HORN & COMPANY

Cyber Security und BAIT: Wachsende Bedrohung trotz komplexer Regulatorik

Ein Diskussionsbeitrag von Horn & Company

Düsseldorf, Juni 2023

- Die digitale Transformation verschärft die **Bedrohungslage** von Finanzinstituten hinsichtlich **Cyber Security** und **sicherem IT-Betrieb:** Neue **Technologien** ermöglichen immer **neue Varianten von Cyberrisiken –** meist **subtiler** und oft **markenschädigender** als das bisher Bekannte

- Parallel zur Bedrohungslage sehen sich Finanzinstitute mit einer **enormen** und **weiter zunehmenden Regulierungsflut** konfrontiert: Entweder im Rahmen eines **Self-Assessments oder nach erfolgtem Audit** stehen daher häufig **umfangreiche Anpassungsbedarfe** ins Haus

- Kein Wunder also, dass die **Investitionen in Cyber Security** bei vielen Banken **exponentiell steigen**. Programme haben mittlerweile eine Größe und einen Umfang erreicht, der **professionelle Planung, Steuerung und Management** erfordert, damit die Kosten nicht völlig aus dem Ruder laufen.

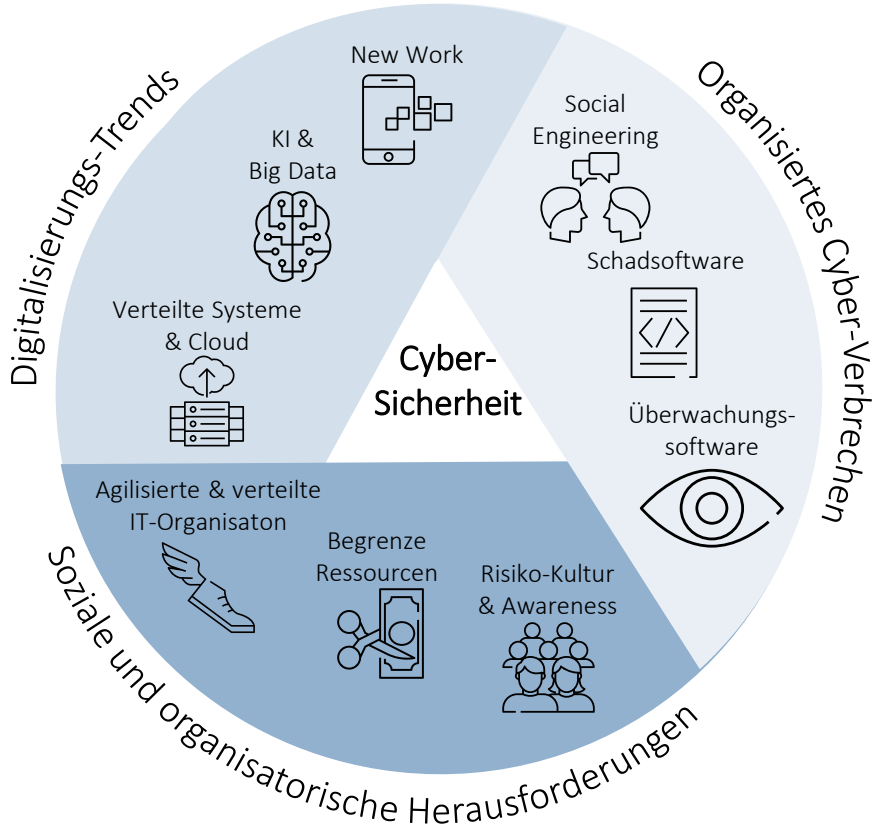
- **Horn & Company** hat einen **verprobten Ansatz** für das fortlaufende **Management** von **Cyber-Security-Programmen.** Dieser stellt sicher, **dass Sicherheitsanforderungen vor dem Hintergrund der vorhandenen Budgets erfüllt werden.** Entscheider gewinnen Vertrauen bzgl. der verlässlichen Einhaltung der Regulatorik.

- **Technische Details** durchdringen wir mit unserem strategischen **Partner EUVIC**. Dadurch gelingen Diskussion und Lösungsfindung wo notwendig im Gegenstromverfahren **vom Management in den „Maschinenraum“ und zurück.** So entsteht ein **notwendiger exklusiver neutraler Gegenpol** zu bekannteren IT-Dienstleistern.

