In der Senatssitzung am 14. Januar 2025 beschlossene Fassung

Der Senator für Inneres und Sport

10.01.2025

Tischvorlage
für die Sitzung des Senats am 14.01.2024

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

A. Problem

Die Bedrohungslage aus dem Cyberraum ist, nicht zuletzt auch durch den völkerrechtswidrigen russischen Angriff auf die Ukraine, aktuell so hoch wie nie. Gleichzeitig führt die fortschreitende Digitalisierung dazu, dass Prozesse und Dienstleistungen zunehmend auf informationstechnische Systeme angewiesen sind und allgemein die Vernetzung weiter zunimmt. Ein besonders hohes Risiko ergibt sich dadurch im Bereich kritischer Infrastrukturen, deren Ausfall weitreichende wirtschaftliche und gesellschaftliche Folgen haben kann.

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 dabei eine Sonderrolle zu, da sie durch ihre staatlichen Dienste maßgeblichen Einfluss auf wirtschaftliche Tätigkeiten und damit auch auf 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 – NIS2UmsuCG). Gemäß der grundgesetzlichen Kompetenzordnung besitzt der Bund dabei die Rege-

lungsbefugnis 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 könnten. Der regionalen Ebene sind insoweit die in den Ressorts zu verortenden Teile der unmittelbaren Landesverwaltung zuzuordnen. Zur Ermittlung der hierbei betroffenen Einrichtungen hat der IT-Planungsrat in seiner 42. Sitzung am 3. November 2023 ein Identifizierungskonzept beschlossen (Beschluss 2023/39), das von den Ländern anzuwenden ist.

Die Umsetzungsfrist zum 17. Oktober 2024 ist neben dem Bund auch von den Ländern zu beachten. Wegen der noch nicht erfolgten bzw. nicht vollständigen Umsetzung, hat die EU-Kommission am 28. November 2024 ein Vertragsverletzungsverfahren (Art. 258 ff. des Vertrages über die Arbeitsweise der Europäischen Union – AEUV) gegen Deutschland eingeleitet. Nach dem Gesetz zur Lastentragung im Bund-Länder-Verhältnis bei Verletzung von supranationalen oder völkerrechtlichen Verpflichtungen (Lastentragungsgesetz – LastG) sind die Länder dabei gemäß ihrem Verursachungsbeitrag anteilig an daraus folgenden etwaigen Kosten (v. a. Strafzahlungen) zu beteiligen.

B. Lösung

Der Senator für Inneres und Sport legt einen Entwurf einer Verwaltungsvorschrift zur Umsetzung der NIS-2-Richtlinie in der Freien Hansestadt Bremen (VV NIS2Ums FHB) nebst Begründung vor.

Die Verwaltungsvorschrift gilt für die in den Anwendungsbereich der NIS-2-Richtlinie fallenden, gemäß dem Beschluss des IT-Planungsrats vom 3. November 2023 in den Ressorts identifizierten, Einrichtungen der unmittelbaren Landesverwaltung. Eine überschießende Richtlinienumsetzung findet grundsätzlich nicht statt. Von der Richtlinie ausgenommen werden neben der kommunalen (bzw. gemäß der NIS-2-Richtlinie „lokalen“) Ebene und Hochschulen insbesondere auch die Bereiche Parlament, Justiz, öffentliche Sicherheit und Strafverfolgung. Die Ressorts haben mit Unterstützung der Zentralstelle Cybersicherheit beim Senator für Inneres und Sport insgesamt 17 Einrichtungen in der Landesverwaltung identifiziert, die in den Anwendungsbereich der NIS-2-Richtlinie fallen.

Die identifizierten Einrichtungen werden zum Zwecke der Gewährleistung ihrer IT- und Cybersicherheit unter anderem verpflichtet, bestimmte Risikomanagementmaßnahmen zu ergreifen sowie erhebliche Sicherheitsvorfälle zu melden oder gegebenenfalls weitergehend zu reagieren. Darüber hinaus müssen Leitungsverantwortliche die Umsetzung der erforderlichen Maßnahmen überwachen und sich regelmäßig in Fragen der Cybersicherheit schulen lassen sowie den Beschäftigten entsprechende Schulungen ermöglichen.

Die NIS-2-Richtlinie gibt zudem vor, dass für zwei Aufgabenkreise jeweils zuständige Stellen benannt werden. Erstens muss eine „zuständige Behörde“ die Umsetzung der Richtlinie koordinieren und vor allem auch die Einhaltung der Verpflichtungen überwachen. Zweitens muss ein „Computer Security Incident Response Team“ (kurz „CSIRT“, alternativ auch „Computernotfallteam“) unter anderem Bedrohungslagen fortlaufend

auswerten, betroffene identifizierte Einrichtungen gegebenenfalls warnen und technische Unterstützung, insbesondere bei Sicherheitsvorfällen, leisten (zu den Aufgaben eines CSIRT vgl. § 3 Absatz 2 VV NIS2Ums FHB sowie Artikel 11 Absatz 3 NIS-2-Richtlinie. Beide Funktionen sollen zukünftig in der Zentralstelle Cybersicherheit beim Senator für Inneres und Sport gebündelt werden.
Die beiden Funktionen werden in dieser Form bisher nicht in der Freien Hansestadt Bremen ausgeübt. Es handelt sich grundsätzlich um neue Aufgabenkreise. Lediglich bestimmte Tätigkeiten des CSIRT, insbesondere der Betrieb eines Warn- und Informationsdienstes sowie die Funktion als Meldestelle bei Sicherheitsvorfällen, werden derzeit für die gesamte öffentliche Verwaltung der Freien Hansestadt Bremen vom CERT Nord wahrgenommen. Bei diesem handelt es sich um ein „Computer Emergency Response Team“ (kurz „CERT“), das die Freie Hansestadt Bremen mit den drei anderen Dataport-Trägerländern (HH, SH und ST) unterhält und das gemäß den Vorgaben des IT-Planungsrats derzeit gewisse Mindestanforderungen abdeckt (vgl. zuletzt den Beschluss 2022/08 des IT-Planungsrat vom 09.03.2022 – „Mindeststandard CERT“).
Nun nach der NIS-2-Richtlinie für bestimmte (identifizierte) Einrichtungen der öffentlichen Verwaltung gestellte zusätzliche und bisher auf Landesebene nicht erfüllte Anforderungen, vor allem die technische Unterstützung bei der Bewältigung von Sicherheitsvorfällen (vgl. § 3 Absatz 2 Satz 4 Nummer 4 VV NIS2Ums FHB bzw. Artikel 11 Absatz 3 Buchstabe c) NIS-2-Richtlinie) erweisen sich strukturell als Fortentwicklung innerhalb des Tätigkeitbereiches des CERT. Wie der derzeitige CERT-Betrieb bzw. die Beauftragung des CERT Nord handelt es sich bei der Funktion als CSIRT daher um eine zentrale Aufgabe im Bereich der Landes-IT. Die Landes-IT befindet sich im Verantwortungsbereich des Senators für Finanzen. Soll die Zentralstelle Cybersicherheit zukünftig als CSIRT im Sinne der NIS-2-Richtlinie fungieren und dabei auch die Tätigkeiten des CERT Nord einschließen (siehe dazu unten unter „C. 2.“), ist es notwendig, dass die Funktion als Auftraggeber für das CERT Nord vom Senator für Finanzen bzw. dem dort angesiedelten Informationssicherheitsbeauftragten des Landes (auch „Chief Information Security Officer“ oder kurz „CISO“) auf den des Senators für Inneres und Sport bzw. dort der Zentralstelle Cybersicherheit übertragen wird, bei weiterhin wahrgenommener Verantwortung für die Landes-IT durch den Senator für Finanzen (dazu Beschlussvorschlag „4.“).

Die Richtlinienumsetzung durch die Verwaltungsvorschrift steht nicht in Konkurrenz zu den sonstigen Gesetzgebungsvorhaben im Bereich der Cybersicherheit. Mit dem beabsichtigten Bremischen Cybersicherheitsbasisgesetz (BremCSBG) sollen kurzfristig neben der grundsätzlichen Aufgabenverteilung im Bereich der IT- und Cybersicherheit auch spezifische Rechtsgrundlagen für im Rahmen der Gewährleistung ihrer IT-Sicherheit erforderliche Datenverarbeitungen durch öffentliche Stellen geschaffen werden. Diese sind auch für die praktische Umsetzung der Anforderungen und Pflichten aus der NIS-2-Richtlinie zweckmäßig, da die einschlägigen allgemeinen Rechtsgrundlagen aus der DSGVO und der BremDSGVOAG (vor allem Artikel 6 DSGVO ggf. i. V. m. § 3 BremDSGVOAG) mit Blick auf die besonderen Verarbeitungsvorgänge zurzeit keine klare und rechtssichere Handhabung ermöglichen. Mittel- und langfristig wird der Erlass eines ganzheitlichen Bremischen Cybersicherheitsgesetzes (BremCSG) angestrebt, das nicht nur die Regelungen des BremCSBG und der VV NIS2Ums FHB zusammenführt, sondern auch weitere für die IT- und Cybersicherheit relevante Bereiche erstmals gesetzlich regelt. Aufgrund der der grundsätzlichen Verantwortung des Senators für Finanzen für die Landes-IT und die IT-Sicherheit der öffentlichen Verwaltung

ist dessen enge fachliche Einbindung bei Erarbeitung der gesetzlichen Grundlagen erforderlich

C. Alternativen

1. Nichtumsetzung und Umsetzung durch Gesetz

Aufgrund der europarechtlichen Verpflichtungen ist die Richtlinie zwingend umzusetzen. Über Form und Mittel der Umsetzung können die Mitgliedsstaaten gemäß Artikel 288 Absatz 3 AEUV jedoch grundsätzlich frei entscheiden.

Die bloße Anpassung bestehender Rechtsvorschriften auf Landesebene kommt zur Umsetzung nicht in Betracht, da es in der Freien Hansestadt Bremen derzeit kein Cyber- bzw. Informationssicherheitsgesetz gibt. Bestehende untergesetzliche Regelungswerke, insbesondere die Informationssicherheitsleitlinie der Freien Hansestadt Bremen (IS-LL FHB), sind dazu ungeeignet. Sie haben bereits einen anderen Anwendungskreis (die IS-LL FHB gilt für die gesamte öffentliche Verwaltung und nicht nur bestimmte identifizierte Einrichtungen), verfolgen andere Zwecke (die IS-LL FHB zielt auf einen einheitlichen Mindestsicherheitsstandard in der Verwaltung, die NIS-2-Richtlinie auf die Funktionsfähigkeit des Binnenmarkts und den Schutz der Bevölkerung hinsichtlich bestimmter kritischer Dienste) und etablieren keine mit der NIS-2-Richtlinie vergleichbare Organisationsstruktur hinsichtlich der Aufgaben und Tätigkeiten einer „zuständigen Behörde“ sowie eines „CSIRT“. Die Umsetzung der NIS-2-Richtlinie stellt insofern eine sinnvolle Ergänzung zu den bestehenden Regelungen dar, wird aufgrund ihrer strukturellen Vorgaben zugleich aber erhebliche Auswirken auf die zukünftige Cybersicherheitsarchitektur im Land haben und neuere Rechtsakte beeinflussen.

Für die Freie Hansestadt Bremen wird – wie in den meisten anderen Ländern auch – angestrebt, die NIS-2-Richtlinie für die betroffenen Teile der Landesverwaltung durch eine Verwaltungsvorschrift und nicht durch ein Gesetz umzusetzen, um die erforderlichen Regelungen schnell und flexibel implementieren zu können. Aufgrund der kurzen Umsetzungsfrist, der Komplexität der Materie sowie der zwischen dem Bund und den Ländern notwendige Koordinierung wäre ansonsten die rechtzeitige bzw. zumindest zeitnahe und richtlinienkonforme Umsetzung gefährdet. Mittel- und langfristig erscheint die Überführung der Regelungen der Verwaltungsvorschrift in ein Landesgesetz, vor allem im Rahmen der Cybersicherheitsgesetzgebung, jedoch zweckmäßig.
Die Umsetzung durch Verwaltungsvorschrift genügt den europäischen Anforderungen. Nach der gefestigten Rechtsprechung des EuGH bedarf die Umsetzung von Richtlinien nicht zwingend eines formellen Gesetzes, solange die praktische Wirksamkeit der Richtlinie effektiv gewährleistet und dadurch ein richtlinienkonformer Zustand herbeigeführt wird. Die Umsetzung durch Verwaltungsvorschrift ist lediglich dann unzureichend, wenn durch die Richtlinie Individualrechte begründet werden sollen, da es in diesen Fällen an einer hinreichenden Rechtssicherheit und Transparenz für die Betroffenen fehlt (vgl. dazu insgesamt *Ruffert* in: Calliess/Ruffert, EUV/AEUV, 6. Auflage 2022, Artikel 288 AEUV Rn. 41 m. w. N.). Dies ist vorliegend jedoch nicht der Fall. Mit der Verwaltungsvorschrift werden lediglich bestimmte Einrichtungen in den Ressorts adressiert, sodass von vorneherein nur der innerstaatliche Bereich und nicht Bürgerinnen und Bürger oder sonstige Individuen betroffen sind. Die Verwaltungsvorschrift gewährleistet über die von ihr ausgehende Selbstbindung eine hinreichende Verbindlichkeit zur Erfüllung der Vorgaben der Richtlinie.

2. Alternative Verortung des „CSIRT“

Die NIS-2-Richtlinie verpflichtet dazu, „ein oder mehrere CSIRT“ einzurichten (Artikel 10 Absatz 1 NIS-2-Richtlinie). Aufgrund der verteilten Kompetenzwahrnehmung von Bund und Ländern bei der Richtlinienumsetzung ist es erforderlich, dass die Freie Hansestadt Bremen, wie die anderen Länder auch, für ihren Umsetzungsbereich ein eigenes CSIRT vorhält. Insbesondere ist es im Rahmen des NIS2UmsuCG des Bundes, in welchem das Bundesamt für Sicherheit in der Informationstechnik (BSI) als CSIRT benannt wird, weder durch den Bundesgesetzgeber intendiert, noch ist es verfassungsrechtlich aufgrund der grundgesetzlichen Verteilung der Verwaltungskompetenzen und des Verbots der sogenannten „Mischverwaltung“ möglich – ein diesen Grundsatz überlagernder Anwendungsvorrang des EU-Rechts besteht vorliegend nicht –, dass das BSI diese Aufgabe ebenso verstetigt für die Landesverwaltung ausübt.

Eine Benennung des CERT Nord als CSIRT kommt nicht in Betracht, da die dafür erforderliche Ausweitung der Leistungen des CERT Nord von den Trägerländern derzeit nicht vorgesehen ist. Vielmehr wird unter den Trägerländern angestrebt, über Dataport als zentralen IT-Dienstleister ein ergänzendes Angebot zu schaffen, dass vor allem die bisher nicht erbrachten technisch-operativen Elemente eines CSIRT gemäß der NIS-2-Richtlinie abdeckt. Die dabei wahrgenommenen Tätigkeiten werden unter der Bezeichnung als „Remote Incident Response Team“ (kurz „RIRT“) und „Mobile Incident Response Team“ (kurz „MIRT“) zusammengefasst und auf diese verteilt. Diese beiden Komponenten würden zusammen mit den bereits vom CERT Nord erbrachten Tätigkeiten als Einheit die Anforderungen an ein CSIRT nach der NIS-2-Richtlinie erfüllen. Da gegenwärtig für die Freie Hansestadt Bremen keine wirtschaftlich tragfähige Alternative in Aussicht steht, wird eine entsprechende Umsetzung angestrebt.
Dabei ist zu beachten, dass die NIS-2-Richtlinie die organisatorische Einheit des CSIRT voraussetzt (vgl. Artikel 10 und 11 NIS-2-Richtlinie). Insofern ist es rechtlich notwendig, dass die Verantwortung für die einzelnen dann extern beauftragten Komponenten CERT, RIRT und MIRT bei einer zuständigen Stelle gebündelt wird. Dafür würde aufgrund der derzeitigen Zuordnung des CERT bzw. der Beauftragung des CERT Nord als zentrale Angelegenheit der Landes-IT zum Geschäftsbereich des Senators für Finanzen grundsätzlich auch eine Verortung des CSIRT bei ihm bzw. beim Informationssicherheitsbeauftragten des Landes in Betracht kommen. Dies wird jedoch entwicklungsperspektivisch nicht als sinnvoll erachtet. Da der Geschäftsbereich des Senators für Finanzen auf die IT-Sicherheit in der öffentlichen Verwaltung beschränkt ist (vgl. die Geschäftsverteilung im Senat), kann ein dort verortetes CERT oder CSIRT nicht über diesen Bereich hinaus agieren, insbesondere nicht zu einem Landes-CSIRT ausgebaut werden, das auch weitere als kritisch definierte Bereiche außerhalb der öffentlichen Verwaltung miteinbezieht. Der Aufbau von Doppelstrukturen wäre in jedem Fall unwirtschaftlich. Angesichts der zunehmenden Verzahnung von Themen der IT-Sicherheit mit denen „kritischer Infrastrukturen“, die nicht zuletzt durch europäische Rechtsakte wie gegenwärtig die NIS-2-Richtlinie oder die Richtlinie (EU) 2022/2555 (sog. „CER-Richtlinie“) intensiv vorangetrieben wird, ist eine übergreifende Bearbeitung bereits jetzt fachlich unverzichtbar und wird es perspektivisch auch organisatorisch und strukturell werden. Der erforderliche Aufwuchs kann insoweit nur im die IT-Sicherheit in der öffentlichen Verwaltung inhaltlich übergeordneten Bereich der „Cybersicherheit“ gelingen. Diese Entwicklung zeigt sich auch am Vorgehen des BSI sowie den Bestrebungen der anderen Länder Das Handlungsfeld der Cybersicherheit liegt im Geschäftsbereich des Senators für Inneres und Sport und wird dort von der

Zentralstelle Cybersicherheit verantwortet. Dort werden schon jetzt allgemeine koordinierende Aufgaben, die insbesondere auch das Sammeln, Auswerten und Verteilen von einschlägigen Informationen zur Cybersicherheit umfassen, wahrgenommen. Dies stellt bereits jetzt Überschneidungen zur klassischen Arbeit eines CERT dar, sodass durch eine Verortung in der Zentralstelle Cybersicherheit erhebliche Synergien geschaffen werden können. Auch wäre so eine engere Anbindung an die von der Zentralstelle Cybersicherheit unterhaltenen Informationskanäle zum BSI – die Zentralstelle fungiert schon gegenwärtig als „Zentrale Kontaktstelle Land“ (ZKL) zum BSI – sowie den anderen im Ressort verantworteten Bereichen Polizei und Verfassungsschutz möglich, die sich ebenfalls mit spezifischen Aspekten der Cyber- und Informationssicherheit befassen. Letztlich fördert die Verortung des CSIRT bei der Zentralstelle Cybersicherheit die mit der Bremischen Cybersicherheitsstrategie von 2023 beschlossene Bestrebung, dort eine Informationsschnittstelle im Sinne eines „Single Point of Contact“ zu schaffen und insofern eindeutige und klare Organisations- und Kommunikationsstrukturen für das Handlungsfeld der Cybersicherheit im Land Bremen zu schaffen.
Die Verortung des CSIRT bei der Zentralstelle Cybersicherheit setzt die Übertragung der Funktion als Auftraggeber für das CERT Nord vom Senator für Finanzen zum Senators für Inneres und Sport voraus (dazu Beschlussvorschlag „4.“). Die generelle Verantwortung des Senators für Finanzen für die verschiedenen Belange der Landes-IT bleibt erhalten.

