EUROPÄISCHE
KOMMISSION

Brüssel, XXX [...](2024)
XXX Entwurf

DURCHFÜHRUNGSVERORDNUNG (EU) DER KOMMISSION .../...

von XXX

zur Festlegung von Vorschriften für die Anwendung der Richtlinie (EU) 2022/2555 hinsichtlich der technischen und methodischen Anforderungen an Maßnahmen des Cybersicherheitsrisikomanagements und zur näheren Bestimmung der Fälle, in denen ein Vorfall in Bezug auf Anbieter von DNS-Diensten, TLD-Namensregistern, Anbietern von Cloud-Computing-Diensten, Anbietern von Rechenzentrumsdiensten, Anbietern von Content-Delivery-Netzen, Anbietern von verwalteten Diensten, Anbietern von verwalteten Sicherheitsdiensten, Anbietern von Online-Marktplätzen, Online-Suchmaschinen und Plattformen für soziale Netzwerkdienste sowie Anbietern von Vertrauensdiensten als erheblich angesehen wird

(Text mit Bedeutung für den EWR)

DURCHFÜHRUNGSVERORDNUNG (EU) DER KOMMISSION .../...

von XXX

zur Festlegung von Vorschriften für die Anwendung der Richtlinie (EU) 2022/2555 hinsichtlich der technischen und methodischen Anforderungen an Maßnahmen des Cybersicherheitsrisikomanagements und zur näheren Bestimmung der Fälle, in denen ein Vorfall in Bezug auf Anbieter von DNS-Diensten, TLD-Namensregistern, Anbietern von Cloud-Computing-Diensten, Anbietern von Rechenzentrumsdiensten, Anbietern von Content-Delivery-Netzen, Anbietern von verwalteten Diensten, Anbietern von verwalteten Sicherheitsdiensten, Anbietern von Online-Marktplätzen, Online-Suchmaschinen und Plattformen für soziale Netzwerkdienste sowie Anbietern von Vertrauensdiensten als erheblich angesehen wird

(Text mit Bedeutung für den EWR)

DIE EUROPÄISCHE KOMMISSION,

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Maß an Cybersicherheit 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)[1] , insbesondere auf Artikel 21 Absatz 5 Unterabsatz 1 und Artikel 23 Absatz 11 Unterabsatz 2,

in Erwägung nachstehender Gründe:

(1) In Bezug auf Anbieter von DNS-Diensten, TLD-Namensregistern, Anbietern von Cloud-Computing-Diensten, Anbietern von Rechenzentrumsdiensten, Anbietern von Content-Delivery-Netzen, Anbietern von verwalteten Diensten, Anbietern von verwalteten Sicherheitsdiensten, Anbietern von Online-Marktplätzen, Online-Suchmaschinen und Plattformen für soziale Netzwerkdienste, und Anbieter von Vertrauensdiensten im Sinne von Artikel 3 der Richtlinie (EU) 2022/2555 ("die betroffenen Einrichtungen"), sollen mit dieser Verordnung die technischen und methodischen Anforderungen an die in Artikel 21 Absatz 2 der Richtlinie (EU) 2022/2555 genannten Maßnahmen festgelegt und die Fälle näher bestimmt werden, in denen ein Vorfall als erheblich im Sinne von Artikel 23 Absatz 3 der Richtlinie (EU) 2022/2555 anzusehen ist.

(2) In Anbetracht des grenzüberschreitenden Charakters ihrer Tätigkeiten und zur Gewährleistung eines kohärenten Rahmens für Vertrauensdiensteanbieter sollte diese Verordnung in Bezug auf Vertrauensdiensteanbieter zusätzlich zur Festlegung der technischen und methodischen Anforderungen an die Maßnahmen des Cybersicherheitsrisikomanagements die Fälle näher bestimmen, in denen ein Vorfall als erheblich anzusehen ist.

(3) Gemäß Artikel 21 Absatz 5 Unterabsatz 3 der Richtlinie (EU) 2022/2555 stützen sich die technischen und methodischen Anforderungen an die im Anhang zu dieser Verordnung aufgeführten Maßnahmen des Cybersicherheitsrisikomanagements auf europäische und internationale Normen und technische Spezifikationen, die für die Sicherheit von Netz- und Informationssystemen relevant sind.

[1] ABl. L 333 vom 27.12.2022, S. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj.

(4) Bei der Anwendung der im Anhang dieser Verordnung aufgeführten technischen und methodischen Anforderungen an Maßnahmen des Cybersicherheitsrisikomanagements sollte im Einklang mit dem Grundsatz der Verhältnismäßigkeit die unterschiedliche Risikoexposition der betreffenden Einrichtungen gebührend berücksichtigt werden, z. B. die Kritikalität der betreffenden Einrichtung, die Risiken, denen sie ausgesetzt ist, die Größe und Struktur der betreffenden Einrichtung sowie die Wahrscheinlichkeit des Auftretens von Vorfällen und deren Schwere, einschließlich ihrer gesellschaftlichen und wirtschaftlichen Auswirkungen.

(5) Im Einklang mit dem Grundsatz der Verhältnismäßigkeit sollten einschlägige Stellen, die aufgrund ihrer Größe nicht in der Lage sind, die technischen und methodischen Anforderungen der Maßnahmen für das Cybersicherheitsrisikomanagement zu erfüllen, in der Lage sein, andere Ausgleichsmaßnahmen zu ergreifen, die geeignet sind, den Zweck dieser Anforderungen zu erfüllen. Beispielsweise könnte es für Kleinstunternehmen schwierig sein, kollidierende Aufgaben und Verantwortungsbereiche voneinander zu trennen. Solche Unternehmen sollten in der Lage sein, Ausgleichsmaßnahmen wie eine gezielte Aufsicht durch die Unternehmensleitung oder eine verstärkte Überwachung und Protokollierung in Betracht zu ziehen.

(6) Die zuständigen Behörden können beschließen, Leitlinien zur Verfügung zu stellen, um die betreffenden Einrichtungen bei der Ermittlung, Analyse und Bewertung von Risiken zu unterstützen, damit die technischen und methodischen Anforderungen an die Schaffung und Aufrechterhaltung eines angemessenen Rahmens für das Risikomanagement erfüllt werden können. Solche Leitlinien können insbesondere nationale und sektorale Risikobewertungen sowie Risikobewertungen speziell für eine bestimmte Art von Unternehmen umfassen. Darüber hinaus können die zuständigen Behörden die Unternehmen dabei unterstützen, geeignete Lösungen für die Behandlung der in diesen Risikobewertungen ermittelten Risiken zu finden und umzusetzen. Die Verpflichtung der betreffenden Stellen, die Risiken für die Sicherheit von Netz- und Informationssystemen zu ermitteln und zu dokumentieren, sowie die Fähigkeit der betreffenden Stellen, die technischen und methodischen Anforderungen der im Anhang dieser Verordnung aufgeführten Maßnahmen für das Risikomanagement im Bereich der Cybersicherheit entsprechend ihren Bedürfnissen und Ressourcen umzusetzen, sollten von solchen Leitlinien unberührt bleiben.

(7) Netzsicherheitsmaßnahmen in Bezug auf: (i) der Übergang zu Kommunikationsprotokollen der neuesten Generation auf der Netzebene, (ii) die Einführung international vereinbarter und interoperabler moderner E-Mail-Kommunikationsstandards und (iii) die Anwendung bewährter Verfahren für die Sicherheit des Internet-Routings und die Routing-Hygiene stellen besondere Herausforderungen hinsichtlich der Ermittlung der besten verfügbaren Standards und Einführungstechniken dar. Um so bald wie möglich ein hohes gemeinsames Niveau der Cybersicherheit in allen Netzen zu erreichen, sollte die Kommission mit Unterstützung der Agentur der Europäischen Union für Cybersicherheit (ENISA) und in Zusammenarbeit mit den zuständigen Behörden, der Industrie - einschließlich der Telekommunikationsbranche - und anderen Interessengruppen die Entwicklung eines Multi-Stakeholder-Forums unterstützen, das die Aufgabe hat, diese besten verfügbaren Normen und Einführungstechniken zu ermitteln. Diese Multi-Stakeholder-Leitlinien sollten die Fähigkeit der betreffenden Stellen, die technischen und methodischen Anforderungen der im Anhang dieser Verordnung aufgeführten Maßnahmen für das Management von Cybersicherheitsrisiken umzusetzen, nicht beeinträchtigen.

(8) Gemäß Artikel 21 Absatz 2 Buchstabe a der Richtlinie (EU) 2022/2555 sollten

wesentliche und wichtige Einrichtungen über Strategien für die Sicherheit von Informationssystemen verfügen. Zu diesem Zweck sollten die betreffenden Stellen ein Konzept für die Sicherheit von Netz- und Informationssystemen sowie themenspezifische Konzepte, wie z. B. Konzepte für die Zugangskontrolle, erstellen. Die Strategie für die Sicherheit von Netz- und Informationssystemen sollte das oberste Dokument sein, in dem das Gesamtkonzept der betreffenden Stellen für die Sicherheit ihrer Netz- und Informationssysteme dargelegt ist, und sollte von der Kommission genehmigt werden.

die Leitungsorgane der betreffenden Einrichtungen. Die themenspezifischen Strategien sollten von einer geeigneten Managementebene genehmigt werden. In der Strategie sollten Indikatoren und Maßnahmen zur Überwachung ihrer Umsetzung und des aktuellen Stands der Netz- und Informationssicherheit der betreffenden Stellen festgelegt werden, um insbesondere die Überwachung der Umsetzung der Maßnahmen zum Management von Cybersicherheitsrisiken durch die Leitungsorgane zu erleichtern.

(9) Für die Zwecke der im Anhang zu dieser Verordnung festgelegten technischen und methodischen Anforderungen sollte der Begriff "Nutzer" alle juristischen und natürlichen Personen umfassen, die Zugang zum Netz und zu den Informationssystemen des Unternehmens haben.

(10) Um anomales Verhalten und potenzielle Vorfälle zu erkennen, sollten die betreffenden Stellen ihre Netz- und Informationssysteme überwachen und Maßnahmen zur Bewertung potenzieller Vorfälle ergreifen. Diese Maßnahmen sollten in der Lage sein, netzgestützte Angriffe auf der Grundlage anomaler Muster des ein- oder ausgehenden Datenverkehrs und verteilte Denial-of-Service-Angriffe rechtzeitig zu erkennen.

(11) Wenn die zuständigen Stellen eine Analyse der Auswirkungen auf den Geschäftsbetrieb durchführen, wird ihnen empfohlen, eine umfassende Analyse vorzunehmen, in der gegebenenfalls die maximal tolerierbare Ausfallzeit, die Ziele für die Wiederherstellungszeit, die Ziele für den Wiederherstellungspunkt und die Ziele für die Bereitstellung der Dienste festgelegt werden.

(12) Um die Risiken zu mindern, die sich aus der Lieferkette eines relevanten Unternehmens und seinen Beziehungen zu seinen Lieferanten ergeben, sollten die relevanten Unternehmen eine Sicherheitspolitik für die Lieferkette festlegen, die ihre Beziehungen zu ihren direkten Lieferanten und Dienstleistern regelt. Diese Unternehmen sollten in den Verträgen mit ihren direkten Zulieferern oder Dienstleistern angemessene Sicherheitsklauseln festlegen, indem sie beispielsweise gegebenenfalls Maßnahmen für das Risikomanagement im Bereich der Cybersicherheit gemäß Artikel 21 Absatz 2 der Richtlinie (EU) 2022/2555 oder andere ähnliche rechtliche Anforderungen verlangen.

(13) Die betreffenden Stellen sollten regelmäßig Sicherheitstests auf der Grundlage einer speziellen Strategie und von Verfahren durchführen, um zu überprüfen, ob die Maßnahmen zum Management von Cybersicherheitsrisiken umgesetzt sind und ordnungsgemäß funktionieren. Sicherheitstests können für bestimmte Netz- und Informationssysteme oder für die betreffende Stelle als Ganzes durchgeführt werden und können automatisierte oder manuelle Tests, Penetrationstests, Schwachstellenscans, statische und dynamische Anwendungstests, Konfigurationstests oder Sicherheitsaudits umfassen. Die betreffenden Stellen können Sicherheitstests für ihre Netz- und Informationssysteme bei der Einrichtung, nach Infrastruktur- oder Anwendungs-Upgrades oder -Änderungen, die sie als wesentlich erachten, oder nach der Wartung durchführen. Die Ergebnisse der Sicherheitstests sollten in die Strategien und Verfahren der betreffenden Stellen zur Bewertung der Wirksamkeit ihrer Sicherheitsmaßnahmen sowie in unabhängige Überprüfungen ihrer Netz- und Informationssicherheitspolitik einfließen.

(14) Um erhebliche Störungen und Schäden zu vermeiden, die durch die Ausnutzung ungepatchter Schwachstellen in Netz- und Informationssystemen verursacht werden, sollten die betreffenden Stellen geeignete Verfahren für die Verwaltung von Sicherheits-Patches festlegen und anwenden, die mit den Verfahren der betreffenden Stellen für die Verwaltung von Änderungen abgestimmt sind. Die betreffenden Stellen

sollten Maßnahmen ergreifen, die in einem angemessenen Verhältnis zu ihren Ressourcen stehen, um sicherzustellen, dass durch die Sicherheitspatches keine zusätzlichen Schwachstellen oder Instabilitäten entstehen. Im Falle einer geplanten Nichtverfügbarkeit des Dienstes aufgrund der Anwendung von Sicherheitspatches werden die betreffenden Stellen aufgefordert, die Kunden im Voraus ordnungsgemäß zu informieren.

(15) Die betreffenden Stellen sollten die Risiken, die sich aus dem Erwerb von IKT-Produkten oder IKT-Dienstleistungen von Lieferanten oder Dienstleistern ergeben, steuern und sich

Zusicherung, dass die IKT-Produkte oder IKT-Dienstleistungen bestimmte Cybersicherheitsschutzniveaus erreichen, beispielsweise durch europäische Cybersicherheitszertifikate und EU-Konformitätserklärungen für IKT-Produkte oder IKT-Dienstleistungen, die im Rahmen eines europäischen Cybersicherheitszertifizierungssystems gemäß Artikel 49 der Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates[2] ausgestellt wurden. Wenn die betreffenden Stellen Sicherheitsanforderungen für die zu erwerbenden IKT-Produkte festlegen, sollten sie die grundlegenden Cybersicherheitsanforderungen berücksichtigen, die im [Gesetz über die Widerstandsfähigkeit gegenüber Computern] festgelegt sind.

(16) Um sich vor Cyber-Bedrohungen zu schützen und die Verhinderung und Eindämmung von Datenschutzverletzungen zu unterstützen, sollten die betreffenden Stellen Lösungen für die Netzsicherheit einführen. Typische Lösungen für die Netzsicherheit sind der Einsatz von Firewalls zum Schutz der internen Netze der betreffenden Stellen, die Beschränkung von Verbindungen und des Zugangs zu Diensten auf das absolut Notwendige oder die Nutzung virtueller privater Netze für den Fernzugriff und die Zulassung von Verbindungen zu Diensteanbietern nur nach einer Genehmigungsanfrage und für einen bestimmten Zeitraum, z. B. für die Dauer eines Wartungsvorgangs.

(17) Um die Netze der betreffenden Stellen und ihre Informationssysteme vor bösartiger und nicht autorisierter Software zu schützen, sollten diese Stellen Software zur Erkennung und Reparatur von Schadsoftware einsetzen. Sind die betreffenden Stellen auf der Grundlage der Risikobewertung der Auffassung, dass der Einsatz von Software zur Erkennung und Reparatur von Schadsoftware nicht angemessen ist oder dass die Software zur Erkennung und Reparatur von Schadsoftware nicht jederzeit verfügbar ist, sollten diese Stellen zusätzliche Maßnahmen und Kontrollen in Erwägung ziehen, die die Verwendung nicht autorisierter Software und die Nutzung bekannter oder mutmaßlich bösartiger Websites verhindern oder erkennen. Die betreffenden Stellen sollten auch Maßnahmen zur Minimierung der Angriffsfläche, zur Verringerung von Schwachstellen, die von Schadsoftware ausgenutzt werden können, zur Kontrolle der Ausführung von Anwendungen auf Benutzer-Workstations oder Benutzer-Endgeräten und zum Einsatz von E-Mail- und Webanwendungsfiltern in Betracht ziehen, um die Exposition gegenüber bösartigen Inhalten zu verringern.

