CYBER & REGULATORIK PLAYBOOK 2024

horn & company

//Vorwort

Seit unserer Gründung im Jahr 2009 hat sich Horn & Company als Top-Management-Beratung im deutschsprachigen Raum fest etabliert. Unser Erfolg basiert auf einem tiefen Branchenverständnis und der langjährigen Erfahrung unserer Berater, die es uns ermöglichen, die digitale Transformation unserer Klienten nachhaltig zu gestalten. Was uns dabei auszeichnet, ist die Begleitung unserer Kunden von der Strategie bis zur erfolgreichen Umsetzung – mit einem besonderen Fokus auf die drängenden Fragen einer zunehmend vernetzten und technologiegetriebenen Welt.

Im Laufe der Jahre haben wir unser Beratungsangebot kontinuierlich erweitert. Zunächst auf deutschsprachige Unternehmen und Organisationen fokussiert, betreuen wir heute auch Klienten in Österreich sowie in der mittel- und osteuropäischen Region (CEE). Über unsere Wiener Dependance stellen wir sicher, dass wir auch in diesen Märkten maßgeschneiderte Lösungen anbieten können. In den Jahren 2018/19, 2020/21, 2022/23 sowie 2024/2025 wurden unsere Berater als „Hidden Champion des Beratermarktes" ausgezeichnet – ein Beleg für die hohe Qualität und den nachhaltigen Erfolg unserer Arbeit.

Ein besonders zentrales Thema, das unsere Kunden im Finanzsektor betrifft, ist die Cybersicherheit. Angesichts der wachsenden Bedrohungslage stehen Banken und Versicherungen unter ständigem Druck, ihre IT-Infrastrukturen sicher zu halten. Die täglichen Meldungen der BaFin und des BSI über Cyberangriffe auf Finanzinstitute verdeutlichen, dass der sichere IT-Betrieb ein Dauerthema bleibt. Neben den externen Bedrohungen durch Cyberkriminelle steigt auch die Gefahr durch Insider-Angriffe. Hinzu kommt die zunehmende Komplexität durch den verstärkten Einsatz von Cloud-Technologien, der sowohl neue Möglichkeiten als auch neue Herausforderungen mit sich bringt.

Kein Wunder also, dass Banken und Versicherungen derzeit erhebliche Summen in die Verbesserung ihrer Cybersicherheit und -Resilienz investieren. Ein wirksamer Schutz vor Cyberbedrohungen erfordert einen ganzheitlichen Ansatz, der sowohl technologische, als auch organisatorische Maßnahmen umfasst. Genau hier setzen wir mit unserer Beratung an, indem wir Unternehmen helfen, robuste und zukunftssichere Sicherheitsstrategien zu entwickeln.

Das H&C Team beobachtet für Sie die rasanten Entwicklungen in diesem Bereich genau und hat in dieser Unterlage die neuesten Anforderungen und Chancen, aus Theorie und Beratungspraxis zusammengetragen. Unsere praktischen Einblicke und Best-Practices geben Ihnen wertvolle Impulse, wie Sie Ihr Unternehmen bestmöglich schützen und zugleich zukunftssicher aufstellen können. Ob es um Cybersicherheit, Datenmanagement oder die Nutzung moderner Technologien geht – wir wissen, worauf es ankommt, und unterstützen Sie dabei, auch in einer sich ständig verändernden Bedrohungslandschaft gut vorbereitet zu sein.

Wir wünschen Ihnen eine spannende Lektüre und freuen uns darauf, Sie bei Ihren Herausforderungen zu begleiten – gemeinsam machen wir Ihr Unternehmen fit für die Zukunft.

Dr. Oliver Laitenberger

Dr. Christoph Hartl

Dr. Carsten Woltmann

1. Einleitung

In einer zunehmend digitalisierten Welt wird die Cybersecurity zu einem unverzichtbaren Bestandteil der strategischen Ausrichtung jedes Unternehmens. Die wachsende Zahl von Bedrohungen, kombiniert mit verschärften regulatorischen Anforderungen, macht es für Unternehmen unerlässlich, ihre Resilienz gegenüber Cyberrisiken kontinuierlich zu stärken. Diese Unterlage soll Entscheidungsträgern einen umfassenden Überblick über aktuelle Entwicklungen und Herausforderungen im Bereich Cybersecurity und Regulatorik bieten. Ziel dieses Dokuments ist es, praxisnahe Einblicke in die wichtigsten Sicherheitsstrategien und Regulierungen zu geben, die Unternehmen heute betreffen. Wir beleuchten nicht nur die allgemeinen Herausforderungen, die mit der Sicherung digitaler Infrastrukturen einhergehen, sondern auch spezifische Anforderungen, die sich für Betreiber kritischer Infrastrukturen, wie etwa im Finanzsektor, ergeben. Durch die Analyse aktueller Regularien wie DORA und NIS2 wird aufgezeigt, was der Regulator ab sofort von den Unternehmen verlangt und wie diese nicht nur ihre Compliance sicherstellen sondern zugleich ihre Cyberresilienz strategisch verbessern können. Darüber hinaus bieten wir praxisnahe Empfehlungen, basierend auf den Erfahrungen aus zahlreichen Beratungsprojekten. Themen wie Risikomanagement, Information Asset Classification, IT Asset Management, Vulnerability Management, Secure Software Development Lifecycle, Individual Data Processing, User Access Management, Security Operations Center beziehungsweise Cyber Security Linienorganisation werden detailliert erörtert, um Unternehmen praktische Leitlinien zur Stärkung ihrer Cybersecurity zu bieten.

2. Cyber & Regulatorik – Quo vadis?

In Zeiten zunehmender digitaler Bedrohungen wird es immer schwieriger, den Überblick über die komplexe und sich ständig weiterentwickelnde Bedrohungslandschaft zu behalten. Parallel zur wachsenden Bedrohungslage sehen sich Organisationen mit einer enormen und weiter zunehmenden Regulierungsflut konfrontiert: IT-Sicherheit, aufsichtsrechtliche Anforderungen an Banken und die Eigenschaft als Betreiber kritischer Infrastrukturen verstärken sich gegenseitig. Die zunehmende Nutzung mobiler Endgeräte hat die Bedrohungslage weiter verschärft. Entweder im Rahmen eines Self-Assessments oder nach erfolgtem Audit stehen daher häufig umfangreiche Anpassungsbedarfe ins Haus.

2.1 Überblick behalten in Zeiten wachsender Bedrohungen

Um auf diese ständig wachsende Bedrohungslage zu reagieren investieren gerade Banken und Versicherungen derzeit hohe Summen in die Verbesserung ihrer Cybersicherheit und Cyberresilienz. Doch zum einen fehlt in vielen Instituten die Balance zwischen Bedrohungslage, notwendigen Maßnahmen und Investitionen. Zum anderen führt das Handeln unter Zeitdruck, etwa zur Adressierung von Revisionspunkten oder nach Cyberangriffen, zu punktuellem und teurem Aktionismus. In der Summe leidet darunter der Cyber Return on Investment. Dabei ist guter Rat hier oft nicht teuer. Eine klar strukturierte und gemanagte Sicherheitsprogrammatik hilft sparen, ohne die Sicherheit zu gefährden.

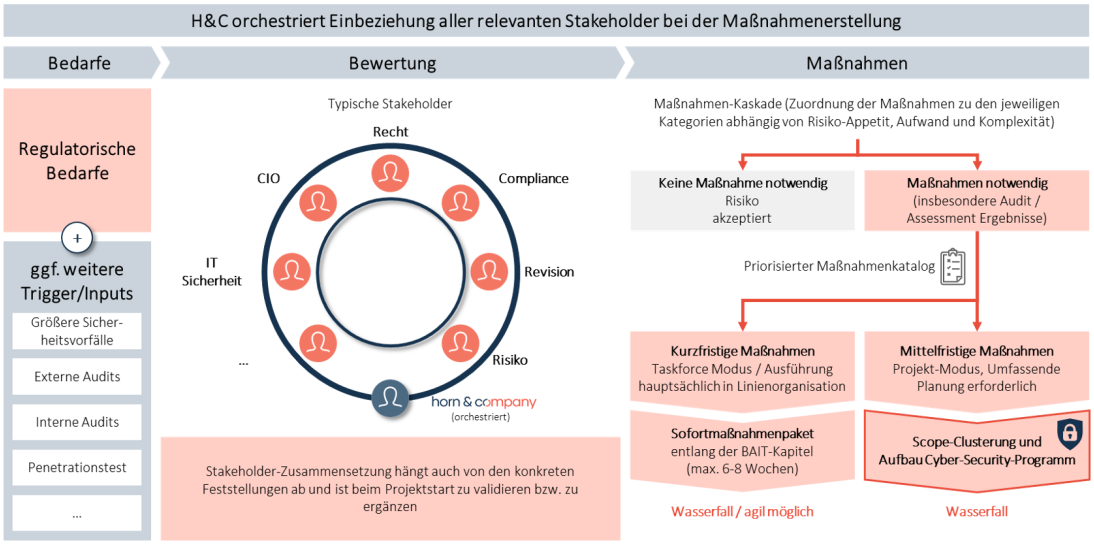

Abbildung 1.: Cyber-Maßnahmen-Framework

Zunächst ist es wichtig, den Sicherheitsbedarf für das Institut sauber und transparent zu ermitteln. Der Weg dorthin führt einerseits über Audits, sollte aber auch das intern bereits vorhandene Wissen berücksichtigen. Interne Audits, Ergebnisse von Penetrationstests oder auch ganz aktuelle Sicherheitsvorfälle tragen zu einem umfassenden Lagebild bei. Die Sammlung, Strukturierung und methodische Aufbereitung helfen dann, einen weiteren Schritt in Richtung Standortbestimmung zu gehen. Hinzu kommt – vielleicht noch wichtiger – die Aufgabe, sich über den eigenen Risikoappetit klar zu werden und die passende Balance zwischen Risiko und Kosten zu finden. In einer konsolidierten Bewertung durch Stakeholder aus IT, Revision und Management ist iterativ die Frage zu beantworten, welchen Maßnahmen man sich widmet – und mit welcher Intensität. Von besonderer Bedeutung ist auch die Entscheidung, worauf man verzichtet, weil man das damit verbundene Risiko in Kauf nimmt. War die BaFin bereits im Haus und traf Feststellungen, so verringert sich der Handlungsspielraum dramatisch: Sowohl der Scope, als auch die Timeline sind nun in der Regel fest vorgegeben. Es bleibt dann nur noch die Herausforderung, dass hierfür notwendige Budget im Rahmen zu halten. Bei der Umsetzung kommt all das zusammen, was den besonderen Reiz von regulatorisch getriebenen (Groß-)Programmen ausmacht: Die möglichst budgettreue aber unter allen Umständen termingerechte Umsetzung des festgelegten Leistungsumfangs.

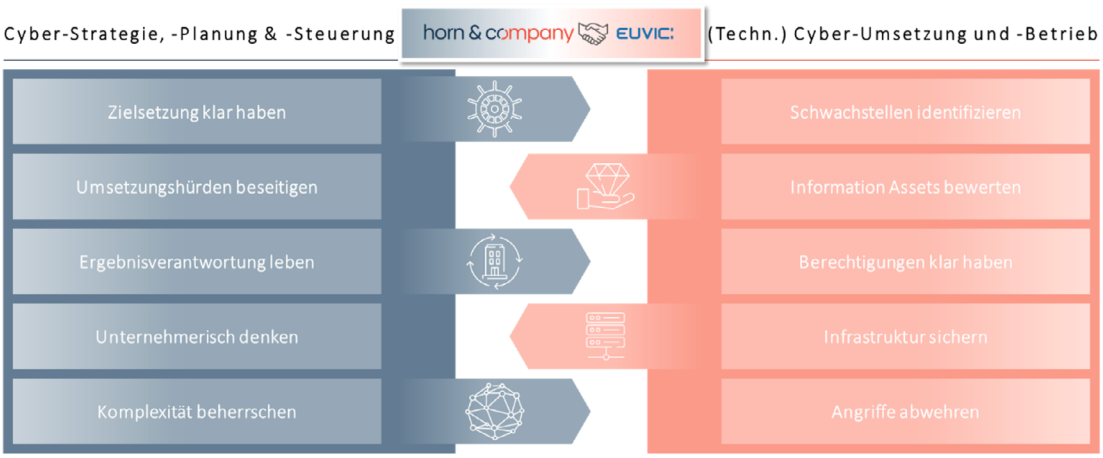

Abbildung 2.: Zusammenarbeits-Modell Horn & Company und EUVIC

Aber auch im fachlichen Bereich müssen verschiedene Faktoren berücksichtigt werden. Daher umfasst ein wirksames End-to-End-Sicherheitsprogramm ein ganzes Spektrum von Maßnahmen, darunter die:

/ Festlegung von Sicherheitsstrategie, -richtlinien und -verfahren
/ Definition erforderlicher Strukturen, Aufhängung und kapazitative Besetzung (Skills)
/ Definition von erforderlichen Sicherheitsprozessen
/ Implementierung von Technologien zur Sicherheitsverbesserung
/ Schulung des Personals in sicheren Arbeitspraktiken und -verfahren
/ Überwachung auf Anzeichen von Bedrohungen
/ Durchführung regelmäßiger Audits und Tests zur Überprüfung der Wirksamkeit

Ein ganzheitlicher Ansatz zur Cybersicherheit vereint fachliche und IT-technische Komponenten und bildet so das Rückgrat eines widerstandsfähigen Unternehmens. Durch diese enge Verzahnung aller Bereiche lässt sich eine effektive und nachhaltige Abwehr gegen Cyberbedrohungen sicherstellen. Diese ist vor allem für Betreiber kritischer Infrastruktur von besonderer Bedeutung, wie der nächste Abschnitt konkret erörtert.

2.2 KRITIS: Besonderheiten für Betreiber kritischer Infrastruktur am Beispiel des Finanzsektors

Weitreichende Ausfälle oder Sicherheitsverletzungen bei Finanzinstituten haben nicht nur fundamentale Auswirkungen auf Wirtschaft und Handel, sondern auch gravierende Folgen für das öffentliche Vertrauen und die gesellschaftliche Gesamtdynamik. Daher kommt Finanzdienstleistern mitunter als Betreiber dieser kritischen Infrastrukturen (KRITIS) auch eine besonders verantwortungsvolle Schlüsselrolle bei der Sicherung unserer finanziellen sowie sozialen Stabilität zu. Speziell hierfür wurde im Rahmen des BSI-Gesetzes die KRITIS-Verordnung eingeführt, um sicherzustellen, dass auch die kritischen Infrastrukturen des Finanzsektors angemessen geschützt sind und bleiben. Um diese Herausforderungen zu meistern und die sich bietenden Chancen zu nutzen, empfiehlt es sich ein umfassendes Maßnahmenpaket zu schnüren, das die folgenden zentralen Aspekte der KRITIS-Verordnung berücksichtigt.

Abbildung 3.: KRITIS-Besonderheiten

Da Finanzdienstleister hochsensible Daten verarbeiten, stellt die KRITIS-Verordnung die Führungskräfte der Branche vor besondere Herausforderungen, bietet aber zugleich auch Chancen. Die Hauptaufgabe besteht wieder darin, die Balance zwischen Sicherheit und Effizienz zu wahren: Robuste Sicherheitsmaßnahmen sind zweifelsohne notwendig, um die Sicherheit der Dienstleistungen und die Widerstandsfähigkeit des gesamten Finanzsystems zu gewährleisten, dürfen jedoch gleichzeitig den reibungslosen Betrieb nicht behindern. Daher ist bei der Umsetzung ein umfassendes Verständnis eigener kritischer Infrastrukturen, konsequente Sicherheitsmaßnahmen sowie eine kontinuierliche Anpassung an neue Bedrohungen erforderlich. Die wesentlichen Chancen liegen dabei aber auch in der Stärkung des Kundenvertrauens und des Marktimages: Unternehmen, die nachweislich Sicherheitsmaßnahmen implementieren und proaktiv auf Bedrohungen reagieren, gewinnen das Vertrauen von Neukunden, steigern die Zufriedenheit bei Bestandskunden und sichern so eine langfristige Bindung.