3. Alternative Verortung der „zuständigen Behörde“

Die Zentralstelle Cybersicherheit wird als geeignete Stelle betrachtet, um die neuen Aufgaben als „zuständige Behörde“ gemäß der NIS-2-Richtlinie wahrzunehmen. Eine diesbezügliche Zuständigkeit des Senators für Finanzen bzw. des Informationssicherheitsbeauftragten des Landes wäre aus mehreren Gründen nicht zweckmäßig. Dafür gesprochen hätte allenfalls die bereits etablierte Stellung des Informationssicherheitsbeauftragten des Landes, die bei Ausübung der Aufsichtsfunktion gegebenenfalls die nach der NIS-2-Richtlinie erforderliche „operative Unabhängigkeit“ gewährleisten könnte. Allerdings soll der Informationssicherheitsbeauftragte des Landes im Rahmen seiner Aufgaben im Bereich des zentralen Informationssicherheitsmanagements gerade bei der Implementierung der Vorgaben der NIS-2-Richtlinie koordinierend und unterstützend auf Seite der öffentlichen Verwaltung tätig werden. Diese wichtige Aufgabe und auch die damit einhergehende Vertrauensstellung könnte durch die gleichzeitige Wahrnehmung von Aufsichtsfunktionen nach der NIS-2-Richtlinie gefährdet werden. Hinzu kommt die derzeit enge organisatorische Verzahnung der Funktion des Informationssicherheitsbeauftragten des Landes mit der Zuständigkeit des Senators für Finanzen für den Betrieb der zentralen IT-Infrastruktur (derzeit in einer Abteilung, teilweise auch in einem Referat). Letzterer Bereich ist aber selbst in wesentlichen Teilen von der Umsetzung der NIS-2-Richtlinie betroffen. Vor allem aber obliegt der „zuständigen Behörde“ nach der NIS-2-Richtlinie auch die koordinierende Zusammenarbeit mit anderen Behörden sowie der Kontakt zum BSI als „zentrale Anlaufstelle“. Dies sind originäre Aufgaben der Zentralstelle, die im Übrigen bereits gegenwärtig als Zentrale Kontaktstelle zum BSI fungiert (siehe dazu schon unter „C. 2.“). Des Weiteren liegt der Fokus der NIS-2-Richtlinie auf Informationstechnik als Teil der kritischen Infrastrukturen, was dem Bereich Cybersicherheit nähersteht und wie auch die engen Bezüge zur CER-Richtlinie zeigen, die ebenfalls zentral im Innenressorts bearbeitet wird. Die Bearbeitung der Cybersicherheitsaspekte Kritischer Infrastrukturen in einem anderen Ressort als die Bearbeitung der physischen Resilienz Kritischer Infrastruktur sowie der

übergreifenden Angelegenheiten des Schutzes Kritischer Infrastrukturen machte den Aufbau von umfangreichen Doppelstrukturen sowie eine permanente ressortübergreifende Koordinierung erforderlich und ist daher unwirtschaftlich und ineffizient.
Zuletzt erleichtert die organisatorische Einheit von „zuständiger Behörde“ und „CSIRT“, die von der NIS-2-Richtlinie explizit ermöglicht werden soll (vgl. Artikel 10 Absatz 1 Satz 2 NIS-2-Richtlinie), die Zusammenarbeit zwischen den beiden Stellen und vermeidet Abgrenzungsschwierigkeiten.

D. Finanzielle und personalwirtschaftliche Auswirkungen / Genderprüfung / Klimacheck

1. Finanzielle und personalwirtschaftliche Auswirkungen

Die Umsetzung der NIS-2-Richtlinie durch die VV NIS2Ums FHB hat voraussichtlich finanzielle und personalwirtschaftliche Auswirkungen, die sich derzeit aber nur begrenzt schätzen und nur teilweise beziffern lassen.

a) Ressorts

In allen Ressorts (einschließlich dem des Senators für Inneres und Sport) sind gemäß den Vorgaben des IT-Planungsrates Einrichtungen identifiziert worden, die in den Anwendungsbereich der Richtlinie fallen und damit auch den Verpflichtungen der VV NIS2Ums FHB unterliegen. Aufgrund der bereits für die öffentliche Verwaltung bestehenden und dabei auch auf Beschlüssen des IT-Planungsrats (siehe insbesondere die vom IT-Planungsrat beschlossene „Leitlinie Informationssicherheit“: Beschluss 2013/01 und 2019/04) basierenden Vorgaben zur Informationssicherheit ist davon auszugehen, dass lediglich die nun durch die NIS-2-Richtlinie neu hinzutretenden Anforderungen einen Mehraufwand auslösen.

So existiert schon gegenwärtig nach Punkt 5.4 der IS-LL FHB eine allgemeine Pflicht zur Meldung von Sicherheitsvorfällen zum CERT Nord, sodass für die nach der VV NIS2Ums FHB vorgesehene Verpflichtung zur Meldung erheblicher Sicherheitsvorfälle (§ 8 VV NIS2Ums FHB) lediglich eine geringfügige Anpassung der bestehenden Prozesse erfolgen muss. Auch die vorgesehene Verantwortlichkeit der Leitungsebene (§ 7 Absatz 1 VV NIS2Ums FHB) ist in Punkt 4.1 der IS-LL FHB festgeschrieben. Hinsichtlich der im Einzelfall bestehenden Pflicht zur Unterrichtung der Öffentlichkeit bei erheblichen Sicherheitsvorfällen (§ 10 VV NIS2Ums FHB) wird davon auszugehen sein, dass diese sich dann im Rahmen der bestehenden Mittel und Stellen bewältigen lässt. Gleiches gilt für die Pflicht zur Wiederholung der ressortinternen Identifizierung alle zwei Jahre (§ 2 Absatz 2 VV NIS2Ums FHB), die erstmalig bereits durchgeführt wurde. Schulungsangebote für die Leitungsebene und Mitarbeiter:innen (§ 7 Absatz 2 VV NIS2Ums FHB) sollen grundsätzlich durch die Zentralstelle Cybersicherheit geschaffen werden (siehe dazu unter „D. 1. b)“).

Kern der nach der NIS-2-Richtlinie bestehenden Verpflichtungen bilden die sogenannten Risikomanagementmaßnahmen (§ 5 VV NIS2Ums FHB). Hinsichtlich dieser ist festzustellen, dass durch die gemäß Punkt 3.1 IS-LL FHB bestehende Anwendung der Standards und Kataloge des BSI schon jetzt in der Landesverwaltung der IT-Grundschutz nach BSI maßgeblich ist. Dieser ist nach erster Einschätzung größtenteils konform mit den Vorgaben des § 5 VV NIS2Ums FHB bzw. Artikel 21 NIS-2-Richtlinie. Es

ist davon auszugehen, dass lediglich einzelne Aspekte wie Business Continuity Management (§ 5 Absatz 2 Satz 2 Nummer 3 VV NIS2Ums FHB), Sicherheit in der Lieferkette (§ 5 Absatz 2 Satz 2 Nummer 4) oder Multi-Faktor-Authentifizierung (§ 5 Absatz 2 Satz 2 Nummer 10 VV NIs2Ums FHB) neu hinzutreten. Derzeit überarbeitet das BSI seinen IT-Grundschutz konform zu den Vorgaben der NIS-2-Richtlinie.

Die Verantwortlichkeit für die Umsetzung der einzelnen Maßnahmen, einschließlich solcher, die nur im zentralen IT-Betrieb in der Verantwortung des Senators für Finanzen umsetzbar sind, liegt im jeweils zuständigen Ressort (einschließlich des Senators für Inneres und Sport). Eine zentrale Schätzung der Mehraufwände ist daher nicht möglich und hängt von den Bewertungen und Gegebenheiten des jeweils verantwortlichen Ressorts sowie dem Maß seiner Betroffenheit ab. Soweit die NIS-2-Richtlinie auf bereits bestehenden Verpflichtungen aufbaut, wird grundsätzlich davon ausgegangen werden können, dass die dafür derzeit zur Verfügung stehenden Mittel und Stellen diesbezüglich ausreichend sind.

b) Zentralstelle Cybersicherheit

Für die Zentralstelle Cybersicherheit entstehen Mehrbedarfe für die neuen, bisher nicht von ihr wahrgenommen Aufgaben. Diese können nicht aus den ihr bisher zur Verfügung stehenden Stellen und Mitteln bewältigt werden.

Als „zuständige Behörde“ muss die Zentralstelle Cybersicherheit – teilweise in Verlagerung vom Senator für Finanzen – folgende neue Aufgaben wahrnehmen, für die insgesamt ein personeller Mehraufwand in Höhe von 1,0 VZE (Laufbahngruppe 2, 2. Einstiegsamt) angenommen wird. Dabei ist von durchschnittlichen Personalkosten in Höhe von 65.630 Euro (BesGr. A 13 BremBesO) bis zu 84.832 Euro (EG 13 TV-L) auszugehen.

Aufgabe	**Regelung in der VV NIS2Ums FHB**	**Bedarf in VZE**
Koordinierung des Identifizierungsprozesses in der Landesverwaltung sowie Verwaltung und Pflege der Liste identifizierter Einrichtungen	§ 2 Absatz 2, § 4	0,05
Zusammenarbeit und Informationsaustausch mit anderen im Bereich Cybersicherheit tätigen oder sonst zuständigen Behörden	§ 3 Absatz 4, §, 4 Absatz 5, § 8 Absatz 4 (i. V. m. § 9 Absatz 4), § 12 Absatz 3	0,15
Planung, Durchführung und Dokumentation von Aufsichtsmaßnahmen	§ 12	0,5
Erstellung und Durchführung von Schulungen	§ 7 Absatz 2, § 5 Absatz 2 Satz 2 Nummer 7	0,3
		Gesamt: 1,0

Hinzu kommen bisher nicht bezifferbare, jedoch schätzungsweise eher geringfügige, Arbeitsplatzkosten bzw. Sachmittelaufwände für die dabei erforderliche Ausstattung

der zusätzlichen VZE in Höhe von 9,7 TEUR. Die Arbeitsplatzkosten der bei der Zentralstelle Cybersicherheit bestehenden 3 VZE werden im Ressortbudget des PPL07 Inneres Land abgedeckt.

Die Aufgaben eines CSIRT (§ 3 Absatz 2 VV NIS2Ums FHB) sollen unter dem Dach der Zentralstelle Cybersicherheit auf Basis ihrer Zuordnung zu den Komponenten CERT, RIRT und MIRT (siehe oben unter „B." und „C. 2.") durch externe Dienstleister umgesetzt werden, sodass insoweit Sachmittelkosten entstehen. Durch die Integration der Tätigkeiten des CERT Nord in das CSIRT entstehen diesbezüglich keine neuen Kosten.
Die für die für die Beauftragung des CERT Nord vorgesehene jährlichen Mittel im PPL 96 in Höhe von 134.000 € werden im Rahmen der Übertragung der Funktion als Auftraggeber unter die Fremdbewirtschaftung des Senators für Inneres und Sport gestellt (FBZ 030).

Es verbleiben zusätzliche Mittelbedarfe für die Beauftragung des RIRT und MIRT. Auf Grundlage anderen Ländern vorliegender Vertragsangebote werden diese für den Aufgabenbereich „technischen Unterstützung bei Sicherheitsvorfällen" (vgl. § 3 Absatz 2 Satz 4 Nummer 4 und 5 VV NIS2Ums FHB) auf jährlich voraussichtlich zwischen 200 und 400 TEUR (Festpreis) geschätzt. Ob weitere (technische) CSIRT-Leistungen, insbesondere die Unterstützung bei der IT-Überwachung in den Einrichtungen (§ 3 Absatz 2 Satz 4 Nummer 2 VV NIS2Ums FHB), Schwachstellenscans (§ 3 Absatz 2 Satz 4 Nummer 6 VV NIS2Ums FHB) und nicht intrusive Überprüfungen bei öffentlich zugänglichen Systemen (§ 11 VV NIS2Ums FHB), im Rahmen der Beauftragung des RIRT umgesetzt werden können oder ob diese ebenfalls als Festpreiskontingente hinzugenommen werden müssen, kann zum aktuellen Zeitpunkt nicht abgeschätzt werden. Daher ist die Kostenschätzung noch nicht weiter eingrenzbar. Zu der konkreten Finanzierung und etwaigen einzugehenden finanziellen Verpflichtungen unter Darlegung der kalkulierten Mehrbedarfe wird eine gesonderte Senatsbefassung des Senators für Inneres und Sport und des Senators für Finanzen erfolgen.

2. Genderprüfung

Der Entwurf hat keine geschlechterspezifischen Inhalte und/oder Auswirkungen. Es werden lediglich Stellen der öffentlichen Verwaltung und keine natürlichen Personen adressiert. Mitarbeiter:innen aller Geschlechter innerhalb der öffentlichen Verwaltung sind gleichermaßen betroffen.

3. Klimacheck

Die Beschlüsse in der Senatsvorlage haben, auf Basis des Klimachecks, voraussichtlich keine Auswirkungen auf den Klimaschutz.

E. Beteiligung / Abstimmung

Die Senatsvorlage wurde mit der Senatskanzlei, der Senatorin für Kinder und Bildung, dem Senator für Kultur, der Senatorin für Arbeit, Soziales, Jugend und Integration, der Senatorin für Bau, Mobilität und Stadtentwicklung, der Senatorin für Gesundheit, Frauen und Verbraucherschutz, der Senatorin für Umwelt, Klima und Wissenschaft,

der Senatorin für Wirtschaft, Häfen und Transformation sowie der Senatorin für Justiz und Verfassung abgestimmt. Die Abstimmung mit dem Senator für Finanzen wurde eingeleitet.

Der Landesbeauftragte für Datenschutz und Informationsfreiheit wurde über den Entwurf der Verwaltungsvorschrift unterrichtet. Die von ihm abgegebene Stellungnahme vom 20.12.2024 liegt dieser Senatsvorlage bei (Anlage 3).

F. Öffentlichkeitsarbeit / Veröffentlichung nach dem Informationsfreiheitsgesetz

Die Vorlage einschließlich des Begründungstextes ist für die Öffentlichkeitsarbeit bzw. für eine Veröffentlichung nach dem Informationsfreiheitsgesetz im Transparenzportal nach Beschlussfassung geeignet.

G. Beschluss

1. Der Senat nimmt die Begründung zur VV NIS2Ums FHB (Anlage 2) zur Kenntnis.
2. Der Senat beschließt entsprechend der Vorlage des Senators für Inneres und Sport vom 10.01.2024 die Verwaltungsvorschrift zur Umsetzung der NIS-2-Richtlinie in der Freien Hansestadt Bremen (VV NIS2Ums FHB) und veranlasst zum nächstmöglichen Zeitpunkt die Verkündung im Amtsblatt der Freien Hansestadt Bremen.

3. Der Senat beschließt die Übertragung der Funktion als Auftraggeber für das CERT Nord sowie aller zugehörigen Bestandteile und des Budgets auf die Zentralstelle Cybersicherheit beim Senator für Inneres und Sport.

Anlage 1: VV NIS2Ums FHB
Anlage 2: Begründung zur VV NIS2Ums FHB
Anlage 3: Stellungnahme des LfDI vom 20.12.2024

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

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.

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

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

A. Allgemeines

I. Ziel und Inhalt

Die Bedrohungslage im Cyberraum ist aktuell so hoch wie nie. Gleichzeitig führt die fortschreitende Digitalisierung dazu, dass Prozesse und Dienstleistungen zunehmend auf informationstechnische Systeme angewiesen sind und die Vernetzung weiter zunimmt. Ein besonders hohes Risiko ergibt sich dadurch im Bereich kritischer Infrastrukturen, deren Ausfall weitreichende wirtschaftliche und gesellschaftliche Folgen haben kann.

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 dabei 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 vorliegende Verwaltungsvorschrift angesprochen.

II. Umsetzung durch Verwaltungsvorschrift

Die Freie Hansestadt Bremen wird, wie viele andere Länder auch, die NIS-2-Richtlinie für die betroffenen Teile der Landesverwaltung zunächst durch eine Verwaltungsvorschrift und nicht durch ein Gesetz umsetzen.

