21. JANUAR 2026

NIS2 & KRITIS-DACHGESETZ

FÜHRUNGSVERANTWORTUNG UND OPERATIVE UMSETZUNG IN DEN IT ORGANISATIONEN VON KRANKENHAUSKONZERNEN

florian.mertl@bwiiw.com
www.bwiiw.com
+491728918803

bwiiw
but what if IT works.

ZUSAMMENFASSUNG

NIS2 (Network and Information Systems Directive 2) und das KRITIS-Dachgesetz markieren einen grundlegenden Wandel in der Verantwortung von Geschäftsführungen und Vorständen von Krankenhauskonzernen. IT-Sicherheit und Resilienz sind keine delegierbaren Technikthemen mehr, sondern explizite Führungsaufgaben mit persönlicher Haftungsrelevanz.

Beide Regelwerke verlangen nachweisbar wirksame Strukturen für den sicheren Betrieb, die Aufrechterhaltung der medizinischen Versorgung und das professionelle Management von Krisen. Dabei geht es nicht um formale Compliance, sondern um die Fähigkeit der Organisation, auch unter außergewöhnlichen Bedingungen handlungsfähig zu bleiben.

Für Geschäftsführungen bedeutet dies:
Die Verantwortung für IT- und Betriebsrisiken verbleibt auf oberster Leitungsebene.
Unzureichende Organisation, fehlende Prozesse oder nicht getestete Wiederanlaufpläne können zu persönlicher Haftung führen.
Delegation an IT oder Technik entbindet nicht von der Verantwortung für Wirksamkeit und Kontrolle.

Dieses Dokument ist keine Rechtsberatung, es bietet eine strukturierte, praxisnahe Orientierung für CIOs und IT Geschäftsführungen, um NIS2 und KRITIS-Dachgesetz nicht isoliert, sondern integriert umzusetzen. Der Leitfaden zeigt in zwei 10 Punkte Plänen, wie Governance, IT-Betrieb, Resilienz und Enterprise Architecture zusammenspielen, um regulatorische Anforderungen in echte Betriebssicherheit zu übersetzen.

Leserinnen und Leser erhalten damit einen umsetzbaren Handlungsrahmen, der Sicherheit, Verlässlichkeit und Führungssouveränität im Krankenhauskonzern stärkt.

florian.mertl@bwiiw.com
www.bwiiw.com
+491728918803

bwiiw
but what if IT works.

INHALTSVERZEICHNIS

florian.mertl@bwiiw.com
www.bwiiw.com
+491728918803

GRUNDVERSTÄNDNIS NIS2 UND KRITIS DACHGESETZ

NIS2 adressiert die Cyber- und Informationssicherheit von Einrichtungen, deren Ausfall erhebliche Auswirkungen auf Gesellschaft und Versorgung hätte. Für Krankenhäuser bedeutet NIS2 eine verbindliche Verpflichtung zu strukturiertem IT Risikomanagement, Incident Handling, Wiederanlauf und Management Verantwortung. NIS2 ist geltendes deutsches Recht und seit Inkrafttreten verbindlich (NIS-2 Umsetzungsgesetz/BSIG-Neufassung).

Das KRITIS Dachgesetz adressiert die physische und organisatorische Resilienz kritischer Infrastrukturen. Es fokussiert sich nicht primär auf IT Sicherheit, sondern auf die Aufrechterhaltung kritischer Versorgungsleistungen bei Ausfällen, Krisen und außergewöhnlichen Ereignissen. Für Krankenhäuser betrifft dies insbesondere Energie, Gebäude, Medizintechnik, Personal, Logistik und IT als betriebskritische Ressource. Das Gesetz befindet sich noch im Gesetzgebungsverfahren, die Pflichten sind jedoch inhaltlich klar definiert.