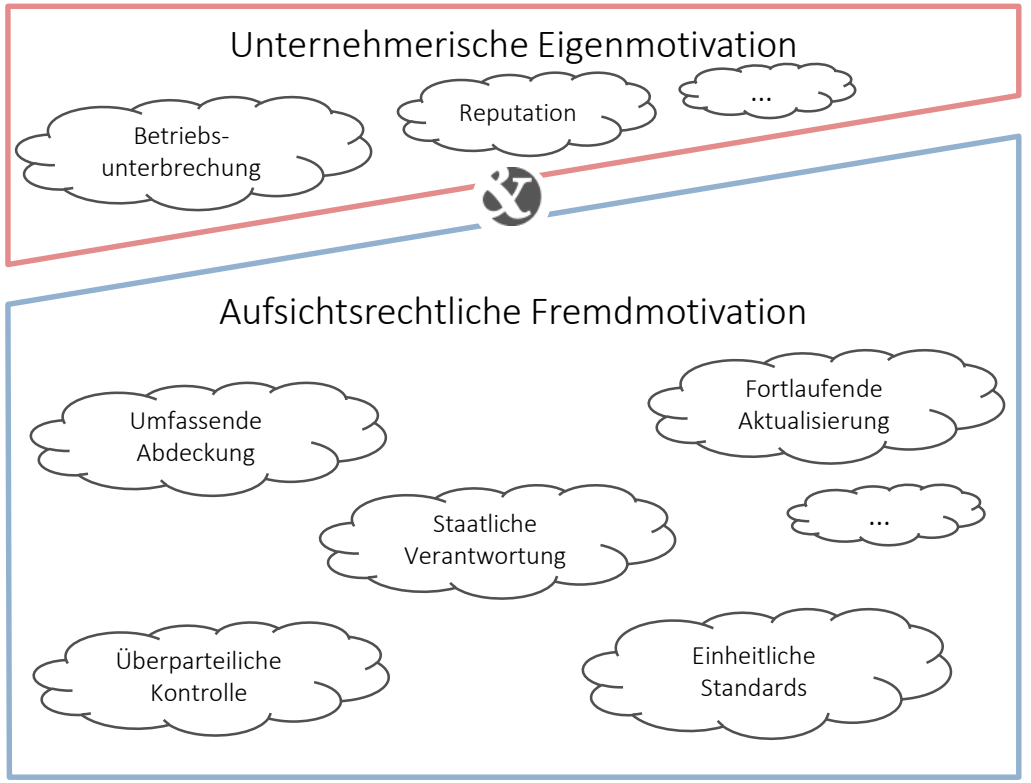
BaFin und Revisoren zeigen Verantwortlichen in Banken die IT-Risiken auf

Bedrohungen und Auswege durch Eigeninitiative oder Regulatorik

Wachsenden Bedrohungen begegnen …



… eigeninitiativ oder durch die Regulatorik initiiert



Die Cyberbedrohung ist real – die Aufsichtsbehörden schnüren über die BAIT das Korsett enger – interne Revisoren machen Feststellungen und fordern vom Top-Management die Einhaltung

Verlässliche Partner lassen Sie das „Hase und Igel“-Rennen rund zum Cyber gewinnen

Horn & Company Cyber-Ökosystem

Cyber-Strategie, -Planung & -Steuerung

Horn & Company ist eine im Kern auf Banken und Versicherungen spezialisierte Top-Management-Beratung mit aktuell bereits ca. 160 Mitarbeitern.

Wir brechen die Komplexität der vielfältigen Cyberthemen und sorgen für klare Strukturen auf Basis eines tiefem Verständnis der Besonderheiten einer Bank

Unser Fokus liegt auf zügiger und sauberer Umsetzung regulatorischer Anforderungen, nicht auf erhöhter Dynamik und Komplexität aufgrund wirtschaftlicher Eigeninteressen

Wir arbeiten für das Management als Auftraggeber und Zielkunde der Programmergebnisse gemeinsam mit EVUIC alle Cyber-Themen ab

HORN & COMPANY

(Techn.) Cyber-Umsetzung und -Betrieb

EUVIC ist führendes, internationales Software-Unternehmen mit weltweit über 5000 Spezialisten und eigenem Betrieb eines **Security Operations Centers** für Finanzinstitute

Wir sind kompetenter Durchführer des CyberExpress Self-Assessments und identifizieren relevante Cyber-Schwach-stellen bevor es zu Vorfällen oder Findings kommt

Unser Fokus liegt auf einem E2E ausgelegten und umgesetzten Cyber-Security-Konzepts – vom Architektur-Blueprint bis zur Operations-Automation

