Amtsblatt
der Europäischen Union

DE
Reihe C

C/2026/3712

13.7.2026

# MITTEILUNG DER KOMMISSION

## Leitlinien für die Anwendung von Artikel 13 Absatz 5 der Richtlinie (EU) 2022/2557 über die Resilienz kritischer Einrichtungen

(C/2026/3712)

## I. EINLEITUNG

1. Ziel der Richtlinie (EU) 2022/2557 über die Resilienz kritischer Einrichtungen ([1]) (im Folgenden „Richtlinie“) ist es, dafür zu sorgen, dass Dienste, die für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen oder wirtschaftlicher Tätigkeiten von wesentlicher Bedeutung sind, im Binnenmarkt ungehindert erbracht werden können. Mit der Richtlinie soll die Resilienz der kritischen Einrichtungen, die solche Dienste erbringen, gestärkt werden, indem ein übergreifender Rahmen für die Resilienz gegenüber allen (natürlichen oder vom Menschen verursachten, unbeabsichtigten oder vorsätzlichen) Gefahren geschaffen wird.

2. Gemäß Artikel 6 Absatz 1 der Richtlinie müssen die Mitgliedstaaten ihre kritischen Einrichtungen für die im Anhang der Richtlinie festgelegten Sektoren und Teilsektoren bis zum 17. Juli 2026 ermitteln. Um ein hohes Resilienzniveau zu erreichen, werden diesen kritischen Einrichtungen in der Richtlinie bestimmte Verpflichtungen auferlegt, darunter die Verpflichtung gemäß Artikel 13, geeignete und verhältnismäßige technische, sicherheitsbezogene und organisatorische Maßnahmen zur Gewährleistung ihrer Resilienz zu ergreifen. In diesem Zusammenhang wurde die Kommission in Artikel 13 Absatz 5 der Richtlinie beauftragt, unverbindliche Leitlinien zu erlassen, in denen die technischen, sicherheitsbezogenen und organisatorischen Maßnahmen, die von den kritischen Einrichtungen ergriffen werden können, näher spezifiziert werden.

3. Im Einklang mit den oben genannten Bestimmungen wurden die Mitgliedstaaten und die Interessenvertreter vor der Annahme dieser Mitteilung im Rahmen eines Workshops am 29. September 2025 konsultiert. Die Gruppe für die Resilienz kritischer Einrichtungen (Critical Entities Resilience Group – CERG) wurde in ihren Sitzungen vom 10. April, 19. Mai und 30. September 2025 zu den Grundzügen der Mitteilung konsultiert. Am 14. November 2025 wurde sie auch zum Entwurf der Mitteilung konsultiert, und am 25. Februar 2026 wurde der CERG eine aktualisierte Fassung übermittelt. Am 6. März 2026 fand eine abschließende Konsultation der CERG zum Entwurf der Leitlinien statt.

4. Diese Mitteilung ist nicht rechtsverbindlich und berührt nicht die Auslegung des EU-Rechts durch den Gerichtshof der Europäischen Union.

## II. UNVERBINDLICHE LEITLINIEN ÜBER MAßNAHMEN ZUR STÄRKUNG DER RESILIENZ

### A. ALLGEMEINE ERWÄGUNGEN

5. Mit diesen unverbindlichen Leitlinien sollen die technischen, sicherheitsbezogenen und organisatorischen Maßnahmen spezifiziert werden, die von kritischen Einrichtungen gemäß Artikel 13 Absatz 1 Buchstaben a bis f der Richtlinie ergriffen werden können. Die Liste der Maßnahmen ist nicht erschöpfend und kann durch weitere Maßnahmen ergänzt werden.

6. Gemäß Artikel 13 Absatz 1 müssen kritische Einrichtungen bei der Umsetzung dieser Maßnahmen Folgendes berücksichtigen:

   a) Die von den Mitgliedstaaten bereitgestellten einschlägigen Informationen über die gemäß Artikel 5 der Richtlinie von den Mitgliedstaaten durchgeführte Risikobewertung. Die Mitgliedstaaten sollten ihren kritischen Einrichtungen zeitnahe, prägnante und maßgeschneiderte Informationen übermitteln. Diese Informationen können die in Artikel 9 Absatz 3 der Richtlinie genannten Berichte umfassen, die der Kommission unter Verwendung des gemeinsamen Berichtsmusters übermittelt werden.

   b) Die einschlägigen Informationen über die Ergebnisse der gemäß Artikel 12 der Richtlinie durchgeführten Risikobewertung durch kritische Einrichtungen. Die kritischen Einrichtungen werden aufgefordert, einen ganzheitlichen Ansatz zu verfolgen: Weg vom einfachen Schutz kritischer Infrastrukturen hin zur Gewährleistung der Kontinuität der von ihnen erbrachten wesentlichen Dienste und Berücksichtigung der Ergebnisse der Risikobewertung bei ihren Maßnahmen zur Stärkung der Resilienz. Zur Unterstützung von Resilienzmaßnahmen sollten kritische Einrichtungen in Erwägung ziehen, umfassende Risikobewertungen durchzuführen, die über ihre direkten Abhängigkeiten hinausgehen und bei denen Aspekte grenzüberschreitender, sektorspezifischer und systemischer gegenseitiger Abhängigkeiten berücksichtigt werden.

([1]) Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates (ABl. L 333 vom 27.12.2022, S. 164).

7. Gemäß Artikel 13 Absatz 1 der Richtlinie müssen die von den kritischen Einrichtungen zu ergreifenden Maßnahmen geeignet und verhältnismäßig sein. Die Eignung und Verhältnismäßigkeit dieser Maßnahmen sollte anhand der Ergebnisse der oben genannten Risikobewertungen bemessen werden.

   a) Unter „geeignet“ sind dabei risikobasierte oder wirkungsbasierte, wirksame und passende Maßnahmen zu verstehen, die für eine vollständige Resilienz der kritischen Einrichtung bei der Erbringung wesentlicher Dienste sorgen können. Die Eignung einer Maßnahme kann sich von einer kritischen Einrichtung zur anderen – je nach der jeweiligen besonderen Situation der Einrichtung – unterscheiden.

   b) Unter „verhältnismäßig“ sind notwendige und ausreichende Maßnahmen zu verstehen, die gemessen am Risikoniveau und der Schwere des Störungen verursachenden Sicherheitsvorfalls nicht unverhältnismäßig sind. Die Maßnahmen sollten auf die jeweilige besondere Situation der betreffenden kritischen Einrichtung zugeschnitten sein und Aspekten wie der Art der erbrachten wesentlichen Dienste, der Lieferkette und gegenseitigen Abhängigkeiten, der Kosteneffizienz der Maßnahmen, der Größe der Einrichtung und den geografischen Auswirkungen der erbrachten Dienste Rechnung tragen.

8. In den Leitlinien werden alle Sektoren berücksichtigt, die unter Kapitel III der Richtlinie fallen ([2]). Die nicht erschöpfende Liste von Beispielen gilt möglicherweise nicht für alle Sektoren und alle Arten kritischer Infrastrukturen gleichermaßen.

9. Die zu ergreifenden Maßnahmen hängen vom Ergebnis der Risikobewertung des Mitgliedstaats und der Risikobewertungen der kritischen Einrichtungen ab.

10. Die von kritischen Einrichtungen gemäß Artikel 13 Absatz 1 Buchstaben a bis f ergriffenen Resilienzmaßnahmen sollten unbeschadet und im Einklang mit den Maßnahmen angewandt werden, die sich aus einschlägigen sektorspezifischen Rechtsvorschriften ergeben, wie den in Erwägungsgrund 31 der Richtlinie genannten Rechtsvorschriften, der Richtlinie zur Netz- und Informationssicherheit 2 (im Folgenden „NIS-2-Richtlinie“) ([3]), dem Europäischen Klimagesetz ([4]), der Verordnung über die Risikovorsorge im Elektrizitätssektor ([5]), der Verordnung über Maßnahmen zur Gewährleistung einer sicheren Gasversorgung ([6]), der Richtlinie über die Sicherheit von Offshore-Erdöl- und -Erdgasaktivitäten ([7]), dem EU-Rahmen für die Gefahrenabwehr im Seeverkehr und in Häfen ([8]), der Datenschutz-Grundverordnung (DSGVO) ([9]), der Verordnung zur Verwirklichung des einheitlichen europäischen Luftraums ([10]), der Verordnung über die Agentur der Europäischen Union für Flugsicherheit ([11]) und der Durchführungsverordnung in Bezug auf die Funktionen des Flugverkehrsmanagementnetzes ([12]).

([2]) Energie, Verkehr, Gesundheit, Trinkwasser, Abwasser, öffentliche Verwaltung, Weltraum, Produktion, Verarbeitung und Vertrieb von Lebensmitteln.

([3]) 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 (ABl. L 333 vom 27.12.2022, S. 80).

([4]) Verordnung (EU) 2021/1119 des Europäischen Parlaments und des Rates vom 30. Juni 2021 zur Schaffung des Rahmens für die Verwirklichung der Klimaneutralität und zur Änderung der Verordnungen (EG) Nr. 401/2009 und (EU) 2018/1999 (ABl. L 243 vom 9.7.2021, S. 1), insbesondere Artikel 5, der sich auf die Anpassung an den Klimawandel bezieht.

