Lizenzbestimmungen

DURCHFÜHRUNGSVERORDNUNG (EU) 2024/2690

...DER KOMMISSION vom 17. Oktober 2024

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

(Text von 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 Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie) (1), insbesondere auf Artikel 21 Absatz 5 Unterabsatz 1 und Artikel 23 Absatz 11 Unterabsatz 2,

in Erwägung nachstehender Gründe:

1

Text	Umsetzung in der VdS 10100
In dieser Verordnung werden in Bezug auf die von Artikel 3 der Richtlinie (EU) 2022/2555 erfassten DNS-Diensteanbieter, TLD-Namenregister, Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltszustellnetzen, Anbieter verwalteter Dienste, Anbieter verwalteter Sicherheitsdienste, Anbieter von Online-Marktplätzen, Online-Suchmaschinen und Plattformen für Dienste sozialer Netzwerke und Vertrauensdiensteanbieter (im Folgenden „betreffende Einrichtungen“) die technischen und methodischen Anforderungen der in Artikel 21 Absatz 2 der Richtlinie (EU) 2022/2555 genannten Maßnahmen festgelegt und die Fälle präzisiert, in denen ein Sicherheitsvorfall gemäß Artikel 23 Absatz 3 der Richtlinie (EU) 2022/2555 als erheblich anzusehen ist.	• Obwohl sich die Verordnung an spezielle Organisationen richtet, gibt sie Hinweise wie NIS-2 zu interpretieren ist. Aus diesem Grund gleichen wir die Vorgaben der Verordnung gegen die Prinzipien, Strukturen und Maßnahmen der VdS 10100 in der aktuellen Version (0.6.5) ab.

2

Text	Umsetzung in der VdS 10100
Angesichts des grenzüberschreitenden Charakters ihrer Tätigkeiten und zur Gewährleistung eines kohärenten Rahmens für Vertrauensdiensteanbieter sollte in dieser Verordnung in Bezug auf Vertrauensdiensteanbieter neben der Festlegung der technischen und methodischen Anforderungen der Risikomanagementmaßnahmen im Bereich der Cybersicherheit ebenfalls präzisiert werden, in welchen Fällen ein Sicherheitsvorfall als erheblich anzusehen ist.	• Keine Maßnahme.

3

Text	Umsetzung in der VdS 10100
Nach Artikel 21 Absatz 5 Unterabsatz 3 der Richtlinie (EU) 2022/2555 beruhen die technischen und methodischen Anforderungen der im Anhang dieser Verordnung festgelegten Risikomanagementmaßnahmen im Bereich der Cybersicherheit auf europäischen und internationalen Normen wie ISO/IEC 27001, ISO/IEC 27002 und ETSI EN 319401 sowie auf technischen Spezifikationen wie CEN/TS 18026:2024, die für die Sicherheit von Netz- und Informationssystemen von Belang sind.	• Die VdS 10100 orientiert sich an den Normen ISO/IEC 27001 und ISO/IEC 27002. • ETSI EN 319401 („Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers“) richtet sich an Vertrauensdiensteanbieter. • CEN/TS 18026:2024 definiert ein „set of cybersecurity requirements for cloud services“ und ist damit nur relevant für Anbieter von Cloud Services. ◦ Sollte als Empfehlung in die VdS 10100 aufgenommen werden (Anforderungen an wichtige/kritische Lieferanten von Cloud-Diensten).

4

Text	Umsetzung in der VdS 10100
Bezüglich der Umsetzung und Anwendung der technischen und methodischen Anforderungen der im Anhang dieser Verordnung festgelegten Risikomanagementmaßnahmen im Bereich der Cybersicherheit sollten — im Einklang mit dem Grundsatz der Verhältnismäßigkeit — die unterschiedlichen Risikoexpositionen der betreffenden Einrichtungen wie Kritikalität der betreffenden Einrichtung, Risiken, denen sie ausgesetzt sind, Größe und Struktur der betreffenden Einrichtung sowie Wahrscheinlichkeit des Eintretens von Sicherheitsvorfällen und deren Schwere, einschließlich ihrer gesellschaftlichen und wirtschaftlichen Auswirkungen, bei der Einhaltung der im Anhang dieser Verordnung festgelegten technischen und methodischen Anforderungen der Risikomanagementmaßnahmen im Bereich der Cybersicherheit gebührend berücksichtigt werden.	• Ist vollständig umgesetzt in „Anhang A Verfahren und Risikomanagement → A.2 Risikomanagement → A.2.4 Risikoanalyse“

5

Text	Umsetzung in der VdS 10100
Können die betreffenden Einrichtungen einige der technischen und methodischen Anforderungen der Risikomanagementmaßnahmen im Bereich der Cybersicherheit wegen ihrer Größe nicht umsetzen, so sollten sie — im Einklang mit dem Grundsatz der Verhältnismäßigkeit — die Möglichkeit haben, andere Ausgleichsmaßnahmen zu ergreifen, die geeignet sind, den Zweck dieser Anforderungen zu erreichen.	• Beschreibt ein Kernprinzip der VdS 10100: Wir stellen ein Paket an Schutzmaßnahmen zur Verfügung, die mithilfe einer Risikoidentifikation, -analyse und -behandlung abgeschwächt werden können.
Bei der Festlegung der Rollen, Verantwortlichkeiten und Weisungsbefugnisse in Bezug auf die Sicherheit der Netz- und Informationssysteme innerhalb der betreffenden Einrichtung könnte es für Kleinstunternehmen schwierig sein, widerstrebende Pflichten und sich widersprechende Verantwortlichkeitsbereiche zu trennen.	• Umgesetzt in 4.2.3 Funktionstrennung • Verantwortlichkeiten können delegiert werden (Flexibilität), die Rollentrennung wird gefordert, kann aber abgeschwächt werden, wenn sie nur mit einem unverhältnismäßig hohen Aufwand durchführbar ist.
Solche Einrichtungen sollten Ausgleichsmaßnahmen wie eine gezielte Beaufsichtigung durch ihr Management oder eine verstärkte Überwachung und Protokollierung in Betracht ziehen können.	• Umgesetzt in 4.2.3 Funktionstrennung • Wenn die Rollentrennung nicht umgesetzt werden kann, müssen andere Maßnahmen wie Überwachung von Tätigkeiten, Kontrollen oder Leitungsaufsicht umgesetzt werden.

6

Text	Umsetzung in der VdS 10100
Bestimmte technische und methodische Anforderungen, die im Anhang dieser Verordnung festgelegt sind, sollten von den betreffenden Einrichtungen angewandt werden, soweit dies angemessen, anwendbar oder durchführbar ist.	•
Hält es eine betreffende Einrichtung es für nicht angemessen, nicht anwendbar oder nicht durchführbar, bestimmte technische und methodische Anforderungen, die im Anhang dieser Verordnung festgelegt sind, anzuwenden, sollte sie ihre diesbezügliche Begründung in verständlicher Weise dokumentieren.	•
Die zuständigen nationalen Behörden können bei der Beaufsichtigung eine angemessene Frist berücksichtigen, die betreffende Einrichtungen benötigen, um die technischen und methodischen Anforderungen der Risikomanagementmaßnahmen im Bereich der Cybersicherheit umzusetzen.	• Betrifft nicht die VdS 10100.

