FMA

Dokumentennummer: 02 / 2018
Veröffentlichungsdatum: 03.07.2018

FMA-LEITFADEN IT-SICHERHEIT IN VERSICHERUNGS- UND RÜCKVERSICHRUNGS-UNTERNEHMEN

INHALTSVERZEICHNIS

ZIELSETZUNG UND HINWEISE

Die zunehmende Digitalisierung birgt – neben vielen Vorteilen im Wirtschaftsleben – neue Gefahren und Risiken, denen Unternehmen, einschließlich der Versicherungs- und Rückversicherungsunternehmen ([R]VU), ausgesetzt sind. Auch für (R)VU, welche immer mehr auf Digitalisierung setzen (müssen), hat sich die Risikolage dadurch deutlich verschärft.

Die Finanzmarktaufsichtsbehörde (FMA) ist sich der immer bedeutender werdenden Möglichkeiten und Risiken, welche aus der Informationstechnologie (IT) resultieren, bewusst und sieht sich aufgrund der gestiegenen Risikolage einer intensivierten IT-Aufsicht verpflichtet. Aus diesem Grund wird den (R)VU seitens der FMA ein Überblick über Ausgestaltung, Anforderungen und Vorkehrungen betreffend die IT-Sicherheit von (R)VU als Orientierungshilfe zur Verfügung gestellt.

Dieser Leitfaden stellt keine Verordnung dar. Er soll für die beaufsichtigten Unternehmen Know-how aufbereiten und die Entwicklung eines gemeinsamen Verständnisses fördern. Über die gesetzlichen Bestimmungen hinausgehende Rechte und Pflichten können aus diesem Leitfaden nicht abgeleitet werden.

Dieser Leitfaden richtet sich an alle Versicherungsunternehmen (§ 5 Z 1 VAG 2016), Rückversicherungsunternehmen (§ 5 Z 2 VAG 2016) sowie an Zweigniederlassungen eines Drittland-Versicherungs- oder Drittland-Rückversicherungsunternehmens (§ 5 Z 18 VAG 2016) und ist auf Gruppenebene sinngemäß anzuwenden (§ 222 Abs. 1 VAG 2016).

Die Ausführungen in diesem Leitfaden sind unter dem Grundsatz der Proportionalität zu sehen. Nach diesem Grundsatz entsprechen Anwendungen der Wesensart, dem Umfang und der Komplexität der mit der Tätigkeit des (R)VU einhergehenden Risiken. Dabei bestimmt das jeweilige (R)VU selbst, welche Methoden, Systeme und Prozesse in Bezug auf die IT-Sicherheit angemessen sind. Die rechtlichen Grundlagen bleiben durch diesen Leitfaden unberührt.

I. RECHTSGRUNDLAGEN

Dieser Leitfaden basiert insbesondere auf § 110 Abs. 2 Z 5 VAG 2016 (Risikomanagement operationeller Risiken) und § 111 Abs. 1 Z 1 VAG 2016 (Gesamtsolvabilitätsbedarf) in Verbindung mit den EIOPA Leitlinien zum Governance-System, EIOPA-BoS-14/253 sowie den EIOPA Leitlinien für die unternehmenseigene Risiko- und Solvabilitätsbeurteilung, EIOPA-BoS-14/259. Bei der Umsetzung zur Behandlung von IT-Risiken empfiehlt die FMA, auf etwaige etablierte Standards zurückzugreifen. Dazu gehören unter anderem:

- **ISO 27001:**[1] Die ISO 2700X-Reihe ist eine Reihe von Standards der IT-Sicherheit. Beispielsweise wurde die ISO 27001 für die Einrichtung, Implementierung, Wartung und laufende Verbesserung eines Informationssicherheitsmanagementsystems erarbeitet.
- **Österreichisches Informationssicherheitshandbuch:**[2] Dieses beschreibt und unterstützt die Vorgehensweise zur Etablierung eines umfassenden Informationssicherheitsmanagementsystems in Unternehmen und der öffentlichen Verwaltung. Das Handbuch eignet sich beispielsweise als Implementierungshilfe für die ISO 27001-Umsetzung.
- **ITIL:**[3] Die IT Infrastructure Library (ITIL) ist ein etablierter Qualitätsstandard, der vordefinierte Prozesse, Funktionen und Rollen für IT-Infrastrukturen von Unternehmen umfasst (Sammlung von Best Practices für Service Management).
- **COBIT:**[4] Das Rahmenwerk Control Objectives for Information and related Technology (COBIT) ermöglicht die Steuerung und Kontrolle des IT-Betriebs durch das Management. COBIT entstand aus einer Sammlung von mehreren IT-Standards, Rahmenwerken, Richtlinien und Best Practices.
- **BSI-Grundschutz**:[5] Der BSI-Grundschutz ist eine Sammlung von Dokumenten des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI), die zur Erkennung und Bekämpfung sicherheitsrelevanter Schwachstellen in IT-Umgebungen dienen.