([5]) Verordnung (EU) 2019/941 des Europäischen Parlaments und des Rates vom 5. Juni 2019 über die Risikovorsorge im Elektrizitätssektor und zur Aufhebung der Richtlinie 2005/89/EG (ABl. L 158 vom 14.6.2019, S. 1), insbesondere die Maßnahmen gemäß den Artikeln 10 und 11.

([6]) Verordnung (EU) 2017/1938 des Europäischen Parlaments und des Rates vom 25. Oktober 2017 über Maßnahmen zur Gewährleistung der sicheren Gasversorgung und zur Aufhebung der Verordnung (EU) Nr. 994/2010 (ABl. L 280 vom 28.10.2017, S. 1), insbesondere die Maßnahmen gemäß Artikel 8.

([7]) Richtlinie 2013/30/EU des Europäischen Parlaments und des Rates vom 12. Juni 2013 über die Sicherheit von Offshore-Erdöl- und -Erdgasaktivitäten und zur Änderung der Richtlinie 2004/35/EG (ABl. L 178 vom 28.6.2013, S. 66), insbesondere die Maßnahmen gemäß Artikel 3.

([8]) Beispielsweise die Richtlinie 2005/65/EG zur Erhöhung der Gefahrenabwehr in Häfen und die Richtlinie 2002/59/EG über die Einrichtung eines gemeinschaftlichen Überwachungs- und Informationssystems für den Schiffsverkeh(.

([9]) Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (ABl L 119 vom 4.5.2016, S. 1).

([10]) Verordnung (EU) 2024/2803 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 zur Verwirklichung des Einheitlichen Europäischen Luftraums, insbesondere Artikel 22 Absatz 2 Buchstabe b (ABl. L, 2024/2803, 11.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2803/oj).

([11]) Verordnung (EU) 2018/1139 des Europäischen Parlaments und des Rates vom 4. Juli 2018 zur Festlegung gemeinsamer Vorschriften für die Zivilluftfahrt und zur Errichtung einer Agentur der Europäischen Union für Flugsicherheit (ABl. L 212 vom 22.8.2018, S. 1).

([12]) Durchführungsverordnung (EU) 2019/123 der Kommission vom 24. Januar 2019 zur Festlegung detaillierter Durchführungsbestimmungen für die Netzfunktionen des Flugverkehrsmanagements (ABl. L 28 vom 31.1.2019, S. 1).

11. Wenn kritische Einrichtungen bei ihren Resilienzmaßnahmen künstliche Intelligenz (KI) einsetzen (z. B. ein KI-System, das den Wasserdruck an einem Staudamm überwacht oder ein Stromnetz steuert), müssen sie sich bewusst sein, dass Hochrisiko-KI-Systeme die Sicherheitsanforderungen des EU-Gesetzes über künstliche Intelligenz ([13]) erfüllen müssen. „Hochrisiko" bedeutet in diesem Zusammenhang, dass die Systeme als Sicherheitsbauteile ([14]) im Rahmen der Verwaltung und des Betriebs kritischer digitaler Infrastruktur, des Straßenverkehrs oder der Wasser-, Gas-, Wärme- oder Stromversorgung verwendet werden sollen ([15]). Ihr Ausfall oder ihre Störung kann in großem Umfang ein Risiko für das Leben und die Gesundheit von Personen darstellen und zu erheblichen Störungen bei der normalen Durchführung sozialer und wirtschaftlicher Tätigkeiten führen.

12. In Verbindung mit Artikel 13 Absatz 2 der Richtlinie heißt es in Erwägungsgrund 30: „Um diese Ziele in Bezug auf die ermittelten Risiken zu erreichen, sollten kritische Einrichtungen die von ihnen ergriffenen Maßnahmen – auch im Interesse der Rechenschaftspflicht und der Wirksamkeit der Maßnahmen – in einem Resilienzplan oder in einem oder mehreren Dokumenten, die einem Resilienzplan gleichwertig sind, hinreichend detailliert beschreiben und diesen Plan in der Praxis anwenden. Hat eine kritische Einrichtung bereits technische, sicherheitsbezogene und organisatorische Maßnahmen ergriffen und Dokumente gemäß anderen Rechtsakten erstellt, die für Maßnahmen zur Verbesserung der Resilienz nach dieser Richtlinie relevant sind, so sollte sie, um Doppelarbeit zu vermeiden, in der Lage sein, diese Maßnahmen und Dokumente zu nutzen, um den Verpflichtungen in Bezug auf die Resilienzmaßnahmen gemäß der vorliegenden Richtlinie nachzukommen."

13. Die Rolle des von der kritischen Einrichtung gemäß Artikel 13 Absatz 3 der Richtlinie benannten Verbindungsbeauftragten ist für die wirksame Annahme und Umsetzung von Maßnahmen zur Stärkung der Resilienz von entscheidender Bedeutung, da er eine effiziente und wirksame Kommunikation und Koordinierung zwischen der kritischen Einrichtung und den zuständigen Behörden in Bezug auf die Verpflichtungen der kritischen Einrichtung und den allgemeinen Resilienzrahmen gewährleistet.

14. Die kritischen Einrichtungen werden aufgefordert, bei der Ergreifung von Maßnahmen zur Stärkung der Resilienz alle einschlägigen Objekte, Anlagen und Ausrüstungen auszumachen und grenzüberschreitende Aspekte und Aspekte gegenseitiger Abhängigkeiten zu berücksichtigen, da die von der Richtlinie erfassten Sektoren stark miteinander verflochten sind, einschließlich physischer, ökologischer, Cyber- und Lieferkettenaspekte. Eine Störung in einem Bereich kann zu Kaskadeneffekten auf dem gesamten Binnenmarkt führen und dadurch die Erbringung wesentlicher Dienste beeinträchtigen.

15. Die Risikobewertung durch kritische Einrichtungen und die nationale Risikobewertung bilden den wichtigsten Mechanismus zur Berücksichtigung gegenseitiger Abhängigkeiten. Im Rahmen der Risikobewertungen ist das Ausmaß der Abhängigkeit anderer Sektoren von dem wesentlichen Dienst, der von der kritischen Einrichtung – gegebenenfalls auch in benachbarten Mitgliedstaaten und Drittländern – erbracht wird, und das Ausmaß der Abhängigkeit der kritischen Einrichtung von den wesentlichen Diensten, der von anderen Einrichtungen in anderen Sektoren – gegebenenfalls auch in benachbarten Mitgliedstaaten und Drittländern – erbracht wird, zu bewerten und zu berücksichtigen.

16. Bei der Ergreifung von Maßnahmen zur Stärkung der Resilienz sollten kritische Einrichtungen in Erwägung ziehen, einschlägige internationale und europäische Standards zu berücksichtigen.

17. Die Besonderheiten kritischer maritimer Infrastruktur sollten berücksichtigt werden: Sie ist schwieriger zu überwachen und zu schützen; die Erkennung und Lokalisierung von Vorfällen sowie Reparaturen sind auf See zeitaufwendiger und kostspieliger.

B. PRÄVENTIONSMAßNAHMEN (Artikel 13 Absatz 1 Buchstabe a der Richtlinie)

18. Kritische Einrichtungen werden aufgefordert, Maßnahmen zu ergreifen, um ihre Resilienz durch die Verbesserung ihrer Fähigkeit zur Verhinderung von Ausfällen oder Störungen zu stärken. Diese Maßnahmen sollten in den in Artikel 13 Absatz 2 der Richtlinie genannten Resilienzplan aufgenommen und als Teil eines integrierten Systems und nicht als isolierte Komponenten betrachtet werden. Die Wirksamkeit einer einzelnen Maßnahme hängt von ihrer Wechselwirkung mit anderen Maßnahmen ab, einschließlich des physischen Schutzes von Räumlichkeiten, der Reaktion auf Störungen verursachende Sicherheitsvorfälle, ihrer Abwehr und der anschließenden Wiederherstellung sowie eines angemessenen Sicherheitsmanagements hinsichtlich der Mitarbeiter.

([13]) Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz) (ABl. L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

([14]) Sicherheitsbauteile kritischer Infrastrukturen sind Systeme, die verwendet werden, um die physische Integrität kritischer Infrastruktur oder die Gesundheit und Sicherheit von Personen und Eigentum zu schützen, die aber nicht notwendig sind, damit das System funktioniert (Artikel 3 Nummer 14 und Erwägungsgrund 55 der KI-Verordnung).

([15]) Anhang III Nummer 2 der KI-Verordnung.

19. Maßnahmen zur Katastrophenvorsorge und zur Anpassung an den Klimawandel sollten auf plausiblen Klimaprojektionen für die gesamte Lebensdauer der kritischen Infrastrukturen beruhen. Kritische Einrichtungen werden aufgefordert, kritische Infrastrukturen (z. B. Rechenzentren oder Umspannwerke) nicht in Hochrisikogebieten anzusiedeln, Maßnahmen zur strukturellen Verstärkung der betreffenden Infrastrukturen (z. B. Brandschutz, Widerstandsfähigkeit gegenüber Hochwasser, Dürre und Detonationen, Abdichtung gegen das Eindringen von Flüssigkeit) sowie nicht-strukturelle Maßnahmen (z. B. Schulungs- und Sicherheitsprotokolle) zu ergreifen, um Zusammenstöße, Explosionen, das Austreten gefährlicher Stoffe oder Strahlung zu verhindern, naturbasierte Lösungen wie die Integration grüner Infrastrukturen (z. B. wiederhergestellte Feuchtgebiete zur Absorption von Sturmfluten oder städtische Wälder zur Verringerung der Auswirkungen des Wärmeinseleffekts auf elektrische Betriebsmittel) zu finden, die unmittelbaren und langfristigen Veränderungen der Klimamuster zu berücksichtigen, die die Integrität des Systems im Laufe der Zeit beeinträchtigen könnten, wie extreme Hitze, Hochwasser und der Anstieg des Meeresspiegels, sich gegen Wasserknappheit zu rüsten, Stresstests durchzuführen, um sicherzustellen, dass die Einrichtung auch unter deutlich ungünstigeren Bedingungen (z. B. wärmere, kältere, feuchtere, trockenere, unbeständige oder nicht der Jahreszeit entsprechende Witterungsbedingungen) funktionieren kann.

