EIOPA-BoS-20/600

Leitlinien zu Sicherheit und Governance im Bereich der Informations- und Kommunikationstechnologie

EIOPA – Westhafen Tower, Westhafenplatz 1 – 60327 Frankfurt – Germany – Tel.: + 49 69-951119-20;
Fax: + 49 69-951119-19; E-Mail: info@eiopa.europa.eu Website: www.eiopa.europa.eu

Inhaltsverzeichnis

Hintergrund

1. Gemäß Artikel 16 der Verordnung (EU) Nr. 1094/2010 kann die EIOPA Leitlinien und Empfehlungen für die zuständigen Behörden und für Finanzinstitute herausgeben, um kohärente, effiziente und wirksame Aufsichtspraktiken zu schaffen und die gemeinsame, einheitliche und kohärente Anwendung des Unionsrechts sicherzustellen.

2. Im Einklang mit Artikel 16 Absatz 3 dieser Verordnung unternehmen die zuständigen Behörden und Finanzinstitute alle erforderlichen Anstrengungen, um diesen Leitlinien und Empfehlungen nachzukommen.

3. Im Zusammenhang mit der als Reaktion auf den FinTech-Aktionsplan der Europäischen Kommission (COM(2018) 109 final) durchgeführten Analyse und dem Plan zur aufsichtlichen Konvergenz 2018-2019[1] der EIOPA sowie im Anschluss an die Interaktion mit mehreren anderen Interessenträgern[2] hat die EIOPA festgestellt, dass spezifische Leitlinien zur Sicherheit und Governance im Bereich der Informations- und Kommunikationstechnologie (IKT) gemäß den Artikeln 41 und 44 der Richtlinie 2009/138/EG ausgearbeitet werden müssen.

4. Wie in der Gemeinsamen Empfehlung der Europäischen Aufsichtsbehörden an die Europäische Kommission dargelegt, spiegeln die EIOPA-Leitlinien zum Governance-System *„nicht angemessen wider, wie wichtig die Einbeziehung von IKT-Risiken (einschließlich Risiken in Bezug auf die Cybersicherheit) ist*". *„Es gibt keine Leitlinien im Hinblick auf wesentliche Elemente, die allgemein als Bestandteil angemessener Anforderungen betreffend die IKT-Sicherheit und IKT-Governance anerkannt sind.*"

5. Bei der Analyse der derzeitigen (Rechts-)Lage in der EU hinsichtlich der oben genannten Gemeinsamen Empfehlung stellte sich heraus, dass die Mehrheit der EU-Mitgliedstaaten nationale Vorschriften für die IKT-Sicherheit und IKT-Governance festgelegt hat. Obwohl die Anforderungen ähnlich sind, ist der Rechtsrahmen nach wie vor fragmentiert. Darüber hinaus ergab eine Umfrage zu den derzeitigen Aufsichtspraktiken eine Vielzahl von Praktiken – von „keiner spezifischen Aufsicht" bis hin zu einer „strengen Aufsicht" (einschließlich „Fernüberwachung" und „Vor-Ort-Inspektionen").

6. Darüber hinaus nimmt die Komplexität der IKT zu, und auch die Häufigkeit von Vorfällen im Zusammenhang mit der IKT (einschließlich Cybervorfällen) steigt, ebenso wie die negativen Auswirkungen solcher Vorfälle auf den operativen Betrieb von Unternehmen. Daher ist das IKT- und Sicherheitsrisikomanagement von grundlegender Bedeutung, damit ein Unternehmen seine strategischen, geschäftlichen, operativen und reputationsbezogenen Ziele erreichen kann.

7. Des Weiteren stützt sich der gesamte Versicherungssektor, gleich, ob es sich um traditionelle oder innovative Geschäftsmodelle handelt, bei der Erbringung von Versicherungsdienstleistungen und beim normalen operativen Betrieb der Unternehmen zunehmend auf IKT, zum Beispiel durch die Digitalisierung im Versicherungssektor (InsurTech, Internet der Dinge usw.) sowie die Vernetzung über Telekommunikationskanäle (Internet, mobile und drahtlose Verbindungen und Weitverkehrsnetze). Dadurch wird der Geschäftsbetrieb der Unternehmen anfällig für Sicherheitsvorfälle, wozu auch Cyberangriffe zählen. Aus diesen

[1] https://www.eiopa.europa.eu/supervisory-convergence-plans-and-reports_en

[2] Der von der EIOPA als Reaktion auf den FinTech-Aktionsplan der Europäischen Kommission veröffentlichte Bericht ist hier abrufbar.

Gründen ist es wichtig, sicherzustellen, dass die Unternehmen angemessen auf das Management ihrer IKT- und Sicherheitsrisiken vorbereitet sind.

8. Da verstärkt die Notwendigkeit erkannt wird, dass Unternehmen für Cyberrisiken[3] gerüstet sind und über einen soliden Cybersicherheitsrahmen verfügen, gehen diese Leitlinien ebenfalls auf die Cybersicherheit im Rahmen der Informationssicherheitsmaßnahmen eines Unternehmens ein. In diesen Leitlinien wird zwar anerkannt, dass die Cybersicherheit im Rahmen des allgemeinen IKT- und Sicherheitsrisikomanagements eines Unternehmens angegangen werden sollte, jedoch ist darauf hinzuweisen, dass Cyberangriffe einige besondere Merkmale aufweisen, die berücksichtigt werden sollten, damit gewährleistet ist, dass durch Maßnahmen zur Informationssicherheit das Cyberrisiko angemessen eingedämmt wird:

   a) Cyberangriffe sind oft schwieriger zu bewältigen (d. h., sie zu ermitteln, sich davor zu schützen, sie zu erkennen, darauf zu reagieren und die Schäden vollständig zu beseitigen) als die meisten anderen Quellen von IKT- und Sicherheitsrisiken; gleichermaßen ist das Ausmaß des Schadens schwer zu bestimmen.

   b) Einige Cyberangriffe können für das Risikomanagement und die Betriebskontinuität getroffene übliche Maßnahmen sowie Verfahren zur Wiederherstellung in Notfällen unwirksam machen, da sie Schadsoftware auf Sicherungssysteme übertragen könnten, mit dem Ziel, dass diese Systeme nicht mehr für die Wiederherstellung verfügbar sind, oder um Sicherungsdaten zu beschädigen.

   c) Dienstleister, Makler, Agenten und Vermittler können zu Kanälen für die Verbreitung von Cyberangriffen werden. Ansteckende stille Bedrohungen können die Vernetzung mittels Kommunikationsverbindungen Dritter nutzen, um sich auf dem IKT-System des Unternehmens einzunisten. Daher kann ein vernetztes Unternehmen mit geringer individueller Relevanz anfällig und eine Quelle der Risikoausbreitung werden, was zu systemischen Auswirkungen führen kann. Unter Beachtung des Grundsatzes des schwächsten Glieds sollte Cybersicherheit nicht nur für wichtige Marktteilnehmer oder kritische Dienstleister ein Anliegen sein.

9. Ziel dieser Leitlinien ist es:

   a) Marktteilnehmern Klarheit und Transparenz hinsichtlich der erwarteten Mindestanforderungen an Informations- und Cybersicherheit, d. h. eine Sicherheits-Baseline, bereitzustellen;

   b) eine potenzielle Aufsichtsarbitrage zu vermeiden;

   c) aufsichtliche Konvergenz im Hinblick auf die Erwartungen und Prozesse, die in Bezug auf IKT-Sicherheit und IKT-Governance anwendbar sind, als Schlüssel für ein angemessenes IKT- und Sicherheitsrisikomanagement zu fördern.

[3] Eine Definition des Begriffs „Cyberrisiko" ist im Cyber-Lexikon des FSB vom 12. November 2018 zu finden, abrufbar unter https://www.fsb.org/wp-content/uploads/P121118-1.pdf.

