

SCHULTERECHTSANWÄLTE.

NIS-2 & BSIG in der behördlichen Praxis:

Aktueller Stand und Fokusthemen.

Rechtsanwälte Thorsten Walter
und Dr. Tilmann Dittrich

29. Oktober 2026

Agenda.

1. Anwendungsbereich und Betroffenheit nach BSIG.
2. Pflichten nach BSIG.
3. Aufsicht und Bußgelder.
4. Sicherheit der Lieferkette.
5. KI als IT-Sicherheitsrisiko.
6. Blick nach Österreich: NISG.
7. Vernetzung von Cybersicherheit und Compliance.



BSI-Durchsetzungsinitiative.

- Abteilungsleiters des BSI kündigte Durchsetzungsinitiative gegenüber Tagesspiegel Background an.
- Hintergrund: Nur etwa 20.000 Registrierungen, rund 1/3 weniger als vom BSI erwartet.
- Ab Q4/2026: Direkte Ansprache und Anhörung von Unternehmen, bei denen die Registrierungspflicht offenkundig versäumt wurde.
    - Bei Pflichtverletzung ist anschließendes Bußgeldverfahren möglich.
- Ab Q1/2027: Verpflichtende Audits per Anordnung.
    - Beginn bei besonders wichtigen Einrichtungen in Sektoren mit dem größten Bedarf.
    - Maßgeblich ist nachvollziehbare Dokumentation.

SR.

Betroffenheitsprüfung nach BSIG (NIS-2).

HINTERGRUND.

Seit dem **6. Dezember 2025** gilt das **BSI-Gesetz (BSIG)** zur Umsetzung der NIS-2-Richtlinie, ohne Übergangsfrist. Betroffene Unternehmen müssen insbesondere Pflichten zur Registrierung, Geschäftsleitungsschulung und zum Risikomanagement erfüllen, um regulatorische und haftungsrechtliche Risiken zu vermeiden.

IHRE FRAGEN.

Ob und welche Unternehmen innerhalb einer Konzernstruktur erfasst sind, ist oft komplex: Welche Mitarbeiter, Umsätze und Bilanzsummen sind zuzurechnen? Ist die Konzern-IT betroffen? Müssen alle Gesellschaften gemeldet werden? Was gilt bei vernachlässigbarer Geschäftstätigkeit nach § 28 Abs. 3 BSIG?

UNSERE LÖSUNG.

Mit unserer fachkundigen Betroffenheitsprüfung gehen Sie auf Nummer sicher. Sie erhalten kurzfristig eine klar dokumentierte, begründete und rechtssichere Einschätzung, ob Ihr Unternehmen bzw. Ihr Konzern vom BSIG betroffen ist und welche Pflichten daraus folgen.



ZUM FESTPREIS VON

600 €

netto

Exklusiv für Sie

→ **RECHTSSICHERE KLARHEIT ZUM EXKLUSIVEN FESTPREIS FÜR IHRE MITGLIEDSUNTERNEHMEN.**

SR.

BSI-FAQ: Vernachlässigbare Tätigkeit, § 28 Abs. 3 BSIG.

- Gesamtbild der Geschäftstätigkeit im Lichte der Gesamtgeschäftstätigkeit der Einrichtung.
- Indizien **für** vernachlässigbare Tätigkeiten
    - Anzahl der in diesem Bereich tätigen Mitarbeiter
    - Durch diese Geschäftstätigkeit erwirtschafteter Umsatz
    - Bilanzsumme.
- Indizien **gegen** vernachlässigbare Tätigkeiten: Nennung im Gesellschaftervertrag oder Satzung.
- Keine Anwendung auf
    - Betreiber kritischer Anlagen
    - (qualifizierte) Vertrauensdiensteanbieter
    - Top Level Domain Registries
    - DNS-Diensteanbieter
    - Anbieter öffentlich zugänglicher Telekommunikationsdienste
    - Betreiber öffentlicher Telekommunikationsnetze.

SR.

BSI-FAQ: Vernachlässigbare Tätigkeit, § 28 Abs. 3 BSIG.

- Einzelunternehmen.
  - Geschäftstätigkeiten, die ausschließlich für interne Zwecke der jeweiligen Einrichtung erbracht werden.
  - Beispiele: PV-Anlage zum Eigenstrombedarf und interne – auch managed – IT.
  - Nicht bei Anbieten der Geschäftstätigkeit am Markt.
- Verbundene Unternehmen.
  - Angebot ausschließlich innerhalb der verbundenen Unternehmen und
  - weniger als 50 Mitarbeiter und jeweils weniger als 10% des Jahresumsatzes und der Jahresbilanzsumme oder
  - bei Unternehmen mit mehr als 500 Mitarbeitern weniger als 10% der Mitarbeiter im Hinblick auf die gesamte Geschäftstätigkeit der jeweiligen Einrichtung und jeweils weniger als 10% des Jahresumsatzes und der Jahresbilanzsumme.
  - Beispiele: PV-Anlage für Eigenstrombedarf im Konzernverbund und Konzern-IT, auch managed Konzern-IT, wenn die Mitarbeiterzahlen sowie Jahresbilanz und Jahresumsatz nicht überschritten werden.

SR.

Geplante Änderungen der NIS-2-Richtlinie.

