

Grundlagen, Methodik und Nachweisführung

Vernetzte KI-Systeme zwischen Informationssicherheit, Patientensicherheit und industrieller Wirkung

Ein gemeinsames Begriffs-, Analyse- und Nachweissystem schaffen. Wer nur technische Maßnahmen sammelt, ohne Systemgrenzen, Wirkung und Beweismaßstab zu klären, kann später weder die Angemessenheit der Maßnahmen noch die verbleibenden Risiken belastbar beurteilen.

Fassung 1.1 · Stand 25. September 2026 · Adressaten: Fachprüfer, Sicherheitsarchitekten, wissenschaftliche Beiräte, Klinik- und Unternehmensleitungen sowie Verantwortliche für die Einführung der nachfolgenden Fachleitfäden.

Dokumenttyp: Fachlich ausgearbeitete Prüf- und Arbeitsfassung; externe Fachbegutachtung ausstehend

Die Fallstudien in diesem Leitfaden-Paket sind ausdrücklich konstruierte Prüfbeispiele; eine externe wissenschaftliche, klinische, juristische oder sicherheitstechnische Begutachtung des Pakets hat nicht stattgefunden.

Steckbrief

Merkmal	Wert
Dokumenttyp	Fachlich ausgearbeitete Prüf- und Arbeitsfassung; externe Fachbegutachtung ausstehend
Zielgruppe	Fachprüfer, Sicherheitsarchitekten, wissenschaftliche Beiräte, Klinik- und Unternehmensleitungen sowie Verantwortliche für die Einführung der nachfolgenden Fachleitfäden.
Recherche- und Rechtsstand	25. September 2026
Umfang	4.120 Wörter, 15 Seiten
Belege	0 Literatureinträge, 15 Quellenadressen
Gliederung	18 nummerierte Abschnitte, 1 Tabellen

Inhalt

1. Zusammenfassung und Erkenntnisziel	4
2. Forschungs- und Entscheidungsfragen	4
3. Der Ausgangsfall: belastbarer Anlass, begrenzte Evidenz	4
4. Untersuchungsdesign und Auswahl der Quellen	5
5. Quellenkritik: fünf unterschiedliche Beweisfunktionen	5
6. Begriffe, die nicht miteinander verwechselt werden dürfen	6
7. Systemgrenzen: vom Gerät zur Leistung	6
8. Wirkungsketten als Kern der Risikoanalyse	7
9. Ein formales Arbeitsmodell ohne Scheingenauigkeit	7
10. Risiko beschreiben statt Zahlen vortäuschen	7
11. Nachweislogik: Behauptung, Argument, Evidenz, Gegenbeleg	8
12. Unabhängigkeit der Schutzebenen	8
13. Betriebszustände und Rückfallfähigkeit	8
14. Wiederherstellung und die Grenzen des Vertrauens	9
15. Ökonomische Bewertung ohne Verlust der Schutzprioritäten	9
16. Verfahren für die lokale Anwendung	9
17. Was ein Prüfungsausschuss aus diesem Band verlangen kann	10
18. Arbeitsunterlagen und gezielte Leseptide	10
Literatur und Quellenstatus	10
12 Rechtliche Hinweise	13
12.1 Keine Beratung	13
12.2 Keine Zusicherung, keine Konformitätsaussage	13
12.3 Rechtsstand	13
12.4 Haftung	13
12.5 Verweise auf fremde Inhalte	13
12.6 Marken und Produktbezeichnungen	13
12.7 Urheberrecht und Nutzung	13
12.8 Keine personenbezogenen Daten	14
12.9 Unabhängigkeit	14
12.10 Anwendbares Recht	14

Impressum und Verantwortlichkeit

Die folgenden Angaben sind wörtlich dem Impressum von fluxlane.eu entnommen, abgerufen am 24. September 2026. Sie wurden nicht ergänzt und nicht umformuliert.

Angabe	Inhalt
Angaben gemäß § 5 DDG	WebTrades GmbH Am Ölberg 2 55459 Grolsheim Deutschland
Vertreten durch	Geschäftsführerin: Laurice Bussmer
Kontakt	Telefon: 0170 890 78 00 E-Mail: info@fluxlane.eu
Registereintrag	Eintragung im Handelsregister Registergericht: Amtsgericht Mainz Registernummer: HRB 54479
Umsatzsteuer-ID	Umsatzsteuer-Identifikationsnummer gemäß § 27 a Umsatzsteuergesetz: DE461650292
Redaktionell verantwortlich	Verantwortlich für den Inhalt nach § 18 Abs. 2 MStV: Laurice Bussmer, Am Ölberg 2, 55459 Grolsheim
Verbraucherstreitbeilegung	Wir sind nicht bereit oder verpflichtet, an Streitbeilegungsverfahren vor einer Verbraucherschlichtungsstelle teilzunehmen.

Redaktioneller Hinweis des Herausgebers (wörtlich)

„fluxlane ist ein unabhängiges, redaktionelles Fachportal für Robotik, autonome physische Systeme und verkörperte KI. Der redaktionelle Geltungsbereich umfasst Industrie und Produktion, Logistik, Medizin, Pflege und Rehabilitation, Service und Haushalt sowie Forschung, Hersteller, Markt und Regulierung; künstliche Intelligenz gehört dazu, auch ohne physischen Körper. Die Inhalte dienen der allgemeinen Information und stellen keine Rechts-, Kauf- oder Anlageberatung dar. Angaben zu Preisen, Verfügbarkeit und Terminen erfolgen ohne Gewähr und können sich jederzeit ändern.“

Zitierweise

FluxLane (2026): *Grundlagen, Methodik und Nachweisführung – Vernetzte KI-Systeme zwischen Informationssicherheit, Patientensicherheit und industrieller Wirkung*. Fassung 1.1, Stand 25. September 2026. Herausgegeben von der WebTrades GmbH, Grolsheim, fluxlane.eu.

Herstellung dieses Dokuments

Das vorliegende PDF ist maschinell aus der Markdown-Fassung des Leitfaden-Pakets gesetzt. Inhaltlich ist dieser Satzvorgang keine neue Sachprüfung; die zugrunde liegende Recherche- und Quellenprüfung ist im Lieferpaket dokumentiert. Gesetzt wurde mit IBM Plex Sans und Sora.

Abbildungsnachweis

Dieses Dokument enthält eine schematische Abbildung: die Autorisierung als zwei unabhängige Prüfpfade (Abschnitt 9). Die Abbildung ist eine begriffliche Visualisierung des Textes, keine Softwarearchitektur eines konkreten Produkts. Ergänzt in Fassung 1.1 am 27. September 2026.

1. Zusammenfassung und Erkenntnisziel

Eine Organisation ist nicht schon deshalb gegen die Folgen autonomer Angriffe gerüstet, weil sie ein Security Operations Center, Backups und einen Notfallplan besitzt. Entscheidend ist, ob ihre Schutzmaßnahmen die tatsächlichen Wirkungsketten abdecken: vom kompromittierten Konto über eine erlaubte Schnittstelle und eine veränderte Information bis zur Entscheidung eines Menschen, eines KI-Agenten oder einer Maschine. Ein formal berechtigter Zugriff kann fachlich unzulässig sein. Eine funktionierende Anwendung kann falsche Daten bereitstellen. Eine sachgerecht gemeinte Abwehrreaktion kann einen klinischen oder industriellen Prozess gefährden.