7

Text	Umsetzung in der VdS 10100
Die ENISA oder die gemäß der Richtlinie (EU) 2022/2555 zuständigen nationalen Behörden können die betreffenden Einrichtungen bei der Ermittlung, Analyse und Bewertung von Risiken zwecks Umsetzung der technischen und methodischen Anforderungen an die Einrichtung und Aufrechterhaltung eines geeigneten Risikomanagementrahmens anleitend unterstützen.	• Betrifft nicht die VdS 10100.
Eine solche Anleitung kann sich insbesondere auf nationale und sektorale Risikobewertungen sowie spezifische Risikobewertungen für eine bestimmte Art von Einrichtung beziehen.	•
Die Anleitung kann auch Instrumente oder Vorlagen für die Entwicklung eines Risikomanagementrahmens auf der Ebene der betreffenden Einrichtungen umfassen.	•
Die betreffenden Einrichtungen können auch mit Rahmen, Anleitungen oder anderen Mechanismen, die im nationalen Recht der Mitgliedstaaten vorgesehen sind, sowie mit einschlägigen europäischen und internationalen Normen beim Nachweis der Einhaltung dieser Durchführungsverordnung unterstützt werden.	•
Darüber hinaus können die ENISA oder die gemäß der Richtlinie (EU) 2022/2555 zuständigen nationalen Behörden die betreffenden Einrichtungen dabei unterstützen, geeignete Lösungen für den Umgang mit den bei solchen Risikobewertungen ermittelten Risiken zu finden und umzusetzen.	•
Eine solche Anleitung sollte die Pflicht der betreffenden Einrichtungen, die bestehenden Risiken für die Sicherheit von Netz- und Informationssystemen zu ermitteln und zu dokumentieren, sowie die Pflicht der betreffenden Einrichtungen, die technischen und methodischen Anforderungen der im Anhang dieser Verordnung festgelegten Risikomanagementmaßnahmen im Bereich der Cybersicherheit entsprechend ihren Bedürfnissen und Ressourcen umzusetzen, unberührt lassen.	•

8

Text	Umsetzung in der VdS 10100
Netzsicherheitsmaßnahmen in Bezug auf i) den Übergang zur neuesten Generation der Kommunikationsprotokolle für die Netzwerkschicht, ii) die Einführung international vereinbarter und interoperabler moderner E-Mail-Kommunikationsnormen und iii) die Anwendung der bewährten Verfahren für die DNS-Sicherheit wie auch die Sicherheit und Hygiene des Internet-Routings bringen besondere Herausforderungen hinsichtlich der Ermittlung der jeweils besten bestehenden Normen und Einführungstechniken mit sich.	• Keine Anforderung, nur Einführungtext.
Um so bald wie möglich ein hohes gemeinsames Cybersicherheitsniveau 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, mit der Wirtschaft — einschließlich der Telekommunikationsbranche — und anderen Interessenträgern die Entwicklung eines Multi-Stakeholder-Forums unterstützen, dessen Aufgabe es wäre, diese besten bestehenden Normen und Einführungstechniken zu ermitteln.	• Betrifft die VdS 10100 nicht.
Die Pflicht der betreffenden Einrichtungen zur Umsetzung der technischen und methodischen Anforderungen der im Anhang dieser Verordnung festgelegten Risikomanagementmaßnahmen im Bereich der Cybersicherheit sollte von solchen Empfehlungen des Multi-Stakeholder-Forums jedoch unberührt bleiben.	• Betrifft die VdS 10100 nicht.

9

Text	Umsetzung in der VdS 10100
Gemäß Artikel 21 Absatz 2 Buchstabe a der Richtlinie (EU) 2022/2555 sollten wesentliche und wichtige Einrichtungen nicht nur über Konzepte für die Risikoanalyse, sondern auch über Konzepte für die Sicherheit der Informationssysteme verfügen.	Die VdS 10100 beinhaltet klare Konzepte für die Sicherheit der IT. • Sie unterscheidet die IT-Ressourcen im ersten Schritt in vier (Schutz-)Klassen: 1. nachrangige IT-Ressourcen 2. alle außer nachrangige IT-Ressourcen 3. wichtige IT-Ressourcen, Untermenge von (2) 4. kritische IT-Ressourcen, Untermenge von (3) • Die VdS definiert für alle vier Schutzklassen technische und/oder organisatorische Sicherheitsmaßnahmen. • Ab der Schutzklasse „wichtig“ ist eine individuelle Risikoidentifikation, -analyse und -behandlung vorgeschrieben.
Zu diesem Zweck sollten die betreffenden Einrichtungen ein Konzept für die Sicherheit von Netz- und Informationssystemen sowie themenspezifische Konzepte, wie z. B. für die Zugangs- bzw. Zugriffskontrolle, festlegen, die mit dem Konzept für die Sicherheit von Netz- und Informationssystemen vereinbar sein sollten.	• Die VdS 10100 stellt themenspezifische Konzepte zur Verfügung, u. a. für IT-Systeme, Mobile IT-Systeme, Netzwerke, Mobile Datenträger, Zugänge und Zugriffsrechte usw..
Das Konzept für die Sicherheit von Netz- und Informationssystemen sollte die übergeordnete allgemeine Unterlage sein, in der der Gesamtansatz der betreffenden Einrichtungen für die Sicherheit ihrer Netz- und Informationssysteme dargelegt wird, und sollte von den Leitungsorganen der betreffenden Einrichtungen genehmigt werden.	•
Die themenspezifischen Konzepte sollten von einer geeigneten Leitungsebene genehmigt werden.	• Umgesetzt in 6 Richtlinien zur Informationssicherheit (IS-Richtlinien) → 6.2 Allgemeine Anforderungen • Richtlinien müssen vom ISB unter Beteiligung des IST entwickelt und vom Topmanagement in Kraft gesetzt werden.

Text	Umsetzung in der VdS 10100
In dem Konzept sollten Indikatoren und Maßnahmen zur Überwachung seiner Umsetzung und des aktuellen Reifegrads der Netz- und Informationssicherheit in den betreffenden Einrichtungen festgelegt werden, um insbesondere die Beaufsichtigung der Umsetzung der Risikomanagementmaßnahmen im Bereich der Cybersicherheit durch die Leitungsorgane zu erleichtern.	•

10

Text	Umsetzung in der VdS 10100
Für die Zwecke der technischen und methodischen Anforderungen im Anhang dieser Verordnung sollte der Begriff „Nutzer“ alle juristischen und natürlichen Personen erfassen, die Zugang zu den Netz- und Informationssystemen der Einrichtung haben.	• Umgesetzt in 3 Begriffe und Abkürzungen → 3.1 Begriffe

