FMA

FMA-LEITFADEN

IT-Sicherheit
in
Wertpapierdienstleistungs-
unternehmen und
Wertpapierfirmen

Entwurf

INHALTSVERZEICHNIS

ZIELSETZUNG UND HINWEISE

Die zunehmende Digitalisierung birgt – neben vielen Vorteilen im Wirtschaftsleben – neue Gefahren und Risiken, denen Unternehmen ausgesetzt sind.

Insbesondere die jüngsten Angriffe auf IT-Systeme von Unternehmen haben deutlich gemacht, wie verwundbar IT-Infrastrukturen sind. Vor allem in Unternehmen, in denen die IT einen immer höheren Stellenwert einnimmt, hat sich die Risikolage dadurch deutlich verschärft.

Die Finanzmarktaufsichtsbehörde (FMA) ist sich der immer bedeutender werdenden Möglichkeiten und Risiken, welche aus der IT resultieren, bewusst und sieht aufgrund der gestiegenen Risikolage die Notwendigkeit gegeben den Wertpapierunternehmen einen Überblick über Ausgestaltung, Anforderungen und Vorkehrungen betreffend die IT-Sicherheit als Orientierungshilfe zur Verfügung zu stellen.

Dieser Leitfaden richtet sich an Wertpapierfirmen im Sinne es § 3 Abs. 1 WAG 2018 und Wertpapierdienstleistungsunternehmen im Sinne des § 4 Abs. 1 WAG 2018. Der 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.

Die Ausführungen in diesem Leitfaden sind unter dem gesetzlich verankerten Grundsatz der Proportionalität zu sehen, sodass die Art, der Umfang und die Komplexität der Geschäfte sowie die Risikostruktur des jeweiligen beaufsichtigten Unternehmens, bei der tatsächlichen Umsetzung Berücksichtigung zu finden haben. Anhand dieser Kriterien bestimmen die beaufsichtigten Unternehmen die für die jeweils erbrachten Dienstleistungen angemessene Methoden, Systeme und Prozesse in Bezug auf die IT-Sicherheit.

Dieser Leitfaden hindert die angesprochenen beaufsichtigten Unternehmen nicht, höhere Standards und bessere Techniken im Umgang mit IT-Risiken festzulegen!

1. RECHTSGRUNDLAGEN UND GRUNDLEGENDES

Für ein einheitliches Begriffsverständnis werden nachstehend die maßgeblichen Definitionen in Bezug auf IT-Sicherheit dargestellt:

- **Informationstechnologie (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.

- **IT-Risiko**[1]
  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.

Im Zuge der Umsetzung dieses Leitfadens sollen potentielle Interessenkonflikte und unvereinbare Tätigkeiten bspw. in Doppelfunktionen vermieden werden. Die Verantwortung für eine angemessene Begrenzung des IT-Risikos obliegt den Geschäftsleitern. Sie initiieren, steuern, hinterfragen und kontrollieren diesbezügliche Strategien und Verfahren und stellen die Kohärenz mit den strategischen Zielen sicher.

Das Wertpapieraufsichtsgesetz 2018 (WAG 2018) enthält eine Reihe organisatorische Vorschriften, die im Besonderm auch die IT und die damit verbundenen IT-Risiken in einem Unternehmen betreffen. Um diesen Bestimmungen in Bezug auf IT entsprechend nachkommen zu können und über ein entsprechendes und adäquates Risikomanagement zu verfügen, bietet sich die Etablierung eines angemessenen Standards an.

Gemäß § 29 Abs. 1 WAG 2018 haben Rechtsträger angemessene Strategien und Verfahren festzulegen, dass alle relevanten Personen des Rechtsträgers den Verpflichtungen des Bundesgesetzes sowie den organisatorischen Anforderungen gemäß Kapitel II der delegierten Verordnung (EU 2017/565) nachkommen. In diesem Kapitel der delegierten Verordnung ist im Artikel 21 Abs. 2 festgelegt, dass Rechtsträger Systeme und Verfahren einzurichten zu haben, die die **Sicherheit**, die **Integrität** und die **Vertraulichkeit** von Informationen gewährleisten, wobei sie die Art der besagten Informationen berücksichtigen.

[1] Festzuhalten ist, dass unter „IT-Risiko“, „IKT-Risiko“ bzw. „Informationssystemrisiko“ das gleiche Risiko adressiert wird und es sich um synonyme Begriffe handelt.

Gemäß Artikel 22 Abs. 3 der delegierten Verordnung (EU 2017/565) hat der Rechtsträger für die Festlegung, Umsetzung und Aufrechterhaltung einer angemessenen **Notfallplanung** zu sorgen, die bei einer Störung ihrer Systeme und Verfahren gewährleisten soll, dass wesentliche Daten und Funktionen erhalten bleiben und Wertpapierdienstleistungen und Anlagetätigkeiten fortgeführt werden oder — sollte dies nicht möglich sein — diese Daten und Funktionen bald zurückgewonnen und die Wertpapierdienstleistungen und Anlagetätigkeiten bald wieder aufgenommen werden.

Die geschaffenen Systeme und Vorkehrungen sind gemäß Artikel 22 Abs. 5 der delegierten Verordnung (EU 2017/565) auf Angemessenheit und Wirksamkeit regelmäßig zu überwachen und zu bewerten. In Bezug auf das Risikomanagement haben Rechtsträger gemäß Artikel 23 Abs. 1 der delegierten Verordnung (EU 2017/565) angemessene Strategien und Verfahren für ihr Risikomanagement festzulegen und auf Dauer umzusetzen, mit denen die mit den Geschäften, Abläufen und Systemen der Firma verbundenen Risiken erfasst werden und gegebenenfalls eine Risikotoleranzschwelle festzulegen.

