EUROPÄISCHE
KOMMISSION

Brüssel, den 17.10.2024
C(2024) 7151 final

ANNEX

ANHANG

der

Durchführungsverordnung der Kommission

mit Durchführungsbestimmungen zur Richtlinie (EU) 2022/2555 im Hinblick auf die technischen und methodischen Anforderungen der Risikomanagementmaßnahmen im Bereich der Cybersicherheit und die Präzisierung der Fälle, in denen ein Sicherheitsvorfall in Bezug auf DNS-Diensteanbieter, TLD-Namenregister, Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltszustellnetzen, Anbieter verwalteter Dienste, Anbieter verwalteter Sicherheitsdienste, Anbieter von Online-Marktplätzen, Online-Suchmaschinen und Plattformen für Dienste sozialer Netzwerke und Vertrauensdiensteanbieter als erheblich gilt

ANHANG

Technische und methodische Anforderungen gemäß Artikel 2 der vorliegenden Verordnung

1. KONZEPT FÜR DIE SICHERHEIT VON NETZ- UND INFORMATIONSSYSTEMEN (ARTIKEL 21 ABSATZ 2 BUCHSTABE A DER RICHTLINIE (EU) 2022/2555)

1.1. Konzept für die Sicherheit von Netz- und Informationssystemen

1.1.1. Für die Zwecke von Artikel 21 Absatz 2 Buchstabe a der Richtlinie (EU) 2022/2555 muss das Konzept für die Sicherheit von Netz- und Informationssystemen

a) den Ansatz der betreffenden Einrichtungen für das Management der Sicherheit ihrer Netz- und Informationssysteme darlegen;

b) für die Geschäftsstrategie und die Ziele der betreffenden Einrichtungen geeignet sein und diese ergänzen;

c) die Ziele der Sicherheit von Netz- und Informationssystemen darlegen;

d) eine Verpflichtung zur kontinuierlichen Verbesserung der Sicherheit von Netz- und Informationssystemen enthalten;

e) eine Verpflichtung enthalten, die für seine Umsetzung erforderlichen angemessenen Ressourcen bereitzustellen, einschließlich des erforderlichen Personals, der erforderlichen Finanzmittel sowie der Verfahren, Instrumente und Technologien;

f) den einschlägigen Mitarbeitenden und interessierten externen Beteiligten mitgeteilt und von ihnen anerkannt werden;

g) die Festlegung der Rollen und Verantwortlichkeiten gemäß Nummer 1.2 enthalten;

h) die aufzubewahrenden Unterlagen und die Dauer ihrer Aufbewahrung aufführen;

i) die themenspezifischen Konzepte aufführen;

j) Indikatoren und Maßnahmen zur Überwachung seiner Umsetzung und des aktuellen Reifegrads der Netz- und Informationssicherheit in den betreffenden Einrichtungen festlegen;

k) das Datum der förmlichen Genehmigung durch die Leitungsorgane der betreffenden Einrichtungen (im Folgenden „Leitungsorgane“) enthalten.

1.1.2. Das Konzept für die Sicherheit von Netz- und Informationssystemen wird von den Leitungsorganen mindestens jährlich sowie bei erheblichen Sicherheitsvorfällen oder wesentlichen Änderungen der Betriebsabläufe oder der Risiken überprüft und – soweit angemessen – aktualisiert. Das Ergebnis der Überprüfung wird dokumentiert.

1.2. Rollen, Verantwortlichkeiten und Weisungsbefugnisse

1.2.1. Im Rahmen ihres Konzepts für die Sicherheit von Netz- und Informationssystemen gemäß Nummer 1.1 legen die betreffenden Einrichtungen Verantwortlichkeiten und

Weisungsbefugnisse für die Sicherheit von Netz- und Informationssystemen fest und ordnen sie den Rollen zu, weisen sie entsprechend dem Bedarf der jeweiligen Einrichtungen zu und teilen dies den Leitungsorganen mit.

1.2.2. Die betreffenden Einrichtungen verlangen von allen Mitarbeitenden und Dritten, die Netz- und Informationssystemsicherheit entsprechend dem festgelegten Konzept für die Sicherheit von Netz- und Informationssystemen, den themenspezifischen Konzepten und den Verfahren der betreffenden Einrichtungen anzuwenden.

1.2.3. Mindestens eine Person muss gegenüber den Leitungsorganen direkt für Fragen der Sicherheit von Netz- und Informationssystemen verantwortlich sein.

1.2.4. Je nach Größe der betreffenden Einrichtungen wird die Sicherheit von Netz- und Informationssystemen durch spezielle Rollen oder Aufgaben abgedeckt, die zusätzlich zu den bestehenden Rollen übernommen werden.

1.2.5. Widerstrebende Pflichten und sich widersprechende Verantwortlichkeiten werden – soweit anwendbar – getrennt.

1.2.6. Die Rollen, Verantwortlichkeiten und Weisungsbefugnisse werden von den Leitungsorganen in geplanten Zeitabständen sowie bei erheblichen Sicherheitsvorfällen oder wesentlichen Änderungen der Betriebsabläufe oder der Risiken überprüft und – soweit angemessen – aktualisiert.

2. KONZEPT FÜR DAS RISIKOMANAGEMENT (ARTIKEL 21 ABSATZ 2 BUCHSTABE A DER RICHTLINIE (EU) 2022/2555)

2.1. Risikomanagementrahmen

2.1.1. Für die Zwecke von Artikel 21 Absatz 2 Buchstabe a der Richtlinie (EU) 2022/2555 führen die betreffenden Einrichtungen einen geeigneten Risikomanagementrahmen ein, um die Risiken für die Sicherheit von Netz- und Informationssystemen zu ermitteln und anzugehen, und erhalten diesen Rahmen aufrecht. Die betreffenden Einrichtungen führen Risikobewertungen durch und dokumentieren diese; auf der Grundlage der Ergebnisse erstellen sie einen Risikobehandlungsplan, setzen diesen um und überwachen ihn. Die Ergebnisse der Risikobewertung und die Restrisiken werden von den Leitungsorganen oder – soweit anwendbar – von Personen akzeptiert, die für das Risikomanagement rechenschaftspflichtig und befugt sind, sofern die betreffenden Einrichtungen für eine angemessene Berichterstattung an die Leitungsorgane sorgen.

2.1.2. Für die Zwecke von Nummer 2.1.1 legen die betreffenden Einrichtungen Verfahren für die Ermittlung, Analyse, Bewertung und Behandlung von Risiken fest („Risikomanagementverfahren im Bereich der Cybersicherheit"). Das Risikomanagementverfahren im Bereich der Cybersicherheit ist – soweit anwendbar – fester Bestandteil des gesamten Risikomanagementverfahrens der betreffenden Einrichtungen. Als Teil des Risikomanagementverfahrens im Bereich der Cybersicherheit müssen die betreffenden Einrichtungen

a) eine Risikomanagementmethodik befolgen;

b) eine Risikotoleranzschwelle im Einklang mit der Risikobereitschaft der betreffenden Einrichtungen festlegen;

c) einschlägige Risikokriterien einführen und pflegen;

d) im Einklang mit einem gefahrenübergreifenden Ansatz die bestehenden Risiken für die Sicherheit von Netz- und Informationssystemen ermitteln und dokumentieren, insbesondere in Bezug auf Dritte sowie auf Risiken, die zu Störungen der Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit der Netz- und Informationssysteme führen könnten, wobei auch punktuelle Ausfälle zu ermitteln sind;

e) die bestehenden Risiken für die Sicherheit von Netz- und Informationssystemen analysieren, einschließlich des Niveaus der Bedrohung, der Wahrscheinlichkeit, der Auswirkung und des Risikos unter Berücksichtigung der Erkenntnisse über Cyberbedrohungen und Schwachstellen;

f) die ermittelten Risiken auf der Grundlage der Risikokriterien bewerten;

g) geeignete Optionen und Maßnahmen für die Behandlung von Risiken bestimmen;

h) die Umsetzung der Maßnahmen für die Behandlung von Risiken fortlaufend überwachen;

i) ermitteln, wer für die Umsetzung der Maßnahmen für die Behandlung von Risiken verantwortlich ist und wann diese erfolgen sollte;

j) die gewählten Maßnahmen für die Behandlung von Risiken in einem Risikobehandlungsplan dokumentieren und die Gründe für das Eingehen der Restrisiken umfassend erläutern.

2.1.3. Bei der Ermittlung und Priorisierung geeigneter Risikomanagementoptionen und -maßnahmen berücksichtigen die betreffenden Einrichtungen die Ergebnisse der Risikobewertung, die Ergebnisse des Verfahrens zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit, die Umsetzungskosten im Verhältnis zum erwarteten Nutzen, die in Nummer 12.1 genannte Klassifizierung von Anlagen und Werten und die in Nummer 4.1.3 genannte Analyse der betrieblichen Auswirkungen.

2.1.4. Die betreffenden Einrichtungen bewerten die Ergebnisse der Risikobewertung und den Risikobehandlungsplan in geplanten Zeitabständen und mindestens jährlich sowie bei wesentlichen Änderungen der Betriebsabläufe oder der Risiken oder bei erheblichen Sicherheitsvorfällen und aktualisieren sie – soweit angemessen.

2.2. Überwachung der Einhaltung

2.2.1. Die betreffenden Einrichtungen überprüfen regelmäßig die Einhaltung ihrer Konzepte für die Sicherheit von Netz- und Informationssystemen, themenspezifischen Konzepten, Vorschriften und Normen. Die Leitungsorgane werden durch regelmäßige Berichterstattung auf der Grundlage der Überprüfungen der Einhaltung über den Stand der Netz- und Informationssicherheit unterrichtet.

2.2.2. Die betreffenden Einrichtungen führen ein wirksames System für die Berichterstattung über die Einhaltung der Bestimmungen ein, das ihren Strukturen, Betriebsumfeldern und Bedrohungslandschaften angemessen ist. Das System für die Berichterstattung über die Einhaltung muss den Leitungsorganen einen fundierten

Überblick über den aktuellen Stand des Risikomanagements der betreffenden Einrichtungen geben können.

2.2.3. Die betreffenden Einrichtungen führen in geplanten Zeitabständen sowie bei erheblichen Sicherheitsvorfällen oder wesentlichen Änderungen der Betriebsabläufe oder der Risiken Maßnahmen zur Überwachung der Einhaltung durch.

2.3. Unabhängige Überprüfung der Netz- und Informationssicherheit

2.3.1. Die betreffenden Einrichtungen überprüfen unabhängig ihren Ansatz für das Management der Sicherheit von Netz- und Informationssystemen und dessen Umsetzung, einschließlich Personen, Verfahren und Technologien.

2.3.2. Die betreffenden Einrichtungen entwickeln Verfahren zur Durchführung unabhängiger Überprüfungen durch Personen mit angemessener Prüfungskompetenz und pflegen diese Verfahren. Wird die unabhängige Überprüfung von Mitgliedern des Personals der betreffenden Einrichtung durchgeführt, so dürfen die Personen, die die Überprüfungen durchführen, nicht dem Personal des zu überprüfenden Bereichs unterstellt sein. Lässt die Größe der betreffenden Einrichtungen eine solche Trennung der Befugnisse nicht zu, so ergreifen die betreffenden Einrichtungen alternative Maßnahmen, um die Unparteilichkeit der Überprüfungen zu gewährleisten.