KRITERIEN ZUR BESTIMMUNG DER BETROFFENHEIT

BETROFFENHEIT NACH NIS2

Krankenhäuser gelten nach NIS2 als besonders wichtige oder wichtige Einrichtungen, wenn sie entweder als Kritische Infrastruktur eingestuft sind oder die im Gesetz definierten Größenkriterien erfüllen. Maßgeblich sind dabei die folgenden Schwellenwerte:

Besonders wichtige Einrichtungen sind Organisationen, die mindestens 250 Beschäftigte haben oder einen Jahresumsatz von über 50 Millionen Euro und zusätzlich eine Jahresbilanzsumme von über 43 Millionen Euro aufweisen

Wichtige Einrichtungen sind Organisationen, die mindestens 50 Beschäftigte haben oder einen Jahresumsatz von über 10 Millionen Euro und zusätzlich eine Jahresbilanzsumme von über 10 Millionen Euro aufweisen

Unabhängig von diesen Größenkriterien gelten Krankenhäuser, die als Kritische Infrastruktur eingestuft sind, automatisch als besonders wichtige Einrichtungen im Sinne von NIS2. Eine gesonderte Prüfung der Beschäftigtenzahlen oder Umsätze ist in diesem Fall nicht erforderlich.

florian.mertl@bwiiw.com
www.bwiiw.com
+491728918803

Für die praktische Umsetzung bedeutet dies, dass große Krankenhausgesellschaften regelmäßig unter NIS2 fallen, selbst wenn einzelne Häuser für sich genommen die Schwellenwerte nicht erreichen.

BETROFFENHEIT ALS KRITIS KRANKENHAUS

Krankenhäuser gelten als Kritische Infrastruktur, wenn sie eine wesentliche Bedeutung für die stationäre medizinische Versorgung der Bevölkerung haben und definierte Schwellenwerte überschreiten.

In der Praxis ist für Krankenhäuser insbesondere folgendes Kriterium maßgeblich:
– mehr als 30.000 vollstationäre Behandlungsfälle pro Jahr

Erreicht oder überschreitet ein Krankenhaus diesen Schwellenwert, gilt es als Betreiber Kritischer Infrastruktur.

Neben dem Schwellenwert sind qualitative Versorgungsaspekte für interne Priorisierung und Resilienzsteuerung relevant, sie ersetzen jedoch nicht die formale KRITIS-Einordnung nach BSI-KritisV.

Diese qualitativen Kriterien sind insbesondere dann relevant, wenn Krankenhäuser Teil größerer Versorgungsverbünde oder regionaler Schwerpunktversorgungen sind.

Konzernperspektive

Für Krankenhauskonzerne ist entscheidend, dass die Betroffenheit nicht ausschließlich auf Ebene einzelner Standorte bewertet werden darf. Maßgeblich ist eine konzernweite Betrachtung, da:

– einzelne Krankenhäuser innerhalb eines Konzerns KRITIS sein können, andere nicht
– Gesellschaften mit zentralen IT- oder Betriebsfunktionen eine kritische Rolle für mehrere Standorte übernehmen
– zentrale IT-Systeme und Plattformen konzernweit versorgungsrelevant sind

Unterschiedliche rechtliche Einheiten können somit unterschiedlich betroffen sein. Die Steuerung von NIS2- und KRITIS-Anforderungen muss dennoch integriert und konzernweit erfolgen, da Ausfälle zentraler IT- oder Betriebsfunktionen unmittelbare Auswirkungen auf mehrere Krankenhäuser haben können.

florian.mertl@bwiiw.com
www.bwiiw.com
+491728918803

EINORDNUNG DER 10 PUNKTE PLÄNE

Die nachfolgenden 10-Punkte-Pläne bilden den operativen Kern dieses Dokuments. Sie übersetzen die Anforderungen aus NIS2 und dem KRITIS-Dachgesetz in konkrete, umsetzbare Maßnahmen für Krankenhauskonzerne und richten sich explizit an CIOs und Führungsteams mit Steuerungs- und Umsetzungsverantwortung.

Beide Regelwerke verfolgen unterschiedliche Schwerpunkte, greifen im operativen Betrieb jedoch eng ineinander. NIS2 adressiert die Sicherheit, Stabilität und Steuerbarkeit von IT-gestützten Prozessen und Informationssystemen. Das KRITIS-Dachgesetz fokussiert die Resilienz kritischer Versorgungsleistungen, bei denen IT-Systeme, Datenflüsse und digitale Abhängigkeiten eine zentrale Rolle spielen. In der Praxis lassen sich diese Anforderungen nicht getrennt umsetzen, sondern müssen in einem integrierten Betriebs- und Steuerungsmodell zusammengeführt werden.