Des Weiteren ist im § 29 Abs. 4 WAG 2018 festgelegt, dass der Rechtsträger angemessene Vorkehrungen zu treffen hat, um die **Kontinuität** und **Regelmäßigkeit** der Wertpapierdienstleistungen und Anlagetätigkeiten zu gewährleisten. Rechtsträger erbringen ihre Dienstleistungen insbesondere auch EDV-unterstützt und berücksichtigen diesen Umstand in ihrer IT. Darüberhinaus hat ein Rechtsträger gemäß § 29 Abs. 6 WAG 2018 über solide Sicherheitsmechanismen zu verfügen, durch die die **Sicherheit** und **Authentifizierung** der Informationsübermittlungswege gewährleistet werden, das **Risiko der Datenverfälschung** und des **unberechtigten Zugriffs** minimiert und ein Durchsickern von Informationen verhindert wird, so dass die **Vertraulichkeit der Daten** jederzeit gewährleistet ist.

Der Inhalt des Leitfadens ist nicht abschließender Natur. Die rechtlichen Grundlagen bleiben durch diesen Leitfaden unberührt.

Insbesondere die folgenden IT-Risiken können für Wertpapierunternehmen relevant (die Liste erhebt keinen Anspruch auf Vollständigkeit) sein:

- Verfügbarkeits- und Kontinuitätsrisiko
  - Inadäquates Kapazitätsmanagement
  - Systemversagen
  - Inadäquate Kontinuitäts- und Notfallwiederherstellungsplanung
  - Schädlichen und zerstörerische Cyber-Attacken
- IT-Sicherheitsrisiko
  - Cyber-Attacken und sonstige externe IT-Attacken
  - Inadäquate interne Sicherheitsvorkehrungen
  - Inadäquate physische Sicherheitsvorkehrungen
- Änderungsrisiko
  - Inadäquate Änderungs- und Entwicklungskontrollen von IT-Systemen
  - Unzureichende IT-Architektur

  - Inadäquates Lebenszyklus- und Patchmanagement
- Datenintegritätsrisiko
  - Funktionsstörung bei der Datenverarbeitung
  - Mangelhaft konzeptionierte Validierungskontrollen
  - Mangelhaft kontrollierte Datenänderungen in den Produktionssystemen
  - Mangelhaft harmonisierte und/oder verwaltete Datenarchitekturen, Datenflüsse, Datenmodelle oder Datenkataloge
- Outsourcingrisiko
  - Unzureichende Ausfallsicherheit von Drittanbietern oder anderen Rechtsträgern der Unternehmensgruppe
  - Inadäquate Outsourcing-Governance
  - Unzureichende Sicherheitsvorkehrungen von Drittanbietern oder anderen Rechtsträgern der Unternehmensgruppe

Neben den zuvor angeführten IT-Risiken können auch Informationssicherheitsrisiken relevant sein.

Bei der Umsetzung zur Behandlung von IT-Risiken empfiehlt es sich auf etwaige etablierte Standards zurückzugreifen. Dazu gehören unter anderem:

- **ITIL**[2]
  Die IT Infrastructure Library (ITIL) ist ein etablierter Qualitätsstandard, in dem sich vordefinierte Prozesse, Funktionen und Rollen für IT-Infrastrukturen von Unternehmen finden (Sammlung von Best Practices für Service Management).

- **BSI-Grundschutz**[3]
  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.

- **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

- **ISO 27001**[5]

[2] https://www.axelos.com/best-practice-solutions/itil
[3] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html
[4] http://www.isaca.org/cobit/pages/default.aspx
[5] https://www.iso.org/standard/54534.html

Die ISO 27001 wurde erarbeitet für die Einrichtung, Implementierung, Wartung und laufende Verbesserung eines Informationssicherheitsmanagementsystems.

- **Österreichisches Informationssicherheitshandbuch**[6]
  Dieses beschreibt und unterstützt die Vorgehensweise zur Etablierung eines umfassenden Informationssicherheitsmanagementsystems in Unternehmen und der öffentlichen Verwaltung. Das Handbuch eignet sich beispielsweise auch als Implementierungshilfe für die Umsetzung für die ISO 27001.

2. IT-STRATEGIE

Die Geschäftsleiter[7] von beaufsichtigten Unternehmen erstellen eine mit der Geschäftsstrategie übereinstimmende IT-Strategie, welche im Einklang mit Art, Umfang und Komplexität der Geschäftstätigkeit steht.

Mit Hilfe der IT-Strategie wird ein unternehmens- und gruppenweites Bewusstsein für Informationssicherheit geschaffen und deren Berücksichtigung in den jeweiligen Fachbereichen verankert. Dies erfolgt bspw. durch Kommunikation auf Gruppenebene und entsprechende Trainings sowie Maßnahmen zur Bewusstseinsbildung der Mitarbeiter.

Ziel ist es einen proaktiven Austausch zwischen der IT-Organisation und den Entscheidungsträgern zu schaffen und eine klare Kompetenzordnung zu erstellen. Dabei wird sichergestellt, dass alle entscheidungsrelevanten Informationen die Geschäftsleitung rechtzeitig und im nötigen Umfang erreichen.