II. DEFINITIONEN

Für Zwecke dieses Leitfadens werden nachstehend die maßgeblichen Definitionen in Bezug auf die IT-Sicherheit dargestellt. Im Übrigen werden grundsätzlich die Definitionen der ISO-Standards verwendet.

- **Informationstechnologie (IT):** IT umfasst alle technischen Mittel, die der Verarbeitung oder Übertragung von Informationen dienen. Zur Verarbeitung von Informationen gehören die Erhebung, die Erfassung, die Nutzung, die Speicherung, die Übermittlung, die programmgesteuerte Verarbeitung, die interne Darstellung und die Ausgabe von Informationen.

[1] https://www.iso.org/standard/54534.html.
[2] https://www.sicherheitshandbuch.gv.at.
[3] Siehe z.B. https://www.etc.at/itil/ oder https://www.axelos.com/best-practice-solutions/itil.
[4] https://www.isaca.org/cobit/pages/default.aspx.
[5] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html.

- **IT-Risiko:**[6] Dieses ist das bestehende oder künftige Risiko von Verlusten aufgrund der Unzweckmäßigkeit oder des Versagens der Hard- und Software technischer Infrastrukturen, welche die Verfügbarkeit, Integrität, Zugänglichkeit und Sicherheit dieser Infrastrukturen oder von Daten beeinträchtigen können. Darunter kann das Risiko aus IT-Verfügbarkeit und -Kontinuität, IT-Sicherheit, IT-Änderungen, IT-Datenintegrität und IT-Auslagerungen fallen.

III. GOVERNANCE

A. ROLLE DES VORSTANDS

Der Vorstand[7] sollte bezüglich der IT-Sicherheit für die Einhaltung der für den Betrieb der Vertragsversicherung geltenden Vorschriften und der anerkannten Grundsätze eines ordnungsgemäßen Geschäftsbetriebs gemäß § 106 VAG 2016 insbesondere

- die Festlegung, Überprüfung und gegebenenfalls die Anpassung der IT-Strategie verantworten,
- die Festlegung, Umsetzung und die bei Bedarf erfolgende zeitnahe Anpassung der IT-Aufbau- und Ablauforganisation verantworten,
- Kriterien zur Steuerung der IT (beispielsweise betreffend die Verfügbarkeit, die Anpassungsfähigkeit an neue Anforderungen, die generelle Qualität) festlegen,
- schriftliche IT-Risikomanagementleitlinien (als Teil der Risikomanagementleitlinien) und Vorgaben zur Informationssicherheit beschließen,
- die Kohärenz der Strategien und Verfahren zum IT-Risiko mit den strategischen Unternehmenszielen sicherstellen.

B. IT-STRATEGIE

Die IT-Strategie und die Geschäftsstrategie sind aufeinander abgestimmt. Die IT-Strategie umfasst insbesondere:

- die strategische Entwicklung der IT-Aufbau- und IT-Ablauforganisation, insbesondere im Hinblick auf Personaleinsatz und Budget,
- einen Überblick über die geplante Anwendungslandschaft,
- die Festlegung von Standards, an denen sich das (R)VU orientiert, unter Darlegung des aktuellen und des geplanten Umsetzungsgrades,
- die grundsätzliche Herangehensweise zur Berücksichtigung der Informationssicherheit in der Unternehmensorganisation,

[6] Bei den synonymen Begriffen „IT-Risiko“, „Informations- und Kommunikationstechnologie (IKT)-Risiko“ bzw. „Informationssystemrisiko“ wird das gleiche Risiko adressiert.
[7] Mit „Vorstand“ ist für Zwecke dieses Leitfadens auch der Verwaltungsrat gemeint (vgl. Art. 1 Z 43 L2-VO [EU] 2015/35 iVm § 106 VAG 2016).