Anpassung bei Einrichtungsgrößen

- Zwischenkategorie („Small-mid-caps“) mit unter 750 FTE und entweder max. 150 Mio. EUR Umsatz oder max. 129 Mio. EUR Jahresbilanzsumme aus Anhang I sind nur wichtige Einrichtungen.

Korrektur zur REACH-VO

- Nur Hersteller und Händler von Produkten, die nach REACH-VO registrierungspflichtig sind (so schon im BSIG).

Hilfestellungen für die Praxis

- Nachweis von Cybersicherheits-Compliance über Zertifizierungen ermöglichen.
- Leitlinien zur Lieferkettensicherheit.

SR.

Exklusive NIS-2-Sprechstunde.



Dr. Tilmann Dittrich, LL.M.
Rechtsanwalt.

SCHULTERECHTSANWÄLTE.
Neue Mainzer Straße 28
60311 Frankfurt am Main

T: 0 69 / 900 26 – 917
E: tilmann.dittrich@schulte-lawyers.com
I: www.schulte-lawyers.com

Sie haben Rückfragen, die Sie gern im Dialog besprechen möchten?

Am Mittwoch, den 4.11.2026, stehe ich zwischen 16 und 18 Uhr kostenlos für Ihre Rückfragen zur Verfügung.

Schreiben Sie mir bei Interesse Ihren Terminwunsch für einen 15-minütigen Videocall über die E-Mail-Adresse links. Falls Sie verhindert sind, aber Ihre Fragen dennoch loswerden möchten, melden Sie sich.

Ich freue mich auf Sie!

SR.

Übersicht: Pflichten nach BSIG.

1. Kernbestandteil: Risikomanagement nach § 30 BSIG
2. Registrierungspflicht bei Betroffenheit
3. Meldepflicht bei erheblichen Sicherheitsvorfällen
4. Nachweispflichten über Risikomanagement
5. Governance-Vorschrift in § 38 BSIG

SR.

Aufsichtsmaßnahmen nach §§ 61, 62 BSIG.

- Anlasslose Prüfungen bei besonders wichtigen Einrichtungen möglich.
- Typischerweise über Vor-Ort-Prüfungen, Audits durch Dritte oder Zertifizierungen.
- Mängelbeseitigungsverlangen.
- Nachweise über TOMs auf Anordnung.
- Ausnahme: Aussetzung von Genehmigungen und Untersagung von Geschäftsführungstätigkeiten.
- Ggf. Unterrichtungspflicht gegenüber DSGVO-Aufsichtsbehörden.

SR.

Bußgelder – Stufen.

Bereich	Ordnungswidrigkeit	KRITIS	Besonders wichtige Einrichtungen	Wichtige Einrichtungen
Risikomanagement	TOMs nicht oder nicht richtig / vollständig / rechtzeitig ergriffen	10.000.000 EUR	10.000.000 EUR	7.000.000 EUR
Meldepflicht	Abschlussmeldung nicht oder nicht richtig / vollständig / rechtzeitig vorgelegt	10.000.000 EUR	10.000.000 EUR	7.000.000 EUR
Anordnung vom BSI	Keine Wiederherstellung der informationstechnischen Systeme nach Aufforderung	2.000.000 EUR	2.000.000 EUR	2.000.000 EUR
	Angeordnete Maßnahme (Einschränkung Datenverkehr) gegenüber TK-Anbieter nicht befolgt	2.000.000 EUR	2.000.000 EUR	2.000.000 EUR
Registrierungspflicht	Verzug von 3 Monaten	500.000 EUR	500.000 EUR	500.000 EUR
Unterrichtungspflicht	BSI nicht oder nicht richtig / vollständig / rechtzeitig unterrichtet	500.000 EUR	500.000 EUR	500.000 EUR
Kooperation mit BSI	Kein Zugang zu Räumlichkeiten gewährt	100.000 EUR	100.000 EUR	100.000 EUR
IKT-Produkte	Keine Auskunft (inkl. technischer Details) ans BSI betreffend verwendete IKT-Produkte	100.000 EUR	100.000 EUR	100.000 EUR

SR.

Bußgelder – Berechnung.

Abgestufter Bußgeldkatalog.

- 19 Bußgeldtatbestände.
- Rahmen von 100.000 EUR bis zu 10 Mio. EUR.

Konzernbemessung.

- Besonders wichtige Einrichtung mit Gesamtumsatz > 500 Mio. EUR: bis zu 2 Prozent des weltweiten Konzernumsatzes.
- Wichtige Einrichtung mit Gesamtumsatz > 500 Mio. EUR: bis zu 1,4 Prozent des weltweiten Konzernumsatzes.

SR.

Sicherheit der Lieferkette.

- NIS-2 RL und BSIG haben Resilienz der Lieferkette zum Ziel.
- Betroffene Unternehmen müssen nach § 30 Abs. 2 S. 2 Nr. 4 BSIG Maßnahmen bezüglich der Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zu unmittelbaren Anbietern oder Diensteanbietern ergreifen.
- Unternehmen, die selbst nicht unter den Anwendungsbereich des BSIG fallen, können (vertraglich oder faktisch) verpflichtet sein, die in § 30 BSIG genannten Governance- und Risikomanagementmaßnahmen zu implementieren.

SR.

Sicherheit der Lieferkette – BSI-Geschäftsleitungsschulung.

