Aulinger

84. Kontiki-Konferenz · 26.06.2026

Bedeutung von IT-Sicherheit und IT-Sicherheitsstandards für kritische Infrastruktur

Dr. Ralf Heine M.M.

Rechtsanwalt · Fachanwalt für Arbeits- und IT-Recht

Nichts ging mehr um Mitternacht

So ächzte Deutschland unter dem Bahn-Total-Stillstand

bild.de, abgerufen am 24.06.2026

Kritische Infrastruktur im digitalen Zeitalter

Warum IT-Sicherheit kritischer Infrastrukturen keine Spezialfrage mehr ist






Kernbotschaft:

- (kritische) Infrastruktur = Grundlage des Alltags
- IT-Sicherheit = Voraussetzung für Versorgungssicherheit und wirtschaftliche Stabilität

Kritische Infrastruktur im digitalen Zeitalter

Warum IT-Sicherheit kritischer Infrastrukturen keine Spezialfrage mehr ist

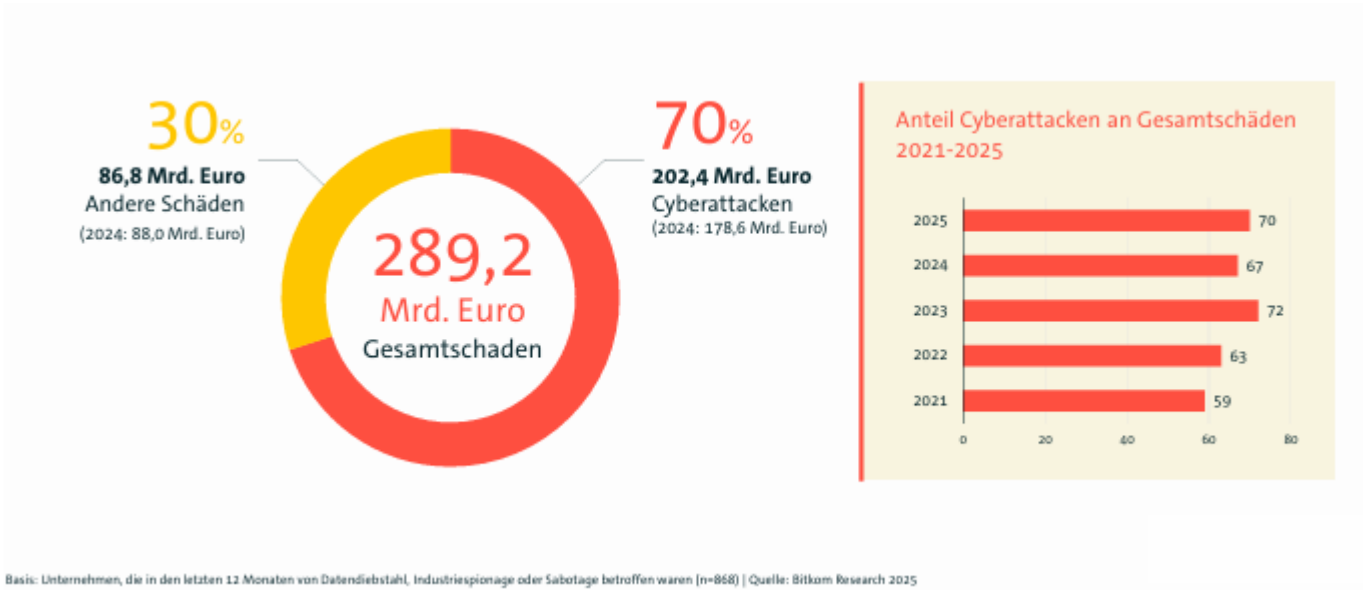


Abbildung 10: Prozentualer Anteil des entstandenen Gesamtschadens, der auf Cyberattacken zurückgeführt werden kann

entnommen aus: Bitkom, Wirtschaftsschutz 2025 – Lagebild der deutschen Wirtschaft

Bedrohungslage:
Cyberangriffe als Betriebs-, Compliance- und Gemeinwohlrisiko

Betriebsunterbrechung | **Daten- & Vertrauensverlust** | **Versorgungs- & Kaskadeneffekt**

Drei Entwicklungen:

1. Professionalisierung der Angreifer (Ransomware-as-a-Service, arbeitsteilig, international)
2. Ausweitung der Angriffsfläche (Cloud, Fernwartung, industrielle Steuerungssysteme)
3. besondere Attraktivität von kritischer Infrasturktur (Erpressbarkeit durch Versorgungsdruck)

Beispiele:

