Der 7-Tage-Vorsprung

Assume Breach. Nicht irgendwann. Jetzt.

Bettina Sterner, BA BA
kaffeekipferl.at
Juli 2026

Die in diesem Whitepaper enthaltenen Ausführungen, Analysen und Schlussfolgerungen spiegeln ausschließlich die persönliche fachliche Einschätzung der Autorin zum Zeitpunkt der Veröffentlichung wider. Sie sind unabhängig entstanden und stehen in keinem Zusammenhang mit aktuellen oder früheren Arbeitgebern, Auftraggebern, Mandanten oder sonstigen Organisationen, denen die Autorin angehört oder angehört hat. Das Whitepaper ersetzt keine rechtliche oder regulatorische Beratung im Einzelfall.

Deutsch

Regulatorische Rahmenbedingungen wie DORA und NIS-2-RL schaffen Erwartungen an das IKT-Drittparteienrisikomanagement – ohne sie zu operationalisieren. Gleichzeitig haben KI-gestützte Angriffswerkzeuge die Zeit zwischen der Veröffentlichung einer Schwachstelle und ihrer aktiven Ausnutzung auf im Durchschnitt sieben Tage verkürzt. Für Unternehmen ohne eigene Softwareentwicklung, die vollständig oder überwiegend auf IKT-Drittdienstleister angewiesen sind, entsteht daraus eine strukturelle Schutzlücke: Der Rechtsrahmen beantwortet die Frage, ob ein Prozess existiert – die relevante Frage lautet jedoch, wie lange eine Organisation im Ernstfall blind ist und was in dieser Zeit passiert. Dieses Whitepaper analysiert die regulatorische Lücke, beleuchtet Konzentrationsrisiken bei Drittdienstleistern und KI-Tools, und gibt konkrete Empfehlungen: Welche Fragen Dienstleister beantworten können müssen – und was vertraglich geregelt sein sollte.

English

Regulatory frameworks such as DORA and NIS2 establish expectations for ICT third-party risk management – without operationalising them. At the same time, AI-assisted attack tooling has compressed the window between vulnerability disclosure and active exploitation to a median of seven days. For organisations without in-house software development that rely entirely or predominantly on ICT third-party providers, this creates a structural protection gap: the regulatory framework answers whether a process exists – the relevant question, however, is how long an organisation remains blind in a real incident and what happens during that time. This whitepaper analyses the regulatory gap, examines concentration risks in third-party providers and AI tools, and provides concrete recommendations: which questions providers must be able to answer – and what should be contractually addressed.

Auf einen Blick:

- **Die Ausgangslage:** KI-gestützte Angriffswerkzeuge haben die Zeit zwischen Bekanntwerden einer Schwachstelle und ihrer aktiven Ausnutzung auf durchschnittlich sieben Tage verkürzt. Patchen kommt damit strukturell zu spät – die Grundannahme muss sich von „vermutlich sicher" zu „vermutlich kompromittiert, bis das Gegenteil bewiesen ist" verschieben (Assume Breach).
- **Die regulatorische Lücke:** DORA und NIS-2-RL verlangen, dass Prozesse existieren – nicht, dass sie schnell genug funktionieren. Weder Fristen noch Schwellenwerte für Time-to-Detect oder Time-to-Contain sind vorgegeben. Diese Lücke müssen Unternehmen selbst schließen.
- **Das Konzentrationsrisiko:** Ein Vorfall bei einem marktbeherrschenden Dienstleister oder KI-Tool trifft nicht nur einen Kunden, sondern potenziell alle gleichzeitig. Das Slaughter-Urteil des US Supreme Court vom 29. Juni 2026 zeigt zusätzlich, wie schnell auch die regulatorische Grundlage für Datentransfers in die USA wegfallen kann.
- **Was zu tun ist:** Das Whitepaper liefert konkrete Fragen für das Dienstleistergespräch (Kapitel 4), vertragliche Mindeststandards und Assume-Breach-Anforderungen (Kapitel 5) sowie ein Kontrollregime, das operative Wirksamkeit statt Prozessexistenz prüft.
- **Für wen:** Unternehmen ohne eigene Softwareentwicklung, die auf IKT-Drittdienstleister angewiesen sind – DORA-pflichtige Finanzunternehmen ebenso wie NIS-2-RL-pflichtige Einrichtungen.

1. Ausgangslage: Eine neue Qualität der Bedrohung

1.1 Die Stellungnahme der österreichischen FMA: Erwartung ohne Maßstab

Im Mai 2026 veröffentlichte die österreichische Finanzmarktaufsicht („FMA") eine Stellungnahme[1] zu den Auswirkungen KI-gestützter Angriffswerkzeuge auf die Cybersicherheit von Finanzunternehmen. Die Kernaussage: Die FMA *„erwartet, dass Finanzunternehmen aktuelle Empfehlungen zeitnah berücksichtigen und ihre bestehenden Maßnahmen gegebenenfalls anpassen*." CERT.at und CERT-EU werden als Quellengrundlage zitiert.

Was die Stellungnahme nicht liefert: Einen konkreten Maßstab, eine Differenzierung nach Institutsgröße oder Risikokategorie, oder eine Operationalisierung der Erwartung. Die einzige spezifische Handlungsempfehlung – die Abhaltung von Table-Top-Übungen – steht in einem bemerkenswerten Missverhältnis zu der Bedrohungslage, die die Stellungnahme selbst beschreibt.

Das ist gewiss keine Kritik an der FMA, sondern eine Beschreibung der strukturellen Grenze aufsichtlicher Kommunikation: Aufsichtsbehörden können Erwartungen formulieren, aber naturgemäß keine Betriebshandbücher schreiben. Die Lücke zwischen Erwartung und Operationalisierung müssen Unternehmen selbst schließen – und genau das ist Gegenstand dieses Whitepapers.

1.2 Was das deutsche BSI dazu sagt – und woher die Zahl „7 Tage" kommt

Das deutsche Bundesamt für Sicherheit in der Informationstechnik („BSI") referenziert in seinem Paper BITS-B 2026-262788-1032[2] vom 22. Juni 2026 einen zentralen Befund: Der durchschnittliche Vorsprung von Angreifern gegenüber Verteidigern nach Bekanntwerden einer Schwachstelle beträgt sieben Tage. Das bedeutet**, dass Schwachstellen im Durchschnitt bereits eine Woche vor Erscheinen eines Patches aktiv ausgenutzt werden**.

Die Ursprungsquelle dieser Zahl ist der M-Trends 2026 Bericht von Mandiant/Google Threat Intelligence Group[3], der auf empirischen Incident-Response-Einsätzen basiert. Eine unkritische Übernahme verbietet sich aus zwei Gründen. Erstens besteht eine mögliche Stichprobenverzerrung: Mandiant wird typischerweise für schwerwiegende, komplexe Vorfälle beauftragt, was den Durchschnitt nach oben verzerren kann. Zweitens befindet sich Mandiant in einer Position mit eigenem kommerziellen Interesse an der Darstellung der Bedrohungslage, da das Unternehmen selbst Threat-Detection- und Incident-Response-Dienstleistungen anbietet. Das macht die Daten nicht falsch, wohl aber einordnungsbedürftig – es handelt sich um Marktdaten eines relevanten, aber nicht neutralen Akteurs, nicht um eine unabhängig validierte Studie.

Eine zusätzliche methodische Einschränkung betrifft nicht die Geschwindigkeit der Bedrohungslage, sondern ihre Bewertung. Ausschließlich technische Bewertungskriterien wie der **CVSS-Base-Score** stoßen durch die Fähigkeit KI-gestützter Werkzeuge, einzelne Schwachstellen zu sogenannten **Exploit-Chains** zu verketten, an ihre Grenzen. Eine Exploit-Chain entsteht, wenn mehrere für sich genommen unscheinbare Schwachstellen so kombiniert werden, dass das Ergebnis ihrer Verknüpfung ein deutlich höheres Schadenspotenzial hat als jede einzelne Schwachstelle für sich.

Der Base Score bewertet eine Schwachstelle jedoch isoliert; er erfasst nicht, dass eine für sich genommen niedrig eingestufte Schwachstelle in Kombination mit einer zweiten, ebenfalls niedrig

[1] FMA Finanzmarktaufsicht, https://www.fma.gv.at/querschnittsthemen/dora/fma-aktivitaeten-zu-dora/, zuletzt aktualisiert am 23. Juni 2026; abgefragt am 30. Juni 2026.

[2] BSI Bundesamt für Sicherheit in der Informationstechnik, https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2026/2026-262788-1032.pdf?__blob=publicationFile&v=2, Version 1.0, 22. Juni 2026; abgefragt am 30. Juni 2026.

[3] Abrufbar unter https://cloud.google.com/security/resources/m-trends?hl=de (Achtung, Schranke – personenbezogene Daten müssen angegeben werden).

eingestuften Schwachstelle ein kritisches Gesamtrisiko ergeben kann – und dass KI-Modelle solche Kombinationen zunehmend automatisiert auffinden. Eine Risikobewertung, die ausschließlich auf dem Base Score basiert, unterschätzt damit systematisch das tatsächliche Bedrohungspotenzial. Das BSI empfiehlt daher eine Ergänzung um umgebungsabhängige Kriterien, etwa die **Environmental-Metrik der CVSS-Version 4.0**, die Faktoren wie die tatsächliche Erreichbarkeit eines Systems, vorhandene kompensierende Kontrollen und den spezifischen Geschäftskontext mit einbezieht.

Das BSI übernimmt die Zahl als Trendindikator, nicht als Naturgesetz – und das ist die angemessene Rahmung. Denn das Bild, das sich aus unabhängigen Quellen ergibt, ist konsistent:

- ENISA Threat Landscape 2025 (4.875 Incidents, Juli 2024 bis Juni 2025): Angreifer weaponisieren neue Schwachstellen binnen Tagen nach der Veröffentlichung. ENISA ist eine unabhängige EU-Behörde ohne kommerzielles Interesse an der Problemdarstellung, mit eigenem Methodikvorbehalt: Open-Source-Reporting liefert kein vollständiges Bild.
- Sophos Active Adversary Report 2026: 3,40 Stunden vom ersten Zugriff bis zum Active Directory-Durchgriff – rund 70 Prozent schneller als im Vorjahr. Diese Zahl beschreibt nicht den Zeitraum vor dem Patch, sondern was passiert, sobald ein Angreifer im System ist.

Die Zahl „7 Tage“ ist somit kein Fakt, sondern ein konsistentes Signal aus Quellen mit unterschiedlichen Methodiken und Interessenslagen. **Die Richtung ist eindeutig: Patching als primäre Schutzmaßnahme ist strukturell überholt.** Die erwähnten knapp dreieinhalb Stunden erklären, warum: Wer erst reagiert, wenn ein Angreifer bereits im System ist, hat bereits verloren.

1.3 Die Beweislastumkehr: Von "wahrscheinlich sicher" zu "wahrscheinlich kompromittiert"

Die in 1.2 dargestellten Zahlen beschreiben eine Geschwindigkeit. Ihre eigentliche Konsequenz liegt jedoch nicht in der Geschwindigkeit selbst, sondern in einem **Paradigmenwechsel**: Einer Verschiebung der Grundannahme, mit der Organisationen auf neu bekannt gewordene Schwachstellen reagieren. Das BSI formuliert das in BITS-B 2026-262788-1032 unmissverständlich: Auf Basis der mit KI einhergehenden vereinfachten und beschleunigten Exploit-Entwicklung sei grundsätzlich davon auszugehen, dass nachträglich gepatchte **Zero-Day-Schwachstellen**[4] bereits ausgenutzt wurden – es sei denn, das Gegenteil wird festgestellt.