Die 10-Punkte-Pläne sind daher bewusst nicht als rechtliche Auslegung, sondern als praktische Arbeitsgrundlage konzipiert. Sie beantworten für jeden Themenbereich die Frage, was konkret organisatorisch, prozessual und strukturell zu tun ist, um Wirksamkeit im Betrieb zu erreichen. Der Fokus liegt auf klaren Verantwortlichkeiten, belastbaren Artefakten, getesteten Prozessen und nachvollziehbarer Entscheidungsfähigkeit gegenüber Geschäftsführung, Revision und Aufsicht.

Ziel der Pläne ist es, CIOs in die Lage zu versetzen, regulatorische Anforderungen nicht als isolierte Compliance-Aufgabe zu behandeln, sondern als Bestandteil einer professionellen IT- und Betriebsführung im Krankenhauskonzern. Richtig umgesetzt schaffen die beschriebenen Maßnahmen nicht nur Rechtssicherheit, sondern erhöhen messbar die Stabilität, Krisenfestigkeit und Steuerbarkeit der medizinischen Versorgung.

Das Dokument beschreibt Best Practise. Das Gesetz verlangt beispielsweise wirksame, angemessene Maßnahmen und Nachweisfähigkeit, konkrete technische Ausprägungen wie „immutable“ ist eine solche Best Practice, aber nicht zwingend als Wortlautpflicht seitens der Gesetzgebung.

florian.mertl@bwiiw.com
www.bwiiw.com
+491728918803

10 PUNKTE PLAN NIS2

1. **Betroffenheit und Scope festlegen:** Erstellen Sie eine konzernweit verbindliche NIS2 Scope Definition. Diese umfasst alle rechtlichen Einheiten, Standorte, IT Services und medizinisch kritischen Anwendungen. Der Scope wird durch die Geschäftsführung freigegeben und jährlich überprüft. Mindestartefakte: Dokumentierter NIS2 Scope je Gesellschaft Freigabevermerk der Geschäftsführung
2. **Konzernweite Governance etablieren:** Definieren Sie eine eindeutige Führungsstruktur für IT Sicherheit. Die Geschäftsführung bleibt verantwortlich, der CIO steuert, der CISO oder ISB verantwortet die operative Umsetzung. Eskalations- und Entscheidungsrechte sind schriftlich festgelegt. Mindestartefakte: Governance Modell Rollen und Verantwortlichkeitsmatrix
3. **Zentrales Asset Repository aufbauen:** Führen Sie ein zentrales, konzernweit verpflichtendes Asset Repository ein. Erfasst werden Applikationen, Infrastrukturen, Cloud Dienste, Netzwerke, medizinische IT Systeme, Schnittstellen und externe Dienstleister. Mindestartefakte: Zentrales Asset Verzeichnis inkl. Klassifikation nach Kritikalität
4. **Schutzbedarfsfeststellung und Risikoanalyse:** Bewerten Sie für jedes kritische Asset die Auswirkungen eines Ausfalls auf die medizinische Versorgung. Priorisieren Sie Risiken anhand von Versorgungsrelevanz, nicht technischer Komplexität. Mindestartefakte: Schutzbedarfsanalyse, Priorisierte Risikoliste
5. **ISMS wirksam etablieren:** Implementieren Sie ein ISMS als Steuerungsinstrument. Ziel ist Transparenz über Risiken, Maßnahmen und Wirksamkeit. Mindestartefakte: ISMS Rahmenwerk, Maßnahmenübersicht
6. **Wiederanlauf und Notfallpläne definieren:** Definieren Sie Wiederanlaufzeiten für alle kritischen Systeme. Legen Sie Abhängigkeiten zwischen Anwendungen, Infrastruktur und Standorten offen. Testen Sie Wiederanlauf regelmäßig. Mindestartefakte: Wiederanlaufpläne und Testergebnisse der Durchführung
7. **Backup und Restore konsequent umsetzen:** Stellen Sie sicher, dass Backups regelmäßig erstellt, geschützt und getestet werden. Offline oder immutable Backups sind für kritische Systeme verpflichtend. Mindestartefakte: Backup Konzept und Backup / Restore Nachweise
8. **Incident Management und Meldeprozesse operationalisieren:** Etablieren Sie einen 24x7 Incident Prozess. Definieren Sie klare Meldewege, Eskalationen und Entscheidungsbefugnisse. Üben Sie den Prozess realistisch. Mindestartefakte: Incident Prozessbeschreibung, Übungsprotokolle
9. **Lieferketten und Dienstleister absichern:** Bewerten Sie alle kritischen Dienstleister hinsichtlich Sicherheits- und Betriebsrisiken. Verankern Sie Mitwirkungspflichten vertraglich. Mindestartefakte: Dienstleisterbewertung, Vertragliche Regelungen
10. **Management Einbindung und Nachweisfähigkeit:** Berichten Sie regelmäßig an die Geschäftsführung über Risiken, Vorfälle und Wirksamkeit. Entscheidungen und Maßnahmen werden nachvollziehbar dokumentiert. Mindestartefakte: Managementberichte, Entscheidungsdokumentation