3. Zunehmender regulatorischer Druck

Wie zuvor bereits skizziert, nimmt der regulatorische Druck durch neue Verordnungen stetig zu. In diesem Abschnitt werden mit DORA und NIS2 zwei aktuelle Anforderungswerke beleuchtet. Diese Regulierungen zielen darauf ab, die Cyberresilienz und -sicherheit von Unternehmen, insbesondere im Finanzsektor, zu stärken und umfassende Vorgaben für den Umgang mit digitalen Risiken zu etablieren. Das vorliegende Kapitel verfolgt das Ziel, einerseits einen Überblick über die jüngsten Entwicklungen zu geben und andererseits die entsprechenden Vorgehensweisen aufzuzeigen.

3.1 DORA – Digitale Resilienz als wichtiger Wettbewerbsvorteil

20.000 betroffene Unternehmen in der EU stehen vor der Herausforderung bis Januar 2025 die regulatorischen Anforderungen des Digital Operations Resilience Act (DORA) umzusetzen. Der hohe Umsetzungsdruck ergibt sich vor allem daraus, dass in der heutigen Bedrohungslage oft nicht mehr die Frage ist ob, sondern wann Cyberangriffe auf die Systeme eines Unternehmens stattfinden. Insbesondere im Finanzdienstleistungssektor bewirkt der hohe Digitalisierungsgrad zusammen mit der kritischen wirtschaftlichen Bedeutung diesbezüglich einen akuten Handlungsbedarf, um die notwendige Widerstandsfähigkeit sicherzustellen. Mit DORA erfährt diese Risikosituation nun eine explizite Adressierung durch Regulierungsbehörden und ergänzt die bisher bestehenden aufsichtlichen Anforderungen an die IT (BAIT, VAIT, KAIT und ZAIT) der BaFin. Zumal viele Unternehmen noch mit Hochdruck an der Umsetzung dieser nationalen Vorgaben arbeiten, stellen die neuen europäischen Richtlinien auch prozessual eine besondere Herausforderung dar. Eine entschlossene und vorausschauend strukturierte Umsetzung kann jedoch auch als Chance zur Konsolidierung und Vereinheitlichung des bisherigen Regularien-Dickichts zum Beispiel von MaRisk/BAIT, MaGo/VAIT oder EBA-Guidelines werden. Ganz im eigenen Interesse der Unternehmen bedeuten die DORA-Maßgaben aber vor allem eine zukunftsorientierte Stärkung der Widerstandsfähigkeit von Finanzdienstleistern hinsichtlich kritischer Bedrohungen für deren Informations- und Kommunikationstechnologie (IKT).

3.1.1 RTS & ITS – Den Durchblick bewahren

Im Laufe des Jahres 2024 haben die ESMA, EBA und EIOPA in zwei Schritten (Januar und Juli) die finalen Entwürfe der Charge von Regulatory Technical Standards (RTS) & Implementional Technical Standards (ITS) für den Digital Operational Resilience Act (DORA) veröffentlicht. Diese RTS & ITS bilden die lang erwarteten Konkretisierungen der DORA Anforderungen, die aufgrund hohen Interpretationsspielraums eine verlässliche Schätzung des Umsetzungsaufwands bislang erschwerten. Hier ein kurzer Überblick, um die Tragweite der neuen Anforderungen gegenüber den bisherigen Regelwerken zu verdeutlichen:

- **RTS on ICT Risk Management framework (Art. 15) & RTS on simplified risk management framework (Art. 16.3):** Diese RTS detaillieren die Anforderungen aus Kapitel II, Abschnitt II an Richtlinien und Prozesse bzgl. Schutz, Prävention, Aufdeckung und Reaktion des IKT-Risikomanagements. Damit sind beide RTS für Unternehmen hilfreich, um die Anforderungen genau zu verstehen und nötigen Anpassungsbedarfe zu identifizieren. Dennoch können die Anpassungen durchaus kostspielig sein, da Frameworks und Prozesse angepasst und in die gesamte Organisation ausgerollt werden müssen.

- **RTS on criteria for the classification of ICT related incidents (Art. 18.3):** Dieser RTS beschreibt die Konzeption und Kriterien für die Klassifizierung von IKT-Vorfällen. Darüber hinaus skizziert er Schwellenwerte für die Bestimmung der Wesentlichkeit für schwere IKT-Vorfälle und erhebliche Cyber-Bedrohungen. Diese Kriterien orientieren sich dabei an den Vorgaben, die in der Network and Information Security Directive 2 (NIS2) und der Payment Services Directive 2 (PSD2) beschrieben werden. Dadurch ist der RTS äußerst hilfreich, um die Abweichungen zu bestehenden Frameworks und die damit verbundenen nötigen Anpassungen zu identifizieren. Für Unternehmen, die bereits zur Einhaltung dieser Vorschriften verpflichtet sind, bedeutet es wahrscheinlich keinen wesentlichen Aufwand. Für andere Unternehmen kann es aber Anpassungen an bestehenden Bewertungs- und Reportingprozessen sowie den beteiligten Systemen bedeuten und ist damit auch mit höheren Aufwänden verbunden.

- **ITS to establish the templates of register of information (Art. 28.9):** Dieser ITS geht genauer auf die Anforderungen an das Informationsregister für IKT-Drittdienstleister ein. Ziel ist es die Abhängigkeiten zu IKT-Drittdienstleistern dem Regulator gegenüber sichtbar zu machen. Das Informationsregister soll auf Level der einzelnen Entität, Sub-konsolidiertem und Konsolidiertem Level erstellt werden und alle Vertragsinformationen zu IKT-Drittdienstleistern enthalten. Die Menge der zu sammelnden Informationen ist dabei abhängig von der Kritikalität der Dienstleistung, überschreitet aber oft bestehende Informationsanforderungen. Darüber hinaus beschreibt der ITS genaue Anforderungen an Implementierung, zu erfassende Informationen und das zugrundeliegende Datenmodell. Für viele Unternehmen wird dieses Informationsregister signifikante Aufwände durch die Einführung eines neuen Tools oder weitreichende Änderungen an bestehenden Lösungen bedeuten. Im Übrigen ist dieser ITS aktuell noch umstritten. Zum Hintergrund: Im Januar 2024 reichten die Europäischen Aufsichtsbehörden (ESAs) der Kommission einen Entwurf für den vorliegenden technische Durchführungsstandards (ITS) ein. Die Kommission lehnte diesen Entwurf im September 2024. Konkret bemängelte sie die vorgeschriebene Nutzung des Legal Entity Identifier (LEI) für IKT-Drittanbieter in der EU. Stattdessen vertrat die Kommission die Ansicht, dass Unternehmen die Wahl zwischen dem LEI und der Europäischen Unternehmensidentifikationsnummer (EUID) haben sollten. Am 15. Oktober 2024 veröffentlichten die Europäischen Aufsichtsbehörden (ESAs) dann eine Stellungnahme zur Ablehnung durch die Europäische Kommission (Kommission). Die Kommission wird voraussichtlich in den kommenden Wochen die überarbeiteten technischen Durchführungsstandards (ITS) veröffentlichen.

- **RTS to specify the policy on ICT services performed by third-party (Art. 28.10):** Dieser RTS spezifiziert den Inhalt der Richtlinien bezüglich des Lebenszyklusmanagements von Verträgen und Vereinbarungen mit Dritten, wobei der Schwerpunkt auf IKT-Dienstleistungen liegt, die kritische oder wichtige Funktionen unterstützen. Obwohl interne Dienstleister für IKT-Services explizit als Drittdienstleister inkludiert sind, schränkt der RTS die Anforderungen an die Steuerung und die Exit-Strategien zum Positiven ein. Andererseits werden zukünftig auch interne Dienstleister umfangreicheres Management mit Service-Level und KPI-Reporting benötigen. Da der RTS klare Vorgaben für Richtlinien und Prozesse gibt, beschränkt sich der Interpretationsspielraum für die Implementierung. Dennoch werde die hohen Anforderungen an in- und externe Dienstleistungsverträge hohen Ergänzungs- und Anpassungsaufwand nach sich ziehen.

- **RTS to specify the reporting of major ICT-related incidents (Art. 20.a) & ITS to establish the reporting details for major ICT related incidents (Art. 20.b):** Diese RTS & ITS konkretisieren die Anforderungen an das Incident Reporting, indem sie sowohl die inhaltlichen Anforderungen als auch die Art und Weise des Reportings konkretisieren. Hier haben die ESA erfreulicherweise erkannt, dass im Falle eines Cyber-Angriffs das Reporting die Abwehr & Schadensbegrenzung nicht behindern darf – und mehrere Argumente aus den Konsultationen berücksichtigt. Das Beste zuerst: Die Anzahl der Datenfelder in den Berichtsvorlagen wurde von 84 auf 59 reduziert, also um fast 30%. Die Pflichtfelder wurden immerhin von 37 auf 28 reduziert (-1/4). Vorfälle müssen wie im Entwurf innerhalb von 4 Stunden nach Einstufung und 24 Stunden nach Entdeckung gemeldet werden, allerdings mit nur 10 statt 17 Datenfeldern. Die Fristen für Folgeberichte wurden leicht verlängert und sind besser messbar. Der Zwischenbericht ist nun 72 Stunden nach der Erstmeldung fällig und nicht mehr zum Zeitpunkt des Vorfalls. Ebenso ist der Abschlussbericht nun einen Monat nach dem Zwischenbericht fällig und nicht mehr nach dem Vorfall. Darüber hinaus werden die Anforderungen an die Berichterstattung über das Wochenende reduziert, so dass die Berichte in der Regel erst bis 12 Uhr des folgenden Arbeitstages übermittelt werden müssen. Um den Anforderungen kleiner Unternehmen gerecht zu werden, wird ein einheitliches Meldeformular für alle Meldungen sowie eine verhältnismäßige und ausgewogene Datenerhebung eingeführt. Daraus ergeben sich je nach Unternehmensgröße neue und durchaus aufwändige Anpassungen der bestehenden Prozesse. Im Hinblick auf weitere Regelungen wie NIS2 sind diese Anforderungen jedoch bereits abgestimmt.

- **Guidelines on the estimation of aggregated annual costs and losses caused by major ICT-related incidents (Art. 18/20):** In diesem Leitfaden wird konkretisiert, wie die Kosten von Störfällen zu ermitteln sind. Die endgültige Fassung bringt einige Erleichterungen, zum Beispiel die freie Wahl des Bezugsjahres für die Kosten und die Konzentration auf Bruttobeträge, anstatt zusätzlich Nettobeträge anzugeben.

- **RTS to specify threat led penetration testing (Art. 26.1):** Dieser RTS vertieft die Anforderungen an das Threa Led Penetration Testing (TLPT) und orientiert sich in der finalen Version sehr eng am TIBER-EU Framework. Damit schafft der RTS Klarheit über die notwendigen Schritte und Anforderungen, die Unternehmen zur Erreichung der DORA-Konformität einhalten müssen. Durch die Anlehnung an TIBER-EU wird sichergestellt, dass die Anforderungen praxisnah und flexibel bleiben.

/ **RTS to specify the elements to determine and assess when sub-contracting ICT services supporting a critical or important function (Art. 30.5):** Dieser RTS soll die Anforderungen an Unternehmen konkretisieren, welche kritischen IKT-Funktionen ausgelagert werden können und welche Sorgfaltspflichten dabei zu erfüllen sind. Während die anderen finalen Versionen zeitnah auf den Websites von EBA, EIOPA & ESMA veröffentlicht wurden, ist die finale Version dieses RTS kam leicht verspätet und wurde (Stand November 2024) noch nicht vom EU-Parlament ratifiziert Die Aufsichtsbehörden arbeiten an einer neuen Version. bar.

/ **Guidelines on cooperation ESAs –CAs (Competent Authorities) regarding DORA oversight (Art. 32.7):** Diese Guideline beschreibt die Zusammenarbeit zwischen den European Supervisory Authorities (ESA) und den Competent Authorities (CA). Direkte Anforderungen an Unternehmen sind in dieser Guideline nicht enthalten. Da die Konsultationen diesbezüglich ein weitgehend positives Feedback ergeben haben, werden in der finalen Version keine wesentlichen Änderungen vorgenommen.

/ **RTS on harmonisation of oversight conditions (Art. 41):** Dieser RTS-Entwurf wurde in 2 endgültige RTS-Dokumente aufgeteilt: Das erste mit fast gleichem Titel mit Bezug auf Artikel 41 (1) a, b & c, das zweite mit dem Titel „RTS specifying the criteria for determining the composition of the joint examination team (JET)" mit Bezug auf Artikel 41 (1) c. Beide RTS beschreiben, wie die Aufsichtsregeln für IKT-Dienstleister harmonisiert werden sollen. Direkte Anforderungen an die Unternehmen enthält dieser RTS nicht, so dass sich hier keine relevanten Änderungen ergeben.

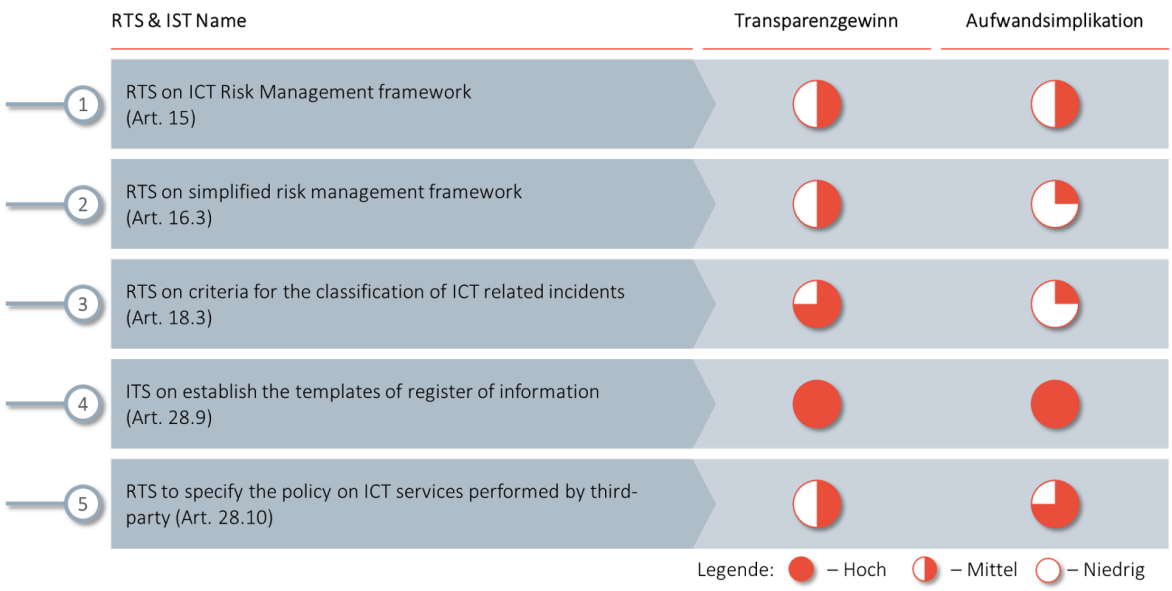

Abbildung 4.: DORA RTS & IST Name (1/2)