Diese Verschiebung geht über eine graduelle Verschärfung hinaus: **Sie kehrt die Beweislast um**. Die bisherige, implizite Default-Annahme in den meisten Security-Prozessen lautete: Ein System gilt als unkompromittiert, bis ein Vorfall erkannt wird. Patchen schließt die Lücke, der Zustand davor gilt retrospektiv als unbedenklich, solange kein Alarm geschlagen hat. Diese Annahme war plausibel, solange der Zeitraum zwischen Disclosure und Exploitation lang genug war, dass Patchen real eine Chance hatte, der Ausnutzung zuvorzukommen.

Genau diese Bedingung ist nicht mehr gegeben. Werden Schwachstellen im Durchschnitt bereits vor Erscheinen eines Patches ausgenutzt, kehrt sich die bisher sinnvolle Default-Annahme um: Ein System, für das eine relevante Schwachstelle bekannt wurde, gilt als kompromittiert, bis durch aktive Prüfung das Gegenteil festgestellt ist. Die Ausnahme, die bewiesen werden muss, ist eine andere geworden: Früher der Vorfall, heute die Unversehrtheit.

Diese Umkehr hat eine direkte Konsequenz für die Priorisierung von Sicherheitsmaßnahmen: Kommt das Patchen strukturell zu spät, kann es nicht mehr die primäre Schutzmaßnahme sein, sondern

[4] Anm.: Eine Zero-Day-Schwachstelle ist eine Sicherheitslücke, die zum Zeitpunkt ihres Bekanntwerdens noch nicht durch einen Patch des Herstellers behoben werden konnte – der Begriff verweist darauf, dass dem Hersteller "null Tage" zur Verfügung standen, um die Lücke zu schließen, bevor sie öffentlich oder durch Angreifer bekannt wurde.

wird zu einer von mehreren – gleichrangig neben der Fähigkeit, eine bereits erfolgte Kompromittierung zu erkennen. **Detection wird damit nicht zur Ergänzung des Patch-Managements**, sondern in der Priorität gleichwertig oder vorrangig. Eine Organisation, die ihre Ressourcen weiterhin primär auf Patch-Geschwindigkeit statt auf Detection-Fähigkeit ausrichtet, optimiert auf jene Maßnahme, die laut BSI strukturell zu spät kommt, und vernachlässigt jene, die zeigen würde, dass es bereits zu spät war.

Diese Verschiebung ist der eigentliche Kern dessen, was „**Assume Breach**" bedeutet: Kein zusätzliches Sicherheitsmodul neben der bestehenden Praxis, sondern der Paradigmenwechsel selbst, aus dem sich andere Prioritäten ableiten.

1.4 Scope: Zielgruppe und Geltungsbereich

Dieses Whitepaper richtet sich dezidiert an Unternehmen ohne eigene Softwareentwicklung – also Organisationen, die vollständig oder überwiegend auf IKT-Drittdienstleister angewiesen sind. Das betrifft DORA-pflichtige Finanzunternehmen ebenso wie NIS-2-RL-pflichtige Einrichtungen außerhalb des Finanzsektors.

Diese Gruppe befindet sich in einer spezifischen strukturellen Position: Sie verfügt über weniger Handlungsspielraum als Organisationen mit eigener Entwicklung, da sie Patches nicht selbst erstellen kann. Gleichzeitig ist ihre Abhängigkeit von Dritten entsprechend höher. Die Frage, welche Fähigkeiten Dienstleister nachweisen müssen und was vertraglich abgesichert sein sollte, ist für diese Gruppe daher keine akademische, sondern eine Frage von unmittelbarer praktischer Tragweite.

2. Was der Rechtsrahmen verlangt – und wo er aufhört

2.1 DORA und die EBA Guidelines: Prozessexistenz statt Prozesseffektivität

Art. 28 ff. DORA[5] verpflichtet Finanzunternehmen im Rahmen des IKT-Drittparteienrisikomanagements – als Teilbereich des umfassenderen, bereits in Art. 5 und Art 6 DORA verankerten IKT-Risikomanagementrahmens – zu spezifischen Anforderungen an Risikobewertung, Vertragsgestaltung und laufende Überwachung von IKT-Drittdienstleistern.

Kapitel V DORA verlangt in Abschnitt I unter dem Titel „Schlüsselprinzipien für ein solides Management des IKT-Drittparteienrisikos" (Art 28ff DORA) u.a. eine Risikobewertung vor Vertragsschluss, vertragliche Mindestanforderungen, ein Informationsregister und Exit-Pläne. Konkretisiert werden diese Anforderungen durch die zu DORA ergangenen technischen Regulierungsstandards (Regulatory Technical Standards, RTS), die von den European Supervisory Authorities (EBA European Banking Authority, ESMA European Securities and Markets Authority, EIOPA European Insurance and Occupational Pensions Authority) gemeinsam erarbeitet wurden – insbesondere die Delegierte Verordnung (EU) 2024/1774 zum IKT-Risikomanagementrahmen[6] und die Delegierte Verordnung (EU) 2024/1773 zur Spezifizierung der Kriterien für die Ausgestaltung von Verträgen mit IKT-Drittdienstleistern[7].

Auch diese Standards bleiben jedoch auf Prozessebene: Sie verlangen Verfahren zur Erkennung anormaler Aktivitäten und zur Reaktion auf IKT-Vorfälle, ohne konkrete Schwellenwerte, Zeitfenster

[5] Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011 („DORA").

[6] Delegierte Verordnung (EU) 2024/1774 der Kommission vom 13. März 2024 zur Ergänzung der Verordnung (EU) 2022/2554 durch technische Regulierungsstandards zur Festlegung der Tools, Methoden, Prozesse und Richtlinien für das IKT-Risikomanagement und des vereinfachten IKT-Risikomanagementrahmens.

[7] Delegierte Verordnung (EU) 2024/1773 der Kommission vom 13. März 2024 zur Ergänzung der Verordnung (EU) 2022/2554 durch technische Regulierungsstandards zur Spezifizierung des detaillierten Inhalts der Leitlinie für vertragliche Vereinbarungen über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen, die von IKT-Drittdienstleistern bereitgestellt werden.

oder Scan-Frequenzen festzulegen. Die Lücke zwischen Prozessexistenz und Prozesseffektivität bleibt damit auch nach diesen technischen Regulierungsstandards bestehen.

Dahinter steckt kein Versäumnis des Gesetzgebers, sondern eine strukturelle Grenze regulatorischer Normierung. Ein Rechtsrahmen kann Pflichten formulieren, aber nicht die operative Geschwindigkeit einer Organisation vorschreiben.

Das bedeutet in der Praxis: Eine Organisation kann sämtliche DORA-Anforderungen formal erfüllen – Risikobewertungen durchführen, Verfahren dokumentieren, Berichte vorlegen – und trotzdem nicht in der Lage sein, eine Schwachstelle innerhalb der vom BSI beschriebenen Zeitfenster zu erkennen oder zu beheben. **Compliance mit DORA stellt sicher, dass die richtigen Prozesse existieren; sie stellt nicht sicher, dass diese Prozesse schnell genug funktionieren, um der in Kapitel 1.3 beschriebenen Beweislastumkehr gerecht zu werden.**

2.2 NIS-2-RL/NISG 2026: Dieselbe Lücke, allerdings ohne den regulatorischen Überbau

Die NIS-2-Richtlinie[8] und das österreichische NISG 2026[9] stellen an betroffene Einrichtungen vergleichbare Anforderungen an das Supply-Chain-Risikomanagement. Art. 21 Abs 2 lit d NIS-2-RL-Richtlinie verlangt Maßnahmen für die Sicherheit der Lieferkette, einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen Einrichtungen und ihren unmittelbaren Anbietern.

Die strukturelle Lücke ist hier dieselbe wie bei DORA: Prozessexistenz wird verlangt, Prozesseffektivität nicht. Für NIS-2-RL-pflichtige Unternehmen außerhalb des Finanzsektors kommt erschwerend hinzu, dass der Konkretisierungsversuch der RTS fehlt – der Rechtsrahmen endet also noch früher.

Auch die Materialien zum NISG 2026 selbst schaffen hier keine zusätzliche Klarheit: Die Erläuterungen zum Gesetz bleiben an den hier relevanten Stellen auf einem Abstraktionsniveau, das für die operative Umsetzung wenig hergibt. Mangels einer eigenen österreichischen Verordnung zu den Risikomanagementmaßnahmen empfiehlt selbst die Wirtschaftskammer Österreich, sich branchenübergreifend an der EU-Durchführungsverordnung (EU) 2024/2690[10] zu orientieren – einer Verordnung, die ursprünglich ausschließlich für digitale Infrastruktur-Einrichtungen wie Telekommunikationsanbieter konzipiert wurde. Substanziell ändert das wenig: Auch dieser Anhang erschöpft sich im Wesentlichen in listenartig aneinandergereihten Themenfeldern – "Risikomanagementrahmen", "Überwachung der Einhaltung", "Sicherheitsmaßnahmen beim Erwerb von IKT-Diensten" – ohne auch nur ansatzweise zu klären, was unter diesen Punkten inhaltlich konkret verlangt wird. Eine Organisation, die anhand dieses Anhangs beurteilen will, ob ihre Maßnahmen ausreichen, betreibt im Ergebnis Kaffeesudlesen: Die Stichworte sind vorhanden, ihre Auslegung bleibt vollständig offen.

Bezeichnend ist, dass selbst die Wirtschaftskammer Österreich an dieser Stelle in eine ähnliche Hilflosigkeit gerät. Speziell zum Nachweis der Lieferketten-Sicherheit verweist die WKO auf das KSÖ

[8] Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 („NIS-2-Richtlinie", „NIS-2-RL").

[9] Bundesgesetz, mit dem das Bundesgesetz zur Gewährleistung eines hohen Cybersicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz 2026 – NISG 2026) erlassen wird und das Telekommunikationsgesetz 2021 und das Gesundheitstelematikgesetz 2012 geändert werden („NISG 2026"), idgF BGBl. I Nr. 94/2025.

[10] Durchführungsverordnung (EU) 2024/2690 der Kommission vom 17. Oktober 2024 mit Durchführungsbestimmungen zur Richtlinie (EU) 2022/2555 im Hinblick auf die technischen und methodischen Anforderungen der Risikomanagementmaßnahmen im Bereich der Cybersicherheit und die Präzisierung der Fälle, in denen ein Sicherheitsvorfall in Bezug auf DNS-Diensteanbieter, TLD-Namenregister, Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltszustellnetzen, Anbieter verwalteter Dienste, Anbieter verwalteter Sicherheitsdienste, Anbieter von Online-Marktplätzen, Online-Suchmaschinen und Plattformen für Dienste sozialer Netzwerke und Vertrauensdiensteanbieter als erheblich gilt.

Cyber Risk Rating als mögliches Instrument. Bei näherer Betrachtung der zugrundeliegenden Schema Policy zeigt sich jedoch ein strukturelles Problem: Sowohl das B Rating als auch das A Rating beruhen ausschließlich auf Selbstdeklaration der bewerteten Organisation – einem first-party conformity assessment ohne unabhängige Vor-Ort-Prüfung. Eine externe, unabhängige Prüfung (third-party conformity assessment) erfolgt erst beim A+ Rating, der Voraussetzung für das Goldlabel. Ein „Sicherheitsnachweis", der in seinen beiden niedrigsten und am weitesten verbreiteten Stufen ausschließlich auf Selbstauskunft beruht, ist kein Nachweis von Wirksamkeit, sondern von Auskunftsbereitschaft. Dies ist keine Kritik am KSÖ-Schema selbst, das diese Einschränkung in seiner Schema Policy transparent offenlegt – es ist eine Beobachtung über die Grenzen dessen, was ein freiwilliges, primär auf Selbstauskunft basierendes Instrument leisten kann. Selbst die Institution, die hier konkrete Orientierung in Aussicht stellt, mündet damit faktisch in dieselbe Lücke zwischen Prozessexistenz und Prozesseffektivität, die diesen Rechtsrahmen insgesamt kennzeichnet.

