Zentralstelle die betroffene Einrichtung sowie, sofern vorhanden, deren übergeordnete Behörde. Die betroffene Einrichtung hat sich daraufhin zu erklären und innerhalb einer ihr von der Zentralstelle gesetzten angemessenen Frist entweder die bisherige Erfüllung der Verpflichtung nachzuweisen oder die erforderlichen Maßnahmen zu deren Erfüllung zu ergreifen und dies nachzuweisen. Besteht der Verdacht nach Satz 2 auch noch nach anschließender erneuter Überprüfung, kann die Zentralstelle im Einvernehmen mit der der Einrichtung übergeordneten Behörde einen Nachweis durch Zertifizierungen, Prüfungen oder Audits verlangen. Anordnungen nach Satz 4 können gegenüber obersten Landesbehörden nicht ergehen.

(2) Um die Einhaltung der sonstigen nach dieser Verwaltungsvorschrift bestehenden Verpflichtungen zu überprüfen, kann die Zentralstelle in ihrer Funktion als zuständige Behörde gemäß § 3 Absatz 1 ab dem 17. Oktober 2026 von den kritischen Einrichtungen der Landesverwaltung entsprechende Auskünfte sowie die Überlassung etwaig vorhandener Unterlagen verlangen. Rechtfertigen Tatsachen die Annahme, dass die Einrichtung ihren Verpflichtungen nicht oder nicht hinreichend nachkommt, fordert sie die betroffene Einrichtung zur Einhaltung und gegebenenfalls zur Nachbesserung innerhalb einer angemessenen Frist auf und informiert, sofern vorhanden, die der Einrichtung übergeordnete Behörde.

(3) Unbeschadet der Zuständigkeiten und Aufgaben der Aufsichtsbehörden gemäß der Verordnung (EU) 2016/679 arbeitet die Zentralstelle in ihrer Funktion als zuständigen Behörde gemäß § 3 Absatz 1 bei der Bearbeitung von Sicherheitsvorfällen, die zur Verletzung des Schutzes personenbezogener Daten führen, eng mit den Aufsichtsbehörden gemäß jener Verordnung zusammen. Stellt die Zentralstelle im Zuge der Beaufsichtigung fest, dass der Verstoß einer kritischen Einrichtung der Landesverwaltung gegen die in den §§ 5, 8 und 10 festgelegten Verpflichtungen eine Verletzung des Schutzes personenbezogener Daten im Sinne von Artikel 4 Nummer 12 der Verordnung (EU) 2016/679 zur Folge haben kann, die gemäß Artikel 33 der genannten Verordnung zu melden ist, unterrichtet sie unverzüglich die in Artikel 55 oder 56 jener Verordnung genannten zuständigen Aufsichtsbehörden. Ist die gemäß der Verordnung (EU) 2016/679 zuständige Aufsichtsbehörde in einem anderen Mitgliedstaat angesiedelt, so setzt die Zentralstelle die zur Übermittlung der Information zuständige nationale Aufsichtsbehörde über die mögliche Verletzung des Schutzes personenbezogener Daten nach Satz 2 in Kenntnis.

§ 13
Cybersicherheitsstrategie

Die Zentralstelle stellt sicher, dass die Bremische Cybersicherheitsstrategie den Anforderungen nach Artikel 7 Absatz 1 und 2 der NIS-2-Richtlinie entspricht. Sie evaluiert diese im Jahr 2025 und danach mindestens alle 5 Jahre auf der Grundlage wesentlicher Leistungsindikatoren, die erforderlichenfalls aktualisiert werden.

§ 14
Inkrafttreten

Diese Verwaltungsvorschrift tritt am 15. Januar 2025 in Kraft.

Bremen, den 14. Januar 2025

Der Senat