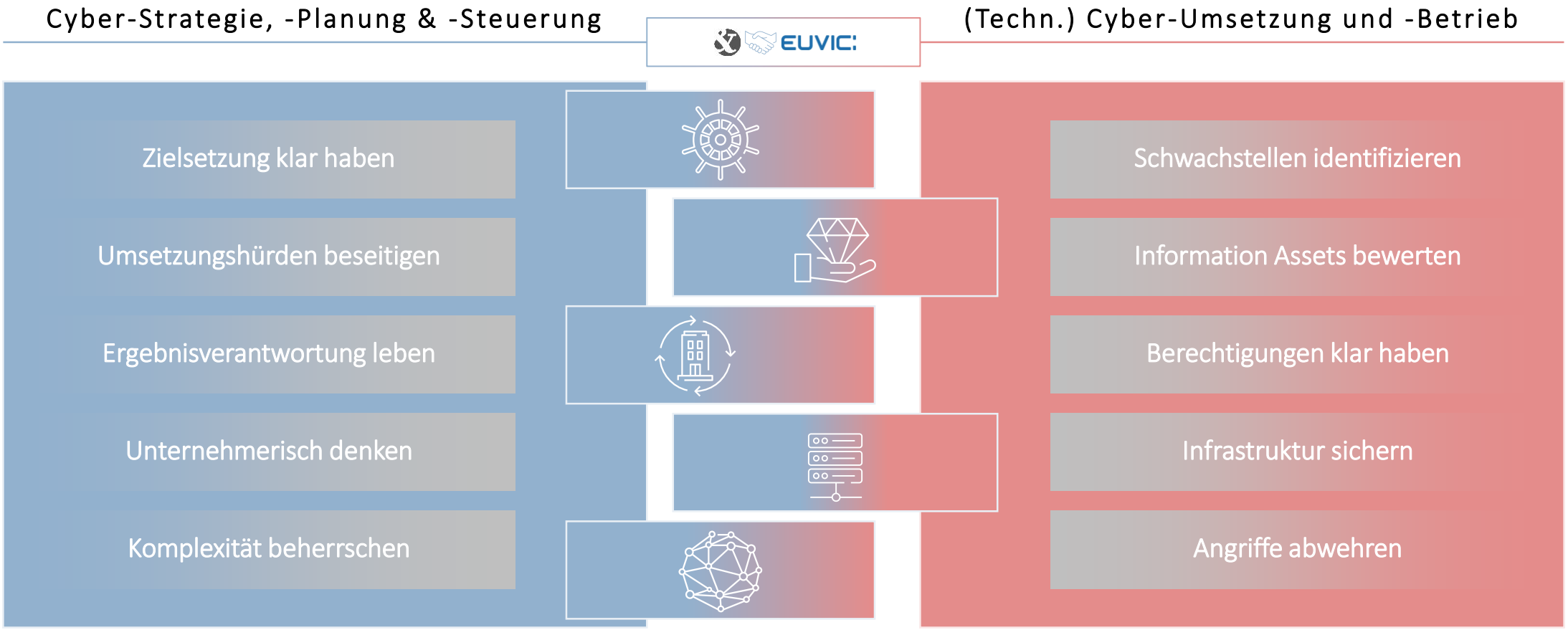
Perfektion ist nie schwarz oder weiß, deshalb sind wir gemeinsam mit Horn & Company umsetzungsstarker Partner für ganzheitliche Cyber-Security-Lösungen

EUVIC

Zusammen mit unserem Partner Euvic decken wir das Spektrum von Strategie, Planung, Steuerung bis hin zur technologischen Umsetzung ab (u.a. bis hin zu einem Cyber Security Operations Center)

Der Mehrwert liegt in der Orchestrierung von Breiten- und Tiefenkompentenz

Anforderungsrahmen für Cyber-Sicherheit



Wir spannen einen ganzheitlichen Rahmen um die heterogenen und vielfältigen Cyber-Themen und sorgen für verlässliche Erfüllung von Cyber-Anforderung durch das Management

Bankaufsichtliche Anforderungen an die IT (BAIT) bilden das Pflichtenheft

Kapitelübersicht BAIT und Kerninhalte

BAIT Kapitel	*Hauptaugenmerk*
IT-Strategie	… ist Teil der Geschäftsstrategie, definiert überprüfbare Ziele und erfüllt gewisse Mindeststandards
IT-Governance	… definiert IT Prozesse, um den Betrieb und die Weiterentwicklung der IT sicherzustellen
Informationsrisikomanagement	… evaluiert und behandelt Informationsrisiken, die sich aus Abweichungen zum Soll-Zustand ergeben
Informationssicherheitsmanagement	… ist ein laufender Prozess mit den Phasen Planung, Umsetzung, Erfolgskontrolle sowie Optimierung
Operative Informationssicherheit	…muss Integrität, Authentizität sowie Vertraulichkeit in Bezug auf IT Systeme und Prozesse gewährleisten
Identitäts- und Rechtemanagement	… vergibt Rechte (Sparsamkeitsprinzip), definiert deren Lebenszyklus und überprüft diese regelmäßig
IT-Projekte und Anwendungsentwicklung	… etabliert einen Prozess zur Entwicklung, Freigabe und Implementierung von IT Systemen (inkl. Test)
IT-Betrieb	… sorgt durch ein aktuelles Komponentenregister und -beziehungen für reibungslosen Prozessablauf
Auslagerungen	… macht Vorgaben zum Outsourcing von IT Dienstleistungen, insbesondere zur Risikobetrachtung
IT-Notfallmanagement	… identifiziert kritische Aktivitäten, Systeme und Prozesse u. erstellt Notfallpläne zur Geschäftsfortführung
Kontaktmanagement Zahlungsdienstnutzer	… minimiert Betrugsrisiken durch Nutzer-Sensibilisierung und durch technische System-Einschränkungen
KRITIS	… ergänzt die BSI-Verordnung zur Sicherstellung der Versorgungssicherheit kritischer Dienstleistungen