Dabei wird den europarechtlichen Anforderungen entsprochen. Gemäß Artikel 288 Absatz 3 des Vertrages über die Arbeitsweise der Europäischen Union (AEUV) sind die Mitgliedstaaten bei der Umsetzung von Richtlinien in der Wahl der Form und Mittel grundsätzlich frei. Die Umsetzung muss jedoch so erfolgen, dass die praktische Wirksamkeit der Richtlinie effektiv gewährleistet ist (Gebot der effektiven Umsetzung von Richtlinien). Nach gefestigter Rechtsprechung des EuGH bedarf es dabei nicht notwendigerweise in jedem Mitgliedstaat eines Umsetzungsaktes des formellen Gesetzgebers in Gestalt der wörtlichen Übernahme der Richtlinienbestimmungen in eine ausdrückliche, besondere Gesetzesvorschrift, sondern es reicht – je nach Richtlinieninhalt – aus, wenn ein allgemeiner rechtlicher Rahmen bestehender verfassungs- und verwaltungsrechtlicher Grundsätze die innerstaatliche Anwendung der Richtlinie sicherstellt. Entscheidend ist insofern das richtlinienkonforme Ergebnis. Die Regelungen müssen lediglich hinreichend verbindlich und durchsetzbar sein. Nach dem EuGH genügt die Umsetzung durch Verwaltungsvorschrift den europarechtlichen Anforderungen lediglich dann nicht, wenn durch die Richtlinie Individualrechte begründet werden sollen, da es in diesen Fällen an einer hinreichenden Rechtssicherheit und Transparenz für die Betroffenen fehle (vgl. dazu insgesamt *Ruffert* in: Calliess/Ruffert, EUV/AEUV, 6. Auflage 2022, Artikel 288 AEUV Rn. 41 m. w. N.). Dies ist vorliegend jedoch nicht der Fall. Mit der Verwaltungsvorschrift werden lediglich bestimmte Einrichtungen in den Ressorts adressiert, sodass von vorneherein nur der innerstaatliche Bereich und nicht Bürgerinnen und Bürger oder sonstige Individuen betroffen sind. Die Verwaltungsvorschrift gewährleistet über die von ihr ausgehende Selbstbindung eine hinreichende Verbindlichkeit zur Erfüllung der Vorgaben der Richtlinie.

Verfassungsrechtliche Bedenken, insbesondere mit Blick auf den Vorbehalt des Gesetzes, bestehen nicht. Mit den unmittelbaren Regelungen der Verwaltungsvorschrift sind keine Eingriffe in Grundrechte oder Selbstverwaltungsrechte verbunden. Auch werden Einrichtungen mit besonderer gesetzlicher oder verfassungsrechtlicher Unabhängigkeit (z. B. die Bremische Bürgerschaft, der Staatsgerichtshof, der Landesrechnungshof oder die oder der Landesbeauftragte für Datenschutz und Informationsfreiheit) nicht adressiert.

Für die praktische Erfüllung der Anforderungen aus der NIS-2-Richtlinie sind andere Rechtsgrundlagen heranzuziehen. Wenn etwa beim Betrieb von Gefahren bzw. Angriffserkennungssystemen oder IT-forensischen Maßnahmen im Rahmen der Bewältigung von Sicherheitsvorfällen durch die Einrichtungen (vgl. § 5 Absatz 2 Satz 2 Nummer 2) oder durch die entsprechende (technische) Unterstützung des Computer Security Incident Response Team (CSIRT) bzw. Computernotfallteam (vgl. § 3 Absatz Satz 4 Nummer 2, 4, 5 und 6) auch grundrechtlich geschützte Daten (v. a. personenbezogene oder dem Fernmeldegeheimnis unterliegende Daten) verarbeitet werden sollen, muss auf gesetzliche Ermächtigungen zurückgegriffen werden können, die den verfassungsrechtlichen und einschlägigen europarechtsrechtlichen Anforderungen genügen (vgl. auch Erwägungsgrund 121 der NIS-2-Richtlinie). Es sollten zeitnah – vorzugsweise im Rahmen der Cybersicherheitsgesetzgebung – entsprechende spezifische landesgesetzliche Regelungen geschaffen werden, um Unsicherheiten hinsichtlich der Anwendung und Reichweite der in Betracht kommenden Rechtsgrundlagen (vor allem in der DSGVO und dem BremDSGVOAG sowie dem TDDDG) zu vermeiden.

Sollte die Umsetzung unvollständig oder nicht fristgerecht bis zum 17. Oktober 2024 erfolgen, kann die Europäische Kommission ein Vertragsverletzungsverfahren gegen die Bundesrepublik Deutschland einleiten. Nach dem Gesetz zur Lastentragung im Bund-Länder-Verhältnis bei Verletzung von supranationalen oder völkerrechtlichen Verpflichtungen (Lastentragungsgesetz – LastG) gilt das Verursacherprinzip, so dass die vertragsverletzenden Gebietskörperschaften (Bund und/oder Länder) für die Kosten aufkommen müssen.

Aufgrund des nahenden Ablaufs der Umsetzungsfrist ist daher eine kurzfristige Umsetzung durch Verwaltungsvorschrift zweckmäßig. Zur Schaffung eines einheitlichen Rechtsrahmens

erscheint mittel- und langfristig die Überführung der Regelungen dieser Verwaltungsvorschrift in ein umfassenderes Bremisches Cybersicherheitsgesetz erstrebenswert.

B. Zu den einzelnen Vorschriften

Zu § 1 (Begriffsbestimmungen)

§ 1 enthält Regelungen zu den in der Verwaltungsvorschrift verwendeten Begriffen.

Zu Absatz 1

In Absatz 1 werden vorab zum Verständnis der nachfolgenden Regelungen wichtige Begriffe definiert. Viele dieser Begriffe sowie die zugehörigen Definitionen wurden wortgleich aus der NIS-2-Richtlinie entnommen. Andere sind wiederum auf die Richtlinie zurückzuführen, wurden aber zum besseren Verständnis an den national bestehenden Rechtsrahmen angepasst. Mittel- und langfristig ist die vollständige Harmonisierung von Begrifflichkeiten der IT- und Cybersicherheit im Land angestrebt. Insbesondere die zukünftige Cybersicherheitsgesetzgebung wird sich unter anderem an hiesigen Bestimmungen orientieren und die zunehmende Europäisierung berücksichtigen.

Zu Nummer 1

Der Begriff der „kritischen Einrichtung der Landesverwaltung“ legt nach § 2 Absatz 1 den grundsätzlichen Geltungsbereich dieser Verwaltungsvorschrift fest. Er enthält mehrere Komponenten, die zusammen den von den Ländern umzusetzenden Anwendungsbereich der Richtlinie aus Artikel 2 Absatz 2 Buchstabe f Ziffer ii abbilden und daher auch dem Identifizierungskonzept des IT-Planungsrates vom 3. November 2023 (Beschluss 2023/39) zugrunde liegen.

Zum einen wird auf die Definition der „Einrichtung der öffentlichen Verwaltung“ nach Artikel 6 Nummer 35 der NIS-2-Richtlinie zurückgegriffen. Im Vordergrund steht dabei insbesondere der Zweck im allgemeinen Interesse liegende Aufgaben zu erfüllen, ohne dabei einen gewerblichen oder kommerziellen Charakter zu haben und die Fähigkeit Verwaltungs- und Regulierungsentscheidungen zu treffen. Dies unterscheidet diese Einrichtungen insbesondere von den sonst in der NIS-2-Richtlinie betroffenen wirtschaftlich tätigen Einrichtungen bzw. Unternehmen. Diese Trennung zeigt sich auch darin, dass im Unterschied zur allgemeinen Definition einer Einrichtung in Artikel 6 Nummer 38 der NIS-2-Richtlinie gemäß Artikel 6 Nummer 35 Buchstabe b der NIS-2-Richtlinie gerade keine eigene Rechtspersönlichkeit der einzelnen Einrichtungen als juristische Personen des öffentlichen Rechts notwendig ist. Dementsprechend ist nicht der Verwaltungsträger als solcher verpflichtet, sondern einzelnen Untergliederungen bzw. Organisationseinheiten und damit grundsätzlich Behörden. Aufgrund der Adressierung der Pflichten sowohl an diese (z. B. der Risikomanagementmaßnahmen nach Artikel 21 der NIS-2-Richtlinie) als auch die Leitungsebene (vor allem in Artikel 20 der NIS-2-Richtlinie) wird eine gewisse organisatorische Selbständigkeit vorauszusetzen sein, die eine eigene Verantwortungsebene enthält. Nach hiesigem Verständnis ist der Begriff daher mit einer Behörde im organisatorischem Sinne („Dienststelle“) gleichzusetzen (zu diesem etwa BVerwG, Beschluss vom 19.03.2012 − 6 P 6/11). Der Begriff schließt zudem insbesondere die Bereiche „Justiz“ und „Parlament“ sowie – für landesrechtliche Bestimmungen weniger relevant – „Zentralbanken“ aus.

Zum anderen beschränkt sich der Geltungsbereich in Übersetzung der „regionalen Ebene“ aus Artikel 2 Absatz 2 Buchstabe f Ziffer ii auf die unmittelbare Landesverwaltung und dort entsprechend der beschränkenden Definition aus Artikel 6 Nummer 35 sowie dem Zweck der Richtlinie auf Einrichtungen innerhalb der Ressorts und nicht auf andere (gegebenenfalls unabhängige) oberste Landesbehörden, wie den Landesrechnungshof, soweit diese nicht schon

unter die oben genannten Bereichsausnahmen fallen oder sonst vom Anwendungsbereich der Richtlinie ausgeschlossen sind. Davon geht auch das Identifizierungskonzept des IT-Planungsrates aus.

Zu Nummer 2

Der Begriff beinhaltet ein „Netz- und Informationssystem“ nach Artikel 6 Nummer 1 der NIS-2-Richtlinie.

Die Definition der Informationstechnik ist bewusst allgemein gefasst, um alle technischen Ausgestaltungen und denkbaren künftigen Entwicklungen auf dem Gebiet der Informationstechnik abzudecken. Unter „technische Mittel" sind alle heutigen und zukünftigen Arten von Hard- und Software- oder Cloudlösungen zu verstehen. Der Begriff „Verarbeitung" schließt alle Vorgänge wie Erfassung, Darstellung, Speicherung oder Übermittlung ein. Eine Bekanntgabe von Informationen an Dritte ist dabei nicht erforderlich. Erfasst werden alle Arten von Informationen, ein Personenbezug ist dabei nicht erforderlich.

Zu Nummer 3

Die Definition verbindet die national anerkannte Definition der „Sicherheit in der Informationstechnik“ nach § 2 Absatz BSIG mit der in der NIS-2-Richtlinie verwendeten der „Sicherheit von Netz- und Informationssystemen“ (Artikel 6 Nummer 2 der Richtlinie).

Mit der „Sicherheit in der Informationstechnik“ ist kein absoluter, sondern lediglich ein relativer Sicherheitsbegriff vorgegeben. Welches Maß an Sicherheit im Einzelfall erreicht sein muss, hängt von den jeweils einschlägigen Sicherheitsstandards ab. In der NIS-2-Richtlinie wird dieser Zusammenhang durch das in bezuggenommene „bestimmte Vertrauensniveau“ deutlich, auf das deshalb auch in vorliegender Definition abgestellt wird. Die NIS-2-Richtlinie bezieht ihre Definition ferner nicht nur auf die durch Informationstechnik verarbeiteten Daten, sondern auch auf die über diese angebotenen oder zugänglichen Dienste. Aus Klarstellungsgründen und zur Harmonisierung mit den weiteren von der NIS-2-Richtlinie vorgegebenen Begrifflichkeiten, insbesondere des „Sicherheitsvorfalls“ und „Beinahe-Vorfalls“, wird diese gesonderte Erwähnung der „Dienste“ übernommen. Aus der Einhaltung von Standards folgt die Notwendigkeit der Implementierung bestimmter Sicherheitsvorkehrungen, namentlich in den betroffenen informationstechnischen Systemen, Komponenten oder Prozessen selbst oder bei deren Anwendung (vgl. § 2 Absatz 2 Satz 4 Nummer 1 und 2 BSIG). Ferner kann sich die „Sicherheit“, anders als es der Wortlaut in Artikel 6 Nummer 2 der NIS-2-Richtlinie vermuten lässt, zweckmäßigerweise nicht nur in der Abwehr des schädigenden Ereignisses selbst erschöpfen, sondern muss auch entsprechende Vor- und Nachbereitungen zur Wahrung der Sicherheit miteinschließen.

Die „Verfügbarkeit von Informationen" erfordert Sicherheitsvorkehrungen, um die Informationen in der vorgesehenen Weise verarbeiten oder übertragen und damit nutzen zu können. Die „Integrität von Informationen" erfordert Sicherheitsvorkehrungen, um deren Inhalt und Form vor unzulässigem Verändern zu schützen. Die „Vertraulichkeit von Informationen" erfordert Sicherheitsvorkehrungen, um einen unbefugten Informationsgewinn über die Informationstechnik und einen ungewollten Abfluss der mit ihr verarbeiteten oder übertragenen Informationen zu verhindern.

Aufgenommen wurde mit Blick auf die europäische Harmonisierung auch das Schutzziel der „Authentizität“, so wie es auch in den einschlägigen Definitionen der NIS-2-Richtlinie (Artikel 6 Nummer 2, 5 und 6) genannt ist. Nach hiesigem Verständnis wird diesem Begriff das anerkannte IT-Schutzziel der Echtheit und Glaubwürdigkeit von Daten und ihrer Urheberschaft (eng. Authenticity) zugeordnet.

Zu Nummer 4

Der Begriff der „Bedrohung in der Informationstechnik“ soll dem der „Cyberbedrohung“ nach Artikel 6 Nummer 10 NIS-2-Richtlinie in Verbindung mit Artikel 2 Nummer 8 der Verordnung (EU) 2019/881 entsprechen und wurde sprachlich angepasst.

Im Kontext der NIS-2-Richtlinie fallen nach hiesigen Verständnis hierunter sowohl abstrakte, von konkreten IT-Systemen unabhängig bestehende Bedrohungslagen, als auch konkrete Gefahren in Bezug auf ein bestimmtes IT-System. Der Begriff ist entsprechend weit auszulegen. Bedrohungen können etwa von bestimmten, sich im Umlauf befindlichen Schadprogrammen, Schwachstellen und anderen Sicherheitsrisiken oder von Gruppierungen und ihrer Vorgehensweise ausgehen. Gerade im Bereich der Cybersicherheit ist die Erforschung von Bedrohungslagen relevant, um Gefahren frühzeitig zu erkennen und Vorbereitungsmaßnahmen zu treffen, da oftmals nach dem Erkennen oder gar dem Schadenseintritt kaum mehr Abwehrmaßnahmen zur Verfügung stehen. Bedrohungen können insbesondere auch bei der Auswertung von Sicherheits- und Beinahe-Vorfällen erkannt werden (vgl. insoweit auch die Aufgaben als CSIRT nach § 3 Absatz 2 Satz 4 Nummer 1).

Zu Nummer 5

Der Begriff soll dem aus Artikel 6 Nummer 11 der NIS-2-Richtlinie entsprechen. Der Wortlaut wurde geringfügig verändert.

Eine „Erhebliche Bedrohung“ beinhaltet gegenüber der allgemeinen „Bedrohung“ nach Nummer 5 eine Qualifikation. Es geht um erhöhte Schadenspotenziale.

Zu Nummer 6

Der Begriff soll dem aus Artikel 6 Nummer 6 der NIS-2-Richtlinie entsprechen. Der Wortlaut wurde geringfügig verändert.

Ein Sicherheitsvorfall liegt vor, wenn mindestens eines der Schutzziele nach Nummer 4 beeinträchtigt wurde. Im Unterschied zum „Beinahe-Vorfall“ nach Nummer 8 ist damit ein Schaden an der IT-Sicherheit eingetreten. In Parallelität zu strafrechtlichen Kategorien (vgl. auch die Begründung zu Nummer 8) kann gewissermaßen von einer „Vollendung“ gesprochen werden.

Zu Nummer 7

Der Begriff entspricht bis auf geringfügige sprachliche Anpassungen der Definition in Artikel 23 Absatz 3 der NIS-2-Richtlinie. Ergänzend ist auf die Möglichkeit vorrangig geltender Durchführungsrechtsakte zu verweisen (vgl. zu § 1 Absatz 2).

Zu Nummer 8

Der Begriff soll dem aus Artikel 6 Nummer 5 der NIS-2-Richtlinie entsprechen. Er wurde lediglich sprachlich geringfügig angepasst.

Den Beinahe-Vorfall zeichnet dabei aus, dass er ein Schadenspotenzial besaß, welches jedoch nicht realisiert wurde und insofern „unvollendet“ geblieben ist. Parallelen können zur strafrechtlichen Kategorie des „Versuchs“ gezogen werden. Der Grund des Ausbleibens des Schadens wird insoweit, insbesondere bei gezielten Angriffen, häufig in einer aktiven Verhinderung liegen. Die Definition schließt aber auch andere Umstände, gegebenenfalls auch zufällige, nicht aus.

Zu Nummer 9

Der Begriff entspricht dem aus Artikel 6 Nummer 8 der NIS-2-Richtlinie.

Mit der Vorgabe ist der Fachbegriff „incident response“ gemeint. Darunter fallen auch die Prävention und Detektion, vor allem durch den Betrieb von Systemen zur Gefahren- bzw. Angriffserkennung.

Zu Nummer 10

Der Begriff entspricht dem aus Artikel 6 Nummer 9 der NIS-2-Richtlinie.

Zu Nummer 11

Der Begriff entspricht dem aus Artikel 6 Nummer 12 der NIS-2-Richtlinie in Verbindung mit Artikel 2 Nummer 12 der Verordnung (EU) 2019/881.

Zu Nummer 12

Der Begriff entspricht dem aus Artikel 6 Nummer 13 der NIS-2-Richtlinie in Verbindung mit Artikel 2 Nummer 13 der Verordnung (EU) 2019/881.