Die vorliegenden Leitfäden untersuchen deshalb nicht die abstrakte Frage, ob KI „sicher“ ist. Untersucht wird, **unter welchen dokumentierten Bedingungen eine konkrete Organisation einem konkreten System bestimmte Handlungen erlauben kann und wie sie diese Erlaubnis zurücknimmt, wenn die Bedingungen entfallen**. Der Gegenstand umfasst Daten, Arbeitsabläufe, Menschen, Hersteller, Kommunikationsverbindungen, Betriebszustände und physische Schutzfunktionen. Die Einbeziehung von Safety ist keine neu erfundene Erweiterung der OT-Sicherheit: NIST behandelt diesen Zusammenhang seit Langem ausdrücklich. Neu in dieser Arbeit ist die anwendungsbezogene Zusammenführung mit der Handlungsvollmacht agentischer Software. [Q02, §§ 2.3.7, 2.4 und 4.2.2; Q09, Projektbeschreibung]

Das Ergebnis ist ein begründeter Prüf- und Handlungsrahmen, keine Zertifizierung und kein Nachweis der Sicherheit eines bereits untersuchten Betriebs. Eine lokale Anlage, Klinik oder Softwareinstallation wurde nicht vermessen. Die Fallstudien sind ausdrücklich konstruierte Prüfbeispiele. Eine externe wissenschaftliche, klinische, juristische oder sicherheitstechnische Begutachtung des Pakets hat nicht stattgefunden. Diese Abgrenzung ist Teil des Nachweissystems und darf beim PDF-Satz nicht entfernt werden.

2. Forschungs- und Entscheidungsfragen

Die erste Leitfrage betrifft die **Übertragbarkeit**: Was lässt sich aus einer berichteten agentengestützten E-Commerce-Angriffskampagne auf Kliniken und industrielle Systeme übertragen? Übertragbar sind zunächst Arbeitsformen wie automatisierte Suche, Delegation und wiederholte Aktionen. Nicht ohne Weiteres übertragbar sind Erfolgsquoten, Kosten, konkrete Zugriffswege oder die Behauptung, dass dieselben Werkzeuge eine Sicherheitssteuerung überwinden könnten. Die Übertragung braucht eine zusätzliche, lokale Analyse der erreichbaren Funktionen.

Die zweite Leitfrage betrifft die **Begrenzbarkeit**: Welche Grenzen müssen vor einer Handlung erzwungen werden, statt erst nachträglich eine Anomalie zu melden? Datenexport, Konfigurationsänderung, Produktfreigabe und Maschinenbewegung unterscheiden sich in Umkehrbarkeit und Schadenslatenz. Eine spätere Untersuchung kann diese Unterschiede nicht rückwirkend aufheben.

Die dritte Leitfrage betrifft die **Betriebsfähigkeit unter Unsicherheit**: Welche Leistung bleibt vertretbar, wenn zentrale Informationen, Identitätsdienste oder Kommunikationswege unzuverlässig sind? Ein Notbetrieb ist kein bloßer technischer Schalter. Er ist ein zeitlich begrenztes Betriebsmodell mit anderen Ressourcen, anderen Kontrollen und eigenen Abbruchbedingungen.

Die vierte Leitfrage betrifft die **Nachweisbarkeit**: Welche Beobachtung würde eine Sicherheitsbehauptung stützen, und welche Beobachtung würde sie widerlegen? Erst diese Gegenprobe trennt eine belastbare Freigabe von einer Sammlung positiver Herstellerangaben. Die fünfte Leitfrage betrifft **Verantwortung**: Wer besitzt die Fachkompetenz und die formale Zuständigkeit, den Betrieb einzuschränken, ein Restrisiko anzunehmen oder die Wiederaufnahme freizugeben?

3. Der Ausgangsfall: belastbarer Anlass, begrenzte Evidenz

Gambit Security veröffentlichte am 22. September 2026 einen Interimsbericht über eine chinesischsprachig gesteuerte, finanziell motivierte Kampagne gegen Onlinehändler. Beschrieben werden 105 Angriffsvorhaben innerhalb eines beobachteten Septemberzeitraums und mindestens 27 unterschiedlich weit kompromittierte Unternehmen. Mehr als 600.000 Kartendatensätze ordnet der Bericht zwei Unternehmen zu. Der genannte Mittelwert von 25,46 US-Dollar betrifft Modellkosten abgeschlossener Scans, nicht den Preis eines erfolgreichen

Einbruchs. Eine automatisierte Bereinigung soll 180 Tabellen einschließlich Backup-Tabellen gelöscht haben. [Q01, Executive Summary, Methodology, Cost und Cleanup]

Diese Angaben sind **berichtete Befunde des Untersuchungsunternehmens**. FluxLane hat weder die Rohdaten noch die Infrastruktur unabhängig forensisch geprüft. Der Bericht selbst benennt Grenzen der Verifikation einzelner Agentenaussagen. Er belegt weder eine bestimmte Staatsangehörigkeit noch einen Angriff auf Krankenhausrobotik. Seine Funktion in diesem Anhang ist eng: Er motiviert die Prüfung, ob unzureichend begrenzte Automatisierung bestehende Schwächen und unbeabsichtigte Schäden vervielfachen kann. Alle anschließenden klinischen und industriellen Szenarien werden unabhängig von der Richtigkeit einzelner Kampagnendetails begründet.

4. Untersuchungsdesign und Auswahl der Quellen

Die Arbeit verwendet eine **strukturierte, integrative Dokumentenanalyse**. Sie verbindet amtliche Rechtsinformationen, technische Behördenleitlinien, öffentlich zugängliche Normbeschreibungen, Spezifikationen, eine empirische Primärstudie, einen klinischen Erfahrungsbericht und den aktuellen Anbieterbericht. Sie ist keine als vollständig deklarierte systematische Literaturübersicht. Es wurden weder sämtliche Datenbanken durchsucht noch eine vollständige Trefferpopulation, ein PRISMA-Flussdiagramm oder eine quantitative Metaanalyse erzeugt. Solche Verfahren nachträglich zu behaupten würde die Aussagekraft nicht erhöhen, sondern die Methodik verfälschen.

Ausgangspunkt war das vorhandene FluxLane-Masterarchiv. Dessen Begriffe und Themenstruktur wurden als redaktionelle Vorarbeit übernommen, nicht als unabhängige externe Evidenz. Anschließend wurden die für den Leitfaden tragenden Sach- und Rechtsbehauptungen an Primärquellen geprüft. Vorrang erhielten Quellen, die Anforderungen selbst formulieren, eigene Beobachtungen berichten oder eine Spezifikation verantworten. Sekundärmeldungen zum Gambit-Fall wurden nicht als zusätzliche unabhängige Bestätigung gezählt.

