valantic

NIS2 - endlich mal ein vernünftiges Gesetz?

Informationen sicher(er) und gesetzeskonform verarbeiten!

Thomas Lang

Fiberdays, 3. April 2025

Agenda

1. Hintergründe & aktueller Status
2. Warum NIS2 „vernünftig“ ist
3. Praktische Handreichungen für die Umsetzung
4. Q&A

Hintergründe & aktueller Status

Sektoren

Seit 2016 NIS1 / KRITIS

Bankwesen

Trinkwasser

Energie

Gesundheits-
wesen

Anbieter digitaler
Dienste

Digitale Infrastruktur

Verkehr

NIS2

Zusätzlich seit NIS2

Verwalter von
IKT-Diensten

Anbieter öffentl.
Netze & Kommuni-
kationsdienste

Öffentliche
Verwaltung

Weltraum

Produktion &
Verarbeitung
(Lebensmittel,
Medizin, chem.
Stoffe)

Forschung

Post und
Kurierdienst

Abfall- und Ab-
wasserwirtschaft

Die Richtlinie **weitet den Geltungsbereich** ihrer Vorgänger-Version erheblich aus. Zahlreiche weitere Branchen gelten nun als „kritischer Sektor“.

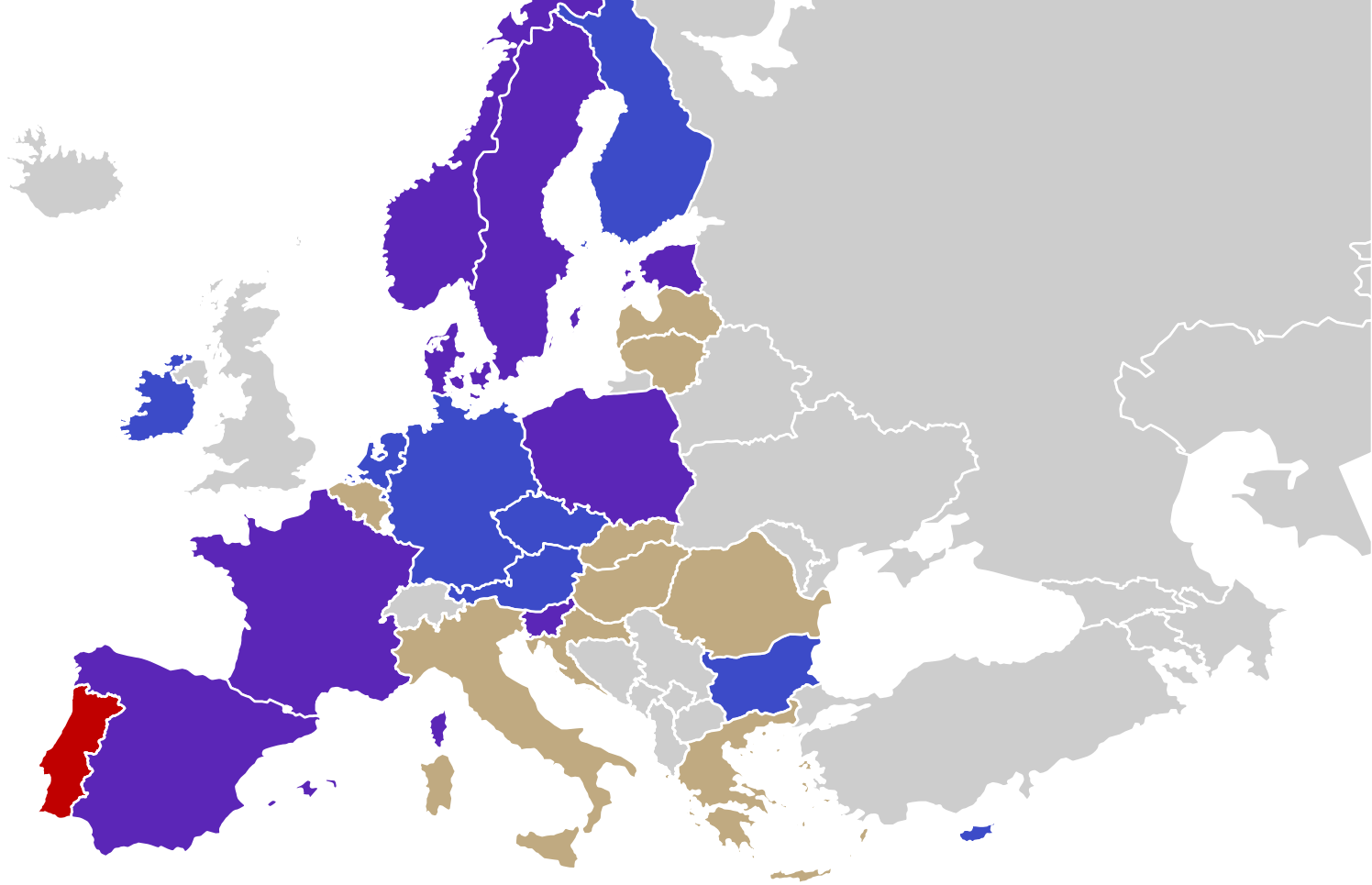
Unternehmen, die in mindestens einen der genannten Sektoren fallen, sind von der Richtlinie erfasst, wenn sie der Größe nach als **„mittleres Unternehmen“** einzustufen sind.

