IDW KNOWLEDGE PAPER

CYBERRISK

TEIL 2: PRÜFUNGEN VON CYBER SECURITY BEI KREDITINSTITUTEN

STAND 12.05.2022

IDW
INSTITUT DER WIRTSCHAFTSPRÜFER

INHALT

Executive Summary 4

1. Einleitung und Motivation **5**

2. Umgang mit Cyberrisiken im Rahmen der Jahresabschlussprüfung von Kreditinstituten 7
2.1. Handelsrechtliche Abschlussprüfung von Kreditinstituten 7
2.1.1. Bedeutung von Cyberrisiken für die Jahresabschlussprüfung von Kreditinstituten 7
2.1.2. Prüferische Reaktion auf identifizierte Cyberrisiken 7
2.2. Umgang mit Cyberrisiken oder Cyberangriffen im Rahmen der aufsichtlichen Prüfung 8
2.2.1. Regulatorische Anforderungen an Kreditinstitute 8
2.2.2. Exkurs: Ausgewählte aufsichtliche Anforderungen in Bezug auf Cyberrisiken 9

3. Prüfung von Cyber Security im Rahmen einer Schwerpunktprüfung durch den Aufsichtsrat oder im Rahmen einer freiwilligen Prüfung außerhalb der Abschlussprüfung 12
3.1. Aufsichtsratsschwerpunkt Cyber Security 13
3.2. Cyber Security-Prüfungen außerhalb der Abschlussprüfung 13
3.3. Exkurs: Potenzielle Inhalte von Schwerpunktprüfungen oder einer freiwilligen Prüfung außerhalb der Abschlussprüfung 14
3.3.1. Bedrohungsanalyse 14
3.3.2. Angemessenheit der Informationssicherheitsorganisation und -funktionen 15
3.3.3. Beurteilung der Wirksamkeit ausgewählter Schutzmaßnahmen zum Schutz vor Cyberrisiken 17

Anlage: Beispiele ausgewählter Untersuchungsgegenstände nach dem NIST-Framework 20

Fußnoten 26

EXECUTIVE SUMMARY

- Cyberrisiken gehören zu den Top-Unternehmensrisiken. Dies belegen bedauerlicherweise auch neuerliche Cyberattacken im Zusammenhang mit dem Krieg in der Ukraine.
- Im politischen Diskurs wird daher zurecht betont, dass sich Privatpersonen wie Unternehmen vor Cyberattacken schützen müssen. Effektive Cyber Security-Vorkehrungen gehören mittlerweile zur Basis nachhaltigen Handelns.
- Die Angemessenheit und Wirksamkeit der Cyber Security-Vorkehrungen sollte regelmäßig hinterfragt und geprüft werden.
- Das vorliegende Knowledge Paper beschreibt, inwiefern eine Auseinandersetzung mit Cyber Security bereits standardmäßig im Rahmen der Abschlussprüfung bzw. bei der aufsichtlichen Prüfung von Kreditinstituten erfolgt.
- Es wird festgehalten, dass die Prüfung von Cyber Security-Maßnahmen nicht per se Gegenstand der gesetzlichen Jahresabschlussprüfung ist. Sollte der Abschlussprüfer jedoch Cyberrisiken identifizieren, die Auswirkungen auf wesentliche Darstellungen in Abschluss und Lagebericht haben können, hat er hierauf angemessen zu reagieren.
- Darüber hinaus wird das Informationssicherheitsmanagement (und damit implizit auch Cyberrisk) bei Kreditinstituten in den weitergehenden aufsichtlichen Prüfungspflichten nach § 29 KWG adressiert. Allerdings hat der Prüfer auch hier keine explizite und umfassende Aussage zur Angemessenheit und Wirksamkeit von Cyber Security Vorkehrungen zu treffen.
- Das Papier beschreibt, dass viele Geschäftsleiter bzw. gesetzliche Vertreter und Aufsichtsorgane bereits die Notwendigkeit von Cyber Security-Prüfungen erkannt haben und daher interne wie externe Prüfungen beauftragen.
- Es wird dargelegt, dass sich für eine tiefergehende Befassung mit der Angemessenheit und Wirksamkeit von Cyber Security von Unternehmen insb. die Beauftragung von ergänzenden Prüfungsschwerpunkten durch den Aufsichtsrat (als Erweiterung der Abschlussprüfung) oder von freiwilligen Cyber Security-Prüfungen auf der Basis von gängigen Prüfungsstandards anbieten.
- Beide Prüfungen werden als probates Mittel angesehen, um die Cyberresilienz zu bewerten, proaktiv notwendige Handlungsfelder zu identifizieren und die Cyber Security im Unternehmen zu verbessern.

1. EINLEITUNG UND MOTIVATION

Durch die zunehmende Digitalisierung und technische Vernetzung von Unternehmen kommt der Informationssicherheit[1] eine besondere Rolle zu, um Vertrauen in Technologie und eine nachhaltige Entwicklung zu gewährleisten. Technologien werden angreifbarer und die Gefahren sowie Angriffe aus dem Cyberraum nehmen stetig zu. Zudem sind derzeit leider auch Angriffe auf Technologien als eine Möglichkeit der modernen Kriegsführung zu beobachten.

Mit steigender Zahl an Cyberangriffen nimmt auch die Relevanz von Cyber Security stetig zu. Im Allianz Risk-Barometer stehen Cyberrisiken 2022 auf Platz 1 der wichtigsten globalen Unternehmensrisiken.[2] Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) meldet in seinem Lagebericht 2021 einen Anstieg der Gefährdungen durch Cyberangriffe. So wurden beispielsweise im Jahr 2021 ca. 15 Mio. Meldungen zu Schadprogramm-Infektionen erfasst, nachdem im Vorjahr ca. 7 Mio.

Meldungen verzeichnet wurden.[3] Um diesen und weiteren IT-Risiken zu begegnen, sind seitens der EU u.a. im Entwurf des Digital Operational Resilience Act (DORA)[4] weitere Maßnahmen geplant, um die Widerstandsfähigkeit gegen IT-bezogene Risiken zu stärken und die diesbezüglichen Regelungen in der EU zu harmonisieren.

Um sich gegen die zunehmenden Bedrohungen zu wappnen, können Unternehmen IT-Systemprüfungen durchführen lassen und hierbei einen Schwerpunkt auf das Management von Cyberrisiken legen. Die Untersuchungen können Gefährdungen sowie notwendige Handlungsfelder frühzeitig identifizieren, um diese proaktiv anzugehen und Informations- und Cyberrisiken insgesamt deutlich zu reduzieren. Zudem können sie bei der Einhaltung der Sorgfaltspflichten der Geschäftsleitung zur Einrichtung von Kontroll- und Überwachungssystemen sowie der Überwachungspflicht des Aufsichtsgremiums unterstützen.

Nachdem in Teil I[5] des IDW Knowledge Paper „Cyber Risk“ vor allem Grundlagen (Arten von Cyberattacken, Schutzmaßnahmen, Standortbestimmung, Organisationen, Strategien) dargestellt wurden, befasst sich Teil II der Reihe mit Cyber Security-Prüfungen. In einem ersten Schritt wird erläutert, ob bzw. inwieweit Cyberrisken bereits als Gegenstand der gesetzlichen Abschlussprüfung adressiert werden. In einem zweiten Schritt werden Festlegungen von Prüfungsschwerpunkten durch den Aufsichtsrat und gesondert beauftragte freiwillige Prüfungen beleuchtet.[6]

Im vorliegenden Knowledge Paper liegt der Fokus auf der Prüfung von Kreditinstituten, da hier die aufsichtlichen Anforderungen an die IT sowie deren Prüfungen besonders ausgeprägt sind. Das IDW möchte mit diesem Knowledge Paper einen weiteren Beitrag für die aus der Sicht des Berufsstands wichtige Debatte zur Prävention vor Cyberangriffen leisten.