- eine Grundsatzstrategie zum IT-Notfallmanagement,
- eine Positionierung zur Zulässigkeit und zu Voraussetzungen bezüglich dem lokalen Einsatz spezifischer IT-Systeme (Hard- und Software-Komponenten) in den einzelnen Organisationseinheiten,
- die Grundsätze eines Lebenszyklus-Managements von Hard- und Software.

Die IT-Strategie ist innerhalb eines angemessenen Zeitraums an Änderungen der strategischen Ziele, der Geschäftstätigkeit, des Geschäftsumfelds oder der Risikolage des (R)VU anzupassen. Das Risikobewusstsein der Mitarbeiter für das IT-Risiko sollte im gesamten Unternehmen forciert werden.

C. IT-GOVERNANCE

Die auf der IT-Strategie basierende IT-Governance gewährleistet einen ordnungsgemäßen Betrieb sowie bei Bedarf erfolgende Anpassungen der IT-Systeme und -Prozesse. Die **technisch-organisatorische Ausstattung** ist angemessen und entspricht den vom Vorstand vorgegebenen Kriterien, die auf der IT-Strategie basieren. Das (R)VU ist bezüglich der IT-spezifischen Anforderungen mit quantitativ und qualitativ angemessenen Personalressourcen ausgestattet.

Interessenskonflikte innerhalb der IT-Aufbau- und Ablauforganisation sollten vermieden bzw. adäquat adressiert werden. Klar abgegrenzte Rollen und Verantwortlichkeiten für Identifikation, Beurteilung, Monitoring, Minimierung, Reporting und Beaufsichtigung der wesentlichen IT-Risiken sollten definiert werden.

Die IT-Governance unterliegt einer regelmäßigen internen Überprüfung.

Im Fall von Auslagerungen der IT-Dienstleistungen sind die Vorgaben des § 109 VAG 2016 zu beachten.

IV. STEUERUNG

A. RISIKOMANAGEMENT VON IT-RISIKEN

IT-Risiken werden im Rahmen des Risikomanagements operationeller Risiken bzw. der Gesamtsolvabilitätsbedarfsbeurteilung behandelt. Risiken zur Informationsverarbeitung, -weitergabe und -speicherung, welche durch adäquate IT-Systeme und -Prozesse unterstützt sind, sollten abgedeckt werden. Ein Überblick über den Informationsverbund, der beispielsweise Informationen, IT-Systeme, Netz- und Gebäudeinfrastrukturen sowie Schnittstellen umfasst, erleichtert das Risikomanagement von IT-Risiken.

Die auf IT-Risiken bezogene Gesamtsolvabilitätsbedarfsbeurteilung durchläuft die folgenden Prozessschritte:

- **Risikoidentifikation**: Mögliche Ursachen für IT-Risiken sind:
  - inadäquate Absicherung der Schnittstellen zum Internet,
  - unzureichende Maßnahmen zur Förderung des Risikobewusstseins der Mitarbeiter,
  - Auslagerungen,
  - wesentliche Änderungen/Umstellungen des IT-Systems, der IT-Prozesse oder von IT-Funktionen.

  Im Rahmen der Risikokategorisierung sollten auch die identifizierten IT-Risiken beschrieben und systematisiert dargestellt werden. Der notwendige Detaillierungsgrad hängt von den unternehmensspezifischen Gegebenheiten ab.
- Die durch die Eintrittswahrscheinlichkeit und das Schadensausmaß determinierte **Risikoanalyse** bildet die Basis für die **Risikobewertung**, welche beispielsweise über eine Risikomatrix abgebildet wird. Insbesondere Cyberrisiken sind beispielsweise durch die Durchführung von Penetrationstests (Ausnutzen von Software-Schwachstellen und Sicherheitslücken in der IT-Infrastruktur, um unberechtigten Zugang zu dieser zu erhalten) adressiert.
- Zur angemessenen **Risikosteuerung** verfügt das (R)VU über eine Methodik zur Ermittlung des Schutzbedarfs der Komponenten des Informationsverbunds. Insbesondere auf die Schutzziele Integrität, Verfügbarkeit, Vertraulichkeit und Authentizität von Informationen sollte dabei abgestellt werden. Auch Erkenntnisse aus dem Notfallmanagement werden dabei berücksichtigt. In Abhängigkeit von der Schutzbedarfskategorie sind Maßnahmenkataloge zur Risikomitigation festgelegt und umgesetzt.