Das schafft eine paradoxe Situation: DORA-pflichtige Finanzunternehmen haben mehr regulatorische Pflichten, aber auch mehr Guidance. NIS-2-RL-pflichtige Unternehmen anderer Sektoren haben weniger Pflichten auf dem Papier, müssen aber dieselbe operative Lücke schließen – mit weitaus weniger Orientierung.

2.3 Zwischenfazit: Die falsche Frage

Der Rechtsrahmen beantwortet die Frage, ob ein Prozess existiert. Die unter KI-beschleunigter Bedrohungslage entscheidende Frage lautet jedoch: Wie lange ist eine Organisation blind, und was geschieht in dieser Zeit?

Diese beiden Fragen sind nicht graduell, sondern strukturell verschieden – und keine derzeit geltende Norm stellt die zweite. Auch keine Aufsichtsbehörde, einschließlich der FMA mit ihrer eigenen Stellungnahme, hat bislang einen Maßstab definiert, der auf Time-to-Detect oder Time-to-Contain abstellt.[11] Wer auf regulatorische Konkretisierung wartet, wartet nicht ab – er nimmt den strukturellen Nachteil bewusst in Kauf.

3. Konzentrationsrisiko: Marktstruktur als unterschätzter Risikofaktor

3.1 Drittdienstleister-Konzentration: Wenn ein Angriff systemisch wird

Ein Sicherheitsvorfall beim Dienstleister betrifft nicht nur den jeweiligen einzelnen Auftraggeber – er betrifft potenziell alle weiteren Auftraggeber desselben Dienstleisters gleichzeitig. Dieses Risiko lässt sich empirisch beobachten: Wenn ein signifikanter Anteil kritischer Infrastruktur auf denselben Anbieter für Edge-Security, Netzwerkkomponenten oder Security-Monitoring setzt, wird ein erfolgreicher Angriff auf diesen Anbieter zu einem systemischen Ereignis.

Das Problem liegt in der Struktur des Marktes selbst – nicht bei einzelnen Anbietern. Dass leistungsfähige, kosteneffiziente Anbieter Marktanteile gewinnen, ist ökonomisch rational und aus Sicht einzelner Unternehmen nachvollziehbar. Die systemische Konsequenz ist jedoch, dass Konzentration **strukturelle Abhängigkeiten** erzeugt: Ein Ausfall oder eine Kompromittierung eines marktbeherrschenden Anbieters entfaltet Wirkung weit über das einzelne betroffene Unternehmen hinaus — und trifft potenziell einen signifikanten Teil der gesamten Nutzergemeinschaft gleichzeitig.

[11] **Time-to-Detect** (auch **Mean Time to Detect, MTTD**) bezeichnet die durchschnittliche Zeitspanne zwischen dem Beginn eines Sicherheitsvorfalls und seiner Erkennung durch die betroffene Organisation. **Time-to-Contain** (**Mean Time to Contain, MTTC**) bezeichnet die durchschnittliche Zeitspanne von der Erkennung eines Vorfalls bis zu dessen wirksamer Eindämmung. Beide Begriffe finden sich als solche in keinem der hier besprochenen Rechtsrahmen. Art. 23 Abs. 2 lit. c der Delegierten Verordnung (EU) 2024/1774 verlangt zwar, dass Erkennungs- und Reaktionsprozesse innerhalb eines vordefinierten Zeitraums abzuarbeiten sind – die Definition dieses Zeitraums obliegt jedoch dem Finanzunternehmen selbst. Ein verbindlicher, regulatorisch vorgegebener Schwellenwert für Time-to-Detect oder Time-to-Contain existiert damit nicht.

DORA und NIS-2-RL adressieren dieses Risiko — und bleiben dabei auf der Prozessebene. Ein dokumentierter Exit-Plan ist keine Exit-Fähigkeit. Beide Regelwerke definieren weder, welche Qualitätsanforderungen ein Exit-Plan erfüllen muss, noch verlangen sie einen Nachweis, dass er unter realen Bedingungen tatsächlich funktioniert. Die Frage, ob eine Organisation in der Lage ist, einen marktbeherrschenden Dienstleister tatsächlich zu ersetzen, bleibt damit regulatorisch unbeantwortet. Dass dies keine akademische Frage ist, zeigt die **laufende IT-Umstellung des österreichischen Justizministeriums:** Die Ablösung von Microsoft Office durch LibreOffice an rund 20.000 Arbeitsplätzen offenbarte Systemabhängigkeiten, die bei der Planung nicht vollständig erfasst worden waren — von der Inkompatibilität eingehender Excel- und Word-Dateien externer Stellen bis hin zu Teilen der Justizverwaltung, die mangels Alternative gar nicht erst umgestellt werden. Der Prozess ist nach Angaben des Ministeriums selbst noch nicht abgeschlossen (Stand Oktober 2025)[12].

3.2 KI-Tool-Konzentration: Die zweite Abhängigkeitsebene

Verschärft wird das durch eine strukturelle Lücke, die die deutsche Aufsichtsbehörde Bundesanstalt für Finanzdienstleistungsaufsicht („BaFin“) in ihrer Orientierungshilfe vom 18. Dezember 2025 explizit benennt — KI-Systeme müssen explizit in den bestehenden IKT-Risikomanagementrahmen integriert werden — eine Anforderung, deren Formulierung impliziert, dass dies in der Praxis nicht selbstverständlich ist.[13] Die Konsequenz ist regulatorisch eindeutig: Ein KI-Anbieter, der nicht im Informationsregister nach Art. 28 Abs. 3 DORA erfasst ist, wird nicht überwacht, nicht als Konzentrationsrisiko bewertet und hat keinen Exit-Plan.

3.3 Regulatorisches Konzentrationsrisiko: Wenn die Rechtsgrundlage wegfällt

Konzentrationsrisiko ist nicht nur ein technisches oder marktstrukturelles Phänomen. Es kann auch auf Ebene des Rechtsrahmens entstehen – wenn ein zentrales regulatorisches Instrument auf einer institutionellen Annahme beruht, die quasi über Nacht wegfällt.

Ein aktuelles Beispiel: Am 29. Juni 2026 hat der US Supreme Court in einem 6:3-Urteil entlang ideologischer Linien die 91 Jahre alte Präzedenzentscheidung „Humphrey's Executor v. United States" (1935) aufgehoben und damit Trumps Entlassung von Federal Trade Comission („FTC“) Kommissarin Rebecca Slaughter als rechtmäßig bestätigt. Der Syllabus des Urteils fasst die Kernaussage zusammen: „What text, history, and structure settle, the Court's precedent confirms—the President may remove his subordinates at will."[14] Justice Neil Gorsuch hielt in seiner zustimmenden Meinung fest, dass der Kongress die ihm erteilten Befugnisse möglicherweise neu überdenken müsse — denn: „independent agencies are not so independent after all."[15]

Die FTC – bisher als unabhängige Behörde konstruiert – ist damit faktisch zu einer politisch weisungsgebundenen Stelle geworden.

Für den EU-US-Datenschutzrahmen (Data Privacy Framework, „DPF“) hat das unmittelbare Konsequenzen. Die Europäische Kommission stützt sich im DPF-Angemessenheitsbeschluss insgesamt 259 Mal auf die FTC — und zwar nicht nur als Durchsetzungsbehörde, sondern ausdrücklich auf deren Unabhängigkeit. Art. 8 Abs. 3 GRC und Art. 16 Abs. 2 AEUV verlangen, dass die Überwachung des

[12] Renate Graber, „Prozentzeichen statt Bundesadler: Wie die Justiz ihre IT umstellt", DER STANDARD, 24. Oktober 2025, https://www.derstandard.at/story/3000000293383/prozentzeichen-statt-bundesadler-wie-die-justiz-ihre-it-umstellt.

[13] Bundesanstalt für Finanzdienstleistungsaufsicht BaFin, „Orientierungshilfe zu IKT-Risiken beim Einsatz von Künstlicher Intelligenz in Finanzunternehmen", 18. Dezember 2025, https://www.bafin.de/SharedDocs/Downloads/DE/Anlage/dl_Anlage_orientierungshilfe_IKT_Risiken_bei_KI.pdf?__blob=publicationFile&v=1.

[14] US Supreme Court, Trump v. Slaughter, No. 25–332, Urteil vom 29. Juni 2026, Syllabus, S. 3, https://www.supremecourt.gov/opinions/25pdf/25-332_qn12.pdf.

[15] US Supreme Court, Trump v. Slaughter, No. 25–332, Urteil vom 29. Juni 2026, Concurring Opinion Justice Gorsuch, S. 13, https://www.supremecourt.gov/opinions/25pdf/25-332_qn12.pdf.

Datenschutzes durch eine unabhängige Stelle erfolgt; dasselbe Erfordernis gilt für Drittstaaten, denen ein angemessenes Schutzniveau attestiert wird. Ob die FTC nach dem heutigen Urteil dieses Kriterium noch erfüllt, ist eine Rechtsfrage, die letztlich der EuGH zu beurteilen haben wird. Max Schrems formulierte es so: „Entscheidend ist, dass der verfassungsrechtliche Rahmen der EU eine unabhängige Aufsicht vorschreibt. Die einzige Möglichkeit, dies zu ändern, wäre ein einstimmiger Beschluss aller EU-Mitgliedstaaten zur Änderung der EU-Verträge."[16]

noyb hat der Europäischen Kommission noch am selben Tag einen formalen Brief geschickt und eine Klage vor dem EuGH für die kommenden Wochen angekündigt — mit der realistischen Einschätzung einer Verfahrensdauer von zwei bis drei Jahren. Bis zu einer Aufhebung durch die Kommission selbst oder einem EuGH-Urteil bleibt der DPF-Beschluss formal in Kraft.

Für das Risikomanagement bedeutet das bereits heute: Organisationen, die personenbezogene Daten auf Basis des DPF in die USA übertragen, stützen sich auf eine Rechtsgrundlage, deren institutionelle Voraussetzungen weggefallen sind. Das illustriert eine Dimension des Konzentrationsrisikos, die in den meisten Risikobetrachtungen noch nicht systematisch erfasst wird: Die regulatorische. Ein einzelnes Gerichtsurteil in einem Drittstaat kann die Transferbasis für einen signifikanten Teil des europäischen Datenverkehrs in die USA in Frage stellen — nicht weil ein Anbieter kompromittiert wurde, sondern weil eine politische Entscheidung eine regulatorische Annahme ausgehebelt hat, auf der Millionen von Verarbeitungsvorgängen beruhen.

Entscheidend für die Praxis ist, dass auch der Rückgriff auf Standardvertragsklauseln (SCC) anstelle des DPF das strukturelle Problem nicht löst. noyb weist in seiner Stellungnahme vom 29. Juni 2026 ausdrücklich darauf hin, dass SCC- und BCR-gestützte Transfers in der Regel auf einem Transfer Impact Assessment beruhen, das seinerseits die Wirksamkeit vormals unabhängiger US-Stellen wie des Privacy and Civil Liberties Oversight Board („PCLOB") oder des Data Protection Review Court voraussetzt.[17] Ob und inwieweit der Wegfall der institutionellen Unabhängigkeit dieser Stellen die Tragfähigkeit bestehender TIAs berührt, ist eine Rechtsfrage, die gerichtlich noch nicht geklärt ist — die Antwort des EuGH wird auch hier die entscheidende sein.