11

Text	Umsetzung in der VdS 10100
Um die bestehenden Risiken für die Sicherheit von Netz- und Informationssystemen zu ermitteln und anzugehen, sollten die betreffenden Einrichtungen einen geeigneten Risikomanagementrahmen einführen und aufrechterhalten.	• Umgesetzt in Anhang A Verfahren und Risikomanagement → A.2 Risikomanagement
Als Teil dieses Risikomanagementrahmens sollten die betreffenden Einrichtungen einen Risikobehandlungsplan aufstellen, umsetzen und überwachen.	• Umgesetzt in Anhang A Verfahren und Risikomanagement → A.2 Risikomanagement → A.2.5 Risikobehandlung
Die betreffenden Einrichtungen können den Risikobehandlungsplan zur Bestimmung und Priorisierung von Optionen und Maßnahmen für die Behandlung von Risiken benutzen.	• Umgesetzt in Anhang A Verfahren und Risikomanagement → A.2 Risikomanagement → A.2.5 Risikobehandlung
Zu den Risikobehandlungsoptionen gehören insbesondere die Vermeidung, die Verringerung oder — in Ausnahmefällen — das Akzeptieren des Risikos.	• Umgesetzt in Anhang A Verfahren und Risikomanagement → A.2 Risikomanagement → A.2.5 Risikobehandlung
Die gewählten Risikobehandlungsoptionen sollten den Ergebnissen der von der betreffenden Einrichtung durchgeführten Risikobewertung entsprechen und mit dem Konzept der betreffenden Einrichtung für die Sicherheit von Netz- und Informationssystemen im Einklang stehen.	• Umgesetzt in Anhang A Verfahren und Risikomanagement → A.2 Risikomanagement → A.2.5 Risikobehandlung
Um den gewählten Risikobehandlungsoptionen Wirkung zu verleihen, sollten die betreffenden Einrichtungen geeignete Risikobehandlungsmaßnahmen ergreifen.	• Umgesetzt in Anhang A Verfahren und Risikomanagement → A.2 Risikomanagement → A.2.5 Risikobehandlung

12

Text	Umsetzung in der VdS 10100
Um Ereignisse, Beinahe-Vorfälle und Sicherheitsvorfälle zu erkennen, sollten die betreffenden Einrichtungen ihre Netz- und Informationssysteme überwachen und Maßnahmen zur Bewertung von Ereignissen, Beinahe-Vorfällen und Sicherheitsvorfällen treffen.	• Umgesetzt in 10 IT-Systeme → 10.4 Basisschutz → 10.4.4 Protokollierung • Umgesetzt in 10 IT-Systeme → 10.6 Zusätzliche Maßnahmen für wichtige IT-Systeme → 10.6.3 Überwachung • Umgesetzt in 11 Netzwerke und Verbindungen → 11.5 Basisschutz → 11.5.3 Segmentierung • Umgesetzt in 11 Netzwerke und Verbindungen → 11.4 Netzübergänge • Umgesetzt in 17 Sicherheitsvorfälle und Krisenmanagement → 17.3 Erkennen
Solche Maßnahmen sollten es ermöglichen, netzgestützte Angriffe auf der Grundlage anomaler Muster des eingehenden oder ausgehenden Verkehrs sowie Denial-of-Service-Angriffe zeitnah zu erkennen.	• Umgesetzt in 17 Sicherheitsvorfälle und Krisenmanagement → 17.3 Erkennen

13

Text	Umsetzung in der VdS 10100
Die betreffenden Einrichtungen werden dazu ermuntert, im Zuge der Durchführung einer Analyse der betrieblichen Auswirkungen (BIA) auch eine umfassende Analyse vorzunehmen, in der sie — soweit angemessen — maximal tolerierbare Ausfallzeiten, Vorgaben für Wiederherstellungszeiten und Wiederherstellungspunkte und Zielvorgaben für die Erbringung der Dienste erfassen.	•

14

Text	Umsetzung in der VdS 10100
Zur Minderung der Risiken, die sich aus der Lieferkette einer betreffenden Einrichtung und ihren Beziehungen zu ihren Anbietern bzw. Lieferanten ergeben, sollten die betreffenden Einrichtungen ein Konzept für die Sicherheit der Lieferkette festlegen, das ihre Beziehungen zu ihren direkten Anbietern und Diensteanbietern regelt.	•
Diese Einrichtungen sollten in die Verträge mit ihren direkten Anbietern oder Diensteanbietern angemessene Sicherheitsklauseln aufnehmen, in denen sie beispielsweise — soweit angemessen — Risikomanagementmaßnahmen im Bereich der Cybersicherheit gemäß Artikel 21 Absatz 2 der Richtlinie (EU) 2022/2555 oder anderer ähnlicher rechtlicher Anforderungen festlegen.	•

15

Text	Umsetzung in der VdS 10100
Die betreffenden Einrichtungen sollten regelmäßig Sicherheitstests auf der Grundlage spezieller Konzepte und Verfahren durchführen, um zu überprüfen, ob die Risikomanagementmaßnahmen im Bereich der Cybersicherheit umgesetzt wurden und ordnungsgemäß funktionieren.	• Fehlt in der VdS 10100. Sollte in Kapitel 19 „Überwachung und Steuerung“ aufgenommen werden.
Sicherheitstests können in bestimmten Netz- und Informationssystemen oder in der betreffenden Einrichtung in ihrer Gesamtheit durchgeführt werden und automatische oder manuelle Tests, Penetrationstests, eine Schwachstellensuche, statische und dynamische Prüfungen der Sicherheit von Anwendungen, Konfigurationstests oder Sicherheitsaudits umfassen.	• Fehlt in der VdS 10100. Sollte in Kapitel 19 „Überwachung und Steuerung“ aufgenommen werden.
Die betreffenden Einrichtungen können Sicherheitstests in ihren Netz- und Informationssystemen bei deren Einrichtung, nach Aufrüstungen der Infrastruktur oder von Anwendungen oder nach Änderungen, die sie für erheblich halten, oder nach einer Wartung durchführen.	• Fehlt in der VdS 10100. Sollte in Kapitel 19 „Überwachung und Steuerung“ oder in „10 IT-Systeme → 10.3 Lebenszyklus → 10.3.3 Inbetriebnahme und Änderung“ (z. B. als Empfehlung) aufgenommen werden.
Die Ergebnisse der Sicherheitstests sollten in die Konzepte und Verfahren der betreffenden Einrichtungen für die Bewertung der Wirksamkeit der Risikomanagementmaßnahmen im Bereich der Cybersicherheit sowie in unabhängige Überprüfungen ihrer Konzepte für die Sicherheit von Netz- und Informationssystemen einfließen.	• Fehlt in der VdS 10100.