  Mögliche Maßnahmen sind:
  - der grundsätzliche Ersatz manueller durch automatisierte Schnittstellen,
  - die Protokollierung von Benutzer- und Administratorentätigkeiten,
  - Passwortvorgaben z.B. zur Passwortlänge und -zusammensetzung, zur Sicherstellung eines notwendigen Sicherheitsniveaus für den Einsatz von Benutzername/Passwort-Verfahren,
  - Umschaltung auf einen Ersatzrechner bei Ausfall des Verwaltungsservers.

  Das vom (R)VU bewusst übernommene IT-Restrisiko ist transparent dargestellt.
- **Risikoberichte** enthalten auch Ausführungen zum Risikomanagement von IT-Risiken.

B. INFORMATIONSSICHERHEITSMANAGEMENT

Zum Schutz von Informationen sind Prozesse etabliert und deren Umsetzung gesteuert. Informationssicherheit bezieht sich insbesondere auf die Aspekte

- Integrität, d.h. Informationen dürfen nur von den vorgesehenen Personen und Prozessen verändert werden,
- Vertraulichkeit, d.h. Informationen dürfen nur für die vorgesehenen Personen und Prozesse offen gelegt werden und

- Verfügbarkeit, d.h. Informationen müssen für die vorgesehenen Personen und Prozesse bereitgestellt sein, wenn diese sie benötigen.

Die konkreten Ziele und der Geltungsbereich des Informationssicherheitsmanagements sollten festgelegt werden. Dabei wird der im Rahmen des Managements von IT-Risiken definierte Schutzbedarf konkretisiert. Die zur Erfüllung der Informationssicherheitsziele ergriffenen **Sicherheitsmaßnahmen** umfassen insbesondere technische Sicherheitsmaßnahmen und organisatorische Abläufe und Prozesse. Mögliche Beispiele sind:

- Schulungen zur Informationssicherheit,
- Datensicherungen und regelmäßige Überprüfung der Funktionalität der Datensicherung (Backup und Restore),
- zentrale und dezentrale Anti-Virus Scans,
- Intrusion Detection/Prevention Systeme (z.B. Überprüfen der Logdaten auf Cyberattacken, laufende Überprüfung der Firewall-Konzepte unter Zuhilfenahme interner oder externer Prüfmethoden, wie z.B. Port-Scans),
- systematisiertes Patchmanagement,
- Evaluierung von Sicherheitsmaßnahmen insbesondere bezüglich neuer Technologien (z.B. hinsichtlich der Verwendung von Cloud-Services, aber auch im Hinblick auf neue Arten von Cyberattacken).

Nach Sicherheitsvorfällen sollten die Auswirkungen auf die Informationssicherheit analysiert und angemessene Nachsorgemaßnahmen veranlasst werden. Aufgrund der laufend steigenden Bedeutung der IT und der zunehmenden Informationsvernetzungen kommt der Organisation des Informationssicherheitsmanagements als **kontinuierlichem Verbesserungsprozess** hohe Bedeutung zu. Das Erfordernis der Ernennung eines Informationssicherheitsbeauftragten, der alle Belange der Informationssicherheit innerhalb des (R)VU und gegenüber Dritten wahrnimmt, sollte überprüft und auf Basis der Evaluierungserkenntnisse eingerichtet werden. In diesem Fall sollten Rollen und Verantwortlichkeiten klar verteilt und Interessenskonflikte adressiert sein und insbesondere die laufende Information und Beratung des Vorstands gewährleistet sein.

C. IT-NOTFALLMANAGEMENT

IT-Risiken sind mit dem Risiko der Betriebsunterbrechung eng verknüpft. Zweck des IT-Notfallmanagements (Business Continuity Management) ist das Treffen angemessener Vorkehrungen, um die Kontinuität und Ordnungsmäßigkeit der IT-unterstützten Tätigkeiten des (R)VU zu gewährleisten. Generell stellt das Notfallmanagement sicher, dass bei einer unvorhergesehenen Störung von Systemen und Verfahren, wesentliche Daten und Funktionen erhalten bleiben und Versicherungs- und Rückversicherungstätigkeiten fortgeführt werden oder – sollte dies nicht möglich sein – die entsprechenden Daten und Funktionen zeitnah wiederhergestellt und der Betrieb der Vertragsversicherung rasch wiederaufgenommen werden. Durch ein angemessenes Notfallmanagement wer-

den die Widerstandsfähigkeit zeitkritischer Geschäftsprozesse des Unternehmens und die Kontinuität der Versicherungs- und Rückversicherungstätigkeiten erhöht und somit auch die Interessen der Versicherten an einer kontinuierlichen Leistungserbringung geschützt.