Eine systematische Befassung der BAIT-Bausteine deckt in vielen Häusern Defizite auf, die zur Erfüllung der Anforderungen behoben werden müssen

Anforderungs-Umsetzung kann proaktiv oder auf Verlangen der Aufsicht hin erfolgen

Szenarioanalyse an Hand des Lebenszyklus der Umsetzung

Self-Assessment

Self-Assessment („Dry Run“) an Hand der BAIT Kapitel zur Identifikation von SOLL-IST-Abweichungen

Hohe **Flexibilität** bezüglich der Dimensionen Umfang und Zeit verbessert die Planbarkeit und reduziert den Budgetbedarf

Priorisierung und Umsetzung der Maßnahmenpakete erfolgt nach **Budgetverfügbarkeit bzw. Risikoappetit**

BaFin Audit

Kritische **Prüfung der Aufsichtsbehörde** legt Mängel gnadenlos offen und gibt den Umsetzungsrahmen vor

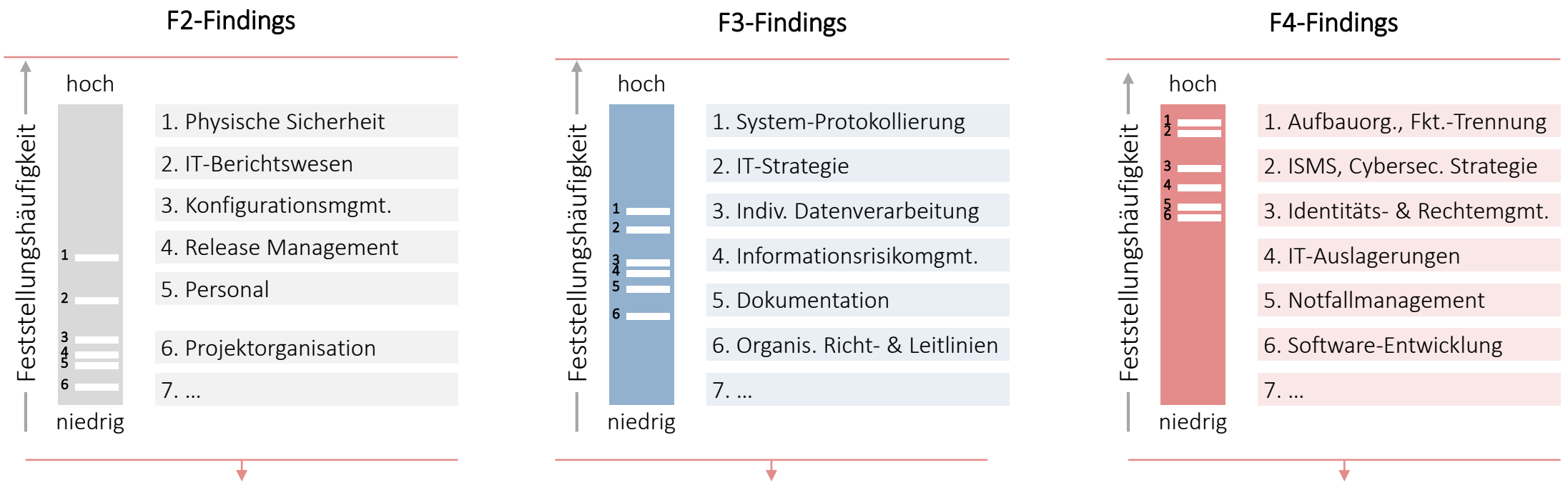
Fixe Vorgaben zu Umfang und Umsetzungszeitraum können das Budget überproportional belasten

Abarbeitung der jeweiligen Maßnahmen steht im Fokus und erfolgt in enger **Abstimmung mit der Aufsicht**

„Die Aufsicht im Nacken“ schränkt den Handlungsspielraum ein, daher ist frühzeitiges und vorbeugendes Handeln auf Basis eines Self-Assessments zu bevorzugen

Auch bei schweren Cyber-Mängeln sind oft noch Handlungsspielräume vorhanden

H&C-Marktblick



Fall 1: Basis ist Self-Assessment

F2-Vorbeugung i.d.R. zurückgestellt	F3-Vorbeugung gem. Risikoappetit	F4-Feststellungen werden vermieden

Fall 2: Basis ist BaFin-Audit

F2-Bearbeitung auf der Zeitachse	F3- u. F4-Bearbeitung unmittelbar anzustoßen

Bei vorbeugendem Handeln (z.B. auf Basis Self-Assessment) kann man sich auf die schwerwiegenden Feststellungen fokussieren. Wenn die BaFin schon da war, ist der Handlungsspielraum kleiner.