Das ist im österreichischen Kontext kein neuer Gedanke — die österreichische Datenschutzbehörde („DSB") hat die strukturelle Problematik bereits zwei Jahre vor dem heutigen Urteil präzise benannt. Mit Bescheid vom 2. Oktober 2024 (2023-0.243.883, DSB-D124.0640/22) stellte die DSB klar, dass SCC allein nicht ausreichen, wenn das Recht des Drittlands ihre Wirksamkeit beeinträchtigt — und dass auch zusätzlich vereinbarte Schutzmaßnahmen wirkungslos bleiben, solange sie die konkrete Rechtsschutzlücke nicht schließen: Die Zugriffs- und Überwachungsmöglichkeiten US-amerikanischer Nachrichtendienste. Fehlt ein Instrument nach Kapitel V DSGVO, das ein angemessenes Schutzniveau tatsächlich gewährleistet, liegt eine Verletzung von Art. 44 DSGVO vor — unabhängig davon, welches Transferinstrument formal gewählt wurde.

Die Slaughter-Entscheidung fügt dieser Analyse eine weitere Dimension hinzu: Mit dem Wegfall der FTC-Unabhängigkeit fehlt nun auch die institutionelle Durchsetzungsebene, auf deren Existenz sich sowohl der DPF-Beschluss als auch die gängige SCC-Praxis bislang gestützt haben. Ob Transfer Impact Assessments, die auf dieser institutionellen Grundlage beruhen, einer gerichtlichen Überprüfung standhalten, ist eine Frage, die der EuGH zu beantworten haben wird — die DSB hat die Richtung dieser Antwort bereits 2024 vorgezeichnet.

3.4 Konsequenzen für die Praxis

[16] noyb, „Supreme Court hat EU-US Datendeal (nebenbei) zerstört", 29. Juni 2026, https://noyb.eu/de/us-supreme-court-just-blew-eu-us-data-transfers.
[17] Ebenda.

Die in den vorangegangenen Abschnitten beschriebenen Konzentrationsrisiken haben konkrete regulatorische und operative Konsequenzen, die unabhängig davon eintreten, ob eine Organisation aktiv handelt oder nicht.

Regulatorisch:

DORA verpflichtet Finanzunternehmen, sämtliche vertraglichen Vereinbarungen mit IKT-Drittdienstleistern im Informationsregister zu erfassen — unabhängig davon, ob sie kritische oder wichtige Funktionen unterstützen. KI-Anbieter und Security-Tool-Anbieter, die nicht erfasst sind, erzeugen damit nicht nur ein operatives Risiko, sondern eine unmittelbare Compliance-Lücke.

Darüber hinaus verpflichtet Art. 28 Abs. 4 lit. c DORA Finanzunternehmen, bei jeder vertraglichen Vereinbarung alle relevanten Risiken zu ermitteln und zu bewerten — einschließlich der Möglichkeit, dass diese Vereinbarung das in Art. 29 DORA genannte **IKT-Konzentrationsrisiko** erhöht. Art. 29 Abs. 1 DORA konkretisiert diese Bewertungspflicht für IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen: Finanzunternehmen haben zu berücksichtigen, ob der Dienstleister nicht ohne Weiteres ersetzbar ist oder ob mehrere Vereinbarungen mit demselben oder eng verbundenen Dienstleistern bestehen.

Für NIS-2-RL-pflichtige Unternehmen außerhalb des Finanzsektors fehlt eine vergleichbar explizite Anforderung — was nicht bedeutet, dass das Risiko nicht existiert, sondern lediglich, dass es regulatorisch bislang nicht adressiert wird.

Zudem: Art. 29 Abs. 2 DORA verpflichtet Finanzunternehmen, bei vertraglichen Vereinbarungen mit IKT-Drittdienstleistern mit Sitz in einem Drittland über IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen zusätzlich zu beachten, dass die Datenschutzvorschriften der Union eingehalten und die Rechtsvorschriften in diesem Drittland wirksam durchgesetzt werden. Mit dem Wegfall der FTC-Unabhängigkeit ist genau diese Durchsetzbarkeit strukturell in Frage gestellt — nicht als abstrakte Möglichkeit, sondern als konkrete regulatorische Realität. DORA-konforme Vertragsbeziehungen mit US-basierten IKT-Drittdienstleistern sind nach dem Slaughter-Urteil damit nicht mehr ohne weiteres darstellbar.

Hinzu kommt eine weitere Ebene: Die Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO verlangt, dass eine Organisation die Rechtmäßigkeit ihrer Verarbeitungstätigkeiten — einschließlich ihrer Drittlandübermittlungen — jederzeit nachweisen kann. Transfer Impact Assessments, die vor dem 29. Juni 2026 auf der Grundlage einer unabhängigen FTC erstellt wurden, bilden die veränderte institutionelle Realität nicht mehr ab. Ihre Überprüfung und Aktualisierung ist damit keine freiwillige Sorgfaltsmaßnahme, sondern eine Voraussetzung dafür, der Rechenschaftspflicht überhaupt nachkommen zu können — und eine, die den ohnehin komplexen Prozess der Drittlandbewertung nach Kapitel V DSGVO zusätzlich belastet.

Operativ:

Das Charakteristische an Konzentrationsrisiko ist die Gleichzeitigkeit: Dasselbe Ereignis trifft viele Organisationen zur selben Zeit. Im Ernstfall — ob Cyberangriff auf einen marktbeherrschenden Security-Anbieter, Ausfall eines dominanten Cloud-Providers oder Aufhebung eines Angemessenheitsbeschlusses — stehen alle betroffenen Organisationen gleichzeitig vor denselben Problemen. Sie konkurrieren um dieselben Ausweichkapazitäten, dieselben Beratungsressourcen, dieselben Alternativanbieter — unter demselben Zeitdruck, zu demselben Zeitpunkt.

Das hat eine direkte Konsequenz für die Bewertung von Exit-Plänen: Ein Exit-Plan, der unter Normalbedingungen funktioniert, ist kein Nachweis von Exit-Fähigkeit. Art. 28 Abs. 8 DORA verlangt, dass Exit-Pläne im Einklang mit Art. 4 Abs. 2 DORA ausreichend getestet und regelmäßig überprüft werden. Der dort verankerte Verhältnismäßigkeitsmaßstab stellt auf Größe, Gesamtrisikoprofil sowie

Art, Umfang und Komplexität der Dienstleistungen des einzelnen Unternehmens ab — nicht auf systemische Marktstrukturrisiken. **Weder DORA noch die ergänzenden RTS verlangen, dass ein Exit-Plan unter den Bedingungen getestet wird, unter denen Konzentrationsrisiko tatsächlich schlagend wird:** Wenn viele Organisationen gleichzeitig denselben Exit suchen, Alternativkapazitäten knapp sind und Zeitdruck herrscht. Genau das ist die Bedingung, unter der ein Exit-Plan gebraucht wird — und genau das ist die Bedingung, für die kein regulatorischer Nachweis verlangt wird. Das ist die Lücke, die im Kontext von Konzentrationsrisiko am schwersten wiegt.

4. Die Fragen, die kein Zertifikat beantwortet

4.1 Das Zertifikat und die falsche Frage

Eine ISO 27001-Zertifizierung belegt, dass eine Organisation einen dokumentierten ISMS-Prozess hat, der vom Leitungsorgan freigegeben und mindestens einmal jährlich überprüft wird. Anhang A 8.8 der ISO 27001:2022 beispielsweise — „Handhabung von technischen Schwachstellen" — verlangt, dass Informationen über technische Schwachstellen verwendeter Informationssysteme eingeholt, die Gefährdung der Organisation bewertet und angemessene Maßnahmen ergriffen werden. Was als „angemessen" gilt, definiert die Organisation selbst — der Standard setzt keine Schwellenwerte für Scan-Frequenz, keine maximale Zeit zwischen CVE-Veröffentlichung und Behebung, keine definierte Mean Time to Detect. Eine Organisation kann das Zertifikat halten und gleichzeitig eine Patch-Latenz haben, die weit außerhalb der in Kapitel 1.2 beschriebenen Zeitfenster liegt — solange sie das intern als akzeptables Risikoniveau dokumentiert und die Wirksamkeitsbewertung entsprechend gestaltet. Die Norm überträgt die Definition von „wirksam" damit weitgehend an die Organisation selbst — und an den Auditor, der diese Selbstdefinition überprüft. Dass diese Konstellation in der Praxis nicht immer zu dem führt, was der Begriff Wirksamkeit nahelegt, ist eine Beobachtung, die das Zertifikat allein nicht entkräften kann.

Das Zertifikat dokumentiert, dass ein Prozess existiert und formal bewertet wurde. Es dokumentiert nicht, was in jenen sieben Tagen passiert, die laut BSI zwischen Bekanntwerden einer Schwachstelle und ihrer aktiven Ausnutzung liegen.

4.2 Vulnerability Management

Die folgenden Fragen sind abgeleitet aus den in den vorangegangenen Kapiteln beschriebenen regulatorischen Lücken sowie aus einschlägigen Standards und aktueller Fachliteratur — insbesondere dem BSI (BITS-B 2026-262788-1032)[18], dem ENISA Threat Landscape 2025[19], der ENISA Technical Implementation Guidance on Cybersecurity Risk Management Measures[20], dem NIST SP 800-40 Rev. 4 (Patch Management)[21], dem NIST SP 800-61 Rev. 3 (Incident Response)[22], den CIS Critical Security Controls v8.1[23] sowie dem MITRE ATT&CK Framework[24].

[18] BSI, BITS-B 2026-262788-1032, 22. Juni 2026, https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2026/2026-262788-1032.pdf?__blob=publicationFile&v=2.

[19] ENISA, Threat Landscape 2025, Oktober 2025, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025.

[20] ENISA, Technical Implementation Guidance on Cybersecurity Risk Management Measures, Version 1.0, Juni 2025, https://www.enisa.europa.eu/sites/default/files/2025-06/ENISA_Technical_implementation_guidance_on_cybersecurity_risk_management_measures_version_1.0.pdf.

[21] National Institute of Standards and Technology NIST, SP 800-40 Rev. 4, Guide to Enterprise Patch Management Planning, April 2022, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r4.pdf.

[22] NIST, SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management, April 2025, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf.

[23] Center for Internet Security, CIS Critical Security Controls v8.1, https://www.cisecurity.org/controls/v8-1. (Achtung, Schranke – personenbezogene Daten müssen angegeben werden).

[24] MITRE, ATT&CK Framework, https://attack.mitre.org.

Sie stellen die persönliche fachliche Einschätzung der Autorin dar und können direkt im Dienstleistergespräch, als Teil eines strukturierten Fragebogens oder als Grundlage für ein technisches Interview genutzt werden.

