

Cybersicherheit und NIS-2-Richtlinie

Resiliente Kliniken: Sicherheit als Führungsaufgabe

Vorstellung

Cybersicherheit und NIS2 – Konsequenzen für die Klinikleitung

Ein Praxisvortrag – kein juristischer Fachvortrag.

*Aus der Praxis.
Für die Praxis.*



Über 30 Jahre
IT-Leiter in einem Krankenhaus
der Maximalversorgung



Seit über 4 Jahren
Informationssicherheitsbeauftragter (ISB)
im selben Unternehmen



Vor dem 4. BSI-Audit
in 2027



Mein Ziel:
Praxisnahe Impulse für Ihre Führung.
Umsetzbar. Wirksam. Resilient.

*Nicht Paragraphen im Fokus –
sondern Lösungen, die im Krankenhaus funktionieren.*



Patientensicherheit



Informationssicherheit



Führungsverantwortung



Resiliente Klinik



Einführung

AKTUELLES BEISPIEL

Cybervorfall Berlin 2026

Datenabfluss in großem Umfang

EIN STARKER
STAAT BRAUCHT
STARKE RESILIENZ



ZENTRALE FAKTEN



Nicht die Frage, ob – sondern wann.

Cybersicherheit ist eine gemeinsame Verantwortung.



Jedes **5.** Krankenhaus war in den letzten 3 Jahren bereits von Cyberkriminalität betroffen.



der Krankenhäuser schätzen die Bedrohungslage durch Cyberkriminalität für ihre Einrichtung als hoch oder sehr hoch ein und erwarten eine Zunahme in den nächsten 2 Jahren.

Jeder **2.** Krankenhaus war bereits von Cyberangriffen auf Zulieferer oder Dienstleister betroffen.



Einführung

Nicht jeder Sicherheitsvorfall ist ein Cyberangriff.

Informationssicherheitsvorfälle können viele Ursachen haben.



Dem Patienten ist egal, warum das KIS nicht funktioniert.

Quelle: Deutsche Krankenhausgesellschaft (DKG), Informationssicherheit in Krankenhäusern (§ 391 SGB V), Umsetzungshinweise / Starter-Paket Informationssicherheit.

Was ist Cybersicherheit?

Cyber-Bedrohungen



Cyber-Risiken



VERTRAULICHKEIT
Schutz vor Zugriff
Nur Berechtigte haben
Zugang zu Informationen.



INTEGRITÄT
Schutz vor Manipulation
Daten und Systeme bleiben
korrekt, vollständig und
unverändert.



VERFÜGBARKEIT
Schutz vor Ausfall
Systeme und Daten sind
bei Bedarf verfügbar
und erreichbar.

NIS2 und BSIG – Der Zusammenhang

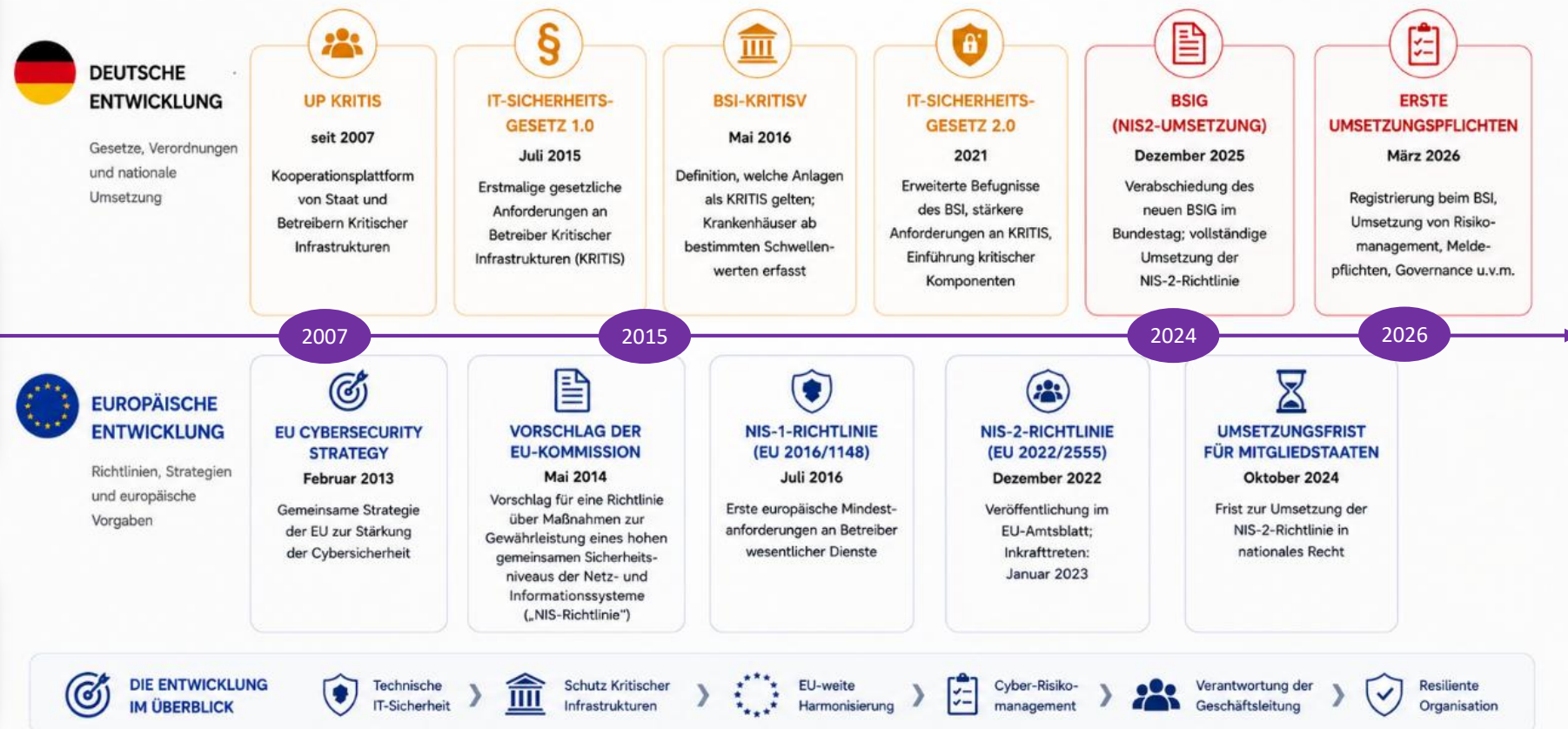
NIS2 =
„Network and Information
System Directive 2“

Richtlinie über Maßnahmen für
ein hohes gemeinsames
Cybersicherheitsniveau in der
Union
(kurz: NIS-2-Richtlinie)

Deutschland setzt die NIS-2-
Richtlinie durch Änderung des BSIG-
Gesetzes
am 6. 12.2025 um.

Entwicklung der Cybersicherheitsgesetzgebung

Vom Schutz kritischer Infrastrukturen zur Verantwortung der Geschäftsleitung



Roadmap durch das BSIG

Die wichtigsten Paragraphen.





