more security. usd

SECURITY CONSULTING

Wir verankern Informationssicherheit ganzheitlich in Ihrem Unternehmen.

WAS UNS WICHTIG IST

„Viele denken bei dem Begriff Cyber Security spontan an komplexe Technik, unklare externe Vorgaben und nicht budgetierten Mehraufwand. Sie spüren die Bedrohung und befürchten gleichzeitig, dass sie in ihren IT-Projekten wertvolle Zeit verlieren. Wir müssen gemeinsam diesen scheinbaren Widerspruch auflösen. In einen Rennwagen baut man die besten Bremsen schließlich auch nicht, um zum Stillstand zu kommen, sondern um schneller zu fahren.

Cyber Security wird zum trivialen Teil der Digitalisierung unserer Welt. Es beginnt mit der Awareness des Managements und motivierten Expertinnen und Experten. Technische Kompetenz, beste Tools und eine effiziente Organisation sind unabdingbar. Lassen Sie uns zusammenarbeiten. Gemeinsam sind wir besser und Ihr Business wird schneller."

Andrea Tubach
Head of Security Consulting

UNSERE BERATUNGSSCHWERPUNKTE

Unsere Beraterinnen und Berater stehen Ihnen effizient und passgenau zur Seite. Beginnend bei der Entwicklung einer für Ihr Unternehmen passenden Cyber Security Strategie, den daraus resultierenden Leitlinien, Prozessen und Organisationsstrukturen ihres ISMS bis hin zum operativen Betrieb Ihrer Sicherheitsorganisation. Unsere Fokusthemen sind dabei:

CYBER SECURITY STRATEGIE

Wir arbeiten mit Ihnen aus, wie Informationssicherheit konkret einen Mehrwert für Ihre Organisation schafft. Basierend auf Ihrer Unternehmens- und IT-Strategie entwickeln wir im Rahmen unseres 5-Phasen-Modells die passende Cyber Security Strategie für Ihren Unternehmenserfolg.

INFORMATIONSSICHERHEIT IM FINANZWESEN

Wir kombinieren Branchen-Know-how zu regulatorischen Anforderungen wie bspw. MaRisk oder BAIT mit Expertenwissen aus der Informationssicherheit und beraten Sie zu Fragestellungen aus der 1st oder 2nd Line-Of-Defense.

ISMS / ISO 27001 BERATUNG

Wir begleiten Sie beim Aufbau und der Optimierung Ihrer Managementsysteme zur Informationssicherheit – von der Konzeption notwendiger Organisationsstrukturen, über Definition der Prozesse bis hin zur Erstellung notwendiger Dokumentationen.

CYBER SECURITY STRATEGIE

SCHUTZ IHRER UNTERNEHMENSWERTE.
ENABLER DIGITALER TRANSFORMATION.

Mit voranschreitender Digitalisierung von Geschäftsprozessen ist die Bedeutung von Cyber Security zum Schutz von Unternehmenswerten kaum mehr in Frage zu stellen. Neben dieser essentiellen Rolle muss Cyber Security heute aber auch zunehmend als Enabler digitaler Transformation im Unternehmen fungieren. Denn nur, wenn sie richtig verankert ist, können Innovationen zügig und sicher realisiert werden.

„Ihre Cyber Security Strategie hat den Spagat zwischen dem Schutz des Vorhandenen und der Sicherung neuer Prozesse durch Innovationen und Agilität zu meistern. Eine spannende Herausforderung. Wir freuen uns, Sie auf diesem Weg zu begleiten."

Andrea Rupprich
Managing Consultant

Dr. Christian Schwartz
Managing Consultant

IHR WEG ZUR CYBER SECURITY STRATEGIE

Wir arbeiten mit Ihnen aus, wie Informationssicherheit konkret einen Mehrwert für Ihre Organisation schafft. Basierend auf Ihrer Unternehmens- und IT-Strategie entwickeln wir im Rahmen unseres 5-Phasen-Modells die passende Strategie für Ihren Unternehmenserfolg.