- Ransomware auf kommunale Dienste
- Lieferkettenangriffe
- Schwachstellen in VPN/Remote-Access
- Angriffe auf Gesundheitseinrichtungen

Kaskadeneffekte

Der Rechtsrahmen:
vom IT-Sicherheitsrecht zur Resilienzregulierung

zwei Regelungsstränge

Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen (BSI-Gesetz - BSIG)

Umsetzung der NIS-2-Richtlinie → IT-Sicherheit besonders wichtiger / wichtiger Einrichtungen

Rolle des BSI → Aufsicht, Meldestelle, Wissens-, Koordinations- und Standardisierungsakteur (§ 3 BSIG)

Dachgesetz zur Stärkung der physischen Resilienz kritischer Anlagen (KRITIS-Dachgesetz - KRITISDachG)

Umsetzung der CER-Richtlinie → physische Resilienz kritischer Anlagen

Rolle des BBK → zentrale Anlaufstelle

Der Rechtsrahmen:
vom IT-Sicherheitsrecht zur Resilienzregulierung

§ 28 BSIG

Besonders wichtige Einrichtungen

- Betreiber kritischer Anlagen
- qualifizierte Vertrauensdiensteanbieter
- TLD-Registries, DNS-Diensteanbieter
- TK-Anbieter (> 50 MA oder > 10 Mio. EUR)
- Einrichtungen Anlage 1 (ab 250 MA / 50 Mio.)
- Bundesverwaltung (§ 29)

Wichtige Einrichtungen

- Einrichtungen Anlage 1 (ab 50 MA / 10 Mio.)
- Einrichtungen Anlage 2 (ab 50 MA / 10 Mio.)
- Vertrauensdiensteanbieter (nicht qualifiziert)

Der Rechtsrahmen:
vom IT-Sicherheitsrecht zur Resilienzregulierung

§ 30 BSIG – Risikomanagementmaßnahmen

geeignete, verhältnismäßige, wirksame technische und organisatorische Maßnahmen gefahrübergreifender Ansatz, Stand der Technik

- Risikoanalyse
- Sicherheit der IT
- Bewältigung von Sicherheitsvorfällen
- Betriebsaufrechterhaltung, Backup, Wiederherstellung
- Krisenmanagement
- Lieferkettensicherheit
- Schwachstellenmanagement
- Wirksamkeitsbewertung

§ 31 BSIG – Verschärfte Anforderungen

Betreiber kritischer Anlagen:
Systeme zur Angriffserkennung (SZA) verpflichtend

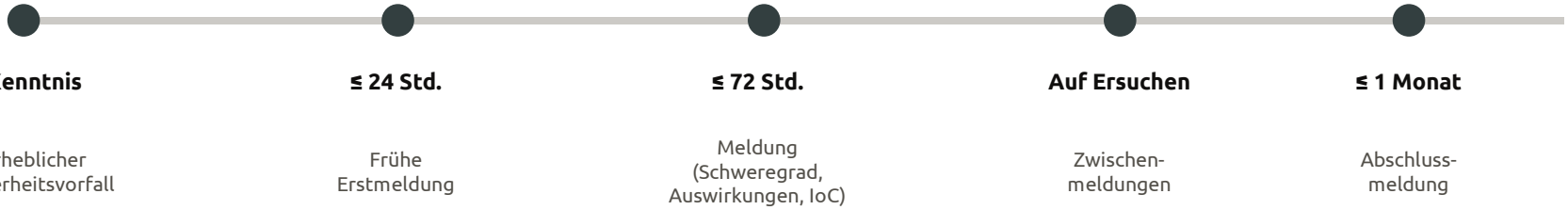
§ 13 KRITIS-Dachgesetz

Resilienzmaßnahmen, Resilienzpläne

Risikomanagement in der Praxis:
was „geeignet, verhältnismäßig und wirksam“ bedeutet

Geeignet	**Verhältnismäßig**	**Wirksam**
Maßnahme zahlt auf reales Risiko ein • MFA • Netzwerksegmentierung • Offline-Backups • Notfallhandbuch	Aufwand/Nutzen-Verhältnis Bei kritischen Anlagen: verschobene Abwägung (§ 31 BSIG)	Maßnahme existiert UND funktioniert • Getestete Backups • Geübte IR-Pläne • Bewertete Dienstleister • Priorisierte Schwachstellen

Meldepflichten und Rolle des BSI:
vom Vorfall zur Lageinformation



Praxis-Hinweise:

- Gemeinsame Meldestelle BSI / BBK
- Betreiber krit. Anlagen: zusätzliche Angaben (Art der Anlage, krit. Dienstleistung, Auswirkungen)
- Meldeprozesse vorab definieren, üben
- Verzahnung mit DSGVO (Art. 33): parallele, koordinierte Bewertung