2. UMGANG MIT CYBERRISIKEN IM RAHMEN DER JAHRESABSCHLUSSPRÜFUNG VON KREDITINSTITUTEN

Gegenstand und Umfang der Jahresabschlussprüfung bei Kreditinstituten ergeben sich aus § 340k Abs. 1 HGB i.V.m. § 317 HGB. Darüber hinaus sind bei Kreditinstituten weitergehende aufsichtliche IT-Prüfungen nach § 29 KWG i.V.m. den Vorgaben der PrüfbV sowie insb. den „Bankenaufsichtlichen Anforderungen an die IT“ (BAIT)[7] durchzuführen.

2.1. Handelsrechtliche Abschlussprüfung von Kreditinstituten

2.1.1. Bedeutung von Cyberrisiken für die Jahresabschlussprüfung von Kreditinstituten

Cyberrisiken bzw. Maßnahmen zur Cyber Security sind nicht per se Gegenstand der gesetzlichen Jahresabschlussprüfung. Im Rahmen der Prüfung hat der Wirtschaftsprüfer vielmehr zunächst zu identifizieren und zu beurteilen, ob Cyberrisiken möglicherweise zu wesentlichen Falschdarstellungen im Abschluss oder Lagebericht führen können und zu würdigen, ob und wie diese ggf. bedeutsamen Risiken im Internen Kontrollsystem berücksichtigt sind. Hierbei sind auch ausgelagerte Bereiche und Funktionen in die Beurteilung einzubeziehen. In diesem Zusammenhang hat der Abschlussprüfer die für die Prüfung relevanten rechnungslegungsbezogenen IT-Systeme dahingehend zu beurteilen, ob sie den Anforderungen – insb. den im IDW RS FAIT 1[8] dargestellten gesetzlichen Ordnungsmäßigkeits- und Sicherheitsanforderungen – entsprechen, um die geforderten Prüfungsaussagen[9] über die Ordnungsmäßigkeit der Buchführung treffen zu können. Erfolgreich durchgeführte Cyberangriffe können wesentliche finanzielle Folgen (Reputations- und finanzielle Schäden) haben und sich somit auf den Jahresabschluss oder Lagebericht auswirken und – auch wenn sie zunächst ggf. unentdeckt bleiben – unternehmensweit zu langfristigen Schäden führen.

2.1.2. Prüferische Reaktion auf identifizierte Cyberrisiken

Bedeutende und schnelle Veränderungen in Informationssystemen, die Einbindung neuer Technologien in Geschäftsabläufe oder die Erweiterung des Betriebs können neue Cyberrisiken mit sich bringen. Daher ist es wichtig, dass Unternehmen die IT- und Informationsrisiken in ihre Risikoin-

ventur einbeziehen und die Angemessenheit und Wirksamkeit der hierfür eingerichteten Kontrollen regelmäßig evaluieren.

Stellt der Abschlussprüfer bei seiner Prüfung ein wesentliches Cyberrisiko fest, hat er dessen Auswirkungen auf den Abschluss und dessen Darstellung im Lagebericht zu würdigen.

Um die Auswirkungen auf die Abschlussprüfung insgesamt zu bewerten, wird sich der Abschlussprüfer mit der Art und Ursache von Cybervorfällen (z.B. Maleware auf den Unternehmensservern oder Datendiebstahl) befassen und die Auswirkungen auf das rechnungslegungsbezogene Kontrollsystem (z.B. Betroffenheit rechnungslegungsrelevanter IT-Anwendungen) und die Rechnungslegung analysieren.

Der Wirtschaftsprüfer gibt jedoch im Rahmen der Abschlussprüfung kein gesondertes Urteil zum rechnungslegungsbezogenen Internen Kontrollsystem oder zur Angemessenheit und Wirksamkeit von Vorkehrungen der Cyber Security ab.

2.2. Umgang mit Cyberrisiken oder Cyberangriffen im Rahmen der aufsichtlichen Prüfung

2.2.1. Regulatorische Anforderungen an Kreditinstitute

Über die Vorschriften zur Prüfung von Jahresabschluss und Lagebericht nach § 340k Abs. 1 HGB i.V.m. § 317 HGB hinaus unterliegen Kreditinstitute weiteren regulatorischen Anforderungen, die Gegenstand der aufsichtlichen Prüfung im Rahmen der Jahresabschlussprüfung sind (§ 29 KWG).

Als zentrale Norm in Bezug auf die Regulatorik für Banken bestimmt § 25a Abs. 1 S. 1 KWG, dass Institute über eine ordnungsgemäße Geschäftsorganisation[10] verfügen müssen. Diese gesetzlichen Vorgaben werden zusammen mit den Vorgaben zur Auslagerung von Aktivitäten und Prozessen (§ 25b KWG) von der BaFin in den Rundschreiben (BA) „Mindestanforderungen an das Risikomanagement (MaRisk)[11]“ sowie (BA) „Bankaufsichtliche Anforderungen an die IT (BAIT)[12]“ konkretisiert.

Cyberrisiken werden in den MaRisk und in den BAIT bislang nur indirekt thematisiert. So finden sich in den MaRisk Vorgaben zu Strategien (Abschnitt AT 4.3), zur technisch-organisatorischen Ausstattung (AT 7.2), zu Notfallkonzepten (AT 7.3), zu Anpassungsprozessen (AT 8) und zu Auslagerungssachverhalten (AT 9). Darüber hinaus können sich Cyberrisiken beispielsweise im Risikomanagement bei den operationellen Risken auswirken (BTR 4).

Da die Vorgaben der BAIT bzgl. der dargestellten Themenbereiche nach Regelungstiefe und -umfang nicht abschließend sind, werden sich Institute bei der Ausgestaltung der IT-Systeme und der dazugehörigen IT-Prozesse grundsätzlich an gängigen Standards[13] orientieren.

Es ist zu berücksichtigen, dass der Abschlussprüfer nach den Vorgaben des KWG bzw. der PrüfbV grundsätzlich keine explizite Aussage speziell zur Angemessenheit oder Wirksamkeit der Cyber Security-Vorkehrungen im Rahmen seiner Berichterstattung über die aufsichtliche Prüfung zu treffen hat.

2.2.2. Exkurs: Ausgewählte aufsichtliche Anforderungen in Bezug auf Cyberrisiken

Im Folgenden werden einzelne Teilaspekte beschrieben, die in den BAIT konkretisiert werden und in Bezug auf Cyberrisiken – unter Berücksichtigung des Grundsatzes der Proportionalität – relevant sein können:

Informationsrisikomanagement

Cyberrisiken können als sog. „Querschnittsrisiken“ bezeichnet werden und maßgeblich Einfluss auf die gesamte Risikolage eines Kreditinstituts haben. Demnach sollten Cyberrisiken mit ihrem operativen, technischen, finanziellen und reputationsrelevanten Bedrohungspotenzial mit allen anderen Risikoarten des Kreditinstituts stringent und konsequent betrachtet und im Informationsrisikomanagement des Instituts abgebildet werden.

Informationssicherheitsmanagement

Im Informationssicherheitsmanagement sind aufbau- und ablauforganisatorische Maßnahmen zu treffen, um Cyberrisiken wirksam zu begegnen. Hierzu zählt zunächst als zentrale 2nd Line-Einheit der Chief Information Security Officer (CISO), der die übergreifende Konzeption und Etablierung eines effektiven Informationssicherheitsmanagementsystems (ISMS) verantwortet. Die Ausprägung dieser 2nd Line-Einheit ist zentral für eine angemessene Definition der Rahmenparameter zum Management von Cyberrisiken.