Phase 1

Identifikation Ihrer Unternehmenstreiber für Cyber Security

Ausgehend von Ihrer Unternehmens- und IT-Strategie identifizieren wir in dieser Phase Ihre Treiber für Cyber Security. Wir beziehen dabei Ihre zu schützenden Kronjuwelen, vorhandene Compliance-Vorgaben, geltende gesetzliche Regularien und Ihre Markttreiber mit ein. So entsteht das Fundament für das Mission Statement Ihrer Cyber Security Strategie, das den Rahmen für die weiteren Phasen bildet.

Phase 2

Ermittlung Ihres Risikokontextes

In dieser Phase wird, beruhend auf Ihren identifizierten Werten und Assets, der hierzu korrespondierende Risikokontext bestimmt. Dabei betrachten wir typische Bedrohungsszenarien und Angriffsprofile mit den Dimensionen Angreifer, Motivation und Methodik. Zudem werden Vorfälle aus der Vergangenheit und Ihre Prädisposition in Betracht gezogen. Diese Ergebnisse verbunden mit Ihrem sogenannten Risikoappetit bilden die Grundlage für die Priorisierung von späteren Handlungsfeldern zur Umsetzung.

Phase 3

Durchführung eines Cyber Security Checks

Basierend auf Ihrem Risikokontext und den für sie geltenden Regularien, Vorgaben oder Industry Best Practices (wie bspw. ISO/IEC 27001/2, CIS Standard, NIST CSF oder die CMMC) führen wir eine Gap-Analyse – einen sogenannten Cyber Security Check – durch. So erhalten wir einen Überblick über vorhandene Lücken (Gaps). Ausgehend von diesen Ergebnissen führen wir eine Risikoanalyse durch. Diese umfasst eine Abschätzung potentieller Schäden in Bezug auf den Verlust der Vertraulichkeit, Integrität oder Verfügbarkeit von Informationswerten sowie eine Evaluierung relevanter Risikoszenarien hinsichtlich der identifizierten Gaps.

Phase 4

Ableitung relevanter Handlungsfelder

In dieser Phase zeigen wir Ihnen basierend auf den Erkenntnissen der vorangegangenen Schritte gezielt strategische Handlungsfelder der Informationssicherheit auf. Sie können prozessualer, technischer oder organisatorischer Natur sein. Diesen Handlungsfeldern werden konkrete Ziele und Maßnahmenpakete zugeordnet, die schließlich einer Priorisierung über eine Aufwand-Wirkungs-Betrachtung unterzogen werden. Handlungsfelder ergeben sich individuell aus ihrem speziellen Unternehmenskontext. Beispielhafte Felder sind Schwachstellen- und Incidentmanagement, Security Awareness, Identity- und Accessmanagement sowie Governance im Bereich der Informationssicherheit.

Phase 5

Finalisierung der Cyber Security Strategie

In der letzten Phase werden die Ergebnisse der vorangegangenen Schritte in Ihrer Cyber Security Strategie konsolidiert und mit allen Stakeholdern in Ihrem Unternehmen abgestimmt. Ziel ist die finale Freigabe zur Umsetzung. Damit haben Sie die Grundlage zur Initiierung Ihres Cyber Security Programms gelegt. Gerne unterstützen wir Sie darüber hinaus beratend bei der Umsetzung Ihres Programms.