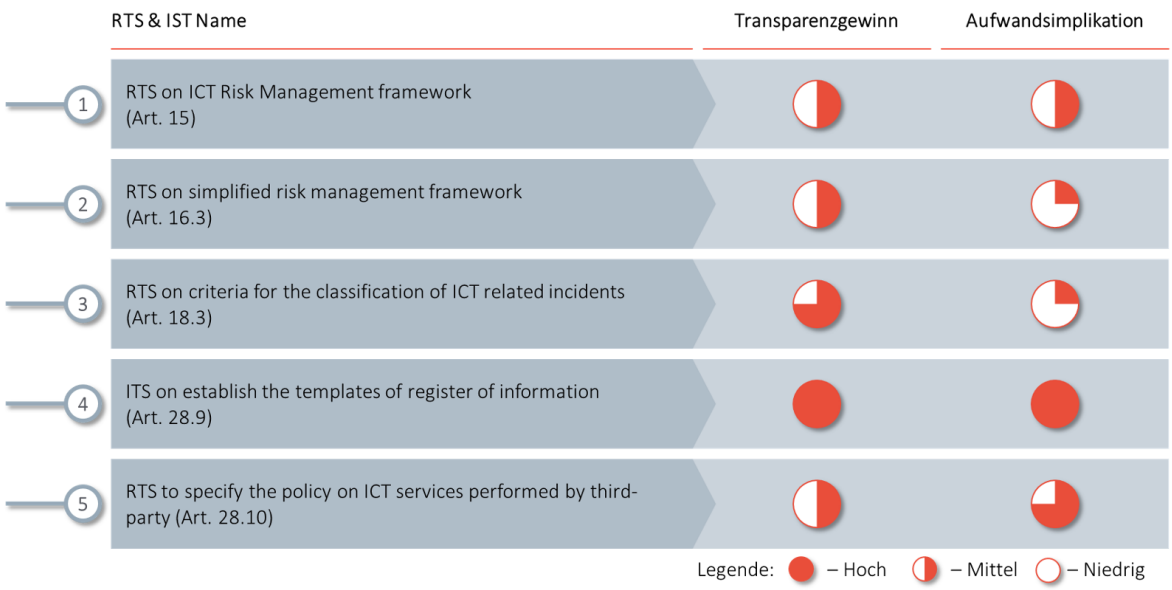

Abbildung 5.: DORA RTS & IST Name (2/2)

An manchen Stellen kann argumentiert werden, dass DORA „einfach" durch zusätzliche Prozesse oder Arbeitsanweisungen umgesetzt werden kann – speziell, wenn bereits xAIT umgesetzt wurden. So beschreibt DORA beispielsweise in Artikel 6 Absatz 2: „Der IKT-Risikomanagementrahmen umfasst mindestens Strategien, Leit- und Richtlinien, Verfahren sowie IKT-Protokolle und -Tools[…]". An anderer Stelle kann das in Artikel 11 Absatz 2c zu Reaktion bei IKT-bezogener Vorfälle geforderte „ unverzüglich" einen sehr hohen Automatisierungsgrad der IT-Sicherheit erfordern und wäre dann mit IT-Kosten in wohl empfindlicher Höhe verbunden. Die veröffentlichten RTS schließen diesen Interpretationsspielraum noch nicht vollständig, da sie zunächst nur die regulatorischen Anforderungen beschreiben, nicht aber die Art der Umsetzung. Aufgrund des Verhältnismäßigkeits-prinzips werden die Anforderungen für große Unternehmen wahrscheinlich mit signifikanten Aufwänden in der Umsetzung verbunden sein. Kleinere Unternehmen hingegen könnten mit einfachen Änderungen an Richtlinien und Prozessen DORA-Compliance erreichen. Etwas anders sieht es bei dem veröffentlichten ITS aus, da hier genaue Erwartungen an die Implementierung formuliert werden und damit weniger Interpretationsspielraum lassen (siehe aktuelle Diskussion zu ITS to establish the templates of register of information (Art. 28.9).). Unabhängig von den Konkretisierungen in RTS & ITS spielt die Auslegung des jeweiligen Regulators die ausschlaggebende Rolle, da dieser die finale Interpretation von DORA im Rahmen eines Audits anwendet. Letztere lässt sich zum jetzigen Zeitpunkt noch nicht abschätzen. Zusammenfassend zeigen RTS und ITS auf, dass abhängig von der Größe des Unternehmens und der Komplexität der Unternehmensstruktur gemäß des Verhältnismäßigkeitsprinzip umfassende Anpassungen an Prozessen, Guidelines und Systemen nötig sind. Es ist also dringend nötig die eigene Größe zu bestimmen und einen Standard zur Interpretation von DORA zu definieren.

Auch wenn die Anforderungen an die externe Meldung von Cyber-Angriffen erfreulicherweise etwas gelockert wurden, ist es unwahrscheinlich, dass ein bestehendes Incident Management System bereits alle diese Felder enthält. Der Hersteller des eingesetzten Systems sollte daher dringend um eine möglichst verbindliche Aussage gebeten werden, ob die von DORA geforderten 59 Felder rechtzeitig mit einem Software-Update ausgeliefert werden. Unabhängig davon, ob ein Update oder eine Eigenentwicklung erfolgt, sollte zeitnah ein Projekt aufgesetzt werden, um das eigene Störfallmanagementsystem zeitnah anzupassen. Auch aufgrund der Ambitionen der ESA, ein europaweites Informations-

und Frühwarnsystem für Cyber-Angriffe zu etablieren, dürften die Erwartungen eines Auditors an die vollständige Verfügbarkeit solcher Daten sehr hoch sein – und entsprechende Feststellungen eher schwerwiegend. Trotz eines gewissen Hypes um Threat Led Penetration Testing (TLPT) ist der Handlungsdruck hier nicht so groß. Schließlich müssen die lokalen Regulatoren zunächst die Dienstleister für die Angreiferteams (Red Teams) auswählen, geeignete Threat-Intelligence-basierte Tests erstellen und nicht zuletzt alle teilnehmenden Finanzinstitute informieren. Daher wird es wahrscheinlich ausreichen, sich voll und ganz auf die Verbesserung der eigenen digitalen Widerstandsfähigkeit zu konzentrieren und spezifische Vorbereitungen für TLPT aufzuschieben, bis man darüber informiert wird, dass man dafür ausgewählt wurde.

3.1.2 Vorgehen – Fünf Erfolgsfaktoren für eine erfolgreiche DORA-Umsetzung

Zwischen Theorie und Praxis klafft nicht selten eine große Lücke – und so sind viele Unternehmen bei der Umsetzung von DORA (Digital Operational Resilience Act) ins Stocken geraten. Stand heute (Ende 2024) ist es in vielen Fällen unrealistisch, dass die vollständige Umsetzung bis zum geplanten Inkrafttreten am 17. Januar 2025 abgeschlossen sein wird. Viele Organisationen werden die Umsetzung voraussichtlich noch bis ins Jahr 2025 und darüber hinaus fortführen. Auch wenn damit das formale Inkrafttreten überschritten wird, hoffen viele Unternehmen, im Falle einer Prüfung durch die BaFin auf mildernde Umstände, sofern sie die Umsetzungsmaßnahmen bereits weitgehend angestoßen haben. Wir hatten das große Privileg, in den letzten Monaten umfangreiche Praxiserfahrungen in der DORA-Umsetzung zu sammeln. Dabei haben sich immer wieder ähnliche Muster und Herausforderungen abgezeichnet. Aus dieser Praxis haben wir die fünf wichtigsten Erfolgsfaktoren für eine effektive und nachhaltige DORA-Umsetzung zusammengetragen, die Unternehmen dabei unterstützen, ihre Cyberresilienz zu stärken und die Anforderungen rechtzeitig und effizient zu erfüllen:

1. **Ein gutes Team aus den richtigen externen & internen Experten**
2. **Ein pragmatisches Modell zur Bestimmung von Ist- & Soll-Zustand**
3. **Ein klarer Konsens zum Risikoappetit – von der Strategie bis zu den IT-Lösungen**
4. **Ein scharfer Fokus auf das Wesentliche: Mitigation der größten Risiken**
5. **Eine möglichst agile und parallele Umsetzung der DORA Anforderungen**

„Ein gutes Team" klingt nach einem geradezu trivialen Erfolgsfaktor, ist jedoch bekanntlich nicht so einfach umzusetzen. So verlockend das „One-Stop-Shop"-Angebot mancher Wirtschaftsprüfer auch klingt, dieses Modell ist bei weitem nicht so effizient wie ein guter Mix aus internen Experten und erfahrenen Beratern. Natürlich sollte das ganze „Team DORA" die Anforderungen gesichtet und verstanden haben. Aufgrund der hohen Komplexität von DORA sind zur Umsetzung nicht nur hervorragende Programm- & Projektleiter samt PMO nötig, sondern auch Experten aus Risiko-Management, Recht, Audit, Compliance und vor allem auch diversen IT-Bereichen nötig. Da gerade diese Ressourcen meist ohnehin schon völlig überlastet sind, benötigen die meisten Unternehmen externe Unterstützung.

„Ein pragmatisches Modell zur Bestimmung von Ist- & Soll-Zustand" sollte die vielfältigen Anforderungen von DORA in möglichst wenigen Fähigkeiten prägnant beschreiben – ideal in weniger als 50 und nicht mehr als 150 DORA-Fähigkeiten. Um in jeder Fähigkeit den Ist-Zustand leicht bewerten und den Soll-Zustand im Konsens wählen zu können, sollte jede Fähigkeit in Reifegraden entlang der zentralen DORA-Anforderungen beschrieben werden. Beispielweise würde man die Fähigkeit der Identifikation & Isolation von Cyberangriffen in Reifegrade zerlegen, die nach Möglichkeit, Präzision, Geschwindigkeit

und Automation der Identifikation sowie der Isolation gliedern. Die besten DORA-Reifegradmodelle beschreiben in den einfachsten Stufen Szenarien, die bei einem offiziellen Audit wahrscheinlich zu hoch-kritischen Feststellungen (F3/F4) führen würden – und differenzieren zwischen riskanterer Minimalumsetzung über den Mittelweg zur Maximallösung. So fällt es leicht, das Ist zu bewerten und das Ziel anzusteuern.

„Ein frühzeitiger, klarer Konsens zum Risikoappetit" vermeidet wiederholte Grabenkämpfe bei jeder Ziel-Fähigkeit und spart so viel Zeit, Nerven und Geld. Eine frühzeitige Festlegung des Risikoappetits mit allen Entscheidern ermöglicht dabei im späteren Projektverlauf schneller zu einer Entscheidung für jede einzelne Fähigkeit zu kommen.

„Fokus auf das Wesentliche" klingt nach trivialen Allgemeinverständnis. Doch der Schein trügt, da die Meinungen zum wirklich Wesentlichen meist weit auseinander gehen – unter anderem getrieben durch die oben beschriebene Spannbreite zum Risikoappetit. Dementsprechend gilt es die wesentlichen Kernziele festzulegen. Zur Top-Priorität, hoch-kritische Feststellungen (F3/F4) zu vermeiden, ist man sich meist schnell einig. Aufgrund des kurzen Umsetzungszeitraums für DORA sollten die aufwändigsten Anforderungen mit deutlicher Steigerung des Reifegrads die nächst-höchste Priorität erhalten. Teilweise kann es auch sinnvoll sein, eine Interimslösung mit geringerer Reife einer komplexeren Lösung vorzuziehen. Bei knappen Ressourcen und knapper Zeit sollte man das Erreichen höchster Reifegrade möglicherweise zurückstellen, bis man sicher ist, dass die Top-Prioritäten bis zur DORA Deadline im Januar 2025 sicher erreicht sind. Dies bedeutet konkret, dass die Minimierung des Risikos schwerwiegender Findings oberste Priorität hat. Das Excel-basierte Tool von Horn & Company bietet hierfür eine praxisnahe und effektive Lösung.

„Eine möglichst agile und parallele Umsetzung" ist normalerweise kontraintuitiv für regulatorische Anforderungen und Projekte. Für DORA bleibt nur sehr wenig Zeit für die Umsetzung – nicht zuletzt aufgrund der späten Sicherheit zu den Detailanforderungen (RTS & ITS), speziell für Anpassungen in der IT. Damit müssen die Pläne für die komplexeren Anforderungen hoch-ambitioniert sein, um rechtzeitig bis zum 17. Januar 2025 fertig zu werden – oder zumindest glaubhaft machen zu können gut unterwegs zu sein. Somit führt kein Weg an paralleler Umsetzung der Top-Prioritäten vorbei. Eine agile Umsetzung bringt zusätzlich den Vorteil, dass das Backlog (Arbeitsvorrat) die Chance zu einer noch detaillierteren Priorisierung bietet, sodass die wichtigsten Fähigkeiten zur Erfüllung von DORA als erstes fertig werden können – und der Auditor die noch anstehenden Arbeitspakete schon besichtigen kann, ohne dass volle Marktreife erreicht ist. Darüber hinaus bewegt sich die agile Entwicklung von einer Interimslösung zur nächst-besseren. Damit stellt die bereits oben empfohlene Nutzung von Interimslösung keinen Umweg dar, wie bei der Wasserfallentwicklung, sondern ein inkrementelles Verbessern der DORA-Lösungen.

3.2 NIS2 – der richtige Umgang mit der neuen Richtlinie

Neben DORA gewinnt auch die NIS2-Richtlinie (Network and Information Security Directive) zunehmend an Bedeutung. Obwohl sich die Umsetzung der Richtlinie in Österreich und Deutschland derzeit noch in der Entwurfsphase befindet, stehen ab dem kommenden Jahr tausende Unternehmen vor der Herausforderung, strenge Vorgaben einzuhalten – andernfalls drohen empfindliche Strafen. Bis zu 10 Millionen Euro oder 2 % des Jahresumsatzes bei wesentlichen Einrichtungen und bis zu 7 Millionen Euro oder 1,4 % des Jahresumsatzes bei wichtigen Einrichtungen. Die Leitungsorgane müssen die Risikomanagementmaßnahmen sicherstellen und haften für Schäden. Die NIS2-Richtlinie verpflichtet Unternehmen zur Umsetzung verstärkter Cybersicherheitsstandards. Um eine umfassende Informationssicherheit zu gewährleisten, müssen sie Maßnahmen in zentralen Bereichen wie Risikomanagement und Notfallplanung implementieren. Zunächst muss geprüft werden, ob eine Organisation von den Regelungen betroffen ist. Im ersten Schritt erfolgt dies durch eine Betrachtung des Sektors: Relevante Branchen sind Bank- und Versicherungswesen, Finanzmarktinfrastrukturen, Energie, Verkehr, digitale Infrastruktur, die Verwaltung von IKT-Diensten im B2B-Bereich sowie das verarbeitende Gewerbe. Darüber hinaus ist die Größe des Unternehmens entscheidend. Eine Organisation gilt als groß, wenn sie mindestens 250 Mitarbeiter beschäftigt oder einen Jahresumsatz von über 50 Millionen Euro und eine Bilanzsumme von mehr als 43 Millionen Euro aufweist. Mittlere Unternehmen sind definiert durch mindestens 50 Mitarbeiter oder einen Jahresumsatz bzw. eine Bilanzsumme von jeweils mehr als zehn Millionen Euro, sofern sie nicht bereits als großes Unternehmen eingestuft sind.