Diagnostizierte Bedarfe werden bewertet und in Handlungsfelder überführt

Umgang mit Feststellungen und Assessmentergebnissen

H&C orchestriert alle relevanten Stakeholder bei der Maßnahmenidentifikation

Bedarfe

BAIT-Bedarfe

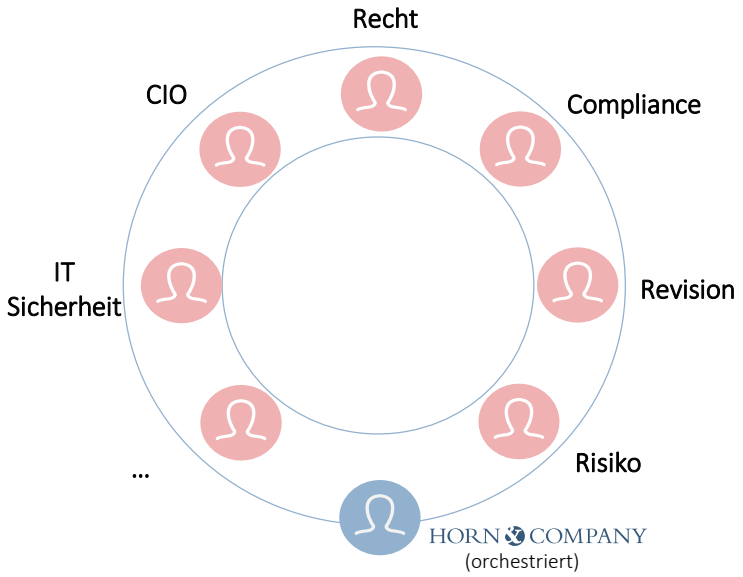
\+

ggf. weitere Trigger/Inputs

- Größere Sicherheitsvorfälle
- Externe Audits
- Interne Audits
- Penetrationstest
- ...

Bewertung

Typische Stakeholder



Stakeholder-Zusammensetzung hängt auch von den konkreten Feststellungen ab und ist beim Projektstart zu validieren bzw. zu ergänzen

Maßnahmen

Maßnahmen-Kaskade (Zuordnung der Maßnahmen zu den jeweiligen Kategorien abhängig von Risiko-Appetit, Aufwand und Komplexität)

Keine Maßnahme notwendig
Risiko akzeptiert

Maßnahmen notwendig
(insbesondere Audit / Assessment Ergebnisse)

Priorisierter Maßnahmenkatalog

Kurzfristige Maßnahmen
Taskforce Modus / Ausführung hauptsächlich in Linienorganisation

Sofortmaßnahmenpaket
entlang der BAIT-Kapitel (max. 6-8 Wochen)

Wasserfall / agil möglich

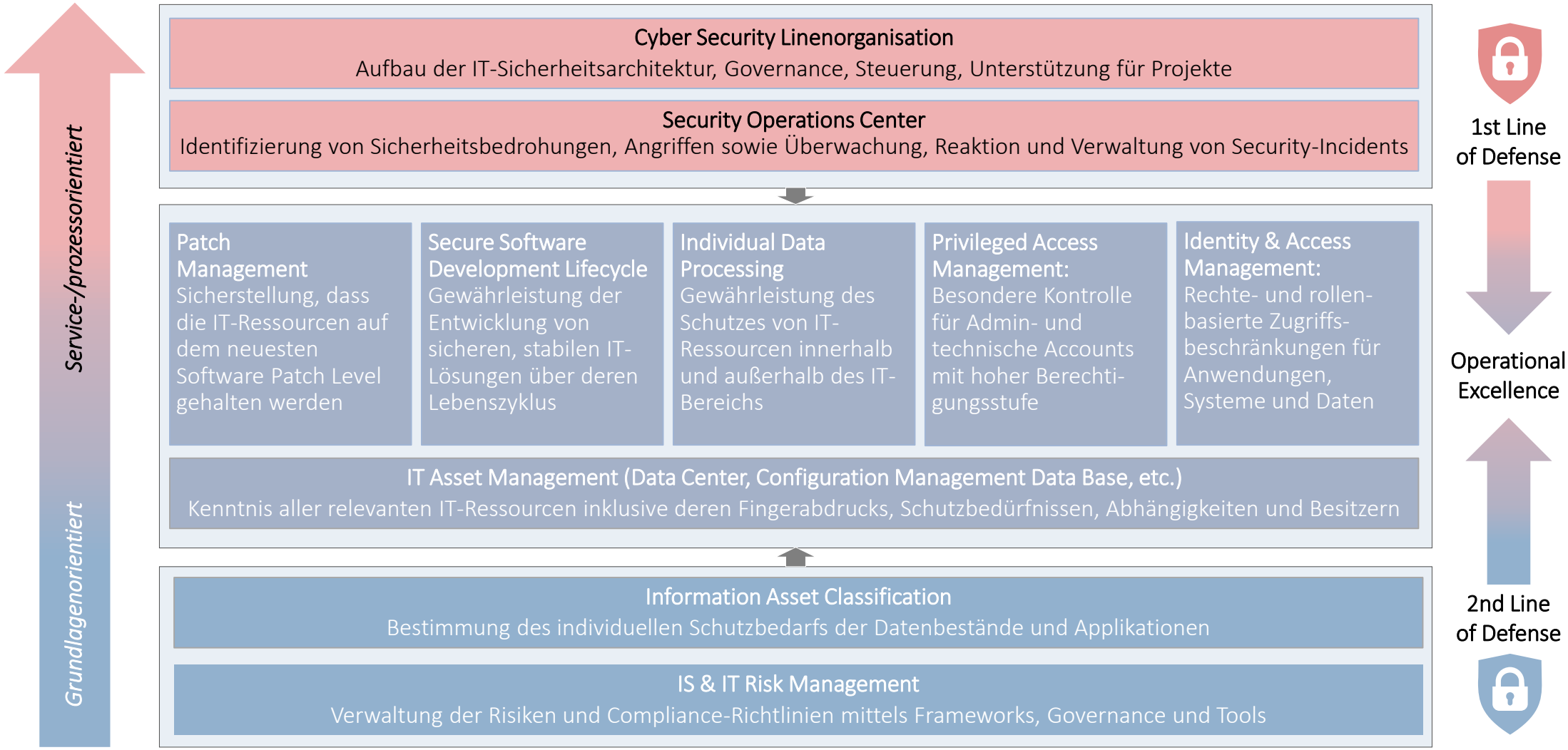
Mittelfristige Maßnahmen
Projekt-Modus, Umfassende Planung erforderlich