Leitlinien zu Sicherheit und Governance im Bereich der Informations- und Kommunikationstechnologie

Einleitung

1. Gemäß Artikel 16 der Verordnung (EU) Nr. 1094/2010[4] richtet die EIOPA diese Leitlinien an die Aufsichtsbehörden, um Orientierungshilfe dahin gehend zu geben, wie Versicherungs- und Rückversicherungsunternehmen (zusammen im Folgenden „Unternehmen") die in der Richtlinie 2009/138/EG[5] (im Folgenden „Solvabilität-II-Richtlinie") und in der Delegierten Verordnung (EU) 2015/35 der Kommission[6] (im Folgenden „Delegierte Verordnung") vorgesehenen Governance-Anforderungen im Zusammenhang mit Sicherheit und Governance im Bereich der Informations- und Kommunikationstechnologie (im Folgenden „IKT") anwenden sollten. Zu diesem Zweck stützen sich diese Leitlinien auf die Bestimmungen zu Governance in den Artikeln 41, 44, 46, 47, 132 und 246 der Solvabilität-II-Richtlinie sowie in den Artikeln 258 bis 260, in Artikel 266, in den Artikeln 268 bis 271 und in Artikel 274 der Delegierten Verordnung. Des Weiteren stützen sich diese Leitlinien auf die Handlungsempfehlungen in den Leitlinien der EIOPA zum Governance-System (EIOPA-BoS-14/253)[7] und auf die Leitlinien der EIOPA zum Outsourcing an Cloud-Anbieter (EIOPA-BoS-20-002)[8].

2. Die Leitlinien sind sowohl auf einzelne Unternehmen als auch sinngemäß auf Ebene der Gruppe anzuwenden.[9]

3. Die zuständigen Behörden sollten bei der Einhaltung oder bei der Überwachung der Einhaltung dieser Leitlinien dem Grundsatz der Verhältnismäßigkeit[10] Rechnung tragen, wodurch sichergestellt werden sollte, dass Governance-Regelungen, einschließlich jener im Zusammenhang mit IKT-Sicherheit und IKT-Governance, der Wesensart, dem Umfang und der Komplexität der Risiken angemessen sind, denen Unternehmen ausgesetzt sind oder ausgesetzt sein könnten.

4. Diese Leitlinien sollten in Verbindung mit und unbeschadet der Solvabilität-II-Richtlinie, der Delegierten Verordnung, den EIOPA-Leitlinien zum Governance-System und den EIOPA-Leitlinien zum Outsourcing an Cloud-Anbieter verstanden werden. Es ist vorgesehen, dass diese Leitlinien technologie- und methodenneutral sind.

Begriffsbestimmungen

5. Für Begriffe, die in diesen Leitlinien nicht definiert sind, gelten die Begriffsbestimmungen der Solvabilität-II-Richtlinie.

6. Für die Zwecke dieser Leitlinien gelten die folgenden Begriffsbestimmungen:

---

[4] Verordnung (EU) Nr. 1094/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 zur Errichtung einer Europäischen Aufsichtsbehörde (Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung), zur Änderung des Beschlusses Nr. 716/2009/EG und zur Aufhebung des Beschlusses 2009/79/EG der Kommission (ABl. L 331, 15.12.2010, S. 48).

[5] Richtlinie 2009/138/EG des Europäischen Parlaments und des Rates vom 25. November 2009 betreffend die Aufnahme und Ausübung der Versicherungs- und der Rückversicherungstätigkeit (Solvabilität II) (ABl. L 335 vom 17.12.2009, S. 1).

[6] Delegierte Verordnung (EU) 2015/35 der Kommission vom 10. Oktober 2014 zur Ergänzung der Richtlinie 2009/138/EG des Europäischen Parlaments und des Rates betreffend die Aufnahme und Ausübung der Versicherungs- und der Rückversicherungstätigkeit (Solvabilität II) (ABl. L 12 vom 17.1.2015, S. 1).

[7] https://www.eiopa.europa.eu/content/guidelines-system-governance_en?source=search

[8] https://www.eiopa.europa.eu/content/guidelines-outsourcing-cloud-service-providers

[9] Artikel 212 Absatz 1 der Richtlinie 2009/138/EG.

[10] Artikel 29 Absatz 3 der Richtlinie 2009/138/EG.

Asset-Eigentümer	Person oder Unternehmen, der bzw. dem die Rechenschaftspflicht und die Verantwortung für ein Informations- und IKT-Asset obliegt.
Verfügbarkeit	Die Eigenschaft, auf Abruf durch eine befugte Stelle zugänglich und nutzbar zu sein (Aktualität)
Vertraulichkeit	Die Eigenschaft, dass Informationen unbefugten Personen, Stellen, Prozessen oder Systemen nicht zugänglich gemacht oder diesen nicht offengelegt werden
Cyberangriff	Jede Art von Hacking, das auf IKT-Systeme abzielt und zu einem offensiven bzw. böswilligen Versuch führt, ein Informationsasset zu zerstören, preiszugeben, zu verändern, zu deaktivieren, zu stehlen oder unbefugt darauf zuzugreifen oder es unbefugt zu nutzen
Cybersicherheit	Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und/oder Informationssystemen über das Cybermedium
IKT-Asset	Ein Software- oder Hardware-Asset in einem Unternehmensumfeld
IKT-Projekte	Jedes Projekt oder ein Teil davon, bei dem IKT-Systeme und IKT-Dienste geändert, ersetzt oder implementiert werden
IKT- und Sicherheitsrisiko	Eine Teilkomponente des operationellen Risikos; Verlustrisiko aufgrund einer Verletzung der Vertraulichkeit, des Verlustes der Integrität von Systemen und Daten, einer unzureichenden oder fehlenden Verfügbarkeit von Systemen und Daten, einer mangelnden Fähigkeit, die IT in einem angemessenen Zeit- und Kostenrahmen zu ändern, wenn sich die Umgebungs- oder Geschäftsanforderungen ändern (d. h. Agilität). Dies umfasst Cyberrisiken sowie Informationssicherheitsrisiken, die aus unzulänglichen oder fehlgeschlagenen internen Prozessen oder externen Ereignissen resultieren, einschließlich Cyberangriffen oder einer unzureichenden physischen Sicherheit.

Informationssicherheit	Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und/oder Informationssystemen. Darüber hinaus können andere Eigenschaften wie Authentizität, Rechenschaftspflicht, Nichtabstreitbarkeit und Zuverlässigkeit einbezogen werden.
IKT-Dienste	Dienste, die über IKT-Systeme und Dienstleister für einen oder mehrere interne oder externe Nutzer erbracht werden
IKT-Systeme	Eine Gruppe von Anwendungen, Diensten, Informationstechnologie-Assets, IKT-Assets oder anderen Informationsverarbeitungskomponenten, zu denen auch die Betriebsumgebung zählt
Informationsasset	Eine Sammlung an schützenswerten materiellen oder immateriellen Informationen
Integrität	Die Eigenschaft der Genauigkeit und Vollständigkeit
Betriebs- oder Sicherheitsvorfall	Ein einzelnes Ereignis oder eine Reihe zusammenhängender ungeplanter Ereignisse, das/die sich negativ auf die Integrität, die Verfügbarkeit und Vertraulichkeit von IKT-Systemen und IKT-Diensten auswirkt/auswirken oder aller Wahrscheinlichkeit nach auswirken wird/werden
Dienstleister	Ein Dritter, der auf der Grundlage einer Outsourcing-Vereinbarung einen Prozess, einen Dienst oder eine Tätigkeit bzw. Teile davon ausführt.
Threat-Led Penetration Testing	Ein kontrollierter Versuch, die Cyberabwehrfähigkeit eines Unternehmens durch die Simulation der Taktiken, Techniken und Verfahren realer Angreifer zu kompromittieren. Solche Penetrationstests basieren auf gezielten Bedrohungserkenntnissen und konzentrieren sich auf die Menschen, Prozesse und Technologien eines Unternehmens mit minimaler vorheriger Kenntnis und minimalen Auswirkungen auf den Betrieb.
Anfälligkeit	Eine Schwachstelle, eine Empfänglichkeit oder ein Fehler eines Assets oder einer Kontrolle, die/der durch eine oder mehrere Bedrohungen ausgenutzt werden kann

7. Die vorliegenden Leitlinien gelten ab dem 1. Juli 2021.

Leitlinie 1 – Verhältnismäßigkeit

8. Die Unternehmen sollten diese Leitlinien auf eine Art und Weise anwenden, die der Wesensart, dem Umfang und der Komplexität der Risiken angemessen ist, die mit ihrer Tätigkeit einhergehen.