Die European Union Agency for Cybersecurity (ENISA) übernimmt die Aufgabe, ein **EU-weites Register aller von der NIS-2-Richtlinie erfassten Einrichtungen** im Bereich digitale Infrastruktur zu schaffen und zu pflegen.

Die Herausforderung liegt in einer rechtlich belastbaren Auslegung der teilweise schwer verständlichen Definitionen.

NIS2: Status und Ausblick

#	In nat. Recht umgesetzt
1	Belgien
2	Kroatien
3	Griechenland
4	Ungarn
5	Italien
6	Littauen
7	Lettland
8	Slowakei
9	Rumänien



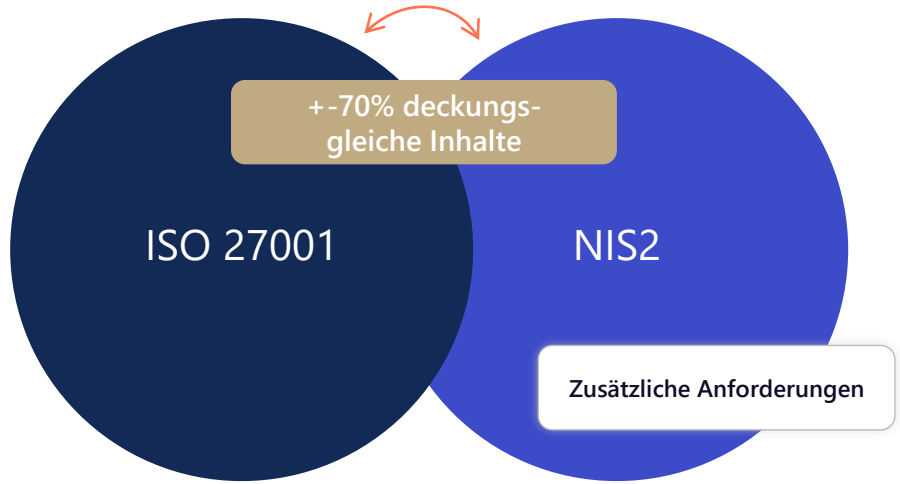
Status
In nationales Recht umgesetzt
Gesetzesvorlage liegt vor
Anhörungsphase
Keine Entwicklung

Warum NIS2 „vernünftig“ ist

Das Ziel der NIS2 Richtlinie

> (…) gemeinsames Cybersicherheitsniveau sicherstellen, um so das Funktionieren des Binnenmarkts zu verbessern.

Altbekanntes und sinnvolle Ergänzungen



Zusätzliche Anforderungen
Berichterstattung über Cybersicherheitsvorfälle und Management von Schwachstellen
Pflichten der Geschäftsleitung
Gewährleistung von Lieferkettensicherheit
Kontinuierliches Risikomanagement