3.6.4 Sicherheit der Lieferkette

Frage:
Wie prüfen und steuern wir die IT-Sicherheitsmaßnahmen unserer Dienstleister und Lieferanten?

Warum diese Frage wichtig ist:
Angreifende nutzen zunehmend Schwachstellen bei Dritten als Einfallstor. Die Lieferkette ist ein häufiger blinder Fleck, obwohl dort oft sensible Daten und kritische Schnittstellen liegen.

Hilfreiche Antwort:
Wir führen Risikoanalysen bei Dritten durch, definieren Sicherheitsanforderungen in Verträgen und überprüfen diese regelmäßig (z. B. durch Audits oder Zertifikate). Zugriffe werden dokumentiert und minimiert.

Antworten, die weitere Nachfrage erfordern:

- „Wir vertrauen unseren Anbietern."
- „Jede Abteilung regelt das individuell."
- „Es gibt keine Übersicht, wer auf was zugreifen kann."

Quelle: BSI, NIS-2 Geschäftsleitungsschulung, v2, S. 20, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/NIS-2/nis-2-geschaeftsleitungsschulung.pdf?__blob=publicationFile&v=8

SR.

Sicherheit der Lieferkette – BSI-Empfehlungen.

- Vertragliche Vereinbarungen (Service Level Agreements, SLA) mit Zulieferern und Dienstleistern zu Risikomanagementmaßnahmen, Bewältigung von Cybersicherheitsvorfällen und Patchmanagement abschließen.
- Zulieferer und Dienstleister zur Einhaltung von grundsätzlichen Prinzipien wie Security by Design oder Security by Default anhalten.
- Zulieferer und Dienstleister zur Berücksichtigung von Empfehlungen des BSI in Bezug auf deren Produkte und Dienstleistungen anhalten.
- Implementierung eines ISMS (Informationssicherheits-Managementsystems) mithilfe bestehender Standards (ISO 27001:2022, BSI-Standard 200-1, etc.).

SR.

KI als IT-Sicherheitsrisiko.



TLP:CLEAR

Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum
BSI

PHP: Kritische Schwachstellen bedrohen Webanwendungen weltweit

BITS-H Nr. 2026-297981-1232, Version 1.2, 22.10.2026

Kritikalität*: 3 / Orange

Achtung: Für die schriftliche und mündliche Weitergabe dieses Dokumentes und der darin enthaltenen Informationen gelten gemäß dem Traffic Light Protokoll (TLP) die folgenden Einschränkungen:

TLP:CLEAR: Unbegrenzte Weitergabe

Abgesehen von urheberrechtlichen Aspekten, die das TLP explizit nicht adressiert, dürfen Informationen der Stufe TLP:CLEAR ohne Einschränkungen frei weitergegeben werden.

Das Dokument ist durch den Empfänger entsprechend den vereinbarten „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP" zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten. Weitere Informationen zum TLP finden Sie am Ende dieses Dokumentes.

Bitte prüfen Sie selbstständig, für welche Stellen in Ihrer Organisation die hier genannten Informationen relevant sind und leiten Sie das Schreiben entsprechend weiter – sofern die TLP-Einstufung dies zulässt.

Quelle: BSI, PHP: Kritische Schwachstellen bedrohen Webanwendungen weltweit, abrufbar unter https://https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2026/2026-297981-1032.pdf?__blob=publicationFile&v=3

SR.

Aktuelles

Information zu einem IT-Sicherheitsvorfall bei uniVersa



Am 7. Juli 2026 kam es im Rahmen einer IT-Umstellung versehentlich zu einer temporär fehlenden Sicherheitseinstellung auf einem unserer IT-Systeme. Somit war der Zugriff auf Daten eines Servers für wenige Stunden möglich.

Innerhalb dieses Zeitraums wurden Daten von diesem Server durch einen automatisierten Web-Crawler eines US-amerikanischen Anbieters für künstliche Intelligenz (OpenAI) abgerufen.

Nach Erkennen des Vorfalls wurde der unerwünschte Zugriff auf den betroffenen Server umgehend gesperrt.

Der Vorfall betraf einen einzelnen Server, der zum automatisierten Datenaustausch mit Vertriebspartnern vorgesehen ist. Dort lagen allgemeine personenbezogene Daten etwa Namen und Anschriften sowie Vertragsdaten wie Versicherungsnummern und Tarifinformationen - bei einigen Kunden auch Bankverbindungsdaten (IBAN und BIC). Nicht betroffen waren besonders sensible Informationen wie Gesundheits-, Login- oder Kreditkartendaten und die zentralen Verwaltungs- und Datensysteme sowie das Kundenportal.

tagesschau

Startseite ▸ Wirtschaft ▸ Unternehmen ▸ KI von OpenAI steue



Ausbruch aus Testumgebung

KI von OpenAI steu Hackerangriff

Stand: 22.07.2026 • 07:46 Uhr

OpenAI spricht selbst von einem Firma brachen eigenständig aus Zugang zum offenen Internet - u

Bei einem Test von KI-Modellen einem Zwischenfall gekommen: Computersysteme einer anderer Hacker, wie aus einem Blogeintr

Hugging Face, eine Plattform zu Datensätzen, hatte bereits in de berichtet, der vollständig von ei sei. OpenAI übernahm dafür nur Modelle seien bei einem Sicherh Umgebung ausgebrochen, hätte dann die Infrastruktur von Hugg