§28 - Einrichtungsarten

§28 BSIG – Einordnung von Einrichtungen

Einführung der Begriffe „besonders wichtige Einrichtung“ und „wichtige Einrichtung“ im Sektor Gesundheit

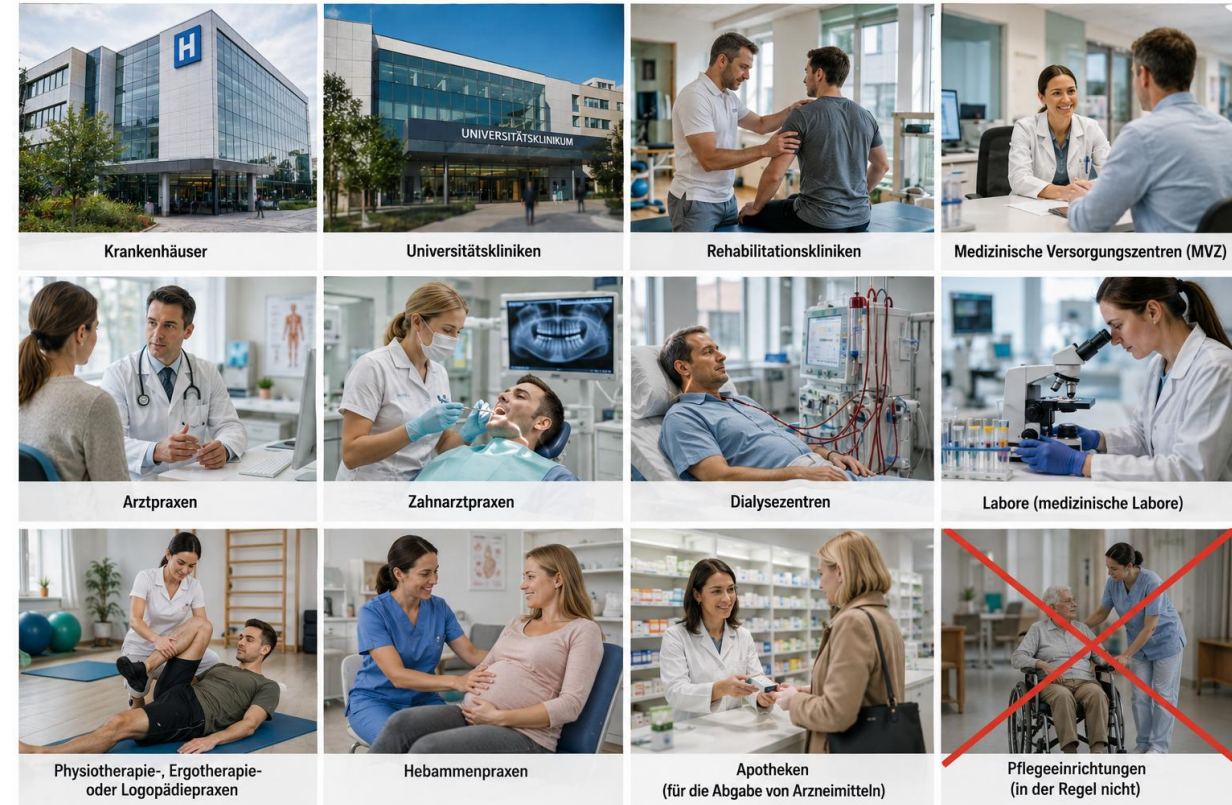
BESONDERS WICHTIGE EINRICHTUNG

- 1** Juristische oder natürliche Person
Bereitstellung von Waren und Dienstleistungen nach Anlage 1, BSIG
- 2** Mind. 250 Beschäftigte oder
Jahresumsatz > 50 Mio. €
und Jahresbilanz > 43 Mio. €
- 3** Betreiber einer kritischen Anlage gemäß BSI-KritisV
(KHs mit > 30.000 vollstationären Patienten / Jahr)

WICHTIGE EINRICHTUNG

- 1** Juristische oder natürliche Person
Bereitstellung von Waren und Dienstleistungen nach Anlage 1 und Anlage 2, BSIG
- 2** Soweit keine besonders wichtige Einrichtung vorliegt
- 3** Mind. 50 Beschäftigte oder
Jahresumsatz > 10 Mio. €
und Jahresbilanz > 10 Mio. €

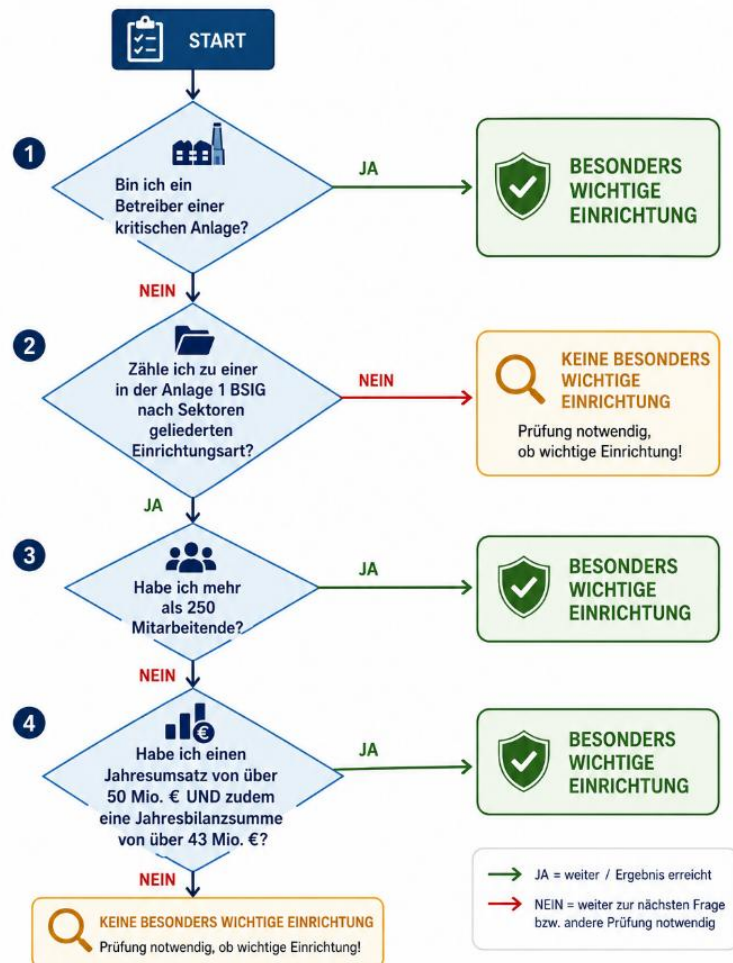
Quellen / Rechtsgrundlagen
BSIG §28 · Anlagen 1 & 2 · BSI-KritisV



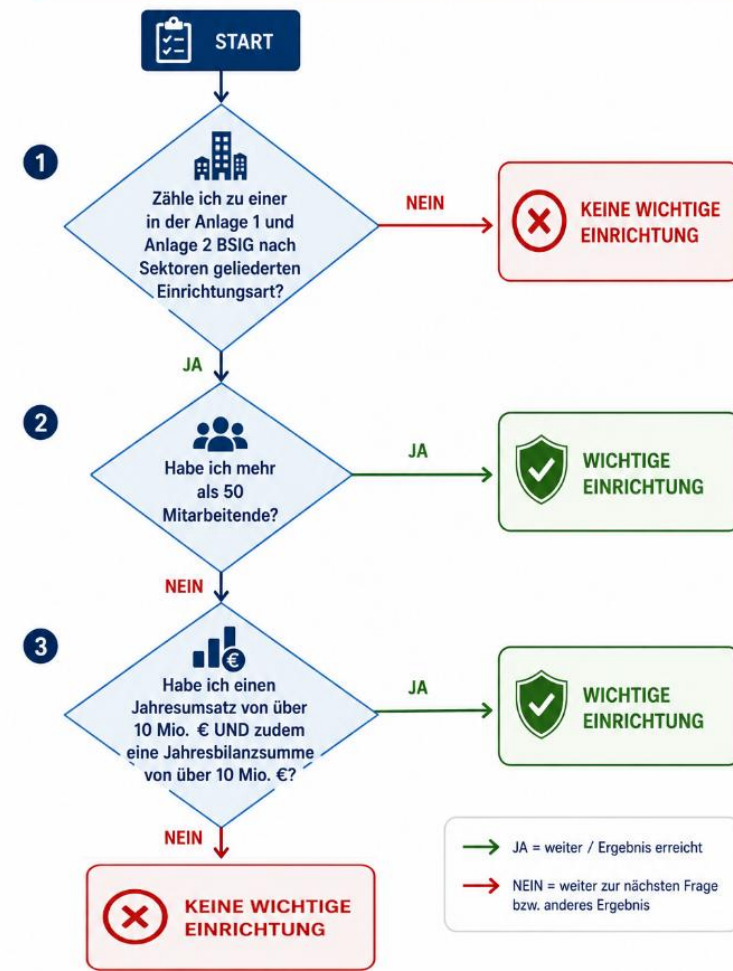


§28 - Sind Sie betroffen?