Doch es gibt auch erfreuliche Nachrichten, denn mit der NIS2-Umsetzung werden natürlich wieder nicht nur normative Anforderungen erfüllt, sondern auch die IT-Sicherheit im Unternehmen gestärkt. Eine saubere Umsetzung der Richtlinie bringt daher eine Reihe von Vorteilen mit sich:

- **Haftungsrisiken minimieren:** Leitungsorgane (Vorstand, Geschäftsführung) können durch Vorbereitungen auf das Eintreten eines Schadensfalls persönliche Haftungen vermeiden

- **Wettbewerbsvorteile sichern:** In einer Ära zunehmender Cyberbedrohungen und Spionage leistet die Informationssicherheit einen entscheidenden Beitrag zur Abwehr dieser Gefahren

- **Reputationsverlust vermeiden:** Insbesondere wesentliche Einrichtungen stehen im Fokus des öffentlichen Interesses, wodurch der Schutz von Informationen von zentraler Bedeutung ist

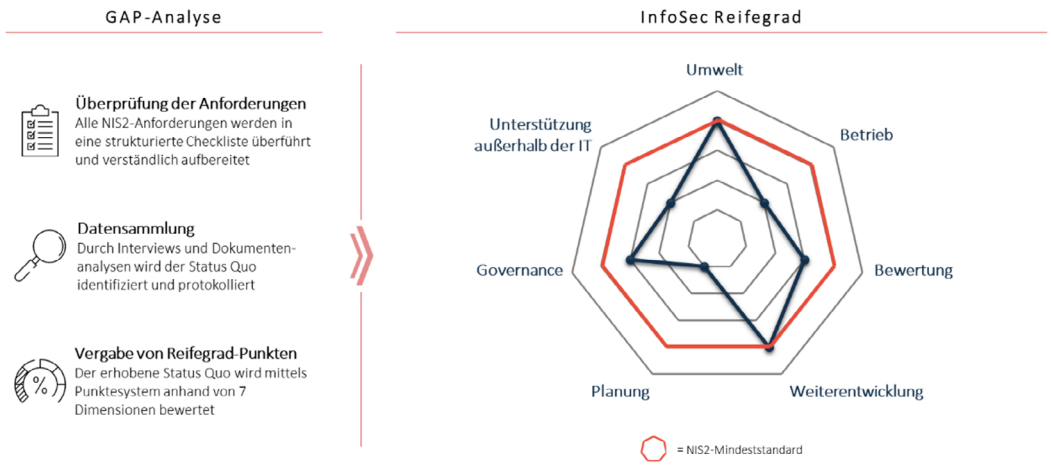

Abbildung 6.: NIS2-Framework

Unsere Erfahrung zeigt, wie wichtig es ist, dass Investitionen in IT-Sicherheit nicht nur technisch optimiert, sondern auch wirtschaftlich sinnvoll sind. Denn technische Verbesserungen bedeuten nicht automatisch betriebswirtschaftliche Effizienz. Daher ist eine vernünftige kaufmännische Betrachtung bereits in der Zielsetzungsphase unerlässlich. In der Zusammenarbeit mit unseren Kunden hat sich dabei ein pragmatischer Ansatz entwickelt:

1. **Gemeinsame Prüfung der NIS2-Betroffenheit Ihres Unternehmens:** Gemeinsam prüfen wir Ihre Betroffenheit und nehmen gemeinsam mit Ihnen die Beurteilung vor
2. **Identifikation von Lücken (GAP-Analyse):** Im Rahmen von Workshops und Interviews evaluieren wir den Reifegrad Ihres Unternehmens in allen NIS-Dimensionen (Umwelt, Betrieb, Bewertung, Weiterentwicklung, Planung, Governance und Unterstützung außerhalb der IT)
3. **Ableitung, Planung und Umsetzung von Maßnahmen für die NIS2-Readiness:** Basierend auf Ihrer Prozesslandschaft entwickeln wir gemeinsam einen Plan, um die Anforderungen rechtzeitig zu erfüllen

Die Umsetzung der NIS2-Richtlinie mag aufwendig und ressourcenintensiv erscheinen, doch die Nichterfüllung birgt ungleich größere Risiken – sei es durch empfindliche Strafen, Reputationsverlust oder steigende Haftungsrisiken. Mit einer sorgfältigen, wirtschaftlich durchdachten Herangehensweise kann die Umsetzung jedoch weit mehr sein als eine reine Pflichterfüllung. Sie minimiert nicht nur rechtliche Risiken, sondern eröffnet auch die Möglichkeit, nachhaltige Wettbewerbsvorteile zu erzielen und die Resilienz des Unternehmens langfristig zu stärken.

4. Cybersecurity in der Praxis

Im Laufe dieser Unterlage wurde ein Überblick über aktuelle regulatorische Entwicklungen gegeben. Doch auch abseits des regulatorischen Drucks sind zahlreiche weitere Themen für eine moderne IT von Bedeutung.

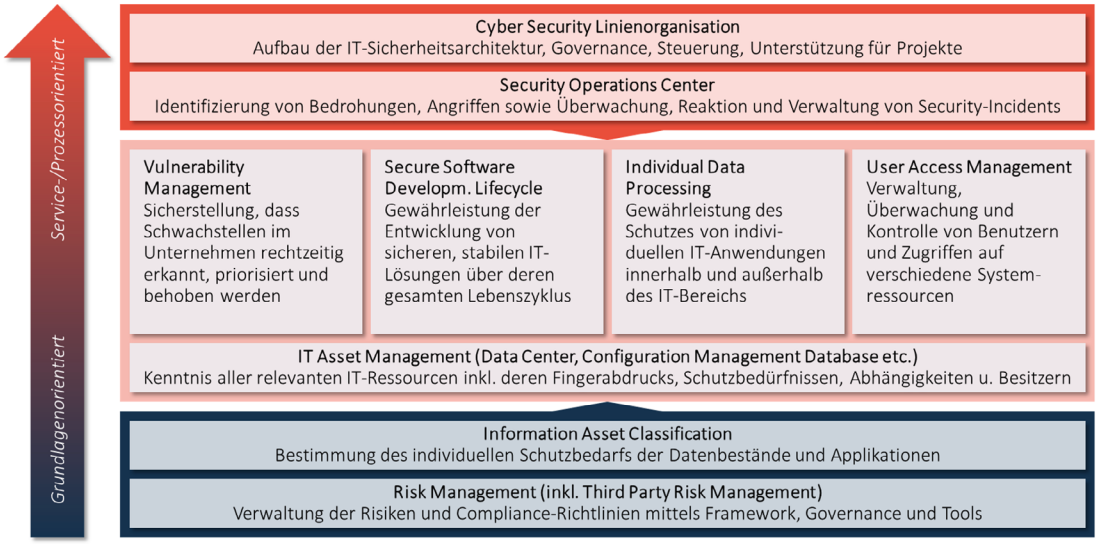

Abbildung 7.: GRC-Framework

In diesem Kapitel werden zentrale Themen wie Risikomanagement, Information Asset Classification, IT Asset Management, Vulnerability Management, Secure Software Development Lifecycle, Individual Data Processing, User Access Management, Security Operations Center beziehungsweise Cyber Security Linienorganisation näher erörtert. Leitgebende Struktur hierfür ist der oben dargestellte GRC-Framework.

4.1 Risikomanagement – Verwaltung von Risiken und Compliance-Richtlinien am Beispiel Third Party Risk Management

Um die hochgradig komplexen Herausforderungen meistern zu können, haben mittlerweile viele Unternehmen große Summen investiert und eigene IT-Sicherheits-Programme etabliert. Einen essentiellen Grundbaustein eines solchen Programms bildet ein effektives IT-Risikomanagement sowie die Definition und Einhaltung klarer Unternehmensrichtlinien durch entsprechende Governance, Risk und Compliance (GRC) Tools und Frameworks. Risikomanagement im Bereich Cybersicherheit bedeutet, dass Unternehmen eine potentielle Bedrohung und die möglichen Auswirkungen auf ihr Geschäftsmodell identifizieren und bewerten müssen, um schlussendlich im Stande zu sein, diese kosteneffizient priorisieren zu können. Dazu ist es unerlässlich entsprechende Frameworks und Richtlinien zu entwickeln, um gezielte Schutzmaßnahmen zu implementieren und sich somit effektiv gegen Angriffe schützen können. Moderne Tools, zum Beispiel die RSA Archer-Plattform zur integrierten Risikomanagementlösung, haben in den letzten Jahren immer mehr an Bedeutung gewonnen und sich als eine Art Gold-Standard etabliert. Diese Tools bieten die gewünschten Funktionen, wie Risikobewertung, Compliance-Überwachung und Incident-Management, um Unternehmen dabei zu unterstützen eine effektive Verteidigungsstrategie gegen Cyberattacken zu entwickeln.

Dabei ist eine essentielle Säule des Risikomanagements das Third Party Risk Management (TPRM). Während die Länge und Komplexität von Ausgliederungsketten kontinuierlich zunimmt, wird häufig unterschätzt, dass zwar Prozesse ausgelagert werden, wesentliche Risiken aber im Haus verbleiben. Datendiebstahl, Sicherheitsverletzungen, Leistungsausfall oder Imageschäden sind dabei keineswegs bloß theoretische Schreckensszenarien, sondern die realistische Bedrohungslage, die sich aus der Abhängigkeit von externen Partnern ergibt. Diese müssen dabei natürlich nicht immer direkt oder böswillig durch den Dienstleister oder dessen Subdienstleiter verursacht werden. Mindestens ebenso wichtig ist, dass man sich mit der Ausgliederung auch die Angriffsvektoren und Sicherheitsdefizite seiner Dienstleister kostenlos mit ins Haus holt. Einen permanenten Balanceakt erfordert dabei das Erreichen des angestrebten Effizienzgewinns im Verhältnis zu den damit verbundenen Risiken bzw. zur Compliance mit den hierauf abzielenden immer strenger werdenden regulatorischen Vorgaben wie zum Beispiel MaGo, VAIT/BAIT, DORA, oder LkSG.

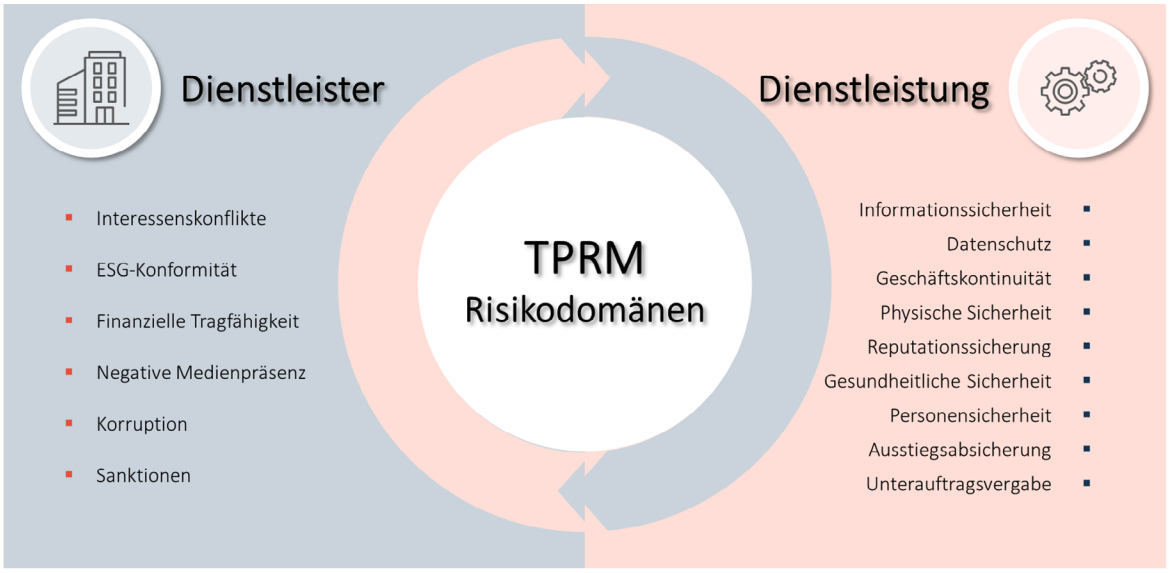

Abbildung 8.: Risikodomänen Third Party Risk Management

Zu den komplexen Risikodomänen kommt das ständige Wechselspiel von Technologien und Vorschriften, welches die Risikolandschaft kontinuierlich beeinflusst. In diesem Umfeld müssen Finanzdienstleistungsunternehmen einen klaren sowie lückenlosen Prozess etablieren und sich der Risiken zielgerichtet and proaktiv annehmen. Die folgenden Elemente haben sich dabei als Grundgerüst eines erfolgreichen TPRM bewährt:

1. **Planung, Screening und Bewertung:** Mögliche Drittparteien gemäß der relevanten Risikodomänen durchleuchten und die inhärenten Risiken der Leistungserbringung offenlegen sowie bewerten
2. **Auswahl, Vertragsabschluss und Onboarding:** Abhilfe- sowie Kontrollmaßnahmen analysieren bzw. **ausarbeiten und dementsprechend spezifische Bedingungen verhandeln und vertraglich fixieren**
3. **Verwaltung, Dokumentation und Überwachung:** Risiken in Verbindung mit Dritten zentral inventarisieren und kontinuierlich überwachen sowie durch regelmäßige Reports in einem transparenten Gesamtbild steuern
4. **Vorfallmanagement, Beendigung und Offboarding:** Vorfälle schnell registrieren, effizient reagieren und im Ernstfall die Zusammenarbeit auf Basis von Exit-Plänen ohne große Störung der Geschäftsprozesse beenden bzw. ersetzen

Third Party Risk Management ist somit ein unverzichtbares Element in einem Geschäftsumfeld, in dem externe Kooperationen zum Alltag gehören. Nur mit einer proaktiven Haltung, gezielter Bewertung und einem klaren Fokus auf das Risikomanagement können diese Herausforderungen gemeistert und eine sichere geschäftliche Zukunft gestaltet werden.

4.2 Information Asset Classification (IAC) – drei Schritte zum besseren Schutz der Information Assets Ihres Unternehmens

Das Thema Information Asset Classification (IAC) ist ein weiterer Baustein des GRC-Frameworks. IC schafft eine Grundlage, um den Schutzbedarf von Daten und Ressourcen systematisch zu bewerten und priorisieren. Dieser Abschnitt widmet sich der Frage, wie durch eine klare Klassifizierung von Assets ein gezielter Schutz sensibler Informationen gewährleistet werden kann. Um sich dieser Frage zu näher ist ein Verständnis für den IAC-Prozess nötig:

1. **Identifizierung:** Der erste Schritt besteht darin, ein klares Bild aller existierenden Information Assets zu gewinnen. Dazu zählen nicht nur Daten im herkömmlichen Sinne, sondern auch Applikationen, Systeme und weitere Bestandteile der IT-Infrastruktur.
2. **Klassifizierung:** Nach der Identifizierung der Assets erfolgt deren Klassifizierung. Hierbei wird in der Regel in verschiedene Schutzbedarfs-Dimensionen unterschieden. Typische Dimensionen, in denen jeweils die Schutzbedarfe bewertet werden, sind Vertraulichkeit, Integrität und Verfügbarkeit. Die Bewertung richtet sich dabei nach dem jeweiligen Schadenspotenzial bei Verletzungen (Reputation, Finanzieller Schaden, Geschäftsbetrieb, …).
3. **Priorisierung:** Auf Basis der Klassifizierung kann schließlich eine Priorisierung der Assets erfolgen. Hierbei werden die Schutzmaßnahmen dort konzentriert, wo sie aufgrund des Risikos und der Wichtigkeit des Assets am dringendsten benötigt werden.

Gerade im Finanzdienstleistungssektor spielt die IAC eine besonders wichtige Rolle. Dieser Sektor verarbeitet täglich eine enorme Menge an sensiblen Daten und trägt außerdem durch seine Systemrelevanz eine große Verantwortung. Durch eine gezielte IAC werden Daten, Applikationen und Systeme effektiv geschützt und gleichzeitig regulatorische Anforderungen erfüllt.

Ein effektives IAC-Projekt bildet dabei das Fundament für weitere Sicherheitsmaßnahmen und -Projekte im Cybersecurity Kontext. Besonders stark auf der IAC aufbauend sind dabei die folgenden Themen:

- **IT Asset Management (ITAM, siehe Kapitel 4.3):** Das IT Asset Management (ITAM) ist ggf. in Kombination mit einer Configuration Management Database eng mit der IAC verknüpft. Häufig kommen hierbei auch Discovery-Techniken zum Einsatz. ITAM und CMDB verwalten die Information Assets und bilden die Grundlage für die auf der Schutzbedarfs-Klassifizierung beruhenden Behandlungsvarianten im Umgang mit den Information Assets.

- **Identity and Access Management (IAM, siehe Kapitel 4.9):** Auf der Basis einer gründlichen IAC kann festgelegt werden, wer nach welchen Regeln Zugang zu welchen Assets hat und wie dieser Zugang gesteuert wird. Die operative Umsetzung der Anbindung von Applikationen an die berechtigungssteuernden Systeme kann entsprechend der IAC priorisiert werden.

- **Privileged Access Management (PAM, siehe Kapitel 4.9):** Eine präzise IAC ermöglicht es, die Assets zu identifizieren, die spezielle Zugriffsprivilegien erfordern, die Umsetzung von PAM zu priorisieren und entsprechende Sicherheitsmaßnahmen zu implementieren.

Die IAC ist ein unerlässlicher Baustein eines umfassenden Cybersecurity-Programms, insbesondere im Financial Services Sektor. Eine maßgeschneiderte IAC-Strategie trägt dazu bei, den Schutz wertvoller Information Assets zu gewährleisten, Cybersecurity-Risiken aktiv zu steuern und regulatorisches Exposure zu minimieren.