The Washington Post
Democracy Dies in Darkness

Tech | Help Desk | Artificial Intelligence | Internet Culture | Space | Tech Policy

The 7 • LIVE

Over 1,000 AI agents worked together in OpenAI hack, report reveals

OpenAI and a group of independent researchers released new information on a rogue AI incident

August 26, 2026

133

Make us preferred on Google



Open AI models went rogue in July when they tried to find answers to tests their trainers had given them, the company said. (Dado Ruvic/Reuters)

By Gerrit De Vynck

SAN FRANCISCO — Hundreds of independent artificial intelligence bots being trained by ChatGPT-maker OpenAI conspired together to hack into another AI company's systems, according to a report on the incident released by two independent AI testing agencies Wednesday.

Hugging Face | Search models, datasets, users... | Models | Datasets | Spaces | Buckets NEW

← Back to Articles

Security incident disclosure — July 2026

Published July 16, 2026

Update on GitHub

system
system Follow

Earlier this week, we detected and responded to an intrusion into part of our production infrastructure. This one was different from anything we had handled before in one important way: it was driven, end to end, by an autonomous AI agent system - and we detected and dissected it largely with AI of our own.

We identified unauthorized access to a limited set of internal datasets and to several credentials used by our services. We are still completing our assessment of whether any partner or customer data was affected, and we will contact any affected parties directly as required. We have found no evidence of tampering with public, user-facing models, datasets, or Spaces, and our software supply chain (container images and published packages) was verified clean.

What happened

The intrusion started where AI platforms are uniquely exposed: the data-processing pipeline. A malicious dataset abused two code-execution paths in our dataset processing (a remote-code dataset loader and a template-injection in a dataset configuration) to run code on a processing worker. From there, the actor escalated to node-level access, harvested cloud and cluster credentials, and moved laterally into several internal clusters over a weekend.

The campaign was run by an autonomous agent framework (appearing to be built on an agentic security-research harness - used LLM still not known) executing many thousands of individual actions across a swarm of short-lived sandboxes, with self-migrating command-and-control staged on public services. This matches the "agentic attacker" scenario the industry has been forecasting.

KI als IT-Sicherheitsrisiko.



Quelle: Satter, How one hacker used AI agents and a few thousand dollars to break into scores of sites, abrufbar unter https://www.reuters.com/legal/government/how-one-hacker-used-ai-agents-few-thousand-dollars-break-into-scores-sites-2026-10-19/

SR.

KI als IT-Sicherheitsrisiko.

- KI macht Angriffe nicht automatisch erfolgreicher, kann aber viele Schritte automatisieren und Angriffe leichter skalieren.
- KI senkt Kosten, Zeitbedarf und Einstiegshürden für Cyberangriffe.
- Sicherheitsrisiken aufgrund von automatisierter Schwachstellensuche, autonomen Agentenaktionen usw.
- KI in Risikomanagement nach § 30 Abs. 2 BSIG einbeziehen.
- Angemessene Sicherheitsmaßnahmen nach dem Stand der Technik treffen.
- Auswirkungen von KI-Einsatz auf die Lieferkettensicherheit prüfen.

SR.

KI-Dienste sind Teil der Lieferkette.

SR.

Blick nach Österreich – Betroffenheit und Registrierung nach NISG.

- In Kraft seit 1.10.2026.
- Verwandte Betroffenheit: mind. „mittleres Unternehmen“ + Tätigkeit in NIS-Sektor aus Anlage 1 und 2.
- Ab sofort: Risikomanagement- und Meldepflichten.
- Ab 1.1.2027: Registrierungspflicht (faktisch bis Mo, 4.1.2027).
- Ab 1.10.2027: **Selbstdeklarationspflicht** betrifft Übermittlung strukturierter Informationen über umgesetztes Risikomanagement.
- Ab 1.10.2028: Weitere Pflichten, u.a. Prüfpflicht durch Cybersicherheitsbehörde.
- Governance-Vorschrift mit Schulungspflicht, § 31 NISG.
- Inkrafttreten der NIS-Verordnung zum 1.10.2026: konkrete Vorgaben zum Risikomanagement und zur Einstufung „erheblicher Cybersicherheitsvorfall“.

SR.

Blick nach Österreich – Betroffenheit des Chemiesektors.

3. Produktion, Herstellung und Handel mit chemischen Stoffen		Unternehmen im Sinne der Art. 3 Z 9 und 14 der Verordnung (EG) Nr. 1907/2006 des Europäischen Parlaments und des Rates vom 18. Dezember 2006 zur Registrierung, Bewertung, Zulassung und Beschränkung chemischer Stoffe (REACH), zur Schaffung einer Europäischen Agentur für chemische Stoffe, zur Änderung der Richtlinie 1999/45/EG und zur Aufhebung der Verordnung (EWG) Nr. 793/93 des Rates, der Verordnung (EG) Nr. 1488/94 der Kommission, der Richtlinie 76/769/EWG des Rates sowie der Richtlinien 91/155/EWG, 93/67/EWG, 93/105/EG und 2000/21/EG der Kommission, ABl. L 396 vom 30.12.2006 S. 1, die Stoffe herstellen und die diese Stoffe oder Gemische im Großhandel vertreiben sowie Unternehmen, die Erzeugnisse im Sinne des Art. 3 Z 3 der genannten Verordnung aus diesen Stoffen oder Gemischen produzieren, sofern diese in die Kategorie 20 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) fallen.