2.3.3. Die Ergebnisse der unabhängigen Überprüfungen, einschließlich der Ergebnisse der Überwachung der Einhaltung gemäß Nummer 2.2 und der Überwachung und Messung gemäß Nummer 7, werden den Leitungsorganen gemeldet. Gemäß den Risikoakzeptanzkriterien der betreffenden Einrichtungen sind Korrekturmaßnahmen zu ergreifen oder Restrisiken zu akzeptieren.

2.3.4. Die unabhängigen Überprüfungen finden in geplanten Zeitabständen sowie bei erheblichen Sicherheitsvorfällen oder wesentlichen Änderungen der Betriebsabläufe oder der Risiken statt.

3. BEWÄLTIGUNG VON SICHERHEITSVORFÄLLEN (ARTIKEL 21 ABSATZ 2 BUCHSTABE B DER RICHTLINIE (EU) 2022/2555)

3.1. Konzept für die Bewältigung von Sicherheitsvorfällen

3.1.1. Für die Zwecke von Artikel 21 Absatz 2 Buchstabe b der Richtlinie (EU) 2022/2555 arbeiten die betreffenden Einrichtungen ein Konzept für die Bewältigung von Sicherheitsvorfällen aus, in dem Rollen, Verantwortlichkeiten und Verfahren für die zeitnahe Erkennung, Analyse, Eindämmung oder Reaktion, die Wiederherstellung sowie Dokumentation und Meldung in Bezug auf Sicherheitsvorfälle festgelegt werden, und setzen dieses um.

3.1.2. Das in Nummer 3.1.1 genannte Konzept muss mit dem Notfallplan für die Aufrechterhaltung und Wiederherstellung des Betriebs gemäß Nummer 4.1 im Einklang stehen. Das Konzept umfasst

a) ein Kategorisierungssystem für Sicherheitsvorfälle, das mit der Bewertung und Klassifizierung von Ereignissen gemäß Nummer 3.4.1 im Einklang steht;

b) wirksame Kommunikationspläne, auch für die Eskalation und Meldung;

c) eine Zuweisung der Rollen bei der Erkennung von Sicherheitsvorfällen und der angemessenen Reaktion darauf an kompetente Mitarbeitende;

d) Dokumente, die im Laufe der Erkennung von Sicherheitsvorfällen und der Reaktion darauf zu verwenden sind, wie Anleitungen für die Reaktion bei Sicherheitsvorfällen, Eskalationsschemata, Kontaktlisten und Vorlagen.

3.1.3. Die in dem Konzept festgelegten Rollen, Verantwortlichkeiten und Verfahren werden in geplanten Zeitabständen sowie bei erheblichen Sicherheitsvorfällen oder wesentlichen Änderungen der Betriebsabläufe oder der Risiken getestet, überprüft und – soweit angemessen – aktualisiert.

3.2. Überwachung und Protokollierung

3.2.1. Die betreffenden Einrichtungen legen Verfahren fest und verwenden Instrumente, um Aktivitäten in ihrem Netz- und Informationssystem zu überwachen und zu protokollieren, damit sie Ereignisse, die als Sicherheitsvorfälle betrachtet werden könnten, erkennen und zur Eindämmung der Auswirkungen entsprechend darauf reagieren können.

3.2.2. Soweit durchführbar, erfolgt die Überwachung automatisch und wird vorbehaltlich der betrieblichen Kapazitäten entweder kontinuierlich oder in regelmäßigen Zeitabständen durchgeführt. Die betreffenden Einrichtungen führen ihre Überwachungstätigkeiten so durch, dass es zu möglichst wenigen falsch positiven und falsch negativen Ergebnissen kommt.

3.2.3. Auf der Grundlage der in Nummer 3.2.1 genannten Verfahren führen, dokumentieren und überprüfen die betreffenden Einrichtungen Protokolle. Die betreffenden Einrichtungen erstellen auf der Grundlage der Ergebnisse der gemäß Nummer 2.1 durchgeführten Risikobewertung eine Liste der Anlagen und Werte, die Gegenstand der Protokollierung sind. Soweit angemessen, müssen die Protokolle Folgendes enthalten:

a) relevanten ausgehenden und eingehenden Netzverkehr;

b) Einrichtung, Änderung oder Löschung von Nutzern der Netz- und Informationssysteme der betreffenden Einrichtungen und Erweiterung der Berechtigungen;

c) Zugriffe auf Systeme und Anwendungen;

d) authentifizierungsbezogene Ereignisse;

e) alle privilegierten Zugriffe auf Systeme und Anwendungen sowie Aktivitäten der Verwaltungskonten;

f) Zugriffe auf kritische Konfigurations- und Backup-Sicherungsdateien oder Änderungen dieser Dateien;

g) Ereignisprotokolle und Protokolle von Sicherheitstools wie Antivirenprogrammen, Angriffserkennungssystemen oder Firewalls;

h) Nutzung der Systemressourcen sowie deren Leistung;

i) physischen Zugang zu Betriebsstätten;

j) Zugang zu ihren Netzwerkausrüstungen und -geräten und deren Nutzung;

k) Aktivierung, Beendigung und Pausieren der verschiedenen Protokolle;

l) Ereignisse im Umfeld.

3.2.4. Die Protokolle werden regelmäßig auf ungewöhnliche oder unerwünschte Trends überprüft. Soweit angemessen, legen die betreffenden Einrichtungen geeignete Werte für Alarmschwellen fest. Bei Überschreitung der festgelegten Alarmschwellenwerte wird – soweit angemessen – automatisch ein Alarm ausgelöst. Der betreffenden Einrichtungen stellen sicher, dass im Falle eines Alarms zeitnah eine qualifizierte und angemessene Reaktion eingeleitet wird.

3.2.5. Die betreffenden Einrichtungen führen und sichern die Protokolle für einen vorab festgelegten Zeitraum und schützen sie vor unbefugten Zugriffen oder Änderungen.

3.2.6. Soweit durchführbar, stellen die betreffenden Einrichtungen sicher, alle Systeme zeitlich synchronisiert sind, um Protokolle zwischen den Systemen für die Ereignisbewertung miteinander in Beziehung setzen zu können. Die betreffenden Einrichtungen erstellen und führen eine Liste aller Anlagen und Werten, die protokolliert werden, und stellen sicher, dass für die Überwachung und Protokollierung Redundanzsysteme zur Verfügung stehen. Die Verfügbarkeit der Überwachungs- und Protokollierungssysteme wird unabhängig von den von ihnen überwachten Systemen überwacht.

3.2.7. Die Verfahren sowie die Liste der protokollierten Anlagen und Werte werden in regelmäßigen Abständen und nach erheblichen Sicherheitsvorfällen überprüft und – soweit angemessen – aktualisiert.

3.3. Meldung von Ereignissen

3.3.1. Die betreffenden Einrichtungen richten einen einfachen Mechanismus ein, über den ihre Mitarbeitenden, Anbieter und Kunden verdächtige Ereignisse melden können.

3.3.2. Die betreffenden Einrichtungen unterrichten – soweit angemessen – ihre Anbieter und Kunden über den Mechanismus für die Meldung von Ereignissen und schulen ihre Mitarbeitenden regelmäßig in Bezug auf dessen Nutzung.

3.4. Bewertung und Klassifizierung von Ereignissen

3.4.1. Die betreffenden Einrichtungen bewerten verdächtige Ereignisse, um festzustellen, ob es sich um Sicherheitsvorfälle handelt, und – falls dies der Fall ist – um deren Art und Schwere zu bestimmen.

3.4.2. Für die Zwecke von Nummer 3.4.1 gehen die betreffenden Einrichtungen wie folgt vor:

a) Sie führen die Bewertung auf der Grundlage vorab festgelegter Kriterien und einer Triage durch, um die Priorisierung der Eindämmung und Beseitigung von Sicherheitsvorfällen zu bestimmen,

b) sie bewerten vierteljährlich, ob wiederholte Sicherheitsvorfälle gemäß Artikel 4 dieser Verordnung vorliegen,

c) sie überprüfen die betreffenden Protokolle für die Zwecke der Bewertung und Klassifizierung von Ereignissen,

d) sie führen ein Verfahren für die Korrelation und Analyse von Protokollen ein, und

e) sie bewerten und klassifizieren Ereignisse neu, falls neue Informationen verfügbar werden, oder nach der Auswertung zuvor verfügbarer Informationen.

3.5. Reaktion auf Sicherheitsvorfälle

3.5.1. Die betreffenden Einrichtungen reagieren auf Sicherheitsvorfälle zeitnah gemäß dokumentierten Verfahren.

3.5.2. Die Verfahren für Reaktionsmaßnahmen bei Sicherheitsvorfällen umfassen folgende Phasen:

a) Eindämmung des Sicherheitsvorfalls, um zu verhindern, dass sich dessen Folgen ausbreiten;

b) Beseitigung, um zu verhindern, dass der Sicherheitsvorfall andauert oder erneut auftritt;

c) erforderlichenfalls Wiederherstellung nach dem Sicherheitsvorfall.

3.5.3. Die betreffenden Einrichtungen erstellen Pläne und Verfahren für die Kommunikation

a) mit den Computer-Notfallteams (CSIRTs) oder – soweit anwendbar – mit den zuständigen Behörden im Zusammenhang mit der Meldung von Sicherheitsvorfällen;

b) zwischen den Mitgliedern des Personals der betreffenden Einrichtung und mit einschlägigen Interessenträgern außerhalb der betreffenden Einrichtung.

3.5.4. Die betreffenden Einrichtungen protokollieren die Tätigkeiten zur Reaktion auf Sicherheitsvorfälle gemäß den in Nummer 3.2.1 genannten Verfahren und sammeln Nachweise.

3.5.5. Die betreffenden Einrichtungen testen ihre Verfahren zur Reaktion auf Sicherheitsvorfälle in geplanten Zeitabständen.

3.6. Überprüfungen nach Sicherheitsvorfällen

3.6.1. Nach Sicherheitsvorfällen führen die betreffenden Einrichtungen im Anschluss an die Wiederherstellung – soweit angemessen – nachträgliche Überprüfungen durch. Bei der Überprüfung nach einem Sicherheitsvorfall wird, soweit möglich, die Ursache des Vorfalls ermittelt und es werden die daraus gezogenen Lehren dokumentiert, um das Auftreten und die Folgen künftiger Vorfälle zu verringern.

3.6.2. Die betreffenden Einrichtungen stellen sicher, dass die Überprüfungen nach Sicherheitsvorfällen zur Verbesserung ihres Konzepts für die Netz- und Informationssicherheit, zu Risikobehandlungsmaßnahmen und Verfahren zur Bewältigung und Erkennung von Sicherheitsvorfällen sowie zur Reaktion darauf beitragen.

3.6.3. Die betreffenden Einrichtungen überprüfen in geplanten Zeitabständen, ob Sicherheitsvorfälle entsprechende Überprüfungen nach sich zogen.