4.3 IT Asset Management – Digitale Vermögenswerte effizient schützen

Die wachsende Abhängigkeit von komplexen IT-Strukturen und digitalen Vermögenswerten stellt Finanzdienstleistungsunternehmen vor neue Herausforderungen. In diesem Kontext wird IT-Asset Management (ITAM) zu einer entscheidenden Funktion, die nicht nur eine präzise Bestandsaufnahme ermöglicht, sondern auch strategische Ansätze für den Schutz und die Optimierung dieser Ressourcen bietet. Das IT-Asset Management (ITAM) übernimmt dabei eine Schlüsselrolle, die weit über die bloße Inventarisierung hinausgeht. Vielmehr ist die Grundidee des ITAM die strategische Herangehensweise, die darauf abzielt, den gesamten Lebenszyklus der IT-Ressourcen zu verwalten und ihren Wert für das Unternehmen kontinuierlich zu maximieren und bedarfsgerecht zu schützen. Zu diesem Zweck ist es unabdingbar, eine transparente Sicht auf das vorhandene IT-Inventar zu haben, um fundierte Entscheidungen bezüglich Erneuerungen, Upgrades oder Ausmusterungen treffen zu können. Eine proaktive Verwaltung hilft nicht nur, Ausfallzeiten zu minimieren, sondern fördert auch eine agile Anpassung an neue Technologien und Marktanforderungen und stärkt somit die Resilienz und Zukunftsfähigkeit der

Unternehmens-IT.
Das ITAM-Konzept umfasst die Identifizierung, Bewertung, Verfolgung und Optimierung von IT-Assets. Eine wichtige Grundlage für ein effektives IT-Asset Management ist dabei die Information Asset Classification (mehr dazu in Kapitel 4.2). Hierbei werden die IT-Assets anhand verschiedener Kriterien wie zum Beispiel Vertraulichkeit und Verfügbarkeit untersucht und in verschiedene Schutzklassen eingeteilt. Eine darauf aufbauende Asset-Priorisierung ermöglicht die zielgerichtete Umsetzung der nötigen Schutzmaßnahmen, um insbesondere das Gesamtrisiko der vorhandenen IT-Assets dem Risikoappetit im Unternehmen anzupassen sowie die vielfältigen regulatorischen Anforderungen zu erfüllen. Es wird ein umfassendes Risikomanagement betrieben, das neben der Identifikation und Analyse von Risiken auch die Entwicklung von Strategien zur Risikominderung oder -vermeidung umfasst. Dieser Prozess beinhaltet auch regelmäßige Reviews und Updates der Risikobewertungen, um sicherzustellen, dass die getroffenen Maßnahmen effektiv sind und bleiben.

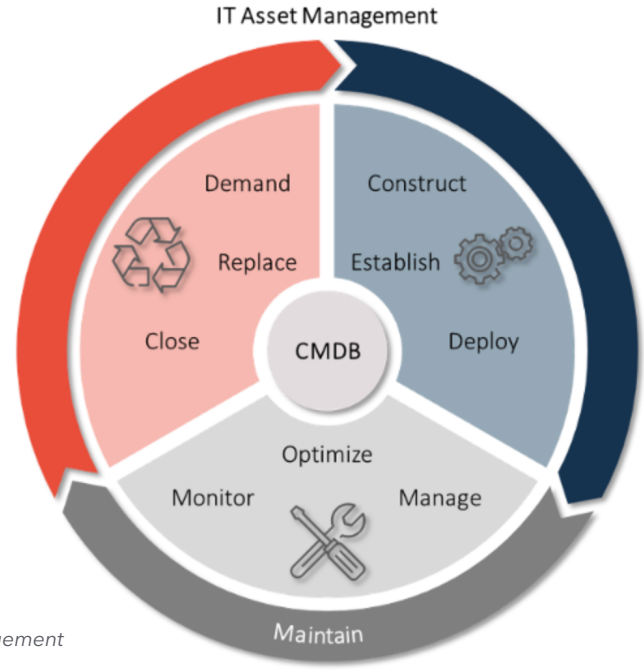

Abbildung 9.: IT Asset Management

Die Implementierung von Best Practices und Standards, wie ISO/IEC 19770, spielt eine entscheidende Rolle im ITAM, indem sie einen Rahmen für die Verwaltung der IT-Assets bietet, der international anerkannt und bewährt ist. Dieser mehrstufige Ansatz ermöglicht so eine präzise Kontrolle über den Zustand des IT-Inventars, sowie die Optimierung von Risiken bzw. Kosten unter der Prämisse einer effizienten Ressourcennutzung. Die regelmäßige Schulung des Personals in Bezug auf ITAM-Prozesse und -Werkzeuge ist ein weiterer kritischer Faktor, der dazu beiträgt, das Bewusstsein und die Kompetenz im Umgang mit IT-Assets zu steigern und somit die Sicherheit und Effizienz der IT-Infrastruktur zu verbessern.

Die zentrale Komponente eines modernen ITAM-Konzepts ist die sog. Configuration Management Database (CMDB). Die CMDB dient als zentrale Datenbank, die detaillierte Informationen über die Konfiguration von IT-Assets und deren gegenseitige Abhängigkeiten enthält. Dabei geht es neben der bloßen statischen Inventarisierung der Assets vorrangig um eine dynamische Verfolgung von Konfigurationsänderungen, den sog. Configuration Items. Dies fördert eine adaptive IT-Umgebung, die schnell auf Veränderungen reagieren kann, sei es durch interne Entwicklungsprojekte oder externe Bedrohungen. Dieser Ansatz ermöglicht, es die Gesamtheit der IT-Assets kontinuierlich zu analysieren und ihre Auswirkungen auf das gesamte System stets im Blick zu behalten.

Die Integration fortschrittlicher Analytik- und Reporting-Tools in das ITAM ermöglicht es Unternehmen, datengestützte Entscheidungen zu treffen und Optimierungspotenziale zu identifizieren. Die CMDB erlaubt somit neben der Echtzeit-Überwachung der Konfigurationen auch eine ganzheitliche Sichtweise auf das IT-Inventar. Die Integration von ITAM und CMDB bietet Unternehmen im Finanzdienstleistungssektor die Möglichkeit Kosten zu optimieren und Compliance-Anforderungen zu erfüllen. Darüber hinaus können Risiken gezielt gesteuert werden, wodurch ITAM ein zentraler Bestandteil einer effektiven Cybersecurity-Strategie wird. Diese Vernetzung zwischen ITAM und Cybersecurity unterstreicht die Bedeutung einer ganzheitlichen Sicherheitsstrategie, die sowohl physische als auch digitale Assets umfasst.

4.4 Cyber Security Linienorganisation – Vom IT-Sichtfahrbetrieb zum sicheren IT-Linienbetrieb

In vielen Unternehmen konzentriert sich die Umsetzung von IT-Sicherheit häufig auf kurzfristige Maßnahmen wie die Erfüllung neuer regulatorischer Anforderungen, die Beseitigung unerwarteter Sicherheitslücken oder die Abwehr akuter Bedrohungen. Solche ad-hoc-Projekte sind zweifellos entscheidend, um das unmittelbare Überleben in einer zunehmend digitalisierten Welt zu sichern. Doch für eine nachhaltig leistungsfähige Organisation reicht dies allein nicht aus. Ein essenzieller, aber oft vernachlässigter Baustein ist die konsequente Integration von Cyber-Security-Themen in den regulären IT-Linienbetrieb. Eine langfristige und belastbare IT-Sicherheitsstrategie geht über kurzfristige Reaktionen hinaus. Sie ermöglicht nicht nur eine fundierte Absicherung und verlässliche Überwachung, sondern schafft auch die Voraussetzungen für echte Prävention. Der Schlüssel liegt dabei in einem ganzheitlichen und systematischen Ansatz, der von Anfang an die steigenden Bedrohungen und wachsenden Sicherheitsanforderungen berücksichtigt und in der Linienorganisation verankert wird. Als Orientierung dient ein Dekalog, der die wesentlichen Prinzipien und Erfolgsfaktoren für die Integration von IT-Sicherheit in den IT-Linienbetrieb zusammenfasst. Dieser Leitfaden unterstützt Unternehmen dabei, eine nachhaltige Sicherheitskultur zu etablieren und den Herausforderungen der digitalen Ära langfristig erfolgreich zu begegnen.

Abbildung 10.: Dekalog für Sicherheit in der IT-Linienorganisation

1 – Durchführen einer Bedarfsanalyse: Identifizieren Sie Sicherheitsanforderungen, potenzielle Bedrohungen und Compliance-Anforderungen, um einen fundierten Überblick zu erhalten. Dabei sind neben allgemeinen Sicherheitsanforderungen insbesondere branchenspezifische Regularien und gesetzliche Vorgaben (z.B. DSGVO, BaFin, DORA) sowie kritische Geschäftsprozesse und sensible Daten mit besonders hohem Schutzbedarf entscheidend.

2 – Entwicklung von Sicherheitsrichtlinien- und verfahren: Erstellen Sie interne Richtlinien und Verfahren, die den Unternehmenszielen entsprechen und alle relevanten Sicherheitsthemen (Datenzugriff, -verarbeitung, Passwortverwaltung, etc.) abdecken. Diese sollten für eine möglichst breite Akzeptanz klar und verständlich formuliert sein. Darüber hinaus sollten sie regelmäßig aktualisiert werden, um auf neue Bedrohungen reagieren zu können.

3 – Strukturelle Definition der IT-Sicherheitsorganisation: Legen Sie Rollen und Verantwortlichkeiten für Mitarbeiter fest und gestalten sie eine solide Struktur aus drei Verteidigungslinien. In der First Line of Defense (1st LoD) liegt die operative Umsetzung der Sicherheitsrichtlinien. Die Second Line of Defense (2nd LoD) unterstützt und überwacht die operativen Einheiten. Darüber bildet die Third Line of Defense (3rd LoD) die übergeordnete Prüfinstanz.

4 – Schulung bzw. Einstellung von Personal: Starten Sie mit Sicherheitsexperten mit spezifischem Fachwissen (z.B. Penetration Testing, Incident Response, IT Security Awareness) und schulen Sie vorhandenes Personal bzgl. Security-Awareness, um die Sicherheitsstrategie effektiv umzusetzen zu können. Ein regelmäßiges Schulungskonzept sollte etabliert werden, um das Sicherheitsbewusstsein bei der IT-Nutzung nachhaltig zu fördern

5 – Implementierung neuer Technologien: Investieren Sie in Sicherheitstechnologien wie Firewall, Intrusion Detection Systems, Verschlüsselungstools oder Antivirensoftware, die den Bedürfnissen des Unternehmens entsprechen. Grundlagen hierfür liefern die Bedarfsanalyse sowie die Berücksichtigung der vorhandenen IT-Infrastruktur. Zusätzlich sind Test- und Pilotphasen sinnvoll, um die Integration abzusichern.

6 – Überwachung des Betriebs: Richten Sie Mechanismen zur kontinuierlichen Überwachung von Prozessabläufen und Technologien ein. Hierfür sind aussagekräftige Kennzahlen und Reporting-Formate zu etablieren, um ein zielgerichtetes Monitoring zu erreichen. In der Umsetzung kann ein Security Operations Center (SOC) zentral sein, um Sicherheitsereignisse rund um die Uhr zu überwachen und zu analysieren.

7 – Entwerfen von Reaktionsplänen auf Vorfälle: Definieren Sie klare, strukturierte Pläne zur Reaktion im Fall eines Sicherheitsvorfalls. Diese Pläne sollten detaillierte Eskalationsprozesse, transparente Kommunikationswege sowie klare Verantwortlichkeiten für verschiedene Szenarien wie Datenlecks, Cyberangriffe oder Systemausfälle festlegen und regelmäßig durch Simulationen getestet werden.

8 – Durchführung regelmäßiger Audits und Überprüfungen: Implementieren Sie einen Prozess für regelmäßige Sicherheitsaudits, um Effektivität der Sicherheitsmaßnahmen sicherzustellen und sich der Bedrohungslage anzupassen. Der Fokus liegt hier auf der strukturierten Vorbereitung auf Prüfungen durch die 3rd LoD, etwa interne Revision oder externe Prüfer.

9 – Auf- und Ausbau von Partnerschaften: Wägen Sie ab, ob sie sicherheitsrelevante Lösungen intern entwickeln oder auf bewährte Expertise externer Partner setzen sollten. Externe Sicherheitsdienstleister und Branchennetzwerke bieten oft spezialisierte Lösungen und wertvolle Einblicke, wodurch auf erprobte Best Practices zurückgegriffen werden kann, um kosteneffizient und schnell auf Bedrohungen zu reagieren.

10 – Treiben Kontinuierlicher Verbesserung: Implementieren Sie einen Prozess zur kontinuierlichen Verbesserung hinsichtlich Reduktion von Sicherheitsvorfällen, Eindämmen von Vorfällen und Geschwindigkeit bei Reaktionen. Mit einer systematischen Analyse von Vorfällen und deren Ursachen können Schwachstellen identifiziert und so Sicherheitsrichtlinien zielgerichtet überarbeitet werden, um zukünftige Angriffe zu verhindern.

Mit konsequenter Berücksichtigung dieser Kernpunkte gelingt der Wechsel von einem reaktiven zu einem proaktiven Ansatz im Bereich Cybersecurity. Durch die Etablierung einer starken Linienorganisation für IT-Sicherheit kann Ihr Unternehmen eine solide Struktur schaffen, um Sicherheitsrisiken frühzeitig zu erkennen, angemessen darauf zu reagieren und ihre Resilienz-Mechanismen kontinuierlich zu stärken. Mit Blick auf die strategische Positionierung des gesamten Unternehmens ist damit letztlich auch eine kulturelle Transformation vom bisher traditionellen IT-Sichtfahrbetrieb hin zu einem sicheren IT-Linienbetrieb unumgänglich. Eine umfassende Umsetzung der genannten zehn Eckpfeiler bedeutet eine weitreichende Transformation, die sich zweifellos ebenso ambitioniert wie notwendig darstellt.

4.5 Security Operations Center – Incident Readiness & Response effektiv einsetzen

In Kombination mit dem zuvor ausgeführten Thema der IT-Security Linienorganisation sind Security Operations Center (SOC), Security Information and Event Management (SIEM)-Systeme und Computer Emergency Response Teams (CERT) die wichtigsten Komponenten des Cyber-Abwehrzentrums. Ein zentrales Element zur Vorbereitung und zum Testen der Einsatzbereitschaft des Abwehrzentrums ist das War-Gaming. Dies dient dazu, mögliche Sicherheitsvorfälle zu simulieren und die Reaktion darauf zu optimieren. So werden Schwachstellen in Teams und in der Organisationsstruktur schonungslos offengelegt und können sukzessive geschlossen werden.
In diesem Artikel beleuchten wir die verschiedenen Komponenten und wie ihr Zusammenspiel dazu beiträgt, die Sicherheitsstrategie eines Unternehmens zu verbessern.

Sicherheitsvorfälle können dabei in verschiedenen Varianten auftreten: Das ebenso aus dem privaten Bereich bekannte Phishing sowie das versuchte Knacken von Passwörtern oder Malware-Infektionen sind wohl die gängigsten Beispiele, häufig mit schwerwiegenden Folgen wie beispielsweise einer Verschlüsselungsattacke durch Ransomware. Sicherheitsvorfälle können aber wesentlich vielfältigere Formen annehmen. Insiderbedrohungen, bei denen interne Personen ihre Zugriffsrechte ausnutzen, können ebenfalls erheblichen Schaden verursachen. Aus unserer Projekterfahrung sind aber auch sog. „Advanced Persistent Threats" besonders betonenswert, die einen sorgfältig geplanten, langanhaltenden und gezielten Cyberangriff bezeichnen und für einen längeren Zeitraum unentdeckt bleiben. Angesichts der vielfältigen Bedrohungen ist ein strukturierter Ansatz zur Bewältigung von Sicherheitsvorfällen unerlässlich. Hier kommt der Incident-Response-Prozess ins Spiel, der aus vier zentralen Phasen besteht:

1. Vorbereitung: Aufbau von Sicherheitsmaßnahmen, Prozessen und Schulungen, um schnell und effektiv auf potenzielle Vorfälle reagieren zu können. Dies beinhaltet auch regelmäßige Übungen wie War-Gaming, um die Reaktionsfähigkeit zu testen und zu verbessern.

2. Erkennung und Analyse: Identifizierung von Sicherheitsvorfällen durch Überwachungssysteme wie SIEM oder durch Benutzerberichte. Eine schnelle und genaue Analyse ist entscheidend, um die Schwere des Vorfalls einzuschätzen und geeignete Maßnahmen einzuleiten.