PRÜFUNG: BESONDERS WICHTIGE EINRICHTUNG



PRÜFUNG: WICHTIGE EINRICHTUNG





§33 Registrierungspflicht

§ 33 BSIG REGISTRIERUNGSPFLICHT

Besonders wichtige und wichtige Einrichtungen sowie Domain-Name-Registry-Diensteanbieter müssen sich beim BSI registrieren und die erforderlichen Angaben übermitteln.



FRIST
Spätestens 3 Monate,
nachdem sie erstmals oder
erneut als relevante Einrichtung
gelten oder Dienste anbieten.

**Nachmeldefrist
des BSI:
31.07.2026**

1 Name der Einrichtung
einschließlich Rechtsform
und ggf. Handelsregister-
nummer



**2 Anschrift und
Kontaktdaten**
inkl. E-Mail-Adresse, öffentliche
IP-Adressbereiche und
Telefonnummern



**3 Relevanter Sektor
oder Branche**
gemäß Anlage 1 oder 2



4 Mitgliedstaaten der EU
Auflistung der EU-Mitgliedstaaten,
in denen Dienste der in Anlage 1
oder 2 genannten Einrichtungsarten
erbracht werden



5 Zuständige Aufsichtsbehörden
des Bundes und der Länder für die
Tätigkeiten, aufgrund derer die
Registrierung erfolgt



(2) Zusätzliche Angaben für Betreiber kritischer Anlagen



Kritische
Dienstleistung



Typen von
kritischen
Komponenten



Öffentliche
IP-Adressbereiche



Anlagenkategorie
und Versorgungs-
kennzahlen



Standort
der Anlagen



Kontaktstelle
(erreichbar
jederzeit)



Die Angaben sind über die **gemeinsame Registrierungsmöglichkeit** des BSI und des BBK zu übermitteln.





§30 - Maßnahmen

NIS2 – Maßnahmen nach Absatz 1

Stand der Technik • Europäische & internationale Normen • Gefahrenübergreifender Ansatz

1 Risikoanalyse und Sicherheit in der Informationstechnik

- Identifikation von Risiken
- Bewertung und Priorisierung
- Maßnahmen zur Risikobehandlung
- Kontinuierliche Überwachung

2 Bewältigung von Sicherheitsvorfällen

- Erkennung und Analyse
- Meldung und Kommunikation
- Eindämmung und Beseitigung
- Nachbereitung und Lessons Learned

3 Aufrechterhaltung des Betriebs (Backup, Wiederherstellung & Krisenmanagement)

- Backup-Management
- Wiederherstellung nach Notfällen
- Notfall- und Krisenpläne
- Regelmäßige Tests und Übungen

4 Sicherheit der Lieferkette

Lieferant	Risika	Bewertung	Status
Cloud-Anbieter	Hoch	Hoch	✓
Softwarehersteller	Mittel	Hoch	✓
IT-Dienstleister	Mittel	Hoch	✓
Rechenzentrum	Mittel	Hoch	✓
Telekommunikation	Mittel	Hoch	✓

- Risikobewertung von Lieferanten
- Sicherheitsanforderungen & Verträge
- Lieferantenbewertung
- Kontinuierliche Überwachung

5 Sichere Entwicklung und Wartung

- Security by Design
- Schwachstellenmanagement
- Updates und Patches
- Sichere Konfigurationen

6 Bewertung der Wirksamkeit von Maßnahmen

- Überwachung und Kennzahlen
- Audits und Bewertungen
- Penetrationstests
- Kontinuierliche Verbesserung

7 Schulungen und Sensibilisierung

IT-SICHERHEIT GEHT UNS ALLE AN!

- Grundlagenschulungen
- Regelmäßige Awareness-Maßnahmen
- Phishing-Simulationen
- Sicherheitskultur fördern

8 Einsatz von kryptographischen Verfahren

- Verschlüsselung von Daten
- Sichere Protokolle und Algorithmen
- Schlüsselmanagement
- Sichere Speicherung

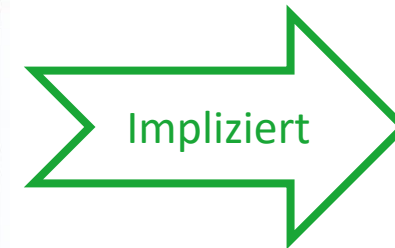
9 Sicherheit des Personals, Zugriffskontrolle & Verwaltung

Benutzer	Rolle
M. Müller	Administrator
S. Schneider	Fachbereich
T. Becker	Lesen
K. Weber	Lesen

- Zugriffskontrolle und Berechtigungen
- Identitäts- und Berechtigungsmanagement
- Verwaltung von IKT-Systemen
- Trennung von Aufgaben

10 Multi-Faktor-Authentifizierung & gesicherte Kommunikation

- Multi-Faktor-Authentifizierung
- Gesicherte Sprach-, Video- und Textkommunikation
- Notfallkommunikationssysteme





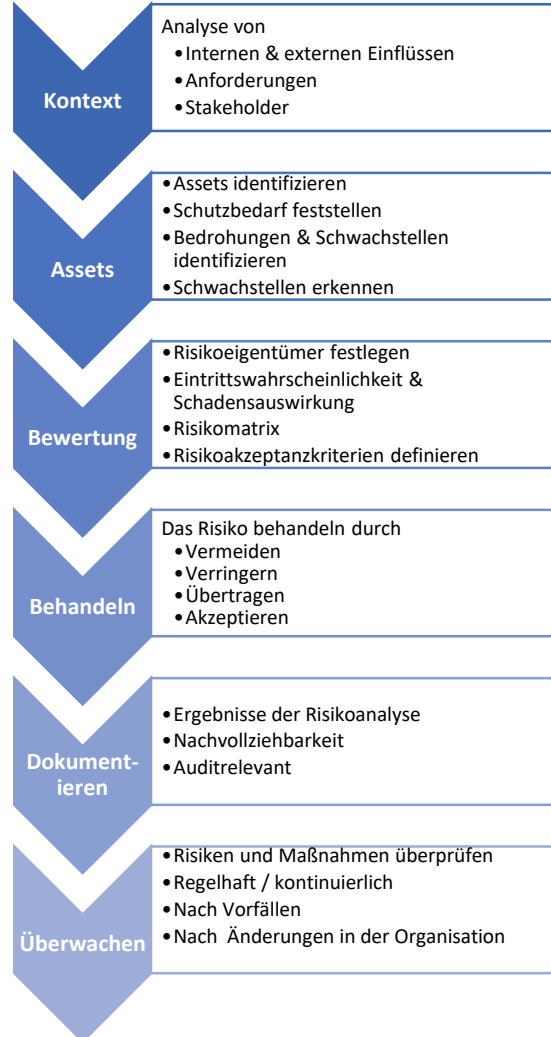
§30 – Maßnahmen

1 Risikoanalyse und Sicherheit in der Informationstechnik



- Identifikation von Risiken
- Bewertung und Priorisierung
- Maßnahmen zur Risikobehandlung
- Kontinuierliche Überwachung