florian.mertl@bwiiw.com
www.bwiiw.com
+491728918803

10 PUNKTE PLAN KRITIS DACHGESETZ

1. **KRITIS Relevanz im IT Verantwortungsbereich festlegen:** Klären Sie konzernweit, welche IT und informationsverarbeitenden Systeme unmittelbar zur Erbringung kritischer Versorgungsleistungen beitragen. Der CIO verantwortet die Abgrenzung seines Wirkbereichs gegenüber Technik, Bau und medizinischem Betrieb. Mindestartefakte: Abgrenzung CIO Verantwortungsbereich KRITIS Liste IT kritischer Systeme
2. **Kritische Versorgungsprozesse IT seitig modellieren:** Modellieren Sie die kritischen Versorgungsprozesse aus IT Sicht. Ordnen Sie diesen Prozessen Applikationen, Datenflüsse, Identitätsdienste und Schnittstellen zu. Mindestartefakte: Prozess / IT Zuordnung, Applikationsabhängigkeiten
3. **IT Asset Repository für KRITIS erweitern:** Stellen Sie sicher, dass alle IT Assets mit KRITIS Relevanz vollständig erfasst sind. Dazu zählen KIS, Subsysteme, Integrationsplattformen, Netzwerke, Rechenzentren, Cloud Dienste und Identitätsinfrastrukturen. Mindestartefakte: IT Asset Repository inkl. Kritikalitätsklassifikation, dazu, saubere CMDB Dokumentation.
4. **IT bezogene All Gefahren Risikoanalyse durchführen** Bewerten Sie Risiken für IT Systeme unabhängig von ihrer Ursache. Berücksichtigen Sie Stromausfall, Netzwerkausfall, Cyberangriffe, Lieferkettenausfälle und Personalverfügbarkeit im IT Betrieb. Mindestartefakte: IT Risikoanalyse, Priorisierte IT Szenarien
5. **IT Resilienzmaßnahmen definieren:** Definieren Sie IT spezifische Resilienzmaßnahmen wie Redundanzen, geografische Trennung, Fallback Verfahren, Offline Betriebsmodi und manuelle Ersatzprozesse. Mindestartefakte: IT Resilienzmaßnahmenplan, Abhängigkeiten und Fallbacks
6. **IT Wiederanlauf und Notfallkonzepte festlegen:** Definieren Sie Wiederanlaufzeiten für alle KRITIS relevanten IT Systeme. Stellen Sie sicher, dass diese mit den medizinischen Anforderungen abgestimmt sind. Mindestartefakte: IT Wiederanlaufpläne, RTO und RPO Definitionen inkl. Business Impact Bewertungen aus dem Business Continuity Management.
7. **Integration in konzernweite Krisenorganisation:** Stellen Sie sicher, dass IT Krisenrollen, Entscheidungsbefugnisse und Eskalationspunkte klar in die konzernweite Krisenorganisation eingebunden sind. Mindestartefakte: IT Krisenrollenbeschreibung, Eskalationsschnittstellen, IT Krisenorganisation, Bereitschaften, Krisenprozesse
8. **Meldeprozesse für KRITIS relevante IT Störungen:** Definieren Sie Meldeprozesse für IT Störungen mit Versorgungsrelevanz. Stimmen Sie diese mit NIS2 Incident Prozessen ab, um Doppelstrukturen zu vermeiden. Mindestartefakte: Meldeprozess IT, KRITIS Kontaktlisten und Erreichbarkeit
9. **Test und Übung aus IT Perspektive:** Führen Sie regelmäßige IT Notfall und Wiederanlaufübungen durch. Testen Sie insbesondere Schnittstellen zwischen zentralem IT Betrieb und Klinikstandorten. Mindestartefakte: Übungspläne Testergebnisse
10. **Nachweisfähigkeit und Management Reporting:** Berichten Sie regelmäßig an Geschäftsführung und Konzernleitung über IT Risiken, Resilienzstatus und Testergebnisse. Halten Sie Entscheidungen und Abweichungen nachvollziehbar fest. Mindestartefakte: Zyklische IT KRITIS Statusberichte