Eingeschlossen wurden Dokumente mit erkennbarem Bezug zu mindestens einer der Wirkungsketten Identität, Autorisierung, Datenintegrität, physische Sicherheit, klinischer Notbetrieb, industrieller Wiederanlauf oder organisatorische Verantwortung. Ausgeschlossen wurden Marketingvergleiche ohne nachvollziehbare Methode, unprüfbare Zahlen zur Erfolgswahrscheinlichkeit autonomer Angriffe und fremde Umsetzungsbehauptungen ohne Angaben zu Systemgrenze und Testumgebung. Proprietäre Normen wurden nur hinsichtlich öffentlich sichtbarer Metadaten und Anwendungsbereiche ausgewertet; nicht zugängliche Klauseln werden nicht als gelesen ausgegeben.

Der Rechercheabschluss ist der 25. September 2026. Quellenregister und Rechercheprotokoll unterscheiden Volltext-/Abschnittszugriff, Abstract-/Metadatenzugriff und technisch blockierten Abruf. Ein Abruffehler beweist nicht, dass ein Dokument nicht existiert. Er begrenzt aber, welche Verifikationsbehauptung diese Arbeit zulässt. Besonders relevant ist dies für konsolidierte EU-Rechtstexte: Die aktuelle Kommissionsdarstellung wurde gelesen, einzelne Normvolltexte waren technisch nicht zugänglich. Diese Grenze bleibt in der Rechtsmatrix sichtbar.

5. Quellenkritik: fünf unterschiedliche Beweisfunktionen

Ein Gesetz und eine Fallstudie beantworten verschiedene Fragen. Der Normtext bestimmt unter seinen Anwendungsvoraussetzungen Pflichten. Er beweist nicht, dass eine bestimmte technische Maßnahme in jeder Umgebung wirksam ist. Eine empirische Studie kann Zusammenhänge zeigen, ohne daraus eine konkrete Betreiberpflicht abzuleiten. Ein technischer Leitfaden bietet fachliche Orientierung, ohne automatisch deutsches Recht zu sein.

Evidenzart	Zulässige Verwendung	Unzulässiger Kurzschluss
Gesetz / Verordnung	Anwendungsbereich und Pflichten prüfen	„Jede Organisation fällt darunter“
Finale Behördenleitlinie / Spezifikation	Technische und organisatorische Entwurfsgrundlage	„Die Umsetzung ist damit zertifiziert“
Norm-Metadaten	Ausgabe und fachlichen Scope identifizieren	Nicht gelesene Detailklauseln als erfüllt erklären
Empirische Studie / Erfahrungsbericht	Beobachtung samt Methode und Grenzen einordnen	Einzelfallergebnis universell oder kausal verallgemeinern
Entwurf / Fachbeitrag / Anbieterbericht	Entwicklung, Hypothese oder berichteten Befund kennzeichnen	Vorläufige Aussage als endgültigen Konsens ausgeben

Für die klinische Übertragbarkeit ist etwa die Beobachtungsstudie von Dameff und Kollegen einschlägig: Sie untersucht Störungen in benachbarten Notaufnahmen während eines regionalen Ransomwareereignisses. Ihr Design trägt Aussagen über beobachtete Zusammenhänge, nicht über eine allgemeine Sterblichkeitssteigerung durch KI-Angriffe. Der Laborbericht von Goodwin und Kollegen ist hier nur über Abstract und Metadaten ausgewertet. Daraus wird keine vollständige Bewertung seiner Interventionen abgeleitet. [Q20, Methods und Limitations; Q21, Abstract]

Bei technischen Quellen wird die Version Bestandteil der Behauptung. SP 800-82 Rev. 3 ist die hier verwendete finale OT-Grundlage; Rev. 4 ist am Stichtag ein Initial Public Draft. Das Agentenidentitätsprojekt des NCCoE und der zugehörige NIST-Fachbeitrag sind fachlich relevant, aber keine verabschiedete neue Pflichtnorm. [Q02; Q03, Status; Q09; Q10]

6. Begriffe, die nicht miteinander verwechselt werden dürfen

Informationssicherheit betrifft hier den Schutz von Vertraulichkeit, Integrität und Verfügbarkeit sowie die dazu notwendige Authentizität und Nachvollziehbarkeit. **Safety** meint die Beherrschung von Gefährdungen für Menschen und gegebenenfalls weitere Schutzgüter durch die Funktion und den Zustand eines Systems. **Security** betrifft den Schutz gegen unbefugte oder missbräuchliche Einwirkung. Die Bereiche überlappen, bleiben aber in ihren Nachweisverfahren unterscheidbar. Die MDCG-Leitlinie stellt ausdrücklich auch Rückwirkungen von Cybermaßnahmen auf Safety dar. [Q02; Q22, Annex IV]

Ein **Fehler** kann zufällig oder systematisch entstehen. Eine **Bedrohung** bezeichnet eine mögliche schädigende Einwirkung mit Akteur, Fähigkeit und Gelegenheit. Eine **Gefährdung** ist ein Zustand, aus dem unter bestimmten Umständen ein Schaden entstehen kann. Ein **Schaden** ist die eingetretene nachteilige Wirkung. Ein manipulierter Datensatz ist daher nicht automatisch eine Patientenverletzung; zwischen beiden liegen Interpretation, Entscheidung, Ausführung und mögliche Schutzbarrieren. Umgekehrt kann schon eine fehlerhafte Zuordnung ohne Datendiebstahl eine relevante Gefährdung darstellen.

Ein **KI-Agent** ist in diesem Anhang Software, die für ein Ziel mehrschrittige Entscheidungen treffen und Werkzeuge aufrufen kann. Die Definition setzt weder Bewusstsein noch vollständige Autonomie voraus. **Physical AI** bezeichnet hier KI-Funktionen, deren Ergebnisse direkt oder über andere Systeme physische Prozesse beeinflussen können. Ein textlicher Vorschlag kann mittelbar relevant sein; ein Roboterbefehl ist unmittelbar relevant. Beide benötigen unterschiedliche Kontrollen.

Authentisierung klärt die Identität. **Autorisierung** entscheidet über eine konkrete erlaubte Handlung. **Delegation** überträgt begrenzte Befugnisse von einem Auftraggeber an einen anderen Akteur. **Fachliche Plausibilität** beurteilt, ob eine Handlung im Prozess sinnvoll ist. **Funktionale Sicherheit** kann nicht daraus abgeleitet werden, dass Identität und Plausibilität geprüft wurden. Ein ordnungsgemäß authentisierter Wartungsdienst kann eine gefährliche Änderung anfordern; eine plausible Änderung kann auf einem falschen Weltmodell beruhen. [Q06; Q14, § 1.1]

7. Systemgrenzen: vom Gerät zur Leistung

Die primäre Analyseeinheit ist die erbrachte Leistung, nicht die Zahl der Server. Eine Klinik will beispielsweise eine Probe dem richtigen Patienten zuordnen und einen Befund rechtzeitig zustellen. Eine Fabrik will ein Werkstück unter zulässigen Bedingungen herstellen und dessen Qualität nachweisen. Beide Leistungen bestehen aus technisch und organisatorisch verteilten Teilfunktionen.