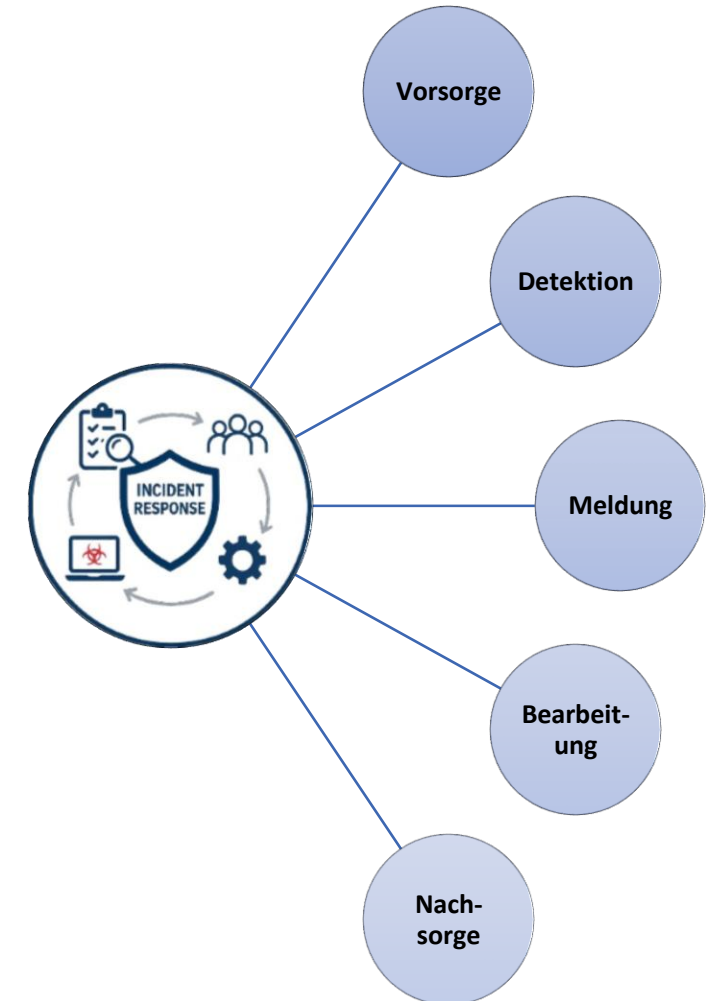
4 RISIKOBEHANDLUNGSMÖGLICHKEITEN



2 Bewältigung von Sicherheitsvorfällen



- Erkennung und Analyse
- Meldung und Kommunikation
- Eindämmung und Beseitigung
- Nachbereitung und Lessons Learned





§30 – Maßnahmen

3 Aufrechterhaltung des Betriebs (Backup, Wiederherstellung & Krisenmanagement)



- Backup-Management
- Wiederherstellung nach Notfällen
- Notfall- und Krisenpläne
- Regelmäßige Tests und Übungen

Business Continuity Management

Ziel: Der Geschäftsbetrieb wird bei Schadensereignissen nicht unterbrochen bzw. in einer angemessenen Zeit fortgesetzt

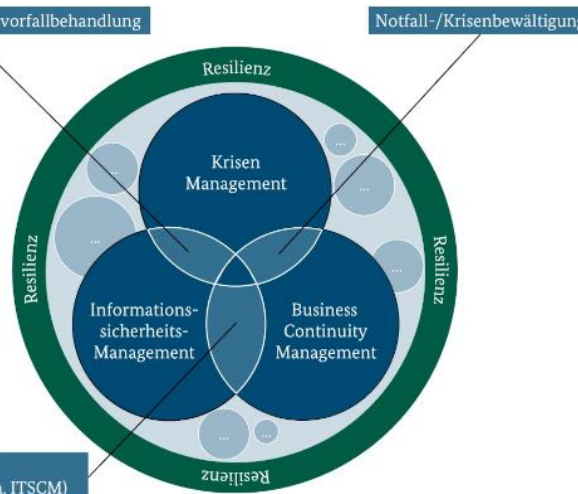
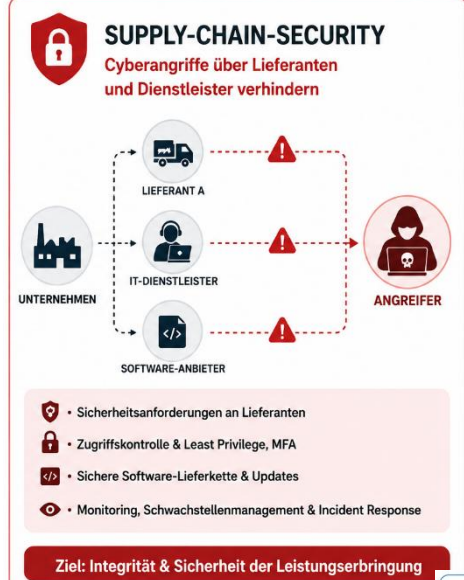
Erfordert organisatorische, technische, bauliche und personelle Maßnahmen

Siehe: BSI-Standard 200-4

4 Sicherheit der Lieferkette



- Risikobewertung von Lieferanten
- Sicherheitsanforderungen & Verträge
- Lieferantenbewertung
- Kontinuierliche Überwachung



Cyber-Supply Chain Risk Management (C-SCRM)





§30 – Maßnahmen

5 Sichere Entwicklung und Wartung



- Security by Design
- Schwachstellenmanagement
- Updates und Patches
- Sichere Konfigurationen



<https://wid.cert-bund.de/portal/wid/kurzinformationen>

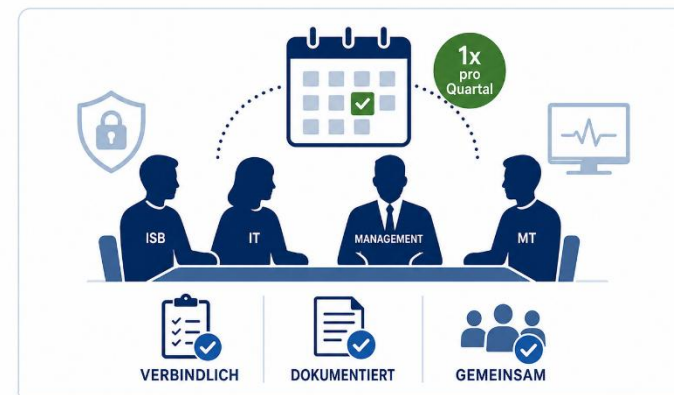
6 Bewertung der Wirksamkeit von Maßnahmen



- Überwachung und Kennzahlen
- Audits und Bewertungen
- Penetrationstests
- Kontinuierliche Verbesserung



Regelmäßiger
Managementtermin?





§30 – Maßnahmen

7 Schulungen und Sensibilisierung



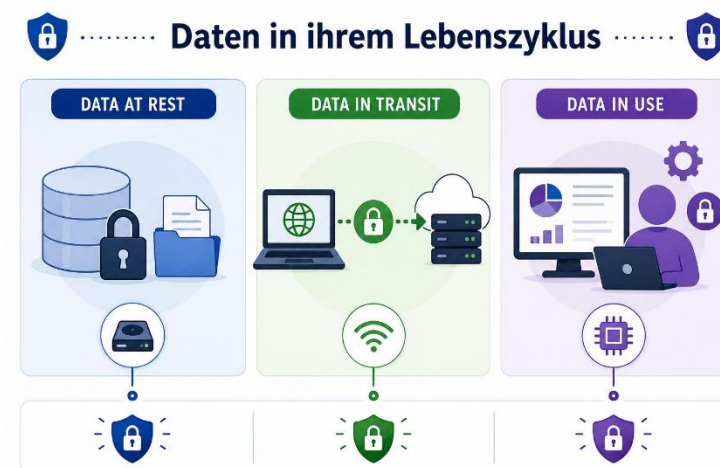
- Grundlagenschulungen
- Regelmäßige Awareness-Maßnahmen
- Phishing-Simulationen
- Sicherheitskultur fördern



8 Einsatz von kryptographischen Verfahren



- Verschlüsselung von Daten
- Sichere Protokolle und Algorithmen
- Schlüsselmanagement
- Sichere Speicherung





§30 – Maßnahmen

9 Sicherheit des Personals, Zugriffskontrolle & Verwaltung



- Zugriffskontrolle und Berechtigungen
- Identitäts- und Berechtigungsmanagement
- Verwaltung von IKT-Systemen
- Trennung von Aufgaben

SCHUTZZONENKONZEPT ZONIERUNG NACH SENSIBILITÄT UND SCHUTZBEDARF



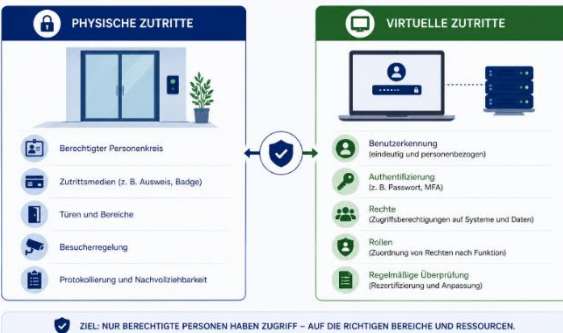
- ÖFFENTLICH**
 - Empfang, Wartebereich
 - Öffentlich zugängliche Bereiche
 - PATIENTENZIMMER**
 - Patientenzimmern
 - Schutz der Privatsphäre
 - BEHANDLUNGS- UND AMBULANZRÄUME**
 - Untersuchungsräume
 - Ambulanz
 - Funktionsräume
 - BÜROS**
 - Verwaltungsbereiche
 - Nicht-öffentliche Bereiche
 - OPS UND TECHNIKRÄUME**
 - Operationssäle
 - Sterilbereiche
 - Technische Betriebsräume
 - Hoher Schutzbedarf
- Je höher die Schutzbedürftigkeit, desto strenger die Zutrittskontrolle und Überwachung.