16

Text	Umsetzung in der VdS 10100
Zur Vermeidung erheblicher Störungen und Schäden, die durch die Ausnutzung nicht behobener Schwachstellen in Netz- und Informationssystemen verursacht werden, sollten die betreffenden Einrichtungen geeignete Sicherheitspatch-Managementverfahren festlegen und anwenden, die mit den Änderungs-, Schwachstellen- und Risikomanagementverfahren sowie anderen einschlägigen Verfahren der betreffenden Einrichtungen im Einklang stehen.	• Umgesetzt in „8 Wissen → 8.2 → Aktualität des Wissens“ in Verbindung mit „10 IT-Systeme → 10.4 Basisschutz → 10.4.2 Software“
Die betreffenden Einrichtungen sollten Maßnahmen ergreifen, die in einem angemessenen Verhältnis zu ihrer Mittelausstattung stehen, um sicherzustellen, dass durch Sicherheitspatches keine zusätzlichen Schwachstellen oder Instabilitäten eingebracht werden.	• Umgesetzt in „10 IT-Systeme → 10.4 Basisschutz → 10.4.2 Software“

Text	Umsetzung in der VdS 10100
Im Falle einer geplanten Nichtverfügbarkeit des Dienstes, die durch die Anwendung von Sicherheitspatches verursacht wird, sollen die betreffenden Einrichtungen ihre Kunden im Voraus angemessen hierüber informieren.	• Fehlt in der VdS 10100. Sollte als Empfehlung aufgenommen werden in „10 IT-Systeme → 10.4 Basisschutz → 10.4.2 Software“

17

Text	Umsetzung in der VdS 10100
Die betreffenden Einrichtungen sollten die Risiken managen, die sich aus dem Erwerb von IKT-Produkten oder -Diensten von Anbietern oder Diensteanbietern ergeben, und sich vergewissern, dass die zu erwerbenden IKT-Produkte oder -Dienste ein bestimmtes Schutzniveau in Bezug auf die Cybersicherheit erreichen, z. B. anhand europäischer Cybersicherheitszertifikate und EU-Konformitätserklärungen für IKT-Produkte oder -Dienste, die im Rahmen eines gemäß Artikel 49 der Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates (2) angenommenen europäischen Systems für die Cybersicherheitszertifizierung ausgestellt wurden.	•
Wenn die betreffenden Einrichtungen Sicherheitsanforderungen für die zu erwerbenden IKT-Produkte festlegen, sollten sie die grundlegenden Cybersicherheitsanforderungen berücksichtigen, die in der Verordnung des Europäischen Parlaments und des Rates über horizontale Cybersicherheitsanforderungen an Produkte mit digitalen Elementen festgelegt sind.	•

18

Text	Umsetzung in der VdS 10100
Zum Schutz vor Cyberbedrohungen und zur Unterstützung der Prävention und Eindämmung von Datenschutzverletzungen sollten die betreffenden Einrichtungen Netzsicherheitslösungen umsetzen.	• Keine Anforderung, nur EInführungstext.

Text	Umsetzung in der VdS 10100
Typische Netzsicherheitslösungen wären der Einsatz von Firewalls zum Schutz der internen Netze der betreffenden Einrichtungen, die Beschränkung der Verbindungen und des Zugangs zu Diensten, soweit solche Verbindungen und Zugriffe unbedingt notwendig sind, aber auch die Verwendung virtueller privater Netze für den Fernzugriff und das Zulassen von Verbindungen von Diensteanbietern nur nach einem Genehmigungsantrag und für einen bestimmten Zeitraum, z. B. für die Dauer von Wartungsarbeiten.	• Firewalls ◦ „11 Netzwerke und Verbindungen → 11.4 Netzübergänge“ ◦ „11 Netzwerke und Verbindungen → 11.5 Basisschutz → 11.5.3 Segmentierung“ • Beschränkung der Verbindungen und des Zugangs zu Diensten: ◦ „10 IT-Systeme → 10.4 Basisschutz → 10.4.3 Beschränkung des Netzwerkverkehrs“ ◦ „10 IT-Systeme → 10.4 Basisschutz → 10.4.9 Zugänge und Zugriffe“ ◦ „11 Netzwerke und Verbindungen → 11.4 Netzübergänge“ ◦ „11 Netzwerke und Verbindungen → 11.5 Basisschutz → 11.5.3 Segmentierung“ • VPN für Fernzugriff: ◦ „11 Netzwerke und Verbindungen → 11.5 Basisschutz → 11.5.4 Fernzugang“ ◦ „11 Netzwerke und Verbindungen → 11.5 Basisschutz → 11.5.5 Netzwerkkopplung“ • Zulassen von Verbindungen von Diensteanbietern nur nach einem Genehmigungsantrag: ◦ „5 Leitlinie zur Informationssicherheit (IS-Leitlinie) → 6.5 Regelungen für Nutzer“ • Zulassen von Verbindungen von Diensteanbietern nur (…) für einen bestimmten Zeitraum„ ◦ Nicht umgesetzt bzw. nicht explizit erwähnt.

19

Text	Umsetzung in der VdS 10100
Zum Schutz der Netze der betreffenden Einrichtungen und ihrer Informationssysteme vor Schadsoftware und nicht genehmigter Software sollten diese Einrichtungen Kontrollen durchführen, um die Verwendung nicht genehmigter Software zu verhindern oder zu erkennen, und sollten — soweit angemessen — Erkennungs- und Reaktionssoftware einsetzen.	•
Ferner sollten die betreffenden Einrichtungen Vorkehrungen in Erwägung ziehen, um ihre Angriffsfläche zu minimieren, Schwachstellen, die durch Angreifer ausgenutzt werden können, zu verringern, die Ausführung von Anwendungen auf Endgeräten zu kontrollieren, und sie sollten E-Mail- und Web-Anwendungsfilter einsetzen, um ihre Exposition gegenüber böswilligen Inhalten zu verringern.	•

20

Text	Umsetzung in der VdS 10100
Gemäß Artikel 21 Absatz 2 Buchstabe g der Richtlinie (EU) 2022/2555 sollen die Mitgliedstaaten sicherstellen, dass grundlegende Verfahren im Bereich der Cyberhygiene angewandt und Schulungen im Bereich der Cybersicherheit durchgeführt werden.	•
Zu den grundlegenden Verfahren der Cyberhygiene gehören beispielsweise Zero-Trust-Grundsätze, Software-Updates, Gerätekonfiguration, Netzwerksegmentierung, Identitäts- und Zugriffsmanagement oder Sensibilisierung der Nutzer, das Organisieren von Schulungen für die Mitarbeitenden und das Schärfen des Bewusstseins für Cyberbedrohungen, Phishing oder Social-Engineering-Techniken.	•
Die Verfahren der Cyberhygiene sind Teil verschiedener technischer und methodischer Anforderungen der im Anhang dieser Verordnung festgelegten Risikomanagementmaßnahmen im Bereich der Cybersicherheit.	•
In Bezug auf grundlegende Verfahren der Cyberhygiene für Nutzer sollten die betreffenden Einrichtungen beispielsweise die Vorgabe eines „leeren Schreibtischs“ und eines „leeren Bildschirms“, die Verwendung der Multi-Faktor-Authentifizierung und anderer Authentifizierungsmittel, einen sicheren Umgang mit E-Mails und ein sicheres Web-Browsen, den Schutz vor Phishing und Social Engineering und sichere Verfahren der Telearbeit in Betracht ziehen.	•

21

Text	Umsetzung in der VdS 10100
Um einen unbefugten Zugang zu den Anlagen und Werten der betreffenden Einrichtungen zu verhindern, sollten die betreffenden Einrichtungen ein themenspezifisches Konzept für den Zugang von Personen und von Netz- und Informationssystemen, wie z. B. zu Anwendungen, festlegen und umsetzen.	•