20. Kritische Einrichtungen werden aufgefordert, die Einrichtung einer Datenbank für Sicherheitsvorfälle, die Einspeisung von Daten in EU-Datenbanken für Sicherheitsvorfälle ([16]) und die Einführung eines Systems zur systematischen Meldung von Sicherheitsvorfällen, das eine Ereignishistorie beinhaltet und nicht nur die Prävention von Sicherheitsvorfällen und die Risikominderung, sondern auch die Wiederherstellung von Objekten ermöglicht, in Erwägung zu ziehen.

21. Um menschliches Versagen zu verhindern, werden kritische Einrichtungen aufgefordert, festzustellen, welche Aufgaben fehleranfällig sind, und geeignete Gegenmaßnahmen zu ergreifen, darunter Automatisierung, kontinuierliche Mitarbeiterschulung, Aufsicht und klare Rechenschaftspflicht, detaillierte Prozessdokumentation, regelmäßige Audits und Inspektionen sowie die Entwicklung einer Kultur der Resilienz und Verantwortung.

22. Um sicherzustellen, dass die Resilienzmaßnahmen im Einklang mit der NIS-2-Richtlinie angewandt werden, werden kritische Einrichtungen aufgefordert, bei der Anwendung ihrer Resilienzmaßnahmen Maßnahmen zu berücksichtigen, die für die Sicherheit von Netz- und Informationssystemen im Sinne der NIS-2-Richtlinie relevant sind. Die in der Durchführungsverordnung (EU) 2024/2690 der Kommission ([17]) festgelegten Maßnahmen, die für bestimmte Arten von Einrichtungen in den Sektoren digitale Infrastruktur, Verwaltung von IKT-Diensten (Business-to-Business) und Anbieter digitaler Dienste im Sinne der NIS-2-Richtlinie ([18]) gelten, sowie die begleitenden ENISA-Umsetzungsleitlinien ([19]) können als weitere Referenz dienen.

23. In Bezug auf die Betriebstechnologie sollten kritische Einrichtungen die Möglichkeit der Umschaltung auf Handbetrieb und „Human-in-the-Loop"-Bestimmungen vorsehen, in denen die spezifischen Bedingungen und Anforderungen für das Eingreifen des Menschen und die manuelle Steuerung als Reaktion auf Gefahren festgelegt sind.

C. PHYSISCHE SCHUTZMAßNAHMEN (Artikel 13 Absatz 1 Buchstabe b der Richtlinie)

24. Kritische Einrichtungen werden aufgefordert, physische Maßnahmen zum Schutz vor natürlichen und vom Menschen verursachten Bedrohungen (z. B. hybride Bedrohungen, Sabotage, Terrorismus, kriminelle Handlungen, militärische Zielplanung/Zielplanung in Kriegszeiten, Spionage) zu ergreifen und Verfahrenskontrollen einzuführen, die dazu dienen, Störungen verursachende Sicherheitsvorfälle zu erkennen, abzuwenden, zu verzögern, abzuwehren, darauf zu reagieren und ihre Auswirkungen zu verringern.

([16]) Im Luftverkehr umfassen die einschlägigen EU-Datenbanken für Sicherheitsvorfälle das System der Agentur der Europäischen Union für Flugsicherheit zur Meldung von Störungen im Flugverkehr, die Register der Netzmanager über Sicherheitsvorfälle und das System zur Meldung von Ereignissen im Bereich der Luftsicherheit.

([17]) 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 (ABl. L, 2024/2690, 18.10.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2690/oj).

([18]) Gemäß Artikel 8 der Richtlinie über die Resilienz kritischer Einrichtungen stellen die Mitgliedstaaten sicher, dass bestimmte Bestimmungen der Richtlinie, einschließlich Artikel 13, nicht für die von ihnen in bestimmten Sektoren, einschließlich des Sektors digitale Infrastruktur, ermittelten kritischen Einrichtungen gelten. Die Mitgliedstaaten können nationale Vorschriften erlassen oder beibehalten, um ein höheres Maß an Resilienz für diese kritischen Einrichtungen zu erreichen, sofern diese Vorschriften mit dem geltenden Unionsrecht vereinbar sind. Verwaltung von IKT-Diensten (Business-to-Business) und Anbieter digitaler Dienste gehören nicht zu den im Anhang der Richtlinie über die Resilienz kritischer Einrichtungen aufgeführten Sektoren.

([19]) https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance.

25. Bei der Planung geeigneter und verhältnismäßiger Maßnahmen zur Stärkung der Resilienz gegenüber vom Menschen verursachten Bedrohungen sollten kritische Einrichtungen die Relevanz bestimmter Bedrohungsszenarien berücksichtigen. Insbesondere werden sie aufgefordert,

i) der Notwendigkeit von Protokollen für eine enge öffentlich-private Abstimmung Rechnung zu tragen, um die operative Zusammenarbeit mit den zuständigen Behörden zu unterstützen und einen angemessenen und gegenseitigen Fluss von Informationen über Bedrohungen und Sicherheitsvorfälle im Interesse einer gemeinsamen Lageerfassung sicherzustellen,

ii) im Falle potenzieller hybrider Bedrohungen durch staatliche Akteure, bei denen es sich – wenn es um kritische Einrichtungen geht – hauptsächlich um Sabotageversuche zur Herbeiführung von Störungen an Objekten und an Ausrüstung oder um Vorbereitungen auf solche Versuche (einschließlich Spionage/Überwachung) handelt, zu berücksichtigen, dass staatliche Akteure möglicherweise entsprechend anfällige oder ausnutzbare Stellvertreter (z. B. Einzelpersonen oder Gruppen) unterstützen und ihnen Anweisungen erteilen, um ihre Ziele zu erreichen, und dass staatliche Akteure möglicherweise koordinierte Angriffe über mehrere Angriffsvektoren in mehreren Bereichen und/oder unter Rückgriff auf mehrere Stellvertreter durchführen,

iii) andere potenzielle Bedrohungen, insbesondere solche, die sich aus Terrorismus und gewaltbereitem Extremismus, kriminellen Handlungen, militärischer Zielplanung, Insider-Bedrohungen, Aktivismus usw. ergeben, zu berücksichtigen.

26. Kritische Einrichtungen werden aufgefordert, Maßnahmen zur Absicherung der Umgebung (Abschreckung und Verzögerung) in Betracht zu ziehen, wie z. B. Hochsicherheitszäune (z. B. Kletterschutz/Schnittfestigkeit), verstärkte Wände, Tore, Abwehr feindlicher Fahrzeuge, Beschilderung und Beleuchtung (z. B. Warnsignale mit hoher Sichtbarkeit zur Abschreckung spontaner Eindringlinge und Sicherheitsbeleuchtung zur Beseitigung von Totzonen bei der Überwachung).

27. Der Zugang von Fahrzeugen, Personal und Waren zu den betreffenden Räumlichkeiten sollte über eine begrenzte Anzahl kontrollierbarer Checkpoints erfolgen. Direkte Zufahrtswege für Fahrzeuge sollten durch eine Kombination physischer Barrieren (z. B. feste und einziehbare Poller, natürliche Hindernisse oder andere Maßnahmen zur Verlangsamung der Geschwindigkeit) begrenzt werden, und der vorgeschriebene Höchstabstand zwischen benachbarten Barrieren sollte eingehalten werden, um das Eindringen von Fahrzeugen zu verhindern.

28. Die äußeren Zugänge (z. B. Tore, Türen) zu den betreffenden Räumlichkeiten sollten robust gebaut sein oder verstärkt werden und mit sicheren Scharnieren und Verriegelungsmechanismen aus- bzw. nachgerüstet werden. Die Rahmen des Gebäudes (z. B. von Fenstern, Dachfenstern) sollten ebenfalls mit Verriegelungsmechanismen und Schutzvorkehrungen (z. B. Stäbe, Gitter, Sicherheitsglas, Schutzmembranen) aus- bzw. nachgerüstet werden. Andersartige Zugänge (z. B. Dachluken, Schächte und Lüftungsöffnungen) zu Anlagen oder Objekten sollten ebenfalls gesichert werden, um zu verhindern, dass sie von Unbefugten geöffnet werden oder sich jemand daran zu schaffen macht.

29. Kritische Einrichtungen werden aufgefordert, die Überwachung der Umgebung und die Detektion in der Umgebung in Erwägung zu ziehen, um Übertretungen in Echtzeit zu erkennen (z. B. Installation von Alarmanlagen oder Einbruchmeldesystemen, einschließlich Innen- und Außensensoren). Diese sollten eine angemessene Erfassung des betreffenden Bereichs gewährleisten, einheitlichen Protokollen für die Überwachung und Reaktion unterliegen und regelmäßigen Funktionsprüfungen unterzogen werden. Legitime Erkennungen, Systemfehler und falsch positive Ergebnisse sollten analysiert und Abhilfemaßnahmen ergriffen werden, um die Integrität zu wahren.