10 Multi-Faktor-Authentifizierung & gesicherte Kommunikation



- Multi-Faktor-Authentifizierung
- Gesicherte Sprach-, Video- und Textkommunikation
- Notfallkommunikationssysteme

ZUTRISSREGELUNGEN PHYSISCHE UND VIRTUELLE ZUTRISS



2FA – ZWEI-FAKTOR-AUTHENTIFIZIERUNG

Zwei verschiedene Faktoren müssen bereitgestellt werden, um Zugriff zu erhalten.



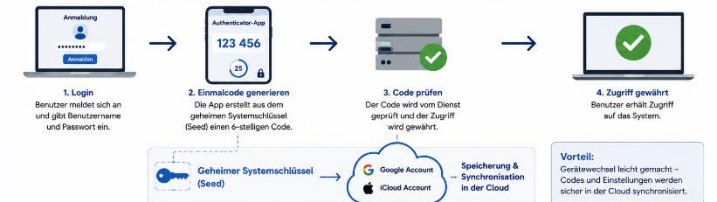
MFA – MULTI-FAKTOR-AUTHENTIFIZIERUNG

Drei oder mehr verschiedene Faktoren müssen bereitgestellt werden, um Zugriff zu erhalten.



AUTHENTICATOR-APPS: SO FUNKTIONIERT ES

Authenticator-Apps erzeugen Einmalcodes (TOTP) auf Basis eines geheimen Systemschlüssels (Seed).



DAS PROBLEM: CLOUD = ZUSÄTZLICHES RISIKO

Wird das Cloud-Konto kompromittiert, gelangt der Angreifer auch an den geheimen Systemschlüssel und kann Einmalcodes generieren – Zugriff auf alle geschützten Konten möglich.





§32 Meldepflichten in Detail

§32 Meldepflichten

Bei erheblichen Sicherheitsvorfällen gilt: 24 Stunden → 72 Stunden → 1 Monat



Meldepflicht für „erhebliche Sicherheitsvorfälle“



Die Meldefristen im Überblick



Interner Meldeweg – unsere Schritte



Aufgabe: schnell erkennen, transparente interne Meldewege, nachvollziehbare Bewertung, fristgerechte Meldung.



§38 – Pflichten GF

§38 Umsetzungs-, Überwachungs- und Schulungspflicht

für Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen

1 Umsetzungs- und Überwachungspflicht



Maßnahmen
umsetzen



Umsetzung
überwachen

2 Haftung bei Pflichtverletzung



Pflichtverletzung



Schaden der
Einrichtung



Haftung nach
Gesellschaftsrecht

3 Schulungspflicht



Risiken erkennen
und bewerten



Risikomanagement
verstehen



Auswirkungen
beurteilen



Regelmäßig
schulen





§61 – Rechte BSI

8

Weitere Anordnungen gegenüber besonders wichtigen Einrichtungen

1

Information der Betroffenen



Informieren Sie unverzüglich die betroffenen Personen.

2

Öffentliche Bekanntmachung von Verstößen



Machen Sie Verstöße nach den Vorgaben des BSI **öffentlich** bekannt.



Unterrichtspflichten bei einem akuten Vorfall gemäß § 35 BSIG beachten.

9

Durchsetzung bei Nichtbefolgung von Anordnungen



**Keine Empfehlung
Pflicht!**



Zusammenarbeit und Abstimmung



BSI



Aufsichtsbehörde

Mögliche Konsequenzen



**Entzug der
Betriebsgenehmigung**



Ausübungsverbot



§65 - Bußgelder

2 Bußgeldtatbestände (Beispiele)

Tatbestand	Rechtsgrundlage (§ 65 BSIG)	Höchst Bußgeld	
		Besonders wichtige Einrichtungen 	Wichtige Einrichtungen
 1 Verstöße gegen die Pflichten zur Umsetzung angemessener technischer und organisatorischer Maßnahmen (§ 30 Abs. 1)	§ 65 Nr. 1 BSIG	bis zu 10.000.000 € oder bis zu 2 % des weltweiten Jahresumsatzes	bis zu 7.000.000 € oder bis zu 1,4 % des weltweiten Jahresumsatzes
 2 Verstöße gegen die Meldepflichten bei Sicherheitsvorfällen (§§ 32, 33)	§ 65 Nr. 2 BSIG	bis zu 10.000.000 € oder bis zu 2 % des weltweiten Jahresumsatzes	bis zu 7.000.000 € oder bis zu 1,4 % des weltweiten Jahresumsatzes
 3 Verstöße gegen die Unterrichtspflichten (§§ 35, 36)	§ 65 Nr. 3 BSIG	bis zu 10.000.000 € oder bis zu 2 % des weltweiten Jahresumsatzes	bis zu 7.000.000 € oder bis zu 1,4 % des weltweiten Jahresumsatzes
 4 Verstöße gegen Mitwirkungs- und Auskunftspflichten gegenüber dem Bundesamt (§§ 60, 61)	§ 65 Nr. 4 BSIG	bis zu 10.000.000 € oder bis zu 2 % des weltweiten Jahresumsatzes	bis zu 7.000.000 € oder bis zu 1,4 % des weltweiten Jahresumsatzes
 5 Verstöße gegen die Pflichten zur Zertifizierung (§§ 56–58)	§ 65 Nr. 5 BSIG	bis zu 1.000.000 €	bis zu 500.000 €
 6 Verstöße gegen sonstige Pflichten nach diesem Gesetz	§ 65 Nr. 6 BSIG	bis zu 100.000 €	bis zu 500.000 €

Tatbestände 1–4: Für diese Tatbestände ordnet § 65 BSIG an, dass § 30 Abs. 2 Satz 3 OWiG anzuwenden ist. Das Höchstmaß der Geldbuße verzehnfacht sich bei einer Geldbuße gegen juristische Personen oder Personenvereinigungen.

Hinweis: Die Verhängung eines Bußgeldes erfolgt nach pflichtgemäßem Ermessen des Bundesamtes. Das Bundesamt berücksichtigt bei der Bemessung des Bußgeldes insbesondere die Schwere und Dauer der Zuwiderhandlung sowie den Verschuldensgrad.

Fazit

Das BSI ist bei
der
Cyberabwehr
nicht ihr Feind -
sondern ihr
Partner.



DIE WAHREN BÖSEN: HACKER & CYBERKRIMINELLE

- MALWARE
- PHISHING
- RANSOMWARE
- DATENDIEBSTAHL
- SYSTEMAUSFALL
- ERPRESSUNG

SCHULTERSCHLUSS FÜR CYBERABWEHR
BSI UND UNTERNEHMEN — GEMEINSAM STARK

WIR KÄMPFEN GEMEINSAM FÜR IHRE SICHERHEIT.

- PARTNERSCHAFT**
BSI und Unternehmen auf Augenhöhe
- PRAXISNAHE UNTERSTÜTZUNG**
Beratung, Hilfestellung und konkrete Lösungen
- WISSEN TEILEN**
Aktuelle Informationen, Warnungen und Best Practices
- VERNETZUNG**
Austausch in Communities und Branchen
- KOMPETENZEN STÄRKEN**
Schulungen, Tools und Sensibilisierung

DAS GESETZ ZWINGT ZU DEM, WAS VERANTWORTUNG EH UND JE ERFORDERT HAT.