In der IT-Strategie wird die strategische Entwicklung der IT-Aufbau- und Ablauforganisation inklusive der dazugehörigen Prozesse festgelegt. Hierbei orientieren sich die beaufsichtigten Unternehmen an bestehenden Standards (z.B. ISO 27001, BSI-Grundschutz).

Des Weiteren werden unter anderen folgende Punkte in die IT-Strategie aufgenommen:

- Entwicklung einer IT-Zielarchitektur mit einem Überblick über die Anwendungslandschaft
- Festlegung von Zuständigkeiten, Rollen und Aufgaben für einen systemischen Informationssicherheitsprozess
- Berücksichtigung von Auslagerungsaspekten
- Festlegung eines Notfallmanagements
- Aussagen zu den in den Fachbereichen selbst betriebenen bzw. entwickelten IT-Systemen (Hardware und Software)

[6] https://www.sicherheitshandbuch.gv.at/

[7] Die Begriffe „Geschäftsleiter“, „Geschäftsführung“ und „Unternehmensführung“ werden im gegenständlichen Leitfaden synonym verwendet. Sollten im Folgenden ausnahmsweise unterschiedliche Aspekte angesprochen werden, wird darauf gesondert hingewiesen.

Wesentliche relevante Themen sind bspw. die Sicherheitsrisiken des Unternehmens, der Schutz seiner Informationen, der Anwendungsbereich, die Sicherheitsanforderungen aus gesetzlichen und vertraglichen Vorgaben, die branchentypischen Standardvorgehensweisen zur Informationssicherheit und der aktuelle Stand im Unternehmen in Bezug auf Informationssicherheit.

Die IT-Strategie unterliegt der Genehmigung und Aufsicht durch die Geschäftsführung und wird in regelmäßigen Abständen sowie anlassbezogen auf ihre Aktualität überprüft und gegebenenfalls (orientiert an den Geschäftszielen) angepasst.

Zudem ist die IT-Strategie eine wichtige Informationsquelle für die IT-Revision. Daher enthält die IT-Strategie auch Aussagen zur geplanten Ausgestaltung der IT, wodurch Planungssicherheit für die IT-Organisation, taktische IT-Planung und Ressourcenplanung ermöglicht wird.

Die IT-Strategie wird von allen Mitarbeitern mitgetragen.

3. IT-GOVERNANCE

Das wesentliche Ziel der IT-Governance ist die optimale Unterstützung der Unternehmensziele und -strategie durch die IT. Sie baut auf der IT-Strategie des Unternehmens auf und ist ein wesentlicher Bestandteil der Unternehmensführung. Die IT-Governance setzt sich unter anderen aus folgenden wesentlichen Elementen zusammen: Prozessstrukturen, Organisationsvorgaben und Führungsstrukturen für die komplette IT-Infrastruktur im Unternehmen. Zweck der IT-Governance ist somit die Steuerung und Überwachung des Betriebs und die Weiterentwicklung der im Unternehmen verwendeten IT-Systeme samt der dazugehörigen IT-Prozesse.

Es liegt im Verantwortungsbereich der Geschäftsleitung – im Einklang mit der IT-Strategie – Regelungen zur Umsetzung der IT-Aufbau- und IT-Ablauforganisation festzulegen (z.B. IT-Risikomanagementrichtlinien, etc.). Dabei gilt es insbesondere unvereinbare Tätigkeiten und Interessenkonflikte (z.B. Trennung von anwendungs-entwickelnden Tätigkeiten und Tätigkeiten im Zuge des operativen IT-Betriebs) zu vermeiden. Zudem werden Prozesse bei Änderungen der Risikosituation oder Rahmenbedingungen zeitnah angepasst.

Die Geschäftsleitung stattet das IT-Risikomanagement (insb. Informationsrisikomanagement, Informationssicherheitsmanagement, IT-Betrieb und Anwendungsentwicklung) entsprechend der Art, dem Umfang, der Komplexität der Geschäftstätigkeit und unter Berücksichtigung der aktuellen und zukünftigen Risikosituation quantitativ und qualitativ angemessen mit Ressourcen aus. Das Unternehmen überwacht seine Risikosituation laufend.

Die beaufsichtigten Unternehmen verfügen über Prozesse zur Identifikation, Bewertung, Steuerung und Überwachung der wesentlichen IT-Risiken und evaluieren diese laufend. Ebenso erfolgt eine klare Abgrenzung der Rollen bzw. Verantwortlichkeiten betreffend Identifikation,

Beurteilung, Monitoring, Minimierung, Reporting und Beaufsichtigung der wesentlichen IT-Risiken.

Abschließend ist festzuhalten, dass die Unternehmensführung ausreichende Ressourcen für die Behandlung von IT-Risiken zur Verfügung stellt. Des Weiteren sorgen sie auch für eine angemessene Aus- und Weiterbildung der betroffenen Mitarbeiter. Darüber hinaus berücksichtigt die Interne Revision des Unternehmens im Rahmen der Audit Planung, IT-Risiken und deren Behandlung in adäquater Weise. Auch die Einbeziehung externer Experten zur Prüfung der Effektivität der getroffenen Maßnahmen ist empfehlenswert.

4. SICHERHEITSRICHTLINIEN

Ein wesentliches Instrument zum Schutz von Informationen sind Sicherheitsrichtlinien. Diese beziehen sich nicht nur auf die Sicherheit der IT-Systeme und der darin gespeicherten Daten, sondern umfassen auch generell das Thema Informationssicherheit (und somit auch die Sicherheit von nicht elektronisch verarbeiteten Informationen). Der Schutz der IT-Systeme ist nur als Teilaspekt der Informationssicherheit zu sehen.