(18) Gemäß Artikel 21 Absatz 2 Buchstabe g der Richtlinie (EU) 2022/2555 müssen die Mitgliedstaaten sicherstellen, dass wesentliche und bedeutende Einrichtungen grundlegende Verfahren der Cyberhygiene und Schulungen zur Cybersicherheit anwenden. Die Cyberhygiene-Praktiken sind Teil der verschiedenen technischen und methodischen Anforderungen der im Anhang dieser Verordnung aufgeführten Maßnahmen für das Management von Cybersicherheitsrisiken. Was die grundlegenden Praktiken der Cyberhygiene betrifft, so sollten die betreffenden Einrichtungen Praktiken wie klare Arbeitsplatz- und Bildschirmrichtlinien, die Verwendung von Passwörtern und anderen Authentifizierungsmitteln, die sichere Nutzung von E-Mails und das sichere Surfen im Internet, den Schutz vor Phishing und Social Engineering sowie sichere Telearbeitspraktiken berücksichtigen.

(19) Um den unbefugten Zugang zu den Informationen und Vermögenswerten der betreffenden Stellen zu verhindern, sollten die betreffenden Stellen eine themenspezifische Richtlinie für den Zugang durch Netz- und Informationssystemprozesse, wie z. B. die Verbindung eines Netzes und Informationssystems mit einem anderen, festlegen und umsetzen.

(20) Um zu verhindern, dass Mitarbeiter z. B. Zugangsrechte innerhalb der betreffenden

Einrichtung missbrauchen, um Schaden anzurichten, sollten die betreffenden Einrichtungen angemessene Maßnahmen für das Sicherheitsmanagement der Mitarbeiter in Betracht ziehen und das Personal für diese Risiken sensibilisieren.

---

[2] Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und die Zertifizierung für Cybersicherheit in der Informations- und Kommunikationstechnologie sowie zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Cybersicherheitsgesetz) (ABl. L 151 vom 7.6.2019, S. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

(21) Die Multi-Faktor-Authentifizierung kann die Cybersicherheit der Einrichtungen erhöhen und sollte von den Einrichtungen insbesondere dann in Betracht gezogen werden, wenn Nutzer von entfernten Standorten aus auf Netz- und Informationssysteme zugreifen oder wenn sie auf sensible Informationen oder privilegierte Konten und Systemverwaltungskonten zugreifen. Die Multi-Faktor-Authentifizierung kann mit anderen Techniken kombiniert werden, um unter bestimmten Umständen auf der Grundlage vordefinierter Regeln und Muster zusätzliche Faktoren zu verlangen, z. B. beim Zugriff von einem ungewöhnlichen Ort, von einem ungewöhnlichen Gerät oder zu einem ungewöhnlichen Zeitpunkt.

(22) Die zuständigen Stellen sollten die Vermögenswerte, die für sie von Wert sind, durch eine solide Vermögensverwaltung verwalten und schützen, die auch als Grundlage für die Risikoanalyse und das Business Continuity Management dienen sollte. Die zuständigen Stellen sollten sowohl materielle als auch immaterielle Vermögenswerte verwalten und ein Bestandsverzeichnis erstellen, die Vermögenswerte einer bestimmten Klassifizierungsstufe zuordnen, die Vermögenswerte verwalten und verfolgen und Maßnahmen zum Schutz der Vermögenswerte während ihres gesamten Lebenszyklus ergreifen.

(23) Der Umgang mit Vermögenswerten sollte die Klassifizierung von Vermögenswerten nach Art, Sensibilität, Risikostufe und Sicherheitsanforderungen sowie die Anwendung geeigneter Maßnahmen und Kontrollen zur Gewährleistung ihrer Verfügbarkeit, Integrität und Vertraulichkeit umfassen. Durch die Klassifizierung von Vermögenswerten nach Risikostufen sollten die betreffenden Stellen in der Lage sein, geeignete Sicherheitsmaßnahmen und -kontrollen zum Schutz von Vermögenswerten anzuwenden, wie z. B. Verschlüsselung, Zugangskontrolle, einschließlich Zugangskontrollen am Rande des Geländes und physische Zugangskontrollen, Auditing, Backups, Protokollierung und Überwachung, Aufbewahrung und Entsorgung. Bei der Durchführung einer Analyse der Auswirkungen auf das Geschäft können die betreffenden Stellen den Geheimhaltungsgrad auf der Grundlage der Folgen einer Störung der Vermögenswerte für die Stellen festlegen. Alle Mitarbeiter der Stellen, die mit Vermögenswerten umgehen, sollten mit den Richtlinien und Anweisungen für den Umgang mit Vermögenswerten vertraut sein.

(24) Da die Fernarbeit in den letzten Jahren immer mehr an Bedeutung gewonnen hat, ist es für die Unternehmen von entscheidender Bedeutung, Regeln für das Personal festzulegen, wie es mit den Vermögenswerten des Unternehmens während der gesamten Dauer seiner Beschäftigung und während des gesamten Lebenszyklus der Vermögenswerte umgeht.

(25) Die Granularität des Bestandsverzeichnisses sollte den Erfordernissen der betreffenden Stellen angemessen sein. Ein umfassendes Bestandsverzeichnis sollte für jeden Vermögenswert zumindest eine eindeutige Kennung, den Eigentümer des Vermögenswerts, eine Beschreibung des Vermögenswerts, den Standort des Vermögenswerts, die Art des Vermögenswerts, die Art und Klassifizierung der in dem Vermögenswert verarbeiteten Informationen, das Datum der letzten Aktualisierung oder des letzten Patches des Vermögenswerts, die Klassifizierung des Vermögenswerts im Rahmen der Risikobewertung und das Ende der Lebensdauer des Vermögenswerts enthalten. Bei der Identifizierung des Eigentümers eines Vermögenswerts sollten die zuständigen Stellen auch die für den Schutz dieses Vermögenswerts verantwortliche Person ermitteln. Bei den Vermögenswerten kann es sich um Software, Hardware, Dienstleistungen, Einrichtungen, Heizungs-, Lüftungs- und Klimaanlagen, Patente, Urheberrechte oder physische Aufzeichnungen handeln.

(26) Die Zuweisung und Organisation von Aufgaben, Zuständigkeiten und Befugnissen im

Bereich der Cybersicherheit sollte eine kohärente Struktur für die Verwaltung und Umsetzung der Cybersicherheit innerhalb der betreffenden Stellen schaffen und eine wirksame Kommunikation bei Vorfällen gewährleisten. Bei der Festlegung und Zuweisung von Zuständigkeiten für bestimmte Rollen sollten die betreffenden Stellen Rollen wie den leitenden Beauftragten für Informationssicherheit, den Beauftragten für Informationssicherheit, den Beauftragten für die Bearbeitung von Vorfällen, den Rechnungsprüfer oder vergleichbare Funktionen in Betracht ziehen.

(27) Gemäß Artikel 21 Absatz 2 der Richtlinie (EU) 2022/2555 müssen die Maßnahmen für das Risikomanagement im Bereich der Cybersicherheit auf einem All-Gefahren-Ansatz beruhen, der darauf abzielt, Netz- und Informationssysteme und die physische Umgebung dieser Systeme vor Ereignissen wie Diebstahl, Brand, Überschwemmung, Telekommunikations- oder Stromausfällen oder unbefugtem physischen Zugang sowie vor Beschädigung und Beeinträchtigung einer wesentlichen oder wichtigen Einrichtung zu schützen

Informations- und Informationsverarbeitungseinrichtungen, die die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der von Netz- und Informationssystemen angebotenen oder über sie zugänglichen Dienste gefährden könnten. Die technischen und methodischen Anforderungen an das Risikomanagement im Bereich der Cybersicherheit sollten daher auch die physische und umgebungsbedingte Sicherheit von Netz- und Informationssystemen betreffen, indem sie Maßnahmen zum Schutz solcher Systeme vor Systemausfällen, menschlichem Versagen, böswilligen Handlungen oder Naturereignissen umfassen. Weitere Beispiele für physische und umweltbedingte Bedrohungen sind Erdbeben, Explosionen, Sabotage, Bedrohung durch Insider, zivile Unruhen, Giftmüll und Umweltemissionen. Die Verhinderung von Verlust, Beschädigung oder Beeinträchtigung von Netz- und Informationssystemen oder von Betriebsunterbrechungen aufgrund des Ausfalls oder der Störung unterstützender Versorgungseinrichtungen sollte zum Ziel der Geschäftskontinuität in den betreffenden Einrichtungen beitragen. Darüber hinaus sollte der Schutz vor physischen und umweltbedingten Bedrohungen zur Sicherheit bei der Wartung von Netzen und Informationssystemen in den betreffenden Stellen beitragen.

(28) Wenn die zuständigen Stellen Schutzmaßnahmen gegen physische und umweltbedingte Bedrohungen konzipieren und umsetzen, Mindest- und Höchstwerte für die Kontrolle physischer und umweltbedingter Bedrohungen festlegen und Umweltparameter überwachen, sollten sie insbesondere die Einrichtung eines separaten Brandabschnitts für das Rechenzentrum, die Verwendung feuerfester Materialien, Sensoren zur Überwachung von Temperatur und Luftfeuchtigkeit, den Anschluss des Gebäudes an ein Brandmeldesystem mit automatischer Benachrichtigung der örtlichen Feuerwehr sowie Brandfrüherkennungs- und -löschsysteme in Betracht ziehen. Die zuständigen Stellen sollten auch regelmäßige Brandschutzübungen und Brandinspektionen durchführen. Um die Stromversorgung sicherzustellen, sollten die zuständigen Stellen außerdem einen Überspannungsschutz und eine entsprechende Notstromversorgung gemäß den einschlägigen Normen in Betracht ziehen.

(29) Mit dieser Verordnung soll näher bestimmt werden, in welchen Fällen ein Vorkommnis als signifikant im Sinne von Artikel 23 Absatz 3 der Richtlinie (EU) 2022/2555 anzusehen ist. Die Kriterien sollten so beschaffen sein, dass die betroffenen Einrichtungen in der Lage sind, zu beurteilen, ob ein Vorfall signifikant ist, damit sie ihn gemäß der Richtlinie (EU) 2022/2555 melden können. Es sollten sowohl horizontale als auch für den jeweiligen Einrichtungstyp spezifische Fälle festgelegt werden, in denen ein Vorfall als signifikant zu betrachten ist.

(30) Um festzustellen, ob ein Vorfall signifikant ist, sollten die betroffenen Unternehmen gegebenenfalls die Anzahl der von dem Vorfall betroffenen Nutzer zählen. Ist eine relevante Einrichtung nicht in der Lage, die Anzahl der betroffenen Nutzer zu berechnen, sollte die Schätzung der relevanten Einrichtung über die mögliche Höchstzahl der betroffenen Nutzer für die Berechnung der Gesamtzahl der von dem Vorfall betroffenen Nutzer herangezogen werden.

(31) Wartungsarbeiten, die zu einer eingeschränkten Verfügbarkeit oder Nichtverfügbarkeit der Dienste führen, sollten nicht als signifikante Vorfälle angesehen werden, wenn die eingeschränkte Verfügbarkeit oder Nichtverfügbarkeit des Dienstes im Rahmen einer geplanten Wartungsmaßnahme erfolgt.

(32) Die Dauer eines Vorfalls sollte ab der Unterbrechung der ordnungsgemäßen Erbringung des Dienstes in Bezug auf Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit bis zum Zeitpunkt der Wiederherstellung gemessen werden. Kann eine

relevante Stelle den Zeitpunkt des Beginns der Unterbrechung nicht bestimmen, sollte die Dauer des Vorfalls ab dem Zeitpunkt der Entdeckung des Vorfalls oder ab dem Zeitpunkt, zu dem der Vorfall in Netz- oder Systemprotokollen oder anderen Datenquellen aufgezeichnet wurde, gemessen werden, je nachdem, welcher Zeitpunkt früher liegt.

(33) Die vollständige Nichtverfügbarkeit eines Dienstes sollte von dem Zeitpunkt an gemessen werden, an dem der Dienst für die Nutzer vollständig nicht mehr verfügbar ist, bis zu dem Zeitpunkt, an dem die regulären Aktivitäten oder Abläufe auf dem Niveau wiederhergestellt sind, das vor dem Vorfall herrschte. Kann eine relevante Stelle nicht feststellen, wann die vollständige Nichtverfügbarkeit eines Dienstes begann, sollte die Nichtverfügbarkeit ab dem Zeitpunkt gemessen werden, an dem sie von dieser Stelle festgestellt wurde.

(34) Bei der Ermittlung der finanziellen Verluste infolge eines Vorfalls sollten die betroffenen Unternehmen alle finanziellen Verluste berücksichtigen, die ihnen infolge des Vorfalls entstanden sind, z. B. Kosten für den Ersatz oder die Verlegung von Software, Hardware oder Infrastruktur, Personalkosten, einschließlich der Kosten für den Ersatz oder die Verlegung von Personal, die Einstellung von zusätzlichem Personal, Vergütung von Überstunden und Wiederherstellung verlorener oder beeinträchtigter Fähigkeiten, Gebühren aufgrund der Nichteinhaltung vertraglicher Verpflichtungen, Kosten für Wiedergutmachung und Entschädigung von Kunden, Verluste aufgrund entgangener Einnahmen, Kosten im Zusammenhang mit interner und externer Kommunikation, Beratungskosten, einschließlich Kosten im Zusammenhang mit Rechtsberatung, forensischen Diensten und Sanierungsdiensten, sowie gezahltes Lösegeld. Die betreffenden Unternehmen sollten die Höhe der finanziellen Verluste auf der Grundlage verfügbarer Daten berechnen und in Fällen, in denen die tatsächliche Höhe der finanziellen Verluste nicht ermittelt werden kann, sollten die Unternehmen diese Beträge schätzen.

(35) Eine große Verzögerung der Antwortzeit sollte als gegeben angesehen werden, wenn ein von einer relevanten Stelle erbrachter Dienst erheblich langsamer ist als die durchschnittliche Antwortzeit. Soweit möglich, sollten objektive Kriterien auf der Grundlage der durchschnittlichen Antwortzeiten der von den betreffenden Stellen erbrachten Dienste zur Bewertung der Verzögerung herangezogen werden.

(36) Für die Zwecke dieser Verordnung sollte ein Netz- und Informationssystem als kompromittiert gelten, wenn die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der von dem System angebotenen oder über das System zugänglichen Dienste beeinträchtigt ist.

(37) Die Kommission hat gemäß Artikel 21 Absatz 5 und Artikel 23 Absatz 11 der Richtlinie (EU) 2022/2555 Ratschläge ausgetauscht und mit der Kooperationsgruppe und der ENISA bei dem Entwurf des Durchführungsrechtsakts zusammengearbeitet.

(38) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 (EG) des Europäischen Parlaments und des Rates[3] konsultiert und hat seine Stellungnahme am [Datum der Stellungnahme] abgegeben.

(39) Diese Verordnung sollte ab dem [18. Oktober 2024] gelten.

(40) Die in dieser Verordnung vorgesehenen Maßnahmen stehen im Einklang mit der Stellungnahme des gemäß Artikel 39 der Richtlinie (EU) 2022/2555 eingesetzten Ausschusses,

HAT DIESE VERORDNUNG ANGENOMMEN:

[3] Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen, Ämter und Agenturen der Union und zum freien Datenverkehr sowie zur Aufhebung der Verordnung (EG) Nr. 45/2001 und der Entscheidung Nr. 1247/2002/EG (ABl. L 295 vom 21.11.2018, S . 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

Artikel 1

Gegenstand

Diese Verordnung legt in Bezug auf Anbieter von DNS-Diensten, TLD-Namensregistern, Anbietern von Cloud-Computing-Diensten, Anbietern von Rechenzentrumsdiensten, Anbietern von Content-Delivery-Netzen, Anbietern von verwalteten Diensten, Anbietern von verwalteten Sicherheitsdiensten, Anbietern von Online-Marktplätzen, Online-Suchmaschinen und Plattformen für soziale Netzwerke und Anbieter von Vertrauensdiensten ("die betroffenen Stellen") legt die technischen und methodischen Anforderungen an die in Artikel 21 Absatz 2 der Richtlinie (EU) 2022/2555 genannten Maßnahmen fest und bestimmt ferner, in welchen Fällen ein Vorfall als erheblich im Sinne von Artikel 23 Absatz 3 der Richtlinie (EU) 2022/2555 anzusehen ist.

Artikel 2

Technische und methodische Anforderungen

Die technischen und methodischen Anforderungen an die in Artikel 21 Absatz 2 Buchstaben a bis j der genannten Richtlinie genannten Maßnahmen des Cybersicherheitsrisikomanagements für die betreffenden Stellen sind im Anhang dieser Verordnung aufgeführt.