Leitlinie 2 – IKT innerhalb des Governance-Systems

9. Das Verwaltungs-, Management- oder Aufsichtsorgan sollte sicherstellen, dass mit dem Governance-System eines Unternehmens, insbesondere dem Risikomanagementsystem und dem internen Kontrollsystem, die IKT- und Sicherheitsrisiken des Unternehmens angemessen beherrscht werden können.

10. Das Verwaltungs-, Management- oder Aufsichtsorgan sollte sicherstellen, dass die Anzahl und Fähigkeiten des Personals des Unternehmens angemessen sind, damit die IKT-Betriebsbedürfnisse und die IKT- und Sicherheitsrisikomanagementprozesse fortlaufend unterstützt werden und die Umsetzung der IKT-Strategie gewährleistet ist. Darüber hinaus sollte das Personal regelmäßig geeignete Schulungen zu IKT- und Sicherheitsrisiken, einschließlich Informationssicherheit, erhalten, wie in Leitlinie 13 dargelegt.

11. Das Verwaltungs-, Management- oder Aufsichtsorgan sollte sicherstellen, dass die zugewiesenen Ressourcen für die Erfüllung der oben genannten Anforderungen angemessen sind.

Leitlinie 3 – IKT-Strategie

12. Das Verwaltungs-, Management- oder Aufsichtsorgan ist insgesamt dafür zuständig, die IKT-Strategie der Unternehmen, die im Rahmen der allgemeinen Geschäftsstrategie und im Einklang mit dieser schriftlich verfasst wurde, aufzustellen und zu genehmigen sowie ihre Kommunikation und Umsetzung zu überwachen.

13. In der IKT-Strategie sollte zumindest Folgendes festgelegt werden:

    a) wie sich die IKT der Unternehmen entwickeln sollte, um ihre Geschäftsstrategie, einschließlich der Entwicklung der Organisationsstruktur, der Geschäftsmodelle, des IKT-Systems und wichtiger Abhängigkeiten mit Dienstleistern, wirksam zu unterstützen und umzusetzen;

    b) Entwicklung der IKT-Architektur, einschließlich Abhängigkeiten mit Dienstleistern und

    c) klare Informationssicherheitsziele, die sich auf IKT-Systeme und IKT-Dienste, Personal und Prozesse konzentrieren.

14. Die Unternehmen sollten sicherstellen, dass die IKT-Strategie zeitnah umgesetzt, angenommen und allen einschlägigen Mitarbeitern und Dienstleistern, soweit zutreffend und relevant, mitgeteilt wird.

15. Die Unternehmen sollten einen Prozess einführen, um die Wirksamkeit der Umsetzung der IKT-Strategie zu überwachen und zu messen. Dieser Prozess sollte regelmäßig überprüft und aktualisiert werden.

Leitlinie 4 – IKT- und Sicherheitsrisiken innerhalb des Risikomanagementsystems

16. Das Verwaltungs-, Management- oder Aufsichtsorgan ist insgesamt dafür zuständig, ein wirksames System zum Management von IKT- und Sicherheitsrisiken im Rahmen des allgemeinen Risikomanagementsystems des Unternehmens festzulegen. Hierzu zählen die Ermittlung der Risikotoleranz für diese Risiken im Einklang mit der Risikostrategie des Unternehmens sowie die Erstellung eines regelmäßigen schriftlichen Berichts über das Ergebnis des Risikomanagementprozesses für das Verwaltungs-, Management- oder Aufsichtsorgan.

17. Im Rahmen ihres allgemeinen Risikomanagementsystems sollten die Unternehmen in Bezug auf IKT- und Sicherheitsrisiken (bei der Festlegung der nachstehend beschriebenen Anforderungen zum Schutz der IKT) zumindest Folgendes berücksichtigen:

    a) Die Unternehmen sollten ihre Geschäftsprozesse, Geschäftstätigkeiten, Geschäftsfunktionen, Rollen und Assets (z. B. Informations- und IKT-Assets) abbilden und diese Abbildung regelmäßig aktualisieren, um deren Bedeutung und wechselseitigen Abhängigkeiten im Hinblick auf IKT- und Sicherheitsrisiken zu ermitteln.

    b) Die Unternehmen sollten alle relevanten IKT- und Sicherheitsrisiken, denen sie ausgesetzt sind, ermitteln und messen und die ermittelten Geschäftsprozesse, Geschäftstätigkeiten, Geschäftsfunktionen, Rollen und Assets (z. B. Informations- und IKT-Assets) im Hinblick auf Kritikalität klassifizieren. Sie sollten außerdem die Schutzanforderungen zumindest im Hinblick auf Vertraulichkeit, Integrität und Verfügbarkeit dieser Geschäftsprozesse, Geschäftstätigkeiten, Geschäftsfunktionen, Rollen und Assets (z. B. Informations- und IKT-Assets) bewerten. Es sollten Asset-Eigentümer benannt werden, die für die Klassifizierung der Assets verantwortlich sind.

    c) Die Methoden zur Bestimmung der Kritikalität und des erforderlichen Schutzniveaus, insbesondere im Hinblick auf die Schutzziele Integrität, Verfügbarkeit und Vertraulichkeit, sollten sicherstellen, dass die sich daraus ergebenden Schutzanforderungen kohärent und umfassend sind.

    d) Die Messung der IKT- und Sicherheitsrisiken sollte auf Grundlage der festgelegten IKT- und Sicherheitsrisikokriterien erfolgen, wobei die Kritikalität der betreffenden Geschäftsprozesse, Geschäftstätigkeiten, Geschäftsfunktionen, Rollen und Assets (z. B. Informations- und IKT-Assets), das Ausmaß bekannter Anfälligkeiten sowie frühere Vorfälle, die negative Auswirkungen auf das Unternehmen hatten, berücksichtigt werden sollten.

    e) Die Bewertung von IKT- und Sicherheitsrisiken sollte regelmäßig durchgeführt und dokumentiert werden. Diese Bewertung sollte auch vor wesentlichen Änderungen der Infrastruktur, Prozesse oder Verfahren vorgenommen werden, die sich auf Geschäftsprozesse, Geschäftstätigkeiten, Geschäftsfunktionen, Rollen und Assets (z. B. Informations- und IKT-Assets) auswirken.

    f) Auf der Grundlage ihrer Risikobewertungen sollten die Unternehmen zumindest Maßnahmen zur Minderung der festgestellten IKT- und Sicherheitsrisiken und zum Schutz von Informationsassets in Übereinstimmung mit ihrer Klassifizierung definieren und einführen. Dies

sollte auch die Festlegung von Maßnahmen zum Management der verbleibenden Risiken umfassen.

18. Die Ergebnisse des Prozesses zum Management von IKT- und Sicherheitsrisiken sollten vom Verwaltungs-, Management- oder Aufsichtsorgan genehmigt und im Rahmen des allgemeinen Risikomanagements des Unternehmens in das operationelle Risikomanagement einbezogen werden.