Zur organisatorischen Umsetzung des Notfallmanagements sollte ein Koordinierungsgremium eingerichtet werden, dem Personen aus verschiedenen Organisationseinheiten angehören (**Notfallteam**).

Die **Phasen** des Notfallmanagements:

- **Entwicklung:**
  - Im Rahmen der **Business Impact Analyse** sollten zeitkritische Geschäftsprozesse, deren Abhängigkeiten und die dazu benötigten IT-Ressourcen identifiziert werden, um diese in Folge besonders absichern zu können. Dafür werden Auswirkungen von Ressourcen- (jedenfalls IT-Systeme, Daten, Personal und Vertragspartner) bzw. Geschäftsprozessausfällen eingeschätzt. Eine Einstufung als „kritisch“ ist im Hinblick auf die Erreichung der (primären) Unternehmensziele und die jeweilige Zeitsensitivität bezüglich der Priorität in der Wiederherstellung vorgenommen.
  - Die **Risikoanalyse**, welche auf etablierte Prozesse des Risikomanagements zurückgreift, dient der Bewertung von Gefährdungen, welche durch das Zusammenwirken von Bedrohungen zur Unterbrechung von Geschäftsprozessen und Schwachstellen entstehen. Die signifikantesten Risiken für das (R)VU sind bestimmt und priorisiert. Bei der Durchführung der Risikoanalyse wird auf die – in der Business Impact Analyse ermittelten – zeitkritischen IT-Prozesse und -Ressourcen abgestellt. Ein breites Spektrum von IT-Notfällen ist berücksichtigt. Diesbezügliche Beispiele sind Cyberattacken, Schadprogramme, Datendiebstähle, Risiken im Zusammenhang mit der Nutzung von Cloud-Leistungen oder die Nutzung von Sicherheitslücken zum unberechtigten Zugang der IT-Infrastruktur.
  - Auf Basis der Business Impact Analyse und der Risikoanalyse werden anschließend IT-spezifische **Notfallplanstrategien** festgelegt. Strategien, die von der vollständigen Aufrechterhaltung der IT-Prozesse und -Ressourcen bis hin zu einem Absehen von Maßnahmensetzungen reichen, hängen auch von Kosten-/Nutzenüberlegungen ab. IT-Notfallplanstrategien sind in **IT-Notfallplänen**, welche die Vorgehensweisen, Ersatzlösungen und die dafür benötigten Ersatzressourcen für die Wiederherstellung bzw. die Fortsetzung der kritischen Prozesse beschreiben, festgelegt.
- **Implementierung:**
  - Bewusstseinsbildungen und **Schulungen** zum IT-Notfallmanagement sind durchgeführt.
  - Regelmäßige – zumindest jährliche – **Tests** von IT-Notfallplänen sollten durchgeführt werden. Bei Prozessänderungen oder bei neuen wesentlichen Bedrohungen sollten zudem Tests ad-hoc durchlaufen werden.
- **Wartung und Aktualisierung:**
  - Anpassungen von Notfallplänen sind auf Basis der Erkenntnisse der IT-Notfallplantests vorgenommen.

V. OPERATIVE UMSETZUNG

A. IT-BETRIEB

Der IT-Betrieb hat die Aufgabe, Hardware und die zum Betrieb der Hardware erforderliche Software in angemessenem Umfang zur Verfügung zu stellen und störungsfrei zu betreiben. Die Anforderungen an den IT-Betrieb eines (R)VU ergeben sich aus der Geschäftsstrategie und lassen sich aus den IT-unterstützten Geschäftsprozessen ableiten.

Zur adäquaten Berücksichtigung der Risiken alternder IT-Systeme sind deren Lebenszyklen überwacht und gemanagt. Zu diesem Zweck ist ein **Inventar bezüglich aller IT-Systeme**, sowie deren Beziehungen, Abhängigkeiten und Schnittstellen vorhanden. Prozesse zur Neu- bzw. Ersatzbeschaffung sowie zu Nachbesserungen bestehen, wobei mögliche Umsetzungsrisiken berücksichtigt sind. Zudem stellen (R)VU die laufende Wartung ihrer IT-Systeme sicher – entsprechende Wartungsverträge sind vorhanden.