Die Position des CISO ist so ausgestaltet, dass er zum einen unabhängig von der Informationstechnologie agieren kann und zum anderen effektiv in das Risikomanagement insgesamt eingebunden ist. Da die notwendigen Reaktionen auf Cyberangriffe im Einzelnen schwer im Voraus zu planen sind, ist Agilität elementar für die Cyberresilienz einer Organisation. Dafür benötigt der CISO ausreichende Informationen, um angemessen kontrollieren und steuern zu können.

Neben der 2nd Line ist die 1st Line und damit die operative IT-Sicherheit für die praktische Umsetzung der Maßnahmen zur Sicherstellung der Cyber Security verantwortlich. Die 1st Line kann sich wiederum in verschiedene Teileinheiten aufgliedern, die spezifische Aufgaben übernehmen, wie z.B.

- Betrieb des Security Operation Center (SOC),
- Betrieb des Security Incident und Event Management (SIEM),
- Durchführung von Penetrationstests und Schwachstellenanalysen.

Des Weiteren können für Spezialsachverhalte weitere Einheiten auch temporär vorgehalten werden (z.B. eine Task-Force bzgl. eines konkreten Cybervorfalls, Computer-Security Incident Response Teams oder Red Teams in Zusammenhang mit dem TIBER-EU Framework der EZB[14]).

Darüber hinaus können weitere organisatorische Maßnahmen betrachtet werden, z.B. Awareness-Maßnahmen in Form von Schulungen.

Operative Informationssicherheit

In der operativen Informationssicherheit werden die Anforderungen des Informationssicherheitsmanagements umgesetzt. Zentral ist hierbei die Frage, inwieweit alle wesentlichen identifizierten Risiken bei den Schutzmaßnahmen berücksichtigt wurden. Übergreifend sollten alle relevanten Maßnahmen in der Informationssicherheitsleitlinie des Kreditinstituts enthalten sein. Zudem sollten spezifische Cyber-Response Pläne für ausgewählte Cyber-Angriffsszenarien (z.B. DDoS-Angriff, Ransomware oder Malware-Verbreitung oder identifizierte Advanced Persistent Threats (APT)) vorliegen.

Die Sicherheit der IT-Systeme ist regelmäßig, anlassbezogen und unter Vermeidung von Interessenskonflikten vom Kreditinstitut zu überprüfen. Ergebnisse sind seitens des Instituts hinsichtlich notwendiger Verbesserungen zu analysieren, und Risiken angemessen zu steuern.

Formen der Überwachung sind z. B.:

- Schwachstellenscans,
- Penetrationstests,
- Simulationen von Angriffen.

Identitäts- und Rechtemanagement

Im Identitäts- und Rechtemanagement ist durch das Institut sicherzustellen, dass die den Benutzern eingeräumten Berechtigungen so ausgestaltet und genutzt werden, wie es den organisatorischen und fachlichen Anforderungen und Vorgaben des Instituts entspricht. Berechtigungskonzepte sind regelmäßig und anlassbezogen vom Institut zu überprüfen und ggf. zu aktualisieren. Maßnahmen zur Verhinderung einer Umgehung des Berechtigungskonzepts sind einzurichten. Hierzu gehören u.a. die Auswahl angemessener Authentifizierungsverfahren, die Implementierung einer Richtlinie zur Wahl sicherer Passwörter und die automatische Überwachung auf Einhaltung dieser Richtlinien. Das Unternehmen hat sicherzustellen, dass Zugriffe und Zugänge jederzeit zweifelsfrei einer handelnden bzw. verantwortlichen Person (möglichst automatisiert) zugeordnet werden können.

IT-Projekte und Anwendungsentwicklung

Bei der Anwendungsentwicklung ist zu gewährleisten, dass je nach Schutzbedarf angemessene Vorkehrungen getroffen werden, denen zufolge die Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der zu verarbeitenden Daten nach jeder erneuten Produktivsetzung einer IT-Anwendung sichergestellt ist. Dies kann z.B. durch:

- Benutzerauthentifizierung,
- Transaktionsautorisierung,
- Prüfpfade (Audit Logs),
- Behandlung von Ausnahmen,
- Code Review oder
- Toolchain-Analyse (d.h. regelmäßige Prüfung auf bekanntgewordene Vulnerabilitäten aller Software-Abhängigkeiten)

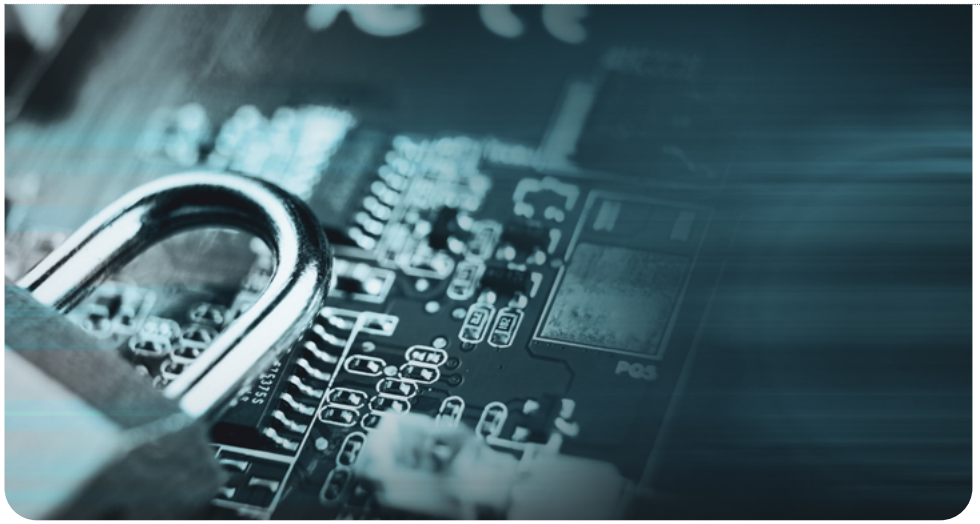
erfolgen. Eine Methodik für das Testen von Anwendungen ist vor ihrem erstmaligen Einsatz und nach wesentlichen Änderungen zu definieren und einzuführen. Die vom Institut durchgeführten Tests haben in ihrem Umfang die Funktionalität der Anwendung, die implementierten Maßnahmen zum Schutz der Informationen und bei Relevanz die Systemleistung unter verschiedenen Stressbelastungsszenarien einzubeziehen. Die fachlich zuständigen Stellen bzw. die Fachabteilung des Instituts haben die Durchführung von Abnahmetests zu verantworten. Testumgebungen zur Durchführung der Abnahmetests haben den für diese wesentlichen Aspekten der Produktionsumgebung zu entsprechen.

IT-Betrieb

Der IT-Betrieb hat zu gewährleisten, dass z.B. Meldungen über ungeplante Abweichungen vom Regelbetrieb (Störungen) und deren Ursachen in geeigneter Weise erfasst, bewertet, insbesondere hinsichtlich möglicherweise resultierender Risiken priorisiert und entsprechend festgelegter Kriterien eskaliert werden. Des Weiteren sind Standardvorgehensweisen (z. B. für Schadcode auf Endgeräten oder Fehlfunktionen) zu definieren und ein geordneter Prozess zur Analyse möglicher Korrelationen von Störungen und deren Ursachen zu etablieren.

Notfallmanagement

Das Institut hat relevante IT-Notfallpläne zu erstellen und zu testen. Im Fokus steht das Notfallkonzept vor allem für IT-Systeme, die zeitkritische Aktivitäten und Prozesse unterstützen. Das Notfallkonzept hat auch Maßnahmen gegen Ausfälle durch Cyberangriffe zu enthalten.