Leitlinie 5 – Revision

19. Die Governance, die Systeme und die Verfahren von Unternehmen zur Bewältigung ihrer IKT- und Sicherheitsrisiken sollten regelmäßig im Einklang mit dem Revisionsplan[11] des Unternehmens von Prüfern geprüft werden, die über ausreichende Kenntnisse und Fähigkeiten sowie über geeignetes Fachwissen auf dem Gebiet von IKT- und Sicherheitsrisiken verfügen, um dem Verwaltungs-, Management- oder Aufsichtsorgan deren Wirksamkeit von unabhängiger Seite zu versichern. Häufigkeit und Schwerpunkt solcher Prüfungen sollten den einschlägigen IKT- und Sicherheitsrisiken angemessen sein.

Leitlinie 6 – Informationssicherheitspolitik und -maßnahmen

20. Die Unternehmen sollten eine vom Verwaltungs-, Management- oder Aufsichtsorgan genehmigte Informationssicherheitspolitik schriftlich festlegen, in der die übergeordneten Grundsätze und Regeln zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit der Unternehmensinformationen festgelegt sind, um die Umsetzung der IKT-Strategie zu unterstützen.

21. Die Informationssicherheitspolitik sollte eine Beschreibung der wichtigsten Rollen und Verantwortlichkeiten für das Informationssicherheitsmanagement enthalten und die Anforderungen an Personal, Prozesse und Technologie in Bezug auf die Informationssicherheit festlegen und dabei berücksichtigen, dass Mitarbeiter auf allen Ebenen für die Gewährleistung der Informationssicherheit des Unternehmens verantwortlich sind.

22. Die Politik sollte innerhalb des Unternehmens kommuniziert werden und für das gesamte Personal gelten. Soweit zutreffend und relevant, sollte die Informationssicherheitspolitik oder Teile davon auch den Dienstleistern mitgeteilt werden und für diese gelten.

23. Basierend auf dieser Informationssicherheitspolitik sollten die Unternehmen spezifischere Informationssicherheitsverfahren und -maßnahmen festlegen und umsetzen, um unter anderem die IKT- und Sicherheitsrisiken, denen sie ausgesetzt sind, zu mindern. Diese Verfahren und Maßnahmen zur Informationssicherheit sollten, soweit zutreffend, alle in diesen Leitlinien beschriebenen Prozesse umfassen.

Leitlinie 7 – Informationssicherheitsfunktion

24. Die Unternehmen sollten im Rahmen ihres Governance-Systems und im Einklang mit dem Grundsatz der Verhältnismäßigkeit eine Informationssicherheitsfunktion einrichten, wobei eine dafür zuständige Person zu benennen ist. Die Unternehmen sollten die Unabhängigkeit und Objektivität dieser Informationssicherheitsfunktion dadurch gewährleisten, dass eine angemessene Trennung von IKT-Entwicklungs-

[11] Artikel 271 der Delegierten Verordnung.

und IKT-Betriebsprozessen sichergestellt ist. Die Funktion sollte gegenüber dem Verwaltungs-, Management- oder Aufsichtsorgan Bericht erstatten.

25. Die typischen Aufgaben der Informationssicherheitsfunktion sind:

    a) Unterstützung des Verwaltungs-, Management- oder Aufsichtsorgans bei der Festlegung und Aufrechterhaltung der Informationssicherheitspolitik der Unternehmen und Kontrolle ihrer Einführung;

    b) Berichterstattung und Beratung auf regelmäßiger und Ad-hoc-Basis gegenüber dem Verwaltungs-, Management- oder Aufsichtsorgan in Bezug auf den Stand der Informationssicherheit und der diesbezüglichen Entwicklungen;

    c) Überwachung und Überprüfung der Umsetzung der Informationssicherheitsmaßnahmen;

    d) Gewährleistung, dass die Anforderungen an die Informationssicherheit bei der Inanspruchnahme von Dienstleistern eingehalten werden;

    e) Gewährleistung, dass alle Mitarbeiter und Dienstleister, die auf Informationen und Systeme zugreifen, angemessen über die Informationssicherheitspolitik informiert werden, beispielsweise durch Schulungen zur Informationssicherheit und Sensibilisierungsveranstaltungen;

    f) Koordinierung der Untersuchung von Betriebs- oder Sicherheitsvorfällen und Meldung relevanter Vorfälle an das Verwaltungs-, Management- oder Aufsichtsorgan.

Leitlinie 8 – Logische Sicherheit

26. Die Unternehmen sollten Verfahren für die logische Zugriffskontrolle oder die logische Sicherheit (Identitäts- und Zugriffsmanagement) im Einklang mit den Schutzanforderungen gemäß Leitlinie 4 festlegen, dokumentieren und umsetzen. Diese Verfahren sollten umgesetzt, durchgesetzt, überwacht und regelmäßig überprüft werden und ebenfalls Kontrollen zur Überwachung von Anomalien umfassen. Mit diesen Verfahren sollten mindestens die folgenden Elemente implementiert werden, wobei der Begriff „Nutzer" auch technische Nutzer umfasst:

    a) Kenntnis, nur wenn nötig („Need to know"), Prinzip der geringsten Privilegien („Least Privilege") und Funktionstrennung: Unternehmen sollten Zugriffsrechte, einschließlich Fernzugriff auf Informationsassets und die zugehörigen Unterstützungssysteme, nach dem „Need to know"-Prinzip verwalten. Die Nutzer sollten nur jene Zugriffsrechte erhalten, die zur Erfüllung ihrer Aufgaben unbedingt erforderlich sind (nach dem „Least Privilege"-Prinzip), d. h., um einen ungerechtfertigten Zugriff auf Daten zu verhindern oder um zu verhindern, dass durch die Zuweisung von Kombinationen von Zugriffsrechten Kontrollen umgangen werden können (Prinzip der „Funktionstrennung").

    b) Zurechenbarkeit von Nutzern: Die Unternehmen sollten die Verwendung generischer und gemeinsam genutzter Nutzerkonten möglichst beschränken und sicherstellen, dass Nutzer hinsichtlich der in den IKT-Systemen durchgeführten Tätigkeiten jederzeit identifiziert und auf eine verantwortliche natürliche Person oder eine autorisierte Aufgabe zurückgeführt werden können.

    c) Privilegierte Zugriffsrechte: Die Unternehmen sollten strenge Kontrollen für privilegierte Systemzugriffe einführen, indem sie die Anzahl der Konten mit

weiterreichenden Systemzugriffsrechten (z. B. Administratorkonten) konsequent begrenzen und diese Konten genau überwachen.

d) Fernzugriff: Um eine sichere Kommunikation zu gewährleisten und das Risiko zu reduzieren, sollte ein administrativer Fernzugriff auf kritische IKT-Systeme nur Personen gestattet werden, die Kenntnis von den entsprechenden Informationen haben müssen („Need to know"-Prinzip), und nur unter Anwendung starker Authentifizierungslösungen erfolgen.

e) Protokollierung von Nutzeraktivitäten: Die Aktivitäten der Nutzer sollten protokolliert und in einer dem Risiko angemessenen Weise überwacht werden, wobei zumindest die Aktivitäten privilegierter Nutzer einzubeziehen sind. Unbeschadet der im EU-Recht und im nationalen Recht festgelegten Aufbewahrungsanforderungen sollten Zugriffsprotokolle gesichert werden, um sie vor unbefugten Änderungen oder Löschungen zu schützen, und sie sollten für einen Zeitraum aufbewahrt werden, welcher der Kritikalität der ermittelten Geschäftsfunktionen, Unterstützungsprozesse und Informationsassets angemessen ist. Die Unternehmen sollten diese Informationen nutzen, um die Identifizierung und Untersuchung ungewöhnlicher Aktivitäten, die bei der Erbringung von Diensten festgestellt wurden, zu vereinfachen.

f) Zugriffsmanagement: Zugriffsrechte sollten zeitnah nach vorab festgelegten Genehmigungsroutinen gewährt, entzogen und geändert werden unter Einbeziehung des Eigentümers des jeweiligen Informationsassets. Falls kein Zugriff mehr erforderlich ist, sollten die Zugriffsrechte unverzüglich widerrufen werden.

g) Bewertung des Zugriffs: Die Zugriffsrechte sollten regelmäßig überprüft werden, um sicherzustellen, dass die Nutzer keine übermäßigen Rechte besitzen und dass die Zugriffsrechte widerrufen/entzogen werden, wenn sie nicht mehr benötigt werden.

h) Die Gewährung, Änderung und Entziehung von Zugriffsrechten sollten in einer Weise dokumentiert werden, die das Verständnis und die Analyse erleichtert.

i) Authentifizierungsmethoden: Die Unternehmen sollten Authentifizierungsmethoden durchsetzen, die stark genug sind, um in angemessener und wirksamer Weise sicherzustellen, dass die Regelungen und Verfahren für die Zugriffskontrolle eingehalten werden. Authentifizierungsmethoden sollten der Kritikalität der IKT-Systeme, der Informationen oder der Prozesse, auf die Zugriff erfolgt, angemessen sein. Dies sollte auf Grundlage des jeweiligen Risikos zumindest starke Passwörter oder stärkere Authentifizierungsmethoden (z. B. Zwei-Faktor-Authentifizierung) umfassen.