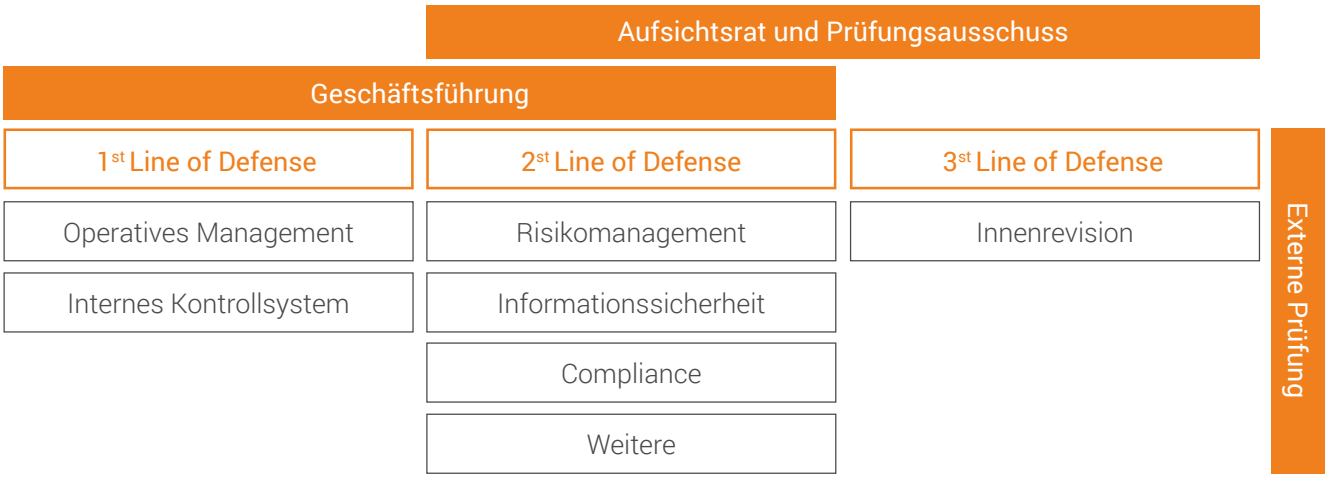
INFORMATIONSSICHERHEIT IM FINANZWESEN

RISIKOBEWUSSTSEIN SCHÄRFEN. STRATEGIEN ENTWICKELN.

Dr. Christian Schwartz
Managing Consultant

„Eines der zentralen Ziele der regulatorischen Anforderungen durch die BaFin ist das Sicherstellen von effektivem Risikomanagement. Zur Umsetzung der stetig steigenden Anforderungen wird immer größerer personeller, organisatorischer und technologischer Aufwand notwendig. Gemeinsam mit unseren Kunden erarbeiten wir Cyber-Security-Strategien, definiere langfristige Ziele und begleite die Harmonisierung mit neuen finanzregulatorischen Anforderungen."

Das Thema IT-Sicherheit stellt einen aufsichtsrechtlichen Schwerpunkt dar. Ein Ziel dieses Vorgehens ist es, die IT-Sicherheit im Markt zu erhöhen und das Risikobewusstsein für Informationssicherheit der betroffenen Unternehmen zu schärfen. Zur Identifikation und Steuerung von Risiken hat sich das 3 Lines-of-Defense-Modell etabliert. In unserer Arbeit spezialisieren wir uns auf Beratung und Unterstützung der 1st und 2nd Line-of-Defense.



Basierend auf "Guidance on the 8th EU Company Law Directive", FERMA / ECIIA (2010), erweitert durch usd AG

ANFORDERUNGEN DER BaFin

Die Anforderungen enthalten einen adaptiven und praxisorientierten Rahmen für die technisch-organisatorische Gestaltung der IT. Mit einem Fokus auf das Management der IT-Ressourcen und auf das Risikomanagement der Informationssicherheit bringen sie nicht unerhebliche Anpassungen der internen Organisationsstruktur mit sich.

Je nach Kontext des regulierten Institutes, beraten wir bei der Umsetzung gemäß:

BAIT	Bankaufsichtliche Anforderungen an die IT
KAIT	Kapitalverwaltungsaufsichtliche Anforderungen an die IT
ZAIT	Zahlungsdiensteaufsichtliche Anforderungen an die IT
VAIT	Versicherungsaufsichtliche Anforderungen an die IT

ISMS / ISO 27001 BERATUNG

GEZIELTES MANAGEMENT IHRER INFORMATIONSSICHERHEIT.