Artikel 3

Bedeutende Vorfälle

1. Ein Vorfall gilt als erheblich im Sinne von Artikel 23 Absatz 3 der Richtlinie 2022/2555 in Bezug auf die betroffenen Einrichtungen, wenn eines oder mehrere der folgenden Kriterien erfüllt sind:

(a) der Vorfall der betreffenden Einrichtung einen finanziellen Schaden verursacht hat oder verursachen kann, der 100 000 EUR oder 5 % des Jahresumsatzes der betreffenden Einrichtung übersteigt, je nachdem, welcher Betrag niedriger ist;

(b) der Vorfall dem betreffenden Unternehmen einen erheblichen Reputationsschaden gemäß Absatz 2 zugefügt hat oder zugefügt werden kann.

(c) der Vorfall die Exfiltration von Geschäftsgeheimnissen im Sinne von Artikel 2 Absatz 1 Nummer 1 der Richtlinie (EU) 2016/943 der betreffenden Einrichtung verursacht hat oder verursachen kann;

(d) das Ereignis den Tod einer natürlichen Person verursacht hat oder verursachen kann;

(e) das Ereignis einen erheblichen Schaden für die Gesundheit einer natürlichen Person verursacht hat oder verursachen kann;

(f) ein erfolgreicher, mutmaßlich böswilliger und unbefugter Zugriff auf Netz- und Informationssysteme stattgefunden hat;

(g) der Vorfall die in Artikel 4 genannten Kriterien erfüllt;

(h) das Ereignis erfüllt eines oder mehrere der in den Artikeln 5 bis 14 genannten Kriterien.

2. Bei der Feststellung des Vorliegens eines erheblichen Reputationsschadens durch einen Vorfall gemäß Absatz 1 Buchstabe b berücksichtigen die betreffenden Stellen, ob eines oder mehrere der folgenden Kriterien erfüllt sind:

(a) Die Medien haben über den Vorfall berichtet;

(b) der Vorfall zu Beschwerden von verschiedenen Benutzern oder kritischen Geschäftsbeziehungen geführt hat;

(c) das Unternehmen aufgrund des Vorfalls nicht in der Lage ist oder wahrscheinlich nicht in der Lage sein wird, die gesetzlichen Anforderungen zu erfüllen;

(d) es wahrscheinlich ist, dass das Unternehmen aufgrund des Vorfalls Kunden verliert, was wesentliche Auswirkungen auf seine Geschäftstätigkeit hat.

3. Geplante Folgen von Instandhaltungsmaßnahmen, die von oder im Auftrag der betreffenden Stellen durchgeführt werden, gelten nicht als signifikante Ereignisse.

4. Bei der Berechnung der Zahl der von einer Störung betroffenen Nutzer für die Zwecke der Artikel 7 und 9 bis 14 berücksichtigen die betreffenden Stellen alle folgenden Punkte:

(a) die Anzahl der Kunden, die einen Vertrag mit dem betreffenden Unternehmen haben, der ihnen Zugang zum Netz und zu den Informationssystemen des betreffenden Unternehmens oder zu den von diesen Netz- und Informationssystemen angebotenen oder über diese Systeme zugänglichen Diensten gewährt;

(b) die Zahl der natürlichen und juristischen Personen, die mit Geschäftskunden verbunden sind, die das Netz und die Informationssysteme der Unternehmen oder die von diesen angebotenen oder über diese Systeme zugänglichen Dienste nutzen.

Artikel 4

Wiederkehrende Vorfälle

Ereignisse, die einzeln nicht als signifikantes Ereignis im Sinne von Artikel 3 gelten, werden gemeinsam als ein signifikantes Ereignis betrachtet, wenn sie alle folgenden Kriterien erfüllen:

(a) sie sind mindestens zweimal innerhalb von 6 Monaten aufgetreten;

(b) sie haben offensichtlich die gleiche Ursache.

Artikel 5

Bedeutende Vorfälle in Bezug auf DNS-Dienstanbieter

In Bezug auf DNS-Diensteanbieter gilt ein Vorfall als erheblich im Sinne von Artikel 3, wenn er eines oder mehrere der folgenden Kriterien erfüllt:

(a) ein rekursiver oder maßgeblicher Domänennamensauflösungsdienst für mehr als 10 Minuten nicht verfügbar ist;

(b) über einen Zeitraum von mehr als einer Stunde beträgt die durchschnittliche Antwortzeit eines rekursiven oder autoritativen Domänennamensauflösungsdienstes auf DNS-Anfragen mehr als 10 Sekunden,

(c) die Integrität, Vertraulichkeit oder Authentizität gespeicherter, übermittelter oder verarbeiteter Daten im Zusammenhang mit der Verwaltung des DNS beeinträchtigt ist, außer in Fällen, in denen die Daten von weniger als 1 000 vom DNS-Diensteanbieter verwalteten Domänennamen, die nicht mehr als 1 % der vom DNS-Diensteanbieter verwalteten Domänennamen ausmachen, aufgrund einer Fehlkonfiguration nicht korrekt sind.

Artikel 6

Bedeutende Vorfälle im Zusammenhang mit TLD-Namensregistern

In Bezug auf TLD-Namensregister gilt ein Vorfall als erheblich im Sinne von Artikel 3, wenn er eines oder mehrere der folgenden Kriterien erfüllt:

(a) ein maßgeblicher Dienst zur Auflösung von Domänennamen ist nicht verfügbar;

(b) über einen Zeitraum von mehr als einer Stunde beträgt die durchschnittliche Antwortzeit eines autoritativen Dienstes zur Auflösung von Domänennamen auf DNS-Anfragen mehr als 10 Sekunden,

(c) die Integrität, Vertraulichkeit oder Authentizität der gespeicherten, übermittelten oder verarbeiteten Daten im Zusammenhang mit der Verwaltung der TLD beeinträchtigt wird.

Artikel 7

Bedeutende Vorfälle im Zusammenhang mit Anbietern von Cloud Computing-Diensten

In Bezug auf Anbieter von Cloud-Computing-Diensten gilt ein Vorfall als erheblich im Sinne von Artikel 3, wenn er eines oder mehrere der folgenden Kriterien erfüllt:

(a) einer oder mehrere der angebotenen Cloud Computing-Dienste länger als 10 Minuten nicht verfügbar sind;

(b) bei einem oder mehreren der erbrachten Cloud-Computing-Dienste die Kunden-Service-Level-Vereinbarung für mehr als 5 % der Nutzer von Cloud-Computing-Diensten in der Union oder für mehr als 1 Million der Nutzer von Cloud-Computing-Diensten in der Union, je nachdem, welche Zahl kleiner ist, für eine Dauer von mehr als einer Stunde nicht eingehalten wird;

(c) die Verfügbarkeit des Cloud-Computing-Dienstes eines Anbieters, mit dem keine Vereinbarung über das Dienstniveau des Kunden besteht, für mehr als 5 % der Nutzer von Cloud-Computing-Diensten in der Union oder für mehr als 1 Million der Nutzer von Cloud-Computing-Diensten in der Union, je nachdem, welche Zahl kleiner ist, für eine Dauer von mehr als einer Stunde eingeschränkt ist;

(d) die Integrität, Vertraulichkeit oder Authentizität gespeicherter, übermittelter oder verarbeiteter Daten im Zusammenhang mit der Erbringung des Cloud Computing-Dienstes infolge einer mutmaßlich böswilligen Handlung beeinträchtigt wird,

(e) die Integrität, Vertraulichkeit oder Authentizität gespeicherter, übermittelter oder verarbeiteter Daten im Zusammenhang mit der Erbringung des Cloud-Computing-Dienstes mit Auswirkungen auf mehr als 5 % der Nutzer des Cloud-Computing-Dienstes in der Union beeinträchtigt wird.

Artikel 8

Bedeutende Vorfälle im Zusammenhang mit Anbietern von Rechenzentrumsdienstleistungen

In Bezug auf Anbieter von Rechenzentrumsdiensten gilt ein Vorfall als erheblich im Sinne von Artikel 3, wenn er eines oder mehrere der folgenden Kriterien erfüllt:

(a) ein oder mehrere Rechenzentrumsdienste eines oder mehrerer der vom Anbieter betriebenen Rechenzentren vollständig nicht verfügbar sind;

(b) die Kunden-Service-Level-Vereinbarung für einen oder mehrere Rechenzentrumsdienste eines oder mehrerer der vom Anbieter betriebenen Rechenzentren für eine Dauer von mehr als einer Stunde nicht erfüllt wird;

(c) die Kunden-Service-Level-Vereinbarung für einen oder mehrere Rechenzentrumsdienste eines oder mehrerer vom Anbieter betriebener Rechenzentren infolge einer mutmaßlich böswilligen Handlung nicht eingehalten wird;

(d) die Integrität, Vertraulichkeit oder Authentizität gespeicherter, übermittelter oder verarbeiteter Daten im Zusammenhang mit der Erbringung des Rechenzentrumsdienstes infolge einer mutmaßlich böswilligen Handlung beeinträchtigt wird,

(e) der physische Zugang zu einem oder mehreren der vom Anbieter betriebenen Rechenzentren gefährdet ist.

Artikel 9

Bedeutende Vorfälle in Bezug auf Anbieter von Content-Delivery-Networks

In Bezug auf Anbieter von Content-Delivery-Netzen gilt ein Vorfall als erheblich im Sinne von Artikel 3, wenn er eines oder mehrere der folgenden Kriterien erfüllt:

(a) eines oder mehrere der Content-Delivery-Netze für mehr als 10 Minuten nicht verfügbar sind;

(b) die Kundendienstvereinbarung für die Leistung des Content-Delivery-Netzes für mehr als 5 % der Nutzer des Content-Delivery-Netzes in der Union oder für mehr als 1 Million der Nutzer des Content-Delivery-Netzes in der Union, je nachdem, welche Zahl kleiner ist, für eine Dauer von mehr als einer Stunde nicht eingehalten wird;

(c) die Verfügbarkeit des Content-Delivery-Netzes eines Anbieters, für den keine Kunden-Service-Level-Vereinbarung besteht, wird durch den Vorfall beeinträchtigt;

(d) die Integrität, Vertraulichkeit oder Authentizität gespeicherter, übermittelter oder verarbeiteter Daten im Zusammenhang mit der Bereitstellung des Netzes für die Bereitstellung von Inhalten infolge einer böswilligen Handlung beeinträchtigt wird,

(e) die Integrität, Vertraulichkeit oder Authentizität gespeicherter, übermittelter oder verarbeiteter Daten im Zusammenhang mit der Bereitstellung des Netzes für die Bereitstellung von Inhalten mit Auswirkungen auf mehr als 5 % der Nutzer des Netzes für die Bereitstellung von Inhalten in der Union beeinträchtigt wird.

Artikel 10

Bedeutende Vorfälle im Zusammenhang mit Anbietern von Managed Services und Managed Security Services

In Bezug auf Anbieter von verwalteten Diensten und Anbieter von verwalteten Sicherheitsdiensten gilt ein Vorfall als erheblich im Sinne von Artikel 3, wenn er eines oder mehrere der folgenden Kriterien erfüllt:

(a) einer oder mehrere der Managed Services oder Managed Security Services länger als 10 Minuten nicht verfügbar sind;

(b) für einen oder mehrere der erbrachten Managed Services oder Managed Security Services die Kunden-Service-Level-Vereinbarung für mehr als 5 % der Dienstleistungsnutzer in der Union oder für mehr als 1 Million der Dienstleistungsnutzer in der Union, je nachdem, welche Zahl kleiner ist, für eine Dauer von mehr als einer Stunde nicht eingehalten wird;

(c) die Verfügbarkeit eines oder mehrerer Managed- oder Managed-Security-Dienste eines Anbieters, für den keine Kunden-Service-Level-Vereinbarung besteht, wird durch den Vorfall beeinträchtigt;

(d) die Integrität, Vertraulichkeit oder Authentizität gespeicherter, übermittelter oder verarbeiteter Daten im Zusammenhang mit der Erbringung des verwalteten Dienstes oder des verwalteten Sicherheitsdienstes infolge einer mutmaßlich böswilligen Handlung beeinträchtigt wird,

(e) die Integrität, Vertraulichkeit oder Authentizität gespeicherter, übermittelter oder verarbeiteter Daten im Zusammenhang mit der Erbringung des verwalteten Dienstes oder des verwalteten Sicherheitsdienstes mit Auswirkungen auf mehr als 5 % der Nutzer des verwalteten Dienstes oder des verwalteten Sicherheitsdienstes in der Union beeinträchtigt wird.

Artikel 11

Bedeutende Vorfälle im Zusammenhang mit Anbietern von Online-Marktplätzen

In Bezug auf Anbieter von Online-Marktplätzen gilt ein Vorfall als erheblich im Sinne von Artikel 3, wenn er eines oder mehrere der folgenden Kriterien erfüllt:

(a) der Online-Marktplatz oder ein Teil seiner Funktionen für mehr als 5 % der Nutzer des Online-Marktplatzes in der Union oder für mehr als 1 Million der Nutzer des Online-Marktplatzes in der Union, je nachdem, welche Zahl kleiner ist, vollständig nicht verfügbar ist;

(b) mehr als 5 % der Nutzer von Online-Marktplätzen in der Union oder mehr als 1 Million der Nutzer von Online-Marktplätzen in der Union, je nachdem, welche Zahl kleiner ist, von großen Verzögerungen bei den Bestellungen betroffen sind;

(c) die Integrität, Vertraulichkeit oder Authentizität gespeicherter, übermittelter oder verarbeiteter Daten im Zusammenhang mit der Bereitstellung des Online-Marktplatzes infolge einer mutmaßlich böswilligen Handlung beeinträchtigt wird,

(d) die Integrität, Vertraulichkeit oder Authentizität gespeicherter, übermittelter oder verarbeiteter Daten im Zusammenhang mit der Bereitstellung des Online-Marktplatzes mit Auswirkungen auf mehr als 5 % der Nutzer des Online-Marktplatzes in der Union beeinträchtigt wird.

Artikel 12

Bedeutende Vorfälle im Zusammenhang mit Anbietern von Online-Suchmaschinen

In Bezug auf Anbieter von Online-Suchmaschinen gilt ein Vorfall als erheblich im Sinne von Artikel 3, wenn er eines oder mehrere der folgenden Kriterien erfüllt:

(a) die Online-Suchmaschine oder ein Teil ihrer Funktionalität für mehr als 5 % der Nutzer von Online-Suchmaschinen in der Union oder für mehr als 1 Million der Nutzer von Online-Suchmaschinen in der Union, je nachdem, welche Zahl kleiner ist, vollständig nicht verfügbar ist;

(b) mehr als 5 % der Nutzer von Online-Suchmaschinendiensten in der Union oder mehr als 1 Million der Nutzer von Online-Suchmaschinendiensten in der Union, je nachdem, welche Zahl kleiner ist, von großen Verzögerungen bei der Antwortzeit betroffen sind;

(c) die Integrität, Vertraulichkeit oder Authentizität gespeicherter, übermittelter oder verarbeiteter Daten im Zusammenhang mit der Bereitstellung der Online-Suchmaschine infolge einer mutmaßlich böswilligen Handlung beeinträchtigt wird,

(d) die Integrität, Vertraulichkeit oder Authentizität gespeicherter, übermittelter oder verarbeiteter Daten im Zusammenhang mit der Bereitstellung der Online-Suchmaschine mit Auswirkungen auf mehr als 5 % der Nutzer der Online-Suchmaschine in der Union beeinträchtigt wird.

Artikel 13

Bedeutende Vorfälle im Zusammenhang mit Anbietern von Plattformen für soziale Netzwerkdienste

In Bezug auf Anbieter von Plattformen für soziale Netzwerkdienste gilt ein Vorfall als erheblich im Sinne von Artikel 3, wenn er eines oder mehrere der folgenden Kriterien erfüllt:

(a) die Plattform des sozialen Netzwerks oder ein Teil ihrer Funktionen für mehr als 5 % der Nutzer der Plattform des sozialen Netzwerks in der Union oder für mehr als 1 Million der Nutzer der Plattform des sozialen Netzwerks in der Union, je nachdem, welche Zahl kleiner ist, vollständig nicht verfügbar ist;

(b) mehr als 5 % der Nutzer von sozialen Netzwerkplattformen in der Union oder mehr als 1 Million der Nutzer von sozialen Netzwerkplattformen in der Union, je nachdem, welche Zahl kleiner ist, von großen Verzögerungen bei der Reaktionszeit betroffen sind;

(c) die Integrität, Vertraulichkeit oder Authentizität gespeicherter, übermittelter oder verarbeiteter Daten im Zusammenhang mit der Bereitstellung der Plattform für soziale Netzwerkdienste infolge einer mutmaßlich böswilligen Handlung beeinträchtigt wird,

(d) die Integrität, Vertraulichkeit oder Authentizität gespeicherter, übermittelter oder verarbeiteter Daten im Zusammenhang mit der Bereitstellung der Plattform für soziale Netzwerkdienste mit Auswirkungen auf mehr als 5 % der Nutzer der Plattform für soziale Netzwerkdienste in der Union beeinträchtigt wird.