Zu Nummer 13

Der Begriff entspricht dem aus Artikel 6 Nummer 14 der NIS-2-Richtlinie in Verbindung mit Artikel 2 Nummer 14 der Verordnung (EU) 2019/881.

Zu Nummer 14

Der Begriff soll dem aus Artikel 6 Nummer 15 der NIS-2-Richtlinie entsprechen. Er führt den in der nationalen Rechtssetzung vielfach verwendeten Begriff der „Sicherheitslücke“ fort (vgl. etwa § 2 Absatz 6 BSIG), ohne dass damit eine wesentliche inhaltliche Änderung verbunden sein dürfte.

Schwachstellen sind unerwünschte Eigenschaften von informationstechnischen Systemen, insbesondere Computerprogrammen, die es Dritten erlauben, gegen den Willen der Berechtigten deren Informationstechnik zu beeinflussen. Eine Beeinflussung muss nicht zwingend darin bestehen, dass sich Dritte Zugang zum System verschaffen und dieses dann manipulieren können. Es genügt auch, dass die Funktionsweise in sonstiger Weise beeinträchtigt werden kann, z. B. durch ein ungewolltes Abschalten. Der Begriff ist somit kontextspezifisch und deswegen notwendigerweise weit gefasst, da Schwachstellen in den unterschiedlichsten Zusammenhängen, oftmals abhängig von der Konfiguration oder Einsatzumgebung, entstehen können.

Zu Nummer 15

Der Begriff entspricht der Legaldefinition aus Artikel 11 Absatz 3 Unterabsatz 1 Buchstabe e der NIS-2-Richtlinie und wird zur Einhaltung der Systematik bei den sonstigen Begriffsbestimmungen behandelt.

Scans nach § 11 (bzw. Artikel 11 Absatz 3 Unterabsatz 3 der NIS-2-Richtlinie) werden gesondert behandelt. Es kann damit offenbleiben, ob sie als spezielle (nicht intrusive) Ausprägung formal unter hiesigen Oberbegriff fallen. Dagegen spricht die besonders in Artikel 11 Absatz 3 Untersatz 2 Satz 2 der NIS-2-Richtlinie beschriebene Zielsetzung solcher nicht intrusiven Scans, die über das Finden produkt- oder dienstbezogener (angeborener) Sicherheitslücken (Schwachstellen nach § 1 Absatz 1 Nummer 14) hinausgeht, indem unsicher konfigurierte IT einbezogen wird.

Zu Absatz 2

Absatz 2 setzt Artikel 23 Absatz 11 Unterabsatz 2 Satz 2 der NIS-2-Richtlinie um.

Zu § 2 (Geltungsbereich)

Mit diesem Paragraphen wird der Geltungsbereich der Verwaltungsvorschrift festgelegt (Absatz 1) und wird das Verfahren zur Identifizierung kritischer Einrichtungen der Landesverwaltung normiert (Absatz 2).

Zu Absatz 1

Satz 1 benennt kritische Einrichtungen der Landesverwaltung als Adressaten dieser Verwaltungsvorschrift. Hinsichtlich des Begriffs kann auf die Ausführungen zu § 1 Absatz 1 Nummer 1 verwiesen werden.

Manche Bestimmungen dieser Verwaltungsvorschrift sind nicht auf kritische Einrichtungen der Landesverwaltung beschränkt. Diese Erweiterung des Anwendungskreises ist aus den entsprechenden Regelungen selbst ersichtlich (z. B. § 3 Absatz 2 Satz 7 und § 9 Absatz 2).

Zu Absatz 2

Kritische Einrichtungen der Landesverwaltung sind ausschließlich solche, die gemäß Artikel 2 Absatz 2 Buchstabe f Ziffer ii der NIS-2-Richtlinie ermittelt wurden. Es findet insoweit keine überschießende Richtlinienumsetzung statt. Sie gelten gemäß Artikel 3 Absatz 2 Satz 1 in Verbindung mit Nummer 10 Alternative 2 Anhang I der NIS-2-Richtlinie als „wichtige Einrichtungen“ und unterliegen dementsprechend den für diese Kategorie geltenden Anforderungen, die mit dieser Verwaltungsvorschrift umgesetzt werden.

Zur Gewährleistung einer einheitlichen Durchführung der risikobasierten Bewertung nach Artikel 2 Absatz 2 Buchstabe f Ziffer ii der NIS-2-Richtlinie in den Ländern hat der IT-Planungsrat in seiner 42. Sitzung am 3. November 2023 ein Identifizierungskonzept beschlossen (Beschluss 2023/39). Dieses ist auch für die Ermittlung der kritischen Einrichtungen im Land Bremen der Maßstab. Wie zur § 1 Nummer 1 dargestellt ergibt sich in Anwendung der NIS-2-Richtlinie daraus eine Beschränkung auf die unmittelbare Landesverwaltung und dort auf Einrichtungen in den Ressorts. Zudem sind gemäß Artikel 2 Absatz 7 der NIS-2-Richtlinie auch Einrichtungen der öffentlichen Verwaltung, die ihre Tätigkeiten in den Bereichen nationale Sicherheit, öffentliche Sicherheit, Verteidigung oder Strafverfolgung ausüben, vom Anwendungsbereich ausgenommen. Der Beschluss des IT-Planungsgrat sieht zudem vor, dass die Kommunalverwaltung („lokale Ebene“) sowie die Hochschulen („Bildungseinrichtungen“) entsprechend der Freistellung gemäß Artikel 2 Absatz 5 der NIS-2-Richtlinie einzubeziehen sind, um eine (richtlinienkonforme) einheitliche Umsetzung in den Ländern zu gewährleisten. Die Möglichkeit der Regulierung außerhalb der Umsetzung der NIS-2-Richtlinie bleibt dabei unberührt.

Mit Satz 2 werden die Senatskanzlei und die Senatorischen Behörden entsprechend dem Identifizierungskonzept formal identifiziert. Als oberste Landesbehörden sind sie gemäß Satz 3 auch für die erstmalige Identifizierung sowie deren regelmäßige Wiederholung für die ihnen nachgeordneten Einrichtungen der unmittelbaren Landesverwaltung in ihrem jeweiligen Geschäftsbereich zuständig. Ihre Verantwortung für diese nachgeordnete Identifizierung entspricht dem Ressortprinzip. Die Ergebnisse der erstmaligen Identifizierung, bei der die Zentralstelle die Ressorts unterstützt, sind zum genannten Stichtag der Zentralstelle mitzuteilen bzw. zu bestätigen. So ist gewährleistet, dass bereits mit Inkrafttreten der Verwaltungsvorschrift der Kreis der erfassten Einrichtungen abschließend feststeht und sich diese dementsprechend frühzeitig auf die praktische Umsetzung vorbereiten können. Damit ist auch die nachträgliche Übermittlung des Namens zur Registrierung nach Artikel 3 Absatz 4 Buchstabe a der NIS-2-Richtlinie überflüssig, was in § 4 Absatz 1 hinsichtlich der Listenführung berücksichtigt wird. Durch die regelmäßige Wiederholung der Identifizierung wird auch die Aktualität der Liste nach § 4 sichergestellt und insofern Artikel 3 Absatz 3 der NIS-2-Richtlinie umgesetzt.

Der Geschäftsbereich der oder des Bevollmächtigten beim Bund und für Europa ist nun in der Senatskanzlei angesiedelt und deshalb nicht selbständig zu erfassen und formal zu identifizieren. Das Landesamt für Verfassungsschutz dagegen ist als selbständige Einrichtung der öffentlichen Verwaltung zu behandeln (vgl. dazu § 1 Absatz 1 Nummer 1). Als Einrichtung der öffentlichen Verwaltung im Bereich „öffentliche Sicherheit“ gemäß Artikel 2 Absatz 7 NIS-2-Richtlinie, ist sie jedoch vom Anwendungsbereich der Richtlinie ausgenommen und muss nach dem Identifizierungskonzept des IT-Planungsrates nicht einbezogen werden.

Zu Absatz 3

Absatz 3 stellt klar, dass bestehende Regelungen zur Sicherheit in der Informationstechnik in der öffentlichen Verwaltung, insbesondere der Informationssicherheitsleitlinie der Freien Hansestadt Bremen (IS-LL FHB), neben der Verwaltungsvorschrift weiterhin Bestand haben. Kritische Einrichtungen der Landesverwaltung können insofern (zusätzlich) auch den dortigen Verpflichtungen und Anforderungen unterworfen sein. In der praktischen Umsetzung dieser Verwaltungsvorschrift wird es auch darum gehen, Strukturen zu bündeln oder so umzugestalten, dass sich keine unzweckmäßigen Dopplungen (z. B. bei den Meldepflichten) ergeben. Mittel- und langfristig kann insbesondere ein ganzheitliches Cybersicherheitsgesetz Abhilfe schaffen.

Zu § 3 (Zuständigkeit und Aufgaben)

§ 3 behandelt die nach der NIS-2-Richtlinie vorgesehenen Funktionen als „zuständige Behörde“ und „Computer-Notfallteam (CSIRT)“ und überträgt sie auf die Zentralstelle Cybersicherheit beim Senator für Inneres und Sport. Zudem wird die allgemeine Zusammenarbeit mit anderen relevanten Behörden geregelt.

Zu Absatz 1

Als „zuständige Behörde“ im Sinne von Artikel 8 Absatz1 und 2 der NIS-2-Richtlinie muss die Einhaltung der verbindlichen Bestimmungen dieser Verwaltungsvorschrift überwacht und müssen die kritischen Einrichtungen der Landesverwaltung diesbezüglich beaufsichtigt werden. Die entsprechenden Befugnisse sind in § 12 abschließend geregelt und gegenüber den Maßnahmen nach Artikel 33 der NIS-2-Richtlinie auf Grundlage von Artikel 31 Absatz 4 Satz 2 der NIS-2-Richtlinie insbesondere zur Wahrung der Ressorthoheit deutlich eingeschränkt (vgl. insoweit die Begründung zu § 12). Diese Funktion wird der Zentralstelle Cybersicherheit beim Senator für Inneres und Sport aufgrund ihrer besonderen Fachkompetenz für die Cybersicherheit zugewiesen. Eine Wahrnehmung durch das Finanzressort, insbesondere durch den Bereich der oder des Informationssicherheitsbeauftragten des Landes (CISO) im Rahmen der Zuständigkeit für die IT-Sicherheit in der öffentlichen Verwaltung, erscheint aus mehreren Gründen nicht sinnvoll. Zum anderen gehen die Zwecke der NIS-2-Richtlinie über die IT-Sicherheit im Teilbereich öffentlichen Verwaltung deutlich hinaus. Es besteht auch ein enger Zusammenhang mit der Richtlinie (EU) 2022/2555, die die physische Resilienz kritischer Einrichtungen betrifft und im Zuständigkeitsbereich des Innenressorts liegt. IT-Sicherheit ist nur ein Teilaspekt im größeren Teilbereich der Cybersicherheit und der Eigenschaft als kritische Infrastruktur. Im Fokus stehen die gesellschaftlichen und wirtschaftlichen Folgen eines Ausfalls der Dienste betroffener Einrichtungen. Des Weiteren soll die oder der CISO im Rahmen ihrer bzw. seiner Aufgaben im Bereich des zentralen Informationssicherheitsmanagements gerade bei der Implementierung der Vorgaben der NIS-2-Richtlinie koordinierend und unterstützend auf Seite der öffentlichen Verwaltung tätig werden. Diese wichtige Aufgabe und auch die damit einhergehende Vertrauensstellung könnte durch die gleichzeitige Wahrnehmung als Aufsichtsbehörde gefährdet werden. Ebenso ist der CISO-Bereich organisatorisch eng mit der Zuständigkeit der Senatorin oder des Senators für Finanzen für den Betrieb der zentralen IT-Infrastrukturen verbunden (derzeit durch ein gemeinsames Referat). Letzterer ist aber selbst in großen Teilen von der Umsetzung der NIS-2-Richtlinie betroffen. Zuletzt ist die Umsetzung

der NIS-2-Richtlnie auch für die Zukunft zu betrachten. Sollen diese in einem Cybersicherheitsgesetz auf Landesebene weitere Anforderungen an die IT-Sicherheit kritischer Infrastrukturen oder sonstiger schützenswerter Einrichtungen außerhalb der Verwaltung aufgestellt werden, müssen auch diese überwacht werden. Dies könnte aufgrund ihrer weiteren Zuständigkeit über die öffentliche Verwaltung hinaus nur die Zentralstelle. Doppelstrukturen wären aufgrund der gleichen Ziele nicht zweckmäßig.

Gleichwohl besteht das Erfordernis einer unabhängigen Stellung von den zu beaufsichtigenden Einrichtungen einschließlich des Innenressorts. Artikel 31 Absatz 4 Satz 1 der NIS-2-Richtlinie verlangt insoweit eine „operative Unabhängigkeit“. Diese soll durch die Verknüpfung der Anordnungsbefugnis für Aufsichtsmaßnahmen an die Position der oder des Chief Cyber Security Officer (CCSO) mit dessen in Satz 3 bis 5 beschriebener besonderer Stellung erreicht werden. Die jeweilige Senatorin oder der jeweilige Senator für Inneres sichert dieser oder diesem zum einen eine unabhängige Aufgabenwahrnehmung zu. Dies kann ähnlich zur Stellung von Datenschutzbeauftragten (vgl. Artikel 38 DSGVO) insbesondere dadurch erreicht werden, dass bei der Aufsichtsausübung keine Weisungen erteilt werden und ein Benachteiligungsverbot besteht. Eine Normierung der Weisungsfreiheit kann in einer Verwaltungsvorschrift mangels Vorliegens einer gesetzlichen Vorschrift im Sinne des § 35 Absatz 1 Satz 3 Beamtenstatusgesetz allerdings allenfalls zu einer entsprechenden Selbstbindung führen, weswegen auf eine diesbezügliche Konkretisierung im Vorschriftstext verzichtet wurde. Des Weiteren wird die operative Unabhängigkeit dadurch erreicht, dass ein direktes Vorspracherecht zur (nach § 7 Absatz 1 verantwortlichen) Leitung der betroffenen kritischen Einrichtung der öffentlichen Verwaltung, gegebenenfalls auch in der Gesamtverantwortlichkeit des zuständigen Senatsmitglieds, besteht. Letzteres kommt in Betracht, wenn dies aufgrund der Schwere des Verstoßes oder der unzureichenden Reaktion durch die nachgeordnete Leitung erforderlich erscheint (zur regulären Beteiligung der übergeordneten Behörden siehe die Begründung zu dem in § 12 vorgesehenen Verfahren). So werden die direkten Kommunikationswege verkürzt und es wird auch die Effektivität der Maßnahmen gestärkt.

Zu Absatz 2

Anforderungen und Aufgabenkreis eines CSIRT im Sinne der NIS-2-Richtlinie sind in deren Artikel 10 und 11 beschrieben. Auch diese Funktion soll die Zentralstelle Cybersicherheit beim Senator für Inneres und Sport ausüben. Die Zentralstelle Cybersicherheit wird als die geeignete Stelle für die Zuweisung der verschiedenen Aufgaben als CSIRT angesehen. Das CERT Nord ist derzeit bloßer Auftragnehmer im Mehrländerverbund und damit formell keine zu ermächtigende Stelle. Zudem ist es nur auf einzelne Komponenten eines CSIRT (Sammeln, Auswerten und Steuern von Informationen; vgl. § 3 Absatz 2 Nummer 1 und Nummer 3) und auf den Teilbereich „öffentliche Verwaltung“ beschränkt. Mit der Zentralstelle besteht auf Landesebene bereits eine Einheit, deren Kernaufgabe das Sammeln, Auswerten und die Steuerung von relevanten Informationen ist und die als sogenannter Single Point of Contact auch nicht auf solche mit Bezug zur öffentlichen Verwaltung beschränkt ist. Die Zentralstelle soll nach ihren Aufgaben gerade ressortübergreifend koordinierend und unterstützend tätig werden, was gerade technische Komponenten beinhalten kann. Sie besitzt das strategische Potenzial, sich zu einem Landes-CERT bzw. -CSIRT entwickeln zu können und ist daher auch für die Umsetzung der NIS-2-Richtlinie eine naheliegende Wahl.

Satz 2 verweist zur Erfüllung der notwendigen Anforderungen auf den Katalog in Artikel 11 Absatz 1 (und ergänzend Artikel 10 Absatz 3) der NIS-2-Richtlinie, der insoweit Bestandteil der hiesigen Regelung wird. Bezuggenommen wird auch auf die vorzuhaltenden technischen Fähigkeiten nach Artikel 11 Absatz 2 der NIS-2-Richtlinie. Die Anforderungen sind ihrer Zweckgebung entsprechend auszulegen. Insbesondere sind nicht für alle in Satz 4 genannten Aufgabenbereiche alle Anforderungen zu erfüllen. Die entsprechende Klarstellung in Satz 2 („so-

weit dies erforderlich ist“) ist insbesondere relevant, wenn Dritte mit der Ausführung bestimmter Aufgabenbereiche beauftragt werden. Dass dies nach den allgemeinen Regeln rechtlich möglich bleibt, stellt Satz 3 klar. Die Zentralstelle bleibt demnach verantwortlich und muss dafür sorgen, dass die jeweils nach der Richtlinie notwendigen Anforderungen eingehalten werden. In datenschutzrechtlicher Hinsicht liegt dann gegebenenfalls ein Auftragsverarbeitungsverhältnis vor. Da die in Satz 4 genannten CSIRT-Aufgaben vielschichtig sind und dabei im Einzelfall eine besondere technische Expertise erforderlich sein kann, die in der Zentralstelle nicht vorhanden ist bzw. die dort nicht dauerhaft vorgehalten werden kann, ist eine Beauftragung Dritter, insbesondere IT-Dienstleister, eine wirtschaftlich zweckmäßige Lösung, die zugleich auch ein hohes fachliches Niveau sichert.