Scope-Clusterung und Aufbau Cyber-Security-Programm

Wasserfall

Handlungsziele in Cyber-Security-Programmatik stringent bis zum „Closing“ steuern

Cyber-Security-Programm: Typische Struktur



Einsatz einer 2nd Opinion sichert BaFin-Anspruch der Endprodukte ab

Zusammenspiel mit Wirtschaftsprüfer als 2nd Opinion

Klares Rollenverständnis

Stakeholder-Interessen	Rollen
Strateg. Ausrichtung	HORN & COMPANY Projektteam & interne Organisation
Handhabbarkeit	
Wirtschaftlichkeit	
BaFin-Tauglichkeit	2nd Opinion: WP

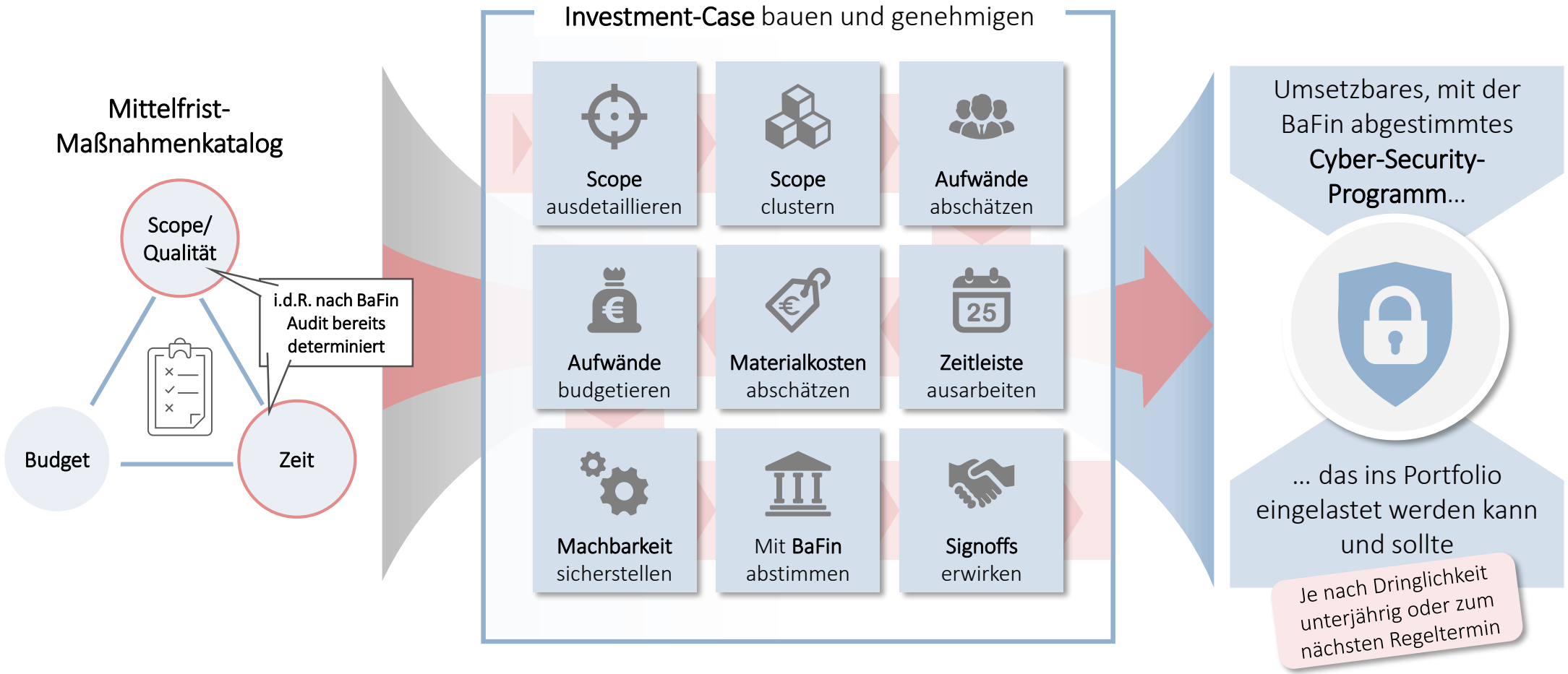
Kernaktivitäten der 2nd Opinion

- Support bei der inhaltlichen Bewertung von BaFin-Feststellungen
- Unterstützung bei der Definition von Maßnahmen und Liefergegenständen
- Konsultation bei Priorisierungsfragen im Rahmen der Abarbeitung der Maßnahmen
- Kernaufgabe der 2nd Opinion ist Abnahme von Maßnahmen u. Liefergegenständen („Soll-Ergebnisse“)
- Zudem sichert die 2nd Opinion die Fortschritts- und ggf. erforderliche Fertigmeldung an die BaFin ab

Checks & Balances: Die 2nd Opinion sichert Qualität der Endprodukte für die BaFin ab

Business-Case verhindert ausufernde Cyber-Kosten u. schleichende Scope-Erodierung