4. BETRIEBSKONTINUITÄTS- UND KRISENMANAGEMENT (ARTIKEL 21 ABSATZ 2 BUCHSTABE C DER RICHTLINIE (EU) 2022/2555)

4.1. Notfallplan für die Aufrechterhaltung und Wiederherstellung des Betriebs

4.1.1. Für die Zwecke von Artikel 21 Absatz 2 Buchstabe c der Richtlinie (EU) 2022/2555 legen die betreffenden Einrichtungen einen Notfallplan für die Aufrechterhaltung und Wiederherstellung des Betriebs fest, der bei Sicherheitsvorfällen Anwendung findet.

4.1.2. Die Abläufe der betreffenden Einrichtungen werden gemäß dem Notfallplan für die Aufrechterhaltung und Wiederherstellung des Betriebs wiederhergestellt. Der Plan beruht auf den Ergebnissen der gemäß Nummer 2.1 durchgeführten Risikobewertung ein und umfasst – soweit angemessen – Folgendes:

a) Zweck, Umfang und Zielgruppe;

b) Rollen und Verantwortlichkeiten;

c) wichtige Kontaktangaben und (interne und externe) Kommunikationskanäle;

d) Bedingungen für die Aktivierung und die Deaktivierung des Plans;

e) Reihenfolge der Wiederherstellung der Betriebsabläufe;

f) Wiederherstellungspläne für bestimmte Betriebsabläufe, einschließlich der Wiederherstellungsziele;

g) erforderliche Ressourcen, einschließlich Sicherungen und Redundanzen;

h) Wiederherstellung und Wiederaufnahme der Tätigkeiten nach vorübergehenden Maßnahmen.

4.1.3. Die betreffenden Einrichtungen führen eine Analyse der betrieblichen Auswirkungen durch, um die möglichen Auswirkungen schwerwiegender Störungen auf ihre Betriebsabläufe zu bewerten, und legen auf der Grundlage der Ergebnisse Kontinuitätsanforderungen für die Netz- und Informationssysteme fest.

4.1.4. Der Notfallplan für die Aufrechterhaltung und Wiederherstellung des Betriebs wird in geplanten Zeitabständen sowie bei erheblichen Sicherheitsvorfällen oder wesentlichen Änderungen der Betriebsabläufe oder der Risiken getestet, überprüft und – soweit angemessen – aktualisiert. Die betreffenden Einrichtungen stellen sicher, dass die aus diesen Tests gezogenen Lehren in die Pläne einfließen.

4.2. Backup-Sicherungs- und Redundanzmanagement

4.2.1. Die betreffenden Einrichtungen machen Sicherungskopien der Daten und stellen ausreichend verfügbare Ressourcen, einschließlich Betriebsstätten, Netz- und Informationssysteme sowie Personal, bereit, um ein angemessenes Maß an Redundanz zu gewährleisten.

4.2.2. Auf der Grundlage der Ergebnisse der gemäß Nummer 2.1 durchgeführten Risikobewertung und des Betriebskontinuitätsplans legen die betreffenden Einrichtungen Sicherungspläne fest, die Folgendes umfassen:

a) Wiederherstellungszeiten;

b) Gewährleistung, dass Sicherungskopien vollständig und genau sind, einschließlich Konfigurationsdaten und Daten, die in der Umgebung von Cloud-Computing-Diensten gespeichert sind;

c) Speicherung von Sicherungskopien (online oder offline) an einem oder mehreren sicheren Orten, die sich nicht im selben Netz wie das System sowie in ausreichend großer Entfernung befinden, um Schäden durch einen Notfall am Hauptstandort zu vermeiden;

d) geeignete physische und logische Zugangskontrollen zu Sicherungskopien entsprechend der Klassifizierungsstufe der Anlagen und Werte;

e) Wiederherstellung von Daten aus Sicherungskopien;

f) Aufbewahrungsfristen entsprechend geschäftlichen und regulatorischen Anforderungen.

4.2.3. Die betreffenden Einrichtungen führen regelmäßige Integritätsprüfungen der Sicherungskopien durch.

4.2.4. Auf der Grundlage der Ergebnisse der gemäß Nummer 2.1 durchgeführten Risikobewertung und des Betriebskontinuitätsplans sorgen die betreffenden Einrichtungen für eine ausreichende Verfügbarkeit von Ressourcen durch eine zumindest teilweise Redundanz der folgenden Elemente:

a) Netz- und Informationssysteme;

b) Anlagen und Werte, einschließlich Betriebsstätten, Ausrüstung und Verbrauchsmaterial;

c) Personal mit der erforderlichen Verantwortlichkeit, Weisungsbefugnis und Kompetenz;

d) geeignete Kommunikationskanäle.

4.2.5. Die betreffenden Einrichtungen stellen – soweit angemessen – sicher, dass sich die Überwachung und Anpassung der Ressourcen, einschließlich Betriebsstätten, Systeme und Personal, ordnungsgemäß auf die Anforderungen an die Sicherung und Redundanz stützen.

4.2.6. Die betreffenden Einrichtungen führen regelmäßige Tests der Wiederherstellung von Sicherungskopien und Redundanzen durch, um sicherzustellen, dass sie bei der Wiederherstellung zuverlässig sind und alle Kopien, Verfahren und Kenntnisse abdecken, die nötig sind, um eine wirksame Wiederherstellung durchzuführen. Die betreffenden Einrichtungen dokumentieren die Testergebnisse und ergreifen erforderlichenfalls Korrekturmaßnahmen.

4.3. Krisenmanagement

4.3.1. Die betreffenden Einrichtungen legen ein Verfahren für das Krisenmanagement fest.

4.3.2. Sie sorgen dafür, dass das Krisenmanagementverfahren mindestens die folgenden Elemente abdeckt:

a) Rollen und Verantwortlichkeiten des Personals und – soweit angemessen – der Anbieter und Diensteanbieter, wobei die Zuweisung der Rollen in Krisensituationen, einschließlich spezifischer zu befolgender Schritte, festgelegt wird;

b) geeignete Kommunikationsmittel zwischen den betreffenden Einrichtungen und den jeweils zuständigen Behörden;

c) Anwendung angemessener Maßnahmen zur Gewährleistung der Aufrechterhaltung der Sicherheit von Netz- und Informationssystemen in Krisensituationen.

Für die Zwecke von Buchstabe b umfasst der Informationsfluss zwischen den betreffenden Einrichtungen und den jeweils zuständigen Behörden sowohl obligatorische Mitteilungen wie Meldungen von Sicherheitsvorfällen und entsprechende Fristen als auch fakultative Mitteilungen.

4.3.3. Die betreffenden Einrichtungen führen ein Verfahren für die Verwaltung und Nutzung der von den CSIRTs oder – soweit anwendbar – den zuständigen Behörden erhaltenen Informationen über Sicherheitsvorfälle, Schwachstellen, Bedrohungen oder mögliche Risikominderungsmaßnahmen ein.

4.3.4. Die betreffenden Einrichtungen testen den Krisenmanagementplan in geplanten Zeitabständen oder nach erheblichen Sicherheitsvorfällen oder wesentlichen Änderungen der Betriebsabläufe oder der Risiken und aktualisieren ihn – soweit angemessen.

5. SICHERHEIT DER LIEFERKETTE (ARTIKEL 21 ABSATZ 2 BUCHSTABE D DER RICHTLINIE (EU) 2022/2555)

5.1. Konzept für die Sicherheit der Lieferkette

5.1.1. Für die Zwecke von Artikel 21 Absatz 2 Buchstabe d der Richtlinie (EU) 2022/2555 legen die betreffenden Einrichtungen ein Konzept für die Sicherheit der Lieferkette fest, das die Beziehungen zu ihren direkten Anbietern und Diensteanbietern regelt, setzen es um und wenden es an, um die ermittelten Risiken für die Sicherheit von Netz- und Informationssystemen zu mindern. Im Rahmen des Konzepts für die Sicherheit der Lieferkette legen die betreffenden Einrichtungen ihre Rolle in der Lieferkette fest und teilen sie ihren direkten Anbietern und Diensteanbietern mit.

5.1.2. Im Rahmen des in Nummer 5.1.1 genannten Konzepts für die Sicherheit der Lieferkette legen die betreffenden Einrichtungen Kriterien für die Auswahl von Anbietern und Diensteanbietern und die Auftragsvergabe an sie fest. Diese Kriterien umfassen Folgendes:

a) die Cybersicherheitsverfahren der Anbieter und Diensteanbieter, einschließlich der Sicherheit ihrer Entwicklungsprozesse;

b) die Fähigkeit der Anbieter und Diensteanbieter, die von den betreffenden Einrichtungen festgelegten Cybersicherheitsspezifikationen zu erfüllen;

c) die allgemeine Qualität und Resilienz der IKT-Produkte und -Dienste und die darin enthaltenen Risikomanagementmaßnahmen im Bereich der Cybersicherheit, einschließlich der Risiken und der Klassifizierungsstufe der IKT-Produkte und -Dienste;

d) die Fähigkeit der betreffenden Einrichtungen, ihre Versorgungsquellen zu diversifizieren und – soweit anwendbar – ihre Abhängigkeit von bestimmten Anbietern zu begrenzen.

5.1.3. Bei der Erstellung ihres Konzepts für die Sicherheit der Lieferkette berücksichtigen die betreffenden Einrichtungen – soweit anwendbar – die Ergebnisse koordinierter Sicherheitsrisikobewertungen kritischer Lieferketten gemäß Artikel 22 Absatz 1 der Richtlinie (EU) 2022/2555.

5.1.4. Auf der Grundlage des Konzepts für die Sicherheit der Lieferkette und unter Berücksichtigung der Ergebnisse der gemäß Nummer 2.1 dieses Anhangs durchgeführten Risikobewertung stellen die betreffenden Einrichtungen sicher, dass in ihren Verträgen mit Anbietern und Diensteanbietern – soweit angemessen – im Rahmen von Leistungsvereinbarungen Folgendes festgelegt wird:

a) Cybersicherheitsanforderungen an die Anbieter oder Diensteanbieter, einschließlich der Anforderungen an die Sicherheit beim Erwerb von IKT-Diensten oder -Produkten gemäß Nummer 6.1;

b) Sensibilisierungs-, Qualifikations- und Ausbildungsanforderungen sowie – soweit angemessen – Zertifizierungen, die von den Mitarbeitenden der Anbieter oder Diensteanbieter verlangt werden;

c) Anforderungen an die Zuverlässigkeitsüberprüfungen der Mitarbeitenden der Anbieter und Diensteanbieter;

d) eine Verpflichtung der Anbieter und Diensteanbieter, den betreffenden Einrichtungen Sicherheitsvorfälle, die ein Risiko für die Sicherheit der Netz- und Informationssysteme dieser Einrichtungen darstellen, unverzüglich zu melden;

e) das Recht auf Prüfung oder das Recht auf Erhalt von Prüfberichten;

f) eine Verpflichtung der Anbieter und Diensteanbieter zur Behebung von Schwachstellen, die ein Risiko für die Sicherheit der Netz- und Informationssysteme der betreffenden Einrichtungen darstellen;

g) Anforderungen an die Unterauftragsvergabe und – sofern die betreffenden Einrichtungen die Vergabe von Unteraufträgen zulassen – Cybersicherheitsanforderungen an Unterauftragnehmer im Einklang mit den unter Buchstabe a genannten Cybersicherheitsanforderungen;

h) Pflichten der Anbieter und Diensteanbieter bei Vertragskündigung, z. B. Abruf und Entsorgung der Informationen, die die Anbieter und Diensteanbieter in Wahrnehmung ihrer Aufgaben erlangten.