Gegenüberstellung NIS2 vs. ISO 27.001

#	Bereich	NIS2-Richtlinie	NIS2 Kapitel	ISO 27001	ISO 27001 Kapitel
1	Risikomanagement und Cybersicherheitsmaßnahmen	- Technische und organisatorische Maßnahmen - Regelmäßige Risikoanalysen und Sicherheitsaudits - Patch-Management - Netzwerk- und Systemsicherheit - Zugriffskontrolle und Authentifizierung - Verschlüsselung sensibler Daten	Artikel 21	- Risikobasierter Ansatz für ISMS - Regelmäßige Risikobewertungen - Sicherheitskontrollen basierend auf Risikoanalysen - Kontinuierliche Verbesserung des ISMS	6. Planung 8. Betrieb
2	Incident Response und Meldepflichten	- Incident-Response-Pläne - Meldung schwerwiegender Vorfälle innerhalb von 24 Stunden - Bereitstellung von Erst-, Zwischen- und Abschlussberichten	Artikel 23, 24	- Incident-Management-Prozesse - Keine spezifischen Zeitvorgaben für Meldungen - Fokus auf interne Prozesse zur Behandlung von Vorfällen	A.16 Informations-sicherheitsvorfälle
3	Governance und Compliance	- Einrichtung eines Cybersecurity-Risikomanagement-Systems - Einbeziehung der Unternehmensleitung - Einhaltung branchenspezifischer Standards	Artikel 21	- Etablierung eines ISMS - Verpflichtung des Top-Managements - Fokus auf allgemeine Best Practices der Informationssicherheit	5. Führung 9. Bewertung der Leistung
4	Supply Chain Security	- Bewertung von Risiken in der Lieferkette - Überprüfung der Sicherheitsmaßnahmen von Lieferanten	Artikel 21(2)(d)	- Lieferantenbeziehungen als Teil des ISMS - Weniger spezifische Anforderungen an die Lieferkette	A.15 Lieferantenbeziehungen
5	Informationsaustausch und Kooperation	- Verpflichtender Informationsaustausch mit Behörden und anderen Unternehmen - Teilnahme an sektorübergreifenden Übungen	Artikel 29	- Keine spezifischen Anforderungen zum externen Informationsaustausch - Fokus auf interne Kommunikation und Bewusstseinsbildung	7.4 Kommunikation
6	Dokumentation und Nachweis	- Dokumentation aller Sicherheitsmaßnahmen - Nachweis der Einhaltung gegenüber Aufsichtsbehörden	Artikel 21(2)	- Umfangreiche Dokumentationsanforderungen für das ISMS - Möglichkeit zur Zertifizierung durch akkreditierte Stellen	7.5 Dokumentierte Information
7	Sektorspezifische Anforderungen	- Detaillierte Anforderungen für bestimmte Sektoren (z.B. Energie, Gesundheit) - Unterscheidung zwischen "wesentlichen" und "wichtigen" Einrichtungen	Anhänge I und II	- Branchenneutrale Anforderungen - Anpassbar auf spezifische Organisationskontexte	4. Kontext der Organisation

Praktische Handreichungen für die Umsetzung

NIS2 Readiness – mit System

- Prüfung des Anwendungsbereichs der NIS2
- Verortung der Sektoren
- Rechtliche Prüfung

- Untersuchung aktueller Status
- GAP-Analyse
- Identifizierung offener Handlungsfelder

- Erstellung eines Reifegrad-Reports
- Ermittlung von Handlungsempfehlungen
- Umsetzungsplanung

- Implementierung identifizierter Maßnahmen
- Training & Awareness
- Kontakt zu Behörden

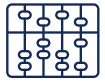
Fokusbereiche der Implementierung

Cyber Strategy & Governance

- Stärkung des Informations-sicherheitsmanagements
- Förderung einer Bewusstseinskultur und Durchführung umfassender Schulungen
- Etablierung robuster Protokolle für Cyber-Risikomanagement und Compliance

Detection & Response

- Verbesserung der Fähigkeiten zur Vorfallsbearbeitung, um schnell auf Cybersicherheitsvorfälle reagieren zu können
- Sicherstellung zeitnaher und präziser Vorfallsmeldeverfahren
- Entwicklung umfassender Strategien für Geschäftskontinuität und Krisenmanagement