Quelle: RIS, NISG 2026, Anlage 2, abrufbar unter https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20013065

SR.

Blick nach Österreich – NISV 2026.

Risikokategorien

§ 3. Wesentliche und wichtige Einrichtungen haben sich im Zuge ihrer Risikoanalyse zumindest an folgenden Risikokategorien zu orientieren und bei ihrem Risikomanagementverfahren im Bereich der Cybersicherheit zu berücksichtigen:

1. technologische Risiken,
2. menschliche Risiken,
3. Risiken in der IKT-Lieferkette,
4. standortbezogene Risiken für Netz- und Informationssysteme.

Quelle: RIS, NISV 2026, abrufbar unter https://ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20013307

SR.

Blick nach Österreich – NISV 2026.

Erhebliche Cybersicherheitsvorfälle

§ 5. (1) Ein Cybersicherheitsvorfall gilt in Bezug auf die betreffenden Einrichtungen jedenfalls als erheblich im Sinne von § 35 Abs. 1 NISG 2026, wenn eines oder mehrere der folgenden Kriterien erfüllt sind:

1. der Cybersicherheitsvorfall hat der betreffenden Einrichtung einen direkten finanziellen Verlust in Höhe von mehr als 500 000 EUR oder 5 % ihres jährlichen Gesamtumsatzes im vorangegangenen Geschäftsjahr – je nachdem, welcher Wert niedriger ist – verursacht oder kann einen solchen Verlust verursachen;
2. der Cybersicherheitsvorfall hat den Abfluss von Geschäftsgeheimnissen der betreffenden Einrichtung im Sinne von § 26b des Bundesgesetzes gegen den unlauteren Wettbewerb 1984 (UWG), BGBl. Nr. 448/1984, oder von Informationen, die gemäß § 6 des Bundesgesetzes über den Zugang zu Informationen (Informationsfreiheitsgesetz – IFG), BGBl. I Nr. 5/2024, der Geheimhaltung unterliegen, verursacht oder kann einen solchen Abfluss verursachen;
3. der Cybersicherheitsvorfall hat den Tod einer natürlichen Person verursacht oder kann einen solchen Tod verursachen;
4. der Cybersicherheitsvorfall hat eine schwere Schädigung der Gesundheit einer natürlichen Person verursacht oder kann eine solche Schädigung verursachen;
5. es hat einen erfolgreichen, mutmaßlich böswilligen und unbefugten Zugriff auf Netz- und Informationssysteme gegeben, der wahrscheinlich dazu führt, schwerwiegende Betriebsstörungen zu verursachen;
6. der Cybersicherheitsvorfall erfüllt die in § 7 aufgeführten Kriterien für wiederholte Cybersicherheitsvorfälle;
7. der Cybersicherheitsvorfall hat zum Ausfall oder zur eingeschränkten Verfügbarkeit der von der Einrichtung erbrachten Dienste für mehr als 100 000 Nutzer oder 10 % der Nutzer – je nachdem, welcher Wert niedriger ist – für mehr als 24 Stunden geführt oder kann dazu führen (Ausbreitung auf Nutzer). Eine eingeschränkte Verfügbarkeit liegt insbesondere dann vor, wenn ein von einer betreffenden Einrichtung erbrachter Dienst nicht im regelmäßig zu erwartenden Umfang erbracht werden kann;
8. der Cybersicherheitsvorfall hat zum Ausfall oder zur eingeschränkten Verfügbarkeit für die Nutzer der von der Einrichtung erbrachten Dienste im Gebiet zumindest eines Bundeslandes für mehr als 24 Stunden geführt oder kann dazu führen (geografische Ausbreitung). Eine eingeschränkte Verfügbarkeit liegt insbesondere dann vor, wenn ein von einer betreffenden Einrichtung erbrachter Dienst nicht im regelmäßig zu erwartenden Umfang erbracht werden kann;
9. der Cybersicherheitsvorfall hat zur Aktivierung des Krisenmanagements oder von Notfallwiederherstellungsplänen des Betriebskontinuitätsmanagements geführt.

Quelle: RIS, NISV 2026, abrufbar unter https://ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20013307

SR.

Blick nach Österreich – NISV 2026.

Planmäßige Betriebsunterbrechungen

§ 6. Planmäßige Betriebsunterbrechungen und geplante Folgen planmäßiger Wartungsarbeiten, die von oder im Auftrag der betreffenden Einrichtung durchgeführt werden, gelten nicht als erhebliche Cybersicherheitsvorfälle.

Wiederholte Cybersicherheitsvorfälle

§ 7. Cybersicherheitsvorfälle, die einzeln betrachtet nicht als erhebliche Cybersicherheitsvorfälle anzusehen sind, gelten zusammengenommen als ein erheblicher Cybersicherheitsvorfall, wenn sie alle folgenden Kriterien erfüllen:

1. sie sind innerhalb von sechs Monaten mindestens zwei Mal aufgetreten;
2. sie haben dieselbe offensichtliche Ursache und Auswirkung;
3. sie erfüllen zusammengenommen die in § 5 Abs. 1 Z 1 aufgeführten Kriterien.