Frage	Warum relevant	Warnsignal
Mit welcher Frequenz werden extern exponierte Systeme auf Schwachstellen gescannt?	Bei KI-beschleunigter Ausnutzung bekannter Schwachstellen ist wöchentliches Scanning strukturell zu langsam. Der relevante Maßstab ist kontinuierliches oder zumindest tägliches Scanning extern exponierter Systeme.	Keine konkrete Frequenzangabe; oder wöchentliches oder selteneres Scanning für extern exponierte Systeme.
Wie lang ist der durchschnittliche Zeitraum zwischen CVE-Veröffentlichung und internem Ticket? Gibt es Belege?	Die Belegpflicht ist entscheidend. Ohne Messung gibt es keine Steuerung. Wer diese Zahl nicht kennt, hat kein funktionierendes Vulnerability Management.	Keine Messung, keine Belegmöglichkeit, oder Durchschnitt über 48h für Critical CVEs.
Was passiert bei einem Critical CVSS außerhalb der Geschäftszeiten?	Was passiert bei einem Critical CVSS-Score außerhalb der Geschäftszeiten ist keine rhetorische Frage — Angreifer orientieren sich nicht an Betriebszeiten. Ein Eskalationsweg, der außerhalb der Kernzeiten nicht belastbar ist, erfüllt seinen Zweck nicht.	Keine dokumentierten Prozesse für die Behandlung kritischer Schwachstellen außerhalb der Geschäftszeiten; fehlende Rufbereitschaft oder Reaktionsfähigkeit für Critical-Ereignisse rund um die Uhr.
Welche der für unser Unternehmen betriebenen Systeme weisen aktuell bekannte Schwachstellen mit einem CVSS-Score von 7,0 oder höher auf, die in den letzten 90 Tagen veröffentlicht wurden?	Diese Frage ist kein Detailcheck, sondern ein Strukturtest: Wer sie nicht ad hoc beantworten kann, hat keine aktuelle und vollständige CMDB — die Grundvoraussetzung für jedes funktionsfähige Vulnerability Management. Ergänzend gilt: Der CVSS-Base-Score allein reicht nicht als Steuerungsgröße, wenn KI-gestützte Werkzeuge einzelne Schwachstellen zu Exploit-Chains verketten können. Eine Schwachstelle mit mittlerem Base-Score kann in Kombination mit einer zweiten ein kritisches Gesamtrisiko ergeben. Die CVSS-Version 4.0 Environmental-Metrik bildet diesen Kontext besser ab.	Keine unmittelbare Auskunft möglich oder Verweigerung; kein nachvollziehbarer Prozess erkennbar, der eine zeitnahe Beantwortung sicherstellt. Beides deutet darauf hin, dass keine aktuelle und vollständige CMDB vorhanden ist.
Wird External Attack Surface Management (EASM) eingesetzt, und wie aktuell ist das Inventar der von außen erreichbaren Systeme?	Ein internes Asset-Inventar erfasst, was die Organisation zu betreiben glaubt. EASM erfasst, was von außen tatsächlich sichtbar und erreichbar ist – inklusive Schatten-IT, vergessener Subdomains und Altsystemen, die niemand mehr auf dem Schirm hat. Das BSI führt EASM explizit als zentralen Baustein, weil Angreifer mit denselben Werkzeugen arbeiten: Sie scannen die Außensicht, nicht das interne CMDB (Configuration Management Database).	Kein EASM-Tool im Einsatz oder ausschließlicher Verweis auf ein internes Asset-Inventar, ohne nachvollziehbare Auskunft darüber, ob und wie die extern sichtbare Angriffsfläche erfasst und aktuell gehalten wird.

External Attack Surface Management (EASM) bezeichnet den kontinuierlichen Prozess der Identifikation, Inventarisierung und Überwachung aller von außen erreichbaren Assets einer Organisation — einschließlich solcher, die intern möglicherweise nicht bekannt sind: Vergessene Subdomains, nicht mehr aktiv betriebene aber noch erreichbare Systeme, exponierte Schnittstellen oder Cloud-Ressourcen, die außerhalb des formalen IT-Prozesses provisioniert wurden. EASM nimmt dabei bewusst die Außenperspektive ein — mit denselben Scan- und Reconnaissance-Methoden, die auch Angreifer verwenden, um potenzielle Angriffspunkte zu identifizieren.

Ein internes Vulnerability Management, das nur bekannte Systeme scannt, hat eine strukturelle Lücke: Es setzt voraus, dass die Organisation weiß, was extern erreichbar ist. Genau diese Voraussetzung ist in der Praxis häufig nicht erfüllt. EASM schließt diese Lücke, indem es nicht beim internen Asset-Inventar ansetzt, sondern beim tatsächlich sichtbaren Perimeter. Das BSI führt aufgrunddessen EASM als wesentlichen Bestandteil seiner Assume-Breach-Empfehlungen: Wer nicht weiß, was von außen sichtbar ist, kann weder schützen noch erkennen, ob ein Angriff bereits stattgefunden hat.

4.3 Angriffserkennung

Die folgenden Fragen zur Angriffserkennung sind direkt aus der in Kapitel 1.3 beschriebenen **Beweislastumkehr** abgeleitet: Wenn davon auszugehen ist, dass eine Kompromittierung bereits stattgefunden hat, bis das Gegenteil bewiesen ist, wird Angriffserkennung („Detection“) zur primären Schutzmaßnahme — nicht mehr Ergänzung des Patch-Managements. Die Grundlage für die nachfolgenden Fragen bilden der Sophos Active Adversary Report 2026[25], das MITRE ATT&CK Framework[26] sowie die ENISA Technical Implementation Guidance on Cybersecurity Risk Management Measures, Abschnitt 3.2 (Monitoring and Logging)[27]. Ergänzend fließen die CIS Critical Security Controls v8.1.2 ein, insbesondere Control 13 (Network Monitoring and Defense)[28].

Frage	Warum relevant	Warnsignale
Ist ein Security Incident and Event Management (System) SIEM im Einsatz – und wer wertet es aus, in welchem Zeitfenster und mit welcher Eskalationslogik?	Ein SIEM ohne definierten Auswertungsprozess und klare Verantwortlichkeiten erfüllt seinen Zweck nicht. Die entscheidende Variable ist nicht die Technologie, sondern ob die generierten Ereignisse von qualifizierten Personen innerhalb eines definierten Zeitrahmens bewertet und eskaliert werden.	Bestätigung des SIEM-Einsatzes ohne konkrete Auskunft darüber, wer die Auswertung vornimmt, in welchem Zeitfenster dies geschieht und welche Eskalationswege bei kritischen Ereignissen greifen.
Was ist die beim Dienstleister definierte Mean Time to Detect (MTTD) für bekannte Angriffsmuster?	Der Sophos Active Adversary Report 2026 dokumentiert eine mediane Zeit von 3,40 Stunden vom ersten Zugriff bis zur vollständigen Kompromittierung des Active Directory. Eine Mean Time to Detect ohne definierte Obergrenze — oder mit einer Obergrenze, die über diesem Schwellenwert liegt — bedeutet, dass eine Erkennung strukturell zu spät käme, um eine Eindämmung vor vollständiger Kompromittierung zu ermöglichen.	Keine definierte MTTD für bekannte Angriffsmuster; oder eine definierte MTTD, die den durch den Sophos-Report belegten medianen Zeitraum bis zum AD-Durchgriff überschreitet.
Ist die Organisation in der Lage, laterale Bewegungen im Netzwerk zu erkennen, bevor ein System kompromittiert ist?	Als Lateral Movement bezeichnet man die Technik, mit der sich ein Angreifer nach dem initialen Zugriff auf ein System schrittweise durch das Netzwerk bewegt, um weitere Systeme zu erreichen, Privilegien auszuweiten und letztlich sein Ziel — etwa den Zugriff auf kritische Systeme oder Daten — zu erlangen. Lateral Movement Detection ist die Grenze zwischen „Wir erkennen Angriffe" und „Wir erkennen Einbrüche":	Keine strukturierte Antwort auf die Frage; oder Bestätigung, dass Detection ausschließlich auf Basis von Endpoint-Alerts nach bereits erfolgter Kompromittierung erfolgt.

[25] Sophos, „Nowhere, man: The 2026 Active Adversary Report", 24. Februar 2026, https://www.sophos.com/en-us/blog/2026-sophos-active-adversary-report.

[26] MITRE, ATT&CK Framework, https://attack.mitre.org.

[27] ENISA, Technical Implementation Guidance on Cybersecurity Risk Management Measures, Version 1.0, Juni 2025, Abschnitt 3.2, https://www.enisa.europa.eu/sites/default/files/2025-06/ENISA_Technical_implementation_guidance_on_cybersecurity_risk_management_measures_version_1.0.pdf.

[28] Center for Internet Security, CIS Critical Security Controls v8.1, https://www.cisecurity.org/controls/v8-1. (Achtung, Schranke – personenbezogene Daten müssen angegeben werden).

Frage	Warum relevant	Warnsignale
	Wer ausschließlich auf Endpoint-Alerts reagiert, erkennt erst, wenn ein System bereits kompromittiert ist — nicht, während sich der Angreifer noch durch das Netzwerk bewegt.	
Wann wurde die Erkennungsfähigkeit zuletzt unter Echtbedingungen durch ein externes Red Team validiert?	Interne Penetrationstests überprüfen bekannte Angriffsvektoren gegen bekannte Systeme — sie testen, was der Tester weiß. Ein Red Team Exercise simuliert demgegenüber einen realen, zielgerichteten Angriff mit unbekannten Methoden gegen eine nicht vorinformierte Verteidigung und misst damit, was die Organisation tatsächlich erkennt und wie sie reagiert. Nur letzteres liefert belastbare Aussagen über die operative Erkennungsfähigkeit unter realer Bedrohungslage.	Kein Red Team Exercise in den letzten 24 Monaten nachweisbar; oder ausschließlicher Verweis auf interne Penetrationstests ohne externe, unabhängige Validierung der Erkennungsfähigkeit.

Das BSI hält in seinem BITS-B 2026-262788-1032 fest, Penetrationstests künftig „ggf. KI-unterstützt" durchzuführen.[29] Das ist, gemessen an der Geschwindigkeit, mit der KI-Werkzeuge die Angriffsoberfläche verändern, eine bemerkenswert zurückhaltende Formulierung — aber immerhin die einzige aufsichtliche Anerkennung, dass bisherige Testansätze unter KI-beschleunigter Bedrohungslage überprüft werden müssen. Für den österreichischen Finanzbereich gibt der TIBER-AT Implementation Guide (Oesterreichische Nationalbank, „OeNB"/FMA, Juli 2025)[30] einen organisatorischen Rahmen für bedrohungsorientierte Penetrationstests — einschließlich Anforderungen an die Auswahl von Red Teams und Dienstleistern. **Was TIBER-AT nicht liefert:** Scoping-Vorgaben, die reale Angriffsbedingungen abbilden — und KI-gestützte Angriffsszenarien kommen darin nicht vor. Für NIS-2-RL-pflichtige Unternehmen außerhalb des Finanzsektors fehlt selbst dieser unvollständige Rahmen.

4.4 Reaktionsfähigkeit

Die folgenden Fragen zur Reaktionsfähigkeit sind abgeleitet aus der in Kapitel 1.3 beschriebenen Beweislastumkehr und den operativen Konsequenzen der in Kapitel 1.2 dargestellten Zeitfenster: Wenn zwischen erstem Zugriff und vollständiger Kompromittierung im Durchschnitt rund dreieinhalb Stunden liegen, ist Reaktionsfähigkeit keine Ergänzung zur Detection — sie ist die letzte verbleibende Schutzmaßnahme, sobald Detection versagt hat oder zu spät einsetzt.

Die Grundlage für die nachfolgende Übersicht bilden die bereits erwähnten Frameworks NIST SP 800-61 Rev. 3 sowie die CIS Critical Security Controls v8.1.2, insbesondere Control 17 (Incident Response Management). Weiters stellen die Fragen in der Übersicht die persönliche fachliche Einschätzung der Autorin dar und können direkt im Dienstleistergespräch, als Teil eines strukturierten Fragebogens oder als Grundlage für ein technisches Interview genutzt werden.

[29] BSI, BITS-B 2026-262788-1032, 22. Juni 2026, https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2026/2026-262788-1032.pdf?__blob=publicationFile&v=2.