22

Text	Umsetzung in der VdS 10100
Um zu verhindern, dass Mitarbeitende beispielsweise ihre Zugangs- und Zugriffsrechte innerhalb der betreffenden Einrichtung missbrauchen können, um Schaden anzurichten, sollten die betreffenden Einrichtungen angemessene Maßnahmen für das Sicherheitsmanagement hinsichtlich ihrer Mitarbeitenden in Erwägung ziehen und ihr Personal für solche Risiken sensibilisieren.	•
Die betreffenden Einrichtungen sollten für den Umgang mit Verstößen gegen ihre Konzepte für die Sicherheit von Netz- und Informationssystemen ein Disziplinarverfahren einführen, bekannt machen und aufrechterhalten, das in andere Disziplinarverfahren der betreffenden Einrichtung eingebettet sein kann.	•
Zuverlässigkeitsüberprüfungen der Mitarbeitenden und — soweit anwendbar — der direkten Anbieter und Diensteanbieter der betreffenden Einrichtungen sollten dem Ziel der Sicherheit des Personals in den betreffenden Einrichtungen dienen und können Maßnahmen wie die Abfrage des Strafregistereintrags einer Person oder die Prüfung der bisherigen Erfüllung ihrer beruflichen Pflichten umfassen, soweit dies für die Aufgaben der Person in der betreffenden Einrichtung angemessen ist und mit dem Konzept der betreffenden Einrichtung für die Sicherheit von Netz- und Informationssystemen im Einklang steht.	•

23

Text	Umsetzung in der VdS 10100
Die Multifaktor-Authentifizierung kann die Cybersicherheit der Einrichtungen verbessern und sollte von den Einrichtungen insbesondere dann in Betracht gezogen werden, wenn Nutzer aus der Ferne auf ihre Netz- und Informationssysteme zugreifen oder wenn sie auf sensible Informationen oder privilegierte Konten und Systemverwaltungskonten zugreifen.	• Umgesetzt in „10 IT-Systeme → 10.4 Basisschutz → 10.4.8 Authentifizierung“
Die Multifaktor-Authentifizierung kann mit anderen Techniken kombiniert werden, um unter bestimmten Umständen zusätzliche Faktoren zu verlangen, die auf vorab festgelegten Regeln und Mustern beruhen, z. B. beim Zugriff von einem ungewöhnlichen Standort aus, mit einem ungewöhnlichen Gerät oder zu einer ungewöhnlichen Zeit.	• Als Empfehlung aufgenommen in „10 IT-Systeme → 10.4 Basisschutz → 10.4.8 Authentifizierung“

24

Text	Umsetzung in der VdS 10100
Die betreffenden Einrichtungen sollten ihre wichtigen Anlagen und Werte mit einem soliden Anlagen- und Wertemanagement verwalten und schützen, das auch als Grundlage für die Risikoanalyse und das Betriebskontinuitätsmanagement dienen sollte.	•

Text	Umsetzung in der VdS 10100
Die betreffenden Einrichtungen sollten sowohl materielle Anlagen als auch immaterielle Werte verwalten und ein entsprechendes Anlagen- und Werteinventar erstellen, ihre Anlagen und Werte mit einer festgelegten Klassifizierung versehen, sie entsprechend behandeln und verfolgen und während ihres gesamten Lebenszyklus Maßnahmen zu ihrem Schutz treffen.	•

25

Text	Umsetzung in der VdS 10100
Das Anlagen- und Wertemanagement sollte eine Klassifizierung der Anlagen und Werte nach Art, Sensibilität, Risikoniveau und Sicherheitsanforderungen sowie die Durchführung geeigneter Maßnahmen und Kontrollen zur Gewährleistung ihrer Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität einschließen.	• Die VdS 10100 beinhaltet ein sehr vereinfachtes Anlagen- und Wertemanagement. Sie unterscheidet die IT-Ressourcen in vier (Schutz-)Klassen: 1. nachrangige IT-Ressourcen 2. alle außer nachrangige IT-Ressourcen 3. wichtige IT-Ressourcen, Untermenge von (2) 4. kritische IT-Ressourcen, Untermenge von (3)
Durch die Klassifizierung der Anlagen und Werte nach Risikoniveau sollten die betreffenden Einrichtungen in die Lage versetzt werden, geeignete Sicherheitsmaßnahmen anzuwenden und Sicherheitskontrollen durchzuführen, um Systeme für Verschlüsselung, Zugangs- bzw. Zugriffskontrolle (einschließlich der Kontrolle des Perimeters und einer physischen und logischen Zugangskontrolle), Sicherungskopien, Protokollierung und Überwachung, Aufbewahrung und Entsorgung zu schützen.	• Die VdS definiert für alle vier Schutzklassen technische und/oder organisatorische Sicherheitsmaßnahmen. • Ab der Schutzklasse „wichtig“ ist eine individuelle Risikoidentifikation, -analyse und -behandlung vorgeschrieben.
Bei der Durchführung einer Analyse der betrieblichen Auswirkungen (BIA) können die betreffenden Einrichtungen die jeweilige Klassifizierungsstufe auf der Grundlage der Folgen einer Störung der Anlagen für die Einrichtungen bestimmen.	• Die VdS 10100 versucht, eine BIA zu vermeiden. • Eine Empfehlung für die Durchführung einer BIA sollte aufgenommen werden.
Alle Mitarbeitenden der Einrichtungen, die Anlagen und Werte verwalten, sollten mit den dafür geltenden Konzepten und Anweisungen vertraut sein.	• Wird umgesetzt ◦ „7 Mitarbeiter → 7.3 Aufnahme der Tätigkeit“ ◦ „8 Wissen → 8.2 Aktualität des Wissens“

26

Text	Umsetzung in der VdS 10100
Die Granularität des Anlagen- und Werteinventars sollte den Bedürfnissen der betreffenden Einrichtungen entsprechen.	•
Ein umfassendes Anlagen- und Werteinventar könnte für jede Anlage bzw. jeden Wert mindestens eine eindeutige Kennung, den jeweiligen Eigentümer, eine Beschreibung, den Standort, die Art der Anlage bzw. des Wertes, die Art und Klassifizierung der damit verarbeiteten Informationen, das Datum der letzten Aktualisierung oder des letzten Patches, die bei der Risikobewertung vergebene Klassifizierung und das Ende der Lebensdauer enthalten.	•
Bei der Identifizierung des Eigentümers einer Anlage bzw. eines Werts sollten die betreffenden Einrichtungen auch die Person angeben, die für den Schutz dieser Anlage bzw. dieses Werts verantwortlich ist.	•

27

Text	Umsetzung in der VdS 10100
Mit der Zuweisung und Organisation von Rollen, Verantwortlichkeiten und Weisungsbefugnissen im Bereich der Cybersicherheit sollte eine kohärente Struktur für die Governance und Umsetzung der Cybersicherheit innerhalb der betreffenden Einrichtungen geschaffen und eine wirksame Kommunikation im Falle von Sicherheitsvorfällen sichergestellt werden.	• Wird umgesetzt: „4 Organisation der Informationssicherheit“
Bei der Festlegung und Zuweisung von Verantwortlichkeiten für bestimmte Aufgaben sollten die betreffenden Einrichtungen bestimmte Rollen wie die des leitenden Beauftragten für die Informationssicherheit, des Beauftragten für die Informationssicherheit, des Beauftragten für die Bewältigung von Sicherheitsvorfällen, des Prüfers oder vergleichbare Funktionen berücksichtigen.	• Die VdS 10100 ordnet dem ISB eine zentrale Funktion zu (siehe „4 Organisation der Informationssicherheit → 4.4 Informationssicherheitsbeauftragter“). • Der ISB darf Aufgaben delegieren (siehe „4 Organisation der Informationssicherheit → 4.2 Verantwortlichkeiten → 4.2.5 Delegieren von Aufgaben“)
Die betreffenden Einrichtungen können bestimmte Rollen und Verantwortlichkeiten auch externen Dritten wie IKT-Diensteanbietern übertragen.	• Setzt die VdS 10100 durch die entsprechende Definition von „Mitarbeiter“ um.