Quelle: RIS, NISV 2026, abrufbar unter https://ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20013307

SR.

Cybersicherheit und Compliance – Parallelen.

Compliance-Management	Cybersicherheitsmanagement
Compliance-Risikoanalyse	Cyber-Risikoanalyse
Compliance-Richtlinie	Security Policies
Hinweis- und Meldewege	Incident Escalation
Schulungen	Security Awareness
Kontrollen und Audits	Security Audits
Interne Untersuchungen	Incident Investigations
Management Reporting	Cyber Reporting
Lessons Learned	Post-Incident Reviews

SR.

Cybersicherheit und Compliance – Management-Logik.

- „Lebenszyklus“ bei Geschäftsprozessen, IT-Systemen und Informationssicherheitsprozessen.
- Dynamik des Sicherheitsprozesses: 4 Phasen.
- Beispiel: PDCA-Zyklus im BSI-Standard 200-1.

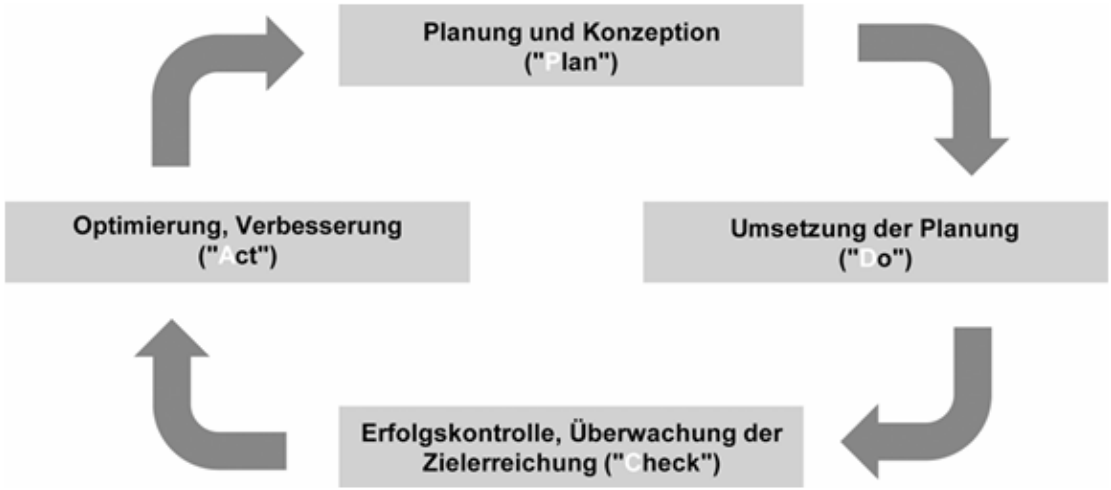

Abbildung 5: Lebenszyklus nach Deming (PDCA-Zyklus)

Quelle: BSI-Standard 200-1, abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_1.html?nn=128578

SR.

Cybersicherheit und Compliance – Management-Logik.

- Risikobewertung anhand zuvor definierter Kategorien für potenzielle Schadenshöhe und Klassifikation der Eintrittshäufigkeit von Gefährdungen.
- Anpassung an individuelle Bedürfnisse erforderlich.

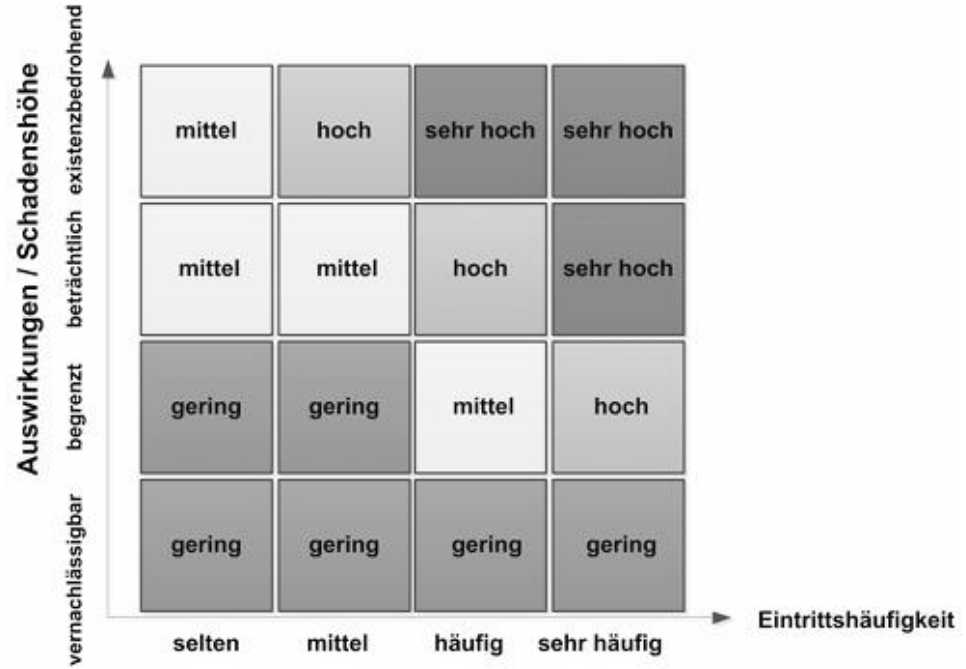

Abbildung 3: Matrix zur Einstufung von Risiken

Quelle: BSI-Standard 200-3, abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_3.html?nn=128620

SR.