Artikel 14

Bedeutende Vorfälle in Bezug auf Vertrauensdiensteanbieter

In Bezug auf Vertrauensdiensteanbieter gilt ein Vorfall als erheblich im Sinne von Artikel 3, wenn er eines oder mehrere der folgenden Kriterien erfüllt:

(a) ein Vertrauensdienst oder ein Teil davon für mehr als 10 Minuten nicht verfügbar ist;

(b) ein Vertrauensdienst oder ein Teil davon für Benutzer oder vertrauende Parteien für mehr als eine Stunde, berechnet auf der Basis einer Kalenderwoche, nicht verfügbar ist;

(c) mehr als 1 % der Kunden des Vertrauensdienstes in der Union sind von großen Verzögerungen bei der Reaktionszeit des Vertrauensdienstes betroffen;

(d) der physische Zugang zu einem oder mehreren Bereichen, in denen sich Netz- und Informationssysteme befinden und zu denen nur vertrauenswürdiges Personal des Vertrauensdiensteanbieters Zugang hat, oder der Schutz dieses physischen Zugangs gefährdet ist;

(e) die Integrität, Vertraulichkeit oder Authentizität gespeicherter, übermittelter oder verarbeiteter Daten im Zusammenhang mit der Erbringung des Vertrauensdienstes mit Auswirkungen auf mehr als 1 % der Kunden des Vertrauensdienstes in der Union beeinträchtigt wird.

Artikel 15

Aufhebung

Die Durchführungsverordnung (EU) 2018/151 der Kommission[4] wird mit Wirkung vom [18. Oktober 2024] aufgehoben.

Artikel 16

Inkrafttreten und Anwendung

Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Diese Verordnung gilt ab dem [18. Oktober 2024].

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

[4] Durchführungsverordnung (EU) 2018/151 der Kommission vom 30. Januar 2018 zur Festlegung von Durchführungsbestimmungen zur Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates im Hinblick auf die Präzisierung der Elemente, die von Anbietern digitaler Dienste bei der Beherrschung der Risiken für die Sicherheit von Netz- und Informationssystemen zu berücksichtigen sind, und der Parameter für

die Feststellung, ob ein Vorfall erhebliche Auswirkungen hat (ABl. L 26 vom 31.1.2018, S. 48, ELI: http://data.europa.eu/eli/reg_impl/2018/151/oj).

Erledigt in Brüssel,

Für die Kommission
Ursula von der Leyen
Die Präsidentin

EUROPÄISCHE
KOMMISSION

Brüssel, XXX [...](2024)
XXX Entwurf

ANHANG

ANHANG

zum

Durchführungsverordnung der Kommission

zur Festlegung von Vorschriften für die Anwendung der Richtlinie (EU) 2022/2555 hinsichtlich der technischen und methodischen Anforderungen an Maßnahmen des Cybersicherheitsrisikomanagements und zur näheren Bestimmung der Fälle, in denen ein Vorfall in Bezug auf Anbieter von DNS-Diensten, TLD-Namensregistern, Anbietern von Cloud-Computing-Diensten, Anbietern von Rechenzentrumsdiensten, Anbietern von Content-Delivery-Netzen, Anbietern von verwalteten Diensten, Anbietern von verwalteten Sicherheitsdiensten, Anbietern von Online-Marktplätzen, Online-Suchmaschinen und Plattformen für soziale Netzwerkdienste sowie Anbietern von Vertrauensdiensten als erheblich angesehen wird

ANHANG

Technische und methodische Anforderungen gemäß Artikel 2 der vorliegenden Verordnung

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

1.1. Politik 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 Stellen für die Verwaltung der Sicherheit ihres Netzes und ihrer Informationssysteme darlegen;

(b) der Geschäftsstrategie und den Zielen der betreffenden Unternehmen angemessen sein und diese ergänzen;

(c) Ziele für die Netz- und Informationssicherheit festzulegen;

(d) Festlegung des Risikotoleranzniveaus in Übereinstimmung mit der Risikobereitschaft der betreffenden Unternehmen;

(e) eine Verpflichtung zur Erfüllung der geltenden Anforderungen in Bezug auf die Sicherheit von Netz- und Informationssystemen enthalten;

(f) eine Verpflichtung zur kontinuierlichen Verbesserung der Sicherheit von Netz- und Informationssystemen beinhalten;

(g) die Verpflichtung enthalten, die für die Umsetzung erforderlichen Ressourcen bereitzustellen, einschließlich des erforderlichen Personals, der finanziellen Mittel, Verfahren, Instrumente und Technologien;

(h) den betroffenen Mitarbeitern und interessierten Kreisen mitgeteilt und von diesen zur Kenntnis genommen werden;

(i) die Aufgaben und Zuständigkeiten gemäß Punkt 1.2. festzulegen;

(j) die aufzubewahrenden Unterlagen auflisten;

(k) die themenspezifischen Maßnahmen auflisten;

(l) Festlegung von Indikatoren und Maßnahmen zur Überwachung ihrer Umsetzung und des aktuellen Stands der Netz- und Informationssicherheit der betreffenden Stellen;

(m) das Datum der förmlichen Genehmigung durch die Leitungsorgane der betreffenden Einrichtungen (die "Leitungsorgane") angeben.

1.1.2. Die Netz- und Informationssystempolitik sowie die themenspezifischen Politiken werden von den Leitungsorganen in geplanten Abständen sowie bei bedeutenden Vorfällen oder wesentlichen Änderungen der Abläufe oder Risiken überprüft und gegebenenfalls aktualisiert. Das Ergebnis der Überprüfungen ist zu dokumentieren.

1.2. Rollen, Zuständigkeiten und Befugnisse

1.2.1. Im Rahmen ihrer Politik für die Sicherheit von Netz- und Informationssystemen gemäß Nummer 1.1 legen die betreffenden Stellen die Zuständigkeiten und Befugnisse für die Sicherheit von Netz- und Informationssystemen fest, weisen sie den Rollen zu, verteilen sie entsprechend den Bedürfnissen der betreffenden Stellen und teilen sie den Leitungsorganen mit.

1.2.2. Die betreffenden Stellen verlangen von ihrem gesamten Personal und von Dritten, dass sie die Sicherheit von Netzen und Informationssystemen im Einklang mit der festgelegten Netz- und Informationssicherheitspolitik, den themenspezifischen Strategien und Verfahren der betreffenden Stellen anwenden.

1.2.3. Mindestens eine Person erstattet den Leitungsorganen in Fragen der Sicherheit der Netze und Informationssysteme direkt Bericht.

1.2.4. Je nach Größe der betreffenden Stellen werden für die Sicherheit von Netzen und Informationssystemen spezielle Funktionen oder Aufgaben zusätzlich zu den bestehenden Funktionen wahrgenommen.

1.2.5. Sich widersprechende Aufgaben und Zuständigkeitsbereiche sind gegebenenfalls zu trennen.

1.2.6. Die Rollen, Zuständigkeiten und Befugnisse werden von den Leitungsorganen in geplanten Abständen sowie bei bedeutenden Zwischenfällen oder wesentlichen Änderungen der Abläufe oder Risiken überprüft und gegebenenfalls aktualisiert.

2. RISIKOMANAGEMENTPOLITIK (ARTIKEL 21 ABSATZ 2 BUCHSTABE A DER RICHTLINIE (EU) 2022/2555)

2.1. Rahmen für das Risikomanagement

2.1.1. Für die Zwecke von Artikel 21 Absatz 2 Buchstabe a der Richtlinie (EU) 2022/2555 müssen die betreffenden Stellen einen angemessenen Rahmen für das Risikomanagement einrichten und aufrechterhalten, um die Risiken für die Sicherheit von Netz- und Informationssystemen zu ermitteln und zu behandeln. Die betreffenden Stellen führen Risikobewertungen durch und dokumentieren sie, und auf der Grundlage der Ergebnisse erstellen sie einen Risikobehandlungsplan, setzen ihn um und überwachen ihn. Die Ergebnisse der Risikobewertung und die Restrisiken werden von den Leitungsorganen oder den Risikoeigentümern akzeptiert, sofern die betreffenden Stellen eine angemessene Berichterstattung an die Leitungsorgane sicherstellen.

2.1.2. Für die Zwecke von Nummer 2.1.1 legen die betreffenden Stellen Verfahren zur Ermittlung, Analyse, Bewertung und Behandlung von Risiken ("Verfahren für das Management von Risiken der Computer- und Netzsicherheit") fest und teilen sie ihren Mitarbeitern mit. Das Verfahren für das Management von Cybersicherheitsrisiken ist gegebenenfalls ein integraler Bestandteil des gesamten Risikomanagementverfahrens der betreffenden Unternehmen. Im Rahmen des Prozesses für das Management des Cybersicherheitsrisikos müssen die betreffenden Stellen:

(a) eine Risikomanagement-Methodik und gegebenenfalls Instrumente auf der

Grundlage einschlägiger europäischer und internationaler Normen umfassen;

(b) Festlegung und Pflege von Risikokriterien, die für die jeweiligen Unternehmen relevant sind;

(c) im Einklang mit einem All-Hazard-Ansatz die Risiken für die Sicherheit der Netz- und Informationssysteme zu ermitteln und zu dokumentieren, insbesondere in Bezug auf Dritte und Risiken, die zu Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit des Netzes und der Informationssysteme führen könnten, einschließlich der Ermittlung einzelner Fehlerquellen;

(d) Identifizierung der Risikoeigner;

(e) Analyse der Risiken für die Sicherheit von Netz- und Informationssystemen, einschließlich der Bedrohung, der Wahrscheinlichkeit, der Auswirkungen und des Risikoniveaus, unter Berücksichtigung der Erkenntnisse über Cyber-Bedrohungen und Schwachstellen;

(f) Bewertung der ermittelten Risiken anhand von Risikokriterien;

(g) Ermittlung und Priorisierung geeigneter Maßnahmen zur Risikobehandlung unter Berücksichtigung der Ergebnisse der Risikobewertung und der Ergebnisse des Verfahrens zur Bewertung der Wirksamkeit der Maßnahmen zum Risikomanagement im Bereich der Cybersicherheit;

(h) festlegen, wer für die Umsetzung der Maßnahmen zum Management der Cybersicherheitsrisiken verantwortlich ist und wann sie umgesetzt werden sollten;

(i) Sensibilisierung des Schlüsselpersonals für die wichtigsten Risiken und für die Maßnahmen zum Management der Cybersicherheitsrisiken;

(j) die gewählten Sicherheitsmaßnahmen und die Gründe, die die Inkaufnahme von Restrisiken rechtfertigen, nachvollziehbar dokumentieren.

2.1.3. Die zuständigen Stellen überprüfen und aktualisieren gegebenenfalls die Ergebnisse der Risikobewertung und den Risikobehandlungsplan in geplanten Abständen und bei wesentlichen Änderungen der Tätigkeiten oder Risiken oder bei bedeutenden Vorfällen.

2.2. Überwachung der Einhaltung

2.2.1. Die zuständigen Stellen überprüfen regelmäßig die Einhaltung ihrer Politik für die Sicherheit der Netze und Informationssysteme sowie der themenspezifischen Politiken, Regeln und Normen. Die Leitungsorgane werden durch regelmäßige Berichterstattung über den Stand der Netz- und Informationssicherheit auf der Grundlage der Überprüfung der Einhaltung der Vorschriften informiert.

2.2.2. Die betreffenden Stellen richten ein wirksames Compliance-Meldesystem ein, das ihren Strukturen, ihrem Betriebsumfeld und ihrer Bedrohungslandschaft angemessen ist. Das Compliance-Meldesystem muss in der Lage sein, den Leitungsorganen einen fundierten Überblick über den aktuellen Stand des Risikomanagements der betreffenden Stellen zu geben.

2.2.3. Die betreffenden Stellen führen die Überwachung der Einhaltung der Vorschriften in geplanten Abständen und bei Auftreten von bedeutenden Vorfällen oder bedeutenden Änderungen der Tätigkeiten oder Risiken durch.

2.3. Unabhängige Überprüfung der Informations- und Netzsicherheit

2.3.1. Die betreffenden Stellen überprüfen unabhängig ihr Konzept für die Verwaltung der

Sicherheit von Netzen und Informationssystemen und dessen Umsetzung, einschließlich Menschen, Verfahren und Technologien.

2.3.2. Die betreffenden Stellen entwickeln und unterhalten Verfahren zur Durchführung unabhängiger Überprüfungen, die von Personen mit angemessener Prüfungskompetenz durchgeführt werden müssen.

Die Personen, die die Überprüfungen durchführen, dürfen nicht dem Personal des überprüften Bereichs unterstellt sein. Wenn die Größe der Einrichtungen eine solche Trennung der Weisungsbefugnisse nicht zulässt, 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 der Vorschriften gemäß Punkt 2.2. und der Überwachung und Messung gemäß Punkt 7, werden den Leitungsorganen mitgeteilt. Gemäß den Risikoakzeptanzkriterien der betreffenden Stellen werden Abhilfemaßnahmen getroffen oder das Restrisiko akzeptiert.

2.3.4. Die unabhängigen Überprüfungen finden in geplanten Abständen und bei bedeutenden Zwischenfällen oder wesentlichen Änderungen der Abläufe oder Risiken statt.

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

3.1. Politik zur Behandlung von Zwischenfällen

3.1.1. Für die Zwecke von Artikel 21 Absatz 2 Buchstabe b der Richtlinie (EU) 2022/2555 legen die betreffenden Stellen eine Strategie für den Umgang mit Zwischenfällen fest, in der die Aufgaben, Zuständigkeiten und Verfahren für die rechtzeitige Erkennung, Analyse, Eindämmung oder Reaktion, Wiederherstellung, Dokumentation und Meldung von Zwischenfällen festgelegt sind.

3.1.2. Die unter Nummer 3.1.1 genannte Politik muss Folgendes umfassen:

(a) ein System zur Kategorisierung von Vorfällen;

(b) wirksame Kommunikationspläne, auch für Eskalation und Berichterstattung;

(c) Zuweisung von Aufgaben zur Erkennung von und angemessenen Reaktion auf Vorfälle an kompetente Mitarbeiter;

(d) Dokumente, die bei der Erkennung von und der Reaktion auf Vorfälle zu verwenden sind, wie z. B. Handbücher für die Reaktion auf Vorfälle, Eskalationstabellen, Kontaktlisten und Vorlagen;

(e) Schnittstellen zwischen der Bearbeitung von Zwischenfällen und dem Business Continuity Management.

3.1.3. Die in der Strategie festgelegten Aufgaben, Zuständigkeiten und Verfahren werden in geplanten Abständen sowie nach bedeutenden Zwischenfällen oder wesentlichen Änderungen der Abläufe oder Risiken getestet und überprüft und gegebenenfalls aktualisiert.

3.2. Überwachung und Protokollierung

3.2.1. Die zuständigen Stellen legen Verfahren fest und verwenden Hilfsmittel zur Überwachung und Protokollierung von Aktivitäten in ihren Netzen und Informationssystemen, um Ereignisse zu erkennen, die als Zwischenfälle betrachtet werden könnten, und entsprechend zu reagieren, um die Auswirkungen zu mildern.

3.2.2. Soweit machbar, wird die Überwachung automatisiert und entweder kontinuierlich oder in regelmäßigen Abständen durchgeführt, je nach den Möglichkeiten des Unternehmens. Die betreffenden Stellen führen ihre Überwachungsmaßnahmen so durch, dass falsch-positive und falsch-negative Ergebnisse auf ein Minimum reduziert werden.