Die Sicherheit von Informationen ist heute elementare Voraussetzung des Unternehmenserfolges, sind Informationen doch Bestandteil nahezu aller Transkationen eines Unternehmens. Ein ganzheitlicher Ansatz zum Management der Informationssicherheit ist notwendig.

Ein sogenanntes Informationssicherheitsmanagementsystem definiert die Regeln und Methoden für ein ganzheitliches Geschäfts- und IT-Sicherheitsmanagement, um Vorgehensweisen zur Informationssicherheit zu initiieren, konkrete Maßnahmen durchzuführen, diese zu überwachen und fortlaufend zu verbessern.

Maximilian Müller
Managing Consultant

„Der Einstieg erfolgt typischerweise über einen ISMS Scope Workshop oder einer Gap Analyse. Diese Workshops zu Beginn sind wichtig, um den Umfang und Aufwand eines ISMS-Implementierungsprojekts besser schätzen zu können."

AUFBAU UND PFLEGE IHRES ISMS

„Egal ob Ihr Unternehmen noch ganz am Anfang steht oder bereits erste Maßnahmen umgesetzt hat, ich begleite Sie in jeder Phase im Bereich der Informationssicherheitsmanagementsysteme. Ich freue mich, dass ich Sie mit meinem Fachwissen hier ganz konkret unterstützen kann."

Ester Widera
Senior Consultant

1. ISMS

Definition der relevanten ISMS-Prozesse auf Basis von Best-Practices, angepasst an Ihr Unternehmen

2.

Unterstützung der 1st und 2nd Line-of-Defense, z.B. bei der Erstellung von Richtlinien oder Auswahl von Maßnahmen

3.

Überprüfung der Umsetzung definierter Vorgaben im Rahmen von Kontrollhandlungen

4.

Identifizierung von Verbesserungspotentialen und Umsetzung von Maßnahmen zur kontinuierlichen Verbesserung des ISMS

INTERNES AUDIT NACH ISO 27001

Mit einem internen Audit nach ISO/IEC 27001:2013 prüfen wir den Reifegrad Ihres ISMS – als Vorbereitung und Voraussetzung für Ihre erfolgreiche Zertifizierung.

VIRTUAL ISO

BEDARFSGERECHTE UNTERSTÜTZUNG

Mit dem usd Virtual Information Security Office erhalten Sie maßgeschneiderte und effiziente Unterstützung im Management ihrer Informationssicherheit.

Basierend auf den für Sie geltenden regulatorischen Anforderungen und Industry Best Practice Standards stellen wir Ihnen die passende Organisation samt Services zur Verfügung. Mit ernanntem Information Security Officer auf unserer Seite oder als reines Security Office mit unterstützendem Service für Ihre eigene ISO Organisation. Schwerpunkte bilden die strategische Entwicklung der Informationssicherheit sowie Weiterentwicklung und Verbesserung des Informationssicherheitsmanagementsystems. Benötigtes Know-how muss so nicht selbst aufgebaut werden – unser Team bringt gebündelte Cyber Security Expertise und aktuelle Qualifizierungen mit.

Andreas Borgwart
Managing Consultant

„Mit unserem Virtual ISO unterstützt Sie gleich ein ganzes Team aus hochqualifizierten Sicherheitsexpert*innen – mit einer festen Ansprechperson für Sie. Wir freuen uns, Ihnen mit unseren jahrelangen Erfahrungen in ISMS Projekten zur Seite zu stehen."