5.1.5. Die betreffenden Einrichtungen berücksichtigen die in den Nummern 5.1.2 und 5.1.3 genannten Elemente im Rahmen des Auswahlverfahrens für neue Anbieter und Diensteanbieter sowie im Rahmen des Vergabeverfahrens gemäß Nummer 6.1.

5.1.6. Die betreffenden Einrichtungen überprüfen das Konzept für die Sicherheit der Lieferkette, überwachen und bewerten Änderungen der Cybersicherheitsverfahren von Anbietern und Diensteanbietern bei wesentlichen Änderungen der Betriebsabläufe oder der Risiken oder bei erheblichen Sicherheitsvorfällen im Zusammenhang mit der Bereitstellung von IKT-Diensten oder mit Auswirkungen auf die Sicherheit der IKT-Produkte von Anbietern und Diensteanbietern und werden erforderlichenfalls im Hinblick auf diese Änderungen tätig.

5.1.7. Für die Zwecke von Nummer 5.1.6 müssen die betreffenden Einrichtungen

a) die Berichte über die Umsetzung der Leistungsvereinbarungen regelmäßig verfolgen – soweit anwendbar;

b) Sicherheitsvorfälle im Zusammenhang mit IKT-Produkten und -Diensten von Anbietern und Diensteanbietern überprüfen;

c) die Notwendigkeit außerplanmäßiger Überprüfungen prüfen und die Ergebnisse verständlich dokumentieren;

d) die Risiken, die sich aus Änderungen im Zusammenhang mit IKT-Produkten und -Diensten von Anbietern und Diensteanbietern ergeben, analysieren und – soweit angemessen – rechtzeitig Risikominderungsmaßnahmen ergreifen.

5.2. Verzeichnis der Anbieter und Diensteanbieter

Die betreffenden Einrichtungen führen ein Verzeichnis ihrer direkten Anbieter und Diensteanbieter, das Folgendes umfasst, und halten es auf dem neuesten Stand:

a) Kontaktstellen für jeden direkten Anbieter und Diensteanbieter;

b) eine Liste der IKT-Produkte, -Dienste und -Prozesse, die der direkte Anbieter oder Diensteanbieter für die betreffenden Einrichtungen bereitstellt.

6. SICHERHEITSMAßNAHMEN BEI ERWERB, ENTWICKLUNG UND WARTUNG VON NETZ- UND INFORMATIONSSYSTEMEN (ARTIKEL 21 ABSATZ 2 BUCHSTABE E DER RICHTLINIE (EU) 2022/2555)

6.1. Sicherheitsmaßnahmen beim Erwerb von IKT-Diensten oder IKT-Produkten

6.1.1. Für die Zwecke von Artikel 21 Absatz 2 Buchstabe e der Richtlinie (EU) 2022/2555 legen die betreffenden Einrichtungen auf der Grundlage der gemäß Nummer 2.1 durchgeführten Risikobewertung Verfahren für das Management der Risiken fest, die sich aus dem Erwerb von IKT-Diensten oder -Produkten für Komponenten ergeben, die für die Sicherheit der Netz- und Informationssysteme der betreffenden Einrichtungen unverzichtbar sind, und setzen sie um.

6.1.2. Für die Zwecke von Nummer 6.1.1 umfassen die in Nummer 6.1.1 genannten Verfahren Folgendes:

a) Sicherheitsanforderungen, die für die zu erwerbenden IKT-Dienste oder -Produkte gelten;

b) Anforderungen an Sicherheitsaktualisierungen während der gesamten Lebensdauer der IKT-Dienste oder -Produkte oder deren Ersatz nach Ablauf des Unterstützungszeitraums;

c) Informationen zur Beschreibung der Hardware- und Softwarekomponenten, die in den IKT-Diensten oder -Produkten verwendet werden;

d) Informationen zur Beschreibung der umgesetzten Cybersicherheitsfunktionen der IKT-Dienste oder -Produkte und der Konfiguration, die für ihren sicheren Betrieb erforderlich ist;

e) die Zusicherung, dass die IKT-Dienste oder -Produkte die Sicherheitsanforderungen gemäß Buchstabe a erfüllen;

f) Methoden zur Validierung, dass die bereitgestellten IKT-Dienste oder -Produkte die angegebenen Sicherheitsanforderungen erfüllen, sowie die Dokumentation der Ergebnisse der Validierung.

6.1.3. Die betreffenden Einrichtungen überprüfen die Verfahren in geplanten Zeitabständen sowie bei erheblichen Sicherheitsvorfällen und aktualisieren sie – soweit angemessen.

6.2. Sicherer Entwicklungszyklus

6.2.1. Vor der Entwicklung eines Netz- und Informationssystems, einschließlich Software, legen die betreffenden Einrichtungen Vorschriften für die Sicherheit der Entwicklung von Netz- und Informationssystemen fest und wenden diese bei der internen Entwicklung von Netz- und Informationssystemen und bei der Auslagerung der Entwicklung von Netz- und Informationssystemen an. Die Vorschriften gelten für alle Entwicklungsphasen, einschließlich Spezifikation, Konzeption, Entwicklung, Umsetzung und Tests.

6.2.2. Für die Zwecke von Nummer 6.2.1 müssen die betreffenden Einrichtungen

a) eine Analyse der Sicherheitsanforderungen in der Spezifikations- und Entwurfsphase jedes Entwicklungs- oder Beschaffungsvorhabens vornehmen, das von den betreffenden Einrichtungen oder im Namen dieser Einrichtungen durchgeführt wird;

b) bei allen Tätigkeiten zur Entwicklung von Informationssystemen bestimmte Grundsätze für den Aufbau sicherer Systeme und für ein sicheres Programmieren wie etwa die Förderung von konzeptintegrierter Cybersicherheit und Null-Vertrauen-Architekturen anwenden;

c) Sicherheitsanforderungen in Bezug auf Entwicklungsumgebungen festlegen;

d) Sicherheitstestverfahren im Entwicklungszyklus einführen und umsetzen;

e) Daten über Sicherheitstests angemessen auswählen, schützen und verwalten;

f) die Testdaten entsprechend der Risikobewertung gemäß Nummer 2.1 bereinigen und anonymisieren.

6.2.3. Bei einer ausgelagerten Entwicklung von Netz- und Informationssystemen wenden die betreffenden Einrichtungen darüber hinaus die in den Nummern 5 und 6.1 genannten Grundsätze und Verfahren an.

6.2.4. Die betreffenden Einrichtungen überprüfen ihre Vorschriften für die Sicherheit der Entwicklung in geplanten Zeitabständen und aktualisieren sie erforderlichenfalls.

6.3. Konfigurationsmanagement

6.3.1. Die betreffenden Einrichtungen ergreifen geeignete Maßnahmen, um Konfigurationen, einschließlich Sicherheitskonfigurationen von Hardware, Software, Diensten und Netzen, festzulegen, zu dokumentieren, umzusetzen und zu überwachen.

6.3.2. Für die Zwecke von Nummer 6.3.1 müssen die betreffenden Einrichtungen

a) Konfigurationen für ihre Hardware, Software, Dienste und Netze festlegen und deren Sicherheit gewährleisten;

b) Verfahren und Instrumente zur Durchsetzung der festgelegten sicheren Konfigurationen für Hardware, Software, Dienste und Netze, für neu installierte Systeme sowie für Systeme, die über ihre gesamte Lebensdauer in Betrieb sind, festlegen und umsetzen.

6.3.3. Die betreffenden Einrichtungen überprüfen die Konfigurationen in geplanten Zeitabständen oder bei erheblichen Sicherheitsvorfällen oder wesentlichen Änderungen der Betriebsabläufe oder der Risiken und aktualisieren sie – soweit angemessen.

6.4. Änderungsmanagement, Reparatur und Wartung

6.4.1. Die betreffenden Einrichtungen wenden Verfahren für das Änderungsmanagement an, um Änderungen an Netz- und Informationssystemen zu kontrollieren. Die Verfahren müssen – soweit anwendbar – mit den allgemeinen Grundsätzen der betreffenden Einrichtungen in Bezug auf das Änderungsmanagement im Einklang stehen.

6.4.2. Die in Nummer 6.4.1 genannten Verfahren gelten für Freigaben, Änderungen und Notfalländerungen an in Betrieb befindlicher Software und Hardware sowie für Änderungen der Konfiguration. Durch die Verfahren wird sichergestellt, dass diese Änderungen dokumentiert und auf der Grundlage der gemäß Nummer 2.1 durchgeführten Risikobewertung im Hinblick auf die möglichen Auswirkungen getestet und bewertet werden, bevor sie umgesetzt werden.

6.4.3. Konnten die regulären Änderungsmanagementverfahren aufgrund eines Notfalls nicht befolgt werden, dokumentieren die betreffenden Einrichtungen das Ergebnis der Änderung und die Begründung für die Nichteinhaltung der Verfahren.

6.4.4. Die betreffenden Einrichtungen überprüfen die Verfahren in geplanten Zeitabständen sowie bei erheblichen Sicherheitsvorfällen oder wesentlichen Änderungen der Betriebsabläufe oder der Risiken und aktualisieren sie – soweit angemessen.

6.5. Sicherheitsprüfung

6.5.1. Die betreffenden Einrichtungen legen ein Konzept und Verfahren für Sicherheitsprüfungen fest, setzen sie um und wenden sie an.

6.5.2. Die betreffenden Einrichtungen

a) legen auf der Grundlage der gemäß Nummer 2.1 durchgeführten Risikobewertung die Notwendigkeit, den Umfang, die Häufigkeit und die Art der Sicherheitsprüfungen fest;

b) führen Sicherheitsprüfungen nach einer dokumentierten Prüfmethode durch, die sich auf die Komponenten erstrecken, die im Rahmen einer Risikoanalyse als für den sicheren Betrieb relevant eingestuft wurden;

c) dokumentieren die Art, den Umfang, den Zeitraum und die Ergebnisse der Prüfungen, einschließlich der Bewertung der Kritikalität und der Risikominderungsmaßnahmen für jede Feststellung;

d) wenden im Falle kritischer Feststellungen Risikominderungsmaßnahmen an.

6.5.3. Die betreffenden Einrichtungen überprüfen ihre Konzepte für die Sicherheitsprüfung in geplanten Zeitabständen und aktualisieren sie – soweit angemessen.

6.6. Sicherheitspatch-Management

6.6.1. Die betreffenden Einrichtungen legen Verfahren, die mit den in Nummer 6.4.1 genannten Änderungsmanagementverfahren im Einklang stehen, und Änderungs-, Schwachstellen- und Risikomanagementverfahren sowie andere einschlägige Verfahren fest und wenden sie an, um sicherzustellen, dass

a) Sicherheitspatches innerhalb einer angemessenen Frist nach ihrer Verfügbarmachung angewendet werden;

b) Sicherheitspatches getestet werden, bevor sie in Produktionssystemen angewendet werden;

c) Sicherheitspatches aus vertrauenswürdigen Quellen stammen und auf ihre Integrität geprüft werden;

d) zusätzliche Maßnahmen umgesetzt und Restrisiken akzeptiert werden, wenn ein Patch nicht verfügbar ist oder nicht gemäß Nummer 6.6.2 angewendet wird.