Das zentrale Dokument auf höchster Ebene ist die Richtlinie zur Informationssicherheit. In dieser wird der Ansatz zur Bewältigung von Informationssicherheitszielen festgelegt. Des Weiteren werden die Ziele und Grundsätze des Unternehmens im Umgang mit Informationssicherheit beschrieben und der Umfang festgelegt. Als Grundlage für den Inhalt dienen die Anforderungen aus der Unternehmensstrategie, Vorschriften, Gesetze und Verträge sowie das aktuelle und zukünftige Umfeld von Bedrohungen in Bezug auf Informationssicherheit.

Die Informationssicherheitsrichtlinie ist Ausgangspunkt für themenspezifische und konkretisierende Richtlinien und Prozesse für Teilbereiche, wie bspw. Netzwerksicherheit, Kryptografie, Authentisierung, Protokollierung, physische Sicherheit/Absicherung der Gebäude und Datacenter, sichere Verwahrung von physischen Daten etc. Dabei werden Schutzmaßnahmen, Methoden zur Identifikation, Reaktionen und Wiederherstellungsabläufe bei Sicherheitsvorfällen definiert.

Jede Richtlinie wird in planmäßigen Abständen oder nach erheblichen Änderungen auf deren Wirksamkeit und Geeignetheit überprüft. Des Weiteren werden die Richtlinien durch die Unternehmensführung genehmigt. Darüberhinaus sind die Richtlinien sämtlichen betroffenen Personen im Unternehmen bekannt und jederzeit verfügbar.

5. INFORMATIONSRISIKOMANAGEMENT/INFORMATIONSSICHERHEITSMANAGEMENT

Als Folge der wachsenden Bedeutung der in Unternehmen eingesetzten IT-Systeme wird der Ausgestaltung der IT-Prozesse zum Schutz von Daten und kritischen Informationen bzw. dem gesamten Informationsrisikomanagement stärkere Beachtung geschenkt.

Die nachfolgenden Ausführungen beziehen sich insbesondere auf die IT-relevanten Aspekte der Informationssicherheit, können aber sinngemäß für die gesamte Informationssicherheit herangezogen werden.

Das Informationsrisikomanagement gewährleistet daher, dass die Informationsverarbeitung und -weitergabe im Unternehmen durch adäquate IT-Systeme (Hardware- und Softwarekomponenten) und Prozesse unterstützt wird. Bei der Ausgestaltung derselben wird beachtet, dass die **Integrität**, die **Verfügbarkeit**, die **Authentizität** und die **Vertraulichkeit der Daten** gewährleistet sind. Das beaufsichtigte Unternehmen etabliert zu diesem Zwecke Prozesse, welche den Schutz von Informationen gewährleisten.

Bezüglich deren Umfang und Qualität erfolgt eine Orientierung an den betriebsinternen Erfordernissen, den Geschäftsaktivitäten und der Risikosituation. In diesem Zusammenhang wird eine entsprechende Risikoanalyse und Risikobewertung durchgeführt, sodass alle relevanten Informationen des Unternehmens entsprechend berücksichtigt werden.

Im Zuge der Etablierung eines Informationsrisikomanagementsystems im Unternehmen werden Interessenskonflikte vermieden. Zudem wird die Berücksichtigung von Schnittstellen und Abhängigkeiten von geschäftsrelevanten Informationen, Geschäftsprozessen, IT-Systemen, Netz- und Gebäudeinfrastrukturen, etc. sichergestellt.

Bezüglich der Risikoüberwachung und -steuerung verfügt das Unternehmen über eine Methodik zur Ermittlung des Schutzbedarfs in Bezug auf Integrität, Verfügbarkeit, Vertraulichkeit und Authentizität von Informationen. In diesem Zusammenhang ist es hilfreich, Informationen in unterschiedliche Schutzbedarfskategorien zu unterteilen. Im Rahmen des Informationsrisikomanagements werden sämtliche kritischen IT-Systeme und –Services (z.B. Kernprozesse des Unternehmens, sensible Daten mit hohem Schadenspotential bei Verlust) anhand von festgelegten Kriterien identifiziert. Des Weiteren ist ein präventiver Maßnahmenkatalog zur Reduzierung der festgestellten Risiken vorhanden. Eine angemessene Dokumentation (bspw. tatsächlich umgesetzte Maßnahmen, Risikobeurteilung) wird sichergestellt.

Auf eine laufende Risikoanalyse (z.B. mögliche Bedrohungen, Schadenspotenzial, Schadenshäufigkeit, Risikoappetit, mögliche Reputationsschäden, Nichterfüllung regulatorischer Anforderungen) wird geachtet und es wird eine regelmäßige Information der Geschäftsleitung über die Risikosituation bzw. deren Veränderung gewährleistet.

Zur Risikoidentifizierung können unter anderen folgende Faktoren herangezogen werden:

- Komplexität der IT-Infrastruktur und der Datenverarbeitungsprozesse
- Wesentliche Änderungen von IT-Systemen und Funktionen

- Abhängigkeiten von ausgelagerten Dienstleistungen und Serviceleistungen Dritter (z.B. Provider, etc.)