Für jede Leistung werden fachlicher Eigentümer, betroffene Personen, Datenobjekte, Geräte, Dienste, Herstellerkontakte und Kommunikationswege erfasst. Hinzu kommen weniger sichtbare Abhängigkeiten: Zeitsynchronisierung, Namensauflösung, Zertifikate, Lizenzserver, Identitätsdienste, Schlüsselverwahrung, Fernwartung, Alarmweiterleitung und die Verfügbarkeit fachkundigen Personals. Die Inventarisierung ist nicht abgeschlossen, solange ein notwendiger Dienst lediglich als „Cloud“ oder „Hersteller“ bezeichnet wird. Es muss erkennbar sein, welche konkrete Funktion er übernimmt und welche Alternative bei seinem Ausfall besteht.

Ein rein technisches Systemdiagramm bleibt dennoch wertvoll. Es wird hier um zwei weitere Sichten ergänzt: einen **Handlungsvollmachtsgraphen** und einen **Leistungsabhängigkeitsgraphen**. Der erste zeigt, welcher Akteur welche Wirkung auslösen darf. Der zweite zeigt, welche Leistung von welcher Ressource abhängt. Diese Arbeitsmodelle sind keine neuen Normen; sie ordnen vorhandene Konzepte für die konkrete Prüfung. Die Überschneidung beider Graphen zeigt besonders kritische Stellen: Ein Dienst ist gefährlich mächtig, wenn er viele wesentliche Leistungen beeinflussen kann und zugleich deren Wiederherstellung kontrolliert.

8. Wirkungsketten als Kern der Risikoanalyse

Die Analyse beginnt mit einem Verlust, den die Organisation vermeiden muss. Danach wird rückwärts geprüft, welche Zustände diesen Verlust ermöglichen und welche Handlungen dorthin führen können. Eine mögliche Kette lautet: kompromittierter Servicezugang → unzulässige Änderung eines Datensatzes → automatische Übernahme in eine Empfehlung → unzureichende menschliche Gegenprüfung → fachlich falsche Handlung. Eine andere lautet: Fehlalarm eines Verteidigungsagenten → ungezielte Netzisolation → Ausfall zentraler Alarmweiterleitung → lokal nicht kompensierter Überwachungsverlust.

Für jeden Übergang wird eine Barriere benannt. Die Barriere kann präventiv, detektierend, begrenzend oder wiederherstellend sein. Diese Rollen sind nicht austauschbar. Ein Audit-Log verhindert den Datenexport nicht. Eine Sicherungskopie korrigiert keine bereits getroffene klinische Entscheidung. Ein sicherer Maschinenstopp schützt nicht notwendigerweise die Vertraulichkeit zuvor kopierter Rezepturen.

Eine belastbare Risikobeschreibung hat deshalb die Form: **Unter den Voraussetzungen A kann Akteur oder Fehler B über Pfad C die unerwünschte Handlung D auslösen. Daraus kann bei Zustand E der Verlust F entstehen. Die Barrieren G und H begrenzen den Pfad unter den Annahmen I. Offen bleibt J.** Diese vollständige Satzstruktur verhindert, dass „KI-Risiko hoch“ an die Stelle einer nachprüfbareren Analyse tritt.

9. Ein formales Arbeitsmodell ohne Scheingenauigkeit

Für die Autorisierung lässt sich eine Entscheidung als Funktion beschreiben:

$\text{Erlaubnis} = f(\text{Identität, Delegation, Ressource, Aktion, Zweck, Prozesszustand, Zeit, Datenvertrauen, Betriebsmodus})$.

Die Funktion liefert nicht nur „ja“ oder „nein“, sondern gegebenenfalls „nur lesend“, „zusätzliche Freigabe erforderlich“ oder „lokal eskalieren“. Die Werte müssen aus festgelegten, überprüfbaren Quellen stammen. Ein Agent darf den Kontext, der seine eigene Berechtigung erweitert, nicht selbst ohne unabhängige Bestätigung setzen. Eine bloße Behauptung „Notfall“ darf keine uneingeschränkte Vollmacht erzeugen.

Die physische Zulässigkeit wird gesondert betrachtet: $\text{Zulässige Wirkung} = g(\text{physischer Zustand, Schutzfunktion, Prozessgrenzen, Betriebsart})$. Beide Funktionen können unterschiedliche Zeit- und Vertrauensanforderungen haben. Eine IT-Autorisierung mit hoher Verfügbarkeit darf keine sicherheitsgerichtete Schutzfunktion ersetzen. Die konkrete Realisierung muss nach dem jeweiligen System- und Produktscope beurteilt werden; dieses Modell verlangt nicht pauschal einen bestimmten Hersteller oder eine bestimmte Safety-Architektur.

Wichtig ist außerdem die Zeitdifferenz zwischen Prüfung und Ausführung. Ein um 10:00 Uhr freigegebener Auftrag kann um 10:03 Uhr unzulässig sein, weil sich der Betriebsmodus geändert hat. Deshalb gehören Ablaufzeit, Abbruchbarkeit, erneute Prüfung an der Ausführungsgrenze und der Umgang mit bereits laufenden Handlungen in den Entwurf. Das ist eine eigene Systemsynthese auf Grundlage von ressourcenbezogener Autorisierung und technischen Delegations-/Widerrufsmechanismen. [Q06; Q13–Q15]

10. Risiko beschreiben statt Zahlen vortäuschen

Der Leitfaden verwendet keine universelle Formel „Eintrittswahrscheinlichkeit mal Schaden“ mit frei erfundenen Zahlen. Bei neuen Angriffspfaden fehlen häufig belastbare Häufigkeitsdaten. Auch ordinalen Klassen wie niedrig, mittel und hoch dürfen nicht nachträglich Eigenschaften einer präzisen Messskala zugeschrieben werden.