3.2.3. Die zuständigen Stellen müssen Protokolle führen, dokumentieren und überprüfen. Die Protokolle müssen Folgendes enthalten:

(a) ausgehender und eingehender Netzwerkverkehr;

(b) Einrichtung, Änderung oder Löschung von Benutzern des Netzes und der Informationssysteme der betreffenden Stellen sowie Erweiterung der Berechtigungen;

(c) Zugang zu Systemen und Anwendungen;

(d) Ereignisse im Zusammenhang mit der Authentifizierung;

(e) alle privilegierten Zugriffe auf Systeme und Anwendungen sowie Aktivitäten, die von administrativen Konten ausgeführt werden;

(f) Zugriff auf oder Änderungen an kritischen Konfigurations- und Sicherungsdateien;

(g) Ereignisprotokolle und Protokolle von Sicherheitstools wie Antivirenprogrammen, Intrusion Detection Systemen oder Firewalls;

(h) Nutzung der Systemressourcen sowie deren Leistung;

(i) ggf. physischer Zugang zu den Einrichtungen;

(j) den Zugang zu ihren Netzeinrichtungen und Geräten und deren Nutzung;

(k) Aktivierung, Stoppen und Anhalten der verschiedenen Protokolle;

(l) Umweltereignisse, wie z. B. Überschwemmungsalarme, wo dies angebracht ist.

3.2.4. Die Protokolle sind auf ungewöhnliche oder unerwünschte Trends zu überprüfen. Die zuständigen Stellen legen geeignete Werte für Alarmschwellen fest. Werden die festgelegten Werte für die Alarmschwellen überschritten, wird gegebenenfalls automatisch ein Alarm ausgelöst. Der verantwortliche Mitarbeiter stellt sicher, dass im Falle eines Alarms eine qualifizierte und angemessene Reaktion eingeleitet wird.

3.2.5. Die zuständigen Stellen müssen die Protokolle über einen bestimmten Zeitraum aufbewahren und sichern und die Protokolle an einem zentralen Ort aufbewahren und vor unbefugtem Zugriff oder Änderungen schützen.

3.2.6. Die zuständigen Stellen stellen sicher, dass alle Systeme über synchronisierte Zeitquellen verfügen, um die Protokolle zwischen den Systemen für die Bewertung von Ereignissen in Beziehung setzen zu können. Die zuständigen Stellen erstellen und führen eine Liste aller Anlagen, die protokolliert werden, und stellen sicher, dass die Überwachungs- und Protokollierungssysteme redundant sind. Die Verfügbarkeit der Überwachungs- und Protokollierungssysteme ist unabhängig zu überwachen.

3.2.7. Die Verfahren sowie die Liste der zu protokollierenden Vermögenswerte werden in regelmäßigen Abständen und nach bedeutenden Vorfällen überprüft und gegebenenfalls aktualisiert.

3.3. Berichterstattung über Ereignisse

3.3.1. Die betreffenden Einrichtungen müssen einen einfachen Mechanismus einrichten, der es ihren Mitarbeitern, Lieferanten und Kunden ermöglicht, verdächtige Vorfälle zu melden.

3.3.2. Die betreffenden Stellen teilen ihren Lieferanten und Kunden das Verfahren zur Meldung von Ereignissen mit und schulen ihre Mitarbeiter regelmäßig in der Anwendung des Verfahrens.

3.4. Bewertung und Klassifizierung von Ereignissen

3.4.1. Die zuständigen Stellen bewerten verdächtige Ereignisse, um festzustellen, ob es sich um Vorfälle handelt, und bestimmen gegebenenfalls deren Art und Schwere.

3.4.2. Für die Zwecke von Nummer 3.4.1 handeln die betreffenden Stellen wie folgt:

(a) die Bewertung auf der Grundlage vorher festgelegter Kriterien und einer Triage durchführen, um die Prioritäten für die Eindämmung und Beseitigung von Zwischenfällen festzulegen;

(b) vierteljährlich das Vorhandensein von wiederkehrenden Ereignissen gemäß Artikel 4 dieser Verordnung zu bewerten;

(c) die entsprechenden Protokolle für die Bewertung und Klassifizierung von Ereignissen zu überprüfen;

(d) ein Verfahren für die Korrelation und Analyse von Protokollen einzuführen und

(e) eine Neubewertung und Neueinstufung von Ereignissen vorzunehmen, wenn neue Informationen verfügbar werden oder nach der Analyse bereits verfügbarer Informationen.

3.5. Reaktion auf Vorfälle

3.5.1. Die zuständigen Stellen reagieren auf Vorfälle gemäß den dokumentierten Verfahren und zeitnah.

3.5.2. Die Verfahren zur Reaktion auf einen Vorfall umfassen die folgenden Schritte:

(a) Eindämmung des Zwischenfalls, um zu verhindern, dass sich die Folgen des Zwischenfalls ausbreiten;

(b) Beseitigung, um zu verhindern, dass der Vorfall weitergeht oder erneut auftritt,

(c) ggf. Wiederherstellung nach dem Vorfall.

3.5.3. Die zuständigen Stellen erstellen Kommunikationspläne und -verfahren:

(a) mit den Computer Security Incident Response Teams (CSIRTs) oder gegebenenfalls mit den zuständigen Behörden im Zusammenhang mit der Meldung von Vorfällen;

(b) mit den relevanten internen und externen Interessengruppen.

3.5.4. Die zuständigen Stellen protokollieren die Maßnahmen zur Reaktion auf Vorfälle und zeichnen die Beweise auf.

3.5.5. Die zuständigen Stellen testen in geplanten Abständen ihre Verfahren zur Reaktion auf Zwischenfälle.

3.6. Überprüfungen nach einem Vorfall

3.6.1. Die zuständigen Stellen führen nach dem Vorfall Überprüfungen durch, um die Ursache des Vorfalls zu ermitteln und Lehren daraus zu ziehen, um das Auftreten und die Folgen künftiger Vorfälle zu verringern.

3.6.2. Die betreffenden Stellen stellen sicher, dass Überprüfungen nach einem Vorfall zur Verbesserung ihres Konzepts für die Netz- und Informationssicherheit, der Maßnahmen zur Risikobehandlung und der Verfahren zur Behandlung, Erkennung und Reaktion auf Vorfälle beitragen.

3.6.3. Die zuständigen Stellen überprüfen in geplanten Abständen, ob signifikante Vorfälle zu Überprüfungen nach dem Vorfall geführt haben.

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

4.1. Pläne für Geschäftskontinuität und Notfallwiederherstellung

4.1.1. Für die Zwecke von Artikel 21 Absatz 2 Buchstabe c der Richtlinie (EU) 2022/2555 müssen die betreffenden Einrichtungen einen Plan für die Kontinuität des Geschäftsbetriebs und die Wiederherstellung des Betriebs im Katastrophenfall erstellen und aufrechterhalten, der im Falle von Zwischenfällen anzuwenden ist.

4.1.2. Der Betrieb der betreffenden Stellen wird gemäß dem Plan zur Aufrechterhaltung des Geschäftsbetriebs und zur Wiederherstellung im Katastrophenfall wiederhergestellt. Der Plan stützt sich auf die Ergebnisse der Risikobewertung und umfasst Folgendes:

(a) Zweck, Umfang und Zielgruppe;

(b) Rollen und Verantwortlichkeiten;

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

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

(e) Reihenfolge der Einziehung der Beträge;

(f) Wiederherstellungspläne für bestimmte Maßnahmen, einschließlich der Wiederherstellungsziele;

(g) erforderliche Ressourcen, einschließlich Backups und Redundanzen;

(h) Wiederherstellung und Wiederaufnahme der Aktivitäten nach vorübergehenden Maßnahmen;

(i) Schnittstellen zur Bearbeitung von Vorfällen.

4.1.3. Die betreffenden Stellen führen eine Analyse der Auswirkungen auf den Geschäftsbetrieb durch, um die potenziellen Auswirkungen schwerwiegender Störungen ihres Geschäftsbetriebs zu bewerten, und legen auf der Grundlage der Ergebnisse der Analyse der Auswirkungen auf den Geschäftsbetrieb Kontinuitätsanforderungen für das Netz und die Informationssysteme fest.

4.1.4. Der Plan zur Aufrechterhaltung des Geschäftsbetriebs und der Notfallwiederherstellungsplan werden in geplanten Abständen und nach bedeutenden Zwischenfällen oder wesentlichen Änderungen der Abläufe oder Risiken getestet, überprüft und gegebenenfalls aktualisiert. Die betreffenden Stellen stellen sicher, dass die aus solchen Tests gewonnenen Erkenntnisse in die Pläne einfließen.

4.2. Verwaltung der Datensicherung

4.2.1. Die betreffenden Stellen bewahren Sicherungskopien der Informationen auf und stellen ausreichende Ressourcen zur Verfügung, einschließlich Einrichtungen, Netz- und Informationssysteme und Personal.

4.2.2. Auf der Grundlage der Ergebnisse der Risikobewertung und des Plans zur Aufrechterhaltung des Geschäftsbetriebs legen die betreffenden Stellen Sicherungspläne fest, die Folgendes umfassen:

(a) Erholungszeiten;

(b) Gewährleistung, dass die Sicherungskopien vollständig und korrekt sind,

einschließlich der in der Umgebung des Cloud-Computing-Dienstes gespeicherten Konfigurationsdaten und Informationen;

(c) Speicherung von Sicherungskopien (online oder offline) an einem oder mehreren sicheren Orten, die sich nicht im selben Netz wie das System befinden und weit genug entfernt sind, um bei einer Katastrophe am Hauptstandort nicht beschädigt zu werden;

(d) angemessene physische und logische Zugangskontrollen zu den Sicherungskopien entsprechend dem Geheimhaltungsgrad der Informationen;

(e) Wiederherstellung von Informationen aus Sicherungskopien, einschließlich Genehmigungsverfahren;

(f) Aufbewahrungsfristen auf der Grundlage der geschäftlichen und gesetzlichen Anforderungen.

4.2.3. Die zuständigen Stellen führen regelmäßige Integritätsprüfungen der Sicherungskopien durch.

4.2.4. Die zuständigen Stellen sorgen für eine ausreichende Verfügbarkeit der Ressourcen, indem sie zumindest eine Teilredundanz der folgenden Punkte sicherstellen:

(a) Netz- und Informationssysteme;

(b) Vermögenswerte, einschließlich Einrichtungen, Ausrüstungen und Material;

(c) Personal mit der erforderlichen Verantwortung, Autorität und Kompetenz;

(d) geeignete Kommunikationskanäle.

4.2.5. Die zuständigen Stellen stellen sicher, dass die Überwachung und Anpassung der Ressourcen, einschließlich der Einrichtungen, Systeme und des Personals, in angemessener Weise auf der Grundlage von Backup- und Redundanzanforderungen erfolgt.

4.2.6. Die betreffenden Stellen führen regelmäßige Tests der Wiederherstellung von Sicherungskopien und Redundanzen durch, um sicherzustellen, dass im Wiederherstellungsfall auf sie Verlass ist und sie die Kopien, Prozesse und Kenntnisse für eine wirksame Wiederherstellung umfassen. Die zuständigen Stellen dokumentieren die Ergebnisse der Tests und ergreifen erforderlichenfalls Korrekturmaßnahmen.

4.3. Krisenmanagement

4.3.1. Die zuständigen Stellen müssen Verfahren für das Krisenmanagement einrichten.

4.3.2. Die betreffenden Stellen stellen sicher, dass die Krisenmanagementprozesse zumindest die folgenden Elemente berücksichtigen:

(a) Aufgaben und Zuständigkeiten des Personals, um sicherzustellen, dass alle Mitarbeiter ihre Aufgaben in Krisensituationen kennen, einschließlich spezifischer Schritte, die zu befolgen sind;

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

(c) Anwendung geeigneter Kontrollen wie unterstützende Systeme, Verfahren und zusätzliche Kapazitäten.

Für die Zwecke von Buchstabe b umfasst der Informationsfluss zwischen den betreffenden Stellen und den jeweils zuständigen Behörden sowohl obligatorische Mitteilungen, wie z. B. Berichte über Vorfälle und damit verbundene Zeitpläne, als auch nicht obligatorische Mitteilungen.

4.3.3. Die betreffenden Stellen führen ein Verfahren zur Verwaltung und Nutzung der von den CSIRTs oder gegebenenfalls den zuständigen Behörden erhaltenen Informationen über Vorfälle, Schwachstellen, Bedrohungen oder Sicherheitskontrollen ein.

4.3.4. Die betreffenden Stellen testen, überprüfen und aktualisieren den Krisenmanagementplan gegebenenfalls regelmäßig oder nach bedeutenden Vorfällen oder wesentlichen Änderungen der Tätigkeiten oder Risiken.

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

5.1. Sicherheitspolitik für die Lieferkette

5.1.1. Für die Zwecke von Artikel 21 Absatz 2 Buchstabe d der Richtlinie (EU) 2022/2555 müssen die betreffenden Stellen ein Sicherheitskonzept für die Lieferkette aufstellen, umsetzen und anwenden, das die Beziehungen zu ihren direkten Lieferanten und Dienstleistern regelt, um die ermittelten Risiken für die Sicherheit von Netz- und Informationssystemen zu mindern. In dem Sicherheitskonzept für die Lieferkette legen die betreffenden Stellen ihre Rolle in der Lieferkette fest und teilen sie ihren direkten Lieferanten und Dienstleistern mit.

5.1.2. Im Rahmen des in Abschnitt 5.1.1 genannten Konzepts für die Sicherheit der Lieferkette legen die betreffenden Stellen Kriterien für die Auswahl und Beauftragung von Lieferanten und Dienstleistern fest. Diese Kriterien müssen Folgendes umfassen:

(a) die Cybersicherheitspraktiken der Lieferanten und Dienstleistungsanbieter, einschließlich ihrer sicheren Entwicklungsverfahren;

(b) die Fähigkeit der Lieferanten und Dienstleister, die von den Einrichtungen festgelegten Cybersicherheitsspezifikationen zu erfüllen;

(c) die Gesamtqualität und Widerstandsfähigkeit von IKT-Produkten und IKT-Dienstleistungen und die darin enthaltenen Maßnahmen zum Management von Cybersicherheitsrisiken, einschließlich der Risiken und der Klassifizierungsstufe der IKT-Produkte und IKT-Dienstleistungen;

(d) die Fähigkeit der betreffenden Unternehmen, ihre Bezugsquellen zu diversifizieren und die Bindung an bestimmte Lieferanten zu begrenzen.

5.1.3. Bei der Festlegung ihres Konzepts für die Sicherheit der Lieferkette berücksichtigen die betreffenden Stellen die Ergebnisse der koordinierten Bewertungen der Sicherheitsrisiken kritischer Lieferketten, die gemäß Artikel 22 Absatz 1 der Richtlinie (EU) 2022/2555 durchgeführt wurden, soweit anwendbar.

5.1.4. Auf der Grundlage des Sicherheitskonzepts für die Lieferkette und unter Berücksichtigung der Ergebnisse der gemäß Nummer 2.1 dieses Anhangs durchgeführten Risikobewertung stellen die betreffenden Stellen sicher, dass in ihren Verträgen mit den Lieferanten und Dienstleistern, gegebenenfalls durch Dienstgütevereinbarungen, Folgendes festgelegt wird

(a) Anforderungen an die Cybersicherheit von Lieferanten oder Dienstleistern, einschließlich der Anforderungen an die Sicherheit beim Erwerb von IKT-Dienstleistungen oder IKT-Produkten gemäß Punkt 6.1;

(b) Anforderungen an die Fähigkeiten und die Ausbildung sowie gegebenenfalls an die Zertifizierungen, die von den Mitarbeitern der Lieferanten oder Dienstleister verlangt werden;

(c) Anforderungen an die Zuverlässigkeitsüberprüfung der Mitarbeiter von Lieferanten und Dienstleistern gemäß Punkt 10.2;

(d) die Verpflichtung der Lieferanten und Dienstleister, die betreffenden Stellen unverzüglich über Vorfälle zu unterrichten, die ein Risiko für die Sicherheit der Netze und Informationssysteme dieser Stellen darstellen;

(e) Bestimmungen über Reparaturzeiten;

(f) das Recht auf Prüfung oder das Recht, Prüfungsberichte zu erhalten;

(g) eine Verpflichtung für Lieferanten und Dienstleister, Schwachstellen zu beheben, die ein Risiko für die Sicherheit des Netzes und der Informationssysteme der betreffenden Einrichtungen darstellen;

(h) Anforderungen an die Vergabe von Unteraufträgen und - sofern die betreffenden Stellen die Vergabe von Unteraufträgen zulassen - Anforderungen an die Cybersicherheit von Unterauftragnehmern im Einklang mit den unter Buchstabe a genannten Cybersicherheitsanforderungen;

(i) Verpflichtungen der Lieferanten und Dienstleister bei Beendigung des Vertrags, wie z. B. Abruf und Beseitigung der von den Lieferanten und Dienstleistern bei der Ausübung ihrer Aufgaben erhaltenen Informationen.