[30] OeNB/FMA, TIBER-AT Implementation Guide, Juli 2025, https://www.oenb.at/dam/jcr:0253da77-47da-44e9-979f-965d95222df1/2025-07-21-TIBER-AT-Implementation-Guide.pdf.

Frage	Warum relevant	Warnsignal
Verfügt der Dienstleister über einen vertraglich vorgebundenen Incident Response-Dienstleister — also einen Anbieter, der auf Basis eines bestehenden Rahmenvertrags im Ernstfall ohne vorherige Ausschreibung oder Vertragsverhandlung sofort aktiviert werden kann?	Zwischen erstem Zugriff und vollständiger Kompromittierung des Active Directory liegen laut Sophos Active Adversary Report 2026 durchschnittlich 3,40 Stunden. Eine Anbietersuche läuft in diesem Zeitfenster nicht ab.	Kein solcher Rahmenvertrag vorhanden; oder IR-Dienstleister wird anlassbezogen gesucht und beauftragt.
Wie viele tatsächliche Sicherheitsvorfälle hat der Dienstleister in den letzten zwölf Monaten für von ihm betriebene Systeme bearbeitet — nicht Tabletop-Übungen, sondern reale Incidents?	Tabletop-Übungen testen Prozesse unter Laborbedingungen. Reale Incidents testen sie unter Stress. Beides ist nicht gleichwertig.	Ausschließlicher Verweis auf jährliche Übungen ohne Erfahrung mit realen Incidents im letzten Jahr.
Besteht außerhalb der Geschäftszeiten dieselbe Reaktionsfähigkeit wie unter der Woche — einschließlich Entscheidungsbefugnis und Eskalationsweg?	Angriffe werden gezielt in Randzeiten platziert, da Erkennungs- und Reaktionsfähigkeit dort strukturell schwächer ist. Freitagabend vor Feiertagen ist in der Incident-Response-Praxis kein Klischee, sondern ein dokumentiertes Angriffsmuster.	Reduzierte Besetzung außerhalb der Kernzeiten ohne kompensatorische Maßnahmen; oder Eskalationswege, die außerhalb der Geschäftszeiten nicht durchgehend mit Entscheidungsbefugnis besetzt sind.
Welche Kommunikationsprozesse bestehen zwischen Dienstleister und Auftraggeber im Ernstfall — wer ist auf Seiten des Dienstleisters mit welcher Reaktionszeit erreichbar, und in welchem Format und Zeitfenster erfolgt die Erstmeldung?	Unter Art. 28 Abs. 1 lit a DORA bleibt das Finanzunternehmen für alle ausgelagerten IKT-Dienstleistungen vollumfänglich verantwortlich — Auslagerung überträgt die Tätigkeit, nicht die Haftung. Für NIS-2-RL-pflichtige Unternehmen ergibt sich dasselbe Prinzip aus Art. 21 NIS-2-Richtlinie. Ein Incident beim Dienstleister ist regulatorisch ein Incident des Auftraggebers — und das auftraggebende Unternehmen muss in der Lage sein, seiner eigenen Melde- und Reaktionspflicht nachzukommen, unabhängig davon, ob der Dienstleister seinerseits bereits reagiert hat.	Keine definierten Kommunikationsprozesse für den Ernstfall; oder Kommunikation beschränkt sich auf eine allgemeine Informationspflicht ohne festgelegten Zeitrahmen, Format und benannte Ansprechpersonen mit Entscheidungsbefugnis.

Die Fragen in diesem Abschnitt prüfen, ob Reaktionsfähigkeit im Ernstfall tatsächlich vorhanden ist. Ob sie vorhanden ist, hat jedoch nicht nur operative Konsequenzen — es hat regulatorische. Die 72-Stunden-Meldefrist nach Art. 33 DSGVO beginnt mit Kenntnis des Verantwortlichen — nicht mit Behebung des Vorfalls. Unter Art. 28 Abs. 1 lit. a DORA bleibt das Finanzunternehmen für alle ausgelagerten IKT-Dienstleistungen vollumfänglich verantwortlich — Auslagerung überträgt die Tätigkeit, nicht die Haftung. Kenntnis setzt voraus, dass der Dienstleister meldet, dass die Meldung den Auftraggeber erreicht und dass dieser in der Lage ist, den Vorfall einzuordnen und weiter zu melden. Kommunikationsprozesse, die im Ernstfall erst geklärt werden müssen, gefährden diese Kette strukturell. Reaktionsfähigkeit ist damit keine operative Frage allein — sie ist eine regulatorische.

Zusammengefasst:

Die drei Fragenblöcke dieses Kapitels folgen einer Logik, die sich direkt aus der in Kapitel 1.3 beschriebenen Beweislastumkehr ergibt: Vulnerability Management adressiert die Frage, ob bekannte Schwachstellen rechtzeitig erkannt und geschlossen werden. Angriffserkennung adressiert die Frage,

ob eine Kompromittierung innerhalb des in Kapitel 1.2 beschriebenen Zeitfensters festgestellt wird. Reaktionsfähigkeit adressiert die Frage, ob die Organisation — und ihr Dienstleister — in der Lage sind, auf eine festgestellte Kompromittierung so zu reagieren, dass regulatorische Pflichten eingehalten werden können.

Kein Zertifikat beantwortet diese Fragen. Sie müssen gestellt — und belegt — werden.

5. Was vertraglich geregelt sein muss — und was DORA und NIS-2-RL dabei schuldig bleiben

Die folgenden Anforderungen sind in drei Ebenen gegliedert: Basis-Anforderungen, die bereits heute aus DORA und NIS-2-RL ableitbar sind; eine Assume-Breach-Ebene, die über den bestehenden Rechtsrahmen hinausgeht, aber aus der in Kapitel 1.3 beschriebenen Beweislastumkehr und der FMA-Stellungnahme begründbar ist; sowie Kontrollen, die operative Wirksamkeit messen statt Prozessexistenz zu dokumentieren. Für jede Anforderung wird ausgewiesen, wo der Rechtsrahmen anknüpft — und wo er endet.

5.1 Vertragliche Mindeststandards: Der regulatorisch abgedeckte Bereich

Art. 30 Abs. 2 DORA enthält einen Katalog von Mindestinhalten, die vertragliche Vereinbarungen mit IKT-Drittdienstleistern enthalten müssen — darunter Anforderungen an Sicherheitsmaßnahmen, Meldepflichten und Audit-Rechte sowie Bestimmungen über Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit in Bezug auf den Datenschutz einschließlich des Schutzes personenbezogener Daten (Art 30 Abs 2 lit c DORA), die unmittelbar für das Schwachstellenmanagement relevant sind. Konkrete Fristen, Schwellenwerte oder operationale Mindeststandards gibt DORA dabei nicht vor. Die NIS-2-RL kennt vergleichbare Mindestvertragsstandards gegenüber Dienstleistern nicht. Die folgenden Anforderungen benennen, was DORA dem Grunde nach verlangt — und wie diese Anforderungen in der vertraglichen Praxis operationalisiert werden sollten, um tatsächlich wirksam zu sein.

Anforderung	Inhalt	Rechtsanknüpfung / Lücke
Patch-SLAs nach CVSS[31]	Critical (CVSS ≥ 9): ≤ 48 Stunden. High (CVSS 7–8,9): ≤ 7 Tage. Medium: ≤ 30 Tage. SLAs müssen messbar und dokumentiert sein.	Art. 30 Abs. 2 lit. c DORA (Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit in Bezug auf den Datenschutz einschließlich des Schutzes personenbezogener Daten) i.V.m. Art. 30 Abs. 2 lit. e DORA (Beschreibungen der Dienstleistungsgüte). Für kritische/wichtige Funktionen zusätzlich Art. 30 Abs. 3 DORA. Art. 21 Abs. 2 NIS-2-RL. Lücke: Keine Vorgabe konkreter Fristen oder Schwellenwerte.
Incident Notification	≤ 4 Stunden bei kritischen Ereignissen, unabhängig von Tageszeit oder Wochentag. Vordefiniertes Format und Eskalationsweg.	Art. 30 Abs. 2 lit. f DORA (Verpflichtung des IKT-Drittdienstleisters, bei einem IKT-Vorfall Unterstützung zu leisten). Art. 21 Abs 2 NIS-2-RL. Lücke: Konkrete Fristen im Verhältnis Dienstleister–Auftraggeber nicht vorgegeben.

[31] Anm.: SLA-Schwellenwerte sollten sich nicht ausschließlich am CVSS-Base-Score orientieren, sondern wo möglich die Environmental-Metrik (CVSS 4.0) berücksichtigen – insbesondere für Systeme, bei denen mehrere für sich genommen niedrig bewertete Schwachstellen in Kombination ein höheres Risiko ergeben können.

Anforderung	Inhalt	Rechtsanknüpfung / Lücke
Audit- und Pentestrechte	Recht auf Pentest sowie anlassbezogenes forensisches Audit nach Incident.	Art. 30 Abs. 3 lit. e DORA (uneingeschränkte Zugangs-, Inspektions- und Auditrechte — nur für kritische/wichtige Funktionen). Art. 30 Abs. 3 lit. d DORA (Beteiligung an TLPT[32] — nur für kritische/wichtige Funktionen). Lücke: Für nicht-kritische Funktionen kein expliziter DORA-Anknüpfungspunkt; Frequenz und Umfang nicht konkretisiert. NIS-2-RL macht gar keine diesbezüglichen Vorgaben.
SBOM-Pflicht	Software Bill of Materials (SBOM)[33] für alle im Auftrag betriebenen oder gelieferten Softwarekomponenten. Aktualisierung bei jeder wesentlichen Änderung.	Art. 13 Abs 4 iVm Anhang I CRA[34] (insb. Teil II des Anhangs I); Bestimmungen gültig ab 11. Dezember 2027. Lücke: Derzeit noch nicht aus DORA/NIS-2-RL direkt ableitbar, aber vertraglich vereinbar.

Die Gegenüberstellung zeigt ein konsistentes Muster: DORA benennt die relevanten Regelungsbereiche — Verfügbarkeit, Integrität, Authentizität, Vertraulichkeit, Dienstleistungsgüte, Unterstützung bei Vorfällen, Audit-Rechte — ohne sie zu operationalisieren. Konkrete Fristen, Schwellenwerte und Prüffrequenzen bleiben der vertraglichen Vereinbarung überlassen. Für nicht-kritische bzw. nicht-wichtige Funktionen fehlen selbst die strukturellen Anknüpfungspunkte teilweise. Die NIS-2-RL bleibt noch weiter zurück. Und dort, wo ein Standard wie der CRA künftig Abhilfe schaffen könnte — etwa bei der SBOM-Pflicht — liegt der Geltungsbeginn noch in der Zukunft. Die Lücke zwischen regulatorischer Anforderung und operativer Wirksamkeit ist damit auch auf Vertragsebene keine Ausnahme, sondern das Grundmuster.

5.2 Assume Breach als Vertragsanforderung

Die nachfolgend dargestellten Anforderungen gehen über das hinaus, was DORA und NIS-2-RL aktuell verlangen. Sie sind jedoch nicht beliebig: Sie folgen unmittelbar aus der in Kapitel 1.3 beschriebenen Beweislastumkehr. Wer davon ausgeht, dass ein System bis zum Beweis des Gegenteils als kompromittiert gilt, kann sich mit einer vertraglichen Pflicht zu „Assume-Breach-Architektur" als allgemeiner Formel nicht begnügen — diese Prämisse muss in überprüfbare Einzelanforderungen übersetzt werden, die sich gegenseitig bedingen.