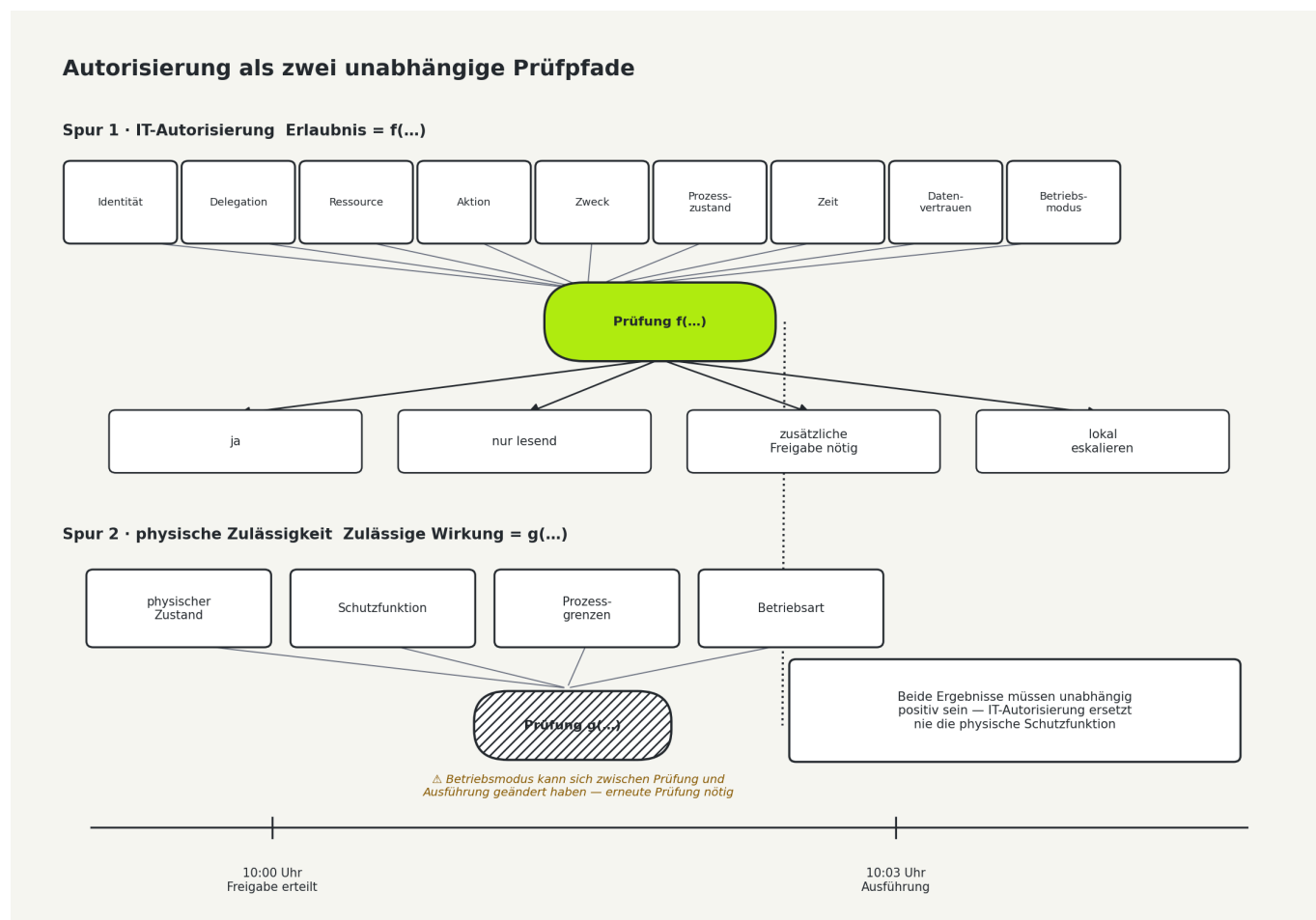


Abbildung · Autorisierung als zwei unabhängige Prüfpfade (zu Abschnitt 9)

Stattdessen wird ein **Risikoprofil** dokumentiert: mögliche Personengefährdung, Versorgungs- oder Produktionsausfall, Integritätsverlust, Vertraulichkeitsverlust, Umweltwirkung und wirtschaftliche Folgen. Hinzu kommen Exposition, vorhandene Akteursfähigkeit, Abhängigkeiten, Erkennbarkeit, Zeit bis zum Schaden, Umkehrbarkeit und Unsicherheit. Eine begründete priorisierte Entscheidung bleibt möglich, ohne eine unbelegte Wahrscheinlichkeit zu behaupten.

Ein selten angenommener, aber rasch irreversibler Safety-Verlust darf nicht durch viele niedrig bewertete Büro-IT-Risiken statistisch verdeckt werden. Ebenso kann ein massenhafter Abfluss sensibler Daten schwerwiegend sein, ohne einen Roboter zu beeinflussen. Die Profile bleiben deshalb mehrdimensional. In einer Entscheidungsvorlage werden Konflikte ausdrücklich benannt, etwa wenn zusätzliche Isolation die Ausbreitung begrenzt, aber die Verfügbarkeit eines gemeinsam genutzten Dienstes verschlechtert.

11. Nachweislogik: Behauptung, Argument, Evidenz, Gegenbeleg

Jede wesentliche Freigabe wird als begründeter Nachweisfall geführt. **Behauptung:** Der Terminagent kann keine unzulässigen Therapieänderungen ausführen. **Argument:** Seine Identität besitzt nur eine begrenzte API-Berechtigung; andere Schreibpfade sind ausgeschlossen. **Evidenz:** geprüfte Policy, Systemkonfiguration, Schnittstelleninventar und reproduzierbarer Negativtest. **Gegenbelegsuche:** Kann derselbe Agent über ein Hilfswerkzeug, ein geteiltes Konto oder einen delegierten Subagenten dennoch schreiben?

Ein Dokument allein ist keine Betriebsevidenz. Eine Policy-Datei zeigt eine Absicht. Ein Test zeigt Verhalten unter festgehaltenen Bedingungen. Eine wiederholte Übung zeigt zusätzlich, ob Menschen und Systeme die vorgesehenen Abläufe ausführen können. Keiner dieser Nachweise garantiert die Abwesenheit sämtlicher unbekannter Fehler. Die Freigabe muss daher Systemversion, Testabdeckung, Ausnahmen und Gültigkeitsbedingungen enthalten.

Die gemeinsame Kontrollsammlung unterscheidet vier Nachweiszustände: **nicht erhoben, dokumentiert, technisch beziehungsweise organisatorisch geprüft** und **im genehmigten Betrieb wiederkehrend bestätigt**. Davon unabhängig wird das Ergebnis als **erfüllt, teilweise erfüllt, nicht erfüllt** oder **nicht anwendbar mit Begründung** ausgewiesen. Ein fehlender Nachweis ist nicht automatisch Beweis einer unsicheren Anlage. Er kann aber die Freigabe einer kritischen Funktion verhindern, weil die behauptete Schutzwirkung nicht hinreichend belegt ist.

12. Unabhängigkeit der Schutzebenen

Zwei Produkte sind nicht schon deshalb unabhängig, weil sie von unterschiedlichen Herstellern stammen. Sie können denselben Administrationszugang, dieselbe Zertifizierungsstelle, dieselbe Updateverteilung, denselben Netzwerkpfad oder dieselbe Stromversorgung benötigen. Die Analyse gemeinsamer Ausfall- und Kompromittierungsursachen ist deshalb konkreter als die Forderung nach „mehreren Schichten“.

Eine sinnvolle Prüfprobe lautet: Kann die Identität, die den operativen Agenten kontrolliert, auch dessen letzte Begrenzung verändern? Kann ein kompromittierter Managementserver sowohl Produktion als auch Backups und Protokolle zerstören? Welche Schutzfunktion bleibt wirksam, wenn zentrale Kommunikation fehlt? Die Antworten müssen an tatsächlichen Konfigurationen und genehmigten Tests belegt werden, nicht an Produktkategorien. Historische Safety-Angriffe machen die Relevanz sichtbar, beweisen aber keine bestimmte Gefährdung der hier betrachteten Systeme. [Q27; Q28]

Auch vollständige physische Trennung ist kein universelles Rezept. Sie kann in bestimmten Fällen erforderlich oder zweckmäßig sein, in anderen Fällen Kommunikation und Diagnose erschweren. Maßgeblich sind Gefährdungsbeurteilung, notwendiger Informationsaustausch und die nachweisbare Begrenzung gemeinsamer Ursachen. Die Leitfäden fordern die Begründung einer Architektur, nicht die pauschale Beschaffung einer vermeintlich universellen Kontrollschicht.