florian.mertl@bwiiw.com
www.bwiiw.com
+491728918803

EINZUHALTENDE TERMINE

TERMINE NIS2

Thema	Wer ist betroffen	Frist	Bedeutung für die Geschäftsführung
Inkrafttreten NIS2 Pflichten	Besonders wichtige und wichtige Einrichtungen	Dezember 2025	Pflichten gelten unmittelbar, keine Übergangsfrist
Registrierung beim BSI	Alle NIS2 betroffenen Einrichtungen	Spätestens 3 Monate nach Eintritt der Registrierungspflicht beziehungsweise nach Eintritt der Betroffenheit	Voraussetzung für Aufsicht, Meldungen und Anordnungen
Incident Erstmeldung	NIS2 betroffene Einrichtungen	Unverzüglich, spätestens 24 Stunden nach Kenntnis bei erheblichem Sicherheitsvorfall	Frühwarnpflicht, Management muss erreichbar sein
Incident Folgemeldung	NIS2 betroffene Einrichtungen	Spätestens 72 Stunden nach Kenntnis bei erheblichem Sicherheitsvorfall	Konkretisierung von Ursache, Wirkung und Maßnahmen
Abschlussbericht Incident	NIS2 betroffene Einrichtungen	Spätestens 1 Monat nach Erstmeldung	Nachweis der Aufarbeitung und Wirksamkeit
Risikomanagement Pflichten	NIS2 betroffene Einrichtungen	Dauerhaft	Organisations und Haftungspflicht der Geschäftsführung
Management Schulungen	Geschäftsführung und Leitungsorgane	Regelmäßig	Verantwortung ist nicht delegierbar

florian.mertl@bwiiw.com
www.bwiiw.com
+491728918803

VORAUSSICHTLICHE TERMINE NACH KRITIS DACHGESETZ (STAND GESETZESENTWURF)

Fristen gemäß Regierungsentwurf, vorbehaltlich Änderungen im Gesetzgebungsverfahren.

Thema	Wer ist betroffen	Voraussichtliche Frist	Bedeutung für die Geschäftsführung
Inkrafttreten KRITIS Dachgesetz	Betreiber kritischer Infrastrukturen	Nach Gesetzesverkündung	Neue Resilienzpflichten treten in Kraft
Registrierung als KRITIS Betreiber	KRITIS Krankenhäuser	Unmittelbar nach Inkrafttreten	Startpunkt aller Folgefristen
Durchführung Risikoanalyse	KRITIS Betreiber	Innerhalb von 9 Monaten nach Registrierung	Zentrale Pflicht zur Bewertung der Versorgungsrisiken
Ableitung Resilienzmaßnahmen	KRITIS Betreiber	Parallel zur Risikoanalyse	Nachweis aktiver Vorsorgepflicht
Erstellung Resilienzplan	KRITIS Betreiber	Spätestens 9 Monate nach Registrierung	Steuerungsinstrument für Krisen
Meldung erheblicher Störungen	KRITIS Betreiber	Unverzüglich nach Eintritt	Ergänzende Meldepflicht zu NIS2
Regelmäßige Überprüfung	KRITIS Betreiber	Wiederkehrend	Dauerhafte Verantwortung der Geschäftsführung

florian.mertl@bwiiw.com
www.bwiiw.com
+491728918803

BASISTHEMEN GUTER IT BETRIEBSFÜHRUNG IM KRANKENHAUSKONZERN

Die nachfolgenden Basisthemen beschreiben die unverzichtbaren Grundlagen einer professionellen IT-Betriebsführung im Krankenhauskonzern und bilden die operative Voraussetzung für Stabilität, Entscheidungsfähigkeit und Krisenfestigkeit im regulären Betrieb wie auch im Ausnahmezustand.