6.6.2. Abweichend von Nummer 6.6.1 Buchstabe a können die betreffenden Einrichtungen verzichten, Sicherheitspatches anzuwenden, wenn die Nachteile der Anwendung der Sicherheitspatches die Vorteile für die Cybersicherheit überwiegen. Die betreffenden Einrichtungen dokumentieren und begründen dies ordnungsgemäß.

6.7. Netzsicherheit

6.7.1. Die betreffenden Einrichtungen ergreifen geeignete Maßnahmen, um ihre Netz- und Informationssysteme vor Cyberbedrohungen zu schützen.

6.7.2. Für die Zwecke von Nummer 6.7.1 müssen die betreffenden Einrichtungen

a) die Architektur des Netzes verständlich und aktuell dokumentieren;

b) Kontrollen festlegen und durchführen, um die internen Netzdomänen der betreffenden Einrichtungen vor unbefugtem Zugriff zu schützen;

c) die Kontrollen so konfigurieren, dass Zugriffe und Netzkommunikation verhindert werden, wenn dies für den Betrieb der betreffenden Einrichtungen nicht erforderlich ist;

d) die Kontrollen für den Fernzugriff auf Netz- und Informationssysteme, einschließlich des Zugangs von Diensteanbietern, festlegen und durchführen;

e) keine Systeme verwenden, die für die Verwaltung der Umsetzung der Sicherheitskonzepte für andere Zwecke verwendet werden;

f) nicht benötigte Verbindungen und Dienste ausdrücklich verbieten oder deaktivieren;

g) – soweit angemessen – den Zugang zu ihren Netz- und Informationssystemen ausschließlich mit von den betreffenden Einrichtungen genehmigten Geräten gewähren;

h) Verbindungen von Diensteanbietern nur nach einem Genehmigungsantrag und für einen bestimmten Zeitraum, z. B. für die Dauer von Wartungsarbeiten, zulassen;

i) die Kommunikation zwischen verschiedenen Systemen nur über vertrauenswürdige Kanäle herstellen, die durch logische, kryptografische oder physikalische Trennung von anderen Kommunikationskanälen isoliert sind, und eine sichere Identifizierung ihrer Endpunkte und den Schutz der Kanaldaten vor Änderung oder Offenlegung ermöglichen;

j) einen Durchführungsplan für den sicheren, angemessenen und schrittweisen vollständigen Übergang zur neuesten Generation der Kommunikationsprotokolle für die Netzwerkschicht annehmen und Maßnahmen zur Beschleunigung dieses Übergangs festlegen;

k) einen Durchführungsplan für die Einführung international vereinbarter und interoperabler moderner E-Mail-Kommunikationsnormen annehmen, um die E-Mail-Kommunikation zur Minderung von Schwachstellen im Zusammenhang mit E-Mail-Bedrohungen zu sichern, und Maßnahmen zur Beschleunigung dieser Einführung festlegen;

l) bewährte Verfahren für die Sicherheit des DNS sowie für die Sicherheit und Hygiene des Internet-Routings bei Verkehr, der aus dem Netz stammt und für das Netz bestimmt ist, anwenden.

6.7.3. Die betreffenden Einrichtungen überprüfen diese Maßnahmen in geplanten Zeitabständen sowie bei erheblichen Sicherheitsvorfällen oder wesentlichen Änderungen der Betriebsabläufe oder der Risiken und aktualisieren sie – soweit angemessen.

6.8. Netzsegmentierung

6.8.1. Die betreffenden Einrichtungen segmentieren ihre Systeme entsprechend den Ergebnissen der Risikobewertung gemäß Nummer 2.1 in Netze oder Zonen. Sie segmentieren ihre eigenen Systeme und Netze von Systemen und Netzen Dritter.

6.8.2. Für diese Zwecke müssen die betreffenden Einrichtungen

a) die funktionale, logische und physische Beziehung, einschließlich des Standorts, zwischen vertrauenswürdigen Systemen und Diensten berücksichtigen;

b) den Zugang zu einem Netz oder einer Zone auf der Grundlage einer Bewertung seiner/ihrer Sicherheitsanforderungen gewähren;

c) Systeme, die für den Betrieb der betreffenden Einrichtungen oder für die Sicherheit unverzichtbar sind, in gesicherten Zonen unterbringen;

d) eine demilitarisierte Zone innerhalb ihrer Kommunikationsnetze aufbauen, um die Sicherheit der Kommunikation, die aus ihren Netzen stammt oder für ihr Netz bestimmt ist, zu gewährleisten;

e) den Zugang zu und die Kommunikation zwischen und innerhalb von Zonen auf diejenigen beschränken, die für den Betrieb der betreffenden Einrichtungen oder für die Sicherheit erforderlich sind;

f) das spezielle Netz für die Verwaltung von Netz- und Informationssystemen vom operativen Netz der betreffenden Einrichtungen trennen;

g) Netzverwaltungskanäle von anderem Netzverkehr trennen;

h) die Produktionssysteme für die Dienste der betreffenden Einrichtungen von den Systemen trennen, die bei der Entwicklung und beim Testen, einschließlich der Sicherung, verwendet werden.

6.8.3. Die betreffenden Einrichtungen überprüfen die Netzsegmentierung in geplanten Zeitabständen sowie bei erheblichen Sicherheitsvorfällen oder wesentlichen Änderungen der Betriebsabläufe oder der Risiken und aktualisieren sie – soweit angemessen.

6.9. Schutz gegen Schadsoftware und nicht genehmigte Software

6.9.1. Die betreffenden Einrichtungen schützen ihre Netz- und Informationssysteme vor Schadsoftware und nicht genehmigter Software.

6.9.2. Zu diesem Zweck führen die betreffenden Einrichtungen insbesondere Maßnahmen durch, um die Verwendung von Schadsoftware oder nicht genehmigter Software aufzudecken oder zu verhindern. Die betreffenden Einrichtungen stellen – soweit angemessen – sicher, dass ihre Netz- und Informationssysteme mit einer Erkennungs- und Reaktionssoftware ausgestattet sind, die regelmäßig im Einklang mit der gemäß Nummer 2.1 durchgeführten Risikobewertung und den vertraglichen Vereinbarungen mit den Anbietern aktualisiert wird.

6.10. Behandlung und Offenlegung von Schwachstellen

6.10.1. Die betreffenden Einrichtungen erlangen Informationen über technische Schwachstellen in ihren Netz- und Informationssystemen, bewerten ihre Exposition gegenüber solchen Schwachstellen und ergreifen geeignete Maßnahmen zum Umgang mit diesen Schwachstellen.

6.10.2. Für die Zwecke von Nummer 6.10.1 müssen die betreffenden Einrichtungen

a) Informationen über Schwachstellen über geeignete Kanäle, wie z. B. Ankündigungen von CSIRTs oder zuständigen Behörden oder von Anbietern oder Diensteanbietern bereitgestellte Informationen, verfolgen;

b) – soweit angemessen – Schwachstellen-Scans durchführen und die Ergebnisse der Scans in geplanten Zeitabständen aufzeichnen;

c) Schwachstellen, die von den betreffenden Einrichtungen als für ihren Betrieb kritisch eingestuft wurden, unverzüglich beheben;

d) sicherstellen, dass die Behandlung von Schwachstellen mit den Verfahren für das Änderungsmanagement, das Sicherheitspatch-Management, das Risikomanagement und das Management von Sicherheitsvorfällen vereinbar ist;

e) ein Verfahren für die Offenlegung von Schwachstellen im Einklang mit den geltenden nationalen Konzepten für die koordinierte Offenlegung von Schwachstellen festlegen.

6.10.3. Wenn dies wegen der möglichen Auswirkungen der Schwachstelle gerechtfertigt ist, erstellen die betreffenden Einrichtungen einen Plan zur Minderung der Schwachstelle und setzen ihn um. Ansonsten dokumentieren und begründen die betreffenden Einrichtungen, warum die Schwachstelle keine Abhilfemaßnahmen erfordert.

6.10.4. Die betreffenden Einrichtungen überprüfen in geplanten Abständen die Kanäle, die sie für die Überwachung von Informationen über Schwachstellen nutzen, und aktualisieren sie – soweit angemessen.

7. KONZEPTE UND VERFAHREN ZUR BEWERTUNG DER WIRKSAMKEIT VON RISIKOMANAGEMENTMAßNAHMEN IM BEREICH DER CYBERSICHERHEIT (ARTIKEL 21 ABSATZ 2 BUCHSTABE F DER RICHTLINIE (EU) 2022/2555)

7.1. Für die Zwecke von Artikel 21 Absatz 2 Buchstabe f der Richtlinie (EU) 2022/2555 legen die betreffenden Einrichtungen ein Konzept und Verfahren fest, setzen sie um und wenden sie an, um zu bewerten, ob die ergriffenen Risikomanagementmaßnahmen im Bereich der Cybersicherheit wirksam umgesetzt und aufrechterhalten werden.

7.2. Das in Nummer 7.1 genannte Konzept und die entsprechenden Verfahren tragen den Ergebnissen der Risikobewertung gemäß Nummer 2.1 und früheren erheblichen Sicherheitsvorfällen Rechnung. Die betreffenden Einrichtungen müssen Folgendes bestimmen:

a) welche Risikomanagementmaßnahmen im Bereich der Cybersicherheit zu überwachen und zu messen sind, einschließlich Verfahren und Kontrollen;

b) die Methoden zur Überwachung, Messung, Analyse und Bewertung, sofern zutreffend, um gültige Ergebnisse sicherzustellen;

c) wann die Überwachung und Messung durchzuführen ist;

d) wer für die Überwachung und die Messung der Wirksamkeit der Risikomanagementmaßnahmen im Bereich der Cybersicherheit zuständig ist;

e) wann die Ergebnisse der Überwachung und der Messung zu analysieren und zu bewerten sind;

f) wer diese Ergebnisse analysieren und bewerten muss.

7.3. Die betreffenden Einrichtungen überprüfen das Konzept und die Verfahren in geplanten Zeitabständen sowie bei erheblichen Sicherheitsvorfällen oder wesentlichen Änderungen der Betriebsabläufe oder der Risiken und aktualisieren sie – soweit angemessen.

8. GRUNDLEGENDE VERFAHREN IM BEREICH DER CYBERHYGIENE UND SCHULUNGEN IM BEREICH DER CYBERSICHERHEIT (ARTIKEL 21 ABSATZ 2 BUCHSTABE G DER RICHTLINIE (EU) 2022/2555)

8.1. Sensibilisierungsmaßnahmen und grundlegende Verfahren im Bereich der Cyberhygiene

8.1.1. Für die Zwecke von Artikel 21 Absatz 2 Buchstabe g der Richtlinie (EU) 2022/2555 stellen die betreffenden Einrichtungen sicher, dass sich ihre Mitarbeitenden, einschließlich der Mitglieder von Leitungsorganen, sowie direkte Anbieter und Diensteanbieter der Risiken bewusst sind, über die Bedeutung der Cybersicherheit informiert werden und Verfahren im Bereich der Cyberhygiene anwenden.