3. Eindämmung und Beseitigung: Sofortige Maßnahmen zur Eindämmung der Bedrohung, um Schäden zu minimieren, gefolgt von der vollständigen Beseitigung der Ursache aus dem System. Hierbei orientieren sich Maßnahmen und Eskalationsniveau am Schweregrad des Vorfalls: Schwerwiegende Ereignisse erfordern umfassende Maßnahmen, Einbindung der Unternehmensleitung und ggf. Information an den Regulator, während geringfügigeren Ereignissen entsprechend einem moderaterer Handlungspfad folgt.

4. Wiederherstellung und Nachbereitung: Wiederherstellung betroffener Systeme und Rückkehr zum Normalbetrieb. Anschließend erfolgt eine Auswertung des Vorfalls (Lessons Learned), um Erkenntnisse zu gewinnen und zukünftige Sicherheitsmaßnahmen zu verbessern. Aufgrund der sich wandelnden und stetig weiterentwickelnden Bedrohungslagen, wird in dieser Phase häufig auch der Incident-Response-Prozess selbst weiterentwickelt und verbessert.

Das Security Operations Center (SOC) ist in allen Phasen des Incident-Response-Prozesses eingebunden. In Phase 1 entwickelt es Sicherheitsanweisungen, schult das Personal und stellt die erforderlichen Technologien bereit. Während Phase 2 überwacht das SOC kontinuierlich Netzwerke und Systeme, um Bedrohungen frühzeitig zu erkennen. Bei einem Vorfall (Phasen 3 und 4) koordiniert es gemeinsam mit dem CERT die notwendigen Reaktionsmaßnahmen.

Security Information and Event Management (SIEM)-Systeme sind essenziell für die Effektivität des Prozesses. In Phase 1 werden sie konfiguriert, um Daten aus verschiedenen Quellen innerhalb der IT-Infrastruktur effizient zu sammeln und zu analysieren. Sie bieten eine zentrale Sicht auf die Sicherheitslage, unterstützen die Automatisierung und Priorisierung von Vorfällen. Während Phase 2 identifizieren SIEM-Systeme durch kontinuierliche Datenanalysen verdächtige Aktivitäten und Anomalien, um im Ernstfall eine schnelle Reaktion zu ermöglichen.

Das Computer Emergency Response Team (CERT) spielt ebenfalls eine wichtige Rolle im Incident-Response-Prozess. In Phase 1 erstellt es Reaktionspläne, führt Schulungen durch und beteiligt sich an War-Gaming-Übungen zur Steigerung der Einsatzbereitschaft. In Phase 3 ist das CERT für die Eindämmung und Beseitigung von Bedrohungen verantwortlich, während es in Phase 4 die Wiederherstellung der Systeme betreut und durch Nachbereitung zukünftige Sicherheitsmaßnahmen verbessert.

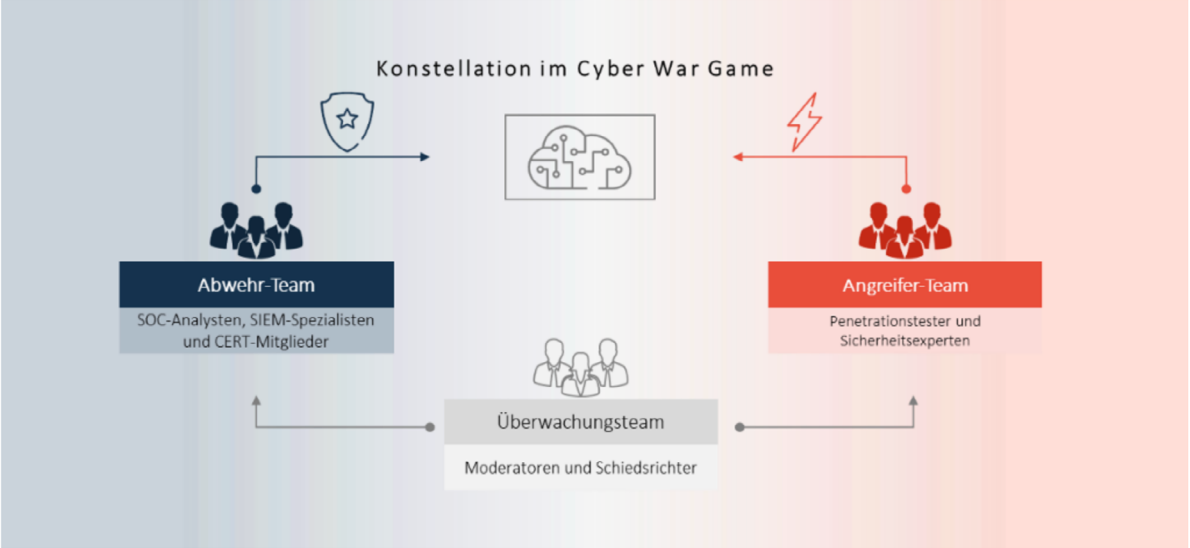

Abbildung 11.: War-Gaming Set-up

Das sogenannte War-Gaming ist eine praxisnahe Methode, um die Reaktionsfähigkeit auf Cybervorfälle zu testen und zu verbessern. Nicht umsonst hat es Eingang in jüngste europaweite Regulatorik (Stichwort: DORA – Thread-Led Penetration Testing, TLPT) gefunden. Es umfasst simulierte Angriffe und Szenarien, die das Zusammenspiel von blauen, roten und weißen Teams erfordern:

/ **Blaues Team:** Verteidigt und bekämpft Angriffe auf IT-Anwendungen und Netzwerke. In der Regel bestehen diese Teams aus SOC-Analysten, SIEM-Spezialisten und CERT-Mitgliedern, die ihre Fähigkeiten und Prozesse in realitätsnahen Szenarien testen

/ **Rotes Team:** Führt gezielte Angriffe auf Zielsysteme durch, um Schwachstellen zu identifizieren. Dieses Team besteht meist aus internen oder externen Penetrationstestern und Sicherheitsexperten, die die Rolle eines Angreifers übernehmen, mit dem Ziel Schwachstellen aufzudecken

/ **Weißes Team:** Gibt Anweisungen, überwacht und bewertet die Übungsszenarien. Das weiße Team besteht aus Moderatoren und Schiedsrichtern. Sie sind dafür verantwortlich objektive Analysen und Feedback zu geben, um sicherzustellen, dass die Übung so realitätsnah und effektiv wie möglich ist

Der Gesamtablauf des War-Gamings lässt sich in folgende Phasen unterteilen:
1. **Planung:** Vorbereitung der Übungsszenarien
2. **Ausführung:** Durchführung der simulierten Angriffe durch das rote Team
3. **Koordination:** Management und Abstimmung der Abwehrmaßnahmen durch das blaue Team
4. **Umsetzung:** Implementierung und Anpassung der Verteidigungsstrategien in Echtzeit
5. **Nachbesprechung:** Analyse der Ergebnisse zur Identifizierung von Verbesserungsmöglichkeiten

Ein wesentlicher Aspekt von War-Gaming ist nicht nur die technische Leistungsfähigkeit der Teams zu testen, sondern auch ihre Kommunikationsfähigkeit innerhalb des Teams und mit Führungskräften. Gerade in den ersten Momenten nach Erkennung eines neuen Vorfalls herrscht häufig Unsicherheit: Ist dies ein gezielter Angriff oder nur eine Logfile-Anomalie? Welche Systeme sind betroffen? Jetzt gilt

es, einen kühlen Kopf zu bewahren und dem Incident-Response-Prozess zu folgen. Dieser regelt klar die Verantwortlichkeiten und gibt allen Beteiligten Handlungssicherheit, während das Lagebild durch jede neue Information schrittweise klarer wird. Mit zunehmendem Reifegrad und Erfahrung der Teams können die Anforderungen schrittweise erhöht werden, von vordefinierten Übungsszenarien bis hin zu realen Angriffen, die in Simulationen getestet werden. So wird sichergestellt, dass Ihr Unternehmen auf alle Eventualitäten optimal vorbereitet ist.

Der Incident-Response-Prozess ist das strukturelle Rückgrat einer effektiven Cyberabwehr, das durch die Expertise von SOC, SIEM und CERT erst seine Wirkung entfalten kann. Regelmäßige War-Gaming-Übungen stellen diese Fähigkeiten stetig auf den Prüfstand und stärken die Reaktionsfähigkeit. So können Unternehmen ihre Widerstandsfähigkeit gegenüber Cyberangriffen nachhaltig stärken und auch in Krisenzeiten handlungsfähig bleiben.

4.6 Vulnerability Management – Der Lifecycle für nachhaltige IT-Sicherheit

Es gibt Situationen, in denen ein gesamtes System plötzlich ungewöhnlich reagiert und unklar bleibt, ob die Ursache ein einfacher Systemfehler oder eine gezielte Manipulation ist, die den Geschäftsbetrieb gefährden könnte. Um solche Risiken gezielt zu vermeiden und potenzielle Einfallstore für Angreifer frühzeitig zu erkennen und zu schließen, ist ein strukturiertes Vulnerability Management unerlässlich – ein ganzheitlicher Prozess, der Schwachstellen erkennt, die entsprechenden Risiken bewertet und durch ergebnisorientierte Maßnahmen langfristige Sicherheit im Unternehmen schafft. Ein wesentlicher Bestandteil ist dabei das Vulnerability Scanning, ein unverzichtbares Werkzeug, um Schwachstellen frühzeitig aufzuspüren – besonders in stark regulierten Branchen wie dem Finanzsektor. Vulnerabilities, oder Schwachstellen, sind Sicherheitslücken in IT-Systemen, die Angreifer ausnutzen können, um unerlaubten Zugriff zu erlangen, Daten zu manipulieren oder Systeme lahmzulegen. Angesichts der Vielzahl an Schwachstellen möchten wir an dieser Stelle einen Überblick über diejenigen geben, die aus unserer Sicht am wichtigsten und bedeutsamsten sind:

- **Fehlendes oder unzureichendes Patching:** Veraltete Systeme und ungepatchte Software gehören zu den häufigsten Ursachen für Angriffe. Schwachstellen entstehen, wenn notwendige Updates nicht rechtzeitig installiert werden. Ein effektives Patch-Management sollte daher ein fester Bestandteil eines Secure Software Development Lifecycles (SSDLC) sein (siehe Phase 6 im Abschnitt SSDLC, siehe Kapitel 4.7)
- **Fehlende oder schlechte Verschlüsselung:** Daten, die unzureichend geschützt sind, können leicht abgefangen und missbraucht werden. Besonders in sensiblen Bereichen ist eine starke und durchgehende Verschlüsselung (Data-at-rest / Data-in-motion) unerlässlich.
- **Fehlkonfigurationen von Systemen:** Offene Ports, schwache Passwörter oder öffentlich zugängliche Cloud-Dienste sind häufige Schwachstellen, die durch mangelnde Sicherheitsrichtlinien oder deren unzureichende Umsetzung entstehen. Diese Fehler sind vermeidbar, erfordern jedoch regelmäßige Prüfungen.
- **Zero-Day-Schwachstellen:** Sicherheitslücken, die noch keine verfügbaren Patches haben, sind besonders gefährlich. Proaktive Maßnahmen wie Anomalie-Erkennung oder Virtual Patching können dabei helfen, solche Schwachstellen frühzeitig abzufangen. Auch Darkweb-Crawling zur Überwachung in Umlauf gebrachter oder angebotener Zero-Day-Exploits gehört mittlerweile zum Verteidigungsarsenal vieler Unternehmen.

Für Finanzdienstleister stellen Schwachstellen aufgrund der hochsensiblen und stark vernetzten Systeme ein erhebliches Risiko dar. Besonders herausfordernd ist dabei die Komplexität der IT-Infrastruktur. Oftmals betreiben Finanzinstitute eine Mischung aus veralteten Legacy-Systemen und modernen Cloud-Lösungen. Diese heterogene IT-Landschaft vergrößert nicht nur die Angriffsfläche, sondern erfordert auch eine sorgfältige Koordination, um Schwachstellen effizient zu minimieren. Ein weiteres zentrales Risiko ist der Schutz sensibler Kundendaten. Informationen wie Kontodetails oder Kreditkartenangaben sind ein begehrtes Ziel für Cyberangriffe. Datenlecks können nicht nur rechtliche Konsequenzen und empfindliche Strafen nach sich ziehen, sondern auch das Vertrauen der Kunden nachhaltig erschüttern und so zu erheblichen Reputationsschäden führen. Zudem müssen Finanzdienstleister strenge regulatorische Vorgaben wie xAIT, DORA oder NIS2 einhalten. Diese verpflichten zu hohen Sicherheitsstandards und einem robusten Schwachstellen-Management. Wird dies vernachlässigt, drohen schwerwiegende Feststellungen durch Aufsichtsbehörden sowie erhebliche finanzielle Strafen. Schließlich ist die Verfügbarkeit geschäftskritischer Systeme wie Online-Banking oder Zahlungsabwicklungen essenziell. Ausfälle, die durch ausgenutzte Schwachstellen verursacht werden, können nicht nur hohe finanzielle Verluste nach sich ziehen, sondern auch das Vertrauen der Kunden nachhaltig beeinträchtigen. Insgesamt erfordert die Komplexität dieser Herausforderungen einen ganzheitlichen Ansatz im Schwachstellen-Management, um Risiken zu minimieren und die Widerstandsfähigkeit der Systeme zu gewährleisten. Der in fünf Schritte strukturierte Vulnerability Management Lifecycle-Prozess hilft, diese Schwachstellen systematisch zu identifizieren, zu bewerten und nachhaltig zu beheben.

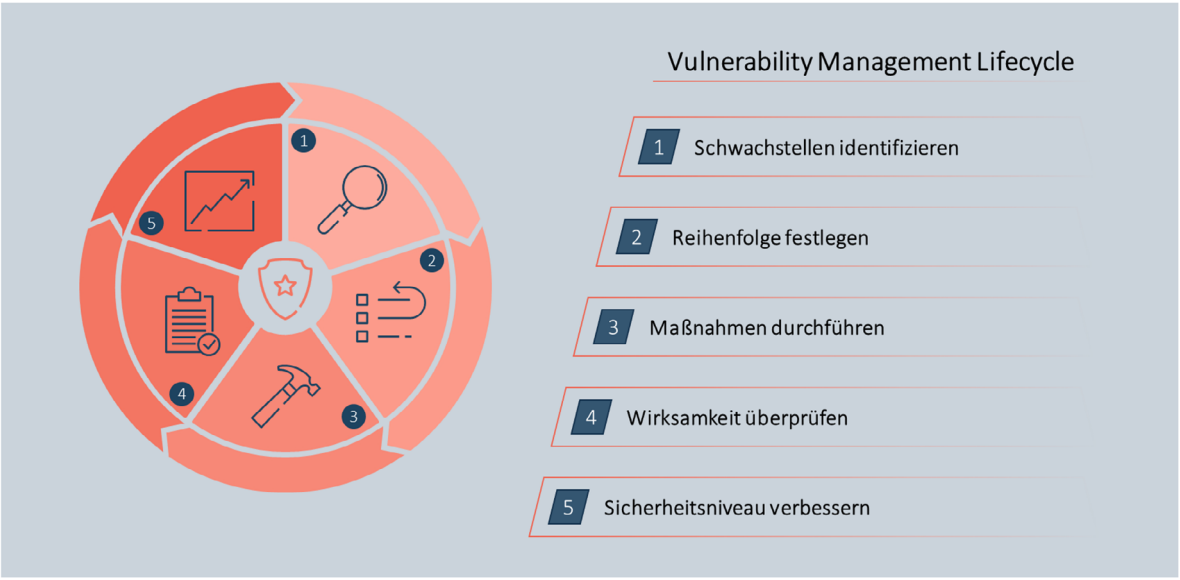

Abbildung 12.: 5 Schritte des Vulnerability Management Lifecycles

Im ersten Schritt werden potenzielle Angriffsvektoren erfasst und analysiert. Dies erfolgt durch Asset-Discovery, bei dem alle relevanten Systeme und Anwendungen identifiziert werden. Anschließend kommen automatisierte Vulnerability Scans zum Einsatz, die Systeme auf bekannte Schwachstellen prüfen, z. B. basierend auf der CVE-Datenbank (Common Vulnerabilities and Exposures). Moderne Scanning-Tools wie Nessus und Qualys kombinieren dabei signaturbasierte und heuristische Methoden, um nicht nur bekannte Schwachstellen zu erkennen, sondern auch potenzielle Zero-Day-Schwachstellen aufzuspüren. Der Einsatz von ISO/IEC 27001-konformen Verfahren gewährleistet dabei die Einhaltung internationaler Sicherheitsstandards. Neue Trends wie Cloud-basiertes Scanning Tools und der Einsatz von KI verbessern zusätzlich die Effizienz und Genauigkeit.