13. Betriebszustände und Rückfallfähigkeit

Normalbetrieb, eingeschränkter Betrieb, isolierter Bereich, lokaler Betrieb, manueller Notbetrieb und sicherer Stillstand sind **mögliche** Zustände. Sie bilden keine zwingende lineare Treppe. Manche Systeme dürfen nie in einen bestimmten Zustand wechseln; andere benötigen einen Übergang mit Nachlauf, Energiehaltung, Spülung oder

zusätzlicher Personalpräsenz. Die zulässigen Zustände müssen aus der Leistung und ihrer Gefährdung abgeleitet werden.

Für jeden Zustand werden Eintrittskriterium, verantwortliche Person, erhaltene und verlorene Funktionen, Ressourcenbedarf, zulässige Dauer, Überwachung und Austrittskriterium festgehalten. Der zeitliche Horizont ist wesentlich. Ein manueller Ablauf kann eine kurze Störung abfangen und bei längerer Dauer an Personalwechseln, Materialmangel oder Dokumentationsrückstand scheitern. „Plan B vorhanden“ ist daher erst sinnvoll, wenn auch seine Erschöpfung berücksichtigt wird.

Der im Master verwendete Begriff „Minimum Viable Hospital“ wird in diesem Anhang als **definierte sichere Mindestversorgung** präzisiert. „Minimum Viable Factory“ bezeichnet entsprechend einen freigegebenen Mindestbetrieb oder einen kontrollierten Stillstand. Der Ausdruck ist eine Denkhilfe, kein medizinischer Mindeststandard oder wirtschaftliches Optimierungsziel.

14. Wiederherstellung und die Grenzen des Vertrauens

Ein Hash bestätigt bei vertrauenswürdigem Vergleich, dass eine Datei gegenüber der Referenz unverändert ist. Eine digitale Signatur kann Herkunft und Integrität im Rahmen ihrer Vertrauenskette belegen. Beides beweist weder die fachliche Richtigkeit des Inhalts noch die Abwesenheit einer schon in der Referenz enthaltenen Manipulation. Ein signiertes falsches Laborergebnis bleibt falsch. Eine authentische, aber fehlerhafte Konfiguration bleibt problematisch.

Statt eines angeblich „nachweislich sauberen“ Zustands wird deshalb ein **begründet validierter Referenzzustand** verwendet. Dokumentiert werden Herkunft, Prüfmethode, bekannte Lücken, zeitliche Reichweite, technische Integrität und fachliche Plausibilisierung. Die Wiederaufnahme erfolgt erst nach einer dazu passenden Entscheidung, nicht automatisch nach erfolgreichem Restore. Backups sind eine notwendige Ressource für viele Wiederherstellungen, aber keine vollständige Rekonstruktion des laufenden Betriebs. [Q08]

Besonders anspruchsvoll ist das Zusammenführen digitaler und manueller Ereignisse. Die Zeit der tatsächlichen Behandlung oder Fertigung und die spätere Zeit der Erfassung bleiben unterscheidbar. Konflikte werden gekennzeichnet und fachlich entschieden; eine automatische Überschreibung würde die Unsicherheit nur verbergen. Dieser Zusammenhang wird in Band 6 und im Abgleichformular praktisch ausgearbeitet.

15. Ökonomische Bewertung ohne Verlust der Schutzprioritäten

Die wirtschaftliche Entscheidung betrifft nicht nur die Anschaffung eines Sicherheitsprodukts. Zu berücksichtigen sind Integration, Wartung, Personal, Schulung, Übungsausfälle, Ersatzbetrieb, Nachweisführung, Datenmigration und spätere Ablösung. Ein günstiger Dienst kann hohe Folgekosten erzeugen, wenn er keine kontrollierte Trennung, keinen Datenexport oder keine nutzbaren Protokolle erlaubt. Das ist eine Analyse von Abhängigkeiten, keine Preisempfehlung für einen bestimmten Anbieter.

Bei begrenztem Budget ist zunächst zu prüfen, welche Maßnahme einen dokumentierten kritischen Pfad tatsächlich unterbricht. Ein zusätzliches Dashboard kann weniger bewirken als die Beseitigung eines geteilten Administrationskontos oder die Wiederherstellung einer lokal notwendigen Alarmfunktion. Die Bewertung darf jedoch erforderliche Schutzmaßnahmen nicht allein mit erwarteten finanziellen Verlusten verrechnen. Gesetzliche Anforderungen, fachliche Sicherheitsgrenzen und die Rechte Betroffener sind gesonderte Entscheidungsbedingungen.

16. Verfahren für die lokale Anwendung

Die Anwendung beginnt mit einem klar abgegrenzten Pilotprozess und einem verantwortlichen Facheigentümer. Danach werden Leistungsabhängigkeiten und Handlungsvollmachten erhoben. Aus unerwünschten Verlusten werden konkrete Wirkungsketten entwickelt. Diese werden mit technischen und organisatorischen Barrieren verbunden, deren Nachweise bereits vor Einführung der Automatisierung festgelegt werden.

Erst anschließend werden ein möglicher Notbetrieb und die Wiederherstellung getestet. Ein Fehler im Test wird nicht durch Umbenennen des Kriteriums beseitigt. Er führt zu einer Änderung, einer erneuten Prüfung oder einer dokumentierten Einschränkung des geplanten Funktionsumfangs. Die Freigabe kann etwa nur lesende Nutzung gestatten und Schreib- oder Steuerfunktionen vorläufig ausschließen. Eine solche Begrenzung ist ein sachliches Ergebnis, kein Scheitern des gesamten KI-Vorhabens.

Die Regelüberprüfung wird durch Änderungen ausgelöst: neue Werkzeuge, neue Modelle, geänderte Berechtigungen, andere Herstellerverbindungen, neue klinische Prozesse, Maschinenumbauten oder relevante Sicherheitsvorfälle. Ein unveränderter Dateiname des Agenten bedeutet nicht, dass die Risikokonstellation gleich geblieben ist. Gleiches gilt für Cloudprodukte mit automatischen Funktionsänderungen.

17. Was ein Prüfungsausschuss aus diesem Band verlangen kann

Ein Ausschuss kann eine nachvollziehbare Systemgrenze, die wichtigsten Verlustszenarien, einen begründeten Quellenstatus und ein transparentes Nachweismodell verlangen. Er kann fragen, welche Behauptung auf Beobachtung, welche auf Norm und welche auf eigener Empfehlung beruht. Er kann auf der Prüfung einer Gegenhypothese bestehen: Könnte dieselbe Schutzmaßnahme selbst einen gefährlichen Zustand erzeugen? Welche unabhängige Information würde die Freigabe widerlegen?