28

Text	Umsetzung in der VdS 10100
Gemäß Artikel 21 Absatz 2 der Richtlinie (EU) 2022/2555 sollten Risikomanagementmaßnahmen im Bereich der Cybersicherheit auf einem gefahrenübergreifenden Ansatz beruhen, der darauf abzielt, Netz- und Informationssysteme und ihr physisches Umfeld vor Ereignissen wie Diebstahl, Feuer, Überschwemmungen und Telekommunikations- oder Stromausfällen oder vor unbefugtem physischen Zugang zu Informationen und Datenverarbeitungsanlagen einer wesentlichen oder wichtigen Einrichtung und vor der Schädigung solcher Informationen und Betriebsstätten und entsprechenden Eingriffen zu schützen, die die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über Netz- und Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigen können.	•
In den technischen und methodischen Anforderungen der Risikomanagementmaßnahmen im Bereich der Cybersicherheit sollten daher auch die physische Sicherheit der Netz- und Informationssysteme und die Sicherheit ihres Umfelds berücksichtigt werden, indem Maßnahmen zum Schutz dieser Systeme vor Systemfehlern, menschlichen Fehlern, böswilligen Handlungen oder natürlichen Phänomenen darin einbezogen werden.	• Wird für wichtige IT-Systeme umgesetzt ◦ „13 Umgebung → 13.2 Server, aktive Netzwerkkomponenten und Netzwerkverteilstellen“ (Empfehlung) ◦ „13 Umgebung → 13.4 Zusätzliche Maßnahmen für wichtige IT-Systeme“ (verpflichtende Maßnahmen)
Weitere physische Bedrohungen und Bedrohungen des Umfelds ergeben sich z. B. aus Erdbeben, Explosionen, Sabotage, Insider-Bedrohungen, Unruhen, giftigen Abfällen und Umweltemissionen.	• Diese Bedrohungen sind in der VdS 10100 nicht erwähnt, bis auf: ◦ Sabotage: „13 Umgebung → 13.4 Zusätzliche Maßnahmen für wichtige IT-Systeme“ (verpflichtende Maßnahmen)

Text	Umsetzung in der VdS 10100
Die Verhinderung von Verlusten, Beschädigungen oder Beeinträchtigungen von Netz- und Informationssystemen oder von Betriebsunterbrechungen infolge des Ausfalls und der Störung unterstützender Versorgungsleistungen sollte ebenfalls zur angestrebten Betriebskontinuität in den betreffenden Einrichtungen beitragen.	• Ausfall/Störung unterstützender Versorgungsleistungen nicht in der VdS 10000 aufgenommen, bis auf: ◦ ungeeignete Umgebungsbedingungen: „13 Umgebung → 13.4 Zusätzliche Maßnahmen für wichtige IT-Systeme“ (verpflichtende Maßnahmen) ◦ unzuverlässige Stromversorgung: „13 Umgebung → 13.4 Zusätzliche Maßnahmen für wichtige IT-Systeme“ (verpflichtende Maßnahmen)
Darüber hinaus sollte sich durch den Schutz vor physischen Bedrohungen und Bedrohungen des Umfelds auch die Sicherheit bei der Wartung von Netz- und Informationssystemen in den betreffenden Einrichtungen erhöhen.	•

29

Text	Umsetzung in der VdS 10100
Die betreffenden Einrichtungen sollten Maßnahmen zum Schutz vor physischen Bedrohungen und Bedrohungen des Umfelds konzipieren und umsetzen, Mindest- und Höchstkontrollwerte für solche Bedrohungen festlegen und Umweltparameter überwachen.	•
So sollten sie beispielsweise die Installation von Früherkennungssystemen für die Überschwemmung von Gebieten, in denen sich Netz- und Informationssysteme befinden, in Erwägung ziehen.	•
In Bezug auf Brandgefahren sollten die betreffenden Einrichtungen insbesondere die Schaffung eines separaten Brandabschnitts für das Rechenzentrum, den Einsatz feuerbeständiger Materialien, die Anbringung von Sensoren zur Überwachung von Temperatur und Feuchtigkeit, den Anschluss des Gebäudes an eine Brandmeldeanlage mit automatischer Benachrichtigung der örtlichen Feuerwehr sowie Brandfrüherkennungs- und Feuerlöschanlagen in Erwägung ziehen.	•
Überdies sollten die betreffenden Einrichtungen regelmäßig Brandschutzübungen und Brandschutzinspektionen durchführen.	•
Um ihre Stromversorgung sicherzustellen, sollten die betreffenden Einrichtungen außerdem einen Überspannungsschutz und eine entsprechende Notstromversorgung nach den einschlägigen Normen in Erwägung ziehen.	•
Da Überhitzung eine Gefahr für die Verfügbarkeit von Netz- und Informationssystemen darstellt, könnten die betreffenden Einrichtungen, insbesondere Anbieter von Rechenzentrumsdiensten, auch den Einbau angemessener, kontinuierlicher und redundanter Klimaanlagen in Erwägung ziehen.	•

30

Text	Umsetzung in der VdS 10100
Ferner soll in dieser Verordnung präzisiert werden, in welchen Fällen ein Sicherheitsvorfall für die Zwecke des Artikels 23 Absatz 3 der Richtlinie (EU) 2022/2555 als erheblich angesehen werden sollte.	•
Die Kriterien sollten so gestaltet sein, dass die betreffenden Einrichtungen beurteilen können, ob ein Sicherheitsvorfall erheblich ist, um ihn dann gemäß der Richtlinie (EU) 2022/2555 zu melden.	• Wird umgesetzt: „17 Sicherheitsvorfälle und Krisenmanagement → 17.2 IS-Richtlinie“
Darüber hinaus sollten die in dieser Verordnung festgelegten Kriterien unbeschadet des Artikels 5 der Richtlinie (EU) 2022/2555 als erschöpfend betrachtet werden.	•
In dieser Verordnung werden die Fälle festgelegt, in denen ein Sicherheitsvorfall als erheblich angesehen werden sollte; dazu werden sowohl horizontale als auch einrichtungsspezifische Fälle festgelegt.	• Wird umgesetzt: „17 Sicherheitsvorfälle und Krisenmanagement → 17.2 IS-Richtlinie“