Die Reihenfolge der nachfolgenden Anforderungen ist daher keine Auflistung, sondern eine Architektur: Netzwerksegmentierung begrenzt den Schaden, falls die Kompromittierungsannahme zutrifft. Identitäts- und Zugriffskontrolle verhindert, dass aus einem kompromittierten Punkt ein vollständiger Zugriff auf weitere Systeme wird. Lateral-Movement-Detection prüft aktiv, ob die Kompromittierungsannahme zutrifft — und ist damit die operative Umsetzung der Beweislastumkehr selbst. Forensik-fähige Protokollierung macht diese Prüfung erst möglich. Recovery unter

[32] Threat-Led Penetration Testing (TLPT) — ein bedrohungsorientierter Penetrationstest, der auf Basis realer, aktueller Bedrohungsszenarien konzipiert wird. Anders als klassische Penetrationstests, die bekannte Schwachstellen gegen bekannte Systeme testen, simuliert TLPT einen zielgerichteten Angriff durch ein professionelles Red Team auf Basis von Threat Intelligence, die spezifisch für die getestete Organisation aufbereitet wird. Im Finanzbereich ist TLPT durch TIBER-EU und dessen nationale Ausprägungen wie TIBER-AT operationalisiert.

[33] Eine Software Bill of Materials (SBOM) ist ein maschinenlesbares Verzeichnis aller Komponenten, Bibliotheken und Abhängigkeiten, aus denen eine Softwarelösung aufgebaut ist — das digitale Äquivalent einer Zutatenliste. Sie ermöglicht es, bei Bekanntwerden einer Schwachstelle in einer bestimmten Komponente unmittelbar festzustellen, welche Systeme betroffen sind, ohne den gesamten Software-Stack manuell durchsuchen zu müssen. Im Kontext des Lieferkettenrisikomanagements ist die SBOM damit eine Grundvoraussetzung für reaktionsfähiges Schwachstellenmanagement — wer nicht weiß, welche Komponenten in einem für ihn betriebenen System verbaut sind, kann auf eine CVE-Veröffentlichung strukturell nicht rechtzeitig reagieren.

[34] Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnungen (EU) Nr. 168/2013 und (EU) 2019/1020 und der Richtlinie (EU) 2020/1828 (Cyberresilienz-Verordnung, „CRA", „Cyber Resilience Act").

Kompromittierungsannahme stellt sicher, dass selbst der letzte Rettungsanker nicht Teil des Problems ist.

Bei der Protokollierung zeigt sich die regulatorische Lücke besonders deutlich: Art. 17 Abs. 3 lit b DORA und Art. 12 Abs. 1 KI-VO - letzterer beschränkt auf Hochrisiko-KI-Systeme im Sinne von Art. 6 KI-VO - verlangen dem Grunde nach, dass protokolliert wird — keiner der beiden Rahmen definiert, wie lange. Die einzige datenschutzrechtliche Grenze nach oben setzt der Grundsatz der Speicherbegrenzung nach Art. 5 Abs. 1 lit. e DSGVO, der jedoch keine feste Frist vorgibt, sondern eine Abwägung im Einzelfall verlangt. Die eigentliche forensisch relevante Frage — wie lange ist sinnvoll — müssen Organisationen selbst beantworten.

Orientierung bietet der gemeinsame Leitfaden „Best Practices for Event Logging and Threat Detection" von ASD's ACSC, CISA, FBI, NSA und internationalen Partnerbehörden (August 2024) [35]: Der Leitfaden hält fest, dass es in manchen Fällen bis zu 18 Monate dauern kann, einen Sicherheitsvorfall zu entdecken, und Malware zwischen 70 und 200 Tage unentdeckt im Netzwerk verweilen kann, bevor sie aktiv Schaden anrichtet — und dass die Aufbewahrungsdauer von Protokolldaten dieser Realität Rechnung tragen muss.

Die forensische Praxis illustriert das konkret: Beim **SolarWinds-Angriff** operierten die Angreifer nach Deployment der kompromittierten Updates im März 2020 neun Monate unentdeckt, bevor der Angriff im Dezember 2020 entdeckt wurde[36]. Eine Aufbewahrungsdauer von weniger als zwölf Monaten hätte bedeutet, dass wesentliche Teile des Angriffsverlaufs zum Zeitpunkt der Entdeckung bereits unwiederbringlich verloren gewesen wären.

Nach Einschätzung der Autorin sind zwölf Monate damit nicht das Optimum, sondern das vertretbare Minimum — bei erhöhtem Risikoprofil ist möglicherweise auch eine längere Aufbewahrung begründbar.

Anforderung	Inhalt	Rechtsanknüpfung / Lücke
Netzwerksegmentierung	Nachweisbare Trennung kritischer Systeme von der übrigen Infrastruktur, sodass eine Kompromittierung eines Segments nicht automatisch auf andere übergreift. Dokumentation der Segmentierungslogik, nicht nur ihrer Existenz.	Art. 9 Abs. 3 lit. c DORA verpflichtet Finanzunternehmen, dem Mangel an Verfügbarkeit, der Beeinträchtigung der Authentizität und Integrität, den Verletzungen der Vertraulichkeit und dem Verlust von Daten vorzubeugen — eine Anforderung, aus der sich Netzwerksegmentierung als technische Schutzmaßnahme ableiten lässt, ohne dass sie explizit vorgeschrieben wird. Lücke: Weder DORA noch die NIS-2-RL konkretisieren, welcher Segmentierungsgrad ausreicht. Ansatz ergänzend in den CERT.at-Empfehlungen, auf die die FMA-Stellungnahme verweist.
Identity- und Zugriffskontrolle	Multi-Faktor-Authentifizierung als Mindeststandard für alle administrativen und extern erreichbaren Zugänge. Privileged Access Management mit Just-in-Time-Vergabe statt dauerhaft bestehender erhöhter Rechte.	Art. 9 Abs. 4 lit. c DORA (Beschränkung des Zugangs auf das für rechtmäßige Tätigkeiten erforderliche Mindestmaß) iVm. Art. 20 und 21 Delegierte Verordnung (EU) 2024/1774. Art. 9 Abs. 4 lit. d DORA (Richtlinien und Protokolle für starke Authentifizierungsmechanismen). Art. 21 Abs. 2 lit. i NIS-2-RL.

[35] Australian Signals Directorate's Australian Cyber Security Centre, Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation, National Security Agency et al., Best Practices for Event Logging and Threat Detection, August 2024, https://www.cyber.gov.au/sites/default/files/2024-08/best-practices-for-event-logging-and-threat-detection.pdf.

[36] National Public Radio, „A 'Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack", 16. April 2021, https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack.

Anforderung	Inhalt	Rechtsanknüpfung / Lücke
		Lücke: Keine explizite Pflicht zu Privileged Access Management oder Just-in-Time-Vergabe in DORA oder NIS-2-RL.
Lateral-Movement-Detection	Vertragliche Pflicht zur Erkennung verdächtiger Bewegungen innerhalb des Netzwerks, nicht nur am Perimeter. Nachweis durch dokumentierte Detection-Use-Cases, nicht nur durch Tool-Vorhandensein.	Art. 10 DORA iVm. Art. 23 Delegierte Verordnung (EU) 2024/1774 (Erkennungsmechanismen für anomale Aktivitäten). Lücke: Lateral-Movement-Detection als eigene Anforderungskategorie ist weder in DORA noch in der NIS-2-RL vorgesehen. Die Anforderung ist direkt aus der in Kapitel 1.3 beschriebenen Beweislastumkehr ableitbar.
Forensik-fähige Protokollierung	Speicherung von Protokolldaten auf einem vom überwachten System getrennten System oder in einer separaten Umgebung, samt eigener Backups dieser Protokolldaten, um Manipulation oder Verlust im Kompromittierungsfall zu erschweren. Aufbewahrungsdauer orientiert sich an der tatsächlichen Erkennungsrealität — mindestens zwölf Monate.	Art. 17 Abs. 3 DORA iVm. Art. 12 Delegierte Verordnung (EU) 2024/1774 (Protokollierungspflicht dem Grunde nach). Art. 12 Abs. 1 KI-VO für Hochrisiko-KI-Systeme im Sinne von Art. 6 KI-VO. Art. 21 Abs. 2 lit. b NIS-2-RL (Bewältigung von Sicherheitsvorfällen) lässt Protokollierung als implizite Voraussetzung erkennen, ohne sie explizit zu verlangen. Lücke: Konkrete Aufbewahrungsfristen sind in keinem dieser Rahmen vorgegeben. Eine Obergrenze ergibt sich aus Art. 5 Abs. 1 lit. e DSGVO (Speicherbegrenzung), soweit die Protokolldaten Personenbezug aufweisen — dieser Grundsatz definiert jedoch keine konkrete Frist, sondern verlangt eine Abwägung im Einzelfall.
Recovery unter Kompromittierungs-annahme	Wiederherstellungsprozesse, die davon ausgehen, dass auch Backups zum Zeitpunkt eines Vorfalls bereits kompromittiert sein könnten. Getrennte, isolierte Backup-Infrastruktur als Nachweispflicht.	Art. 12 DORA (Datensicherungs-Policy). Ansatz in CERT.at-Empfehlungen (funktionierende Recovery-Prozesse, zitiert in FMA-Stellungnahme). Lücke: Weder DORA noch NIS-2-RL verlangen eine Backup-Architektur, die explizit Kompromittierungsresistenz nachweist.
MTTD/MTTC als KPIs	Mean Time to Detect und Mean Time to Contain als vertraglich definierte, messbare KPIs mit quartalsweiser Berichtspflicht. Schwellenwerte: MTTD ≤ 2 Stunden, MTTC ≤ 4 Stunden für bekannte Angriffsmuster.[37]	Lücke: Kein Rechtsrahmen stellt auf Detection- oder Containment-Geschwindigkeit ab. Aus der Sorgfaltspflicht nach Art. 28 Abs. 4 DORA begründbar; für NIS-2-pflichtige Unternehmen fehlt selbst dieser Anknüpfungspunkt. Zur Herleitung der Schwellenwerte siehe Kapitel 2.

[37] Verbindliche regulatorische Schwellenwerte für Time-to-Detect oder Time-to-Contain existieren nach derzeitigem Stand nicht. Weder die NIS-2-Richtlinie noch DORA geben eine Frist vor, innerhalb derer ein Vorfall erkannt werden muss.
Auch die ENISA Technical Implementation Guidance, die als detaillierteste verfügbare Konkretisierung der NIS-2-RL-Anforderungen gilt, bleibt an dieser Stelle abstrakt: Sie verlangt in Abschnitt 7 eine Policy zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen mit regelmäßigen Reviews (mindestens alle zwei Jahre), ohne konkrete Kennzahlen wie Mean Time to Detect oder Mean Time to Contain zu benennen oder Schwellenwerte vorzugeben. Selbst die detaillierteste verfügbare Konkretisierung schweigt also genau an der Stelle, die im ersten Kapitel als entscheidend identifiziert wurde.
Die in diesem Whitepaper vorgeschlagenen Zielwerte (MTTD ≤ 2 Stunden, MTTC ≤ 4 Stunden) sind daher keine zitierte Branchenkennzahl, sondern eine eigene Ableitung aus der in Kapitel 1 dargestellten Sophos-Zahl: Wenn ein Angreifer im Schnitt bereits 3,4 Stunden nach dem ersten Zugriff vollen Zugriff auf das Active Directory erlangt, muss die Erkennung deutlich darunter liegen, um vor diesem Punkt überhaupt eine realistische Chance auf wirksame Eindämmung zu haben. Ein MTTD-Zielwert von 2 Stunden lässt rechnerisch noch ein Zeitfenster von rund 1,4 Stunden für Eindämmungsmaßnahmen, bevor der mediane Zeitpunkt der vollständigen Kompromittierung erreicht ist – mit entsprechend geringem Sicherheitspuffer. Dieser Wert ist als ambitionierte, aus der Bedrohungslage abgeleitete Zielmarke zu verstehen, nicht als etablierter Industriestandard.