Problemfeld „Projektkosten und Scope-Creep“



Jede nachträgliche Änderung am Business-Case erfolgt ausschließlich via Change Requests gemäß eines definierten Change Frameworks

Gezieltes Erwartungsmanagement vermeidet Revisions-BaFin-„Überraschungen“

Regelmäßiges Austauschformat mit BaFin zum Umsetzungsstand

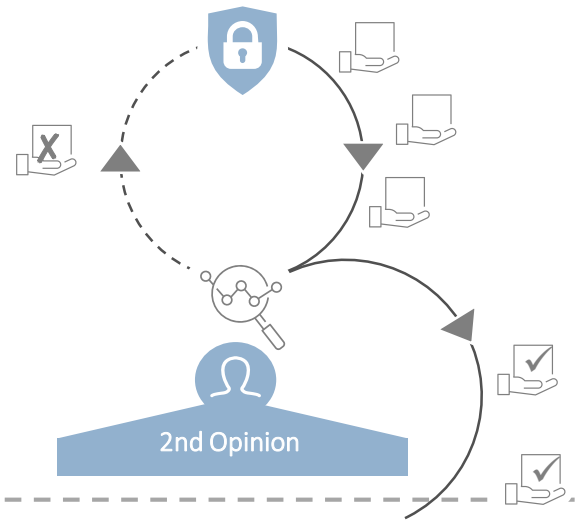
Laufende Umsetzung Cyber-Security-Programm

Regelmäßiges Austauschformat mit Revison/ BaFin

Falls rein vorbeugend gehandelt wird (Self-Assessment), ist BaFin-Austausch optional

Kontinuierliche Lieferkontrolle durch 2nd Opinion

Cyber-Security-Programm



In Gesprächen mit BaFin zur Umsetzung von Anforderungen…

… mögliche Hürden frühzeitig adressieren…

… und Feedback sowie Lösungen diskutieren

Freigabe durch 2nd Opinion

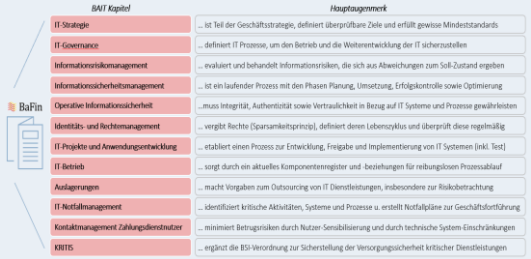
Formale „Fertig“-Meldung von Ergebnissen

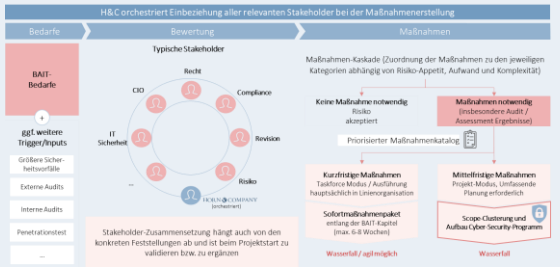
Prüfung und Freigabe

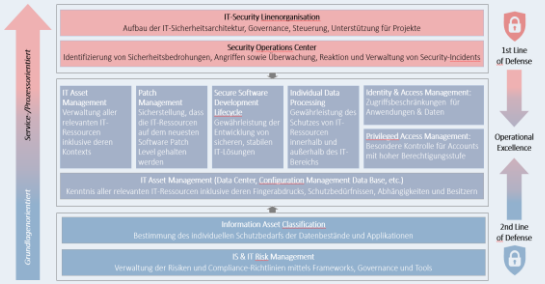
Austausch mit der BaFin nutzen, um Anpassungsbedarfe frühzeitig zu erkennen, Umsetzungsaufwände auf passendem Niveau zu halten und Cyber-Security-Programm schneller abzuschließen