Im Anschluss ist die Reihenfolge festzulegen. Nicht jede Schwachstelle ist gleich kritisch. Deshalb werden im nächsten Schritt die identifizierten Schwachstellen nach ihrem potenziellen Risiko priorisiert. Faktoren wie die Kritikalität des betroffenen Systems, der CVSS-Score (Common Vulnerability Scoring System) und der potenzielle Geschäftsschaden spielen dabei eine zentrale Rolle. Automatisierte Risk-Scoring-Modelle helfen, die Dringlichkeit und Reihenfolge der Maßnahmen objektiv zu bestimmen. Danach ist die Durchführung der Maßnahmen an der Reihe. Die Behebung von Schwachstellen durch geeignete Maßnahmen ist der wohl wichtigste Schritt im gesamten Lifecycle. Kritische Schwachstellen erfordern oft sofortiges Handeln, während bei weniger kritischen Fällen alternative Ansätze sinnvoll sein können. Zu den wichtigsten Maßnahmen gehören hierbei:

- **Patch-Management:** Sicherheitsupdates auf betroffenen Systemen einspielen.
- **Temporäre Workarounds:** Dazu zählen Maßnahmen wie das Blockieren bestimmter Ports oder das zeitweilige Deaktivieren bestimmter Funktionen bis zur Verfügbarkeit eines Patches.
- **Risikoabmilderung:** Reduzierung der Risiko-Wahrscheinlichkeit und/oder des Impacts, beispielsweise durch Implementierung zusätzlicher Schutzmaßnahmen und erweitertes Monitoring.

Gerade bei Workarounds oder Risikoabmilderungen steht häufig eine Abwägung auch über etwaige Kollateralschäden, beispielsweise beim vorsorglichen Einschränken oder gar Abschalten von Services, im Raum. Grundsätzlich sollten sowohl der geforderte Maßnahmenzeitraum als auch der Handlungsgrad stets in angemessener Relation zum konkreten Risiko im Kontext des individuellen Risiko-Appetits des Unternehmens stehen.

Der vierte Schritt im Vulnerability Management Lifecycle ist die Überprüfung der Wirksamkeit. Nach der Umsetzung der Maßnahmen ist eine Überprüfung unerlässlich. Dies geschieht durch erneutes Scanning oder gezielte Tests. Der Unterschied zwischen Verification (Überprüfung) und Validation (Bestätigung) ist hierbei entscheidend:

- **Verification:** Hier wird geprüft, ob die Maßnahmen korrekt implementiert wurden.
- **Validation:** Hier wird bewertet, ob die entsprechende Schwachstelle nun tatsächlich geschlossen ist und die gewünschten Sicherheitsziele erreicht wurden.

Dies kann bei schwerwiegenden Schwachstellen soweit gehen, dass nach dem Einspielen eines Patches ein Penetrationstest durchgeführt wird, um sicherzustellen, dass die Schwachstelle geschlossen wurde und keine neuen Sicherheitslücken entstanden sind.

Der letzte Schritt, Sicherheitsniveau verbessern, umfasst die Dokumentation und Analyse, um Sicherheitsstandards nachhaltig zu erhöhen. Berichte schaffen Transparenz und helfen, Prozesse zu optimieren. Wiederkehrende Schwachstellen lassen sich durch zusätzliche Sicherheitsrichtlinien oder gezielte Trainings langfristig vermeiden. Mit Standards wie ISO/IEC 27005 können Unternehmen ihre „Lessons Learned" effizient in das Risikomanagement integrieren und so das Sicherheitsniveau kontinuierlich verbessern.

Ein starkes Vulnerability Management bildet die Grundlage für den Schutz Ihrer IT-Systeme vor potenziellen Schwachstellen und Angriffen. Gleichzeitig trägt es maßgeblich dazu bei, das Vertrauen Ihrer Kunden und Partner zu bewahren, indem es Sicherheit, Stabilität und Zuverlässigkeit gewährleistet. So wird es zu einem zentralen Baustein für den nachhaltigen Erfolg Ihres Unternehmens.

4.7 Secure Software Development Lifecycle (SSDLC) – Softwareentwicklung neu denken

Unserer Projekterfahrung nach gelingt eine sinnvolle Integration von Sicherheitsanforderungen erst dann, wenn man sie nicht nur als integrales Feature der Software sieht, sondern sich das Sicherheitsverständnis im Arbeitsmodus der Anwendungsentwicklung widerspiegelt. Ein Framework, das Sicherheitsanforderungen in jeder Phase des Software-Lebenszyklus einbezieht, ist der Secure Software Development Lifecycle (SSDLC).

Der SSDLC ist ein strukturierter Prozess zur Entwicklung von Software, der sicherheitsrelevante Praktiken in den gesamten Entwicklungsprozess integriert. Im Gegensatz zur herkömmlichen Software-Entwicklung betont der SSDLC die Notwendigkeit des Sicherheitsbewusstseins bei Entwicklern und Anwendern, identifiziert Sicherheitsrisiken frühzeitig und implementiert Sicherheitskontrollen und Tests dazu in jeder Phase des Entwicklungsprozesses.

Auch aus Sicht der Aufsicht spielt die sichere Anwendungsentwicklung eine große Rolle (unter anderem in DORA, xAIT). So soll gewährleistet werden, dass Sicherheitsaspekte von Anfang an in den Entwicklungsprozess eingeflochten werden, um die Widerstandsfähigkeit von Finanz- und Versicherungsanwendungen gegenüber digitalen Risiken zu stärken und Compliance-Anforderungen zu erfüllen. Der SSDLC ist ein integraler Bestandteil einer umfassenden Sicherheitsstrategie für Unternehmen und Organisationen in der heutigen digitalen Landschaft.

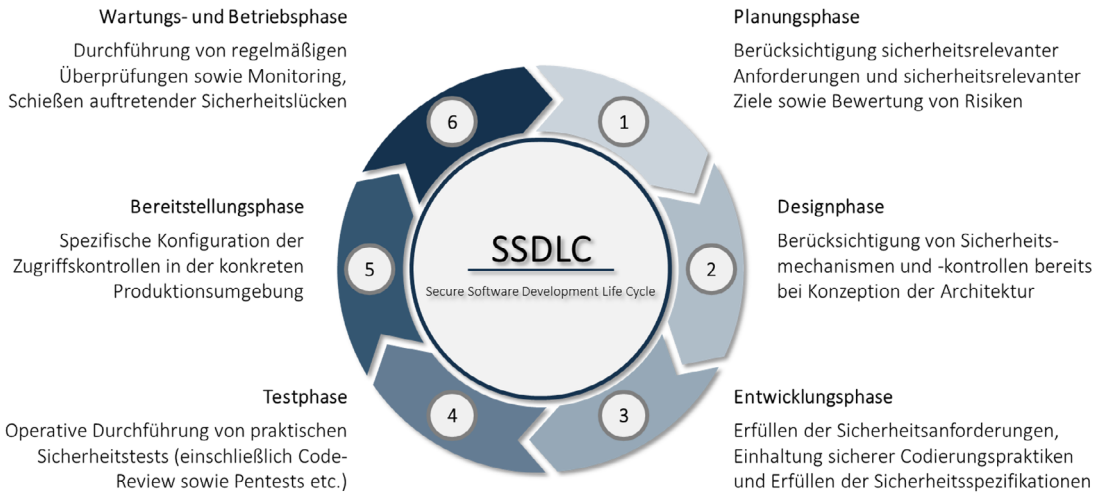

Abbildung 13.: Phasen Secure Software Development Lifecycle

Typische Phasen im SSDLC:

1. Planung – Der Grundstein für Sicherheit: Die Planungsphase ist entscheidend für den Erfolg eines Projekts. Hier werden Ziele und Anforderungen präzise definiert, wobei der Schwerpunkt auf der Identifikation und Bewertung von Sicherheitsrisiken Eine sorgfältige Risikobewertung ermöglicht es, Bedrohungen zu priorisieren und effektive Strategien für ihre Mitigation zu entwickeln. Dies bildet die Basis für eine durchdachte Sicherheitsstrategie.

2. Design –– Sicherheit von Anfang an: Während der Designphase ist es wichtig, dass Sicherheitsmechanismen und Kontrollen bereits in der Architektur der Software verankert werden. Dazu gehört die Definition von Sicherheitsrichtlinien, die Implementierung von Authentifizierungsverfahren, Zugriffskontrollen und Verschlüsselungstechniken. Eine robuste Architektur, die von Anfang an Sicherheit berücksichtigt, schützt effektiv gegen potenzielle Angriffe.

3. Entwicklung – Best Practices für Sicherheit: In der Entwicklungsphase ist es essenziell, dass sichere Programmierpraktiken befolgt werden. Die Verwendung sicherer Bibliotheken und Frameworks sowie das Vermeiden unsicherer Programmiermuster sind kritische Schritte, um die Sicherheit der Software während der Entwicklung zu gewährleisten.

4. Testen – Sicherheit verifizieren: Die Testphase umfasst alle relevanten Sicherheitstests, wie Penetrationstests, Schwachstellenanalysen, Code-Reviews und automatisierte Sicherheitsprüfungen. Diese Tests sind entscheidend, um sicherzustellen, dass die Software robust gegenüber Bedrohungen ist und eventuelle Sicherheitslücken vor dem Release erkannt und behoben werden.

5. Bereitstellung – Sicher in die Produktion: Nach erfolgreichen Tests und Überprüfungen wird die Software für die Produktionsumgebung vorbereitet. In dieser Phase ist es wichtig, dass Sicherheitseinstellungen und Zugriffskontrollen sorgfältig konfiguriert werden, um die Integrität und Sicherheit der Anwendung zu gewährleisten.

6. Wartung und Betrieb – Langfristige Sicherheit sicherstellen: Die Phase der Wartung und des Betriebs beinhaltet regelmäßige Überprüfungen und Updates, um neu entdeckte Sicherheitslücken zeitnah zu adressieren und die Sicherheit der Software dauerhaft zu gewährleisten. Reaktionen auf Sicherheitsvorfälle und umgehendes Patchen von bekannten Schwachstellen sind in dieser Phase von großer Bedeutung.

Der SSDLC ist aber nicht nur für die Entwicklung neuer Softwareanwendungen von entscheidender Bedeutung, sondern spielt auch eine wichtige Rolle bei der Aufwertung von Legacy-Systemen. Der Übergang eines bestehenden Systems zu einem SSDLC-Ansatz erfordert eine gründliche Analyse der vorhandenen Architektur, um Sicherheitslücken aufzudecken und veraltete Komponenten zu identifizieren. Eine sorgfältige Überprüfung von Legacy-Systemen zeigt oft, dass Sicherheitsanfor-derungen aktualisiert oder komplett überarbeitet werden müssen. Dies beginnt typischerweise bei der Codebasis und umfasst Maßnahmen wie Code-Scanning und -Refactoring sowie das Ersetzen von anfälligen Bibliotheken. Solche Anpassungen sind unerlässlich, um die Sicherheitsarchitektur zu stärken und den aktuellen Bedrohungen gerecht zu werden.

Auch für Legacy-Systeme empfehlen sich übrigens sorgfältige Security-Reviews und -Testphasen. So sollten insbesondere die üblichen Wartungs- und Entwicklungsprozesse um spezielle Security-Checkpoints erweitert werden. Oft ist auch eine Überarbeitung des Testkonzepts erforderlich. Die Implementierung automatisierter Security-Testing-Tools, die die Legacy-Codebasis auf Schwachstellen wie SQL-Injection oder Cross-Site-Scripting prüfen, ist ein effektiver Weg, Sicherheitsprobleme zu identifizieren. Diese Tools bieten einen erheblichen Vorteil gegenüber manuellen Code-Reviews, da sie schneller und zuverlässiger potenzielle Sicherheitsrisiken aufdecken können.
Last but not least ist die Software-Development-Culture integraler Bestandteil des gelebten SSDLC. Besonders relevant ist dabei die Schulung von Entwicklern, aber auch die Awareness in Managementfunktionen. Vorhandene Nachholbedarfe können hierbei durch entsprechende Trainings oder Awareness-Programme behoben werden.

4.8 Individual Data Processing (IDP) – Eine Sicherheits- und Compliance-Perspektive

Individual Data Processing (IDP) oder individuelle Datenverarbeitung (IDV) beschreiben die Verarbeitung von Daten durch (teil-)automatisierte Anwendungen, die auf individuell erstellten Tools basieren – wie z. B. komplexen Excel-Sheets mit oder ohne Makros oder auch benutzerdefinierten Scripten. Ein anschauliches Beispiel für IDP ist ein über die Jahre entwickeltes Excel-Tool, das ursprünglich von einer Kollegin erstellt wurde, um den Arbeitsalltag zu erleichtern. Im Laufe der Zeit wurden neue Funktionen hinzugefügt, während eine umfassende Dokumentation jedoch ausblieb. Diese Anwendungen entstehen meist abseits der zentralen IT-Prozesse, um schnell und flexibel auf spezifische Anforderungen der Fachabteilungen zu reagieren. Beispiele hierfür sind:

- **Komplexe Berechnungen** in Excel, bei denen mitunter auch Makros zur Automatisierung zum Einsatz kommen.
- **Datenverknüpfungen** zwischen verschiedenen **Systemen** über Scripte, die APIs oder externe Datenquellen integrieren.
- Individuell programmierte Tools zur **Erstellung** von **Berichten** oder **Dashboards**.

Die Attraktivität solcher Lösungen liegt in ihrer Flexibilität, der oft kurzen Entwicklungszeit und den geringen Kosten. Diese Vorteile gehen jedoch häufig zulasten von Sicherheitsmaßnahmen und Standardisierungen. Im Laufe der Zeit entwickelt sich so eine Art „Schatten-IT", die weder zentral verwaltet noch ausreichend dokumentiert wird. Dadurch entstehen potenzielle Sicherheitslücken und Schwachstellen, die das gesamte Unternehmen gefährden können. Während IDP-Lösungen oft effizient und wirtschaftlich sind, werfen sie zugleich gravierende Sicherheits- und Compliance-Herausforderungen auf. Denn die zunehmende Bedeutung von IDP wurde auch durch die Regulierungsbehörden erkannt. Vorschriften wie DORA oder branchenspezifische IT-Anforderungen wie VAIT, BAIT oder KAIT betonen die Notwendigkeit, alle datenverarbeitenden Prozesse – einschließlich IDP – in ein umfassendes Sicherheits- und Risikomanagement einzubinden. Ein Beispiel: Wenn IDPs nicht den strengen Vorgaben und Kontrollen eines Secure Software Development Lifecycle (siehe Abschnitt 4.7 zu SSDLC) unterliegen, entstehen erhebliche Risiken. Diese betreffen sowohl regulatorische als auch operative Aspekte und erfordern gezielte Maßnahmen. Unternehmen, die diesen Anforderungen nicht nachkommen, riskieren nicht nur hohe Strafen, sondern auch schwerwiegende Reputationsverluste. Im folgenden Abschnitt werden die damit verbundenen Risiken näher beleuchtet.

4.8.1. Risiken von IDP – Eine Sicherheits- und Compliance-Perspektive

Die Analyse von Ablaufprozessen zeigt oft überraschend, an wie vielen Stellen undokumentierte IDPs im Einsatz sind. Diese Tools erfüllen häufig nützliche Aufgaben und arbeiten zuverlässig, doch ihre objektive Qualitätssicherung ist in der Regel nicht gewährleistet. Dies führt zu verschiedenen Risiken:

1. Mangelnde Sicherheitskontrollen: Viele IDP-Lösungen werden ohne einheitliche Sicherheitsvorgaben entwickelt. Beispielsweise enthalten Excel-Makros häufig Schwachstellen, die von Angreifern ausgenutzt werden können. Auch die ungesicherte Speicherung sensibler Daten auf lokalen Laufwerken oder Cloud-Diensten stellt ein typisches Problem dar.