1. **Incident Management:** Betreiben Sie einen 24x7 Incident Prozess. Klassifizieren Sie Störungen nach Versorgungsrelevanz. Stellen Sie Entscheidungsfähigkeit sicher. Mindestartefakte: Incident Prozess inkl. Bereitschaftsregelung.
2. **Problem Management:** Analysieren Sie strukturelle Ursachen schwerer oder wiederkehrender Incidents. Leiten Sie nachhaltige Maßnahmen ab. Mindestartefakte: Problem-Analysen, Maßnahmenverfolgung, Zeitziele pro erfasstem Problem.
3. **Change Management:** Steuern Sie Änderungen kontrolliert. Bewerten Sie Risiken vor Umsetzung. Kritische Änderungen benötigen Freigaben. Mindestartefakte: Change Prozess, Freigabeprotokolle, Change-Quoten Messung in Korrelation zu Incidents, Changes ohne Approval
4. **Eskalationsmanagement:** Definieren Sie klare Eskalationsstufen. Legen Sie fest, wann Management eingebunden wird. Mindestartefakte: Eskalationsschema, Kontaktketten
5. **Krisenmanagement:** Was konkret zu tun ist Etablieren Sie strukturierte Krisenprozesse. Stellen Sie schnelle Entscheidungsfähigkeit sicher. Mindestartefakte: Krisenhandbuch, Übungsnachweise
6. **Notfall und Wiederanlaufprozesse:** Definieren Sie Wiederanlaufprioritäten aus Versorgungssicht. Testen Sie Wiederanlauf regelmäßig. Mindestartefakte: Wiederanlaufpläne, Testergebnisse
7. **Kommunikationsprozesse:** Regeln Sie interne und externe Kommunikation in Störungen und Krisen. Mindestartefakte: Kommunikationsleitfäden, Freigaberegeln
8. **Dokumentation und Nachvollziehbarkeit:** Dokumentieren Sie Prozesse, Entscheidungen und Maßnahmen vollständig. Mindestartefakte Dokumentationsstandards Ablagestruktur
9. **Regelbetrieb und Ausnahmemodus:** Definieren Sie Umschaltpunkte zwischen Normalbetrieb und Krisenmodus. Mindestartefakte: Betriebsmodi Definition, Entscheidungsregeln

florian.mertl@bwiiw.com
www.bwiiw.com
+491728918803

ENTERPRISE ARCHITECTURE ALS ORDNUNGSRAHMEN FÜR NIS2 UND KRITIS

EINORDNUNG

NIS2 und KRITIS Dachgesetz stellen keine isolierten IT Anforderungen dar. Beide Regelwerke verlangen Transparenz über Zusammenhänge zwischen Versorgung, Prozessen, Applikationen, Daten, Infrastruktur und Betrieb. Genau hier setzt Enterprise Architecture an. Enterprise Architecture ist kein Dokumentationszweck, sondern der Ordnungsrahmen, mit dem ein Krankenhauskonzern Komplexität steuerbar macht und regulatorische Anforderungen dauerhaft operationalisiert.

WARUM ENTERPRISE ARCHITECTURE NOTWENDIG IST

Krankenhauskonzerne sind historisch gewachsen. Versorgungsprozesse, IT Landschaften und Betriebsmodelle unterscheiden sich je Standort. Ohne einen architekturbasierten Ordnungsrahmen bleiben NIS2 und KRITIS Einzelmaßnahmen ohne nachhaltige Steuerungswirkung. Enterprise Architecture verbindet fachliche Versorgungssicht mit technischer Realität.

Enterprise Architecture schafft insbesondere Transparenz über kritische Versorgungsprozesse und deren IT Abhängigkeiten, Nachvollziehbarkeit von Auswirkungen bei Ausfällen einzelner Systeme und ist eine konsistente Grundlage für Risiko, Wiederanlauf und Resilienzentscheidungen

ZENTRALE ARCHITEKTURBAUSTEINE IM KONTEXT VON NIS2 UND KRITIS

Prozess-Applikations Korrelation:

Enterprise Architecture verknüpft medizinische und administrative Prozesse mit den sie unterstützenden Applikationen. Für NIS2 und KRITIS ist entscheidend, welche Prozesse versorgungsrelevant sind und welche IT Systeme diese Prozesse ermöglichen. Diese Korrelation bildet die Grundlage für Schutzbedarfsfeststellung, Priorisierung und Wiederanlauf.