27. Der elektronische Zugriff auf Daten und IKT-Systeme durch Anwendungen sollte auf ein für die Erbringung der relevanten Dienstleistung erforderliches Mindestmaß beschränkt werden.

Leitlinie 9 – Physische Sicherheit

28. Die physischen Sicherheitsmaßnahmen der Unternehmen (z. B. Schutz vor Stromausfall, Feuer, Wasser und unbefugtem physischem Zugriff) sollten festgelegt, dokumentiert und umgesetzt werden, um die Räumlichkeiten, Rechenzentren und sensiblen Bereiche der Unternehmen vor unbefugtem Zugang und vor Elementarereignissen zu schützen.

29. Der physische Zugriff auf IKT-Systeme sollte nur berechtigten Personen gestattet sein. Die Berechtigung sollte in Übereinstimmung mit den Aufgaben und Verantwortlichkeiten Einzelner erteilt und auf Personen beschränkt werden, die entsprechend geschult wurden und beaufsichtigt werden. Der physische Zugriff sollte regelmäßig überprüft werden, um sicherzustellen, dass Zugriffsrechte sofort widerrufen/entzogen werden, sobald sie nicht mehr erforderlich sind.

30. Die Schutzmaßnahmen gegenüber Elementarereignissen sollten der Bedeutung der Gebäude und der Kritikalität der Tätigkeiten oder der in diesen Gebäuden beherbergten IKT-Systeme angemessen sein.

Leitlinie 10 – Sicherheit des IKT-Betriebs

31. Die Unternehmen sollten Verfahren zur Gewährleistung der Vertraulichkeit, Integrität und Verfügbarkeit von IKT-Systemen und IKT-Diensten einführen, um die Auswirkungen von Sicherheitsproblemen auf die Erbringung von IKT-Diensten zu minimieren. Diese Verfahren sollten entsprechend die folgenden Maßnahmen umfassen:

    a) Identifizierung potenzieller Anfälligkeiten, die bewertet und behoben werden sollten, indem sichergestellt wird, dass IKT-Systeme sowie die von den Unternehmen ihren internen und externen Nutzern zur Verfügung gestellte Software auf dem neuesten Stand sind, indem kritische Sicherheitspatches, einschließlich aktueller Virenschutzdefinitionen, eingespielt oder indem kompensierende Kontrollen eingeführt werden;

    b) Implementierung sicherer Konfigurations-Baselines für alle kritischen Komponenten wie Betriebssysteme, Datenbanken, Router oder Switches;

    c) Einführung einer Netzwerksegmentierung, von Systemen zur Verhinderung von Datenlecks und einer Verschlüsselung des Netzwerkverkehrs (entsprechend der Klassifizierung der Informationsassets);

    d) Einführung eines Endgeräteschutzes, z. B. für Server, Workstations und mobile Geräte; die Unternehmen sollten bewerten, ob die Endgeräte die von ihnen festgelegten Sicherheitsstandards erfüllen, bevor ihnen der Zugriff zum Unternehmensnetzwerk gewährt wird;

    e) Gewährleistung, dass Mechanismen zur Integritätsprüfung vorhanden sind, um die Integrität der IKT-Systeme zu überprüfen;

    f) Verschlüsselung von Daten im Ruhezustand und bei der Übertragung (gemäß der Klassifizierung der Informationsassets).

Leitlinie 11 – Überwachung der Sicherheit

32. Die Unternehmen sollten Verfahren und Prozesse zur kontinuierlichen Überwachung von Aktivitäten, die sich auf ihre Informationssicherheit auswirken, festlegen und umsetzen. Die Überwachung sollte zumindest Folgendes umfassen:

    a) interne und externe Faktoren, einschließlich Geschäfts- und IKT-Administrationsfunktionen;

    b) von Dienstleistern, anderen Einrichtungen und internen Nutzern ausgeführte Transaktionen und

    c) potenzielle interne und externe Bedrohungen.

33. Für die Überwachung sollten die Unternehmen geeignete und wirksame Kapazitäten bereitstellen, um ungewöhnliche Aktivitäten und Bedrohungen, wie physische oder

logische Angriffe, Verletzungen der Vertraulichkeit, Integrität und Verfügbarkeit von Informationsassets, bösartigen Code und öffentlich bekannte Anfälligkeiten von Soft- und Hardware, zu erkennen, zu melden und darauf zu reagieren.

34. Die Berichterstattung im Rahmen der Sicherheitsüberwachung sollte es den Unternehmen erleichtern, die Art von Betriebs- und Sicherheitsvorfällen zu verstehen, Tendenzen zu erkennen, die eigenen internen Untersuchungen zu unterstützen und angemessene Entscheidungen zu treffen.

Leitlinie 12 – Überprüfung, Bewertung und Testen der Informationssicherheit

35. Die Unternehmen sollten eine Vielzahl unterschiedlicher Überprüfungen, Bewertungen und Tests in Bezug auf die Informationssicherheit durchführen, um die wirksame Ermittlung von Anfälligkeiten ihrer IKT-Systeme und IKT-Dienste sicherzustellen. So können Unternehmen Gap-Analysen anhand von Informationssicherheitsstandards, Konformitätsprüfungen, interne und externe Prüfungen der Informationssysteme oder Überprüfungen der physischen Sicherheit durchführen.

36. Die Unternehmen sollten ein Rahmenwerk für Informationssicherheitstests schaffen und implementieren, um die Robustheit und Wirksamkeit ihrer Informationssicherheitsmaßnahmen zu bewerten, und sicherzustellen, dass dieser Rahmen Bedrohungen und Anfälligkeiten berücksichtigt, die durch die Bedrohungsüberwachung und den Prozess zur Bewertung von IKT- und Sicherheitsrisiken ermittelt werden.

37. Tests sollten auf sichere Weise und von unabhängigen Prüfern durchgeführt werden, die über ausreichende Kenntnisse und Fähigkeiten sowie über geeignetes Fachwissen in Bezug auf das Testen von Informationssicherheitsmaßnahmen verfügen.

38. Die Unternehmen sollten regelmäßig Tests durchführen. Umfang, Häufigkeit und Methode der Tests (z. B. Penetrationstests, darunter auch Threat-Led Penetration Testing) sollten dem ermittelten Risikoniveau angemessen sein. Tests kritischer IKT-Systeme und Schwachstellenscans sollten jährlich durchgeführt werden.

39. Die Unternehmen sollten sicherstellen, dass Tests der Sicherheitsmaßnahmen bei Änderungen der Infrastruktur, Prozesse oder Verfahren sowie bei Änderungen aufgrund wesentlicher Betriebs- oder Sicherheitsvorfälle oder bei der Freigabe neuer oder in großem Umfang geänderter kritischer Anwendungen durchgeführt werden. Die Unternehmen sollten die Ergebnisse der Sicherheitstests überwachen und auswerten und Sicherheitsmaßnahmen entsprechend anpassen, was im Fall kritischer IKT-Systeme unverzüglich erfolgen sollte.