30. Kritische Einrichtungen werden aufgefordert, in Erwägung zu ziehen, Videosysteme zu nutzen, die eine klare und umgebungsspezifische Echtzeitüberwachung und Aufzeichnungen der Überwachung der einschlägigen Objekte, Anlagen und Ausrüstungen sowie der Zugangswege und Zugänge zu den Räumlichkeiten bieten. Die zeitliche Synchronisierung der Überwachung, der Aufzeichnungsstatus und die Speicherfristen sollten regelmäßig überprüft werden. Die Einrichtungen sollten die Aufnahmen routinemäßig überprüfen, um sicherzugehen, dass Gesichter, Handlungen und Ereignisse nach möglichen Sicherheitsvorfällen zu den vorgesehenen forensischen Zwecken identifizierbar sind. Kritische Ersatzkomponenten (z. B. Speichermedien, Stromaggregate) sollten entsprechend in Reserve gehalten werden.

31. Kritische Einrichtungen werden aufgefordert, dafür zu sorgen, dass die Beleuchtungsanlagen eine gleichmäßige Beleuchtung der Eingänge, Parkplätze, Gehwege und Sichtfelder der Kameras ermöglichen, wobei Blendung und tiefer Schatten zu vermeiden sind, die die Erkennung oder Aufzeichnung behindern könnten. Die Notbeleuchtung sollte regelmäßig getestet werden. Abhilfemaßnahmen (z. B. Austausch von Lampen, Anpassung des Erfassungsbereichs, Zurückschneiden von Pflanzen) sollten regelmäßig durchgeführt werden.

32. Die Beschilderung sollte deutlich auf sicherheitsbezogene Beschränkungen und Überwachungsmaßnahmen hinweisen, klare Datenschutzhinweise enthalten und eindeutig die jeweiligen Zugangswege für Personal, Besucher und Lieferanten aufzeigen.

33. Kritische Einrichtungen werden aufgefordert, Maßnahmen zur Zugangskontrolle (Verweigerung des Zugangs) durch mehrstufige Sicherheitsbereiche, physische Zugangsverwaltung (z. B. Ausweislesegeräte, biometrische Scanner), Zugangsschleusen und verriegelbare Türen in Erwägung zu ziehen. Es sollte der Einsatz von Sicherheitspersonal vor Ort für Kontrollgänge und die Verwaltung der Kontrolle des Zugangs zu den betreffenden Einrichtungen, Eingängen oder Ausrüstungen in Betracht gezogen werden. Dem Sicherheitspersonal sollten auch Funktionen mit Blick auf die Reaktion auf Sicherheitsvorfälle übertragen werden. Es sollte engen und regelmäßigen Kontakt zu den zuständigen Strafverfolgungsbehörden und Akteuren im Verteidigungsbereich halten.

34. Räume und Einhausungen, in denen Infrastrukturen oder Anlagen für Strom, Wasser, Gas, Heizung, Lüftung, Klimatisierung, Telekommunikation, Sicherheit, Netze oder andere sensible Infrastrukturen oder Ausrüstungen untergebracht sind, sollten verschlossen sein und Zugangskontrollen unterliegen; dies sollte durch verhältnismäßige Maßnahmen ergänzt werden, mit denen verhindert wird, dass sie von Unbefugten geöffnet werden oder sich jemand daran zu schaffen macht.

35. Poststellen und Auslieferungslager sollten sich außerhalb relevanter Objekte, Anlagen, Ausrüstungen und stark genutzten Bereichen befinden und für die Absonderung und die sichere Untersuchung potenziell verdächtiger Gegenstände ausgerüstet sein. Das Personal sollte über klare Verfahren für den Umgang mit verdächtigen Gegenständen aufgeklärt sein, einschließlich Isolation, Deeskalation und Benachrichtigung der einschlägigen internen und externen Interessenvertreter. Für den Bedarfsfall sollten Öffnungswerkzeuge und persönliche Schutzausrüstung zur Verfügung stehen. Bei wertvollen oder kontrollierten Lieferungen sollte die Lieferkette vom Eingang bis zum Empfänger dokumentiert werden. Es sollten in regelmäßigen Abständen stichprobenartige Kontrollen durchgeführt und aufgezeichnet werden.

36. Für alle externen Objekte, Anlagen oder Ausrüstungen sollten ebenfalls verhältnismäßige Schutzmaßnahmen gelten. Alle physischen Schutzmaßnahmen, die von kritischen Einrichtungen ergriffen werden, müssen regelmäßigen Routineinspektionen und -wartungen unterzogen werden.

37. Maßnahmen in Bezug auf Zugangskontrollen für das Personal und die physische Informationssicherheit von sensiblen Daten oder Verschlusssachen entbinden nicht von den in der NIS-2-Richtlinie festgelegten Risikomanagementverpflichtungen im Bereich der Cybersicherheit ([20]).

38. Neben der ihnen in Teil F dieser Leitlinien zum Sicherheitsmanagement für die Mitarbeiter zur Verfügung stehenden Orientierungshilfe werden kritische Einrichtungen aufgefordert, ein einziges verbindliches Register physischer Schlüssel und (elektronischer) Zugangskennungen zu führen, einschließlich Ausstellungs-, Widerrufs- und Rückgabedaten. Verloren gegangene oder gestohlene Schlüssel oder Zugangskennungen sollten unverzüglich widerrufen werden, und Schlösser sollten mit neuen Schlüsseln ausgestattet oder ausgetauscht werden, wenn der Verdacht einer Kompromittierung besteht.

39. Kritische Einrichtungen werden aufgefordert, dafür zu sorgen, dass die Zugangsrechte dem Prinzip der minimalen Berechtigung folgen und regelmäßig oder bei Wechsel des Postens überprüft werden. Die Konzeption der betreffenden Räumlichkeiten sollte auf einer Einteilung in Bereiche basieren, die mittels entsprechender Maßnahmen für ausgewählte Personen (z. B. Unterscheidung zwischen öffentlichen Bereichen, Arbeitsbereichen, Sperrzonen und kritischen Bereichen) kontrolliert werden und für die eine Kombination aus physischen, technischen und administrativen Kontrollen gilt. Der Zugang sollte protokolliert werden. Besucher sollten über einen kontrollierten Zugang geleitet, registriert, mit einer sichtbaren Identifikation versehen und über den Empfang hinaus begleitet werden, es sei denn, es wurde eine andere Genehmigung erteilt. Diese Identifikation sollte unmittelbar nach dem Verlassen der Einrichtung deaktiviert werden. Die entsprechenden Verfahren sind einfach zu halten, zu dokumentieren und dem gesamten Personal, insbesondere dem Empfangs- und Sicherheitspersonal, mitzuteilen.

40. Bestände an sensiblen Informationen sollten so platziert, geschützt und gespeichert werden, dass das Risiko einer Beeinträchtigung der Integrität dieser Informationen (z. B. unbefugtes oder unbeabsichtigtes Einsehen, Manipulation, Diebstahl, Umweltschäden) verringert wird, und der Zugang sollte nach dem Grundsatz „Kenntnis nur, wenn nötig“ erfolgen.

41. Kritische Einrichtungen werden aufgefordert, ein Verzeichnis und/oder Register der Bestände an sensiblen Informationen zu erstellen und zu führen. Die Informationen sollten entsprechend ihrer Bedeutung für die Geschäftstätigkeit oder Sicherheit eingestuft werden. Die Einrichtungen sollten dann ein System nutzen, um Informationen zu dokumentieren (z. B. Zugangsbeschränkungen unterliegend, intern, öffentlich oder gleichwertiges) und sollten sie entsprechend kennzeichnen und handhaben. Die Vorschriften und Verfahren für die Einstufung und Handhabung sollten allen betroffenen Mitarbeitern mitgeteilt und regelmäßig überprüft werden. Dazu gehören Vorschriften für den Schreibtisch- und Bildschirmzugang zu Informationen und für die Erstellung oder Vervielfältigung von Informationen.

([20]) Artikel 21.

42. Gegebenenfalls sollten kritische Einrichtungen die geltenden nationalen Vorschriften für den Schutz von Verschlusssachen, die als für die nationale Sicherheit relevant erachtet werden, beachten.

43. Wenn externe Interessenvertreter Zugang zu Informationen benötigen, werden kritische Einrichtungen aufgefordert, die Ausarbeitung von Nutzerleitlinien und Geheimhaltungsvereinbarungen oder gegebenenfalls anderer einschlägiger vertraglicher Mechanismen zu erwägen.

44. Alle Einrichtungen mit Beständen an sensiblen Informationen (z. B. Archive, Serverräume) oder andere Bereiche, denen sensible Informationen entnommen werden könnten, sollten als Sicherheitszonen mit besonders strengen Kontrollen im Hinblick auf den Zugang, das Einsehen und die Entnahme ausgewiesen und überwacht werden.

45. Kritische Einrichtungen sollten sicherstellen, dass die Zugangsrechte regelmäßig kontrolliert und überprüft werden. Für sensible Informationen sollten Aufbewahrungsfristen festgelegt werden. Nach Ablauf dieser Fristen oder wenn andere Entwicklungen eine Neueinstufung der Informationen erfordern, sollten geeignete Maßnahmen ergriffen werden, um diese Daten zu bereinigen oder zu vernichten.