8.1.2. Für die Zwecke von Nummer 8.1.1 bieten die betreffenden Einrichtungen ihren Mitarbeitenden, den Mitgliedern ihrer Leitungsorgane sowie – soweit angemessen – direkten Anbietern und Diensteanbietern gemäß Nummer 5.1.4 ein Sensibilisierungsprogramm an, das

a) zeitlich so geplant ist, dass die Maßnahmen wiederholt werden und neue Mitarbeitende erreichen;

b) mit dem Konzept für die Sicherheit von Netz- und Informationssystemen, den themenspezifischen Konzepten und den einschlägigen Verfahren für die Sicherheit von Netz- und Informationssystemen im Einklang steht;

c) einschlägige Cyberbedrohungen, bestehende Risikomanagementmaßnahmen im Bereich der Cybersicherheit, Kontaktstellen und Ressourcen für zusätzliche Informationen und Beratung zu Cybersicherheitsfragen sowie Verfahren im Bereich der Cyberhygiene für Nutzer abdeckt.

8.1.3. Das Sensibilisierungsprogramm wird – soweit angemessen – in geplanten Zeitabständen im Hinblick auf seine Wirksamkeit getestet. Das Sensibilisierungsprogramm wird in geplanten Zeitabständen aktualisiert und angeboten, wobei Änderungen der Verfahren im Bereich der Cyberhygiene sowie die aktuelle Bedrohungslage und die Risiken für die betreffenden Einrichtungen zu berücksichtigen sind.

8.2. Sicherheitsschulungen

8.2.1. Die betreffenden Einrichtungen ermittelt Mitarbeitende, deren Rollen sicherheitsrelevante Fähigkeiten und Fachkenntnisse erfordern, und stellt sicher, dass sie in Bezug auf die Sicherheit von Netz- und Informationssystemen regelmäßig geschult werden.

8.2.2. Die betreffenden Einrichtungen führen ein Schulungsprogramm im Einklang mit dem Konzept für die Sicherheit von Netz- und Informationssystemen, den themenspezifischen Konzepten und anderen einschlägigen Verfahren für die Sicherheit von Netz- und Informationssystemen ein, in dem der Schulungsbedarf für bestimmte Rollen und Positionen auf der Grundlage von Kriterien festgelegt wird, setzen es um und wenden es an.

8.2.3. Die Schulung gemäß Nummer 8.2.1 muss für die Funktion des Mitarbeitenden relevant sein, und ihre Wirksamkeit ist zu bewerten. Die Schulung muss den bestehenden Sicherheitsmaßnahmen Rechnung tragen und Folgendes umfassen:

a) Anweisungen für die sichere Konfiguration und den sicheren Betrieb der Netz- und Informationssysteme, einschließlich mobiler Geräte;

b) Unterrichtung über bekannte Cyberbedrohungen;

c) Schulung in Bezug auf das Verhalten bei sicherheitsrelevanten Ereignissen.

8.2.4. Die betreffenden Einrichtungen führen Schulungen für Mitglieder des Personals durch, die in neue Positionen oder Rollen wechseln, die sicherheitsrelevante Fähigkeiten und Fachkenntnisse erfordern.

8.2.5. Das Programm wird regelmäßig aktualisiert und durchgeführt, wobei geltende Konzepte und Vorschriften, zugewiesene Rollen und Verantwortlichkeiten sowie bekannte Cyberbedrohungen und technische Entwicklungen berücksichtigt werden.

9. KRYPTOGRAFIE (ARTIKEL 21 ABSATZ 2 BUCHSTABE H DER RICHTLINIE (EU) 2022/2555)

9.1. Für die Zwecke von Artikel 21 Absatz 2 Buchstabe h der Richtlinie (EU) 2022/2555 legen die betreffenden Einrichtungen ein Konzept und Verfahren in Bezug auf Kryptografie fest, setzen sie um und wenden sie an, um eine angemessene und wirksame Nutzung von Kryptografie sicherzustellen, damit die Vertraulichkeit, Authentizität und Integrität der Daten im Einklang mit der Anlagen- und Werteklassifizierung der betreffenden Einrichtungen und den Ergebnissen der gemäß Nummer 2.1 durchgeführten Risikobewertung geschützt sind.

9.2. In dem Konzept und den Verfahren gemäß Nummer 9.1 wird Folgendes festgelegt:

a) im Einklang mit der Einstufung der Anlagen und Werte der betreffenden Einrichtungen die Art, Stärke und Qualität der kryptografischen Maßnahmen, die zum Schutz der Anlagen und Werte der betreffenden Einrichtungen erforderlich sind, einschließlich der Daten, die gespeichert sind oder gerade übermittelt werden;

b) die auf der Grundlage von Buchstabe a anzunehmenden Protokolle oder Protokollfamilien sowie kryptografische Algorithmen, Kryptierungsstärke,

kryptografische Lösungen und Nutzungsverfahren, die zu genehmigen und für die Verwendung in den betreffenden Einrichtungen erforderlich sind, – soweit angemessen – nach einem Krypto-Agilitätsansatz;

c) der Ansatz der betreffenden Einrichtungen in Bezug auf das Schlüsselmanagement, – soweit angemessen – einschließlich der Methoden für

i) die Generierung verschiedener Schlüssel für kryptografische Systeme und Anwendungen;

ii) die Ausstellung und Erlangung von Public-Key-Zertifikaten;

iii) die Verteilung von Schlüsseln an die vorgesehenen Einrichtungen, einschließlich wie der Schlüssel nach Erhalt zu aktivieren ist;

iv) die Speicherung von Schlüsseln, einschließlich wie autorisierte Nutzer Zugang zu Schlüsseln erhalten;

v) die Änderung oder Aktualisierung von Schlüsseln, einschließlich Vorschriften darüber, wann und wie Schlüssel geändert werden können;

vi) den Umgang mit beeinträchtigten Schlüsseln;

vii) den Widerruf von Schlüsseln, einschließlich wie Schlüssel zurückzuziehen oder zu deaktivieren sind;

viii) die Wiederherstellung verlorener oder beschädigter Schlüssel;

ix) die Sicherung oder Archivierung von Schlüsseln;

x) die Vernichtung von Schlüsseln;

xi) die Protokollierung und Prüfung von Managementtätigkeiten im Zusammenhang mit Schlüsseln;

xii) die Festlegung von Aktivierungs- und Deaktivierungsfristen für Schlüssel, damit die Schlüssel nur für den angegebenen Zeitraum gemäß den Vorschriften der Organisation für das Schlüsselmanagement verwendet werden können.

9.3. Die betreffenden Einrichtungen überprüfen ihr Konzept und ihre Verfahren in geplanten Zeitabständen und aktualisieren sie – soweit angemessen –, wobei sie dem Stand der Technik im Bereich der Kryptografie Rechnung tragen.

10. SICHERHEIT DES PERSONALS (ARTIKEL 21 ABSATZ 2 BUCHSTABE I DER RICHTLINIE (EU) 2022/2555)

10.1. Sicherheit des Personals

10.1.1. Für die Zwecke von Artikel 21 Absatz 2 Buchstabe i der Richtlinie (EU) 2022/2555 stellen die betreffenden Einrichtungen sicher, dass ihre Mitarbeitenden und gegebenenfalls ihre direkten Anbieter und Diensteanbieter ihre Verantwortlichkeiten im Bereich der Sicherheit verstehen und sich zu ihrer Einhaltung verpflichten, soweit dies für die angebotenen Dienste und den Arbeitsplatz angemessen ist und mit dem

Konzept der betreffenden Einrichtungen für die Sicherheit von Netz- und Informationssystemen im Einklang steht.

10.1.2. Die unter Nummer 10.1.1 genannte Anforderung umfasst Folgendes:

a) Mechanismen, mit denen sichergestellt wird, dass alle Mitarbeitenden, direkten Anbieter und Diensteanbieter gegebenenfalls die von den betreffenden Einrichtungen gemäß Nummer 8.1 angewandten Standardverfahren im Bereich der Cyberhygiene verstehen und befolgen;

b) Mechanismen, mit denen sichergestellt wird, dass sich alle Nutzer mit administrativem oder privilegiertem Zugang ihrer Rollen, Verantwortlichkeiten und Weisungsbefugnisse bewusst sind und entsprechend handeln;

c) Mechanismen, mit denen sichergestellt wird, dass die Mitglieder der Leitungsorgane ihre Rollen, Verantwortlichkeiten und Weisungsbefugnisse in Bezug auf die Sicherheit von Netz- und Informationssystemen verstehen und entsprechend handeln;

d) Mechanismen für die Einstellung von Personal, das für die jeweiligen Rollen qualifiziert ist, wie z. B. Überprüfung der Referenzen, Überprüfungsverfahren, Validierung von Zeugnissen oder schriftliche Prüfungen.

10.1.3. Die betreffenden Einrichtungen überprüfen die Zuweisung von Personal zu bestimmten Rollen gemäß Nummer 1.2 sowie ihre Mittel für Personal in geplanten Zeitabständen und mindestens einmal jährlich. Sie aktualisieren die Zuweisung der Rollen erforderlichenfalls.

10.2. Zuverlässigkeitsüberprüfung

10.2.1. Die betreffenden Einrichtungen stellen – soweit durchführbar – sicher, dass Zuverlässigkeitsüberprüfungen ihrer Mitarbeitenden und – soweit anwendbar – der direkten Anbieter und Diensteanbieter gemäß Nummer 5.1.4 durchgeführt werden, wenn dies für deren Rollen, Verantwortlichkeiten und Weisungsbefugnisse erforderlich ist.

10.2.2. Für die Zwecke von Nummer 10.2.1 müssen die betreffenden Einrichtungen

a) Kriterien festlegen, in denen aufgeführt ist, welche Rollen, Verantwortlichkeiten und Weisungsbefugnisse nur von Personen wahrgenommen werden dürfen, deren Zuverlässigkeit überprüft wurde;

b) sicherstellen, dass bei diesen Personen Überprüfungen gemäß Nummer 10.2.1 durchgeführt werden, bevor sie mit der Wahrnehmung dieser Rollen, Verantwortlichkeiten und Weisungsbefugnisse beginnen, wobei die geltenden Gesetze, Vorschriften und ethischen Normen im Verhältnis zu den geschäftlichen Anforderungen, der Klassifizierung der Anlagen und Werte gemäß Nummer 12.1 und den Netz- und Informationssystemen, auf die zugegriffen werden soll, sowie den wahrgenommenen Risiken zu berücksichtigen sind.

10.2.3. Die betreffenden Einrichtungen überprüfen ihr Konzept in geplanten Zeitabständen und aktualisieren es – soweit angemessen.