Satz 4 zählt die Aufgaben des CSIRT nach Artikel 11 Absatz 3 Unterabsatz 1 der NIS-2-Richtlinie auf. Der Wortlaut wurde geringfügig angepasst und es wurden kleinere Änderungen vorgenommen. So wurden die in Artikel 11 Absatz 3 Unterabsatz 1 Buchstabe a der NIS-2-Richtlinie beschriebenen (unterschiedlichen) zwei Aufgabenbereiche vorliegend geteilt (Nummer 1 und Nummer 2). Die Leistung von (technischer) Unterstützung bei der Bewältigung von Sicherheitsvorfällen (Nummer 5) wird im Zusammenhang mit deren Erwähnung in Artikel 23 Absatz 5 der NIS-2-Richtlinie beschrieben und dementsprechend ebenso als Leistung „auf Ersuchen“ bewertet. Dem werden vorliegend auch die Tätigkeiten im Bereich der incident response“ als „Remote“ und „Mobile Incident Response Team“ („RIRT“ und „MIRT“) zugeordnet. Die in Nummer 5 erwähnte Datenforensik beschreibt dabei eine hierfür wesentliche Fähigkeit. Der Begriff des Schwachstellenscans aus Nummer 6 wird bereits in § 1 Absatz 1 Nummer 15 definiert. Auf die dortigen Ausführungen, insbesondere zum Verhältnis zu Überprüfungen durch CSIRT nach § 11 bzw. Art. 10 Absatz 3 Unterabsatz 2 der NIS-2-Richtlinie, wird verwiesen. Die Aufgaben eines Koordinators zur Offenlegung von Schwachstellen nach Artikel 12 Absatz 1 der NIS-2-Richtlinie (vgl. Artikel 10 Absatz 3 Unterabsatz 1 Buchstabe g der NIS-2-Richtlinie) ist nach hiesiger Auffassung nicht auf Landesebene, sondern durch den Bund, umzusetzen und wird vorliegend deshalb nicht erwähnt.

Satz 5 setzt die in Artikel 12 Absatz 3 Unterabsatz 3 der NIS-2-Richtlinie vorgesehene Priorisierungsmöglichkeit um.

Satz 6 stellt klar, dass die Zentralstelle für die CSIRT-Leistungen nach Satz 4, die auf Ersuchen erbracht werden, Kosten (Gebühren und Auslagen) erheben kann. Dies widerspricht nicht der NIS-2-Richtline, da die erfassten Einrichtungen grundsätzlich selbst für ihre IT-Sicherheit verantwortlich sind und das CSIRT mit seinen in Artikel 10 Absatz 3 genannten Kompetenzen nur bei Bedarf „unterstützend“ tätig sein soll. Das CSIRT soll nicht als vergünstigter IT-Dienstleister auftreten, zumal entsprechende Leistungen realistisch gar nicht unbegrenzt vorgehalten werden könnten. Ein Schwachstellenscan etwa kann bereits mehrere Tausend Euro kosten. Es gilt das Bremische Gebühren- und Beitragsgesetz (BremGebBeitrG).

Satz 7 stellt klar, dass die Aufgaben aus Satz 4 auch über den Kreis kritischer Einrichtungen der Landesverwaltung hinausgehen können. Wenn ein CSIRT mit entsprechenden Fähigkeiten aufzubauen ist, wird es zweckmäßig seine Tätigkeiten und Leistungen zumindest auch für die unmittelbare Landesverwaltung und mindestens die Verwaltung der Stadtgemeinde Bremen und gegebenenfalls auch der Stadtgemeinde Bremerhaven vorhalten. Potenziell besteht sogar über den Bereich der öffentlichen Verwaltung hinaus das Entwicklungspotenzial zu seinem Landes-CSIRT. Eine endgültige verbindliche Festlegung sollte zweckmäßigerweise im Rahmen der ganzheitlichen Cybersicherheitsgesetzgebung erfolgen. Ein Anspruch anderer Einrichtungen wird durch hiesige Regelung nicht begründet.

Zu Absatz 3

Absatz 3 Satz 1 setzt für die Funktion als „zuständige Behörde“ Artikel 8 Absatz 5, für die als „CSIRT“ Artikel 10 Absatz 2 der NIS-2-Richtlinie um. Satz 2 setzt für Letztere ergänzend Artikel 11 Absatz 2 der NIS-2-Richtlinie um.

Zu Absatz 4

Mit Absatz 4 wird Artikel 13 Absatz 4 und, soweit es durch Landesregelung möglich ist, auch Absatz 5 der NIS-2-Richtlinie umgesetzt. Eine nähere Ausgestaltung der Zusammenarbeit mit den zuständigen Behörden nach der Richtlinie (EU) 2022/2557 (sog. CER-Richtlinie) wird voraussichtlich im beabsichtigten KRITIS-Dachgesetz des Bundes erfolgen.

§ 4 (Liste kritischer Einrichtungen der Landesverwaltung)

§ 4 betrifft die nach Artikel 3 Absatz 3 der NIS-2-Richtlinie zu erstellende Liste.

Zu Absatz 1

Mit Absatz 1 wird insoweit Artikel 3 Absatz 3 Satz 1 und Absatz 4 Unterabsatz 1 der NIS-2-Richtlinie umgesetzt.

Die gesetzte Frist zur erstmaligen Mitteilung liegt bewusst weit vor der nach Artikel 3 Absatz 3 und Artikel 3 Absatz 5 (dort 17.04.2025), um gegebenenfalls noch notwendige Nachfragen stellen und Ergänzungen vornehmen zu können. Die Frist betrifft lediglich die aufgeführten genannten zusätzlichen Informationen. Die Namen der kritischen Einrichtungen der Landesverwaltung stehen bereits mit bei Inkrafttreten der Verwaltungsvorschrift durch die am 17. Oktober 2024 abgeschlossene Identifizierung nach § 2 Absatz 2 Satz 3 fest, sodass auf die Umsetzung von Artikel 3 Absatz 4 Unterabsatz 1 Buchstabe a der NIS-2-Richtlinie an dieser Stelle verzichtet werden kann bzw. diese bereits durch § 2 Absatz 2 Satz 3 abschließend erfolgt ist. Die Angaben aus Artikel 3 Absatz 4 Unterabsatz 1 Buchstabe b der NIS-2-Richtlinie wurden vorliegend zwischen der Anschrift, den Kontaktdaten und den IP-Adressbereichen aufgrund der unterschiedlich verfolgten Zwecke aufgeteilt. Anzugeben sind die Anschriften der Haupt- und gegebenenfalls weiterer vorhandener Liegenschaften der Einrichtung. Des Weiteren sind aktuelle Kontaktdaten (Name, Email, Telefonnummern etc.) der für die IT-Sicherheit verantwortlichen Personen, in jedem Fall der Leitung sowie, wenn vorhanden, der oder dem Informationssicherheitsbeauftragten mitzuteilen, um im Bedarfsfall einen schnellen und unmittelbaren Kontakt herstellen zu können. Zuletzt sind auch die einschlägigen IP-Adressbereiche mitzuteilen. Dies kann insbesondere auch für Maßnahmen nach § 11 relevant sein.

Satz 3 und 4 regeln die Anpassung der Liste nach Wiederholung der Identifizierung im Verfahren nach § 2 Absatz 2 Satz 2. Im Fall der erstmaligen Identifizierung besteht eine Frist von 3 Monaten, um die Angaben nach Satz 2 der Zentralstelle mitzuteilen. Ist eine Einrichtung nicht mehr erfasst, ist sie mit ihren Angaben vollständig aus der Liste zu entfernen.

Zu Absatz 2

Absatz 2 statuiert eine unverzügliche Mitteilungspflicht bei Änderungen der Angaben nach Absatz 1 Satz 2. Damit wird Artikel 3 Absatz 4 Unterabsatz 2 der NIS-2-Richtlinie entsprochen.

Zu Absatz 3

Mit Absatz 3 wird Artikel 3 Absatz 3 Satz 2 der NIS-2-Richtlinie umgesetzt. Klargestellt wird dabei, dass konsequenterweise auch die korrekte Durchführung des Verfahrens nach § 2 Absatz 2 Satz 2 zu prüfen ist, da die Liste sonst schon nicht hinsichtlich der erfassten Einrichtungen aktuell ist.

Zu Absatz 4

Die in der Liste enthaltenen Daten sind sensibel und daher entsprechend der jeweils geltenden Verschlusssachenanweisung für das Land Bremen zu klassifizieren. Das Bundesamt für Sicherheit in der Informationstechnik erhält nach Absatz 5 lediglich die Mitteilung über die Anzahl an identifizierten Einrichtungen.

Zu Absatz 5

Absatz 5 setzt Artikel 3 Absatz 5 Buchstabe a der NIS-2-Richtlinie um. Da das BSI als zentrale Anlaufstelle im Sinne des Artikel 8 Absatz 3 der NIS-2-Richtlinie die Zahlen zentral an die EU-Kommission und die Kooperationsgruppe übermittelt, sind diese ihm mitzuteilen. Die geltende Frist wurden dabei mit dem Bund abgestimmt. Die Mitteilungspflicht besteht nur für die in den Anwendungsbereich der NIS-2-Richtlinie fallenden kritischen Einrichtungen der Landesverwaltung und ist deshalb durch Verweis auf § 2 Absatz 2 Satz 1auf jene beschränkt.

Zu § 5 (Risikomanagementmaßnahmen)

§ 5 dient der Umsetzung von Artikel 21 der NIS-2-Richtlinie.

Zu Absatz 1

Absatz 1 setzt Artikel 21 Absatz 1 und Absatz 4 der NIS-2-Richtlinie um.

Satz 1 statuiert den Grundsatz, dass geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen zu ergreifen sind, um die Sicherheit in der Informationstechnik (§ 1 Absatz 1 Nummer 3) zu gewährleisten. Diese abstrakten Anforderungen müssen von den betroffenen Einrichtungen für ihre jeweilige Informationstechnik für den Einzelfall angewendet werden. Es kann keinen verallgemeinerbaren Maßnahmenkatalog geben. Maßgeblich sind insbesondere der individuelle Schutzbedarf bzw. das jeweilige Risiko (§ 1 Absatz 1 Nummer 10). Die NIS-2-Richtlinie gibt jedoch bestimmte zu ergreifende Mindestmaßnahmen auf (vgl. Artikel 21 Absatz 2 der NIS-2-Richtlinie sowie Absatz 2 Satz 2). Es sind dabei sämtliche informationstechnischen Systeme, Komponenten und Prozesse zu berücksichtigen, die von der jeweiligen Einrichtung für die Erbringung ihrer Dienste, das heißt für ihren gesamten Betrieb, genutzt werden. Aufgrund der Vernetzung von IT-Systemen kann nur dieser ganzheitliche Ansatz zu einem effektiven Schutz führen. Dementsprechend reicht es nicht, nur die Informationstechnik zu schützen, die für die Dienste genutzt werden, deren Bewertung nach Artikel 2 Absatz 2 Buchstabe f Ziffer ii der NIS-2-Richtlinie zur Einbeziehung in dem Geltungsbereich der Richtlinie bzw. dieser Verwaltungsvorschrift geführt hat.

Satz 2 setzt Artikel 21 Absatz 1 Unterabsatz 2 um und konkretisiert die Vorgaben zur Verhältnismäßigkeit der zu ergreifenden Maßnahmen.

Satz 3 statuiert eine Dokumentationspflicht für die ergriffenen Risikomanagementmaßnahmen, einschließlich der Mindestvorgaben nach Absatz 2 Satz 2 als Ausfluss der Verpflichtung nach Absatz 1 Satz 1. Dies ermöglicht eine effektive Kontrolle nach § 12 Absatz 1, die sich im Ausgangspunkt auf schriftliche Nachweise stützt. Entsprechende Dokumentationen können beispielsweise sein: interne Richtlinien, Handlungsanweisungen, Checklisten, Mitarbeiterschulungen, Vereinbarungen, Merkblätter o.ä., aber auch Auditberichte, Zertifizierungen oder Prüfungen.

Zu Absatz 2

Absatz 2 dient der Umsetzung von Artikel 21 Absatz 1 Unterabsatz 2 und vor allem von Artikel 21 Absatz 2.

Die Anforderungen an die zu ergreifenden Maßnahmen nach Absatz 1 Satz 1 richten sich auch nach dem Stand der Technik und einschlägigen europäischen und internationalen Normen, (z.B. ISO 27001 / ISO 27002 sowie dem IT-Grundschutzkompendium). Ebenso müssen sie

auf einen gefahrenübergreifenden Ansatz beruhen (sog. „All-Gefahren-„ bzw. „All-Hazards-Ansatz“), der auch den physischen Schutz der Informationstechnik beinhaltet (vgl. Artikel 21 Absatz 2 der NIS-2-Richtlinie).

Die in Satz 2 aufgezählten Maßnahmen, die den in Artikel 21 Absatz 2 Buchstabe a bis j der NIS-2-Richtlinie entsprechen, sind nach dem jeweiligen Schutzbedarf und dem jeweiligen Risiko (siehe Absatz 1) im mindesten zu prüfen und dabei auf ihre Anwendbarkeit hin zu bewerten. Soweit derzeit absehbar, gehen diese zwar teilweise über den derzeit in der Verwaltung weitgehend praktizierten Standard des IT-Grundschutz (vgl. Beschluss 2019/04 des IT-Planungsrats sowie Punkt 3.5 der IS-LL FHB) hinaus, werden im Übrigen aber von diesem weitgehend abgedeckt. Nach vorläufiger Bewertung könnte ein erheblicher Mehraufwand insbesondere im Bereich des sog. Business Continuity Managements und gegebenenfalls bei der Multi-Faktor-Authentifizierung entstehen. Generell müssen alle Risikomanagementmaßnahmen in Hinblick auf den aktuellen Umsetzungsstand geprüft und die daraus voraussichtlich umzusetzenden Maßnahmen bewertet werden.

Unter „Konzepte in Bezug auf die Risikoanalyse und Sicherheit für informationstechnische Systeme“ nach Nummer 1 sind Richtlinien zu Risiken und zur Informationssicherheit zu verstehen. Die kritischen Einrichtungen der Landesverwaltung werden damit verpflichtet, diese Richtlinien in ihrem Zuständigkeitsbereich zu erlassen, sofern dies nicht bereits erfolgt ist. Hierzu gehören insbesondere die Durchführung einer allgemeinen Risikoanalyse sowie der Aufbau eines Informationssicherheitsmanagements.

Die „Bewältigung von Sicherheitsvorfällen“ nach Nummer 2 wird in § 1 Absatz 1 Nummer 9 definiert. Gemeint sind Maßnahmen der sog. incident response. Hierzu gehört die Ermittlung der Gefahr eines Sicherheitsvorfalls, Maßnahmen zur Verhinderung und dessen Aufdeckung, Maßnahmen zur Reaktion darauf und zur Wiederherstellung sowie der Minderung seiner Folgen. Unabhängig davon unterstützt das CSIRT betroffene Einrichtungen bei der Bewältigung von Sicherheitsvorfällen (siehe § 3 Absatz 2 Satz 4 Nummer 4 und § 8 Absatz 3 Satz 2).

Nach Nummer 3 wird auf Maßnahmen zur Aufrechterhaltung des Betriebs sowie zum Krisenmanagement Bezug genommen. Als Beispiele für Ersteres werden ein Backup-Management und Wiederherstellung nach einem Notfall (z. B. einem Sicherheitsvorfall) genannt. Gemeint sein dürften Maßnahmen im Bereich des sog. Business Continuity Managements.

Nummer 4 betrifft die Sicherheit in der Lieferkette. Ergänzend dazu gelten die Anforderungen nach Absatz 3. Lieferketten werden zunehmend globaler und komplexer. Um den Gefahren zu begegnen, die von sog. digitalen Supply-Chain-Attacken ausgehen, sind die kritischen Einrichtungen der Landesverwaltung verpflichtet, Risiken, die von unmittelbaren Lieferanten oder Diensteanbietern ausgehen, im Rahmen ihres Risikomanagements zu berücksichtigen. Unter Maßnahmen zur Sicherheit der Lieferkette sind beispielsweise vertragliche Vereinbarungen mit Zulieferern und Dienstleistern zu Risikomanagementmaßnahmen, die Bewältigung von Cybersicherheitsvorfällen sowie die Einhaltung durch den Auftraggeber vorgegebener Mindestanforderungen an die Cybersicherheit zu nennen.

Nach Nummer 5 sind Maßnahmen zur Sicherheit bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen zu ergreifen. Da durch die Ausnutzung von Schwachstellen in informationstechnischen Systemen erhebliche Störungen und Schäden verursacht werden können, ist ihre rasche Erkennung und Behebung ein wichtiger Faktor bei der Verringerung des Risikos. Hierbei ist der gesamte Lebenszyklus der informationstechnischen Systeme zu berücksichtigen. Zudem müssen geeignete Prozesse zum Management und zur Offenlegung von Schwachstellen vorgesehen werden.

Unter Nummer 6 fallen Maßnahmen und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen in der IT-Sicherheit. Insbesondere müssen kritische Einrichtungen der Landesverwaltung regelmäßig evaluieren, ob die gewählten Maßnahmen noch dem

Stand der Technik entsprechen, sich organisatorische Änderungen ergeben haben, die die Effektivität der Maßnahmen und Prozesse beeinflussen bzw., dass die gewählten Maßnahmen noch wirksam sind.

Nach Nummer 7 werden kritische Einrichtungen der Landesverwaltung zu Verfahren im Bereich Cyberhygiene sowie (ergänzend zur Pflicht der Einrichtungsleitung nach § 7 Absatz 2) zur Durchführung von Schulungen zur Schärfung des Bewusstseins der Mitarbeitenden bezüglich der IT-Sicherheit verpflichtet (vgl. auch Erwägungsgrund 89 der NIS-2-Richtlinie). Unter dem Begriff „Cyberhygiene" im Sinne der NIS-2-Richtlinie werden verschiedene grundlegende Verfahren und Herangehensweisen umschrieben, welche allgemein zu einer Verbesserung des Cybersicherheitsniveaus einer Einrichtung führen können. Dies kann beispielsweise Regelungen für sichere Passwörter, die Einschränkung von Zugriffskonten auf Administratorenebene sowie die Netzwerksegmentierungen beinhalten. Ob sich aus dieser Anforderung weitere Maßnahmen jenseits der ohnehin umzusetzenden Risikomanagementmaßnahmen ergeben werden, ist zum aktuellen Zeitpunkt noch unklar.