46. In Bezug auf die von unbemannten Systemen ([21]) (Drohnen) ausgehenden Bedrohungen werden kritische Einrichtungen aufgefordert, Maßnahmen zu ergreifen, um die Erkennung, Verfolgung und Identifizierung unbemannter Systeme (z. B. Radar, Funkfrequenzscanner, Tageslicht-/Wärmebildkameras, akustische Sensoren) zu erleichtern. Soweit möglich, sollten kritische Einrichtungen auch mit Anbietern von Telekommunikationsdiensten zusammenarbeiten, um Zugang zu Daten zu erhalten, die von Technologien der integrierten Sensorik und Kommunikation (Integrated Sensing And Communication – ISAC) generiert werden, um unerlaubte Drohnenaktivitäten innerhalb ihres Sicherheitsbereichs aufzudecken.

47. Der Bedrohung durch Spionage/Überwachung durch nicht kooperative unbemannte Systeme sollte entgegengewirkt werden, indem die Sicht (aus der Luft, von See oder vom Boden aus) auf sensible Anlagen oder Ausrüstungen behindert wird (z. B. Abdeckung oder Platzierung an einer anderen Stelle) und gegebenenfalls sichergestellt wird, dass diese in geschlossenen Einrichtungen untergebracht sind.

48. Kritische Einrichtungen sollten auch das Risiko von gegen Einrichtungen, Anlagen oder Ausrüstung gerichtete Sabotageakte durch nicht kooperative unbemannte Systeme mindern. Beispiele für Risikominderungsmaßnahmen sind Drohnenabwehrnetze oder Schutzdächer sowie andere strukturverstärkende Maßnahmen wie detonationsfeste Fenster, Verstärkung der Dachkonstruktion oder vollständige bauliche Einhausungen.

49. Kritische Einrichtungen können in Erwägung ziehen, geografische Zonen für die Bewältigung und Eindämmung von Risiken im Zusammenhang mit unbefugtem oder unsicherem Drohnenbetrieb in der Nähe ihrer Räumlichkeiten einzurichten. Entscheidungen zur Einrichtung solcher Zonen sollten von Fall zu Fall einer Risiko- und Verhältnismäßigkeitsprüfung unterzogen werden, wobei die potenzielle Sensibilität von Informationen zu berücksichtigen ist, die durch die Veröffentlichung geografischer Daten über kritische Einrichtungen offengelegt werden könnten. Zu diesem Zweck müssten die Einrichtungen mit den zuständigen nationalen Behörden zusammenarbeiten, damit sichergestellt wird, dass die einschlägigen geografischen Zonen im Einklang mit dem geltenden Luftverkehrsrahmen ordnungsgemäß festgelegt und digital veröffentlicht werden. Diese Zonen sollten es Drohnenbetreibern zumindest ermöglichen, Geo-Sensibilisierungsfunktionen zu nutzen. Im Zuge der Weiterentwicklung der technischen Fähigkeiten und sofern der Rechtsrahmen es gestattet, können kritische Einrichtungen auch die schrittweise Einführung und Nutzung von Geofencing-Funktionen erwägen. Geofencing kann als vorbeugende Schutzmaßnahme dienen, indem die Wahrscheinlichkeit eines unbeabsichtigten Eindringens konformer Drohnen in Schutzzonen verringert wird. Kritische Einrichtungen sollten eine direkte operationelle Verbindung zum Verwalter der geografischen Zone halten. Dadurch könnte rechtzeitig erkannt werden, ob es sich bei Drohnentätigkeiten in ihrer Nähe um erlaubte oder nicht erlaubte Drohnentätigkeiten handelt, und könnten die Lageerfassung und die Koordinierung mit den zuständigen Behörden verbessert werden.

50. Es ist von entscheidender Bedeutung, Partnerschaften und die Kommunikation mit Drohnenabwehrbeauftragten in lokalen Strafverfolgungs- und Verteidigungsbehörden oder mit anderen Akteuren, die gesetzlich mit Risikominderungsaufgaben (z. B. Einsatz von Störsendern, Spoofing und andere kinetische oder nicht kinetische Maßnahmen) betraut sind, zu stärken. Zu diesem Zweck werden kritische Einrichtungen aufgefordert, den Einsatz von Drohnenabwehrsystemen zum Schutz ihrer Umgebung im Einklang mit dem einschlägigen Rechtsrahmen zu erleichtern.

([21]) Mitteilung COM(2026)81 der Kommission vom 11. Februar 2026 „Aktionsplan zur Drohnen- und Drohnenabwehrsicherheit".

D. REAKTIONS-, ABWEHR- UND BEGRENZUNGSMAßNAHMEN (Artikel 13 Absatz 1 Buchstabe c der Richtlinie)

51. Kritische Einrichtungen werden aufgefordert, die folgenden Maßnahmen zur Begrenzung der Folgen von Sicherheitsvorfällen in Erwägung zu ziehen.

a) Externes Krisen- und Katastrophenmanagement: Maßnahmen zur Begrenzung der negativen externen Folgen eines schwerwiegende Störungen verursachenden Sicherheitsvorfalls und rasche Unterrichtung der zuständigen Krisen- und Katastrophenmanagementbehörden, damit externe Schutzmaßnahmen ergriffen werden können. Dies erfordert eine enge Abstimmung mit den zuständigen Behörden, die Einrichtung bewährter Kommunikationskanäle sowie regelmäßige Krisen- und Katastrophenmanagementübungen.

b) Externe Unterstützung: Maßnahmen zur wirksamen Integration der externen Unterstützung in die Maßnahmen zur Reaktion vor Ort (einschließlich des Managements schwerer Unfälle, Abhilfe- und Notfallmaßnahmen).

c) Konzeption von ausfallsicheren Infrastrukturen, sodass gewährleistet ist, dass Störungen die Sicherheit der Menschen (einschließlich der Sicherheit des Personals) nicht beeinträchtigen und die Auswirkungen von Kaskadeneffekten auf andere Anlagen begrenzt werden. Durch „Safe-to-fail"-Funktionen können bei einem Ausfall wesentliche Funktionen der Infrastruktur aufrechterhalten oder kontrollierte Abschaltverfahren unterstützt werden, die Schäden an der Ausrüstung verhindern und gewährleisten, dass die Ausrüstung wieder in Betrieb genommen werden kann, sobald die Bedingungen dies zulassen. Die Aufrechterhaltung kritischer lebenserhaltender Bedingungen oder der passiven Überlebensfähigkeit kann durch eine angemessene Speicherkapazität, die Kontrolle über die Wärmekapazität, eine angemessene Notversorgung und die Sicherheit von Gefahrstoffen erreicht werden.

52. Kritische Einrichtungen werden aufgefordert, bei der Konzeption der „Safe-to-fail"-Infrastruktur, die folgenden Elemente zu berücksichtigen: die Speicherkapazität, die in Worst-Case-Ausfallszenarien erforderlich ist, um kritische lebenserhaltende Bedingungen aufrechtzuerhalten, die zur Aufrechterhaltung kritischer Betriebsabläufe und zur Unterstützung der kontrollierten Abschaltung des Infrastrukturbetriebs erforderliche Notversorgung, die Sicherheit aller in kritischen Infrastrukturen gelagerten oder vorhandenen Gefahrstoffe, wobei sicherzustellen ist, dass sie in die Kodierungs- und Managementpläne für Gefahrstoffe aufgenommen und im Falle eines Ausfalls der Infrastrukturen angemessen gesichert werden, sowie thermische Sicherheitsmaßnahmen für kritische Infrastrukturanlagen, in denen Personal oder temperaturempfindliche Ausrüstung untergebracht sind. Diese Maßnahmen können sowohl Wärme- als auch Kälteerzeugungsfähigkeiten umfassen, um schwere Schäden aufgrund extremer Temperaturen bei länger dauernden Störungen zu verhindern.

53. Kritische Einrichtungen werden aufgefordert, Maßnahmen zu ergreifen, um die Verfügbarkeit und die Wartungs- und Reparaturkapazitäten sicherzustellen und ihren Versorgungsbedarf klar zu definieren, die Versorgungsquellen mittels alternativer Anbieter und Versorgungswege zu diversifizieren, die Infrastruktur zu stärken, Redundanzen zu implementieren und Backup-Systeme mit Spezifikationen für die Funktion, die Dauer und die Wiederherstellungspriorität einzurichten.

54. Kritische Einrichtungen werden aufgefordert, geeignete Maßnahmen zu ergreifen, um insbesondere bei Inanspruchnahme von Hochrisikoanbietern die Integrität von in der Ausrüstung verwendeten IT-Netzen, -Systemen und -Softwarelösungen und den Schutz gegen Interferenzen durch Funkfrequenzsignale und Cyberangriffe zu gewährleisten.

55. Alternative Stromversorgungssysteme können Generatoren und Batterien für die unterbrechungsfreie Stromversorgung (USV) umfassen. Backup-Systeme sollten regelmäßig getestet werden; die autonome Stromversorgung sollte für mindestens 72 Stunden gewährleistet sein, und es sollten Lieferantenverträge zur Leistung von Soforthilfe (Versorgung, Interventionen und Reparaturen) aktiviert werden.