Applikations und Integrationslandkarte

Eine konsolidierte Applikationslandkarte zeigt, welche Systeme konzernweit genutzt werden, wo Redundanzen bestehen und wo kritische Single Points of Failure liegen. Integrationsplattformen und Schnittstellen werden explizit berücksichtigt, da sie häufig hochkritische Abhängigkeiten darstellen.

Übergang von CMDB zu Architektur Repository

florian.mertl@bwiiw.com
www.bwiiw.com
+491728918803

Klassische CMDBs erfassen technische Konfigurationen, reichen aber für NIS2 und KRITIS nicht aus. Enterprise Architecture erweitert diese Sicht um fachliche Bedeutung, Kritikalität und Abhängigkeiten. Ziel ist ein integriertes Architektur Repository, das operative Daten aus der CMDB mit fachlicher Kontextualisierung verbindet.

Kritikalitätsbewertung und Priorisierung

Enterprise Architecture ermöglicht eine einheitliche Kritikalitätsbewertung über Standorte hinweg. Kritikalität wird nicht technisch, sondern aus Versorgungssicht bestimmt. Daraus leiten sich Prioritäten für Schutzmaßnahmen, Wiederanlaufzeiten und Investitionen ab.

Ableitung von Wiederanlauf und Resilienz

Auf Basis der Architekturmodelle lassen sich realistische Wiederanlaufpläne erstellen. Abhängigkeiten zwischen Applikationen, Infrastruktur und Standorten werden sichtbar und können in Szenarien getestet werden. Enterprise Architecture verhindert damit theoretische Notfallkonzepte ohne Umsetzbarkeit.

Enterprise Architecture als Führungsinstrument

Für CIOs wird Enterprise Architecture zum zentralen Steuerungsinstrument. Architekturmodelle dienen nicht der Dokumentation, sondern der Entscheidungsfindung. Sie ermöglichen faktenbasierte Diskussionen mit Geschäftsführung, Medizin und Technik über Risiken, Prioritäten und Investitionen.

Mindestartefakte einer wirksamen Enterprise Architecture

Capability Map der medizinischen Versorgung, Prozess Applikations Matrix für kritische Leistungen, Applikationslandkarte mit Kritikalitätsbewertung, Abhängigkeitsmodelle zwischen IT Betrieb, Infrastruktur und Standorten in einem Architektur Repository als Single Source of Truth.

DISCLAIMER

Dieses Dokument stellt keine Rechtsberatung dar. Es dient ausschließlich als fachliche und operative Orientierungshilfe zur praktischen Umsetzung der Anforderungen aus NIS2 und dem KRITIS-Dachgesetz aus Sicht der IT- und Betriebsorganisation von Krankenhauskonzernen.

Die Inhalte basieren auf dem zum Zeitpunkt der Erstellung bekannten gesetzlichen Rahmen, veröffentlichten Gesetzestexten sowie dem aktuellen Stand der Gesetzgebung und Verwaltungspraxis. Trotz sorgfältiger Erstellung wird keine Gewähr für die Vollständigkeit, Richtigkeit oder Aktualität der dargestellten Inhalte übernommen.

Insbesondere ersetzt dieses Dokument nicht die individuelle rechtliche Prüfung durch qualifizierte Rechtsberatung. Gesetzliche Anforderungen können sich ändern, unterschiedlich ausgelegt werden oder je nach Einzelfall, Organisationsstruktur und regionalem Kontext variieren.

Jegliche Haftung für Entscheidungen oder Maßnahmen, die auf Grundlage dieses Dokuments getroffen werden, ist ausgeschlossen. Die Verantwortung für die rechtssichere Auslegung und Umsetzung der gesetzlichen Vorgaben verbleibt bei den jeweiligen Organisationen und deren Leitungsorganen.

KONTAKT

Florian Mertl
Gründer und Geschäftsführer der bwiiw GmbH
www.bwiiw.com
florian.mertl@bwiiw.com
+49 1728918803