3. PRÜFUNG VON CYBER SECURITY IM RAHMEN EINER SCHWERPUNKTPRÜFUNG DURCH DEN AUFSICHTSRAT ODER IM RAHMEN EINER FREIWILLIGEN PRÜFUNG AUSSERHALB DER ABSCHLUSSPRÜFUNG

Der in § 340k Abs. 1 HGB i.V.m. § 317 HGB geregelte Gegenstand und Umfang der Abschlussprüfung kann selbstverständlich nicht eingeschränkt werden. Eine Erweiterung des Prüfungsauftrags ist gleichwohl möglich, z.B. durch die Abstimmung zusätzlicher Prüfungsschwerpunkte. Hierdurch kann der Abschlussprüfer den Aufsichtsrat bei seiner Überwachungstätigkeit über den gesetzlich gesetzten Rahmen der Abschlussprüfung hinaus unterstützen und einen Mehrwert generieren. Um die Tiefe von Prüfungshandlungen unternehmens- oder risikospezifisch auszurichten, kann alternativ zu Schwerpunktsetzungen durch den Aufsichtsrat im Rahmen einer Abschlussprüfung auch eine gesonderte Beauftragung von IT-Prüfungen außerhalb der Abschlussprüfung *(IDW PS 860)*[15] erfolgen.[16] So kann eine im Vergleich zur Abschlussprüfung spezifische Befassung mit Informationssicherheitsrisiken und eine gesonderte Betrachtung der Angemessenheit und Wirksamkeit der Maßnahmen zur Cyber Security ermöglicht werden.

3.1. Aufsichtsratsschwerpunkt Cyber Security

Aufgrund der steigenden Gefährdungslage durch Cyberrisiken in den letzten Jahren, ist zunehmend festzustellen, dass Aufsichtsräte eine Schwerpunktprüfung zur Cyber Security beauftragen. Der konkrete Gegenstand der Prüfung („Scope“) wird vor Beginn der Prüfung zwischen Aufsichtsrat und Abschlussprüfer geregelt und ggf. während der Vorstellung der Prüfungsplanung in der Sitzung des Prüfungsausschusses erörtert. Wichtig ist bei der Festlegung des Schwerpunkts, dass keine mit der Prüfung unvereinbare Tätigkeit, z.B. in Form einer Beratung, vereinbart wird. Während der Prüfung kann zu bestimmten Zeitpunkten eine mündliche Berichterstattung zum jeweils aktuellen Status der Prüfung gegenüber dem Aufsichtsrat erfolgen. Das Ergebnis der Prüfung wird zudem in die Berichterstattung zur Abschlussprüfung einbezogen.

Der Scope der Prüfung ist maßgeblich bestimmt durch die individuelle Risikosituation des Instituts, die wiederum maßgeblich von der Geschäftstätigkeit oder auch vom Umfang externer Leistungsbeziehungen abhängt. Ausgangspunkt für die Definition des Scopes kann die vom Institut selbst erstellte Gefährdungsanalyse für Cyberrisiken sein. In die Betrachtung sollten auch Auslagerungsbeziehungen, insb. mit Bezug auf Kern-IT-Dienstleistungen oder auch maßgebliche Business-Process-Auslagerungen bei der Definition des Prüfungsumfangs einbezogen werden. Hier kann auch die verstärkte Nutzung von Cloud-Dienstleistungen eine Rolle spielen, die ggf. eine weitere Schwerpunktsetzung darstellen kann.

In der Praxis ergeben sich häufig aus Sonderprüfungen der Bankenaufsicht oder auch Prüfungen der Internen Revision Anlässe für das Festlegen von Prüfungsschwerpunkten. In diesen Fällen wird üblicherweise auf die bereits identifizierten Risiken abgestellt. In einer Konkretisierung kann erfahrungsgemäß auch der Wunsch des Aufsichtsrats einfließen, ein Gesamtbild zur Cyber Security zu erhalten. Soweit Projekte zur Reduzierung identifizierter Risiken durch das Institut initiiert wurden, kann die Schwerpunktsetzung im Bereich Cyber Security zudem mit Elementen einer projektbegleitenden Prüfung im Rahmen der Jahresabschlussprüfung kombiniert bzw. ergänzt werden.

3.2. Cyber Security-Prüfungen außerhalb der Abschlussprüfung

IDW PS 860 adressiert speziell die IT-Prüfung außerhalb der Abschlussprüfung. Die Entwicklung des *IDW PS 860* war maßgeblich dadurch begründet, dass bis zu diesem Zeitpunkt ein Prüfungsstandard für die IT-Prüfung außerhalb der Abschlussprüfung fehlte und insofern bei der IT-Sicherheit keine standardisierten Verfahren angewendet werden konnten. Der eingeführte Prüfungsstandard steht im Einklang mit dem International Standard on Assurance Engagements (ISAE) 3000 (Revised)[17] und ermöglicht einen breiten Anwendungsbereich.[18]

Nach *IDW PS 860*[19] kann zwischen zwei Auftragsarten unterschieden werden: Zum einen kann die Erklärung zum IT-System Gegenstand der Prüfung sein und zum anderen kann eine direkte IT Prüfung durchgeführt werden.[20] Im Folgenden wird lediglich die direkte IT-Prüfung betrachtet.

Gegenstand der direkten IT-Prüfung ist das abgegrenzte IT-System hinsichtlich der Einhaltung bestimmter Kriterien. Die direkte Prüfung kann als Angemessenheitsprüfung „Design & Implementation" (D&I) und darüber hinaus als Wirksamkeitsprüfung „Operating Effectiveness" (OE) durchgeführt werden.

Im Rahmen der Prüfung von D&I sind die vorhandenen Kontrollen auf Mängel in der Konzeption zu untersuchen. Im Anschluss kann die Prüfung der OE erfolgen. Unterschiede im Vergleich zu einer Prüfung aufgrund eines Aufsichtsratsschwerpunkts gibt es bei einer IT-Prüfung außerhalb der Jahresabschlussprüfung im Wesentlichen bzgl. des zeitlichen Ablaufs, des Prüfungsurteils sowie der Berichterstattung.

3.3. Exkurs: Potenzielle Inhalte von Schwerpunktprüfungen oder einer freiwilligen Prüfung außerhalb der Abschlussprüfung

3.3.1. Bedrohungsanalyse

Ausgangspunkt ist die Erhebung der vom Institut definierten Vorgaben und Prozesse zur Durchführung von Bedrohungs- und Gefährdungsanalysen. Die verwendete Methodik und die Ergebnisse der Unternehmensanalysen sind im Einzelnen in die Berichterstattung des Prüfers aufzunehmen. Die Ableitung von Kriterien sollte an gängigen IT-Standards ausgerichtet werden.

Bei institutsspezifischen Besonderheiten kann es sinnvoll sein, Sollmaßnahmen für besondere Bedrohungen/Gefährdungen zu definieren und auf die Differenzierung bei definierten Sollschutzniveaus ("Sprunghöhe in den Maßnahmen") näher einzugehen. Ihre Angemessenheit kann insb. anhand von Spezifika des Geschäftsmodells, der Komplexität der technischen Infrastruktur oder der Exposition nach außen bewertet werden.

Gegenstand der Prüfung werden vor allem die Aspekte Aktualität, Nachvollziehbarkeit, Angemessenheit und Vollständigkeit betrachteter Bedrohungen und Gefährdungen sein. Darüber hinaus sind die Kommunikation und Abstimmung der Verfahren mit den relevanten Einheiten im Unternehmen sowie wesentlichen Stakeholdern zu validieren. Besondere Bedeutung kommt hierbei der Beurteilung der Nachvollziehbarkeit der Dokumentation zu.