Anforderung	Inhalt	Rechtsanknüpfung / Lücke
Exploit Response SLA	Separate SLA-Kategorie für Schwachstellen, für die aktive Ausnutzung bekannt ist (CISA Known Exploited Vulnerabilities Catalog[38] oder äquivalent). Unabhängig vom regulären Patch-Zyklus: Reaktionszeit ≤ 24 Stunden.	Lücke: Weder DORA noch NIS-2-RL kennen den Status aktiver Ausnutzung als eigenständige SLA-Kategorie. Eine eigene vertragliche Regelung ist daher erforderlich.
Transparenz über KI-Werkzeuge	Vertragliche Pflicht zur Offenlegung aller KI-Werkzeuge in Entwicklung und Betrieb, die auf Daten des Auftraggebers zugreifen oder für dessen Systeme eingesetzt werden. Meldepflicht bei wesentlichen Änderungen.	Art. 28 DSGVO (Pflicht des Auftragsverarbeiters, weitere Auftragsverarbeiter nur mit Genehmigung des Verantwortlichen hinzuzuziehen), soweit KI-Werkzeuge personenbezogene Daten des Auftraggebers verarbeiten. Lücke: Außerhalb des Anwendungsbereichs von Art. 28 DSGVO — also bei KI-Werkzeugen ohne Personenbezug — besteht keine explizite Transparenzpflicht gegenüber dem Auftraggeber. Die Anforderung ist insoweit ausschließlich vertraglich zu verankern.
Operational getesteter Exit-Plan	Nachweis eines operational getesteten Exit-Plans — nicht nur eines dokumentierten. Jährliche Bestätigung der operativen Machbarkeit durch den Dienstleister.	Art. 28 Abs. 8 DORA iVm. Art. 28 Abs. 7 DORA: Ausstiegsstrategien müssen den Risiken Rechnung tragen, die auf der Ebene des IKT-Drittdienstleisters entstehen können — einschließlich wesentlicher Änderungen, die sich auf die Vereinbarung oder die Verhältnisse des Dienstleisters auswirken, sowie jedem erheblichen Risiko im Zusammenhang mit der angemessenen und kontinuierlichen Bereitstellung der IKT-Dienstleistungen. Art. 21 Abs. 2 lit. d NIS-2-RL (Sicherheit der Lieferkette). Lücke: Die Pflicht zur Ausstiegsstrategie trifft das Finanzunternehmen — nicht den Dienstleister. Der Nachweis, dass der Dienstleister seinerseits in der Lage ist, die Übertragung der IKT-Dienstleistungen auf einen anderen Anbieter operativ zu ermöglichen, ist weder in DORA noch in der NIS-2-RL explizit verlangt.

Die vorstehenden Anforderungen sind nicht als Wunschliste zu verstehen, sondern als operative Übersetzung einer einzigen Prämisse: Wer davon ausgeht, dass eine Kompromittierung bereits stattgefunden hat oder jederzeit stattfinden kann, muss seine Vertragsbeziehungen mit IKT-Drittdienstleistern an dieser Annahme ausrichten. Die Hoffnung, dass der Perimeter hält, ist keine Strategie.

Der Rechtsrahmen schafft dafür eine Grundlage, aber keine ausreichende Operationalisierung. Was DORA und NIS-2-RL verlangen, sind Prozesse — was sie nicht verlangen, ist Geschwindigkeit, Wirksamkeit und Nachweisbarkeit unter realen Bedingungen. **Genau diese Lücke schließen die hier beschriebenen Anforderungen:** Sie übersetzen regulatorische Prozessexistenz in operative Prozesseffektivität — und machen diese vertraglich messbar. Ob ein Dienstleister die vereinbarten Anforderungen tatsächlich erfüllt, zeigt sich nicht im Vertragstext, sondern im Ernstfall. Sicherheit lässt

[38] CISA Cybersecurity and Infrastructure Security Agency, Known Exploited Vulnerabilities Catalog, https://www.cisa.gov/known-exploited-vulnerabilities-catalog.

sich vertraglich nicht herstellen. Was der Vertrag liefert, ist Nachweisbarkeit, Steuerungsmöglichkeit und im Ernstfall die Grundlage für Konsequenzen.

5.3 Kontrollen: Operative Wirksamkeit statt Dokumentenprüfung

Kontrollen, die ausschließlich auf Dokumentation und Zertifizierung abstellen, messen Prozessexistenz — nicht Prozesseffektivität. Kapitel 4.1 hat gezeigt, warum das unter KI-beschleunigter Bedrohungslage nicht ausreicht. Die folgenden Kontrollen sind entsprechend ausgestaltet: Sie messen, ob die vereinbarten Anforderungen unter realen Bedingungen funktionieren — nicht ob sie dokumentiert sind.

Anforderung	Inhalt	Rechtsanknüpfung / Lücke
Jährlich	Aktueller Pentest-Bericht (externer Dienstleister). SBOM-Review für alle im Auftrag betriebenen Komponenten. Nachweis Red Team Exercise.	Art. 30 Abs. 3 lit. d DORA (Beteiligung an TLPT) und Art. 30 Abs. 3 lit. e DORA (Zugangs-, Inspektions- und Auditrechte) — jeweils nur für IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen. Art. 21 Abs. 2 lit. b und lit. d NIS-2-RL (Behandlung von Sicherheitsvorfällen; Sicherheit der Lieferkette). Lücke: Weder DORA noch NIS-2-RL sehen eine explizite Pflicht zu Penetrationstests oder Red Team Exercises gegenüber Dienstleistern vor; für nicht-kritische Funktionen fehlt in DORA ein Anknüpfungspunkt. Frequenz und Umfang sind in keinem der beiden Rahmen konkretisiert.
Quartalsweise	Bericht MTTD/MTTC gegen definierte KPIs. Patch-Compliance-Rate je CVSS-Kategorie. Liste offener CVEs ≥ 7,0 in betriebenen Systemen.	Art. 30 Abs. 2 lit. e DORA (Beschreibung der Dienstleistungsgüte mit messbaren Leistungszielen). Art. 21 Abs. 2 lit. d NIS-2-RL (Sicherheit der Lieferkette) als mittelbarer Anknüpfungspunkt. Lücke: Kein Rechtsrahmen verlangt KPI-Reporting in dieser Granularität gegenüber Dienstleistern.
	EASM-Report: aktuelles Inventar extern erreichbarer Assets, Abgleich mit internem Asset-Register, Identifikation unbekannter/vergessener Systeme	Art. 9 Abs. 3 lit. c DORA (Verpflichtung, dem Mangel an Verfügbarkeit und Verlust von Daten vorzubeugen). Art. 21 Abs. 2 lit. a NIS-2-RL (Konzepte für Risikoanalyse und Sicherheit von Informationssystemen). Lücke: Kein Rechtsrahmen verlangt EASM explizit; das BSI empfiehlt EASM im BITS-B 2026-262788-1032 ausdrücklich als Maßnahme zur Erkennung der eigenen Angriffsfläche.
Anlassbezogen	Technisches Interview mit Security-Team nach Incident oder bei BSI/ENISA-Advisory zu genutzter Software. Forensisches Audit-Recht bei festgestellter Vertragsverletzung.	Art. 30 Abs. 3 lit. e DORA (Zugangs-, Inspektions- und Auditrechte für kritische/wichtige Funktionen). Art. 21 Abs. 2 lit. b NIS-2-RL (Behandlung von Sicherheitsvorfällen). Lücke: Trigger für anlassbezogene Prüfungen sind in keinem der beiden Rahmen definiert; für nicht-kritische Funktionen fehlt in DORA ein expliziter Anknüpfungspunkt.

Kontrollen sind kein Selbstzweck. Sie sind die einzige Möglichkeit, zwischen einem Dienstleister, der seine vertraglichen Zusagen einhält, und einem, der sie dokumentiert, zu unterscheiden. Der Rechtsrahmen schreibt Kontrollen vor — er schreibt nicht vor, dass sie etwas messen müssen, das für die tatsächliche Bedrohungslage relevant ist. Diese Lücke ist keine Nachlässigkeit des Gesetzgebers, sondern die strukturelle Grenze regulatorischer Normierung: Was in sieben Tagen zwischen Bekanntwerden einer Schwachstelle und ihrer aktiven Ausnutzung passiert, lässt sich nicht in einer

Verordnung vorschreiben. Es lässt sich aber vertraglich vereinbaren, quartalsweise messen und anlassbezogen prüfen. Wer das nicht tut, hat die regulatorischen Anforderungen erfüllt — und die eigentliche Frage nie gestellt.

6. Fazit: Der Rechtsrahmen schafft Erwartung — die Lücke müssen Unternehmen selbst schließen

Der Rechtsrahmen schafft Erwartung ohne Maßstab. Die FMA-Stellungnahme hat das implizit bestätigt: Sie benennt das Problem, beschreibt die Bedrohungslage, referenziert CERT.at und CERT-EU — und endet mit der Aufforderung, Tabletop-Übungen abzuhalten. Eine Lösung ist das nicht – eher ein Eingeständnis, dass sie nicht von der Aufsicht kommen wird.

Die Lücke zwischen regulatorischer Erwartung und operativer Wirksamkeit müssen Unternehmen selbst schließen — mit den richtigen Fragen an Dienstleister, messbaren KPIs in Verträgen und einem Kontrollregime, das operative Wirksamkeit prüft statt Prozessexistenz zu dokumentieren.

Assume Breach zu akzeptieren bedeutet keine Kapitulation, sondern schlicht: Der Bedrohungslage Rechnung zu tragen, in der Schwachstellen im Median bereits ausgenutzt werden, bevor ein Patch verfügbar ist — und die Grundlage für eine Sicherheitsarchitektur, die tatsächlich schützt statt nur compliant ist.

7. Ausblick: Was sich verändern könnte

DORA sieht in Art. 58 Abs. 1 eine formale Evaluierung durch die Kommission bis Januar 2028 vor. Der Gegenstand dieser Evaluierung ist eng definiert: Er betrifft die Kriterien für die Benennung kritischer IKT-Drittdienstleister, Drittlandregelungen und die Funktionsweise des Überwachungsrahmens — nicht die in diesem Paper beschriebenen operativen Lücken. Die NIS-2-RL sieht in Art. 40 eine Überprüfung durch die Kommission bis Oktober 2027 vor; auch hier liegt der Fokus auf Anwendungsbereich und Wirksamkeit der Richtlinie insgesamt.

Am 20. Januar 2026 veröffentlichte die Kommission im Rahmen eines Cybersicherheitspakets zwei Vorschläge: Den Cybersecurity Act 2 (COM(2026) 11 final) sowie einen separaten Änderungsvorschlag zur NIS-2-RL (COM(2026) 13 final). [39] Die vorgeschlagenen NIS-2-Anpassungen betreffen Geltungsbereich und Schwellenwerte — nicht die strukturellen Lücken bei operativen Schutzanforderungen, die dieses Paper beschreibt.

Ob künftige Entwicklungen diese Lücken schließen werden, ist damit nicht zu erwarten. Die in diesem Paper beschriebenen Maßnahmen sind bereits heute mit der FMA-Stellungnahme als Anknüpfungspunkt begründbar und vertretbar. Wer auf regulatorische Konkretisierung wartet, wartet zu lang.

[39] Europäische Kommission, Vorschlag zur Änderung der Richtlinie (EU) 2022/2555 (NIS-2-RL), 20. Januar 2026, https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-eu-cybersecurity-act.