IT-Sicherheitsstandards

Standard	Zweck / Vorteil	Grenze / Einsatz
BSI IT-Grundschutz	Praxisnah, detailliert, systematisch, Bausteinmodell	National, umfangreich in der Umsetzung
ISO/IEC 27001	International, Zertifizierung schafft Vertrauen	Ersetzt nicht BSIG-spezifische Anforderungen
B3S	Branchengerecht, BSI-Eignungsfeststellung möglich	Nur für jeweilige Branche
KRITIS-Dachgesetz	Branchenspezifische Resilienzstandards ergänzend	Neu, Konkretisierung ausstehend

Standards = Werkzeugkasten, kein Selbstzweck
Ziel: integriertes Sicherheitsmanagement

Governance, Geschäftsleitung und Haftung:
IT-Sicherheit als Leitungsaufgabe

§ 38 BSIG: Geschäftsleitungspflichten

- Risikomanagementmaßnahmen umsetzen und überwachen
- Regelmäßige Schulung
- Cybersecurity ≠ Delegation nach unten
- GL muss Organisation schaffen, Ressourcen bereitstellen, Risiken verstehen

Haftung & Bußgeldrisiken

- Überschneidung: IT-Sicherheitsrecht, Gesellschaftsrecht, Datenschutz, Organisationsverschulden
- § 65 BSIG: bis 10 Mio. € (bes. wichtige Einrichtungen)
- bis 7 Mio. € (wichtige Einrichtungen)
- ggf. umsatzbezogen

Gute Governance

- regelmäßiges Risikoreporting
- klare Verantwortlichkeiten
- dokumentierte Entscheidungen
- realistischer Maßnahmenplan
- regelmäßige Tests, Eskalationskultur

Praktische Umsetzung:
Zehn Punkte für ein belastbares KRITIS-Sicherheitsprogramm

1. Anwendungsbereich klären
2. Kritische Dienstleistung definieren
3. ISMS etablieren (IT-Grundschutz, ISO 27001)
4. Verfügbarkeit & Wiederherstellung priorisieren
5. Detektion & Reaktion stärken (SOC, IR, § 31)
6. Lieferkette einbeziehen (§ 30, Verträge, Exit)
7. Melde- & Kommunikationsprozesse vorab regeln
8. Schulungen für Mitarbeitende & Führungskräfte
9. Wirksamkeit testen (Tabletop, Pentests, Audits)
10. Nachvollziehbar dokumentieren (Nachweise, Haftung)

Fazit und Ausblick:
Resilienz als Leitprinzip

Recht verlangt Risikomanagement
BSIG: erweitertes, verschärftes Pflichtensystem (Risikomanagement, Meldepflichten, GL-Verantwortung, Sanktionen)

Standards schaffen Orientierung
BSI, ISO 27001, B3S = Orientierung, kein Ersatz für Risikoverständnis

Resilienz entscheidet im Ernstfall
Compliance ist notwendig, aber nicht ausreichend → Resilienz als Leitprinzip

Beginnen Sie nicht mit der Frage nach dem Dokument für die nächste Prüfung.

Beginnen Sie mit der Frage, welche kritische Dienstleistung Ihrer Organisation im Ernstfall unbedingt aufrechterhalten werden muss.

Vielen Dank.

Aulinger

Dr. Ralf Heine M.M.

Rechtsanwalt
Partner
Fachanwalt für Arbeits- und IT-Recht

+49 234 68779-341
ralf.heine@aulinger.eu

Qualifikation

- mehr als 15 Jahre Berufserfahrung im Bereich Arbeitsrecht, IT- und Datenschutzrecht
- Fachanwalt für Arbeits- sowie Informationstechnologierecht
- zert. Datenschutzauditor- und beauftragter
- gelistet als einer der „**Best Lawyers Germany**“ seit 2024

Tätigkeitsschwerpunkte

- laufende Beratung im Arbeits-, Vertrags-, IT- und Datenschutzrecht
- Strukturierung Datenschutzmanagement und Datenschutz-Compliance
- Legal Due Diligence (Kauf- und Verkaufsseite)
- IT- und Datenschutzrecht und Vertragsrecht
- Litigation (Arbeitsrecht / IT- und Datenschutz)

Aulinger

Ihr Ansprechpartner

Dr. Ralf Heine M.M.
Rechtsanwalt
Fachanwalt für Arbeits- und IT-Recht

+49 234 68779341
ralf.heine@aulinger.eu

Aulinger Bochum
Josef-Neuberger-Straße 4
44787 Bochum

Aulinger Essen
Frankenstraße 348
45133 Essen