56. Im Hinblick auf die Resilienz der Wasserversorgung können kritische Einrichtungen den Wasserverbrauch bei Störungen auf kritische Funktionen beschränken und alternative Quellen wie Reservebrunnen, Speichertanks, tragbare Aufbereitungsanlagen und flexible Speicheroptionen nutzen. Kritische Einrichtungen im Trinkwassersektor werden aufgefordert, vorrangige zu beliefernde Orte zu ermitteln, um eine angemessene Reaktion in Notfallsituationen oder bei Versorgungsunterbrechungen zu gewährleisten. Wenn kritische Einrichtungen Resilienzmaßnahmen ergreifen, müssen sie sicherstellen, dass Wasser für den menschlichen Gebrauch die in der Richtlinie (EU) 2020/2184 festgelegten Qualitätsstandards erfüllt ([22]).

([22]) Richtlinie (EU) 2020/2184 des Europäischen Parlaments und des Rates vom 16. Dezember 2020 über die Qualität von Wasser für den menschlichen Gebrauch (Neufassung) (ABl. L 435 vom 23.12.2020, S. 1).

57. Bei anderen sektorspezifischen Versorgungsleistungen (z. B. Warmwasser, Kaltwasser, Dampferzeuger) und Versorgungsgütern (z. B. Chemikalien, Rohstoffe, Ersatzteile) sollte bei der Notfallplanung in den Lieferketten gegebenenfalls ein Wechsel von zeitorientierten („just in time“) zu bedarfsorientierten Bestandsmodellen („just in case“) erwogen werden. Alternative Systeme sollten vorab festgelegte Reserveressourcen und -güter (Puffer und Sicherheits-/Notfallvorräte) umfassen.

58. Kritische Einrichtungen werden aufgefordert, umfassende Wartungsprogramme auf der Grundlage von Herstellerempfehlungen, Betriebserfahrungen und Risikobewertungen zu entwickeln. Die vorausschauende Wartung kann mithilfe fortschrittlicher Überwachungstechnologien mit integrierten Sensornetzen erfolgen. Eine regelmäßige und vorausschauende leistungsbasierte Wartung, bei der Datenanalysen und KI-Tools zur Überwachung des Alterns und zur Vorhersage von Ausfällen eingesetzt werden, könnte sich zur Optimierung des Zeitplans für alle erforderlichen Arbeiten eignen. Es sollten klare Protokolle für die Reaktion auf Warnmeldungen des Überwachungssystems festgelegt werden, einschließlich der Überprüfung von Warnmeldungen, der Bewertung der Dringlichkeit und der Mobilisierung von Wartungsressourcen. In diesen Protokollen sollten Eskalationsverfahren für Situationen festgelegt werden, die sofortige Aufmerksamkeit erfordern. Die automatisierte Überwachung sollte durch regelmäßige Inspektionen der Infrastrukturen ergänzt werden.

59. In Bezug auf die Governance sollte kritischen Einrichtungen bewusst sein, dass Resilienz Teil der gesamten Governance-Struktur sein muss – von der höchsten bis zur untersten Ebene. Sie sollten Resilienzziele festlegen und eine Resilienzstrategie, -politik und -planung annehmen, diese den einschlägigen Interessenvertretern nach dem Grundsatz „Kenntnis nur, wenn nötig“ mitteilen und regelmäßig Überprüfungen durchführen. Dabei sollte vorhandenen Schwachstellen und der Frage Rechnung getragen werden, wie es besser gelingen könnte, einen Sicherheitsvorfall zu verhindern, sich davor zu schützen, darauf zu reagieren, einen solchen abzuwehren, die Folgen eines solchen Vorfalls zu begrenzen, einen Sicherheitsvorfall aufzufangen, ihn zu bewältigen und die anschließende Wiederherstellung zu gewährleisten.

60. Kritische Einrichtungen werden aufgefordert, klare Entscheidungshierarchien festzulegen. Auf der Leitungsebene und in Funktionen, die das Resilienz- oder Risikomanagement umfassen, sollten entsprechende Kompetenzen im Bereich Resilienz konsolidiert werden, um eine angemessene resilienzbezogene Strategie, Politik und operative Planung zu gewährleisten. Kritische Einrichtungen werden aufgefordert, die Ernennung eines Resilienzbeauftragten in Erwägung zu ziehen und für eine klare Abgrenzung zwischen Koordinierungsfunktionen und Zuständigkeiten für die Umsetzung der Resilienzziele zu sorgen.

61. In diesem Zusammenhang ist auch der Aufbau und die Formalisierung der Zusammenarbeit mit den zuständigen Behörden, einschließlich politischer Entscheidungsträger, Strafverfolgungsbehörden, Notdiensten und Akteuren im Verteidigungsbereich, von Bedeutung. Kritische Einrichtungen werden aufgefordert, die Aufgaben und Verfahren für den Informationsaustausch, die Meldung und Koordinierung von Sicherheitsvorfällen und die gegenseitigen Erwartungen klarzulegen.

62. Der Aufbau und die Formalisierung einer Zusammenarbeit mit einschlägigen privaten Akteuren im Sektor der Einrichtung, in anderen Sektoren und in anderen Mitgliedstaaten kann ebenfalls in Betracht gezogen werden.

63. Es sollten Krisenkommunikationsprotokolle festgelegt werden, um bei Sicherheitsvorfällen eine zeitnahe und korrekte Weitergabe von Informationen an interne und externe Interessenvertreter (einschließlich Kunden und Öffentlichkeit) zu gewährleisten. Kritische Einrichtungen sollten über vorab genehmigte Kommunikationsvorlagen, Abläufe für die Benachrichtigung der Interessenvertreter und Mehrkanal-Kommunikationsfähigkeiten, einschließlich redundanter Systeme, verfügen. Die Kommunikation sollte an unterschiedliche Zielgruppen angepasst werden, einschließlich unter Berücksichtigung mehrerer Sprachen und der Barrierefreiheitsanforderungen.

64. Eine Konzeption mit Redundanzen auf mehreren Ebenen sorgt dafür, dass Dienste grenzüberschreitend sowie auf nationaler, regionaler und lokaler Ebene mit wirksamer Interoperabilität erbracht werden können.

65. Kritische Einrichtungen werden aufgefordert, dafür zu sorgen, dass die Notfallverfahren Mehrkanal-Warnsysteme mit Geotargeting-Fähigkeiten wie den weltraumgestützten Galileo-Satellitendienst für Notfallwarnungen, klare Befehlsketten für die Kommunikation, einschließlich benannter Sprecher, und gefahrenspezifische Standardarbeitsanweisungen (Standard Operating Procedures – SOP), die auf standortspezifische Risiken zugeschnitten sind, umfassen. Kritische Einrichtungen sollten über eine Notfallausrüstung verfügen, Notfallteams benennen und schulen und sicherstellen, dass Evakuierungsverfahren zugänglich sind und regelmäßig entsprechende Übungen stattfinden.

E. WIEDERHERSTELLUNGSMAßNAHMEN (Artikel 13 Absatz 1 Buchstabe d der Richtlinie)

66. Um die Aufrechterhaltung des Betriebs zu gewährleisten, werden kritische Einrichtungen aufgefordert, Redundanzmaßnahmen in Erwägung zu ziehen, mit denen sichergestellt wird, dass wesentliche Dienste bei Ausfall der Primärsysteme weiterhin erbracht werden können. Solche Maßnahmen können umfassen: Ermittlung der spezifischen, besonders kritischen Teildienste, sodass diese als erste wiederhergestellt werden (Rangfolge der Dienste), Aufrechterhaltung der Fähigkeit zum manuellen Betrieb der Hardware bei Ausfall oder Manipulation der automatisierten oder KI-gestützten Systeme sowie Wiederherstellung der Belegschaftsstärke bei einem Störungen verursachenden Sicherheitsvorfall.

67. Alternative Standorte für die Wiederherstellung nach einem Notfall können heiße Standorte (vollständig eingerichtet und sofort nutzbar), warme Standorte (teilweise eingerichtet) oder kalte Standorte (müssen nach einer Störung noch eingerichtet werden) sein. Die Ausweichstandorte sollten ausreichend weit von den Primäranlagen entfernt sein, gleichzeitig aber zugänglich bleiben. Nach Möglichkeit sollten mobile Anlagen (z. B. Kommandozentralen) in Betracht gezogen werden. Backups sollten an physisch getrennten oder logistisch abgetrennten Orten aufbewahrt werden.

68. Unbeschadet der NIS-2-Richtlinie ([23]) sollten kritische Einrichtungen auf der Grundlage von Abschätzungen der Folgen für den Betrieb (Business Impact Assessments – BIA) umfassende Pläne zur Aufrechterhaltung des Betriebs (Business Continuity Plans – BCP) entwickeln und pflegen, in denen die kritischen Funktionen, die Prioritäten für die Wiederherstellung und die Vorgaben für die Wiederherstellungszeit (Recovery Time Objectives – RTO) und für die Wiederherstellungspunkte (Recovery Point Objectives – RPO), einschließlich des Abschlusses von Dienstgütevereinbarungen (Service Level Agreements – SLA), festgehalten sind. In den BCP sollten klare Aktivierungskriterien, die Mittelzuweisung, die Aufgabenverteilung und die Koordinierungsmechanismen für die Phasen Reaktion, Wiederherstellung, Wiederaufnahme und Wiedereinsetzung festgelegt werden. Sie sollten in geplanten Zeitabständen sowie nach erheblichen Sicherheitsvorfällen oder Änderungen am Betrieb getestet, überprüft und aktualisiert werden.