5.1.5. Die betreffenden Stellen berücksichtigen die in den Abschnitten 5.1.2 und 5.1.3 genannten Elemente im Rahmen des Auswahlverfahrens für neue Lieferanten und Dienstleister sowie im Rahmen des in Abschnitt 6.1 genannten Beschaffungsprozesses.

5.1.6. Die betreffenden Stellen überprüfen das Sicherheitskonzept für die Lieferkette und überwachen und bewerten die Änderungen der Cybersicherheitspraktiken von Lieferanten und Dienstleistern in geplanten Abständen und bei wesentlichen Änderungen der Betriebsabläufe oder Risiken oder bei wesentlichen Vorfällen, die mit der Erbringung von IKT-Dienstleistungen zusammenhängen oder Auswirkungen auf die Sicherheit des IKT-Produkts von Lieferanten und Dienstleistern haben, und ergreifen erforderlichenfalls entsprechende Maßnahmen.

5.1.7. Für die Zwecke von Punkt 5.1.5. müssen die betreffenden Stellen:

(a) regelmäßige Überwachung der Berichte über die Umsetzung der Dienstleistungsvereinbarungen, sofern zutreffend;

(b) Überprüfung von Vorfällen im Zusammenhang mit IKT-Produkten und IKT-Dienstleistungen von Lieferanten und Dienstleistern;

(c) die Notwendigkeit außerplanmäßiger Überprüfungen zu beurteilen und die Ergebnisse nachvollziehbar zu dokumentieren;

(d) die Risiken zu analysieren, die sich aus Änderungen im Zusammenhang mit IKT-Produkten und IKT-Dienstleistungen von Lieferanten und Dienstleistern ergeben, und gegebenenfalls rechtzeitig Abhilfemaßnahmen zu ergreifen.

5.2. Verzeichnis von Lieferanten und Dienstleistern

Die betreffenden Stellen führen ein Verzeichnis ihrer direkten Zulieferer und Dienstleistungserbringer und halten es auf dem neuesten Stand, einschließlich:

(a) Kontaktstellen für jeden Direktlieferanten und Dienstleistungsanbieter;

(b) eine Liste von IKT-Produkten, IKT-Dienstleistungen und IKT-Prozessen, die der direkte Lieferant oder Dienstleister den Einrichtungen zur Verfügung stellt.

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

6.1. Sicherheit beim Erwerb von IKT-Dienstleistungen oder IKT-Produkten

6.1.1. Für die Zwecke von Artikel 21 Absatz 2 Buchstabe e der Richtlinie (EU) 2022/2555 legen die betreffenden Stellen Prozesse und Verfahren fest und setzen diese um, um die Risiken zu beherrschen, die sich aus dem Erwerb von IKT-Dienstleistungen oder IKT-Produkten für Komponenten ergeben, die für die Sicherheit der Netz- und Informationssysteme der betreffenden Stellen kritisch sind, und zwar auf der Grundlage der Risikobewertung bei Lieferanten oder Dienstleistern während ihres gesamten Lebenszyklus.

6.1.2. Für die Zwecke von Nummer 6.1.1. gelten die in Nummer 6.1.1 genannten Prozesse und Verfahren als
6.1.1. muss umfassen:

(a) Sicherheitsanforderungen, die für die zu erwerbenden IKT-Dienstleistungen oder IKT-Produkte gelten sollen;

(b) Anforderungen in Bezug auf Sicherheitsaktualisierungen während der gesamten Lebensdauer der IKT-Dienstleistungen oder IKT-Produkte bzw. deren Austausch nach Ablauf des Supportzeitraums;

(c) Informationen zur Beschreibung der in den IKT-Dienstleistungen oder IKT-Produkten verwendeten Hardware- und Softwarekomponenten;

(d) Informationen, die die implementierten Cybersicherheitsfunktionen der IKT-Dienste oder IKT-Produkte und die für deren sicheren Betrieb erforderliche Konfiguration beschreiben;

(e) Gewährleistung, dass die IKT-Dienstleistungen oder -Produkte die Sicherheitsanforderungen gemäß Buchstabe a erfüllen;

(f) geeignete Methoden zur Validierung der Konformität der gelieferten IKT-Dienste oder IKT-Produkte mit den angegebenen Sicherheitsanforderungen sowie die Dokumentation der Ergebnisse der Validierung.

6.1.3. Die zuständigen Stellen überprüfen und aktualisieren die Prozesse und Verfahren gegebenenfalls in geplanten Abständen und bei bedeutenden Zwischenfällen.

6.2. Sicherer Lebenszyklus der Entwicklung

6.2.1. Die zuständigen Stellen legen Regeln für die sichere Entwicklung von Netz- und Informationssystemen, einschließlich Software, fest, setzen sie um und wenden sie an, wenn sie Netz- und Informationssysteme beschaffen oder entwickeln. Die Regeln müssen alle Entwicklungsphasen abdecken, einschließlich Spezifikation, Entwurf, Entwicklung, Implementierung und Test.

6.2.2. Die betreffenden Stellen müssen:

(a) eine Analyse der Sicherheitsanforderungen in der Spezifikations- und Entwurfsphase jedes Entwicklungs- oder Beschaffungsprojekts durchführen, das von den betreffenden Stellen oder im Auftrag dieser Stellen durchgeführt wird;

(b) Anwendung von Grundsätzen für die Entwicklung sicherer Systeme und von Grundsätzen für die sichere Kodierung auf die Entwicklung von Informationssystemen, z. B. Förderung von "Cybersecurity by Design" und "Zero Trust"-Architekturen;

(c) Sicherheitsanforderungen für Entwicklungsumgebungen festzulegen;

(d) Einführung und Umsetzung von Sicherheitstestverfahren im Entwicklungszyklus;

(e) angemessene Auswahl, Schutz und Verwaltung von Sicherheitstestinformationen;

(f) die Testdaten entsprechend der Risikobewertung zu bereinigen und zu anonymisieren.

6.2.3. Für die ausgelagerte Entwicklung und Beschaffung von Netz- und Informationssystemen wenden die betreffenden Stellen die unter den Nummern 5 und 6.1 genannten Strategien und Verfahren an.

6.2.4. Die betreffenden Stellen überprüfen und aktualisieren gegebenenfalls ihre Regeln für die sichere Entwicklung in geplanten Abständen.

6.3. Konfigurationsmanagement

6.3.1. Die zuständigen Stellen müssen Konfigurationen, einschließlich Sicherheitskonfigurationen von Hardware, Software, Diensten und Netzen, festlegen, dokumentieren, umsetzen und überwachen.

6.3.2. Für die Zwecke von Punkt 6.3.1. müssen die betreffenden Stellen:

(a) Konfigurationen, einschließlich Sicherheitskonfigurationen, für ihre Hardware, Software, Dienste und Netze festzulegen;

(b) Festlegung und Umsetzung von Prozessen und Werkzeugen zur Durchsetzung der festgelegten Konfigurationen, einschließlich der Sicherheitskonfigurationen, für Hardware, Software, Dienste und Netze, sowohl für neu installierte Systeme als auch für im Betrieb befindliche Systeme während ihrer gesamten Lebensdauer.

6.3.3. Die betreffenden Stellen überprüfen und aktualisieren die Konfigurationen gegebenenfalls in geplanten Abständen oder wenn wesentliche Vorfälle oder wesentliche Änderungen der Abläufe oder Risiken auftreten.

6.4. Änderungsmanagement, Reparatur und Wartung

6.4.1. Die betreffenden Stellen wenden Verwaltungsverfahren für Änderungen, Reparaturen und Wartung von Netz- und Informationssystemen an. Gegebenenfalls müssen die Verfahren mit den allgemeinen Grundsätzen der betreffenden Stellen für das Änderungsmanagement übereinstimmen.

6.4.2. Die in Nummer 6.4.1 genannten Verfahren sind für Freigaben, Änderungen und Notfalländerungen von Betriebssoftware, Hardware und Änderungen der Konfiguration anzuwenden.

6.4.3. Falls die regulären Änderungskontrollverfahren aufgrund eines Notfalls nicht eingehalten werden konnten, dokumentieren die betreffenden Stellen das Ergebnis der Änderung und die Erklärung, warum die Verfahren nicht eingehalten werden konnten.

6.4.4. Die betreffenden Stellen überprüfen und aktualisieren die Verfahren gegebenenfalls in geplanten Abständen und bei bedeutenden Zwischenfällen oder wesentlichen Änderungen der Abläufe oder Risiken.

6.5. Sicherheitstests

6.5.1. Die betreffenden Stellen müssen eine Politik und Verfahren für Sicherheitstests festlegen, umsetzen und anwenden.

6.5.2. Die betreffenden Stellen müssen:

(a) auf der Grundlage der Risikobewertung die Notwendigkeit, den Umfang, die Häufigkeit und die Art der Sicherheitstests festzulegen;

(b) Durchführung von Sicherheitstests nach einer dokumentierten Testmethodik, die die Komponenten abdeckt, die in einer Risikoanalyse als relevant für den sicheren Betrieb identifiziert wurden;

(c) Art, Umfang, Zeit und Ergebnisse der Tests zu dokumentieren, einschließlich der Bewertung der Kritikalität und der Abhilfemaßnahmen für jede Feststellung;

(d) Anwendung von Abhilfemaßnahmen im Falle kritischer Feststellungen.

6.5.3. Die betreffenden Stellen überprüfen und aktualisieren gegebenenfalls ihre Strategien für Sicherheitstests in geplanten Abständen.

6.6. Verwaltung von Sicherheits-Patches

6.6.1. Die zuständigen Stellen legen Verfahren fest und wenden diese an, um sicherzustellen, dass:

(a) Sicherheitspatches innerhalb eines angemessenen Zeitraums nach ihrer Verfügbarkeit angewendet werden;

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

(c) Sicherheits-Patches stammen aus vertrauenswürdigen Quellen und werden auf ihre Integrität geprüft;

(d) zusätzliche Maßnahmen ergriffen und Restrisiken in Kauf genommen werden, wenn ein Patch nicht verfügbar ist oder nicht gemäß Nummer 6.6.2 angewendet wird.

6.6.2. Abweichend von Nummer 1 Buchstabe a können die betreffenden Stellen beschließen, keine Sicherheits-Patches anzuwenden, wenn die Nachteile der Anwendung der Sicherheits-Patches den Nutzen für die Cybersicherheit überwiegen. Die betreffenden Stellen müssen die Gründe für eine solche Entscheidung ordnungsgemäß dokumentieren und begründen.

6.7. Sicherheit im Netz

6.7.1. Die betreffenden Stellen ergreifen geeignete Maßnahmen zum Schutz ihrer Netze und Informationssysteme vor Cyber-Bedrohungen.

6.7.2. Für die Zwecke von Punkt 6.7.1. müssen die betreffenden Stellen:

(a) die Architektur des Netzes in verständlicher und aktueller F o r m zu dokumentieren;

(b) Festlegung und Anwendung von Kontrollen zum Schutz der internen Netzbereiche der betreffenden Stellen vor unberechtigtem Zugriff;

(c) Kontrollen zu konfigurieren, um Zugriffe zu verhindern, die für den Betrieb d e r betreffenden Einheiten nicht erforderlich sind;

(d) Festlegung und Anwendung von Kontrollen für den Fernzugriff auf Netz- und Informationssysteme, einschließlich des Zugriffs durch Diensteanbieter;

(e) die für die Verwaltung der Umsetzung der Sicherheitspolitik verwendeten Systeme nicht für andere Zwecke zu nutzen;

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

(g) gegebenenfalls den Zugang zu den Netzen und Informationssystemen der betreffenden Stellen ausschließlich mit von diesen Stellen zugelassenen Geräten gestatten;

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

(i) die Kommunikation zwischen verschiedenen Systemen nur über vertrauenswürdige Kanäle herzustellen, die durch logische, kryptografische oder physische Trennung von anderen Kommunikationskanälen isoliert sind und eine gesicherte Identifizierung ihrer Endpunkte sowie den Schutz der Kanaldaten vor Veränderung oder Offenlegung gewährleisten;

(j) einen Umsetzungsplan für den sicheren und vollständigen Übergang zu Kommunikationsprotokollen der neuesten Generation auf der Netzebene zu verabschieden, um die Angriffsfläche der Netze zu verringern, und Maßnahmen zur Beschleunigung dieses Übergangs festzulegen;

(k) einen Umsetzungsplan für die Einführung international vereinbarter und interoperabler moderner E-Mail-Kommunikationsstandards zur Sicherung der E-Mail-Kommunikation zu verabschieden, um Schwachstellen im Zusammenhang mit E-Mail-Bedrohungen zu verringern, und Maßnahmen zur Beschleunigung dieser Einführung festzulegen;

(l) Anwendung bewährter Verfahren für die Sicherheit des Internet-Routings und die Routing-Hygiene des vom Netz ausgehenden und für das Netz bestimmten Verkehrs.

6.7.3. Die betreffenden Stellen überprüfen und aktualisieren diese Maßnahmen gegebenenfalls in geplanten Abständen sowie bei bedeutenden Zwischenfällen oder wesentlichen Änderungen der Abläufe oder Risiken.

6.8. Segmentierung des Netzes

6.8.1. Die betreffenden Stellen segmentieren die Systeme in Übereinstimmung mit den Ergebnissen der Risikobewertung gemäß Nummer 2.1 in Netze oder Zonen. Sie trennen ihre Systeme und Netze von den Systemen und Netzen Dritter.

6.8.2. Zu diesem Zweck müssen die betreffenden Einrichtungen:

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

(b) die gleichen Sicherheitsmaßnahmen auf alle Netz- und Informationssysteme in derselben Zone anzuwenden;

(c) den Zugang zu einem Netz oder einer Zone auf der Grundlage einer Bewertung seiner Sicherheitsanforderungen zu gewähren;

(d) alle Systeme, die für den Betrieb der betreffenden Einrichtungen oder für die Sicherheit kritisch sind, in einer oder mehreren gesicherten Zonen unterzubringen;

(e) den Zugang und die Kommunikation zwischen und innerhalb von Zonen auf das beschränken, was für den Betrieb der betreffenden Stellen oder für die Sicherheit erforderlich ist;

(f) Trennung des speziellen Netzes für die Verwaltung der Netz- und Informationssysteme vom Betriebsnetz der betreffenden Stellen;

(g) Netzverwaltungskanäle vom übrigen Netzverkehr abtrennen;

(h) die Produktionssysteme für die Dienste der Unternehmen von den Entwicklungs- und Testsystemen zu trennen, einschließlich Backups.

6.8.3. Die betreffenden Stellen überprüfen und aktualisieren gegebenenfalls die Netzsegmentierung in geplanten Abständen und bei bedeutenden Vorfällen oder wesentlichen Änderungen der Abläufe oder Risiken.

6.9. Schutz vor bösartiger und nicht zugelassener Software

6.9.1. Die betreffenden Stellen schützen ihre Netze und Informationssysteme vor bösartiger und nicht genehmigter Software.

6.9.2. Zu diesem Zweck stellen die betreffenden Stellen insbesondere sicher, dass ihre Netz- und Informationssysteme mit Software zur Erkennung und Reparatur von Schadsoftware ausgestattet sind, die entsprechend der Risikobewertung und den vertraglichen Vereinbarungen mit den Anbietern regelmäßig aktualisiert wird.

6.10. Umgang mit Schwachstellen und Offenlegung

6.10.1. Die betreffenden Stellen informieren sich über technische Schwachstellen in ihren Netzen und Informationssystemen, bewerten ihre Gefährdung durch solche Schwachstellen und ergreifen geeignete Maßnahmen zur Behebung der Schwachstellen.

6.10.2. Für die Zwecke von Punkt 6.10.1. müssen die betreffenden Stellen:

(a) Überwachung von Informationen über Schwachstellen über geeignete Kanäle, z. B. durch Bekanntmachungen von CSIRTs, zuständigen Behörden oder Informationen von Lieferanten oder Dienstleistern.

(b) gegebenenfalls Schwachstellen-Scans durchzuführen und die Ergebnisse der Scans in geplanten Abständen zu dokumentieren;

(c) ohne unnötige Verzögerung die Schwachstellen zu beseitigen, die von den betreffenden Stellen als kritisch für ihren Betrieb eingestuft werden;

(d) sicherstellen, dass ihr Umgang mit Schwachstellen mit ihren Verfahren für das Änderungs- und Störungsmanagement vereinbar ist;

(e) ein Verfahren zur Offenlegung von Schwachstellen im Einklang mit der geltenden nationalen koordinierten Politik zur Offenlegung von Schwachstellen festlegen.

6.10.3. Wenn die potenziellen Auswirkungen der Schwachstelle dies rechtfertigen, müssen die betreffenden Stellen einen Plan zur Behebung der Schwachstelle erstellen und umsetzen. In anderen Fällen müssen die betreffenden Stellen dokumentieren und begründen, warum die Schwachstelle nicht behoben werden muss.