3.3.2. Angemessenheit der Informationssicherheitsorganisation und -funktionen

Aufbauorganisatorische Vorkehrungen zu Cyber Security

Bei der Würdigung der aufbauorganisatorischen Vorkehrungen wird bei einer Schwerpunktprüfung oder einer freiwilligen Prüfung außerhalb der Jahresabschlussprüfung eine breitere und tiefere Sicht in Bezug auf Cyberrisiken eingenommen. Der Fokus liegt auf der konkreten Ausprägung von Sonderfunktionen und speziellen Sicherungsmechanismen, der Vorgabendefinition von 1st und 2nd-Line-Einheiten sowie der Tiefe und dem Detaillierungsgrad der Ausgestaltung spezifischer Regelungen. Diese müssen aus der initial betrachteten Gefährdungs-/Bedrohungsanalyse abgeleitet sein und sich an den besonderen Risiken des Instituts orientieren.

Ableitung von Schutzmaßnahmen für Cyber Security

Die Ableitung von Schutzmaßnahmen zur Cyber Security erfolgt anhand der vorgenannten Bedrohungs- und Gefährdungsanalyse.

Übergreifend sollten alle relevanten Maßnahmen in der Informationssicherheitsleitlinie der Bank enthalten sein. Zudem sollten spezifische Cyber Response-Pläne für ausgewählte Cyberangriffsszenarien (z.B. DDoS-Angriff, Ransomware oder Malware Verbreitung oder identifizierte Advanced Persistent Threats (APT)) vorliegen. Die Pläne sollen Hilfestellung zur Qualifizierung eines akuten Vorfalls geben und Handlungsoptionen für spezifische Angriffsszenarien konkret beschreiben. Mit ihrer Hilfe können zudem Verfahren und Prozesse bei Cybervorfällen standardisiert und im Vorfeld getestet werden, was im Notfall zu einer höheren Handlungssicherheit führt und die Auswirkungen eines Cybervorfalls minimiert.

Beurteilung der Angemessenheit der definierten aufbau- und ablauforganisatorischen Maßnahmen

Zur Beurteilung der Verfahren bietet sich eine Orientierung an gängigen IT-Standards an. Hierfür ist es notwendig, dass der Prüfer über spezifische Kenntnisse in der Prüfung der Einhaltung der betrachteten Standards verfügt. Der aktuell am häufigsten genutzte Standard ist das Cyber Security Framework des NIST[21], nach dem die Cyber Security anhand eines Phasenmodells umzusetzen und in der Prüfung entsprechend zu beurteilen ist.

Exkurs: NIST-Framework

- **"Identify":** Verständnis des Managements von Cyberrisiken und deren Auswirkungen auf Informationssysteme, Daten und Prozesse
- **"Protect":** Kontrollen und Schutzmaßnahmen zum Schutz des Unternehmens vor Cyberrisiken
- **"Detect":** Kontinuierliche Überwachung der IT und Erkennung von Cyberangriffen in Echtzeit
- **"Respond":** Fähigkeiten zur Analyse und Mitigierung laufender Angriffe sowie zur Begrenzung der Ausweitung und Auswirkungen
- **"Recover":** Vorkehrungen und Prozesse zur Aufrechterhaltung und Wiederherstellung des Geschäftsbetriebs

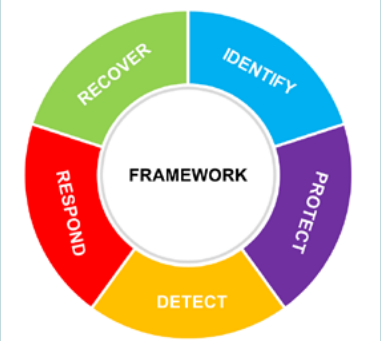


Abbildung 1: NIST Framework (Quelle: https://www.nist.gov/cyberframework/online-learning/five-functions)

Ziel der Prüfung ist die Beurteilung, ob die Maßnahmen des zu prüfenden Instituts zur Cyber Security eine angemessene Abdeckung der Kontrollanforderungen des NIST-Standards vorsehen. Dabei werden die getroffenen Vorkehrungen und Verfahren sowohl in der 2nd als auch in der 1st Line berücksichtigt.

Im Rahmen der Schwerpunktsetzung durch den Aufsichtsrat bzw. bei einer Prüfung außerhalb der Jahresabschlussprüfung kann eine Fokussierung bzw. Eingrenzung auf bestimmte Teilaspekte der Umsetzung von Kontrollen oder Phasen des NIST-Frameworks erfolgen. Erfahrungsgemäß ist eine Schwerpunktprüfung, z.B. mit Blick auf die Erkennung von und Reaktion auf Cybervorfälle, eine sinnvolle Ergänzung zur Jahresabschlussprüfung. Durch eine Fokussierung auf bestimmte Themenfelder bzw. bei einem definierten Schutzniveau kann die Schwerpunktprüfung problemorientiert eingegrenzt werden und die Detaillierung der Untersuchung auch unter Wirtschaftlichkeitsaspekten deutlich erhöht werden.

In der Praxis hat sich insb. der phasenweise Ansatz des NIST-Frameworks bewährt. In der Anlage findet sich eine beispielhafte Aufzählung möglicher Untersuchungsgegenstände auf der Basis des NIST-Framework.

3.3.3. Beurteilung der Wirksamkeit ausgewählter Schutzmaßnahmen zum Schutz vor Cyberrisiken

Ausgangspunkt für die Würdigung der Wirksamkeit von Schutzmaßnahmen ist die Beurteilung der Angemessenheit wesentlicher implementierter aufbau- und ablauforganisatorischer Vorkehrungen zum Schutz vor Cybervorfällen mit besonderem Fokus auf der nachvollziehbaren Ableitung der Vorkehrungen aus dem in der Bedrohungsanalyse ermittelten Bedrohungsprofil. Bei der Beurteilung der Wirksamkeit der Maßnahmen sollte sich der Prüfer auf spezifische Kernelemente fokussieren, die sinnvollerweise die bereits bei der Angemessenheitsbeurteilung vorgenommene Schwerpunktsetzung reflektiert.

Das Spektrum möglicher Prüfungshandlungen erstreckt sich von der Befragung von Mitarbeitern (z.B. um Erkenntnisse über die „Awareness“ gegenüber Cyberbedrohungen zu eruieren), über die Inspektion relevanter Dokumente (z.B. Behandlung von Informationssicherheitsvorfällen) bis hin zur Durchführung eigener Schwachstellenscans, dem Einsatz weitergehender Analysetools, der Durchführung von Penetrationstests oder der Adaption von Elementen sogenannter Red Teaming Assessments, bei denen der Geprüfte nur begrenzt über die von “Angreifern” vorgenommenen Handlungen informiert ist.

Es empfiehlt sich, das Ambitionsniveau, die Tiefe der Prüfung und die Breite des Einsatzes von Methoden und technischen Hilfsmitteln initial mit dem Auftraggeber und ggf. relevanten Dienstleistern abzustimmen, sodass das Prüfprogramm entsprechend zielorientiert ausgestaltet werden kann. In Einzelfällen sind diese in Absprachen mit dem geprüften Unternehmen auch vorab zu testen, um keine Schäden oder Betriebsunterbrechungen zu verursachen. Die von den Prüfungshandlungen adressierten Sicherheitsvorkehrungen und Kontrollen sollten unter Risikogesichtspunkten ausgewählt werden und im Hinblick auf für das Institut relevante Bedrohungsszenarien relevant sein. Ebenfalls ist vorab zu analysieren, welche Bestandteile des Informationsverbunds besondere Relevanz für Cyberbedrohungen aufweisen, z.B. wegen ihrer Exposition nach außen (Endpoint Security), wegen der Schutzbedürftigkeit der mit ihnen verarbeiteten Informationen oder wegen ihrer Vulnerabilität aufgrund nicht umgesetzter Schutzmaßnahmen.