Leitlinie 13 – Schulungen und Sensibilisierungsmaßnahmen zum Thema Informationssicherheit

40. Die Unternehmen sollten Schulungsprogramme zum Thema Informationssicherheit für alle Mitarbeiter, einschließlich der Verwaltungs-, Management- oder Aufsichtsorgane, einführen, um sicherzustellen, dass diese Personen ihre Aufgaben und Verantwortlichkeiten so wahrnehmen, dass menschliches Versagen, Diebstahl, Betrug, Missbrauch oder Verlust verringert werden. Die Unternehmen sollten sicherstellen, dass im Rahmen des Schulungsprogramms regelmäßig Schulungen für das gesamte Personal vorgesehen sind.

41. Die Unternehmen sollten regelmäßige Programme zur Sensibilisierung für Sicherheitsfragen erarbeiten und durchführen, um ihr Personal, einschließlich der Verwaltungs-, Management- oder Aufsichtsorgane, dahingehend zu schulen, wie mit Risiken im Zusammenhang mit der Informationssicherheit umzugehen ist.

Leitlinie 14 – Management des IKT-Betriebs

42. Unternehmen sollten den IKT-Betrieb auf der Grundlage der IKT-Strategie verwalten. In Dokumenten sollte festgelegt werden, wie Unternehmen IKT-Systeme und IKT-Dienste betreiben, überwachen und kontrollieren, wobei ebenfalls kritische IKT-Prozesse, -Verfahren und -Betriebsabläufe dokumentiert werden sollten.

43. Die Unternehmen sollten Protokollierungs- und Überwachungsverfahren für kritische IKT-Aktivitäten einführen, um die Erkennung, Analyse und Korrektur von Fehlern zu ermöglichen.

44. Die Unternehmen sollten ein aktuelles Verzeichnis ihrer IKT-Assets führen. Das Verzeichnis der IKT-Assets sollte hinreichend detailliert sein, um die sofortige Identifizierung eines IKT-Assets, seines Standorts, seiner Sicherheitsklassifizierung und seiner Eigentümerschaft zu ermöglichen.

45. Die Unternehmen sollten den Lebenszyklus von IKT-Assets überwachen und verwalten, um zu gewährleisten, dass diese weiterhin die Geschäfts- und Risikomanagementanforderungen erfüllen und unterstützen. Die Unternehmen sollten darüber wachen, dass die IKT-Assets von ihren Anbietern oder unternehmensinternen Entwicklern unterstützt werden und dass alle relevanten Patches und Upgrades auf der Basis eines dokumentierten Prozesses angewendet werden. Die Risiken aufgrund veralteter oder nicht unterstützter IKT-Assets sollten bewertet und gemindert werden. Außer Betrieb genommene IKT-Assets sollten sicher gehandhabt und entsorgt werden.

46. Die Unternehmen sollten Prozesse zur Kapazitätsplanung und zur Leistungs- und Kapazitätsüberwachung einführen, um wesentlichen Leistungsproblemen von IKT-Systemen und Engpässen bei IKT-Kapazitäten vorzubeugen, diese rechtzeitig zu erkennen und zeitnah darauf zu reagieren.

47. Die Unternehmen sollten Verfahren zur Sicherung und Wiederherstellung von Daten und IKT-Systemen festlegen und einführen, um sicherzustellen, dass sie bei Bedarf wiederhergestellt werden können. Umfang und Häufigkeit der Sicherungen sollten im Einklang mit den Anforderungen an die Wiederherstellung des Geschäftsbetriebs und abhängig von der Kritikalität der Daten und der IKT-Systeme festgelegt und entsprechend der durchgeführten Risikobewertung beurteilt werden. Die Sicherungs- und Wiederherstellungsverfahren sollten regelmäßig getestet werden.

48. Die Unternehmen sollten sicherstellen, dass Datensicherungen und Sicherungen des IKT-Systems an einem oder mehreren Standorten außerhalb des primären Standorts gespeichert werden, die sicher sind und in ausreichender Entfernung vom primären Standort liegen, sodass sie nicht den denselben Risiken ausgesetzt sind.

Leitlinie 15 – Management von IKT-Vorfällen und -Problemen

49. Die Unternehmen sollten einen Prozess zum Management von Vorfällen und Problemen einrichten und umsetzen, um Betriebs- und Sicherheitsvorfälle zu überwachen und zu protokollieren und es den Unternehmen zu ermöglichen, kritische Geschäftsfunktionen und -prozesse bei Störungen fortzuführen oder wiederaufzunehmen.

50. Die Unternehmen sollten geeignete Kriterien und Schwellenwerte für die Klassifizierung eines Ereignisses als Betriebs- oder Sicherheitsvorfall sowie Frühwarnindikatoren festlegen, die eine frühzeitige Erkennung solcher Vorfälle ermöglichen.

51. Zur Minimierung der Auswirkungen negativer Ereignisse und zur Ermöglichung einer zeitnahen Wiederherstellung sollten die Unternehmen geeignete Verfahren und Organisationsstrukturen schaffen, um eine kohärente und integrierte Überwachung, Bearbeitung und Weiterverfolgung von Betriebs- und Sicherheitsvorfällen zu gewährleisten und sicherzustellen, dass die Hauptursachen ermittelt und geklärt und Abhilfemaßnahmen ergriffen werden, damit eine Wiederholung des Vorfalls verhindert wird. Der Vorfall- und Problemmanagementprozess sollte mindestens Folgendes umfassen:

    a) Verfahren zur Ermittlung, Verfolgung, Protokollierung, Kategorisierung und Einstufung von Sicherheitsvorfällen entsprechend den vom Unternehmen definierten Prioritäten sowie je nach Geschäftskritikalität und auf Grundlage der Dienstleistungsverträge;

    b) Rollen und Zuständigkeiten für verschiedene Vorfallszenarien (z. B. Fehler, Funktionsstörungen, Cyberangriffe);

    c) ein Problemmanagementverfahren zur Ermittlung, Analyse und Lösung der Hauptursache eines oder mehrerer Vorfälle; die Unternehmen sollten die Betriebs- oder Sicherheitsvorfälle analysieren, die innerhalb und/oder außerhalb des Unternehmens festgestellt wurden oder aufgetreten sind, und sollten die wichtigsten Erkenntnisse aus diesen Analysen berücksichtigen und die Sicherheitsmaßnahmen entsprechend aktualisieren;

    d) wirksame interne Kommunikationspläne, einschließlich der Meldung von Vorfällen und Eskalationsverfahren, die ebenfalls sicherheitsbezogene Kundenbeschwerden umfassen, um sicherzustellen, dass

        i. Vorfälle mit potenziell hohen negativen Auswirkungen auf kritische IKT-Systeme und IKT-Dienste der zuständigen Geschäftsleitung gemeldet werden;

        ii. das Verwaltungs-, Management- oder Aufsichtsorgan bei bedeutenden Vorfällen auf Ad-hoc-Basis informiert wird, zumindest über die Auswirkungen, die Reaktion und die zusätzlichen Kontrollen, die als Folge der Vorfälle festzulegen sind;

    e) Verfahren zur Reaktion auf Vorfälle, um die Auswirkungen der Vorfälle zu mindern und sicherzustellen, dass der Dienst zeitnah betriebsbereit und sicher ist;

    f) spezifische externe Kommunikationspläne für kritische Geschäftsfunktionen und -prozesse, um

        i. mit einschlägigen Interessenträgern zusammenzuarbeiten, damit wirksam auf den Vorfall reagiert und dieser behoben werden kann;

        ii. gegebenenfalls externe Beteiligte (z. B. Kunden, andere Marktteilnehmer, zuständige Behörden bzw. Aufsichtsbehörden) im Einklang mit geltenden Rechtsvorschriften zeitnah zu informieren, wozu auch die Meldung von Vorfällen zählt.