6.10.4. Die zuständigen Stellen überprüfen und aktualisieren gegebenenfalls in geplanten Abständen die Kanäle, die sie zur Überwachung von Informationen über Sicherheitsrisiken nutzen.

7. POLITIKEN UND VERFAHREN ZUR BEWERTUNG DER WIRKSAMKEIT VON MAßNAHMEN ZUM MANAGEMENT VON CYBERSICHERHEITSRISIKEN (ARTIKEL 21 ABSATZ 2 BUCHSTABE F DER RICHTLINIE (EU) 2022/2555)

7.1.1. Für die Zwecke von Artikel 21 Absatz 2 Buchstabe f der Richtlinie (EU) 2022/2555 müssen die betreffenden Stellen eine Strategie und Verfahren festlegen, umsetzen und anwenden, um zu bewerten, ob die in Punkt 1.1. genannte Strategie für die Sicherheit von Netz- und Informationssystemen wirksam umgesetzt und aufrechterhalten wird.

7.1.2. Die in Nummer 7.1 genannten Grundsätze und Verfahren müssen den Ergebnissen der Risikobewertung gemäß Nummer 2.1 und früheren bedeutenden Vorfällen Rechnung tragen. Die Verfahren müssen Sicherheitsbewertungen und Sicherheitstests umfassen. Die betreffenden Stellen legen fest:

(a) welche Maßnahmen zum Management von Cybersicherheitsrisiken überwacht und gemessen werden sollen, einschließlich der Prozesse und Kontrollen;

(b) die Methoden für die Überwachung, Messung, Analyse und Bewertung, soweit zutreffend, um gültige Ergebnisse zu gewährleisten;

(c) wann die Überwachung und Messung durchgeführt werden soll;

(d) der für die Überwachung und Messung der Wirksamkeit der Maßnahmen zum Management der Cybersicherheitsrisiken verantwortlich ist;

(e) wenn die Ergebnisse der Überwachung und Messung analysiert und bewertet werden sollen;

(f) der diese Ergebnisse zu analysieren und zu bewerten hat.

7.1.3. Die betreffenden Stellen überprüfen und aktualisieren die Grundsätze und Verfahren gegebenenfalls in geplanten Abständen sowie bei bedeutenden Vorfällen oder wesentlichen Änderungen der Abläufe oder Risiken.

8. GRUNDLEGENDE PRAKTIKEN DER CYBERHYGIENE UND SICHERHEITSSCHULUNGEN (ARTIKEL 21 ABSATZ 2), BUCHSTABE G) DER RICHTLINIE (EU) 2022/2555)

8.1. Bewusstseinsbildung und grundlegende Praktiken der Cyber-Hygiene

8.1.1. Für die Zwecke von Artikel 21 Absatz 2 Buchstabe g der Richtlinie (EU) 2022/2555 stellen die betreffenden Einrichtungen sicher, dass ihre Mitarbeiter sich der Risiken bewusst sind, über die Bedeutung der Cybersicherheit informiert sind und Praktiken der Cyberhygiene anwenden.

8.1.2. Die betreffenden Stellen bieten allen Mitarbeitern, einschließlich der Mitglieder der Leitungsorgane, ein Sensibilisierungsprogramm an, das Folgendes umfasst

(a) über einen längeren Zeitraum geplant werden, so dass die Aktivitäten wiederholt werden und neue Mitarbeiter einbeziehen;

(b) im Einklang mit der Netz- und Informationssicherheitspolitik, den themenspezifischen Strategien und den einschlägigen Verfahren für die Netz- und Informationssicherheit festgelegt werden;

(c) die bestehenden Maßnahmen zum Risikomanagement im Bereich der

Cybersicherheit, Kontaktstellen und Ressourcen für zusätzliche Informationen und Beratung in Fragen der Cybersicherheit sowie Praktiken der Cyberhygiene für die Nutzer.

8.1.3. Das Sensibilisierungsprogramm wird auf seine Wirksamkeit hin überprüft, aktualisiert und in geplanten Abständen angeboten, wobei Änderungen der Cyberhygiene-Praktiken sowie die aktuelle Bedrohungslage und die Risiken für die betreffenden Einrichtungen berücksichtigt werden.

8.2. Sicherheitsschulung

8.2.1. Die betreffenden Stellen stellen sicher, dass Mitarbeiter, deren Aufgaben sicherheitsrelevante Fähigkeiten und Fachkenntnisse erfordern, Schulungen zur Netz- und Informationssystemsicherheit erhalten.

8.2.2. Die betreffenden Stellen müssen ein Schulungsprogramm im Einklang mit der Netz- und Informationssicherheitspolitik, den themenspezifischen Politiken und anderen einschlägigen Verfahren zur Netz- und Informationssicherheit aufstellen, umsetzen und anwenden, in dem der Schulungsbedarf für bestimmte Rollen und Positionen anhand von Kriterien festgelegt ist.

8.2.3. Die unter Punkt 8.2.1. genannte Schulung muss für die Tätigkeit des Mitarbeiters relevant sein, und ihre Wirksamkeit ist zu bewerten. Die Schulung muss die bestehenden Sicherheitsmaßnahmen berücksichtigen und Folgendes abdecken:

(a) regelmäßige und dokumentierte Anweisungen für die sichere Konfiguration und den sicheren Betrieb des Netzes und der Informationssysteme, einschließlich mobiler Geräte;

(b) regelmäßige und dokumentierte Unterrichtung über bekannte Cyber-Bedrohungen;

(c) regelmäßige und dokumentierte Schulung des Verhaltens beim Auftreten sicherheitsrelevanter Ereignisse.

8.2.4. Die zuständigen Stellen führen Schulungen für Mitarbeiter durch, die in neue Positionen oder Funktionen wechseln, die sicherheitsrelevante Fähigkeiten und Fachkenntnisse erfordern.

8.2.5. Das Programm wird in regelmäßigen Abständen aktualisiert und durchgeführt, wobei die geltenden Richtlinien und Vorschriften, die zugewiesenen Rollen und Zuständigkeiten sowie bekannte Cyber-Bedrohungen und technologische Entwicklungen berücksichtigt werden.

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

9.1.1. Für die Zwecke von Artikel 21 Absatz 2 Buchstabe h der Richtlinie (EU) 2022/2555 müssen die betreffenden Stellen eine Politik und Verfahren in Bezug auf die Kryptografie einführen, umsetzen und anwenden, um einen angemessenen und wirksamen Einsatz der Kryptografie zum Schutz der Vertraulichkeit, Authentizität und Integrität von Informationen im Einklang mit der Informationsklassifizierung der betreffenden Stellen und den Ergebnissen der Risikobewertung sicherzustellen.

9.1.2. In der Politik und den Verfahren gemäß Nummer 9.1 wird festgelegt:

(a) im Einklang mit der Klassifizierung der Vermögenswerte der betreffenden Einrichtungen die Art, Stärke und Qualität der kryptografischen Maßnahmen, die zum Schutz der Vermögenswerte der betreffenden Einrichtungen erforderlich sind;

(b) auf der Grundlage von Buchstabe a die anzunehmenden Protokolle sowie die

kryptografischen Algorithmen, die Verschlüsselungsstärke, die kryptografischen Lösungen und die Verwendungspraktiken, die für die Verwendung in den Einrichtungen zu genehmigen und vorzuschreiben sind, gegebenenfalls nach einem Konzept der kryptografischen Flexibilität;

(c) der Ansatz der betreffenden Stellen für das Schlüsselmanagement, einschließlich der Methoden für Folgendes:

(i) Erzeugung von Schlüssel für verschiedene kryptografische Systeme und Anwendungen;

(ii) Ausstellung und Erhalt von Zertifikaten mit öffentlichem Schlüssel;

(iii) die Verteilung von Schlüsseln an die vorgesehenen Stellen, einschließlich der Frage, wie Schlüssel nach Erhalt aktiviert werden;

(iv) Speicherung von Schlüsseln, einschließlich der Frage, wie autorisierte Benutzer Zugang zu den Schlüsseln erhalten;

(v) das Ändern oder Aktualisieren von Schlüsseln, einschließlich der Regeln, wann und wie die Schlüssel zu ändern sind;

(vi) Umgang mit kompromittierten Schlüsseln;

(vii) Widerruf von Schlüsseln, einschließlich der Frage, wie man Schlüssel zurückziehen oder deaktivieren kann;

(viii) Wiederherstellung von verlorenen oder beschädigten Schlüsseln;

(ix) Sichern oder Archivieren von Schlüsseln;

(x) Schlüssel zu zerstören;

(xi) Protokollierung und Prüfung der wichtigsten verwaltungsbezogenen Aktivitäten;

(xii) Festlegung von Aktivierungs- und Deaktivierungsdaten für Schlüssel, um sicherzustellen, dass die Schlüssel nur für den angegebenen Zeitraum gemäß den Regeln der Organisation für die Schlüsselverwaltung verwendet werden können;

(xiii) Bearbeitung rechtlicher Anträge auf Zugang zu kryptografischen Schlüsseln.

9.1.3. Die betreffenden Stellen überprüfen und aktualisieren gegebenenfalls ihre Grundsätze und Verfahren in geplanten Abständen unter Berücksichtigung des Stands der Technik im Bereich der Kryptografie.

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

10.1. Sicherheit der Humanressourcen

10.1.1. Für die Zwecke von Artikel 21 Absatz 2 Buchstabe i der Richtlinie (EU) 2022/2555 stellen die betreffenden Stellen sicher, dass ihre Mitarbeiter und direkten Zulieferer und Dienstleister, soweit zutreffend, ihre Sicherheitsverantwortung verstehen, nachweisen und sich dazu verpflichten, je nach den angebotenen Diensten und der Tätigkeit und im Einklang mit der Politik der betreffenden Stellen für die Sicherheit der Netz- und Informationssysteme.

10.1.2. Die in Nummer 10.1.1 genannte Anforderung muss Folgendes umfassen:

(a) Mechanismen, mit denen sichergestellt wird, dass alle Mitarbeiter, direkten Zulieferer und Dienstleister, soweit zutreffend, die Standard-Cyber-

Hygiene-Praktiken verstehen und befolgen, die die Unternehmen gemäß Punkt 8.1. anwenden;

(b) Mechanismen, die sicherstellen, dass alle Benutzer mit administrativem oder privilegiertem Zugang ihre Rollen, Verantwortlichkeiten und Befugnisse kennen und befolgen;

(c) Mechanismen, die sicherstellen, dass die Leitungsorgane ihre Rolle, Zuständigkeiten und Befugnisse in Bezug auf die Sicherheit der Netze und Informationssysteme verstehen;

(d) Mechanismen für die Einstellung von qualifiziertem Personal, wie z. B. Referenzprüfungen, Überprüfungsverfahren, Validierung von Zertifizierungen oder schriftliche Tests.

10.1.3. Die zuständigen Stellen überprüfen in geplanten Abständen, mindestens jedoch einmal jährlich, die Zuweisung von Personal zu bestimmten Aufgaben gemäß Nummer 1.2 sowie die Bindung von Ressourcen. Sie aktualisieren die Zuweisung erforderlichenfalls.

10.2. Hintergrundkontrollen

10.2.1. Die betreffenden Stellen führen bei ihren Mitarbeitern, direkten Zulieferern und Dienstleistern Zuverlässigkeitsüberprüfungen durch, sofern dies für deren Rolle, Aufgaben und Befugnisse erforderlich ist.

10.2.2. Für die Zwecke von Punkt 10.2.1. müssen die betreffenden Stellen:

(a) Kriterien aufstellen, die festlegen, welche Rollen, Verantwortlichkeiten und Befugnisse nur von Personen ausgeübt werden dürfen, die einer Zuverlässigkeitsüberprüfung unterzogen wurden;

(b) eine Überprüfung des Hintergrunds dieser Personen vorzunehmen, bevor sie diese Rollen, Verantwortlichkeiten und Befugnisse ausüben, wobei die geltenden Gesetze, Vorschriften und ethischen Grundsätze im Verhältnis zu den geschäftlichen Anforderungen, der Klassifizierung der Informationen und des Netzes und der Informationssysteme, auf die zugegriffen werden soll, sowie den wahrgenommenen Risiken zu berücksichtigen sind.

10.2.3. Die betreffenden Stellen überprüfen und aktualisieren die Politik in geplanten Abständen und bringen sie gegebenenfalls auf den neuesten Stand.

10.3. Verfahren bei Beendigung oder Wechsel des Beschäftigungsverhältnisses

10.3.1. Die betreffenden Stellen stellen sicher, dass die Zuständigkeiten und Pflichten im Bereich der Netz- und Informationssystemsicherheit, die auch nach Beendigung oder Wechsel des Beschäftigungsverhältnisses ihrer Mitarbeiter gelten, festgelegt, durchgesetzt, mitgeteilt und verstanden werden.

10.3.2. Für die Zwecke von Punkt 10.3.1. müssen die betreffenden Stellen:

(a) in die Beschäftigungsbedingungen, den Arbeitsvertrag oder die Vereinbarung die Verantwortlichkeiten und Pflichten aufnehmen, die auch nach Beendigung des Beschäftigungsverhältnisses oder des Arbeitsvertrags noch gelten, wie z. B. Vertraulichkeitsklauseln;

(b) eine Zugangskontrollpolitik einführen, die sicherstellt, dass die Zugangsrechte bei Beendigung des Arbeitsverhältnisses oder bei einem Wechsel der Person entsprechend geändert werden;

(c) sicherstellen, dass der Arbeitnehmer nach einem Wechsel des Arbeitsplatzes die neuen Aufgaben erfüllen kann.

10.4. Disziplinarverfahren

10.4.1. Die zuständigen Stellen müssen ein Disziplinarverfahren für den Umgang mit Verstößen gegen die Sicherheitsrichtlinien für Netze und Informationssysteme einführen, mitteilen und aufrechterhalten. Das Verfahren muss den einschlägigen rechtlichen, gesetzlichen, vertraglichen und geschäftlichen Anforderungen Rechnung tragen.

10.4.2. Die zuständigen Stellen überprüfen und aktualisieren gegebenenfalls das Disziplinarverfahren in geplanten Abständen sowie bei Bedarf aufgrund rechtlicher Änderungen oder erheblicher Veränderungen bei den Tätigkeiten oder Risiken.

11. ZUGANGSKONTROLLE (ARTIKEL 21 ABSATZ 2 BUCHSTABE I DER RICHTLINIE (EU) 2022/2555)

11.1. Zugangskontrollpolitik

11.1.1. Für die Zwecke von Artikel 21 Absatz 2 Buchstabe i der Richtlinie (EU) 2022/2555 müssen die betreffenden Stellen logische und physische Zugangskontrollstrategien für den Zugang von Personen und Prozessen zu Netz- und Informationssystemen auf der Grundlage von Geschäftsanforderungen sowie von Sicherheitsanforderungen an Netz- und Informationssysteme festlegen, dokumentieren und umsetzen.

11.1.2. Die unter Ziffer 11.1.1. genannten Maßnahmen müssen:

(a) den Zugang von Personen, einschließlich Mitarbeitern, Besuchern und externen Stellen wie Lieferanten und Dienstleistern;

(b) den Zugang durch Netz- und Informationssystemprozesse zu adressieren;

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

11.1.3. Die betreffenden Stellen überprüfen und aktualisieren die Strategien gegebenenfalls in geplanten Abständen sowie bei bedeutenden Vorfällen oder wesentlichen Änderungen der Tätigkeiten oder Risiken.

11.2. Verwaltung der Zugangsrechte

11.2.1. Die betreffenden Stellen gewähren, ändern, entfernen und dokumentieren die Zugriffsrechte auf Netz- und Informationssysteme gemäß der in Nummer 11.1 genannten Zugriffskontrollpolitik.

11.2.2. Die betreffenden Stellen müssen:

(a) Zuweisung und Entzug von Zugriffsrechten auf der Grundlage der Grundsätze "Kenntnisnahme erforderlich", "geringstmögliches Recht" und "Aufgabentrennung";

(b) sicherstellen, dass die Zugangsrechte bei Beendigung oder Wechsel des Beschäftigungsverhältnisses entsprechend geändert werden;

(c) sicherstellen, dass der Zugang zu den Netz- und Informationssystemen von ihrem Eigentümer genehmigt wird;

(d) sicherstellen, dass die Zugangsrechte den Zugang von Dritten, wie Lieferanten

und Dienstleistern, angemessen berücksichtigen, insbesondere durch Begrenzung des Umfangs und der Dauer der Zugangsrechte;

(e) ein Register der erteilten Zugriffsrechte zu führen;

(f) bei der Verwaltung der Zugriffsrechte die Protokollierung anwenden.