In den folgenden Abschnitten werden beispielhaft Untersuchungsgegenstände für die Phasen „Detect“ und „Respond“ des NIST-Framework zur Ermittlung der Wirksamkeit getroffener Maßnahmen für die folgenden Bereiche beschrieben:

- SOC- und SIEM-Fähigkeiten,
- Patch- und Schwachstellenmanagement,
- Sicherheitsmanagement im Windows Active Directory.

SOC- und SIEM-Fähigkeiten

Zur Erkennung und Alarmierung erkannter Angriffe und Bedrohungen nutzen Unternehmen inzwischen überwiegend Security Information and Event Management Systeme (SIEM). Diese schaffen Transparenz über verdächtige Aktivitäten in Netzwerken anhand von Log-Daten, die aus diversen Quellen gesammelt, aufbereitet, auf der Basis vordefinierter Regeln analysiert und korreliert werden können. Der Umfang der zugrundeliegenden Protokollierung und somit auch die Vorgabe, welche Protokollinformationen eine SIEM-Lösung benötigt, wird für IT-Systeme aus den Sicherheitsvorgaben des Instituts abgeleitet und umgesetzt. Im Anschluss erfolgt eine gezielte Überwachung auf der Basis systemspezifischer und systemübergreifender Use Cases (Auswertungsregeln), die von der Organisation festgelegt und beschrieben werden müssen. Das SIEM ist somit eine Schlüsselkomponente für die Fähigkeiten einer Organisation, sicherheitsrelevante Bedrohungen zu erkennen ("detect").

Schlägt eine vordefinierte Auswertungsregel an oder detektiert die SIEM-Lösung mittels anderer Methoden anormales Verhalten, erfolgt i.d.R. eine Alarmierung, auf die ein Security Operations Center (SOC) reagieren muss. Die Aufgaben des SOC sollten darüber hinaus die proaktive Analyse und Recherche sicherheitsrelevanter Informationen, die Beratung der Organisation in Fragen der IT Security sowie weitere Aufgaben zur Cyber Security umfassen.

Das SOC ist somit eine Schlüsselkomponente für die Fähigkeiten einer Organisation auf sicherheitsrelevante Bedrohungen zu reagieren ("respond").

Beispielhaft kann durch den Prüfer eine Einsichtnahme in die Systeme zum Nachvollzug des technischen Aufbaus / der Architektur und Konfiguration der SIEM-Plattform sowie der Anbindung von Quellsystemen oder eine Validierung von Fokus und Reichweite der Leistungsfelder des SOC, z.B. in Bezug auf interne Szenarien oder den Leistungsschnitt mit Dienstleistern, erfolgen, um die Wirksamkeit der SOC- und SIEM-Fähigkeiten zu prüfen.

Patch- und Schwachstellenmanagement

Sicherheitslücken und Schwachstellen in IT-Systemen stellen potenzielle Einfallstore für Angreifer dar. Es ist von zentraler Bedeutung, dass bestehende Schwachstellen rechtzeitig vom Institut erkannt werden. Das mit der Schwachstelle einhergehende Risiko ist vom Institut zu bewerten, um angemessene Maßnahmen zur Risikobehandlung und -reduktion zu treffen. Um eine systematische Identifizierung von Schwachstellen sicherzustellen, ist vom Institut eine regelmäßige bzw. kontinuierliche Überprüfung von IT-Systemen erforderlich, um festzustellen, ob die Sicherheitsrichtlinien und -standards erfüllt werden. Zur Beurteilung der Wirksamkeit des Patch- und Schwachstellenmanagements kann z.B. der Scope bzw. der Abdeckungsgrad der durchgeführten Penetrationstests auf Basis vorliegender Ergebnisberichte analysiert und geprüft werden, ob die Behebung von Schwachstellen im Einklang mit den definierten Verfahren steht (z.B. zeitnahe Einspielung von Sicherheitspatches).

Sicherheitsmanagement im Windows Active Directory

Über Windows Active Directory Domänen wird die Authentifizierung von Mitarbeitern über Benutzer-Accounts sowie die Berechtigung für Administration und ggf. weitere Berechtigungen im Netzwerk abgebildet. Das Ziel möglicher Untersuchungshandlungen ist die Identifikation von Anomalien und Schwachstellen innerhalb der Domänen in Bezug auf Benutzer, Computer und Berechtigungen. Häufige Schwachstellen sind beispielsweise versehentlich vergebene Privilegien für Standardbenutzer oder besonders exponierte Service-Accounts mit schwachem Passwort. Als mögliche Prüfungshandlungen bieten sich z.B. die technisch unterstützte Extraktion wesentlicher Informationen zur Konfiguration, zu Benutzern sowie Domänendaten für Windows AD Domänen und Auswertung der Ergebnisse im Hinblick auf Auffälligkeiten oder die Analyse von Logon-Scripten und Dateien auf SYSVOL und NETLOGON Shares für alle erreichbaren Domänen an.

Hinweise:

- Über die aufgezählten Vorkehrungen hinaus bietet es sich ggf. an, weitere Analysen und Prüfungshandlungen zur Beurteilung der Wirksamkeit der getroffenen Vorkehrungen im Hinblick auf die Entdeckungs- und Reaktionsfähigkeiten der Organisation durchzuführen. Beispielsweise könnte geprüft werden, ob Maßnahmen zur Verhinderung einer unautorisierten Offenlegung von Unternehmensinformationen angemessen und wirksam ergriffen wurden (z.B. durch Auswertung von Threat Intelligence-Quellen). Dies betrifft auch potenziell sicherheitsrelevante Mitarbeiterinformationen (z. B. Mailadressen und Passwörter) sowie potenzielle Datenabflüsse von Stakeholdern des Unternehmens (z. B. Kundendaten).
- Wenn bereits Prüfungen von der Internen Revision oder auch von Externen, z.B. in Form von Sonderprüfungen durch die Bankenaufsicht, durchgeführt wurden, die direkt oder indirekt Cyber Security zum Gegenstand hatten, finden Prüfungsfeststellungen dieser Prüfungen Berücksichtigung im Rahmen der beauftragten Schwerpunktprüfung oder einer freiwilligen Prüfung außerhalb der Abschlussprüfung zur Cyber Security. Insbesondere werden eingeleitete Maßnahmen und deren Umsetzungsstand beurteilt, um eine ganzheitliche Beurteilung des Status zu ermöglichen und ggf. weitere notwendige Handlungsbereiche aufzuzeigen.

ANLAGE: BEISPIELE AUSGEWÄHLTER UNTERSUCHUNGSGEGENSTÄNDE NACH DEM NIST-FRAMEWORK

Identify

Cyber Governance

- Cyber Strategie
- Definition von Risikokapazität
- Verankerung in der schriftlich fixierten Ordnung (sfO)
- Aufbau- und Ablauforganisation
- Maßnahmen in Zusammenhang mit Auslagerungen und externen Dienstleistern

Cyber Threat Modelling

- Cyber Threat Model[22] zur Analyse der potenziellen Schwachstellen und Risiken
- Nachvollziehbare Angriffsszenarien sowie daraus abgeleitete Handlungsstrategien
- Berücksichtigung der Rolle der Bank im Rahmen von kritischen Infrastrukturen (KRITIS)
- Definition der eigenen „Crown-Jewels“, also der wichtigsten Assets des Instituts

Informationssicherheitsmanagementsystem (ISMS)

- Definition von Regeln und Methoden, um die Informationssicherheit in einem Unternehmen oder einer Organisation zu gewährleisten, z.B. anhand des vom Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlichten IT-Grundschutz-Kompendium[23]

Information Risk Management (IRM)