Das beaufsichtigte Unternehmen richtet je nach Art, Umfang, Komplexität der Geschäftstätigkeit und unter Berücksichtigung der aktuellen und zukünftigen Risikosituation die Funktion eines Informationssicherheitsbeauftragten ein, dessen zentrale Aufgabe die Verantwortung aller Belange der Informationssicherheit innerhalb des Unternehmens und gegenüber Dritten. Darüber hinaus ist er auch für die Überprüfung und Überwachung der Einhaltung der Informationssicherheitsprozesse und -richtlinien zuständig. Sofern im Unternehmen etabliert, unterstützt der Informationssicherheitsbeauftragte zudem die Geschäftsleitung bei der Festlegung und Anpassung der Informationssicherheitsrichtlinie, steht dieser beratend zur Seite und berichtet dieser regelmäßig. Darüber hinaus obliegen ihm die Durchführung von Schulungsmaßnahmen und die Setzung von Sensibilisierungsmaßnahmen im Unternehmen betreffend die Informationssicherheit. Weitere Aufgaben sind bspw. die Beteiligung bei der Erstellung von Notfallkonzepten und Projekten mit IT-Relevanz sowie die Untersuchung von Sicherheitsvorfällen. Zudem steht der Informationssicherheitsbeauftragte mit seiner Expertise betroffenen Abteilungen zur Verfügung.

Die Funktion des Informationssicherheitsbeauftragten ist grundsätzlich organisatorisch und prozessual unabhängig ausgestaltet und im eigenen Unternehmen etabliert. Maßgeblich für die konkrete Ausgestaltung der Funktion ist neben dem bereits erwähnten Propertionalitätsgrundsatz die Zielsetzung, Interessenkonflikte der mit dieser Funktion betrauten Personen zu vermeiden. Z.B. sollte der Informationssicherheitsbeauftragte nicht in die Situation kommen zwischen Informationssicherheit und reiner Funktionalität von Geschäftsabläufen entscheiden zu müssen.

6. BENUTZERBERECHTIGUNGSMANAGEMENT

Aufgrund der Anzahl an unterschiedlichen IT-Systemen bzw. Programmen, die in einem Unternehmen verwendet werden (z.B. Windows-Anmeldung, Webmail, RSA-Token, eigene Software, Anwendungsprogramme), sind die Ansprüche an das Benutzerberechtigungsmanagements sehr hoch geworden.

Das Benutzerberechtigungsmanagement stellt sicher, dass ausschließlich autorisierte Benutzer auf IT-Services und Anwendungen zugreifen können, wie es die organisatorischen und fachlichen Vorgaben des Unternehmens vorsehen. In diesem Zusammenhang wird ein Prozess definiert in dem die Berechtigungsvergabe auf IT-Ressourcen geregelt ist (Einrichtung, Zugriff und Nutzung, Bearbeitung, Deaktivierung, Löschung). Die Vergabekriterien von Berechtigungen berücksichtigen dabei den Grundsatz der minimalen Rechtevergabe bzw. das Need-to-know-Prinzip und sind nachvollziehbar sowie konsistent. Zudem werden Funktionstrennungen gewahrt und Interessenkonflikte vermieden.

Das Benutzerberechtigungsmanagement verhindert vor allem missbräuchliche Verwendung und unautorisierte Manipulation von Daten und IT-Systemen.

Das Berechtigungskonzept berücksichtigt unter anderem folgende Themen:

- Passwortmanagement (Komplexität, Länge und Lebensdauer von Passwörtern)
- Richtlinien für Sonderberechtigung (z.B. Administrationsrechte, Systemaccounts, etc.)
- Zuständigkeiten bei der Vergabe von Rechten (z.B. Informationseigentümer bzw. Business Data Owner)
- Mehrfachverwendung von Zugangsdaten ist zu verhindern oder in Ausnahmefällen zu dokumentieren
- Zugangsberechtigungen müssen jederzeit einer handelnden Person zuordenbar sein

Die Einräumung, Änderung, Deaktivierung und Löschung von Berechtigungen ist nachvollziehbar, zuordenbar und auswertbar dokumentiert. Eingeräumte Berechtigungen werden regelmäßig überprüft, ob sie dem Berechtigungskonzept bzw. den -prozessen entsprechen, nur wie vorgesehen eingesetzt werden und weiterhin benötigt werden, wobei auf eine entsprechende Dokumentation geachtet wird. Zusätzlich werden die Berechtigungen auch durch eine unabhängige Stelle (z.B. Interne Revision) regelmäßig kontrolliert. Durch technisch-organisatorische Maßnahmen (z.B. angemessene Authentifizierungsverfahren, Verschlüsselung von Daten, technische Protokollierung von Benutzer- und Administratorentätigkeiten („Logging“) wird eine Manipulation der Berechtigungskonzepte verhindert.

7. SCHWACHSTELLENMANAGEMENT

Das Schwachstellenmanagement als integraler Bestandteil der IT-Sicherheit ist ein zyklischer Prozess zur Identifikation, Klassifizierung und Beseitigung von Schwachstellen insbesondere in Software und Firmware.