-  Schutzpflichten erfüllen
Risiken erkennen und managen
-  Verantwortung übernehmen
für Unternehmen und Kunden
-  Zukunft sichern
durch Cybersicherheit

CYBERSICHERHEIT IST KEIN KOSTENFAKTOR. SONDERN VERTRUEN. STABILITÄT. ZUKUNFT.

-  SCHUTZ VON MENSCHEN, DATEN UND SYSTEMEN
-  AUSFÄLLE VERMEIDEN. GESCHÄFT SICHERN.
-  VERTRAUEN STÄRKEN. WETTBEWERBSFÄHIG BLEIBEN.
-  INNOVATION ERMÖGLICHEN. ZUKUNFT GESTALTEN.
-  VERANTWORTUNG WAHRNEHMEN.
-  GEMEINSAM MEHR ERREICHEN.

SICHERE UNTERNEHMEN. STARKE WIRTSCHAFT. VERTRAUEN SCHAFFEN. ZUKUNFT GESTALTEN.

Aber auch eine
mächtige
Behörde

Fazit

Es ist noch nie
ein Meister
vom Himmel
gefallen - nur
Übung macht
den Meister ...

Den Notfall üben statt **im Notfall üben**



ÜBUNG

- ✓ Alarmierung
- ✓ Kommunikation
- ✓ IT-Backup
- ✓ Notfallkontakte
- ✓ Abläufe

NOTFALLPLAN

- ✓ Alarmierung
- ✓ Kommunikation
- ✓ IT-Backup
- ✓ Notfallkontakte
- ✓ Abläufe

NETZWERKAUSFALL
Keine Verbindung zu Servern und Diensten

WAS TUN?

- IT anrufen?
- Technik?
- Geschäftsführung?
- Abwarten?

IT-SYSTEME NICHT VERFÜGBAR
Bitte warten Sie. Wir arbeiten an einer Lösung.

Sicherheit **Routine** **Schnelle Abläufe** **Schutz für Patienten & Personal** **Unklarheit** **Planlosigkeit** **Zeitverlust** **Risiken für Patienten & Personal**

Geben Sie Ihren
Mitarbeitenden
den Freiraum
zum üben.

Fazit

Schützen Sie Ihr
Krankenhaus
organisatorisch
und technisch!



Aber verlassen
Sie sich nicht zu
100% auf den
Schutz.
Planen Sie das
Scheitern ein
und sichern auf
interne Bereiche
gegeneinander
ab.

Vielen Dank für Ihre Aufmerksamkeit



Moderne **Technik**



Perfekte **Organisation**



Aufmerksame **Menschen**



Cyber**SICHER**heit!



Frank Ebling
ISB

Westpfalz-Klinikum GmbH
✉: febling@westpfalz-klinikum.de
☎: 0631 203 1121

Frank Ebling
✉: feb@hcc-isms.de

Hinweis gemäß EU AI Act, Art. 50: Diese Folien wurden mit KI-Unterstützung erstellt; Inhalte wurden fachlich geprüft.

Das BSI-G – eine Auswahl

Paragraph	QR-Code
Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen (BSI-Gesetz - BSI-G) - Inhaltsübersicht	
§ 2 Begriffsbestimmungen	
§ 28 Besonders wichtige Einrichtungen und wichtige Einrichtungen	
§ 30 Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen	
§ 31 Besondere Anforderungen an die Risikomanagementmaßnahmen von Betreibern kritischer Anlagen	
§ 32 Meldepflichten	
§ 33 Registrierungspflicht	
§ 35 Unterrichtungspflichten	

Paragraph	QR-Code
§ 38 Umsetzungs-, Überwachungs- und Schulungspflicht für Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen	
§ 39 Nachweispflichten für Betreiber kritischer Anlagen	
§ 41 Untersagung des Einsatzes kritischer Komponenten	
§ 61 Aufsichts- und Durchsetzungsmaßnahmen für besonders wichtige Einrichtungen	
§ 65 Bußgeldvorschriften	
Anlage 1: Sektoren besonders wichtiger und wichtiger Einrichtungen	
Anlage 2: Sektoren wichtiger Einrichtungen	

§32 Meldepflichten

§32 Meldepflichten

Meldung erheblicher Sicherheitsvorfälle

Wer muss melden?



Besonders wichtige Einrichtungen



Wichtige Einrichtungen

Gemeinsame Meldestelle



Bundesamt für Sicherheit in der Informationstechnik



Bundesamt für Bevölkerungsschutz und Katastrophenhilfe



Meldeweg eingerichtet

Die Verpflichtung nach Satz 1 gilt frühestens ab Einrichtung des Meldewegs.



Hinweis

Alle Meldungen sind über die gemeinsame Meldestelle an BSI und BBK zu übermitteln.

(1) Meldungen im Rahmen eines erheblichen Sicherheitsvorfalls

1 Frühe Erstmeldung



unverzüglich, spätestens innerhalb von 24 Stunden nach Kenntniserlangung

Angabe, ob der Verdacht besteht, dass der erhebliche Sicherheitsvorfall

- auf rechtswidrige oder böswillige Handlungen zurückzuführen ist oder
- grenzüberschreitende Auswirkungen haben könnte

2 Meldung über den Sicherheitsvorfall



unverzüglich, spätestens innerhalb von 72 Stunden nach Kenntniserlangung

Bestätigung oder Aktualisierung der in Nr. 1 genannten Informationen und

- erste Bewertung des erheblichen Sicherheitsvorfalls, einschließlich Schweregrad und Auswirkungen
- gegebenenfalls Angabe von Kompromittierungsindikatoren

3 Zwischenmeldung



auf Ersuchen des Bundesamtes

Übermittlung relevanter Statusaktualisierungen

4 Abschlussmeldung



spätestens binnen Monat nach Übermittlung der Meldung gemäß Nr. 2*

Enthält insbesondere:

- a) ausführliche Beschreibung des Sicherheitsvorfalls, einschließlich seines Schweregrads und Auswirkungen
- b) Angaben zur Art der Bedrohung beziehungsweise ihrer zugrunde liegenden Ursache
- c) Angaben zu den betroffenen und laufenden Abhilfemaßnahmen
- d) gegebenenfalls die grenzüberschreitenden Auswirkungen des Sicherheitsvorfalls

(2) Dauert der Sicherheitsvorfall zum Zeitpunkt der Abschlussmeldung noch an



Statt einer Abschlussmeldung ist eine Fortschrittsmeldung vorzulegen.



Fortschrittsmeldung enthält Informationen zum aktuellen Stand, ergriffene Maßnahmen und Ausblick.



Die Abschlussmeldung ist dem Bundesamt nach abschließender Bearbeitung des Sicherheitsvorfalls vorzulegen.



Ziel: Frühzeitige Information, wirksame Bewertung und koordinierte Reaktion zur Stärkung der Resilienz und Sicherheit.

<https://portal.bsi.bund.de/>

§32 Meldepflichten in Detail

§38 Umsetzungs-, Überwachungs- und Schulungspflicht für Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen

1 Umsetzungs- und Überwachungspflicht

Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen sind verpflichtet, die von diesen Einrichtungen nach § 30 zu ergreifenden Risikomanagementmaßnahmen umzusetzen und ihre Umsetzung zu überwachen.



Maßnahmen umsetzen

Die erforderlichen Risikomanagementmaßnahmen wirksam umsetzen.



Umsetzung überwachen

Die Wirksamkeit der Maßnahmen fortlaufend überwachen und bewerten.

2 Haftung bei Pflichtverletzung

Geschäftsleitungen, die ihre Pflichten nach Absatz 1 verletzen, haften ihrer Einrichtung für einen schuldhaft verursachten Schaden nach den auf die Rechtsform der Einrichtung anwendbaren Regeln des Gesellschaftsrechts.