Die angemessene Antwort ist kein pauschales Sicherheitsversprechen. Sie ist ein überprüfbarer Zusammenhang zwischen vorgesehenem Nutzen, zugelassenen Handlungen, verbleibendem Risiko und belastbaren Rückfallmöglichkeiten. Die Fachbände, Kontrollen und Fallstudien übersetzen diese Grundstruktur in konkrete Klinik-, Industrie- und Softwareentscheidungen.

18. Arbeitsunterlagen und gezielte Leseptide

Für die erste Anwendung werden **F01 System- und Leistungssteckbrief**, **F02 Abhängigkeitsregister**, **F03 Handlungsvollmachten**, **F04 Risiko- und Gefährdungsfall** sowie **F05 Nachweisfall** aus dem Formularband benötigt. Die Kontrollen **K01–K08** konkretisieren Systemgrenzen, Rollen, Risikoketten und Nachweisführung. Die Klinikvertiefung steht in Band 2, die industrielle Vertiefung in Band 3. Band 4 behandelt die technische Durchsetzung von Handlungsvollmachten; Band 5 trennt Governance und Rechtsgrundlagen; Band 6 beschreibt Prüfung, Reaktion und Wiederanlauf.

Ergebnis dieses Bandes: Ein System darf nicht durch eine einzige Kennzahl oder ein pauschales „KI-sicher“ freigegeben werden. Freigegeben wird ein beschriebener Nutzungsumfang unter dokumentierten Bedingungen, anhand geeigneter Nachweise und mit einer benannten Entscheidungskompetenz.

<!-- GENERATED_LOCAL_BIBLIOGRAPHY -->

Literatur und Quellenstatus

Die folgenden Angaben gehören zu diesem Band. Das vollständige Quellenregister erläutert Verwendungszweck und Zugriff. Quellenstatus und Grenzen sind bei jeder Weiterverwendung zu erhalten. Die Q-Nummern im Text beziehen sich auf diese Einträge; Fundstellen bezeichnen die externe Quelle, nicht eine erfundene PDF-Seite dieses Bandes.

Q01 – Eyal Sela / Gambit Security. Autonomous AI agents are hacking online retailers for \$25 a company. 2026-09-22. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: Executive Summary; Methodology; Cost; Data Exfiltration / Cleanup. Zugriff: Web-Volltext und relevante Abschnitte gelesen. Grenze: Keine unabhängige Prüfung der Rohlogs durch FluxLane. Einzelne Agentenaussagen laut Bericht nicht unabhängig bestätigt. Keine Klinik-/Robotikfallstudie.

Q02 – Keith Stouffer et al. / NIST. Guide to Operational Technology (OT) Security, SP 800-82 Rev. 3. 2023-09-28. DOI: 10.6028/NIST.SP.800-82r3. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: §§ 2.3.7, 2.4, 3.3, 4.2.2, 5.2, 5.3, 6.2.10–6.2.12, 6.3–6.5; gedruckte S. 25, 28, 38–42, 55, 69–79, 122–138. Zugriff: Landingpage und relevante PDF-Abschnitte gelesen; PDF-Stichprobe visuell geprüft. Grenze: Freiwillige US-Leitlinie, kein deutscher Konformitätsnachweis. Der Leitfaden ergänzt eigene Überlegungen;

Kapitelverweise sind keine wörtlichen Normanforderungen.

Q03 – NIST. Guide to Operational Technology (OT) Security, SP 800-82 Rev. 4, Initial Public Draft. 2026-09-21. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: Status / Announcement / Abstract; Kommentierungsfrist 30.11.2026. Zugriff: Landingpage einschließlich Entwurfsstatus gelesen. Grenze: Nicht final und keine ersetzende verbindliche Grundlage. Inhaltlicher Horizont, nicht Abnahmekriterium.

Q06 – Scott Rose; Oliver Borchert; Stu Mitchell; Sean Connelly / NIST. Zero Trust Architecture, SP 800-207. 2020-08. DOI: 10.6028/NIST.SP.800-207. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: Abstract; ressourcenbezogenes Vertrauen und getrennte Authentisierung/Autorisierung. Zugriff: Offizielle Publikationsseite / Abstract gelesen. Grenze: Zero Trust garantiert weder Prozesssicherheit noch korrekte Daten. Die vorgeschlagene Agentenarchitektur ist eigene Synthese.

Q08 – NIST. OT Backup Quick Start Guide, SP 1339. 2026-06-17. DOI: 10.6028/NIST.SP.1339. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: Abstract; Backup und Recovery für OT. Zugriff: Publikationsseite / Beschreibung gelesen. Grenze: Ein Backup- oder Hashnachweis ist kein Beweis fachlicher Datenrichtigkeit. Konkrete Recovery-Gates sind eigene Ableitungen.

Q09 – NIST NCCoE. Software and AI Agent Identity and Authorization. Projektstand abgerufen 2026-09-25. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: Project overview; Identity and Authorization. Zugriff: Projektseite gelesen. Grenze: Projektseite ist kein verabschiedeter Standard und keine gesetzliche Pflicht.

Q10 – NIST Cybersecurity Insights. Back to the Future: Why Agentic AI Needs a Strong Identity Foundation. 2026-08-27. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: Agent identities; credentials; authorization; consent fatigue. Zugriff: Webtext gelesen. Grenze: Fachbeitrag, keine Norm. Zustimmungsermüdung ist hier qualitativ behandelt, nicht als populationsweite Effektgröße.

Q13 – T. Lodderstedt et al. / IETF. Best Current Practice for OAuth 2.0 Security, RFC 9700. 2025-01. DOI: 10.17487/RFC9700. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: § 2 Best Practices; § 4 Threats and Mitigations. Zugriff: RFC-Webvolltext / relevante Abschnitte gelesen. Grenze: OAuth ist eine technische Grundlage, kein fertiges Agenten- oder Safety-Berechtigungsmodell.

Q14 – M. Jones et al. / IETF. OAuth 2.0 Token Exchange, RFC 8693. 2020-01. DOI: 10.17487/RFC8693. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: § 1.1 Delegation vs. Impersonation; § 4.1 act claim. Zugriff: RFC-Webvolltext / Delegationsabschnitte gelesen. Grenze: Token Exchange allein begrenzt keine physische Wirkung und erzeugt keine vollständige Verantwortlichkeitskette.

Q15 – T. Lodderstedt et al. / IETF. OAuth 2.0 Token Revocation, RFC 7009. 2013-08. DOI: 10.17487/RFC7009. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: § 2.1–2.2 Revocation Request / Response; § 3 Implementation Note. Zugriff: RFC-Webvolltext / Widerrufsabschnitte gelesen. Grenze: Ein Tokenwiderruf hebt bereits ausgeführte oder autonom weiterlaufende Maschinenaktionen nicht auf. Diese Folgerung ist eigene Systemanalyse.

Q20 – Christian Dameff et al.. Ransomware Attack Associated With Disruptions at Adjacent Emergency Departments in the US. 2023-05-08. DOI: 10.1001/jamanetworkopen.2023.12270. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: JAMA Network Open 6(5):e2312270; Methods; Results; Limitations. Zugriff: Web-Volltext, Methoden, Ergebnisse und Limitationen gelesen. Grenze: Assoziation, keine randomisierte Kausalidentifikation; begrenzte regionale Übertragbarkeit; keine Studie über KI-Angriffe.