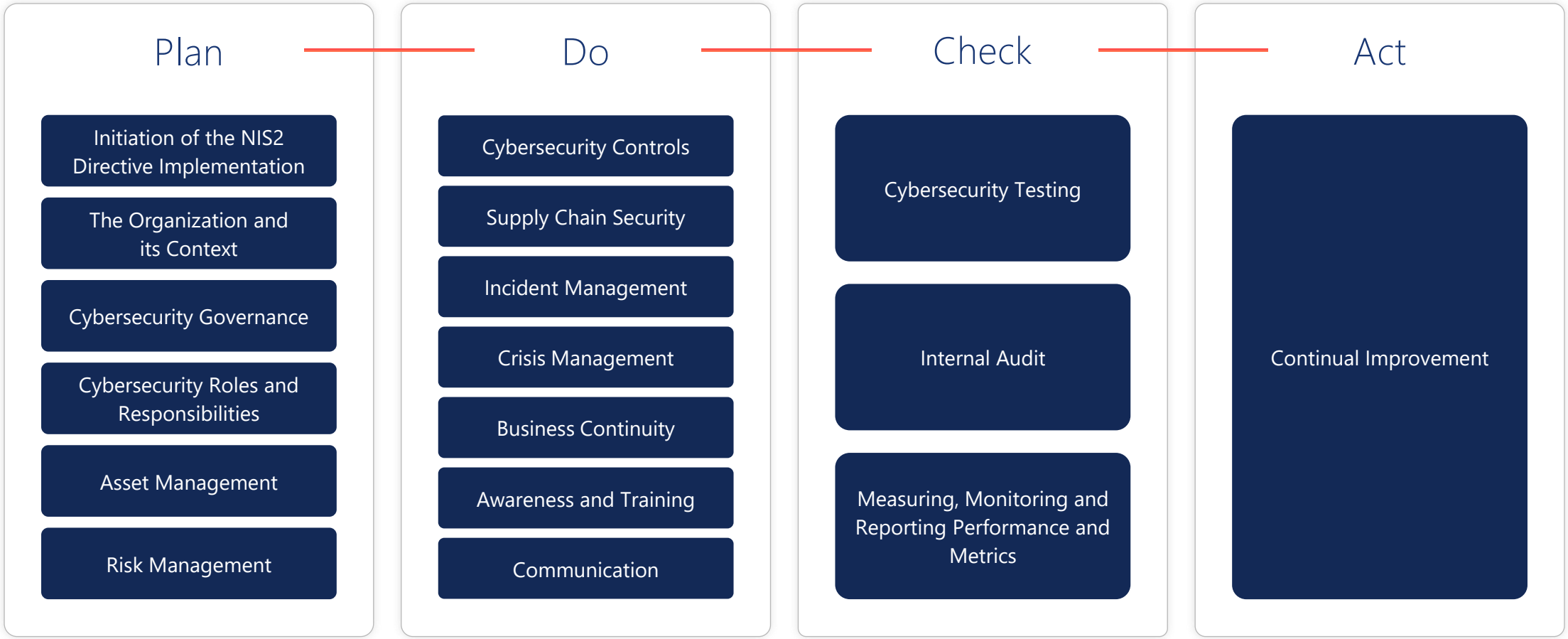
Infrastructure & Application Security

- Implementierung fortschrittlicher Maßnahmen zur Sicherung der Infrastruktur und des Netzwerks
- Vorgabe sicherer Entwicklungspraktiken für Anwendungen und Software
- Verbesserung der Identitäts- und Zugriffskontroll-mechanismen
- Management der Risiken im Zusammenhang mit Beziehungen zu Dritten

Da die endgültige Fassung der NIS-2-Gesetzgebung Gestalt annimmt, sollte proaktiv Maßnahmen geplant werden, um die Richtlinie einzuhalten. Zu den ersten zu berücksichtigenden Schritten gehören:

- Implementierung eines robusten Informationssicherheits-Managementsystems (ISMS) auf Basis von ISO/IEC 27001, das die NIS-2-Anforderungen und andere relevante Spezifikationen berücksichtigt.
- Expertenberatung bei der Implementierung von Sicherheitskontrollen zur Stärkung der Cybersicherheit des Unternehmens.
- Schulungen und Sensibilisierungsveranstaltungen für den Vorstand.
- Umfassende Bewertung der Incident-Management-Fähigkeiten, um Verbesserungspotenziale zu identifizieren.

Implementation Framework



valantic

Meldepflichten nach NIS-2 im Überblick

24h

Erstanmeldung innerhalb von einem Tag

72h

Folgemeldung innerhalb von drei Tagen mit Bewertung der Erstmeldung hinsichtlich Schwerem Auswirkungen und Komprimittierung

Meldepflicht bei erheblichen Sicherheitsvorfällen für regulierte Einrichtungen gemäß NIS2

30d

Abschlussmeldung oder Fortschrittsmeldung innerhalb eines Monats mit Beschreibung, Ursachen, Maßnahmen und grenzüberschreitenden Auswirkungen

Zwischenmeldungen auf Nachfrage des BSI

Pflichten der Geschäftsleitung

Pflichten der Geschäftsleitung gemäß NIS2: Die Geschäftsleitung hat mehrere explizite Pflichten, darunter:

a) Warnungen über Verstöße gegen die Richtlinie ausgeben,

b) verbindliche Anweisungen zur Verhinderung oder Behebung von Sicherheitsvorfällen erlassen und Fristen für deren Umsetzung festlegen,

c) bestimmte Maßnahmen zur Einhaltung der Cybersecurity-Risikomanagementmaßnahmen oder Berichtspflichten anordnen,