- Definition und Inventarisierung von kritischen Assets (Informationsverbund)
- Einbezug von Cyberrisiken im Risikomanagementprozess, u.a. die Definition von Toleranzen und Schwellenwerten sowie bei der Durchführung von Gefährdungsanalysen
- Prozesse zum Soll-Ist-Abgleich
- Maßnahmen zum Schutz vertraulicher Daten vor nicht autorisierten Zugriffen und zur Verhinderung von unkontrollierten Datenabflüssen

Protect

Cyber Maßnahmen

Maßnahmen und Ergebnisse, um eine Aussage über ihre Wirksamkeit abgeben zu können, insb.:

- **Information Protection Processes and Procedures**
  - Maßnahmen im Bereich Data Leakage, die als Kontrolle für identifizierte sensible Daten als präventive Verhinderung von unerwünschten Datenabflüssen im Unternehmen dienen, z.B. die Kontrolle zur Sicherung respektive Zerstörung von Datenträgern und die Etablierung von Standards im Rahmen der Systementwicklung mit Resilienzeigenschaften
  - Maßnahmen für das frühzeitige Erkennen und Verhindern von Angriffen durch eine ausreichende Protokollierung und Überwachung von systemseitig erzeugten Ereignissen
  - Maßnahmen zur Sicherstellung der Integrität des Gesamtsystems, die sich aus der Integrität von Teilsystemen ergibt, mit dem Ziel, ausschließlich autorisierte Veränderungen zu erlauben, z.B. die jeweilige Integrität von Software, Hardware und der Daten, die zwischen den Teilsystemen ausgetauscht werden
- **Awareness and Training**
  - Durchführung und Teilnehmerkreis von Awareness-Schulungen als Sensibilisie-

rungsmaßnahme für einen bewussten und sicheren Umgang mit IT-Systemen

- „Ransomware-sichere Verfahren“ für eine ordnungsgemäße Datensicherung zur Aufbewahrung von Kopien/Backups mit den dazugehörigen notwendigen Wiederherstellungstests
- Implementierung eines Schwachstellen-, Lebenszyklus-, Berechtigungs-Management und CERT-Meldungen innerhalb des Instituts

- **Protective Technology**
  - Sicherheitsvorkehrungen zum Aufbau und Etablierung von kontrollierten Zugängen im Netzwerk der Organisation als eine stabile Command und Control-Umgebung mit der Einrichtung von Schutzzonen durch die Segmentierung des Netzwerkes
  - Maßnahmen organisatorischer und technischer Natur zum Schutz von Unternehmensdaten für den Remote Access auf Ressourcen des Instituts, durch sichere VPN-Verbindungen oder die Vergabe von Benutzerrechten sowie die Überwachung von Anwendungen
  - Verwendung von Verschlüsselungslösungen (Data-at-Rest / Data-in-Transit) für Daten zur Verweigerung der Zugriffs- und Leserechte auf Klardaten

Detect

Anomalies and Events

- Prozesse zur Ermittlung eines Normalzustands (“baseline”) für Netzwerkaktivitäten sowie Datenflüsse für Systeme und Benutzer
- Vorgaben zur Behandlung und Dokumentation von Sicherheitsvorfällen (Security Incident Management) sowie zur Analyse von Angriffszielen und -methoden
- Konzeption zur Sammlung von Event-Daten aus unterschiedlichen Quellen bzw. Sensoren
- Prozesse des Informationsrisikomanagements einschließlich der Durchführung von Risiko- bzw. Auswirkungsanalysen für Sicherheitsvorfälle
- Nachvollziehbare Festlegung von Alarmierungsschwellen für verschiedene Incident-Klassen

Security Continuous Monitoring

- Prozesse zur Überwachung der Systeme und Netzwerke, um potenzielle Cybervorfälle zu identifizieren, ausgehend von präventiven Vorkehrungen zur Protokollierung von Events, zur Überwachung der Verbindung zu externen Netzwerken und Systemen, zum Schutz vor Denial of Service-Attacken, zur Steuerung und Pflege von Accounts und Berechtigungen sowie zur sicheren Durchführung von Systemänderungen bzw. Konfigurationen
- Vorkehrungen zur Überwachung der physischen Infrastruktur, um potenzielle Cybervorfälle zu identifizieren, ausgehend von präventiven Vorkehrungen im Bereich des physischen Zutrittsschutzes
- Prozesse zur Überwachung sensibler Accounts sowie zur Sicherstellung der revisionssicheren Protokollierung definierter Events
- Prozesse zur Identifikation der unerlaubten Veröffentlichung von Informationen des Instituts
- Vorkehrungen zur ausschließlichen Nutzung und Verteilung freigegebener und lizenzierter Softwareprodukte sowie zur Identifikation von Schadcode sowie unerlaubten mobilen Codes und Spam in Informationssystemen
- Prozesse zur Überwachung sicherheitsrelevanter Aktivitäten sowie Einhaltung definierter Sicherheitsvorgaben bei externen Dienstleistern
- Vorkehrungen zur Identifikation und Überwachung nicht autorisierter Verbindungen, Geräte sowie Software, u.a. ausgehend von der Erstellung und Pflege eines Inventars aller Informationssysteme
- Prozesse zur Durchführung regelmäßiger Schwachstellenscans in den Informationssystemen, um angemessene Gegenmaßnahmen umzusetzen

Detection Process

- Prozesse zur Identifikation von Cybervorfällen auf der Basis klar definierter Rollen und Verantwortlichkeiten, ausgehend von Verfahren zur Planung und Durchführung regelmäßiger Sicherheitsuntersuchung sowie vom Einsatz robuster und getesteter Mechanismen zur Verhinderung bzw. Identifikation von Sicherheitsverstößen
- Vorgaben zur Kommunikation relevanter Informationen zu den identifizierten Cybervorfällen
- Mechanismen zur kontinuierlichen Verbesserung der Prozesse zur Identifikation von Cybervorfällen

Respond and Recover

Response Planning

- Prozesse zur Erstellung, zur Pflege sowie regelmäßigen Überprüfung von Incident-Response- bzw. Notfallplänen, um nach einer Kompromittierung oder einem Ausfall die Wiederherstellung der Informationssysteme in einen stabilen Zustand unter Mitwirkung aller erforderlichen Ressourcen zu gewährleisten

Communications

- Vorgaben zur regelmäßigen und anlassbezogenen Durchführung von Trainings, Übungen und Tests, um sicherzustellen, dass Mitarbeiter ihre Rolle und die erforderlichen Abläufe zur Reaktion auf Cybervorfälle verstehen und die Wirksamkeit der Vorkehrungen zur Wiederherstellung von Informationssystemen gegeben ist
- Konzepte und Vorgaben für den Informationsaustausch mit externen Stakeholdern sowie mit Informationsdiensten (CERT) bezüglich Trends, Sicherheitslücken und Informationssicherheitsvorfällen, um die Informationsbasis und somit die Qualität zur Reaktion auf Cybervorfälle zu verbessern
- Prozesse zur internen und externen Berichterstattung von Informationssicherheitsvorfällen

Analysis

- Prozesse zur Untersuchung von Warnmeldungen bzgl. sicherheitsrelevanter Ereignisseaus den vorhandenen Überwachungsmechanismen und zur Erlangung eines Verständnisses über die Auswirkungen von sicherheitsrelevanten Ereignissen
- Vorgaben zur konsistenten Kategorisierung von Incidents im Einklang mit Incident Response-Plänen
- Vorgaben zur Initiierung forensischer Analysen bzgl. sicherheitsrelevanter Ereignisse, ausgehend von Mechanismen zur Protokollierung von Events in den Informationssystemen
- Prozesse zur Aufnahme, Analyse und Reaktion bzgl. Schwachstellen, die der Organisation aus internen und externen Quellen (z. B. interne Sicherheitsuntersuchungen, Nachrichtenkanäle oder CERT) bekannt werden

Mitigation

- Vorkehrungen und Regelungen zur Sicherstellung, dass sicherheitsrelevante Ereignisse sowie identifizierte neue Schwachstellen kontrolliert bzw. mitigiert oder unter bestimmten Voraussetzungen akzeptiert werden können

Improvements / Lessons Learned

- Prozesse zur kontinuierlichen Verbesserung von Incident-Response- bzw. Notfallplänen, unter Berücksichtigung neu gewonnener Informationen, z.B. Berichterstattung und Fortschritte in der Branche sowie Überprüfung der vorhandenen Prozesse

FUSSNOTEN

[1] Unter Informationssicherheit wird hier auch Cyber Security verstanden.