69. Die Krisenmanagementverfahren sollten Befehlsstrukturen für Sicherheitsvorfälle (Incident Command Structures – ICS) mit klar definierten Entscheidungsbefugnissen und dokumentierten Aktionsplänen für Sicherheitsvorfälle umfassen. Kritische Einrichtungen sollten die Einrichtung von Krisenteams mit vordefinierten Rollen, Eskalationsprotokollen, angemessener Schulung und Kommunikationskanälen (primär und alternativ) in Erwägung ziehen, um eine rasche und koordinierte Reaktion auf Störungen verursachende Sicherheitsvorfälle zu gewährleisten.

70. Bei der Personalplanung sollte dem Bedarf an Kapazitätspuffern Rechnung getragen werden, indem ein Dienstplan für Zeiten erhöhten Personalbedarfs, Schulungsprogramme und vorab festgelegte Vereinbarungen über gegenseitige Hilfe mit Partnerorganisationen aufrechterhalten werden. Kritische Einrichtungen sollten Kompetenzrahmen und Nachfolgepläne entwickeln, um bei kritischen Aufgaben entsprechende Solidität zu gewährleisten und die Betriebsfähigkeit bei längeren Störungen oder Personalengpässen aufrechtzuerhalten.

71. Um eine wirksame Wiederherstellung nach Sicherheitsvorfällen zu gewährleisten, sollten kritische Einrichtungen über abgestufte Wiederanlaufprotokolle verfügen, bei denen der Wiederherstellung kritischer Funktionen auf der Grundlage von Risikobewertungen oder BIA-Ergebnissen Vorrang eingeräumt wird. Diese Protokolle sollten systematische Validierungsverfahren für kritische Systeme, umfassende Tests der Datenintegrität und -funktionalität, Qualitätskontrollmaßnahmen und einen kontrollierten Übergang vom Notfall- zum Normalbetrieb durch schrittweise Kapazitätserhöhungen und Leistungsüberwachung umfassen.

72. Bei Untersuchungen nach einem Sicherheitsvorfall sollten strukturierte Methoden wie eine Ursachenanalyse verwendet werden, um systemische Ursachen anstatt nur sich unmittelbar zeigende Anzeichen ausfindig zu machen. Nach jeder Übung und jedem tatsächlichen Sicherheitsvorfall sollten nach Maßnahmen erfolgende Überprüfungen (After Action Reviews – AAR) durchgeführt werden, um die gewonnenen Erkenntnisse zu erfassen, wobei die Ergebnisse systematisch festgehalten und in aktualisierte Verfahren, Schulungsprogramme und Risikobewertungen integriert werden sollten, um ein erneutes Auftreten zu verhindern und die organisatorische Resilienz zu stärken.

73. In Bezug auf die Lieferketten ist Resilienz von entscheidender Bedeutung, wenn es um die Wiederherstellung nach Störungen verursachenden Sicherheitsvorfällen geht. Im Einklang mit ihren Risikobewertungen sollten kritische Einrichtungen in Erwägung ziehen, die Lieferkette für die Erbringung ihrer wesentlichen Dienste zu kartieren, langfristige Strategien für die Resilienz der Lieferkette zu entwickeln und den Notfallplan für die Lieferkette regelmäßig zu überprüfen und zu aktualisieren. Sie werden aufgefordert, alternative Lieferketten für den Fall zu ermitteln, dass es bei ihrem/ihren Hauptlieferanten zu Störungen kommt.

([23]) Insbesondere Artikel 21 Absatz 2 Buchstabe c der NIS-2-Richtlinie.

74. Kritische Einrichtungen sollten eine strategische Bevorratung in Erwägung ziehen, einschließlich Sicherheitsvorräten, Mechanismen für eine rasche Neuversorgung und eine externe, vor gängigen Bedrohungen geschützte Lagerung, damit es bei Störungen der Lieferkette nicht zu Unterbrechungen der Erbringung wesentlicher Dienste kommt.

75. Der Abschluss förmlicher Verträge mit anderen, im selben Sektor tätigen Einrichtungen über die gemeinsame Nutzung von Ressourcen, Ausrüstung oder Personal während weitreichender Wiederherstellungsmaßnahmen sollte ebenfalls in Betracht gezogen werden.

F. F. MAßNAHMEN ZUM SICHERHEITSMANAGEMENT HINSICHTLICH DER MITARBEITER (Artikel 13 Absatz 1 Buchstabe e der Richtlinie)

76. Personalbezogene Bedrohungen sollten bewertet und angegangen werden, um das Risiko von menschlichem Versagen, Sabotage, Insider-Bedrohungen und Fehlzeiten aufgrund von Krankheit, Notfällen oder externen Bedrohungen zu mindern. Kritische Einrichtungen werden aufgefordert, Kategorien von Personal, das kritische Funktionen ausübt, festzulegen, und entsprechende Listen zu erstellen, einschließlich des Personals externer Dienstleister (Auftragnehmer und Unterauftragnehmer).

77. Bei der Erstellung dieser Listen sollten die kritischen Einrichtungen die Besonderheiten der erbrachten wesentlichen Dienste berücksichtigen und diese Dienste mit dem an ihrer Erbringung beteiligten Personal verknüpfen. Zu diesem Zweck sollten kritische Einrichtungen ein klares, umfassendes und aktuelles Verzeichnis dieser Personalkategorien führen.

78. Neben den oben genannten Erwägungen im Zusammenhang mit den Zugangsrechten werden kritische Einrichtungen aufgefordert, festzulegen, wem und unter welchen Bedingungen Zugang zu Räumlichkeiten, kritischen Infrastrukturen und sensiblen Informationen gewährt wird. Es sollten wirksame Verfahren für die Gewährung und den sofortigen Entzug des physischen Zugangs und des Systemzugangs vorhanden sein, und die Zugangsrechte sollten strikt durchgesetzt werden.

79. Kritische Einrichtungen werden aufgefordert, Zugangsrechte nur nach dem Grundsatz „Kenntnis nur, wenn nötig“ bzw. „Zugang nur, wenn nötig“ einzuräumen; dem Personal sollte nur das für die Wahrnehmung seiner Aufgaben erforderliche Mindestmaß an Zugang gewährt werden. Es sollten Umsetzungsstrategien wie eine funktionsbasierte Zugangskontrolle (Role Based Access Control – RBAC) ([24]), eine leistungsstarke Authentifizierung und ein leistungsstarkes Identitätsmanagement ([25]), Aufgabentrennung ([26]), zeitliche Beschränkungen und ein „Just-in-time“-Zugang ([27]) eingeführt und regelmäßige Audits und Überprüfungen durchgeführt werden.

80. In Bezug auf Zuverlässigkeitsüberprüfungen und zur Gewährleistung eines hohen Maßes an Sicherheit für die Mitarbeiter ist es wichtig, robuste interne Verfahren für die Beantragung von Zuverlässigkeitsüberprüfungen gemäß Artikel 14 der Richtlinie einzurichten und die Kategorien von Personen festzulegen, die einer solchen Zuverlässigkeitsüberprüfung unterzogen werden müssen. Es sollten auch Verfahren für den Umgang mit Mitarbeitern eingerichtet werden, denen die Sicherheitsermächtigung entzogen wurde.

81. Kritische Einrichtungen werden aufgefordert, ein System für Zuverlässigkeitsüberprüfungen einzurichten, in dessen Rahmen festgelegt wird, welche Funktionen sensibel sind, für welche Funktionen direkter Zugang oder Fernzugang zu Räumlichkeiten, Informationen oder Steuerungssystemen gewährt wird und welche Arten von Kontrollen bei den einzelnen sensiblen Funktionen durchzuführen sind, z. B. Identitätsüberprüfung oder Prüfung von Strafregister, Beschäftigungsnachweisen und Ausbildung.

82. Gegebenenfalls sollten die Maßnahmen mit den die Zuverlässigkeitsüberprüfung betreffenden Tätigkeiten gemäß der Durchführungsverordnung (EU) 2024/2690 der Kommission ([28]) im Einklang stehen. Zudem sollte die Kohärenz mit den von der betreffenden Einrichtung gemäß Artikel 21 Absatz 2 Buchstabe i der NIS-2-Richtlinie im Hinblick auf die Sicherheit des Personals ergriffenen Maßnahmen sichergestellt werden.

([24]) Dies könnte bedeuten, dass spezifische Funktionen wie „physischer Sicherheitsbediensteter“ definiert werden, vorab festgelegte Zugangsrechte zugeteilt werden und das Personal den entsprechenden Funktionen zugewiesen wird.

([25]) Hierzu zählen beispielsweise eine Multi-Faktor-Authentifizierung und eindeutige Kennungen.

([26]) Dies könnte bedeuten, die Zugangskontrolle so zu gestalten, dass eine einzelne Person nicht über ausreichende Zugangsrechte verfügt, um einen kritischen Prozess mit hohem Risiko alleine abzuschließen. So sollte beispielsweise die Person, die eine Systemänderung genehmigt, nicht mit der Person identisch sein, die die Änderung durchführt.

([27]) Mitarbeitern sollte der Zugang nur vorübergehend gewährt werden, wenn sie ihn für bestimmte Aufgaben tatsächlich benötigen. Die Zugangsrechte sollten anschließend unverzüglich widerrufen werden. Es sollte eine Regelung geben, nach der die Zugangsrechte gegebenenfalls außerhalb spezifischer Arbeitszeiten eingeschränkt werden.