Nummer 8 verpflichtet zum, auf den Anforderungen des Schutzbedarfs basierenden, Einsatz von kryptografischen Konzepten und Verfahren sowie zum Einsatz von Verschlüsselung. Kryptografie ist ein weit verbreitetes Mittel, um die Informationssicherheit in den Schutzzielen Vertraulichkeit, Integrität und Authentizität zu gewährleisten. Mit Hilfe von kryptografischen Verfahren werden Informationen verschlüsselt, sodass deren Inhalt ohne den zugehörigen Schlüssel nicht lesbar ist. Kryptografische Verfahren können eingesetzt werden, um Online-Transaktionen zu schützen, die Kommunikation zu sichern und persönliche Informationen zu speichern.

Maßnahmen nach Nummer 9 tragen dem Umstand Rechnung, dass Sicherheitsrisiken auch durch Mitarbeitende und Dienstleister entstehen können. Daher ist sicherzustellen, dass Mitarbeitende nur auf die Informationen zugreifen können, die sie benötigen, um ihre Arbeit zu erledigen und dass sie diese Informationen nicht missbrauchen oder unbefugt weitergeben. Der in der englischen Textfassung zu Artikel 21 Absatz 2 Buchstabe i der NIS-2-Richtlinie verwendete Begriff „human resources security“ umfasst unter anderem Maßnahmen zur Zutritts- und Zugriffskontrolle. Der Begriff des „Anlagenmanagements“ (in der englischen Textfassung “asset management“) bezieht sich nach hiesiger Ansicht auf die Verwaltung der IT-Ausstattung und nicht zwangsläufig auf den physischen Schutz von Liegenschaften.

Nummer 10 betrifft Maßnahmen zur Authentifizierung und die Schaffung von Notfallkommunikationssystemen. Hierbei wird, wo erforderlich, der Einsatz von Multi-Faktor-Authentifizierung (MFA) benannt. MFA ist eine Authentifizierungsmethode, bei der eine Benutzerin oder ein Benutzer mindestens zwei Faktoren zur Verifizierung angeben muss, um Zugriff auf eine Anwendung oder Ressource zu erhalten. Dies sollte insbesondere für privilegierte Benutzer, wie Administratorenaccounts, relevant sein. Die kontinuierliche Authentifizierung ist eine Methode zur Überprüfung der Identität einer Benutzerin oder eines Benutzers während einer Sitzung. Gesicherte Sprach-, Video- und Textkommunikation bezieht sich auf die Nutzung logisch oder physisch von öffentlichen oder anderen privaten Netzen getrennter Kommunikationswege für Sprach-, Video- und Telekommunikationsdaten, die bei Bedarf noch durch Verwendung von Verschlüsselungstechnologien ergänzt oder ersetzt werden können.

Insbesondere noch zu klären sind weiterführende Abgrenzungen, die den physischen Schutz von IT-Systemen und den entsprechenden Anlagen betreffen mit Blick auf die Richtlinie (EU) 2557/2022 (sog. CER-Richtlinie), da mehrere der aufgeführten Risikomanagementmaßnahmen auch physische Schutzkomponenten aufweisen.

Zu Absatz 3

Absatz 3 setzt Artikel 21 Absatz 3 der NIS-2-Richtlinie um.

Bei Festlegung der nach Absatz 2 Satz 2 Nummer 4 zu ergreifenden Maßnahmen zur Gewährleistung der Sicherheit in der Lieferkette sind zum einen 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, zu berücksichtigen. Zum anderen sind die Ergebnisse der gemäß Artikel 22 Absatz 1 der NIS-2-Richtlinie durchgeführten koordinierten Risikobewertungen kritischer Lieferketten zu beachten.

Zu Absatz 4

Absatz 4 regelt (klarstellend) den Vorrang etwaig auf Grundlage von Artikel 21 Absatz 4 Unterabsatz 2 der NIS-2-Richtlinie erlassener Durchführungsrechtsakte der Europäischen Kommission.

Zu § 6 (Verwendung zertifizierter IKT-Produkte, -Dienste und –Prozesse)

§ 6 betrifft die Nutzung europäischer Schemata für die Cybersicherheitszertifizierung.

Zu Absatz 1

Mit Absatz 1 wird Artikel 24 Absatz 1 der NIS-Richtlinie umgesetzt.

Die Richtlinie sieht insoweit vor, dass die Mitgliedsstaaten erfasste Einrichtungen dazu verpflichten können, spezielle IKT-Produkte, -Dienste und -Prozesse (siehe § 1 Absatz 1 Nummer 11, 12 und 13) zu verwenden, die im Rahmen europäischer Schemata für die Cybersicherheitszertifizierung, die gemäß Artikel 49 der Verordnung (EU) 2019/881 angenommen wurden, zertifiziert sind. Dabei ist es unerheblich, ob diese von den betroffenen Einrichtungen selbst entwickelt wurden oder extern beschafft werden. Es zählt lediglich die Nutzung. Zweck der Verpflichtung ist es, durch die Zertifizierung die Erfüllung bestimmter in Artikel 21 genannter Anforderungen nachzuweisen.

Zur Wahrung der Ressorthoheit erfolgt die Umsetzung auf Landesebene kooperativ. Die Entscheidungskompetenz zur Anordnung der Verpflichtung gegenüber den kritischen Einrichtungen der Landesverwaltung verbleibt nach den bestehenden Zuständigkeiten in den Ressorts. Dies bewegt sich im Rahmen der Ermächtigung des Mitgliedsstaates nach Artikel 24 Absatz 1 der NIS-2-Richtlinie. Aufgrund ihrer hohen Fachkompetenz kann die Zentralstelle aber entsprechende Empfehlungen abgeben. Dabei handelt sie zur Wahrung der übergreifenden Interessen der Sicherheit der IT in der öffentlichen Verwaltung im Benehmen mit der oder dem CISO.

Diese besondere Verpflichtung ist nur verhältnismäßig, wenn ein erhöhtes Risiko (§ 1 Absatz 1 Nummer 10) hinsichtlich eines durch Informationstechnik erbrachten als kritisch bewerteten Dienstes besteht. Als kritischer Dienst kommen vor allem solche in Betracht, die gemäß § 2 Absatz 2 bzw. dem dort in Bezug genommenen Konzept des IT-Planungsrates zur Identifizierung geführt haben (vgl. Art. 2 Absatz 2 Buchstabe f Ziffer ii der NIS-2-Richtlinie: „Dienste, deren Störung erhebliche Auswirkungen auf kritische gesellschaftliche oder wirtschaftliche Tätigkeiten haben könnte“). Die Verpflichtung setzt voraus, dass überhaupt entsprechende Zertifizierungsschemata vorhanden sind. Vorab ist auch zu prüfen, dass für die einzubeziehenden Produkte, Dienste oder Prozesse eine ausreichende Verfügbarkeit am Markt sichergestellt ist. Die Empfehlung der Zentralstelle hat sich gleichermaßen an diese Maßstäbe zu halten.

Zu Absatz 2

Absatz 2 regelt (klarstellend) den Vorrang etwaig auf Grundlage von Artikel 24 Absatz 2 der NIS-2-Richtlinie erlassener Durchführungsrechtsakte der Europäischen Kommission.

Zu § 7 (Leitungsverantwortung und Schulungen)

§ 7 betrifft die Verantwortung der Leitungsebene sowie Schulungen und ist Artikel 20 der NIS-2-Richtlinie nachempfunden.

Zu Absatz 1

Absatz 1 dient dabei der Umsetzung von Artikel 20 Absatz 1 der NIS-2-Richtlinie.

Die Leitung einer kritischen Eirichtung der öffentlichen Verwaltung hat demnach die verpflichtenden Maßnahmen nach § 5 zu billigen und zu überwachen. Dies entspricht der in Punkt 4.1 IS-LL FHB festgeschriebenen Verantwortung. Betroffen ist die Leiterin oder der Leiter einer hinreichend verselbstständigten Einrichtung entsprechend den Ausführungen zu § 1 Nummer 1 (Behörden- bzw. Dienststellenleitung). Auch bei Einschaltung von Hilfspersonen (z. B. einer oder eines Informationssicherheitsbeauftragten) bleibt die Leitung letztverantwortlich.

Die Möglichkeit, für Verstöße haftbar gemacht zu werden, ist für die Außenhaftung durch die Regeln der Amtshaftung, die keine persönliche Inanspruchnahme vorsieht, und für die Innenhaftung durch das Recht des öffentlichen Dienstes bzw. das Beamtenrecht abschließend festgelegt. Sie bleiben dementsprechend auch gemäß Artikel 20 Absatz 1 Unterabsatz 2 der NIS-2-Richtlinie unberührt.

Zu Absatz 2

Mit Absatz 2 wird Artikel 20 Absatz 2 der NIS-2-Richtlinie umgesetzt.

Die Leitung muss regelmäßig selbst an beschriebenen Schulungen teilnehmen. Auch soll sie den Mitarbeiterinnen und Mitarbeitern regelmäßig entsprechende Schulungen anbieten bzw. die Teilnahme an solchen ermöglichen. Diese Pflichten ergänzen und konkretisieren insoweit in Bezug auf die Leitungsebene die Maßnahmen nach § 5 Absatz 2 Satz 2 Nummer 7.

Zu § 8 (Meldung erheblicher Sicherheitsvorfälle)

Mit § 8 wird die nach Artikel 23 der NIS-2-Richtlinie bestehende Meldeverpflichtung bei erheblichen Sicherheitsvorfällen für kritische Einrichtungen der Landesverwaltung geregelt. Anderweitig bestehende Meldeverpflichtungen, etwa nach Punkt 5.4. IS-LL FHB, bleiben daneben bestehen (vgl. auch § 9 Absatz 5).

Zu Absatz 1

Absatz 1 setzt das in Artikel 23 Absatz 4 Unterabsatz 1 Buchstabe a bis d der NIS-2-Richtlinie beschriebene mehrstufige Meldeverfahren um. Nummer 1 behandelt dabei die frühe Erstmeldung, Nummer 2 die bestätigende Erstmeldung, Nummer 3 die Zwischenmeldung und Nummer 4 die Abschlussmeldung.

Die Verpflichtung besteht für eine kritische Einrichtung, wenn bezüglich der von ihr genutzten IT ein erheblicher Sicherheitsvorfall gemäß den Kriterien nach § 1 Absatz 1 Nummer 7 (ggf. in Verbindung mit einem Durchführungsrechtakt nach § 1 Absatz 2) vorliegt. Die Meldeverpflichtung wird nicht dadurch aufgehoben, dass ein Dienstleister (z. B. Dataport AöR als zentraler staatlicher IT-Dienstleister) mit dem Betrieb der IT beauftragt wurde und gegebenenfalls auch deshalb als erstes Kenntnis über den Vorfall erlangt. Die Verantwortung liegt bei der Einrichtung. Sie muss für die Erfüllung der Pflicht gewährleisten. Dies schließt die Möglichkeit ein, dass die Meldeverpflichtung durch den Dienstleister im Auftrag der Einrichtung (oder gegebenenfalls übergeordnet durch das Ressort) erfüllt wird. Es verbleiben dann Kontroll- und Überwachungspflichten.

Die Zentralstelle fungiert als zuständige Meldestelle. Dabei kann es dahinstehen, ob sie dies gemäß Artikel 23 Absatz 1 Satz 1 der NIS-2-Richtlinie in ihrer Funktion als zuständige Behörde oder als CSIRT nach § 3 Absatz 1 und Absatz 2 tut. Die Zentralstelle ist in der Ausgestaltung

des Meldeweges grundsätzlich frei. Zweckmäßigerweise sollte ein einheitliches und kohärentes Meldesystem etabliert werden, das auch die bereits bestehenden Meldepflichten zum CERT-Nord nach Punkt 5.4 der IS-LL FHB berücksichtigt, sodass im Falle eines „erheblichen Sicherheitsvorfalles“ keine zweifache Meldung erforderlich ist bzw. ein gemeinsamer Meldeweg zur Verfügung steht. Infolgedessen wäre auch ein schneller und effizienter Informationsaustausch der beteiligten Stellen sicherzustellen.

Für die „Kenntniserlangung“ im Sinne von Nummer 1 und Nummer 2 genügt es, dass eine Mitarbeiterin oder ein Mitarbeiter der Einrichtung oder des von ihr mit dem Betrieb der IT beauftragten Dienstleisters innerhalb seiner Arbeitszeit Kenntnis über einen erheblichen Sicherheitsvorfall erlangt.

Zu Absatz 2

Absatz 2 setzt Artikel 23 Absatz 4 Unterabsatz 1 Buchstabe e der NIS-2-Richtlinie um.

Er regelt den Sonderfall, dass ein Sicherheitsvorfall einen Monat nach der ausführlichen Erstmeldung gemäß Absatz 1 Nummer 2 noch andauert. In diesem Fall ist anstatt einer Abschlussmeldung eine Fortschrittmeldung und die Abschlussmeldung einen Monat nach Bearbeitung des Vorfalls vorzulegen.

Zu Absatz 3

Absatz 3 setzt Artikel 23 Absatz 5 der NIS-2-Richtlinie um.

Da die Zentralstelle gemäß § 3 Absatz 2 auch als CSIRT fungiert, ist sie die kompetente Stelle für Orientierungshilfen, operative Beratungen und erforderlichenfalls auch für die technische Unterstützung als „RIRT“ und „MIRT“, soweit sie von der betroffenen kritischen Einrichtung der Landesverwaltung darum ersucht wird (vgl. dazu die Aufgabe nach § 3 Absatz 2 Satz 4 Nummer 4 und die entsprechenden Ausführungen in der zugehörigen Begründung dazu).

Die Richtlinie sieht vor, dass die Meldestelle den betroffenen Einrichtungen lediglich Orientierungshilfen zur Mitteilung an die Strafverfolgungsbehörden anbietet, wenn ein krimineller Hintergrund bei einem erheblichen Sicherheitsvorfall vermutet wird. Eine Mitteilungspflicht an die Strafverfolgungsbehörde seitens der Einrichtungen besteht nach der Richtlinie dagegen nicht. Diese Zurückhaltung ist bei der Betroffenheit innerhalb der Verwaltung aber nicht geboten. Anders als in der freien Wirtschaft wird durch die Beteiligung der Strafverfolgungsbehörden keine hemmende Wirkung auf die Erfüllung der Meldepflicht zu erwarten sein. Die betroffenen Einrichtungen sind wie die Strafverfolgungsbehörden selbst Teil der Landesverwaltung. Bei der Meldung handelt es sich um eine amtliche Pflicht. Persönliche wirtschaftliche Interessen bestehen nicht. Gleichzeitig besteht bei einer Straftat, die gegen die staatliche Infrastruktur gerichtet ist, ein erhöhtes öffentliches Interesse. Zudem kann durch eine Mitteilung dazu beigetragen werden, das Dunkelfeld im Bereich Cybercrime zu mindern. In der Gesamtabwägung rechtfertigt dies die Pflicht, jedenfalls die hiesigen gewichtigen „erheblichen“ Sicherheitsvorfälle, die die besonders schützenswerten „kritischen“ Einrichtungen der öffentlichen Verwaltung betreffen, grundsätzlich an die Strafverfolgungsbehörden melden zu müssen. Die Ausgestaltung als Soll-Vorschrift ermöglicht es im Ausnahmefall, gegenläufigen Interessen Rechnung zu tragen. Dies deckt sich auch mit dem Erwägungsgrund 107 der NIS-2-Richtlinie, nachdem die Mitgliedsstaaten die unter die Richtlinie fallenden Einrichtungen bei einem mutmaßlichen schwerwiegenden kriminellen Hintergrund dazu anhalten sollen, den Strafverfolgungsbehörden Mitteilung zu machen. Bei freiwilligen Meldungen und Mitteilungen nach § 9 besteht jedoch wegen § 9 Absatz 3 bzw. Artikel 30 Absatz 2 Unterabsatz 2 Satz 2 (konsequenterweise) keine entsprechende Pflicht.

Orientierungshilfen zur Strafverfolgung können etwa Hinweise auf zuständige Stellen sein oder solche zu Strafanzeigen sowie etwaig notwendigen Strafanträgen.

Gegebenenfalls kann es im weiteren Verlauf zu einer Zusammenarbeit der Zentralstelle mit den Strafverfolgungsbehörden kommen (vgl. auch § 3 Absatz 4).

Zu Absatz 4

Mit der Nummer 1 dieses Absatzes wird Artikel 23 Absatz 1 Unterabsatz und Absatz 6 der NIS-2-Richtlinie umgesetzt, mit der Nummer 2 Artikel 23 Absatz 9, soweit es um erhebliche Sicherheitsvorfälle geht.