11.2.3. Die zuständigen Stellen überprüfen die Zugriffsrechte in geplanten Abständen und ändern sie aufgrund organisatorischer Änderungen. Die zuständigen Stellen dokumentieren die Ergebnisse der Überprüfung einschließlich der erforderlichen Änderungen der Zugriffsrechte.

11.3. Privilegierte Konten und Systemverwaltungskonten

11.3.1. Die betreffenden Stellen unterhalten Richtlinien für die Verwaltung von privilegierten Konten und Systemverwaltungskonten.

11.3.2. Die unter Ziffer 11.3.1. genannten Maßnahmen müssen:

(a) Einführung einer starken Identifizierung, Authentifizierung, wie z. B. Multi-Faktor-Authentifizierung, und Autorisierungsverfahren für privilegierte Konten und Systemverwaltungskonten;

(b) bestimmte Konten einzurichten, die ausschließlich für die Systemadministration verwendet werden, z. B. für die Installation, Konfiguration, Verwaltung oder Wartung;

(c) die Privilegien für die Systemverwaltung so weit wie möglich zu individualisieren und einzuschränken,

(d) dafür sorgen, dass Systemverwaltungskonten nur für die Verbindung zu Systemverwaltungssystemen verwendet werden.

11.3.3. Die zuständigen Stellen überprüfen die Zugriffsrechte von privilegierten Konten und Systemadministrationskonten in geplanten Abständen und passen sie an organisatorische Änderungen an; sie dokumentieren die Ergebnisse der Überprüfung, einschließlich der erforderlichen Änderungen der Zugriffsrechte.

11.4. Verwaltungssysteme

11.4.1. Die zuständigen Stellen beschränken und kontrollieren die Nutzung von Systemverwaltungssystemen.

11.4.2. Zu diesem Zweck müssen die betreffenden Einrichtungen:

(a) Systemverwaltungssysteme nur für die Systemverwaltung und nicht für andere Tätigkeiten zu verwenden;

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

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

11.5. Identifizierung

11.5.1. Die zuständigen Stellen verwalten den gesamten Lebenszyklus der Identitäten von Netz- und Informationssystemen und ihrer Nutzer.

11.5.2. Zu diesem Zweck müssen die betreffenden Einrichtungen:

(a) Einrichtung eindeutiger Identitäten für Netz- und Informationssysteme und deren

Benutzer;

(b) die Identität der Nutzer mit einer einzigen Person verknüpfen;

(c) Überwachung der Identitäten von Netz- und Informationssystemen;

(d) die Protokollierung auf die Verwaltung von Identitäten anwenden.

11.5.3. Die zuständigen Stellen lassen Identitäten, die mehreren Personen zugewiesen sind, wie z. B. gemeinsame Identitäten, nur dann zu, wenn sie aus geschäftlichen oder betrieblichen Gründen erforderlich sind und einem ausdrücklichen Genehmigungsverfahren und einer entsprechenden Dokumentation unterliegen.

11.6. Authentifizierung

11.6.1. Die betreffenden Stellen setzen sichere Authentifizierungsverfahren und -technologien auf der Grundlage von Zugangsbeschränkungen und der Politik der Zugangskontrolle ein.

11.6.2. Zu diesem Zweck müssen die betreffenden Einrichtungen:

(a) sicherstellen, dass die Stärke der Authentifizierung der Klassifizierung des Objekts, auf das zugegriffen werden soll, angemessen ist;

(b) die Zuteilung an Benutzer und die Verwaltung geheimer Authentifizierungsinformationen durch ein Verfahren zu kontrollieren, das die Vertraulichkeit der Informationen gewährleistet, einschließlich der Beratung des Personals über den angemessenen Umgang mit Authentifizierungsinformationen;

(c) die Änderung der Authentifizierungsdaten bei der ersten Anmeldung und bei Verdacht auf Weitergabe der Daten an eine unbefugte Person verlangen;

(d) die Rücksetzung der Authentifizierungsdaten und die Sperrung von Benutzern nach einer vordefinierten Anzahl von erfolglosen Anmeldeversuchen verlangen;

(e) inaktive Sitzungen nach einer vordefinierten Zeit der Inaktivität zu beenden; und

(f) für den Zugriff auf privilegierte oder administrative Konten separate Anmeldedaten benötigen.

11.6.3. Die betreffenden Stellen verwenden Authentifizierungsmethoden, die dem neuesten Stand der Technik entsprechen, entsprechend dem bewerteten Risiko und der Klassifizierung des Vermögensgegenstands, auf den zugegriffen werden soll, sowie eindeutige Authentifizierungsinformationen.

11.6.4. Die betreffenden Stellen überprüfen die Identitäten regelmäßig und deaktivieren sie unverzüglich, wenn sie nicht mehr benötigt werden.

11.7. Multi-Faktor-Authentifizierung

11.7.1. Die betreffenden Stellen stellen sicher, dass die Nutzer beim Zugang zum Netz und zu den Informationssystemen der Stellen durch mehrere Authentifizierungsfaktoren oder kontinuierliche Authentifizierungsmechanismen authentifiziert werden, gegebenenfalls in Übereinstimmung mit der Klassifizierung des Gutes, auf das zugegriffen werden soll.

11.7.2. Die zuständigen Stellen stellen sicher, dass die Stärke der Authentifizierung der Klassifizierung des Vermögenswertes, auf den zugegriffen werden soll, angemessen ist.

12. VERMÖGENSVERWALTUNG (ARTIKEL 21 ABSATZ 2 BUCHSTABE I) DER RICHTLINIE (EU) 2022/2555)

12.1. Klassifizierung der Vermögenswerte

12.1.1. Für die Zwecke von Artikel 21 Absatz 2 Buchstabe i der Richtlinie (EU) 2022/2555 legen die betreffenden Stellen für alle Informationen und Vermögenswerte, die in den Anwendungsbereich ihrer Netze und Informationssysteme fallen, Geheimhaltungsgrade für das erforderliche Schutzniveau fest.

12.1.2. Für die Zwecke von Punkt 12.1.1. müssen die betreffenden Stellen:

(a) ein System von Geheimhaltungsgraden für Informationen und Vermögenswerte festzulegen;

(b) alle Informationen und Vermögenswerte auf der Grundlage der Anforderungen an Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit einer Klassifizierungsstufe zuordnen, um den erforderlichen Schutz je nach Sensibilität, Kritikalität, Risiko und Geschäftswert anzugeben,

(c) die Verfügbarkeitsanforderungen der Informationen und Anlagen mit den in ihren Geschäfts- und Notfallplänen festgelegten Bereitstellungs- und Wiederherstellungszielen abzustimmen.

12.1.3. Die zuständigen Stellen überprüfen regelmäßig die Geheimhaltungsgrade von Informationen und Vermögenswerten und aktualisieren sie gegebenenfalls.

12.2. Umgang mit Informationen und Vermögenswerten

12.2.1. Die betreffenden Stellen legen eine Politik für den ordnungsgemäßen Umgang mit Informationen und Vermögenswerten gemäß ihrer Netz- und Informationssicherheitspolitik fest, setzen diese um und wenden sie an, und teilen sie allen mit, die Informationen und Vermögenswerte nutzen oder damit umgehen.

12.2.2. Die Politik muss:

(a) den gesamten Lebenszyklus der Informationen und Vermögenswerte abdecken, einschließlich Erwerb, Nutzung, Speicherung, Transport und Entsorgung;

(b) Anweisungen für die sichere Verwendung, die sichere Aufbewahrung, den sicheren Transport und die unwiederbringliche Löschung und Vernichtung der Informationen und Vermögenswerte geben;

(c) vorsehen, dass Ausrüstungen, Hardware, Software und Daten nur nach Genehmigung durch von den Leitungsorganen gemäß den Richtlinien ermächtigte Stellen in externe Räumlichkeiten verbracht werden dürfen,

(d) vorsehen, dass die Übermittlung auf sichere Art und Weise entsprechend der Art der zu übermittelnden Vermögenswerte oder Informationen erfolgen muss.

12.2.3. Die betreffenden Stellen überprüfen und aktualisieren die Politik gegebenenfalls in geplanten Abständen und bei bedeutenden Vorfällen oder wesentlichen Änderungen der Tätigkeiten oder Risiken.

12.3. Richtlinie für Wechseldatenträger

12.3.1. Die betreffenden Stellen müssen eine Strategie für die Verwaltung von Wechseldatenträgern festlegen, umsetzen und anwenden und diese ihren Mitarbeitern und Dritten mitteilen, die in den Räumlichkeiten der betreffenden Stellen oder an anderen Orten, an denen die Wechseldatenträger mit dem Netz und den Informationssystemen der betreffenden Stellen verbunden sind, mit Wechseldatenträgern umgehen.

12.3.2. Die Politik muss:

(a) ein technisches Verbot des Anschlusses von Wechseldatenträgern vorsehen, es sei denn, es gibt einen organisatorischen Grund für deren Verwendung;

(b) vorsehen, dass die Selbstausführung von solchen Datenträgern deaktiviert und die Datenträger auf bösartigen Code gescannt werden, bevor sie auf den Systemen der Einrichtungen verwendet werden;

(c) Maßnahmen zur Kontrolle und zum Schutz von tragbaren Speichermedien, die Daten enthalten, während des Transports und der Lagerung vorzusehen;

(d) gegebenenfalls Maßnahmen für den Einsatz kryptografischer Techniken zum Schutz von Informationen auf Wechseldatenträgern vorsehen.

12.3.3. Die betreffenden Stellen überprüfen und aktualisieren die Politik gegebenenfalls in geplanten Abständen und bei bedeutenden Vorfällen oder wesentlichen Änderungen der Tätigkeiten oder Risiken.

12.4. Bestandsaufnahme der Vermögenswerte

12.4.1. Die betreffenden Stellen erstellen und führen ein vollständiges, genaues, aktuelles und konsistentes Inventar ihrer Vermögenswerte. Sie halten Änderungen an den Einträgen im Inventar in nachvollziehbarer Weise fest.

12.4.2. Die Granularität des Bestandsverzeichnisses der Vermögenswerte muss den Erfordernissen der betreffenden Stellen entsprechen. Das Inventar muss Folgendes umfassen:

(a) die Liste der Operationen und Dienstleistungen und ihre Beschreibung,

(b) die Liste der Netz- und Informationssysteme und anderer zugehöriger Vermögenswerte, die den Betrieb und die Dienste der Einrichtungen unterstützen.

12.4.3. Die zuständigen Stellen überprüfen und aktualisieren das Inventar und ihre Vermögenswerte regelmäßig und dokumentieren die Historie der Änderungen.

12.5. Rückgabe oder Löschung von Vermögenswerten bei Beendigung des Beschäftigungsverhältnisses

Die betreffenden Stellen müssen Verfahren einrichten, umsetzen und anwenden, die sicherstellen, dass ihre Vermögenswerte, die sich in der Obhut des Personals befinden, bei Beendigung des Beschäftigungsverhältnisses zurückgegeben werden, und die Hinterlegung und Rückgabe dieser Vermögenswerte dokumentieren.

13. UMWELT UND PHYSISCHE SICHERHEIT (ARTIKEL 21 ABSATZ 2 BUCHSTABEN C, E UND I)

13.1. Unterstützende Dienstprogramme

13.1.1. Für die Zwecke von Artikel 21 Absatz 2 Buchstabe c der Richtlinie (EU) 2022/2555 verhindern die betreffenden Stellen den Verlust, die Beschädigung oder die Beeinträchtigung von Netz- und Informationssystemen oder die Unterbrechung ihres Betriebs aufgrund des Ausfalls oder der Unterbrechung von Hilfsdiensten.

13.1.2. Zu diesem Zweck müssen die betreffenden Einrichtungen:

(a) Schutz von Einrichtungen vor Stromausfällen und anderen Störungen, die durch Ausfälle von Versorgungseinrichtungen wie Strom, Telekommunikation, Wasserversorgung, Gas, Abwasser, Lüftung und Klimaanlagen verursacht werden;

(b) gegebenenfalls die Nutzung von Redundanz bei den Versorgungsdiensten in Betracht ziehen;

(c) Schutz der Versorgungsdienste für Strom und Telekommunikation, die Daten transportieren oder Netz- und Informationssysteme versorgen, vor Abhören und Beschädigung;

(d) die unter Buchstabe c genannten Versorgungsdienste zu überwachen und dem zuständigen internen oder externen Personal Ereignisse zu melden, die außerhalb des zulässigen Kontrollbereichs gemäß Nummer 13.2.2 Buchstabe b liegen und die Versorgungsdienste betreffen;

(e) gegebenenfalls Verträge für die Notversorgung mit entsprechenden Dienstleistungen abschließen, z. B. für den Brennstoff für die Notstromversorgung;

(f) die ständige Funktionsfähigkeit zu gewährleisten, die Versorgung mit den für den Betrieb der angebotenen Dienstleistung erforderlichen Netz- und Informationssystemen zu überwachen, zu warten und zu prüfen, insbesondere die Stromversorgung, die Temperatur- und Feuchtigkeitskontrolle, die Telekommunikation und die Internetverbindung.

Für die Zwecke von Buchstabe d dokumentieren, kommunizieren und stellen die betreffenden Stellen Strategien und Anweisungen zur Verfügung, die die Wartung, insbesondere die Fernwartung, Löschung, Aktualisierung und Wiederverwendung von Vermögenswerten, die Informationen verarbeiten, beschreiben, einschließlich solcher in ausgelagerten Räumlichkeiten oder durch externes Personal. Die Stellen statten Vermögenswerte, die Informationen verarbeiten, mit automatischen Ausfallsicherungen und anderen Redundanzen aus.

13.1.3. Die betreffenden Stellen testen, überprüfen und aktualisieren die Schutzmaßnahmen gegebenenfalls regelmäßig oder nach bedeutenden Vorfällen oder wesentlichen Änderungen der Tätigkeiten oder Risiken.

13.2. Schutz vor physischen und ökologischen Bedrohungen

13.2.1. Für die Zwecke von Artikel 21 Absatz 2 Buchstabe e der Richtlinie (EU) 2022/2555 müssen die betreffenden Stellen die Folgen von Ereignissen verhindern oder verringern, die auf physische und ökologische Bedrohungen wie Naturkatastrophen und andere absichtliche oder unabsichtliche Bedrohungen zurückzuführen sind.

13.2.2. Zu diesem Zweck müssen die betreffenden Einrichtungen:

(a) auf der Grundlage der Ergebnisse der Risikobewertung Schutzmaßnahmen gegen physische und ökologische Bedrohungen zu konzipieren und umzusetzen;

(b) Festlegung von Mindest- und Höchstwerten für die Kontrolle von physischen und umweltbedingten Bedrohungen;

(c) Überwachung der Umweltparameter und Meldung von Ereignissen außerhalb der unter Buchstabe b genannten Mindest- und Höchstkontrollschwellen.

13.2.3. Die betreffenden Stellen testen, überprüfen und aktualisieren gegebenenfalls die Schutzmaßnahmen gegen physische und umweltbedingte Bedrohungen regelmäßig oder nach signifikanten Vorfällen oder signifikanten Änderungen der Tätigkeiten oder Risiken.

13.3. Perimeter- und physische Zugangskontrolle

13.3.1. Für die Zwecke von Artikel 21 Absatz 2 Buchstabe i der Richtlinie (EU) 2022/2555 verhindern und überwachen die betreffenden Stellen den unbefugten physischen Zugang zu ihren Netz- und Informationssystemen sowie deren Beschädigung und Störung.

13.3.2. Zu diesem Zweck müssen die betreffenden Einrichtungen:

(a) auf der Grundlage der Risikobewertung Sicherheitsabgrenzungen festzulegen und zu verwenden, um Bereiche zu schützen, in denen sich Netz- und Informationssysteme und andere zugehörige Vermögenswerte befinden;

(b) die unter Buchstabe a genannten Bereiche durch geeignete Zugangskontrollen und Zugangspunkte zu schützen;

(c) Gestaltung und Umsetzung der physischen Sicherheit von Büros, Räumen und Anlagen,

(d) ihre Räumlichkeiten ständig auf unbefugten physischen Zugang überwachen.

13.3.3. Die betreffenden Stellen testen, überprüfen und aktualisieren gegebenenfalls die Maßnahmen zur physischen Zugangskontrolle regelmäßig oder nach bedeutenden Zwischenfällen oder wesentlichen Änderungen der Abläufe oder Risiken.