Wir orchestrieren Ihren BAIT-Compliance-Prozess von Anfang bis Ende

E2E-Begleitung durch H&C und Euvic







1

BAIT Self-Assessment

Wir begleiten das BAIT Self-Assessment mit unserer fachlichen Expertise und ordnen die Ergebnisse in den Kontext des Gesamtunternehmens ein

2

Bewertung und Priorisierung

Wir moderieren die Priorisierungs-Workshops mit Stakeholdern, definieren einen abgerundeten Katalog zur Umsetzung aller Maßnahmen und koordinieren die Investment-Case-Erstellung für die Umsetzung

3

Umsetzung

Wir steuern den Aufbau eines Cyber-Security-Programms für die Umsetzung der einzelnen Maßnahmen und steuern den gesamten Programm-Lebenszyklus vom Kick-Off bis zum Closing

Wir offerieren als ganzes oder in Teilen die wesentlichen Cybersecurity Services

Wesentliche Kompetenzfelder

Kompetenzfelder Cyber

IT Network Security

- LAN, WAN und Internet
- Remote Access, Secure Cloud Connectivity
- Cybersecurity as-a-service

Public Cloud Security

- Public Cloud Security Posture Management
- Cloud Workload Protection
- Azure/GCP/AWS

Modern Workplace Security

- Sicheres Remote-Arbeiten
- Endpoint Security (inkl. EDR)
- Secure BYOD, Mobile Devices Management

Infrastruktur

OT/IoT Infrastructure Security

- OT Network Segmentierung
- Asset und Vulnerability Management
- Threat Detection, Secure OT Access

Cloud-Lösungen

Private Cloud Security

- Virtual Environment…
- … inkl. VM und Container
- SDDC Security

Work Support

Cybersecurity Operations

- Support für Arbeit von Security Teams…
- … z.B. SIEM, SOAR
- Threat Modellierung, Risikoanalyse

H&C und EUVIC decken die volle Spannbreite an Cybersecurity Services bis hin zur Unterstützung durch ein Security Operations Center ab

Wir strukturieren über unseren „CyberExpress“-Framework Ihre Cyber-Diskussion

CyberExpress Framework

CyberExpress Self-Assessment

Diagnose:

- Identifizierung des Geschäftskontexts
- Identifizierung von Cyber-Bedrohungen und -Risiken
- Planung von Mitigation von Cyberrisiken
- Sicherheitsbewertung der Infrastruktur-konfiguration und -scoring

Level1 „Basic Control“	▪ Cybersecurity Asset Management & Vulnerability Management ▪ Basis-Endpunktsicherheitslösung ▪ Netzwerksegmentierung und Traffic Control
Level2 „High Control“	▪ Netzwerkzugriffskontrolle ▪ Logmanagement & Audittrail ▪ DNS Sicherheitslösung
Level 3 „Full Control“	▪ Netzwerk- und Endpunkt-Erkennungs- und -Antwortsysteme (NDR& EDR) ▪ Erweiterte Protokollverwaltung und Ereigniskorrelation ▪ Automatisierung von Sicherheitsvorgängen

CyberExpress Self-Assessment wurde als Antwort für die heutigen Bedrohungen und Bedürfnisse in der Infrastruktur-Cybersecurity entwickelt – speziell für Organisationen mit kritischer Infrastruktur

Wir unterstützen punktuell (Standardtechnologien) und ganzheitlich (SOC)

Leistungsspektrum

Von spezifischen Cyber-Technologien …

… bis hin zum Security Operation Center (SOC)

Zur Erzielung bestmöglicher Ergebnisse für unsere Kunden unterstützen wir bei Einsatz von gängigen Cybersecurity-Lösungen …

… bis hin zur Übernahme der Cyber-Aktivitäten. Entsprechende Zertifizierungen, wie z.B. ISO 9001, ISO 14001 oder ISO 27001 liegen vor

Im Rahmen der Leistungserbringung verfügen wir über einen Pool an Cyber-Expertinnen, um alle Bedarfe aus einer Hand abdecken zu können

Wir stehen für Sie als Ansprechpartner zur Verfügung!

Kontaktdaten

HORN COMPANY

EUVIC

Dr. Oliver Laitenberger

Geschäftsführender Partner

oliver.laitenberger@horn-company.de
Telefon: +49 162 2726 009

Dr. Christoph Hartl

Partner

christoph.hartl@horn-company.de
Mobil: +49 162 2726 024

Dr. Carsten Woltmann

Associate Partner

carsten.woltmann@horn-company.de
Mobil: +49 162 2726 043

Marcin Wojtaszek

CTO Euvic

marcin.wojtaszek@euvic.com
Telefon: +49 214 84054966

HORN & COMPANY

Internationale Top-Management-Beratung

DÜSSELDORF | BERLIN | FRANKFURT | HAMBURG | KÖLN | MÜNCHEN | NEW YORK | SINGAPUR | WIEN