Das BSI wird bei der Umsetzung der NIS-2-Richtlinie voraussichtlich als zentrale Anlaufstelle gemäß Artikel 8 Absatz 3 und 4 der NIS-2-Richtlinie benannt und fungiert deshalb auch als nationale Verbindungsstelle zu anderen Mitgliedsstaaten und zu den zuständigen europäischen Stellen. Zudem kommt der zentralen Anlaufstelle auch innerstaatlich eine koordinierende Rolle zu; sie soll die Zusammenarbeit mit anderen zuständigen Behörden gewährleisten. Nach Nummer 1 dieses Absatzes ist das BSI deshalb als zentrale Anlaufstelle bei grenz- oder sektorenübergreifenden erheblichen Sicherheitsvorfällen zu informieren. „Grenzübergreifend“ ist ein solcher nach hiesiger Auffassung dann, wenn er mindestens einen weiteren Mitgliedsstaat betrifft (siehe Artikel 23 Absatz 6 der NIS-2-Richtlinie; vgl. ebenso die Definition des „Cybersicherheitsvorfalls großen Ausmaßes“ nach Artikel 6 Nummer 7 der NIS-2-Richtlinie). Die Betroffenheit muss sich dabei nicht zwingend aus einer Beeinträchtigung der Sicherheit von IT-Systemen in jenem Mitgliedsstaat ergeben. Aus Artikel 23 Absatz 4 Unterabsatz 1 Buchstabe a und d der NIS-2-Richtlinie und dem Zweck der Richtlinie die Funktionsfähigkeit des Binnenmarktes zu gewährleisten wird vielmehr deutlich, dass bereits „grenzüberschreitende Auswirkungen“ ausreichen. Im Vordergrund stehen der durch den Vorfall gestörte Dienst der Einrichtung und die davon ausgehenden negativen Beeinträchtigungen für den Binnenmarkt und die Bevölkerung. Im hiesig geregelten Bereich der öffentlichen Verwaltung dürfte die Relevanz dann allerdings gering sein, da Verwaltungsdienste im Regelfall nur die nationale Ebene tangieren. „Sektorenübergreifend“ dürften Sicherheitsvorfälle sein, wenn die verursachten Störungen zu Kaskadeneffekten führen, die sich auf die Erbringung von Diensten in andere Sektoren auswirken (vgl. „Erwägungsgrund 37). Nach dem Zweck der Regelung in Artikel 23 Absatz 1 Unterabsatz 3 der NIS-2-Richtlinie wird es unter Berücksichtigung von Artikel 8 Absatz 4 der NIS-2-Richtlinie jedoch darum gehen, die Zusammenarbeit zwischen verschiedenen für die Sektoren zuständigen nationalen Behörden zu stärken. Die Informationspflicht ist insoweit dahingehend teleologisch zu reduzieren, dass sie nicht pauschal, sondern nur bei Betroffenheit der Zuständigkeit einer anderen (nationalen) Behörde, greift. Möglich erscheint es auch, dass in einem Sektor mehrere Behörden zuständig sind. Im Föderalsystem muss dies auch dahingehend verstanden werden, dass das BSI gegebenenfalls auch die Koordinierung zwischen zuständigen Landesbehörden übernimmt, wenn ein Sicherheitsvorfall mehrere Länder betrifft. Die Fälle, in denen Dienste einer Landesverwaltung Auswirkungen auf andere Länder haben oder die Zuständigkeit anderer Landesverwaltung gegeben ist, dürften jedoch ebenso die Ausnahme bleiben.

Nummer 2 betrifft die Übermittlung statistischer Daten zu den gemeldeten erheblichen Sicherheitsvorfällen an das BSI, damit dieses als nationale Anlaufstelle seine Pflicht zur Erstellung eines Berichts an die ENISA gemäß Artikel 23 Absatz 9 der NIS-2-Richtlinie erfüllen kann. Der benannte Stichtag sowie das Intervall der Übermittlung ist mit dem Bund und den anderen Ländern abgestimmt. Dieser Bericht enthält auch Daten zu freiwilligen Meldungen und Mitteilungen nach Artikel 30 der NIS-2-Richtlinie bzw. nach § 9 dieser Verwaltungsvorschrift (vgl. auch § 9 Absatz 4).

Zu Absatz 5

Absatz 5 regelt (klarstellend) den Vorrang etwaig auf Grundlage von Artikel 23 Absatz 11 Unterabsatz 1 der NIS-2-Richtlinie erlassener und die Pflichtmeldung nach Artikel 23 Absatz 1 der NIS-2-Richtlinie betreffende Durchführungsrechtsakte der Europäischen Kommission.

Zu § 9 (Freiwillige Meldungen und Mitteilungen)

Artikel 9 regelt freiwillige Meldungen im Sinne des Artikel 30 der NIS-2-Richtlinie. Aufgrund der besonderen Anforderungen an den Umgang mit einem Sicherheitsvorfall oder Beinahe-Vorfall, bei dem es tatsächlich in einem IT-System zu einer Verletzung der IT-Schutzziele nach § 1 Absatz 1 Nummer 3 gekommen ist oder diese zumindest konkret gefährdet waren, wird im Unterschied zur Richtlinie bei der vorliegenden Umsetzung begrifflich zwischen einer vorfallsbezogenen „Meldung“ und einer „Mitteilung“ mit sonst für die IT-Sicherheit relevanten Informationen, insbesondere zu Bedrohungen in der Informationstechnik, unterschieden. Andernfalls könnte das Meldeverfahren nach Artikel 23 der NIS-2-Richtlinie, auf das Artikel 30 Absatz 2 Unterabsatz 1 Satz 1 der NIS-2-Richtlinie verweist, gar nicht sinnvollerweise angewandt werden, da dieses auf die Bewältigung von Sicherheitsvorfällen nach einer konkreten Verletzung der Schutzziele der IT-Sicherheit nach § 1 Absatz 1 Nummer 3 zugeschnitten ist und nicht auf den Empfang sonstiger relevanter Informationen zur Cybersicherheit.

Zu Absatz 1

Absatz 1 betrifft die freiwillige Meldung von „sonstigen“, also nicht erheblichen, Sicherheitsvorfällen sowie Beinahe-Vorfällen. Diese können freiwillig an die Zentralstelle über den von ihr festgelegten Weg gemeldet werden. Die Umsetzung von Artikel 30 Absatz 1 Buchstabe a der NIS-2-Richtlinie erfolgt insofern nur in Bezug auf Vorfälle. Die Mitteilung von Informationen zu „Bedrohungen in der Informationstechnik“ (siehe § 1 Absatz 1 Nummer 4) bzw. „Cyberbedrohungen“ im Sinne der NIS-2-Richtlinie fällt entsprechend der oben beschriebenen Unterscheidung zwischen „Meldungen“ und „Mitteilungen“ unter Absatz 2 dieses Paragraphen.

Satz 2 setzt insoweit Artikel 30 Absatz 2 Unterabsatz 1 Satz 1 der NIS-2-Richtlinie um. In dem Verweis auf das Meldeverfahren nach § 8 bzw. Artikel 23 der NIS-2-Richtlinie könnte ein Widerspruch zu § 9 Absatz 2 bzw. Artikel 30 Absatz 2 Unterabsatz 2 Satz 2 der NIS-2-Richtlinie gesehen werden, da die dort normierten Anforderungen verbindlich angeordnet werden. Dagegen spricht gleichwohl, dass die Zielrichtung auch einer freiwilligen Meldung ins Leere geht, wenn sie nicht entsprechend dem Verfahren systematisch bearbeitet und so ein beidseitiger Nutzen sowohl für die meldende Stelle, die Unterstützung erhält, als auch für die Meldestelle, die Informationen erhält, generiert wird. Bei einer freiwilligen Meldung unterwirft sich die meldende Einrichtung bewusst diesem Verfahren und muss daher auch dessen Anforderungen entsprechen. Gleichwohl ist eine Kontrolle oder Sanktionierung bei Verstößen gegen das Meldeverfahren mangels Meldepflicht nicht vorgesehen.

Klarzustellen ist jedoch, dass die in § 8 Absatz 3 Satz 3 vorgesehene grundsätzliche Mitteilungspflicht an die Polizei bei freiwilligen Meldungen aufgrund von Artikel 30 Absatz 2 Unterabsatz 2 Satz 2 der NIS-2-Richtlinie nicht gilt.

Satz 3 setzt Artikel 30 Absatz 2 Unterabsatz 1 Satz 2 der NIS-2-Richtlinie um.

Zu Absatz 2

Absatz setzt Artikel 30 Absatz 1 Buchstabe a der NIS-2-Richtlinie hinsichtlich Bedrohungen in der Informationstechnik bzw. Cyberbedrohungen im Sinne der NIS-2-Richtlinie sowie Artikel 30 Absatz 1 Buchstabe b der NIS-2-Richtlinie um.

Das Sammeln und Auswerten von Informationen liegt unabhängig von der Umsetzung der NIS-2-Richtlinie im allgemeinen Aufgabenkreis der Zentralstelle. Dementsprechend nimmt sie auch von jeder Einrichtung (sowie von jeder sonstigen Stelle und jeder Person) in ihrer Funktion als eine allgemeine Kontakt- und Anlaufstelle Informationen entgegen. Dies gilt sowohl in Bezug auf die öffentliche Verwaltung als auch für private Kreise.

Soweit Verfahrensweisen nach § 8 bzw. Artikel 23 der NIS-2-Richtlinie entsprechend anwendbar erscheinen (z. B. die Antwort der Zentralstelle nach § 8 Absatz 3 Satz 1), sind diese bei der Annahme von Mitteilungen nach diesem Absatz 2 in Umsetzung von 30 Absatz 2 Unterabsatz 1 Satz 1 der NIS-2-Richtlinie zu beachten, auch wenn die Unterscheidung zwischen vorfallsbezogenen Meldungen und sonstigen Mitteilungen einer pauschalen Anwendung grundsätzlich entgegensteht (siehe dazu oben zu Absatz 1).

Zu Absatz 3

Mit Absatz 3 wird Artikel 30 Absatz 2 Unterabsatz 2 S. 2 der NIS-2-Richtlinie umgesetzt. Auf die Ausführungen zu Absatz 5 wird verwiesen.

Zu Absatz 4

Durch den Verweis auf § 8 Absatz 4 Nummer 1 wird zum einen Artikel 30 Absatz 2 Unterabsatz 2 Satz 1 in Verbindung mit Artikel 23 Absatz 1 Unterabsatz 3 und Absatz 6 sowie Artikel 13 Absatz 3 der NIS-2-Richtlinie umgesetzt. Grenz- oder sektorenübergreifende Sachverhalte können nur aus einer Beeinträchtigung der Dienste der Einrichtung erwachsen, sodass Beinahe-Vorfälle (klarstellend) ausgenommen werden. Hinsichtlich der Mitteilung an die zentrale Anlaufstelle wird auf die entsprechenden Ausführungen zu § 8 Absatz 4 Nummer 1 verwiesen. Entsprechende Vorfälle werden ohnehin selten sein, da bei einem grenz- oder sektorenübergreifenden Sachverhalt bereits ein erheblicher Sicherheitsvorfall im Sinne der § 1 Absatz 1 Nummer 7 zu erwägen sein dürfte, der nach § 8 Absatz 1 gemeldet werden muss.

Durch den Verweis auf § 8 Absatz 4 Nummer 2 wird Artikel 23 Absatz 9 der NIS-2-Richtlinie im Übrigen umgesetzt. Aus dem Wortlaut des Artikel 23 Absatz 9 der NIS-2-Richtlinie ergibt sich nicht eindeutig, dass auch die Beinahe-Vorfälle „erheblich“ sein müssen. Allerdings wäre es widersprüchlich, wenn hier niedrigere Anforderungen als hinsichtlich der erfassten erheblichen Bedrohungen und erheblichen Sicherheitsvorfälle gelten würden, zumal es nicht einmal zu einer Verletzung der Schutzziele der Sicherheit in der Informationstechnik gekommen ist. Es erscheint zweckmäßig die „Erheblichkeit“ eines Beinahe-Vorfalls fiktiv dadurch zu bestimmen, ob der Vorfall als erheblicher Sicherheitsvorfall im Sinne der § 1 Absatz 1 Nummer 7 einzustufen wäre, wenn das potenziell schädigende Ereignis eingetreten bzw. nicht verhindert worden wäre.

Durch Verweis auf § 8 Absatz 5 wird Artikel 23 Absatz 11 Unterabsatz 1 der NIS-2-Richtlinie im Übrigen umgesetzt.

Zu Absatz 5

Dieser Absatz stellt klar, dass die hiesig geregelten „freiwilligen Meldungen“ nicht die nach der IS-LL FHB bestehenden Melde- und Mitteilungsverpflichtungen, insbesondere nach deren Punkt 5.4, aufheben. In praktischer Hinsicht wird ein Meldesystem zweckmäßigerweise so auszugestalten sein, dass keine doppelten Meldungen an das CERT Nord und die Zentralstelle erforderlich sind, sondern ein einheitlicher Meldeweg zu Verfügung steht (vgl. bereits die Ausführungen zu § 8 Absatz 1).

Zu § 10 (Unterrichtung betroffener Kreise und der Öffentlichkeit)

§ 10 behandelt bei einem (erheblichen) Sicherheitsvorfall die verpflichtende Einbeziehung betroffener Empfänger von Diensten (betroffene Kreise) sowie der weiteren Öffentlichkeit.

Zu Absatz 1

Absatz 1 setzte Artikel 23 Absatz 1 Unterabsatz 1 Satz 2 der NIS-2-Richtlinie um. Die (potenziellen) Empfänger von Diensten der kritischen Einrichtungen der Verwaltung erfahren so von sie betreffenden, durch den erheblichen Sicherheitsvorfall ausgelösten Beeinträchtigungen

und können sich rechtzeitig vorbereiten. Dadurch werden die Folgen des Vorfalls geringgehalten. Zur Vereinfachung des Verfahrens, insbesondere aufgrund der Vielzahl von potenziellen Empfängern von Verwaltungsdiensten, genügt eine Veröffentlichung im Internet.

Zu Absatz 2

Absatz 2 Satz 1 betrifft die Fälle, in denen von kritischen Einrichtungen der Landesverwaltung mittels Informationstechnik angebotenen oder zugänglichen Dienste selbst eine erhebliche Bedrohung in der Informationstechnik für die Dienstempfänger ausgeht. Der Dienst muss also mit der IT der Dienstempfänger insoweit verbunden sein, dass Bedrohungen sich auf diese auswirken können und entsprechende von ihnen zu ergreifende Gegenmaßnahmen im Raum stehen. Solche Dienste sind wegen der Vielfalt denkbarer Verwaltungstätigkeiten bei kritischen Einrichtungen der Landesverwaltung gerade nicht ausgeschlossen, sodass der entsprechende Artikel 23 Absatz 2 der NIS-2-Richtlinie vorliegend umzusetzen war.

Die „erhebliche Bedrohung in der Informationstechnik“ (bzw. erhebliche Cyberbedrohung im Sinne der NIS-2-Richtlinie) wird in § 1 Absatz Nummer 5 definiert. Der Wortlaut des Artikel 23 Absatz 2 der NIS-2-Richtlinie macht es nicht unbedingt erforderlich, dass der erheblichen Bedrohung auch ein erheblicher Sicherheitsvorfall (oder überhaupt ein Sicherheitsfall) bei der verpflichteten kritischen Einrichtung der öffentlichen Verwaltung vorangegangen ist. Gleichwohl dürfte bei Vorliegen eines Sicherheitsvorfalles aufgrund des Maßes der Betroffenheit der Dienstempfänger bei einer erheblichen Bedrohung nach den Merkmalen des § 1 Absatz 1 Nummer 7 Buchstabe b das Überschreiten der Schwelle zur Erheblichkeit wahrscheinlich sein. Die „Bedrohung“ wird in den Fällen dieses Absatzes aus Sicht der Dienstempfänger zudem eine konkrete Gefahr für die Sicherheit in der Informationstechnik darstellen (vgl. dazu auch die Ausführungen zu § 1 Absatz 1 Nummer 4).

Absatz 2 Satz 2 regelt (klarstellend) den Vorrang etwaig auf Grundlage von Artikel 23 Absatz 11 Unterabsatz 1 der NIS-2-Richtlinie erlassener und Artikel 23 Absatz 2 der NIS-2-Richtlinie betreffender Durchführungsrechtsakte der Europäischen Kommission.

Zu Absatz 3

Absatz 3 setzt Artikel 23 Absatz 7 der NIS-2-Richtlinie um und regelt die Möglichkeit, die Öffentlichkeit über den erheblichen Sicherheitsvorfall zu informieren. In erster Linie geht es dabei um präventive Aspekte. Diese betreffen nach dem Wortlaut der Richtlinie nicht nur laufende Sicherheitsvorfälle, sondern auch abgeschlossene, soweit dadurch neue erhebliche Sicherheitsvorfälle verhindert werden können. Gerade in diesen Fällen wird ein (überwiegendes) öffentliches Interesse aber nur bestehen, wenn sich aus dem abgeschlossenen Sicherheitsvorfall relevante und noch aktuelle Erkenntnisse mit einem präventiven Nutzen für die Öffentlichkeit ableiten lassen. Dass die Sensibilisierung der Öffentlichkeit zur Bewältigung (vgl. dazu die Begriffsbestimmung nach § 1 Absatz 1 Nummer 9) eines laufenden Sicherheitsvorfalls notwendig ist, wird außerhalb der Fälle § 10 Absatz 2 in Bezug auf Einrichtungen der öffentlichen Verwaltung ebenso voraussichtlich selten anzunehmen sein, etwa zum Zwecke der Schadensminderung hinsichtlich der weiteren Auswirkungen der Beeinträchtigung der Dienste.

Mit dem Kriterium der Erforderlichkeit geht eine Beschränkung auf solche Fälle einher, in denen gleichgeeignete alternative Handlungsmöglichkeiten zur Erreichung der präventiven Ziele nicht bestehen. Zudem steht die Veröffentlichung im Ermessen der Zentralstelle und ist insofern auch offen für die Berücksichtigung gegenläufiger Interessen und Belange (z. B. des Geheimschutzes).

Die Norm ist zudem offen für weitere (unbenannte) Fälle einer Veröffentlichung aufgrund eines überwiegenden öffentlichen Interesses.

Durch das Anhörungsrecht der betroffenen Einrichtung wird eine Beteiligung zur Einbeziehung ihrer Interessen sichergestellt.

Zu § 11 (Nicht intrusive Überprüfungen bei öffentlich zugänglichen Systemen)

§ 11 behandelt die Befugnis nach Artikel 11 Absatz 3 Unterabsatz 2 der NIS-2-Richtlinie als CSIRT nicht intrusive Scans an öffentlich zugänglichen Schnittstellen von IT-Systemen durchzuführen und setzt die Richtlinie entsprechend um.