Leitlinie 16 – Management von IKT-Projekten

52. Die Unternehmen sollten eine IKT-Projektmethodik (einschließlich unabhängiger Erwägungen zu Sicherheitsanforderungen) einrichten, die einen angemessenen Governance-Prozess und Leitungsfunktionen bei der Projektdurchführung umfasst, um die Umsetzung der IKT-Strategie mittels IKT-Projekten wirksam zu unterstützen.

53. Unternehmen sollten Risiken, die sich aus dem IKT-Projektportfolio ergeben, angemessen überwachen und mindern, wobei auch Risiken zu berücksichtigen sind, die sich aus Wechselwirkungen zwischen verschiedenen Projekten und aus Abhängigkeiten mehrerer Projekte von denselben Ressourcen und/oder derselben Sachkompetenz ergeben können.

Leitlinie 17 – Erwerb und Entwicklung von IKT-Systemen

54. Die Unternehmen sollten einen Prozess für den Erwerb, die Entwicklung und die Pflege von IKT-Systemen konzipieren und umsetzen, um sicherzustellen, dass Vertraulichkeit, Integrität und Verfügbarkeit der zu verarbeitenden Daten nachvollziehbar gesichert sind und die definierten Schutzanforderungen erfüllt werden. Dieser Prozess sollte unter Anwendung eines risikobasierten Ansatzes konzipiert werden.

55. Die Unternehmen sollten sicherstellen, dass vor dem Erwerb oder der Entwicklung von Systemen die funktionalen und nicht funktionalen Anforderungen (einschließlich Anforderungen an die Informationssicherheit) und die technischen Ziele klar definiert werden.

56. Die Unternehmen sollten sicherstellen, dass Vorkehrungen getroffen wurden, um eine unbeabsichtigte Veränderung oder eine absichtliche Manipulation der IKT-Systeme während der Entwicklung zu verhindern.

57. Die Unternehmen sollten über eine Methodik zum Testen und zur Genehmigung von IKT-Systemen, IKT-Diensten und Informationssicherheitsmaßnahmen verfügen.

58. Die Unternehmen sollten IKT-Systeme, IKT-Dienste und Informationssicherheitsmaßnahmen angemessen testen, um potenzielle Sicherheitsschwachstellen, -verletzungen und -vorfälle zu ermitteln.

59. Die Unternehmen sollten die Trennung der Produktionsumgebung von den Entwicklungs-, Test- und anderen Nicht-Produktionsumgebungen gewährleisten.

60. Die Unternehmen sollten Maßnahmen ergreifen, um die Integrität des Quellcodes (sofern verfügbar) von IKT-Systemen zu schützen. Ferner sollten sie die Entwicklung, die Implementierung, den Betrieb und/oder die Konfiguration der IKT-Systeme umfassend dokumentieren, um eine unnötige Abhängigkeit von Fachexperten zu reduzieren.

61. Die Prozesse der Unternehmen für den Erwerb und die Entwicklung von IKT-Systemen sollten auch für IKT-Systeme gelten, die von den Endnutzern der Geschäftsfunktion außerhalb der IKT-Organisation unter Verwendung eines risikobasierten Ansatzes entwickelt oder verwaltet werden (z. B. Business Managed Applications und Endnutzer-Computeranwendungen). Die Unternehmen sollten ein Register dieser Anwendungen führen, die kritische Geschäftsfunktionen oder -prozesse unterstützen.

Leitlinie 18 – IKT-Änderungsmanagement

62. Die Unternehmen sollten einen Prozess für das IKT-Änderungsmanagement einrichten, um sicherzustellen, dass alle Änderungen an IKT-Systemen auf kontrollierte Weise erfasst, bewertet, getestet, genehmigt, autorisiert und implementiert werden. Änderungen im Rahmen dringender oder notfallbedingter IKT-Änderungen sollten rückverfolgbar sein und dem betreffenden Asset-Eigentümer im Nachhinein für eine nachträgliche Analyse mitgeteilt werden.

63. Die Unternehmen sollten bestimmen, ob Änderungen der bestehenden Betriebsumgebung Auswirkungen auf die bestehenden Sicherheitsmaßnahmen haben oder zusätzliche Maßnahmen zur Minderung der betreffenden Risiken erforderlich machen. Diese Änderungen sollten im Einklang mit dem formalen Änderungsmanagementprozess des Unternehmens stehen.

Leitlinie 19 – Betriebliches Kontinuitätsmanagement

64. Im Rahmen der Gesamtstrategie für die Betriebskontinuität des Unternehmens ist das Verwaltungs-, Management- oder Aufsichtsorgan für die Festlegung und Genehmigung der IKT-Kontinuitätspolitik des Unternehmens zuständig. Die IKT-Kontinuitätspolitik sollte innerhalb des Unternehmens angemessen kommuniziert werden und für das gesamte einschlägige Personal und gegebenenfalls für Dienstleister gelten.

Leitlinie 20 – Business-Impact-Analyse

65. Im Rahmen eines soliden Betriebskontinuitätsmanagements sollten die Unternehmen eine Business-Impact-Analyse durchführen, um anhand interner und/oder externer Daten- und Szenarioanalysen zu bewerten, inwieweit das Unternehmen schwerwiegenden Betriebsunterbrechungen ausgesetzt sein kann und welche quantitativen und qualitativen Auswirkungen diese haben können. Bei der Business-Impact-Analyse sollten auch die Kritikalität der ermittelten und klassifizierten Geschäftsprozesse, Geschäftstätigkeiten, Geschäftsfunktionen, Rollen und Assets (z. B. Informations- und IKT-Assets) und ihre wechselseitigen Abhängigkeiten gemäß Leitlinie 4 berücksichtigt werden.

66. Die Unternehmen sollten sicherstellen, dass ihre IKT-Systeme und IKT-Dienste so konzipiert und auf ihre Business-Impact-Analyse abgestimmt sind, dass beispielsweise bestimmte kritische Komponenten redundant ausgelegt sind, um Störungen durch Ereignisse mit Auswirkungen auf diese Komponenten zu verhindern.

Leitlinie 21 –Betriebskontinuitätsplanung

67. In den allgemeinen Betriebskontinuitätsplänen der Unternehmen sollten wesentliche Risiken berücksichtigt werden, die sich negativ auf IKT-Systeme und IKT-Dienste auswirken könnten. Die Pläne sollten entsprechende Ziele unterstützen, um die Vertraulichkeit, Integrität und Verfügbarkeit der Geschäftsprozesse, Geschäftstätigkeiten, Geschäftsfunktionen, Rollen und Assets des Unternehmens (z. B. Informations- und IKT-Assets) zu schützen und, sofern erforderlich, wiederherzustellen. Die Unternehmen sollten sich bei der Erstellung dieser Pläne gegebenenfalls mit einschlägigen internen und externen Interessenträgern abstimmen.

68. Die Unternehmen sollten Betriebskontinuitätspläne einrichten, um sicherzustellen, dass sie auf mögliche Ausfallszenarien innerhalb einer Wiederherstellungszeit

(Recovery Time Objective, RTO – maximale Zeitspanne, innerhalb der ein System oder ein Prozess nach einem Vorfall wiederhergestellt werden muss) und eines Wiederherstellungspunkts (Recovery Point Objective, RPO – maximaler Zeitraum, während dessen Daten bei einem Vorfall entsprechend einer vorgegebenen Dienstgüte verloren gehen können) angemessen reagieren können.

69. Die Unternehmen sollten in ihren Betriebskontinuitätsplänen eine Reihe unterschiedlicher Szenarien berücksichtigen, einschließlich extremer, aber plausibler Szenarien und Cyberangriffsszenarien, und die potenziellen Auswirkungen solcher Szenarien bewerten. Ausgehend von diesen Szenarien sollten die Unternehmen beschreiben, wie die Kontinuität von IKT-Systemen und IKT-Diensten sowie die Informationssicherheit des Unternehmens gewährleistet werden.