Nach diesem Gesetz haften sie nur, wenn die für die Einrichtung maßgeblichen gesellschaftsrechtlichen Bestimmungen keine Haftungsregelung nach Satz 1 enthalten.



Pflichtverletzung
Verletzung der Pflichten aus Absatz 1.



Schaden der Einrichtung
Schadensersatz gegenüber der Einrichtung.



Haftung nach Gesellschaftsrecht
Haftung nach den auf die Rechtsform anwendbaren Regeln des Gesellschaftsrechts.



Eine Haftung nach diesem Gesetz besteht nur, wenn keine haftungsregelnden Bestimmungen im anwendbaren Gesellschaftsrecht enthalten sind.

3 Schulungspflicht

Die Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen müssen regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zu erlangen.



Risiken erkennen und bewerten

Fähigkeiten zur Erkennung und Bewertung von Risiken im Bereich der IT-Sicherheit.



Risikomanagement verstehen

Kenntnisse zu Risikomanagementpraktiken im Bereich der IT-Sicherheit.



Auswirkungen beurteilen

Die Auswirkungen von Risiken und Risikomanagementpraktiken auf die von der Einrichtung erbrachten Dienste beurteilen.



Regelmäßig schulen

Regelmäßige Teilnahme an Schulungen sicherstellen und Kenntnisse aktuell halten.



§61 – Rechte BSI

8 Weitere Anordnungen gegenüber besonders wichtigen Einrichtungen



Das Bundesamt



1 Unterrichtung betroffener Personen

Unterrichtung der natürlichen oder juristischen Personen, für die sie Dienste erbringen oder Tätigkeiten ausüben und die potenziell von einer erheblichen Cyberbedrohung betroffen sind

- über die Art der Bedrohung und mögliche Abwehr- oder Abhilfemaßnahmen, die diese Personen als Reaktion auf die Bedrohung ergreifen können.



2 Öffentliche Bekanntmachung von Verstößen

Informationen zu Verstößen gegen die in Absatz 1 genannten Verpflichtungen nach durch das Bundesamt bestimmten Vorgaben öffentlich bekannt zu machen.

9 Durchsetzung bei Nichtbefolgung von Anordnungen

Kommt eine Einrichtung trotz Fristsetzung den Anordnungen des Bundesamtes nicht nach,



kann das Bundesamt dies der zuständigen Aufsichtsbehörde mitteilen.

Die zuständige Aufsichtsbehörde kann, als letztes Mittel:



- 1 die erteilte Genehmigung nach dem jeweiligen Fachrecht vorübergehend ganz oder teilweise aussetzen.



- 2 unzuverlässigen Geschäftsleitungen die Ausübung der Tätigkeit, zu der sie berufen sind (§ 2 Nr. 13), vorübergehend untersagen.



Die Aussetzung nach Nummer 1 und die Untersagung nach Nummer 2 sind nur solange zulässig, bis die besonders wichtige Einrichtung den Anordnungen des Bundesamtes nachkommt, wegen deren Nichtbefolgung sie ausgesprochen wurden.

BSI - #nis2know-Infopakete

 Bundesamt
für Sicherheit in der
Informationstechnik

KONTAKT ENGLISH GEBÄRDENSPRACHE LEICHTE SPRACHE NUTZUNGSBEDINGUNGEN LOGIN

Deutschland
Digital-Sicher-BSI

Das BSI Themen IT-Sicherheitsvorfall Karriere Service **BSI-Portal** 🔍

Regulierte Wirtschaft > NIS-2-regulierte Unternehmen > #nis2know-Infopakete

#nis2know-Infopakete

#nis2know

Unter dem Hashtag #nis2know bietet das BSI den vom NIS-2-Umsetzungsgesetz betroffenen Einrichtungen Unterstützungsangebote in unterschiedlichen Formaten. Eines dieser Formate sind die #nis2know-Infopakete, in denen Unternehmen, kurz und verständlich aufbereitet, die wichtigsten Informationen zu spezifischen NIS-2-Themen finden.

Weitere Informationen

 Registrierungspflicht	 Mein Unternehmenskonto (MUK)	 NIS-2-Meldepflicht	 NIS-2 Risikoanalyse
 Sichere Lieferkette	 DORA und NIS-2	 NIS-2-Geschäftsleitungsschulung	 BCM
 Kryptografische Verfahren	 Risikomanagementmaßnahmen	 Incident Response	 Bewertung der Wirksamkeit von Maßnahmen

↑

https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-Infopakete/infopakete_node.html

 Bundesamt
für Sicherheit in der
Informationstechnik

KONTAKT ENGLISH GEBÄRDENSPRACHE LEICHTE SPRACHE NUTZUNGSBEDINGUNGEN LOGIN

Deutschland
Digital-Sicher-BSI

Das BSI Themen IT-Sicherheitsvorfall Karriere Service **BSI-Portal** 🔍

NIS-2-regulierte Unternehmen > #nis2know-Infopakete > Gesundheit

#nis2know: Gesundheitswesen

Informationen zur NIS-2-Betroffenheit im Gesundheitsbereich

#nis2know

- Was ändert sich mit NIS-2?
- Wer ist im Sektor Gesundheitswesen betroffen?
- Betreiber kritischer Anlagen
- Besonders wichtige und wichtige Einrichtungen
- Ausnahme für Einrichtungen der Langzeitpflege
- "Betrifft mich die Gesetzesänderung?" – Fallbeispiele zur Betroffenheit
- Ambulanzen
- Blutkonservenlagerung
- Hersteller von Medizinprodukten
- Homecare-Einrichtungen und Catering
- Homöopathie

https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-Infopakete/NIS-2-Gesundheit/NIS-2-Gesundheit_node.html

Openkritis

OpenKRITIS ist eine gemeinnützige Plattform für Kritische Infrastrukturen mit dem Ziel, regulierten Unternehmen neutrale Informationen zu NIS2, KRITIS und Cybersecurity bereitzustellen. Die Inhalte auf OpenKRITIS basieren auf öffentlichen Quellen, Gesetzen und Regulatorik sowie vielen Jahren Praxiserfahrungen bei Betreibern und in der Beratung.

Quelle: <https://www.openkritis.de/about.html>



<https://www.openkritis.de/>



KRITIS – auf den zweiten Blick

OpenKRITIS ist eine gemeinnützige Plattform für den Schutz Kritischer Infrastrukturen. Wir unterstützen Betreiber und Prüfer in der KRITIS und NIS2-Regulierung: Klare Strukturen zur Umsetzung von Cybersecurity, Governance und Prüfungen.



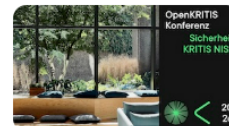
NIS2 und KRITIS

- Die **NIS2-Umsetzung** in Deutschland
- Neues **KRITIS-Dachgesetz** für Resilienz
- EU: **NIS2, CER, DORA, CSA** und **NCCS**
- **OpenKRITIS-School** und **Konferenz** für KRITIS
- OpenKRITIS **RSS, LinkedIn, News, Op-Eds**



Kritische Infrastrukturen

- Erste Schritte als **regulierte Einrichtung**
- **Registrierung** und **Meldepflicht** ans BSI
- Umsetzung **ISMS, BCMS, IT-Sicherheit**
- **Standards:** NIS2, CER & ISO 27001-Mappings
- Regulierte **Sektoren, Einrichtungen, Anlagen**



OpenKRITIS-Konferenz 2026: Sicherheit mit NIS2 und KRITIS

Die Umsetzung von NIS2 und KRITIS-Dachgesetz bei Betreibern

Konferenz • Vorträge & Diskussion • 28. September 2026 in Siegburg

BBK – Bundesamt für Bevölkerungsschutz und Katastrophenhilfe



The screenshot shows the BBK website with a navigation bar at the top containing links like 'Kontrast', 'English', and social media icons. The main banner features a large orange circle on the left with the text 'In Leichter Sprache: Vorsorge und Verhalten bei Hitze'. To the right of the circle is a photograph of a tree where the left side is green and the right side is bare, set against a background of a green field and a cracked, dry field. Below the main title, there is a short paragraph about hot days in Germany and a 'ZUM THEMA' button. At the bottom left of the banner area, there is a 'vorlesen' button with a speaker icon.