Ein **Prozess zum Umgang mit Störungen** sowie zu deren Ursachenerfassungen ist festgelegt. Beispielsweise sind mögliche Korrelationen von Störungen und deren Ursachen, die Vorgehensweise der Bearbeitung, Ursachenanalyse, Lösungsfindung und Nachverfolgung erfasst.

Ein im Einklang mit dem Notfallmanagement und den Geschäftsprozessen stehendes **Datensicherungskonzept** sollte vorgegeben werden. Test zur Wiederherstellbarkeit und Lesbarkeit von Datensicherungen sind regelmäßig und anlassbezogen durchgeführt.

B. BENUTZERBERECHTIGUNGEN

Die Vergabe von Benutzerberechtigungen entspricht dem **Need-to-know-Prinzip**. Diesem Prinzip kommt etwa in den folgenden Bereichen eine besondere Bedeutung zu:

- Die Unzulässigkeit der Eingliederung der Schadenregulierung der Rechtsschutzversicherung in eine Organisationseinheit, die auch die Schadenregulierung in anderen Versicherungszweigen besorgt (§ 99 Abs. 1 VAG), bedingt dementsprechend getrennte Benutzerberechtigungen.
- Im Falle von Auslagerungen ist für das (R)VU selbst sowie für den Abschlussprüfer und die FMA ein effektiver Zugang zu den Daten des Dienstleisters betreffend die ausgelagerten Funktionen oder Geschäftstätigkeiten sichergestellt (§ 109 VAG).

Zur Verhinderung von Berechtigungsumgehungen sollten **präventive Maßnahmen** getroffen werden. Die Protokollierung von Benutzer- und Administratorentätigkeiten, beispielsweise im Bereich der Schadenbearbeitung, beugt etwa allfälligen Datenmanipulationen vor. Erteilte Berechtigungen sollten hinsichtlich der vorgesehenen Verwendung regelmäßig überprüft und gegebenenfalls angepasst werden.

Das Benutzerberechtigungskonzept und die technischen Benutzerberechtigungssysteme sollten mit dem unternehmensspezifischen Risikoprofil im Einklang stehen.

C. IT-PROJEKTE, ANWENDUNGSENTWICKLUNGEN UND ZUGEKAUFTE SOFTWARE[8]

Das (R)VU sollte über eine Gesamtübersicht über alle wesentlichen IT-Projekte und Anwendungsentwicklungen verfügen. Bei der Umsetzung wird auf Folgendes geachtet:

- Wesentliche **IT-Projekte** sollten vorab – insbesondere unter Einbezug der Risikomanagement- und der Compliancefunktion – auf deren Auswirkungen auf die IT-Aufbau- und IT-Ablauforganisation sowie die dazugehörigen IT-Prozesse untersucht werden. Ein adäquates Risikocontrolling sollte eingerichtet werden. Besonders bei Einsatz vergleichsweise alter IT-Infrastruktur nimmt die Steuerung von IT-Projekten einen hohen Stellenwert ein. Deshalb sollten wesentliche IT-Projekte und deren Risiken dem Vorstand regelmäßig und anlassbezogen berichtet werden.
- **Anwendungen** und **Anwendungsentwicklungen** sollten nachvollziehbar dokumentiert werden. Für Anwendungsentwicklungen – beispielsweise für die Entwicklung individueller Softwarekomponenten – sollten angemessene Prozesse festgelegt werden. Diese umfassen ein System zur Anforderungsgenerierung in den Organisationseinheiten, die technische Umsetzung sowie einen geregelten Test- und Abnahmeprozess. Vor dem erstmaligen Einsatz im Echtbetrieb bzw. nach wesentlichen Änderungen sollten Anwendungen auf deren Funktionalität, auf Sicherheitskontrollen sowie auf Systemleistungen in unterstellten Stresssituationen getestet werden.

  Auf die Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der zu verarbeitenden Daten sollte bereits im Stadium der Anwendungsentwicklung geachtet werden.

  Anwendungen sollten im laufenden Betrieb auf mögliche Mängel überwacht, auf deren Ursachen untersucht und bei Bedarf nachgebessert werden.

[8] Die nachstehenden Ausführungen betreffen sinngemäß auch zugekaufte Software.