Q21 – Goodwin et al.. Anatomy of a Cyberattack: Part 2: Managing a Clinical Pathology Laboratory During 25 Days of Downtime. 2022. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: American Journal of Clinical Pathology 157(5):653–663; Abstract. Zugriff: PubMed-Abstract / Metadaten gelesen; Volltext nicht ausgewertet. Grenze: Nur Abstractzugriff; keine Detailbehauptungen über Interventionseffekt, Kennzahlen oder Volltextmethodik.

Q22 – Medical Device Coordination Group / Europäische Kommission. MDCG 2019-16 rev. 1: Guidance on Cybersecurity for medical devices. 2020-07 (Rev. 1). [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: Abschnitte zu Design / Post-market; Annex IV, gedruckte S. 46. Zugriff: Relevante PDF-Abschnitte gelesen; Inhaltsverzeichnis und Annex IV visuell geprüft. Grenze: Leitlinie ist ausdrücklich nicht rechtsverbindlich; kein Ersatz für MDR/IVDR oder den Normvolltext.

Q27 – MITRE. ATT&CK for ICS: Loss of Safety, T0880. abgerufen 2026-09-25. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: Description; Mitigations; References. Zugriff: Eintrag gelesen. Grenze: Taxonomie belegt keine Angriffsquote und keine lückenlose Historie.

Q28 – MITRE. Triton Safety Instrumented System Attack, C0030. abgerufen 2026-09-25. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: Campaign description; techniques; references. Zugriff: Eintrag und Einordnung gelesen. Grenze: Kontextquelle; keine eigene forensische Verifikation; keine agentische KI-Kampagne.

Arbeitsmittel: Kontrollkatalog, Formularbuch, Fallstudien und Claim–Evidence-Matrix.

12 Rechtliche Hinweise

12.1 Keine Beratung

Diese Veröffentlichung ist ein redaktionelles Erzeugnis. Sie stellt keine Rechtsberatung, keine medizinische, pflegerische, arbeitsrechtliche oder datenschutzrechtliche Beratung und keine Beschaffungs- oder Vergabeberatung dar. Sie ersetzt insbesondere nicht die Prüfung durch Rechtsanwaltschaft, Datenschutzaufsicht, Medizinprodukteberatung, Vergabestelle, Ethikkommission nach Medizinprodukterecht oder Arbeitnehmervertretung. Wer auf Grundlage dieses Dokuments entscheidet, entscheidet auf eigene Verantwortung und hat den Sachverhalt vorher eigenständig fachlich prüfen zu lassen.

12.2 Keine Zusicherung, keine Konformitätsaussage

Die beschriebenen Verfahren, Prüfstufen und Checklisten sind redaktionelle Vorschläge. Sie sind keine Zusicherung einer Eigenschaft, kein garantiertes Ergebnis und kein Nachweis der Einhaltung einer Rechtsvorschrift. Wer ein Verfahren aus diesem Dokument anwendet, erfüllt damit keine gesetzliche Anforderung; ob eine Anforderung erfüllt ist, entscheidet die zuständige Stelle am Einzelfall.

12.3 Rechtsstand

Rechtsstände, Fristen und Fundstellen beziehen sich auf den im Dokumentkopf genannten Tag. Der KI-Rechtsrahmen wird laufend geändert; ein älterer Fristenplan darf nicht unverändert weiterverwendet werden. Genannte Gesetze und Verordnungen sind in ihrer jeweils geltenden Fassung heranzuziehen.

12.4 Haftung

Die Inhalte wurden mit Sorgfalt erstellt und, soweit im Methodenteil beschrieben, gegengeprüft. Für Richtigkeit, Vollständigkeit und Aktualität wird gleichwohl keine Gewähr übernommen. Eine Haftung des Herausgebers ist auf Vorsatz und grobe Fahrlässigkeit beschränkt; dies gilt nicht bei der Verletzung des Lebens, des Körpers oder der Gesundheit sowie bei zwingender gesetzlicher Haftung.

12.5 Verweise auf fremde Inhalte

Dieses Dokument verweist auf Inhalte Dritter, insbesondere auf Behörden-, Fachgesellschafts-, Normen- und Fachverlagsseiten. Auf deren Gestaltung und Inhalt hat der Herausgeber keinen Einfluss; für sie ist jeweils der dortige Anbieter verantwortlich. Die Adressen waren zum im Literaturverzeichnis genannten Prüfzeitpunkt erreichbar. Die Nennung eines Produkts, Herstellers oder Dienstes ist weder eine Empfehlung noch eine Bewertung seiner Eignung.

12.6 Marken und Produktbezeichnungen

Genannte Produkt-, Marken- und Unternehmensbezeichnungen sind Kennzeichen ihrer jeweiligen Inhaber und werden ausschließlich zur Beschreibung des Sachverhalts verwendet. Aus der Nennung folgt keine Verbindung zwischen dem Herausgeber und dem jeweiligen Unternehmen und keine Aussage über Zulassungs-, Konformitäts- oder Zertifizierungsstatus.

12.7 Urheberrecht und Nutzung

Dieses Dokument, sein Text, seine Tabellen und seine Abbildungen sind urheberrechtlich geschützt. Rechteinhaberin ist die WebTrades GmbH. Zulässig sind das Lesen, das Speichern und der Ausdruck für den eigenen Gebrauch sowie das Zitieren einzelner Stellen mit vollständiger Quellenangabe nach der im Impressum genannten Zitierweise. Die Vervielfältigung, Bearbeitung, Verbreitung, öffentliche Zugänglichmachung oder kommerzielle Verwertung des Dokuments oder wesentlicher Teile daraus bedarf der vorherigen schriftlichen Zustimmung der Rechteinhaberin. Das gilt ausdrücklich auch für die Übernahme von Tabellen und Abbildungen.

12.8 Keine personenbezogenen Daten

Für dieses Dokument wurden keine personenbezogenen Daten verarbeitet. Es beruht auf veröffentlichter Literatur, amtlichen Rechtsquellen und Veröffentlichungen von Fachgesellschaften; es wurden weder Beschäftigte befragt noch Patientendaten verwendet. Wer die hier beschriebenen Verfahren auf eine reale Einrichtung anwendet, verlässt diesen Rahmen: Die Auswertung von Tätigkeits-, Alarm- oder Quittierungsdaten unterliegt der Datenschutz-Grundverordnung und in der Regel der Mitbestimmung.

12.9 Unabhängigkeit

Dieses Dokument ist ohne Auftrag, ohne Finanzierung und ohne inhaltliche Beteiligung eines Herstellers, Krankenhausträgers, Kostenträgers, Verbands oder Beratungsunternehmens entstanden. Es besteht kein Vergütungs- oder Beteiligungsverhältnis zu einem der genannten Unternehmen oder Institutionen. Genannt werden Systeme, Anbieter und Dokumente, weil sie in den beschriebenen Gegenstand fallen, nicht weil sie beworben werden sollen.

12.10 Anwendbares Recht

Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts. Gesetzliche Verbraucherschutzvorschriften bleiben unberührt.