In diesem Zusammenhang ist festzustellen, dass heutzutage zum Schutz vor Bedrohungen ein Virenschutzprogramm alleine nicht mehr ausreichend ist. Unternehmen etablieren zusätzlich unter anderem folgende Schutzmaßnahmen:

- Zeitnahe Installation von aktuellen Sicherheitsupdates zur Vermeidung von offenen Sicherheitslücken
- Klare organisatorische und technische Regelungen zur Absicherung von Firewalls und sonstigen verwendeten Netzwerkkomponenten
- Sicherstellung eines aktuellen Informationsstands durch Heranziehung geeigneter Informationsquellen
- Regelmäßige Logdatenerfassung und –auswertung
- Regelmäßige Überprüfung der Funktionalität der Datensicherung (Backup und Restore)

Beaufsichtigte Unternehmen verfügen über angemessene Verfahren, Prozesse und Maßnahmen, um Daten vor Verlust bzw. Beschädigung zu schützen. Gleiches gilt für den Schutz vor Schadprogrammen („Malware“), Datendiebstahl und Cyberkriminalität.

Die Cyberkriminalität, bzw. die Cyber-Risiken umfassen sämtliche Bedrohungen für die IT des Unternehmens, die sich aus dem Cyberspace[8] ergeben. Die Cyber-Risiken sind nur eine Teilmenge möglicher IT-Risiken.

In weiterer Folge werden Maßnahmen zur Schwachstellenbeseitigung getroffen und die Wirksamkeit der umgesetzten Maßnahmen regelmäßig überprüft. Bspw. werden im Rahmen des Schwachstellenmanagements regelmäßige Überprüfungen der IT-Infrastruktur in Bezug auf IT-Schwachstellen (z.B. Penetrationstests, Kontrolle von Firewall-Loggings, Funktionalität des Virenscanners, etc.) durchgeführt. Die Erkenntnisse dieser Überprüfungen fließen in die relevanten Sicherheitsrichtlinien und das IT-Risikomanagement ein.

Weiters analysieren Unternehmen die Auswirkungen der Schwachstellen (auf Server, Anwendungen, Netzwerke, Systeme, etc.) und klassifizieren deren Risiko, um in einem weiteren Schritt Strategien festlegen zu können, wie Schwachstellen künftig verhindert und besser beseitigt werden können.

Da sich die Risikosituation ständig verändert, wird das Schwachstellenmanagement regelmäßig evaluiert.

8. IT-PROJEKTE, ANWENDUNGSENTWICKLUNG UND ZUGEKAUFTE SOFTWARE[9]

Beaufsichtigte Unternehmen erstellen im Falle von IT-Projekten eine Analyse, die vorab die damit einhergehenden wesentlichen Veränderungen in den IT-Systemen – in Hinblick auf deren Auswirkung auf die IT-Aufbau- und IT-Ablauforganisation sowie die dazugehörigen IT-Prozesse – aufzeigt und eine Bewertung der damit verbundenen Risiken vornimmt.

Um mögliche Beeinträchtigungen des Risikoprofils des Unternehmens identifizieren zu können, werden IT-Projekte angemessen gesteuert, deren Risiken laufend berücksichtigt und dies vollständig dokumentiert. Unternehmen überwachen und steuern die festgelegten Vorgehensmodelle bei IT-Projekten angemessen. Der Geschäftsleitung werden wesentliche IT-Projekte und deren Risiken in regelmäßigen Intervallen und anlassbezogen berichtet. Im Rahmen ihrer Aufgaben erfolgt die Einbeziehung von einzelnen Organisationseinheiten des Unternehmens an den IT-Projekten (Risikomanagement, Compliance, Interne Revision).

Für Anwendungsentwicklungen (v.a. Eigenentwicklungen) werden angemessene Prozesse festgelegt, welche auch den Fachbereich im erforderlichen Maß einbinden. Die Prozesse ent-

[8] Unter dem Begriff Cyberspace ist das komplexe Umfeld zu verstehen, welches aus der Interaktion von Menschen, Software und Diensten im Internet durch daran angeschlossene technische Hilfsmittel und Netzwerke entsteht, die in keiner physischen Form existieren.
[9] Die nachstehenden Ausführungen sind sinngemäß auch für zugekaufte Software zu berücksichtigen.

halten Vorgaben hinsichtlich Anforderungen, Ziele, Umsetzung, Qualitätssicherung, Test, Abnahme und Freigabe der Anwendung. Die Anwendung und deren Entwicklung werden insbesondere in Bezug auf vorgenommene Änderungen angemessen dokumentiert, um etwaigen Manipulationen vorzubeugen (z.B. Software-Quellcode-Kontrollsystem). In diesem Zusammenhang wird auf die jederzeitige Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der zu verarbeitenden Daten – bereits vor der Produktion bis hin zum Austausch, Archivieren, Entsorgen oder Vernichten von Anwendungen – geachtet (Sicherheitslücken-Screening).

Für die mehrstufigen Anwendungstests vor Produktivsetzung bzw. nach wesentlichen Änderungen wird eine Methodik implementiert, die unter verschiedenen Stressbelastungsszenarien die Funktionalität der Anwendung, die Sicherheitskontrollen und die Systemleistungen abdeckt. In diesem Zusammenhang werden neben der Produktionsumgebung entsprechende Entwicklungs- und Testumgebungen implementiert. Diese geben die Produktionsumgebung effizient wieder. Die Produktivsetzung von System- bzw. Anwendungsänderungen erfolgt erst nach ausführlichen Tests, um etwaige Störungen des Geschäftsbetriebs zu verhindern. Die Testaktivitäten und -ergebnisse werden dokumentiert. Die zuständige Fachabteilung trägt bei Anwendungsentwicklungen sowohl die Verantwortung für die Erhebung, die Bewertung, die Dokumentation der maßgeblichen Anforderungen, als auch für den Abnahmetest der Anwendung. Nach Produktivsetzung wird der Betrieb laufend überwacht. Bei Abweichungen vom Regelbetrieb werden die entsprechenden Maßnahmen veranlasst. Die Unternehmen verfügen über einen Prozess zur Verwaltung und Überwachung der Lebenszyklen der verwendeten IT-Systeme, um sicherzustellen, dass diese den aktuellen Anforderungen an das Geschäfts- und Risikomanagement entsprechen und Softwareentwicklungen seitens des Anbieters weiterhin möglich sind.