[2] Vgl. Allianz Risk Barometer 2022, https://www.allianz.com/content/dam/onemarketing/azcom/Allianz_com/press/document/Allianz_Risk_Barometer_2022_FINAL.pdf (Abruf 12.05.2022).

[3] Vgl. BSI: Die Lage der IT-Sicherheit in Deutschland 2021 (bund.de), https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2021.pdf;jsessionid=25E35714E184C43B30A298D567B52C73.internet471?__blob=publicationFile&v=3 (Abruf 04.05.2022).

[4] Vgl. Proposal for a Regulation of the European Parliament and the Council on digital operational resilience for the finanial sector and amending Regulations; https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020SC0198&from=EN (Abruf 05.05.2022).

[5] Vgl. IDW, Knowledge Paper Cyberrisk, Teil 1: Grundlagen – Definitionen, Maßnahmen, Risikolage und Organisation, https://www.idw.de/blob/133572/ca9fea53a51afa16df74831f1a4e38fe/down-cyberrisk-data.pdf (Abruf 04.05.2022).

[6] In diesem Knowledge Paper erfolgt keine umfangreiche Darstellung der Prüfungsmethodik. Ebenso hat dieses Papier nicht das Ziel, den komplexen Prüfungsansatz vertiefend zu erläutern.

[7] Rundschreiben 10/2017 (BA) in der Fassung vom 16.08.2021, Bankaufsichtliche Anforderungen an die IT (BAIT), https://www.bundesbank.de/resource/blob/863264/6e6c87e41efd6d70b48b587ec899b89b/mL/2017-10-bait-2021-data.pdf.

[8] *IDW Stellungnahme zur Rechnungslegung: Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie (IDW RS FAIT 1)*, Stand 24.09.2002.

[9] Gemeint ist hier die Berichterstattung des Prüfers nach § 340k Abs. 1 HGB i.V.m. § 317 Abs. 1 Satz 1 HGB und § 321 Abs. 2 HGB.

[10] Diese muss ein angemessenes Risikomanagement umfassen, welches eine angemessene personelle und technisch-organisatorische Ausstattung des Instituts (§ 25a Abs. 1 S. 3 Nr. 4 KWG) sowie ein angemessenes Notfallmanagement (§ 25a Abs. 1 S. 3 Nr. 5 KWG), insbesondere für IT-Systeme, beinhaltet.

[11] https://www.bundesbank.de/resource/blob/600412/5e84286665488cd27b7a31aa7663a77b/mL/2021-08-16-rundschreiben-data.pdf, in der Fassung vom 16.8.2021.

[12] Rundschreiben 10/2017 (BA) in der Fassung vom 16.08.2021, Bankaufsichtliche Anforderungen an die IT (BAIT), https://www.bundesbank.de/resource/blob/863264/6e6c87e41efd6d70b48b587ec899b89b/mL/2017-10-bait-2021-data.pdf.

[13] Zu diesen zählen beispielsweise der IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik oder die internationalen Sicherheitsstandards ISO/IEC 270XX der International Organization for Standardization und NIST 800-XX, bzw. für Auslagerungen *IDW RS FAIT 5.*

[14] TIBER-EU FRAMEWORK – How to implement the European framework for Threat Intelligence-based Ethical Red Teaming (europa.eu) (Stand: Mai 2018), https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf (Abruf 04.05.2022).

[15] *IDW Prüfungsstandard: IT-Prüfung außerhalb der Abschlussprüfung: Gegenstand, Ziel und Umfang der Prüfung (IDW PS 860)* (Stand 02.03.2018).

[16] Für Prüfungen bei Einsatz von Informationstechnologie ist *IDW Prüfungsstandard: Projektbegleitende Prüfung bei Einsatz von Informationstechnologie (IDW PS 850 n.F. (01.2022))* (Stand 24.01.2022) anwendbar, für Prüfungen einer Anwendungsentwicklung *IDW Prüfungsstandard: Die Prüfung von Softwareprodukten (IDW PS 880 n.F (01.2022))* (Stand 24.01.2022).

[17] International Standard on Assurance Engagements 3000 (Revised): Assurance Engagements Other than Audits or Reviews of Historical Financial Information (Stand Dezember 2013).

[18] Vgl. *IDW Prüfungsstandard: IT-Prüfung außerhalb der Abschlussprüfung: Gegenstand, Ziel und Umfang der Prüfung (IDW PS 860)* (Stand 02.03.2018).

[19] Unsere Ausführungen beschränken sich im Folgenden auf Prüfungen i.S.d. *IDW PS 860*, können jedoch auch analog für Prüfungen i.S.d. ISAE 3000 (Rev.) angewendet werden.

[20] Vgl. *IDW Prüfungsstandard: IT-Prüfung außerhalb der Abschlussprüfung: Gegenstand, Ziel und Umfang der Prüfung (IDW PS 860)* (Stand 02.03.2018), Tz. 12-22.

[21] Das Framework bietet Hilfestellungen, um Cyber-Sicherheitsaktivitäten zu implementieren und zu steuern sowie um Cyber-Sicherheitsrisiken als Teil der Risikomanagementprozesse der Organisation zu berücksichtigen. (The Five Functions/ NIST, https://www.nist.gov/cyberframework/online-learning/five-functions (Abruf 05.05.2022).

[22] Vgl. Cyber Threat Modeling: Survey, Assessment, and Representative Framework, https://apps.dtic.mil/sti/pdfs/AD1108051.pdf (Abruf 05.05.2022).

[23] Vgl. Broschüre Informationssicherheit mit System – Der IT-Grundschutz des BSI, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/sonstiges/Informationssicherheit_mit_System.html?nn=128656, (Abruf 05.05.2022) .

Ihre Notizen:

Ihre Notizen:

Ihre Notizen:

Dieses Knowledge Paper wurde vom IDW Arbeitskreis „IT-Prüfungen bei Instituten“ entwickelt.

Wir freuen uns über Ihre Anmerkungen. Sie können diese direkt an Frau Elisabeth Kern, Institut der Wirtschaftsprüfer in Deutschland e.V., Postfach 320580, 40420 Düsseldorf oder an elisabeth.kern@idw.de senden.

Copyright © Institut der Wirtschaftsprüfer in Deutschland e.V., Düsseldorf 2022.

Bildrechte:

Seite 4, 5, 7, 12, 20: anatolir©Adobe-Stock.com, Seite 4: BillionPhotos.com©Adobe-Stock.com, Seite 6: adam121©Adobe-Stock.com, Seite 12: sasun Bughdaryan©Adobe-Stock.com, Seite 20: kras99©Adobe-Stock.com

INSTITUT DER WIRTSCHAFTSPRÜFER IN DEUTSCHLAND E.V.
WIRTSCHAFTSPRÜFERHAUS

Tersteegenstr. 14
40474 Düsseldorf

Postfach 32 05 80
40420 Düsseldorf

Telefon: +49 (0) 211/4561-0
Telefax: +49 (0) 211/4561097

E-Mail: info@idw.de
Web: www.idw.de

IDW
INSTITUT DER WIRTSCHAFTSPRÜFER