31

Text	Umsetzung in der VdS 10100
Gemäß Artikel 23 Absatz 4 der Richtlinie (EU) 2022/2555 sollten die betreffenden Einrichtungen dazu verpflichtet sein, erhebliche Sicherheitsvorfälle innerhalb der in dieser Bestimmung festgelegten Fristen zu melden.	• Wird umgesetzt: „17 Sicherheitsvorfälle und Krisenmanagement → 17.4 Reaktion“
Diese Meldefristen laufen ab dem Zeitpunkt, zu dem die Einrichtung Kenntnis von solchen erheblichen Vorfällen erlangt.	• Wird umgesetzt: „17 Sicherheitsvorfälle und Krisenmanagement → 17.4 Reaktion“
Die betreffende Einrichtung muss daher Sicherheitsvorfälle melden, die nach der von ihr vorgenommenen Anfangsbewertung schwerwiegende Betriebsstörungen des Dienstes oder finanzielle Verluste für diese Einrichtung verursachen oder andere natürliche oder juristische Personen beeinträchtigen könnten, indem sie erhebliche materielle oder immaterielle Schäden nach sich ziehen.	• Wird umgesetzt: „17 Sicherheitsvorfälle und Krisenmanagement → 17.4 Reaktion“
Wenn also eine betreffende Einrichtung ein verdächtiges Ereignis feststellt oder ihr ein mutmaßlicher Sicherheitsvorfall von einem Dritten, z. B. von einer Person, einem Kunden, einer Einrichtung, einer Behörde, einer Medienorganisation oder aus anderer Quelle, zur Kenntnis gebracht wird, sollte sie das verdächtige Ereignis zeitnah bewerten, um festzustellen, ob es sich um einen Sicherheitsvorfall handelt, und, falls dies der Fall ist, seine Art und Schwere zu bestimmen.	• Wird umgesetzt: „17 Sicherheitsvorfälle und Krisenmanagement → 17.4 Reaktion“
Es ist daher davon auszugehen, dass die betreffende Einrichtung von dem erheblichen Sicherheitsvorfall Kenntnis hatte, sobald sie nach einer solchen Anfangsbewertung mit hinreichender Gewissheit feststellt, dass ein erheblicher Sicherheitsvorfall vorliegt.	• Keine Anforderung.

32

Text	Umsetzung in der VdS 10100
Im Hinblick auf die Feststellung, ob ein Sicherheitsvorfall erheblich ist, sollten die betreffenden Einrichtungen — soweit zutreffend — die Zahl der von dem Sicherheitsvorfall betroffenen Nutzer ermitteln, wobei sie Geschäfts- und Endkunden, mit denen die betreffenden Einrichtungen eine Vertragsbeziehung unterhalten, sowie natürliche und juristische Personen, die mit den Geschäftskunden in Verbindung stehen, berücksichtigen sollten.	•
Ist eine betreffende Einrichtung nicht imstande, die Zahl der betroffenen Nutzer zu berechnen, sollte sie bei der Bestimmung der Gesamtzahl der von dem Sicherheitsvorfall betroffenen Nutzer ihre Schätzung der möglichen Höchstzahl betroffener Nutzer zugrunde legen.	•
Die Bedeutung eines Sicherheitsvorfalls, an dem ein Vertrauensdienst beteiligt ist, sollte nicht nur anhand der Zahl der Nutzer, sondern auch der Zahl der vertrauenden Beteiligten bestimmt werden, da diese im Hinblick auf Betriebsstörungen und materielle oder immaterielle Schäden gleichermaßen von einem erheblichen Vorfall, an dem ein Vertrauensdienst beteiligt ist, beeinträchtigt werden können.	•
Deshalb sollten Vertrauensdiensteanbieter bei ihrer Feststellung, ob ein Sicherheitsvorfall erheblich ist, — soweit anwendbar — auch die Zahl der vertrauenden Beteiligten berücksichtigen.	•
Zu diesem Zweck sollten vertrauende Beteiligte als natürliche oder juristische Personen verstanden werden, die einen Vertrauensdienst in Anspruch nehmen.	•

33

Text	Umsetzung in der VdS 10100
Wartungsarbeiten, die zu einer eingeschränkten Verfügbarkeit oder zur Nichtverfügbarkeit der Dienste führen, sollten nicht als erhebliche Sicherheitsvorfälle angesehen werden, wenn die eingeschränkte Verfügbarkeit oder Nichtverfügbarkeit des Dienstes im Rahmen eines planmäßigen Wartungsvorgangs eintritt.	•
Darüber hinaus sollte es nicht als erheblicher Sicherheitsvorfall angesehen werden, wenn ein Dienst aufgrund planmäßiger Unterbrechungen wie etwa im Voraus vertraglich vereinbarter Unterbrechungen oder Nichtverfügbarkeiten nicht verfügbar ist.	•

34

Text	Umsetzung in der VdS 10100
Die Dauer eines Sicherheitsvorfalls, der die Verfügbarkeit eines Dienstes beeinträchtigt, sollte ab dem Beginn der Störung der ordnungsgemäßen Erbringung des Dienstes bis zum Zeitpunkt der Wiederherstellung gemessen werden.	•

Text	Umsetzung in der VdS 10100
Wenn eine betreffende Einrichtung nicht imstande ist, den Zeitpunkt des Beginns der Störung zu bestimmen, sollte die Dauer des Sicherheitsvorfalls ab dem Zeitpunkt gemessen werden, zu dem der Sicherheitsvorfall erkannt wurde, oder ab dem Zeitpunkt, zu dem der Sicherheitsvorfall in Netz- oder Systemprotokollen oder anderen Datenquellen aufgezeichnet wurde, je nachdem, welcher Zeitpunkt früher ist.	•

35

Text	Umsetzung in der VdS 10100
Eine vollständige Nichtverfügbarkeit eines Dienstes sollte von dem Zeitpunkt an gemessen werden, zu dem der Dienst für die Nutzer vollständig nicht verfügbar ist, bis zu dem Zeitpunkt, zu dem die gewöhnlichen Tätigkeiten oder Abläufe wieder das vor dem Sicherheitsvorfall bestehende Dienstniveau erreicht haben.	•
Wenn eine betreffende Einrichtung nicht imstande ist, den Zeitpunkt des Beginns der vollständigen Nichtverfügbarkeit eines Dienstes zu bestimmen, sollte die Nichtverfügbarkeit ab dem Zeitpunkt gemessen werden, zu dem sie von der Einrichtung festgestellt wurde.	•