Bei Anwendungen, die von Unternehmen selbst entwickelt und betrieben werden, wird ein allgemein gültiger Standard in Form einer Richtlinie zur Etablierung von Eigenanwendungen (z.B. Regelungen zur Identifizierung solcher Anwendungen, Dokumentation, Testmethodik, Schutzbedarfsklassifizierung, Einhaltung von Programmierstandards, Rezertifizierung der Berechtigungen usw.) erstellt. Darüber hinaus wird ein zentrales Register dieser Anwendungen geführt.

9. IT-BETRIEB UND DATENINTEGRITÄT

Als IT-Betrieb ist in diesem Zusammenhang die Organisationseinheit eines Unternehmens gemeint, welche die Aufgabe hat, die erforderliche IT-Infrastruktur (Hardware und Software) in angemessenem Umfang zur Verfügung zu stellen und störungsfrei zu betreiben. Die Anforderungen an den IT-Betrieb eines Unternehmens ergeben sich aus der Geschäftsstrategie und lassen sich aus sämtlichen Geschäftsprozessen ableiten. Die Funktionsweise des IT-Betriebs ist angemessen dokumentiert.

Beaufsichtigte Unternehmen verwalten und steuern sämtliche IT-Komponenten unter Einbeziehung der Abhängigkeiten zwischen den Systemen inklusive regelmäßiger sowie anlassbezogener Aktualisierung des erfassten Inventars. Zudem bestehen Prozesse zur Neu- bzw. Ersatzbeschaffung sowie Nachbesserung unter Berücksichtigung möglicher Umsetzungsrisiken. Zudem stellen Unternehmen die laufende Wartung ihrer IT-Systeme sicher und verfügen über entsprechende Wartungsverträge.

Störungsmeldungen werden vom Unternehmen in geeigneter Weise erfasst, bewertet und priorisiert. Kriterien, ob die Geschäftsleitung über einen Störungsfall informiert wird, sind festgelegt. Ein Prozess zur Vorgehensweise bei Störmeldungen liegt vor. In diesem ist die Vorgehensweise für die Bearbeitung, Ursachenanalyse, Lösungsfindung und Nachverfolgung definiert.

Beaufsichtigte Unternehmen verfügen über einen schriftlichen Rahmen für die Ermittlung, das Verständnis, die Messung und die Minderung des Datenintegritätsrisikos, wobei auf das Risikoprofil des Unternehmens abgestellt wird. Schriftlich festzuhalten sind zudem die Verfahren zur Datensicherung, die Anforderungen an die Verfügbarkeit (Verfahren zur Wiederherstellbarkeit), die Lesbarkeit (auch von Datensicherungen) und Aktualität der Daten sowie die für die Datenverarbeitung notwendigen IT-Systeme. Auch in Hinblick auf ein funktionierendes Business Continuity Management (BCM) werden regelmäßige und anlassbezogene Tests durchgeführt, die die Verfahren für eine erfolgreiche Datenwiederherstellung in angemessener Zeit prüfen und deren Funktionalität bestätigen.

10. IT-AUSLAGERUNGEN

Gemäß § 34 WAG 2018 haben Rechtsträger bei der Auslagerung von wesentlichen betrieblichen Aufgaben an Dritte (Dienstleister) Vorkehrungen zu treffen, um unnötige zusätzliche Geschäftsrisiken zu vermeiden. Im Zuge der Auslagerung prüfen Rechtsträger die Wesentlichkeit der ausgelagerten IT bzw. IT-Diensleistungen.

Zum Zweck der Wesentlichkeitsprüfung legen Unternehmen in einer Auslagerungs-Policy konkret auf die jeweiligen Geschäftsprozesse bezogene Kriterien fest, anhand derer entschieden wird, ob eine wesentliche IT-Auslagerung vorliegt.

Die Auslagerungs-Policy umfasst die Identifikation, Analyse und Messung von IT-Risiken im Zusammenhang mit ausgelagerten Dienstleistungen. Die Inhalte werden auf Art, Umfang und Komplexität des Unternehmens abgestimmt. Dabei werden unter anderen folgende Themen berücksichtigt:

- Analyse zur Abschätzung und Einordnung möglicher Folgen von IT-Auslagerungen auf das Risikomanagement
- Regelmäßige Überprüfung der Risikoanalyse auf Aktualität und Kritikalität der Dienstleistung
- Etablierung eines Monitorings der jeweiligen ausgelagerten Dienstleistung

- Erstellung eines Notfallmanagementplans im Falle einer Vertragsunterbrechung oder –beendigung
- Schriftliche Vereinbarung (Service Level Agreement) zur Gewährleistung der Aufrechterhaltung der Dienstleistungen mit dem Dienstleister insbesondere in Bezug auf das Notfallmanagement
- Risikenbehandlungen, Anforderungen und Maßnahmen, die für das beaufsichtigte Unternehmen gelten, werden auch für den Dienstleister verbindlich und vertraglich festgelegt

Bei Ausfall der ausgelagerten Systemfunktionen bzw. Dienstleistungen wird der Geschäftsbetrieb nicht beeinträchtigt.