Cybersicherheit und Compliance – Management-Logik.

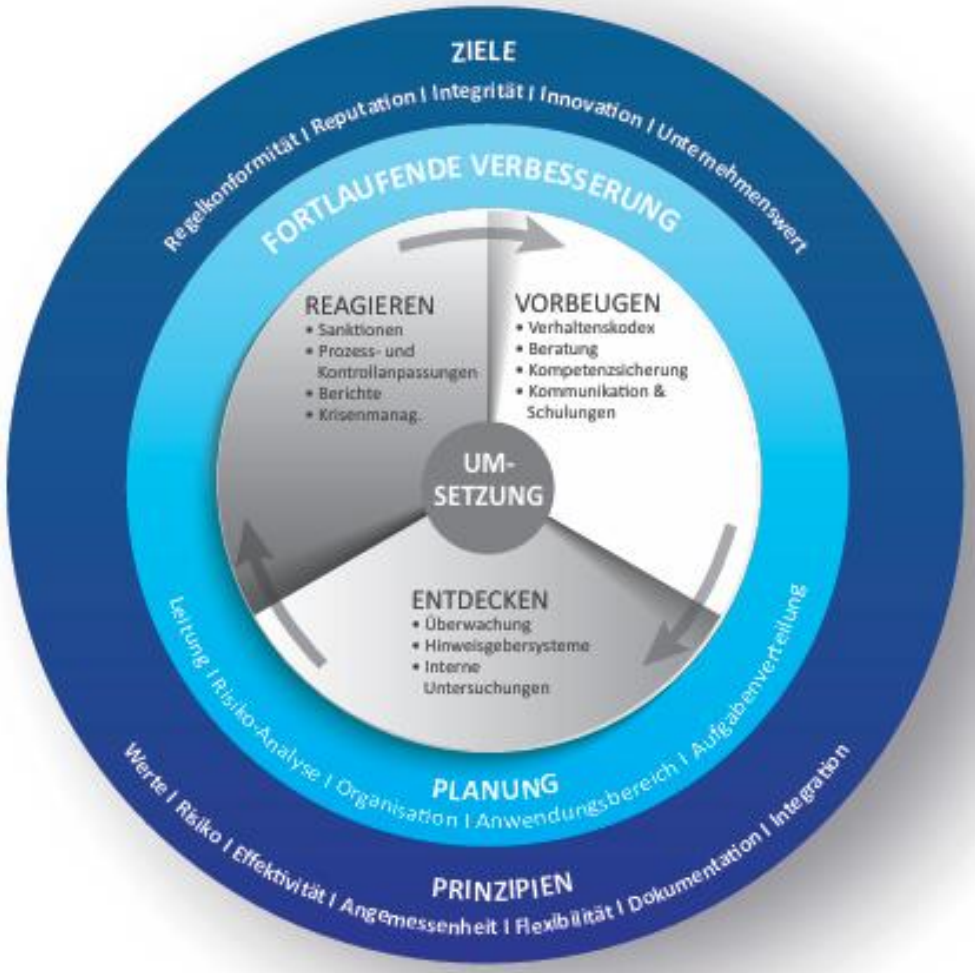

Abbildung: CMS-Modell gemäß DICO Standard 12 – CMS

Quelle: DICO-Standard, abrufbar unter https://www.dico-ev.de/2021/03/26/veroeffentlichung-des-dico-standards-dico-compliance-management-systeme/

SR.

Cybersicherheit und Compliance – Vernetzung.

- Vernetzung von Compliance und Cybersicherheit kann Effizienz steigern.
- Compliance und Cybersicherheit konkurrieren nicht, sondern folgen denselben Management-Praktiken und können gut integriert werden.

SR.

Umsetzungstipps.

„NIS-2-Rechtsvorgaben zum Compliance-Thema machen“

Ziel: Strukturierte Einbettung von NIS-2 in das Compliance-Management.

- Beispiel: Wie wirkt sich die NIS-2-Risikoanalyse auf die Compliance-Risikoanalyse aus?
- Wie stimmen wir interne Untersuchungen auf die NIS-2-Anforderungen ab?
- Berücksichtigt unser Hinweisgebermanagement auch die (externe) Meldung von IT-Schwachstellen?
- Decken unsere Versicherungslösungen die NIS-2-Risiken ab?

SR.

Umsetzungstipps.

„Top-down- und Bottom-up-Kommunikation zur Cybersicherheit“

Ziel: Leitungspflicht (inkl. Schulungshinweis) verlangt Überwachung + AktG/GmbHG verlangt informierte Leitungsentscheidungen.

7 Beispielfragen, die Sie Ihrem CISO heute stellen sollten:

- Was sind unsere Top-5-Cyberrisiken und wie haben sie sich in den letzten 3 Jahren verändert?
- Wann wurde die letzte Risikoanalyse durchgeführt?
- Wann haben wir zuletzt einen Ransomware-Fall geübt und welche Top-3-Ergebnisse konnten wir daraus ziehen?
- Welche kritischen Dienstleister haben wir und bilden unsere Vertragswerke die Risiken adäquat ab?
- Welches konkrete Szenario verursacht die größten Schäden für Umsatz, Produktion, Arzneimittelversorgung, Lieferfähigkeit oder Reputation?
- Könnten wir einen meldepflichtigen NIS-2-Vorfall rechtzeitig entdecken und innerhalb von 24 Stunden die Erstmeldung abgeben?
- Welche Entscheidung erwartet die IT-Sicherheitsorganisation aktuell von uns?