 **BBK**

In Leichter Sprache: Vorsorge und Verhalten bei Hitze

In Deutschland gibt es immer mehr heiße Tage. Das kann gefährlich für die Gesundheit sein. So können Sie sich vor Hitze schützen.

 **ZUM THEMA**

 **vorlesen** 



https://www.bbk.bund.de/DE/Home/home_node.html

BSI-Portal – Melde- und Registrierungsportal für NIS2-regulierte Unternehmen

Hinweis:

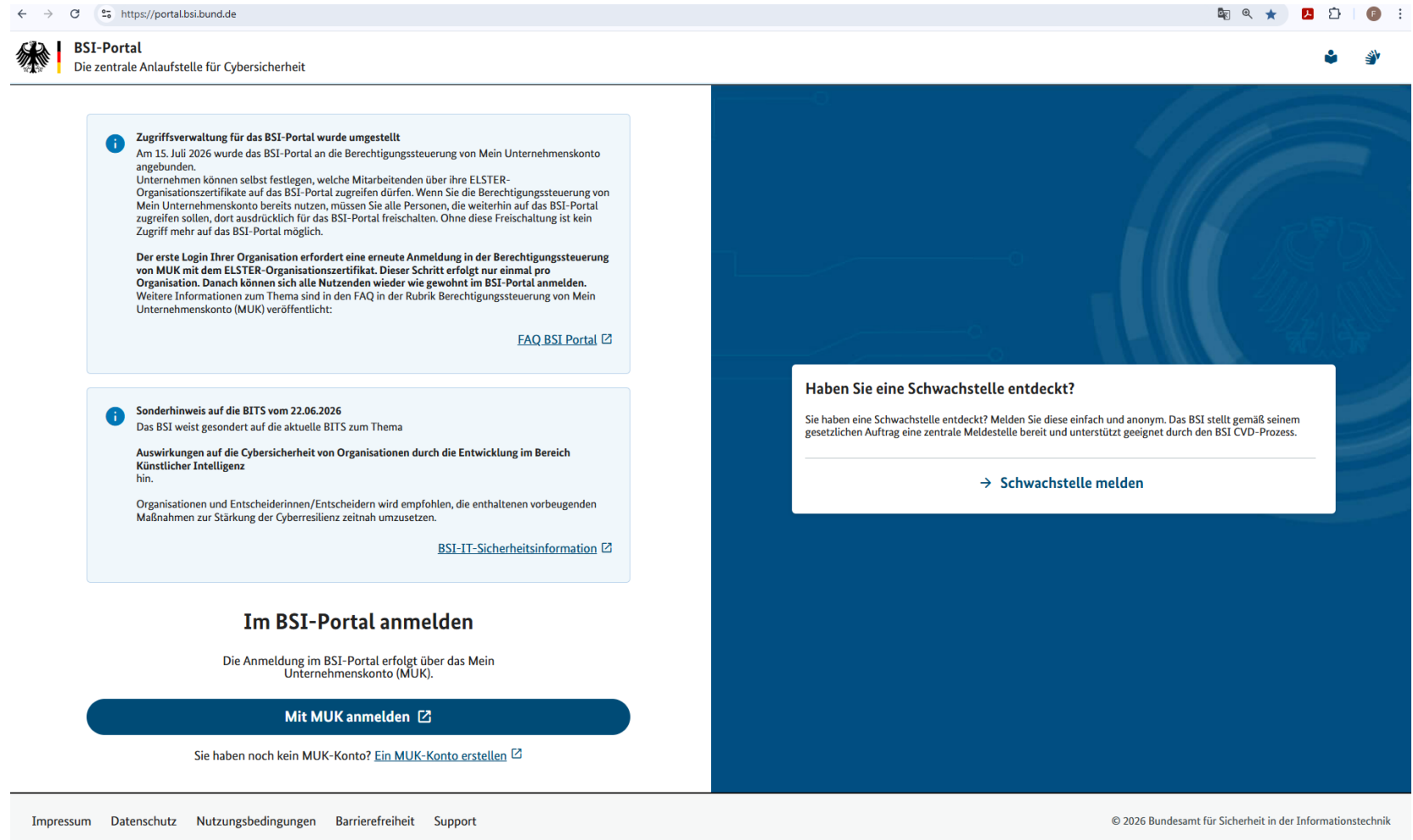
Die Anmeldung im BSI-Portal erfolgt über das Mein Unternehmenskonto (MUK) in Verbindung mit einem Elster-Unternehmenszertifikat.

Über den Link

„[Ein MUK-Konto erstellen](#)“ kann ein solches Konto bzw. das notwendige Zertifikat erstellt werden.



<https://portal.bsi.bund.de/>



The screenshot shows the BSI-Portal website. The header includes the BSI logo and the text "BSI-Portal Die zentrale Anlaufstelle für Cybersicherheit". The main content area has a blue background with white text. It features two informational boxes: one about access management changes and another about the BITS from 22.06.2026. Below these is a section titled "Im BSI-Portal anmelden" with instructions on how to register using a MUK account. A large button labeled "Mit MUK anmelden" is prominent. To the right, there is a white box titled "Haben Sie eine Schwachstelle entdeckt?" with a link to "Schwachstelle melden". The footer contains links for Impressum, Datenschutz, Nutzungsbedingungen, Barrierefreiheit, and Support, along with a copyright notice for 2026.

Zugriffsverwaltung für das BSI-Portal wurde umgestellt
Am 15. Juli 2026 wurde das BSI-Portal an die Berechtigungssteuerung von Mein Unternehmenskonto angebunden. Unternehmen können selbst festlegen, welche Mitarbeitenden über ihre ELSTER-Organisationszertifikate auf das BSI-Portal zugreifen dürfen. Wenn Sie die Berechtigungssteuerung von Mein Unternehmenskonto bereits nutzen, müssen Sie alle Personen, die weiterhin auf das BSI-Portal zugreifen sollen, dort ausdrücklich für das BSI-Portal freischalten. Ohne diese Freischaltung ist kein Zugriff mehr auf das BSI-Portal möglich.
Der erste Login Ihrer Organisation erfordert eine erneute Anmeldung in der Berechtigungssteuerung von MUK mit dem ELSTER-Organisationszertifikat. Dieser Schritt erfolgt nur einmal pro Organisation. Danach können sich alle Nutzenden wieder wie gewohnt im BSI-Portal anmelden. Weitere Informationen zum Thema sind in den FAQ in der Rubrik Berechtigungssteuerung von Mein Unternehmenskonto (MUK) veröffentlicht.
[FAQ BSI Portal](#)

Sonderhinweis auf die BITS vom 22.06.2026
Das BSI weist gesondert auf die aktuelle BITS zum Thema Auswirkungen auf die Cybersicherheit von Organisationen durch die Entwicklung im Bereich Künstlicher Intelligenz hin.
Organisationen und Entscheiderinnen/Entscheider wird empfohlen, die enthaltenen vorbeugenden Maßnahmen zur Stärkung der Cyberresilienz zeitnah umzusetzen.
[BSI-IT-Sicherheitsinformation](#)

Im BSI-Portal anmelden
Die Anmeldung im BSI-Portal erfolgt über das Mein Unternehmenskonto (MUK).
Mit MUK anmelden
Sie haben noch kein MUK-Konto? [Ein MUK-Konto erstellen](#)

Haben Sie eine Schwachstelle entdeckt?
Sie haben eine Schwachstelle entdeckt? Melden Sie diese einfach und anonym. Das BSI stellt gemäß seinem gesetzlichen Auftrag eine zentrale Meldestelle bereit und unterstützt geeignet durch den BSI CVD-Prozess.
[→ Schwachstelle melden](#)

Impressum Datenschutz Nutzungsbedingungen Barrierefreiheit Support

© 2026 Bundesamt für Sicherheit in der Informationstechnik