11. VERFÜGBARKEIT UND KONTINUITÄT, NOTFALLMANAGEMENT

Unter Verfügbarkeits- und Kontinuitätsrisiko ist das Risiko aus Beeinträchtigungen der Leistung und Verfügbarkeit von IT-Systemen zu verstehen. Insbesondere manifestiert sich das Risiko aus der mangelnden Fähigkeit der zeitkritischen Wiederherstellung von Leistungen, die aufgrund von Hardware- oder Softwareversagen geschädigt wurden, sowie durch allgemeine Schwächen im Management von IT-Systemen.

Ein Rahmenwerk zur Identifikation, Messung und Begrenzung des Verfügbarkeits- und Kontinuitätsrisikos wird daher implementiert. Dabei werden kritische Geschäftsprozesse und die dazu gehörigen IT-Ressourcen identifiziert, analysiert und in die geschäftlichen Ausfallsicherheits- und Kontinuitätspläne eingebunden.

Ein adäquates Notfallmanagement umfasst Strategien, Pläne, Handlungen und physische Maßnahmen zur Notfallvorsorge, Notfallbewältigung und Notfallnachsorge, um kritische Prozesse und Ressourcen bei unvorhergesehenen Unterbrechungen präventiv zu schützen und rasch wiederherzustellen.

Die Hauptaufgaben des Notfallmanagements sind zum einen, die Stabilisierung der Geschäftsprozesse, um die Wahrscheinlichkeit eines Schadenszwischenfalls zu minimieren und zum anderen, die bestmögliche Vorbereitung auf Zwischen- oder Notfälle sicherzustellen. Dabei gewährleisten Geschäftsfortführungs- und Wiederanlaufpläne, dass im Notfall zeitnah Ersatzlösungen zur Verfügung stehen und innerhalb eines angemessenen Zeitraums der Normalbetrieb wieder ermöglicht wird.

Die Festlegung von präventiven Maßnahmen, Sicherungs- und Wiederherstellungsverfahren, Störfallmanagement- und Eskalationsprozessen, Kapazitätsplanungslösungen in Richtlinien, Standards und operativen Kontrollen dient der Schaffung eines adäquaten Rahmenwerks. Die festgelegten Maßnahmen sind dazu geeignet, das Ausmaß von Schäden zu reduzieren.

Die Kontinuität und Ausfallsicherheit ist ausreichend robust ausgestaltet und wird durch Notfallübungen überprüft, um eine rechtzeitige Wiederherstellung nach Betriebsstörungen zu gewährleisten. Die Notfallübungen müssen entsprechend geplant und dokumentiert werden.

Zur Erleichterung der Umsetzung des Notfallmanagements ist ein Koordinierungsgremium eingerichtet, dem Personen aus verschiedenen Organisationseinheiten angehören. Notfallpläne werden im Unternehmen kommuniziert und entsprechende Schulungen durchgeführt. Beschrieben werden dabei Informationen zur direkten Notfallbewältigung, Kontaktinformationen und Handlungsanweisungen, welche im Notfall durchzuführen sind.

Im Fall einer Auslagerung verbleibt die Verantwortung für angemessene Notfallpläne in Bezug auf die ausgelagerten Tätigkeiten beim auslagernden Unternehmen. Dabei kommt der Dienstleister den festgelegten Notfallplananforderungen des Unternehmens nach. Notfallkonzepte sind aufeinander abgestimmt.

12. BESONDERE ASPEKTE BEI WERTPAPIERFIRMEN BZW. WERTPAPIERDIENSTLEISTUNGSUNTERNEHMEN

Ein Spezialthema in Bezug auf IT-Risiken und das Outsourcing-Risiko ist bei Wertpapierunternehmen die Heranziehung von vertraglich gebundenen Vermittlern (VGV) als auch Wertpapiervermittlern (WPV) für ihre Wertpapierdienstleistungen. Auch hier liegt es in der Verantwortung des Rechtsträgers, dass Informationen, die diesen zur Verfügung gestellt und von diesen bearbeitet werden, entsprechend geschützt werden. Das heißt der Rechtsträger trifft Maßnahmen, die dafür sorgen, dass Anforderungen und Verpflichtungen, die für das beaufsichtigte Unternehmen gelten, auch für den WPV und VGV verbindlich sind. Insbesondere werden unter anderem folgende Fragestellungen betrachtet:

- Werden sämtliche relevanten Informationen, die sich bei den VGV und WPV befinden, angemessen geschützt?
- Sind die bei den VGV und WPV verwendeten Applikationen und Systeme (z.B. Cloud, WLAN, mobile Geräte, etc.) als sicher zu beurteilen?
- Wird eine regelmäßige Wartung (z.B. Security-Patches, Antivirus-Programme, Wartung der Firewall, etc.) in Bezug auf IT-Sicherheit bei den VGV und WPV durchgeführt?
- Befinden sich bei den VGV und WPV Informationen, die als wesenglich zu betrachten sind und nicht gesichert werden?
- Gibt es bei den WPV und VGV entsprechende Vorkehrungen in Bezug auf Zugriffskontrolle?
- Verfügen die WPV und VGV über ein angemessenes Passwortmanagement (Komplexität, Länge und Lebensdauer von Passwörtern)?
- Wurden bei den VGV und WPV im Falle einer Auslagerung der IT bzw. von IT-Dienstleistungen entsprechende Sicherheitsvorkehrungen getroffen?