([28]) Nummer 10.2 des Anhangs.

83. Die Anforderung, dass das Personal angemessen qualifiziert und geschult sein muss, und die Bereitstellung solcher Schulungen, tragen zur Gewährleistung eines angemessenen Sicherheitsmanagements hinsichtlich der Mitarbeiter und zur Sensibilisierung des Personals für Resilienzmaßnahmen bei und untermauern die von der betreffenden kritischen Einrichtung ergriffenen Resilienzmaßnahmen. Die Risikobewertung kritischer Einrichtungen, die Art der von ihnen erbrachten wesentlichen Dienste und die geplanten oder ergriffenen Maßnahmen sollten maßgeblich für die Art und den Umfang der Schulungen sein, derer ihr Personal bedarf, damit dieses nicht nur allgemein über Resilienzmaßnahmen informiert ist, sondern auch technisch und verfahrenstechnisch in der Lage ist, seine Aufgaben auf resiliente Weise wahrzunehmen.

84. Die Schulungs- und Qualifikationsanforderungen beziehen sich unter anderem auf die Risikobewertung (z. B. für das Führungspersonal/das mit der Einhaltung der Vorschriften zur Risikominderung betraute Personal), die Aufrechterhaltung des Betriebs und das Krisenmanagement (z. B. für das für die Aufrechterhaltung des Betriebs zuständige Personal), die physische Sicherheit (z. B. für Sicherheitspersonal und Mitarbeiter mit Zugangsrechten), die Reaktion auf Sicherheitsvorfälle und deren Eindämmung (z. B. für Betriebspersonal, benannte Notfall-Reaktionsteams), die Zugangskontrolle und die Sicherheitsüberprüfung (Personalabteilung, Sicherheitspersonal und Führungskräfte mit kritischen Funktionen) und die allgemeine Sensibilisierung für Resilienzmaßnahmen (aller Mitarbeiter).

85. Die Qualifikationsanforderungen hängen von den Besonderheiten der betreffenden kritischen Einrichtung und den von ihr erbrachten wesentlichen Diensten ab. Ziel dieser Anforderungen sollte es sein, sicherzustellen, dass das Personal im Rahmen der von kritischen Einrichtungen ergriffenen Resilienzmaßnahmen über die Kompetenz verfügt, die Aufgaben auszuführen, die in der Risikobewertung und dem Resilienzplan und in den im Resilienzplan enthaltenen Protokollen zur Aufrechterhaltung des Betriebs und zur Reaktion auf Sicherheitsvorfälle festgelegt sind. Die Qualifikationsanforderungen beziehen sich auf betriebliche, technische und organisatorische Aufgaben sowie auf Aufgaben im Zusammenhang mit dem Management, der Sicherheit und der Sicherheitsüberprüfung. Die erforderlichen Qualifikationen sollten in der internen Resilienz- und Personalpolitik der betreffenden kritischen Einrichtung festgelegt werden.

### G. SENSIBILISIERUNGSMAßNAHMEN (Artikel 13 Absatz 1 Buchstabe f)

86. Ein solides Programm zur Sensibilisierung des Personals für die von der kritischen Einrichtung ergriffenen Resilienzmaßnahmen und zur Schaffung einer Sicherheitskultur ist von wesentlicher Bedeutung. Das Personal ist in jeder Phase des Resilienzzyklus von entscheidender Bedeutung – von der Verhinderung von Störungen verursachenden Sicherheitsvorfällen über die Eindämmung von Insider-Bedrohungen bis hin zur Reaktion auf Sicherheitsvorfälle durch die Aktivierung der einschlägigen Verfahren, die Meldung von Vorfällen, die Gewährleistung der Aufrechterhaltung des Betriebs und die Wiederherstellung des vorherigen Zustands. Ohne sachkundiges Personal würden möglicherweise selbst die besten technischen, sicherheitstechnischen und organisatorischen Maßnahmen fehlschlagen.

87. Vorbehaltlich sensibler Informationen und nach dem Grundsatz „Kenntnis nur, wenn nötig“, wird mit der Sensibilisierung für Resilienzmaßnahmen eine optimale Resilienzkultur geschaffen, die dafür sorgt, dass Resilienz beim Personal als ein gemeinsamer Wert verstanden wird und mit der das Risiko von Insider-Bedrohungen oder Social Engineering verringert wird.

88. Sensibilisierungsmaßnahmen sollten in Verbindung mit den Maßnahmen für grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit gemäß der NIS-2-Richtlinie ([29]) ergriffen werden.

89. Schulungen, die von einer kritischen Einrichtung organisiert werden, müssen den unter den Nummern 82 und 83 genannten Schulungsanforderungen der kritischen Einrichtung entsprechen. Die Schulungen sollten sich auf die von der Einrichtung gemäß Artikel 13 Absatz 1 Buchstaben a bis e der Richtlinie ergriffenen Resilienzmaßnahmen erstrecken und somit den gesamten Resilienzzyklus abdecken, das heißt: Verständnis der Bedrohungslage, der Rolle der kritischen Einrichtung bei der Aufrechterhaltung essenzieller gesellschaftlicher Funktionen und der schwerwiegenden Folgen von Störungen bei der Erbringung der Dienste, Erkennen und unverzügliches Melden von verdächtigen Tätigkeiten, Schwachstellen oder ungewöhnlichen Vorfällen und Reaktion auf Sicherheitsvorfälle und Eindämmung selbiger. Personal, das kritische Funktionen wahrnimmt, sollte funktionsspezifische Schulungen erhalten.

90. Kritische Einrichtungen werden ferner aufgefordert, Schulungen zu geschlechtersensiblen Ansätzen in Erwägung zu ziehen, die zusammen mit der Überwachung einschlägiger Indikatoren die Resilienz, Rechenschaftspflicht und langfristige Nachhaltigkeit stärken können.

([29]) Artikel 21 Absatz 2 Buchstabe g der NIS-2-Richtlinie.

91. Informationsmaterial, das dem Personal zur Verfügung gestellt wird, sollte direkten Bezug zur Risikobewertung der Einrichtung und zu den ergriffenen Resilienzmaßnahmen haben. Dieses Informationsmaterial sollte klar und leicht verständlich sein und Erläuterungen zur kritischen Rolle der Einrichtung und zu den Auswirkungen von Störungen auf Gesellschaft und Wirtschaft, zu sämtlichen Gefahren, zu zentralen Sicherheitsgrundsätzen wie „Sehen Sie etwas, sagen Sie etwas“ und zum Prinzip der minimalen Berechtigung beim Zugang zu sensiblen Informationen enthalten.

92. Das Informationsmaterial könnte auch visuelles Material zur Kurzübersicht über z. B. Verletzungen der physischen Sicherheit, den Ausfall von Strom/Konnektivität oder die Entdeckung verdächtiger Pakete sowie Ablaufdiagramme für die Meldung von Sicherheitsvorfällen, dem Plan zur Aufrechterhaltung des Betriebs entnommene Hinweise zur Aufrechterhaltung des Betriebs, Leitlinien für den physischen Schutz und die Regelungen für die Zugangskontrolle enthalten. Für ein Höchstmaß an Sensibilisierung sollte dieses Material in unterschiedlicher Form, z. B. digital ([30]) und physisch ([31]), bereitgestellt werden und interaktiv gestaltet ([32]) sein.

93. Übungen sind von entscheidender Bedeutung, um den Resilienzplan einer kritischen Einrichtung zu verifizieren und sicherzustellen, dass das Personal seine Aufgaben bei einem tatsächlichen Sicherheitsvorfall wirksam wahrnehmen kann. Im Rahmen eines gefahrenübergreifenden Ansatzes könnten die Einrichtungen diskussionsbasierte Übungen wie Simulationsübungen ([33]) und betriebsbasierte Übungen wie Wiederholungsübungen ([34]) organisieren.

94. Bei der Organisation von Übungen sollten kritische Einrichtungen den Fokus auf das Ergebnis ihrer Risikobewertung richten, den gesamten Resilienzzyklus erproben und gegebenenfalls eine gute sektorübergreifende Koordinierung mit anderen kritischen Einrichtungen sicherstellen, um sektorübergreifende Abhängigkeiten zu testen. Sie sollten sicherstellen, dass im Falle von Störungen verursachenden Sicherheitsvorfällen mit einschlägigen Behörden wie Strafverfolgungsbehörden, der Feuerwehr, anderen Notdiensten und Ersthelfern im Allgemeinen zusammengearbeitet wird und sollten diese Stellen in die Übungen einbeziehen.

([30]) Zum Beispiel Intranet, obligatorische E-Learning-Module mit Quizfragen, kurze Videos, Bildschirmschoner mit wichtigen Sicherheitshinweisen.

([31]) Zum Beispiel Plakate, Faltblätter, Karten zur Kurzübersicht.

([32]) Zum Beispiel häufig gestellte Fragen.

([33]) Testen der Koordinierungs-, Entscheidungs- und Kommunikationsprozesse während eines simulierten Sicherheitsvorfalls (z. B. größerer Infrastrukturausfall, länger anhaltender Stromausfall, Verletzung der internen Sicherheit).

([34]) Testen eines spezifischen, zeitkritischen Verfahrens wie z. B. die Ingangsetzung des Notstromaggregats, die Evakuierung eines kritischen Bereichs oder die Isolierung eines kompromittierten Bedienfelds.