Die Regelung ist vergleichbar mit der derzeitigen Fassung des § 7b Absatz 1 BSIG, geht aber entsprechend den Vorgaben der NIS-2-Richtlinie über Portscans hinaus und schließt etwa auch andere webseiten-/domainbasierte Methoden ein. Die Scans bzw. Überprüfungen werden bewusst nicht weiter konkretisiert, um sie entsprechend dem technischen Fortschritt entwicklungsoffen zu halten. Anders als Schwachstellenscans im Sinne von § 1 Absatz 1 Nummer 15 bzw. Artikel 11 Absatz 3 Unterabsatz 1 Buchstabe e der NIS-2-Richtlinie dürfen solche Überprüfungen nie intrusiv sein und keinerlei nachteilige Auswirkung auf die Arbeits- und Funktionsfähigkeit der Einrichtung, insbesondere hinsichtlich ihrer Dienste, haben (vgl. Satz 4). Sie sind (konsequenterweise) auch nicht wie nach § 3 Absatz 2 Satz 4 Nummer 5 bzw. Artikel 11 Absatz 3 Unterabsatz 1 Buchstabe e der NIS-2-Richtlinie von einem Ersuchen der betreffenden kritischen Einrichtung der öffentlichen Verwaltung abhängig und können anlasslos und jederzeit erfolgen. Mit „öffentlich zugänglichen“ Schnittstellen von IT-Systemen sind solche gemeint, die allgemein erreichbar sind, insbesondere über das Internet. Das Eindringen in nicht öffentliche Netze ist daher unzulässig. Die nach der NIS-2-Richtlinie bezeichneten „anfälligen oder unsicher konfigurierten“ Systeme werden durch die Begriffe der „Schwachstellen“ und anderen „Sicherheitsrisiken“ ergänzt. Die Zielsetzung hiesiger Überprüfungen geht damit über den Schwachstellenscan im Sinne des § 1 Absatz 1 Nummer 15 hinaus, welcher sich deshalb auch nicht als Oberbegriff eignet (vgl. insoweit die Begründung zu § 1 Absatz 1 Nummer 15).

Durch die beschriebenen (nicht intrusiven) Überprüfungen wird auch nicht in Grundrechte eingegriffen. Es sind weder personenbezogenen Daten betroffen noch wird auf dem Fernmeldegeheimnis unterliegende Kommunikationsvorgänge zugegriffen. Zudem wird das System nur in einem sehr begrenzten Umfang geprüft und schon gar nicht derart tiefgreifend ausgespäht, dass in das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme eingegriffen würde. Eine gesetzliche Regelung ist deshalb nicht erforderlich. Sollte diese Schwelle im Einzelfall überschritten werden, könnte sich die Zentralstelle nicht auf hiesige Regelung berufen.

Nach Satz 2 ist die für den Betrieb verantwortliche Stelle zu unterrichten, insbesondere um unmittelbar auf etwaige festgestellte Risiken reagieren zu können. Darüber hinaus sind, falls diese nicht für den Betrieb verantwortlich sind, die betroffenen Einrichtungen und die übergeordnete Behörde als Betroffene über ihre jeweiligen Informationssicherheitsbeauftragten zu informieren sowie die oder der CISO als weitere für die IT-Sicherheit in der öffentlichen Verwaltung zuständige Stelle.

Satz 3 betrifft den Sonderfall, dass bei einer unmittelbaren Gefährdung sofortiger Handlungsbedarf besteht. In diesem Fall kann der den Betrieb des Systems durchführende IT-Dienstleister selbst benachrichtigt werden, um die notwendigen Maßnahmen zu ergreifen. Dies gilt auch, wenn im Einzelfall unklare Verantwortlichkeiten bestehen sollten. Diese sollten im Nachgang sinnvollerweise aufgeklärt werden.

Zu § 12 (Kontrolle und Aufsicht)

In § 12 wird die Beaufsichtigung der kritischen Einrichtungen der Landesverwaltung durch die Zentralstelle als „zuständige Behörde“ im Sinne der NIS-2-Richtlinie (vgl. § 3 Absatz 1) gere-

gelt. Absatz 1 betrifft die Kontrolle der Einhaltung der Verpflichtung zu Risikomanagementmaßnahmen nach § 5, Absatz 2 die der sonstigen nach dieser Verwaltungsvorschrift bestehenden Verpflichtungen. Absatz 3 regelt die besondere Zusammenarbeit der zuständigen Behörde mit den zuständigen Aufsichtsbehörden bei Verletzung des Schutzes personenbezogener Daten gemäß Artikel 35 der NIS-2-Richtlinie.

§ 12 sieht ein abgestuftes System der Aufsicht vor, dass insbesondere auf Kooperation mit den betroffenen Einrichtungen und den übergeordneten Behörden setzt und die Ressorthoheit angemessen berücksichtigt. Insoweit wird von der Möglichkeit des Artikel 31 Absatz 4 Satz 2 der NIS-2-Richtlinie Gebrauch gemacht, Aufsichts- und Durchsetzungsmaßnahmen im Einklang mit den nationalen rechtlichen und institutionellen Rahmenbedingungen verhältnismäßig, aber auch wirksam, zu gestalten. Ein völliger Verzicht auf Aufsichtsmaßnahmen durch die zuständige Behörde ist demnach nicht möglich. Der für „wichtige Einrichtungen“ im Sinne der NIS-2-Richtlinie geltende Maßnahmenkatalog des Artikel 33 der NIS-2-Richtlinie wird insoweit nur teilweise berücksichtigt.

Zur Wahrung der operativen Unabhängigkeit der Zentralstelle bei Ausübung der Aufsicht sind die nachfolgenden Maßnahmen ausschließlich durch die oder den CCSO anzuordnen (siehe dazu § 3 Absatz 1 Satz 3, 4 und 5 und die entsprechenden Ausführungen).

Gemäß der Freistellung nach Artikel 34 Absatz 7 der NIS-2-Richtlinie wurde bei der Umsetzung auch auf die Regelungsmöglichkeit zur Verhängung von Geldbußen gegen kritische Einrichtungen der Landesverwaltung verzichtet.

Zu Absatz 1

Die Aufsicht der Kontrolle der nach § 5 bestehenden Verpflichtungen ist für die IT- und Cybersicherheit besonders relevant und wird auch von der NIS-2-Richtlinie als essentiell hervorgehoben (vgl. Artikel 33 Absatz 1 der NIS-2-Richtlinie, der „insbesondere“ auf Artikel 21 der Richtlinie verweist).

Nach § 12 Absatz 1 ist insoweit ein abgestuftes Aufsichtssystem vorgesehen. Die Zentralstelle hat entsprechend der nach Artikel 33 Absatz 2 Unterabsatz 1 Buchstabe d) und e) der NIS-2-Richtlinie vorgesehenen Maßnahmen zunächst ein Auskunftsrecht und die Befugnis zur Einsicht in schriftliche Unterlagen. Die Umsetzung der Maßnahmen nach § 5 muss nach dessen Absatz 1 Satz 3 gerade dokumentiert werden. Dokumentationen können beispielsweise sein: interne Richtlinien, Handlungsanweisungen, Checklisten, Mitarbeiterschulungen, Vereinbarungen, Merkblätter o.ä., aber auch Auditberichte, Zertifizierungen oder Prüfungen (vgl. auch die entsprechenden Ausführungen zu § 5 Absatz 1). Ergeben sich insbesondere durch diese Kontrolle, gegebenenfalls aber auch aus anderen Quellen (z. B. interne oder externe Hinweise), Tatsachen, die darauf schließen lassen, dass die Maßnahmen ganz oder teilweise nicht oder nicht richtig umgesetzt sind, muss die betroffene Einrichtung innerhalb einer von der Zentralstelle gesetzten Frist den Verdacht entkräften oder, falls die Verpflichtung tatsächlich nicht eingehalten wird, innerhalb einer Frist die festgestellten Mängel beseitigen und dies hinreichend nachweisen. Über den Verdacht wird, sofern vorhanden, auch die übergeordnete Behörde informiert, die im Rahmen ihrer Aufsicht gegebenenfalls ebenso erforderliche Aufsichtsmaßnahmen einleiten kann. Bestehen nach Ablauf der Frist immer noch ein entsprechender Verdacht, kann die Zentralstelle im Einvernehmen mit der übergeordneten Behörde einen Nachweis durch Zertifizierungen, Prüfungen oder Audits verlangen. Die Kosten dafür hat dann die Einrichtung zu tragen. Diese Maßnahmen entsprechen dann weiteren in der NIS-2-Richtlinie in Bezug auf wichtige Einrichtungen vorgesehenen (vgl. Artikel 33 Absatz 2 Unterabsatz 1 Buchstabe b, c und f der NIS-2-Richtlinie). Sind oberste Landesbehörde als kritische Einrichtungen der Landesverwaltung selbst betroffen, können sie allerdings nicht gegen ihren Willen zur Nachweisführung durch Zertifizierungen, Prüfungen oder Sicherheitsaudits durch die Zentralstelle verpflichtet werden.

Die Anforderungen an den Verdachtsgrad sind nicht zu überhöhen. Mit ihm soll die schlechte Informationslage der Zentralstelle berücksichtigt werden, die, auch zur Wahrung der Ressorthoheiten, keinen vollständigen Einblick in die internen Abläufe der Einrichtung erlangen kann. Ein Vollbeweis ist nicht erforderlich. Der Verdacht muss aber über bloße Vermutungen hinausgehen.

Die Zentralstelle wird Maßnahmen nicht vor dem bezeichneten Stichtag beginnen. Dies schafft eine Zeitspanne, in der sich die kritischen Einrichtungen der Landesverwaltung nochmals mit ihren Pflichten auseinandersetzen und deren Erfüllung, gegebenenfalls auch schon nach den derzeitig geltenden Standards, überprüfen können. Gleichwohl sind die Verpflichtungen der NIS-2-richtlinie gemäß deren Artikel 41 Absatz 1 Unterabsatz 2 bei fristgemäßer Umsetzung bereits am 18. Oktober 2024 anzuwenden. Die hiesig normierte Frist zur Ausübung der Aufsicht berücksichtigt die Überprüfung die Anwendung der Richtlinie durch die Kommission nach Artikel 40 der NIS-2-Richtlinie erstmals im Oktober 2027.

Zu Absatz 2

Absatz 2 betrifft die Kontrolle der anderen nach der Verwaltungsvorschrift bestehenden Verpflichtungen (vor allem die Meldepflicht nach § 8 sowie die Leitungsverantwortung und Schulungspflicht nach § 7, die Unterrichtungspflichten nach §10, die Identifizierungspflicht nach § 2 Absatz 2 Satz 3 sowie die mit der Listenführung nach § 4 einhergehenden Mitteilungspflichten). Hier beschränken sich die Befugnisse der Zentralstelle im Grundsatz ebenso auf Auskunftsrechte und die Vorlage gegebenenfalls vorhandener schriftlicher Unterlagen, wobei keine flankierende Dokumentationspflicht besteht, sodass ein Verdacht der Nichterfüllung nicht hierauf allein gestützt werden kann. Rechtfertigen Tatsachen die Annahme, dass die Verpflichtungen nicht erfüllt werden, fordert die Zentralstelle zur Einhaltung und, sofern dies hinsichtlich der verletzten Verpflichtung in Betracht kommt, zur Nachbesserung innerhalb einer angemessenen Frist auf. Sie informiert, sofern vorhanden, in jedem Fall die zuständigen übergeordneten Behörden, damit diese im Rahmen ihrer Aufsicht tätig werden können.

Hinsichtlich des festgelegten Stichtages wird auf die Ausführungen zu Absatz 1 verwiesen.

Zu Absatz 3

Absatz 3 trifft ergänzend zu § 3 Absatz 4 besondere Regelungen zur Zusammenarbeit mit den zuständigen Datenschutzbehörden bei Verletzung des Schutzes personenbezogener Daten. Satz 1 setzt dabei Artikel 31 Absatz 3 um, Satz 2 und 3 dagegen Artikel 35 Absatz 1 und Absatz 3 der NIS-2-Richtlinie. Artikel 35 Absatz 2 der NIS-2-Richtlinie ist wegen des Gebrauchmachens von der Freistellung nach Artikel 34 Absatz 7 der NIS-2-Richtlinie nicht umzusetzen.

Zu § 13 (Cybersicherheitsstrategie)

Der Paragraph betrifft den Erlass und die Fortschreibung einer Cybersicherheitsstrategie. Nach übereinstimmender Auslegung des Artikel 7 der NIS-2-Richtlinie durch den Bund und die Länder ist es erforderlich, dass neben dem Bund auch jedes Land eine Cybersicherheitsstrategie erlassen muss, die den in der Richtlinie beschriebenen Anforderungen nach Artikel 7 Absatz 1 und Absatz 2 genügt. Nach hiesiger Ansicht ist dies in der Freien Hansestadt Bremen bereits durch die im April 2023 erlassene Bremische Cybersicherheitsstrategie hinreichend erfolgt, sodass kurzfristig kein Nachbesserungsbedarf besteht. Artikel 7 Absatz 4 der NIS-2-Richtlinie gibt vor, dass eine Evaluation derselben mindestens alle 5 Jahre erfolgen muss. Dieses wird durch Satz 2 der § 13 festgeschrieben, wobei bereits für 2025 eine Evaluation vorgesehen ist und auch anschließend kürzere Fristen möglich bleiben sollen.

Zu § 14 (Inkrafttreten)

Der Paragraph regelt das Inkrafttreten der Verwaltungsvorschrift.

**Der Landesbeauftragte
für Datenschutz und
Informationsfreiheit**

**Freie
Hansestadt
Bremen**

Der Landesbeauftragte für Datenschutz und Informationsfreiheit
Arndtstraße 1 • 27570 Bremerhaven

Der Senator für Inneres und Sport
Abteilung 3
Referat 36

NUR PER E-MAIL

Auskunft erteilt:
Herr Dr. Schwichtenberg

Tel. +49 421 361-98480

E-Mail:
office@datenschutz.bremen.de

T-Zentrale: +49 421 361-20 10
+ 49 471 596-20 10

PGP-Fingerprint: 89B5 D54E 72FE C489 E88F 6616
5FFB 6169 45DE 18AB

Datum und Zeichen Ihres Schreibens:

Unser Zeichen: (bitte bei Antwort angeben)
41-010-10.24/7#4

Bremerhaven, 20.12.2024

Verwaltungsvorschrift zur Umsetzung der NIS-2-Richtlinie in der Freien Hansestadt Bremen (VV NIS2Ums FHB)
hier: Stellungnahme des LfDI

Sehr geehrter Herr Tasler-Lohroff,
sehr geehrte Damen und Herren,

in der oben genannten Angelegenheit bedankt sich der Landesbeauftragte für Datenschutz und Informationsfreiheit (LfDI) für die Übermittlung des Entwurfs der Verwaltungsvorschrift zur Umsetzung der NIS-2-Richtlinie in der Freien Hansestadt Bremen (VV NIS2Ums FHB) und für die Möglichkeit zur Stellungnahme. Gerne nimmt der LfDI im Folgenden diese Möglichkeit in verkürzter Form wahr.

Die Stellungnahme erfolgt lediglich in verkürzter Form, da die VV NIS2Ums FHB keine Regelungen zur Datenverarbeitung durch die zuständigen Stellen vorsieht. Der LfDI erachtet derartige Regelungen jedoch zwingend für notwendig und weist daher nachdrücklich darauf hin, dass der Erlass eines Bremischen Cybersicherheits(basis)gesetzes mit den erforderlichen Befugnissen zur Datenverarbeitung zeitnah erfolgen muss. Der Entwurf des Gesetzes wurde bereits mit dem LfDI abgestimmt. Seine Stellungnahme zu diesem Gesetz vom 30.07.2024 hat er dem Senator für Inneres und Sport übermittelt.

Ohne ein derartiges Gesetz kommt zur Legitimierung der mit der VV NIS2Ums FHB verbundenen Datenverarbeitungen nur § 3 Abs. 1 Bremisches Ausführungsgesetz zur Datenschutzgrundverordnung (BremDSGVOAG) in Betracht, wobei je nach Fallkonstellation zwischen § 3 Abs. 1 Nr. 1 und Nr. 2 BremDSGVOAG zu differenzieren ist. § 3 Abs. 1 BremDSGVOAG kann als allgemein und unspezifisch gehaltener Erlaubnistatbestand jedoch nur Datenverarbeitungen mit geringer Eingriffsintensität legitimieren (siehe dazu bspw. HK-BremDSGVOAG/IFG/*Buchner,* DSGVOAG § 3 Rn. 5). Die Datenverarbeitungen, die mit der NIS-2-Richtlinie und mit der vorgelegten Rechtsvorschrift verbunden

sind, gehen Regelfall jedoch mit intensiveren Eingriffen einher, insbesondere in die Grundrechte der Beschäftigten der Freien Hansestadt Bremen. So wird z.B. die Bewältigung von Sicherheitsvorfällen im Sinne des § 1 Abs. 1 Nr. 9 VV NIS2Ums FHB in Einzelfällen eine Auswertung von Protokoll- und/oder sogar Inhaltsdaten erfordern, die auch dem Fernmeldegeheimnis unterliegen können. Für derartige Eingriffe ist § 3 Abs. 1 BremDSGVOAG keine hinreichende Legitimationsgrundlage. Auch der Bundesgesetzgeber hat daher etwa für die Verarbeitung von Protokolldaten spezifische Rechtsgrundlagen geschaffen (siehe z.B. §§ 8,9 BSIG-E). Derartige Befugnisse braucht es auch in der Freien Hansestadt Bremen, damit nicht zuletzt datenschutzrechtliche Aspekte und Anliegen der Cybersicherheit und NIS-2-Richtlinie, die im Ausgangspunkt gar nicht konträr zueinanderstehen, in Ausgleich gebracht werden können.

Mit freundlichen Grüßen
Im Auftrag

gez. Schwichtenberg

Dr. Schwichtenberg