UNSERE SECURITY CONSULTANTS

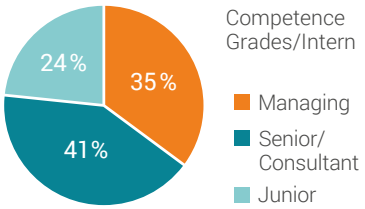
Wir sind ein flexibles und interdisziplinäres Team bestehend aus erfahrenen Managing Consultants, Senior Consultants und engagierten Junioren. Unser Team kombiniert Branchen-Know-how mit Expert*innenwissen aus der Informationssicherheit. Gemeinsam treibt uns an, Sicherheit ganzheitlich im Unternehmen zu verankern.

Unsere Erfahrungen und unser Know-how bringen wir in diversen Veröffentlichungen, Lehraufträgen, Forschungsprojekten und Fachgruppen ein. Wir sind unter anderem Gründungsmitglied des CAST Forums, Partner des ATHENE und engagieren uns in verschiedenen Fachgruppen der ISACA.

WAS WIR MITBRINGEN

ERFAHRUNG

Unsere Beraterinnen und Berater bringen mehrjährige Erfahrung in relevanten Informationssicherheitsprojekten mit. Neben Erfahrungen im Finanzwesen verfügen wir über Branchenexpertise im Tourismus und Handel. Unser Fachwissen in der Informationssicherheit wird mit Projektmanagement Know-how abgerundet.



UNSERE ZERTIFIZIERUNGEN

- CISA (Certified Information Security Auditor)
- CISM (Certified Information Security Manager)
- CRISC (Certified in Risk and Information Systems Control)
- CISSP (Certified Information Systems Security Professional)
- ISO 27001 Lead Auditor
- CompTIA Security+
- ITIL v3 Foundation
- IT-Sicherheitsbeauftragter für öffentliche Verwaltung
- PMP (Project Management Professional)
- Prince2 Foundation
- Qualys Certified Specialist (Vulnerability Management)
- QSA (Qualified Security Assessor)
- Scrum Master
- Zertifizierter Wirtschaftsschutzbeauftragter
- IHK Fremdsprachenkorrespondent
- IHK Zertifizierter Projektleiter
- PECB Certified ISO 22301 Implementer (Themengebiet des BCMS)

WEITERENTWICKLUNG

„Neben einem strukturierten, fachlichen Onboarding-Programm für unsere neuen Kolleginnen und Kollegen investieren wir fortlaufend in unsere Weiterbildung und die Erreichung international anerkannter Zertifizierungen."

Dr. Richard Grewe
Managing Consultant

WIR SCHÜTZEN UNTERNEHMEN VOR HACKERN UND KRIMINELLEN.

ÜBER DIE usd AG

So dynamisch und vielfältig wie die Bedrohung, ist unsere Arbeit. Als akkreditierter Auditor beraten und zertifizieren wir Unternehmen nach den Vorgaben der Kreditkartenindustrie und weiterer IT-Sicherheitsstandards weltweit. Die Expert*innen des usd HeroLabs identifizieren Schwachstellen in IT-Systemen und Applikationen. Unsere Security Consultants beraten Unternehmen ganzheitlich in Fragen der Informationssicherheit, des Risikomanagements und der IT-Compliance. Wir tragen Verantwortung, die Cyber Security Transformation Academy (CST Academy) fördert Austausch und Wissenstransfer in der Community. more security ist unsere Mission.

UNSERE KUNDEN

Seit über 25 Jahren beraten wir internationale Unternehmen verschiedener Branchen in Fragen der Informationssicherheit, vom Start-up bis zum Großkonzern. Dabei ist unsere Zusammenarbeit geprägt von gegenseitigem institutionellem und persönlichem Vertrauen und langfristigen Partnerschaften.

REFERENZEN

Sie haben Fragen oder Interesse?
Sprechen Sie mich gerne an.

Felix Schmidt
usd Team Lead Sales
Security Consulting

Telefon: +49 6102 8631-190
E-Mail: vertrieb@usd.de
www.usd.de

usd AG
Frankfurter Str. 233, Haus C1
63263 Neu-Isenburg