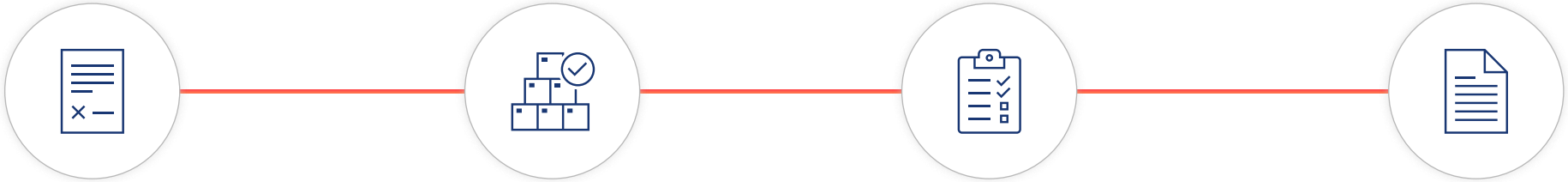
d) betroffene natürliche oder juristische Personen über signifikante Cyber-Bedrohungen informieren,

e) Empfehlungen aus Sicherheitsprüfungen innerhalb eines angemessenen Zeitrahmens umsetzen, und

f) einen respektierten Überwachungsbeauftragten benennen (intern / extern, z.B. „CISOaaS“).

g) Darüber hinaus muss die Geschäftsleitung sicherstellen, dass alle notwendigen Maßnahmen zur Cybersecurity-Risikomanagement in der Organisation umgesetzt werden.

Sicherheit in der Lieferkette



Unternehmen müssen eine **Richtlinie entwickeln**, die Sicherheits-anforderungen an ihre direkten Lieferanten und Dienstleister definiert und diese hinsichtlich ihrer Kritikalität kategorisiert.

Verträge müssen **relevante Sicherheits-anforderungen festlegen**, wie bspw. Schulung der Mitarbeiter, Meldung von Informations-sicherheitsvorfällen, Auditrechte und Schwachstellen-management.

Die Richtlinie und deren **Einhaltung muss regelmäßig überprüft** werden.

Unternehmen müssen ein **aktuelles Verzeichnis ihrer Lieferanten und Dienstleister führen**, einschließlich der bereitgestellten IKT-Produkte und -Dienste sowie Kontaktdaten.

Beispiel: Risikomanagement

Im Risikomanagement werden Assets bewertet (Schutzbedarf) und Risiken unter Berücksichtigung der Rahmenbedingungen (Bedrohungen, Schwachstellen) ermittelt, aus denen dann Maßnahmen abgeleitet werden. Zudem ist Risikomanagement ein elementarer Bestandteil eine ISMS und eines BCMS.

1 Methode / Scope

Abstimmung Vorgehensweise und Scope

- Welche Assets werden betrachtet?
- Welche Quellen zu Bedrohungen und Schwachstellen werden genutzt?
- Welche Optionen bei der Vorgehensweise in Schutzbedarfsfeststellung und Risikoanalyse werden gewählt? (Stufen im Schutzbedarf, Kappungsgrenzen etc.)

2 Basisinformationen

Ermittlung der Basisinformationen

- Asset-Liste
- Bedrohungen
- Schwachstellen
- Optional: Datenmodell und standardisierte potenzielle Risiken

3 Schutzbedarf

Ermittlung des Schutzbedarfs

- pro ausgewählten Asset gem. Scope
- Aufgrund der zu erwartenden Anzahl an Assets ist hier das größte Arbeitsvolumen im Rahmen der Analysen zu erwarten, daher empfiehlt sich hier der Einsatz der besonders effizienten erweiterten Schutzbedarfsfeststellung

4 Risikoanalyse

Risikoanalyse

- für alle Assets mit relevantem SB
- Ableitung der Risiken aus potenziellen Risiken, Bedrohungen und Schwachstellen
- Ermittlung von Eintrittswahrscheinlichkeit und Schadenshöhe
- Ableitung von Maßnahmen und deren Kosten
- Entscheidung über Maßnahmen
- Erstellung der Restrisikodeklarationen

5 Maßnahmen

Umsetzung der Maßnahmen

- Mitigation gem. Bewertung
- Anpassung des Risikoregisters
- Reporting des Maßnahmenstatus und der Risikoentwicklung

Q & A

Kontakt und Unterlagen

THOMAS LANG

Partner | Geschäftsführer

+49 171 680 4635

thomas.lang@mc.valantic.com

MEHR ERFAHREN