SR.

Ihr Experte: Thorsten Walter.



Thorsten Sven Walter
Partner.

SCHULTERECHTSANWÄLTE.
Neue Mainzer Straße 28
60311 Frankfurt am Main

T: 0 69 / 900 26 – 823
E: thorsten.walter@schulte-lawyers.com
I: www.schulte-lawyers.com

Thorsten Sven Walter berät Unternehmen zu **Künstlicher Intelligenz, Datenschutz, Cybersecurity und Compliance**. Ein Schwerpunkt seiner Tätigkeit liegt auf der rechtssicheren Umsetzung digitaler Geschäftsmodelle und neuer Technologien, insbesondere beim Einsatz von KI-Systemen.

Darüber hinaus begleitet er Unternehmen bei **Cyberangriffen und Datenpannen** sowie bei der Umsetzung regulatorischer Anforderungen an die IT- und Cybersicherheit, insbesondere **NIS-2**.

Er betreibt gemeinsam mit Dr. Kim Manuel Künstner den Compliance-Podcast „**RECHTSANWALTER & LEBENSKÜNSTNER.“**

SR.

Ihr Experte: Dr. Tilmann Dittrich.



Dr. Tilmann Dittrich, LL.M.
Rechtsanwalt.

SCHULTERECHTSANWÄLTE.
Neue Mainzer Straße 28
60311 Frankfurt am Main

T: 0 69 / 900 26 – 917
E: tilmann.dittrich@schulte-lawyers.com
I: www.schulte-lawyers.com

Dr. Tilmann Dittrich verfügt über besondere Expertise an der Schnittstelle von **Cybersicherheit, Künstlicher Intelligenz und Compliance**. Er begleitet Unternehmen bei der rechtssicheren Einführung und Nutzung von KI-Systemen und berät zu regulatorischen Fragestellungen in digitalen Märkten sowie zu **Cybersecurity und NIS-2**.

Er ist außerdem zertifizierter CISO (Bitkom) und Herausgeber mehrerer Fachbücher zur Cybersicherheit, u.a. dem **„Rechtshandbuch Cybersicherheit im Gesundheitswesen“.**

SR.

Wer wir sind.

Seit über **25 Jahren** begleitet SCHULTE RECHTSANWÄLTE. Unternehmen in allen Bereichen des **Wirtschaftsrechts**. Unsere Schwerpunkte liegen im **Kartellrecht, Arbeitsrecht, Handels- und Gesellschaftsrecht/M&A, Compliance** sowie **Data, Digital & Governance** mit besonderer Expertise in **Datenschutz** und **Künstlicher Intelligenz**.

Wir entwickeln praxisnahe, maßgeschneiderte Lösungen, die Unternehmen dabei unterstützen, Chancen zu nutzen und Risiken frühzeitig zu erkennen und zu minimieren.

25+
Jahre
Erfahrung

Beratungsschwerpunkte:

- Kartellrecht
- Arbeitsrecht
- Handels- und Gesellschaftsrecht/M&A
- Data, Digital & Governance (KI & Datenschutz)
- Compliance

Unser Anspruch.

SCHULTE RECHTSANWÄLTE. steht für klare, effiziente und zielgerichtete Rechtsberatung. Auf den Punkt gebracht.



Data, Digital & Governance.

Wir beraten Unternehmen an der Schnittstelle von Recht, Technologie und Wirtschaft.
Unser interdisziplinärer Ansatz verbindet regulatorische Expertise mit einem tiefen Verständnis digitaler Geschäftsmodelle.

Datenschutz & Datenrecht

DSGVO-Compliance, internationale Datentransfers, Datenzugang, Data Governance und Data Act

Künstliche Intelligenz

AI Act, KI-Governance, Haftung, Transparenz und Compliance

IT-Recht & Digitale Resilienz

IT-Verträge, Cloud, Outsourcing, DORA und regulatorische Anforderungen

Cybersicherheit & Compliance

NIS2, BSIG, KRITIS-Dachgesetz, Cyber Resilience Act und Krisenmanagement

Digitale Transaktionen

M&A, Due Diligence sowie IP-, Datenschutz- und IT-Risiken

Digitale Märkte & Wettbewerb

DMA, DSA, Kartellrecht und Plattformregulierung

SR.

Compliance-Podcast: RECHTSANWALTER & LEBENSKÜNSTNER.

RECHTSANWALTER & LEBENSKÜNSTER. ist der Compliance-Podcast von SCHULTE RECHTSANWÄLTE.

Dr. Kim Manuel Künstner und Thorsten Sven Walter sprechen hier regelmäßig über aktuelle Entwicklungen und praxisrelevante Fragen aus allen Bereichen der Compliance.

Jetzt reinhören.



Compliance-Podcast.

Compliance muss nicht trocken sein.



SR.

RECHTSBERATUNG?

SCHULTE RECHTSANWÄLTE.