36

Text	Umsetzung in der VdS 10100
Bei der Bestimmung der direkten finanziellen Verluste infolge eines Sicherheitsvorfalls sollten die betreffenden Einrichtungen alle finanziellen Verluste berücksichtigen, die ihnen infolge des Sicherheitsvorfalls entstanden sind, wie etwa Kosten für die Ersetzung oder Verlegung von Software, Hardware oder Infrastruktur, Personalkosten, einschließlich Kosten im Zusammenhang mit der Ersetzung oder Verlegung von Personal, der Einstellung zusätzlichen Personals, der Vergütung von Überstunden und der Wiederherstellung verloren gegangener oder beeinträchtigter Kompetenzen, Gebühren wegen Nichteinhaltung vertraglicher Verpflichtungen, Kosten für Ausgleichs- und Entschädigungszahlungen an Kunden, Verluste wegen entgangener Einnahmen, Kosten für interne und externe Kommunikation, Beratungskosten, einschließlich Kosten im Zusammenhang mit Rechtsberatung, forensischen Dienstleistungen und Behebungsdienstleistungen, und sonstige Kosten im Zusammenhang mit dem Sicherheitsvorfall.	•
Geldbußen wie auch Kosten, die für den laufenden Geschäftsbetrieb erforderlich sind, sollten jedoch nicht als finanzielle Verluste infolge eines Sicherheitsvorfalls betrachtet werden, darunter etwa Kosten für die allgemeine Wartung von Infrastruktur, Ausrüstung, Hardware und Software, Kosten für die laufende Fortbildung des Personals, um dessen Kompetenzen auf dem aktuellen Stand zu halten, interne oder externe Kosten für die Verstärkung des Geschäftsbetriebs nach dem Vorfall, einschließlich für Aufrüstungen, Verbesserungen und Initiativen zur Risikobewertung, sowie Versicherungsprämien.	•
Die betreffenden Einrichtungen sollten die Höhe der finanziellen Verluste auf der Grundlage vorliegender Daten berechnen, und wenn die tatsächliche Höhe der finanziellen Verluste nicht bestimmt werden kann, sollten die Einrichtungen solche Beträge schätzen.	•

37

Text	Umsetzung in der VdS 10100
Die betreffenden Einrichtungen sollten auch verpflichtet sein, Sicherheitsvorfälle zu melden, die den Tod natürlicher Personen oder erhebliche Schädigungen der Gesundheit natürlicher Personen verursacht haben oder verursachen können, denn bei solchen Vorfällen handelt es sich um besonders schwere Fälle, die erhebliche materielle oder immaterielle Schäden verursachen.	•
So könnte beispielsweise ein Sicherheitsvorfall, der eine betreffende Einrichtung beeinträchtigt, dazu führen, dass Gesundheits- oder Notdienste nicht zur Verfügung stehen oder dass die Vertraulichkeit oder Integrität von Daten verloren geht und sich dies auf die Gesundheit natürlicher Personen auswirkt.	•
Bei der Feststellung, ob ein Sicherheitsvorfall erhebliche Schädigungen der Gesundheit einer natürlichen Person verursacht hat oder verursachen kann, sollten die betreffenden Einrichtungen berücksichtigen, ob der Vorfall schwere Verletzungen und Erkrankungen verursacht hat oder verursachen kann.	•
In dieser Hinsicht sollten die betreffenden Einrichtungen nicht dazu verpflichtet sein, zusätzliche Informationen einzuholen, die ihnen nicht zugänglich sind.	•

38

Text	Umsetzung in der VdS 10100
Von einer eingeschränkten Verfügbarkeit sollte insbesondere dann ausgegangen werden, wenn ein von einer betreffenden Einrichtung erbrachter Dienst deutlich langsamer als die durchschnittliche Antwortzeit ist oder wenn nicht alle Funktionen eines Dienstes verfügbar sind.	•
Zur Bewertung von Verzögerungen bei der Antwortzeit sollten — soweit möglich — objektive Kriterien auf der Grundlage der durchschnittlichen Antwortzeiten der von den betreffenden Einrichtungen erbrachten Dienste herangezogen werden.	•
Eine Funktion eines Dienstes kann beispielsweise aus einer Chat-Funktion oder einer Bildsuchfunktion bestehen.	• Keine Vorgabe, nur ein Beispiel.

39

Text	Umsetzung in der VdS 10100
Ein erfolgreicher, mutmaßlich böswilliger und unbefugter Zugriff auf Netz- und Informationssysteme einer betreffenden Einrichtung sollte als erheblicher Sicherheitsvorfall betrachtet werden, wenn er zu schwerwiegenden Betriebsstörungen führen kann.	•
Wenn sich beispielsweise ein Cyberangreifer in den Netz- und Informationssystemen einer betreffenden Einrichtung einnistet, um künftig eine Störung der Dienste zu verursachen, sollte der Sicherheitsvorfall als erheblich betrachtet werden.	•

40

Text	Umsetzung in der VdS 10100
Wiederholte Sicherheitsvorfälle, die offensichtlich dieselbe Ursache haben und einzeln betrachtet die Kriterien für einen erheblichen Sicherheitsvorfall nicht erfüllen, sollten zusammen dennoch als erheblicher Sicherheitsvorfall betrachtet werden, sofern sie zusammen das Kriterium für finanzielle Verluste erfüllen und zumindest zweimal innerhalb von sechs Monaten aufgetreten sind.	•
Solche wiederholten Sicherheitsvorfälle können auf erhebliche Mängel und Schwächen in den Verfahren für das Cybersicherheitsrisikomanagement der betreffenden Einrichtung und deren Reifegrad im Bereich der Cybersicherheit hindeuten.	•
Darüber hinaus können solche wiederholten Sicherheitsvorfälle erhebliche finanzielle Verluste bei der betreffenden Einrichtung verursachen.	•

41

Text	Umsetzung in der VdS 10100
Die Kommission hat sich mit der Kooperationsgruppe und der ENISA über den Entwurf des Durchführungsrechtsakts gemäß Artikel 21 Absatz 5 und Artikel 23 Absatz 11 der Richtlinie (EU) 2022/2555 ausgetauscht und mit ihnen zusammengearbeitet.	• Keine Maßnahme.

42

Text	Umsetzung in der VdS 10100
Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates (3) angehört und gab am 1. September 2024 seine Stellungnahme ab.	• Keine Maßnahme.

43

Text	Umsetzung in der VdS 10100
Die in dieser Verordnung vorgesehenen Maßnahmen entsprechen der Stellungnahme des nach Artikel 39 der Richtlinie (EU) 2022/2555 eingesetzten Ausschusses —	• Keine Maßnahme.

HAT FOLGENDE VERORDNUNG ERLASSEN: (...)

Ich möchte...
...etwas in diesem Artikel kommentieren.☐
Ihre Kontaktdaten (für Rückfragen, optional)

Only edit this fieldset if “...etwas in diesem Artikel kommentieren.” is set.

Name (optional) Ihre Mailadresse (optional)
Wir möchten wissen, dass Sie ein Mensch sind

Only edit this fieldset if “...etwas in diesem Artikel kommentieren.” is set.

Geben Sie hier die Zahl 'zwanzig minus elf' als Ziffer ein. *
Ihr Feedback

Only edit this fieldset if “...etwas in diesem Artikel kommentieren.” is set.

Wie finden Sie diesen Artikel? * bitte wählen
Was fanden Sie besonders gut? (optional)

Only edit this fieldset if “...etwas in diesem Artikel kommentieren.” is set.

Was sollte besser werden? (optional)

Only edit this fieldset if “...etwas in diesem Artikel kommentieren.” is set.

Only edit this fieldset if “...etwas in diesem Artikel kommentieren.” is set.

Feedback absenden