Leitlinie 22 – Reaktions- und Wiederherstellungspläne

70. Aufgrund der Business-Impact-Analysen und plausibler Szenarien sollten Unternehmen Reaktions- und Wiederherstellungspläne ausarbeiten. In diesen Plänen sollten die Bedingungen festgelegt werden, die unter Umständen die Auslösung eines Plans und der zu ergreifenden Maßnahmen erfordern, um die Integrität, Verfügbarkeit, Kontinuität und Wiederherstellung zumindest der kritischen IKT-Systeme, IKT-Dienste und Daten von Unternehmen zu gewährleisten. Mit den Reaktions- und Wiederherstellungsplänen sollten die Wiederherstellungsziele der Unternehmen erreicht werden.

71. In den Reaktions- und Wiederherstellungsplänen sollten sowohl kurzfristige als auch gegebenenfalls langfristige Wiederherstellungsmöglichkeiten berücksichtigt werden. Die Pläne sollten zumindest

    a) die Wiederherstellung des Betriebs wichtiger IKT-Dienste, Geschäftsfunktionen, Unterstützungsprozesse und Informationsassets und ihre wechselseitigen Abhängigkeiten in den Mittelpunkt stellen, um negative Auswirkungen auf den Betrieb des Unternehmens zu verhindern;

    b) dokumentiert und den Geschäfts- und Unterstützungseinheiten zur Verfügung gestellt werden und im Notfall leicht zugänglich sein; außerdem sollten in ihnen die Rollen und Zuständigkeiten eindeutig definiert sein, und

    c) gemäß den Erkenntnissen aus Vorfällen, Tests, neu ermittelten Risiken und Bedrohungen sowie geänderten Wiederherstellungszielen und -prioritäten aktualisiert werden.

72. Ferner sollten in den Plänen alternative Optionen berücksichtigt werden, wenn eine Wiederherstellung aufgrund der Kosten, der Risiken, der Logistik oder unvorhergesehener Umstände kurzfristig nicht machbar ist.

73. Im Rahmen der Reaktions- und Wiederherstellungspläne sollten die Unternehmen Kontinuitätsmaßnahmen erwägen und umsetzen, um den Ausfall von Dienstleistern zu mindern, die für die Kontinuität der IKT-Dienste der Unternehmen von entscheidender Bedeutung sind (im Einklang mit den Bestimmungen der EIOPA-Leitlinien zum Governance-System und der EIOPA-Leitlinien zum Outsourcing an Cloud-Anbieter).

Leitlinie 23 –Testen der Pläne

74. Die Unternehmen sollten ihre Betriebskontinuitätspläne testen und sicherstellen, dass der Betrieb ihrer kritischen Geschäftsprozesse, Geschäftstätigkeiten, Geschäftsfunktionen, Rollen und Assets (z. B. Informations- und IKT-Assets) sowie deren wechselseitigen Abhängigkeiten (einschließlich der von Dienstleistern

bereitgestellten Assets) auf der Grundlage des Risikoprofils des Unternehmens regelmäßig getestet werden.

75. Die Betriebskontinuitätspläne sollten auf Basis von Testergebnissen, aktuellen Bedrohungserkenntnissen und Erfahrungen aus früheren Ereignissen regelmäßig aktualisiert werden. Alle relevanten Änderungen bei Wiederherstellungszielen (einschließlich Wiederherstellungszeit –RTO und Wiederherstellungspunkt – RPO) und/oder Änderungen bei Geschäftsprozessen, Geschäftstätigkeiten, Geschäftsfunktionen, Rollen und Assets (z. B. Informations- und IKT-Assets) sollten ebenfalls einbezogen werden.

76. Die Tests der Betriebskontinuitätspläne sollten belegen, dass mit den Plänen die Lebensfähigkeit des Unternehmens aufrechterhalten werden kann, bis die kritischen Operationen entsprechend einer vorgegebenen Dienstgüte oder Toleranz gegenüber Auswirkungen wiederhergestellt sind.

77. Die Testergebnisse sollten dokumentiert und alle aus den Tests resultierenden festgestellten Mängel analysiert, behandelt und dem Verwaltungs-, Management- oder Aufsichtsorgan gemeldet werden.

Leitlinie 24 – Krisenkommunikation

78. Bei einer Störung oder einem Notfall und während der Umsetzung der Betriebskontinuitätspläne sollten die Unternehmen sicherstellen, dass sie über wirksame Maßnahmen zur Krisenkommunikation verfügen, sodass alle relevanten internen und externen Interessenträger, einschließlich der einschlägigen Aufsichtsbehörden – sofern gemäß den nationalen Vorschriften erforderlich –, sowie die relevanten Dienstleister zeitnah und angemessen informiert werden.

Leitlinie 25 – Outsourcing von IKT-Diensten und IKT-Systemen

79. Unbeschadet der EIOPA-Leitlinien zum Outsourcing an Cloud-Anbieter sollten die Unternehmen sicherstellen, dass bei der Auslagerung von IKT-Diensten und IKT-Systemen die für den IKT-Dienst oder das IKT-System geltenden relevanten Anforderungen erfüllt werden.

80. Im Falle der Auslagerung kritischer oder wichtiger Funktionen sollten die Unternehmen sicherstellen, dass die vertraglichen Verpflichtungen des Dienstleisters (z. B. Vertrag, Dienstgütevereinbarungen, Kündigungsbestimmungen in den einschlägigen Verträgen) mindestens Folgendes umfassen:

    a) angemessene und verhältnismäßige Ziele und Maßnahmen hinsichtlich der Informationssicherheit, darunter beispielsweise Mindestanforderungen an die Informationssicherheit, Spezifikationen des Lebenszyklus der Unternehmensdaten, Prüfung und Zugriffsrechte sowie Anforderungen bezüglich des Standorts von Datenzentren, Datenverschlüsselungsanforderungen und Prozesse zur Gewährleistung der Netzwerksicherheit und zur Überwachung der Sicherheit;

    b) Dienstgütevereinbarungen zur Gewährleistung der Kontinuität der IKT-Dienste und IKT-Systeme und der Leistungsziele unter normalen Umständen sowie im Rahmen von Notfallplänen im Falle einer Dienstunterbrechung und

    c) Prozesse zur Handhabung von Betriebs- und Sicherheitsvorfällen, einschließlich Eskalation und Meldung.

81. Die Unternehmen sollten diese Dienstleister im Hinblick darauf überwachen, inwieweit diese die Sicherheitsziele, die Sicherheitsmaßnahmen und die Leistungsziele erfüllen, und sich Gewissheit darüber verschaffen.

Regeln über die Einhaltung von Vorschriften und Berichterstattung

82. Das vorliegende Dokument enthält Leitlinien, die gemäß Artikel 16 der Verordnung (EU) Nr. 1094/2010 herausgegeben wurden. Gemäß Artikel 16 Absatz 3 dieser Verordnung unternehmen die zuständigen Behörden und Unternehmen alle erforderlichen Anstrengungen, um den Leitlinien und Empfehlungen nachzukommen.

83. Die zuständigen Behörden, die diesen Leitlinien nachkommen bzw. dies beabsichtigen, sollten sie in angemessener Weise in ihren Regulierungs- bzw. Aufsichtsrahmen integrieren.

84. Die zuständigen Behörden bestätigen der EIOPA innerhalb von zwei Monaten nach Erscheinen der übersetzten Fassungen, ob sie diesen Leitlinien nachkommen oder nachzukommen beabsichtigen, und nennen die Gründe, wenn dies nicht der Fall ist.

85. Geht bis zum Ablauf dieser Frist keine Antwort ein, so wird davon ausgegangen, dass die zuständigen Behörden ihrer Berichterstattungspflicht nicht nachkommen, und sie werden als solche gemeldet.

Schlussbestimmung bezüglich der Überprüfung

86. Die vorliegenden Leitlinien unterliegen der Überprüfung durch die EIOPA.