10.3. Verfahren zur Beendigung oder Änderung des Beschäftigungsverhältnisses

10.3.1. Die betreffenden Einrichtungen stellen sicher, dass die Verantwortlichkeiten und Pflichten in Bezug auf die Sicherheit von Netz- und Informationssystemen, die auch nach der Beendigung oder der Änderung des Beschäftigungsverhältnisses ihrer Mitarbeitenden gültig bleiben, vertraglich festgelegt und durchgesetzt werden.

10.3.2. Für die Zwecke von Nummer 10.3.1 nehmen die betreffenden Einrichtungen in die Arbeits- und Beschäftigungsbedingungen, den Vertrag oder die Vereinbarung der betreffenden Person die Verantwortlichkeiten und Pflichten auf, die auch nach Beendigung des Beschäftigungsverhältnisses oder des Vertrags gültig bleiben, wie z. B. Vertraulichkeitsklauseln.

10.4. Disziplinarverfahren

10.4.1. Die betreffenden Einrichtungen führen ein Disziplinarverfahren für den Umgang mit Verstößen gegen die Konzepte für die Sicherheit von Netz- und Informationssystemen ein, machen es bekannt und erhalten es aufrecht. In dem Verfahren sind die einschlägigen rechtlichen, gesetzlichen, vertraglichen und geschäftlichen Anforderungen zu berücksichtigen.

10.4.2. Die betreffenden Einrichtungen überprüfen das Disziplinarverfahren in geplanten Zeitabständen sowie – soweit angemessen – bei rechtlichen Änderungen oder bei wesentlichen Änderungen der Betriebsabläufe oder der Risiken und aktualisieren es gegebenenfalls.

11. ZUGRIFFSKONTROLLE (ARTIKEL 21 ABSATZ 2 BUCHSTABEN I UND J DER RICHTLINIE (EU) 2022/2555)

11.1. Konzept für die Zugriffskontrolle

11.1.1. Für die Zwecke von Artikel 21 Absatz 2 Buchstabe i der Richtlinie (EU) 2022/2555 legen die betreffenden Einrichtungen auf der Grundlage von geschäftlichen Anforderungen sowie Anforderungen an die Sicherheit von Netz- und Informationssystemen Konzepte für die logische und physische Kontrolle des Zugangs zu ihren Netz- und Informationssystemen fest, dokumentieren sie und setzen sie um.

11.1.2. Die in Nummer 11.1.1. genannten Konzepte müssen

a) für den Zugang von Personen, einschließlich Personal, Besuchern und externen Einrichtungen wie Anbietern und Diensteanbietern, gelten;

b) für den Zugang von Netz- und Informationssystemen gelten;

c) sicherstellen, dass der Zugang nur Nutzern gewährt wird, die angemessen authentifiziert wurden.

11.1.3. Die betreffenden Einrichtungen überprüfen die Konzepte in geplanten Zeitabständen sowie bei erheblichen Sicherheitsvorfällen oder wesentlichen Änderungen der Betriebsabläufe oder der Risiken und aktualisieren sie – soweit angemessen.

11.2. Management von Zugangs- und Zugriffsrechten

11.2.1. Die betreffenden Einrichtungen gewähren, ändern, löschen und dokumentieren Zugangs- und Zugriffsrechte für die Netz- und Informationssysteme im Einklang mit dem in Nummer 11.1 genannten Konzept für die Zugriffskontrolle.

11.2.2. Die betreffenden Einrichtungen

a) gewähren und entziehen Zugangs- und Zugriffsrechte auf der Grundlage des Grundsatzes „Kenntnis nur, wenn nötig“ (*Need-to-know*), des Grundsatzes der Nutzungsnotwendigkeit (*Need-to-use*) und des Grundsatzes der Aufgabentrennung;

b) stellen sicher, dass die Zugangs- und Zugriffsrechte bei Beendigung oder Änderung des Beschäftigungsverhältnisses entsprechend geändert werden;

c) stellen sicher, dass der Zugang zu Netz- und Informationssystemen von den einschlägigen Personen genehmigt wird;

d) stellen sicher, dass die Zugangs- und Zugriffsrechte dem Zugang bzw. Zugriff Dritter, wie Besucher, Anbieter und Diensteanbieter, angemessen Rechnung tragen, insbesondere durch Beschränkung der Zugangs- und Zugriffsrechte in Bezug auf Umfang und Dauer;

e) führen ein Register der gewährten Zugangs- und Zugriffsrechte;

f) protokollieren das Management von Zugangs- und Zugriffsrechten.

11.2.3. Die betreffenden Einrichtungen überprüfen die Zugangs- und Zugriffsrechte in geplanten Zeitabständen und ändern sie bei organisatorischen Änderungen. Die betreffenden Einrichtungen dokumentieren die Ergebnisse der Überprüfung, einschließlich der erforderlichen Änderungen der Zugangs- und Zugriffsrechte.

11.3. Privilegierte Konten und Systemverwaltungskonten

11.3.1. Die betreffenden Einrichtungen halten sich an Grundsätze für das Management von privilegierten Konten und Systemverwaltungskonten als Teil des in Nummer 11.1 genannten Konzepts für die Zugriffskontrolle.

11.3.2. Mit den in Nummer 11.3.1 genannten Konzepten

a) müssen starke Verfahren zur Identifizierung, Authentifizierung (z. B. Multifaktor-Authentifizierung) und Genehmigung für privilegierte Konten und Systemverwaltungskonten eingerichtet werden;

b) müssen spezielle Konten eingerichtet werden, die ausschließlich für Systemverwaltungsvorgänge, wie Installation, Konfiguration, Verwaltung oder Wartung, zu verwenden sind;

c) müssen die Systemverwaltungsrechte so weit wie möglich individuell zugeschnitten und einschränkt werden;

d) muss festgelegt werden, dass Systemverwaltungskonten ausschließlich zur Verbindung mit Systemverwaltungssystemen verwendet werden.

11.3.3. Die betreffenden Einrichtungen überprüfen die Zugangs- und Zugriffsrechte für privilegierte Konten und Systemverwaltungskonten in geplanten Zeitabständen, ändern diese bei organisatorischen Änderungen und dokumentieren die Ergebnisse der Überprüfung, einschließlich der erforderlichen Änderungen der Zugriffsrechte.

11.4. Systemverwaltungssysteme

11.4.1. Die betreffenden Einrichtungen beschränken und kontrollieren die Nutzung von Systemverwaltungskonten im Einklang mit dem in Nummer 11.1 genannten Konzept für die Zugriffskontrolle.

11.4.2. Für diese Zwecke müssen die betreffenden Einrichtungen

a) Systemverwaltungssysteme ausschließlich für die Zwecke der Systemverwaltung und nicht für andere Vorgänge verwenden;

b) solche Systeme logisch von Anwendungssoftware, die nicht für Systemverwaltungszwecke verwendet wird, trennen;

c) den Zugang zu Systemverwaltungssystemen durch Authentifizierung und Verschlüsselung schützen.

11.5. Identifizierung

11.5.1. Die betreffenden Einrichtungen verwalten den gesamten Lebenszyklus der Identitäten (Kennungen) der Netz- und Informationssysteme und ihrer Nutzer.

11.5.2. Für diese Zwecke müssen die betreffenden Einrichtungen

a) eindeutige Kennungen für die Netz- und Informationssysteme und deren Nutzer einrichten;

b) die Nutzerkennung mit einer einzigen Person verknüpfen;

c) die Überwachung der Kennungen der Netz- und Informationssysteme sicherstellen;

d) das Management von Identitäten (Kennungen) protokollieren.

11.5.3. Die betreffenden Einrichtungen genehmigen Kennungen, die mehreren Personen zugewiesen wurden, wie z. B. gemeinsame Kennungen, nur dann, wenn sie aus geschäftlichen oder operativen Gründen erforderlich sind, einem ausdrücklichen Genehmigungsverfahren unterliegen und dokumentiert werden. Die betreffenden Einrichtungen berücksichtigen Kennungen, die mehreren Personen im Rahmen des in Nummer 2.1 genannten Rahmens für das Risikomanagement im Bereich der Cybersicherheit zugewiesen wurden.

11.5.4. Die betreffenden Einrichtungen überprüfen regelmäßig die Kennungen der Netz- und Informationssysteme und ihrer Nutzer und deaktivieren sie unverzüglich, falls sie nicht mehr benötigt werden.

11.6. Authentifizierung

11.6.1. Die betreffenden Einrichtungen verwenden sichere Authentifizierungsverfahren und -techniken auf der Grundlage von Zugangsbeschränkungen und des Konzepts für die Zugriffskontrolle.

11.6.2. Für diese Zwecke müssen die betreffenden Einrichtungen

a) sicherstellen, dass die Stärke der Authentifizierung für die Klassifizierung der Anlage bzw. des Werts, auf die zugegriffen werden soll, angemessen ist;

b) die Verwaltung geheimer Authentifizierungsinformationen und deren Zuweisung an die Nutzer durch ein Verfahren kontrollieren, das die Vertraulichkeit der Informationen gewährleistet, einschließlich Anweisungen an das Personal in Bezug auf den angemessenen Umgang mit Authentifizierungsinformationen;

c) die Änderung von Authentifizierungsdaten zu Beginn, sodann in vorab festgelegten Zeitabständen und immer dann verlangen, wenn der Verdacht besteht, dass die Authentifizierungsdaten beeinträchtigt wurden;

d) das Zurücksetzen der Authentifizierungsdaten und die Sperrung von Nutzern nach einer vorab festgelegten Anzahl erfolgloser Anmeldeversuche verlangen;

e) inaktive Sitzungen nach einem im Voraus festgelegten Zeitraum der Inaktivität beenden und

f) für den Zugriff auf privilegierte Konten oder Verwaltungskonten gesonderte Authentifizierungsdaten verlangen.

11.6.3. Die betreffenden Einrichtungen verwenden – soweit durchführbar – modernste Authentifizierungsmethoden, die dem damit verbundenen bewerteten Risiko und der Klassifizierung der Anlage bzw. des Werts, auf die zugegriffen werden soll, entsprechen, sowie eindeutige Authentifizierungsinformationen.

11.6.4. Die betreffenden Einrichtungen überprüfen die Authentifizierungsverfahren und -techniken in geplanten Zeitabständen.

11.7. Multifaktor-Authentifizierung

11.7.1. Die betreffenden Einrichtungen stellen sicher, dass die Nutzer – soweit angemessen – durch mehrere Authentifizierungsfaktoren oder kontinuierliche Authentifizierungsmechanismen für den Zugang zu den Netz- und Informationssystemen der betreffenden Einrichtungen im Einklang mit der Klassifizierung der Anlage bzw. des Werts, auf die zugegriffen werden soll, authentifiziert werden.

11.7.2. Die betreffenden Einrichtungen stellen sicher, dass die Stärke der Authentifizierung für die Klassifizierung der Anlage bzw. des Werts, auf die zugegriffen werden soll, angemessen ist.

12. ANLAGEN- UND WERTEMANAGEMENT (ARTIKEL 21 ABSATZ 2 BUCHSTABE I DER RICHTLINIE (EU) 2022/2555)

12.1. Anlagen- und Werteklassifizierung

12.1.1. Für die Zwecke von Artikel 21 Absatz 2 Buchstabe i der Richtlinie (EU) 2022/2555 legen die betreffenden Einrichtungen für alle Anlagen und Werte (einschließlich Informationen), die in den Anwendungsbereich ihrer Netz- und Informationssysteme fallen, Klassifizierungsstufen für das erforderliche Schutzniveau fest.