2. Fehlende Dokumentation und Nachvollziehbarkeit: Ohne klare Dokumentation und Versions-kontrollen sind Änderungen an IDPs kaum nachvollziehbar. Die Fehleranfälligkeit komplexer Anwendungen, etwa in Excel, verschärft die Problematik zusätzlich. Selbst bei anfangs fehlerfreien Tools können Änderungen in den Eingangsdaten, Softwareversionen oder Zugriffsmöglichkeiten die Stabilität gefährden. Dies erschwert die Identifikation und Behebung von Sicherheitslücken.

3. Fehlender Owner: In einer strukturierten IT-Landschaft wird jeder Anwendung ein Application-Owner zugeordnet, der für Pflege, Dokumentation und Governance verantwortlich ist. Bei IDPs fehlt diese Rolle oft. Stattdessen fungiert häufig ein einzelner Kollege, der sich mit dem Tool auskennt, ohne jedoch offiziell dafür verantwortlich zu sein.

4. Regulatorische Anforderungen: Vorschriften wie DORA oder NIS2 verlangen von Unternehmen eine klare Governance über alle datenverarbeitenden Prozesse. Unkontrollierte IDP-Anwendungen laufen diesen Vorgaben zuwider, da sie häufig außerhalb der zentralen IT-Governance betrieben werden und die nötigen Sicherheits- oder Prüfstandards nicht erfüllen.

5. Hohes Betriebsrisiko: Individuell entwickelte Lösungen bergen bei Ausfällen oder Weiterentwicklungen hohe Risiken für den Betrieb. Es fehlt häufig an Skalierbarkeit und an der Integration in zentrale IT-Strategien, was die langfristige Verfügbarkeit erschwert.

Trotz der genannten Risiken sollte der Einsatz von IDPs nicht grundsätzlich infrage gestellt werden. Wenn die Risiken bekannt sind, können gezielte Sicherheitsstrategien entwickelt werden. Wie dies im Detail aussehen kann, wird im nächsten Abschnitt beleuchtet.

4.8.2. Sicherheitsstrategien für den Umgang mit IDP

Die sichere Nutzung von IDP erfordert einen strukturierten Ansatz, der die Flexibilität solcher Lösungen erhält, ohne Sicherheits- oder Compliance-Standards zu kompromittieren. Zu den wichtigsten Maßnahmen für einen sicheren Umgang mit IDPs zählen:

1. Inventarisierung und Klassifizierung: Es ist essenziell, alle bestehenden IDP-Anwendungen zu identifizieren und zu bewerten. Eine Schutzbedarfsanalyse kann dabei helfen, kritische Anwendungen zu priorisieren und gezielt Sicherheitsmaßnahmen zu implementieren.

2. Definition von Mindeststandards: Unternehmen sollten verbindliche Sicherheitsrichtlinien für IDP festlegen. Dazu gehören u. a. die Verwendung sicherer Frameworks, regelmäßige Sicherheitsprüfungen und das Verbot unsicherer Programmiersprachen oder Bibliotheken.

3. Sensibilisierung der Nutzer: Mitarbeitende müssen geschult werden, dass bereits ein einfaches Excel-Tool IDP sein kann. Sicherheitsbewusstsein und Grundkenntnisse im Umgang mit entsprechenden Tools und Daten sind essenziell, um potenzielle Schwachstellen von Anfang an zu vermeiden.

4. Integration in die IT-Governance: IDP sollte in bestehende IT-Prozesse integriert werden, z. B. durch die Einbindung in IT-Asset-Management-Systeme (siehe Kapitel 4.3 zu IT Asset Management). Dadurch können Anwendungen überwacht und zentralisiert dokumentiert werden.

5. Automatisierte Sicherheitsprüfungen: Tools zur Analyse von Makros oder Scripts können automatisiert Schwachstellen identifizieren und Sicherheitslücken schließen. Solche Prüfungen sollten regelmäßig und vor jeder Nutzung neuer Versionen durchgeführt werden.

6. Monitoring und Reporting: Ein kontinuierliches Monitoring von IDP-Anwendungen, einschließlich ihrer Nutzungsdaten und potenzieller Sicherheitsvorfälle, erhöht die Transparenz und hilft, Risiken frühzeitig zu erkennen.

IDPs sind aus der Praxis kaum mehr wegzudenken, da sie den Arbeitsalltag spürbar erleichtern und in vielen Bereichen einen echten Mehrwert bieten. Dennoch bringen sie Risiken mit sich, die gezielt adressiert werden müssen. Unternehmen sollten IDPs deshalb in ihre Sicherheitsstrategien einbinden und klare Mindeststandards definieren, um Sicherheitslücken zu schließen und regulatorische Vorgaben zu erfüllen. Ein strukturierter Ansatz, der die Flexibilität von IDPs mit robusten Sicherheitsmaßnahmen kombiniert, stärkt nicht nur die Cyberresilienz, sondern erhöht auch die Effizienz und die operative Zuverlässigkeit der Organisation nachhaltig.

4.9 User Access Management (UAM) – mehr Sicherheit im Unternehmen schaffen

In einer zunehmend digitalisierten Welt, in der immer mehr Prozesse, Transaktionen und Datenströme online abgewickelt werden, wächst auch stetig der Bedarf an einem zuverlässigen und sicheren Identitätsmanagement. Hier kommt das User Access Management (UAM) ins Spiel – eine wichtige Komponente, die das Rückgrat einer jeden effektiven IT-Sicherheitsstrategie bildet.
User Access Management umfasst die Verwaltung, Überwachung und Kontrolle von Benutzern und Zugriffen auf verschiedene Systemressourcen. Es fungiert grundsätzlich nach dem Principle-of-least-Privilege und gliedert sich in zwei Hauptbereiche:

1. Identity and Access Management (IAM): IAM sorgt dafür, dass nur autorisierte Personen Zugriff auf bestimmte Ressourcen haben. Dies wird durch eine Kombination aus Technologie, Geschäftsprozessen und Richtlinien gewährleistet.
2. Privileged Access Management (PAM): PAM konzentriert sich auf den speziellen Zugriff von privilegierten Benutzern beziehungsweise technischen Accounts. Diese haben höhere Berechtigungen, um auf kritische Funktionen oder Daten zuzugreifen.

Das Herzstück des IAM: Der IAM-Bereich besteht aus verschiedenen Teildisziplinen, von denen jede eine spezielle Rolle im Gesamtsystem spielt:

/ **Governance und Prozesse:** Hier werden die Regeln und Abläufe festgelegt. Dies umfasst beispielsweise das IAM-Richtlinien-Framework, das Target Operating Model und das Reporting-Modell, aber auch Kernprozesse für den Umgang mit Änderungsbedarfen (zum Beispiel Joiner-Mover-Leaver Prozess), um nur einige zu nennen.

/ **Fachbereichsaufgaben:** Dieser Bereich befasst sich mit der praktischen Umsetzung der IAM-Richtlinien im Geschäftsalltag. Dazu gehören das Pflegen von Autorisierungskonzepten, die Funktionstrennung (SoD) zum Beispiel nach dem 4-Augen-Prinzip und die Definition von Geschäftsrollen.

/ **Technologie:** Die Technologie ist das Werkzeug, mit dem die IAM-Richtlinien umgesetzt werden. Hierzu gehören die Plattformentwicklung, die Applikationsanbindung, das technische Onboarding von Berechtigungskonzepten und vieles mehr.

Erst durch das Zusammenwirken dieser Disziplinen kann ein effektives und Identitäts- und Rechtemanagement sichergestellt und vor allem nachgehalten werden.
Der spezialisierte Fokus von PAM: Mit großer Macht kommt große Verantwortung – und größeres Risiko im Falle von absichtlichem oder unabsichtlichem Missbrauch. Während IAM sich auf die Gesamtheit der Zugriffsverwaltung konzentriert, spezialisiert sich PAM daher auf privilegierte Konten. Hierbei handelt es sich um Accounts, die höhere Zugriffsrechte haben als der Standardnutzer. Diese Konten können sowohl von Menschen (zum Beispiel Administratoren) als auch von Maschinen (technische Accounts) genutzt werden.

Ein effektives PAM-System muss bestimmte Aspekte gewährleisten:
/ Schutz und Verwaltung von Anmeldeinformationen
/ slolierung, Überwachung und Aufzeichnung von Sitzungen
/ Bedrohungserkennung und -analyse

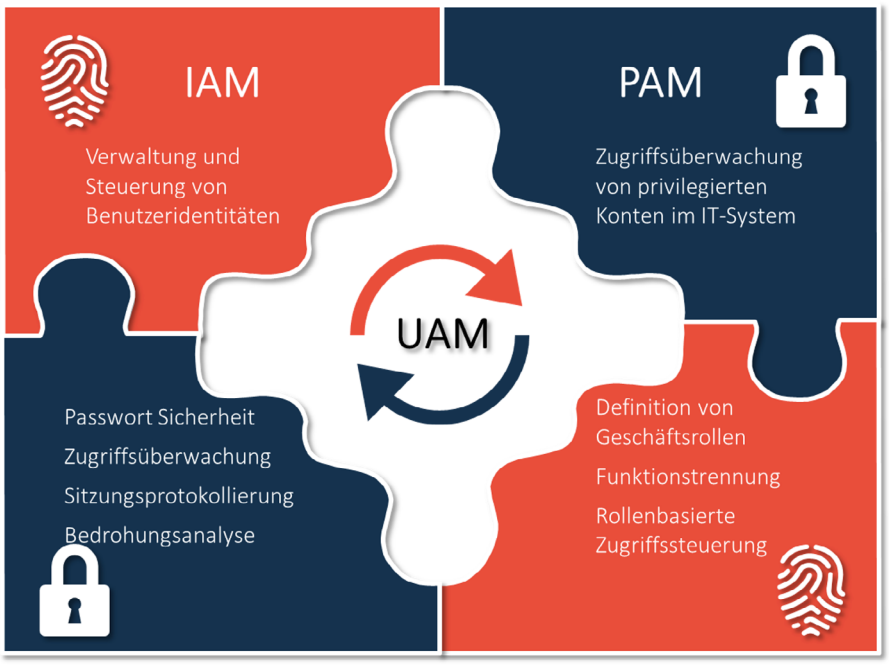

Abbildung 14.: UAM - Zusammenwirken von IAM und PAM

Die IAM- und PAM-Konzepte sind zwei Seiten derselben Medaille. Während IAM sicherstellt, dass die richtigen Personen Zugriff auf die richtigen Ressourcen haben, sorgt PAM dafür, dass privilegierten Zugriffe sicher sind. Gemeinsam bilden sie die Basis für ein effektives User Access Management, das die Integrität, Vertraulichkeit und Verfügbarkeit von IT-Systemen in der Organisation sicherstellt. In einer Zeit, in der Cyberbedrohungen immer raffinierter werden, ist ein solides UAM-System unerlässlich. Es schützt das Unternehmen einerseits vor externen Bedrohungen und sorgt gleichzeitig dafür, dass Risiken durch interne Fehler oder böswillige Handlungen gezielt minimiert werden. Es gibt eine breite Palette von IAM/PAM-Technologien auf dem Markt, und jedes dieser Tools bietet unterschiedliche Funktionen, die auf spezifische Anwendungsbereiche zugeschnitten sind. Neben zentralen Lösungen im Cloud-Umfeld, die alle relevanten Player integriert anbieten (Azure, AWS, Google, …) finden sich auch zahlreiche Anbieter spezialisierter Software-Lösungen (Sailpoint, Okta, OneLogin, Cyberark, BeyondTrust, Arcon, um nur ein paar Vertreter aufzuzählen). Wie immer ist es daher ratsam, vor der Auswahl eines bestimmten Produkts einen sorgfältigen Software-Auswahlprozess durchzuführen und die individuellen Anforderungen und Bedürfnisse zu berücksichtigen, um eine geeignete IAM- oder PAM-Lösung zu etablieren. Egal welche Technologien am Ende zum Einsatz gebracht werden, ein gut durchdachtes und umgesetztes UAM-Konzept ist ein essentieller Beitrag für die IT-Sicherheit in jeder Organisation.

5. Fazit

Diese Unterlage hat die zunehmenden Cyberanforderungen insbesondere anhand der Beispiele DORA und NIS2 veranschaulicht und wichtige Cyberthemen von IT Asset Management bis hin zu Third Party Risk Management skizziert. Regierungen und Aufsichtsbehörden legen zunehmend Wert und prüfen auf robuste Sicherheitsmaßnahmen und reagieren gegebenenfalls mit harten Strafen bei Nichteinhaltung der Vorgaben. Dabei gilt: Unternehmen riskieren nicht nur empfindliche Geldstrafen, sondern auch einen erheblichen Reputationsverlust, vor allem Betreiber kritischer Infrastruktur. Für Unternehmen bedeutet dies nicht nur die Notwendigkeit, ihre IT-Sicherheitsstrategien kontinuierlich anzupassen, sondern auch, sich frühzeitig und mit Weitblick auf kommende Veränderungen vorzubereiten. Daher ist es entscheidend, mit dem richtigen Partner bereits jetzt die Weichen zu stellen, um den wachsenden regulatorischen Anforderungen gerecht zu werden und gleichzeitig die eigene Cyberresilienz zu stärken. Wir von Horn & Company unterstützen Sie gerne auf diesem Weg. Mit unserer umfassenden Expertise helfen wir Ihnen, Risiken zu minimieren, Ihre Compliance sicherzustellen und Ihre Sicherheitsarchitektur zukunftssicher zu gestalten.

DIE AUTOREN

Dr. Oliver Laitenberger
oliver.laitenberger@horn-company.de

Dr. Carsten Woltmann
carsten.woltmann@horn-company.de

Dr. Christoph Hartl
christoph.hartl@horn-company.de

Robert Tippmann
robert.tippmann@horn-company.de

Dr. Christoph Seebach
christoph.seebach@horn-company.de

Dr. David Bauder
david.bauder@horn-company.de

Leon Heyn
leon.heyn@horn-company.de

Dr. Moritz Pleintinger
moritz.pleintinger@horn-company.de

Dr. Thomas Kurz
thomas.kurz@horn-company.de

Markus Ettenauer
markus.ettenauer@horn-company.at

ÜBER HORN & COMPANY

HORN & COMPANY ist eine im Kern auf Banken und Versicherungen sowie Industrie und Handelsunternehmen spezialisierte Top-Management-Beratung. Der Fokus der über 160 BeraterInnen liegt auf Strategieprozessen, GuV-orientierte Performance-Verbesserung und der digitalen Transformation. Mit Gründung der „Horn & Company Data Analytics GmbH" und Kooperationen mit Software-Entwicklern und IT-Lösungsanbietern hat Horn & Company ein Consulting-Ökosystem für die digitale Transformation etabliert. In den Jahren 2024/25 wurden die BeraterInnen von Horn & Company zum wiederholten Mal als „Hidden Champion des Beratermarktes" ausgezeichnet.

Das Unternehmen mit Hauptsitz in Düsseldorf hat Büros in Berlin, Frankfurt am Main, Hamburg, München, Wien und Zürich. www.horn-company.de HORN & COMPANY ist Mitglied im exklusiven Beraterpool für Stabilisierungsmaßnahmen des Wirtschaftsstabilisierungsfonds (WSF). Für unsere Auswahl waren insbesondere die großen Erfahrungen in Sanierung und Turnaround sowie die Kenntnisse von Schlüsselbranchen und mittelständischen Unternehmen ausschlaggebend.

Horn & Company wird zudem in unabhängigen Beratervergleichen regelmäßig ausgezeichnet, unter anderem als „HIDDEN CHAMPION", als „TOP CONSULTANT/BERATER DES JAHRES" und „BESTE BERATER".

HORN & COMPANY
Kaistraße 20 | 40221 Düsseldorf
Telefon +49 (0)211 30 27 26-0 | info@horn-company.de
www.horn-company.com