12.1.2. Für die Zwecke von Nummer 12.1.1 müssen die betreffenden Einrichtungen

a) ein System von Klassifizierungsstufen für Anlagen und Werte festlegen;

b) allen Anlagen und Werte eine Klassifizierungsstufe zuordnen, die auf Vertraulichkeits-, Integritäts-, Authentizitäts- und Verfügbarkeitsanforderungen beruht, um den entsprechend ihrer Sensibilität, ihrer Kritikalität, ihres Risikos und ihres Geschäftswerts erforderlichen Schutz anzugeben;

c) die Verfügbarkeitsanforderungen in Bezug auf die Anlagen und Werte an die in ihrem Notfallplan für die Aufrechterhaltung und Wiederherstellung des Betriebs festgelegten Ziele für die Bereitstellung und Wiederherstellung anpassen.

12.1.3. Die betreffenden Einrichtungen überprüfen regelmäßig die Klassifizierungsstufen der Anlagen und Werte und aktualisieren sie – soweit angemessen.

12.2. Behandlung von Anlagen und Werten

12.2.1. Die betreffenden Einrichtungen legen ein Konzept für die ordnungsgemäße Behandlung von Anlagen und Werten (einschließlich Informationen) im Einklang mit ihrem Konzept für die Sicherheit ihrer Netz- und Informationssysteme fest, setzen es um und wenden es an und teilen dieses Konzept für die ordnungsgemäße Behandlung von Anlagen und Werten allen Personen mit, die Anlagen und Werte nutzen oder damit umgehen.

12.2.2. Das Konzept muss

a) den gesamten Lebenszyklus der Anlagen und Werte abdecken, einschließlich Erwerb, Verwendung, Speicherung, Transport und Entsorgung;

b) Vorschriften für die sichere Verwendung, die sichere Speicherung, den sicheren Transport und die unwiederbringliche Löschung und Vernichtung der Anlagen und Werte;

c) vorsehen, dass die Übertragung unter Berücksichtigung der Art der zu übertragenden Anlage bzw. des zu übertragenden Werts sicher erfolgt.

12.2.3. Die betreffenden Einrichtungen überprüfen das Konzept in geplanten Zeitabständen sowie bei erheblichen Sicherheitsvorfällen oder wesentlichen Änderungen der Betriebsabläufe oder der Risiken und aktualisieren dieses – soweit angemessen.

12.3. Konzept für Wechseldatenträger

12.3.1. Die betreffenden Einrichtungen legen ein Konzept für das Management von Wechseldatenträgern fest, setzen es um und wenden es an und teilen es ihren Mitarbeitenden und Dritten mit, die Wechseldatenträger in den Räumlichkeiten der betreffenden Einrichtungen oder an anderen Orten, an denen die

Wechseldatenträger mit den Netz- und Informationssystemen der betreffenden Einrichtungen verbunden sind, benutzen.

12.3.2. Das Konzept muss

a) eine technische Sperrung von Verbindungen mit Wechseldatenträgern vorsehen, es sei denn, es liegen organisatorische Gründe für deren Nutzung vor;

b) vorsehen, dass die Selbstausführung von Dateien von solchen Datenträgern verhindert wird und die Datenträger auf Schadcodes gescannt werden, bevor sie in den Systemen der betreffenden Einrichtungen verwendet werden können;

c) Maßnahmen zur Kontrolle und zum Schutz von tragbaren Speichergeräten, die gespeicherte und gerade übermittelte Daten enthalten, vorsehen;

d) gegebenenfalls Maßnahmen für den Einsatz kryptografischer Verfahren zum Schutz von Daten auf Wechseldatenträgern vorsehen.

12.3.3. Die betreffenden Einrichtungen überprüfen das Konzept in geplanten Zeitabständen sowie bei erheblichen Sicherheitsvorfällen oder wesentlichen Änderungen der Betriebsabläufe oder der Risiken und aktualisieren dieses – soweit angemessen.

12.4. Anlagen- und Werteinventar

12.4.1. Die betreffenden Einrichtungen erstellen und pflegen ein vollständiges, genaues, aktuelles und kohärentes Inventar ihrer Anlagen und Werte. Sie erfassen Änderungen der Einträge im Anlagen- und Werteinventar auf nachvollziehbare Weise.

12.4.2. Die Granularität des Anlagen- und Werteinventars liegt auf einem Niveau, dass den Bedürfnissen der betreffenden Einrichtungen entspricht. Das Inventar umfasst Folgendes:

a) die Liste der Betriebsabläufe und Dienste und ihre Beschreibung,

b) die Liste der Netz- und Informationssysteme und anderer zugehöriger Anlagen und Werte, die die Abläufe und die Dienste der betreffenden Einrichtungen unterstützen.

12.4.3. Die betreffenden Einrichtungen überprüfen und aktualisieren regelmäßig das Inventar und ihre Anlagen und Werte und dokumentieren den Verlauf der Änderungen.

12.5. Abgabe, Rückgabe oder Löschung von Anlagen und Werten bei Beendigung des Beschäftigungsverhältnisses

Die betreffenden Einrichtungen legen Verfahren fest, setzen sie um und wenden sie an, um sicherzustellen, dass ihre Anlagen und Werte, die sich in der Verwahrung des Personals befinden, bei Beendigung des Beschäftigungsverhältnisses abgegeben, zurückgegeben oder gelöscht werden, und dokumentieren die Abgabe, Rückgabe und Löschung dieser Anlagen und Werte. Ist die Abgabe, Rückgabe oder Löschung von Anlagen und Werten nicht möglich, so stellen die betreffenden Einrichtungen sicher, dass die Anlagen und Werte gemäß Nummer 12.2.2 nicht mehr auf die Netz- und Informationssysteme der betreffenden Einrichtungen zugreifen können.

13. SICHERHEIT DES UMFELDS UND PHYSISCHE SICHERHEIT (ARTIKEL 21 ABSATZ 2 BUCHSTABEN C, E UND I DER RICHTLINIE (EU) 2022/2555)

13.1. Unterstützende Versorgungsleistungen

13.1.1. Für die Zwecke von Artikel 21 Absatz 2 Buchstabe c der Richtlinie (EU) 2022/2555 verhindern die betreffenden Einrichtungen Verluste, Schäden oder Beeinträchtigungen von Netz- und Informationssystemen oder Unterbrechungen ihres Betriebs aufgrund des Ausfalls und der Störung unterstützender Versorgungsleistungen.

13.1.2. Für diese Zwecke müssen die betreffenden Einrichtungen – soweit angemessen –

a) ihre Betriebsstätten vor Stromausfällen und anderen Störungen schützen, die durch Ausfälle bei unterstützenden Versorgungsunternehmen z. B. für Strom, Telekommunikation, Wasser, Gas, Abwasser, Lüftung und Klimatisierung verursacht werden;

b) die Nutzung von Redundanzsystemen für Versorgungsleistungen in Erwägung ziehen;

c) Versorgungsleistungen, die Strom und Telekommunikationsdienste für den Transport von Daten oder für den Betrieb von Netz- und Informationssystemen bereitstellen, vor Abhörung und Beschädigung schützen;

d) die unter Buchstabe c genannten Versorgungsleistungen überwachen und dem zuständigen internen oder externen Personal die Ereignisse melden, die außerhalb der in Nummer 13.2.2 Buchstabe b genannten Mindest- und Höchstkontrollwerteliegen und Auswirkungen auf die Versorgungsleistungen haben;

e) Verträge über die Notversorgung mit entsprechenden Leistungen abschließen, z. B. für Brennstoff für die Notstromversorgung;

f) die kontinuierliche Wirksamkeit, Überwachung, Wartung und Erprobung der Netz- und Informationssysteme, die für den Betrieb des angebotenen Dienstes erforderlich sind, gewährleisten, insbesondere Strom, Temperatur- und Feuchtigkeitsregelung, Telekommunikation und Internetverbindung.

13.1.3. Die betreffenden Einrichtungen testen die Schutzmaßnahmen in geplanten Zeitabständen oder nach erheblichen Sicherheitsvorfällen oder wesentlichen Änderungen der Betriebsabläufe oder der Risiken und aktualisieren sie – soweit angemessen.

13.2. Schutz vor physischen Bedrohungen und Bedrohungen des Umfelds

13.2.1. Für die Zwecke von Artikel 21 Absatz 2 Buchstabe e der Richtlinie (EU) 2022/2555 verhindern oder verringern die betreffenden Einrichtungen die Folgen von Ereignissen, die von physischen Bedrohungen und Bedrohungen des Umfelds wie Naturkatastrophen und anderen vorsätzlichen oder unbeabsichtigten Bedrohungen ausgehen, auf der Grundlage der Ergebnisse der gemäß Nummer 2.1 durchgeführten Risikobewertung.

13.2.2. Für diese Zwecke müssen die betreffenden Einrichtungen – soweit angemessen –

a) Schutzmaßnahmen gegen physische Bedrohungen und Bedrohungen des Umfelds konzipieren und umsetzen;

b) Mindest- und Höchstkontrollwerte für physische Bedrohungen und Bedrohungen des Umfelds bestimmen;

c) die Umgebungsparameter überwachen und dem zuständigen internen oder externen Personal Ereignisse melden, die außerhalb der in Buchstabe b genannten Mindest- und Höchstkontrollwerte liegen.

13.2.3. Die betreffenden Einrichtungen testen die Schutzmaßnahmen gegen physische Bedrohungen und Bedrohungen des Umfelds in geplanten Zeitabständen oder nach erheblichen Sicherheitsvorfällen oder wesentlichen Änderungen der Betriebsabläufe oder der Risiken und aktualisieren sie – soweit angemessen.

13.3. Perimeter und physische Zutrittskontrolle

13.3.1. Für die Zwecke von Artikel 21 Absatz 2 Buchstabe i der Richtlinie (EU) 2022/2555 verhindern und überwachen die betreffenden Einrichtungen unbefugten physischen Zutritt zu, Beschädigungen von und Eingriffe in ihre Netz- und Informationssysteme.

13.3.2. Für diese Zwecke müssen die betreffenden Einrichtungen

a) auf der Grundlage der gemäß Nummer 2.1 durchgeführten Risikobewertung Sicherheitsperimeter festlegen und nutzen, um Bereiche zu schützen, in denen sich Netz- und Informationssysteme und andere zugehörige Anlagen befinden;

b) die unter Buchstabe a genannten Bereiche durch geeignete Zutrittskontrollen und Zugangspunkte schützen;

c) Maßnahmen für die physische Sicherheit von Büros, Räumen und Betriebsstätten konzipieren und umsetzen;

d) ihrer Räumlichkeiten kontinuierlich in Bezug auf unbefugten physischen Zutritt überwachen.

13.3.3. Die betreffenden Einrichtungen testen die Maßnahmen zur physischen Zutrittskontrolle in geplanten Zeitabständen oder nach erheblichen Sicherheitsvorfällen oder wesentlichen Änderungen der Betriebsabläufe oder der Risiken und aktualisieren sie – soweit angemessen.